



Gigabit Web-Managed PoE Switch

User Manual

Legal Information

User Manual

©2019 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/en/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS.

Gigabit Web-Managed PoE Switch User Manual

YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement



This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: <http://www.recyclethis.info>.



2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: <http://www.recyclethis.info>.

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Preface

Applicable Models




This manual is applicable to DS-3E15XXP series switch and guides you to complete the configuration and operation of the switch.

About the Default

- Default administrator account: admin.
- Default IP address: 192.168.1.64.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

- This is a class A product and may cause radio interference in which case the user may be required to take adequate measures.
- Ensure that your devices powered via the PoE port have their shells protected and fire-proofed, because the switches are not compliant with the Limited Power Source (LPS) standard.

Contents

Chapter 1 Introduction	1
Chapter 2 Activation and Login	2
Chapter 3 Device Management	4
Chapter 4 Switch Configuration	7
4.1 Port Configuration	7
4.1.1 Attribute Configuration	7
4.1.2 Port Mirroring	8
4.1.3 Port Rate-Limiting	9
4.1.4 Storm Control Configuration	10
4.1.5 Long-Range Mode Configuration	11
4.2 Link Aggregation Configuration	12
4.3 VLAN Configuration	14
4.3.1 Add a VLAN	14
4.3.2 Configure a Port	15
4.4 QoS Configuration	16
4.5 SNMP Configuration	18
4.5.1 SNMP Proxy Settings	19
4.5.2 SNMP Trap Settings	19
4.6 STP Configuration	20
4.6.1 Global Configuration	20
4.6.2 STP Port Configuration	22
4.6.3 STP Status View	24
4.7 PoE Management	24
Chapter 5 System Management	26
5.1 Time Sync	26
5.2 Device Operation	26

5.3 Configuration File Export	27
5.4 Configuration File Import	27
5.5 Device Upgrade	28
5.6 Log Management	28
5.7 User Management	29
5.8 Security Management	30

Chapter 1 Introduction

DS-3E15XXP series switches are layer 2 PoE switches, providing advanced PoE power supply technology and gigabit networks design on the basis of high-performance access. The switches support Web management, various layer 2 management protocols such as STP/RSTP, VLAN, link aggregation, SNMP, QoS to ensure stable data upload.

Chapter 2 Activation and Login

For the first time usage, you must activate the switch and configure the password.

Before You Start

The computer and the switch are on the same network segment.

Steps

Note

Take DS-3E1510P as an example. All figures in this manual are for illustration purpose only.

1. Enter the default IP 192.168.1.64 in the browser address bar.

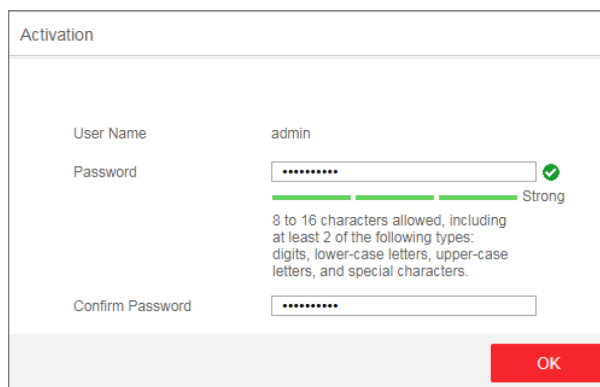


Figure 2-1 Activation

Note

You are recommended to use the newest version of the following browsers: IE 10+, Edge, and Chrome 31+.

2. Configure the password and confirm it.
3. Click **OK**.

Go to the login page.

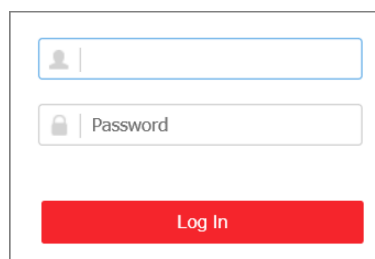
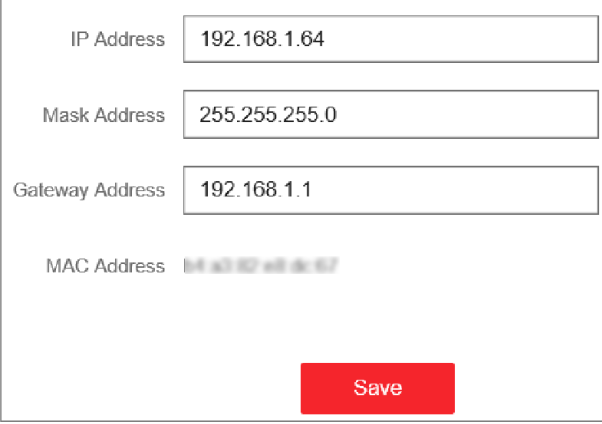


Figure 2-2 Login

4. Enter the **User Name** and **Password**, and click **Log In**.
5. **Optional:** Change the network configuration.

1) Go to **System Management** → **Network Configuration** .



The screenshot shows a web configuration page for network settings. It contains four input fields: IP Address (192.168.1.64), Mask Address (255.255.255.0), Gateway Address (192.168.1.1), and MAC Address (88-63-82-48-6c-87). A red Save button is located at the bottom right of the form.

IP Address	192.168.1.64
Mask Address	255.255.255.0
Gateway Address	192.168.1.1
MAC Address	88-63-82-48-6c-87

Save

Figure 2-3 Network Configuration

2) Change the IP address, mask address, and the gateway address as needed. You can log in to the switch with the new IP address next time.

 **Note**

You are recommended to change the network configuration to better manage the switch.

