LUMINYS

SUL-10MLA

8-Port LumiPower Unmanaged Megabit Switch (PoE++)

User Manual

sales@collsam.com
(951) 282-8707

support@collsam.com
(213) 210-6744

Foreword

General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the 8-Port LumiPower switch (referred to as “the device”). Please read it carefully before using the platform and store it safely for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	September 2025

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 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.

Symbol	Definition
	Offers methods to help you troubleshoot issues or save time.
	Provides more context and information.

Important Safeguards and Warnings

Transportation and Storage Requirements

- Only transport and store the device under the allowed humidity and temperature conditions.

Installation Requirements

- Follow local electrical codes and safety standards. Ensure stable voltage that meets the device’s power requirements.
- Workers at heights must use safety gear, including helmets and harnesses.
- Do not place the device in direct sunlight or near heat sources.
- Keep away from moisture, dust, and smoke.
- Place in a ventilated area and avoid blocking airflow.
- Use only the adapter or cabinet power supply provided by the manufacturer.
- The power supply must meet ES1 requirements of IEC 62368-1 and not exceed PS2. Always follow the label on the device.
- Do not connect the device to multiple power supplies, to prevent damage.
- The device is a Class I appliance; connect it to a grounded socket.
- Ground with copper wire of at least 2.5 mm^2 and resistance no higher than 4 Ω.
- Use a voltage stabilizer and surge protector if required by site conditions.
- Leave at least 10 cm clearance on the sides and top for heat dissipation.
- Ensure the power plug and coupler remain accessible to disconnect power when needed.

Operation Requirements

- Do not disassemble the device without professional guidance.
- Operate only within the rated power input and output.
- Verify the power supply before use.
- Power off the device before removing wires to avoid injury.
- Do not unplug the power cord while the adapter is powered on.
- Use only within the specified humidity and temperature range.
- Keep liquids away from the device, and do not place containers with liquid on top.
- This is a Class A product; in home environments it may cause radio interference, requiring corrective measures.
- Do not block the ventilation with items such as newspapers, cloths, or curtains.
- Keep open flames, such as candles, away from the device.

Maintenance Requirements

- Shut down the device before performing maintenance.
- Label critical components on the circuit diagram with warning markers.

Table of Contents

Introduction

About the Device

The 8-Port LumiPower Switch is a Layer 2 hardened switch that supports long-distance Ethernet power supply. It includes eight 10/100 Mbps Ethernet ports, one 1000 Mbps Ethernet port, and one 1000 Mbps fiber port. It offers three self-adaptive modes—IEEE, E100, and E10—and supports transmission over both twisted pair and coaxial cable.

