

Ethernet Switch (Industrial Managed Switch)

Quick Start Guide



V1.0.3






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, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.3	Updated the initializing and adding the device.	January 2024
V1.0.2	Updated the images.	September 2023
V1.0.1	Updated the features.	August 2021
V1.0.0	First release.	July 2021

Privacy Protection Notice

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

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

- 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.....	3
3 Installation.....	4
4 Wiring.....	5
4.1 Connecting GND Cable.....	5
4.2 Connecting Power Cord.....	5
4.3 Connecting SFP Ethernet Port.....	7
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 First Login through Console Port.....	12
5.2 Login through Web.....	13
5.3 Restoring to Factory Settings.....	13
6 Initializing and Adding the Device.....	14
6.1 Initializing the Device.....	14
6.2 Webpage Initialization.....	14
6.3 Adding the Device.....	14
Appendix 1 Security Recommendation.....	16

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 solid and sealed all-metal case design and efficient surface heat dissipation make it can work in the environment from -40°C to $+75^{\circ}\text{C}$ (-14°F to $+167^{\circ}\text{F}$). 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 Telnet, web management, SNMP and other functions, the device can be remotely managed. It can directly connect to iLinksView.

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.
- Support one-stop maintenance.
- All-gigabit port design. Uplink port includes two forms: Ethernet port and optical port.
- 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.
- 250 m long-distance PoE transmission (10 Mbps).
- PoE watchdog (available for models with PoE Ethernet port).
- Supports STP, RSTP, and MSTP.
- IEEE802.1Q-based VLAN configuration.
- Manual link aggregation and static LACP.
- Wide voltage design.
- Desktop mount and DIN-rail mount.

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)

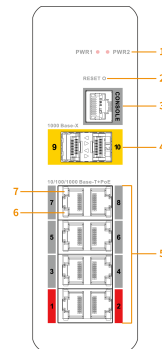
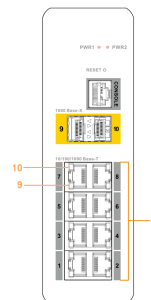


Figure 2-2 Front panel (without PoE port)



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.

No.	Description
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.
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

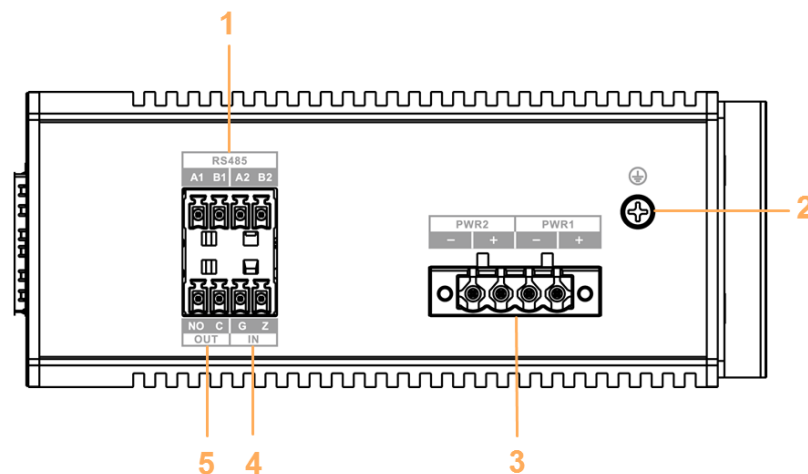


Table 2-2 Port description

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

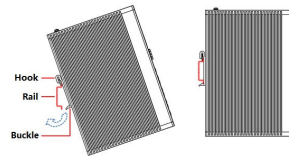
3 Installation

The device supports DIN-rail mount. Hang the switch hook on the rail, 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