Chapter 3 Device Management

After logging in to the Web, you can go to **Device Status** to view the device status, including the device information, working status, port status, port statistics, and PoE status.

Device Information

Device Model	DS-3E1510P-E
Device Serial No	XXXXXXXXXXXXXXXXXXXX
Device Program Version	V1.0.0.00000000
Number of Ports	10
Management VLAN	1
MAC Address Aging Time (s)	300

sec

Save

Figure 3-1 Device Information

- **Management VLAN:** The management VLAN is VLAN 1 by default that cannot be edited.
- **MAC Address Aging Time:** Aging time for MAC address table entries. The range is from 10 to 100,000 seconds. The default is 300 seconds.

Working Status

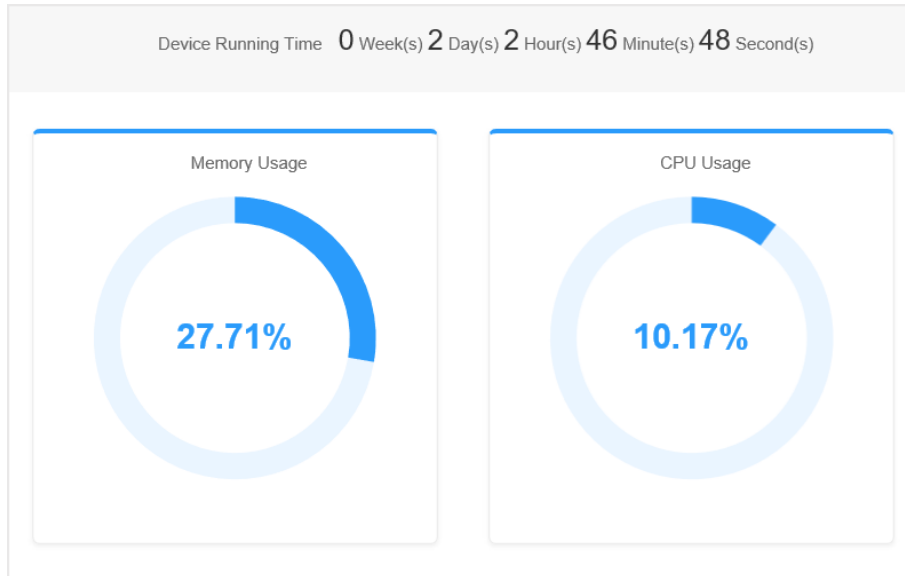


Figure 3-2 Working Status

View the device running time, memory usage, and CPU usage.

Port Status

Port Name	Connection Status	Rate	Duplex	Flow Control
Ge1	Disconnected	-	-	-
Ge2	Connected	1000M	Full-Duplex	Off
Ge3	Disconnected	-	-	-
Ge4	Connected	1000M	Full-Duplex	Off
Ge5	Disconnected	-	-	-
Ge6	Disconnected	-	-	-
Ge7	Disconnected	-	-	-
Ge8	Connected	1000M	Full-Duplex	On
Ge9	Connected	1000M	Full-Duplex	On
Ge10	Disconnected	-	-	-

Figure 3-3 Port Status

View the connection status, rate, duplex, and flow control of all ports.

Port Statistics

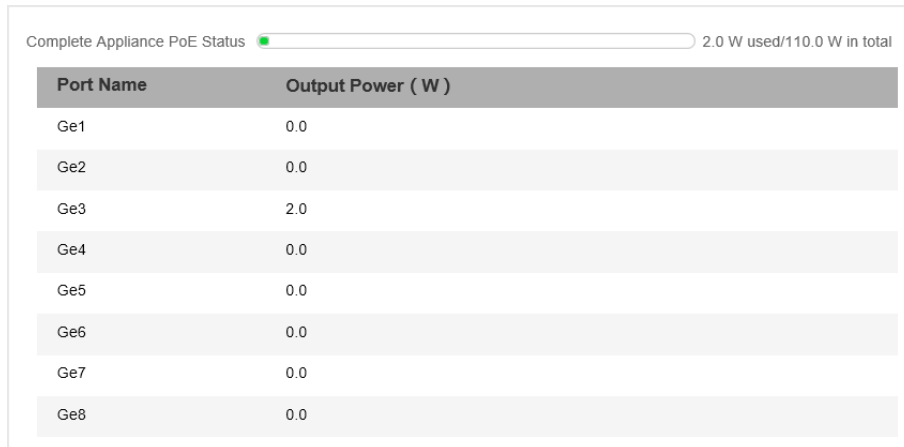
Refreshing Rate: 30 sec

Port	Number of Bytes Sent	Number of Packets Sent	Sending Rate	Number of Bytes Received	Number of Packets Received	Receiving Rate
Ge1	-	-	-	-	-	-
Ge2	-	-	-	-	-	-
Ge3	122429454	339425	28.650Kbps	6796845	18694	768bps
Ge4	-	-	-	-	-	-
Ge5	-	-	-	-	-	-
Ge6	-	-	-	-	-	-
Ge7	-	-	-	-	-	-
Ge8	23731162	43851	34.656Kbps	119619685	339806	29.388Kbps
Ge9	-	-	-	-	-	-
Ge10	121936735	324630	27.620Kbps	4763966	11181	522bps

Figure 3-4 Port Statistics

- **Refreshing Rate:** 10 sec, 30 sec, 60 sec, and **Manually Refresh** is available.
- **Refresh:** When you choose **Manually Refresh**, you can click **Refresh** to refresh the statistics.
- **Reset:** You can click **Reset** to clear all the statistics.

