



Ethernet Switch (Industrial Managed Switch)

Quick Start Guide



V1.0.0






Foreword

General

This manual mainly introduces the hardware, installation, wiring steps, and quick configurations of the industrial managed 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
 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



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.
 - ◇ 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.




- 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.

Operation Requirements



-  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.



- 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.



- 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: -40 °C to +75 °C (-40 °F to +167 °F).
- 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.
- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

Maintenance Requirements



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.



Power off the device before maintenance.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
2 Port and Indicator.....	2
2.1 Front Panel.....	2
2.2 Side Panel.....	4
3 Installation.....	5
4 Wiring.....	6
4.1 Connecting GND Cable.....	6
4.2 Connecting Power Cord.....	6
4.3 Connecting SFP Ethernet Port.....	8
4.4 Connecting Ethernet Port.....	8
4.5 Connecting PoE Ethernet Port.....	9
4.6 Connecting Alarm Terminal.....	9
4.7 Connecting RS-485 Terminal.....	10
4.8 Connecting Console Port.....	10
5 Quick Operation.....	12
5.1 Login through Web.....	12
5.2 Restoring to Factory Settings.....	12
6 Usage Mode.....	13
6.1 Managing the Device by Cloud Management.....	13
6.1.1 Managing the Device by DoLink Care App.....	13
6.1.2 Managing the Device by DoLink Care Webpage.....	14
6.2 Managing the Device by Local Webpage.....	15
6.2.1 Initializing the Device.....	15
6.2.2 Logging in to the Device.....	16
Appendix 1 Security Commitment and Recommendation.....	17

1 Overview

1.1 Introduction

The device is designed for on-site transmission and application in severe environment. Equipped with high performance switching engine and large buffer memory, it features low transmission delay and high reliability. The protection for power input end overcurrent, overvoltage and EMC can effectively resist the interference from static electricity, lightning, and pulse. The dual power backup guarantees stable operation for the system. With web management, SNMP and other functions, the device can be remotely managed.

In addition, based on the DoLink Care Cloud Server, this device can be managed through the DoLink Care app, the network topology diagram function can be used to quickly locate the problem. The device is applicable for uses 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.
- All-gigabit port design. Uplink port includes two forms: Ethernet port and optical port.



Different devices have different forms.

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



This feature is only available for PoE devices. And 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.

- 250 m long-distance PoE transmission (10 Mbps).



This feature is only available for PoE devices. And 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.

- PoE watchdog (available for models with PoE Ethernet port).
- Supports STP, RSTP, and ERPS.
- IEEE802.1Q-based VLAN configuration.
- Manual link aggregation and static LACP.
- Wide voltage design.
- Desktop mount and DIN-rail mount.
- The solid and sealed all-metal case design and efficient surface heat dissipation make it can work in the environment from -40°C to $+75^{\circ}\text{C}$ (-40°F to $+167^{\circ}\text{F}$).

2 Port and Indicator

2.1 Front Panel

The following figures are for reference only, and might differ from the actual product.

Figure 2-1 Front panel (with PoE port)

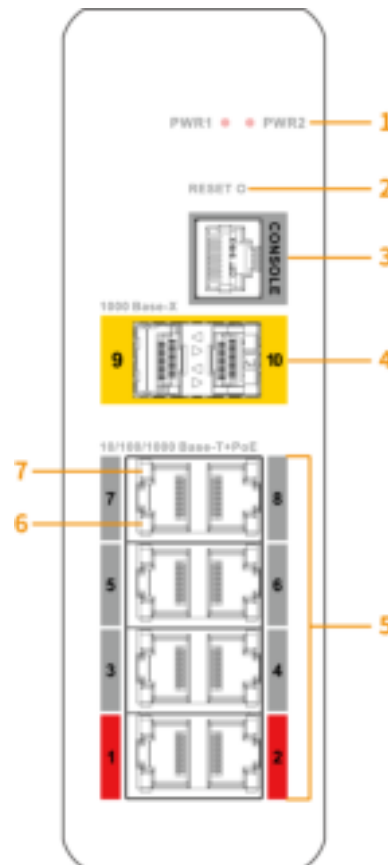
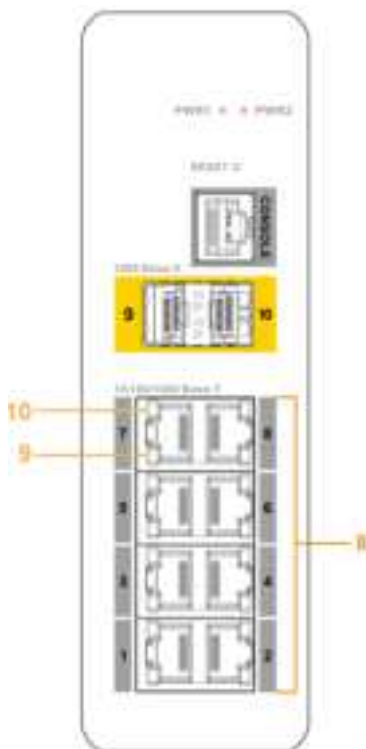


