**Manuals+** — User Manuals Simplified.

# dahua CS4218-16ET-135 Ethernet Cloud Managed PoE Switch User Guide

**Ethernet Switch
(Cloud Managed PoE Switch)
Quick Start Guide**

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

**Contents**

## Foreword

**General**
This manual introduces the installation, functions and operations of the cloud managed switch (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe 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 the usage mode. | July 2024 |
| V1.0.0 | First release. | January 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'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 section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

⚠ Transport the device under allowed humidity and temperature conditions.

Storage Requirements

⚠ Store the device under allowed humidity and temperature conditions.

### Installation Requirements

⚠ **DANGER**

Stability Hazard
Possible result: The device might fall down and cause serious personal injury.
Preventive measures (including but not limited to):

- Only use furniture and structures that can safely support the device.
- Carefully arrange the cables connected to the device to avoid people tripping over them and pulling on them.

⚠ WARNING

- 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.
- Please follow the electrical requirements to power the device.

◊ Following are the requirements for selecting a power adapter.
○ The power supply must conform to the requirements of IEC 60950-1 ans IEC 62368-1 standards.
○ The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
○ When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
◊ We recommend using the power adapter provided with the device.
◊ When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

⚠

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.

- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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 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.

**Operation Requirements**

⚠️ DANGER

- ⚠️ The device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.
  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.
  Preventive measures (including but not limited to):
  ◊ Keep new and used batteries out of reach of children.
  ◊ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  ◊ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions
  Preventive measures (including but not limited to):
  ◊ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  ◊ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  ◊ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  ◊ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

⚠️ 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.

⚠

- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: –10 °C to +55 °C (+14 °F to +131 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

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.

## Overview

### 1.1 Introduction

The Cloud managed device is a layer-2 commercial device. With a full-metal design, the Device has great heat dissipation capabilities on its shell surface, and is able to work in environments that range from –10 °C to +55 °C (+14 °F to +131 °F).
In addition, based on the DoLynk Care Cloud Server, the Device can be managed through the DoLynk Care app or webpage, the network topology diagram function can be used to quickly locate the problem. The cloud managed switch supports management through an on-premises web interface. The Device is applicable in different scenarios, including buildings, homes, factories and offices.

### 1.2 Features

- Features mobile management by app.
- Supports network topology visualization.
- Supports one-stop maintenance.
- The gray ports conform with IEEE802.3af and IEEE802.3at standards, the orange ports conform with Hi-PoE or IEEE802.3bt standard and the red ports conform with IEEE802.3bt standards.
- Supports LLDP (Link Layer Discovery Protocol).

- Supports DHCP (Dynamic Host Configuration Protocol) Client.

- Supports VLAN configuration based on IEEE802.1Q.

- STP/RSTP is available on select models.

- Manual link aggregation is available on select models.

- Supports long-distance power supply.

- Desktop mount and rack mount for 16/24 port. Desktop mount and wall mount for 4/8 port.

## Port and Indicator

### 2.1 Front Panel
### 2.1.1 Front Panel (4/8-port)
The following figure uses an 8-port 100 Mbps cloud managed device as an example, and might differ from the actual product.
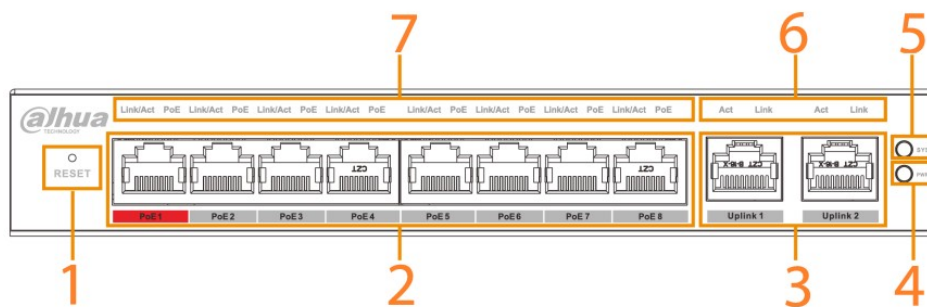