PoE Status



Complete Appliance PoE Status ■ 2.0 W used/110.0 W in total

Port Name	Output Power (W)
Ge1	0.0
Ge2	0.0
Ge3	2.0
Ge4	0.0
Ge5	0.0
Ge6	0.0
Ge7	0.0
Ge8	0.0

Figure 3-5 PoE Status

View the complete appliance PoE status and the output power of each PoE port.

Chapter 4 Switch Configuration

4.1 Port Configuration

4.1.1 Attribute Configuration

The basic parameters can influence the working status of ports. Configure the parameters according to the actual situation.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Attribute Configuration** .

Port Name	Speed	Duplex	Flow Control	Enable
Ge1	10M	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge2	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge3	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge4	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge5	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge6	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge7	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge8	auto	auto	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge9	1000M	full	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ge10	1000M	full	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 4-1 Port Attribute Configuration

2. Configure the parameters.

Speed

The speed of data transmission of the port.

- PoE port: The default is **auto**.
- SFP port: The default is **1000 M** that cannot be edited.

Duplex

The duplex mode of the port.

- PoE port: The default is **auto**.
- SFP port: The default is **full** that cannot be edited.

Flow Control

Enabling the flow control can prevent data loss in data transmission.

Enable

Enable or disable the port link.

3. Click **Save** to complete the configuration.

4.1.2 Port Mirroring

Port mirroring monitors network traffic by sending copies of all incoming and outgoing packets from one port to a mirroring port.

Steps

1. Go to **Switch Configuration → Basic Configuration → Port Configuration → Port Mirroring** .

Attribute Configuration **Port Mirroring** Port Rate-Limiting Storm Control Long-Range Mode

Port Mirroring Enable

Mirror Port

Mirror Source Configuration

Port Name	Mirror Direction
Ge1	Disable Mirror
Ge2	Inbound
Ge4	Outbound
Ge5	Inbound and Outbound
Ge6	Disable Mirror
Ge7	Disable Mirror
Ge8	Disable Mirror
Ge9	Disable Mirror
Ge10	Disable Mirror

Save

Figure 4-2 Port Mirroring

2. Check **Enable** of **Port Mirroring**.
3. Configure the parameters according to the actual situation.

Table 4-1 Parameters of Port Mirroring

Parameter	Description
Mirror Port	Surveillance port.

Parameter	Description
	You can only set one port as the mirror port.
Mirror Source	The port that is under surveillance. You can set one or more ports as the mirror source.
Mirror Direction	Surveillance direction. <ul style="list-style-type: none"> • Disable Mirror: The port is not under surveillance. • Inbound: The inbound data of the port is under surveillance. • Outbound: The outbound data of the port is under surveillance. • Inbound and Outbound: Both inbound and outbound data of the port are under surveillance.

4. Click **Save** to complete the port mirroring configuration.

4.1.3 Port Rate-Limiting

Configure the port sending and receiving rate according to the actual situation.

Steps

1. Go to **Switch Configuration → Basic Configuration → Port Configuration → Port Rate-Limiting** .

Port Name	Sending Rate-Limiting	Sending Rate-Limiting Value (Mbps)	Receiving Rate-Limiting	Receiving Rate-Limiting Value (Mbps)
Ge1	Rate-Limiting	100	Rate-Limiting	100
Ge2	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge3	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge4	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge5	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge6	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge7	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge8	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge9	No Rate-Limiting	1000	No Rate-Limiting	1000
Ge10	No Rate-Limiting	1000	No Rate-Limiting	1000

Figure 4-3 Port Rate-Limiting

2. Configure the parameters.

Table 4-2 Parameters of Port Rate-Limiting

Parameter	Description
Sending Rate-Limiting	<ul style="list-style-type: none">• Rate-Limiting: The data sending rate of the port is limited.• No Rate-Limiting: The data sending rate of the port is not limited.
Sending Rate-Limiting Value	Only editable when the sending rate of the port is limited. The range is from 1 to 1000 Mbps.
Receiving Rate-Limiting	<ul style="list-style-type: none">• Rate-Limiting: The data receiving rate of the port is limited.• No Rate-Limiting: The data receiving rate of the port is not limited.
Receiving Rate-Limiting Value	Only editable when the receiving rate of the port is limited. The range is from 1 to 1000 Mbps.

3. Click **Save** to complete the configuration.

4.1.4 Storm Control Configuration

Storm control prevents the ports from being disrupted by a broadcast, multicast, or unknown unicast storm. Errors in the protocol-stack implementation, or mistakes in network configuration, can cause a storm. The storm congests the network and degrades the network performance.

The packets passing from the port will be determined by the storm control if they are unknown unicast, multicast, or broadcast. When the packets number exceeds the threshold, the incoming data is dropped.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Storm Control** .

Port Name	Storm Control	Storm Control Mode	Rate Threshold (Mbps)
Ge1	On	Multicast	1 <input type="range"/> 1000 888
Ge2	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge3	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge4	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge5	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge6	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge7	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge8	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge9	Off	Unknown Unicast	1 <input type="range"/> 1000 1000
Ge10	Off	Unknown Unicast	1 <input type="range"/> 1000 1000

Figure 4-4 Storm Control

2. Select the port on which you want to enable storm control. Configure **Storm Control** as **on**.
3. Configure **Storm Control Mode** as **Broadcast**, **Multicast**, or **Unknown Unicast**. The threshold applies to the chosen mode.
4. Configure the number of frames in Mbps that you want the port to handle in **Rate Threshold**.
5. Click **Save** to complete the configuration.

