Ethernet Switch (Hardened Optical & Electrical Aggregation Switch)

Quick Start Guide

V1.0.1

Foreword

General

This manual mainly introduces the hardware, installation, and wiring steps of the Hardened Optical & Electrical Aggregation 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 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
V1.0.1	Updated the initializing and adding the device.	January 2024
V1.0.0	First release.	October 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

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.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- 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.
- 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.
- 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:–20 °C to +55 °C (–4 °F to +131 °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 Rear Panel 4

3 Installation 5

3.1 Preparations 5

3.2 Desktop Mount 5

3.3 Rack Mount 5

4 Wiring 7

4.1 Connecting GND Cable 7

4.2 Connecting SFP Ethernet Port 7

4.3 Connecting Ethernet Port 8

4.4 Connecting Console Port 8

4.5 Connecting Power Cord 9

5 Quick operation 10

5.1 Login through Web 10

5.2 Restoring to Factory Settings 10

6 Initializing and Adding the Device 11

6.1 Initializing the Device 11

6.2 Webpage Initialization 11

6.3 Adding the Device 11

Appendix 1 Security Recommendation 13

1 Overview

1.1 Introduction

The device is a hardened switch. Equipped with a high-performance switching engine and large buffer memory, it features low transmission delay and high reliability. With dual-power redundant backup, it can work in environments that range from –20°C to 55°C (–4°F to +131°F). With protection against overvoltage, EMC and overcurrent from power input terminals, the device effectively resists interference from static electricity, lightning, and pulses. With web management, SNMP and other functions, the device can be remotely managed.

In addition, based on the DoLynk Care Cloud Server, this device can be managed through the DoLynk 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 ports, and the uplink ports are 10 gigabit optical ports.
- Supports STP/RSTP.
- IEEE802.1Q-based VLAN configuration.
- Static link aggregation and LACP.
- Graphical web management with simple and easy operation.
- Supports dual-power redundancy.
- EMC high protection design.
- Desktop and rack mount.

2 Port and Indicator

2.1 Front Panel

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

Figure 2-1 Front panel(electrical aggregation)

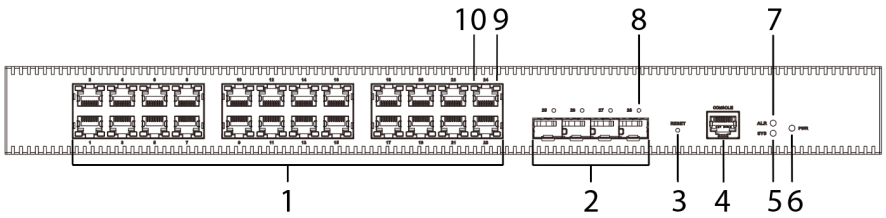


Table 2-1 Front panel description

No.	Name	Description
1	RJ-45 port	10/100/1000 Mbps self-adaptive Ethernet port.
2	SFP + Port	Supports 1/10 Gbps.
3	Reset button	Press and hold for over 5s, wait until all the indicators are solid on, and then release. The device recovers to the default settings.
4	Console port	Equipment debugging serial port.
5	System (SYS) indicator	• Flashes: The system works normally. • Off: The system is not working normally.
6	Power (PWR) indicator	• On: Power on. • Off: Power off.
7	Alarm (ALR) indicator	• On: The device has an abnormal alarm. • Off: The device has no abnormal alarm.
8	Uplink SFP+ optical port status indicator	• On: Optical ports connected to device. • Off: Optical ports not connected to device. • Flashes: Data transmission is in progress.
9	Port status indicator	• Green solid on: The port is connected to the device, and the transmission rate is negotiated to 1000 Mbps. • Green flashes: Data transmission is in progress. • Off: Not connected to device.
10		• Yellow solid on: The port is connected to the device, and the transmission rate is negotiated to 10/100 Mbps. • Yellow flashes: Data transmission is in progress. • Off: No data transmission in progress.

Figure 2-2 Front panel (optical aggregation)

