Embedded Video Storage Server (EVS50, EVS70 Series)

User's Manual

V2.1.0

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change passwords and use strong passwords:

The primary reason that systems get "hacked" lies in weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password is made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update firmware:

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

"Nice to have" recommendations to improve your network security

1. Change your password regularly:

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change default HTTP and TCP ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward only ports you need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable auto-login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without appropriate credentials from accessing the system.

8. Use a different user name and password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone to collect those passwords and try them out on your video surveillance system. Using a

different user name and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit features of guest accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions required to perform their job.

10. UPnP:

● Once enabled, UPnP will automatically try to forward ports in your router or modem. Functionally, this brings convenience to the user. However, if your system automatically forwards the ports and you keep the default credentials, you may end up with unwanted visitors.

● If you have manually forwarded the HTTP and TCP ports in your router/modem, we recommend you to close this function. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. SNMP is limited to temporary use for tracing and testing purposes.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known vulnerabilities involving Multicast. Close it when it is not used to enhance your network security.

13. Check the log:

Check the system log to see if anyone has gained unauthorized access to your system. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically lock down the device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way is to install the recorder in a lockbox, a locking server rack, or a room with lock and key.

15. Connect IP cameras to the PoE ports on the back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from other networks and cannot be accessed directly.

16. Isolate NVR and IP camera network:

The network your NVR and IP camera resides on should not be the same as your public computer network. This will prevent unauthorized visitors from getting access to the network that the security system requires to function properly.

Regulatory Information

FCC Information

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC conditions:

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

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

FCC compliance:

This equipment has been tested and found to comply with the limits for a digital device, pursuant to Part 15 of the FCC Rules. This equipment generates, uses and radiates radio frequency energy and, if not installed and used in accordance with the guide, may cause harmful interference to radio communication.

- For Class A device, these limits are designed to provide reasonable protection against harmful interference in a commercial environment. 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 or her own expense.
- For Class B device, these limits are designed to provide reasonable protection against harmful interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.

General

This User's Manual (hereinafter referred to as "the Manual") introduces the functions and operations of the EVS series (hereinafter referred to as "the Device").

Models

Series	Model
Middle-class	Middle-class 16-HDD single-controller, middle-class 24-HDD single-controller, middle-class 36-HDD single-controller, middle-class 48-HDD single-controller
High-end	High-end 24-HDD single-controller, high-end 48-HDD single-controller

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, may result in property damage, data loss, lower performance, or unpredictable result.
ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
ESD	Electrostatic sensitive devices. Indicates a device that is sensitive to electrostatic discharge.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First release	—
2	V2.0.0	Baseline switch	October 2017
3	V2.0.1	Add privacy protection notice	May 2018
4	V2.0.2	Add FCC information	September 2018
5	V2.1.0	Update information about GDPR Add AI playback and routing functions Update user management and playback functions	October 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to comply with local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures including but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area, providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall govern.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the printed User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between printed User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in description of technical data, functions and operations, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Go to our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Operation Requirement

- Do not place or install the Device in a place exposed to sunlight or near the heat source.
- Keep the Device away from dampness, dust or soot.
- Keep the Device installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure there is no object filled with liquid on the Device to prevent liquid from flowing into the Device.
- Install the Device in a well-ventilated place, and do not block the ventilation of the Device.
- Operate the device within the rated range of power input and output.
- Do not dissemble the Device.
- Transport, use and store the Device under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Device; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

1 Overview

1.1 Introduction

The Device is designed for the management, storage and application of high-definition video data. It uses Linux operation system and professional customized hardware platform, and it is configured with multiple Hard Disk Drive (HDD) management system, front-end HD device management system, HD video analysis system and large capacity video storage system.

It adopts high-traffic data network transmission & forward technology and multi-channel video decoding & display technology, and realizes intelligent management, secure storage, fast forwarding and HD decoding of large capacity and multi-channel HD video data.

The Device provides standard network file sharing service and offers integrated IP SAN/NAS solution. It provides centralized storage solutions with large capacity, high scalability and high security for all kinds of video monitoring systems.

1.2 Front Panel

1.2.1 Middle-class 16-HDD Single-controller

Figure 1-1 Front panel

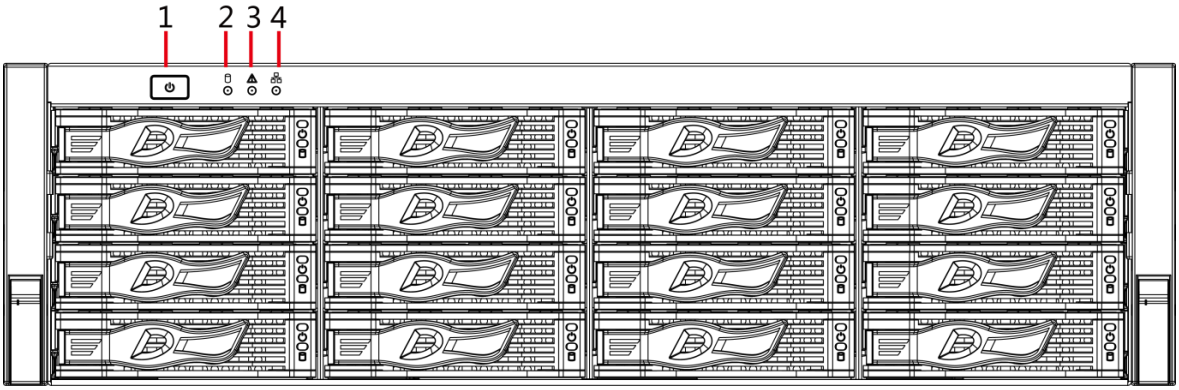


Table 1-1 Front panel interfaces

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the Device is power on. ● If the Device is off, press this button to turn the Device on. ● To turn off the Device, press and hold this button for five seconds.
2	HDD status indicator	● The light is out when the HDD is in normal operation. ● The blue light keeps on if no HDD, HDD error or insufficient HDD space.

No.	Indicator/Button	Description
3	Alarm status indicator	● Device with simple power: The light is out. ● Device with dual power: The light is out when the device is in normal operation. The red light keeps on if there is abnormal redundant power.
4	Network status indicator	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

1.2.2 Middle-class 24-HDD Single-controller / Middle-class 36-HDD Single-controller / High-end 24-HDD Single-controller

Figure 1-2 Front panel

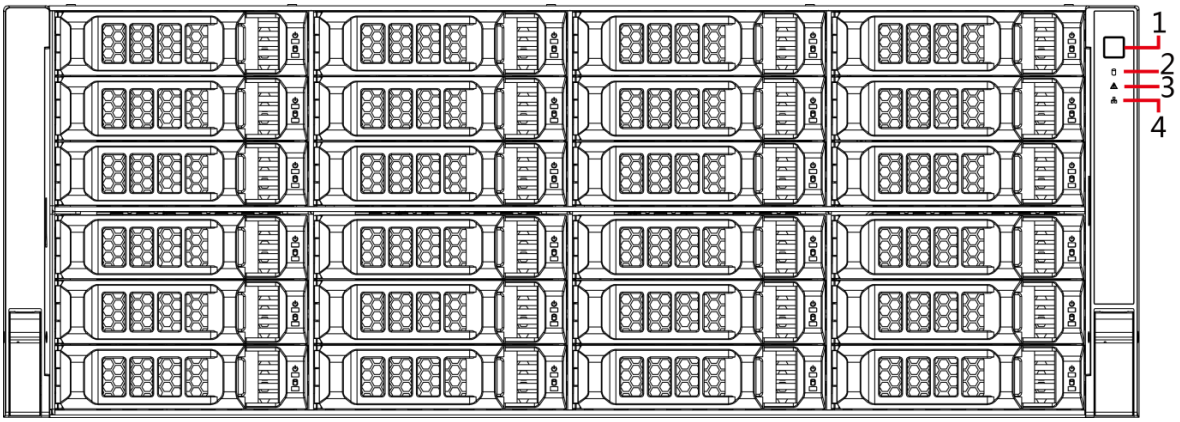


Table 1-2 Front panel interfaces

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the device is power on. ● If the device is off, press this button to turn the device on. ● To turn off the Device, press and hold this button for five seconds.
2	HDD status indicator	● The light is out when the HDD is in normal operation. ● The blue light keeps on if no HDD, HDD error or insufficient HDD space.
3	Alarm status indicator	● The light is out when the device is in normal operation. ● The red light keeps on when the power fails or the temperature/fan is abnormal.
4	Network status indicator	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

1.2.3 High-end 48-HDD Single-controller

Figure 1-3 Front panel

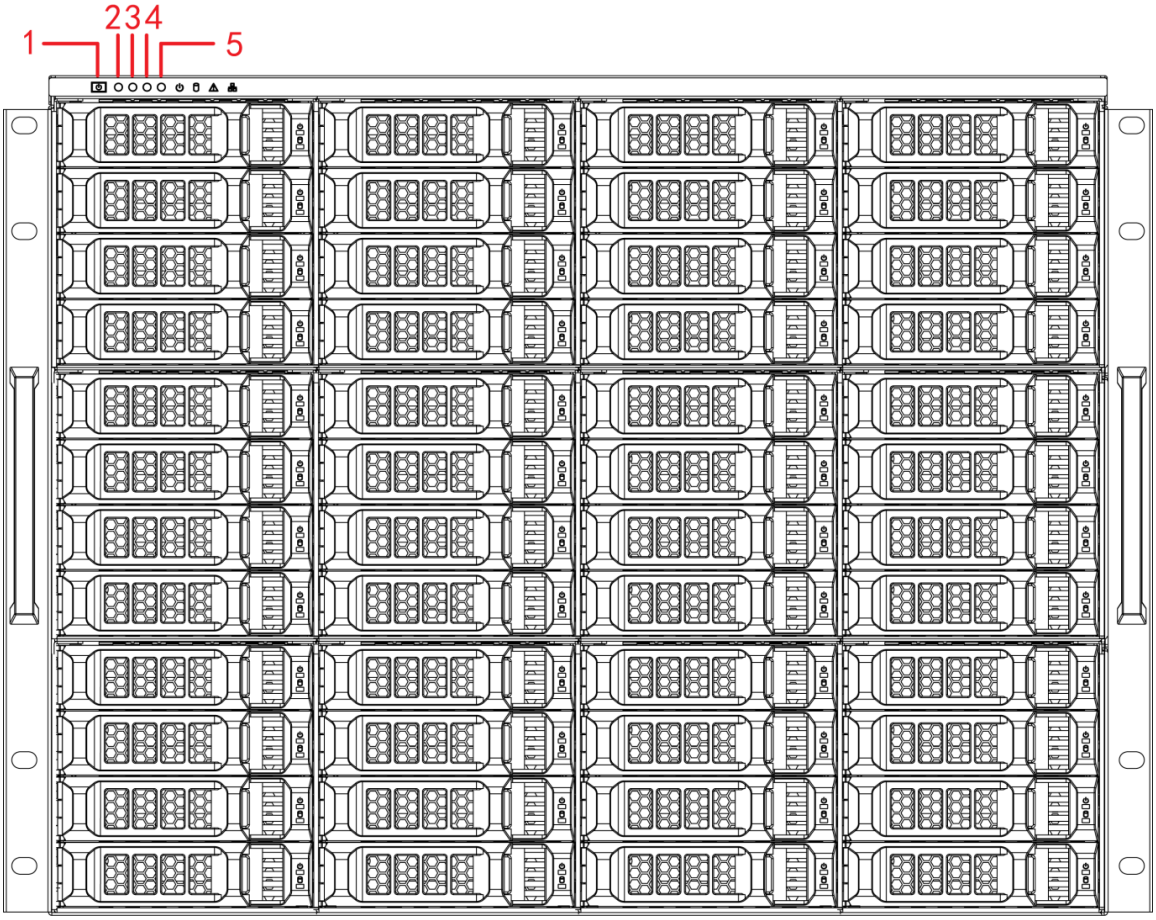


Table 1-3 Front panel interfaces

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the device is power on. ● If the device is off, press this button to turn the device on. ● To turn off the Device, press and hold this button for five seconds.
2	HDD status indicator	● The light is out when the HDD is in normal operation. ● The blue light keeps on if no HDD, HDD error or insufficient HDD space.
3	Alarm status indicator	● The light is out when the device is in normal operation. ● The red light keeps on when the power fails or the temperature/fan is abnormal.
4	Network status indicator	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

No.	Indicator/Button	Description
5	Disk slot number	Shows the number of disk slot. ● 01–64: disk slot number. ● E1–E4: controller slot number. Do not optionally pull out the controller, otherwise the installed HDD may not be recognized.

1.2.4 Middle-class 48-HDD Single-controller

Figure 1-4 Front panel

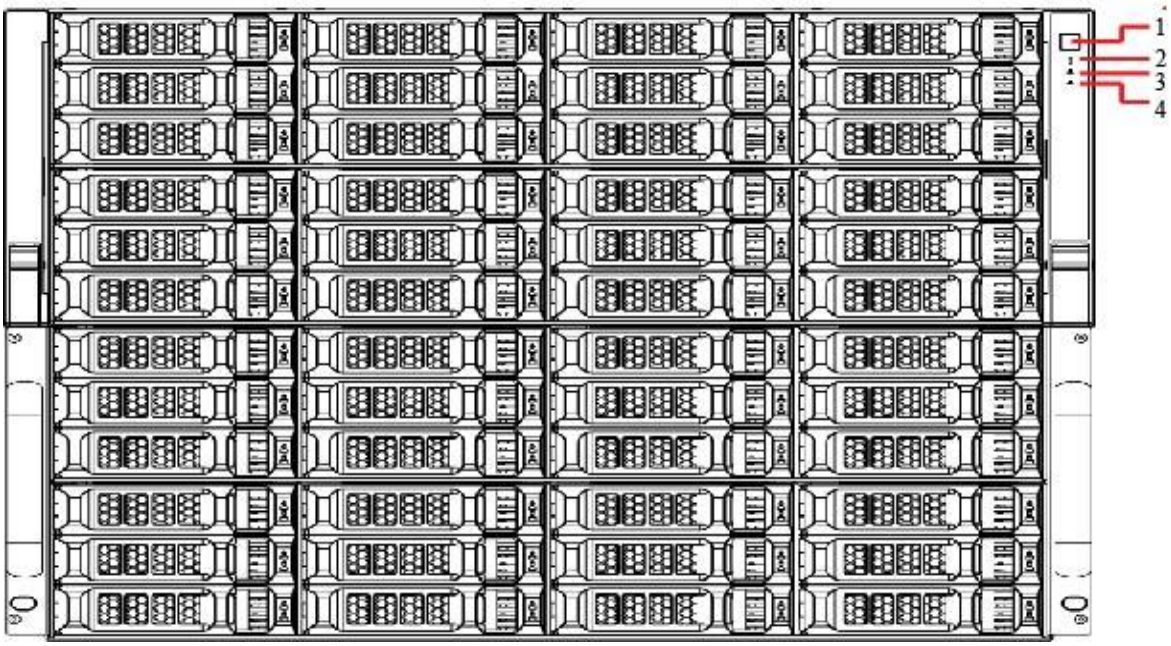


Table 1-4 Front panel interfaces

No.	Indicator /Button	Description
1	Power button	Turns on or off the Device. This button keeps blue light on when the device is power on. To turn off the Device, press and hold this button for five seconds.
2	HDD status indicator	● The light is out when the HDD is in normal operation. ● The blue light keeps on if there is no HDD, HDD error or insufficient HDD space.
3	Alarm status indicator	● The light is out when the device is in normal operation. ● The red light keeps on when the power fails or the temperature/fan is abnormal.
4	Network status indicator	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

1.3 Rear Panel

1.3.1 Middle-class 16-HDD Single-controller

Figure 1-5 Middle-class 16-HDD single-controller with single power

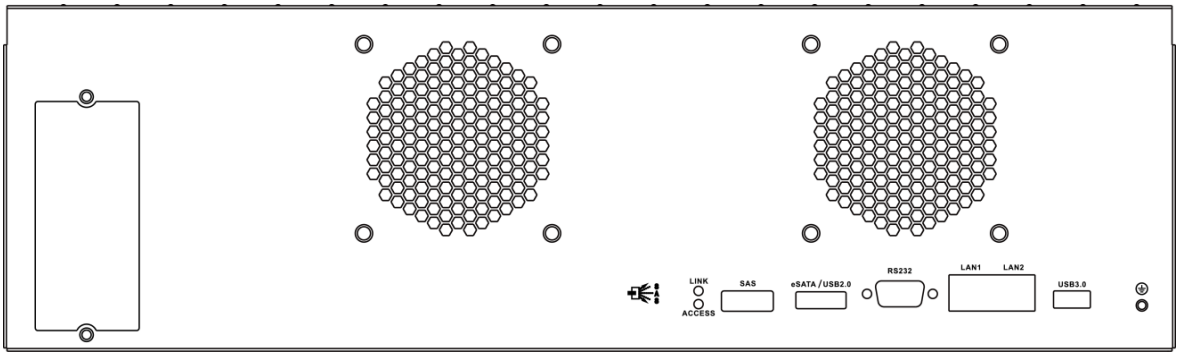


Figure 1-6 Middle-class 16-HDD single-controller with redundant power

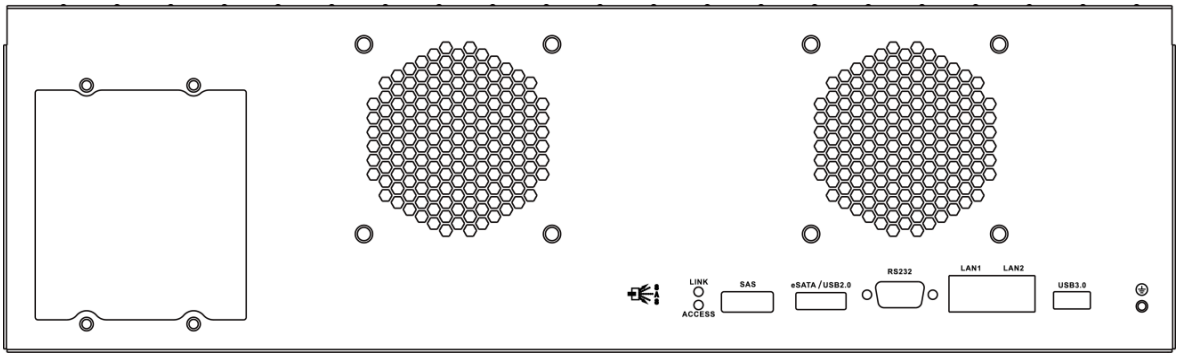


Table 1-5 Rear panel interfaces

Interface/Indicator	Description
USB3.0	Connects the mouse and USB storage devices.
LAN1, LAN2	Gigabit data port. Used for data transmission.
RS-232	RS-232 interface.
eSATA, USB2.0	Multiplex interface for eSATA and USB2.0.
SAS	Connects the IN port of the expansion drawer.
Link/ACCESS	Status indicator for SAS interface.
Power interface	Connects AC power. Middle-class 16-HDD single-controller includes devices with single power and devices with dual power.
Power switch	Turns on/off the device.

1.3.2 Middle-class 24-HDD Single-controller

Figure 1-7 Rear panel (5 Ethernet ports)

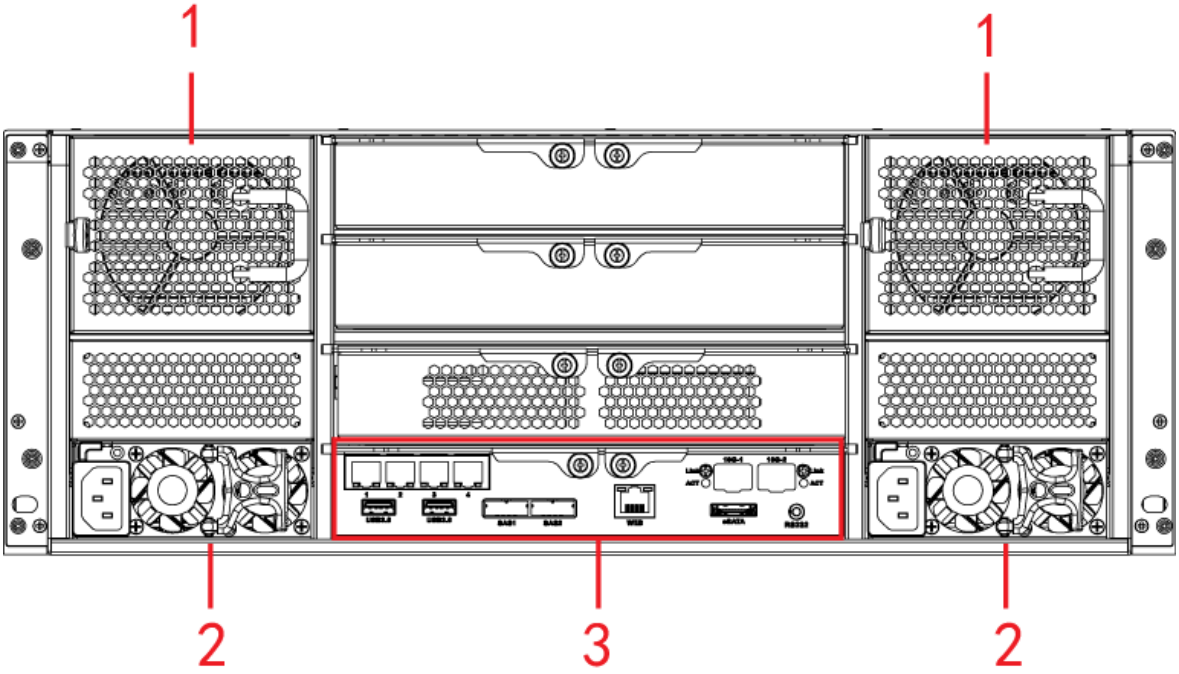


Figure 1-8 Rear panel (7 Ethernet ports)

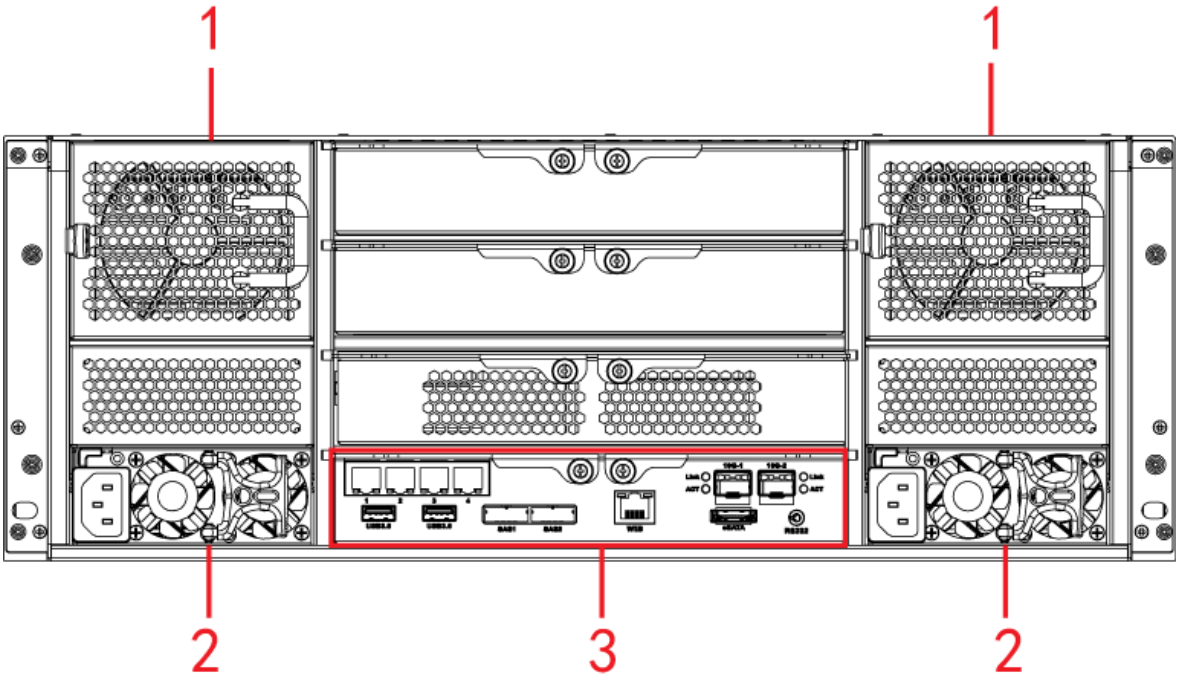


Figure 1-9 Rear panel (9 Ethernet ports)

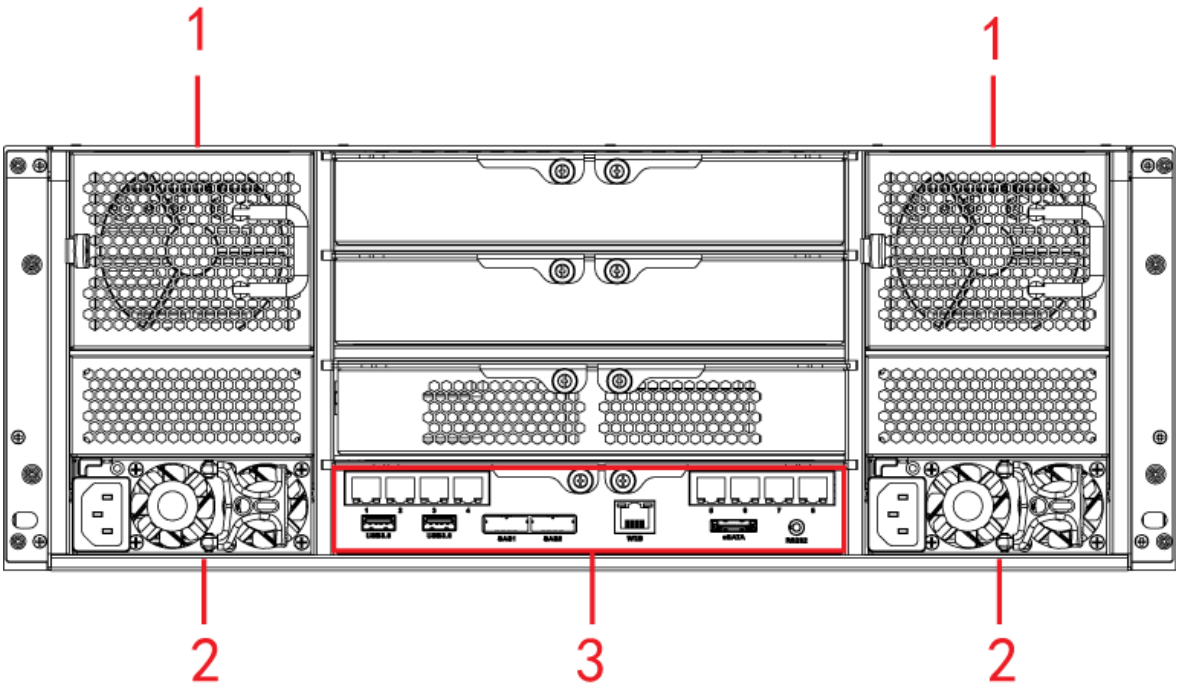


Table 1-6 Rear panel interfaces

No.	Interface	Description
1	Fan	Used for case cooling.
2	Power interface	Connects AC power.
3	Master control module	See Table 1-7.

Table 1-7 Master control module interfaces

Interface/Indicator	Description
1–4/5–8	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA	eSATA interface.
SAS1, SAS2	Connects the IN port of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port. Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status indicator of the 10 gigabit port.

1.3.3 Middle-class 36-HDD Single-controller

Figure 1-10 Rear panel (5 Ethernet ports)

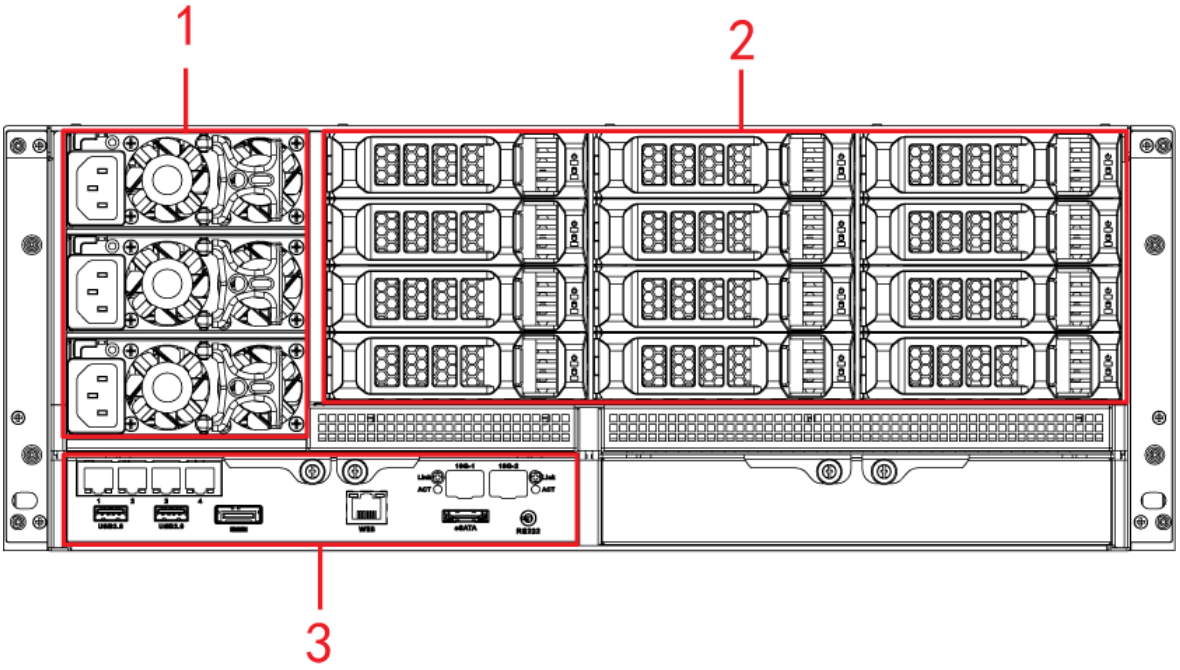


Figure 1-11 Rear panel (7 Ethernet ports)

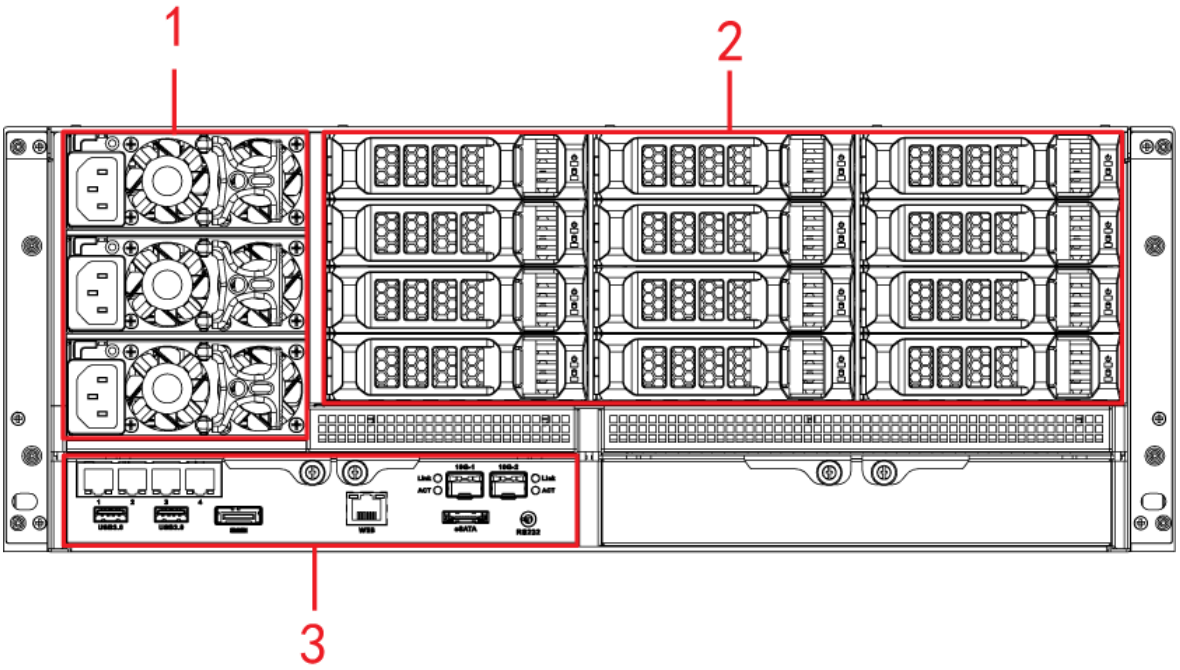


Figure 1-12 Rear panel (9 Ethernet ports)

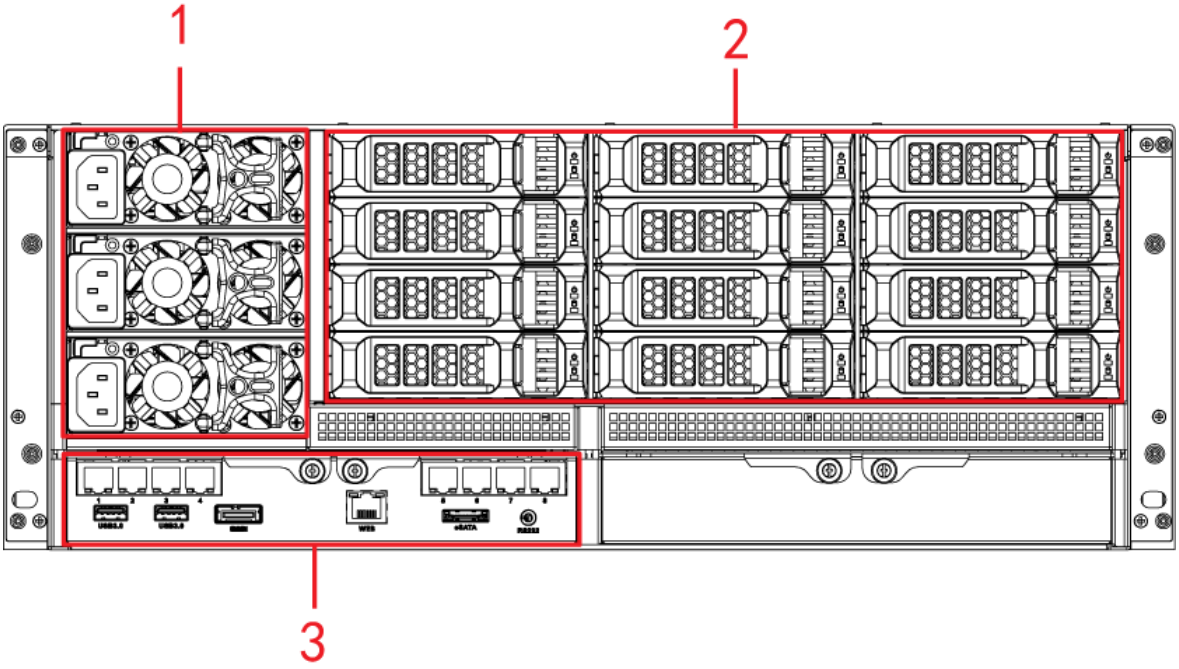


Table 1-8 Rear panel interfaces

No.	Interface	Description
1	Power interface & fan	Connects AC power and cools the case.
2	HDD slot	Installs HDD from No. 25 to No. 36.
3	Master control module	See Table 1-9.

Table 1-9 Master control module interfaces

Interface/Indicator	Description
1–4/5–8	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA	eSATA interface.
SAS	Connects the IN port of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port. Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status indicator of the 10 gigabit port.

1.3.4 Middle-class 48-HDD Single-controller

Figure 1-13 Rear panel

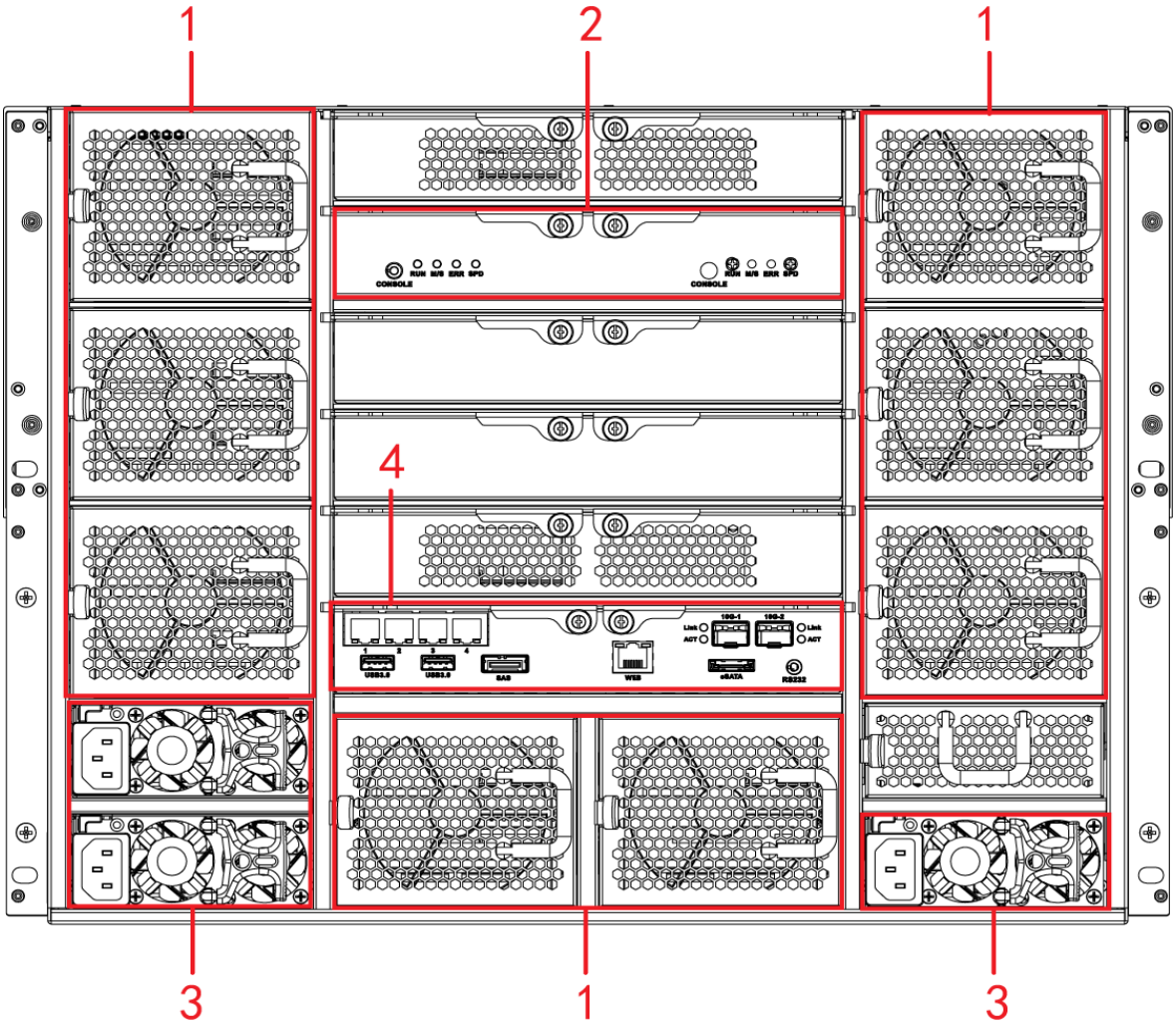


Table 1-10 Rear panel interfaces

No.	Interface	Description
1	Fan	Used for case cooling.
2	SAS expansion controller	See Table 1-12.
3	Power interface	Connects AC power.
4	Master control module	See Table 1-11.

Table 1-11 Master control module interfaces

Interface	Description
EX-1–EX-4/1–4	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA	eSATA interface.
SAS	Connects the IN port of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
ERR	ERR is on when the system is abnormal, and it is out when the system is in normal operation.

Interface	Description
RUN	RUN light flickers when the device is power on and running.
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port. Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status indicator of the 10 gigabit port.

Table 1-12 SAS expansion controller interfaces

Indicator	Description
CONSOLE	Serial port. It is mainly used for debugging the device and logging in the command line interface.
RUN	RUN light flickers when the device is power on and running.
M/S	The light is out in normal operation.
ERR	ERR is on when the system is abnormal, and it is out when the system is in normal operation.
SPD	SAS speed indicator. When lines are normally connected, the light keeps on if the speed is below 6G and the light goes out if the speed reaches 6G.

1.3.5 High-end 24-HDD Single-controller

Figure 1-14 Rear panel (5 Ethernet ports)

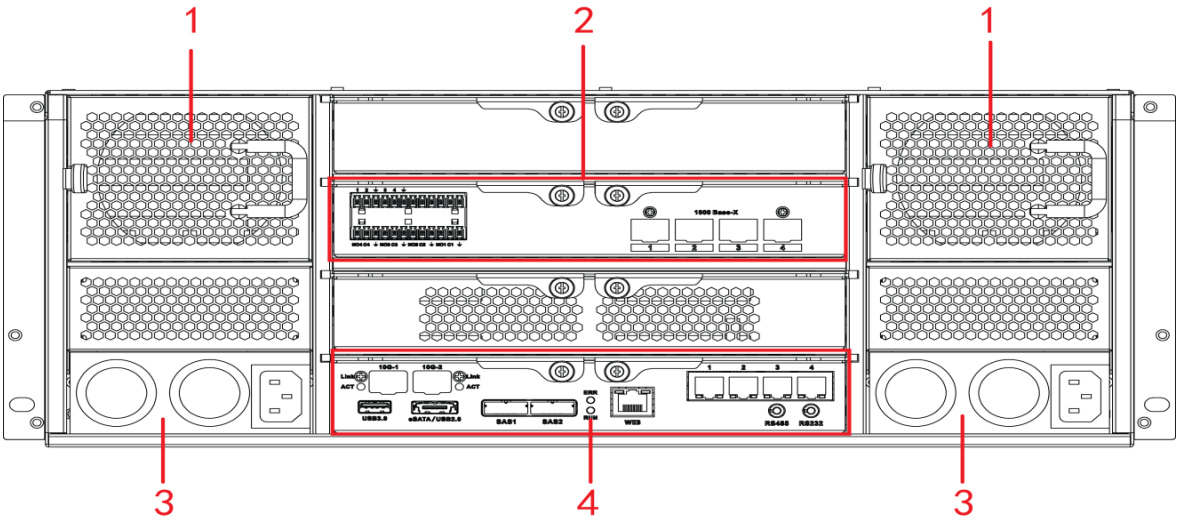


Figure 1-15 Rear panel (7 Ethernet ports)

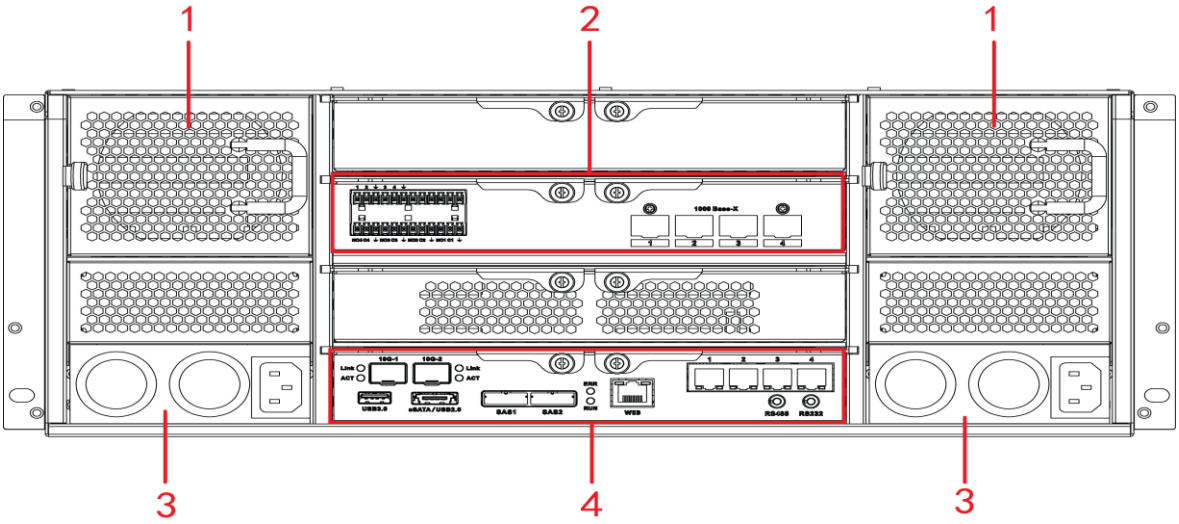


Figure 1-16 Rear panel (9 Ethernet ports)

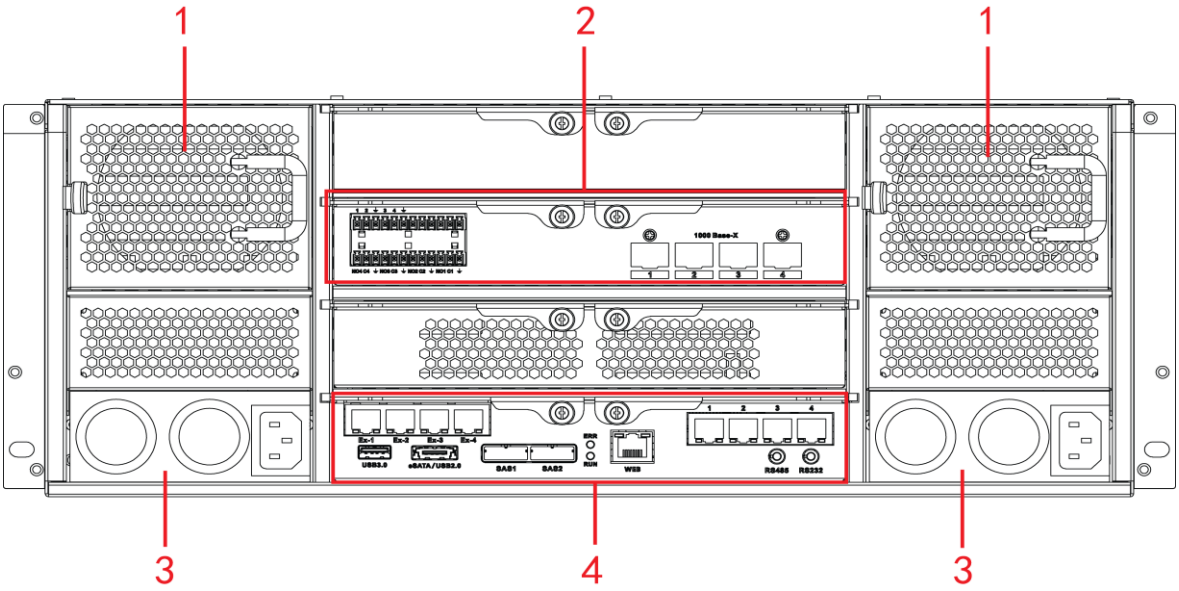


Table 1-13 Rear panel interfaces

No.	Interface	Description
1	Fan	Used for case cooling.
2	Alarm module	● 1–4 corresponds to ALARM1–ALARM4. Alarm input is effective when connected to low level. ● NO1 C1, NO2 C2, NO3 C3, and NO4 C4. Open the four sets normally to link to output (switching value). ● ⏚ GND.
3	Power interface	Connects AC power.
4	Master control module	See 0.

Table 1-14 Master control module interfaces

Interface	Description
EX-1–EX-4/1–4	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA/USB2.0	Multiplex interface for eSATA and USB2.0.
SAS1, SAS2	Connects the IN interface of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
ERR	ERR is on when the system is abnormal, and it is out when the system is in normal operation.
RUN	RUN light flickers when the device is power on and running.
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port. Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status indicator of the 10 gigabit port.

1.3.6 High-end 48-HDD Single-controller

Figure 1-17 Rear panel (5 Ethernet ports)

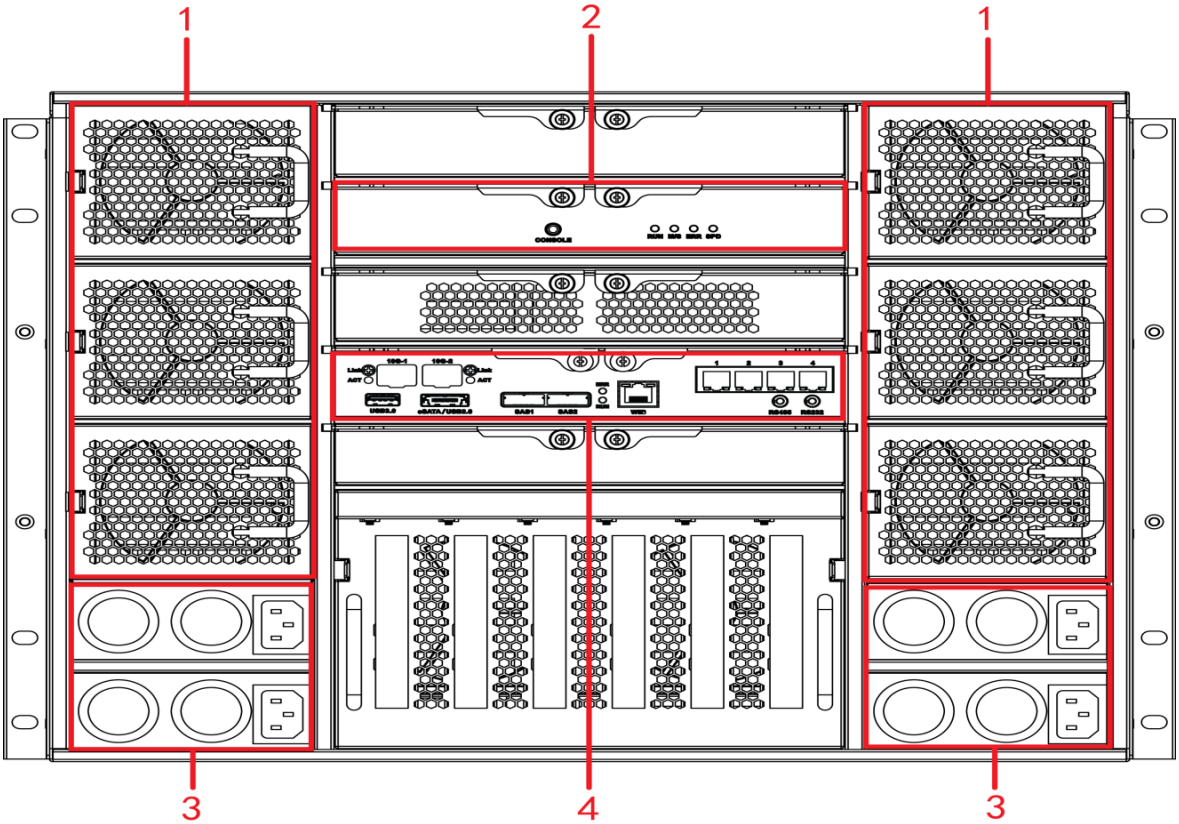


Figure 1-18 Rear panel (7 Ethernet ports)

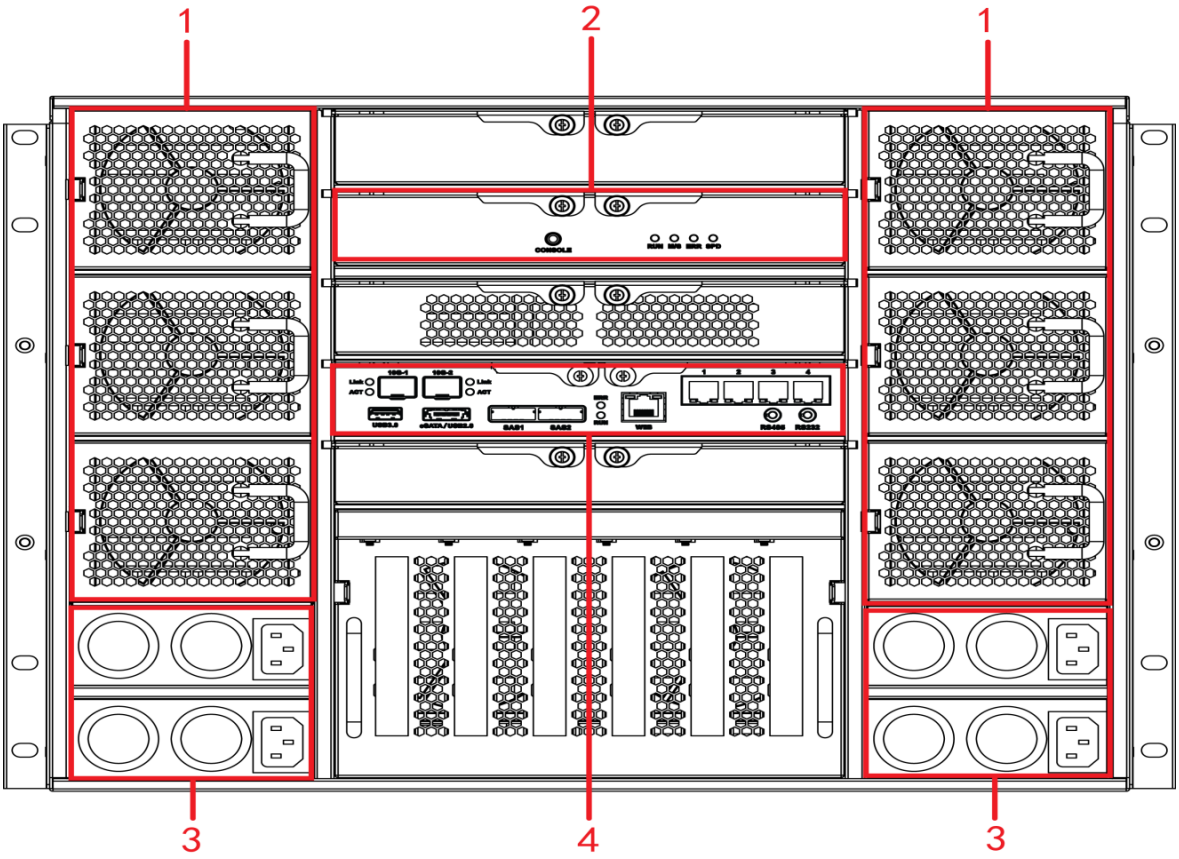


Figure 1-19 Rear panel (9 Ethernet ports)

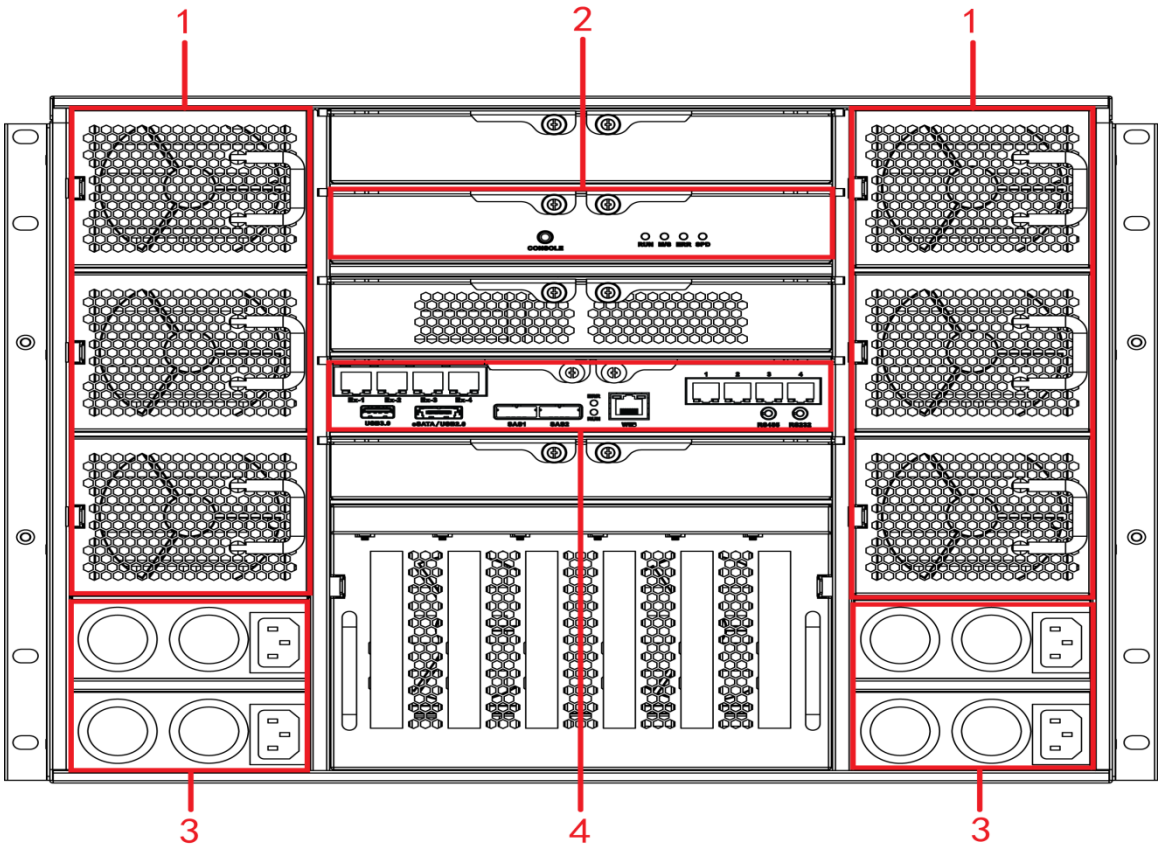


Table 1-15 Rear panel interfaces

No.	Interface	Description
1	Fan	Used for case cooling.