4.1.5 Long-Range Mode Configuration

When long-range mode is enabled, the transmission distance of the port can reach 300 meters, and the rate is 10 Mbps.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Port Configuration** → **Long-Range Mode** .

Port Name	Enable
Ge1	<input checked="" type="checkbox"/>
Ge2	<input checked="" type="checkbox"/>
Ge3	<input type="checkbox"/>
Ge4	<input type="checkbox"/>
Ge5	<input type="checkbox"/>
Ge6	<input type="checkbox"/>
Ge7	<input type="checkbox"/>
Ge8	<input type="checkbox"/>

[Save](#)

Figure 4-5 Long-Range Mode Configuration

2. Check **Enable** of the port.
3. Click **Save** to complete the configuration.

4.2 Link Aggregation Configuration

Link aggregation is used to aggregate physical ports to create a logical channel. The advantages of link aggregation are higher transmission speed with wider bandwidth.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **Link Aggregation** → **Load Balancing Configuration** to configure **Load Balancing Mode**.

Load Balancing Configuration Aggregation Group Configuration

Load Balancing Mode: Source and Destination MAC

Save

Figure 4-6 Load Balancing

Source and Destination MAC

Load balancing is performed based on source and destination MAC addresses on all the packets.

2. Add a link aggregation group in **Aggregation Group Configuration**.

Load Balancing Configuration Aggregation Group Configuration

+ Add X Delete

The rate, duplex, and flow control, VLAN and long-range configuration of all ports in the aggregation group must be the same.

Aggregation Group ID	Group Members
<input type="checkbox"/> LAG3	Ge9, Ge10

Figure 4-7 Link Aggregation Group

- 1) Click **Add**.

Add Link Aggregation Group

Aggregation Group: (1-8)

Available Port List: Ge1, Ge2, Ge3, Ge4, Ge5, Ge6, Ge7, Ge8

Group Members (0)

Add >> << Delete

OK Cancel

Figure 4-8 Add a Link Aggregation Group

- 2) Enter the group number in the **Aggregation Group** field. The range is from 1 to 8.
- 3) Move the ports that are to be assigned to the group from the **Available Port List** to the **Group Members** list.

Note

- You can delete the ports from the **Group Members** by clicking **Delete**.
 - The rate, duplex, flow control, VLAN, and long-range configuration of all ports in one aggregation group must be the same.
-

4) Click **OK** to add a link aggregation group.

4.3 VLAN Configuration

A Virtual Local Area Network (VLAN) is a group of devices located on different LAN segments that are configured to communicate as if they were attached to the same wire. LANs are based on logical instead of physical connections, which is flexible for device connection.

4.3.1 Add a VLAN

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **VLAN** → **802.1Q VLAN** .
2. Click **Add**.

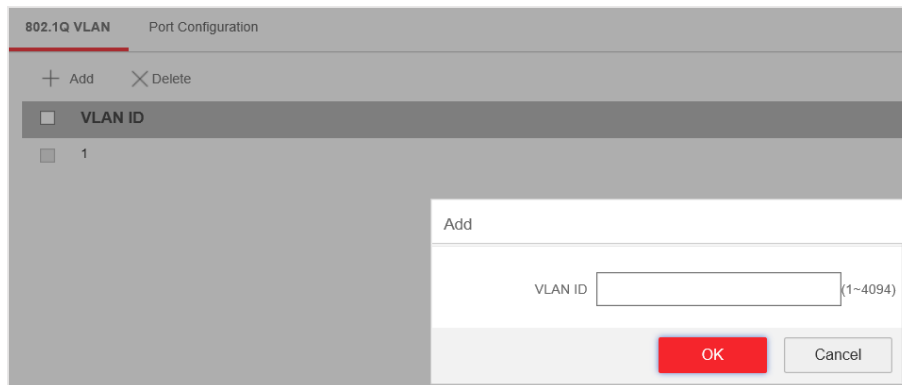


Figure 4-9 Add a VLAN

3. Enter a VLAN ID.

Note

- A maximum of 128 VLANs are supported.
 - The range is from 1 to 4094.
-

4. **Optional:** You can also delete a VLAN by clicking **Delete**.
-

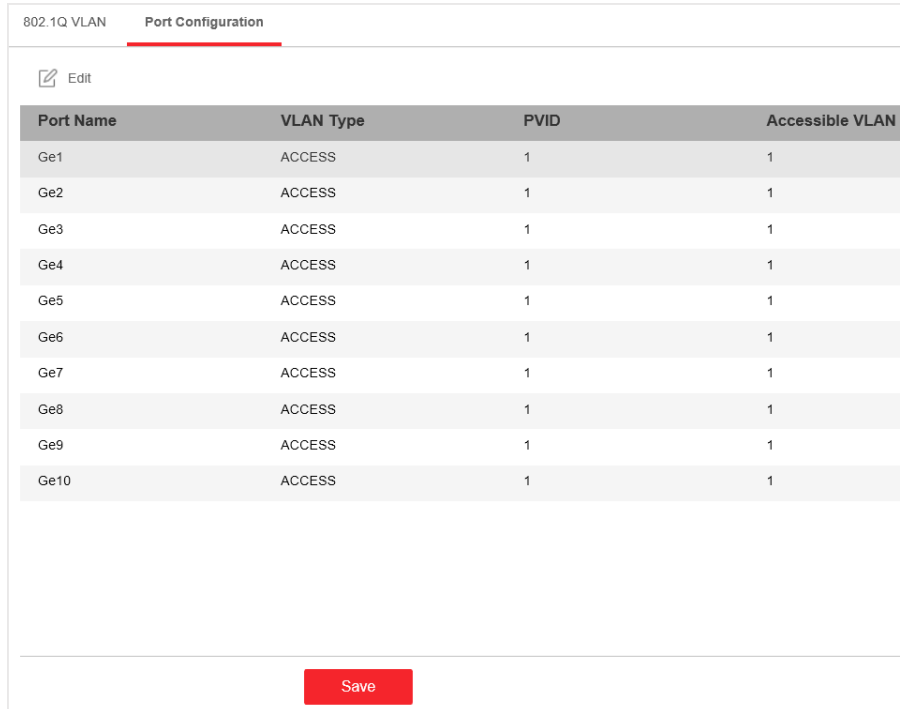
Note

You cannot delete the VLAN 1, because VLAN 1 is the Management VLAN.