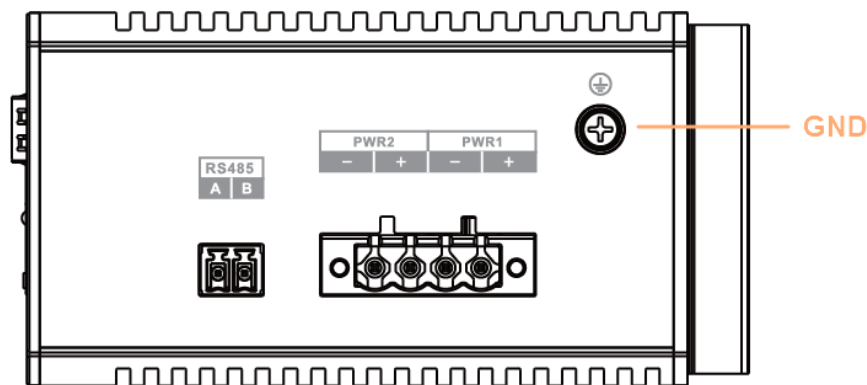
4 Wiring

4.1 Connecting GND Cable

Background Information

Device GND connection helps ensure 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.

Figure 4-1 GND port



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.



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 4-2 Power terminal

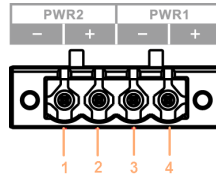


Table 4-1 Power terminal description

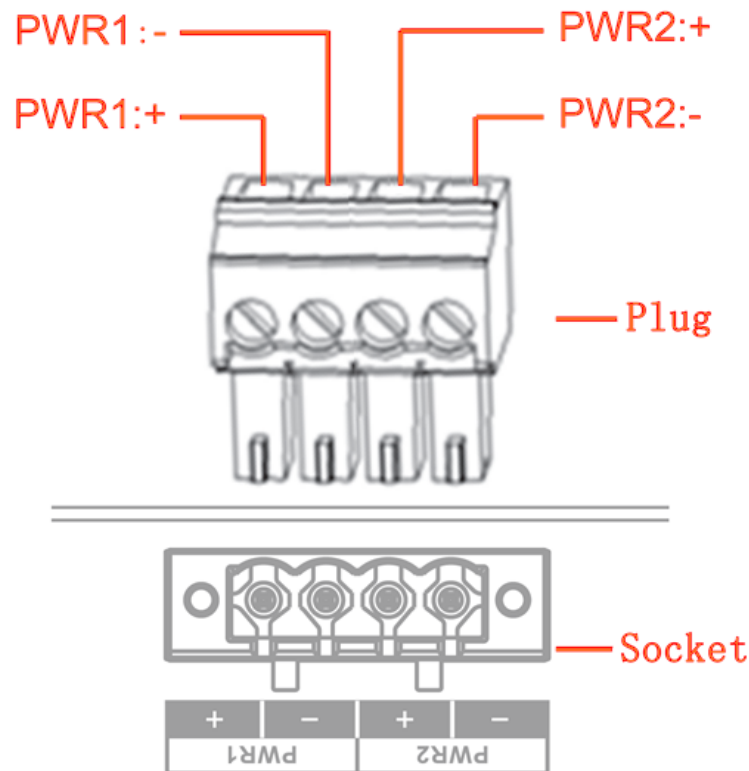
No.	Signal Name	DC Wiring Definition
1	-	PWR2-
2	+	PWR2+
3	-	PWR1-
4	+	PWR1+

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 4-3 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 4-4 SFP module structure

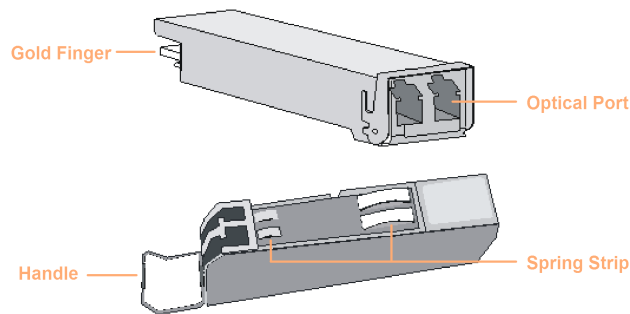
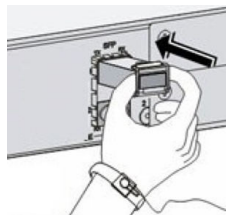


