LUMINYS

Cloud Managed Series Switches

Quick Start Guide

sales@collsam.com
(951) 282-8707

support@collsam.com
(213) 210-6744

Foreword

General

This manual covers the installation, functions, and operation of the cloud-managed switch (referred to as "the switch"). Please read it thoroughly before use and keep it for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	September 2024

Privacy Protection Notice

As a device user or data controller, you may collect personal data such as facial images, fingerprints, and license plate numbers. It's essential to comply with local privacy laws to safeguard individuals' rights. This includes providing clear identification of surveillance areas and necessary contact information.

Disclaimer

While we strive to ensure the accuracy and completeness of this document, we do not provide any formal guarantees. The use and results derived from this document are the sole responsibility of the user. We also reserve the right to modify its contents without prior notice.

About the Manual

- This manual is for reference only and may have minor discrepancies with the actual product.
- We are not liable for damages resulting from improper operation contrary to this manual.
- The manual will be updated to align with the latest laws and regulations. For more information, refer to the paper manual, scan the QR code, use our CD-ROM, or visit our official website. Minor differences may exist between electronic and paper versions.
- All designs and specifications are subject to change without notice. Product updates may lead to discrepancies between the manual and the actual product. Contact customer service for the latest information and documentation.
- There may be errors or inaccuracies in the descriptions of functions, operations, and technical data. We reserve the right of final interpretation in case of questions or disputes.
- If the manual cannot be opened, please update your reader software or try another compatible reader.
- All trademarks and company names mentioned are the properties of their respective owners.
- For assistance, visit our website or contact your supplier or customer service.
- We reserve the right of final interpretation in case of questions or disputes.

Safety Instructions

The following symbols might appear in the manual.

Symbol	Definition
	Indicates a risk hazard that, if not avoided, may result in death, injury, property damage, data loss, decreased performance, or unpredictable outcomes.
	Offers methods to help you troubleshoot issues or save time.

Important Safeguards and Warnings

Installation Requirements

- Comply with all local electrical safety codes and standards when operating the product.
- Check if the power supply is correct before operating the product.
    - Follow the electrical requirements to power the product:
        - The power supply must conform to the IEC 60950-1 and IEC 62368-1 standards.
        - The voltage must meet SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
        - The power supply must meet LPS requirements and not exceed PS2.
    - We recommend using the power adapter provided with the product.
    - The power supply requirements (such as rated voltage) are subject to the product label.
- Do not connect the product to more than two power supplies unless otherwise specified.
- The product must be installed in a location only professionals can access to avoid the risk of non-professionals becoming injured from accessing the area while the product is in operation. Professionals must have full knowledge of the safeguards and risks when using the product.

Operation Requirements

- Do not open the cover when the product is powered on.
- Do not touch the heat dissipation component of the product.

Table of Contents

Overview

Introduction

The Luminys Cloud Managed series consists of Layer 2 commercial switches with long-distance PoE capabilities, powering devices up to 250 meters away. The 8-port and 16/24-port models offer PoE ports with a power supply of up to 90 W.

Designed with a full-metal casing, these switches ensure excellent heat dissipation and operate effectively in environments ranging from –10 °C to +55 °C (14 °F to 131 °F).

Additionally, the network topology diagram function allows for quick problem identification. These switches are suitable for various settings, including homes, factories, and offices.

Features

- 10/100 Mbps or 10/100/1000 Mbps PoE Ethernet ports; uplink ports support gigabit optical or Ethernet connections.
- White ports comply with IEEE802.3af and IEEE802.3at standards; blue ports (including port 1 on the 8-port model) conform to IEEE802.3bt standards.
- Provides long-distance power supply up to 250 meters.

  Note: In Extend Mode, the transmission distance of the PoE port is up to 250 meters 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.

- Mobile management available via app.
- Supports LLDP (Link Layer Discovery Protocol).
- Supports DHCP (Dynamic Host Configuration Protocol) Client.
- VLAN configuration based on IEEE802.1Q is supported.
- STP/RSTP is available on select models.
- Desktop and rack mounting for 16/24-port models; desktop and wall mounting for 4/8-port models.

