100 Mbps PoE Switch Client

User Manual

Legal Information

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/***).

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. 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-3E1XXXP series switches.

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.
ℹ **Note**	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

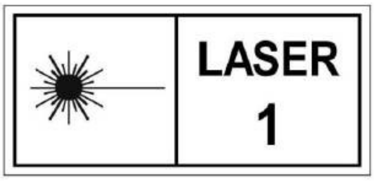
⚠ **Danger**

- 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.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- The device must be connected to an earthed mains socket-outlet.
- Install the device according to the instructions in this manual.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Keep body parts away from fan blades. Disconnect the power source during servicing.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- This device is not suitable for use in locations where children are likely to be present.

- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas. Dispose of used batteries according to the instructions.

⚠ **Caution**

- CAUTION: Double pole/Neutral fusing. After operation of the fuse, parts of the device that remain energized might represent a hazard during servicing.
- The device has been designed, when required, modified for connection to an IT power distribution system.
- This device is suitable for mounting on concrete or other non-combustible surface only.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the device on a bed, sofa, rug or other similar surface.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The device shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the device.
- Burned fingers when handling the cover area of the device. Wait one-half hour after switching off before handling the parts.
- CLASS 1 LASER PRODUCT



Contents

Chapter 1 Product Introduction

DS-3E1XXXP series switches (hereinafter referred to as "the device") are layer 2 PoE switches, providing advanced PoE power supply technology on the basis of high-performance access. The switches support client management, network topology management, link aggregation, port management and so on. The switches are suitable for small-scale LAN device access.

Chapter 2 Device Management

The device can be configured and managed through iVMS-4200 software, mainly including network parameter configuration, port configuration, link aggregation configuration, network topology display and so on.

Note

- This chapter will briefly introduce the device management through the iVMS-4200 software. For other functions, please refer to *User Manual of iVMS-4200 Client Software*.
- All pictures in this manual are for illustration only, and the specific interface is subject to the actual interface.

2.1 Activating Devices

For the inactive devices, you are required to create a password to activate them before they can be added to the software and work properly.

Before You Start

Make sure the device to be activated is connected to the network and is in the same subnet with the PC running the client.

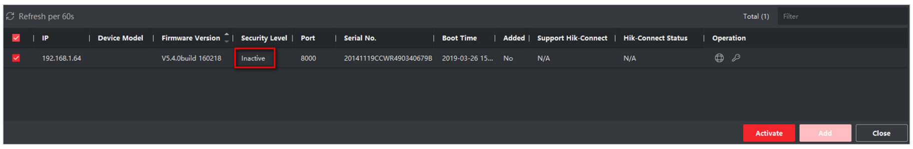
Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area at the bottom of the page.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.



Refresh per 60s

Total (1)

☑	IP	Device Model	Firmware Version	Security Level	Port	Serial No.	Boot Time	Added	Support Hik-Connect	Hik-Connect Status	Operation
☑	192.168.1.64		V5.4.0build 160218	Inactive	8000	20141119CCWR490340679B	2019-03-26 15...	No	N/A	N/A	

Figure 2-1 Online Inactive Device

5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Click **OK** to activate the device.

2.2 Adding Devices

The client provides various device adding modes including IP/domain, IP segment, cloud P2P, ISUP protocol, and HiDDNS. The client also supports importing multiple devices in a batch when there are large amount of devices to be added. The section only introduces one mode, namely, adding a detected online device.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Select an online device in the **Online Device** area, and click **Add** to open the device adding window.

   Note

   For the inactive device, you need to create the password for it before you can add the device properly. For detailed steps, refer to ***Activating Devices*** .
5. Enter the required information.

   Name

   Enter a descriptive name for the device.

   IP Address

   Enter the device's IP address. The IP address of the device is obtained automatically in this adding mode.

   Port

   You can customize the port number. The port number of the device is obtained automatically in this adding mode.

   User Name

By default, the user name is ***admin***.

Password

Enter the device password.

