LUMINYS

Cloud Managed Series Switches

User Manual

sales@collsam.com
(951) 282-8707

HTTPS://COLLSAM.COM

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	October 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 is 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.

Cloud Management

Follow the steps below to set up a LumiCloud account and add devices to the platform.

Creating a LumiCloud Account

You must create an account to use LumiCloud. Features such as trusting devices and purchasing service packages will require company authentication in addition to account creation.

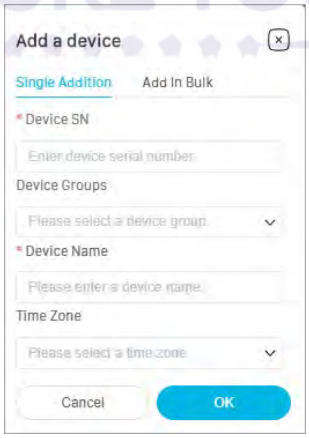
1. Navigate to the LumiCloud webpage.
2. Click **Sign Up**.
3. Enter your email address, password, and installer number. You will be emailed a verification code to complete registration.
4. Enter the verification code and click **Sign Up**.

Adding a Device

1. Login to your LumiCloud account.
2. Click on the home page and then select **Network**.
3. Click **Add Device**. Select **Single Addition** or **Add in Bulk**.

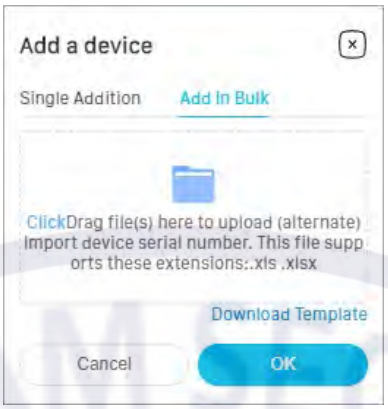
Single Addition

1. Enter device SN, device name, select a device group and time zone.
2. Click **OK**.



Add in Bulk

1. Download the template file and enter the device SNs and device names.
2. Upload the template file to import device information.
3. Click **OK**.



Setup and Login

The Luminys Cloud Managed series has web access functionality, allowing you to log in to the web interface to manage and configure the device.

Initialization

Prerequisites

Ensure the following requirements are met before initializing your device:

- Confirm the device is connected to a power source.
- Ensure the device is connected to your computer and the IP addresses of both devices are on the same network.
- By default, DHCP is enabled on the device. The device will receive an IP address from a DHCP server when connected to a network. You can retrieve the device's IP address from an upstream device such as a router. If no DHCP server is available, the default IP address for the device will be **192.168.1.100**.

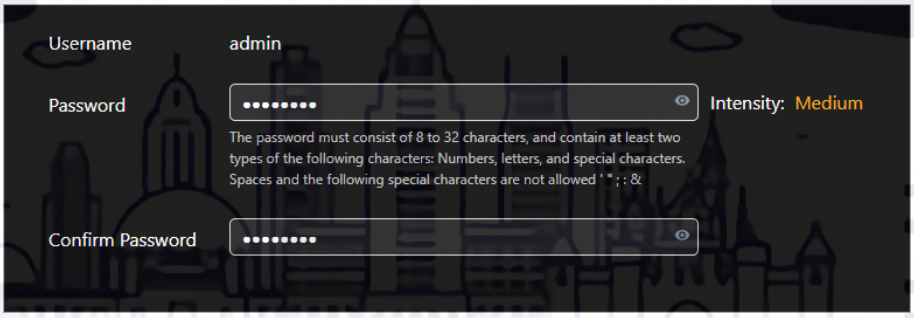
  You can use LumiUtility to obtain the IP address of specific devices.

Initializing Your Device

Follow the steps below to initialize the device prior to use.

1. Go to the password setup page by entering the camera's IP address in your browser's address bar.
2. Choose your preferred language and click **Next**.
3. Input the desired password. Click the **Complete** when done.

   - The default username is **admin**.
   - Your password must be 8–32 characters with at least two types of characters (numbers, letters, and any visible characters other than' " ; : &).