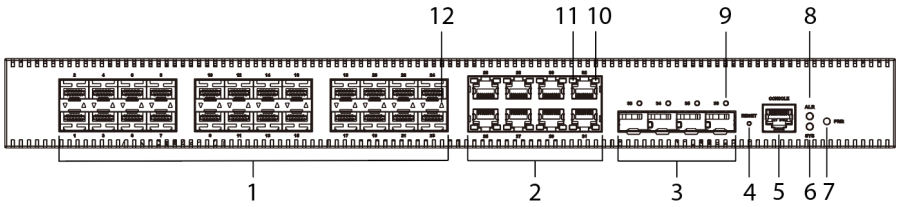


Table 2-2 Front panel description

No.	Name	Description
1	SFP Port	Supports 10/100/1000 Mbps.
2	RJ-45 port	10/100/1000 Mbps self-adaptive Ethernet port.
3	SFP + Port	Supports 1/10 Gbps.
4	Reset button	Press and hold for over 5s, wait until all the indicators are solid on, and then release. The device recovers to the default settings.
5	Console port	Equipment debugging serial port.
6	System (SYS) indicator	• Flashes: The system works normally. • Off: The system is not working normally.
7	Power (PWR) indicator	• On: Power on. • Off: Power off.
8	Alarm (ALR) indicator	• On: The device has an abnormal alarm. • Off: The device has no abnormal alarm.
9	Uplink SFP+ optical port status indicator	• On: Optical ports connected to device. • Off: Optical ports not connected to device. • Flashes: Data transmission is in progress.
10	Port status indicator	• Green solid on: The port is connected to the device, and the transmission rate is negotiated to 1000 Mbps. • Green flashes: Data transmission is in progress. • Off: Not connected to device.
11		• Yellow solid on: The port is connected to the device, and the transmission rate is negotiated to 10/100 Mbps. • Yellow flashes: Data transmission is in progress. • Off: No data transmission in progress.
12	SFP optical port status indicator	• Solid on: Connected to the device. • Flashes: Data transmission is in progress. • Off: Not connected to the device.

2.2 Rear Panel

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

Figure 2-3 Rear panel(electrical aggregation)

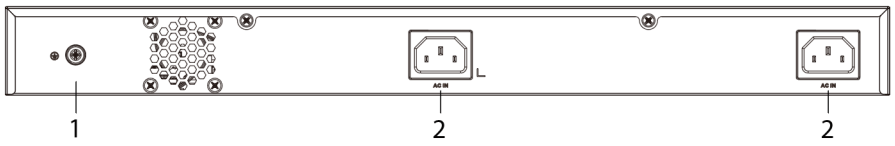


Table 2-3 Rear panel description(electrical aggregation)

No.	Description
1	Grounding screw.
2	Power interface, supporting 100-240 VAC.

Figure 2-4 Rear panel(optical aggregation)

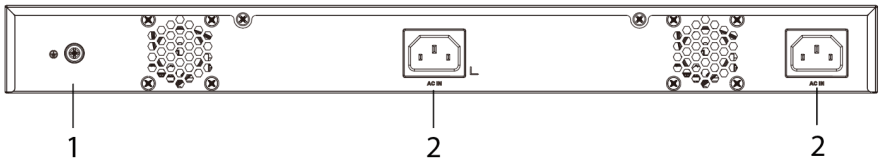


Table 2-4 Rear panel description(optical aggregation)

No.	Description
1	Grounding screw.
2	Power interface, supporting 100-240 VAC.

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

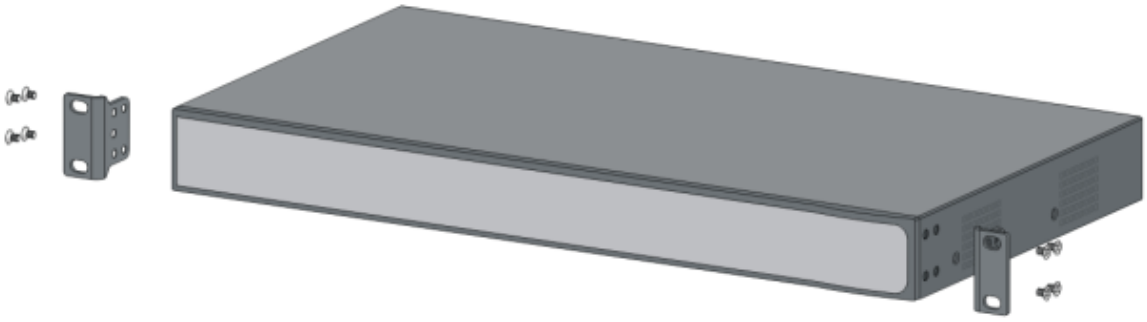
The switch supports desktop mount. Place it on a steady and stable desktop.

