



# dahua PFS3220-16GT-240 PoE Switch 16-24-Port Unmanaged Desktop Switch User Guide

[Home](#) » [Dahua](#) » dahua PFS3220-16GT-240 PoE Switch 16-24-Port Unmanaged Desktop Switch User Guide 

## dahua PFS3220-16GT-240 PoE Switch 16-24-Port Unmanaged Desktop Switch User Guide



### Contents

- [1 Foreword](#)
- [2 Important Safeguards and Warnings](#)
- [3 Overview](#)
- [4 Port and Indicator](#)
- [5 Installation](#)
- [6 Wiring](#)
- [7 Appendix 1 Cybersecurity](#)
- [Recommendations](#)
- [8 Documents / Resources](#)
- [9 Related Posts](#)






## Foreword

### General

This manual mainly introduces the hardware, installation, and wiring steps of the 16/24-port unmanaged desktop switch (hereinafter referred to as “the device”).

## Safety Instructions

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 <b>Danger</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>Warning</b>	Indicates a medium or low potential hazard which, if not avoided, could result in a slight or moderate injury.
 <b>Caution</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 <b>Tips</b>	Provides methods to help you solve a problem or save time.
 <b>Note</b>	Provides additional information as a supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.1	Updated the long distance description.	August 2023
V1.0.0	First release.	June 2021

## Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car 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's 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.

## **Important Safeguards and Warnings**

This manual was designed to help you use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you keep the manual for future reference.

## **Operation Requirements**

- Transport, use, and store the device in allowed humidity and temperature ranges.
- Avoid liquids splashing on the device. Do not place objects full of liquid on the device to avoid liquid flowing into the device.
- Do not disassemble the device without professional instruction.
- Use the device at rated input and output voltage.
- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- When removing the cable, power off the device first to avoid personal injury.
- Operating temperature range:  $-10^{\circ}\text{C}$  to  $+55^{\circ}\text{C}$ .
- This is a class A product. In a domestic environment this may cause radio interference in which case the user may be required to take adequate measures.

## **Installation Requirements**

- Observe all safety procedures and wear required protective equipment provided for your use while working at height.
- Use the battery properly to avoid fire, explosions, and other dangers.
- Do not expose the device directly to sunlight, and keep it away from heat.
- Do not install the device in a damp environment, and keep it away from dust and soot.
- Install the device in a well-ventilated environment. Do not block the vent of the device.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to power requirements of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Connect the device with the adapter before power on.
- Do not connect the device to more than one power supply. Otherwise, the device might be damaged.
- 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.
- Be sure to ground the device (cross section of copper wire:  $> 2.5\text{ mm}^2$ ; resistance to ground:  $\leq 4\ \Omega$ ).
- Voltage stabilizers and lightning protection devices are optional according to the power supply and surrounding

environment.

- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Do not block the ventilator of the device with objects, such as newspaper, table cloth or curtains.
- Do not put open flames, such as a lit candle, on the device.

## Maintenance Requirements

- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

## Overview

### Introduction

The device is a layer-2 commercial switch. It provides a high-performance switching engine and large buffer memory to ensure smooth video stream transmission. With a full-metal design, the device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from  $-10^{\circ}\text{C}$  to  $+55^{\circ}\text{C}$ . With its DIP design, it provides a variety of work modes that suit different scenarios. The device also supports power consumption management, which allows it to adapt to fluctuations in the power consumption of terminal devices. This ensures stable operation.

The device is applicable for use in different scenarios, including homes, offices, small malls and on server farms.

### Features

- 16/24 × 10/100 Mbps or 10/100/1000 Mbps PoE Ethernet port.

All ports meet the requirements of IEEE802.3af and IEEE802.3at standards. The red ports also conform with Hi-PoE and IEEE802.3bt standards, and the orange ports conform with Hi-PoE standard.

- Desktop PoE Switch series support 250 m long-distance PoE transmissions, which can be enabled by DIP switch.



In Extend Mode, the transmission distance of the PoE port is up to 250 m but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.

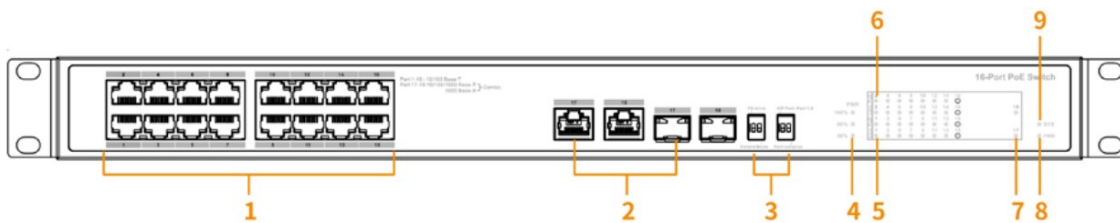
- Desktop PoE Switch series support PoE watchdog for real-time detection of terminal device status.
- Power consumption management.
- Desktop mount and rack mount.