Logging in to Your Device

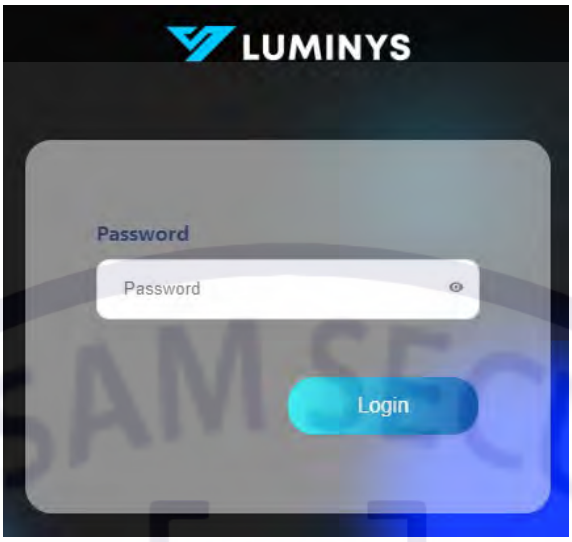
Prerequisites

Ensure the following requirements are met before logging in to your device:

- Confirm the device has been initialized.
- Ensure the device is connected to your computer and the IP addresses of both devices are on the same network.

Log in to Your Device

1. Go to the login page by entering the camera's IP address in your browser's address bar.
2. Enter your password and click **Login**.



Navigating the Home Page

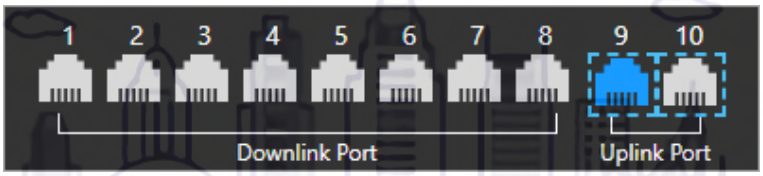
After logging in, the system will redirect you to the Home page. The left side of the page contains a menu bar. At the top, you can view the status of each port. In the upper-right corner, you have options to hide or display port information, log out, restart the device, switch system languages, and scan QR codes for additional information.

The home page may differ from the image shown below.

Port Key

- **Blue**: Connected to device.
- **Grey**: Not connected to device.

You can hover over a port icon to view its connection infrormation, status, and power consumption. You can also click a port to go to the port page to view this information.



Homepage Information

The homepage supports the following functions.

- **Device Information**: Configure the device name, management VLAN, and cloud management.

  After enabling management VLAN, you can only access the webpage of the device through a management VLAN IP address.

- **Port Information**: Displays the link status, flow control status, and VLAN mode of each port.

Port Parameter Descriptions

Parameter	Description
Port	Displays all device ports.
Port description	Configure the port description. Alternatively, you can navigate to **Switch Config** and then click **Port** to set the port description.

Parameter	Description	
Link Status	• The port is connected if the port rate and duplex mode are displayed. • The port is disconnected if the link status reads DOWN.	
Flow Control Status	View the status of the flow control function, including **On** and **Off**. You can navigate to **Switch Config** and the click **Port** to configure.	
VLAN Mode	Includes **Access** and **Trunk**.	
PVID	The VLAN of the port.	You can navigate to **Switch Config** and the click **Port** to configure.
Tagged VLAN	The VLAN ID for the port that is allowed to be tagged when sending packets.	
Untagged VLAN	The VLAN ID for the port that is allowed to be untagged when sending packets.	
TX/RX Rate	The current reception or sending rate divided by the negotiated rate for a time period (usually 5 minutes).	
Media Type	• **COPPER**: RJ-45 port. • **FIBER**: Fiber port.	