4.3.2 Configure a Port

Steps

1. Select a port to configure on the **Port Configuration** page.



Port Name	VLAN Type	PVID	Accessible VLAN
Ge1	ACCESS	1	1
Ge2	ACCESS	1	1
Ge3	ACCESS	1	1
Ge4	ACCESS	1	1
Ge5	ACCESS	1	1
Ge6	ACCESS	1	1
Ge7	ACCESS	1	1
Ge8	ACCESS	1	1
Ge9	ACCESS	1	1
Ge10	ACCESS	1	1

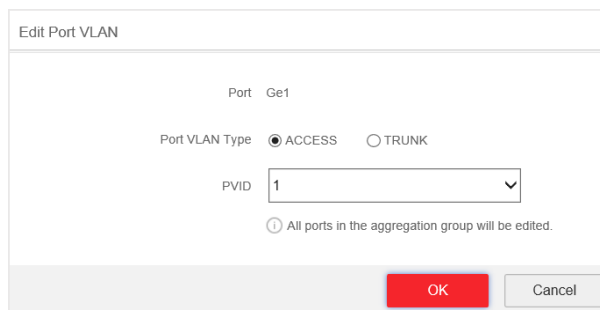
Figure 4-10 VLAN Port Configuration

2. Click **Edit**.

3. Configure the port VLAN.

- **Access Port**

- An access port transports traffic to and from only the specified VLAN, usually the default VLAN, VLAN 1.
- Select **Port VLAN Type** as **ACCESS**, and select the **PVID**.



802.1Q VLAN Port Configuration

Edit

Port Name	VLAN Type	PVID	Accessible VLAN
Ge1	ACCESS	1	1
Ge2	ACCESS	1	1
Ge3	ACCESS	1	1
Ge4	ACCESS	1	1
Ge5	ACCESS	1	1
Ge6	ACCESS	1	1
Ge7	ACCESS	1	1
Ge8	ACCESS	1	1
Ge9	ACCESS	1	1
Ge10	ACCESS	1	1

Save

Edit Port VLAN

Port Ge1

Port VLAN Type ACCESS TRUNK

PVID

① All ports in the aggregation group will be edited.

OK Cancel

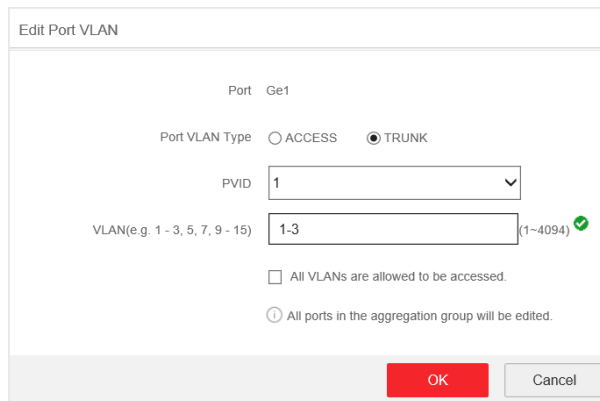
Figure 4-11 Edit an Access Port VLAN

Note

All ports in the same aggregation group will be edited automatically at the same time.

- Trunk Port

- A trunk port is a port that is assigned to carry traffic for all the VLANs.
- Select **Port VLAN Type** as **TRUNK**, select the **PVID** and enter the **VLAN** that are allowed to be accessed.



Port Ge1

Port VLAN Type ACCESS TRUNK

PVID

VLAN(e.g. 1 - 3, 5, 7, 9 - 15) (1~4094) ✓

All VLANs are allowed to be accessed.

All ports in the aggregation group will be edited.

OK Cancel

Figure 4-12 Edit a Trunk Port VLAN

Note

- All ports in the same aggregation group will be edited automatically at the same time.
 - You can check **All VLANs are allowed to be accessed.** to assign the port to all the VLANs.
-

4. Click **OK**.

5. Click **Save** to save the configuration.

4.4 QoS Configuration

Quality of Service (QoS) includes the transmission bandwidth, delay, packet loss rate and etc. Increasing network bandwidth, decreasing network delay, and reducing packet losses can improve QoS in network service. You can configure the scheduling mode and port priority of QoS.

Steps

1. Go to **Switch Configuration** → **Basic Configuration** → **QoS** → **Scheduling Mode** to select a scheduling type.

Scheduling Mode Port Priority

Scheduling Type NORMAL SP WRR

Weight for Low Priority

Weight for High Priority

Save

Figure 4-13 Scheduling Mode

NORMAL

First In First Out (FIFO) mode. Transmit the message coming in first. QoS is not enabled.

SP

Strict Priority mode. Transmit the message according to the actual priority configuration.

WRR

Weighted Round Robin mode. Transmit the message according to the respective weight for low priority and high priority.

