Ethernet Switch (4&8-Port Hardened Cloud Managed Switch)

Quick Start Guide

V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the 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
V1.0.0	First release.	July 2024

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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):

- Before extending the rack to the installation position, read the installation instructions.
- When the device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the device is installed on it.

⚠ 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 and 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.
- Make sure to install a circuit breaker in the external power circuit.
- A 16 A overcurrent protection device is required to be installed in the external power circuit of the product.
- 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.
- All-pole power switches that meet the requirements of GB4943.1 standard should be installed in the electrical facilities of the building.

Operating 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

- Operating the device in a domestic environment may cause radio interference.

- Place the device in a location that children cannot easily access.
- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Ground the device to protective ground before you power it on.

⚠

- 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: –30 °C to +65 °C (–22 °F to +149 °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.

Table of Contents

1 Overview

1.1 Introduction

The device is a hardened cloud managed switch. High-performance swap engine and large-capacity cache enable lag-free transmission of video streams. It has low transmission delay, large buffer and is highly reliable. In addition, based on the DoLynk Care Cloud Server, this device can be managed through the DoLynk Care app and the network topology diagram function can be used to quickly locate the problem. It adopts a dial design and provides multiple operating modes to meet the needs of different scenarios.

The device is applicable for uses in different scenarios, including corridors, factories and parks.

1.2 Features

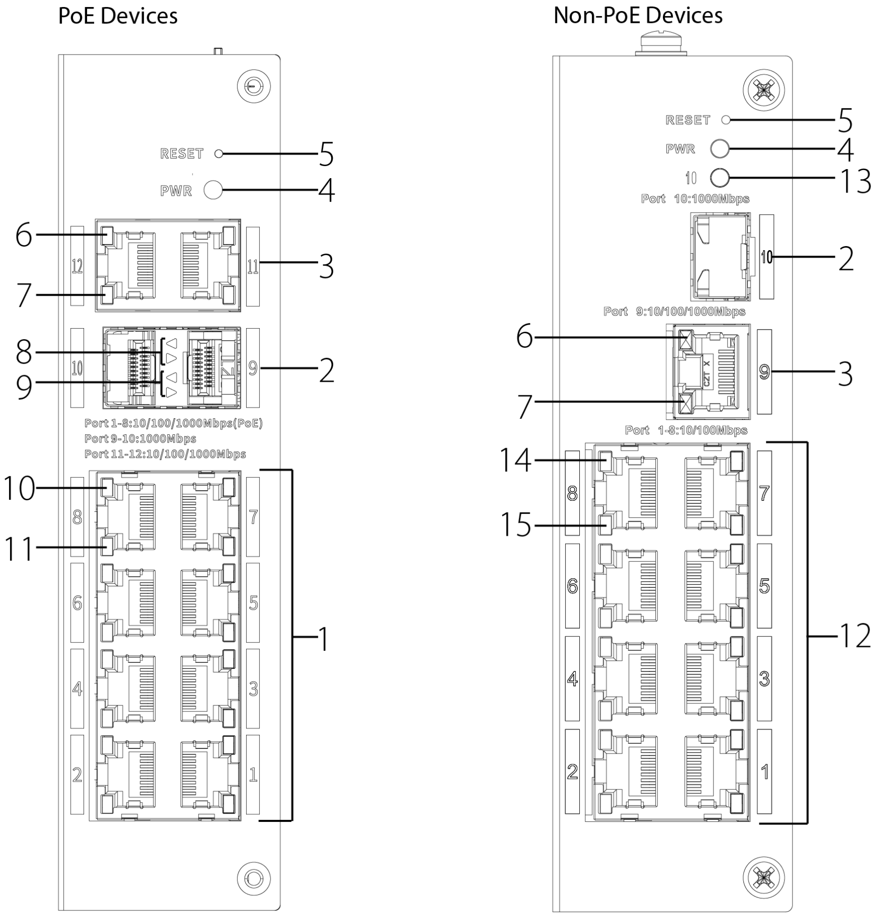
- 4/8 100 Mbps or 1000 Mbps Ethernet ports (some models are PoE Ethernet ports), uplink port supports 1 Gbps optical port or Ethernet port.
- Supports managed mode switch. Controlled by dual in-line package (DIP) switch, the device supports on-premises webpage and cloud management when enabled, enabled by factory default. Switches to unmanaged switch when shut down.
- Supports IEEE802.3af, IEEE802.3at standard. Red ports support IEEE802.3bt, and are compatible with Hi-PoE. Orange ports conform to Hi-PoE.
- Supports network topology visualization.
- Supports mobile management by app.
- Supports one-stop maintenance.
- Supports Link Layer Discovery Protocol.
- Supports Dynamic Host Configuration Protocol.
- Some models support STP/RSTP Ring Network Protocol.
- VLAN configuration based on IEEE802.1Q.
- With its full metal and fanless design, the device has great heat dissipation and low power consumption, working in environments ranging from–30 °C to +65 °C (–22 °F to +149 °F).
- Some models support manual link aggregation.
- Desktop mount, DIN-rail mount and wall mount (some models).