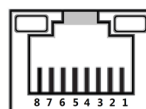
Figure 4-5 SFP module installation



4.4 Connecting Ethernet Port

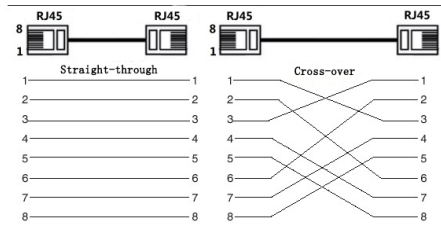
Ethernet port is a standard RJ-45 port. With self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode. It supports MDI/MDI-X self-recognition of the cable, therefore, you can use cross-over cable or straight-through cable to connect terminal device to network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

Figure 4-6 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 4-7 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.



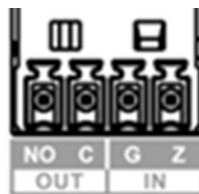
When connecting to a non-PoE device, the device needs to be used with an isolated power supply.

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 raised for 5 seconds, it will be lowered again).

Figure 4-8 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 is closed and the NO pin is disconnected. When an alarm occurs, the C pin is disconnected and the NO pin is closed.

Table 4-2 External port electrical parameters

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

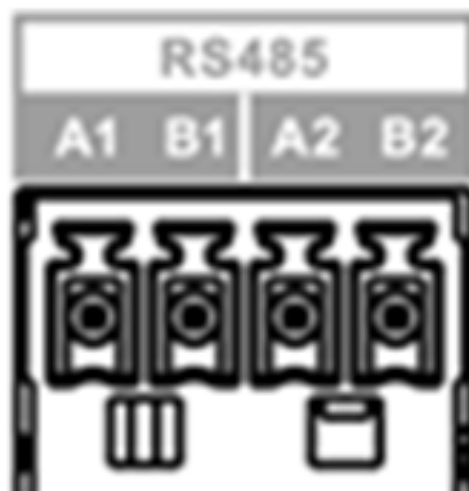
Procedure

- 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).

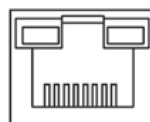
Figure 4-9 RS-485 terminal



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 4-10 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 4-11 Cable sequence

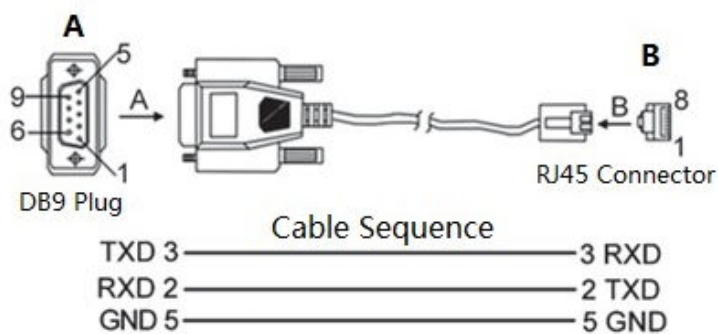


Table 4-3 Port pin description

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 First Login through Console Port

Background Information

You can log in to the local interface through the console port.

Procedure

Step 1 Power off the PC.

Step 2 Use default console port cable to connect PC and device. First insert the DB-(hole) plug of console port cable into the 9-pin serial port of PC, and then insert the RJ-45 plug into the console port of the device.

1. Insert the DB-(hole) plug of console port cable into the 9-pin serial port of PC.
2. Insert the RJ-45 plug into the console port of the device.



