



Ethernet Switch (Hardened Managed Switch)

Quick Start Guide








Foreword

General

This manual introduces the installation, functions and operations of the Hardened Managed switch (hereinafter referred to as "the device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.2	<ul style="list-style-type: none">Updated the content of the GND cable.Updated the quick operation.	June 2025
V1.0.1	Updated the contents of initializing and adding the device.	January 2024
V1.0.0	First release.	August 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 to: 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 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



Stability Hazard

Possible result: The device might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

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





- 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.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operating 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.
- Ground the device to protective ground before you power it on.



- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: -30 °C to +65 °C (-22 °F to +149 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements

**DANGER**

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

**WARNING**

Power off the device before maintenance.

Table of Contents

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 Preparations.....	5
3.1 Desktop Mount.....	5
3.2 DIN-rail Mount.....	5
4 Wiring.....	6
4.1 Connecting GND Cable.....	6
4.2 Connecting SFP Ethernet Port.....	6
4.3 Connecting Power Cord.....	7
4.4 Connecting PoE Ethernet Port.....	8
5 Quick Operation.....	9
5.1 Logging in to the Webpage.....	9
5.2 Restoring the Device to Its Factory Settings.....	9
Appendix 1 Security Commitment and Recommendation.....	10

1 Overview

1.1 Introduction

The product is a hardened switch. Equipped with a high performance switching engine, the switch performs optimally. It has low transmission delay, large buffer and is highly reliable. With its full metal and fanless design, the device has great heat dissipation and low power consumption, working in environments ranging from $-30\text{ }^{\circ}\text{C}$ to $+65\text{ }^{\circ}\text{C}$ ($-22\text{ }^{\circ}\text{F}$ to $+149\text{ }^{\circ}\text{F}$). 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. In addition, through cloud management, webpage management, SNMP (Simple Network Management Protocol), and other functions, the device can be remotely managed. The device is applicable for uses in different scenarios, including buildings, homes, factories and offices.



Cloud management refers to managing this device through the DoLynk apps and webpages. Scan the QR code in the packaging box to learn how to perform cloud management operations.

1.2 Features

- Features mobile management by app.
- Supports network topology visualization.
- Supports one-stop maintenance.
- 100/1000 Mbps downlink electrical ports (PoE) and 1000 Mbps uplink electrical ports or optical ports.



The uplink ports might differ depending on different models.

- Supports IEEE802.3af, IEEE802.3at standard. Red ports support IEEE802.3bt, and are compatible with Hi-PoE. Orange ports conform to Hi-PoE.
- Supports 250 m long-distance PoE power supply.



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.
- Supports network topology visualization. ONVIF displays end devices like IPC.
- Perpetual PoE.
- VLAN configuration based on IEEE802.1Q.
- Fanless design.
- Desktop mount and DIN-rail mount.

2 Port and Indicator

2.1 Front Panel

Front Panel (100 Mbps)



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

Figure 2-1 Front panel (100 Mbps)

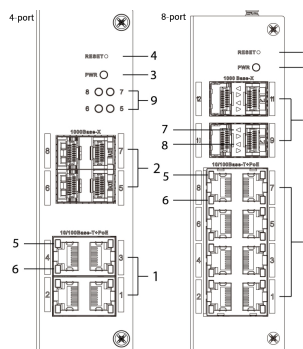


Table 2-1 Interface description

No.	Description
1	10/100 Mbps self-adaptive PoE port.
2	1000 Mbps uplink optical port.
3	Power indicator. <ul style="list-style-type: none"> ● On: Power on. ● Off: Power off.
4	Reset Button. Press and hold for over 5 seconds, wait until all the indicators are solid on, and then release. The device recovers to the default settings.
5	PoE port status indicator. <ul style="list-style-type: none"> ● On: Powered by PoE. ● Off: Not powered by PoE.
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: Data transmission is in progress.

No.	Description
7	Connection status indicator (Link) for uplink optical port. <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device.
8	Data transmission status indicator (Act) for uplink optical port. <ul style="list-style-type: none"> ● Flashes: 10 Mbps/100 Mbps/1000 Mbps data transmission is in progress. ● Off: No data transmission.
9	Connection or data transmission status indicator (Link/Act) uplink optical port. <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Data transmission is in progress.