Figure 2-2 Front panel (without PoE port)



The following are all the ports and indicators on the front panel of the industrial managed switch. The actual device may only have a part of them.

Table 2-1 Description of front panel

No.	Description
1	Power Indicator. <ul style="list-style-type: none"> Green: Normal power connection. Red: Abnormal power connection.
2	Reset button. Press and hold it for more than 5 s, and release after the panel status indicators are all on to restore the device to default settings.
3	Console port.
4	1000 Mbps optical port.
5	10/100/1000 Mbps adaptive PoE port.
6	Single-port connection or data transmission status indicator (Link/Act). <ul style="list-style-type: none"> On: Connected to device. Off: Not connected to device. Flashes: Transmitting data.
7	Single-port PoE status indicator. <ul style="list-style-type: none"> On: Powered by PoE. Off: Not powered by PoE.

No.	Description
8	10/100/1000 Mbps Ethernet port.
9	Single-port data transmission status indicator (Act). <ul style="list-style-type: none"> Flashes: Transmitting data. Off: No data transmission.
10	Single-port connection status indicator (Link). <ul style="list-style-type: none"> On: Connected to device. Off: Not connected to device.

2.2 Side Panel

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

Figure 2-3 Side panel

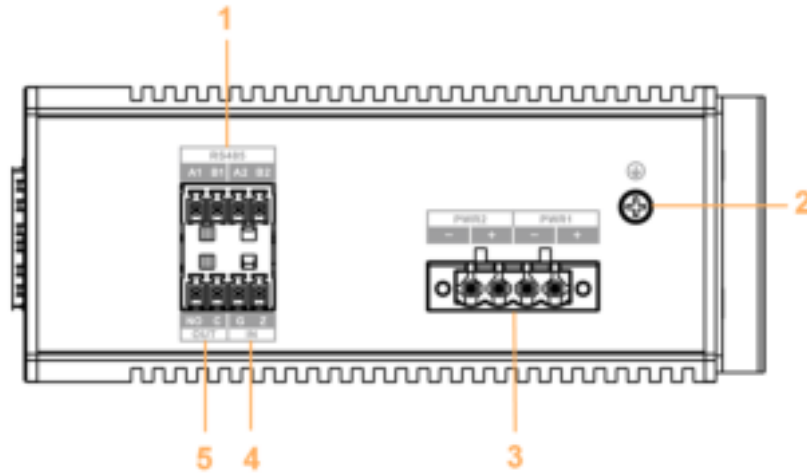


Table 2-2 Port description

No.	Description
1	RS-485 port
2	GND screw
3	Power port (dual power backup)
4	Alarm input port
5	Alarm output port

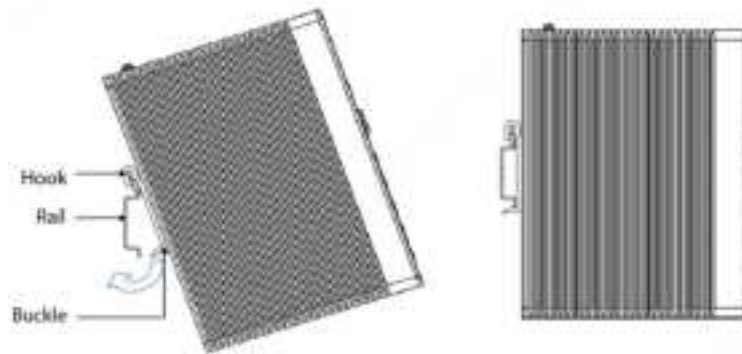
3 Installation

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



The width of the guide rail supported by the device is 50 mm.

Figure 3-1 DIN rail



4 Wiring

4.1 Connecting GND Cable

Background Information

Device GND connection ensures device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and power off the device before disconnecting the GND cable. There is a GND screw on the device cover board for the GND cable, which is called enclosure GND.