No.	Interface	Description
2	SAS expansion controller	See Table 1-17.
3	Power interface	Connect AC power.
4	Master control module	See Table 1-16.

Table 1-16 Master control module interfaces

Interface/Indicator	Description
EX-1–EX-4/1–4	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA/USB2.0	Multiplex interface for eSATA and USB2.0.
SAS1, SAS2	Connects the IN interface of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
ERR	ERR is on when the system is abnormal, and it is out when the system is in normal operation.
RUN	RUN light flickers when the device is power on and running.
RS485	RS485 interface.
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port.  Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status indicator of the 10 gigabit port.

Table 1-17 SAS expansion controller interfaces

Interface/Indicator	Description
CONSOLE	Serial port. It is mainly used for debugging the device and logging in the command line interface.
RUN	RUN light flickers when the device is power on and running.
M/S	The light is out in normal operation.
ERR	ERR is on when the system is abnormal, and it is out when the system is in normal operation.
SPD	SAS speed indicator. When lines are normally connected, the light keeps on if the speed is below 6G, and the light goes out if the speed reaches 6G.

1.4 Menu Items

This section introduces the icons and buttons you will frequently meet when using the Device.

Icon/Button	Description
Copy	After setting a channel, click this icon and you can copy the configuration of the current channel to other channels.
Default	Click this icon to restore default configuration. Click **OK** to save the default configuration.

Icon/Button	Description
Refresh	Click this icon to get the latest configuration information.
OK	Click this icon to save the modified configuration item.
Cancel	Click this icon to cancel the modified configuration item and close the window.
	Check box. You can select multiple configuration items at the same time. : Selected.
	Radio button. You can select a configuration item. : Selected.
	Drop-down list. Click this icon to display the drop-down menu.

2 Installation and Power Up

2.1 Installing HDD

The HDD is not installed by default on factory delivery. You need to install it by yourself.

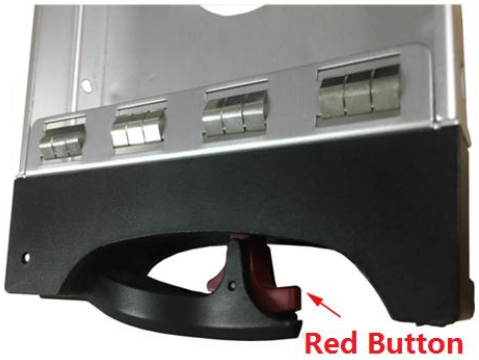
WARNING

Some devices are heavy and should be carried jointly by several persons to avoid any personnel injury.

2.1.1 Middle-class 16-HDD Single-controller Series

Step 1 Press the red button on the HDD box in the front panel and unlock the handle. See Figure 2-1.

Figure 2-1 Opening the handle



Step 2 Pull out to take the empty HDD box. See Figure 2-2.

Figure 2-2 HDD box

Step 3 Put the HDD into the disk box and fasten the screws on both sides of the box. See Figure 2-3.

Figure 2-3 Fastening the screws

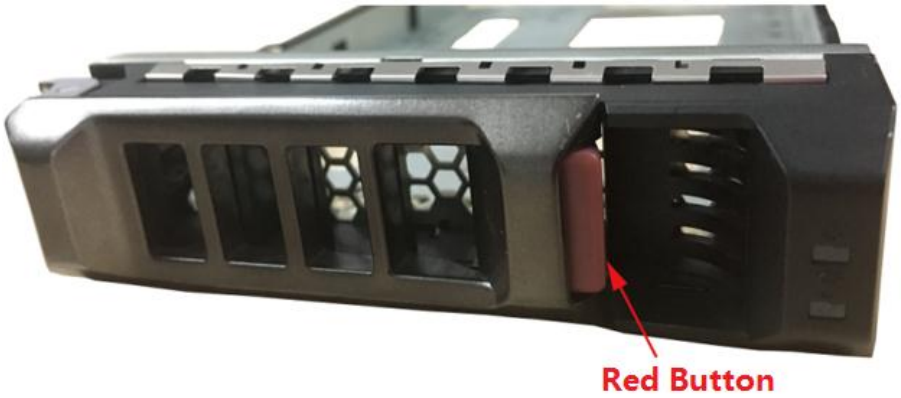
To avoid any damage to the slot, do not close the handle if the HDD box has not been pushed to the bottom.

Step 4 Insert the HDD box into the HDD slot, push it to the bottom, and then lock the handle.

2.1.2 Other Series

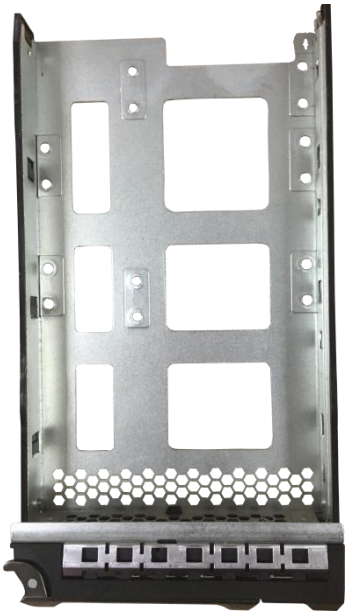
Step 1 Press the red button on the HDD box in the front panel and unlock the handle. See Figure 2-4.

Figure 2-4 Opening the handle



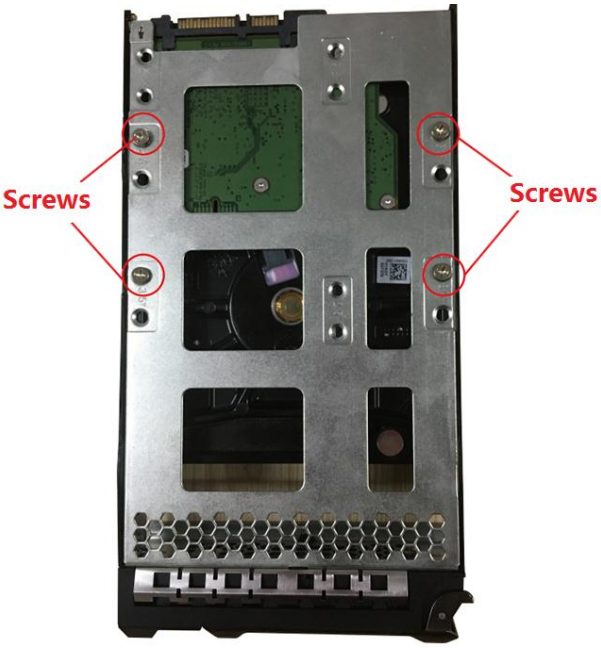
Step 2 Pull out to take the empty HDD box. See Figure 2-5.

Figure 2-5 HDD box



Step 3 Put the HDD into the disk box and fasten the screws at the bottom of the box. See Figure 2-6.

Figure 2-6 Locking the screws



To avoid any damage to the slot, do not close the handle if the HDD box has not been pushed to the bottom.

Step 4 Insert the HDD box into the HDD slot, push it to the bottom and lock the handle.

2.2 Power Up

2.2.1 Preparation

Properly connect the cables before powering up the Device and check against the following items:

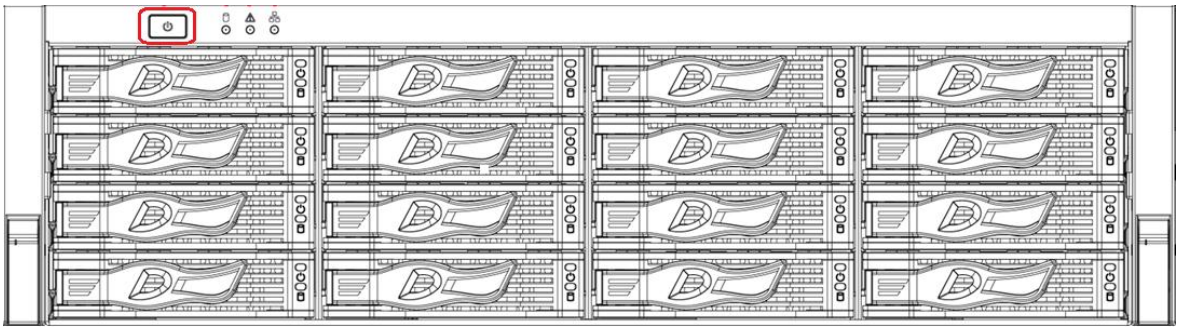
- Make sure that GND is connected correctly.
- Different models of devices need different sources of power supplies. Make sure that all power lines are connected correctly.
- Check whether the supplied power voltage complies with the device requirement.
- Check whether the network cables and SAS cables are connected correctly.

2.2.2 Powering Up the Device

This section takes middle-class 16-HDD single-controller series as the example.

Press the power button on the front panel. See Figure 2-7.

Figure 2-7 Front panel



See "1.2.1 Middle-class 16-HDD Single-controller" for the corresponding description table of front panel, and check whether the indicators are normally displayed.

- If the indicators are normal, the device is powered up successfully.
- If the indicators are abnormal, remove the abnormalities according to the corresponding notes and power up the Device again.

3 Web Basic Operations

The system supports device access and management through web at personal computer (PC).

The web client system provides functions such as information viewing, storage management, system configuration, and playback monitoring.

The following contents are only for your reference. Different models have different functions. See the corresponding model.

3.1 Connecting the Network

Before logging in web, connect your PC and the Device to the same network, and make sure the network between them is normal.

Step 1 Connect the device to the network.

Step 2 Set IP address, subnet mask and gateway IP for PC and the device respectively.

- If there is no router in the network, assign IP address of the same network segment for PC and the Device.
- If there is router in the network, set the corresponding gateway IP and subnet mask for PC and the Device respectively.

The Ethernet ports of the Device have different default IP.

- Single-control device: Network interface card (NIC) 1 to NIC n corresponds to default IP 192.168.1.108 to 192.168.n.108.
- Dual-control device: Different slots have different default IP.
  - ◇ Slot 1: NIC 1 to NIC n corresponds to default IP 192.168.1.108 to 192.168.n.108.
  - ◇ Slot 2: NIC 1 to NIC n corresponds to default IP 192.168.1.109 to 192.168.n.109.
- The ports are for standard NIC, extension NIC, and web management card. You need to confirm the default IP according to the actual device condition.

Step 3 On PC, execute the command of *Ping device IP address* to check whether the network is connected.

3.2 Initializing the Device

When you log in the device for the first time, you need to set the login password of the administrator account (admin by default).

Step 1 Open the browser and enter the IP address in the address bar.

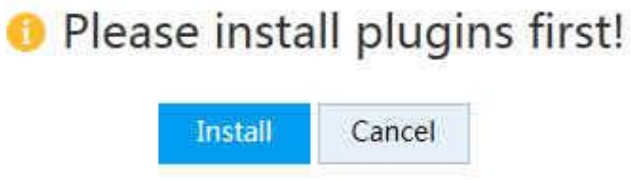
The default IP address of single-control device is 192.168.1.108.

The default IP address of dual-control device is 192.168.0.108.

Step 2 Press Enter.

The system prompts you to install plugins. See Figure 3-1.

Figure 3-1 Install plugins interface

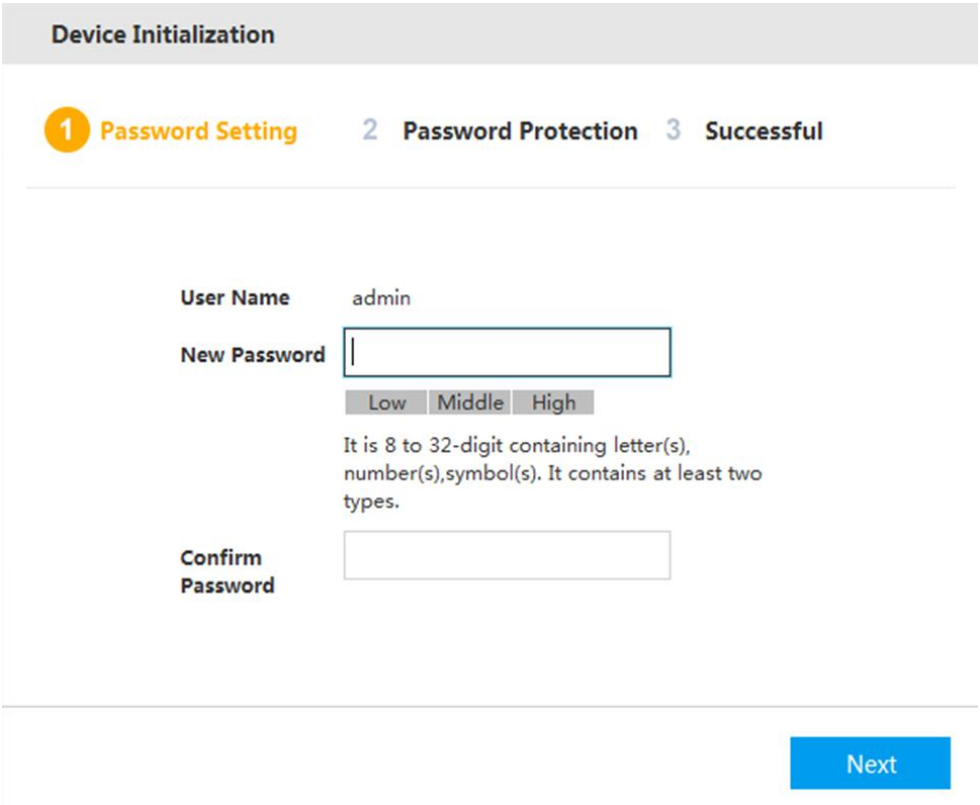


Install plugins only when logging in to the web for the first time.

Step 3 Click **Install**. Complete the installation as prompted.

The **Device Initialization** interface is displayed. See Figure 3-2.

Figure 3-2 Password setting



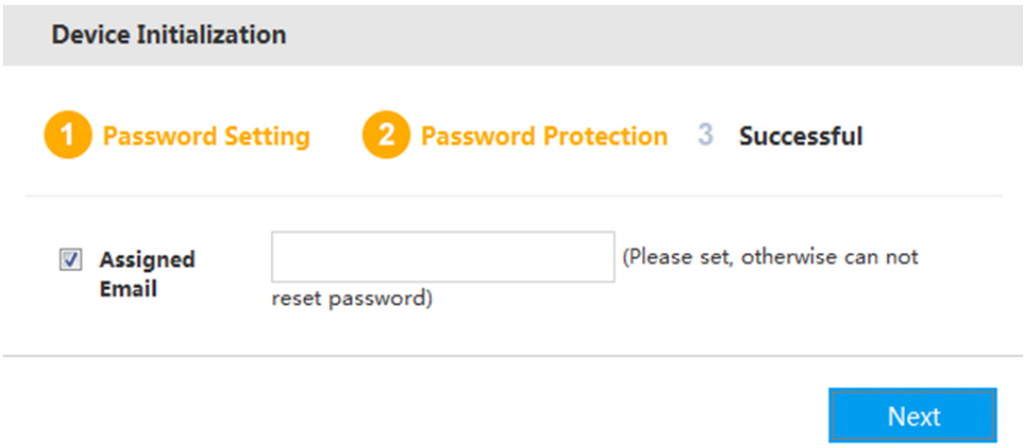
Step 4 In the **New Password** box, enter the new password.

The password consists of 8 to 32 characters. It combines letter(s), number(s) and symbol(s) (at least two of them). Set high security password based on the password strength tip.

Step 5 Click **Next**.

The **Password Protection** interface is displayed. See Figure 3-3.

Figure 3-3 Password protection



Step 6 In the **Assigned Email** box, enter the assigned email.

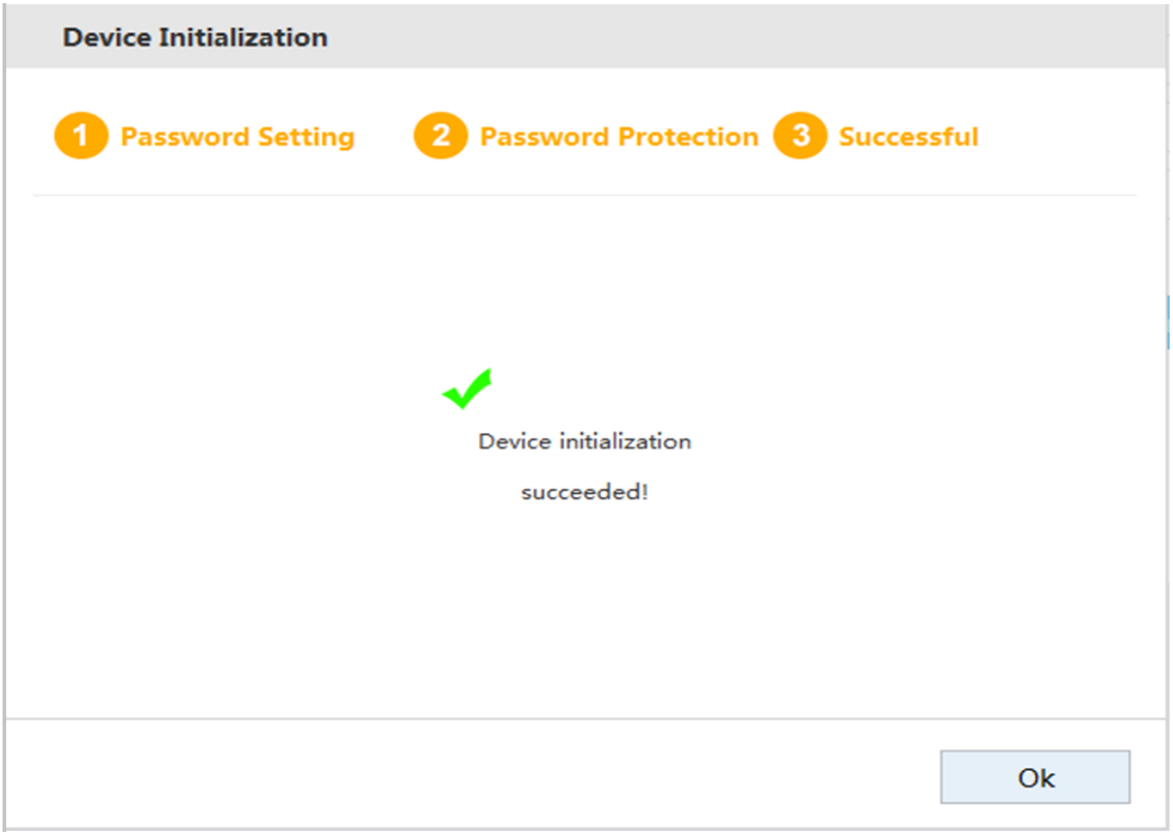
After entering the assigned email, you can reset the admin password through the email. For details, see "3.12.1.3 Resetting Password."

- If you do not need to set the password protection, you can clear the **Assigned Email** check box.
- If you have not entered the assigned email, you can enter **Setup > Account > User** to set it after the initialization is completed. For details, see "3.12.1.2 Modifying Password."

Step 7 Click **Next**.

The **Successful** interface is displayed. See Figure 3-4.

Figure 3-4 Device initialization succeeded



Step 8 Click **Ok** to complete the device initialization.

3.3 Logging in Web

You can access and manage the device remotely by logging in web through the browser.

Step 1 Open the browser, enter the IP address in the address bar, and then press Enter.

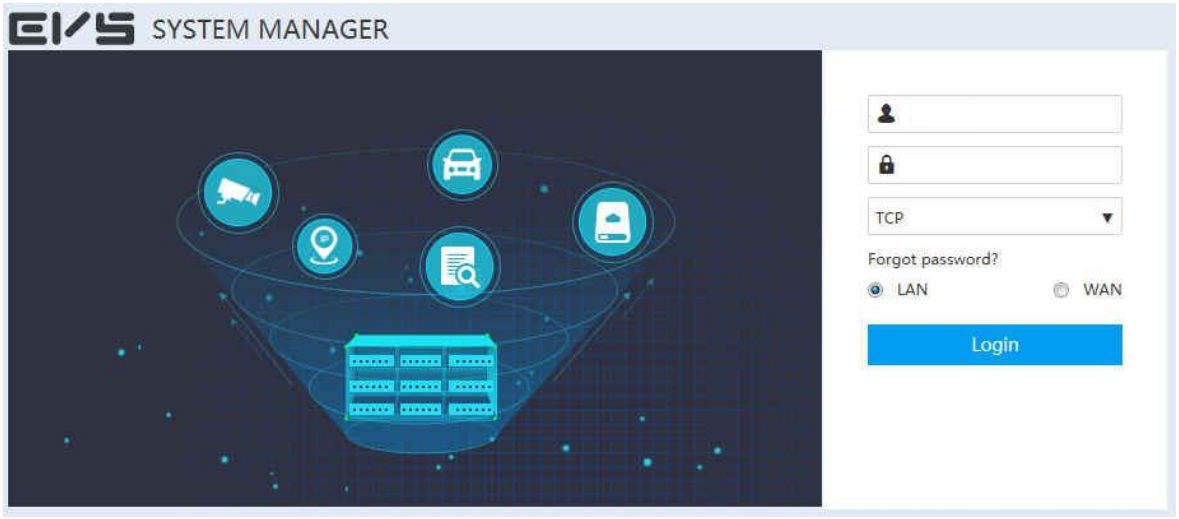
The **Control Installation** interface is displayed.

Step 2 Click Install.

The system downloads the control automatically. Click **Run** to install the control. The **Web login** interface is displayed after successful installation. See Figure 3-5.

- You need to install the control only when logging in for the first time.
- If the system does not allow to download the control, check whether any other plugins are installed which prohibit the download and reduce the security level of IE.

Figure 3-5 Web login interface



Step 3 Enter the user name and password, and then select the network connection type.

- The default user name of the administrator is admin, and the password is the one you set in device initialization. To ensure security, it is recommended that you change the password regularly and keep it properly.
- Connection types include TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and multicast.
- You can select Local Area Network (LAN) or Wide Area Network (WAN) to log in.
  - ◇ LAN: LAN login.
  - ◇ WAN: WAN login.

Step 4 Click **Login**.

The **SYSTEM MANAGER** interface is displayed. See Figure 3-6. For details, see Table 3-1.

Figure 3-6 System manager

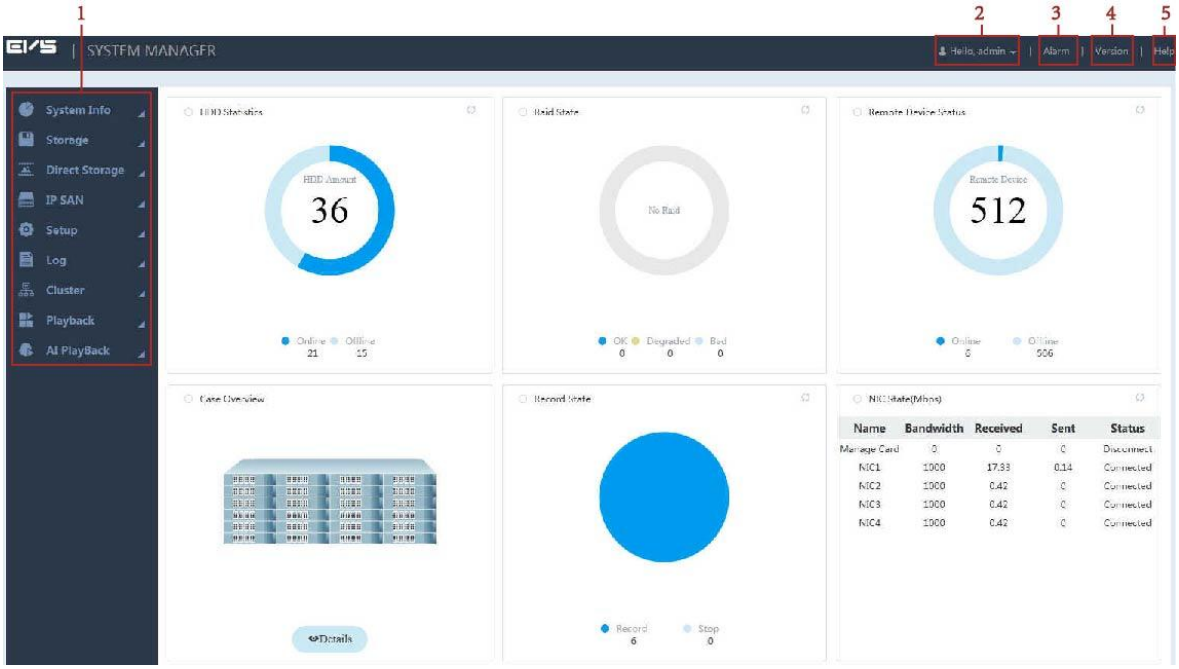


Table 3-1 System manager

No.	Name	Description
1	Function bar	You can view the basic system information, configure system parameters and play monitoring images and videos.
2	User name	Displays the current login user name. Click  at the right side of the user name and you can perform quickly set configuration and user logout. ● Quickly set: You can configure video, AI playback and IP SAN. ● Exit: Log out the current user.
3	Alarm	Click **Alarm** and you can search the alarm logs of the Device. For details, see "3.16.4 Alarm Log."
4	Version	Click **Version** and you can view the version information of the Device, including video channel, S/N, web, system version, security baseline version, Bios version and Onvif Client version.
5	Help	Click **Help** and you can get the User's Manual for the Device.

3.4 Initial Configuration

3.4.1 Setting IP

Set the Device information such as the IP address and DNS server according to the network plan.

Step 1 Select **Setup > TCP/IP > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 3-7 and Figure 3-8. For details, see Table 3-2.

Figure 3-7 Setting TCP/IP (single-control device)

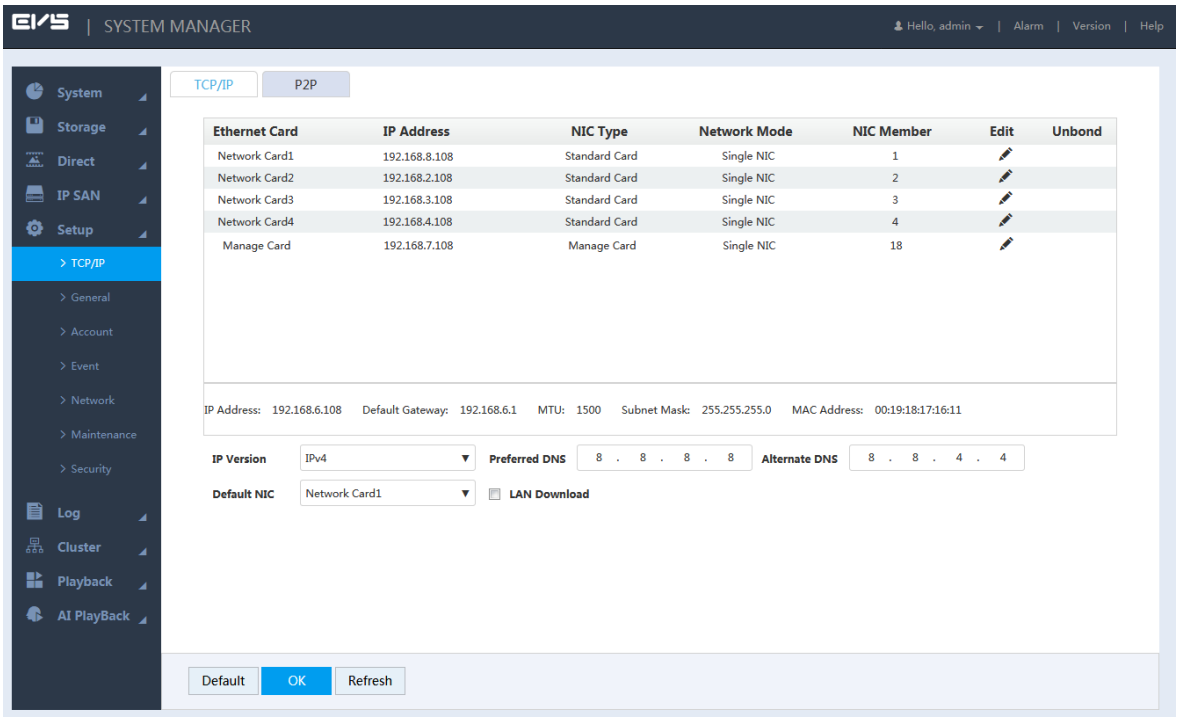


Figure 3-8 Setting TCP/IP (dual-control device)

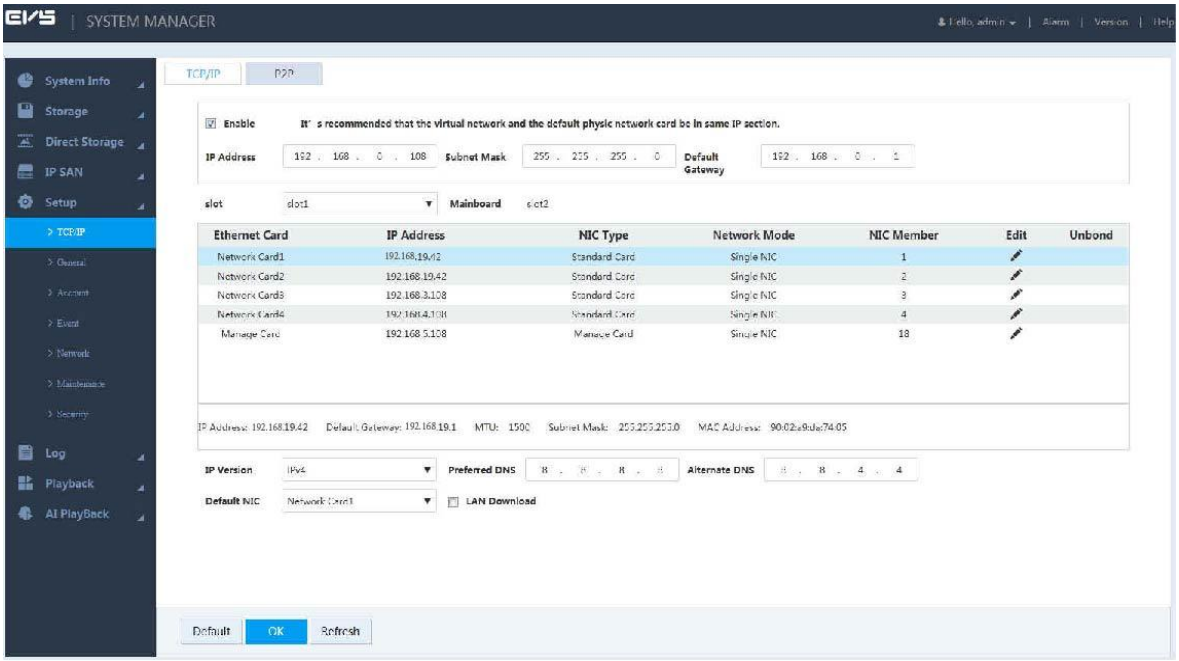


Table 3-2 TCP/IP setting parameters

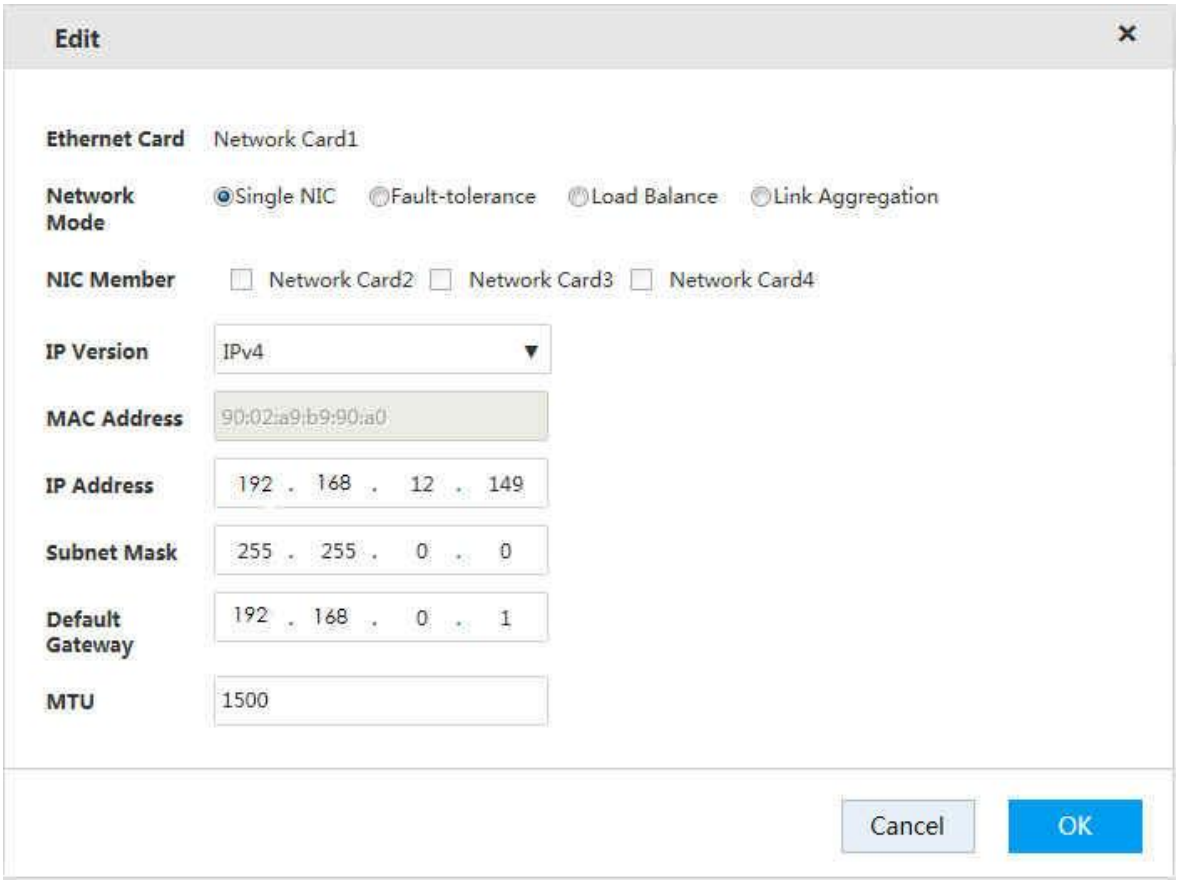
Parameter	Description
Enable	Enter the virtual IP address of the dual-control device. The main control board and sub control board of dual-control device have their respective physical IP. After setting the virtual IP, in spite of switching between the main and sub control boards, the user can always log in web normally with the virtual IP.
IP Address	
Subnet Mask	
Default Gateway	

Parameter	Description
Slot	Select the slot of the dual-control device. The corresponding NIC information is displayed in the list. Only dual-control device supports this function.
IP Version	Select the IP version, including IPv4 and IPv6 formats.
Preferred DNS	Enter the IP address of preferred DNS server.
Alternate DNS	Enter the IP address of alternate DNS server.
Default NIC	Select the default NIC of the Device.
LAN Download	Select the check box. If network bandwidth allows, the LAN download speed is 1.5–2 times of the normal download speed.

Step 2 Click .

The **Edit** interface is displayed. See Figure 3-9.

Figure 3-9 Editing



Step 3 Configure the parameters. For details, see Table 3-3.

Table 3-3 NIC editing parameters

Parameter	Description
Ethernet Card	Displays the current NIC name.

Parameter	Description
Network Mode	Displays the network mode of the Device. ● Single NIC: The NIC is used alone. You can select one NIC to provide HTTP or RTSP service. You need to set one default NIC (default is Network Card1) to request the network service started by Email and File Transfer Protocol (FTP). Once the card is offline, the system triggers a disconnection alarm. ● Fault-tolerance: In this mode, the Device communicates with external devices through NIC bonding. You can focus on one host IP address. At the same time, you need to set one master card. Usually there is only one running card (master card).The system will enable the alternate card when the master card malfunctions. The system will not be offline only if all cards are offline. Notice that all cards need to be in the same LAN. ● Load balance: In this mode, the Device communicates with external devices through NIC bonding. Workload is balanced among all cards. Their network loads are generally the same. The system will not be offline only if all cards are offline. Notice that all cards need to be in the same LAN. ● Link aggregation: The system uses NIC bonding to realize communication function. All bonded NICs are working together and bearing the network load. The system allocates the corresponding ports to the specified switches according to the port load setting. Once one port link malfunctions, the system stops sending out data from current port. The system can calculate the new load and specify the new port(s) to send out data. The system calculates again to specify the port(s) once the malfunction port becomes available.  ● The Device only supports LACP link aggregation. ● The Link Aggregation network mode is available when the switch supports link aggregation and is configured with link aggregation.
NIC	When the **Network Mode** is set as **Single NIC**, you can bond the current NIC to any other one.  Management NIC does not support this function.
IP Version	You can select IPv4 or IPv6 Format. Currently both IP addresses are supported.
MAC Address	Displays the MAC address of the Device.
IP Address	Set the IP address, subnet mask and default gateway of the Device according to the actual network planning.
Subnet Mask	
Default Gateway	

Parameter	Description
MTU	Enter the MTU (Maximum Transmission Unit) value of the NIC. The default value is 1,500 bytes. The suggested value is 1,500 or 1,492. ● 1,500: The maximum and default value of the Ethernet packet. It is a typical network connection setting without PPPoE and VPN. It is the default setting of some routers, network adapters and switches. ● 1,492: Optimum value of PPPoE.  ● Modifying MTU will lead to NIC restart and network interruption. This will affect the running operations. Operate with care. ● It is recommended to view the MTU value of the gateway first, and set the MTU value of the Device to be the same or slightly smaller than that of the gateway. This will reduce sub package and improve network transmission efficiency.

Step 4 Click **OK** to save the configuration.

3.4.2 Adding Remote Device

After adding the remote device, the Device can receive, store, and manage the video stream transmitted by the remote device. You can browse, playback, manage, and store several remote devices.

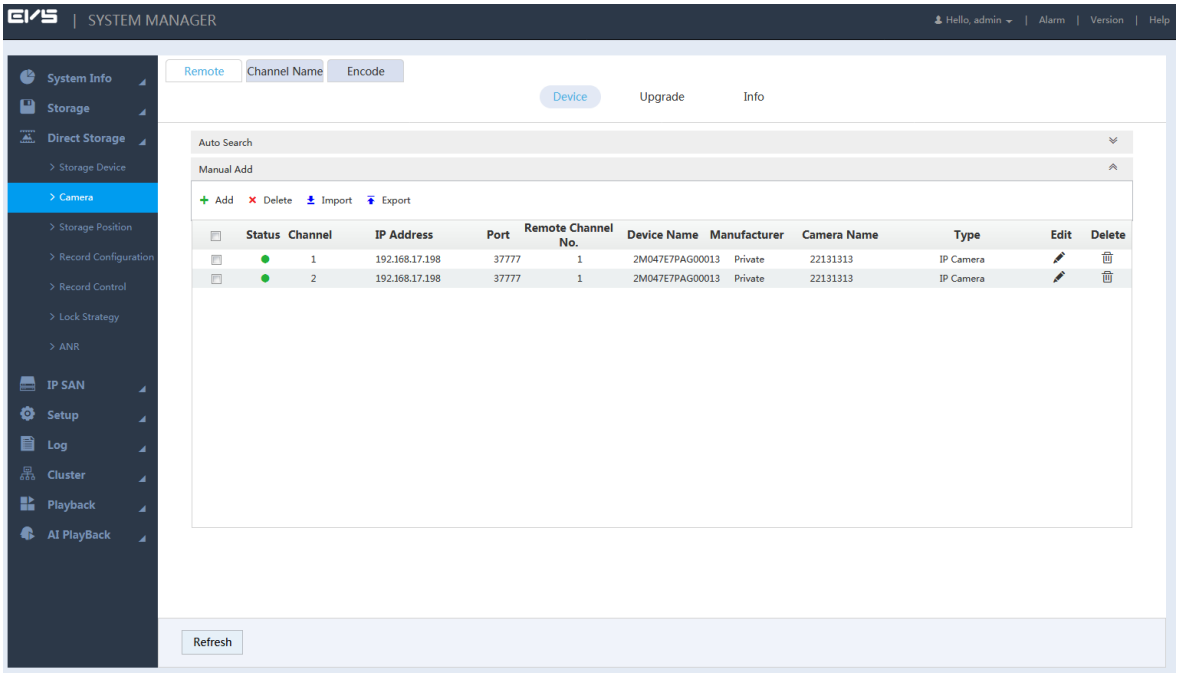
The system supports adding remote devices in three ways: adding by search, adding one device, batch add and importing from template.

- Adding by search: You can search for the remote devices in the same LAN and select the ones you want to add. If you are not clear about the IP address of the device you need to add, this method is recommended.
- Adding one device: Add a few remote devices. In this way, you need to know the IP address, user name and password of the device.
- Batch add: When the first three sections of the remote device IP addresses are the same (e.g. 192.168.1.1–192.168.1.255), and the user name and password of the devices are also the same, this method is recommended.
- Importing from template: Import remote devices in batch through the template file.

Step 1 Select **Direct Storage > Camera > Remote > Device**.

The **Device** interface is displayed. See Figure 3-10.

Figure 3-10 Remote device



Step 2 Add remote device.

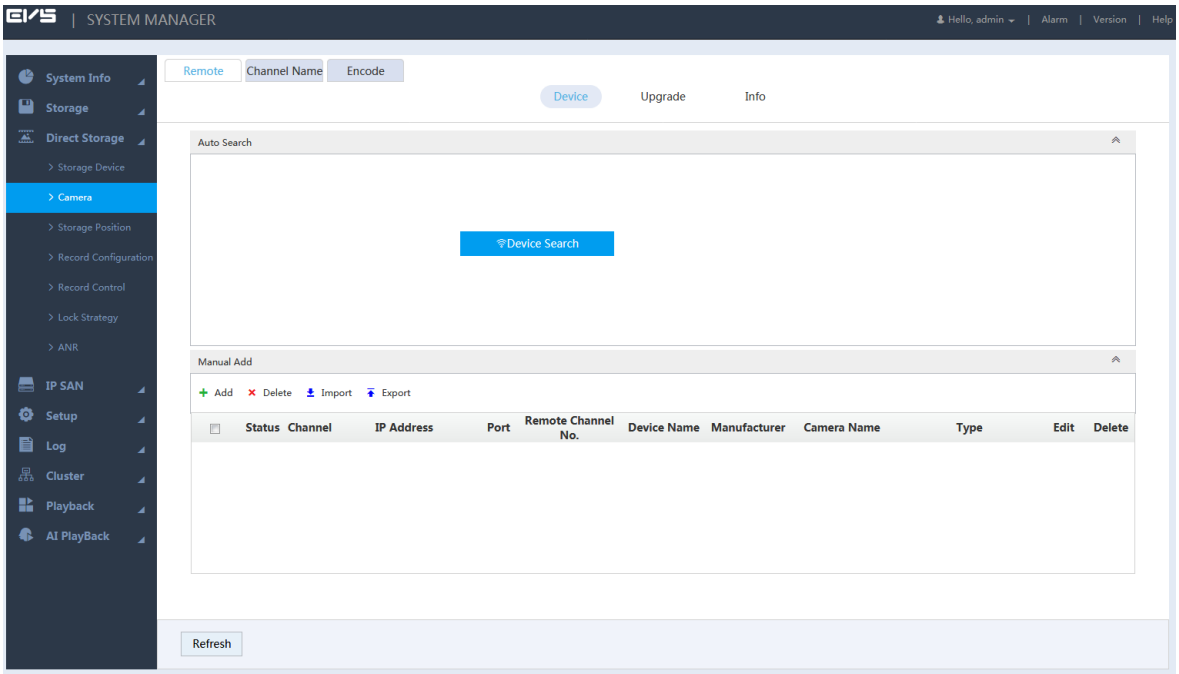
You can use adding by search, adding one device, batch add or importing from template.

- Adding by search

1) Click  at the right side of **Auto Search**.

The **Auto Search** interface is displayed. See Figure 3-11.

Figure 3-11 Automatic search



2) Click **Device Search**.

The results are displayed. See Figure 3-12. For details, see Table 3-4.

When the obtained IP address and port number is the same as that of the remote device you have already added, this device will not appear in the result list.

Figure 3-12 Search results

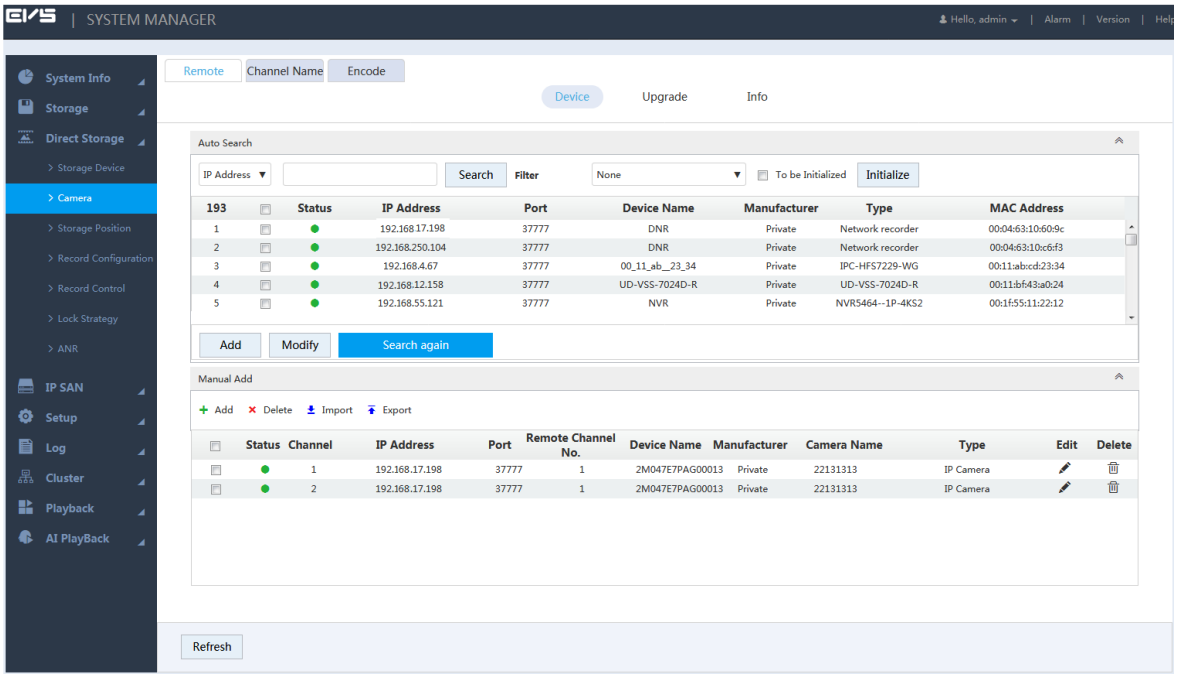


Table 3-4 Auto search icons

Icon/Parameter	Description
IP Address ▼	Select the remote devices you need to add through IP address or MAC address. 1. Click IP Address ▼ to select IP Address or MAC Address. 2. Enter the IP address or MAC address of the remote device in the text box at the right side of IP Address ▼. 3. Click **Search**. The results are displayed.
Initialization	Select the **To Be Initialized** check box and click **Initialize**, you can modify the login password and IP address.
Filter	Set filter conditions according to device model. The system only displays the remote device information that meets the filter conditions. This facilitates users to search for devices they need to add.
Modify	Select the check box of the corresponding remote device and click **Modify** to change the IP address of the device. ● The IP address of the remote device can be modified only when the **Manufacturer** is **Private**. ● You can only modify one IP address at a time.
Search again	Click this icon to search the remote devices again.

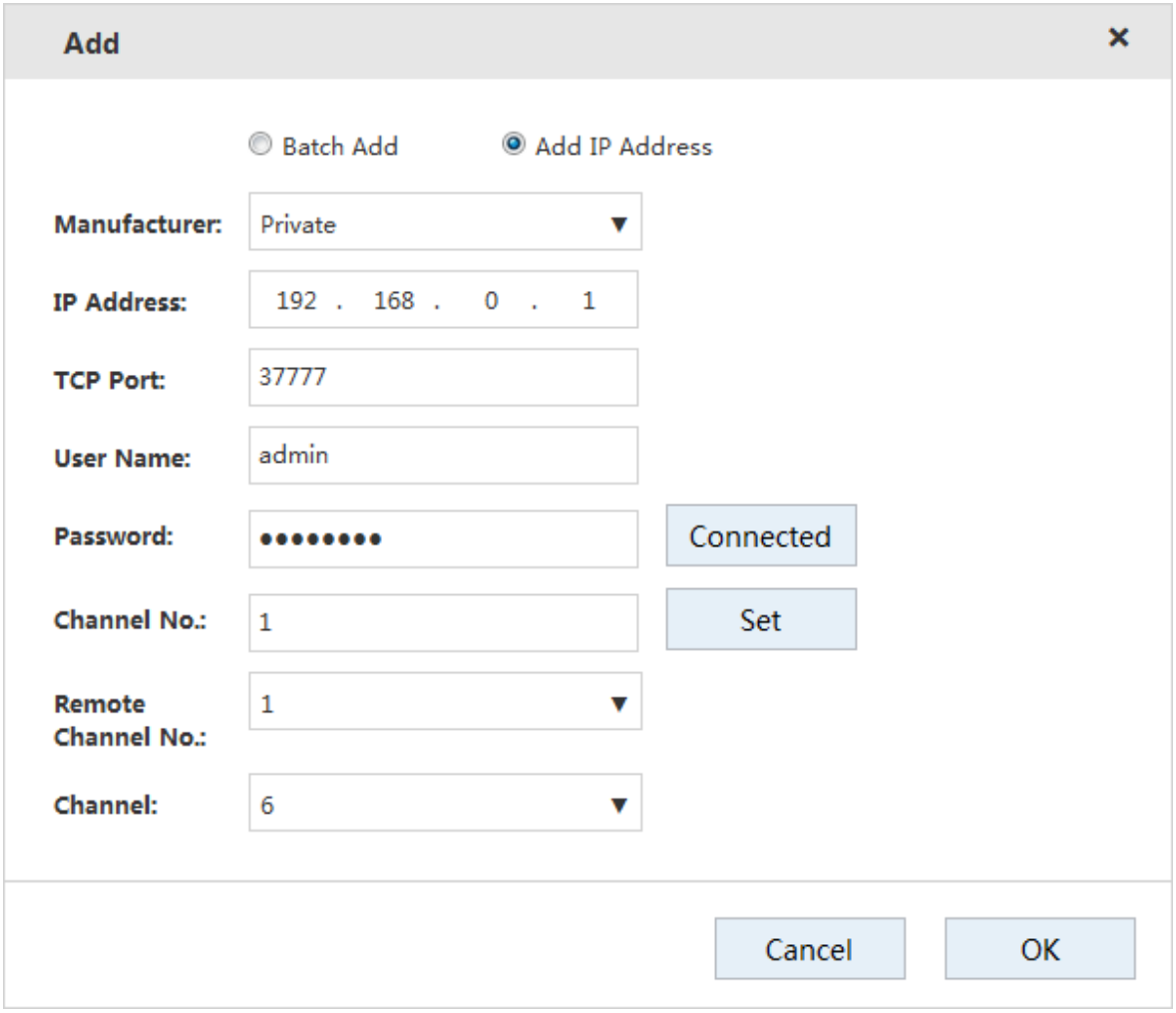
3) Double-click the remote device, or select the check box of the corresponding device and click **Add**, the system adds this remote device to the added list.