Front Panel (1000 Mbps)

Figure 2-2 Front panel (1000 Mbps)

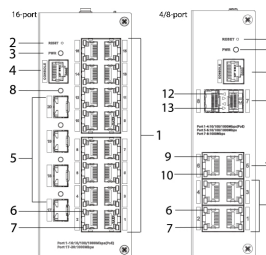



Table 2-2 Interface description

No.	Description
1	10/100/1000 Mbps self-adaptive PoE port.
2	Reset Button. Press and hold for over 5 s, wait until all the indicators are solid on, and then release. The device recovers to the default settings.
3	Power indicator. <ul style="list-style-type: none"> ● On: Power on. ● Off: Power off.
4	Console port. Serial port.
5	1000 Mbps uplink optical port.
6	PoE port status indicator. <ul style="list-style-type: none"> ● On: Powered by PoE. ● Off: Not powered by PoE.

No.	Description
7	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: Data transmission is in progress.
8	Data transmission and connection status indicator (Link/Act) for uplink optical port. <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device. ● Flashes: Data transmission is in progress.
9	Connection status indicator (Link) for Ethernet port. <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device.
10	Data transmission status indicator (Act) for Ethernet port. <ul style="list-style-type: none"> ● Flashes: 10/100/1000 Mbps data transmission is in progress. ● Off: No data transmission.
11	10/100/1000 Mbps uplink Ethernet port.  Only 4-port switches supports uplink Ethernet ports.
12	Connection status indicator (Link) for uplink optical port. <ul style="list-style-type: none"> ● On: Connected to device. ● Off: Not connected to device.
13	Data transmission status indicator (Act) for uplink optical port. <ul style="list-style-type: none"> ● Flashes: 1000 Mbps data transmission is in progress. ● Off: No data transmission.

2.2 Side Panel

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

Figure 2-3 Side panel

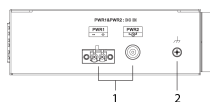


Table 2-3 Interface description

No.	Name
1	Power port, dual-power backup. Supports 53 VDC or 54 VDC.
2	Ground terminal.

3 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.

3.1 Desktop Mount

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

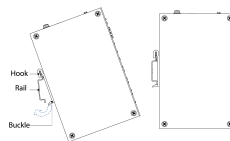
3.2 DIN-rail Mount

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



Different models support different width of the rail. 4/8-port supports 38 mm and 16-port supports 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. It is called enclosure GND.

Procedure

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



Use a yellow-green protective grounding wire with the cross-sectional area of at least 4 mm² and the grounding resistance of no more than 4 Ω.

4.2 Connecting SFP Ethernet Port

Background Information

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 4-1 SFP module structure

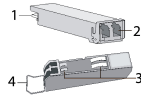
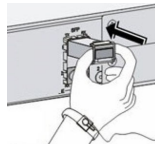


Table 4-1 Description SFP module

No.	Name
1	Gold finger
2	Optical port
3	Spring strip
4	Handle

Figure 4-2 SFP module installation



4.3 Connecting Power Cord

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

Background Information



WARNING

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



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

Figure 4-3 Power terminal

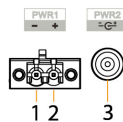


Table 4-2 Power terminal definition

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

Procedure

- Step 1 Connect the device to ground.
- Step 2 Take off the power terminal plug from the device.
- Step 3 Plug one end of the power cord into the power terminal plug and secure the power cord.



The area of power cord cross section is more than 0.75 mm² and the maximum cross section area of the wiring is 2.5 mm².

- 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.

4.4 Connecting PoE Ethernet Port

If the terminal device has a PoE Ethernet port, you can directly connect the terminal device PoE Ethernet port to the switch PoE Ethernet port through network cable to achieve synchronized network connection and power supply. The maximum distance between the switch and the terminal device is about 100 m.



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

5 Quick Operation

5.1 Logging in to the Webpage

You can log in to the webpage to perform operations on the device and manage it.



For first-time login, follow the on-screen prompts to set your password.

Table 5-1 Default factory settings

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

5.2 Restoring the Device to Its Factory Settings

There are 2 ways to restore the device to its factory settings.

- Press and hold the **Reset** button for 5 seconds.
- Log in to the webpage of the device and perform the required steps for factory reset. For information on these steps, see the user manual of the device.

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 Allowlist**

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

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