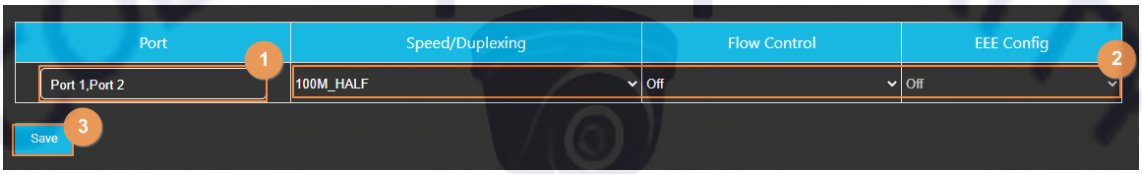
Configuration

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

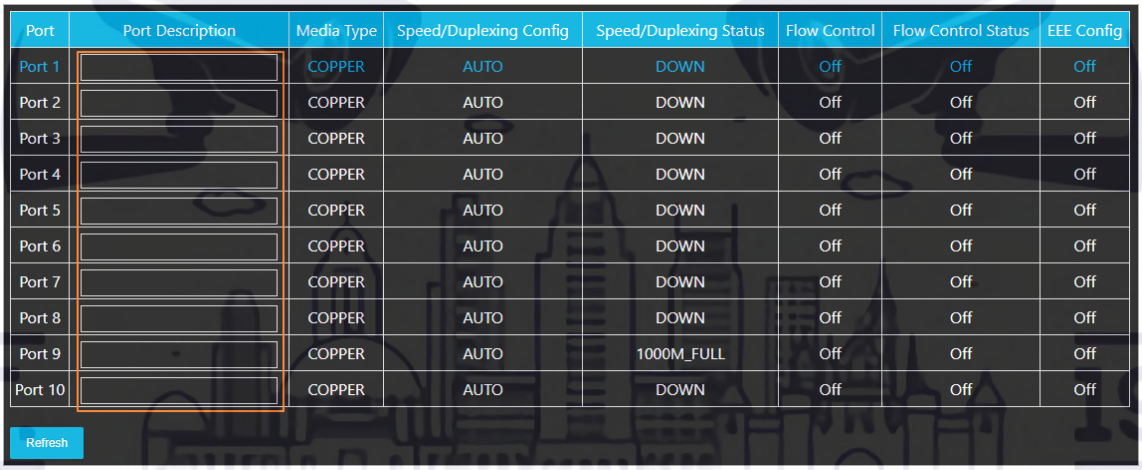
Configuring Port Information

You can configure the port parameters, including speed/duplexing and flow control. The port parameters will directly affect the working mode of the port.

1. Navigate to **Switch Config** and click **Port**.
2. Select the port number, configure the parameters, and then click **Save**.
   - **Speed/Duplexing**: Configure the speed and the duplex mode. The speed/duplexing is set as **Auto** for combination ports.
   - **Flow Control**: Enable the flow control function to prevent network congestion, reduce data loss, and improve network stability and data reliability.
   - **EEE Config**: Enable the EEE (Energy-Efficient Ethernet) function to reduce power consumption when the network is idle.



3. In the **Port Description** box, enter the description of the port. The description cannot exceed 16 characters and can only use letters, numbers, and any visible characters other than' " ; : &.



Port Parameter Descriptions

Parameter	Description
Media Type	• **COPPER**: RJ-45 port. • **FIBER**: Fiber port
Speed/Duplexing Config	Displays speed and duplex mode.
Speed/Duplexing Status	• The port is connected if the port rate and duplex mode are displayed. • The port is disconnected if the link status reads DOWN.
Flow Control Status	Displays the current flow control status.
EEE Config	Displays whether the EEE function is enabled.

Configuring a VLAN

You can assign the port to a VLAN. By default, the VLAN is set to VLAN1.

Definition of a VLAN

A Local Area Network (LAN) can be logically divided into multiple subsets, each with its own broadcast domain, known as a Virtual LAN (VLAN). VLANs are created logically rather than physically, allowing isolation of broadcast traffic within each VLAN.

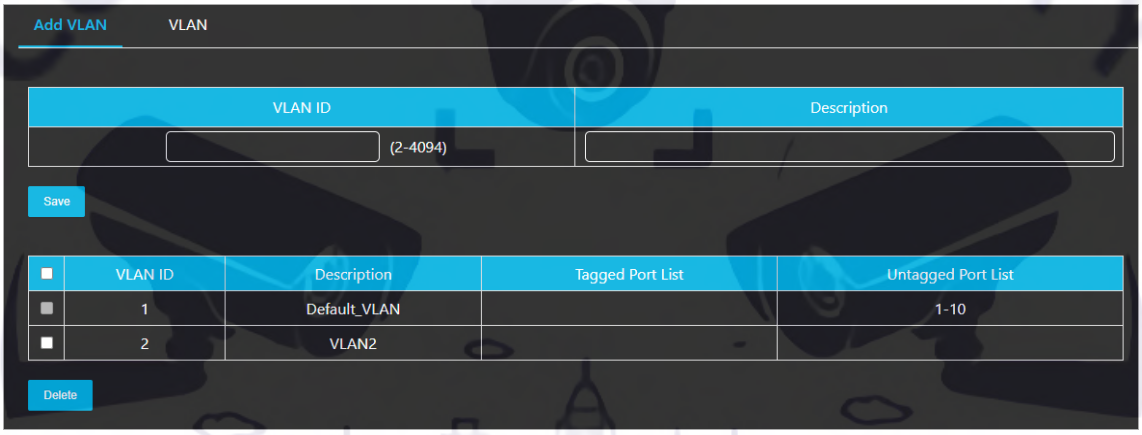
There are two main port types:

- **Access Port:** This port is assigned to a single VLAN and is typically used to connect to end devices like computers.
- **Trunk Port:** This port allows traffic from multiple VLANs to pass through, enabling the transmission and reception of messages from various VLANs. It is commonly used for inter-switch connections.