- Single add

1) Click + in the **Manual Add** area and select **Add IP Address**.

The **Add** interface is displayed. See Figure 3-13.

Figure 3-13 Adding one device



2) Configure the parameters. For details, see Table 3-5.

Table 3-5 Adding device

Parameter	Description
Manufacturer	Select the manufacturer in the drop-down box according to the actual situation. Different models support different manufacturer protocols. You need to refer to the actual situation.
IP Address	Set the IP address of the remote device.
TCP Port	Provides services with TCP protocol. You can set the port according to actual needs. The default is 37777. You need to set it when the **Manufacturer** is set as **Private**.

Parameter	Description
RTSP Port	Set the RTSP port No. of the remote device. The default is 554.  You do not need to configure it when the **Manufacturer** is set as **Private** or **Custom**.
HTTP Port	Set the HTTP port of the remote device. The default is 80.  You do not need to configure it when the **Manufacturer** is set as **Private** or **Custom**.
HTTPS Port	HTTPS communication port. It can be set according to your actual needs. The default is 443.  This function requires the remote device to be connected through Onvif. Select encryption.
User Name/Password	Enter the user name and password to log in the remote device.
Channel No.	Enter the **Channel No.** or click **Connect** to get the total channel number of the front-end device.  It is recommended to obtain the channel number of the front-end device by clicking **Connect**. If the total number of channels entered does not conform to the channel number of the front-end device, it might cause adding failure.
Remote Channel No.	After getting the remote channel number, click **Set** to get the number of the channel needed to connect.
Channel	The channel number of the remote device in the local device. Configure the remote device in the corresponding channel of the local device. For example, configure the channel name and it corresponds to this channel number.
Encryption	When the remote device is connected via Onvif, select encryption. The system will encrypt and protect the transmitted data.  This function requires the front-end IPC to open the HTTPS port.

Parameter	Description
Connection Mode	Automatic, TCP and UDP are available. For Onvif device, also includes MULTICAST. ● When the remote device is connected through private protocol, the default connection mode is TCP. ● When the device is connected through Onvif, four connection modes are available: automatic, TCP, UDP and MULTICAST. ● When the device is connected through other vendor protocols, TCP and UDP are supported.

3) Click **OK** to complete adding.

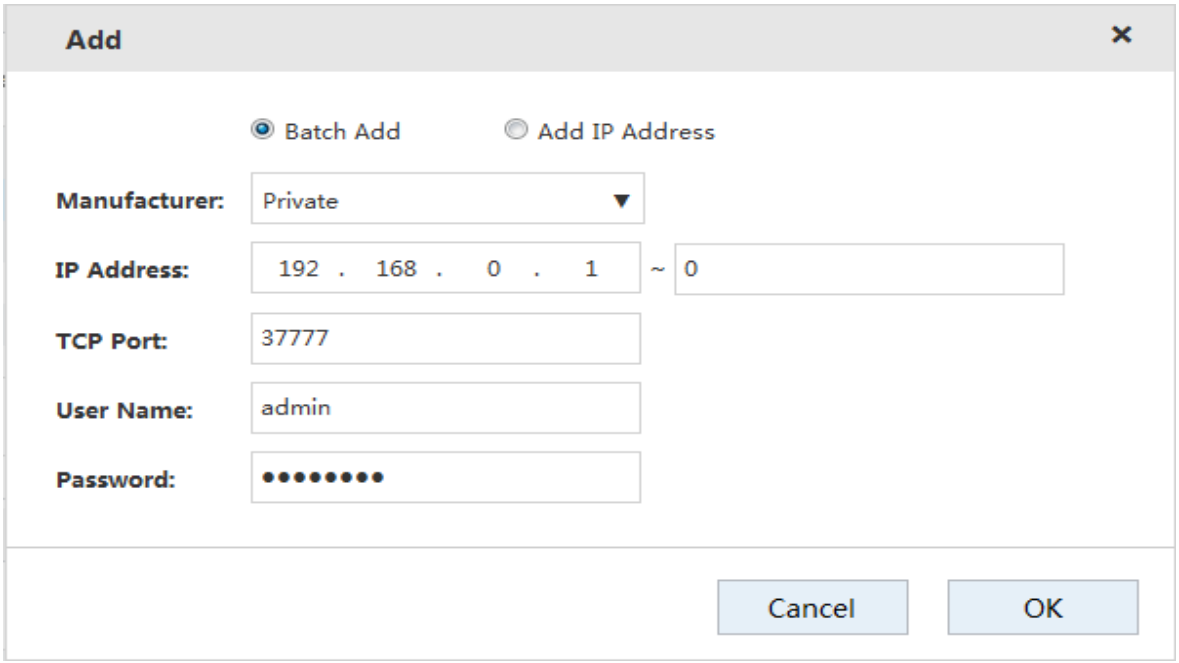
- Batch add

Batch add only supports adding remote devices in the same network segment.

1) Click + in the **Manual Add** area and select **Batch Add**.

The **Add** interface is displayed. See Figure 3-14.

Figure 3-14 Batch add



2) Enter the search range for the fourth segment of the IP address.

Batch add only supports devices with the first three segments of the IP address are the same. You need to enter the search range of the fourth segment. For example: 192.168.1.1–192.168.1.255.

3) Set other parameters. For details, see Table 3-5.
4) Click **OK** to complete adding.

- Importing from template

1) Click ↑ to select storage path. Click **Save** to export the template file.

◇ The default name of template file is *RemoteConfig_20181017_Eng.csv* or *RemoteConfig_20181017_Eng.backup.* "*.csv*" refers to non-encrypted file, "*.backup*" refers to encrypted file, and "*20181017*" refers to the date of exporting the file.

◇ Template files in different languages cannot be imported into each other.

2) According to actual situation, enter information of the remote device in the template file and save it.

Do not change the extension of the template file. Otherwise, the import will fail.

3) Click to select the template file.

4) Click **Open** to add the remote device.

After adding, if the **Status** turns , then the connection is successful. If it turns , the connection fails. Check the reason.

3.4.3 Record Setting Strategy

You can set record plan and snapshot plan. Records of different channels, dates and time periods can be acquired. You can configure key frames and live key frames to reduce the space usage of the record.

3.4.3.1 Configuring Record Plan

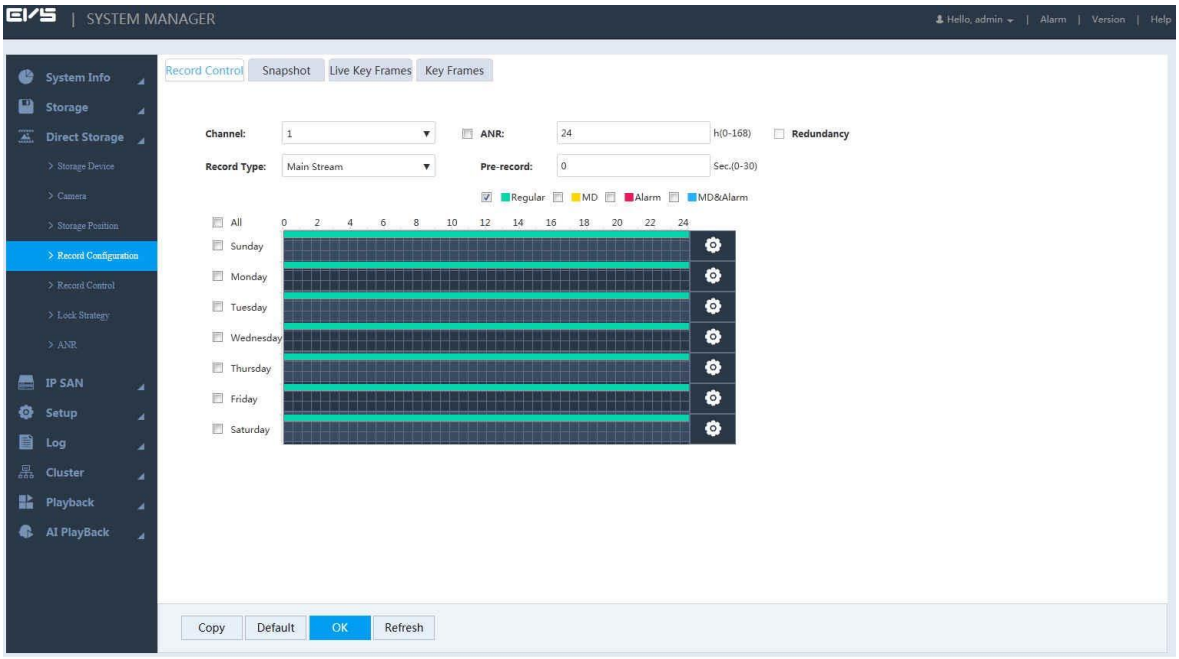
The system performs video recording according to record plan. For example, when you set the time period of alarm videos to 6:00–18:00, the system automatically takes records if any alarm occurs during this period.

The factory default plan is 24-hour continuous ordinary record for all the channels. You can modify it according to the actual needs.

Step 1 Select **Direct Storage > Record Configuration > Record Control**.

The **Record Control** interface is displayed. See Figure 3-15.

Figure 3-15 Record plan



Step 2 Configure the parameters. For details, see Table 3-6.

Table 3-6 Record parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.
ANR (Automatic Network Replenishment)	Select the check box to enable the function. ● When the Device and IPC is disconnected, IPC keeps on recording. After the network recovery, the Device downloads the records during the disconnection period from IPC, so as to keep the record integrity. ● Enter the max record upload time period in the text box. If the time of network outage is longer than the set period, the system only uploads the records during the set time period. This function requires IPC to be installed with SD card.

Parameter	Description
Redundancy	When multiple disks are available in the Device, select one disk to be the redundancy to realize secondary backup of records. The records are stored in different disks at the same time to guarantee data security. 1. Set a redundant disk. 2. Select the check box to enable redundancy. ◇ If the selected channel is not recording a video, redundancy works from the next time. ◇ If the selected channel is recording a video, all the current record files will be packed and the new strategy (redundancy or not) will be executed to store the record. The recording in the redundant disk corresponds to a backup of recording in the read-write disk. Images are not backed up.
Record Type	Select the record type, including main stream and sub stream.
Pre-record	Start to record 0–30 seconds (according to the stream size and status) before the preset action.

Step 3 Select the alarm type. See Figure 3-16.

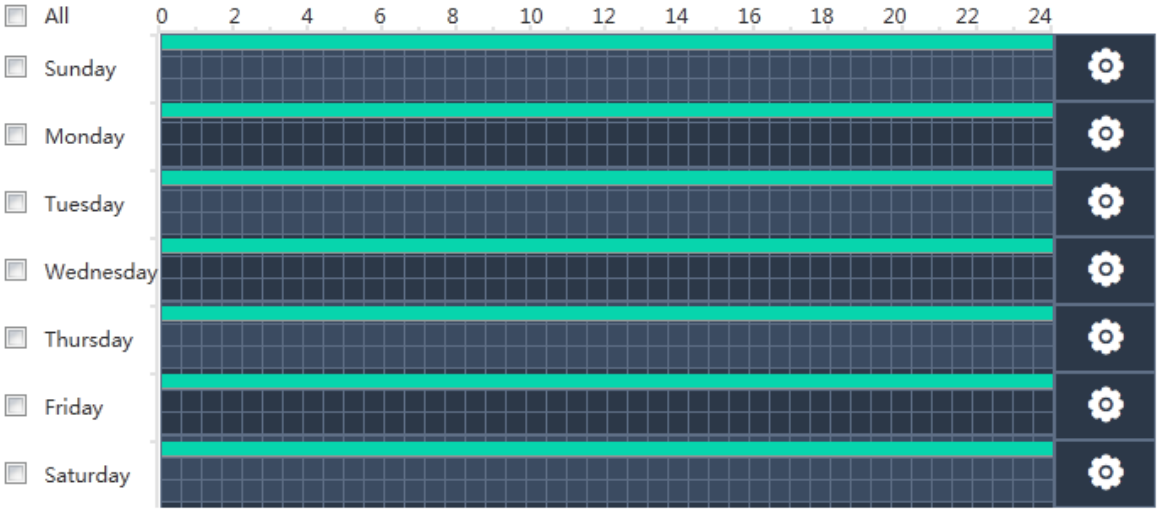
Figure 3-16 Alarm type

- When you select the **MD**, **Alarm** or **MD & Alarm**, you need to enable the alarm record linkage for the corresponding channel.
- The color bar in Figure 3-17 indicates the record type of the corresponding time period.

Step 4 Set the record plan period. It includes drawing and editing.

After adding holidays, you can also set holiday record plan.

Figure 3-17 Time period setting



- Drawing:

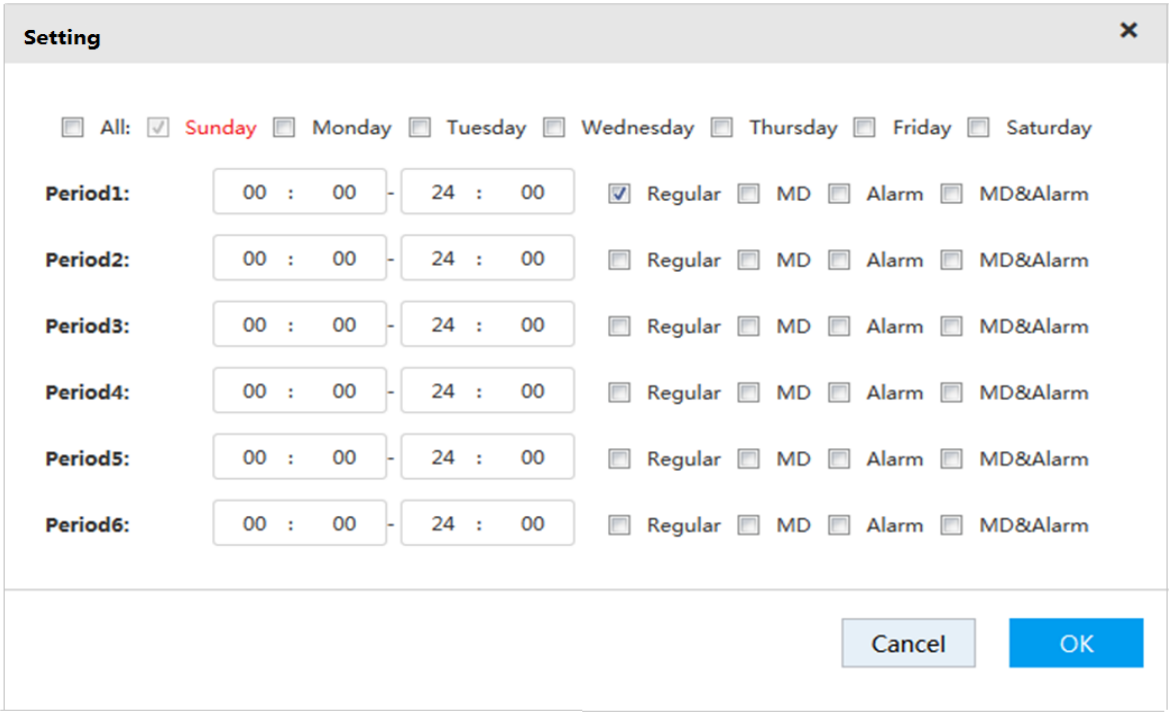
1) Select the weekday.
   - ◇ Select the **All** check box and you can synchronously edit or draw the periods for all the weekdays.
   - ◇ You can select multiple weekdays to edit at the same time.
2) Hold the left button of the mouse and move the mouse in the period bar to draw the period.
   - ◇ You can set six periods for each day. The Device performs recording in the corresponding period.
   - ◇ When the record time is overlapped, see the following record priority: MD & alarm > alarm > MD > regular.

- Editing:

1) Select the corresponding weekday and click  .

   The **Setting** interface is displayed. See Figure 3-18.

Figure 3-18 Period setting



2) Select the weekday, record type and period.
3) Click **OK** to save the configuration.

   The system returns to the **Record Control** interface.

Step 5 Click **OK** to save the configuration.

The record plan works after the auto record function is enabled. For details of enabling auto record, see "3.4.4 Enabling Record Function."

3.4.3.2 Setting Snapshot Plan

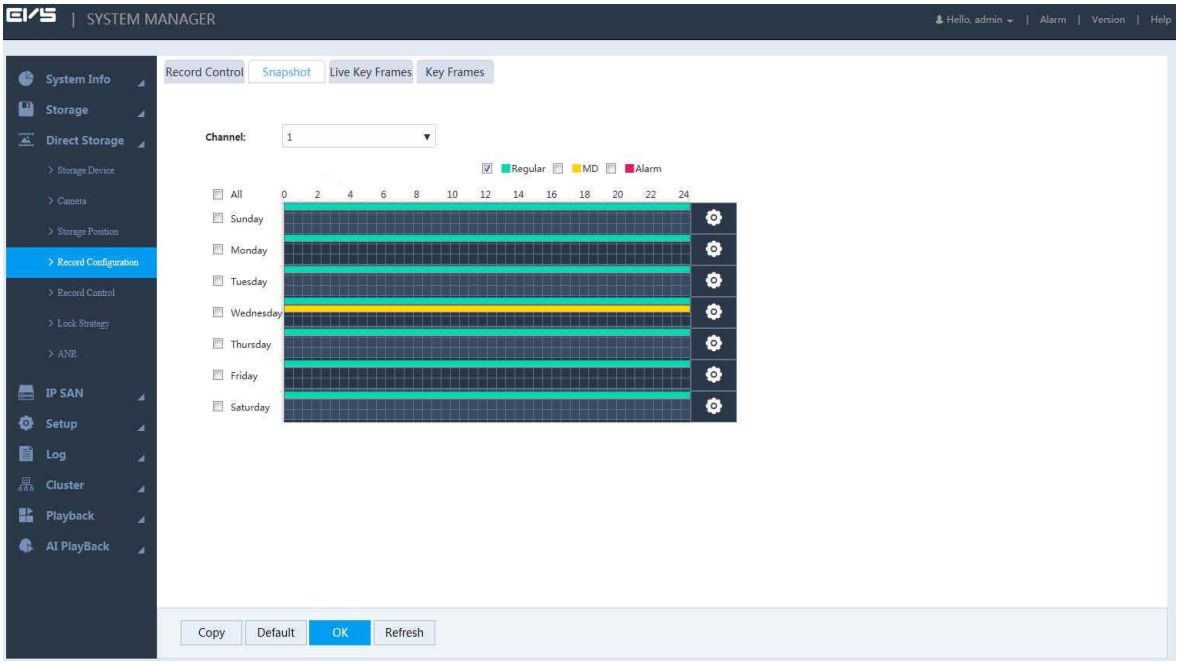
With snapshot plan, the system captures images according to the set time and type. For example, if you set the capture time of Emergency type at 6:00–18:00 of each Monday, the system will automatically capture images of Emergency and of this time period.

Select **Direct Storage > Record Configuration > Snapshot**.

The **Snapshot** interface is displayed. See Figure 3-19.

The way of setting snapshot plan is the same with record plan setting. For setting snapshot plan, see details in "3.4.3.1 Record Plan Settings."

Figure 3-19 Snapshot plan



The snapshot plan works after enabling the auto snapshot function. For details of enabling auto snapshot, see "3.4.4 Enabling Record Function."

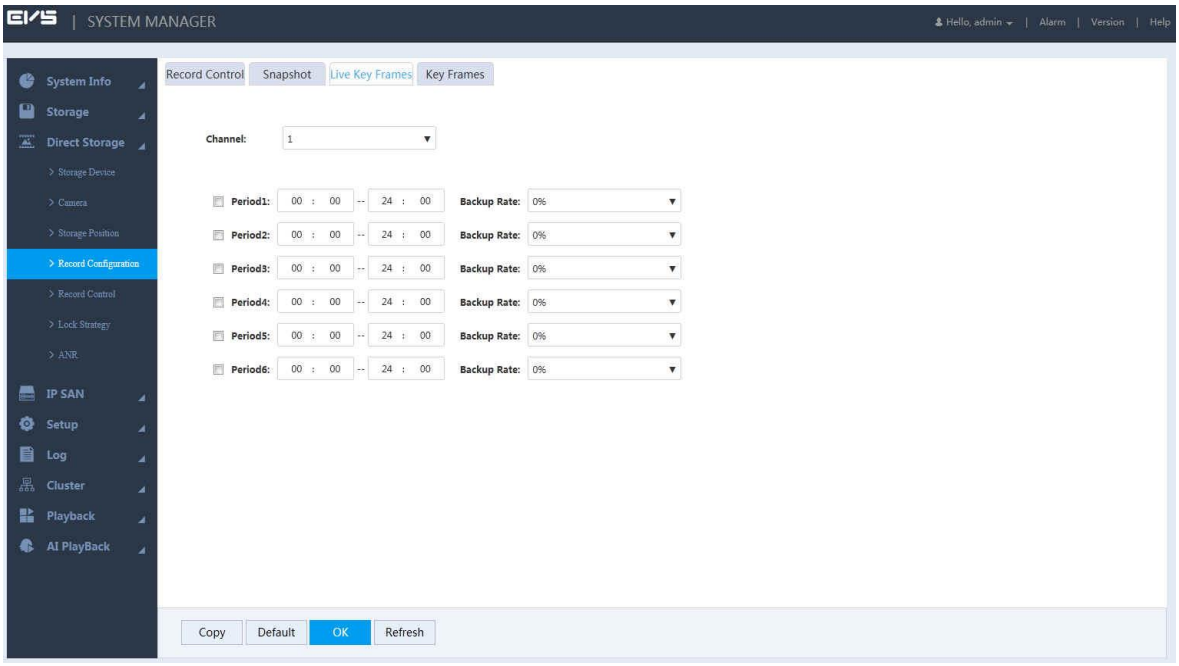
3.4.3.3 Setting Live Key Frame

You can set period and backup rate of a channel. Based on the settings, the system will delete non-key frames in part or in whole when storing the record. This helps save the space usage of record.

Step 1 Select **Direct Storage > Record Configuration > Live Key Frames**.

The **Live Key Frames** interface is displayed. See Figure 3-20.

Figure 3-20 Live key frames



Step 2 Configure the parameters. For details, see Table 3-6.

Table 3-7 Live key frame parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.
Period	Select the time period of live key frame. The system supports setting 6 periods at most.
Backup Rate	Select the backup rate of each period. Backup rate refers to the retention rate of non-key frames. For example, 0% backup rate means only key frames are retained, and all the non-key frames are deleted; 100% means all frames are retained.

3.4.3.4 Setting Key Frame

If storage is limited and a relatively long record is required, you can delete the non-key frames of the saved record through key frame settings. In this way, only key frames will be saved, and more storage will be available. But this will influence record fluency and continuity.

- With key frame settings, part of the record data may be discarded, leaving only the configured key frame data.
- Be cautious with setting key frames, as this operation may influence record fluency and continuity.

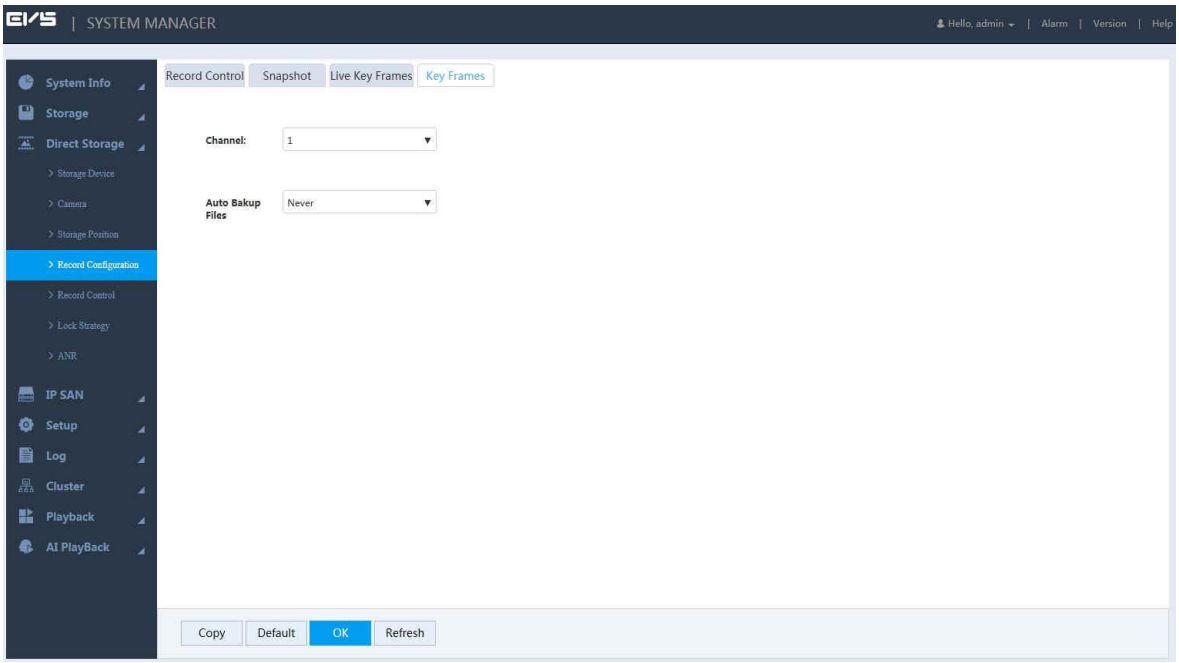
Preparation

Setting key frame requires a separate disk to store the record after the non-key frames are deleted. The original record in this disk will be deleted. For details of setting key frame, see "3.13.2.1 Setting Disk Attribute."

Step 1 Select **Direct Storage > Record Configuration > Key Frames**.

The **Key Frames** interface is displayed. See Figure 3-15.

Figure 3-21 Key frames



Step 2 Configure the parameters. For details, see Table 3-6.

Table 3-8 Key frame parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.
Auto Backup Files	Select the way of backing up files. ● Never: Never delete non-key frames of record files. ● Customized: you can select to delete non-key frames of record files 3–30 days ago. After deletion, store the record file in the disk.

Step 3 Click **OK** to save the configuration.

3.4.4 Enabling Record Function

After setting record and snapshot plans, you need to enable auto record and auto snapshot functions so that the system can perform operations automatically.

Record includes auto record and manual record. You can select different record modes for the main stream and the sub stream.

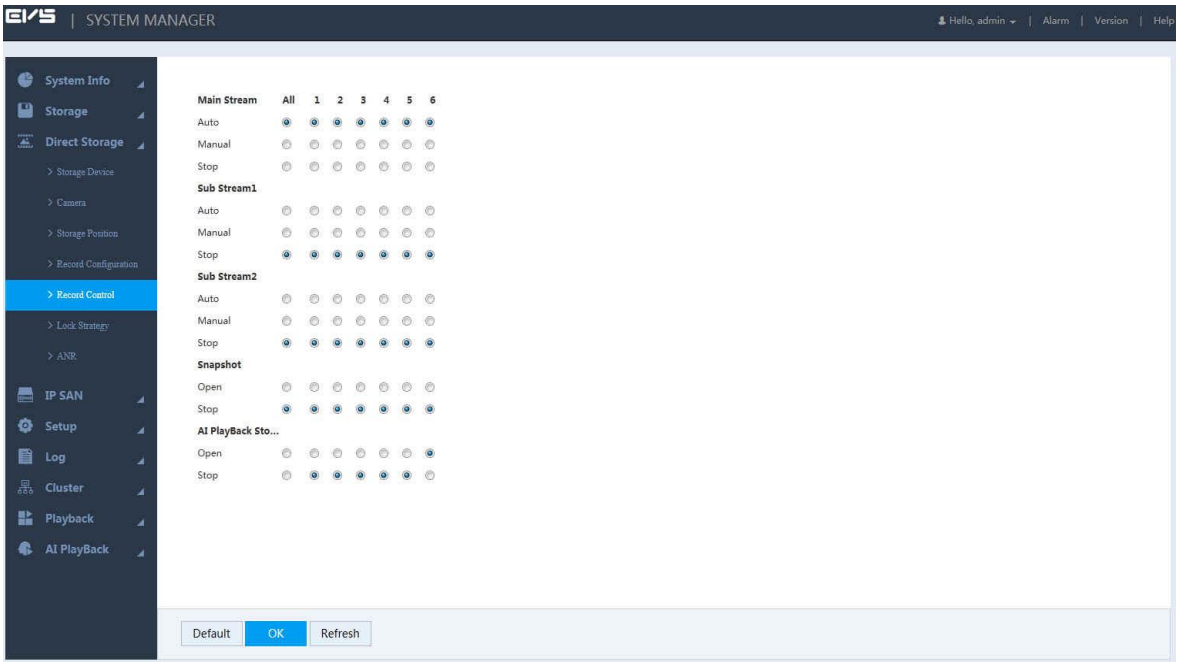
- Auto record: The system automatically takes records according to the set record type and record time.
- Manual record: The system takes 24-hour continuous records in the channel.

Manual record requires the user to have the storage setting authority.

Step 1 Select **Direct Storage > Record Control**.

The **Record Control** interface is displayed. See Figure 3-22.

Figure 3-22 Record control



Step 2 Configure the parameters. For details, see Table 3-9.

Table 3-9 Record control parameters

Parameter	Description
Channel	Displays all the channels with remote devices added. You can select a single channel or multiple channels or select **All** for all the channels.
Status	Displays the current status of the corresponding channel. ● : Not selected. ● : Selected.
Main Stream Sub Stream	Select the record mode of the main stream and sub streams, including manual, auto and stop. ● Manual: Highest priority. In spite of the current channel status, all the channels start regular recording after enabling **Manual**. ● Auto: Making records according to the set record plan (regular, MD and alarm). For details, see "3.4.3.1 Configuring Record Plan." ● Stop: All the channels stop recording.
Snapshot	Select single or multiple channel(s) and open/close the snapshot of the corresponding channel.
AI Playback Storage	Select single or multiple channel(s) and open/close AI playback of the corresponding channel.

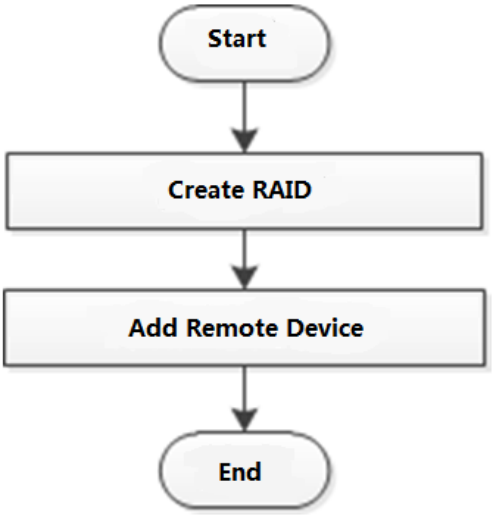
Step 3 Click **OK** to save the configuration.

3.5 Video Direct Storage

Video direct storage refers to storing the video stream transmitted by IPC into the Device directly. There is no need for excessive forwarding. This helps reduce the operating pressure of the management server.

For the procedure to configure video direct storage, see Figure 3-23.

Figure 3-23 Video direct storage

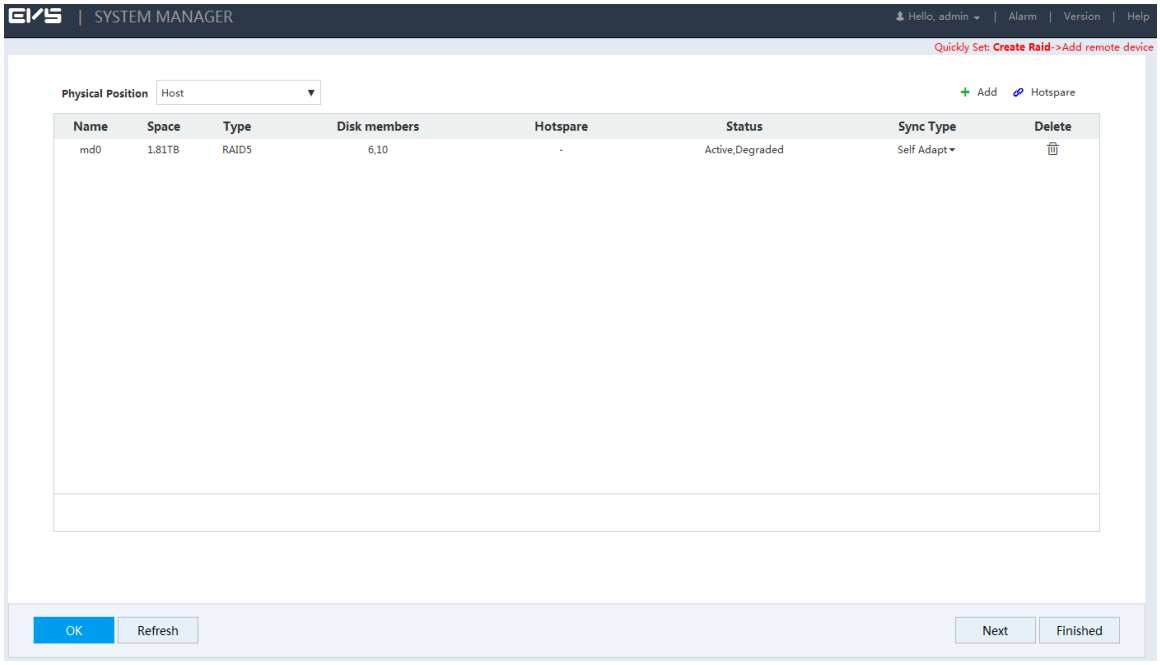


Step 1 Click  at the right side of the user name. Select **Quickly Set > Video**.

The **Create Raid** interface is displayed. See Figure 3-24.

The steps to quick configure the video direct storage scenario are displayed at the top right of the screen.

Figure 3-24 RAID management

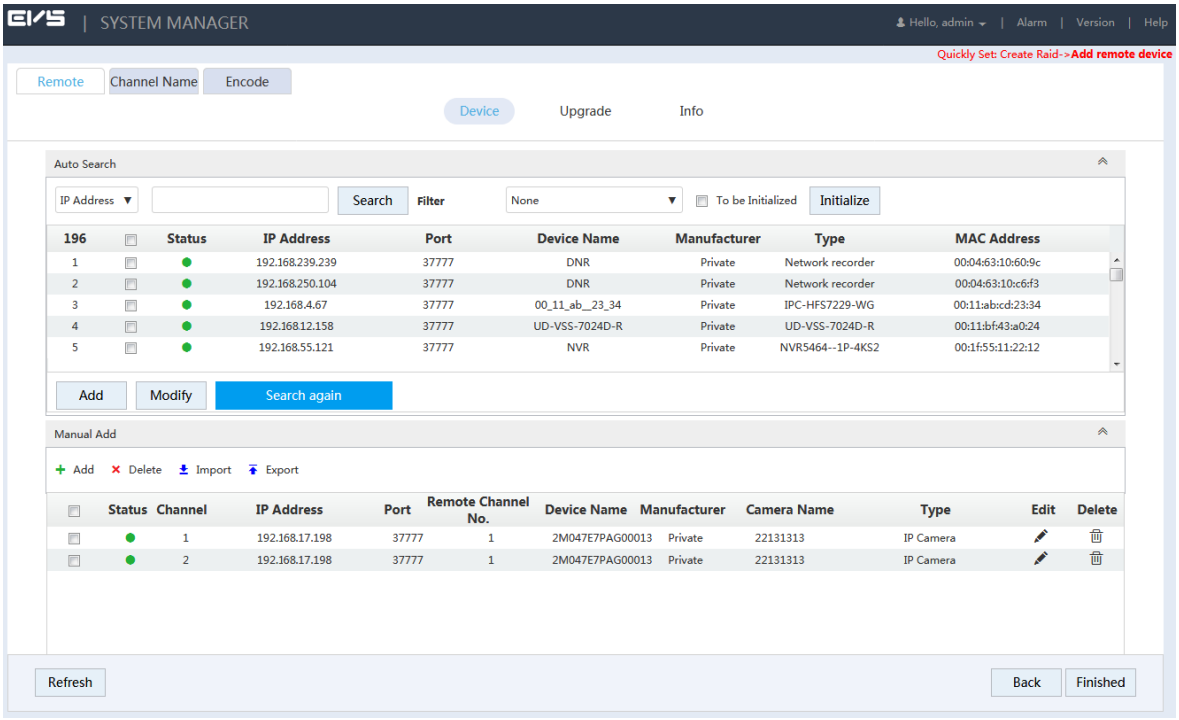


Step 2 Create RAID. For details, see "3.13.5.1 Creating RAID."

Step 3 Click **Next**.

The **Add remote device** interface is displayed. See Figure 3-25.

Figure 3-25 Adding remote device



Step 4 Add remote device. For details, see "3.4.2 Adding Remote Device."

Step 5 Click **Finished** to save the configuration.

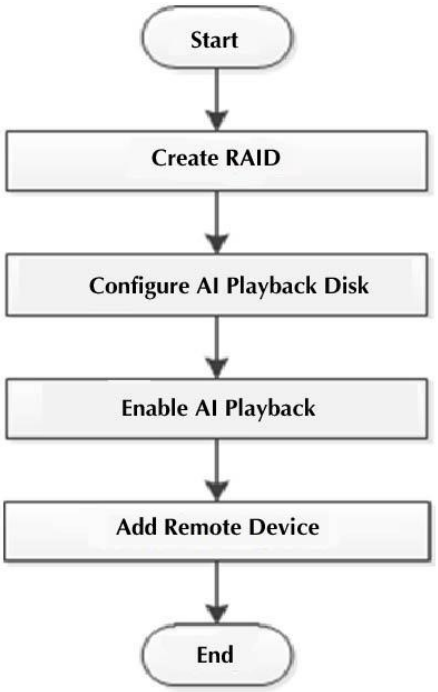
3.6 AI Playback

AI playback is an intelligent function for you to check and play back the results of IVS analyse, vehicle analyse, face detect and human trait.

3.6.1 Configuring AI Playback

For the procedure to configure AI playback, see Figure 3-26.

Figure 3-26 AI playback

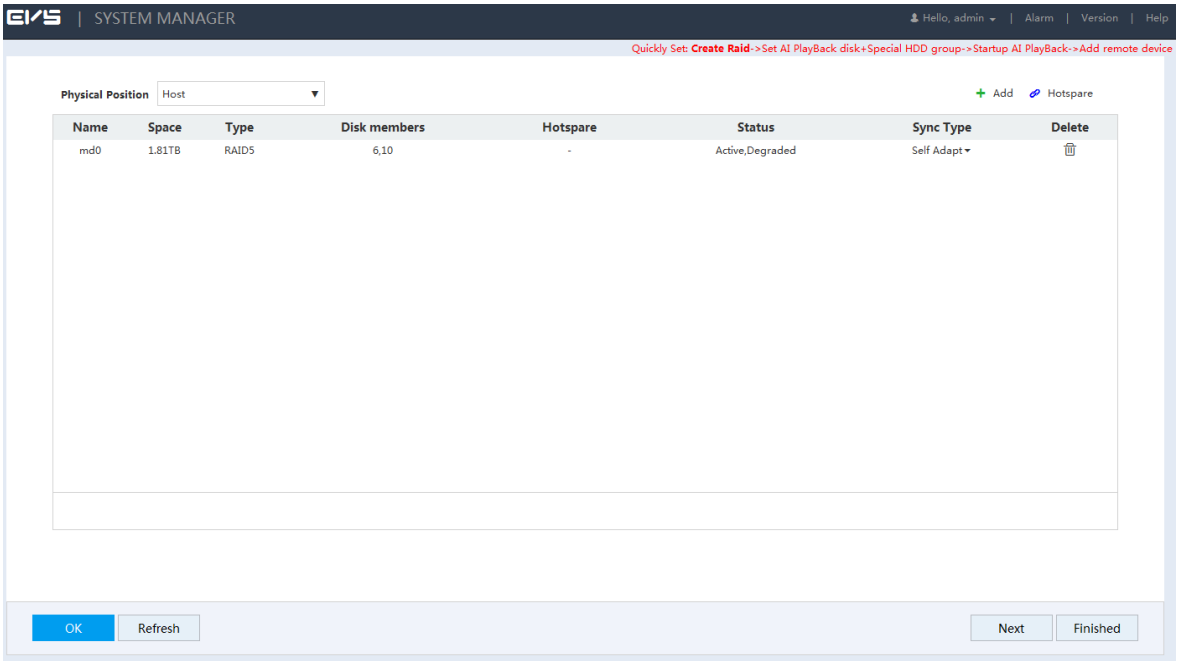


Step 1 Click  at the right side of the user name. Select **Quickly Set > AI PlayBack**.

The **Create Raid** interface is displayed. See Figure 3-27.

The steps to quick configure the AI playback scenario are displayed at the top right of the screen.

Figure 3-27 RAID management

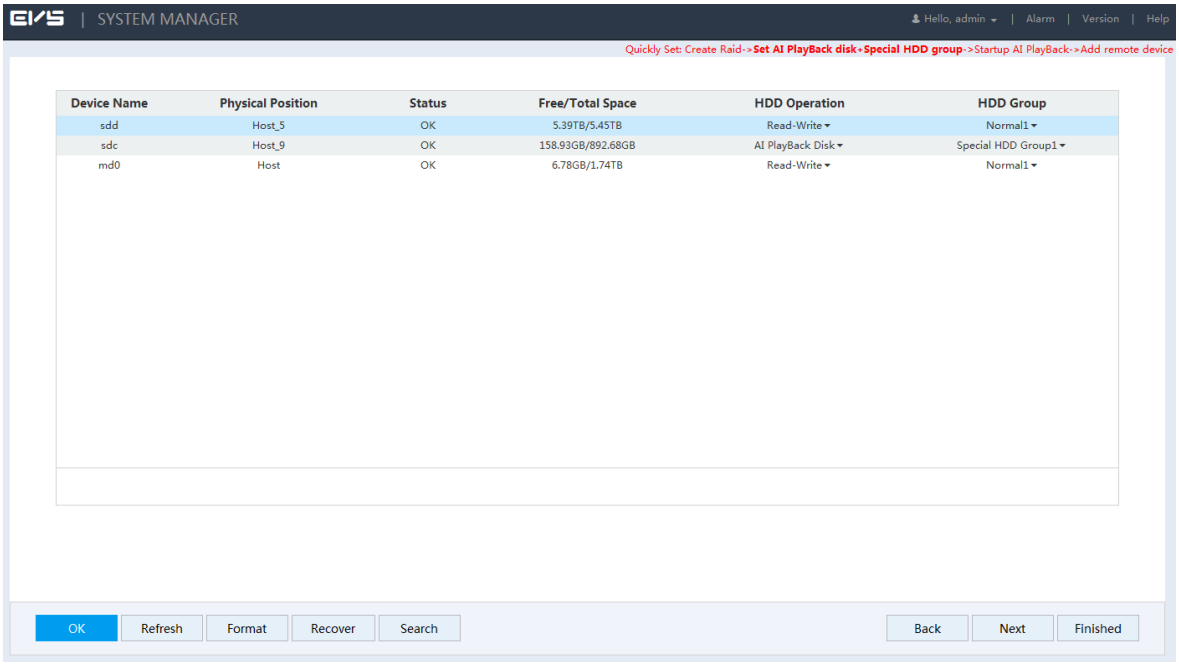


Step 2 Create RAID. For details, see "3.13.5.1 Creating RAID."

Step 3 Click **Next**.

The **Set AI PlayBack disk + Special HDD group** interface is displayed. See Figure 3-28.

Figure 3-28 Setting AI playback HDD and special HDD group



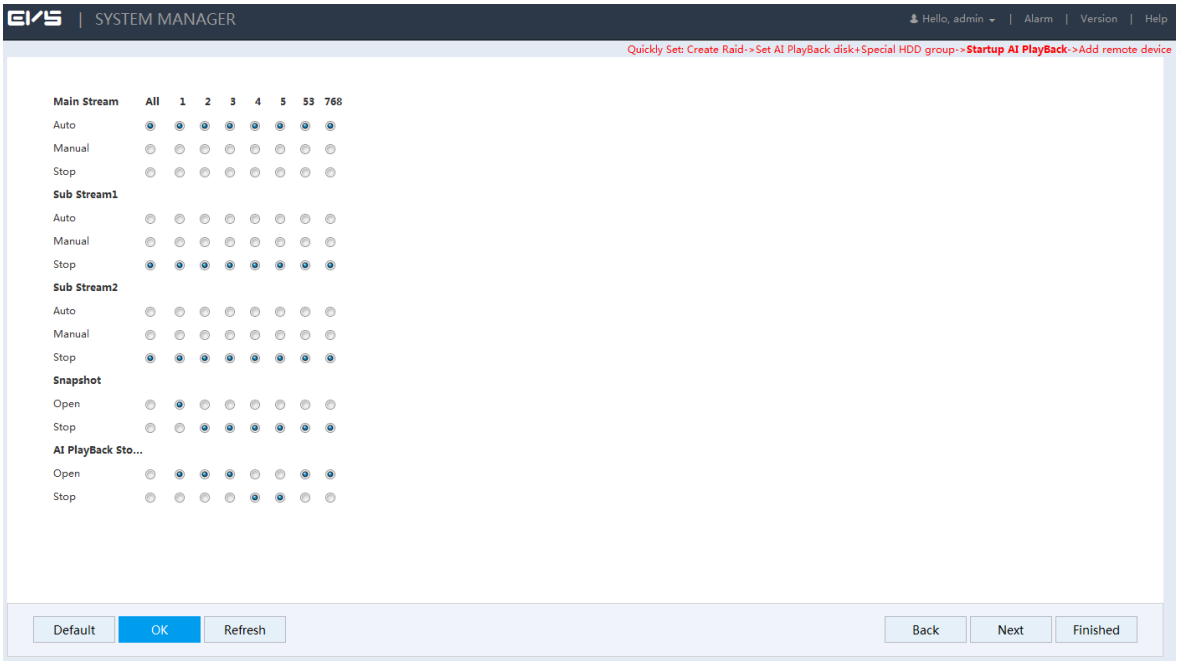
Step 4 Set AI playback HDD and HDD group.

1) Set the **HDD Operation** of one or several disks to **AI PlayBack Disk**.
2) Set the **HDD Group** of the AI playback disk to **Special HDD Group**.
3) Click **OK** to save the configuration.

Step 5 Click **Next**.

The **Startup AI PlayBack** interface is displayed. See Figure 3-29.

Figure 3-29 AI playback startup

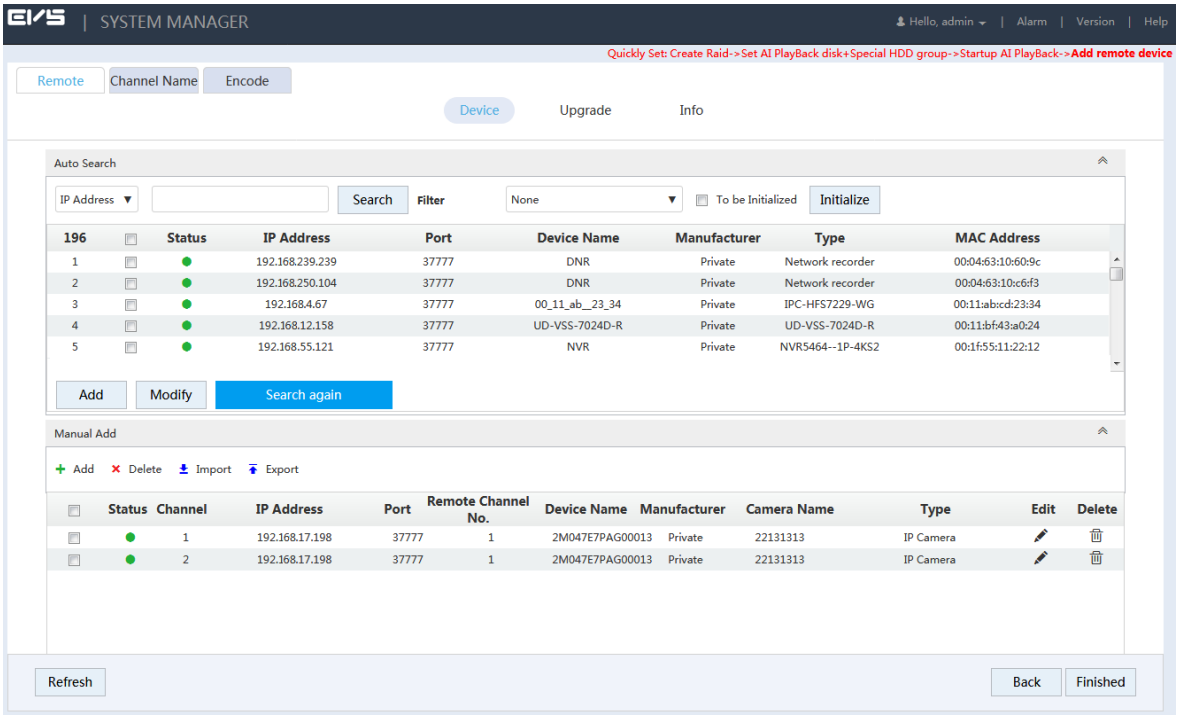


Step 6 Enable the **AI Playback Storage** of the channels and click **OK** to save the configuration.

Step 7 Click **Next**.

The **Add remote device** interface is displayed. See Figure 3-30.

Figure 3-30 Adding remote device



Step 8 Add remote device. For details, see "3.4.2 Adding Remote Device."

Step 9 Click **OK** to save the configuration.

After the configuration, you can search the AI playback video. For details, see "3.6.2 Searching AI Playback"

3.6.2 Searching AI Playback

The system supports searching or downloading AI records, including records of IVS analyse, vehicle analyse, face detect and human trait functions.

Preparation

To enable the search and download functions, you need to configure AI playback first.

The system supports only front-end AI analysis function. Different cameras support different functions. Refer to the actual product for the functions available.

3.6.2.1 IVS Analyse

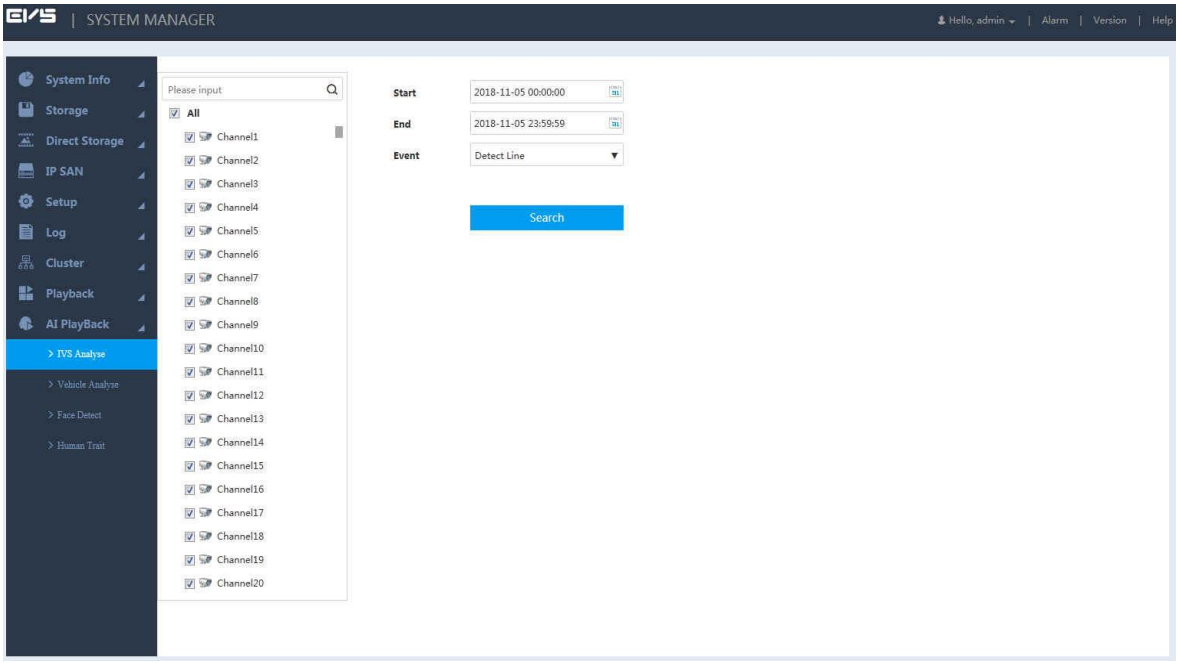
IVS analyse refers to extracting the key information in the record through image processing and analysis, and matching it with the preset detection rules. When the detected behavior matches the rule, the system performs alarm linkage actions.

IVS analyse includes analyzing events of detect line, detect region, abandoned object, motion, face detection, number stat, video abnormal and video unfocus.

Step 1 Select **AI PlayBack > IVS Analyse**.

The **IVS Analyse** interface is displayed. See Figure 3-31.