Figure 2-1 Front panel (4/8-port)

Table 2-1 Description of front panel (4/8-port)

| No. | Name | Description |
|---|---|---|
| 1 | Reset button | Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the Device to default settings. |
| 2 | PoE ports | 4/8 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive PoE Ethernet ports. |
| 3 | Uplink ports | 10/100/1000 Mbps self-adaptive Ethernet ports.<br>● The number of the uplink ports might differ from different models. Please refer to the actual product.<br>● Some models support 1000 Mbps optical ports. Please refer to the actual product. |
| 4 | Power indicator | ● On: Power on.<br>● Off: Power off. |
| 5 | System status indicator (SYS) | Flashes: The system works normally. |
| 6 | Uplink port status indicators | Link indicator.<br>● On: Connected to the Device.<br>● Off: Not connected to the Device. |
| | | Activity indicator.<br>● Flashing: Transmitting data.<br>● Off: Not transmitting data. |
| 7 | PoE port status indicators | PoE port status indicator.<br>● On: Powered by PoE.<br>● Off: Not powered by PoE. |
| | Link/Act indicator | Link/Act indicator.<br>● On: Connected to the Device.<br>● Off: Not connected to the Device.<br>● Flashing: Transmitting data. |

### 2.1.2 Front Panel (16/24-port)

The following figure uses a 16-port 100 Mbps cloud managed device as an example, and might differ from the actual product.
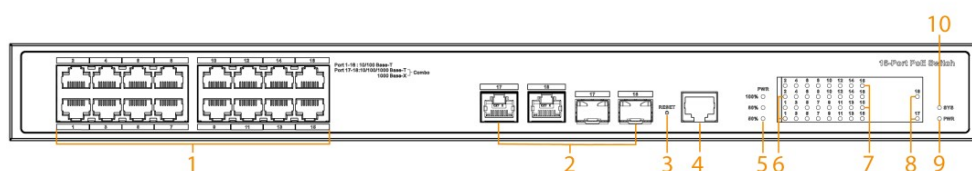
Figure 2-2 Front panel (16/24-port)



Table 2-2 Description of front panel (16/24-port)

| No. | Name | Description |
|---|---|---|
| 1 | PoE ports | 16/24 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports. |
| 2 | Uplink ports | 10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical ports. The uplink ports are combo ports on select models. |
| 3 | Reset button | Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the Device to default settings. |
| 4 | Console serial port | Device debugging port.<br>Only supported by select models. |
| 5 | PoE output power indicator | ● On: Connected to device.<br>● Off: Not connected to device.<br>● Flashing: Transmitting data. |
| 6 | Link/Act indicator | ● On: Connected to the Device.<br>● Off: Not connected to the Device.<br>● Flashing: Transmitting data. |
| 7 | PoE port status indicators | ● On: Powered by PoE.<br>● Off: Not powered by PoE. |
| 8 | Uplink port status (Link) indicators | ● On: Connected to device.<br>● Off: Not connected to device. |
| 9 | Power indicator | ● On: Power on.<br>●Off: Power off. |
| 10 | System status indicator (SYS) | Flashes: The system works normally. |

**2.2 Rear Panel**
**2.2.1 Rear Panel (4/8-port)**

📖

The figures might differ from different models. Please refer to the actual product.

Figure 2-3 Rear panel (4/8 port)



Table 2-3 Description of rear panel (4/8 port)

| No. | Name | Description |
|---|---|---|
| 1 | Ground terminal | Connecting GND.<br>● Normal GND connection of the Device guarantees device lightning protection and anti-interference. You must connect the GND cable before powering on the Device and power off the Device before disconnecting the GND cable.<br>● The sectional area of the GND cable must be more than 2.5 mm2, and the GND resistance must be less than 4 Ω. |
| 2 | Power port | Supports 53 VDC or 54 VDC. |

## 2.2.2 Rear Panel (16/24-port)

📖

The figures might differ from different models. Please refer to the actual product.