### Port and Indicator

#### Front Panel

The following figure is for reference only, and might differ from the actual product.

**Figure 2-1 Front panel**



Following are all the ports and indicators on the front panel of the 16/24-port unmanaged desktop switch. The actual device might only have some of these ports and indicators.

**Table 2-1 Description of front panel**

No.	Description
1	10/100 Mbps or 10/100/1000 Mbps self-adaptive PoE Ethernet ports.
2	Uplink port, including 10/100/1000 Mbps self-adaptive Ethernet port and 1000 Mbps optical port.
3	<p><b>DIP switch</b></p> <ul style="list-style-type: none"> <li>• <b>PD Alive (PoE Watchdog):</b> When a terminal device crash is detected, power down and restart the terminal device.</li> <li>• <b>Extend Mode:</b> Extends the maximum transmission distance to 250 m, but reduces average transmission speed to 10 Mbps. In Extend Mode, the transmission distance of the PoE port is up to 250 m but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.</li> <li>• <b>VIP Port:</b> Enable the QoS mode through the DIP switch to achieve priority transmission of corresponding Ethernet ports.</li> <li>• <b>Port Isolation:</b> The port isolation mode can be enabled through the DIP switch. When this function is enabled, the downlink ports are independent, the flow is not interoperable, and the downlink port and uplink port can communicate with each other.</li> </ul> <p>Only supported by some models.</p>
4	<p><b>PoE output power indicator</b></p> <ul style="list-style-type: none"> <li>• <b>Solid green:</b> Total power <math>\leq 50\%</math>.</li> <li>• <b>Solid green and yellow:</b> <math>50\% &lt; \text{total power} \leq 80\%</math>.</li> <li>• <b>Solid green, yellow and red:</b> <math>80\% &lt; \text{total power}</math>.</li> </ul>
5	<p><b>Single-port connection status indicator (Link)</b></p> <ul style="list-style-type: none"> <li>• <b>On:</b> Connected to device.</li> <li>• <b>Off:</b> Not connected to device.</li> </ul>
6	<p><b>PoE port status indicator</b></p> <ul style="list-style-type: none"> <li>• <b>On:</b> Powered by PoE.</li> <li>• <b>Off:</b> Not powered by PoE.</li> </ul>

7	<b>Uplink port connection status indicator (Link)</b> <ul style="list-style-type: none"> <li>• <b>On:</b> Connected to device.</li> <li>• <b>Off:</b> Not connected to device.</li> </ul>
8	<b>System status indicator (SYS)</b> <ul style="list-style-type: none"> <li>• <b>Flashing:</b> Operation is normal.</li> <li>• <b>Off:</b> Operation is not normal.</li> </ul>
9	<b>Power indicator</b> <ul style="list-style-type: none"> <li>• <b>On:</b> Power on.</li> <li>• <b>Off:</b> Power off.</li> </ul>

## Rear Panel

The following figure is for reference only, and might differ from the actual product.

**Figure 2-2 Rear panel**



**Table 2-2 Description of rear panel**

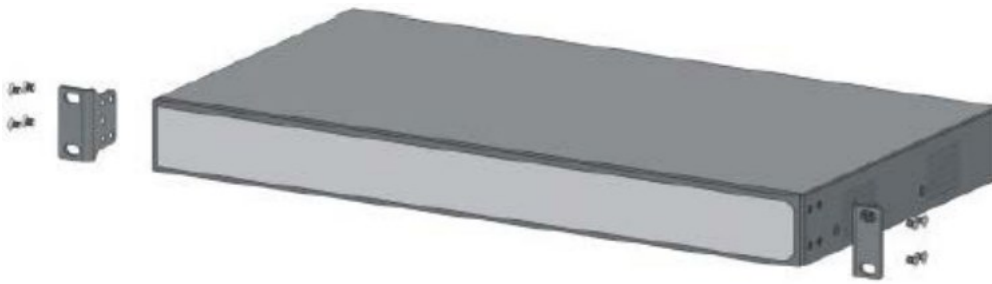
No.	Description
1	Power switch.
2	Power port, supports 100 –240 VAC.
3	Ground terminal.

## Installation

The device supports rack mount.