Figure 3-31 IVS analyse interface



Step 2 Select the parameters. For details, see Table 3-10.

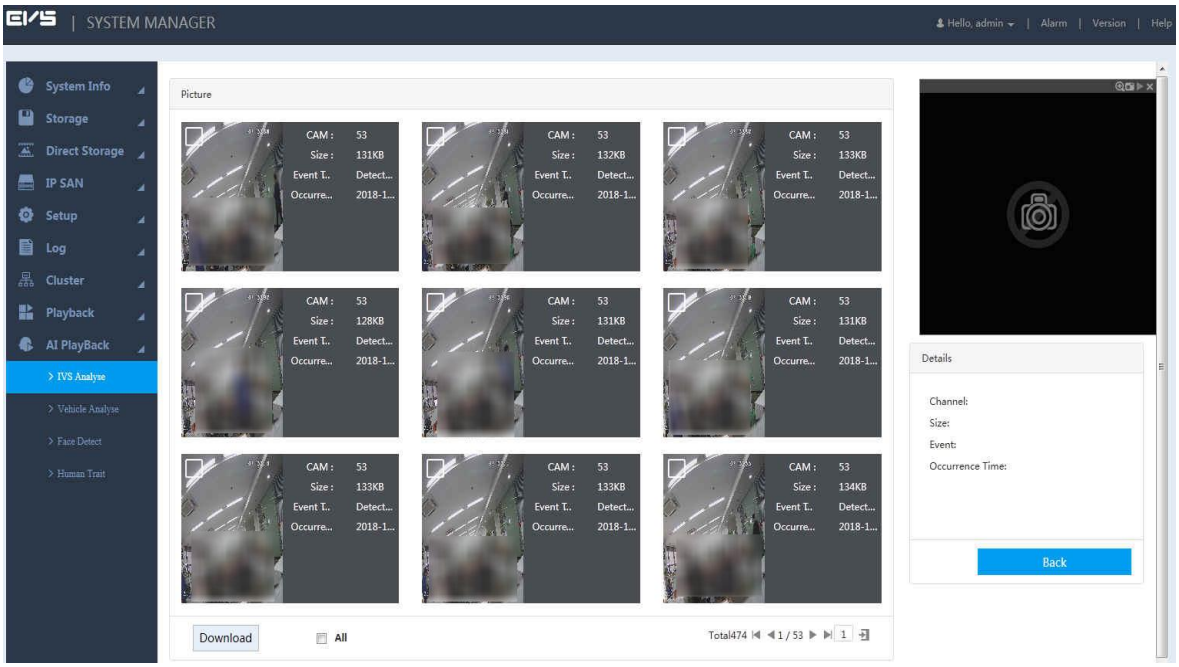
Table 3-10 IVS analyse parameters

Parameter	Description
Channel	Select the channel(s) you want to search. You can select a single channel or multiple channels, or select **All** to search all the channels.
Start	Select the start time and end time of your search.
End	
Event	Select the AI playback event you want to search, including detect line, detect region, abandoned object, motion, face detection, number stat, video abnormal and video unfocus.

Step 3 Click **Search**.

The IVS analyse results are displayed. See Figure 3-32.

Figure 3-32 IVS analyse results



Step 4 Check the record.

- Click the picture, and the system will display the details of the picture at the bottom right.
- Double-click the picture, and the system will play the main stream recording about 10s before and after the picture in the upper right window. For play details, see Table 3-11.

You can double-click the play interface to switch between full-screen and small-screen play.

Table 3-11 Instructions of record operation

Icon	Description
	Click on any point in the screen and scroll your mouse wheel to zoom in or out on the screen.
	Snapshot the current screen that plays video.
	Pause video play.
	Close the current screen that plays video.

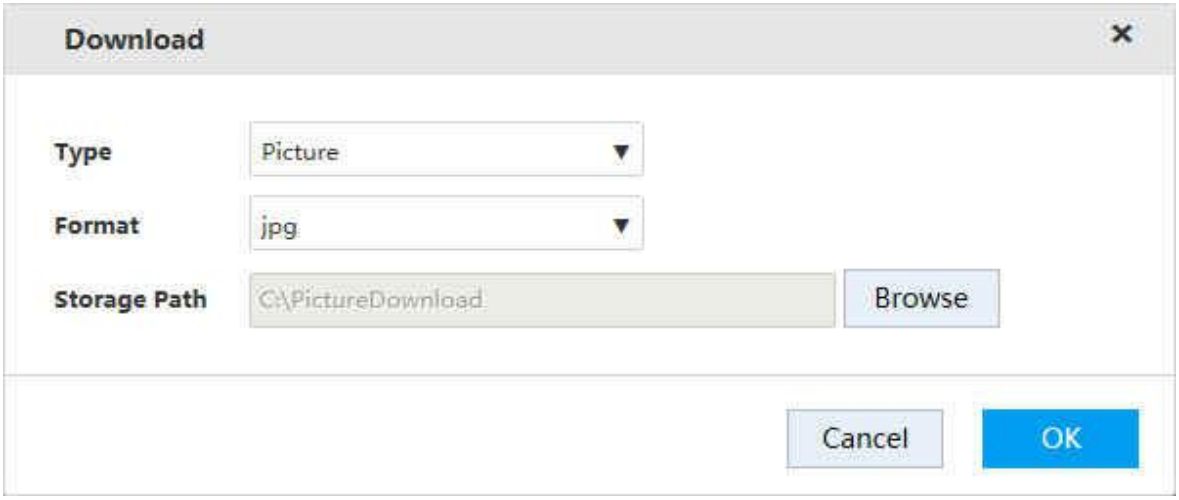
Download

On the interface of IVS analyse results (see Figure 3-32), select one or more picture(s), and click Download.

The **Download** interface is displayed. See Figure 3-33.

You can download relevant pictures and records to your local PC.

Figure 3-33 Download interface



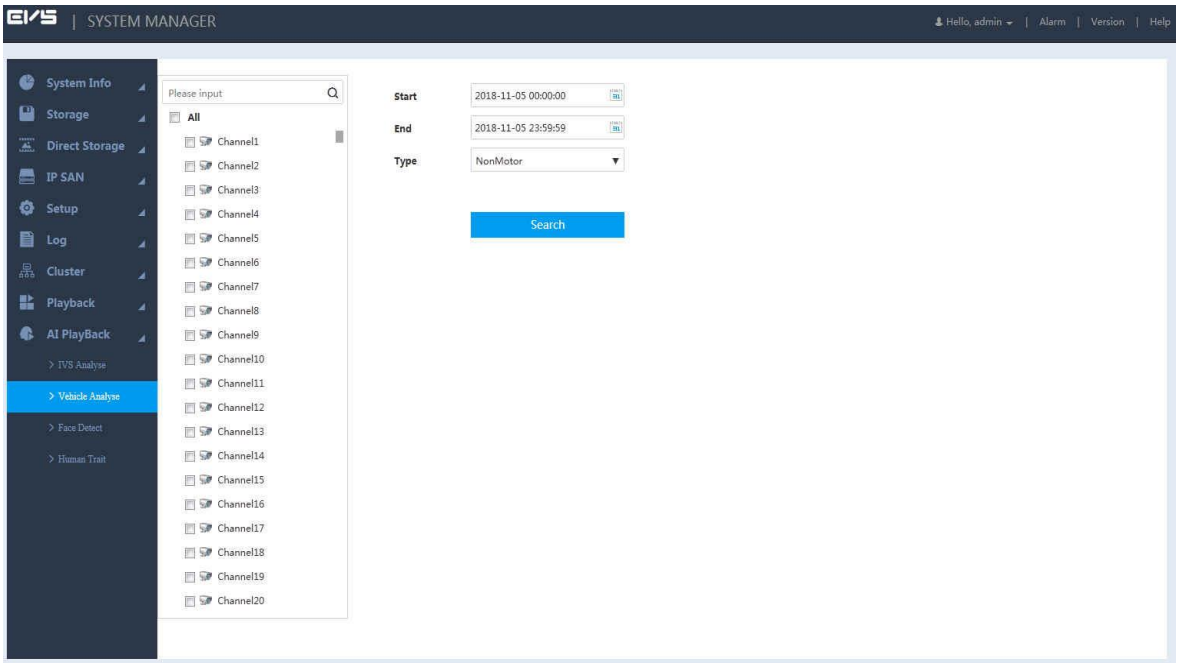
3.6.2.2 Vehicle Analyse

Vehicle analyse uses video image recognition technology to extract vehicle information in the video image. If the detected vehicle information matches the time rule, the system performs alarm linkage actions.

Step 1 Select **AI PlayBack > Vehicle Analyse**.

The **Vehicle Analyse** interface is displayed. See Figure 3-34.

Figure 3-34 Vehicle analyse interface



Step 2 Configure the parameters. For details, see Table 3-12.

Table 3-12 Vehicle analyse parameters

Parameter	Description
Channel	Select the channel(s) you want to search. You can select a single channel or multiple channels, or select **All** to search all the channels.

Parameter	Description
Start	Select the start time and end time of your search.
End	
Type	Select the type of vehicle, which includes non-motor and intelligent traffic.
Event	Select the traffic event. Events include traffic gate, red light running, yellow light running, over white line, over yellow line, retrograde, illegal turn left, illegal turn right, illegal U-turn, cross lane, illegal parking, traffic jam, traffic idle, stop in waiting area, lack speed, over speed, driving wrong route, BV in road, vehicle in road, stay, traffic pedestrian priority, vehicle in bus route, illegal backing, over stop line, parking on yellow box, traffic restricted plate, without safe belt, traffic no passing, driver smoking, driver calling, traffic pedestrian, driver throwing, traffic pedestrian run red light, space parking, space no parking, space over line, truck forbid, right after straight, right after people, queue jump, big bend small turn, and turn left after straight.  This function is available only when Intelligent Traffic is selected as the Type.
Logo	You can select all, unknown, Audi, Honda, Buick, Volkswagen, Toyota, BMW, Peugeot, Ford, Mazda, Nissan, Hyundai, Suzuki, Citroen, Benz, BYD, Geely, Lexus, Chevrolet, Chery, Kia, Charade, DF, Naveco, SGMW, and Jinbei.  This function is available only when Intelligent Traffic is selected as the Type.
Lane	Select the lane.  This function is available only when Intelligent Traffic is selected as the Type.
Speed Range	Select the speed range of the vehicle. 0km/h–180km/h is available. Select the checkbox to enable this function.  This function is available only when Intelligent Traffic is selected as the Type.
Plate Number	Input the plate number. Select the checkbox to enable this function.

Step 3 Click **Search**.

The vehicle analyse results will be displayed.

Step 4 Check the record.

- Click the picture, and the system will display the details of the picture at the bottom right.
- Double-click the picture, and the system will play the main stream recording about 10s before and after the picture in the upper right window. For play details, see Table 3-11.

You can double-click the play interface to switch between full-screen and small-screen play.

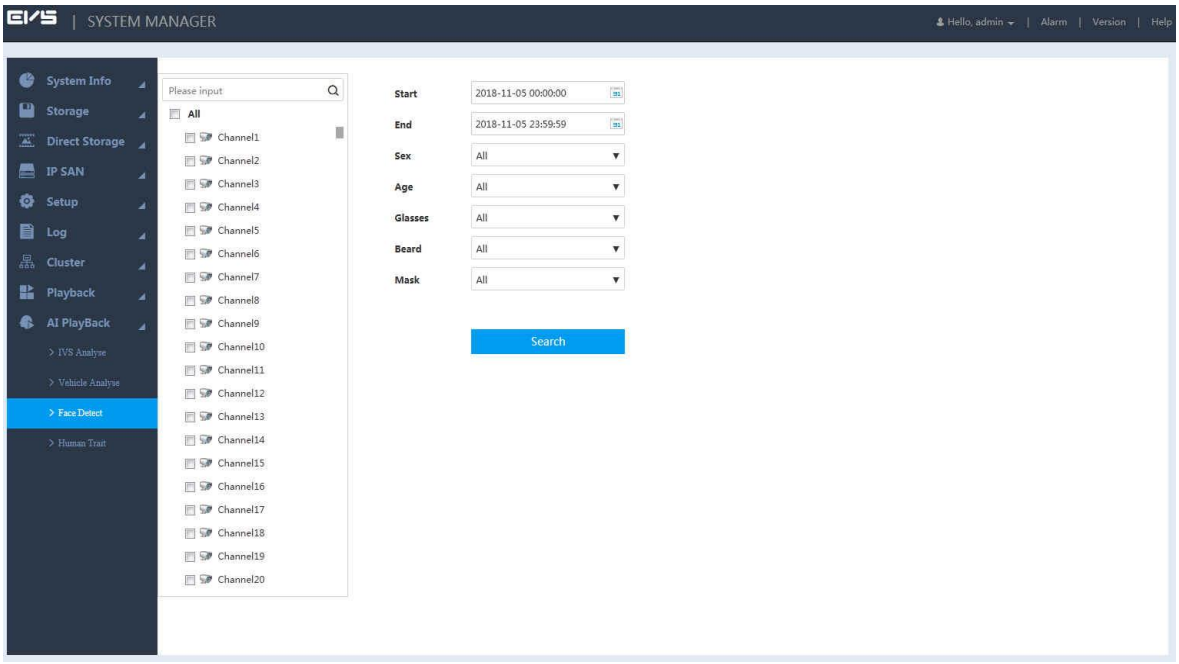
3.6.2.3 Face Detect

This function aims to analyse and process the video image captured by the camera, and detect if the video image contains any face. You can filter out the video that contains face and play it back.

Step 1 Select **AI PlayBack > Face Detect**.

The **Face Detect** interface is displayed. See Figure 3-35.

Figure 3-35 Face detect interface

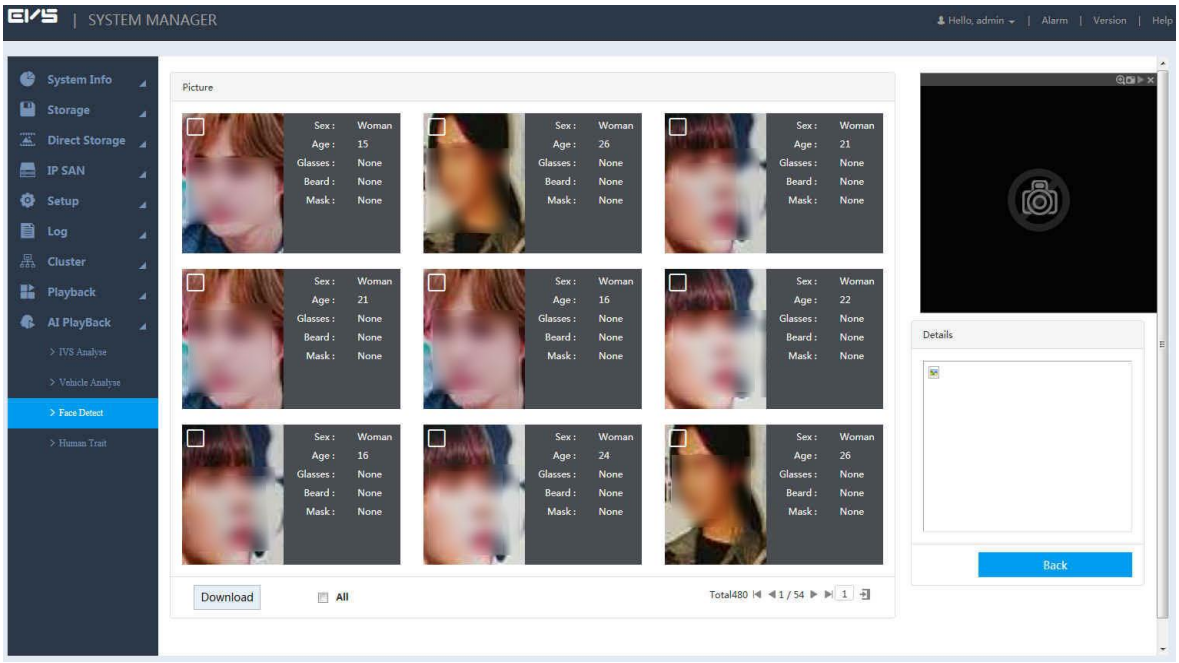


Step 2 Select channel(s), start and end time, and set other filter conditions.

Step 3 Click **Search**.

The system displays pictures that meet filter conditions. See Figure 3-36 as the example.

Figure 3-36 Face detect results



Step 4 Check the record.

- Click the picture, and the system will display the details of the picture at the bottom right.
- Double-click the picture, and the system will play the main stream recording about 10s before and after the picture in the upper right window. For play details, see Table 3-11.

You can double-click the play interface to switch between full-screen and small-screen play.

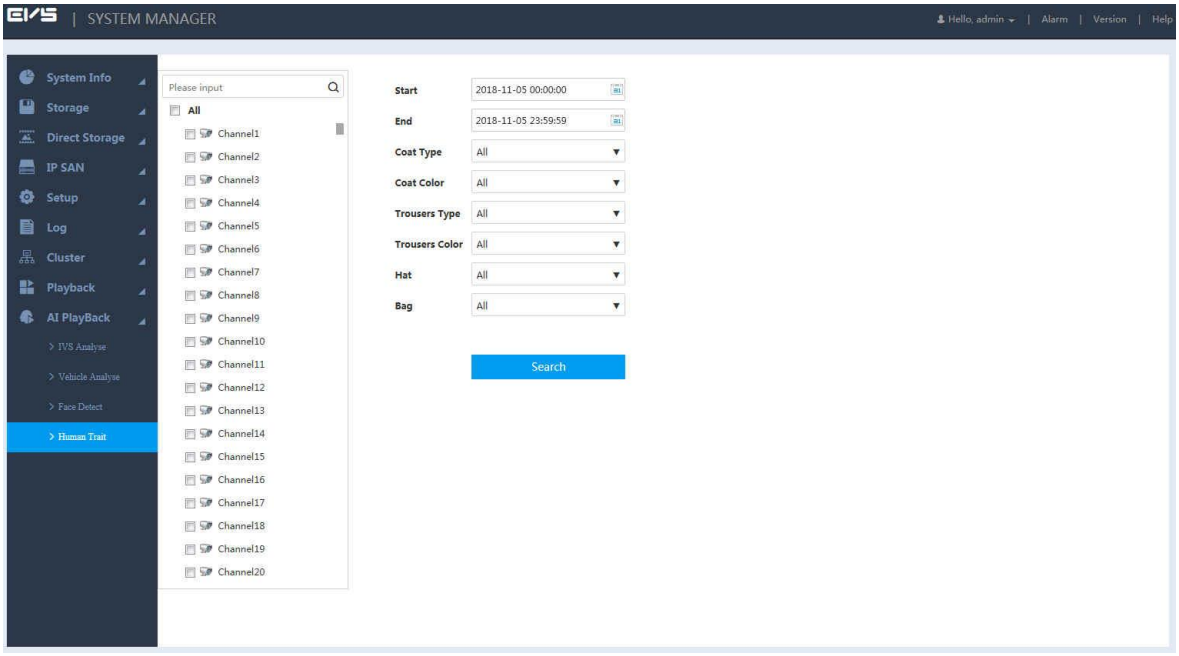
3.6.2.4 Human Trait

This function aims to analyse and process the video image captured by the camera, and detect if the video image contains any human. You can filter out the video that contains human and play it back.

Step 1 Select **AI PlayBack > Human Trait**.

The **Human Trait** interface is displayed. See Figure 3-37.

Figure 3-37 Human trait interface

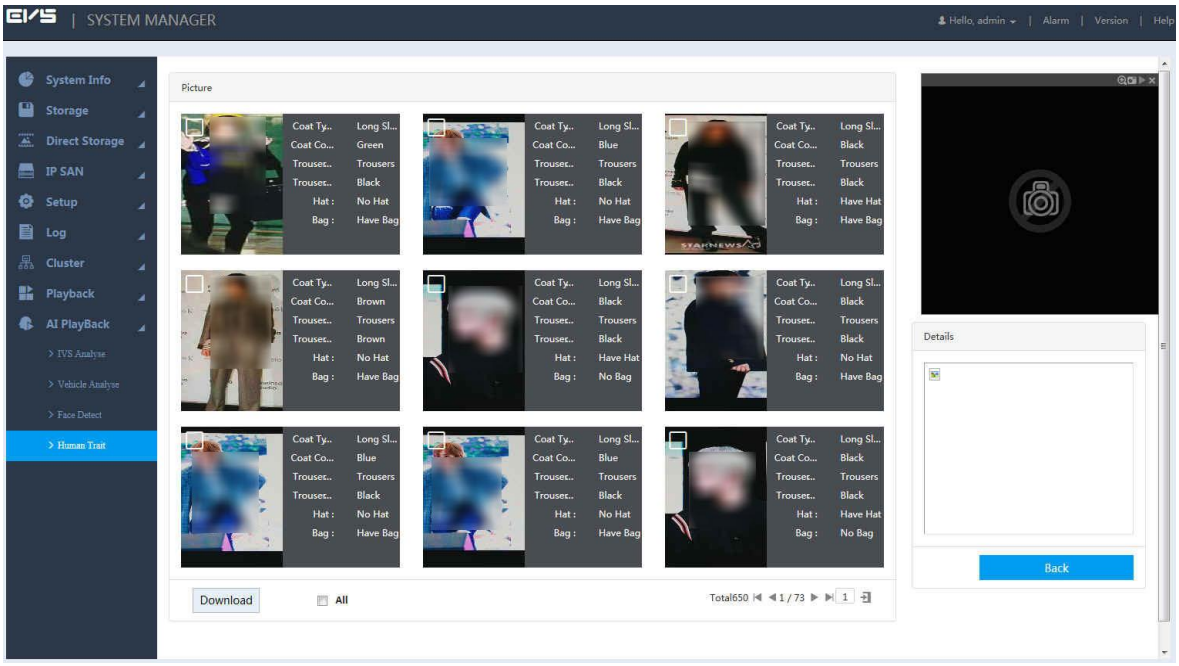


Step 2 Select channel(s), start and end time, and set other filter conditions.

Step 3 Click **Search**.

The system displays pictures that meet the filter conditions. See Figure 3-38 as the example.

Figure 3-38 Human trait results



Step 4 Check the record.

- Click the picture, and the system will display the details of the picture at the bottom right.
- Double-click the picture, and the system will play the main stream recording about 10s before and after the picture in the upper right window. For play details, see Table 3-11.

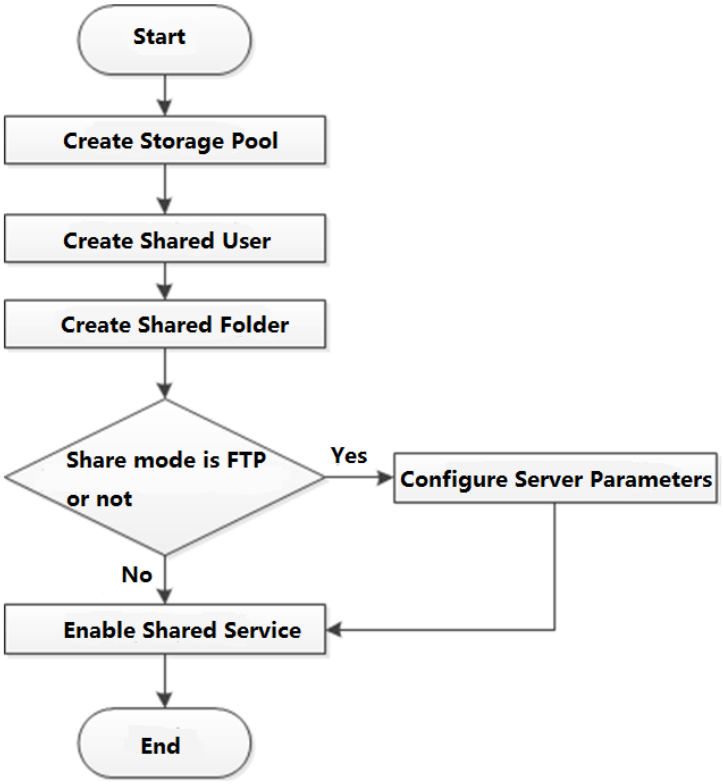
You can double-click the play interface to switch between full-screen and small-screen play.

3.7 IP SAN

Internet Protocol Storage Area Network (IP SAN) is a kind of network storage technology based on IP network. It builds disks and RAID into a virtual logical device (i.e. storage pool) and shares the storage path with other devices through NFS, iSCSI, FTP and SAMBA to enable other devices to store data into the shared path.

For the procedure to configure IP SAN, see Figure 3-39.

Figure 3-39 Configuring IP SAN



3.7.2 Creating Storage Pool

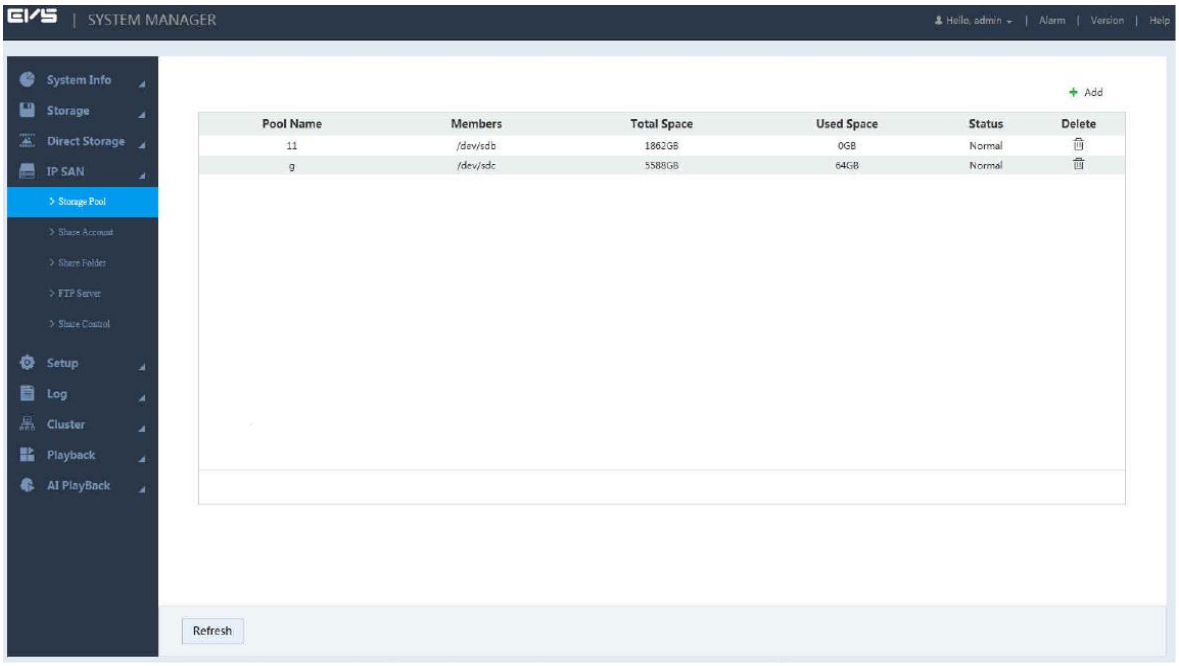
Storage pool is a logical device that is virtualized by the storage devices, which is managed by the system and can be composed of multiple actual disks or RAID. It is one of the main means to realize virtual storage.

When creating the storage pool, the system will format the selected disk. Operate with care.

Step 1 Select **IP SAN > Storage Pool**.

The **Storage Pool** interface is displayed. See Figure 3-40.

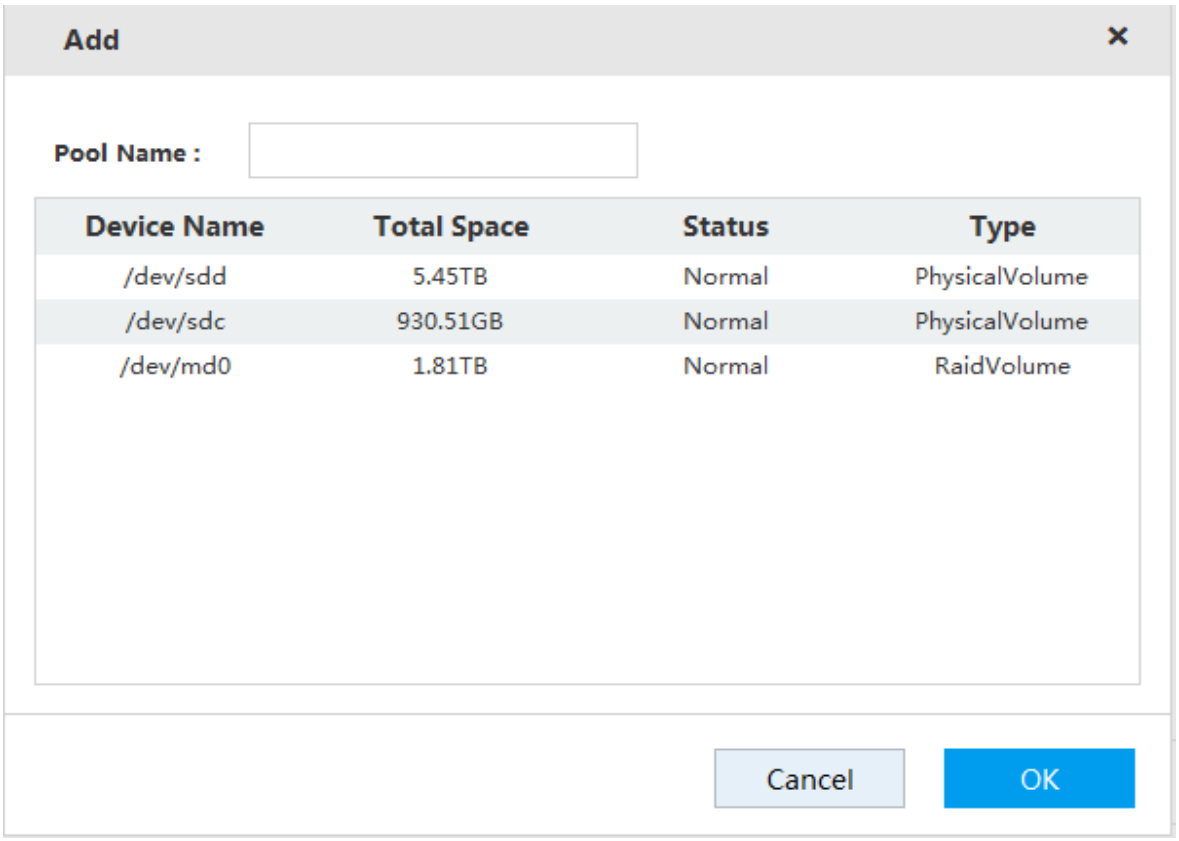
Figure 3-40 Storage pool



Step 2 Click + .

The **Add** interface is displayed. See Figure 3-41.

Figure 3-41 Adding storage pool



Step 3 Enter the **Pool Name** and select the disk or RAID group.

By default, sd*x* (x ranges from a to z) refers to disk, such as /dev/sda. Md*x* (x is a number) refers to RAID group, such as /dev/md0.

Step 4 Click **OK** to save the configuration.

A dialogue box pops up. Click **Yes**.

The system starts to create the storage pool. After the creation, the system returns to the **Storage Pool** interface. You can view the new pool information here.

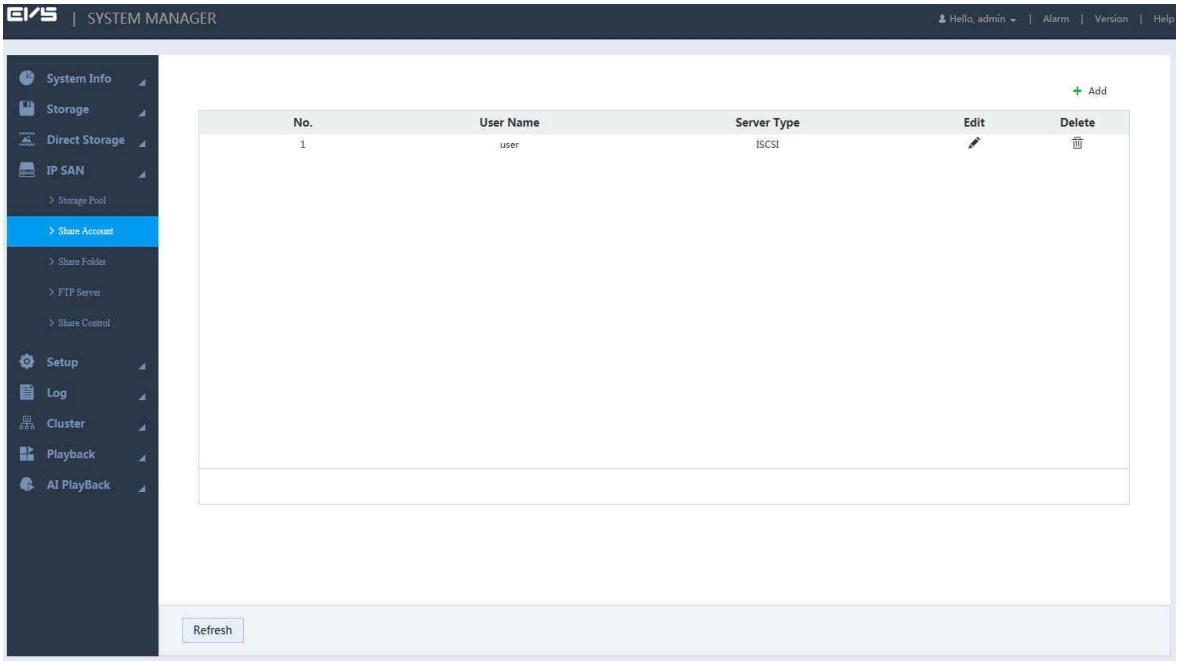
3.7.3 Managing Share Account

You need to access and manage the share folder with a share account.

Step 1 Select **IP SAN > Share Account**.

The **Share Account** interface is displayed. See Figure 3-42.

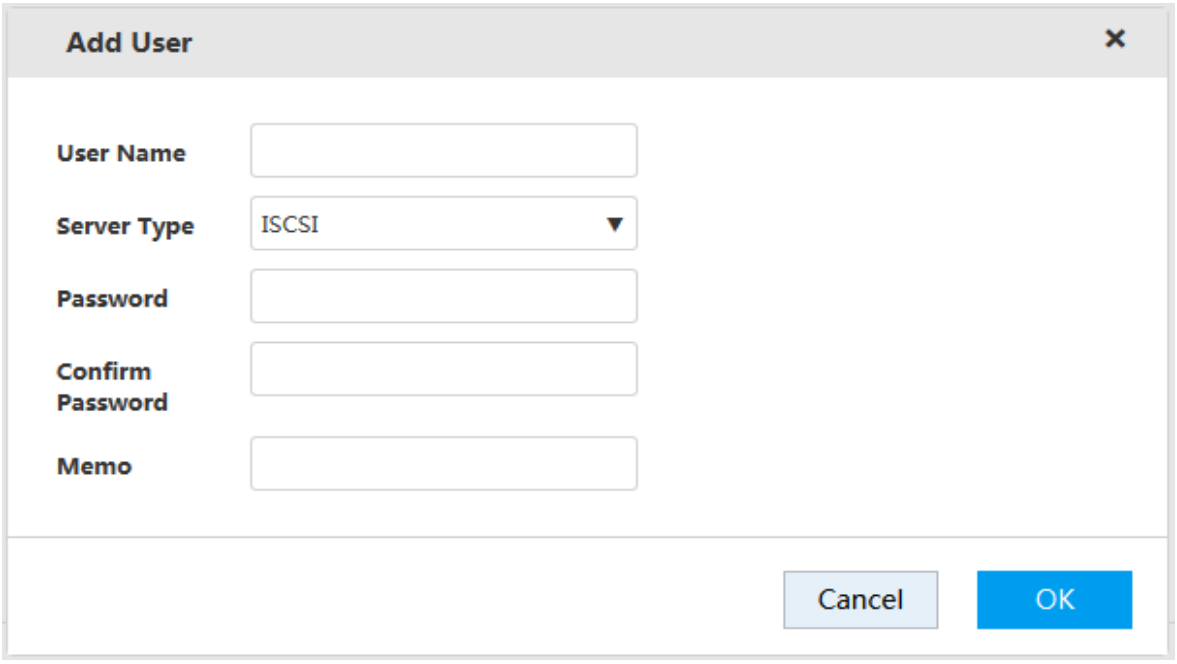
Figure 3-42 Share account management



Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-43.

Figure 3-43 Adding shared user



Step 3 Configure the parameters. For details, see Table 3-13.

Table 3-13 Adding user parameters

Parameter	Description
User Name	Enter the name of the share account.
Server Type	Select the corresponding service type of the share account: iSCSI, FTP/SAMBA or iSCSI/FTP/SAMBA.
Password	Enter and confirm the password of the share account. When you select iSCSI or iSCSI/FTP/SAMBA for the server type, the password shall consist of 12 characters.
Confirm Password	
Memo	Enter memo to help recognize and manage the account.

Step 4 Click **OK** to save the configuration.

The system returns to the **Share Account** interface. You can view the new account information here.

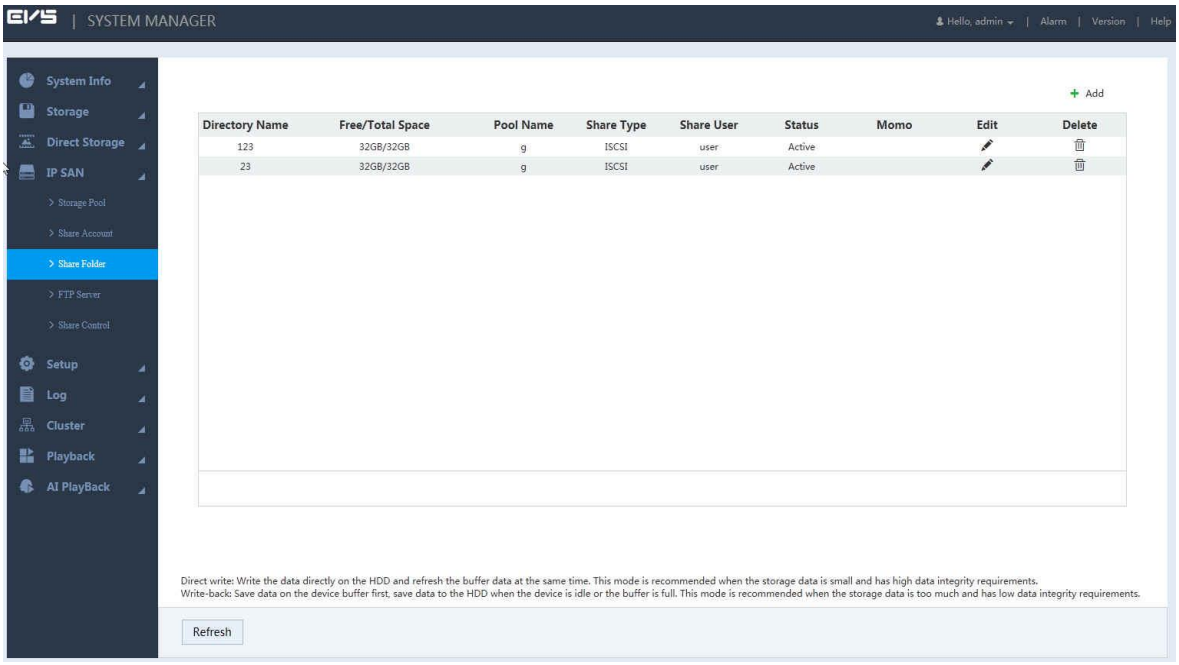
3.7.4 Setting Share Folder

You can access the share folder on other devices through the share account.

Step 1 Select **IP SAN > Share Folder**.

The **Share Folder** interface is displayed. See Figure 3-44.

Figure 3-44 Share folder



Step 2 Click + .

The Add interface is displayed. See Figure 3-45 or Figure 3-46.

Figure 3-45 Adding share folder (NFS)

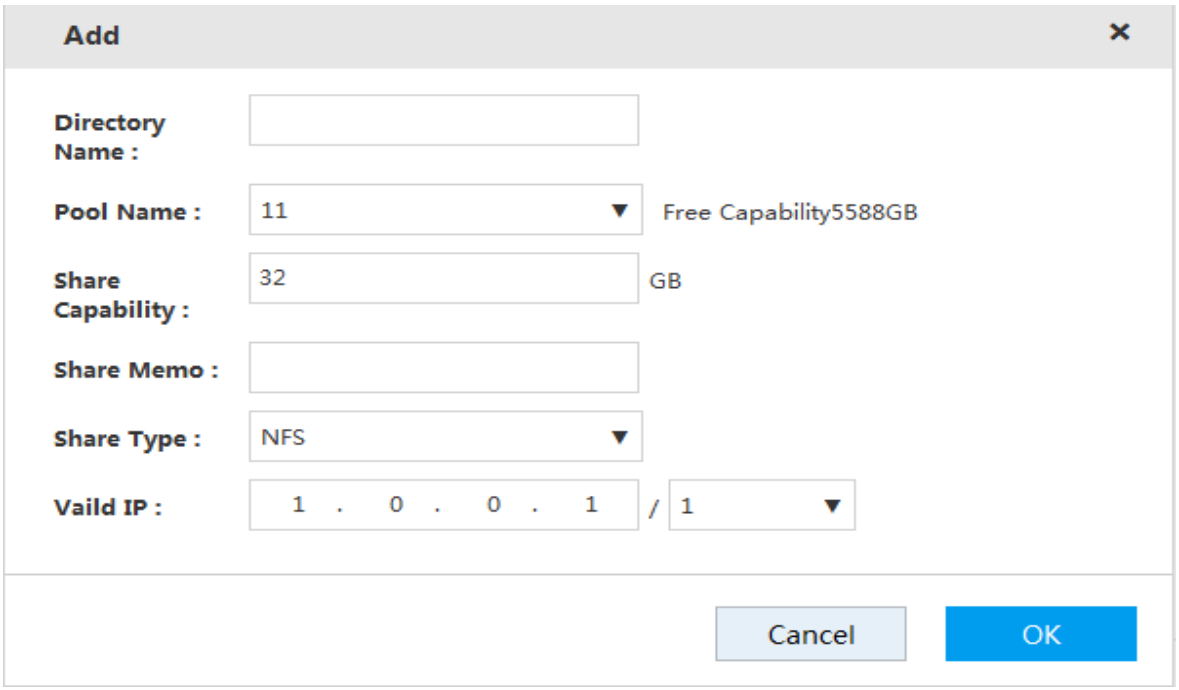
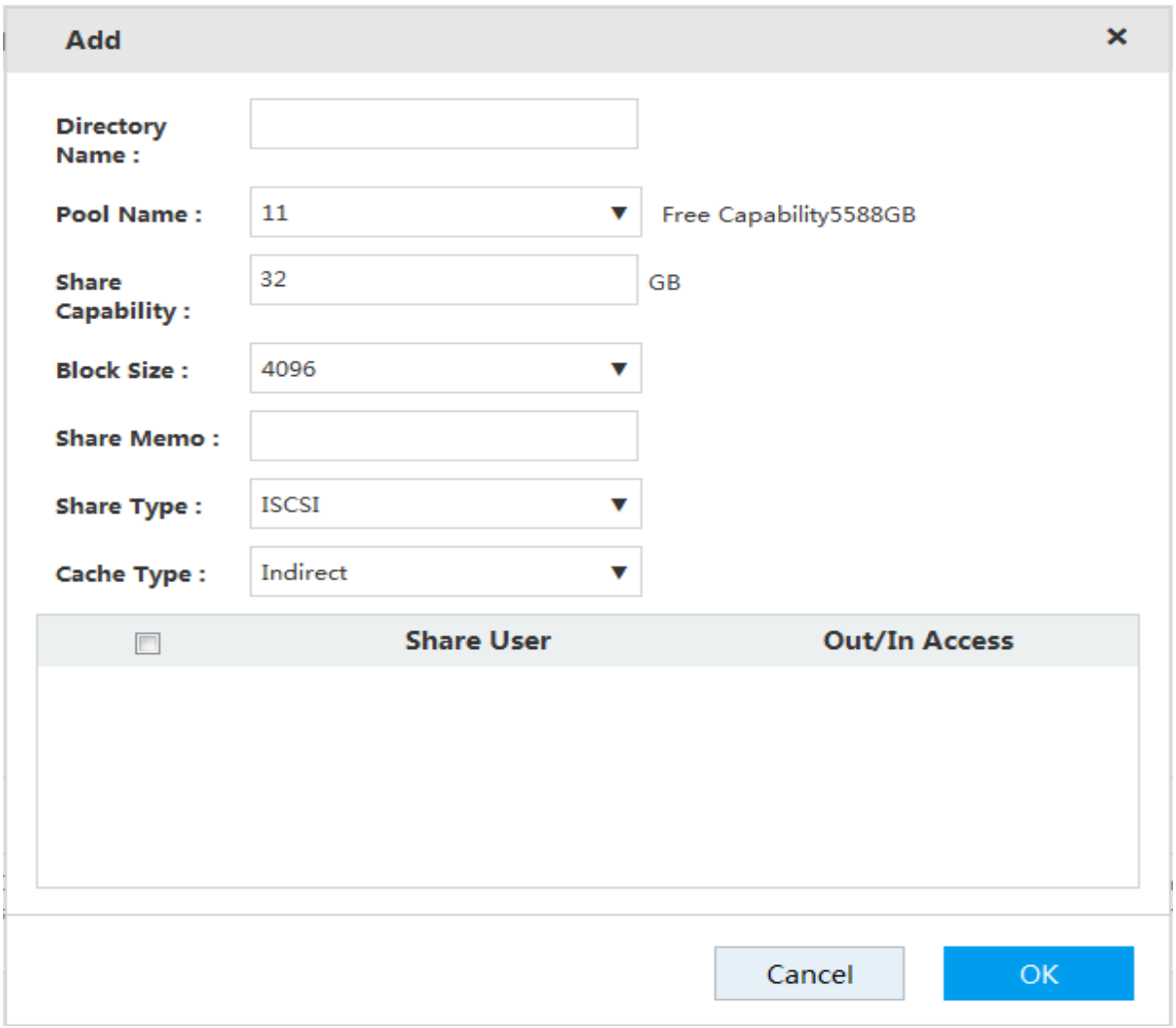


Figure 3-46 Adding share folder (iSCSI)



Step 3 Configure the parameters. For details, see 0.

Table 3-14 Share folder parameters

Parameter	Description
Directory Name	Enter the name of the share folder.
Pool Name	Select the pool in which you need to create the share folder.  Free capability refers to the max available volume of the storage pool.
Share Capability	Enter the available space of the share folder.
Share Memo	(Optional) It helps to recognize and manage the share folder.
Share Type	Select the **Share Type**: ● NFS: Provides share services to Linux users. ● FTP: Provides share services to Windows and Linux users at the same time. ● SAMBA: Provides share services to Windows users. ● iSCSI: Provides share services to iSCSI users.
Valid IP	Set the IP address and subnet mask of the hosts allowed to access this share folder. For example: When the valid IP is 192.168.10.108/24, it means the IP address is 192.168.10.108 and the subnet mask is 255.255.255.0. All the IP hosts in this segment can access the share folder.  This parameter needs to be configured when the **Share Type** is set as NFS.
Valid User	Select the shared user and set its out/in access authority. ● When the **Share Type** is set as FTP and SAMBA and no valid user is selected, only the admin account has the access permission. Other accounts do not have the authority. ● When the **Share Type** is set as iSCSI and no valid user is selected, all the users have the access permission.  ● You need to select the valid user when select FTP, SAMBA or iSCSI as the share type. ● FTP default admin account: ftpuser; default password: 111111111111. SAMBA default admin account: admin; default password: 888888888888.

Parameter	Description
Cache Type	It includes **Direct** and **Indirect**. ● Direct: Store the data directly into the disk and update the data in cache. When you have little data but high integrity request, direct strategy is recommended. ● Indirect: Store data in the cache first and transfer it to the disk when the system is free or the cache is full. When you have a large amount of data and the data integrity request is low, indirect strategy is recommended. You need to configure this item when the share type is iSCSI.
Block Size	Select the block size of share folder, including 512Byte, 1024Byte, 2048Byte and 4096Byte. You need to configure this item when the share type is iSCSI.

Step 4 Click **OK** to save the configuration.

The system returns to the **Share Folder** interface. You can view the new share folder information here.

When you create the share folder for the first time or create share folder under the condition of system auto maintenance, the system will force off the auto maintenance. After configuring the IP SAN, you can enable auto maintenance manually.

3.7.5 Setting FTP Parameters

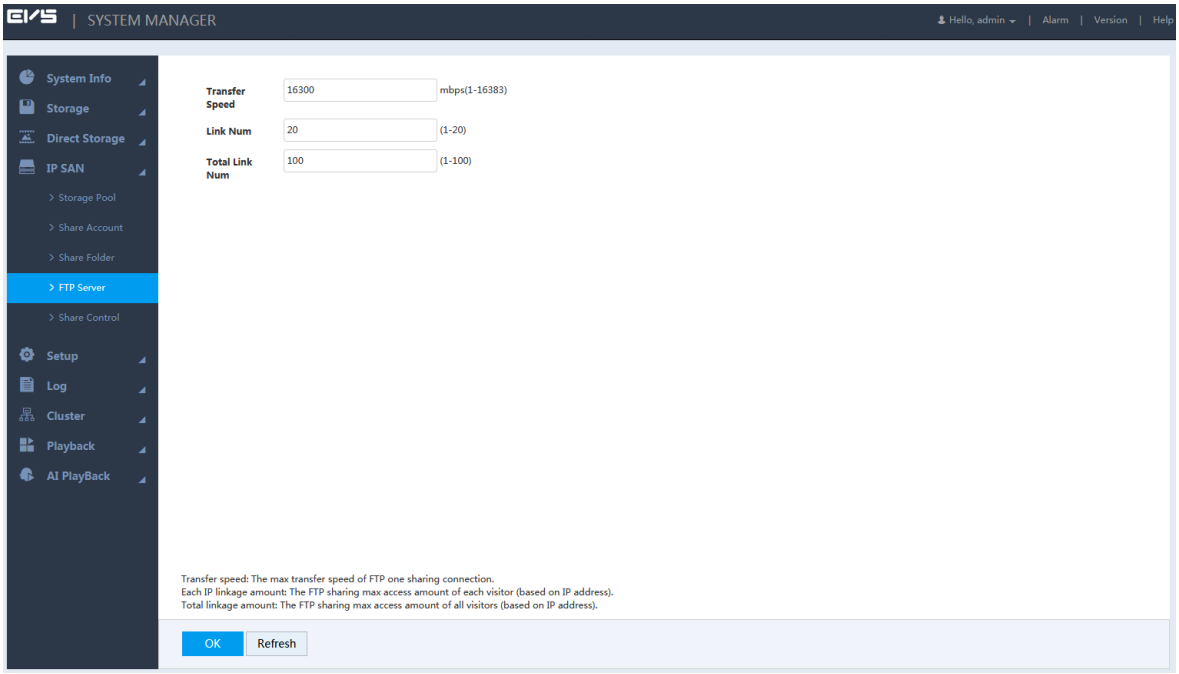
Set the transmission speed and max connection number in FTP share.

You need to set the FTP parameters when the share type is set as FTP.

Step 1 Select **IP SAN > FTP Server**.

The **FTP Server** interface is displayed. See Figure 3-47.

Figure 3-47 FTP Parameters



Step 2 Enter the parameters. For details, see Table 3-15.

Table 3-15 FTP server parameters

Parameter	Description
Transfer Speed	Enter the max transfer speed during single transmission.
Link Number	Enter the max connection number for each user (taking IP as a reference unit) to access FTP share at the same time.
Total Link Number	Enter the max connections for all the users (taking IP as a reference unit) to access FTP share at the same time.

Step 3 Click **OK** to save the configuration.

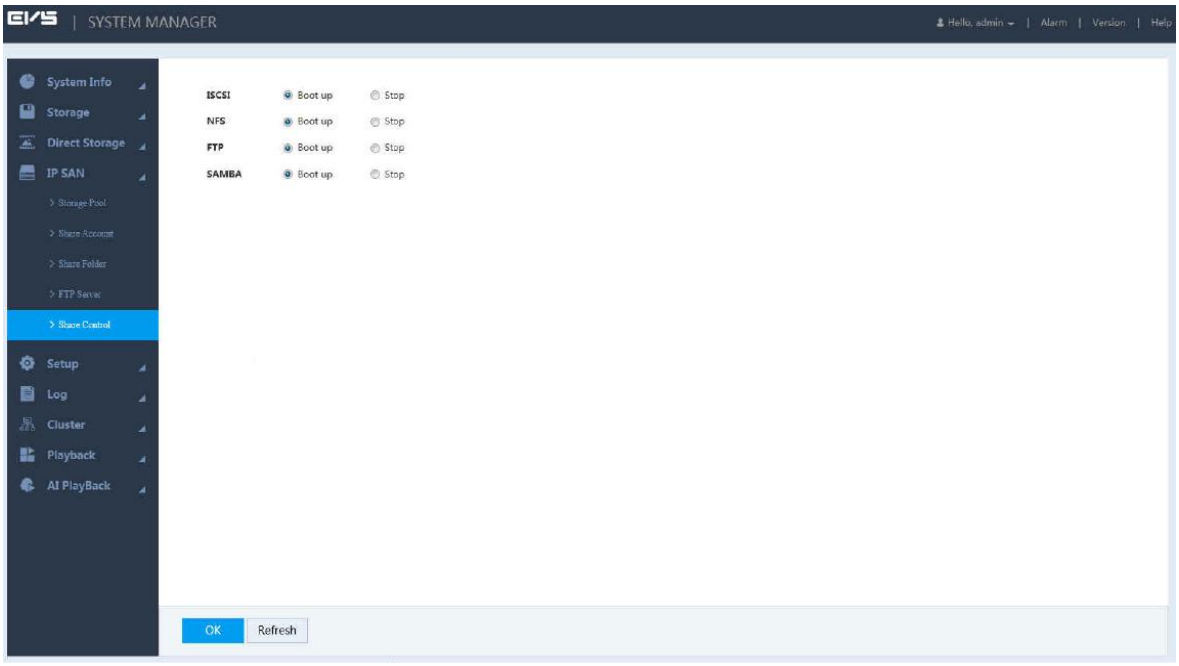
3.7.6 Opening Share Services

After enabling the shared service, the user can remotely access the share folder.