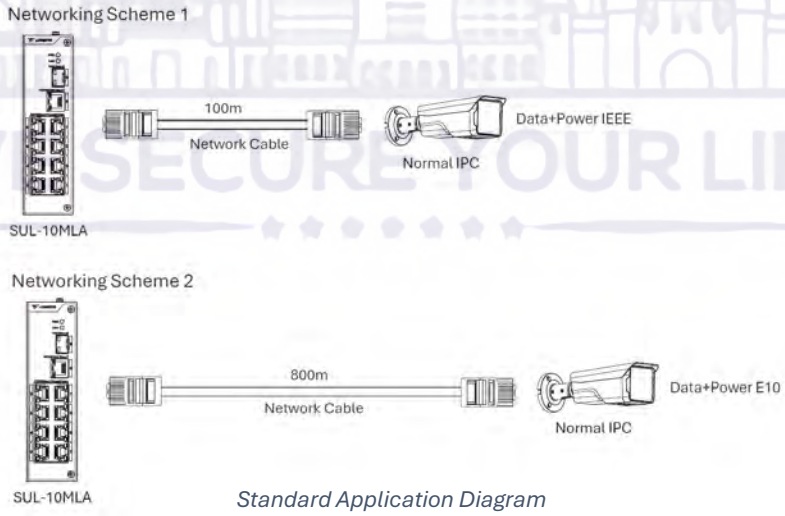
Features

Permission Management

- Layer 2 hardened PoE switch.
- Supports IEEE802.3, IEEE802.3u, IEEE802.3ab/z, and IEEE802.3X standards.
- 4K MAC address capacity with auto learning and aging.
- Supports MDI/MDIX auto-sensing.
- Ports 1 to 8 are RJ-45, 10/100 Mbps auto-sensing, supporting IEEE802.3af, IEEE802.3at, and IEEE802.3bt (Ports 1to 2) PoE standards. Port 9 is RJ45, 10/100/1000 Mbps auto-sensing.
- Designed for wide industrial temperature ranges.
- Metal housing construction.
- Equipped with one 1000 Mbps auto-sensing fiber port, one 10/100/1000 Mbps auto-sensing RJ45 port, and eight 10/100 Mbps auto-sensing RJ45 ports.
- Ports 1 and 2 support IEEE802.3bt 90 W PoE.
- Provides three transmission modes: IEEE, E100, and E10. Over twisted pair, IEEE mode supports up to 100 m, E100 up to 300 m, and E10 up to 800 m. Over coaxial, IEEE supports up to 100 m, E100 up to 400 m, and E10 up to 1000 m (Ethernet over Coax converter required).
- Uses a 120 W power adapter.

Standard Application Diagram

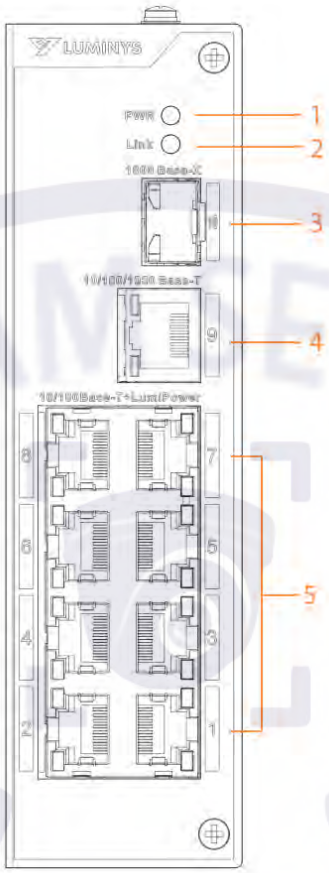
Below is a diagram of a standard application for the device.



Standard Application Diagram

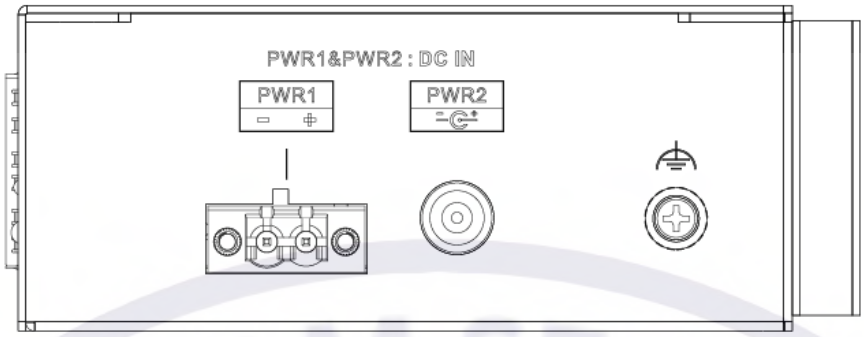
Structure

Front Panel



Number	Name	Description
1	PWR	Power and PoE status indicator. The power indicator LED shows PoE status with three states: single port powered, single port not powered, and device overload. • A single flash means the device is powering off. • A double flash means the device is powering on.
2	Link/Act	Fiber port status LED. The port indicator LED shows the active transmission mode: IEEE, E100, or E10. • If the LED is continuously on, the transmission mode is IEEE. • If the LED is on for three seconds and off for one second, the transmission mode is E100. • If the LED is on for one second and off for one second, the transmission mode is E10.
3	100/1000 Base-X	1000 Mbps auto-sensing fiber port.
4	10/100/1000 Base-T	10/100/1000 Mbps auto-sensing RJ-45 port.
5	10/100 Base-T	Eight (8) 10/100 Mbps auto-sensing PoE R-J45 ports.