⚠ **Caution**

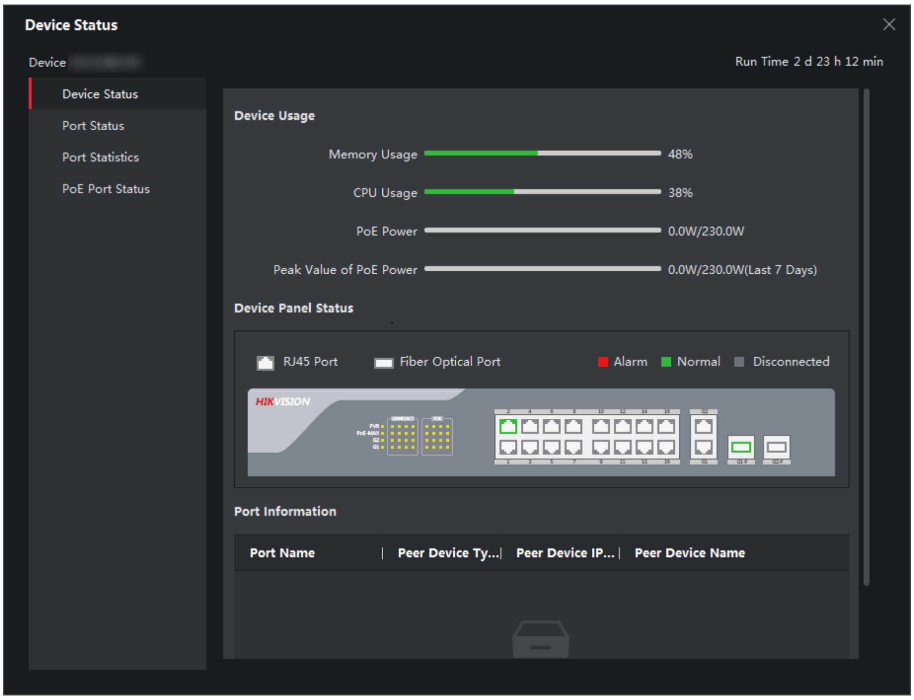
The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. Click **Add**.

Chapter 3 Device Status

In the **Device Management → Device** interface, click ▤ to view the device status, port status, PoE port status, and port statistics.



Device Status

Device [redacted]

Run Time 2 d 23 h 12 min

Device Usage

Memory Usage 48%

CPU Usage 38%

PoE Power 0.0W/230.0W

Peak Value of PoE Power 0.0W/230.0W(Last 7 Days)

Device Panel Status

Port Information

Port Name	Peer Device Ty...	Peer Device IP...	Peer Device Name

Figure 3-1 Device Status

Device Status

You can view the device usage, device panel status and port information.

Port Status

You can view the bitrate, duplex and flow control of ports.

Port Statistics

You can view the number of bytes sent or received, the number of packets sent or received, sending or receiving rate, and peak value of sending or receiving rate.

Note

Drag the sliding bar to view all data.

PoE Port Status

You can view the enabling status and output power of different ports.

Chapter 4 Typology Display

In **Typology** interface, you can view the relationships among different devices added and configure the typology.

4.1 Relate Operations

Select a device added, go to ⊞ → **General Application** → **Typology** to enter the typology display interface.

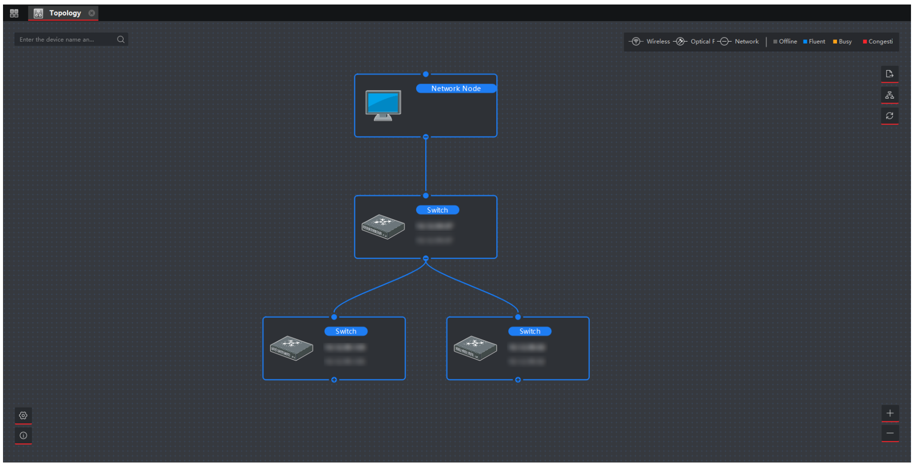


Figure 4-1 Typology Display

Interface Description

- On the upper-left corner, you can enter another name or IP address of a device to view the corresponding typology.
- On the upper-right corner, you can view the icon of lines and the meaning of different colors, select two device to show the flash of the signal transmission between them, and export or refresh the typology.
- On the lower-left corner, you can do the typology settings and view the tips.
- On the lower-right corner, you can click the icons or scroll your mouse wheel to enlarge or narrow the typology.