Step 1 Select **IP SAN > Share Control**.

The **Share Control** interface is displayed. See Figure 3-48.

Figure 3-48 Share control



Step 2 Start or stop the share service according to actual needs.

Step 3 Click **OK** to save the configuration.

3.8 Remote Device

You can add, edit and upgrade your remote device. In addition, you can set the channel name and stream parameters of your remote device.

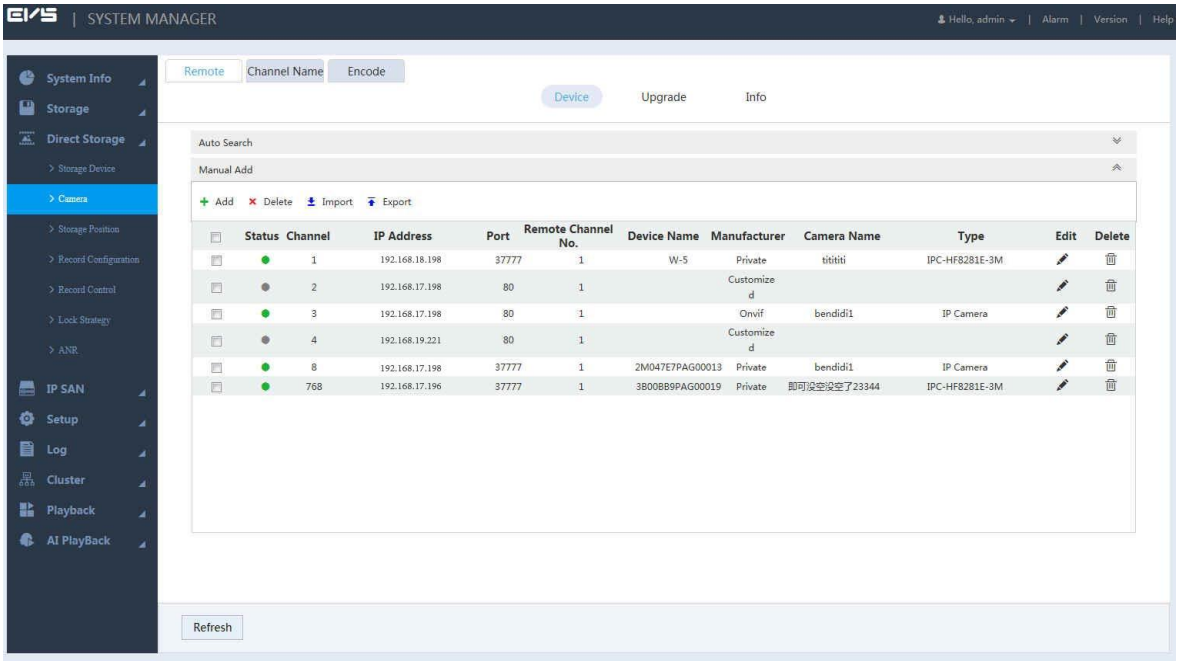
3.8.1 Initializing Remote Device

When initializing your remote device, you can modify its login password and IP address.

Step 1 Select **Direct Storage > Camera > Remote > Device**.

The **Device** interface is displayed. See Figure 3-49.

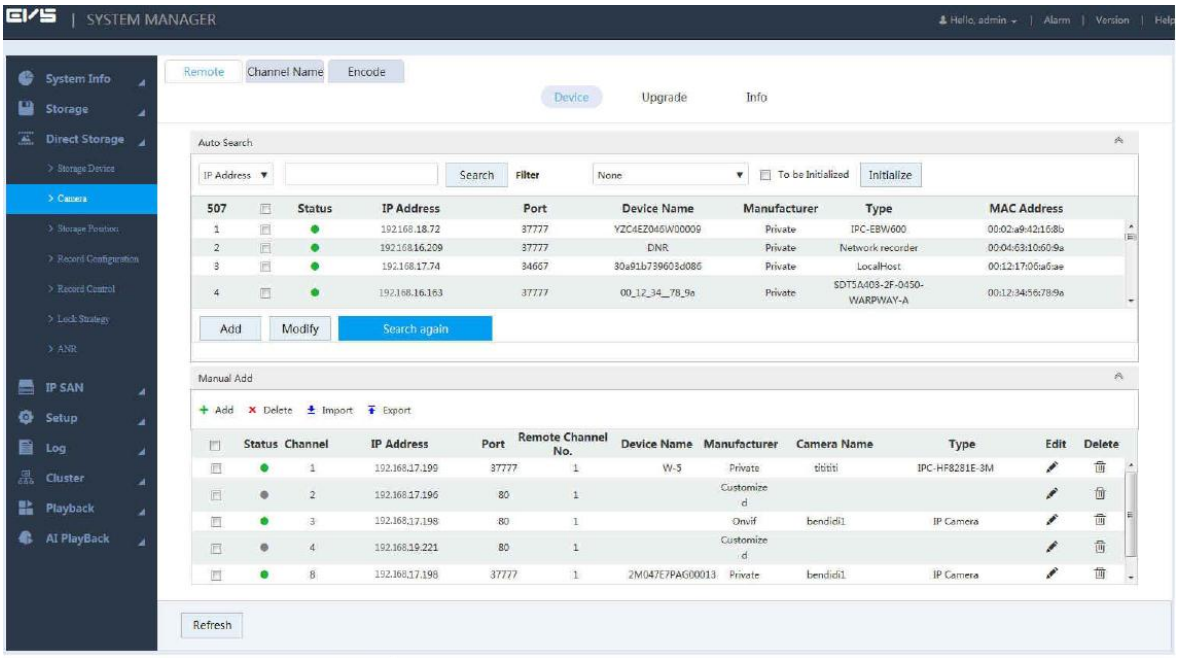
Figure 3-49 Device interface



Step 2 Click at the right side of Auto Search, and then click **Device Search**.

The system searches the remote device of the LAN and displays the search results. See Figure 3-50.

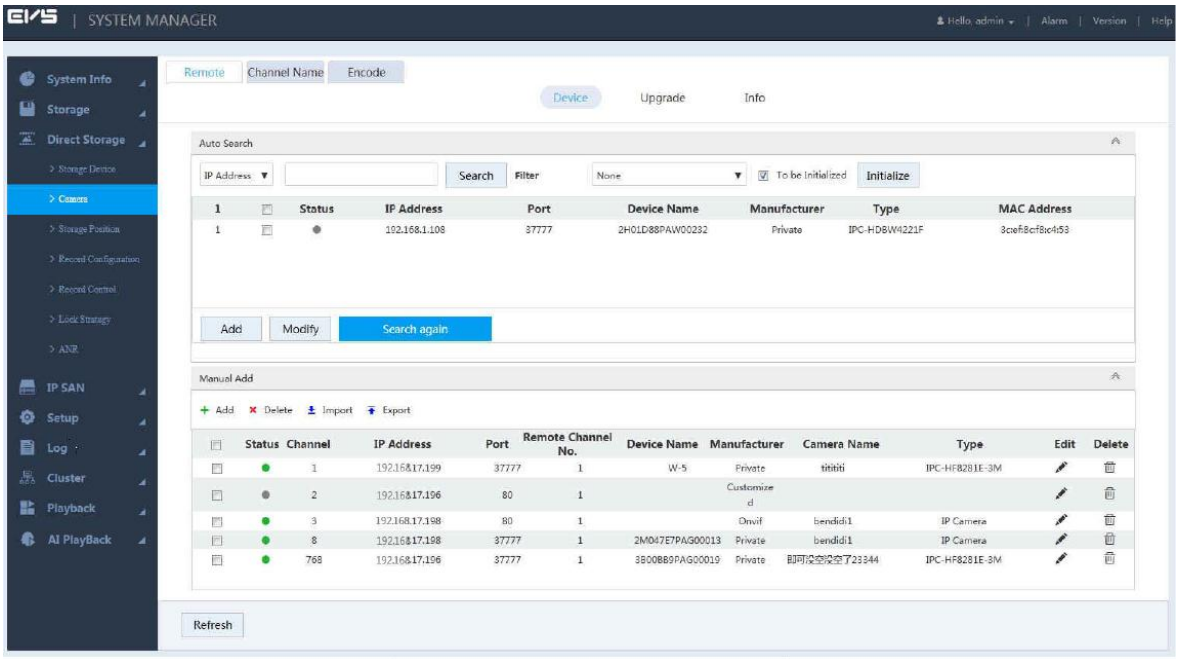
Figure 3-50 Search result interface



Step 3 Select To be initialized.

The system displays device that needs to be initialized. See Figure 3-51.

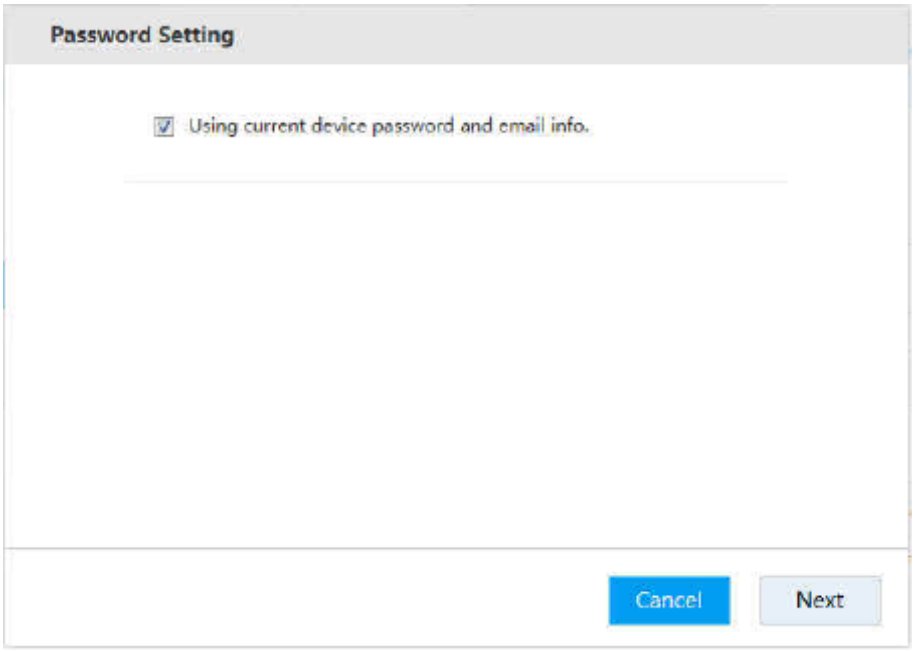
Figure 3-51 Device needs to be initialized



Step 4 Select the device to be initialized. Click **Initialize**.

The system displays **Password Setting** interface. See Figure 3-52.

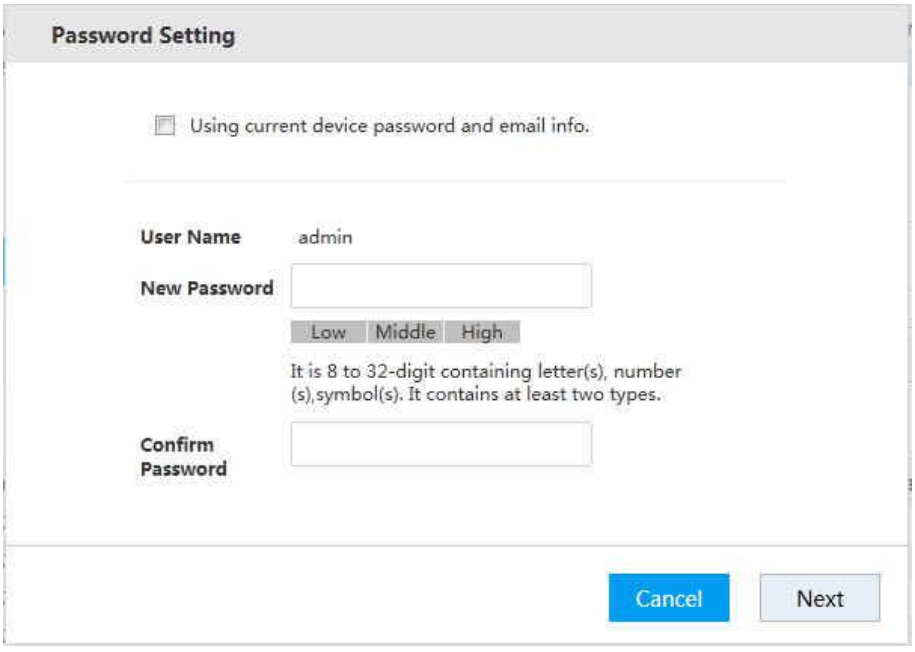
Figure 3-52 Password setting (1)



Step 5 Set the password of the remote device.

If you do not select **Using current device password and email info**, and the interface will be displayed as is shown in Figure 3-53. In this case, you need to manually set the password.

Figure 3-53 Password setting (2)

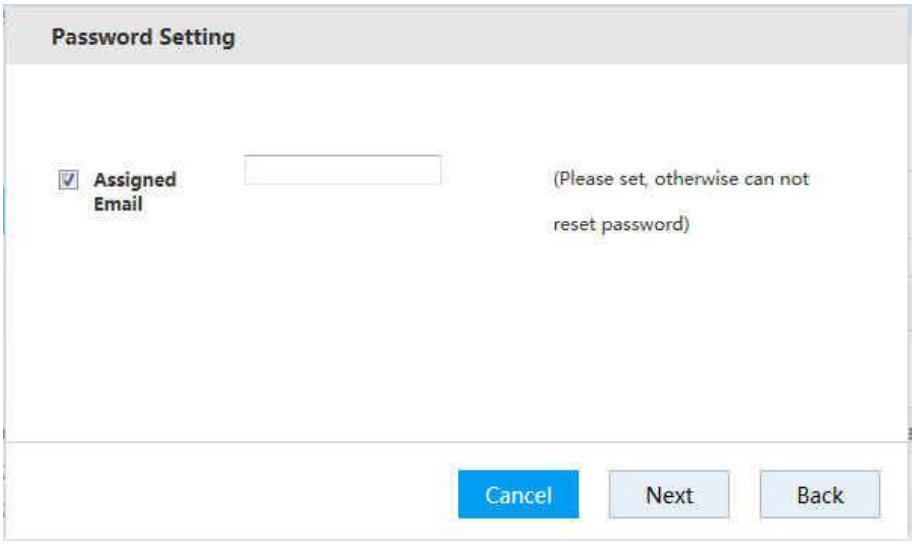


- When selecting **Using current device password and email info**, the remote device automatically uses the login password of the admin user. Click **Next** and the interface in Figure 3-55 is displayed. In this case, skip to Step 7 to continue.
- The new password can be set from 8 characters through 32 characters, and contains characters from at least two of the following categories: number, letter and special characters (including "!", "?", "@", "#", "$", "%", "+", "=", ".", ",", "*", "_", and "-").

Step 6 After manually setting the password, click **Next**. The system will prompts you to enter the assigned email. See Figure 3-54.

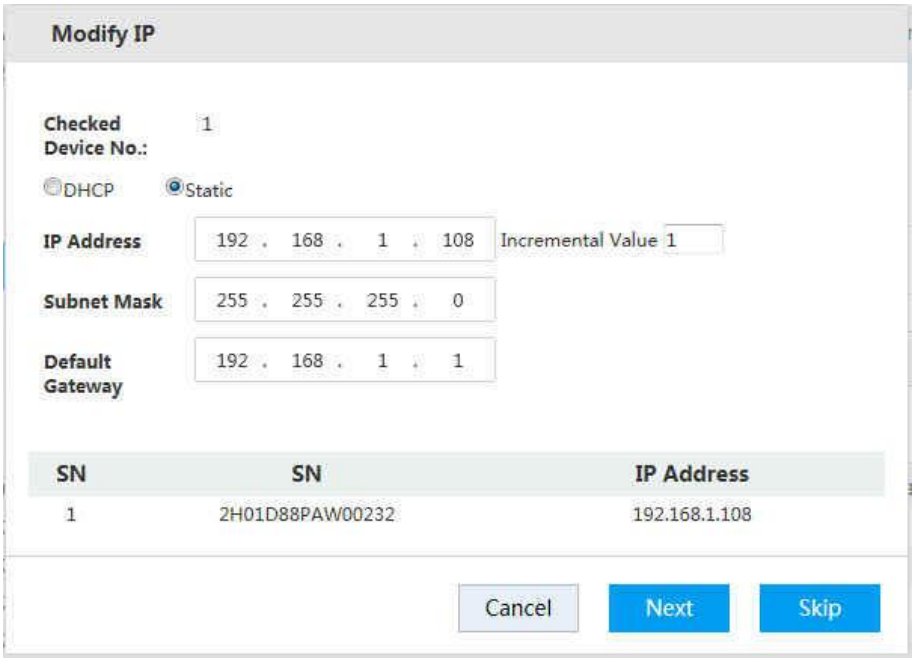
Enter the assigned email, and then click **Next**.

Figure 3-54 Password setting (3)



Step 7 The **Modify IP** interface is displayed. See Figure 3-55.

Figure 3-55 Modify IP interface



Step 8 Set the IP address of the remote device.

- When selecting **DHCP**, you do not need to enter IP address, subnet mask, and default gateway. The system automatically assigns an IP address to the remote device.
- When selecting **Static**, you need to enter IP address, subnet mask, and default gateway. To assign IP addresses to remote devices, the system increments according to the fourth section of the IP address.

- When modifying IP addresses of multiple remote devices at the same time, if the addresses are not in the same network segment, the system will change them to the same segment.

- When modifying static IP addresses, if the addresses conflict, the system will prompt the user for IP conflict. If the addresses are modified in batches, the system will skip the conflicting IP, and re-assign the addresses according to the incremental value.
- If you do not need to set the IP address of the remote device, click **Skip**. The system will start device initialization. See Figure 3-56.

Figure 3-56 Device Initialization interface

3.8.2 Modifying IP address

You can modify the IP address of the remote device that has not been added.

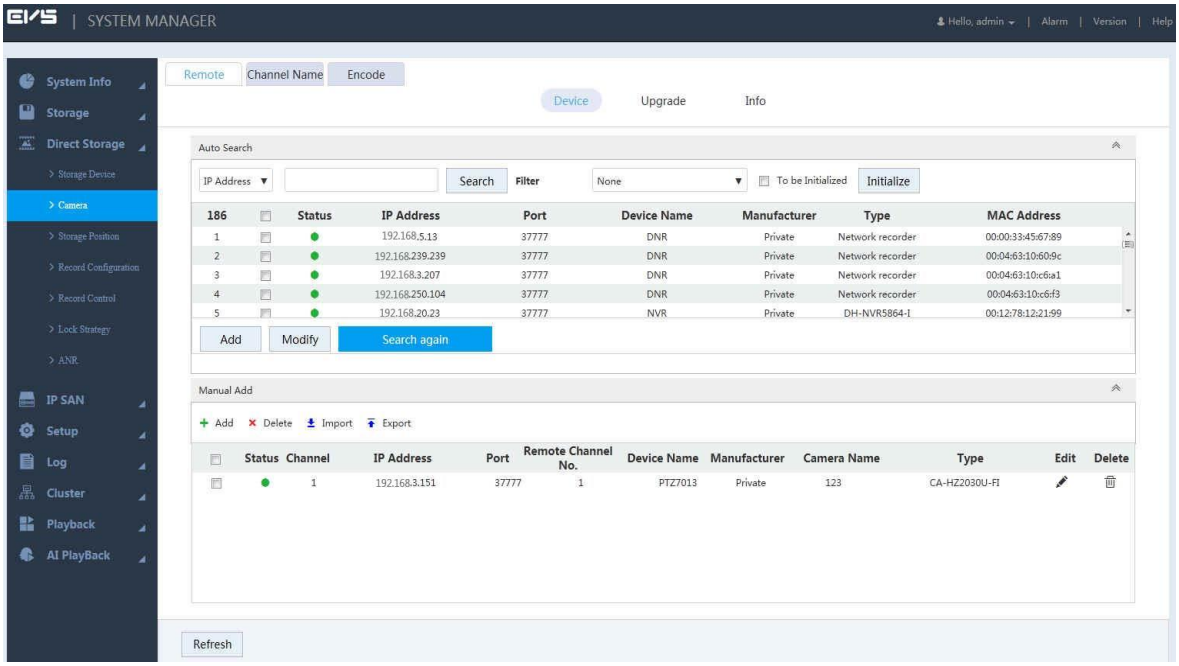
Step 1 Select **Direct Storage > Camera > Remote > Device**.

The **Device** interface is displayed.

Step 2 Click  at the right side of **Auto Search**.

The **Auto Search** interface is displayed. See Figure 3-57.

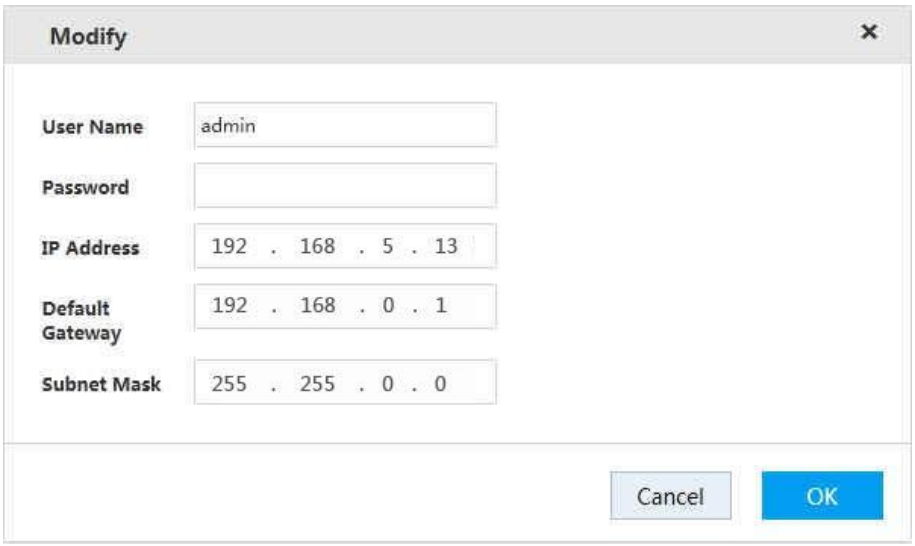
Figure 3-57 Device interface



Step 3 Select the remote device that needs to modify, and click **Modify**.

The **Modify** interface is displayed. See Figure 3-58.

Figure 3-58 Modify interface



Step 4 Enter the **User Name** and **Password** of the remote device, and set the **IP Address**, **Default Gateway**, and **Subnet Mask**.

Step 5 Click **OK** to save the configuration.

3.8.3 Importing/Exporting IP address

Importing IP Address

The system supports importing IP address.

Step 1 Select **Direct Storage > Camera > Remote > Device**.

The **Device** interface is displayed.

Step 2 Click . Find the file path, select the file to import, and click OK.

After completing import, the information imported will be shown in the list of devices added.

If the imported IP is duplicated with the IP of added remote device, the system will prompt whether to overwrite the added remote device. You can choose to overwrite or add new IP configuration as needed.

Exporting IP Address

The system supports exporting the entire list of devices added, and save it in the PC.

Step 1 Select **Direct Storage > Camera > Remote > Device**.

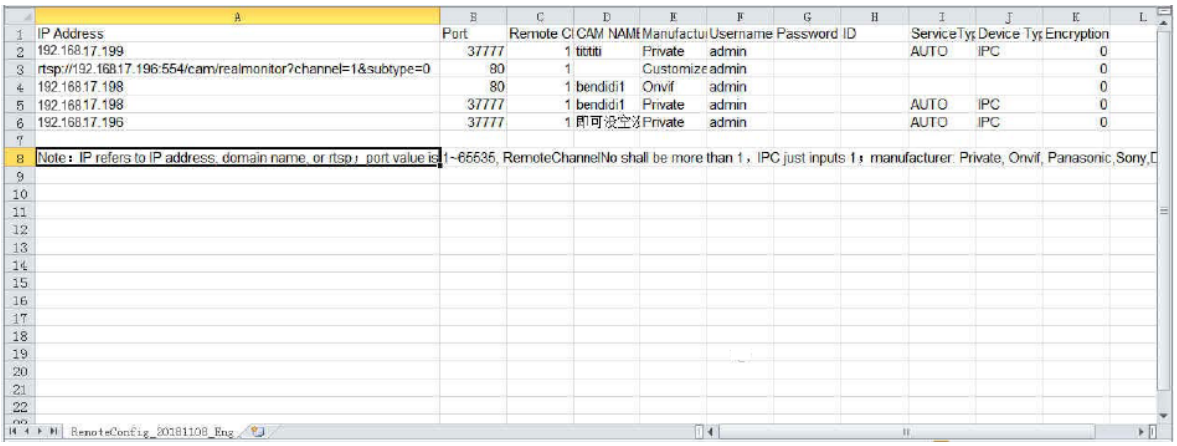
The **Device** interface is displayed.

Step 2 Click . The **File Backup Encrypt** interface is displayed. See Figure 3-59.

Figure 3-59 File Backup Encrypt interface

- The system selects **Open** by default. In this case, the exported file suffix is ".backup", which can only be opened on this device. It will not be able to open on other devices.
- If not select **Open**, the exported file suffix will be ".csv", which can be viewed and edited in Excel, see Figure 3-60. If encryption is set as "0", it means the channel closes encryption; if "1", it means the channel opens encryption.
- If you want to import the ".csv" file, fill in all the passwords in the Excel, otherwise, the import will fail.

Figure 3-60 Exported file



	IP Address	Port	Remote Cl	CAM NAME	Manufactur	Username	Password	ID	ServiceTyp	Device Typ	Encryption
2	192.168.17.199	37777	1	tititi	Private	admin			AUTO	IPC	0
3	rtsp://192.168.17.196:554/cam/realmonitor?channel=1&subtype=0	80	1		Customize	admin					0
4	192.168.17.198	80	1	bendidi1	Onvif	admin					0
5	192.168.17.198	37777	1	bendidi1	Private	admin			AUTO	IPC	0
6	192.168.17.196	37777	1	即可设定义	Private	admin			AUTO	IPC	0
8	Note：IP refers to IP address, domain name, or rtsp；port value is	1~65535, RemoteChannelNo shall be more than 1；IPC just inputs 1；manufacturer: Private, Onvif, Panasonic, Sony,D									

Step 3 Select the save path of the exported file, and click **OK**.

IP export succeeded.

The exported file suffix is ".csv", and the information of IP address, port, remote channel, camera name, manufacturer, username, password, service type, device type, and encryption will be included.

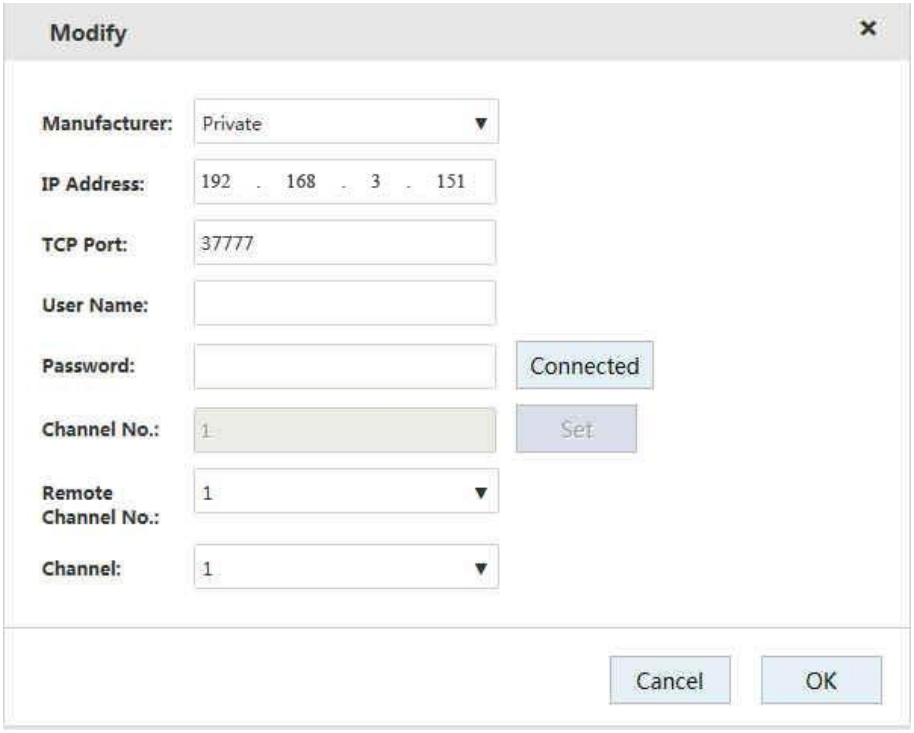
3.8.4 Editing Remote Device

You can modify or delete remote devices added.

- Click , the **Modify** interface is displayed. See Figure 3-61.

  You can modify the information of the remote device. For details, see Table 3-5.

Figure 3-61 Modify interface



- Select the device, and click or to delete the device.

3.8.5 Upgrading Remote Device

The system supports upgrading the remote device on web interface.

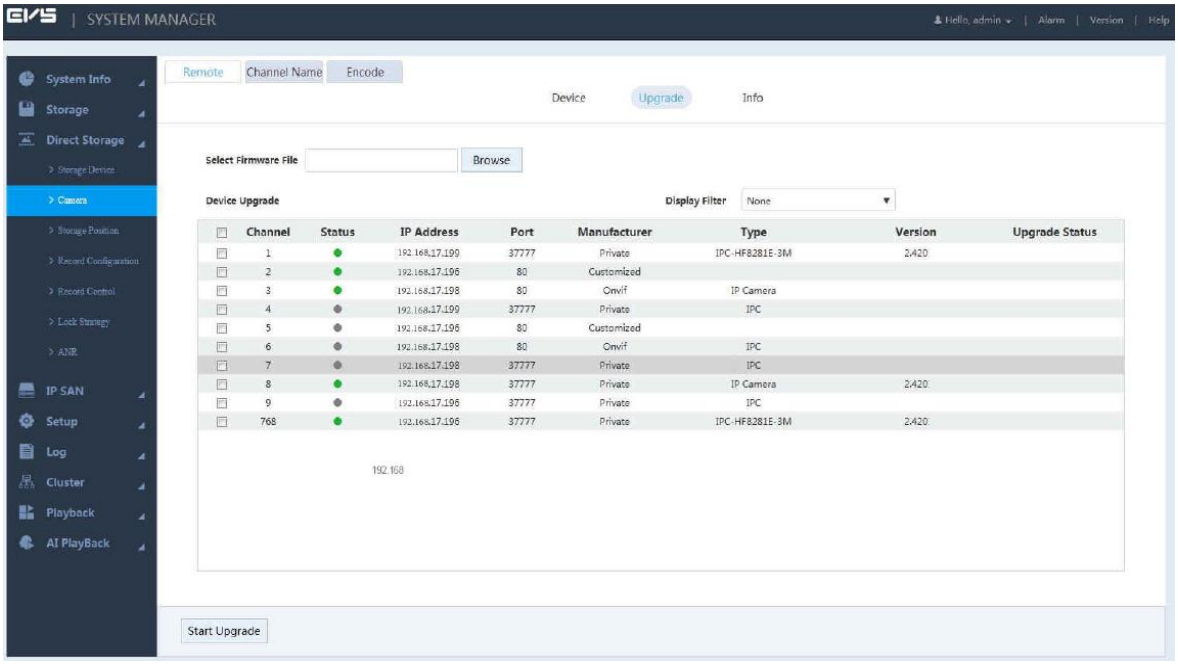
Preparation

You need to obtain the firmware file related to the device before upgrading.

Step 1 Select **Direct Storage > Camera > Remote > Upgrade**.

The **Upgrade** interface is displayed. See Figure 3-62.

Figure 3-62 Upgrade interface



Step 2 Select the device you want to upgrade.

- The system only supports upgrading devices with , and supports simultaneous upgrading of 8 devices at most.
- If there are lots of remote devices, you can set **Type** to select the device(s) you want to upgrade.

Step 3 Click **Browse** to import the firmware file.

Step 4 Click **Start Upgrade**, and the system starts device upgrading.

3.8.6 Viewing information

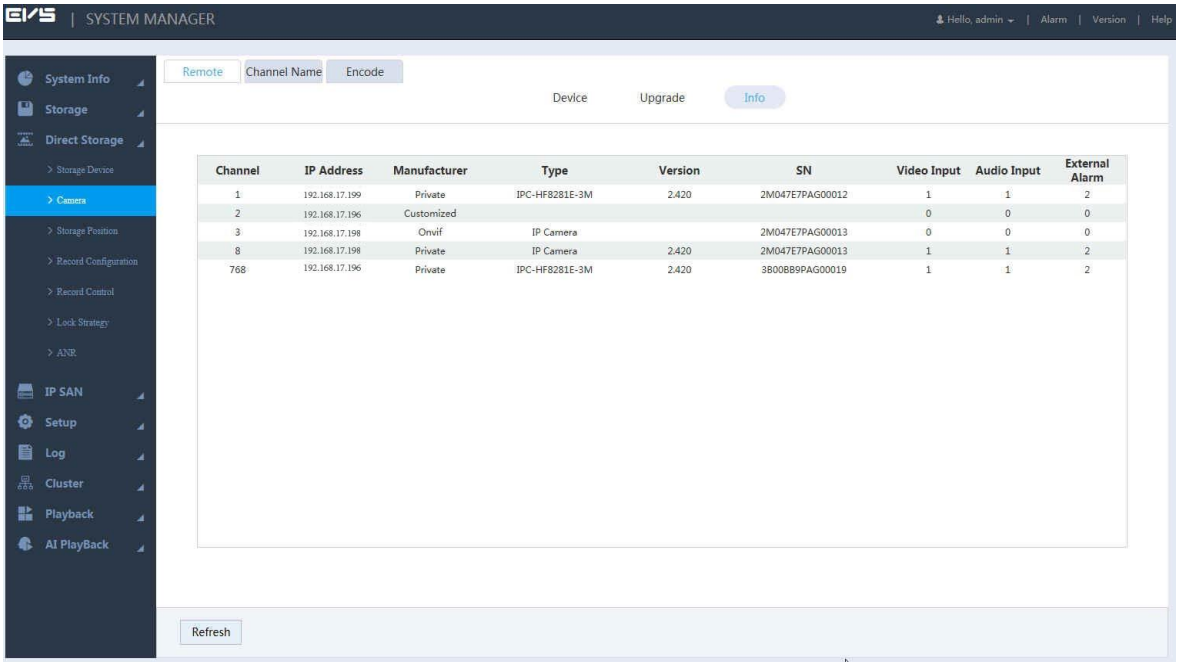
View the information of the remote device, such as channel, IP address, manufacturer, type, version, SN, video input, audio output, and external alarm.

Select **Direct Storage > Camera > Remote > Info**.

The **Info** interface is displayed. See Figure 3-63.

- You can click **Refresh** to update the information of remote device.

Figure 3-63 Info interface



3.8.7 Setting Channel Name

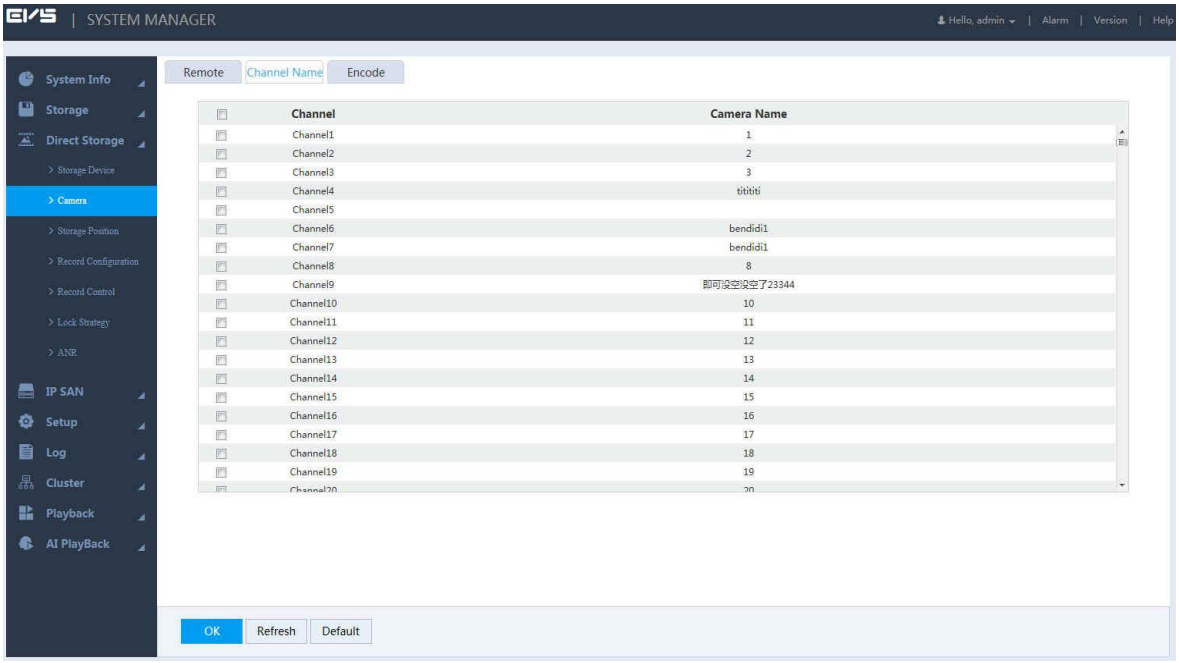
The system supports setting the channel name of remote device.

Select **Direct Storage > Camera > Channel Name**.

The **Channel Name** interface is displayed. See Figure 3-64.

Double-click the camera name of the channel that you want to set, and then modify the name.

Figure 3-64 Channel Name interface



3.8.8 Setting Encoding Parameters

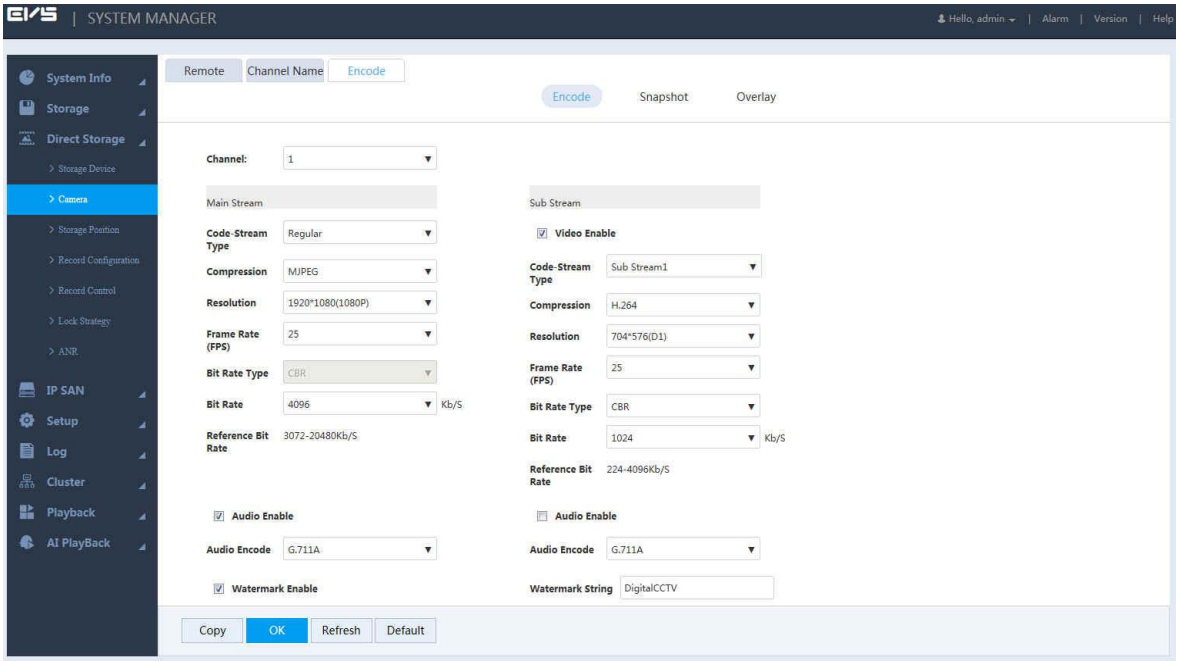
You can set video encoding parameters, including the video stream, image stream, and video overlay.

3.8.8.1 Setting video stream parameters

Step 1 Select **Direct Storage > Camera > Encode > Encode**.

The **Encode** interface is displayed. See Figure 3-65.

Figure 3-65 Encode interface



Step 2 Configure the parameters. See Table 3-16.

Table 3-16 Video stream parameters

Parameter	Description
Channel	Select the channel number.
Video Enable	Select the **Video Enable** check box to enable the video function of the sub stream.
Code-Stream Type	Select the stream type of the record. Main stream supports regular, MD and alarm. Sub stream only supports regular stream.
Compression	Select the encoding mode of the video stream. ● H.264: Main Profile encoding mode. ● H.265: Main Profile encoding mode. ● MJPEG: It needs high stream value to guarantee the image quality. It is recommended to use the max value of the reference stream.
Resolution	The higher the resolution, the better the image quality.
Frame Rate (FPS)	The higher the frame rate, the more fluent the image. FPS varies with the resolution.
Bit Rate Type	Select the stream control type of the video. ● CBR: The bit rate changes slightly close to the set value. ● VBR: The bit rate varies with the monitoring scenario. ● It is recommended to select CBR when the monitoring scenario changes slightly, and select VBR when the scenario changes significantly. ● MJPEG only corresponds to CBR.

Parameter	Description
Bit Rate	● Main stream: Set the bit rate to change the image quality. The larger the value, the better the quality. The reference bit rate provides the best bit rate range. ● Sub stream: In CBR, the bit rate changes slightly close to the set value. In VBR, the bit rate automatically changes with the image and keeps the max value close to the set number.
Reference Bit Rate	The system recommends the best bit rate range according to the configured resolution and FPS.
Audio Enable	Select the check box, and then the record is a file that combines video and audio streams.
Audio Encoding	Select the audio encoding format.
Watermark Enable	Select the check box to see if the record is tampered. For details of watermark verification, see "3.11.3Record Verification."
Watermark String	Enter the string for watermark verification. The default string is DigitalCCTV. The watermark string only consists of number(s), letter(s), underline(s) and strikethrough(s), and contains 128 characters at most.
Copy	After setting a channel, click **Copy**, and you can apply the settings to other channels.

Step 3 Click **OK** to save the configuration.

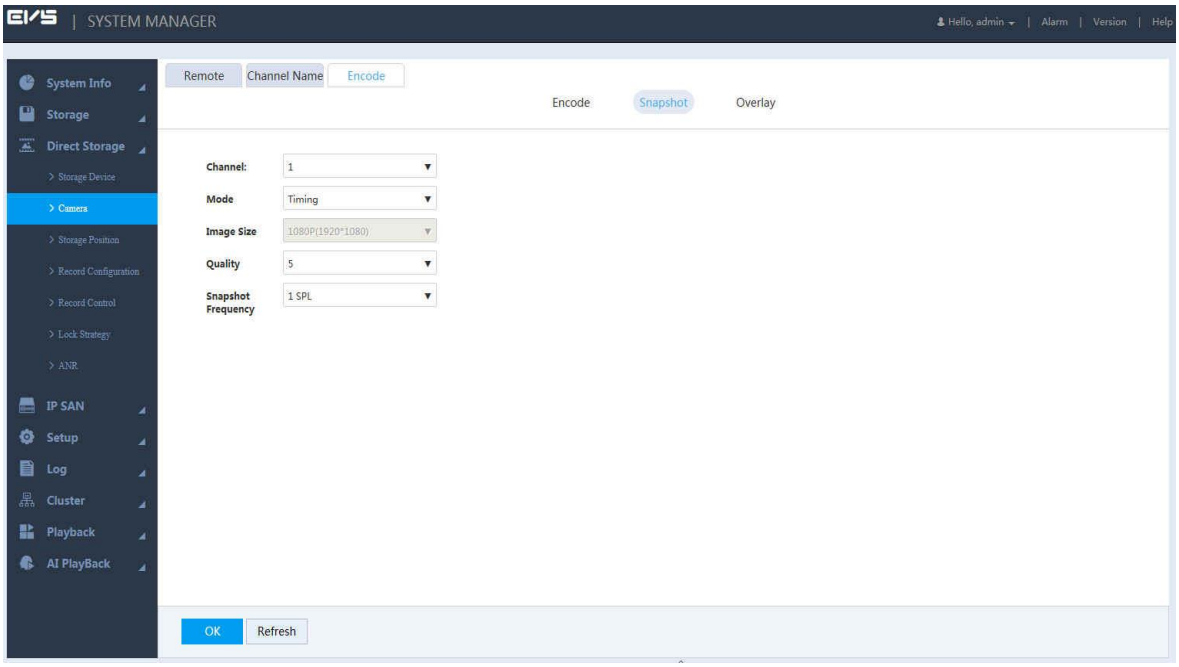
3.8.8.2 Setting Image Stream

You can set the image stream parameters, including snapshot mode, image size, image quality, and snapshot frequency.

Step 1 Select **Direct Storage > Camera > Encode > Snapshot**.

The **Snapshot** interface is displayed. See Figure 3-66.

Figure 3-66 Image stream



Step 2 Configure the parameters. For details, see Table 3-17.

Table 3-17 Image stream parameters

Parameter	Description
Channel	Select the channel number.
Mode	Select the snapshot mode, including **Timing** and **Trigger**. ● Timing: Takes snapshot according to the set plan. For details, see "3.4.3.2 Setting Snapshot Plan." ● Event: Takes snapshot according to the set triggering events. For details, see "3.9 Configuring Events."
Image Size	The snapshot image size keeps consistent with the resolution of the main stream set in **Encode** of remote device.
Quality	Select the quality level of the snapshot image (Level 1–Level 6). The larger the value, the better the quality.
Snapshot Frequency	The default value is from 1 SPL to 7 SPL. Select **Customized** to define the frequency by yourself. You can set up to 3600 SPL.

Step 3 Click **OK** to save the configuration.

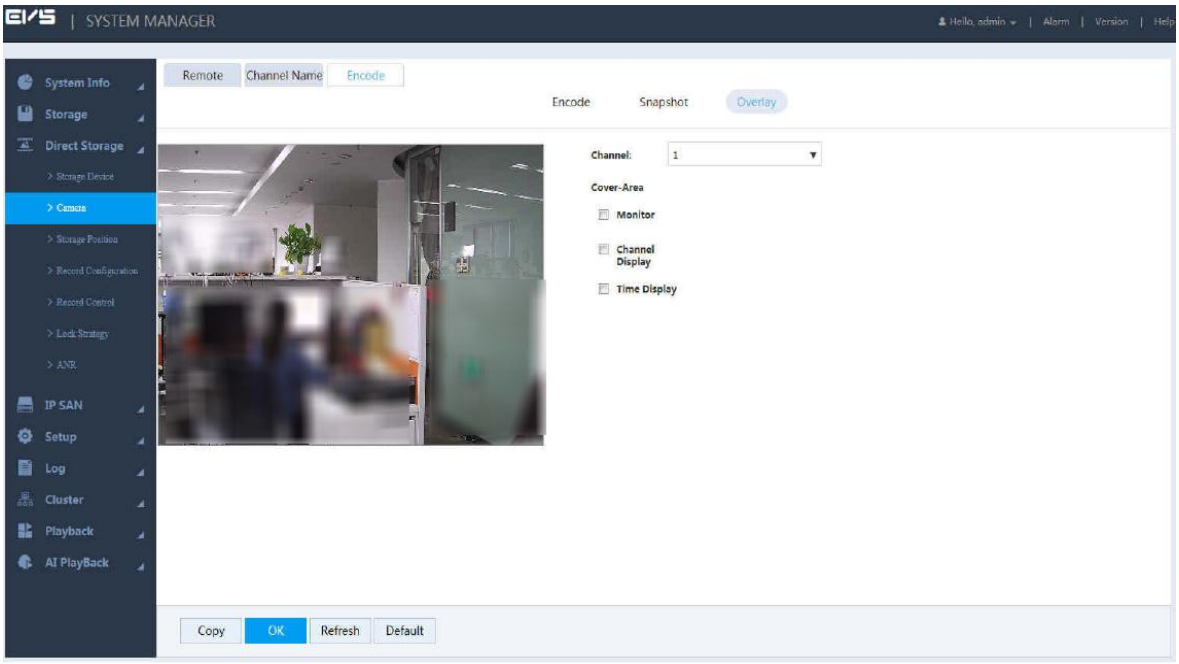
3.8.8.3 Setting Video Overlay

You can set the information of video overlay, including channel number, cover area, channel display, and time display.

Step 1 Select **Direct Storage > Camera > Encode > Overlay**.

The **Overlay** interface is displayed. See Figure 3-67.

Figure 3-67 Overlay interface



Step 2 Configure the parameters. For details, see Table 3-18.

Table 3-18 Video overlay parameters

Parameter	Description
Channel	Select the channel number.
Cover-Area	Select an area in the monitor screen as the cover-area. The area will be blocked and unavailable to view. 1. Select the **Monitor** check box. 2. Click **Set** at the right side. 3. Click **Add** to add cover-area in the monitor screen. ● Drag any corners of the cover-area to change the size of the area. ● Select and drag the cover-area to change the position of the area. ● Click **Clear** to clear all the areas. ● Select the cover-area, and click **Delete** to delete the selected area. ● Each channel supports up to four cover-areas. 4. Click **OK** to save the configuration.
Channel Display Time Display	Displays the time or channel in the video screen. 1. Select **Channel Display** or **Time Display** check box. 2. Click **Set** at the right side. 3. Drag the time or channel description in the screen to the proper position. 4. Click **OK** to save the configuration. 5. Click **Refresh**, and then the time or channel you set is displayed.

Step 3 Click **OK** to save the configuration.

3.9 Configuring Events

You can configure the linkages of video detection, alarm events, and abnormal events. When the alarm is triggered, the Device automatically performs the pre-set linked actions.

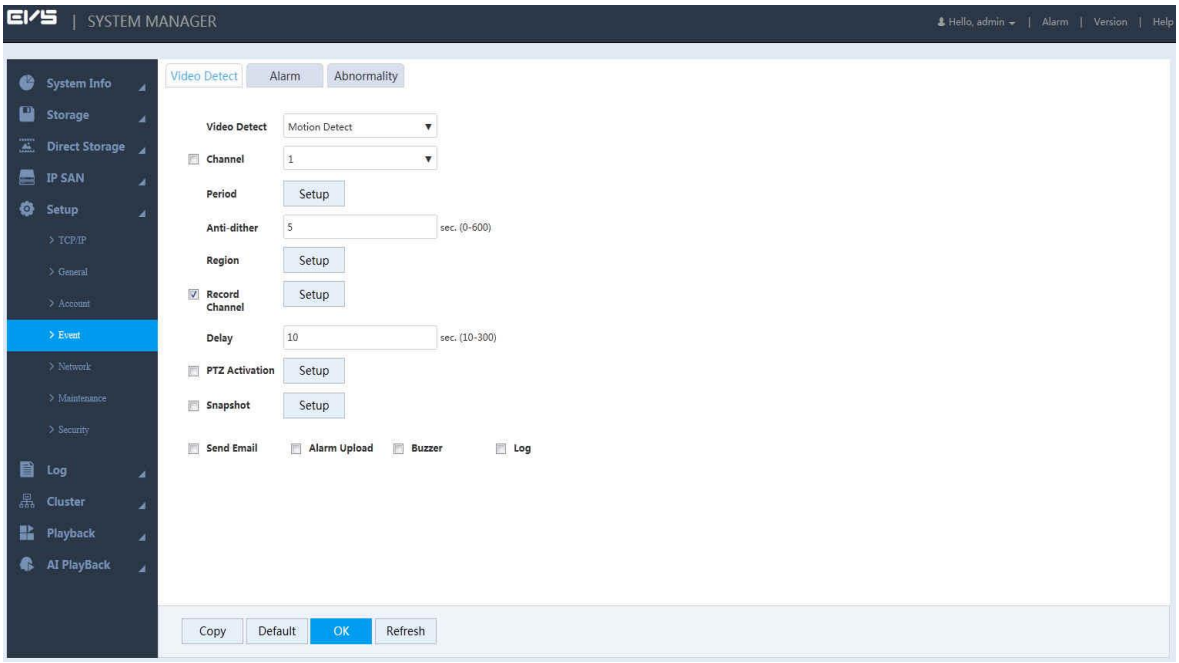
3.9.1 Video Detect

Video detect adopts computer vision and image processing technology. By analyzing the video images, it checks whether there is obvious change in the image. If yes (like object moves, image becomes fuzzy), the system performs alarm linkage.

Step 1 Select **Setup > Event > Video Detect**.

The **Video Detect** interface is displayed. See Figure 3-68.

Figure 3-68 Video detect



Step 2 Select the video detect type.

- Motion detect: When the moving target appears in the monitoring screen, and the moving speed reaches the pre-set sensitivity, the system performs alarm linkage.
- Video loss: After connecting the remote device, the system executes alarm linkage when it detects video loss in the remote device.
- Tampering: When the monitoring screen is covered by some object, resulting in the output of a single-color image, the system executes alarm linkage.