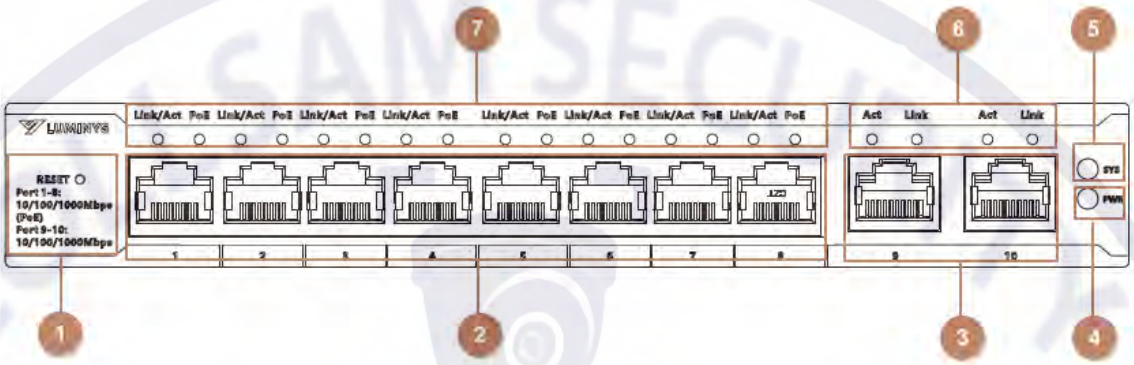
Port and Indicator

Front Panel

Front Panel (4/8-port)

The figure below uses an 8-port 1000 Mbps cloud-managed switch as an example and may differ from the actual product.

Front panel (4/8-port)



Description of front panel (4/8-port)

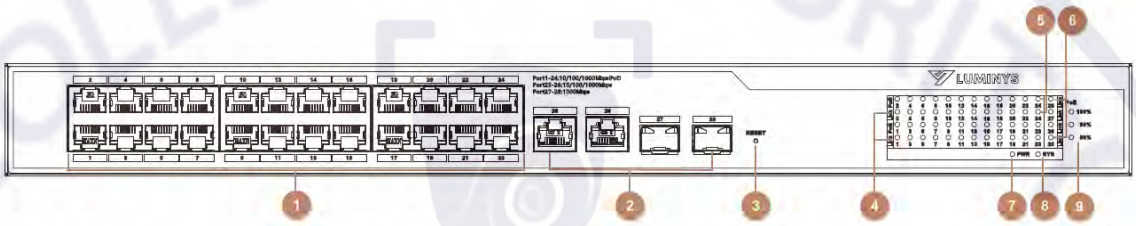
No.	Name	Description
1	Reset button	Press and hold for more than 5 seconds, then release once all panel status indicators are lit to restore the switch to default settings.
2	PoE ports	4/8 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive PoE Ethernet ports.
3	Uplink ports	10/100/1000 Mbps self-adaptive Ethernet ports. **Note:** • The number of uplink ports may vary by model; please refer to the actual product. • Some models support 1000 Mbps optical ports; consult the actual product for details.
4	Power indicator	• On: Power on. • Off: Power off.
5	System status indicator (SYS)	Flashes: The system works normally.
6	Uplink port status indicators	Link indicator. • On: Connected to device. • Off: Not connected to device.
		Activity indicator. • Flashing: Transmitting data. • Off: Not transmitting data.

No.	Name	Description
7	PoE port status indicators	PoE port status indicator. • On: Powered by PoE. • Off: Not powered by PoE.
	Link/Act indicator	Link/Act indicator. • On: Connected to device. • Off: Not connected to device. • Flashing: Transmitting data.

Front Panel (16/24-port)

The figure below uses a 16-port 1000 Mbps cloud-managed switch as an example and may differ from the actual product.

Front panel (16/24-port)



Description of front panel (16/24-port)

No.	Name	Description
1	PoE ports	16/24 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports.
2	Uplink ports	10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical ports.
3	Reset button	Press and hold for more than 5 seconds, then release once all panel status indicators are lit to restore the switch to default settings.
4	Link/Act indicator	Link/Act indicator. • On: Connected to device. • Off: Not connected to device. • Flashing: Transmitting data.
5	PoE port status indicators	PoE port status indicator. • On: Powered by PoE. • Off: Not powered by PoE.
6	Uplink port status (Link) indicators	Link indicator. • On: Connected to device. • Off: Not connected to device.
7	Power indicator	• On: Power on. • Off: Power off.
8	System status indicator (SYS)	Flashes: The system works normally.
9	PoE output power indicator	• Only solid green: PoE output power ≤ 50%. • Solid green and yellow: 50% < PoE output power ≤ 80%. • Solid green, yellow and red: 80% < PoE output power.

Rear Panel

Rear Panel (4/8-port)

The figures may vary by model; please refer to the actual product.