Note

If you enter the typology interface for the first time, no typology is displayed, please click ⟳ to refresh it.

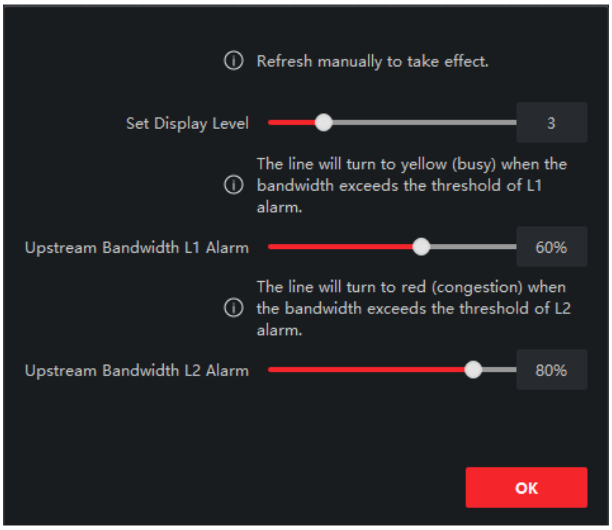
Relate Operations/Icons Description

Actions/Icons	Operation Description
Double click a device.	Show the device type and IP, panel status, and port information.
Double click a line.	Show transmission rate, port information, etc.
Right-click a device.	Jump to **Device Status** interface. For details, see ***Device Status*** .
	Show the alarm information and event information, and cancel the alarm.
	Jump to **Remote Configuration** interface.
	Set the device as root node.
	Edit the device name.
	Select the path and format to export the typology.
	Select IPC and current devices to show the flash of the signal transmission between them.

4.2 Typology Settings

Steps

1. Click ⚙ on the lower-left corner to do the typology settings.
   - Set display level: 1 to 10.
   - Set upstream bandwidth L1 alarm: 1% to 100%. The line will turn to yellow (busy) when the bandwidth exceeds the threshold of L1 alarm.
   - Set upstream bandwidth L2 alarm: 1% to 100%. The line will turn to red (congestion) when the bandwidth exceeds the threshold of L2 alarm.
2. Click **OK**.



ⓘ Refresh manually to take effect.

Set Display Level 3

ⓘ The line will turn to yellow (busy) when the bandwidth exceeds the threshold of L1 alarm.

Upstream Bandwidth L1 Alarm 60%

ⓘ The line will turn to red (congestion) when the bandwidth exceeds the threshold of L2 alarm.

Upstream Bandwidth L2 Alarm 80%

Figure 4-2 Typology Settings

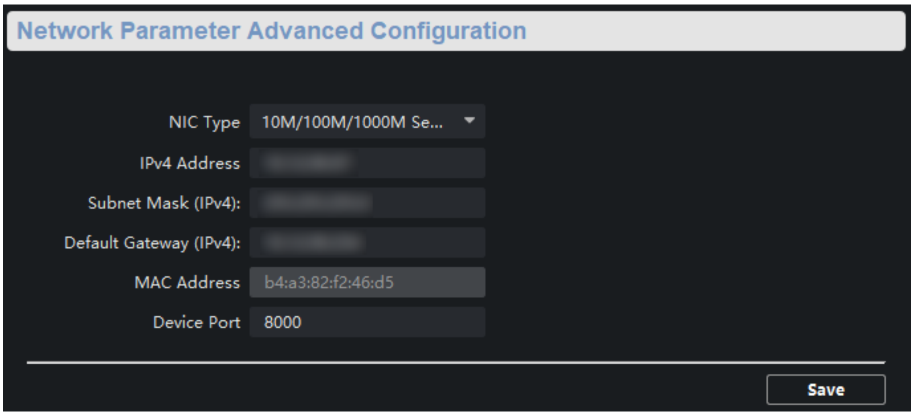
Note

After changing the typology settings, you need to click ⟳ to view the latest typology.