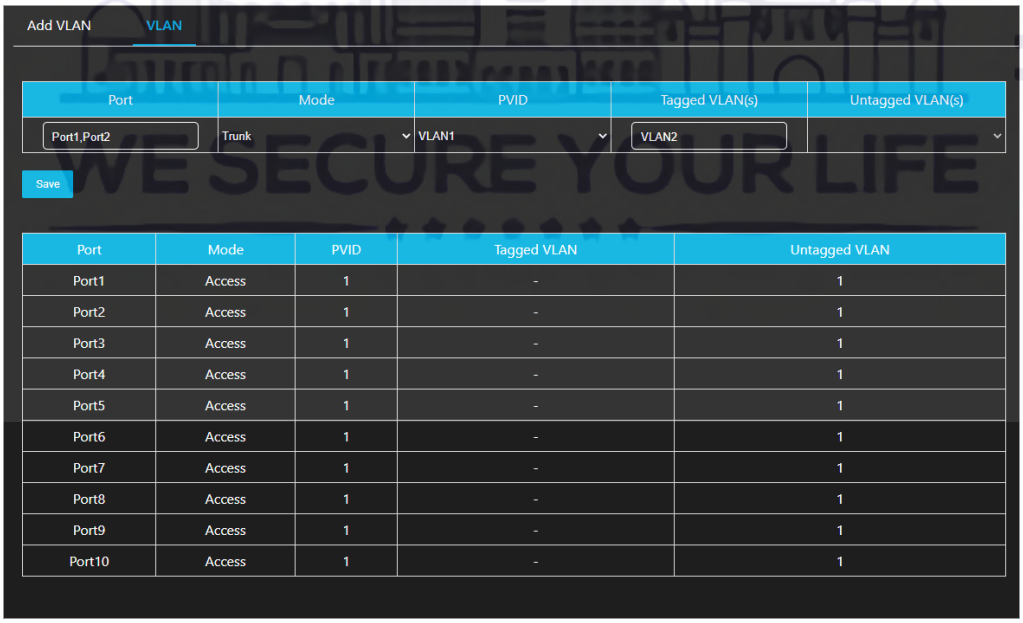
Add and Configure a VLAN

1. Navigate to **Switch Config** > **VLAN** > **Add VLAN**.
2. Enter the VLAN ID and description. Click **Save** when done.

To delete the VLAN, select it and then click delete. VLAN1 cannot be deleted.



3. Click the **VLAN** tab to configure the port VLAN parameters.
4. Select one or more ports.
5. Select the VLAN mode, including **Access** and **Trunk**.



6. Configure the PVID, tagged VLAN, and untagged VLAN. Click **Save** when done.

- **Access Mode**: When the port is in Access mode, you need to configure the untagged VLAN. The untagged VLAN specifies the VLAN ID that the port uses to send packets without VLAN tags.
- **Trunk Mode**: In Trunk mode, you should configure both the PVID and the tagged VLAN. The PVID (Port VLAN ID) indicates the default VLAN to which the port belongs, and by default, it is set to VLAN 1. The tagged VLAN determines which VLAN IDs are allowed to be tagged when sending packets through the port.

Frame Processing Comparison

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access	When the port receives an untagged frame, it adds a VLAN tag with the default VLAN ID (PVID) to the frame.	• Accepts the tagged frame if the frame's VLAN ID matches the default VLAN ID. • Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	After the PVID tag is removed, the frame is transmitted.
Trunk	• Adds a tag with the default VLAN ID to an untagged frame and accepts the frame if the interface allows the default VLAN ID. • Adds a tag with the default VLAN ID to an untagged frame and discards the frame if the interface denies the default VLAN ID.	• Accepts a tagged frame if the VLAN ID in the frame is allowed by the interface. • Discards a tagged frame if the VLAN ID in the frame is not permitted by the interface.	• If the frame's VLAN ID matches the default VLAN ID and is permitted by the interface, the device removes the tag and transmits the frame. • If the frame's VLAN ID differs from the default VLAN ID but is still permitted by the interface, the device will transmit the frame without modifying the tag.