Figure 2-3 Rear panel (4/8 port)

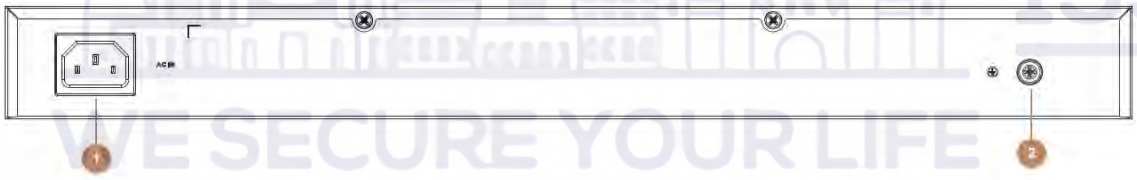
Table 2-3 Description of rear panel (4/8 port)

No.	Name	Description
1	Ground terminal	Connecting GND. **Note:** • A proper GND connection ensures lightning protection and reduces interference for the switch. Connect the GND cable before powering on the switch, and power off the switch before disconnecting the GND cable. • The GND cable must have a cross-sectional area of at least 2.5 mm^2, with a resistance of less than 4 Ω.
2	Power port	Supports 53 VDC or 54 VDC.

Rear Panel (16/24-port)

The figures may vary by model; please refer to the actual product.

Rear panel (16/24 port)



Description of rear panel (16/24 port)

No.	Name	Description
1	Power port	Supports 100–240 VAC.

No.	Name	Description
2	Ground terminal	Connecting GND. **Note:** • A proper GND connection ensures lightning protection and reduces interference. Connect the GND cable before powering on the switch, and power off the switch before disconnecting the GND cable. • The GND cable must have a cross-sectional area of at least 2.5 mm^2, with a resistance of less than 4 Ω.

Installation

Different installation methods apply to various models. Please choose the appropriate method as needed.

Preparation

- Choose the appropriate installation method as needed.
- Install the switch on a solid, flat surface.
- Leave approximately 10 cm of open space around the switch for heat dissipation and proper ventilation.

Desktop Mount

The switch supports desktop mounting and can be placed directly on a solid, flat surface.

Rack Mount

Follow the steps below to install the switch on a rack.

1. Attach the mounting brackets to each side of the switch and secure them with the provided screws.
2. Mount the switch onto the rack.

Wall Mount

Follow the steps below to install the switch on a wall.

1. Drill two M4 screws into the wall, leaving a 4 mm gap between the wall and the screw heads.

   Note:
   - Screws are not included; purchase as needed.
   - Ensure the distance between the screws matches the wall-mount hole spacing (77.8 mm for the 4-port switch and 128.4 mm for the 8-port switch).

2. Align the wall-mount holes on the device's back cover with the screws and hang the device on them.

Wiring

Connecting GND

A proper GND connection is essential for ensuring lightning protection and reducing interference for the device. Follow the steps below to ensure correct connection.

1. Remove the ground screw from the device and set it aside. Insert the ground screw through the round hole of the OT terminal of the ground cable, then turn the screw clockwise with a cross screwdriver to secure the OT terminal.
2. Use needle-nose pliers to curl the other end of the ground cable into a loop.
3. Connect the looped end of the ground cable to the ground bar and tighten the hex nut clockwise with a wrench to secure it to the ground terminal.

Connect GND

Connecting Power Cord

Before connecting the power cord, ensure that the device is properly grounded. Follow the steps below to connect the power cord.

1. Connect one end of the power cord into the power jack of the device accurately.
2. Connect the other end of the power cord to the external power socket.

Connecting Ethernet Port

The Ethernet port features a standard RJ-45 connector with self-adaptive functionality, automatically configuring to full or half-duplex operation. It supports MDI/MDI-X cable recognition, allowing you to use either crossover or straight-through cables to connect terminal devices to the network.

Connecting SFP Ethernet Port

- Avoid touching the gold finger of the SFP optical module during installation.
- Do not remove the dust plug from the SFP optical module until you are ready to connect the optical fiber.
- Ensure the optical fiber is unplugged before inserting the SFP optical module into the slot.

Follow the steps below to connect the SFP ethernet port.

1. Wear an antistatic wristband, ensuring it is in good contact with your skin and that the device is properly grounded.
2. Raise the handle of the SFP optical module vertically and hold the module on both sides.
3. Gently push the optical module into the slot horizontally until it is securely connected.
4. Remove the dust cap from the LC connector of the optical fiber and the dust plug from the SFP optical module.
5. Connect the LC connector of the optical fiber to the SFP optical module.