Chapter 5 Network Configuration

In **Network** interface, you can configure basic parameters as needed.

Go to ⚙ → **Network** → **General** to configure NIC type, IPv4 address, subnet mask, default gateway, MAC address, and device port.



Network Parameter Advanced Configuration

NIC Type: 10M/100M/1000M Se...

IPv4 Address: [redacted]

Subnet Mask (IPv4): [redacted]

Default Gateway (IPv4): [redacted]

MAC Address: b4:a3:82:f2:46:d5

Device Port: 8000

Figure 5-1 Network Configuration

Note

After the IPv4 address is reset, the device IP may not be in the same network segment as the computer IP of the client, so it cannot be configured and managed. It is recommended to use the SADP tool to plan the IP address of the device when the device is activated for the first time.

Chapter 6 Port Configuration

Select ⚙ → **Port Configuration** to enter the interface.

Note

Different devices have different functions, so the actual interface shall prevail.

6.1 Attribute Configuration

The basic parameters can influence the working status of ports. Configure the bitrate, duplex, and flow control, and enable or disable ports according to the actual situations in the **Attribute Configuration** interface.

Bitrate

The data transmission rate of the port. The rate includes auto, 10 Mbps, 100 Mbps, and 1000 Mpbs. The default is **Auto Negotiation**. The configurable rate varies with different ports.

Duplex

The duplex mode of the port. Only **Auto Negotiation** is available for the current version.

Flow Control

Enabling the flow control can prevent data loss in data transmission. The default is **Enable**.

Enable

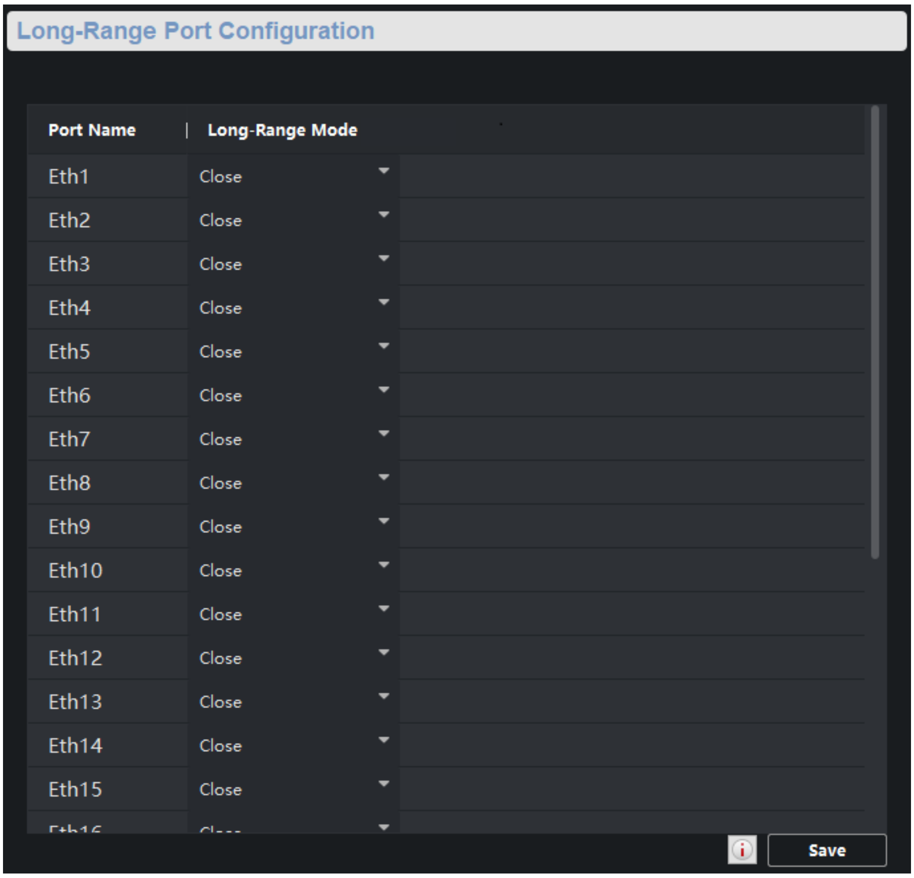
Enable or disable the port link. After you disable the port link, the data of the port stops transmission, but the power is supplied for other devices.