PoE Management

PoE (Power over Ethernet) allows the device to supply power remotely to Powered Devices (PD) through Ethernet cables via its electrical ports. This feature enables centralized power distribution and easy backup, eliminating the need for external power sources for network terminals, as they only require a single network cable for both power and data. Non-PoE switches do not support this functionality.

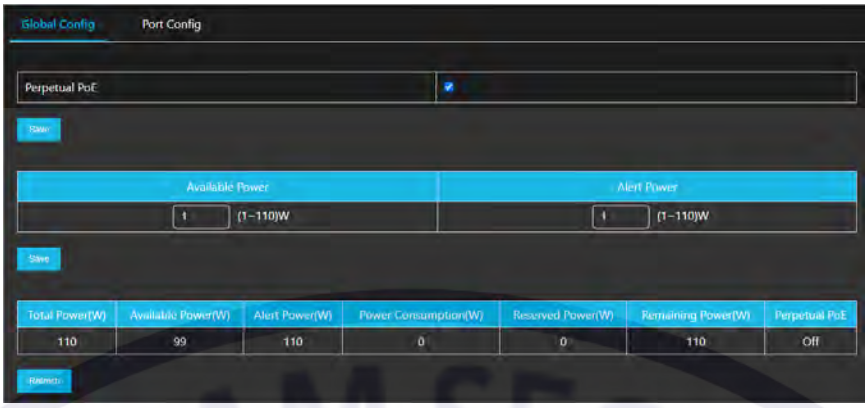
Global Configuration

Follow the steps below to configure perpetual PoE, available power, and alert power.

1. Navigate to **Switch Config → PoE → Global Config**.
2. Select **Perpetual PoE** and click **Save** to allow PoE-powered devices to continue receiving power even after a device restarts.
3. Configure available power and alert power. Click **Save** when done.

   - The total power, available power, alert power, power consumption, reserved power, remaining power and perpetual PoE are displayed at the bottom of the page. The reserved power is the total power minus the alert power.
   - The alert power must be set higher than the available power.
   - Available power refers to the maximum power that can be supplied to powered devices. New powered devices can be powered on as long as the total power consumption is below the available power.

- During operation, actual power usage may fluctuate. If power consumption exceeds the alert power, ports will be powered off in order of priority, starting with the lowest-priority ports (higher port numbers) until the total power usage falls below the alert power.



Port Configuration

Follow the steps below to configure the PoE function of the port.

1. Navigate to **Switch Config → PoE → Port Config**.
2. Select the port number and enable the PoE, long distance PoE, PoE watchdog, and force PoE as needed. Click **Save** when finished.
   - **PoE**: The device connects Powered Devices (PD) using network cables to supply remote power through its Ethernet electrical ports.
   - **Long-Distance PoE**: After you enable long distance PoE, the maximum transmission distance will change from 100 m to 250 m. Transmission speed will be reduced to 10 Mbps.

     Transmission distances might vary due to power consumption of connected devices and the cable type and status.
   - **PoE Watchdog**: When PoE watchdog is enabled, you can monitor Powered Devices (PD) to ensure they remain online by checking their status at specified time intervals. If no data transmission is detected, the PoE port will automatically power off and restart the PD.

     The time intervals for monitoring PD device status increase progressively, starting from 1 minute and doubling each time (1, 2, 4, 8, 16 minutes, and so on), with a maximum interval of 1024 minutes.
   - **Force PoE**: When the powered device connected to the port is a non-standard device, this function allows you to force the PoE power supply to ensure it receives power.

     ⚠
     - After enabling Force PoE, the port will supply power to the connected powered device, regardless of whether it meets the standard requirements.
     - Force PoE and PoE watchdog cannot be enabled at the same time.

Description of PoE Parameters

Parameter	Description
Level	Displays the power supply level of the terminal devices. The power supply level ranges from 0 through 8.
Power Consumption (W)	Displays the current PoE power consumed by the corresponding single port.
PoE Enable	Displays whether PoE is enabled for the port.
Long Distance PoE	
PoE Watchdog	
Force PoE	

Security

Port Isolation

Port isolation ensures Layer 2 message isolation between ports. This function enhances network security and offers users a more flexible networking solution. Follow the steps below to enable port isolation.