2. Configure the port priority in **Port Priority**.

Scheduling Mode **Port Priority**

Port Name	Priority
Ge1	High Priority <input type="button" value="v"/>
Ge2	High Priority <input type="button" value="v"/>
Ge3	Low Priority <input type="button" value="v"/>
Ge4	Low Priority <input type="button" value="v"/>
Ge5	Low Priority <input type="button" value="v"/>
Ge6	Low Priority <input type="button" value="v"/>
Ge7	Low Priority <input type="button" value="v"/>
Ge8	Low Priority <input type="button" value="v"/>

Figure 4-14 Port Priority

3. Click **Save** to complete the configuration.

4.5 SNMP Configuration

Simple Network Management Protocol (SNMP) is a widely used application-layer communication protocol for monitoring network performance. SNMP network is composed of the Network Management System (NMS) and the Agent. NMS is the SNMP manager, and Agent sends Traps to NMS.

4.5.1 SNMP Proxy Settings

Steps

1. Go to **Switch Configuration** → **L2 Configuration** → **SNMP Configuration** → **SNMP Proxy Settings** to configure SNMP proxy.

Community Name	Access Mode
public	Read-Only
private	Read/Write

Figure 4-15 Proxy Settings

- 1) Enable **SNMP**.
- 2) Define the **Community Name**.

Community Name

The community name is an authentication mechanism, similar to a password, which is used to limit the data transmission between NMS and Agent.

- **Read-Only Community Name:** The Community name accessible to NMS with read permission. The default is **public**.
- **Read/Write Community Name:** The Community name accessible to NMS with read and write permission. The default is **private**.

- 3) Click **Save**.

4.5.2 SNMP Trap Settings

Steps

1. Enable **Trap** on the **SNMP Trap Settings** page.


Trap Target Host	Community Name	SNMP Version
------------------	----------------	--------------

Figure 4-16 Trap Settings

2. Click **Add** to add a trap.

Figure 4-17 Add a Trap

Table 4-3 Parameters of a Trap

Parameter	Description
Target Host IP	The IP address of NMS.
Community Name	The password used for authentication.
SNMP Version	<p>The Agent supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c).</p> <p> Note The prerequisite of successful connection between NMS and Agent is that the SNMP version of NMS and Agent must be the same.</p>

3. Click **OK**.
4. Click **Save** to add a trap.
5. **Optional:** You can check the trap and click **Delete** to delete a trap.

4.6 STP Configuration

Spanning-Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. The STP uses a spanning-tree algorithm to select one switch as the root of a spanning tree. STP determines the topology by transmitting Bridge Protocol Data Unit (BPDU) packets between devices. Spanning-tree operation creates a stable network.

4.6.1 Global Configuration

Steps

1. Go to **Switch Configuration → L2 Configuration → STP Configuration → Global Configuration**.
2. Check **Enable STP**.

Global Configuration
STP Port Configuration
STP Status

① The maximum aging time must meet the following conditions:

Maximum Aging Time $\geq 2 \times (\text{Hello Time} + 1)$

Maximum Aging Time $\leq 2 \times (\text{Forwarding Delay} - 1)$

Enable STP

STP Mode

Bridge Priority ✔

Hello Time s ✔

Maximum Aging Time s ✔

Forwarding Delay s ✔


Save

Figure 4-18 Global Configuration

3. Configure the parameters.

Table 4-4 Parameters of STP

Parameter	Description
STP Mode	<ul style="list-style-type: none"> • STP: Spanning-tree protocol. • RSTP: Rapid spanning-tree protocol. RSTP provides faster spanning tree convergence after a topology change.
Bridge Priority	<p>The lower the number, the higher the priority. The range is from 0 to 61,440 seconds, in increments of 4096; the default is 32,768. Valid values are 0, 4096, 12288, 16384 ... and 61440.</p> <p>A switch with higher bridge priority is more likely to become a root bridge.</p>
Hello Time	The time between each BPDU that is sent on a port, which is used for port link diagnosis. The range is from 1 to 10 seconds. The default is 2 seconds.
Maximum Aging Time	The maximum length of time that passes before a bridge port saves its configuration BPDU information.

Parameter	Description
	<p>The range is from 6 to 40 seconds. The default is 20 seconds.</p> <p> Note</p> <p>The maximum aging time must meet the following conditions:</p> <ul style="list-style-type: none">• Maximum Aging Time \geq (Hello Time + 1)• Maximum Aging Time \leq (Forwarding Delay - 1)
Forwarding Delay	<p>The time interval that is spent in the listening and learning state when the topology changes. The range is from 4 to 30 seconds. The default is 15 seconds.</p>

4. Click **Save**.

4.6.2 STP Port Configuration

If a loop occurs, you can set port priority so that the spanning tree can select the port with the highest priority to forward data.

Steps

1. The port is enabled by default on the **STP Port Configuration** page.

Global Configuration **STP Port Configuration** STP Status

Port Name	Port	Port Priority
Ge1	<input checked="" type="checkbox"/>	128
Ge2	<input checked="" type="checkbox"/>	128
Ge3	<input checked="" type="checkbox"/>	128
Ge4	<input checked="" type="checkbox"/>	128
Ge5	<input checked="" type="checkbox"/>	128
Ge6	<input checked="" type="checkbox"/>	128
Ge7	<input checked="" type="checkbox"/>	128
Ge8	<input type="checkbox"/>	128
Ge9	<input checked="" type="checkbox"/>	128
Ge10	<input checked="" type="checkbox"/>	128

Save

Figure 4-19 Port Priority

2. Configure the Port Priority.

Port Priority

- The lower the number, the higher the priority, the more probably the port becomes the root port.
- The range is from 0 to 240, in increments of 16; the default is 128. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240.