Note

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

6.2 Long-Range Port Configuration

When the long-range mode is enabled, the transmission distance of the port can reach 250 meters, and the rate is 10 Mbps. When the long-range mode is disabled, the rate is restored to auto.



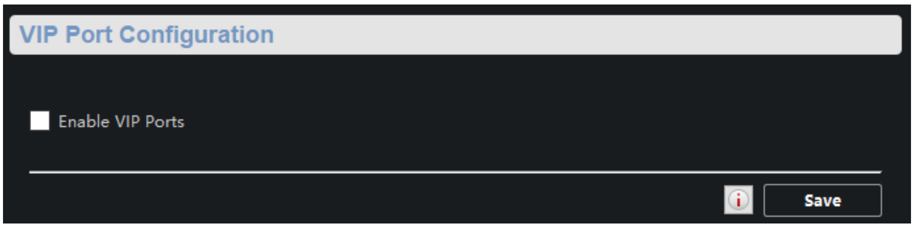
Long-Range Port Configuration

Port Name	Long-Range Mode
Eth1	Close
Eth2	Close
Eth3	Close
Eth4	Close
Eth5	Close
Eth6	Close
Eth7	Close
Eth8	Close
Eth9	Close
Eth10	Close
Eth11	Close
Eth12	Close
Eth13	Close
Eth14	Close
Eth15	Close
Eth16	Close

Figure 6-1 Long-Range Configuration

6.3 VIP Port Configuration

VIP ports refer to high priority ports, which is identified by the red area on the device. In the case of uplink congestion, the data for the ports in this area is transmitted first.



