

Optical Module

Quick Start Guide



V1.0.0

Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2024

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



- 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.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.

Operating Requirements



- Place the device in a location that children cannot easily access.
- Do not disassemble the device without professional instruction.



- 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.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Category.....	1
2 Installation.....	2
Appendix 1 Security Recommendation.....	3

1 Overview

1.1 Introduction

Optical modules are designed for the transmission of optical signals through optical fiber. They exhibit low signal loss and long transmission distances, making them highly advantageous for long-distance communications. Optical module series includes both enterprise-level and industrial-grade products, each with varying levels of protection. They offer different speeds, such as 100 Mbps, 1 Gbps and 10 Gbps to accommodate optical port switches for long-range transmission. These modules are ideal for transferring optical fiber video data while setting up security monitoring points and establishing long-distance private IP data transfer networks.

1.2 Category

Single Mode Optical Fiber

The single mode in the optical module refers to the optical module used in conjunction with single mode fiber. It uses LD or LED with narrow spectrum as the light source. It can transmit data signals with extremely high bandwidth, so the transmission distance is very far. The logo on the single mode optical module is **SMF**, the optical fiber is yellow, and the wavelength is mainly near the 1310 nm and 1550 nm.



Select the corresponding optical fiber wire according to the optical module model. For single mode optical modules, select single fiber, and for multiple mode optical modules, select double fiber.

Applicable Scene

The bandwidth potential of single mode optical modules makes them become the best choice for high-speed and long-distance data transfer, and they are mostly used for long-distance transmission. Single mode optical modules can support 20 km and 40 km long-distance transmission, and the transmission rates are 155 Mbps, 1.25 Gbps, 10 Gbps, 40 Gbps and 100 Gbps and so on.

Multiple Mode Optical Fiber

The multiple mode optical module uses optical devices and multimode optical fibers to achieve the best transmission feature. It can transmit multiple modes of light. The logo on the multiple mode optical module is **MMF**.

Applicable Scene

Multiple mode optical modules are mostly used in networks with relatively short transmission distances, such as local area networks (LANs). These networks usually have many nodes, many connectors, many detours, a large number of connectors and couplings, and a large number of light sources consumed per unit optical fiber length. Consuming multiple mode optical modules can effectively reduce network costs. Multiple mode optical modules can support transmission distances of 300 m, 2 km and so on. The transmission rates are 155 Mbps, 1.25 Gbps, 10 Gbps, 40 Gbps and 100 Gbps and so on.

2 Installation

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

1. Lift the handle of SFP module upward vertically and make it get stuck to the top hook.
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 the 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 2-1 SFP module structure

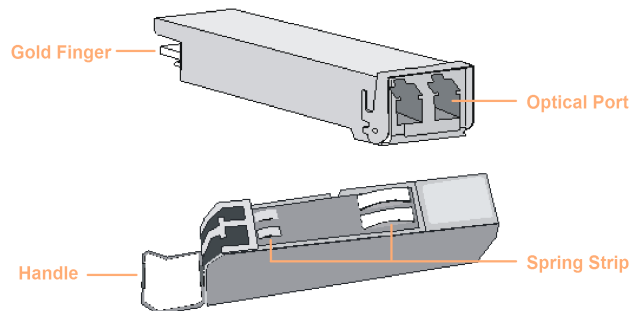
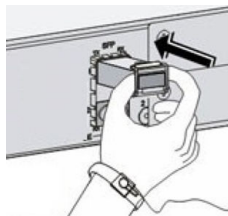


Figure 2-2 SFP module installation



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;
- 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**

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).