 **Note**

If the priority of the port is the same, spanning tree uses the port ID to select a port as the root port.

3. Click Save.

4.6.3 STP Status View

You can check the global status of STP settings and the status of each port.

Go to **Switch Configuration** → **L2 Configuration** → **STP Configuration** → **STP Status** .

The screenshot shows the 'STP Status' configuration page. It has two main sections: 'Global Status' and 'Port Status'.

Global Status:

- Bridge ID: 32768 b4-a3-82-ec-03-af
- Root Bridge ID: 32768 b4-a3-82-ec-03-aa
- Root Bridge Hello Time: 2
- Root Bridge Maximum Aging Time: 20
- Root Bridge Forwarding Delay: 15

Port Status:

Port Name	Path Cost	Port Role	Port Status
Ge1	20000	Disable Port	disabled
Ge2	20000	Disable Port	disabled
Ge3	200000	Designated Port	forwarding
Ge4	20000	Disable Port	disabled
Ge5	20000	Disable Port	disabled
Ge6	20000	Disable Port	disabled
Ge7	20000	Disable Port	disabled

Figure 4-20 STP Status

4.7 PoE Management

PoE Settings

The screenshot shows the 'PoE Settings' configuration page. It has two tabs: 'PoE Settings' (selected) and 'PoE Watchdog'.

Port Name	PoE
Ge1	<input checked="" type="checkbox"/>
Ge2	<input checked="" type="checkbox"/>
Ge3	<input checked="" type="checkbox"/>
Ge4	<input checked="" type="checkbox"/>
Ge5	<input checked="" type="checkbox"/>
Ge6	<input checked="" type="checkbox"/>
Ge7	<input checked="" type="checkbox"/>
Ge8	<input checked="" type="checkbox"/>

Figure 4-21 PoE Settings

You can enable PoE to supply power for the powered devices (PDs).

 **Note**

Enabling or disabling PoE has no influences on data transmission of the port.

PoE Watchdog

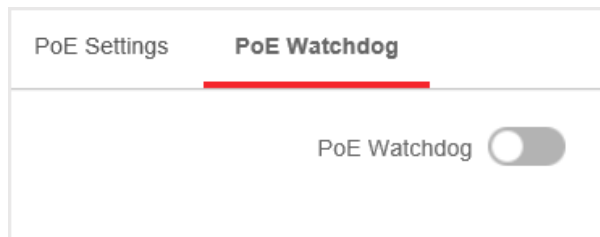


Figure 4-22 PoE Watchdog

You can enable PoE watchdog to auto-detect and restart cameras that do not respond.

Chapter 5 System Management

5.1 Time Sync

Steps

1. Go to **System Settings** → **Time Settings** . You can view the **Device Time**.

Figure 5-1 Time Settings

2. Select **Time Zone**.

3. Select **Time Sync. Method**

4. Set time synchronization mode.

- **Manual Time Sync.:** Click or check **Sync. with computer time** to synchronize the device time.

Figure 5-2 Manual Sync

- **NTP Time Sync.:** Enter the **NTP Server Address**, and set the time sync. interval.

Figure 5-3 NTP Sync

5. Click **Save**.

5.2 Device Operation

When the switch malfunctions or fails to work properly, you can restart or restore the switch.

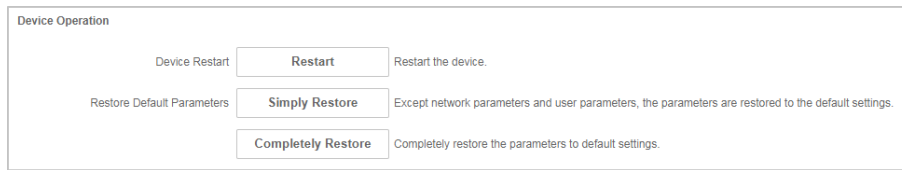


Figure 5-4 Device Operation

Restart

Click **Restart** to remotely restart the switch.

Restore

- **Simply Restore:** Except network configuration and user parameters, all of the other parameters are restored to the default settings.
- **Completely Restore:** Completely restore the parameters to default settings.



Caution

Parameters cannot be recovered after being restoring to default settings.

5.3 Configuration File Export

You can export the configuration file for local backup.

Steps

1. Go to **System Management** → **System Maintenance** → **Export & Import** .
2. Click **Export**.
3. Set a password for the exported configuration file.

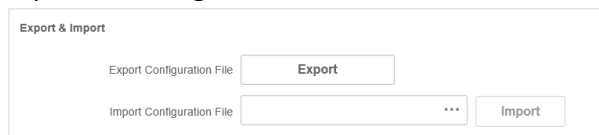


Figure 5-5 Export Configuration file



Note

Please remember the password, because you need to enter the password when importing the configuration files.

4. Click **OK**.

5.4 Configuration File Import

You can import the configuration file to configure the system easily.

Steps

1. Go to **System Management** → **System Maintenance** → **Export & Import** .

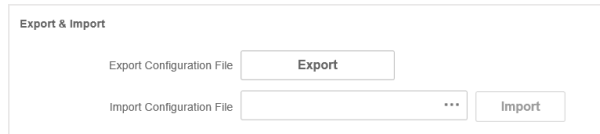


Figure 5-6 Export Configuration file

2. Click ... to select the configuration file.
3. Click **Import**.

5.5 Device Upgrade

You can upload the upgrade file to upgrade your switch.