VIP Port Configuration

□ Enable VIP Ports

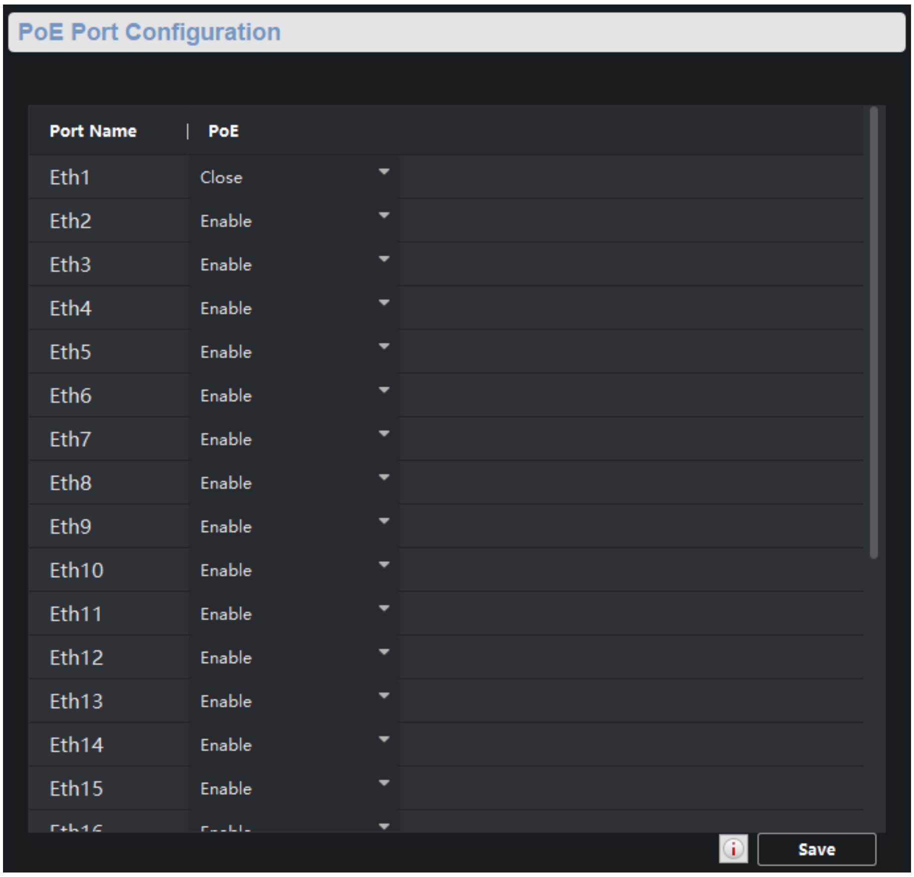
Figure 6-2 VIP Port Configuration

6.4 PoE Port Configuration

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 Port Configuration

Port Name	PoE
Eth1	Close
Eth2	Enable
Eth3	Enable
Eth4	Enable
Eth5	Enable
Eth6	Enable
Eth7	Enable
Eth8	Enable
Eth9	Enable
Eth10	Enable
Eth11	Enable
Eth12	Enable
Eth13	Enable
Eth14	Enable
Eth15	Enable
Eth16	Enable

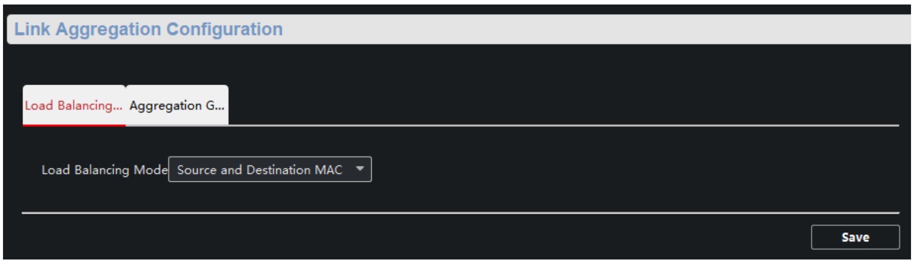
Figure 6-3 PoE Port Configuration

Chapter 7 Link Aggregation Configuration

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

Steps

1. Select ⚙ → **Link Aggregation** → **Load Balancing Configuration** .



Load Balancing Mode Source and Destination MAC

Figure 7-1 Load Balancing Configuration

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

2. Select ⚙ → **Link Aggregation** → **Aggregation Group** .

Note

Only gigabit ports can be added into aggregation groups.

3. Click **Add**.

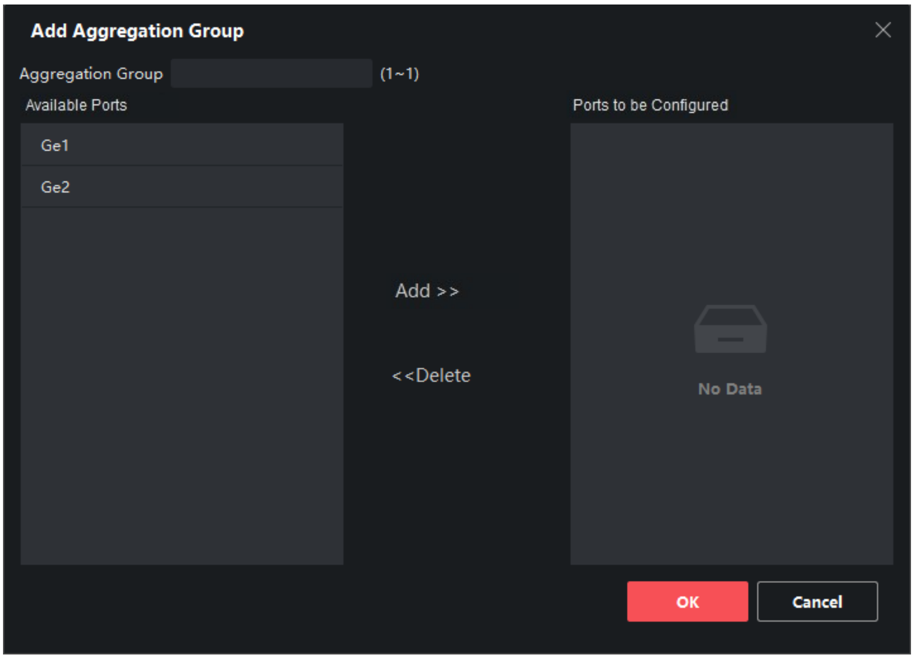


Figure 7-2 Add Aggregation Group

4. Enter the group number in the **Aggregation Group** field.
5. Move the ports that are to be assigned to the group from the **Available Ports** to the **Ports to be Configured** list.