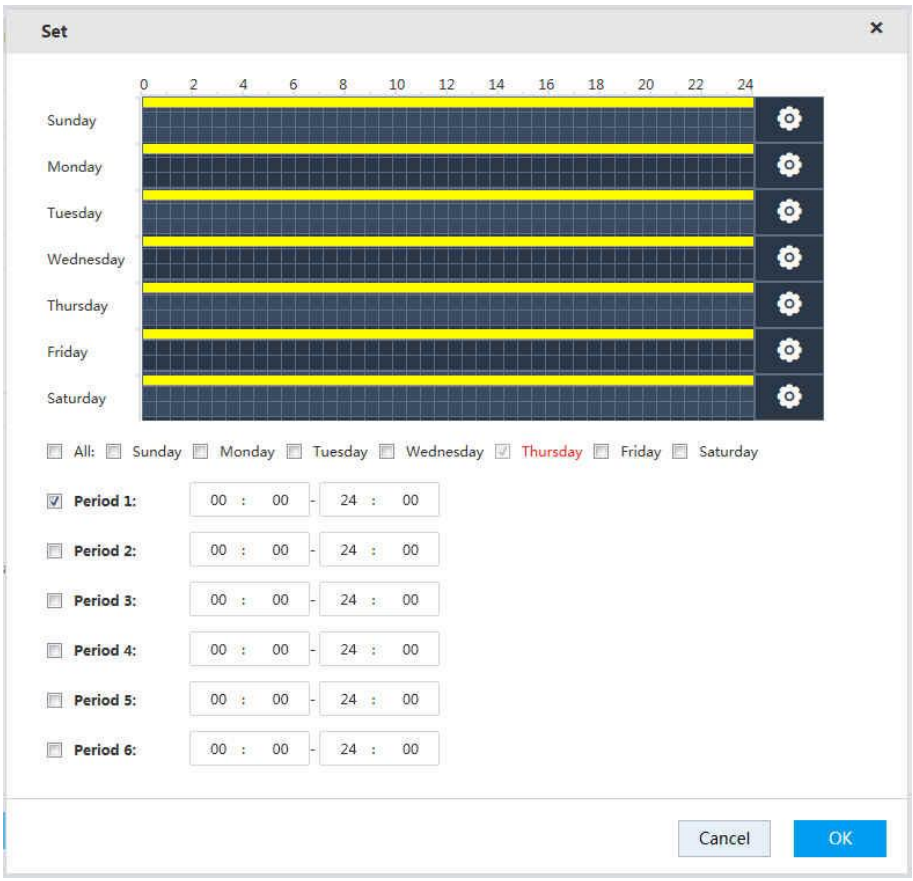
Step 3 Select the check box at the left side of **Channel**, and choose the channel number to enable video detection function.

Step 4 Set the **Period** of arm and disarm.

After setting, alarm linkage will be triggered during the set periods.

1. Click **Setup** at the right side of **Period**. The Setup interface is displayed. See Figure 3-69.

Figure 3-69 Period setup



2. Set the period of arm and disarm. You can use drawing and editing methods.

- Drawing: Hold down the left mouse button, and move the mouse in the time figure to choose the period.
- Editing: Click  corresponding to the day, select the check box of the corresponding period, and then enter the time value. Six periods are available for each day.

Select the check boxes of corresponding days, and you can set periods for multiple or all the days.

3. Click **OK** to save the configuration.

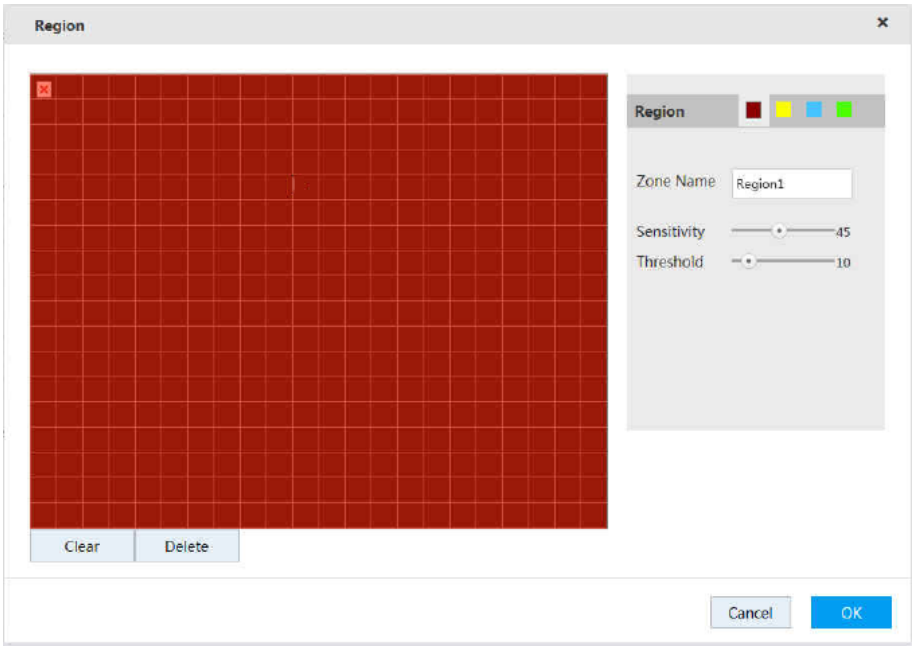
Step 5 Set the video detect region.

Only **Motion Detect** supports this function.

1) Click **Setup** at the right side of **Region**.
The **Region** interface is displayed. See Figure 3-70.

The region is made up of 22*18 (PAL) or 22*15 (NTSC) small regions.

Figure 3-70 Region interface



2) Select the region(s). Different regions are marked with different colors.

Different front-end devices support different number of regions. See the actual interface.

3) In the monitor screen, hold down the left mouse button and move the mouse to select the detect region.

- You can select multiple detect areas until the whole monitoring screen is selected.
- Channel alarm condition: if any one of the four regions triggers the alarm, the channel to which the area belongs triggers alarm.

4) Configure the parameters. For details, see Table 3-19.

Table 3-19 Region setting parameters

Parameter	Description
Zone Name	Enter the zone name to distinguish different zones.
Sensitivity	The higher the sensitivity, the more likely it is to trigger motion detection. Also, it is prone to increase false alarm rate, so it is recommended to keep the default value.
Threshold	When the percentage of the target/detect region which triggers alarm is larger than the set threshold, it triggers alarm. For example: The threshold is 10, and it triggers alarm when the detected target takes 10% of the whole detect region.

5) Click **OK** to save the configuration.

Step 6 Configure the parameters in Figure 3-71. For details, see Table 3-20.

Figure 3-71 Video detect interface

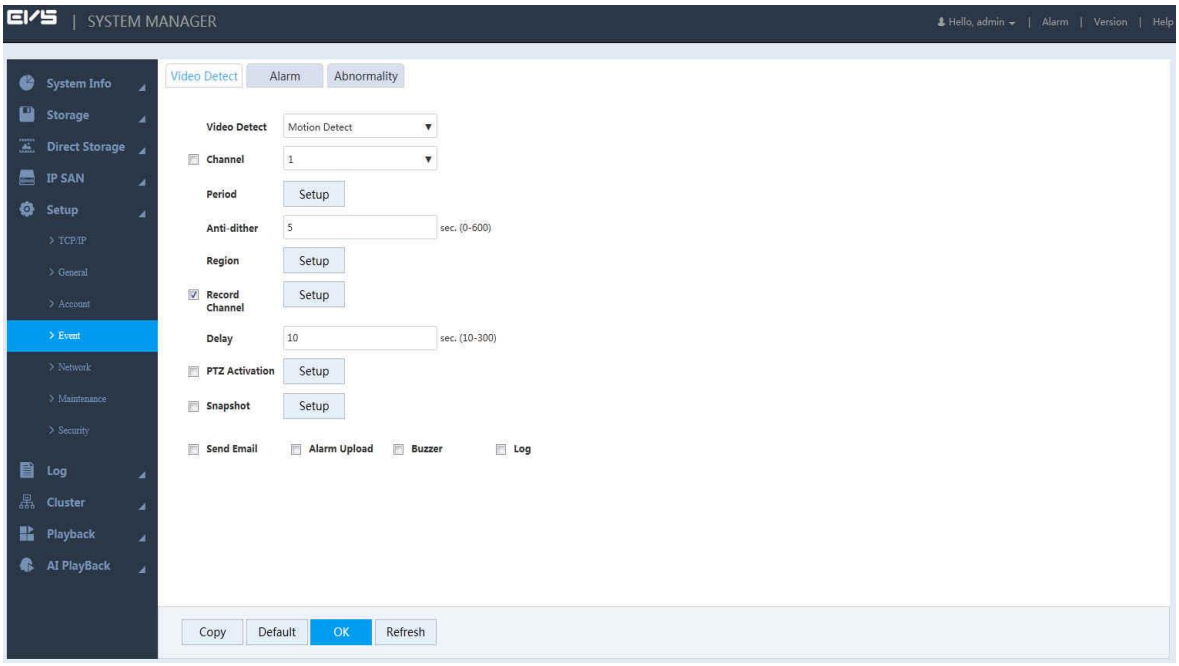


Table 3-20 Video detect parameters

Parameter	Description
Period	Alarm linkage works only in the set time period. For details, see "Period Setup."
Anti-dither	Only record the alarm event once during the set anti-dither time period. Only **Motion Detect** supports this function.
Record Channel	Select the check box, click **Setup** at the right side, and then select the channels as needed (multiple choices available). When an alarm occurs, the Device links to the selected channel for video recording. You need to configure record plan and enable auto record function. For details, see "3.4.3.1 Configuring Record Plan" and "3.4.4 Enabling Record Function."
Delay	The record delays for a short time when the alarm finishes. The range is 10–300 seconds.
PTZ Activation	Select the check box, click **Setup** at the right side, and then select the channel and action. When an alarm occurs, the device links to the selected channel to perform the set action. ● **Motion Detect** only supports pre-set PTZ point. ● Corresponding PTZ actions need to be set first. For details, see "3.10.3 PTZ Console."

Parameter	Description
Snapshot	Select the check box, click **Setup** at the right side, and then select the channel. When an alarm occurs, the device links to the selected channel for snapshot. You need to set snapshot plan and enable auto snapshot function. For details, see "3.4.3.2 Setting Snapshot Plan" and "3.4.4 Enabling Record Function."
Send Email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. You need to set the Email first. For details, see "3.14.3.2.2 Email Settings."
Alarm Upload	Select the check box. The device uploads the alarm signal to the network (including alarm center) when an alarm occurs. Only some models support this function. See the actual device.
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.
Log	Select the check box. When an alarm occurs, the Device records the alarm information and saves it to the log.

Step 7 Click **OK** to save the configuration.

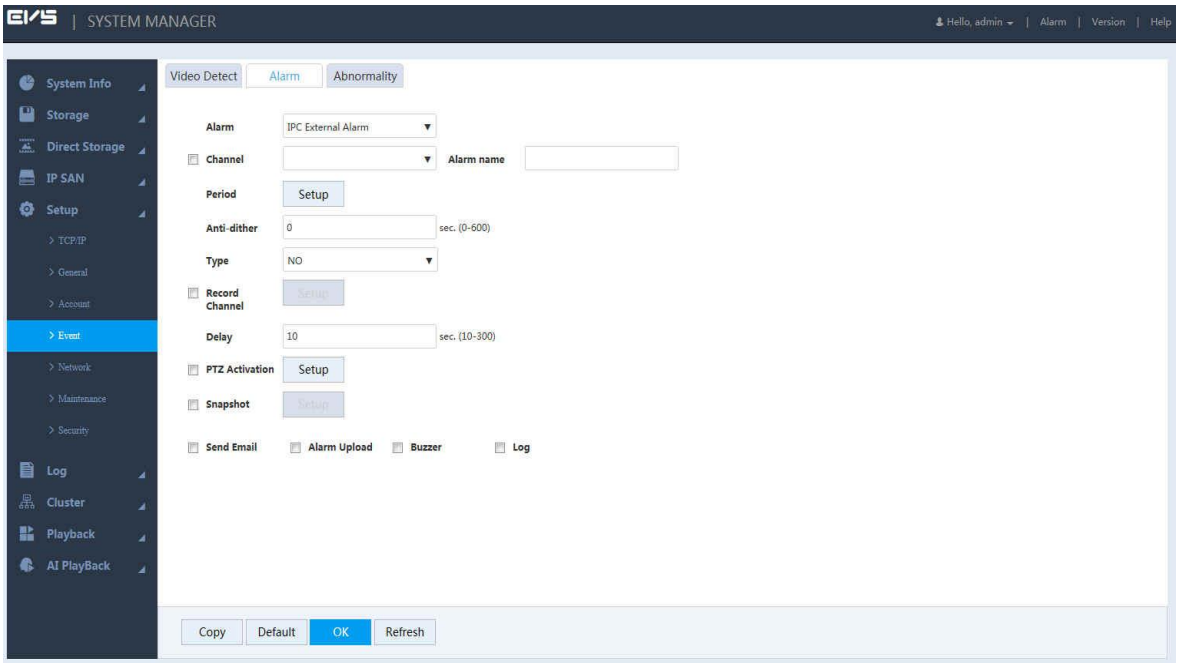
3.9.2 Setting Alarm

You can select different types of input according to different sources, and set the alarm output mode. It includes IPC external alarm and IPC off-line alarm.

Step 1 Select **Setup > Event > Alarm**.

The **Alarm** interface is displayed. See Figure 3-72.

Figure 3-72 Setting Alarm



Step 2 Configure the parameters. For details, see Table 3-21.

Table 3-21 Alarm setting parameters

Parameter	Description
Alarm	Select alarm type. ● IPC External Alarm: When the external alarm device of IPC triggers alarm, this alarm device uploads alarm signal to the Device through the network, and the system executes alarm linkage. ● IPC Offline Alarm: When the network connection between the Device and IPC is broken, the system executes alarm linkage.
Channel	Select the check box, and select the channel from the drop-down list. This operation enables the alarm function of the selected channel.
Period	Select the period of arm and disarm. For details, see Step 4 of "3.9.1 Video Detect."
Alarm Name	Select the name of alarm.
Anti-dither	Only record alarm event once during the set anti-dither time period.
Type	Select the type of the remote device, including NO and NC.
Record Channel	Select the check box, click **Setup** at the right side, and then select the channels as needed (multiple choices available). When an alarm occurs, the Device links to the selected channel for video recording. You need to configure record plan and enable auto record function. For details, see "3.4.3.1 Configuring Record Plan" and "3.4.4 Enabling Record Function."
Delay	The record delays for a short time when the alarm finishes. The range is 10–300 seconds.

Parameter	Description
PTZ Activation	Select the check box, click **Setup** at the right side, and then select the channel and action. When an alarm occurs, the device links to the selected channel to perform the set action. ● Corresponding PTZ actions need to be set first. For details, see "3.10.3 PTZ Console."
Snapshot	Select the check box, click **Setup** at the right side, and then select the channel. When an alarm occurs, the device links to the selected channel for snapshot. You need to set snapshot plan and enable auto snapshot function. For details, see "3.4.3.2 Setting Snapshot Plan" and "3.4.4 Enabling Record Function."
Send Email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. You need to set the Email first. For details, see "3.14.3.2.2 Email Settings."
Alarm Upload	Select the check box. When an alarm occurs, the device uploads the alarm signal to **Alarm** at the top right of the web page. Only some models support this function. See the actual device.
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.
Log	Select the check box. When an alarm occurs, the Device records the alarm information and saves it to the log.

Step 3 Click **OK** to save the configuration.

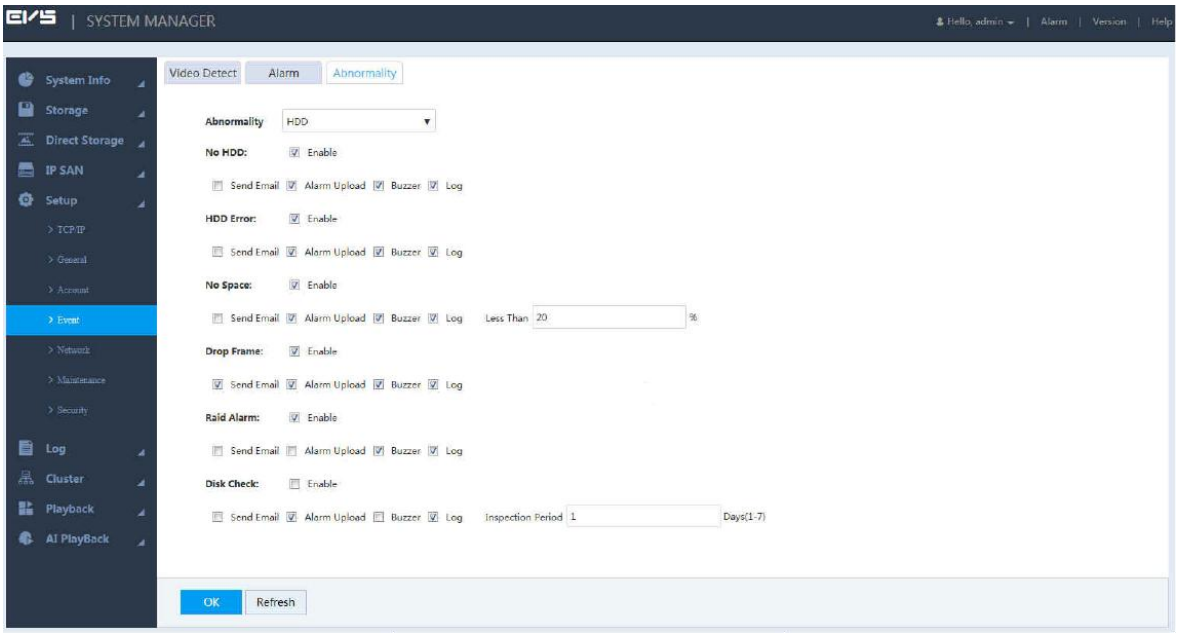
3.9.3 Handling Abnormality

You can set the alarm mode of abnormal events. When abnormal events occur during the operation of the Device, the system executes alarm linkage.

Step 1 Select **Setup > Event > Abnormality**.

The **Abnormality** interface is displayed. See Figure 3-73.

Figure 3-73 Abnormality handling



Step 2 Configure the parameters. For details, see Table 3-22.

Table 3-22 Parameters of abnormality handling

Parameter	Description
Abnormality	Select the type of abnormality. ● **HDD**: Configure the type and alarm way of HDD abnormal events, including no HDD, HDD error, no space, drop frame, RAID alarm, and disk check. With HDD error, hot spare failure, RAID degradation or failure, the system triggers alarm, and you need to change your HDD immediately. ● **Network**: Configure the type and alarm way of network abnormal events, including offline alarm, IP conflict and MAC conflict. ● **Shared Server Error**: Configure the type and alarm way of share service abnormal events, including abnormal share services and storage pool abnormality. ● **The Others**: Configure the type and alarm way of other abnormal events, including fan, temperature and power fault. ● **The Others** abnormal events of dual-control devices also support alarm of abnormal version. ● If platform is designed with the Device, it is necessary to configure the platform with alarm upload function. Check regularly the device and HDD alarms uploaded by web or the platform.
Enable	Select the check box to enable the corresponding abnormal event.

Parameter	Description
Send Email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. You need to set the Email first. For details, see "3.14.3.2.2 Email Settings."
Alarm Upload	Select the check box. When an alarm occurs, the device uploads the alarm signal to **Alarm** at the top right of the web page. Only some models support this function. See the actual device.
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.
Log	Select the check box. When an alarm occurs, the Device records the alarm information and saves it to the log.
Space	Free space of the HDD. An alarm occurs when the actual remaining free space of HDD is less than the percentage set. This function is available only when **No Space** is enabled.
Disk Check	The inspection interval of HDD. Range: 1–7 day(s).
Fan Alarm	Select the check box to enable fan alarm, and set the normal speed range of the fan. An alarm occurs when the fan speed is below the minimum or above the maximum. This function is available only when **The Others** is selected.
Temperature Alarm	Select the check box to enable temperature alarm, and set the normal temperature range. An alarm occurs when the temperature is below the minimum or above the maximum. This function is available only when **The Others** is selected.
Power Fault	Select the check box to enable power fault alarm. An alarm occurs when power fault happens. This function is available only when **The Others** is selected.

Step 3 Click **OK** to save the configuration.

3.10 Real-time Monitoring

Select **Playback > Preview**.

The **Preview** interface is displayed. See Figure 3-74. For details, see Table 3-23.

Figure 3-74 Real-time monitoring

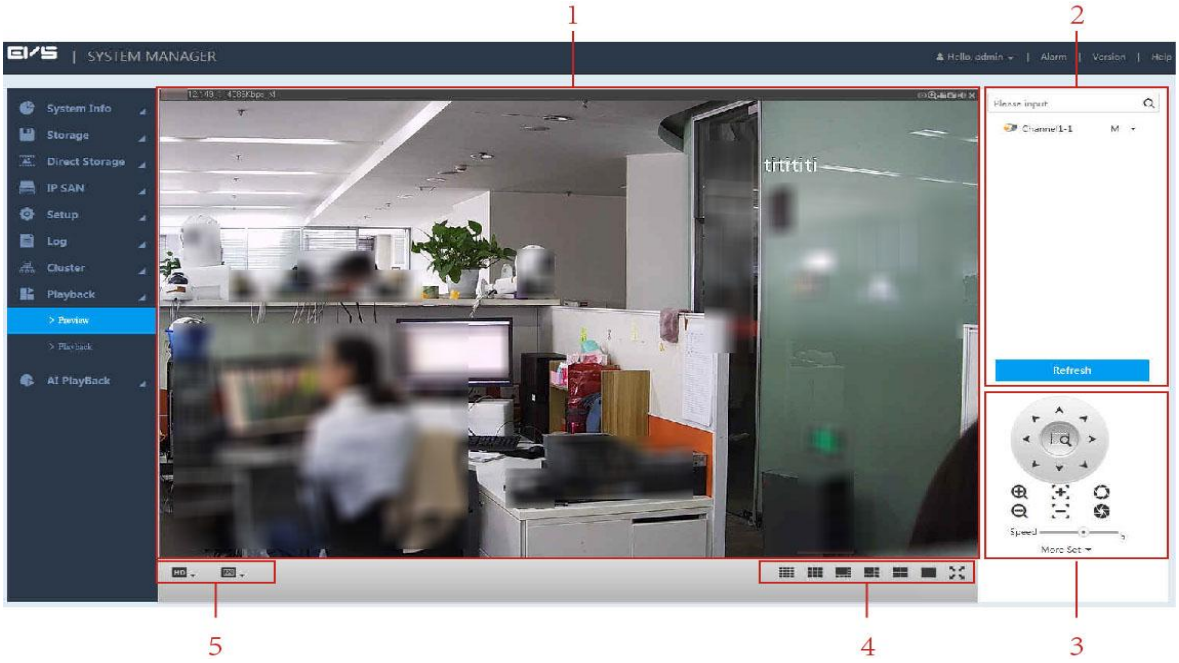


Table 3-23 Real-time monitoring

No.	Description
1	Real-time monitoring window. For details, see "3.10.1 Real-time Monitoring Window"
2	Monitoring channel list. For details, see "3.10.2 Monitoring Channel List."
3	PTZ console. For details, see "3.10.3 PTZ Console."
4	Switch the number of real-time monitoring windows. Icons from left to right: 16-screen, 9-screen, 8-screen, 6-screen, 4-screen, single-screen and full-screen.
5	Set the fluency and quality of real-time monitoring images. You can flexibly adjust the priority of image fluency or video real-time during real-time monitoring. Fluency emphasizes the smoothness of the video images, and real-time performance emphasizes video images in real-time, which can meet the needs of different users.

3.10.1 Real-time Monitoring Window

Click the remote device online in the monitoring channel list to open the real-time monitoring screen of this device. For the picture of real-time monitoring window, see Figure 3-75. For details, see Table 3-24.

- Click the drop-down list of the remote device in the monitor channel list to select the main stream or sub stream for real-time monitoring.
- If you want to select sub stream for real-time monitoring, the remote device needs to support and enable sub stream.

Figure 3-75 Real-time monitoring window

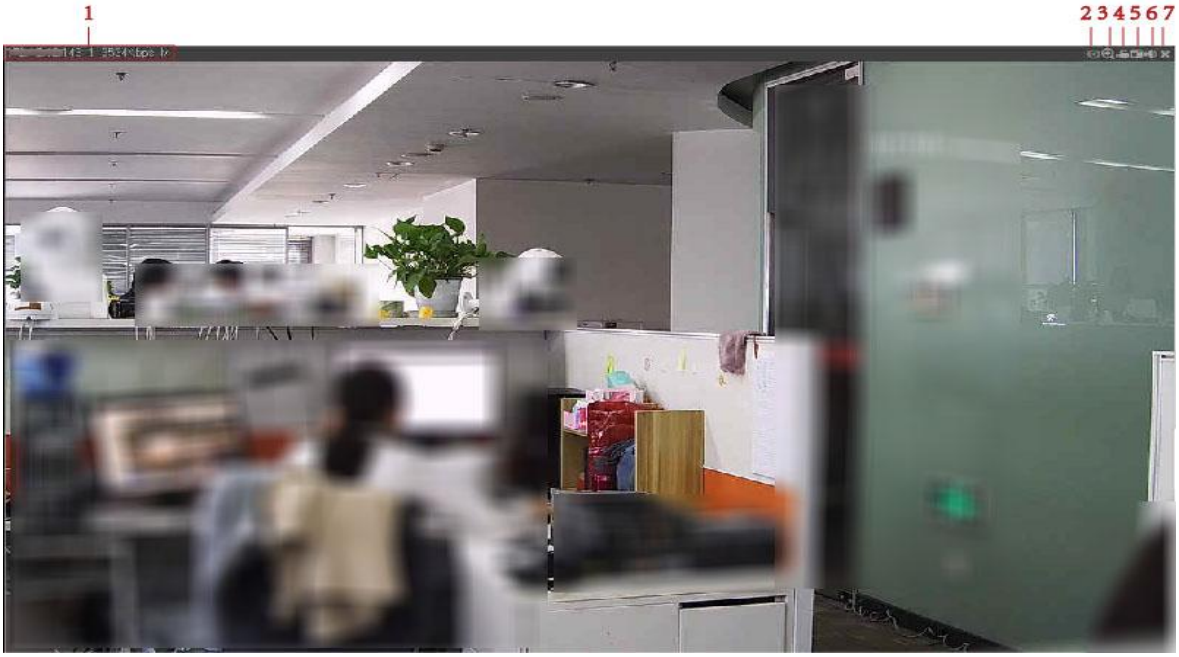


Table 3-24 Real-time monitoring window icons

No.	Name	Description
1	Stream	Displays the current stream value and decoding mode. M: main stream. S1: sub stream1. S2: sub stream2.
2	Fisheye	Click this icon to adjust the mounting mode and display mode of the fish-eye camera. For details, see "3.10.4 Fisheye."
3	Zoom	Partial enlargement. Click the icon, and drag the left mouse button in the video screen to select any area that will zoom in. Click this icon again or right-click to restore the original state.
4	Record	Local record. Click this icon to start recording. Click the icon again to stop it. The default storage path: C:\RecordDownload. For detailed operations to modify the default storage path, see "3.14.2.1 Setting General Information."
5	Snapshot	Picture snapshot. Click this icon to start snapshot. Click this icon again to stop snapshot. The default storage path: C:\PictureDownload. For detailed operations to modify the default storage path, see "3.14.2.1 Setting General Information."
6	Audio	Turn on/off audio. If the audio is off, there is no sound in the monitoring image.
7	Close	Close the current video.

3.10.2 Monitoring Channel List

For the monitoring channel list, see Figure 3-76. For details, see Table 3-25.

Figure 3-76 Monitoring channel list

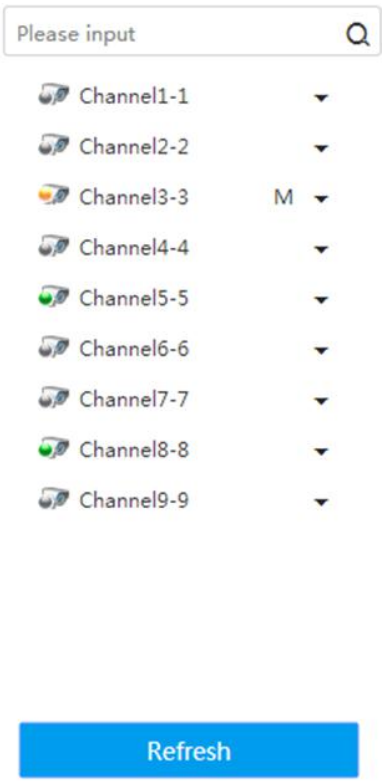
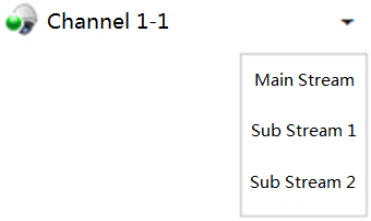


Table 3-25 Icons in the monitoring channel list

Icon/Parameter	Description
Please input	Enter the channel name in the text box, and click or press Enter. The system displays the items that meet the condition. Supports fuzzy queries. That is, enter any character of the channel name and the channel can be searched.
Channel state icon	Displays the state of the remote device corresponding to the current channel. ● Remote device is online. ● Remote device is offline. ● Remote device is playing real-time monitoring images.

Icon/Parameter	Description
	Click the drop-down list after the channel name to select the main stream or sub stream for play. If you want to select sub stream for real-time monitoring, the remote device needs to support and enable sub stream.
Refresh	Click this icon to refresh the list.

3.10.3 PTZ Console

Through the PTZ console, you can set the PTZ direction, step, zoom, iris, preset point, tour, pattern, scan boundary, light, wiper and horizontal rotation. See Figure 3-77.

- PTZ rotation supports 8 directions: Up, down, left, right, upper left, upper right, lower left and lower right.
- Click and then click any position of the monitor screen. The screen will adjust automatically centering on the mouse click.
- The larger the step size, the faster it rotates. For example, the speed of step 8 is much faster than that of step 1.
- Click **More Set** to configure the scan, preset point, tour and other auxiliary functions. For details, see 0.

Figure 3-77 PTZ console

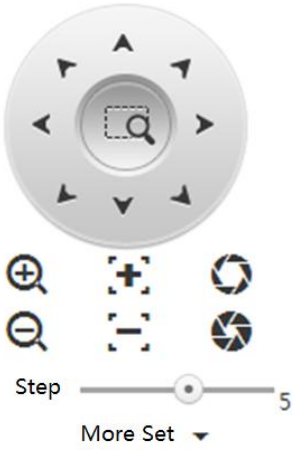


Table 3-26 PTZ parameters

No.	Parameter	Description
1	Preset	Set the preset points of the camera including details, add and delete. ● Add Turn the camera to the needed position, enter preset value in the **Preset** text box, and then click **Add** to add the preset point. ● Details Enter the preset value in the **Preset** text box and click **Details**. The camera automatically turns to the preset position. ● Delete Enter the preset value in the **Preset** text box and click **Del** to delete this preset point.
2	Scan	The camera starts linear scan according to the fixed boundaries. 1. Select **Scan** in the drop-down list and click **Set**. 2. Select the left boundary through the direction icon and click **Set Left** to confirm the left boundary. 3. Select the right boundary through the direction icon and click **Set Right** to confirm the right boundary. 4. Click **Start**. The camera starts rotation according to the set path.
3	Tour	The camera rotates among multiple preset points. ● Setting On the **Tour** interface, enter the value of tour path and click **Add**. Enter the value of preset, click **Add Preset** or **Del Preset**, and then you can add or delete preset points in the path.  You can repeatedly click Add Preset or Del Preset to add or delete preset points in this point path. ● Delete On the **Tour** interface, enter the value of tour path and click **Del** to delete this tour path. ● Start On the **Tour** interface, enter the value of tour path, click **Start**, and then the camera starts rotating according to the path.
4	Pattern	Set the camera to rotate according to a fixed process. See below: 1. Select **Pattern** in the drop-down list and enter the pattern value. 2. Click **Add**. Configure other settings on the main interface, such as zoom, focus, iris and direction. Return to the pattern interface and click **Stop** to complete the setting. 3. Click **Start**. The camera starts rotation according to the set pattern.
5	Pan	Select **Pan** in the drop-down list and click **Start**. The camera rotates 360° corresponding to the original position. Click **Stop** to end the rotation.

No.	Parameter	Description
6	AUX	Select **AUX** in the drop-down list and enter the value in the **Aux** box. Click **Aux On** to open the corresponding auxiliary function, and click **Aux Off** to close the function.
7	Light Wiper	Control light wiper switch of the external device through RS485. This function shall be supported by the external device.
8	Flip	Select **Flip** in the drop-down list and click **Flip**. The camera can vertically turn 180° corresponding to the original position.
9	Reset	Select **Reset** in the drop-down list, and click **Reset** to turn the camera back to the default position.

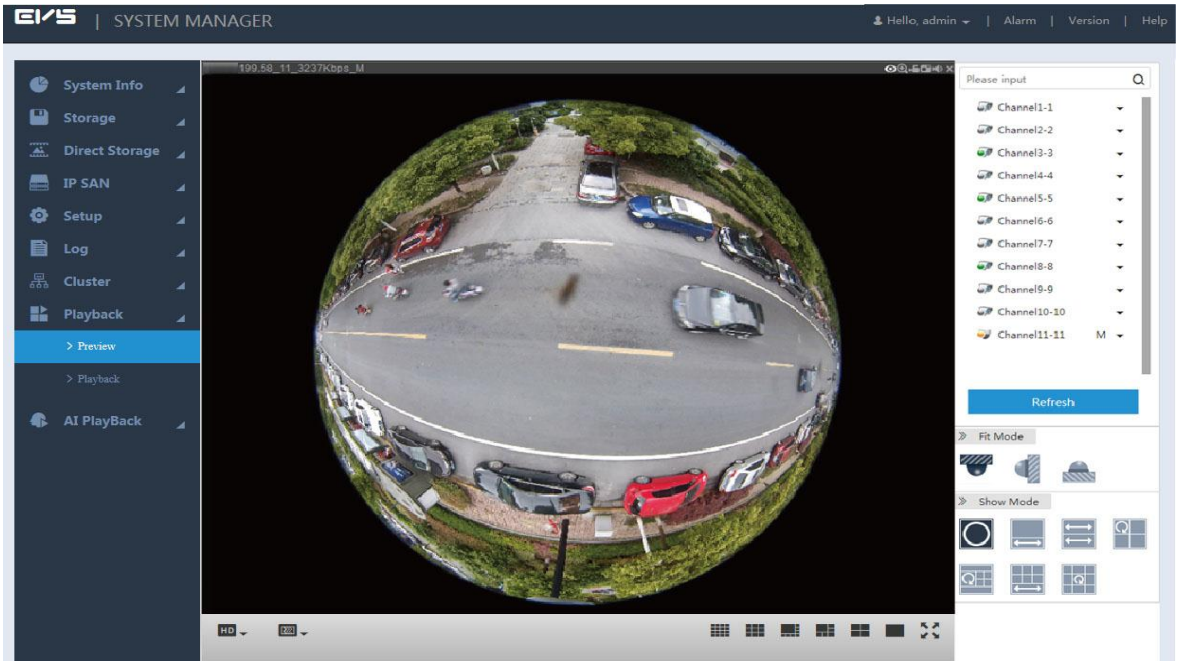
3.10.4 Fisheye

After opening the real-time monitoring screen, click  on the upper right corner of the window. The **Fisheye** interface is displayed. See Figure 3-78.

You can adjust the **Fit Mode** and **Show Mode.**

Only fisheye channel supports fisheye settings. If the current channel is not a fisheye channel, the system prompts that the channel **Doesn't support fisheye dewarping**.

Figure 3-78 Fisheye settings



Mounting modes include top, wall and ground. Different mounting modes support different display modes. For details, see Table 3-27.

Table 3-27 Fisheye mounting modes

Mounting Mode	Display Mode
Top/Ground Mounting	360° original panoramic image.
	One correction screen+ one panoramic drawing.
	Two panoramic drawings.

Mounting Mode	Display Mode
	One 360° panoramic image + three correction screens.
	One 360° panoramic image + four correction screens.
	Four correction screens + one panoramic drawing.
	One 360° panoramic image + eight correction screens.
Wall Mounting	360° original panoramic image.
	Panoramic drawing.
	One 360° panoramic image + three correction screens.
	One 360° panoramic image + four correction screens.
	One 360° panoramic image + eight correction screens.

Top-mounting one 360° panoramic image + four correction screens: you can do corrections for the colorful area in the right panoramic image, or move the mouse to adjust the position of the small images at the right side. See Figure 3-79.

Corrections available: Zoom in, zoom out, move and rotate the images with the mouse.

Figure 3-79 Operations of fisheye

3.11 Record Management

The system supports playback, download and management of record files.

3.11.1 Record Playback

Select **Playback > Playback > Playback**.

The **Playback** interface is displayed. See Figure 3-80. For details, see Table 3-28.

Figure 3-80 Playback interface

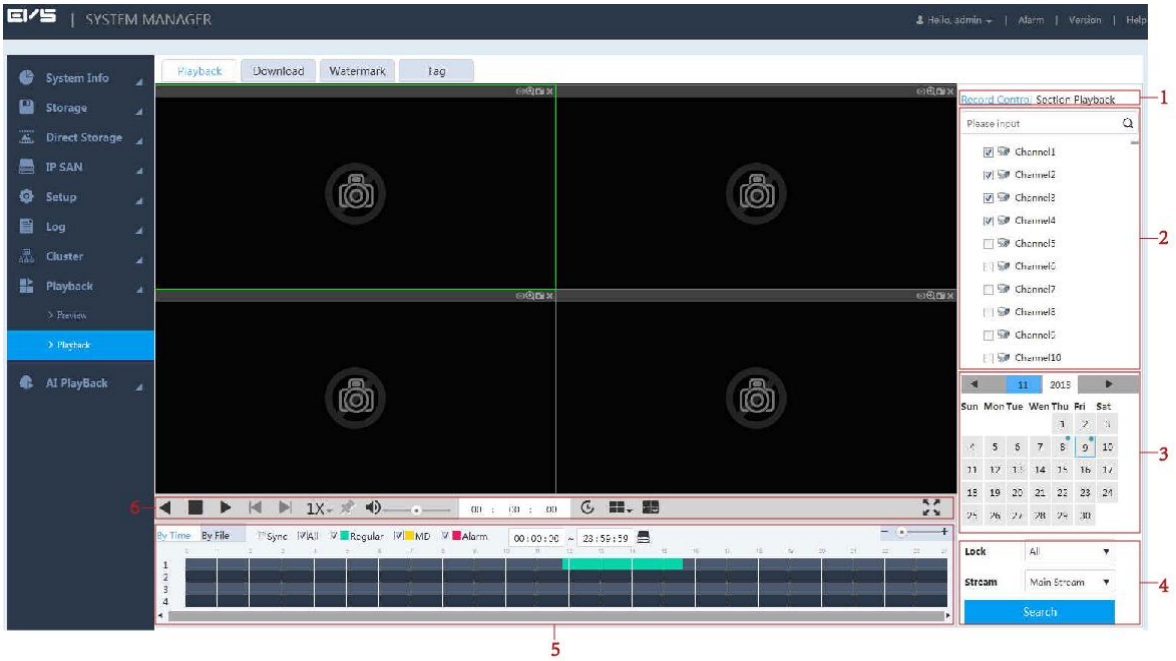


Table 3-28 Playback parameters

No.	Name	Description
1	Playback Type	Includes record control and section playback. ● Record control: Playback according to the stored record files. ● Section playback: Synchronously play multiple sections of the record file. This helps improve playback speed. For details, see "3.11.1.1 Section Playback."
2	Channel List	Select the channel(s). Enter the channel name into the text box, click or press Enter, and then the system displays the channels meeting the search condition.
3	Calendar	Click the date, and the record track of that day is updated on the timeline. Date with a blue point (6) means that the record file on that day is available.
4	Record Search	● Lock: Includes all, locked and mark. ● Stream: Includes main stream and sub stream.
5	Record Display List	Supports listing by time or by file, and record clip backup. For details, see "3.11.1.2 Record Display List."
6	Playback Control Bar	For details, see "3.11.1.3 Record Playback Control Bar."

3.11.1.1 Section Playback

Section playback refers to the sync play of multiple sections from a long record file. It can improve the playback speed and quickly position the needed video point to save your time.

The minimum time of playback section is no less than five minutes by default. If the section is less than five minutes, the system automatically reduces the playback screen(s). For example: a nine-minute record is set to play in four screens. In this case, the system plays the record in one screen, and the rest three screens have no image.

Step 1 Click **Section Playback** at the top right corner of the **Playback** interface.

Step 2 Click  and select the split screen number.

When you select different split numbers, the icons are different.
For details of screen split, see Table 3-29.

Table 3-29 Screen split icons

Icon	Description
	No split.
	Four split screens.
	Eight split screens.
	16 split screens.

Step 3 Select the channel needed for playback. Click  .

Section playback starts.

- Click the timeline, and the system starts playback from the pointed time.
- During the playback, the section mark (triangle) is displayed on the timeline.

3.11.1.2 Record Display List

Select the date with record, and the system displays record file by time and by file.

- Display by time: See Figure 3-81. Click any position on the timeline to play back the video record of corresponding time.
- Display by file: See Figure 3-82. Double-click the file name to play back the video record.

For details, see Table 3-30.

Records of different types are displayed in different colors on the timeline. : Regular, : Motion detection (MD), : Alarm.

Figure 3-81 Display by time

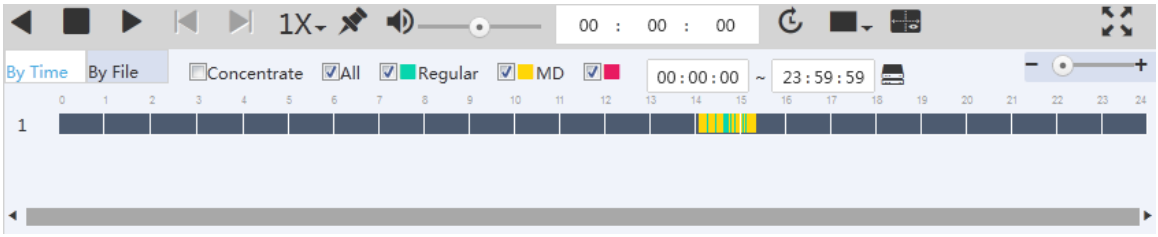


Figure 3-82 Display by file

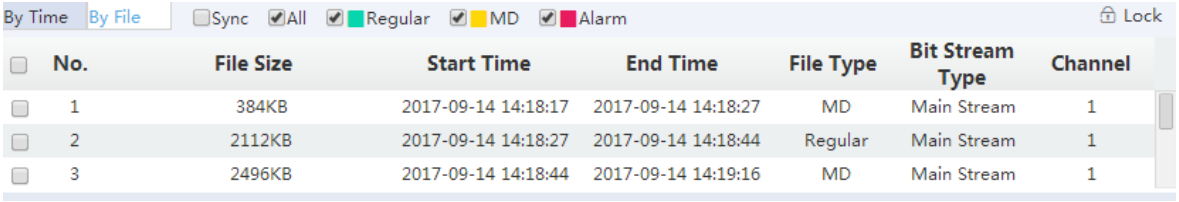


Table 3-30 Record display list

Icon	Description
By Time By File	Set the record display type: ● By Time: Displays record by timeline. See Figure 3-81. ● By File: Displays record by file list. See Figure 3-82.
Sync	By checking the Sync box, you can play videos of the same time recorded by different channels. Through the playback control bar, you can choose to simultaneously stop or speed up the video play. When switching to one screen, the icon changes into Concentrate. In this case, you can do concentrated playback. For details, see "3.11.1.5 Concentrated Playback."
All Regular MD Alarm	Select the check box and only the corresponding record files are displayed.
00:00:00 ~ 23:59:59	Clip a record and save it in PC. 1. Select a record file. 2. Select the start time on the timeline. Click to start clip. 3. Select the end time on the timeline. Click to end the clip. 4. Click , select storage path, and then store the clipped record.
− +	Adjust the time unit of the timeline.

Icon	Description
Lock	Lock a file to avoid overwriting. For details, see "3.11.1.4 Locking and Unlocking Files." This function is available only when displaying **By File**.

3.11.1.3 Record Playback Control Bar

For the record playback control bar, see Figure 3-83. For details, see Table 3-31.

Figure 3-83 Record playback control bar

Table 3-31 Icons on the record playback control bar

Icon	Description
	Play backward/Pause. ● To play backward, click . Then it starts to play backward, and the icon changes to . Click to stop playing backward. ● Click to back to normal playback state.
	Stop. Click this icon to stop playing the record.
	Play. Click this icon to start playing record and the icon changes to . Click to pause.
	Previous/next frame. ● When pausing record playback, click or to playback previous or next frame record. ● When playing single frame record, click (Play) or to back to normal playback state.
1X	Set playback speed, including 1×, 2×, 4×, 8× and 16×.
	Add a tag. During the playback, click this icon, enter the tag name, and then click **OK** to mark the record file. You can search the record by tag adding time and keywords, and playback the record. For details, see "3.11.4 Tag Management."
	Adjust the volume.

Icon	Description
00 : 00 : 00	Positioning. Set a time point and click to play the record from this time point.
	Screen split. Click this icon to set the screen split number, including 16, 9, 4 and 1 screen(s). Different models support different split numbers. See the actual interface displayed.
	IVS rule. Click this icon and the IVS rules set on the remote device are displayed. This function is available only when the remote device has set IVS rules.
	Full-screen display.

3.11.1.4 Locking and Unlocking Files

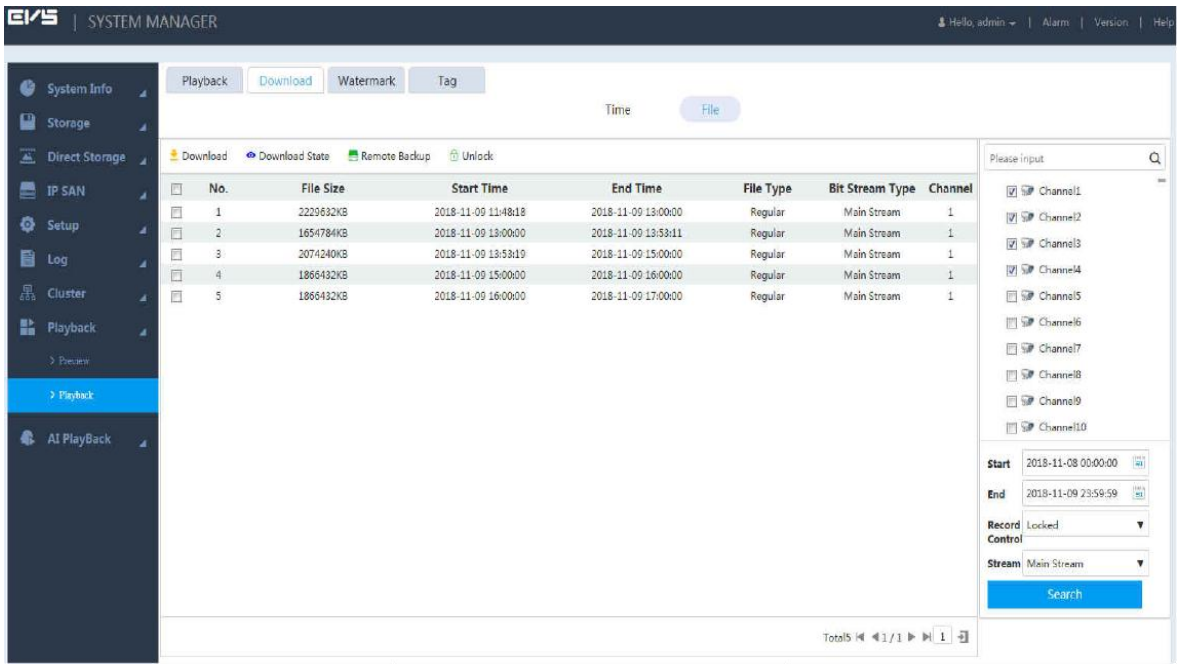
Step 1 Select **Playback > Playback > Download > File**.

Step 2 Select **Channel**, and configure **Start**, **End**, and **Stream**. Select **Locked** from the **Record Control** drop-down list.

Step 3 Click **Search**.

The locked files are displayed. See Figure 3-84.

Figure 3-84 Files to unlock



Step 4 Select the file(s) you want to unlock, and click to unlock.

3.11.1.5 Concentrated Playback

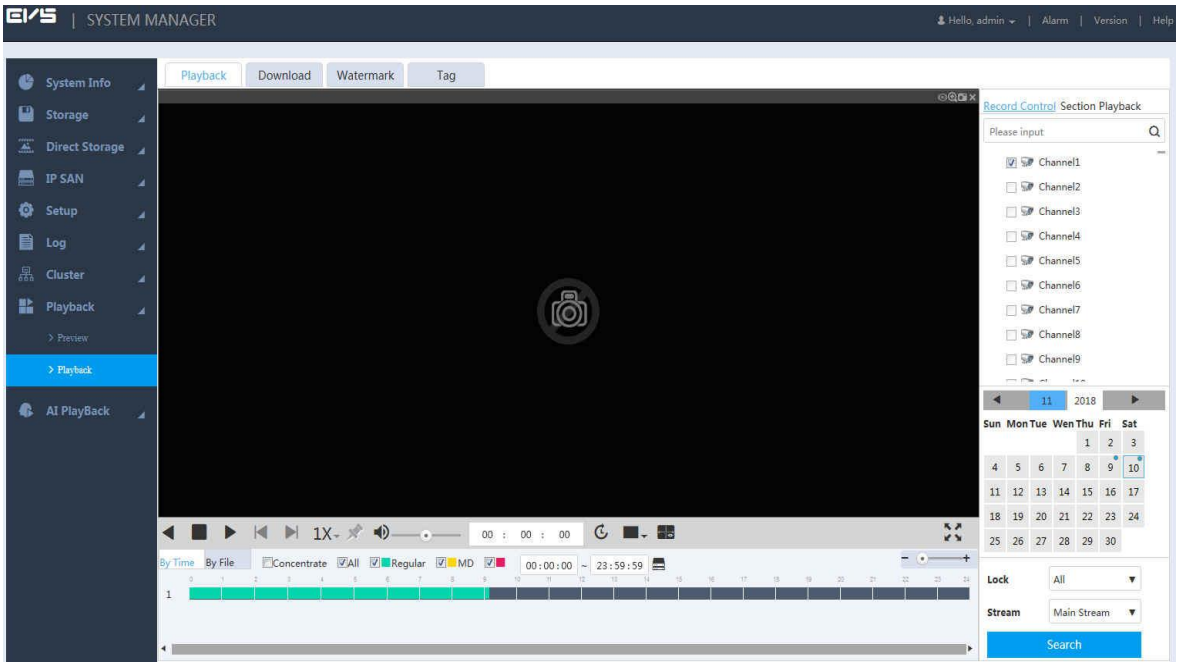
Concentrated playback refers to fast playback of record at 16× speed. It only restores to normal paly speed when the remote device has enabled smart alarm and alarm events happen.

- Only support one-screen concentrated.
- There is no voice during concentrated playback, and it will play next record automatically when the current record finishes playing.

Step 1 Select **Playback > Playback > Playback**.

The **Playback** interface is displayed. See Figure 3-85.

Figure 3-85 Playback interface



Step 2 On the **Playback** interface, select the channel and date of concentrated playback.

Step 3 Click to switch to single-screen play. You do not need to switch if it shows .

Step 4 Click , and it becomes . This enables IVS rules.

Step 5 Click Concentrate.

Step 6 Click , or the position with record on the timeline.

The system starts concentrated playback.

3.11.2 Record Download

The system supports downloading record by file or by time and stores it to PC or external USB.

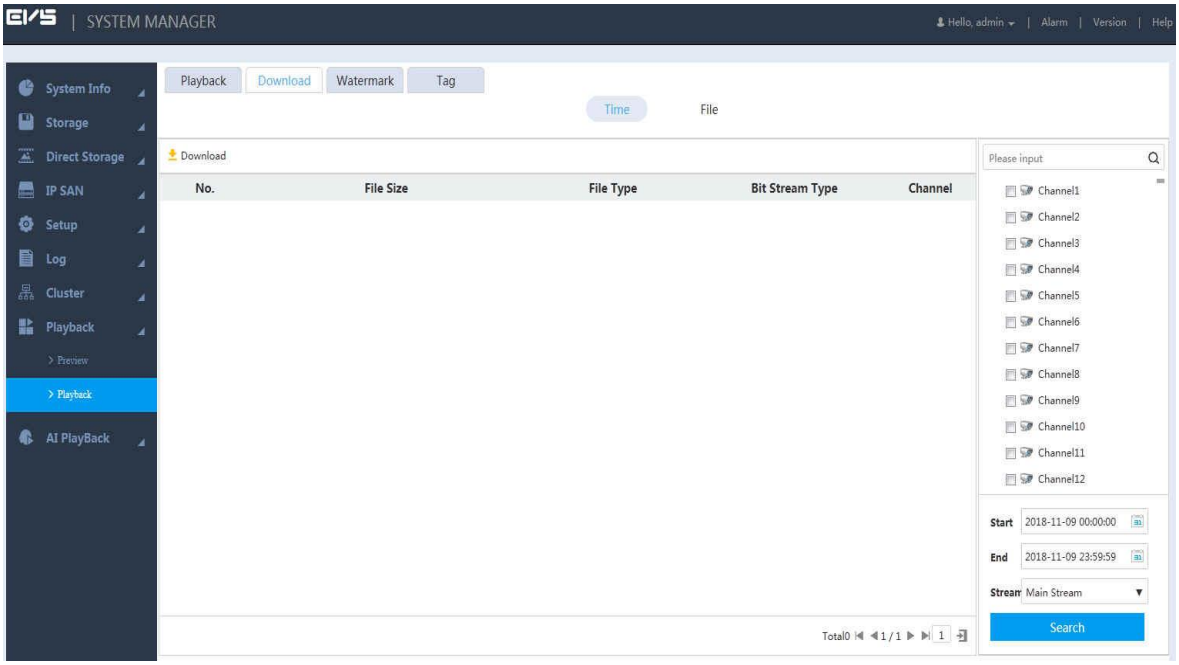
3.11.2.1 Download by Time

You can locally download video files according to the set record period, and other conditions like channel and stream type.