Connecting PoE Ethernet Port

You can connect the device's PoE Ethernet port directly to the switch's PoE Ethernet port using a network cable for simultaneous network connection and power supply. When Extend Mode is disabled, the maximum distance between the switch and the device is approximately 100 meters.

- An isolated power supply is required when connecting to a non-PoE device.

Initializing the Switch

You can log in to the webpage to initialize the device and modify the IP address when the device is not connected to the Internet.

Note:

- Device initialization is required for first-time use or after a reset.
- DHCP Client is enabled by default. If no IP address is assigned, you can use the default IP address (usually 192.168.1.100, as indicated on the device label).
- LumiUtility can only detect the device. LumiUtility cannot be used to initialize the device.
- The switch and computer must be on the same network segment to be initialized.
- Plan the network segment accordingly to connect the switch.

Appendix 1 Cybersecurity Recommendations

Account Management

1. **Use complex passwords.**
   - The password should be at least 8 characters long.
   - Include at least two types of characters: uppercase letters, lowercase letters, numbers, and symbols.
   - Avoid using the account name or its reverse.
   - Do not use consecutive characters (e.g., 123, abc).
   - Do not use repeating characters (e.g., 111, aaa).
2. **Change passwords periodically.**
   It's advisable to regularly change the device password to minimize the risk of it being guessed or cracked.
3. **Allocate accounts and permissions appropriately.**
   Add users based on service and management needs, assigning the minimum necessary permissions.
4. **Enable account lockout function.**
   The account lockout function is enabled by default. Keep it enabled to enhance account security; after multiple failed login 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 a password reset function. To reduce the risk of unauthorized access, update this information promptly if there are any changes. When setting security questions, avoid using easily guessed answers.

Service Configuration

1. **Enable HTTPS**
   It's recommended to enable HTTPS for secure access to web services.
2. **Encrypted transmission of audio and video**
   If your audio and video data contents are important or sensitive, use encrypted transmission function to reduce the risk of your audio and video data being eavesdropped on during transmission.
3. **Turn off non-essential services and use safe mode**
   It's advisable to disable services such as SSH, SNMP, SMTP, UPnP, and AP hotspot when not in use or required to reduce attack surfaces. If these services are necessary, consider the following safe modes:
   - SNMP: Use SNMP v3 with strong encryption and authentication passwords.
   - SMTP: Use TLS for accessing the mailbox server.
   - FTP: Use SFTP with complex passwords.
   - AP Hotspot: Use WPA2-PSK encryption with complex passwords.
4. **Change HTTP and other default service ports**
   It is advisable to change the default ports for HTTP and other services to any port between 1024 and 65535 to reduce the risk of being targeted by threat actors.

Network Configuration

1. **Enable Allow list**
   It is recommended to enable the allow list function and only permit IP addresses on the allow list to access the device. Be sure to add your computer's IP address and any supporting device IP addresses to the allow list.
2. **MAC address binding**
   It is advisable to bind the gateway's IP address to the device's MAC address to mitigate the risk of ARP spoofing.
3. **Build a secure network environment**
   To enhance device security and reduce potential cyber risks, the following measures are recommended:
   - **Disable Port Mapping**: Turn off the port mapping function on the router to prevent direct access to internal devices from the external network.
   - **Network Partitioning**: Based on actual network needs, partition the network. If there is no communication requirement between two subnets, consider using VLANs and gateways to achieve network isolation.
   - **Implement 802.1x Access Authentication**
     Establish an 802.1x access authentication system to minimize the risk of unauthorized terminal access to the private network.

Security Auditing

1. **Check online users**
   Check online users regularly to identify illegal users.
2. **Check device log**
   Review logs to learn about the IP addresses attempting to log in and track key operations performed by authorized users.
3. **Configure network log**
   The device can only retain a limited number of logs. To save logs for an extended period, it's recommended to enable the network log function to synchronize critical logs to a network log server for future reference.

Software Security

1. **Update firmware in time**
   It is important to update device firmware to the latest version to ensure access to the latest features and security enhancements. If the device is connected to the public network, enable the automatic detection function for online upgrades to receive timely firmware update notifications from the manufacturer.
2. **Update client software in time**
   It is recommended to download and use the latest client software.

Physical Protection

It is recommended to implement physical protection for devices, especially storage devices. Consider placing them in a dedicated machine room or cabinet and establish access control and key management to prevent unauthorized personnel from damaging hardware and peripheral equipment (e.g., USB flash drives, serial ports).