Figure 2-4 Rear panel (16/24 port)



Table 2-4 Description of rear panel (16/24 port)

| No. | Name | Description |
|---|---|---|
| 1 | DIP switch | Supported by select models. |
| 2 | Power port | Supports 100–240 VAC. |
| 3 | Ground terminal | Connecting GND.<br>📖<br>● Normal GND connection of the Device guarantees device lightning protection and anti-interference. You must connect the GND cable before powering on the Device and power off the Device before disconnecting the GND cable.<br>● The sectional area of the GND cable must be more than 2.5 mm2, and the GND resistance must be less than 4 Ω. |

## Installation

Different installation methods suit for different models. Please select appropriate methods as needed.

### 3.1 Preparation

- Select an appropriate installation method as needed.
- Install the Device on a solid and flat surface.
- Leave around 10 cm of open space around the Device for heat dissipation and to ensure good ventilation.

### 3.2 Desktop Mount
The Device supports desktop mount. You can directly place it on a solid and flat desktop.
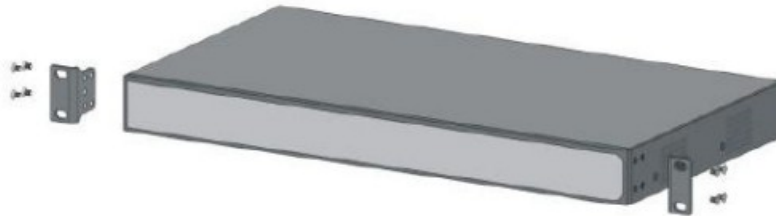
### 3.3 Rack Mount

The Device supports rack mount.

**Procedure**
**Step 1**

Attach the mounting brackets to the Device (one on each side), and fix them with the provided screws.
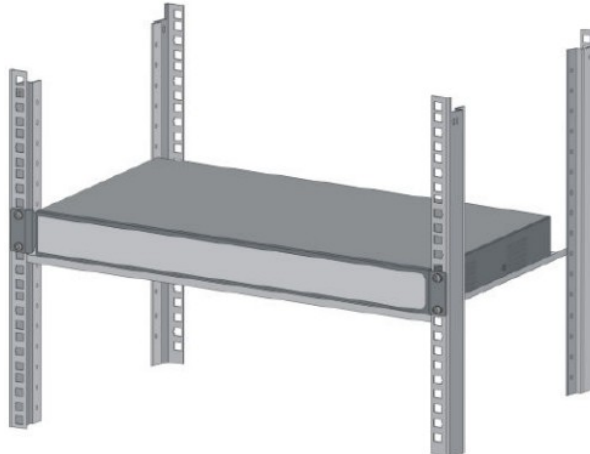
Figure 3-1 Attach the mounting brackets



**Step 2**

Fix the Device onto the rack.

Figure 3-2 Fix the Device onto the rack



### 3.4 Wall Mount

Procedure
**Step 1**

Drill two M4 screws into the wall, leaving a space of 4 mm between the wall and the head of the screw.
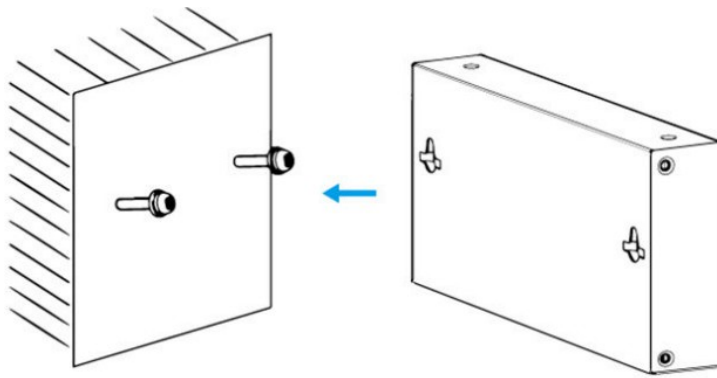
- Screws do not come with the package. Purchase them as needed.
- Make sure that the distance between the screws is the distance between the wallmount holes (77.8 mm for a 4-port switch and 128.4 mm for an 8-port switch).