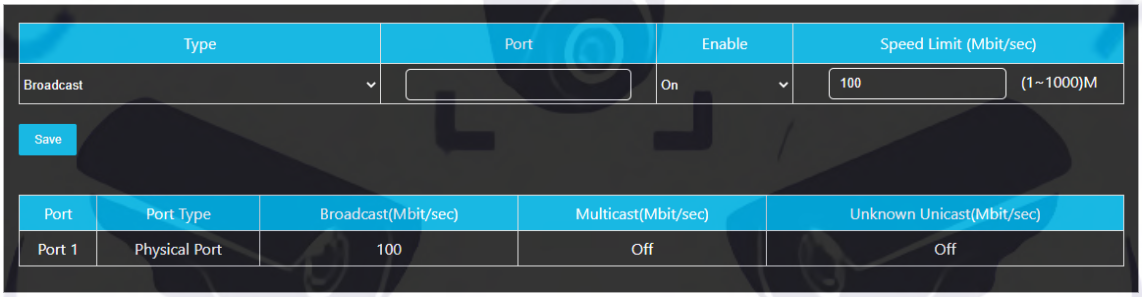
1. Navigate to **Security → Port Isolation**.
2. Enable port separation and click **Save**.

   After port isolation is enabled, only downlink ports will be isolated. Data can only be transferred between uplink and downlink ports.

Storm Control

Broadcast frames can continuously circulate on the network, disrupting communication, and degrading performance. Storm control limits broadcast traffic on a port by discarding frames that exceed a specified threshold, reducing the risk of broadcast storms and ensuring proper network operation. Follow the steps below to enable storm control.

1. Navigate to **Security →Storm Control**.
2. Select the type and port, enable storm control, and then enter the speed.

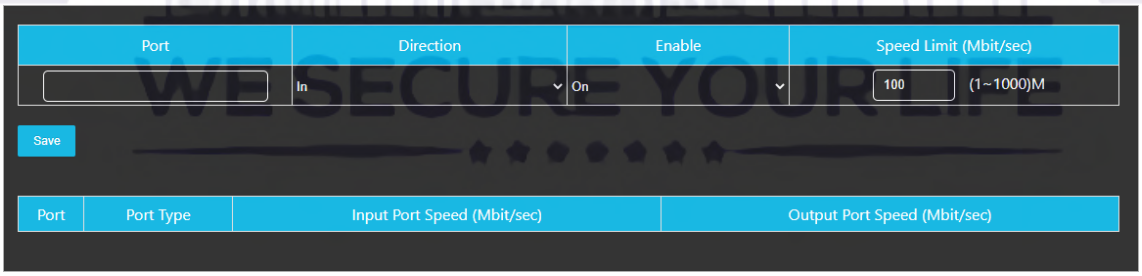


3. Click **Save**.

Port Speed Limit

Follow the steps below to set the rate limiting policy to control the flow of data packets entering and exiting the port.

1. Select **Security** > **Port Speed Limit**.
2. Select port and direction, enable the port speed limit, and then enter the speed. The direction includes entrance and exiting.



3. Click **Save**.

Network Settings

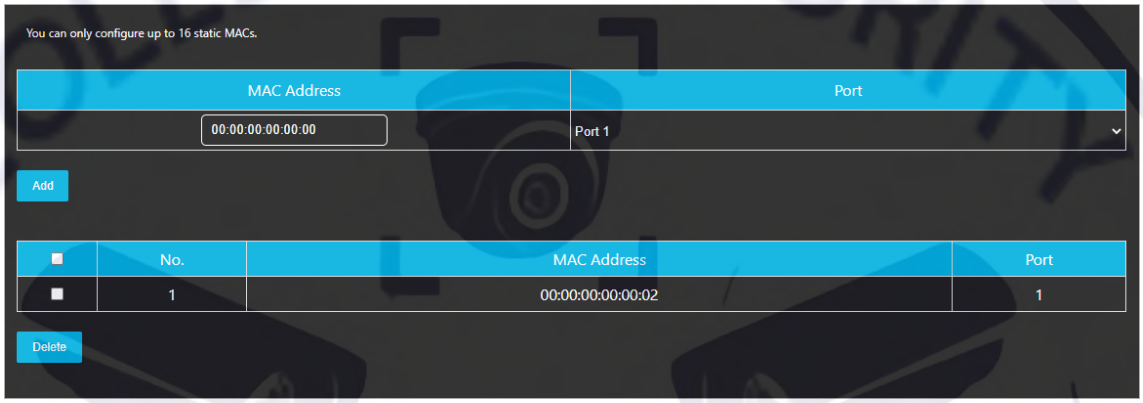
Configuring MAC Tables

The MAC (Media Access Control) table records the association between MAC addresses and ports, including their corresponding VLANs. When forwarding a packet, the device checks the table for the destination MAC address. If found, the packet is forwarded through the corresponding port. If not, the device broadcasts the packet to all VLAN ports except the receiving port.