Step 1 Select **Playback > Playback > Download > Time**.

The **Time** interface is displayed. See Figure 3-86.

Figure 3-86 Time interface



Step 2 Select **Channel**, and configure **Start**, **End** and **Stream**.

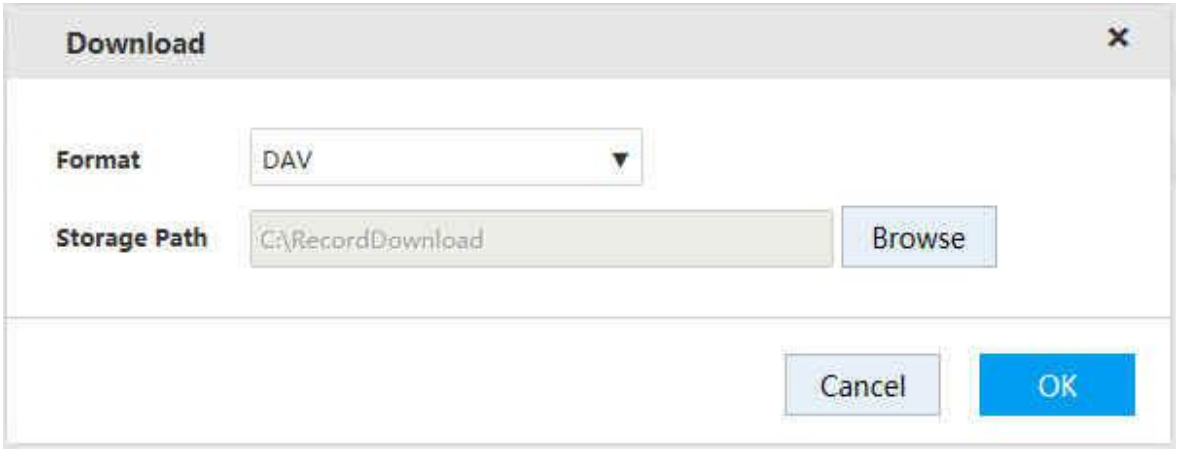
Step 3 Click **Search**.

The record files meeting the conditions are displayed.

Step 4 Select the file and click .

The **Download** interface is displayed. See Figure 3-87.

Figure 3-87 Download



Step 5 Select **Format** from the drop-down list and **Storage Path**.

The default storage path is C:\RecordDownload. For details to modify the path, see "3.14.2.1 Setting General Information."

Step 6 Click **OK**.

The system starts to download the record file.

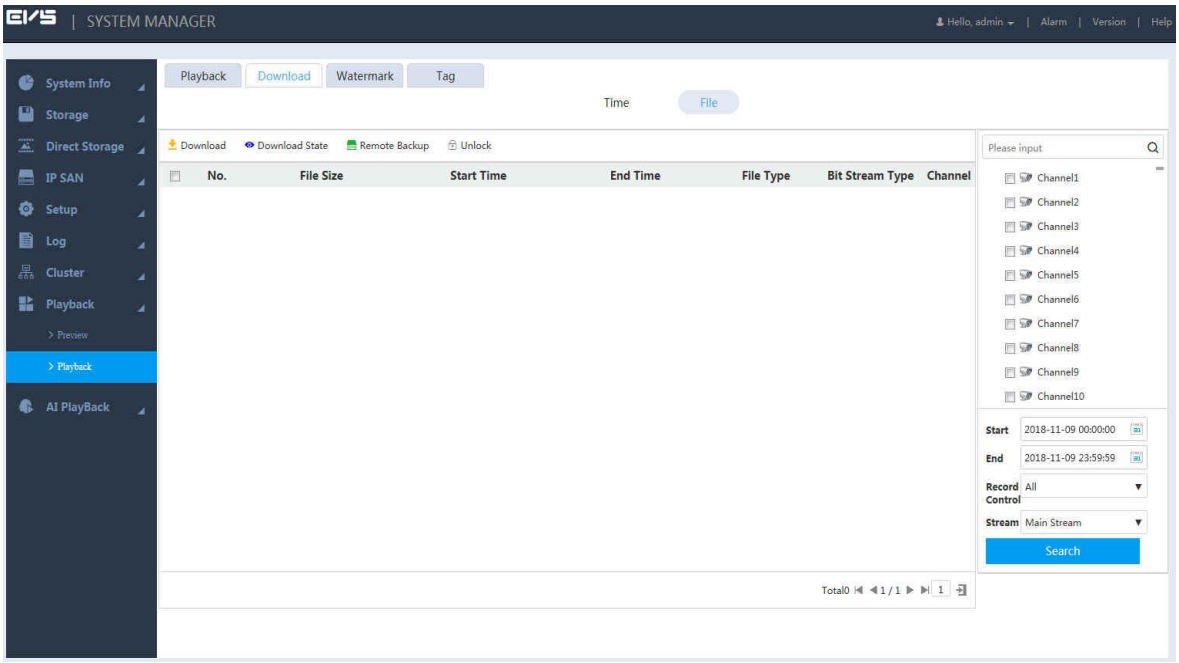
3.11.2.2 Download by File

Search the record files or images according to conditions such as channel, stream type, record type, start time and end time, and then select the needed record or image to download and backup.

Step 1 Select **Playback > Playback > Download > File**.

The **File** interface is displayed. See Figure 3-88.

Figure 3-88 File interface

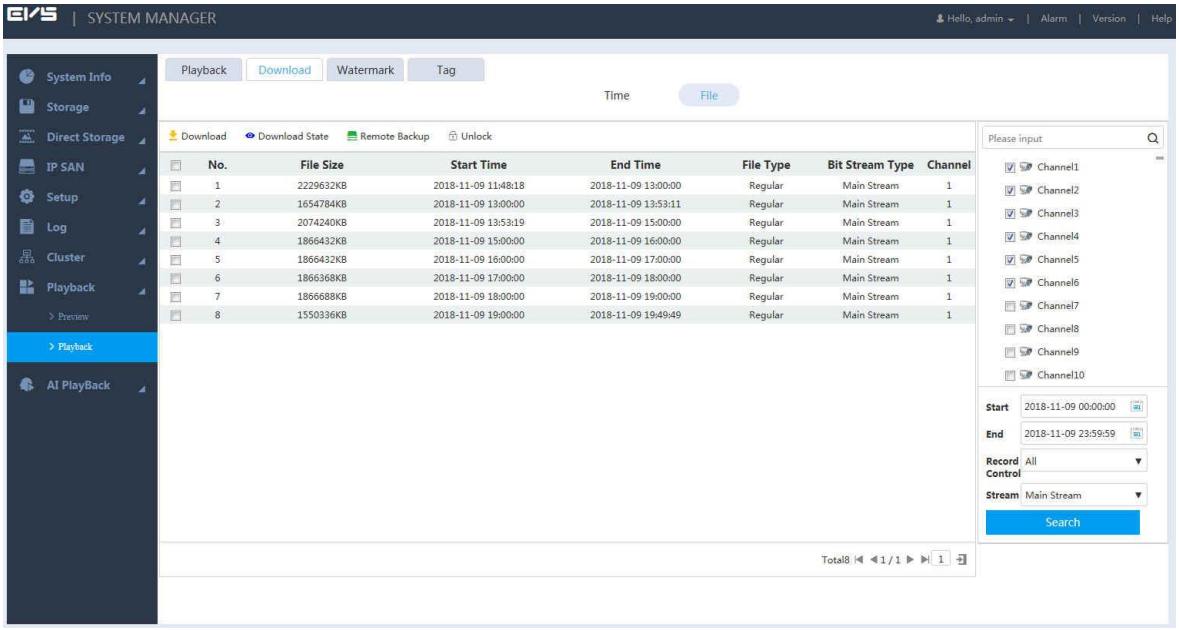


Step 2 Select **Channel**, and configure **Start**, **End**, **Record Control** and **Stream**.

Step 3 Click **Search**.

The record files meeting conditions are displayed.

Figure 3-89 Search results



Step 4 Locally download the record or backup the record to external USB device.

- Download

  Select the record and click .

  Select the **Format** and **Storage Path**. For details, see Step 4 of "3.11.2.1 Download by Time."

  The system starts record download.
- Remote backup

  Connect the USB to the USB interface of PC, select the record, and then click .

  The system starts to back up the file to external USB device.

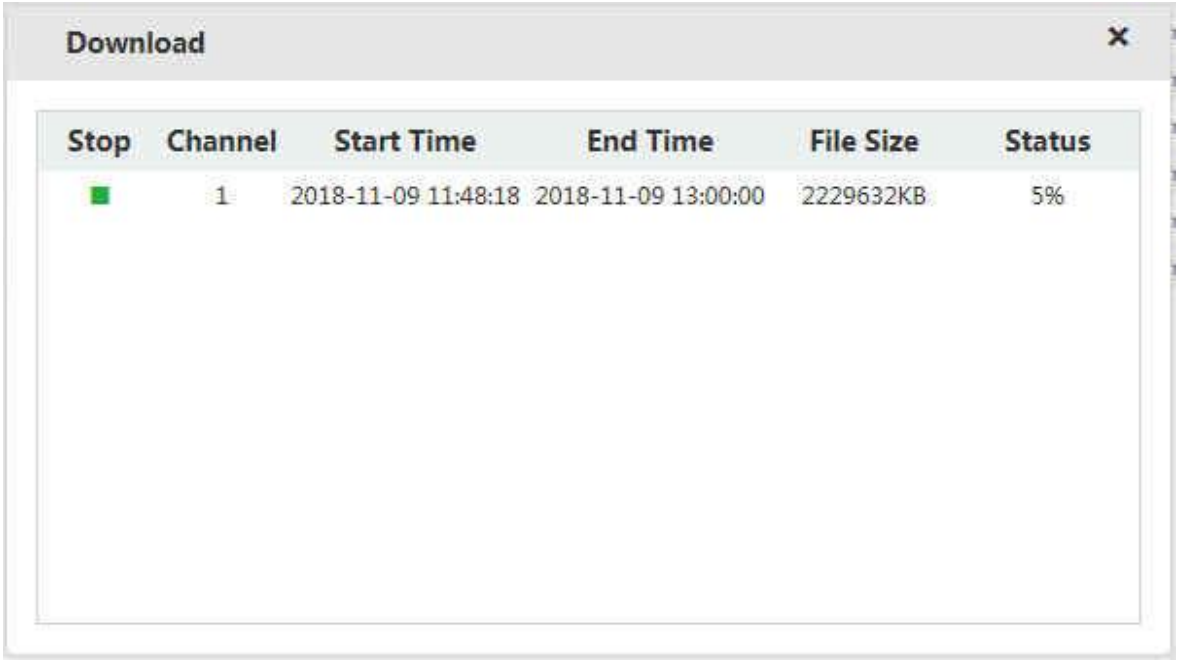
Step 5 (Optional) Click .

The **Download** interface is displayed. See Figure 3-90.

You can view the download progress on this interface.

Click to stop download.

Figure 3-90 Download



3.11.3 Record Verification

You can check whether the downloaded record file is tampered through watermark verification.

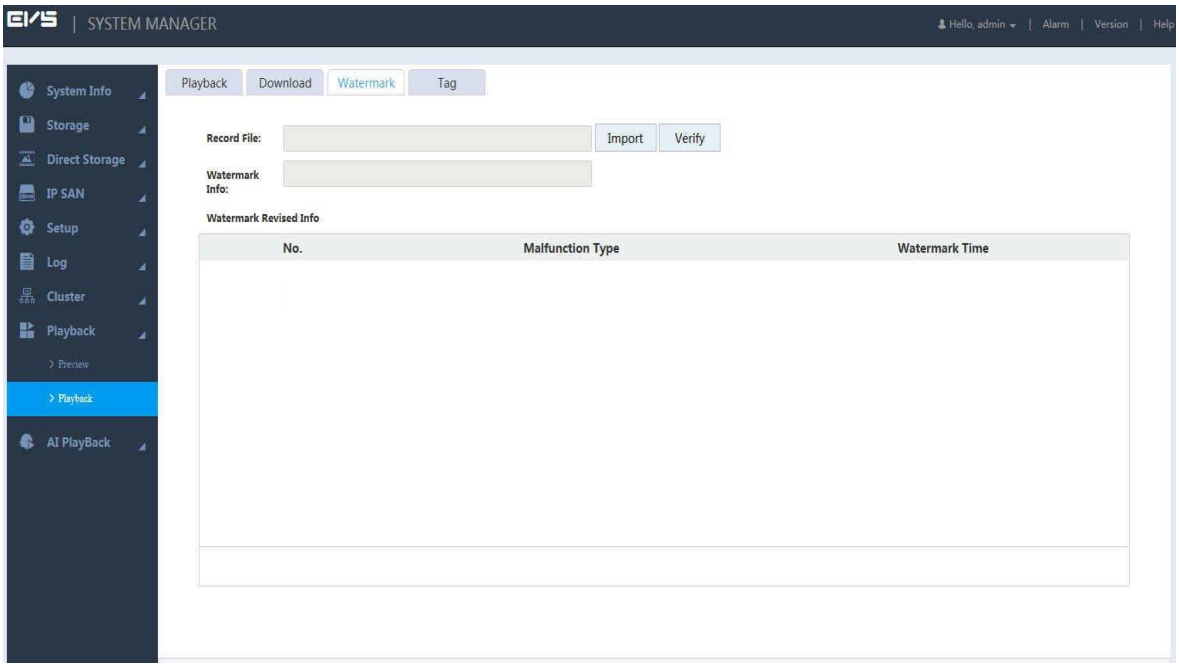
Preparation

The watermark verification function is enabled on the Device. For details, see "3.8.8.1 Setting video stream parameters."

Step 1 Select **Playback > Playback > Watermark**.

The **Watermark** interface is displayed. See Figure 3-91.

Figure 3-91 Watermark verification

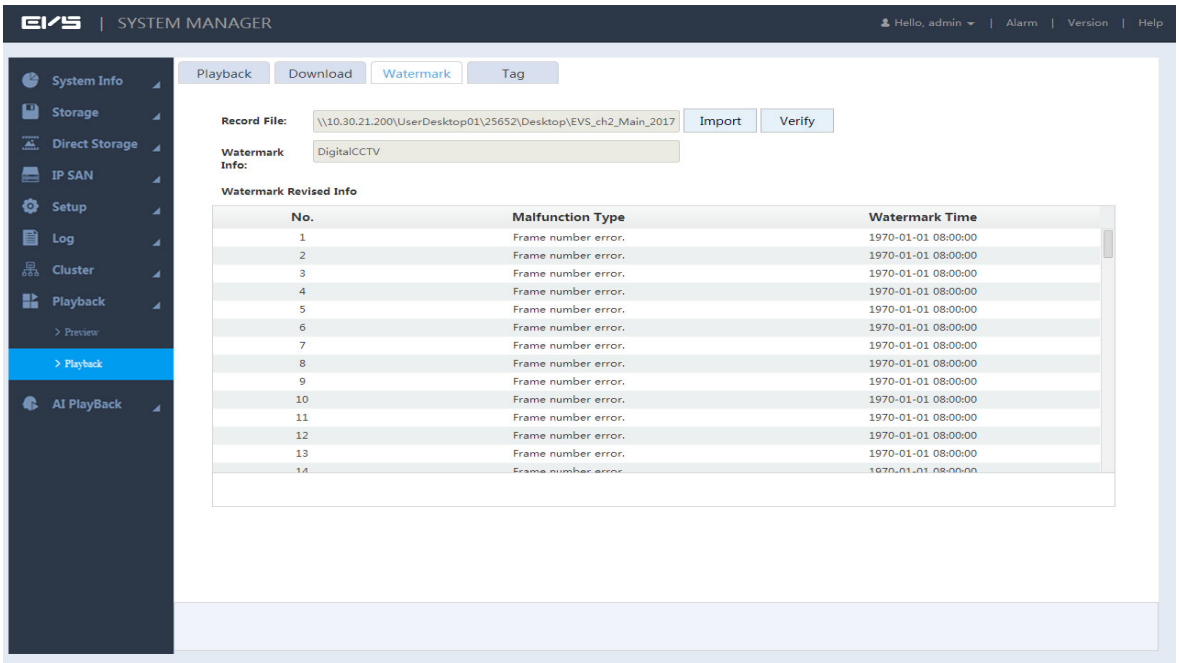


Step 2 Click **Import** to import the record needed to verify.

Step 3 Click **Verify**.

The system starts to verify the record files, and the progress and results are displayed. See Figure 3-92.

Figure 3-92 Verification results



3.11.4 Tag Management

When playing back record, you can add tags to the records with important information. After adding the tag, you can search by tag adding time and keywords, and playback relevant records. This helps obtain needed video information quickly.

Step 1 Select **Playback > Playback > Tag**.

The **Tag** interface is displayed.

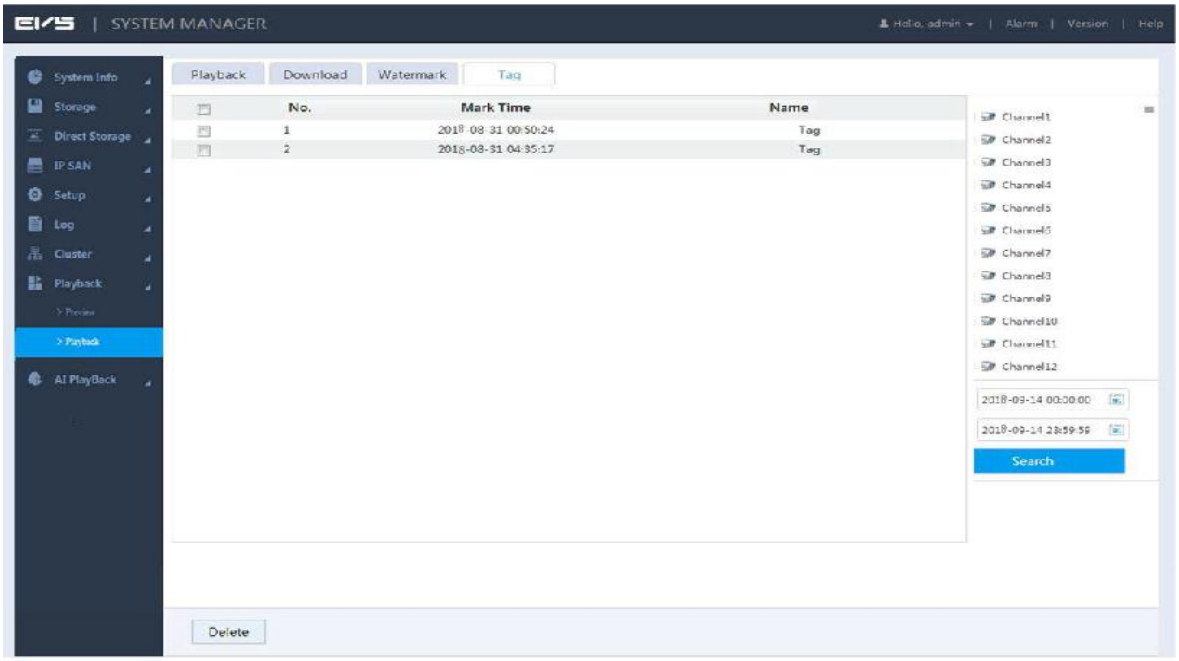
Step 2 Select **Channel**, and configure **Start** and **End**.

Step 3 Click **Search**.

The files with the searched tag are displayed. See Figure 3-93.

Select the tag file and click **Delete** to delete the file.

Figure 3-93 Tag management



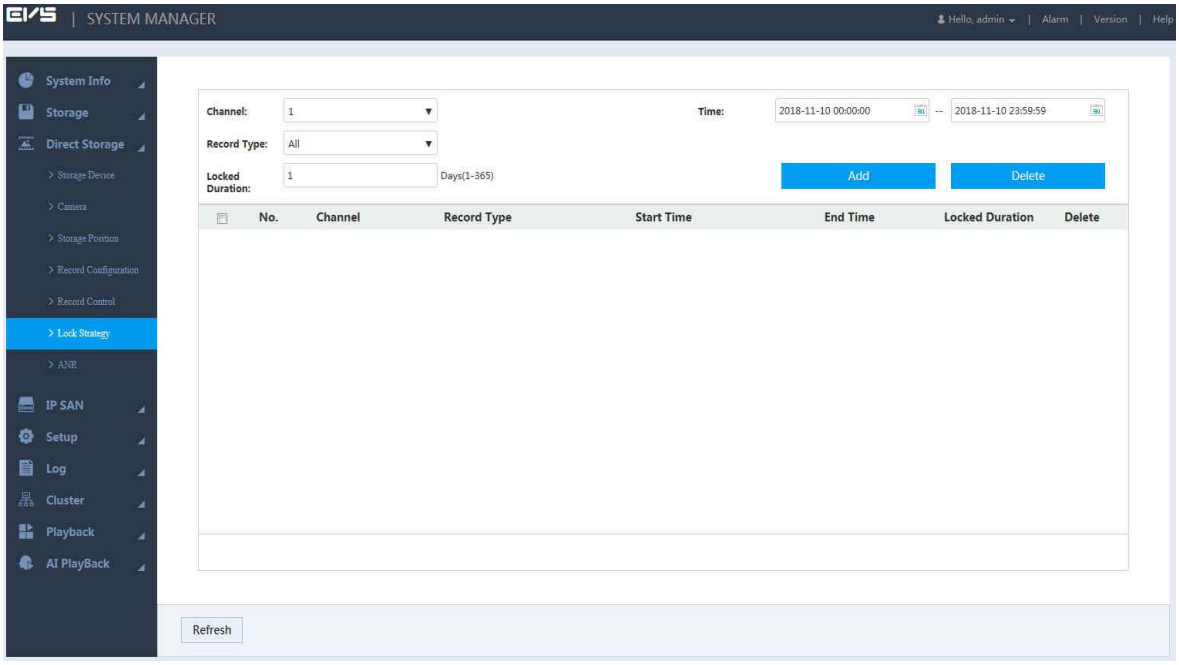
3.11.5 Setting Lock Strategy

Lock the video record to prevent it from being deleted.

Step 1 Select **Direct Storage > Lock Strategy**.

The **Lock Strategy** interface is displayed. See Figure 3-94.

Figure 3-94 Lock strategy



Step 2 Configure parameters. For details, see Table 3-32.

Table 3-32 Lock strategy parameters

Parameter	Description
Channel	Select the channel number. Select **All** to set same parameters for all the channels.
Time	Select the time period to lock the record.
Record Type	Select the record type to lock, including All, Normal, Alarm, and MD.
Locked Duration	During the locked duration, the locked record will not be deleted.

Step 3 Click **Add**.

The system locks the selected record, and lists the file in the below list.

Click to unlock the record file.

3.11.6 ANR

The Device with ANR function retrieves stored video data from IPC after network recovery. This function helps ensure the completeness of video record.

This function requires IPC to be installed with SD card.

Two ANR modes are available: Automatic and Manual.

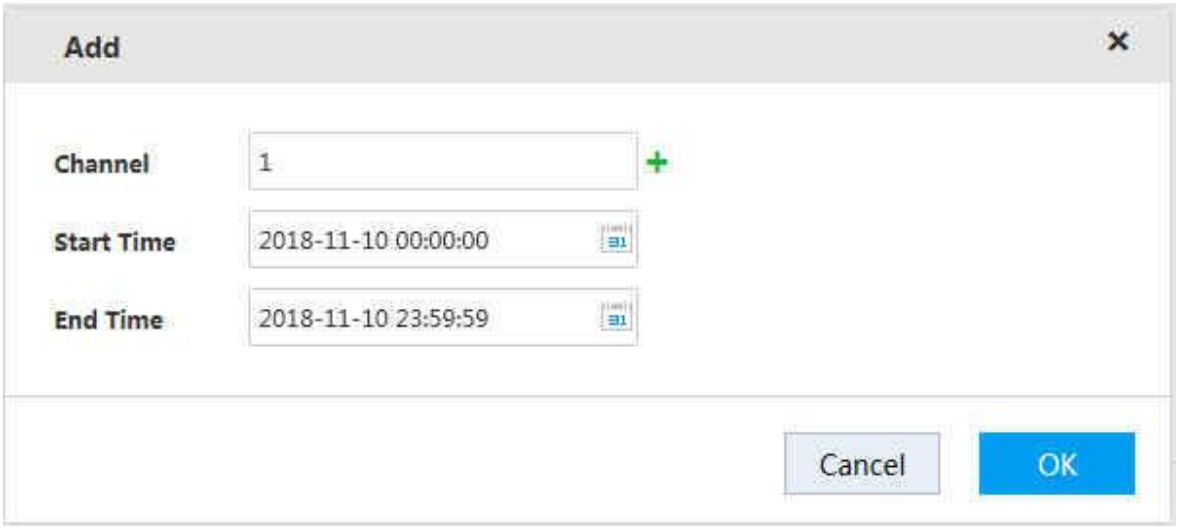
- Automatic: After network recovery, the Device automatically downloads the record from IPC. For details, see "3.4.3.1 Configuring Record Plan."
- Manual: If you do not enable ANR function when configuring record plan, the system will not automatically downloads record data from IPC. In this case, you need to manually set download plan.

Step 1 Select **Direct Storage > ANR**.

Step 2 Click to add backup record.

The **Add** interface is displayed. See Figure 3-95.

Figure 3-95 Adding backup record



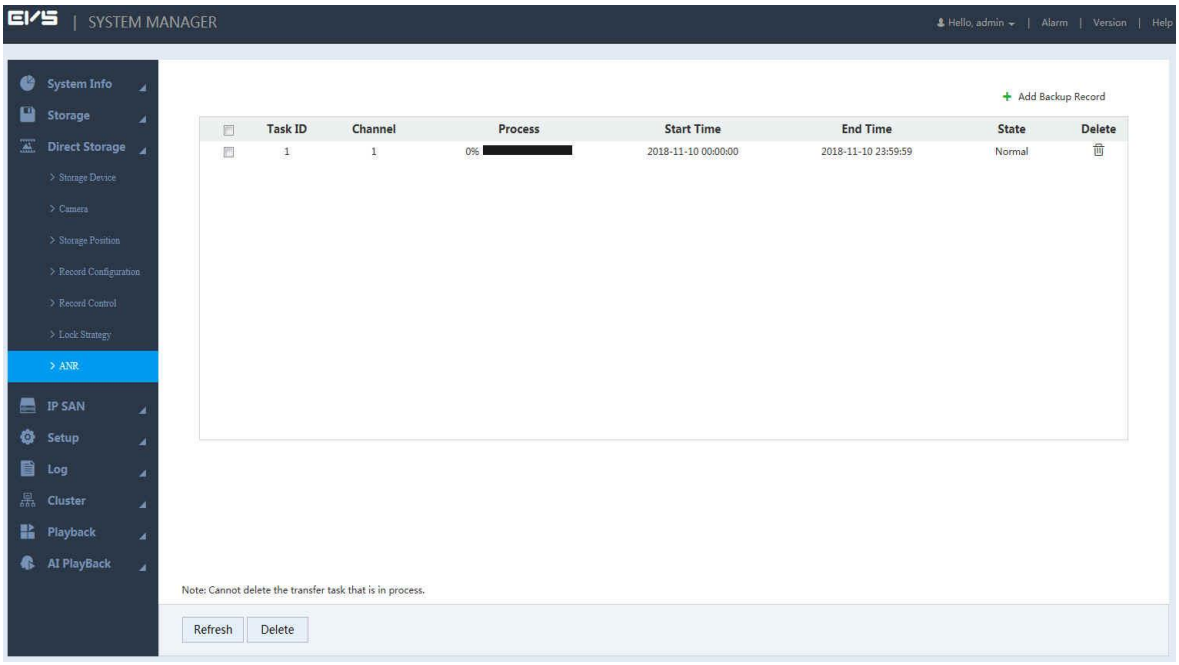
Step 3 Select channel, set start time and end time.

The system supports simultaneous record upload of several consecutive channels. You can click + to choose the range of channels.

Step 4 Click **OK**, and then back to the Add Backup Record interface.

You can view the upload progress of record on this interface. See Figure 3-96.

Figure 3-96 Upload progress



Task(s) in progress cannot be deleted.

3.12 User Management

User management includes management of user group and user. Each user name and group name is unique, and cannot be repeated.

- The factory default user name is admin. The password is the one set in device initialization.
- You can set up to 64 users or 20 user groups.
- Factory default groups: User and admin. The admin group cannot be deleted.
- Users in the group can modify its authority in the group authority. To facilitate user management, it is recommended that the authority of common users is lower than that of advanced users.
- Each user must belong to and only belongs to one group. When selecting a group to which the user belongs, the authority of the user can only be a subset of group authorities, and cannot exceed the authority attribute of the group.
- The user name is a string of 1–32 byte(s), and group name is a string of 1–64 byte(s). Both names can only contain letter(s), number(s), underline(s), and hyphen(s).

3.12.1 User

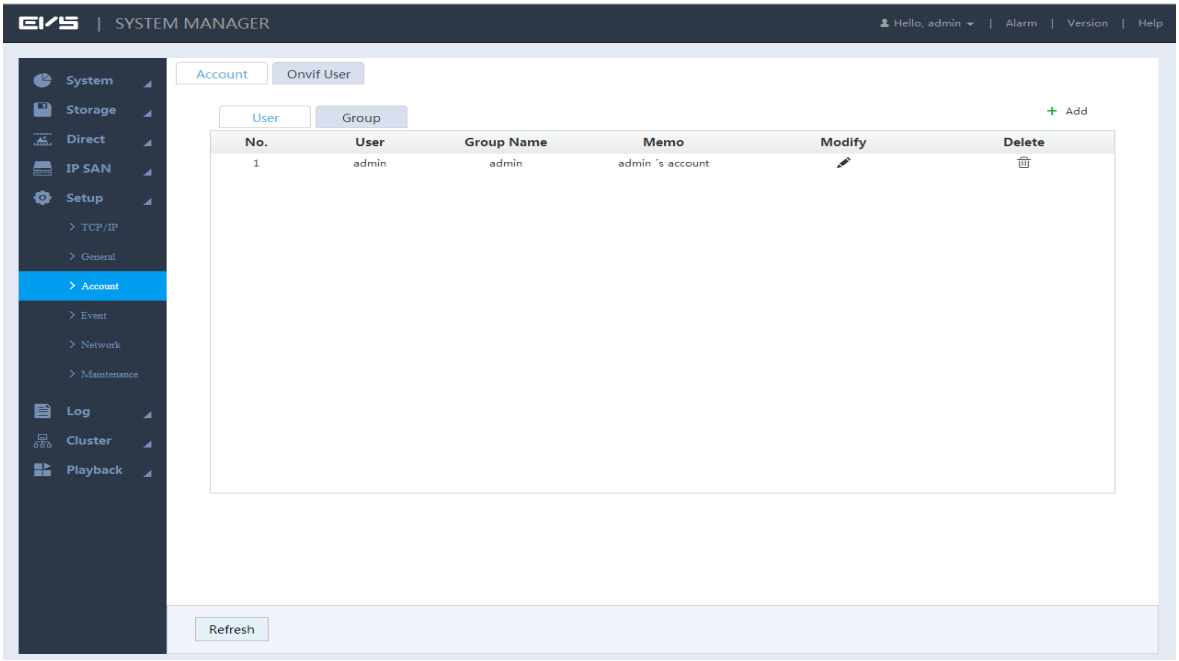
User information management includes adding, deleting and modifying users. It also includes adding users to a group and setting user authority.

3.12.1.1 Adding User

Step 1 Select **Setup > Account > Account > User**.

The **User** interface is displayed. See Figure 3-97.

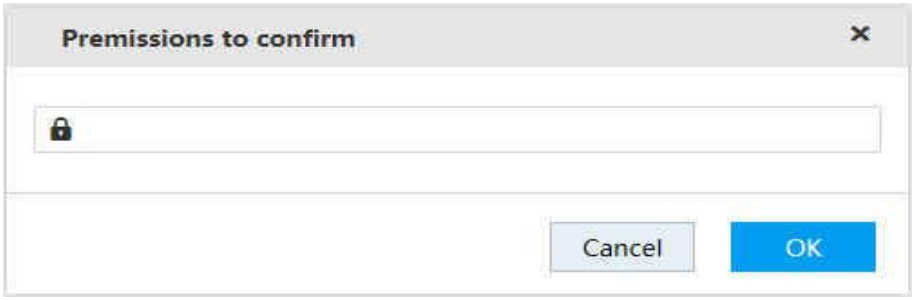
Figure 3-97 User interface



Step 2 Click + .

The **Permissions to confirm** interface is displayed. See Figure 3-98.

Figure 3-98 Permissions to confirm

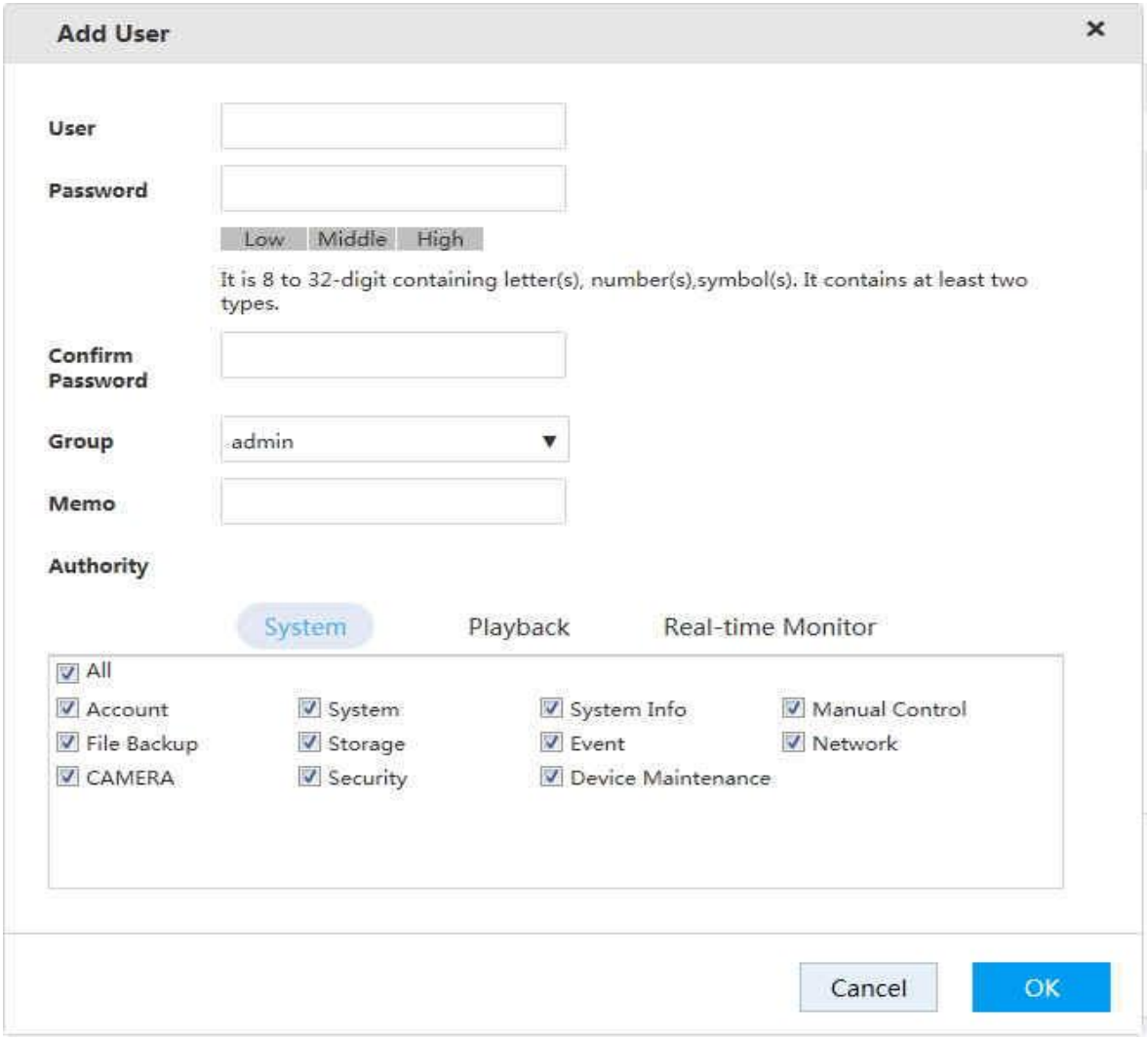


Permission to confirm is required when logging in to add user for the first time, or no operation on this interface for five minutes.

Step 3 Enter the login password, and then click **OK**.

The **Add User** interface is displayed. See Figure 3-99.

Figure 3-99 Adding user



Step 4 Configure the parameters. For details, see Table 3-33.

Table 3-33 Parameters of adding user

Parameter	Description
User	Enter the user name.
Password	Enter and confirm the password. It is an 8-digit to 32-digit string containing at least two categories of the following: letter(s), number(s) and special character(s) (including "!", "?", "@", "#", "$", "%", "+", "=", ".", ",", "*", "_", "-"). It is recommended to set a high security password according to the strength prompt.
Confirm Password	
Group	Select the group to which the new user belongs. For details of adding groups, see "3.12.2 User Group."
Memo	Enter memo information to help recognize and manage the user.

Parameter	Description
Authority	Select the user authorities of system, playback and real-time monitor. ● You can modify user authorities in group authorities. The authorities of admin user cannot be modified. ● To facilitate the management of users, it is recommended that the authorities of common users are lower than that of advanced users.

Step 5 Click **OK** to save the configuration.

Click to edit user information and click to delete a user.

3.12.1.2 Modifying Password

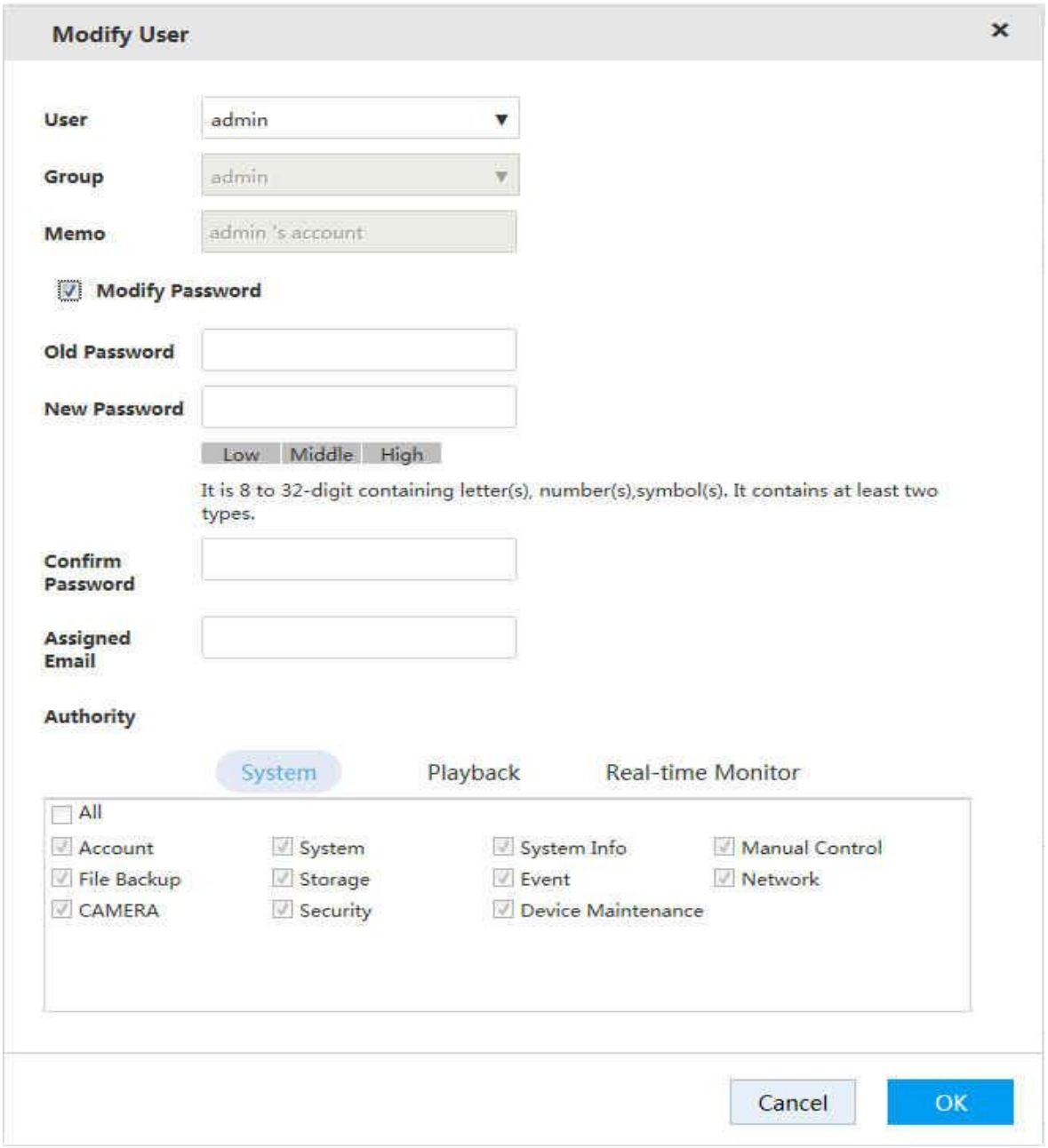
With user management authority, you can modify your password and password of other users.

Step 1 On the **User** interface, click of the corresponding user.

Step 2 Select the **Modify Password** check box.

The **Modify User** interface is displayed. See Figure 3-100.

Figure 3-100 Modifying user



Step 3 Enter your old password, new password and confirm the password.

It is an 8-digit to 32-digit string containing at least two categories of the following: letter(s), number(s) and special character(s) (including "!", "?", "@", "#", "$", "%", "+", "=", ".", ",", "*", "_", "-").

You need to enter the old password when modifying your password. If modifying the password of others, you are not required to enter the old password of others.

Step 4 Assign email.

After entering the assigned email, you can reset the password through email if you forgot the password for admin account. For details, see "3.12.1.3 Resetting Password"

Only the admin account supports assigned email. See the actual interface.

Step 5 Click **OK** to save the configuration.

3.12.1.3 Resetting Password

If you forgot the password for admin account, you can reset it through the assigned email.

Step 1 Open the browser, and enter the IP address of the Device in the address bar. Press Enter.

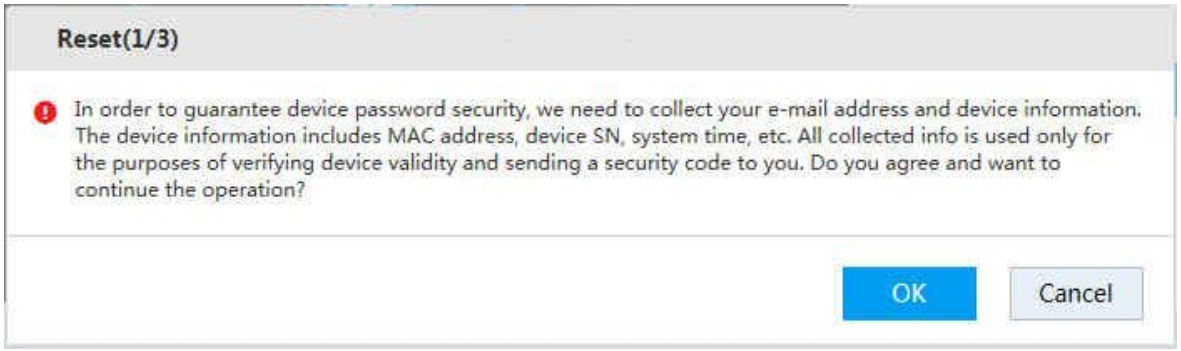
The **Login** interface is displayed. See Figure 3-101.

Figure 3-101 Login interface

Step 2 Click **Forgot password?**

The **Reset(1/3)** interface is displayed. See Figure 3-102.

Figure 3-102 Resetting password (1)

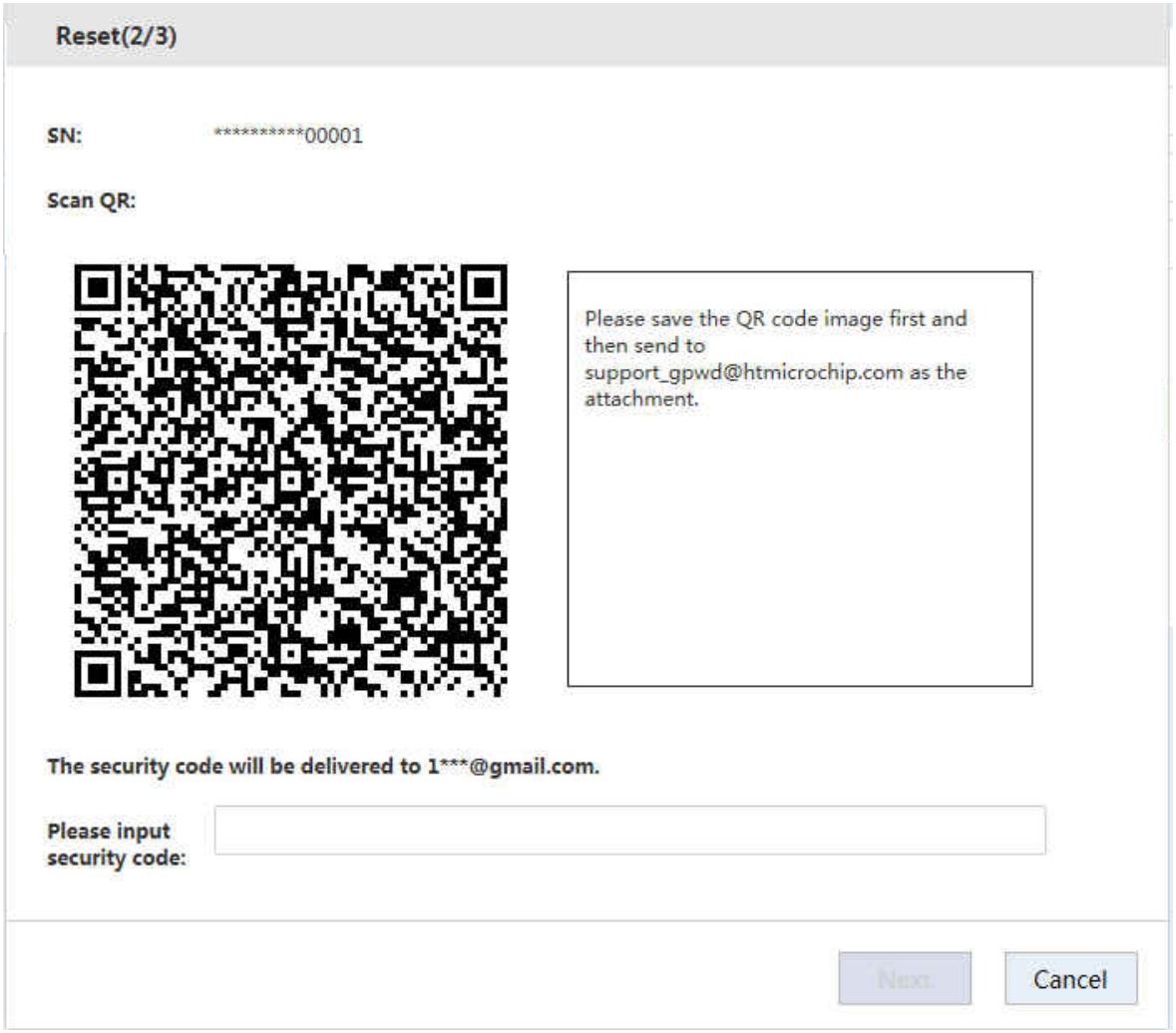


After clicking OK, the system will collect some of your information for password resetting, such as phone number, MAC address, and device serial number, etc. Read carefully, and confirm if you agree with the collection operation.

Step 3 Click **OK**.

The **Reset(2/3)** interface is displayed. See Figure 3-103.

Figure 3-103 Resetting password (2)



Step 4 Scan the QR code according to interface prompt to obtain the security code.

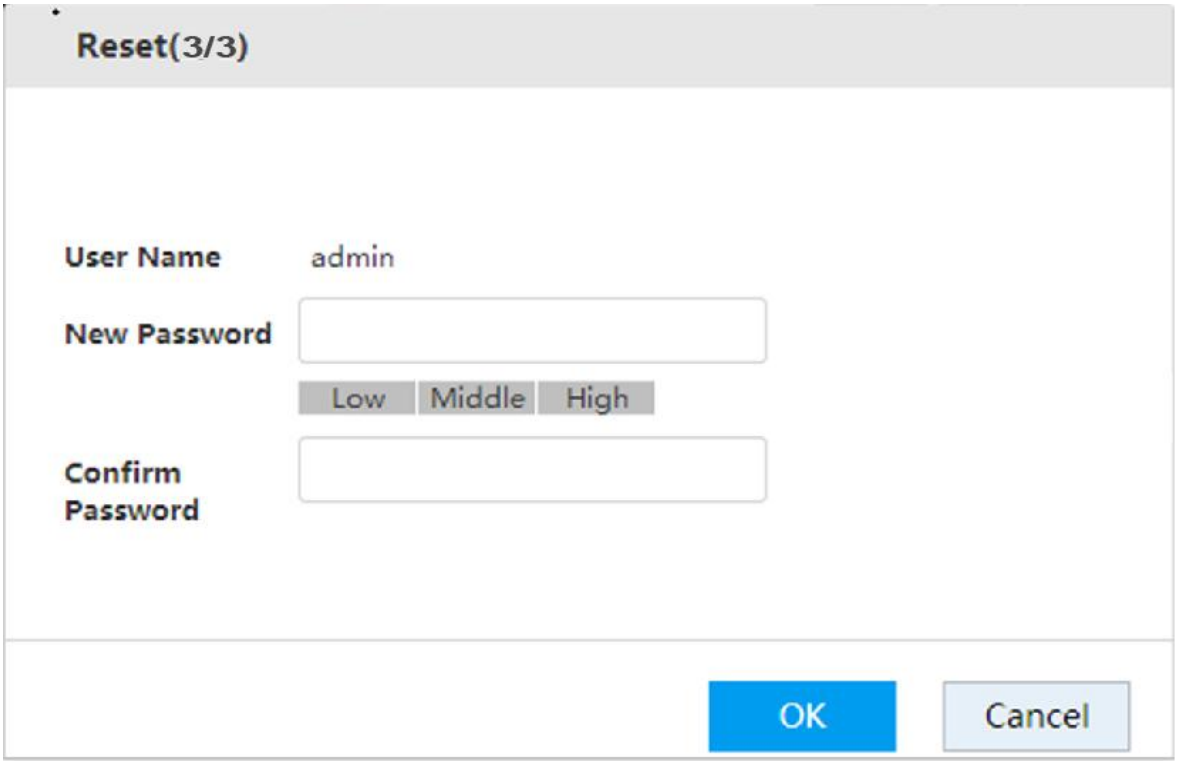
- You can obtain the security code for twice at most by scanning the same QR code. If you need more times, refresh the QR interface.
- Use the security code to reset the password within 24 hours, otherwise it will be invalid.

Step 5 Enter the security code in the **Please input security code** text box.

Step 6 Click **Next**.

The **Reset(3/3)** interface is displayed. See Figure 3-104.

Figure 3-104 Resetting password (2)



Step 7 Enter the new password and confirm password.

It is an 8-digit to 32-digit string containing at least two categories of the following: letter(s), number(s), and special character(s) (including "!", "?", "@", "#", "$", "%", "+", "=", ".", ",", "*", "_", "-"). It is recommended to set a high security password according to the strength prompt.

Step 8 Click **OK** to complete password reset.

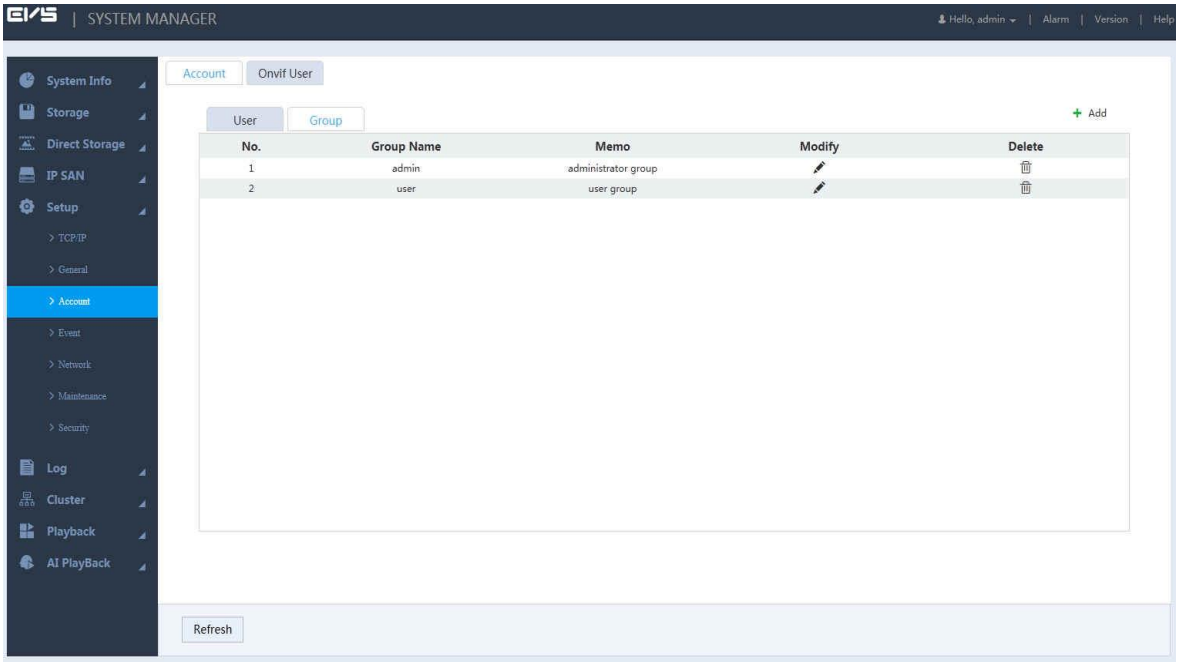
3.12.2 User Group

In the entire network, users accessing the Device might have different authorities. You can group the users with the same authorities as a group. This helps maintain and manage user information.