Procedure

- Step 1** Remove the GND screw at the enclosure GND with a cross screwdriver.
- Step 2** Connect one end of the GND cable with the cold-pressed terminal, and fix it on the enclosure GND with the GND screw.
- Step 3** Connect the other end of the GND cable to the ground.



The sectional area of the GND cable shall be more than 2.5 mm², and the GND resistance shall to be less than 4 Ω.

4.2 Connecting Power Cord

Background Information

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.



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, 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.



The sectional area of power cable shall be more than 0.75 mm² (max sectional area 2.5 mm²); ground resistance is required to be less than 4 Ω.

Figure 4-1 Power terminal

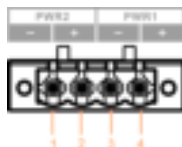


Table 4-1 Power terminal description

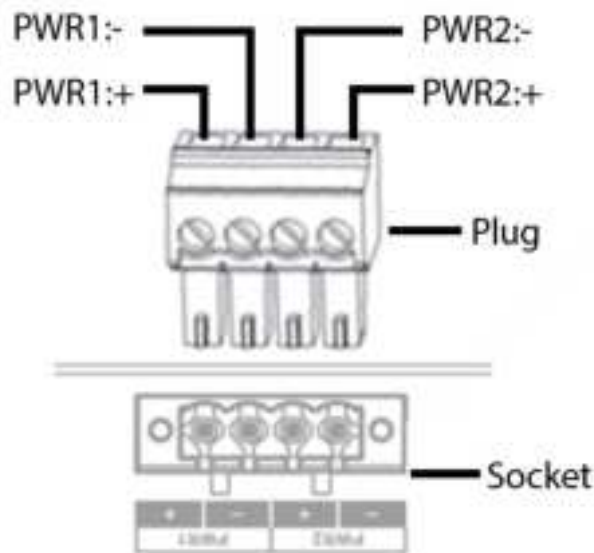
No.	Signal Name	DC Wiring Definition
1	-	PWR2-
2	+	PWR2+
3	-	PWR1-
4	+	PWR1+

The operation steps of connecting power terminal plug and socket are shown as follows.

Procedure

- Step 1** Connect the device to ground.
- Step 2** Take off the power terminal plug from the device.
- Step 3** Insert one end of the power cable into the power terminal plug according to the requirement.

Figure 4-2 Fix the power cable



- 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, it means power connection is correct if the light is on.



The device supports 48–57 VDC. Please confirm if the power supply conforms to the requirement marked on the device before connecting to power, which is to avoid causing damage to the device.

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

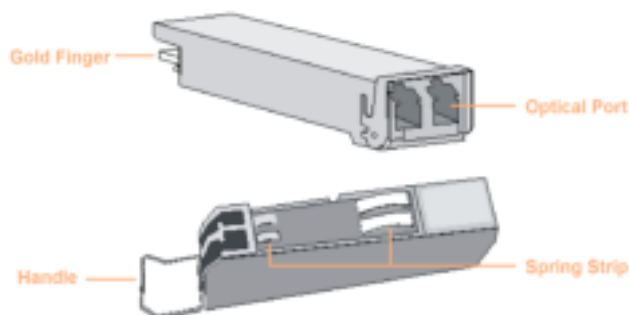


Figure 4-4 SFP module installation



4.4 Connecting Ethernet Port

Ethernet port is a 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

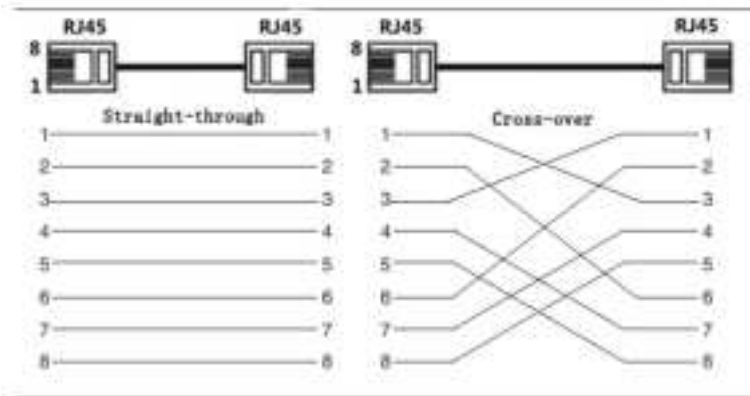
the cable, therefore, you can use cross-over cable or straight-through cable to connect terminal device to network device.