2 Port and Indicator

2.1 Front Panel

The following is an example of a PoE and a non-PoE appearance. The actual device might only include part of it. Please refer to the interface introduction in conjunction with the actual object for details.

Figure 2-1 Front panel



PoE Devices

Non-PoE Devices

Table 2-1 Interface description

No.	Description
1	10/100 Mbps or 10/100/1000 Mbps self-adaptive PoE Ethernet port
2	1000 Mbps optical port
3	10/100 Mbps or 10/100/1000 Mbps self-adaptive uplink port
4	Power (PWR) indicator ● On: Power on. ● Off: Power off.

No.	Description
5	Reset button Press and hold for longer than 5 seconds, wait until all the indicators are solid on, and then release. The device recovers to the default settings. Only effective in the managed mode.
6	Uplink optical port status (Link) indicator ● On: Optical ports connected to the device. ● Off: Optical ports not connected to the device.
7	Uplink optical port data transmission status (Act) indicator ● Off: No data transmission in progress. ● Flashes: Data transmission is in progress.
8	Optical port connection or data transmission status (Link) indicator ● On: Optical ports connected to the device. ● Off: Optical ports not connected to the device.
9	Optical port connection or data transmission status (Act) indicator ● Off: No data transmission in progress. ● Flashes: Data transmission is in progress.
10	PoE network port power supply status indicator ● On: Use PoE power supply. ● Off: Not using PoE power supply.
11	Single port connection or data transmission status (Link/Act) indicator ● On: The port is connected to the device. ● Flashes: Data transmission is in progress. ● Off: The port is not connected to the device.
12	10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet port
13	Optical port connection/data transmission status (Act) indicator Flashes: Data transmission is in progress.
14	Single port connection status (Link) indicator ● On: The port is connected to the device. ● Off: The port is not connected to the device.
15	Single port data transmission status (Act) indicator ● Flashes: Data transmission is in progress. ● Off: No data transmission in progress.

2.2 Side panel

The following is an example of a PoE and a non-PoE appearance. The actual device might only include part of it. Please refer to the interface introduction in conjunction with the actual object for details.