**Step 2**

Align the wall-mount holes on the back cover of the Device with the screws, and hang the Device on the screws.

Figure 3-3 Wall mount

## Wiring

### 4.1 Connecting GND Cable
Background Information
Normal GND connection of the Device is the important guarantee for Device lightning protection and anti-interference.

### Procedure
**Step 1**
Remove the ground screw on the Device and place it properly. 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.
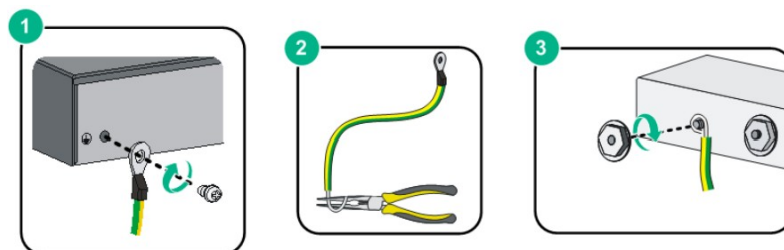**Step 2**
Wind the other end of the ground cable into a circle with needle-nose pliers.
**Step 3**
Connect the other end of the ground cable to the ground bar, turn the hex nut clockwise with a wrench to fasten the other end of the ground cable to the ground terminal.

Figure 4-1 Connect GND



### 4.2 Connecting Power Cord
**Background Information**
Before connecting the power cord, make sure that the Device is reliably grounded.
Procedure

**Step 1** Connect one end of the power cord into the power jack of the Device accurately.
**Step 2** Connect the other end of the power cord to the external power socket.

### 4.3 Connecting Ethernet Port
Ethernet port adopts standard RJ-45 port. With 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 cable or straight-through cable to connect terminal device to network device.
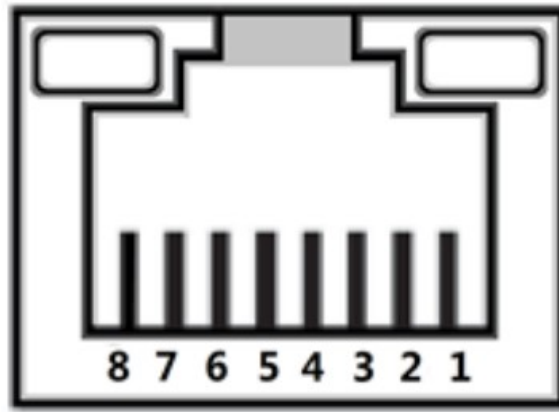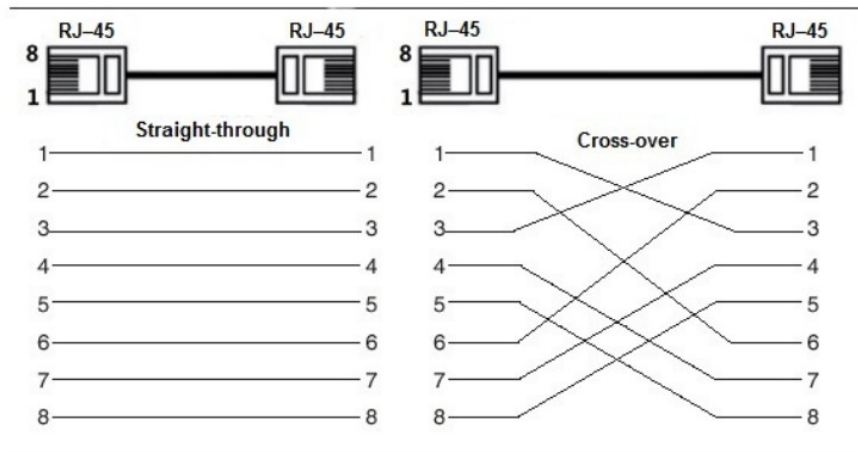
Figure 4-2 Ethernet port pin number

Figure 4-3 Pin description



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).