Follow the steps below to configure the device's MAC tables.

1. Select **Network Settings → MAC Management → Static MAC** to view the MAC table information.
2. Configure the MAC address, VLAN ID and port. Click **Add** when done.

   - You can only configure up to 16 static MACs.
   - To delete a static MAC, select the MAC and click **Delete**.



3. Click the **MAC Search** tab, enter the MAC address or select the port, and then click **Search** to find a specific MAC address.

4. Click the **MAC List** tab to view MAC addresses. Up to 100 items can be displayed. To search for more information, navigate to **MAC Search**.

   Click **Clear** and then **OK** to clear the information

Configuring Loop Protection

To enable loop protection, select **Network Settings → Loop Protection**, enable the feature, and click **Save**. Once loop protection is activated, the port responsible for the loop will be disabled and will automatically restore itself once the loop is eliminated.

Smart Monitoring

Viewing Port Statistics

Follow the steps below to view port statistics.

1. Select **Smart Monitoring → Port Statistics**.
2. View the port type, receiving usage, and sending usage. Click **Reset** to reset the port statistics.

Port	Port Type	RX Usage	TX Usage	RX/TX Bytes	Successful RX/TX Packet	Failed RX/TX Packet
1	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
2	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
3	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
4	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
5	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
6	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
7	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
8	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0
9	Physical Port	0.01%	0.01%	28.02MB/1.32MB	335190/11695	0/0
10	Physical Port	0%	0%	0.00B/0.00B	0/0	0/0

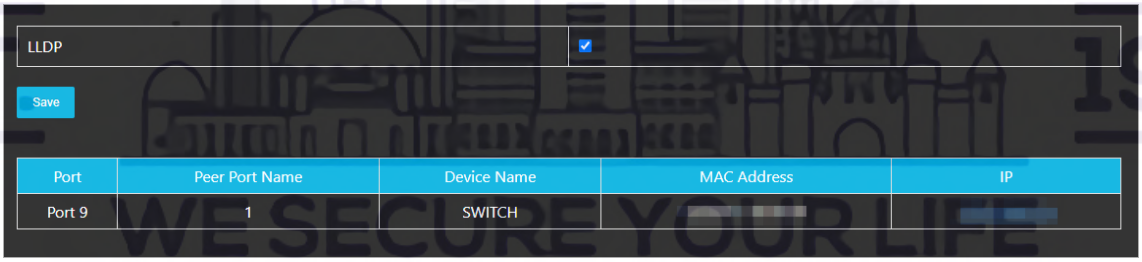
Reset

Viewing Device List and LLDP Information

LLDP (Link Layer Discovery Protocol) is a standard protocol for link layer discovery. It encapsulates essential information, such as management addresses and device numbers, in TLV (Type Length Value) structures within LLDPDUs (Link Layer Discovery Protocol Data Units) sent to neighboring devices. These devices store the information in a standard MIB (Management Information Base), allowing network management to assess link communication states.

Follow the steps below to view the device list and LLDP information.

1. Select **Network Monitoring → Device List**.
2. Enable the LLDP, and then Click **Save**.
3. View the information of LLDP remote device.

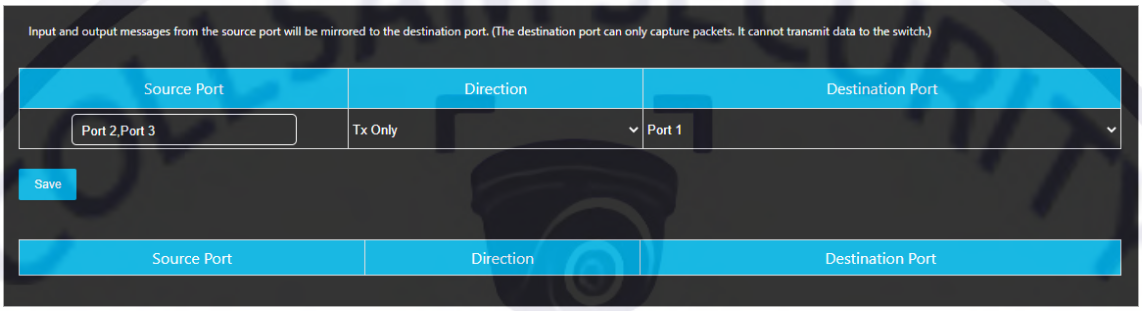


Maintenance

Configuring Port Mirroring

Mirroring duplicates traffic from a specified source (mirrored source) to a destination port (observing port) for analysis. The copied traffic, called mirrored traffic, is sent through the observing port to a monitoring device. Follow the steps below to configure port mirroring.