Figure 4-5 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 4-6 Cable connection



4.5 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.



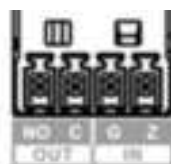
When connecting to a non-PoE device, the device needs to be used with an isolated power supply.

4.6 Connecting Alarm Terminal

Background Information

The alarm terminal is located on the side panel of the device, which is used for alarm input and output. When the device detects the alarm input signal (alarm in low level), it will switch the alarm output terminal for a short time (after the alarm out level is lowered for 5 seconds, it will be raised again).

Figure 4-7 Alarm terminal





C pin is a normally open switch, and NO pin is a normally closed switch. When the device is working, the C pin and the NO pin are both disconnected. When an alarm occurs, the C pin and the NO pin are both connected.

Table 4-2 External port electrical parameters

Parameter	Value
Max. voltage	125 VAC/ 60 VDC
Max. current	2 A
Max. power	60 W
Max. insulation and voltage resistance	2 kV

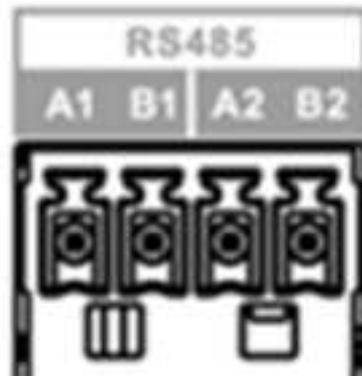
Procedure

- Step 1 Take off the alarm terminal plug from the device.
- Step 2 Insert the two wires of the alarm terminal into plugs of alarm terminal according to the description above, and fix the wires firmly.
- Step 3 Insert the alarm terminal plug which is connected to cable back to the corresponding alarm terminal socket of the device.

4.7 Connecting RS-485 Terminal

The RS-485 data conversion port is located on the side panel of the device. There are two groups in total. Each group can independently convert between RS-485 data and Ethernet data (tcp/udp).

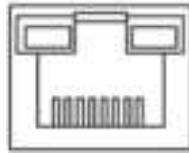
Figure 4-8 RS-485 terminal



4.8 Connecting Console Port

Use RJ-45 to DB-9 cable to connect the device console port and 9-pin serial port on your PC. Operating the hyper terminal software of the Windows system can call the console software of the device. Through the console software, you can configure, manage, and maintain the device.

Figure 4-9 Console port



One end of RJ-45 to DB-9 cable is RJ-45 connector, which needs to be inserted into the console port of the device; the other end is DB-9 plug, which needs to be inserted into the 9-pin serial port which controls the computer.

Figure 4-10 Cable sequence

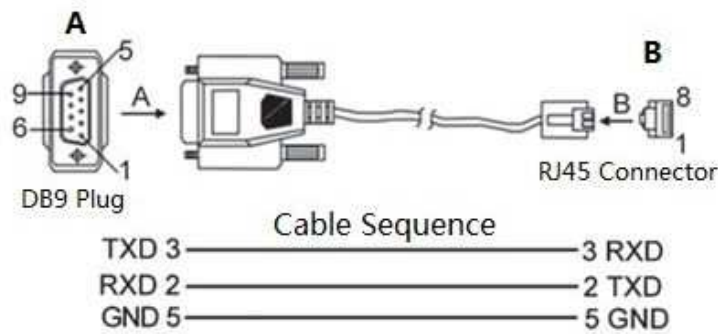


Table 4-3 Port pin description

DB9 Pin	RJ-45 Pin	Signal	Description
2	3	RXD	Receive data.
3	2	TXD	Transmit data.
5	5	GND	Ground.

5 Quick Operation

5.1 Login through Web

You can log in to the device through web for management and operation. For details, see web operation manual.

Table 5-1 Default factory configuration

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	You need to set the password for the first login.

5.2 Restoring to Factory Settings

There are two ways to restore the device to factory settings.

- Press and hold the **Reset** button for 5 seconds to restore the device to factory settings.
- Log in to web or use command line. For details, see the web operation manual or command line reference manual.

6 Usage Mode

6.1 Managing the Device by Cloud Management

The cloud managed switch supports device management through the DoLink Care app and webpage.

6.1.1 Managing the Device by DoLink 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 DoLink Care app.

Figure 6-1 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 DoLink Care app, you need to create and manage operator accounts on DoLink Care portal. For details, see *DoLink 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 6-2 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.

6.1.2 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.

6.2 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.

6.2.1 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**.

6.2.2 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.

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;
- Establish 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