Steps

1. Go to **System Management** → **System Maintenance** → **Device Upgrade**

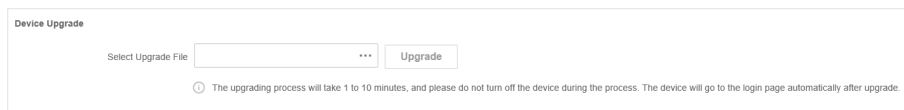


Figure 5-7 Upgrade

2. Click ... to select an upgrade patch.
3. Click **Upgrade**.

Note

If upgrading failed or the device cannot function, please contact our technical support engineers.

Result

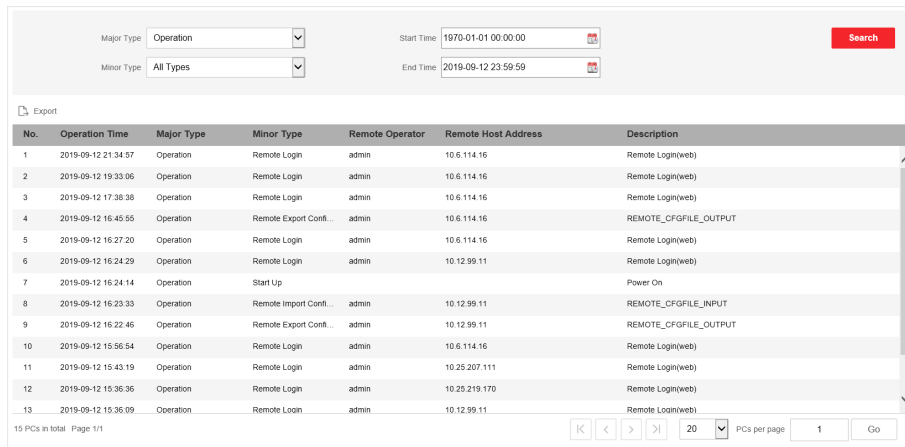
The device will restart automatically when upgrade finished.

5.6 Log Management

System operation logs can be searched and exported for backup.

Steps

1. Go to **System Management** → **Log Management** .



The screenshot shows a web interface for log management. At the top, there are search filters: Major Type (Operation), Minor Type (All Types), Start Time (1970-01-01 00:00:00), and End Time (2019-09-12 23:59:59). A red Search button is on the right. Below the filters is an Export button. The main area is a table with 13 rows of log entries. The table has columns for No., Operation Time, Major Type, Minor Type, Remote Operator, Remote Host Address, and Description. The bottom of the interface shows pagination controls: 15 PCs in total, Page 1/1, and a dropdown menu for PCs per page (set to 20) with a Go button.

No.	Operation Time	Major Type	Minor Type	Remote Operator	Remote Host Address	Description
1	2019-09-12 21:34:57	Operation	Remote Login	admin	10.6.114.16	Remote Login(web)
2	2019-09-12 19:33:06	Operation	Remote Login	admin	10.6.114.16	Remote Login(web)
3	2019-09-12 17:38:38	Operation	Remote Login	admin	10.6.114.16	Remote Login(web)
4	2019-09-12 16:45:55	Operation	Remote Export Confil...	admin	10.6.114.16	REMOTE_CFGFILE_OUTPUT
5	2019-09-12 16:27:20	Operation	Remote Login	admin	10.6.114.16	Remote Login(web)
6	2019-09-12 16:24:29	Operation	Remote Login	admin	10.12.99.11	Remote Login(web)
7	2019-09-12 16:24:14	Operation	Start Up			Power On
8	2019-09-12 16:23:33	Operation	Remote Import Confil...	admin	10.12.99.11	REMOTE_CFGFILE_INPUT
9	2019-09-12 16:22:46	Operation	Remote Export Confil...	admin	10.12.99.11	REMOTE_CFGFILE_OUTPUT
10	2019-09-12 15:56:54	Operation	Remote Login	admin	10.6.114.16	Remote Login(web)
11	2019-09-12 15:43:19	Operation	Remote Login	admin	10.25.207.111	Remote Login(web)
12	2019-09-12 15:36:36	Operation	Remote Login	admin	10.29.219.170	Remote Login(web)
13	2019-09-12 15:36:09	Operation	Remote Login	admin	10.12.99.11	Remote Login(web)

Figure 5-8 Log Management

2. Set search conditions, including **Major Type**, **Minor Type**, **Start Time** and **End Time**.
3. Click **Search**.

 **Note**

A maximum of 2000 search results can display. Please narrow down the search scope if there are too many search results.

4. **Optional:** Click **Export** to export all the search results.

 **Note**

Logs can be exported in Excel. A prompt window will pop up when the logs are exported successfully.

5.7 User Management

Regularly change the password can guarantee the security of the device.

Steps

1. Go to **System Management** → **User Management**.
2. Click **Edit**.

No.	User Name
1	admin

Edit

User Name:

Old Password:

New Password:

8 to 16 characters allowed, including at least 2 of the following types: digits, lower-case letters, upper-case letters, and special characters.

Confirm Password:

Figure 5-9 User Management

3. Enter the old password.
4. Enter a new password and confirm it.
5. Click **OK**.

5.8 Security Management

SSH

HTTPS Port:

SSH Service:

SADP Service:

Figure 5-10 Security Management

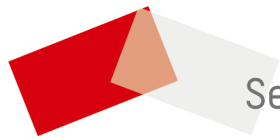
The device supports SSH security service. SSH can prevent the information leakage in the remote management of the device. SSH is disabled by default.

Note

The user name of SSH is **root**, and the password is the device login password.

SADP

After enabling SADP, you can activate the device, change the password and the network information, and etc. SADP is enabled by default.



See Far, Go Further