1. Select **Maintenance → Port Mirroring**.
2. Select the source port, direction, and destination port. Directions include Tx Only, Rx Only, and Both.
   - **Tx Only**: Only supports sending traffic.
   - **Rx Only**: Only supports receiving traffic.
   - **Both**: Supports both sending and receiving.



3. Click **Save**.

Configuring Firmware

Restore Factory Default

Follow the steps to restore the firmware to factory default settings.

1. Select **Maintenance → Firmware Config**.
2. Click **Default**, enter the password, and then click **OK**.

⚠ All parameters will be restored to the default setting except the IP address, subnet mask, gateway, and DNS. You can restore all parameters though the reset button.

Update Firmware

Follow the steps to update your device's firmware.

1. Select **Maintenance** > **Firmware Config**.
2. Click **Browse** to import the update file, and then click **Update**.
3. Click **OK**.

💡 It may take up to 3 minutes for the software to update. The system will automatically restart after an update.

Restart Device

To restart your device, navigate to **Maintenance → Firmware Config**, click **Restart**, and then click **OK**.

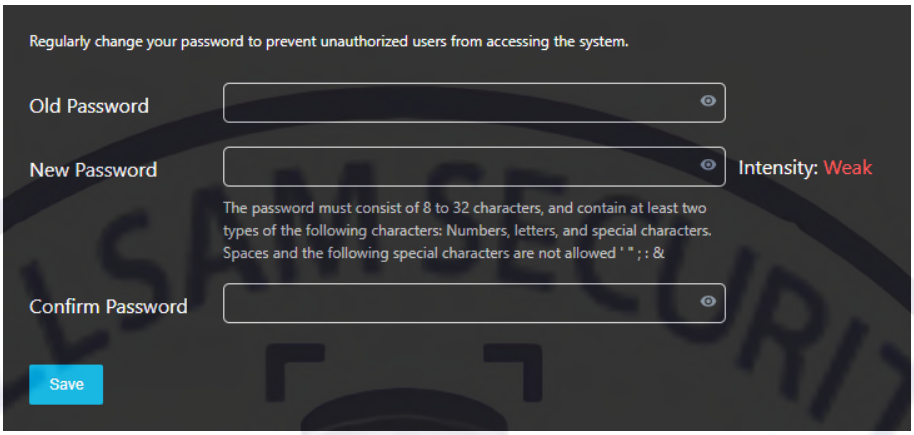
💡 You can also click ✳ in the upper-right corner to restart the device.

Change the Device Password

Follow the steps below to change your device password.

1. Navigate to **Maintenance → Change Password.**
2. Enter the old password and type in the new password. Input the new password in the **Confirm Password** box.

   Your password must be 8–32 characters with at least two types of characters (numbers, letters, and any visible characters other than' " ; : &).



Configuring Network

Follow the steps below to configure the IP address and DNS server.

1. Select **Maintenance** > **Network**.
2. Configure the parameters. Click **Save** when done.
   - **Enable DHCP**: After enabling DHCP, new IP will be automatically acquired and assigned.
   - **Disable DHCP**: Enter the IP address, subnet mask, and gateway to configure a static IP address.
   - **Enable Auto Obtain DNS**: The device automatically obtains the IP address of the DNS server in the network.
   - **Disable Auto Obtain DNS**: Enter the IP addresses of the DNS1 and DNS2.

Viewing Device Information

To view device information, navigate to **Maintenance** > **Device Information**. You can view information such as the device name, software version, MAC address, and running time. You can also enable cloud management through this page.

Viewing Log Information

To view log information, navigate to **Maintenance → Log Information**.

Viewing Legal Information

To view legal information, navigate to **Maintenance → Legal Statement**, and click the corresponding tab to view the software license agreement, privacy policy, and open-source software notice.

Appendix: 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).