3.3 Rack Mount

Procedure

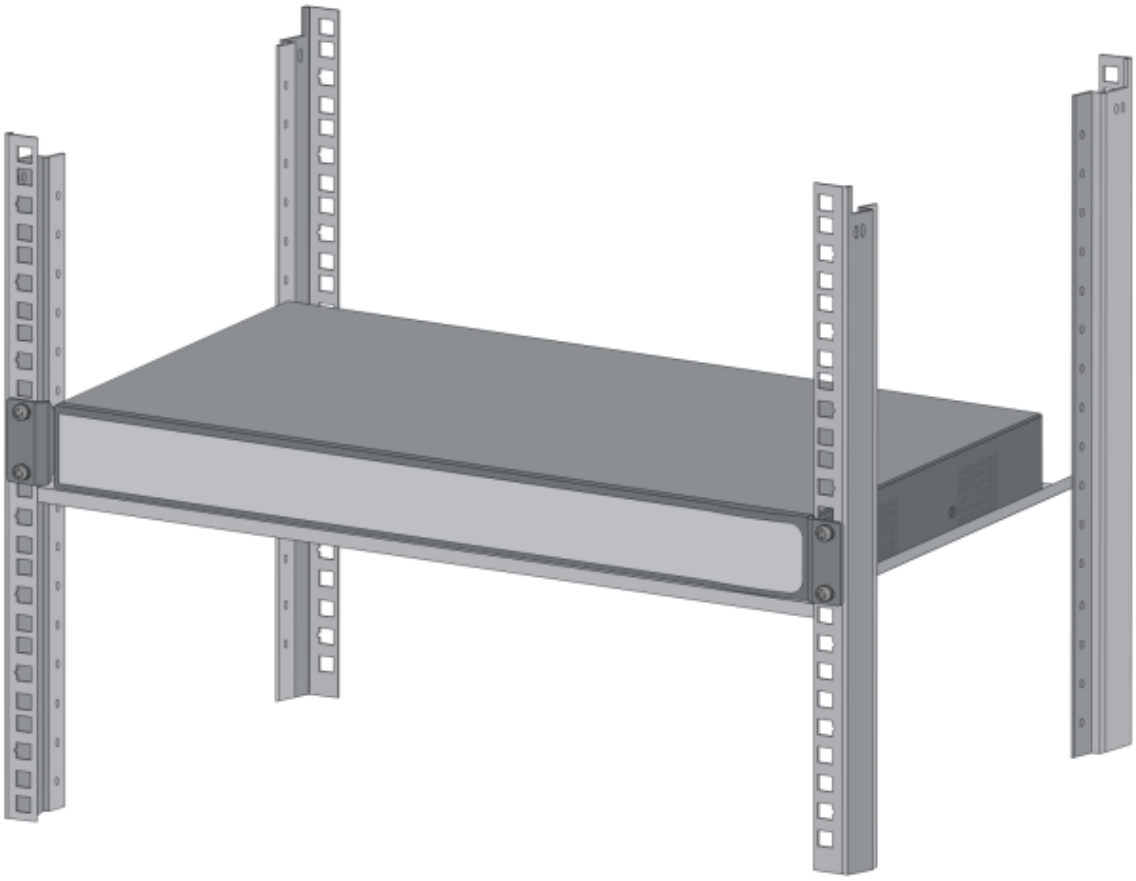
Step 1 Attach the mounting bracket to the device side panel (one on each side) and secure it with the screws provided with the rack.

Figure 3-1 Install racket



Step 2 Install the device to the rack with screws.

Figure 3-2 Install device



4 Wiring

4.1 Connecting GND Cable

There is a GND screw on the device cover board for the GND cable, which is called enclosure GND. Connect one end of the GND cable with the cold-pressed terminal, and then fix it on the enclosure GND with the GND screw. The other end of the GND cable should be reliably connected to the ground.

- Normal GND of the device is the important guarantee for device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and then power off the device before disconnecting the GND cable.
- The sectional area of the GND cable should be more than 2.5 mm^2, and the GND resistance shall be less than 4 Ω.

4.2 Connecting SFP Ethernet Port

Background Information

WARNING

The signal is transmitted through laser by optical fiber cable. The laser conforms to the requirement of level 1 laser products. To avoid injury of eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

Before installing SFP module, wear antistatic gloves, and then wear antistatic wrist strap. Make sure that the antistatic gloves and the antistatic wrist strap are in good contact.

Figure 4-1 SFP module structure

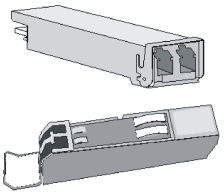
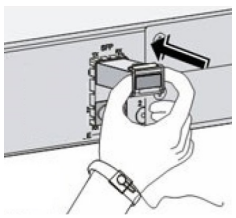


Figure 4-2 SFP module installation



Procedure

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

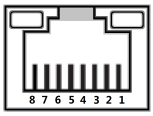
Step 2 Hold the SFP module by both sides, and then push it gently into the SFP slot till the SFP module is firmly connected to the slot.

Both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot.