Figure 2-2 Side panel

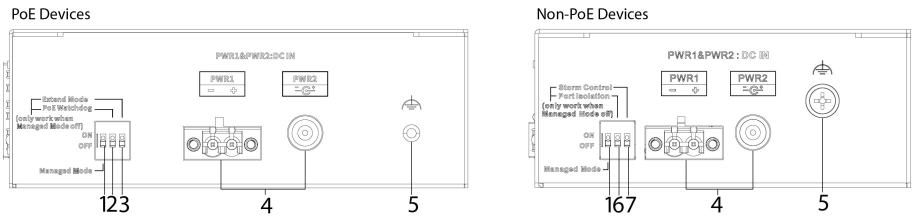


Table 2-2 Interface description

No.	Description
1	Managed Mode Use the dual in-line package (DIP) switch to switch between managed and unmanaged modes. The managed mode includes on-premises web management and cloud management, which are enabled by default. Everytime the DIP switch flipped, the device would experience a reboot. The configuration under managed mode will temporarily reserved when the managed mode switched off. The configuration will be restored once managed mode is enabled again.
2	PoE Watchdog The PD keep alive mode is enabled through the dual in-line package (DIP) switch. When a terminal device crash is detected, the terminal device is restarted due to power failure. The factory default is off. Only works when managed mode off.
3	Extend Mode Enable long distance transmission mode via dual in-line package (DIP) switch. The factory default is off. ● Only works when managed mode off. ● In Extend Mode, the transmission rate drops to 10 Mbps. The actual transmission distance is strongly related to the PoE power and wire mass. The advertised distance is only the laboratory distance.
4	Power port, dual-power backup PoE devices support 48–57 VDC power supply. Non-PoE devices support 12 VDC power supply.

No.	Description
5	Ground terminal
6	Port Isolation Port isolation is achieved through dual in-line package (DIP) switch. After it is turned on, the downstream ports are isolated from each other, the downstream ports and uplink ports communicate normally, and the uplink ports are not isolated. The factory default is off. 📖 Only works when managed mode off.
7	Storm Control Storm control is achieved through a dual in-line package (DIP) switch. When enabled, the unicast, multicast, and broadcast suppression restriction rates are 5 Mbps, and the factory default is off. 📖 Only works when managed mode off.

3 Installation

3.1 Preparations

- Select a proper installation method according to your actual needs.
- Make sure that the working platform is stable and steady.
- Leave about 10 cm space for heat dissipation to ensure good ventilation.

3.2 Desktop Mount

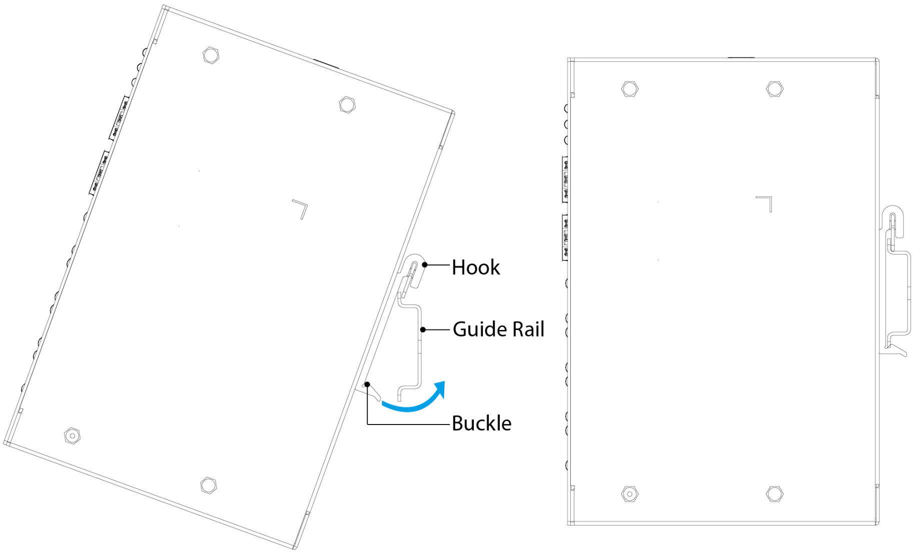
The device supports desktop mount. Place it on a steady and stable desktop.

3.3 DIN-rail Mount

The device supports DIN-rail mount. Hang the device hook on the guide rail, and press the device to make the buckle into the guide rail.

The width of guide rail supported by the device is 35 mm.