- Confirm the sign on the port during connection, in case it may plug into the wrong port.
- Plug out RJ-45 and then DB-9 when removing console port cable.

Figure 5-1 Connect PC and switch



Step 3 Power on the PC.

Step 4 Run terminal simulation program on the PC.

Step 5 Select the serial port which is to connect the device, set the terminal communication parameters. The parameter value has to be in accordance with the value on the device, the default is shown as follows.

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: None
- Flow control: None



If the PC uses Windows Server 2003 operating system, add hyper terminal program in the Windows component and then log in the manage the device according to the way introduced in this manual; If PC uses Windows Server 2008, Windows Vista, Windows 7 or other operating systems, please prepare third-party terminal control software, refer to the software operation guide or online help for operation method.

Step 6 After powering on the device, the device self-check information is displayed on the terminal program.

Step 7 Enter username and press Enter.

Step 8 Enter password and press Enter.

The command line prompt (SWITCH#) is displayed, as shown in the following figure.

Press ENTER to get started

Username: admin

Password:

SWITCH#

Step 9 (Optional) Enter corresponding command to configure the device or check device operating status.



You can enter ? anytime if you need help.


5.2 Login through Web

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



For first login, you need to change the password according to the interface prompt.

Table 5-1 Default factory configuration

Parameter	Description
IP address	192.168.1.110/255.255.255.0
Username	admin
Password	<ul style="list-style-type: none"> Web: admin iLinksView : lt_91_il_02_nmp  <p>When using the iLinksView to manage the device, note that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the device.</p>

5.3 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 Initializing and Adding the Device

6.1 Initializing the Device

- You can use DoLynk Care app to scan the QR code of the Device, and then add and initialize the Device when the Device is connected to Internet.
- You can log in to the webpage to initialize the Device and modify the IP address when the Device is not connected to Internet.



- Device initialization is required for first-time use or after the Device has been reset.
- DHCP Client is enabled by default. If no IP address is assigned, the default IP address can be used. (See from the Device label, usually 192.168.1.110.)
- Device initialization is available only when the Device and the computer are on the same network segment.
- Plan the network segment properly to connect the Device to the network.
- Different models support different methods of local initialization. For details, see the technical specifications.
- Webpage initialization is only supported on partial models.

6.2 Webpage Initialization

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



The Device has no initial password. You can set your password according to the webpage prompts when you log in for the first time and initialize the Device.

6.3 Adding the Device

Quickly add the Device to the DoLynk Care by scanning the QR code or manually enter the SN on the Device.

Procedure

- Step 1** Download and turn on the DoLynk Care, and then tap **+Add Device**.

Figure 6-1 DoLynk Care app

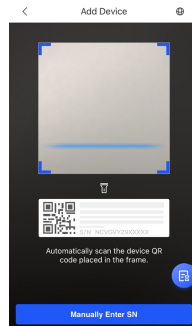


For more details, see *DoLynk Care User's Manual*.


- Step 2** Tap **+** on the upper-right corner of the **Home** screen, select **Scan the Code to Add**, and then tap **Next**.

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

Figure 6-2 Scan the QR code



Step 3 You need select **Switch** and select a site, and then tap **OK**.

If there is no site, tap , and then select a site.

Step 4 If the Device has not been initialized, you could modify the SC Code as the initial password on the label. Enter the Device password, and then tap **Save**.

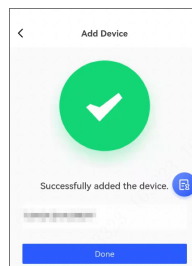
If the Device has been initialized, enter the Device password, and then tap **Save**.

Figure 6-3 Enter the device password



Step 5 Tap **Done**.

Figure 6-4 Add device



Select **Me** > **HELP** > **User's_Manual** in DoLink Care for more details.

Appendix 1 Security Recommendation

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 logout function

The account logout 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

The 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, it is recommended 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. **5.2 Update client software in time**

It is recommended 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).