Rear Panel



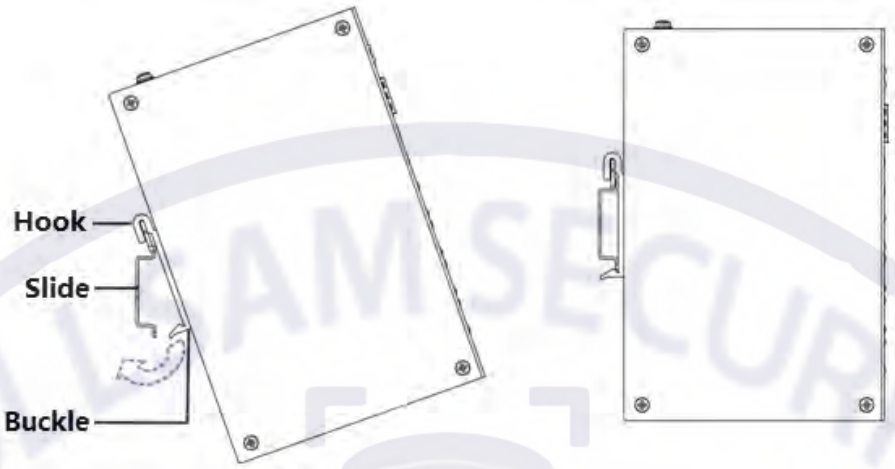
Parameter	Function
PWR1	Supports 48—57 VDC.
PWR2	Supports 48—57 VDC.
⏚	Ground wire.

PoE Power Supply

- Six (6) 100 Mbps R-J45 ports supporting IEEE802.3af and IEEE802.3at PoE standards.
- Two (2) 100 Mbps RJ-45 ports supporting IEEE802.3af, IEEE802.3at, and IEEE802.3bt 90 W PoE.
- Total PoE power usage must not exceed the device's reserved PoE capacity (120 W).

Installation

The product supports DIN rail installation. Place the switch hook on the rail, then press the LumiPower switch until the buckle locks into the slot. The slide width is 38 mm.



DIN Rail Mount Installation

Appendix: LumiPower Supply Specifications

CAT Cable

Cable Length (m/ft)	Communication Bandwidth (Mbps)	PoE Max. Load Capacity (W)	IEEE802.3bt Max. Load Capacity (W)	Network Operating Mode
100 m (328 ft)	100	25.5	71.3	IEEE/E100
200 m (656 ft)	100	25.5	52	E100
300 m (984 ft)	100	25.5	40	E100
400 m (1,312 ft)	10	23	30	E10
500 m (1,640 ft)	10	20	25	E10
800 m (2,625 ft)	10	13	13	E10

RG-59 Coaxial Cable

Cable Length (m/ft)	Communication Bandwidth (Mbps)	PoE Max. Load Capacity (W)	Network Operating Mode
100 m (328 ft)	100	25.5	IEEE/E100
200 m (656 ft)	100	25.5	E100
300 m (984 ft)	100	22	E100
400 m (1,312 ft)	100	15	E100
500 m (1,640 ft)	10	12	E10
800 m (2,625 ft)	10	8	E10
1,000 m (3,281 ft)	10	6	E10

Appendix: Cybersecurity Recommendations

Account Management

1. Use complex passwords.

Follow the guidelines below to create a strong password:

- 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 permission 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. Change passwords periodically.

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. Allocate accounts and permission appropriately.

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. Enable account lockout function.

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 Allowlist.

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 logs.

Review logs to learn about the IP addresses attempting to log in and track key operations performed by authorized users

3. Configure network logs.

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 on 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 on 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).