Figure 3-1 DIN-rail mount



3.4 Wall Mount (Only Some Models Support)

Procedure

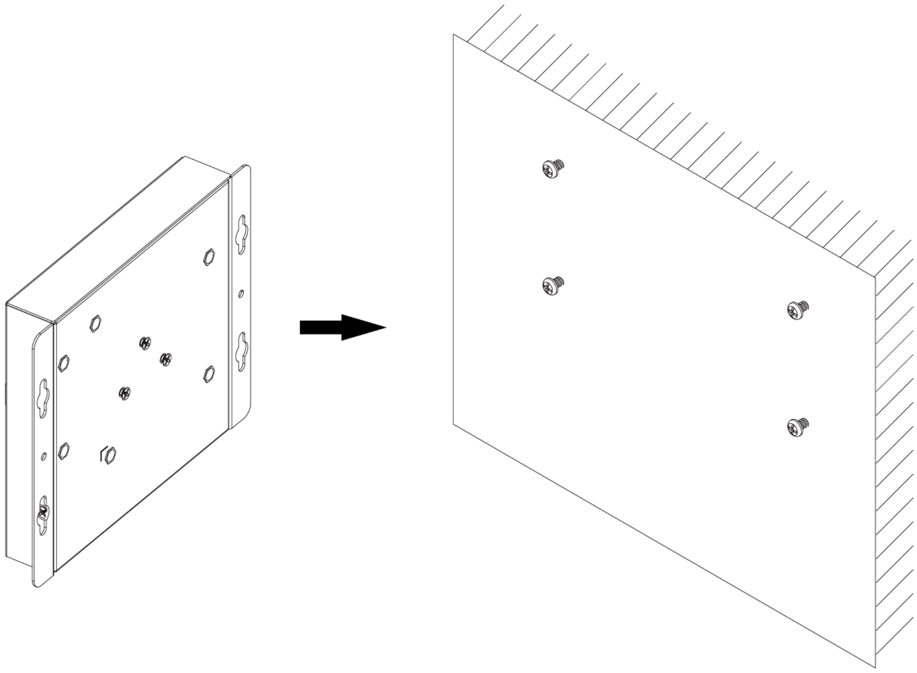
Step 1 Drill 4 self-tapping screws into the wall according to the spacing of the switch wall-mounting holes.

- The distance between the screws matches the distance between the two wall mounting holes.

- Leave a space of 2 mm between the wall and the head of the screw.

Step 2 Align the wall-mount holes of the device with the screws, hang the device on the screws, and then lock the screws.

Figure 3-2 Wall mount



4 Wiring

4.1 Connecting GND Cable

Normal GND connection of the device is the important guarantee for device lightning protection and anti-interference. You must connect the grounding wire normally and ground it before powering on and disconnect it after powering off.

Procedure

Step 1 Use a crosshead screwdriver to remove the earthing screw on the side panel of the device.

The grounding wire of the chassis is called chassis ground.

Step 2 Connect one end of the grounding wire to the terminal crimping and fix it to the chassis ground with an earthing screw.

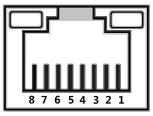
Step 3 Connect the other end of the grounding wire to the ground securely.

The area of grounding wire cross section is more than 2.5 mm^2. The grounding resistance is required to be less than 4 Ω.

4.2 Connecting Ethernet Port

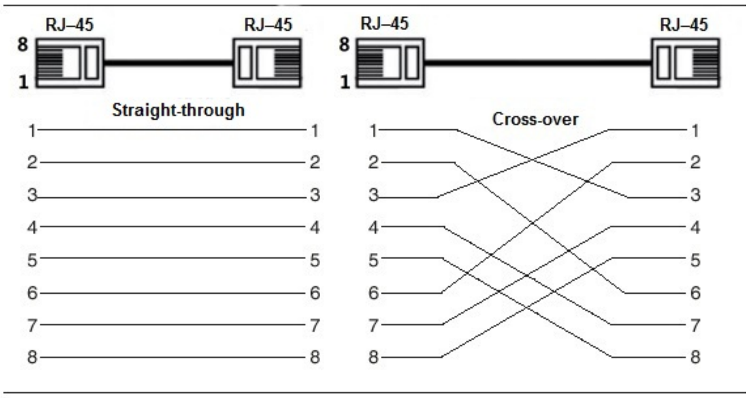
Ethernet port adopts standard RJ–45 port. Equipped with self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode, and supports MDI/MDI-X self-recognition function of the cable, which means that the switch can use cross-over cable or straight-through cable to connect terminal device to network device.