## 4.4 Connecting SFP Ethernet Port

 WARNING

- 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.

**Procedure**
**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
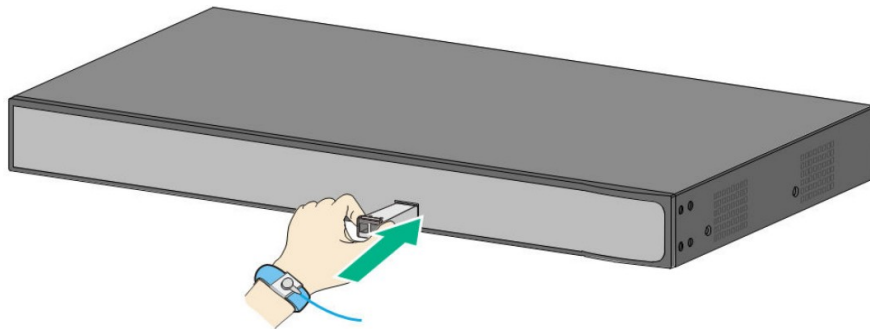
**Step 4** Remove the dust cap of the LC connector of the optical fiber and the dust plug of the SFP optical module.
**Step 5** Connect the LC connector of the optical fiber to the SFP optical module.

Figure 4-5 Connect optical fiber
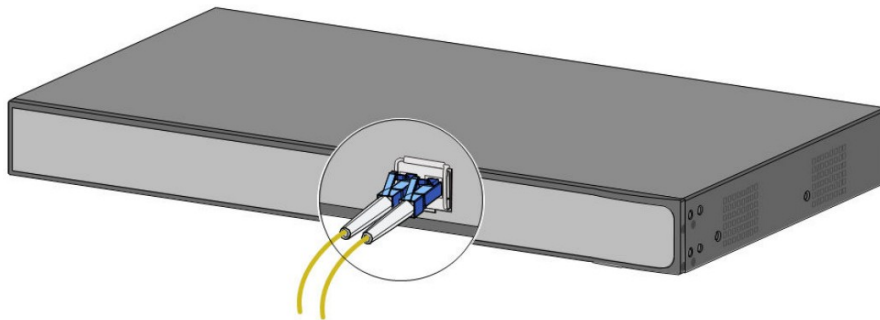


## 4.5 Connecting PoE Ethernet Port
You can directly connect the Device PoE Ethernet port to the switch PoE Ethernet port through network cable to achieve synchronized network connection and power supply. With Extend Mode disabled, the maximum distance between the switch and the Device is about 100 m.

⚠️

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

## Usage Mode

### 5.1 Managing the Device by Cloud Management
The cloud managed switch supports device management through the DoLynk Care app and webpage.

### 5.1.1 Managing the Device by DoLynk Care App
Prerequisites

- Make sure that the Device is connected to the power and the network before adding the Device.
- Make sure you have downloaded the DoLynk Care app.

Figure 5-1 QR code for app download



**https://webview.cossecurity.com/download/cos/cos.html**

**Procedure**

**Step 1** On the Home screen, tap +Add and then it goes to sites screen.

**Step 2** Tap 🔧 on the upper left corner of the Home screen, and then tap the account profile.
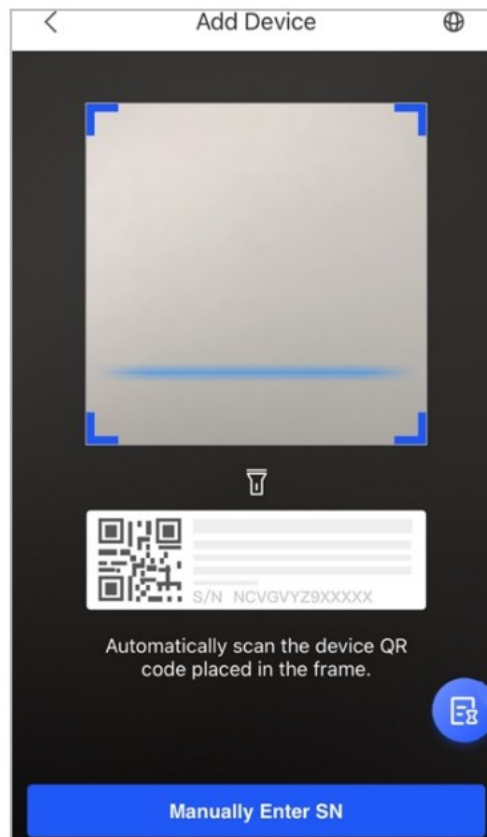
📖