4.3 Connecting Ethernet Port

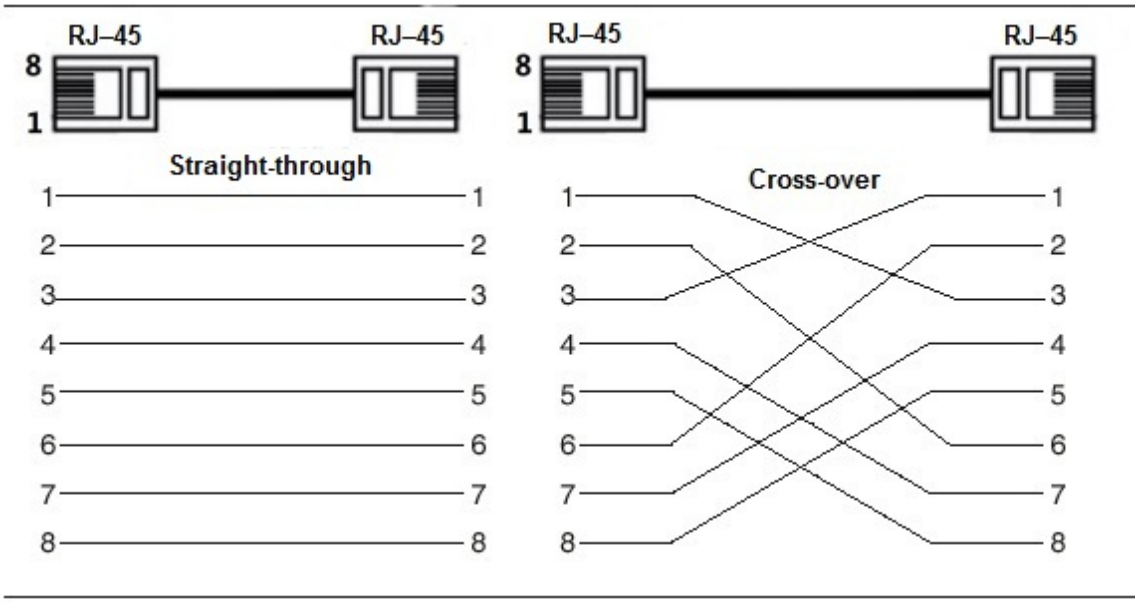
Ethernet port adopts standard RJ–45 port. Equipped with self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode, and supports MDI/MDI-X self-recognition function of the cable, which means that the switch can use cross-over cable or straight-through cable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

Figure 4-3 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).

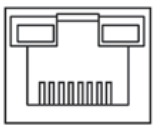
Figure 4-4 Pin description



4.4 Connecting Console Port

The switch console port and computer controlling 9-pin serial port are connected with RJ-45 DB9 cable. You can call the console software of the device by operating the superterminal software of the Windows system for device configuration, maintenance, and management.

Figure 4-5 Console port



One end of RJ–45 DB9 cable is RJ–45 connector, which needs to be inserted into the console port of the device. And the other end is DB9 plug, which needs to be inserted into the computer controlling 9-pin serial port.

Figure 4-6 Cable sequence of RJ45 DB9

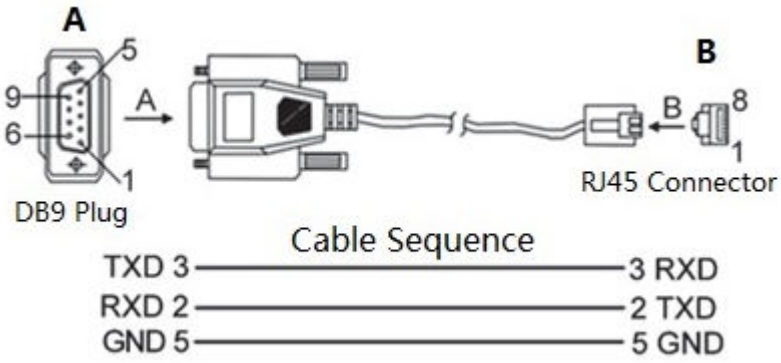


Table 4-1 Pin description

DB9 pin	RJ–45 pin	Signal	Description
2	3	RXD	Receiving data
3	2	TXD	Sending data
5	5	GND	GND

4.5 Connecting Power Cord

Background Information

Make sure that the switch is reliably grounded before connecting the power cord.

Procedure

Step 1 Connect one end of the power cord into the power jack of the device accurately.

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

5 Quick operation

5.1 Login through Web

Background Information

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	• Web: admin • iLinksView : lt_91_il_02_nmp 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.

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 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 accroding 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**.

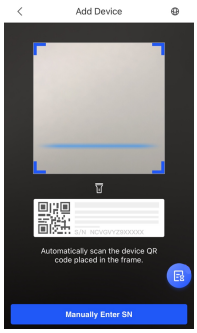
Figure 6-1 DoLynk Care app

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.

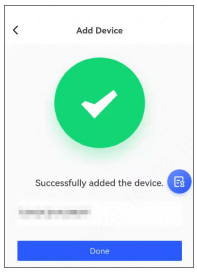
Step 4 If the Device has not been initialized, you could modify the SC Code as the initial password on the label. Enter the Device password, and then tap **Save**.

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 DoLynk 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 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**

   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;
   - 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. **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).