Figure 4-1 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 4-2 Pin description



4.3 Connecting SFP Ethernet Port

Prerequisites

We recommend wearing antistatic gloves before installing SFP module, and then wear antistatic wrist, and confirm the antistatic wrist is well linked to the surface of the gloves.

Procedure

Step 1 Lift the handle of SFP module upward vertically and make it get stuck to the top hook.

Step 2 Hold the SFP module on both sides and push it gently into the SFP slot till the SFP module is firmly connected to the slot (You can feel that both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).

⚠ WARNING

The device uses laser to transmit signal via optical fiber cable. The laser conforms to the requirements of level 1 laser products. To avoid injury upon eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

- 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 port.
- Do not directly insert the SFP optical module with the optical fiber inserted into the slot. Unplug the optical fiber before installing it.

Figure 4-3 SFP module structure

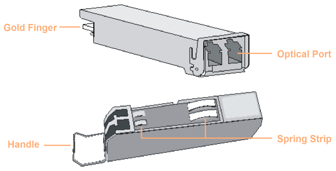
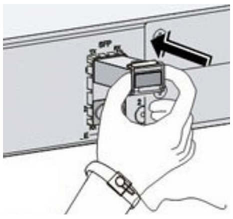


Figure 4-4 SFP module installation



4.4 Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect the terminal device PoE Ethernet port to the switch PoE Ethernet port through 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.

4.5 Connecting Power Cord

Redundant power input supports two-channel power, which are PWR2 and PWR1. You can select the other power for continuous power supply when one channel of power breaks down, which greatly improves the reliability of network operation.

Background Information

WARNING

To avoid personal injury, do not touch any exposed wire, terminal and areas with danger voltage of the device and do not dismantle parts or plug connector during power on.

- Before connecting power supply, make sure that the power supply conforms to the power supply requirements on the device label. Otherwise, it might cause device damage.
- We recommend using an isolated adapter to connect the device.

Figure 4-5 Power terminal

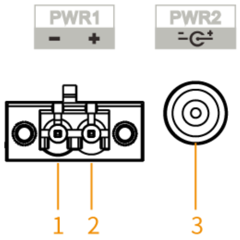


Table 4-1 Power terminal definition

No.	Port Name
1	Din rail power supply negative terminal
2	Din rail power supply positive terminal
3	Power adapter input port

Procedure

Step 1 Connect the device to ground.

Step 2 Take off the power terminal plug from the device.

Step 3 Plug one end of the power cord into the power terminal plug and secure the power cord.

The area of power cord cross section is more than 0.75 mm^2 and the maximum cross section area of the wiring is 2.5 mm^2.

Step 4 Insert the plug which is connected to power cable back to the corresponding power terminal socket of the device.

Step 5 Connect the other end of power cable to the corresponding external power supply system according to the power supply requirement marked on the device, and check if the corresponding power indicator light of the device is on, and it means power connection is correct if the light is on.

5 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

Procedure

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

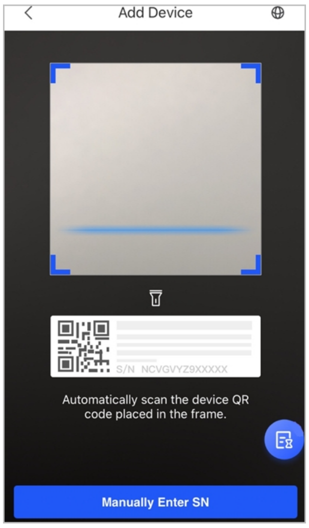
Step 2 Tap on the upper-left corner of the **Home** screen, and then tap the account profile.

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



Automatically scan the device QR code placed in the frame.

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 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 Logging in to 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 User's Manual.

5.3 Using as an Unmanaged Device

The cloud managed switch supports plug and play as an unmanaged switch.

When managed mode is off, the device has no IP address. Otherwise, when multiple devices are networking, the default IP address for all devices will be 192.168.1.110 which may result in 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).

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