Before assigning an operator on the DoLynk Care app, you need to create and manage operator accounts on DoLynk Care portal. For details, see DoLynk Care User's Manual.

**Step 3** Add the Device by scanning the QR code or manually entering SN of the Device.

1. On the Home screen, tap ⊕ and then select QR code.

   Figure 5-2 Add the device



2. You can scan the QR code to obtain the SN or tap ✏️ to manually enter the SN.

   📖

   When adding the Device through the SN, you need to enter the SN and password. The default password before device initialization is the SC code which can be obtained from the label on the Device.

3. Select a site, and then tap OK.

**Step 4** Select Done, and then you can view the Device in the device list.

📖

Tap 🔧, and then select Account > Help and Feedback > User's_Manual for more details.

**5.1.2 Managing the Device by DoLynk Care Webpage**

Prerequisites

- Make sure that the Device is connected to the power and the network before adding the Device.

- You do not need to apply the account again if you have already applied for an account through the app.

**Procedure**
**Step 1** Open the browser and enter the URL  **https://care.dolynkcloud.com**, and then press the Enter key.
**Step 2** Enter the email and password, and then click Log in.
**Step 3** Add the Device.

1. Click Devices on the console page.

2. Click Add Sites > Add.

3. Enter the Device name, Device SN and password.

You must select a site for the Device. You can select an existing site from the list or create a new site.



- When adding the Device through the SN, you need to enter the SN and password.

  The default password before device initialization is the SC code which can be obtained from the labeling on the

  Device.

- You cannot add the Device which has been bound to an account.

- If you add a switch, you can change the Device password following the on-screen instructions.

**Step 4** Click OK.



Click  on the upper right corner of the screen to go to the Help page, and then view the document on the platform, including user's manual, FAQ, and more.

**5.2 Managing the Device by Local Webpage**
The Cloud Managed Switch provides webpage access functionality. You can log in to the webpage to manage and configure the Device.

**5.2.1 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 segment.

- Device initialization is required for first-time use or after the Device has been reset.

- Plan the network segment properly to connect the Device to the 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 the ConfigTool to obtain the IP address on select models.

**Procedure**

**Step 1** Open the browser, enter the IP address of the Device in the address bar, 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 username is admin.
- Configure a high security password according to the prompt of password strength. A password should be 8-32 characters containing at least two types among numbers, letters and common characters (any visible characters other than' " ; : &).

**Step 5** Click Complete.

**5.2.2 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 segment.

**Procedure**
**Step 1** Open the browser, enter the IP address of the Device in the address bar, and then press the Enter key.
**Step 2** Enter the password.
**Step 3** Click Login.

For details, see the web operation manual.

**5.3 Using as an Unmanaged Device**

The Cloud Managed Switch supports plug and play as an unmanaged switch.

Make sure the Device is connected to the power supply. The default IP address is 192.168.1.110 and it might have an IP address conflict.

## 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 Allow list**

   It is recommended that you turn on the allow list function, and only allow IP in the allow list to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allow list.

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).



## Documents / Resources

| | |
|---|---|
| Ethernet Switch (Cloud Managed PoE Switch) Quick Start Guide | **dahua CS4218-16ET-135 Ethernet Cloud Managed PoE Switch** [pdf] User Guide CS4218-16ET-135, CS4218-16ET-135 Ethernet Cloud Managed PoE Switch, Ethernet Cloud Managed PoE Switch, Cloud Managed PoE Switch, Managed PoE Switch, PoE Switch, Switch |

## References

- **User Manual**