Note

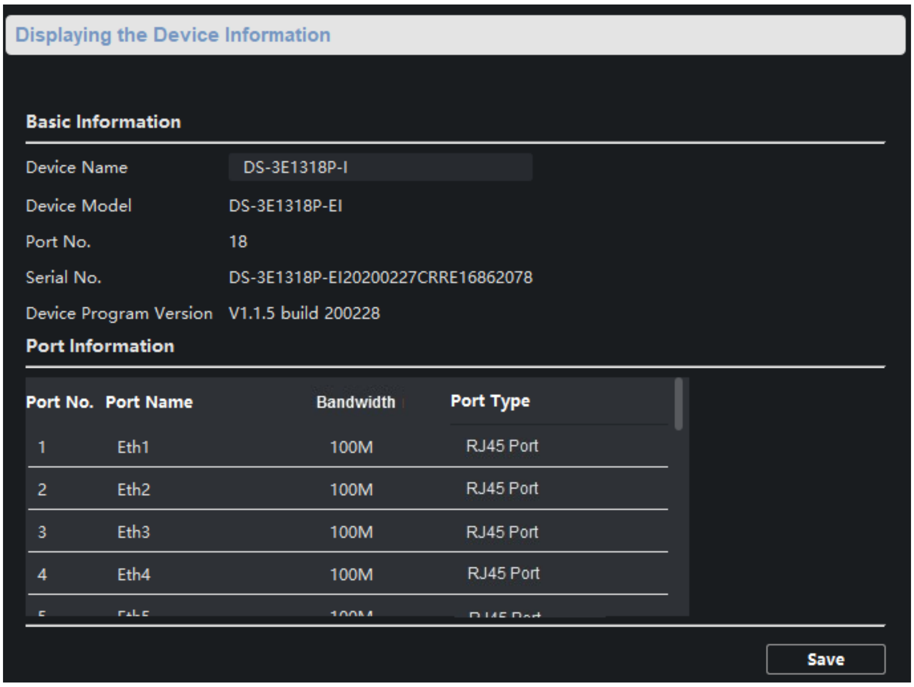
- You can delete the ports from the **Ports to be Configured** by clicking **Delete**.
- Up to 4 ports can be added a link aggregation group.
- The rate, duplex, flow control, and long-range configuration of all ports must be the same in the aggregation group.

6. Click **OK** to add a link aggregation group.

Chapter 8 System Configuration

8.1 Device Information

Select ⚙ → **System** → **Device Information** to view the device information including the device name, device model, port No., and port information.



Displaying the Device Information

Basic Information

Device Name	DS-3E1318P-I
Device Model	DS-3E1318P-EI
Port No.	18
Serial No.	DS-3E1318P-EI20200227CRRE16862078
Device Program Version	V1.1.5 build 200228

Port Information

Port No.	Port Name	Bandwidth	Port Type
1	Eth1	100M	RJ45 Port
2	Eth2	100M	RJ45 Port
3	Eth3	100M	RJ45 Port
4	Eth4	100M	RJ45 Port
5	Eth5	100M	RJ45 Port