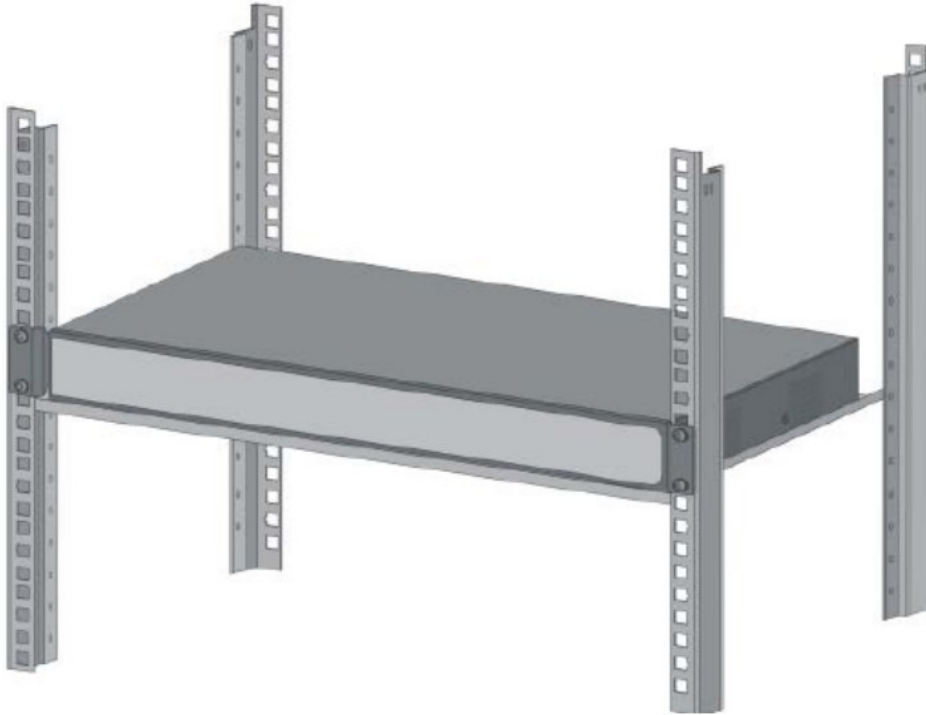
**Step 1** Attach the mounting bracket to the device side panel (one on each side) and secure it with the screws provided with the rack.

**Figure 3-1 Install bracket**



**Step 2** Attach the device to the rack with screws.

**Figure 3-2 Install device**



## Wiring

### Connecting GND

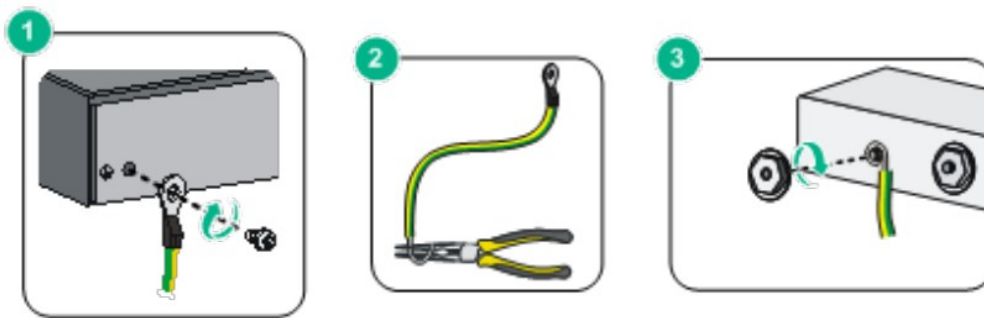
Normal GND connection of the device guarantees device lightning protection and anti-interference.

**Step 1** Remove the ground screw from the device and pass the ground screw through the round hole of the OT terminal of the ground cable. Turn the ground screw clockwise with a cross screwdriver to fasten the OT terminal of the ground cable.

**Step 2** Wind the other end of the ground cable into a circle with the needle-nose pliers.

**Step 3** Connect the other end of the ground cable to the ground bar, then turn the hex nut clockwise with a wrench to fasten the other end of the ground cable to the ground terminal.

**Figure 4-1 Connect GND**



## Connecting Power Cord

Before connecting the power cord, make sure that the device is securely grounded.

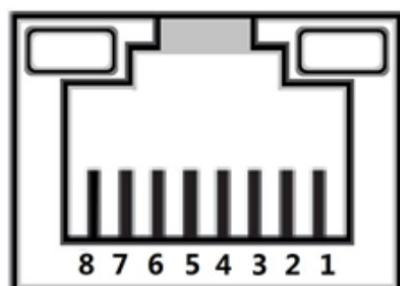
**Step 1** Connect one end of the power cord to the power jack of the device.