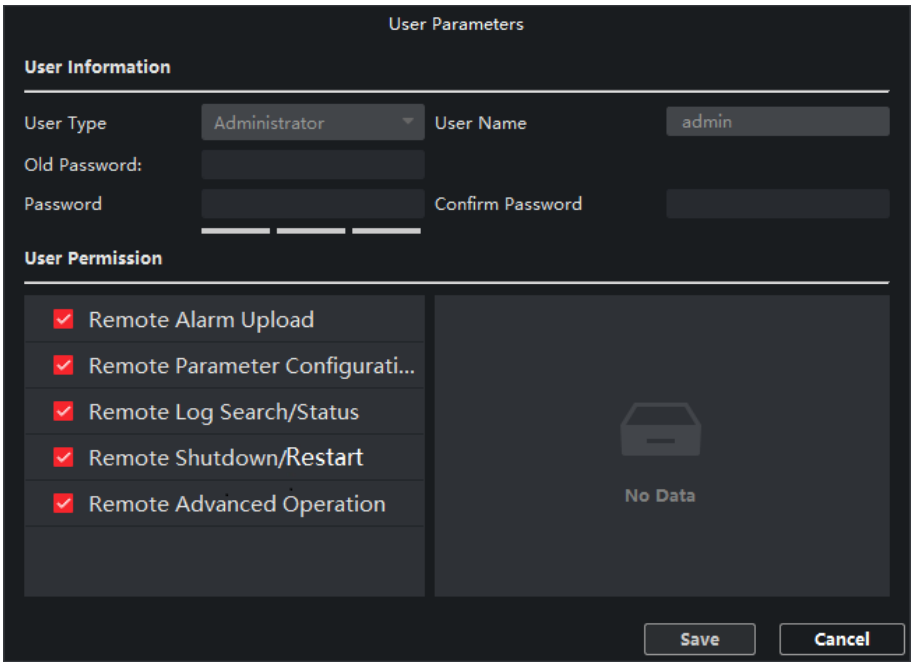
Figure 8-1 Device Information

8.2 User Management

The device only supports one admin user. Users cannot be added or deleted. You can only edit the passwords, IP addresses and permissions of the user.

Steps

1. Select ⚙ → **System** → **User** .
2. Click **Edit** or double-click the user to edit the password, IP address or permission of the user.



User Parameters

User Information

User Type: Administrator
User Name: admin
Old Password:
Password
Confirm Password

User Permission

☑ Remote Alarm Upload
☑ Remote Parameter Configurati...
☑ Remote Log Search/Status
☑ Remote Shutdown/Restart
☑ Remote Advanced Operation

No Data

Figure 8-2 User Parameters

Password

8 to 16 characters allowed, including at least 2 of the following types: digits, lower-case letters, upper-case letters, and special characters. The password strength of the device can be automatically checked. We highly recommend you change your password regularly in order to increase the security of your product.

User Permission

Configure different permissions according to actual needs.

8.3 Device Maintenance

You can restart the device, restore the defaults, upload the upgrade file to upgrade your device.

Steps

1. Select ⚙ → **System** → **System Maintenance** .
2. Select function button to realize different functions.
   - **Reboot**: Click **Reboot** to remotely restart the device.
   - **Restore Default Settings**: Except network configuration and user parameters, all of the other parameters are restored to the default settings.
   - **Restore All**: All parameters are restored to the default settings. After restoration, the device needs to be activated again.
   - **Import Configuration File**: Select the configuration file, and enter the password for file export. After import, the devices will be restarted automatically.

- **Export Configuration File**: Set and confirm the password for file export, and click **OK**. Select a storage path, and click **Save**.
- Click ⋯ to select the upgrade file, and click **Upgrade**. The upgrading progress is shown below.

Note

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

8.4 Log Management

System operation logs can be searched and exported for backup.

Steps

1. Select ⚙ → **System** → **Log Query** .
2. Set search conditions.

   Search Mode

   By Type, **By Time**, **By Time&Type** or **All** can be selected.

   Major Type

   Operation, **Event**, and **All** can be selected. If you select the search mode as by time, the major type cannot be set.

   Minor Type

   Minor type is different under different major type. If you select the search mode as by time, the major type cannot be set.

   Start Time

   It refers to the start time for the logs. If you select the search mode as by type, the major type cannot be set.

   End Time

   It refers to the end time for the logs. If you select the search mode as by type, the major type cannot be set.
3. Click **Search**.
4. Click **Backup**, and select a backup path.
5. Click **Backup**.

8.5 Security Configuration

If the IP is locked because you enter a wrong password, the admin user can log in to the client at the PC (the IP is not locked) and enter the **Security** interface to unlock the locked IP.

Steps

Note

If you need to unlock it immediately, you can contact the admin user.

1. Select ⚙ → **System** → **Security** .
2. Unlock the IPs.
   - Click unlock icon to unlock single IP.
   - Click **Unlock All** to unlock all of the IPs.

   Note

   - If the admin user is locked, you need to change the IP to log in admin again and unlock the locked IP.
   - The maximum number of consecutive wrong passwords allowed for ordinary users is 5, and for admin users is 7.

See Far, Go Further