**Step 2** Connect the other end of the power cord to the external power socket.

## Connecting Ethernet Port

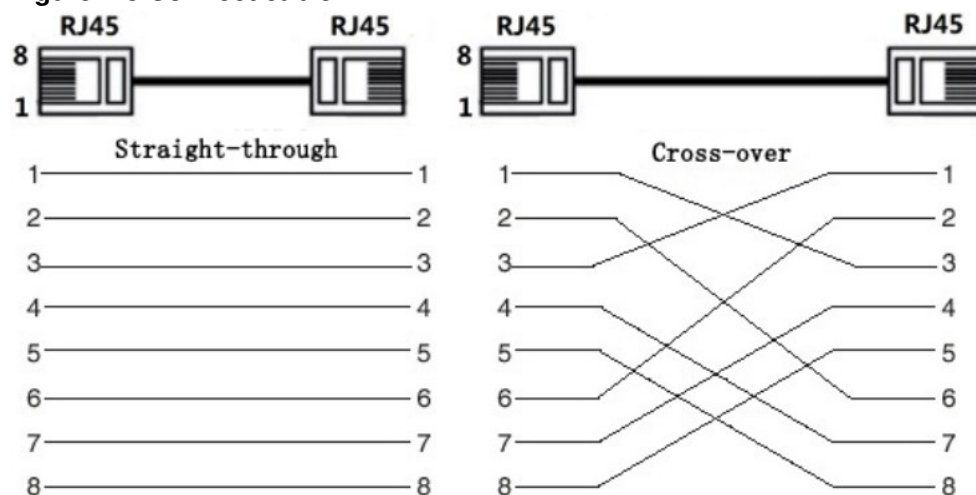
Ethernet port is a standard RJ-45 port. With its self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use cross-over cables or straight-through cables to connect the terminal device to the network device.

**Figure 4-2 Ethernet port pin number**



The cable connection of RJ-45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

**Figure 4-3 Connect cable**





## Connecting SFP Ethernet Port

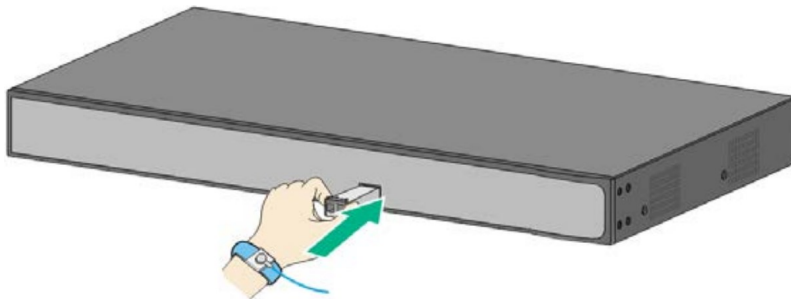
- When installing the SFP optical module, do not touch the gold finger of the SFP optical module.
  - Do not remove the dust plug of the SFP optical module before connecting the optical fiber.
  - Do not directly insert the SFP optical module into the slot while the optical fiber is inserted in it.
- Unplug the optical fiber before installing it.

**Step 1** Wear the antistatic wrist band, and confirm that the antistatic wrist band is in good contact with your skin and the device is reliably grounded.

**Step 2** Turn up the handle of the SFP optical module vertically and hold the optical module on both sides with your hands.

**Step 3** Push the optical module gently into the slot in the horizontal direction until the SFP optical module is firmly connected to the slot.

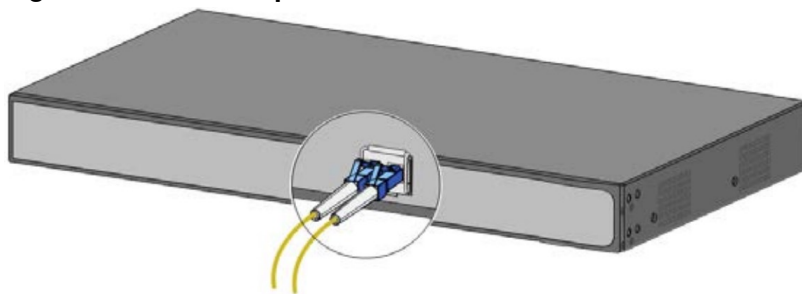
**Figure 4-4 Install SFP module**



**Step 4** Remove the dust cap of the LC connector of the optical fiber and the dust plug of the SFP optical module.

**Step 5** Connect the LC connector of the optical fiber to the SFP optical module.

**Figure 4-5 Connect optical fiber**



## Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect this port to the switch PoE Ethernet port through the network cable to achieve synchronized network connection and power supply. The maximum distance between the switch and the terminal device is about 100 m.



When connecting to a non-PoE device, the device needs to be used with an isolated power supply

## 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 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.

## **Documents / Resources**

PoE Switch (16/24-port Unmanaged  
Desktop Switch)  
Quick Start Guide



10231

## [dahua PFS3220-16GT-240 PoE Switch 16-24-Port Unmanaged Desktop Switch](#) [pdf] User Guide

PFS3220-16GT-240 PoE Switch 16-24-Port Unmanaged Desktop Switch, PFS3220-16GT-240, PoE Switch 16-24-Port Unmanaged Desktop Switch, 16-24-Port Unmanaged Desktop Switch, Unmanaged Desktop Switch, Desktop Switch, Switch