Step 1 Select **Setup > Account > Account > Group**.

The **Group** interface is displayed. See Figure 3-105.

Figure 3-105 Group interface



Step 2 Click + .

The **Permissions to confirm** interface is displayed. See Figure 3-106.

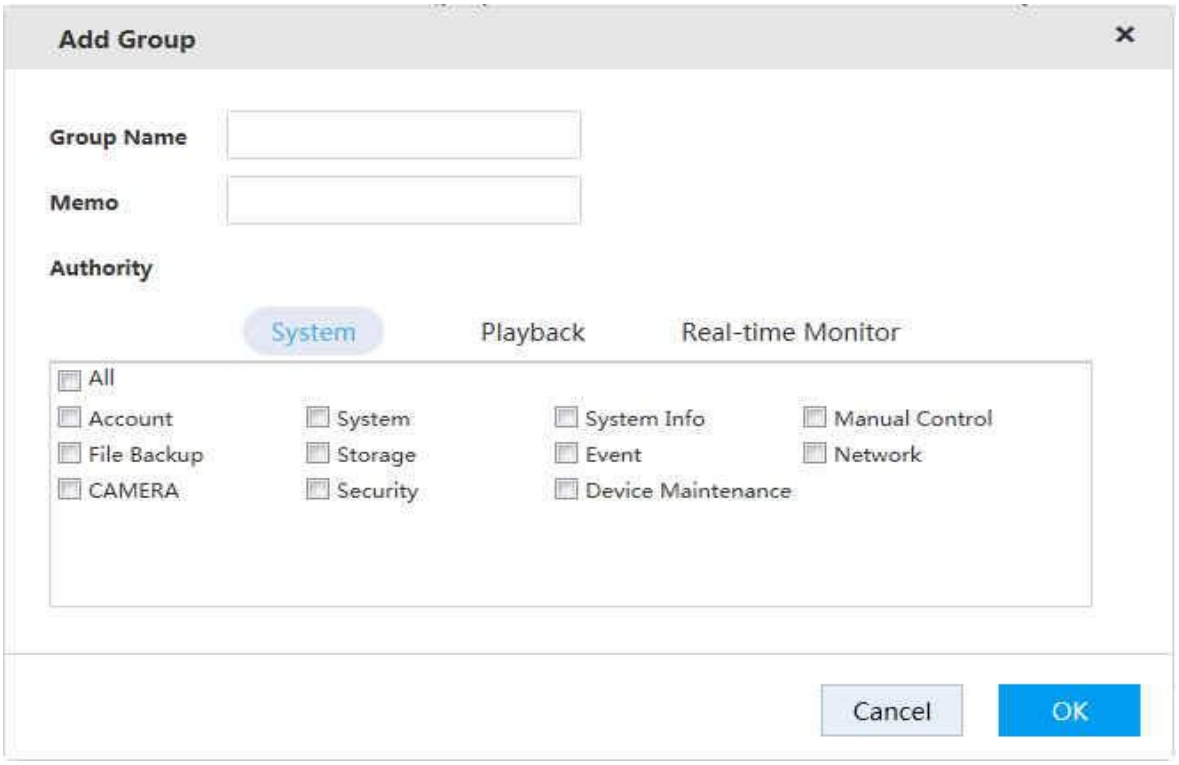
Figure 3-106 Permissions to confirm

Permission to confirm is required when logging in to add group for the first time, or no operation on this interface for five minutes.

Step 3 Enter the login password, and then click **OK**.

The **Add Group** interface is displayed. See Figure 3-107.

Figure 3-107 Adding group interface



Step 4 Configure the parameters. For details, see Table 3-34.

Table 3-34 Parameters of adding group

Parameter	Description
Group Name	Enter the user group name.
Memo	Enter memo information to help recognize and manage user group.
Authority	Select the authorities of system, playback and real-time monitor.

Step 5 Click **OK** to save the configuration.

Click to edit group information, and click to delete the group.

3.12.3 Onvif User

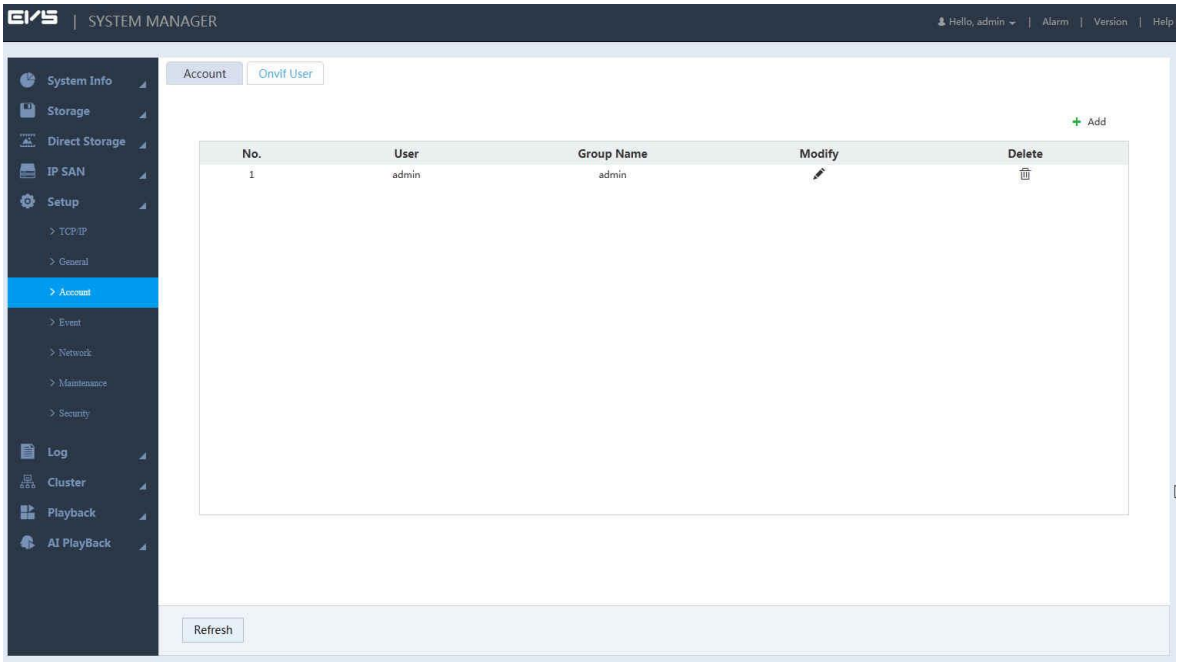
When devices of other manufacturers access the Device through Onvif protocol, the Onvif account needs to be verified.

This section introduces the management of Onvif user information.

Step 1 Select **Setup > Account > Onvif User**.

The **Onvif User** interface is displayed. See Figure 3-108.

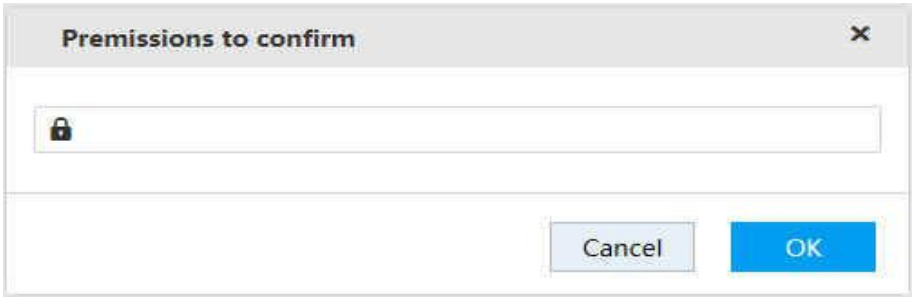
Figure 3-108 Onvif user



Step 2 Click + .

The **Permissions to confirm** interface is displayed. See Figure 3-109.

Figure 3-109 Permissions to confirm

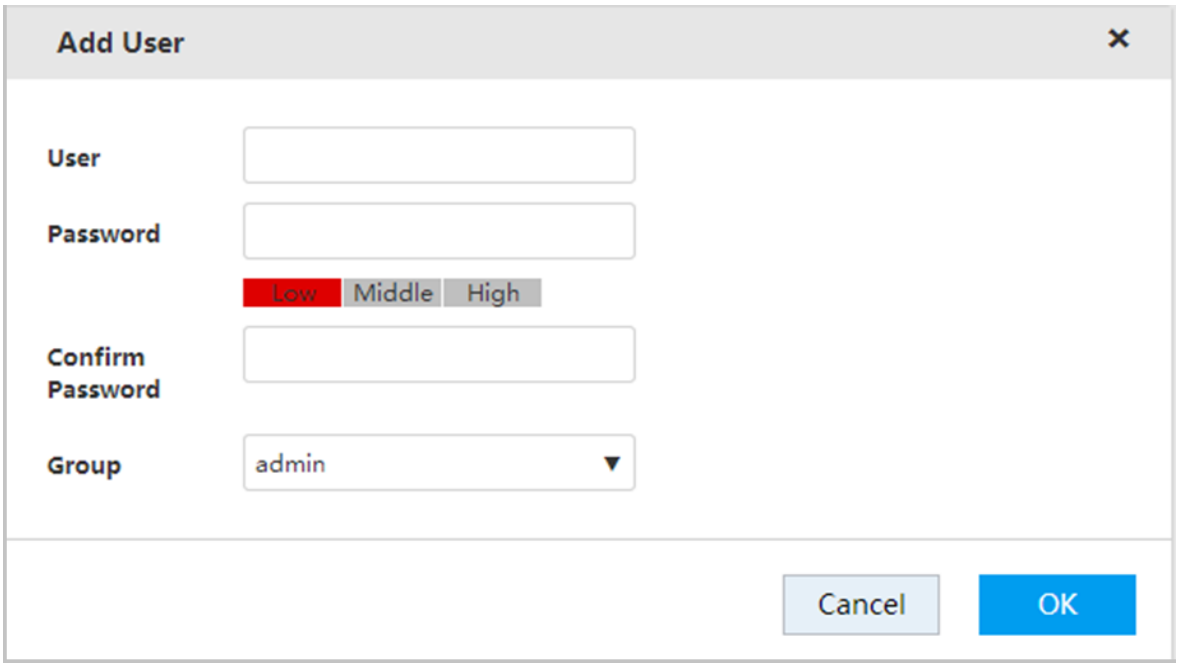


Permission to confirm is required when logging in to add user for the first time, or no operation on this interface for five minutes.

Step 3 Enter the login password, and then click **OK**.

The **Add User** interface is displayed. See Figure 3-110.

Figure 3-110 Adding user



Step 4 Configure the parameters. For details, see Table 3-35.

Table 3-35 Adding user parameters

Parameter	Description
User	Enter the user name.
Password	Enter and confirm the password. The new password can be set from 8 characters through 32 characters, and contain characters from at least two of the following categories: number, letter and special characters (excluding"'", '"', ";", ":" and "&"). It is recommended to set a high security password according to the strength prompt.
Confirm Password	
Group	Select the group to which the new user belongs. For detailed description of adding groups, see "3.12.2 User Group."

Step 5 Click **OK** to save the configuration.

Click to edit user information, and click to delete the user.

3.12.4 Online User

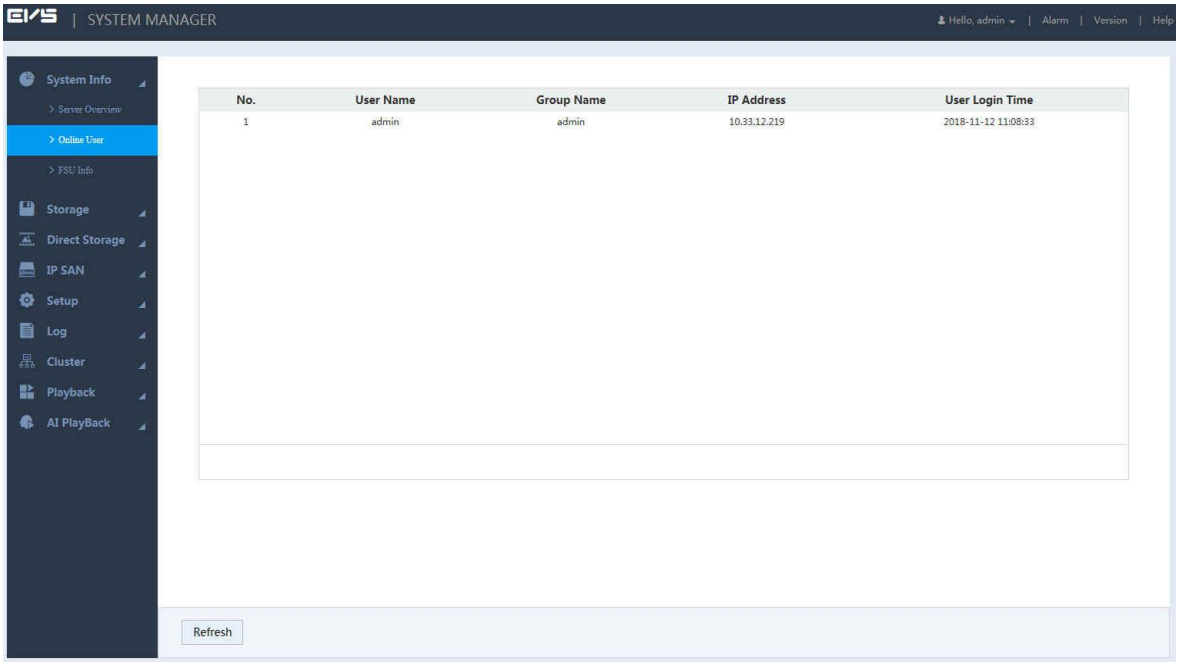
View the information of the current online users connected with the Device.

Select **System Info > Online User**.

The **Online User** interface is displayed. See Figure 3-111.

The system automatically refreshes the online user information every five seconds. You can also click **Refresh** to manually update online user information.

Figure 3-111 Online user



3.13 Storage Management

Storage management includes management of storage resources (such as record files) and storage space to improve space utilization. It includes the management of physical HDD, network HDD and RAID.

- Physical HDD: Disks directly installed in the Device.
- Network HDD: The virtual storage space mapped to the Device through network.
- RAID: Organize multiple independent physical disks into disk arrays. RAID provides higher storage performance and data redundancy.

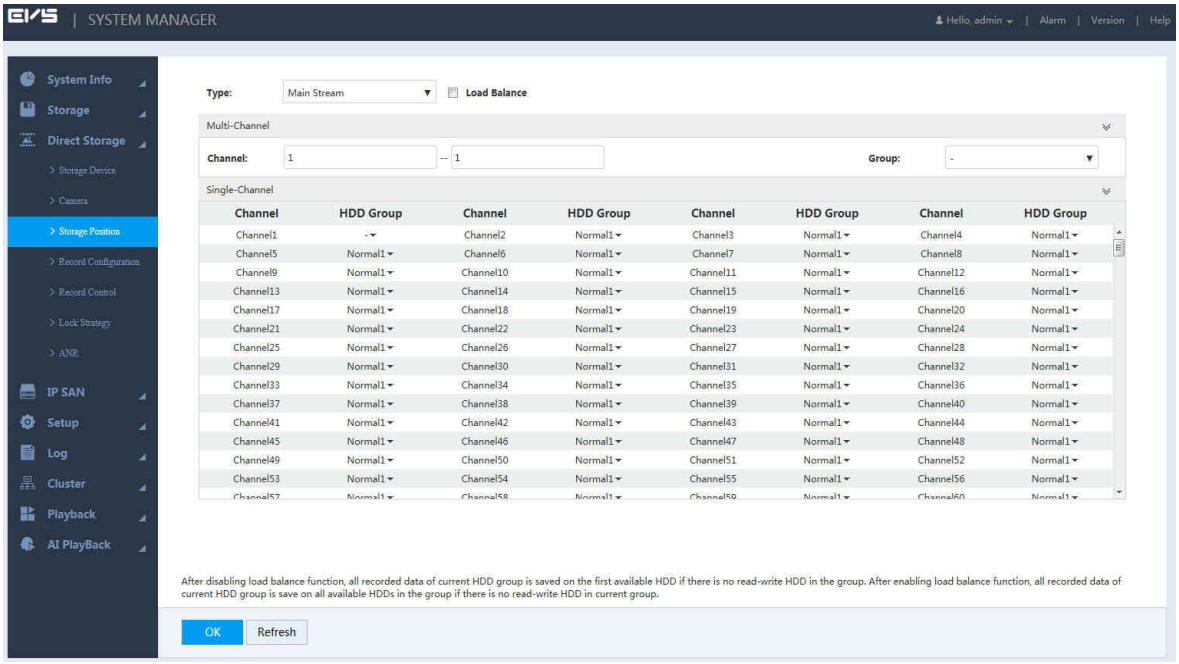
3.13.1 Storage Position

You can save the recorded videos and snapshots of a specific channel to the path you need.

Step 1 Select **Direct Storage > Storage Position**.

The **Storage Position** interface is displayed. See Figure 3-112.

Figure 3-112 Storage position



Step 2 Select the **Type** of record or image, including main stream, sub stream, image storage, and AI playback storage.

Step 3 (Optional) Select **Load Balance**.

- After enabling load balance, if there is no read-write HDD in a HDD group, all recorded data of this group will be evenly saved on all available HDD groups.
- After disabling load balance, if there is no read-write HDD in a HDD group, all recorded data of this group will be saved on the first available HDD group.

Step 4 Set the HDD group of each channel.

You can set the HDD group of one channel, or HDD groups of multiple channels.

- **Multi-Channel**: You need to set the channel range (for example 1–100) as well as the group.
- **Single-Channel**: Set the HDD group of channel by selecting from the drop-down list of HDD group.

Step 5 Click **OK** to save the configuration.

3.13.2 Storage Device

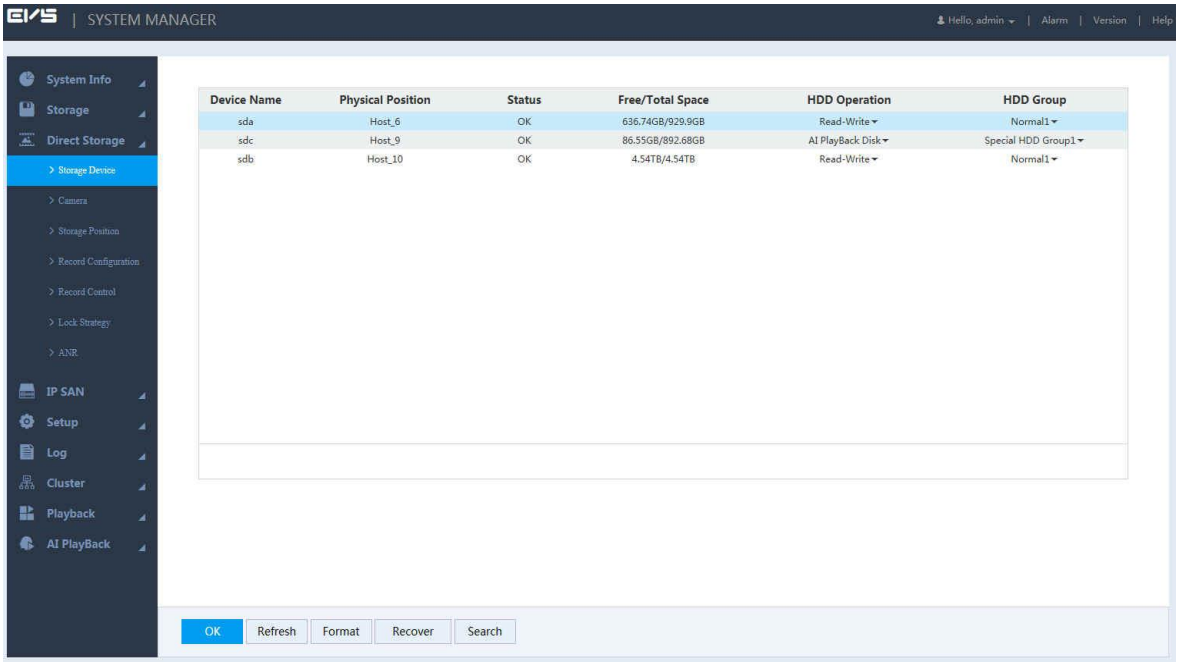
You can view disk information, set disk and disk group attribute, format disk, recover picture database, and search record.

3.13.2.1 Setting Disk Attribute

Step 1 Select **Direct Storage > Storage Device**.

The Storage Device interface is displayed. See Figure 3-113.

Figure 3-113 Storage position



Step 2 Configure the parameters. For details, see Table 3-36.

Table 3-36 Storage device parameters

Parameter	Description
Device Name	Displays the name of disk or RAID.
Physical Position	Displays the physical position of disk or RAID.
Status	Displays the current operational condition of disk or RAID.
Free/Total Space	Displays the free space and total space of disk or RAID.
HDD Operation	Click the drop-down list of corresponding disk or RAID, and select its attribute. ● Read-Write: Supports reading and storing data. ● Read-Only: Only supports reading data. No storing data is available. ● Redundant-HDD: Backup disk. Used for storing redundant record. ● DrawFrame Disk: Only used for storing record after deleting non-key frames. ● AI PlayBack Disk: Supports storing AI images and records.
HDD Group	Click the drop-down list of corresponding disk or RAID, and select its HDD group. AI playback disk is in special HDD group, read-write disk is in normal group, and other disks do not need to set HDD group.

Step 3 Click **OK** to save the configuration.

3.13.2.2 Formatting Disk

Formatting disk will clear all the data in a disk. Operate with care.

On the **Storage Device** interface, select the disk you want to format, and click **Format**. All the data in this disk will be cleared.

3.13.2.3 Recovering Image Database

When the image database is abnormal, you can execute picture recovery on the AI playback disk.

On the **Storage Device** interface, select the corresponding disk, and click **Recover** to recover the picture database.

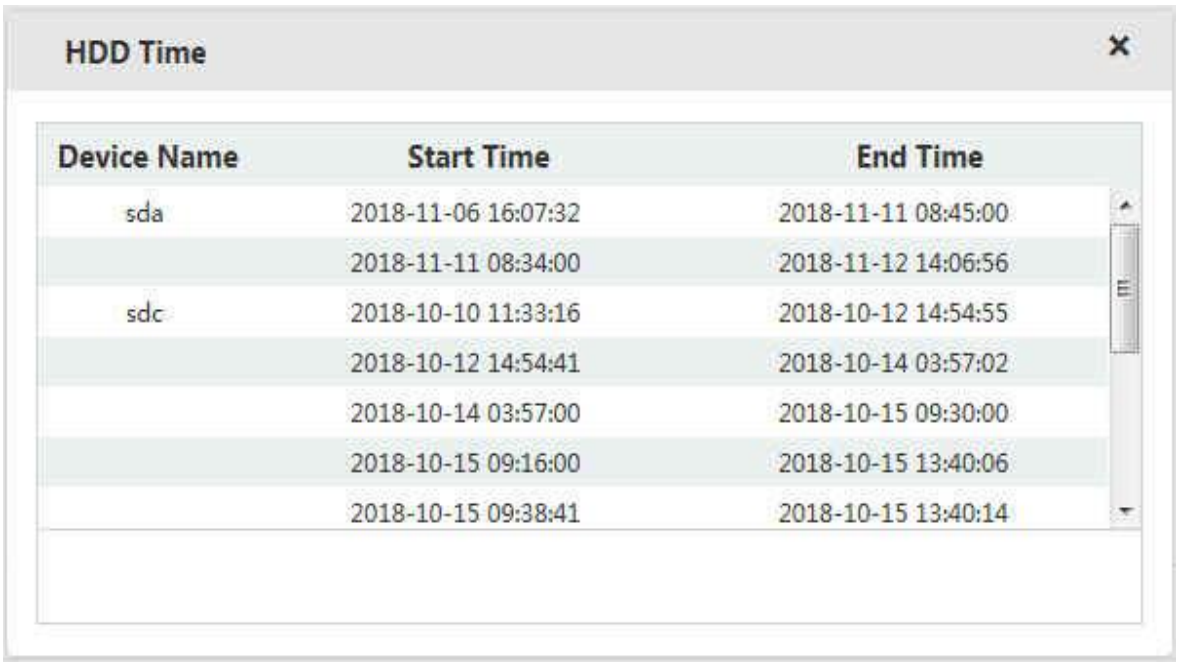
3.13.2.4 Searching record

On the **Storage Device** interface, select a disk, and click **Search**.

The **HDD Time** interface is displayed. See Figure 3-114.

On this interface, you can check the time of record in specified disks.

Figure 3-114 HDD Time



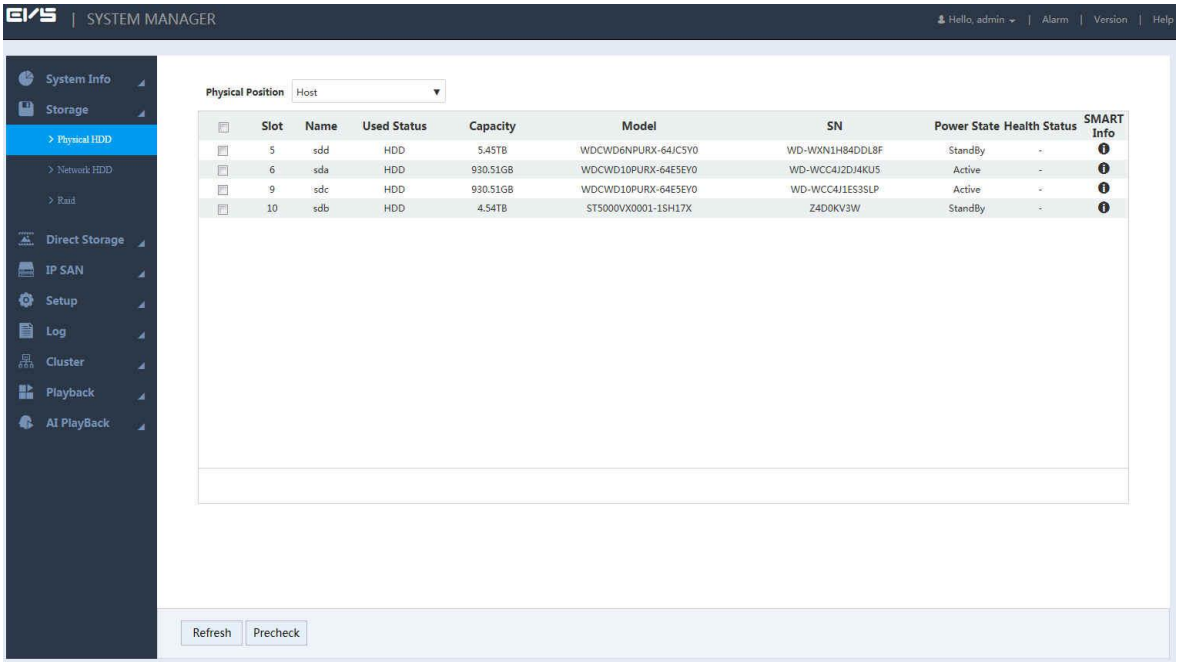
3.13.3 Physical HDD

Check the use status, capacity, manufacturer, serial number, power status, health status and Self-Monitoring Analysis and Reporting Technology (SMART) information of physical disks.

Select **Storage > Physical HDD**.

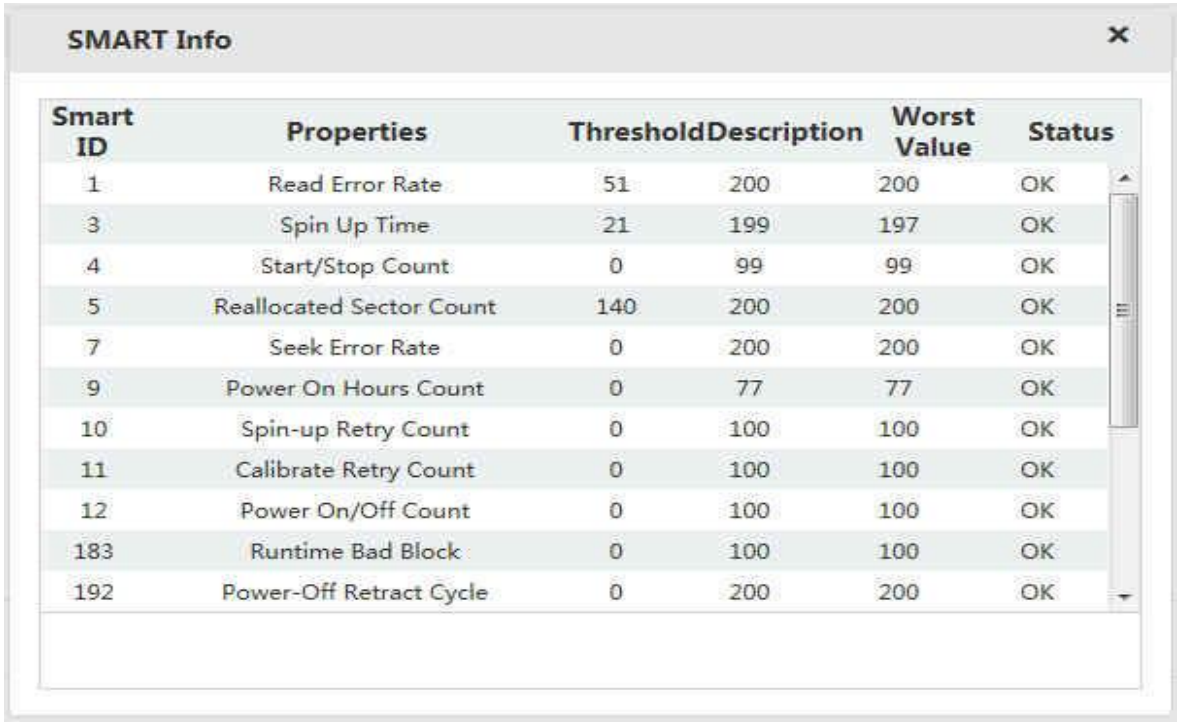
The **Physical HDD** interface is displayed. See Figure 3-115.

Figure 3-115 Physical HDD



- Click the drop-down box of **Physical Position** to select the position of the physical HDD you want to view.
- Click **Refresh** to update the physical HDD list.
- Select the physical HDD and click **Precheck**. The system can check the operation status of the disk to help you understand disk performance and replace disk with errors timely.
- Click , and the **SMART Info** interface is displayed. See Figure 3-116.

Figure 3-116 SMART Info



3.13.4 Network HDD

Set the network HDD by iSCSI, and then map the network HDD to the Device, so that the Device can store data through network HDD.

- iSCSI is a kind of storage technology running SCSI protocol in the IP network.
- The network HDD mapped to the Device cannot be used to create RAID.

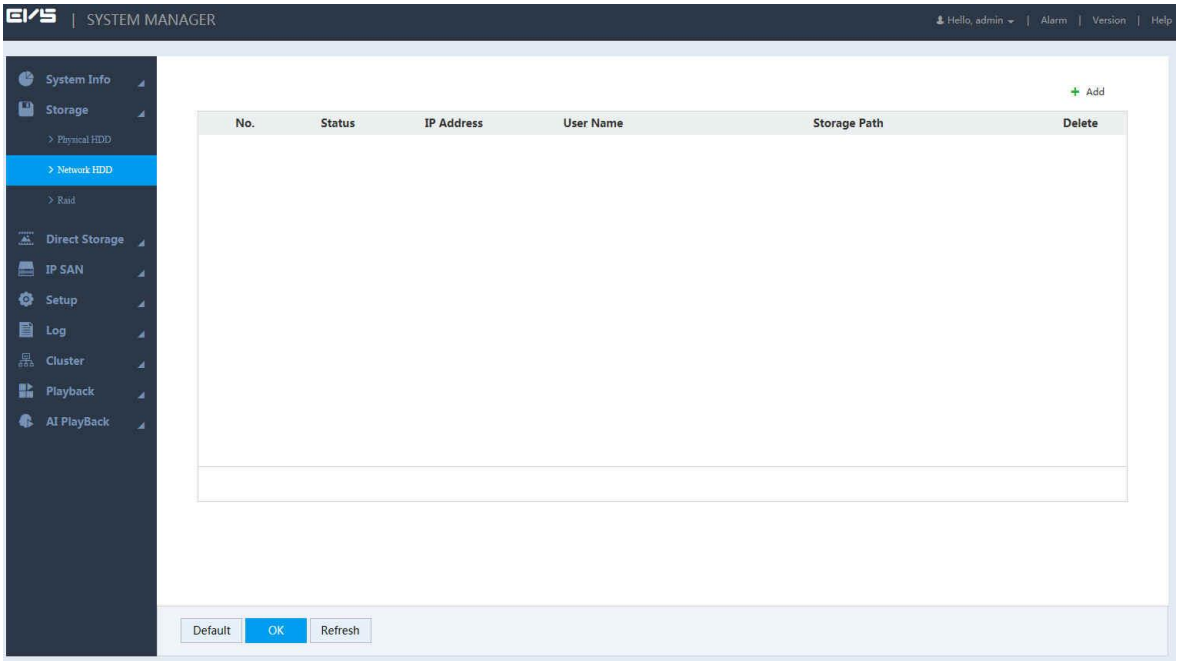
Preparation

iSCSI server is enabled and has provided the shared folder list.

Step 1 Select **Storage > Network HDD**.

The **Network HDD** interface is displayed. See Figure 3-117.

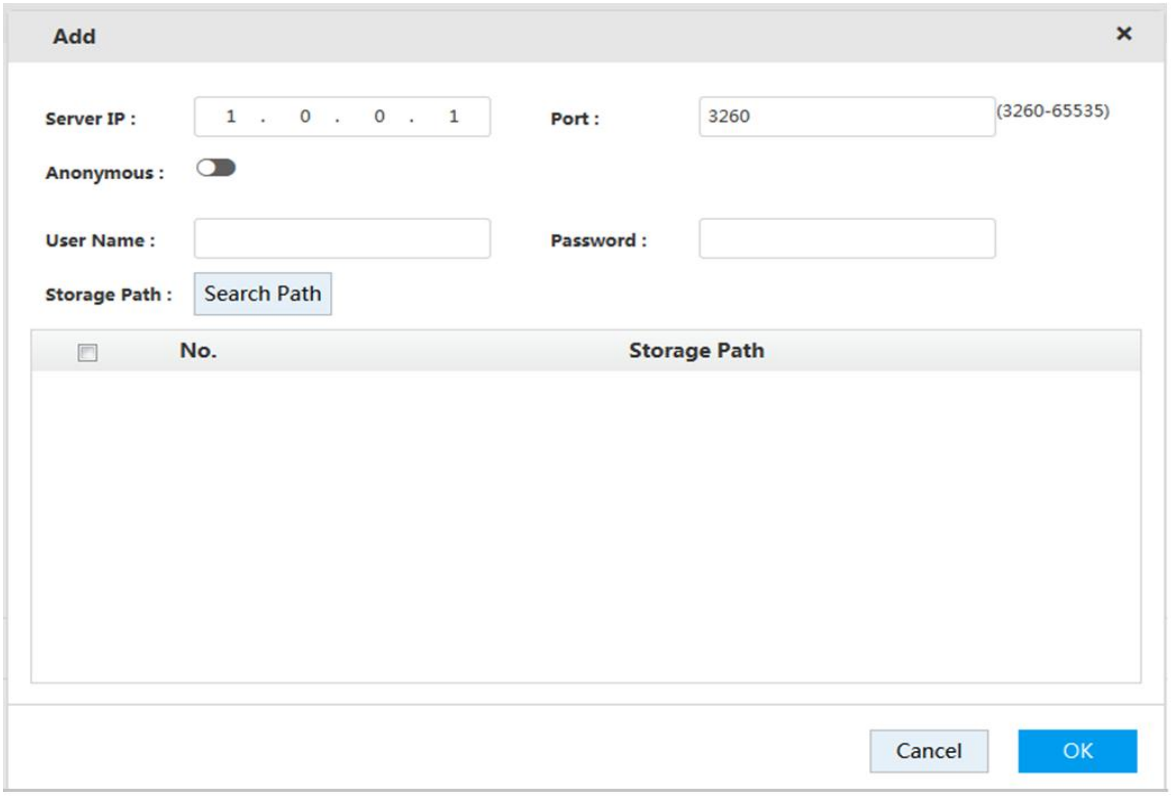
Figure 3-117 Network HDD



Step 2 Click + .

The **Add** interface is displayed. See Figure 3-118.

Figure 3-118 Adding network HDD



Step 3 Configure the parameters. For details, see Table 3-37.

Table 3-37 Network HDD parameters

Parameter	Description
Server IP	Enter the IP address of iSCSI server.
Port	Enter the port number of iSCSI server. The default value is 3260.
Anonymous	When access permission is not set for iSCSI server, you can choose to log in the iSCSI server in anonymity. ● : Anonymous login enabled. You do not need to enter the user name and password. ● : Anonymous login disabled.
User Name Password	If the iSCSI server has set access permission when it creates the share file list, you need to enter the user name and password.
Storage Path	Click Search Path to select the stored path of the network HDD. iSCSI server has generated the corresponding path when it creates the share file list. Each path represents an iSCSI shared disk.

Step 4 Click **OK** to save the configuration.

The system returns to the **Network HDD** interface. You can view the added disk information on this interface.

- Click , and then click **OK** to delete a network HDD. Click **Refresh** to update the network HDD list.
- You can set the disk group of network HDDs on the **Storage Device** interface. For details, see 3.13.2.1 Setting Disk Attribute."

3.13.5 RAID Management

Redundant Arrays of Independent Disks (RAID) organizes multiple independent physical disks to a logical disk group, so that it can provide higher storage performance and data redundancy technology.

- The disk group set for AI playback disk cannot be used to create RAID.
- Currently the following RAID types are supported: RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60, SRAID, RAID2.0, and RAIDJ. For details, see "Appendix 1 RAID Introduction."

3.13.5.1 Creating RAID

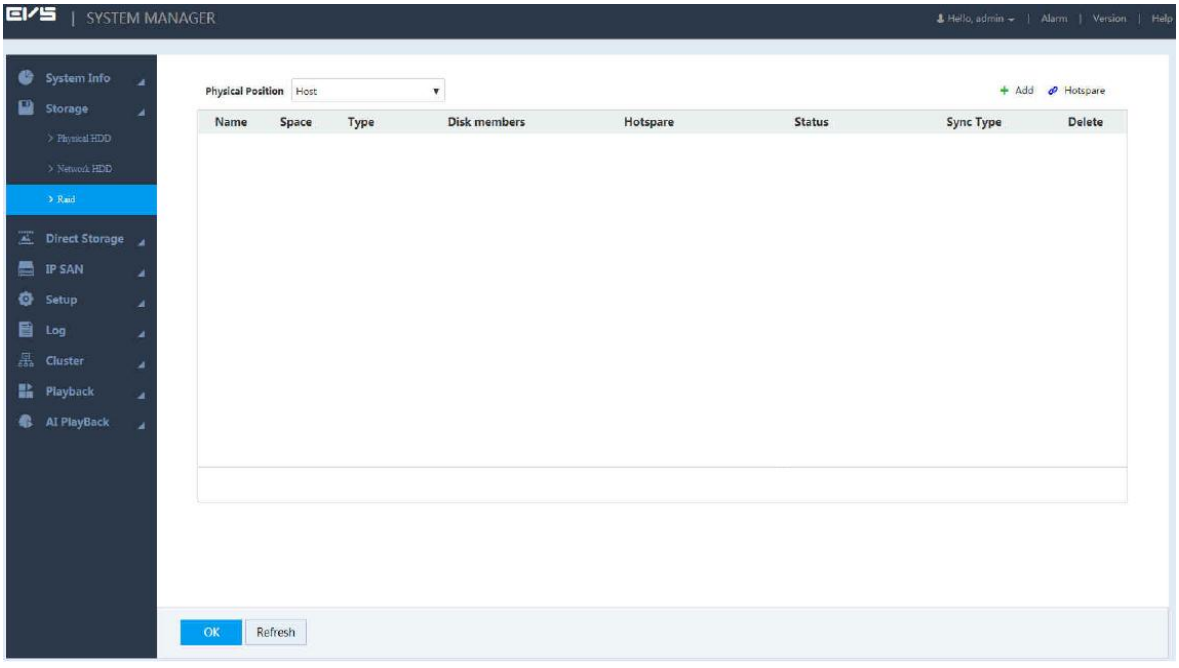
RAID has different levels (such as RAID5, RAID6), and each level has its own data protection, data availability and performance level. You can create RAID according to actual needs.

The system will clear the original data in the disk when creating RAID. Operate with care.

Step 1 Select **Storage > Raid**.

The **Raid** interface is displayed. See Figure 3-119.

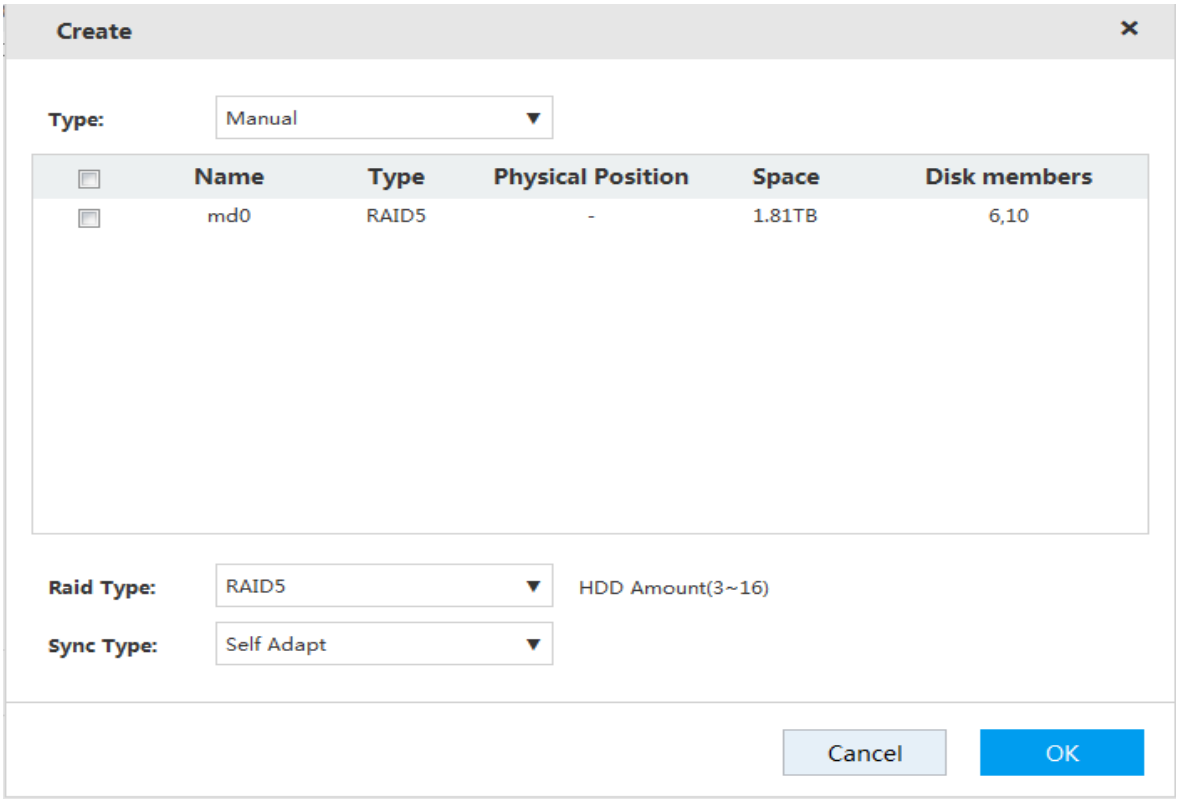
Figure 3-119 Raid management



Step 2 Click + .

The **Create** interface is displayed. See Figure 3-120.

Figure 3-120 Creating RAID



Step 3 Select the parameters. For details, see Table 3-38.

Table 3-38 RAID creation parameters

Parameter	Description
Type	Select the RAID creation type, including manual, shortcut, and Raid2.0. When you choose shortcut RAID creation, the system automatically creates RAID 5 according to the shortcut RAID creation strategy. For details, see Table 3-39. Raid2.0 provides different storage strategies for the same RAID based on your data security requirements. For example, for data of the file system, it offers data security as high as RAID1; for data of ordinary files, it ensures the same security and space utilization of RAID5.
HDD	Select the HDD you want to use to create RAID. Different RAID types need different numbers of disks, depends on the actual situation.
RAID Type	Select the RAID type you want to create.

Parameter	Description
Check Disk	If you select "RAIDJ" as the Raid type, you need to set the check disk. The number of check disk is limited to 1–8.  RAIDJ cannot be created if there is no check disk, the number of check disks is more than 8, or the number of data disk is less than 2 or more than 8.
Raid Strategy	Select Raid strategy. ● If "Raid5" is selected as the Raid type, the system supports 2D+1P, 4D+1P and 8D+1P. ● If "Raid6" is selected as the Raid type, the system supports 2D+2P, 4D+2P, and 8D+2P.  Only when selecting "Raid2.0" as the Type will the system support this function.
Hot Spare Strategy	Select hot spare strategy. Three types of strategies are supported: low, middle and high.  Only when selecting "Raid2.0" as the Type will the system support this function.
Sync Type	Select the sync mode of the business resources allocation. ● Self Adapt: Automatically adjust the RAID sync speed according to the current business loads.  When there is no external business, sync is performed at a high speed. When there is external business, sync is performed at a low speed. ● Sync First: Resource priority is assigned to RAID sync. ● Business First: Resource priority is assigned to business operations. ● Balance: Resource is evenly distributed to RAID sync and business operations.  Only when selecting "Manual" as the Type and "Raid 5" as the Raid Type will the system support this function.

Step 4 Click **OK** to save the configuration.

The system returns to the **Raid** interface. You can view the added RAID information on this interface.

- Click  to delete a RAID, and click **Refresh** to update the RAID list.
- Double-click the RAID line, and you can view the detailed information.

Shortcut RAID Creation Strategy

When the disks are fully installed, the system creates RAID5 according to the policy in Table 3-39.

In the below table, the value 9, 5 and 3 refer to the HDD number in the RAID and 1 refers to hot spare. For example: When fully-installed 24 disks, the creation strategy is 9+9+5+1. Three RAID groups and one hot spare are created, in which the RAID groups respectively include 9 disks, 9 disks and 5 disks.

Table 3-39 Shortcut RAID creation strategy

Full Disk Number	Creation Strategy
16	5+5+5+1
24	9+9+5+1
36	9+9+9+5+3+1
48	(9+9+5+1)*2
64	9*6+5+3+1+1
72	(9+9+5+1)*3

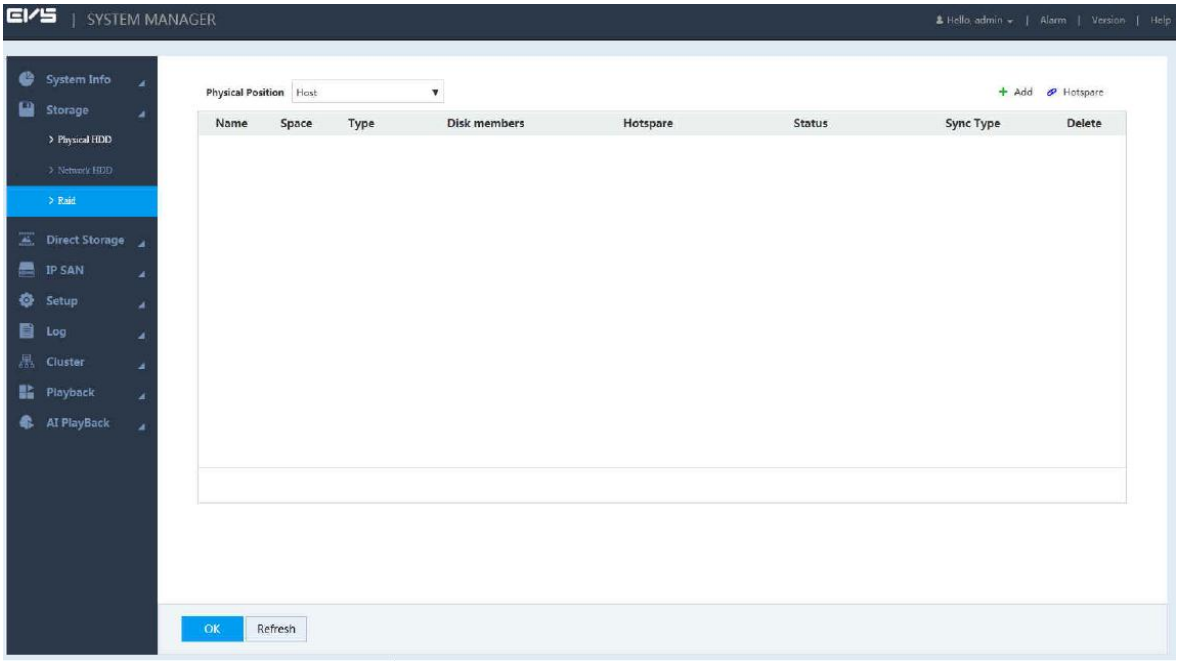
3.13.5.2 Hotspare Management

When a member disk of the RAID group is fault or abnormal, the hot spare disk replaces it to work. This helps avoid data loss and guarantee the reliability of the storage system.

Step 1 Select **Storage > Raid**.

The **Raid** interface is displayed. See Figure 3-121.

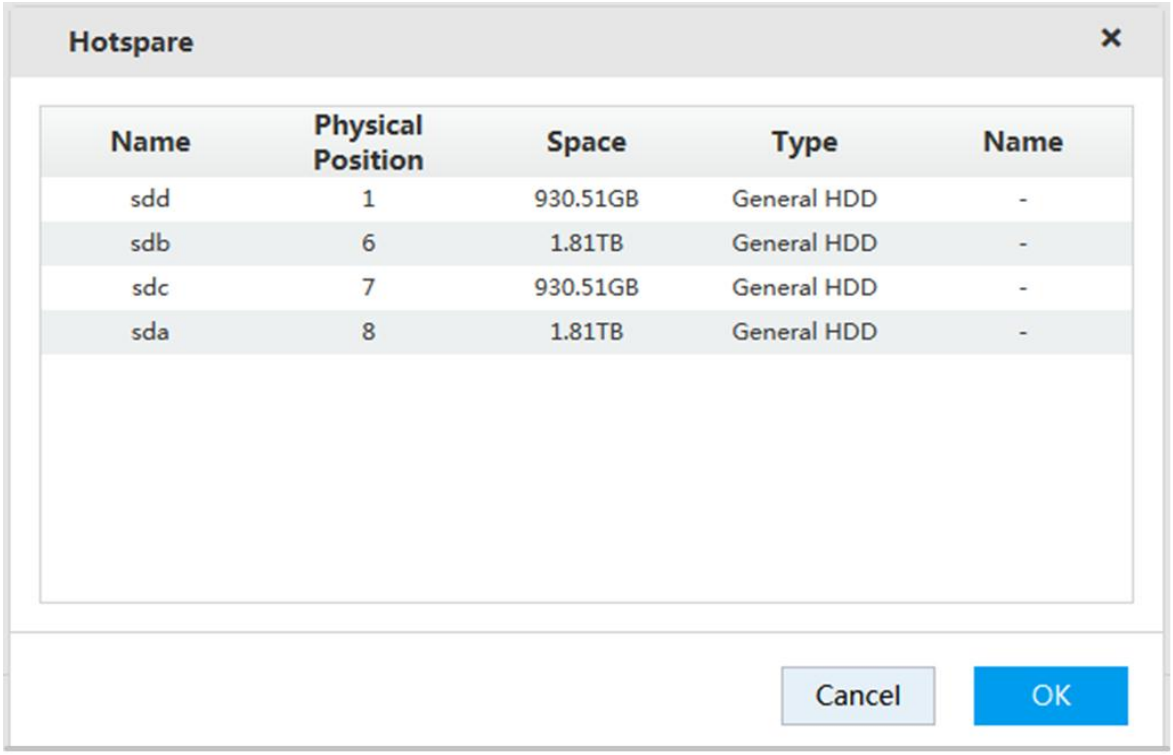
Figure 3-121 RAID management



Step 2 Click .

The **Hotspare** interface is displayed. See Figure 3-122.

Figure 3-122 Hotspare management



Step 3 Double-click the corresponding **Type** to set the disk to general HDD, private hot spare or general hot spare.

- General HDD: A general disk member in the RAID.
- Private hot spare: Double-click the corresponding **Name**, select the RAID group, and then this HDD is used as a hot spare only for the corresponding RAID.
- General hot spare: It is used as a hot spare for all the RAID groups.

Step 4 Click **OK** to save the configuration.

3.14 Configuring the System

Configure the network, basic information and alarm events, including TCP/IP settings, general settings, user management, event configuration, network application, and system maintenance.

3.14.1 Setting TCP/IP

TCP/IP settings include the IP address settings of the Device and P2P settings. Dual-control devices also support virtual IP configuration.

3.14.1.1 Setting IP

According to network plan, set the Device information such as the IP address, and DNS server. Select **Setup > TCP/IP > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 3-123 and Figure 3-124. For details, see 3.4.1 Setting IP.

Figure 3-123 TCP/IP settings (single-control device)

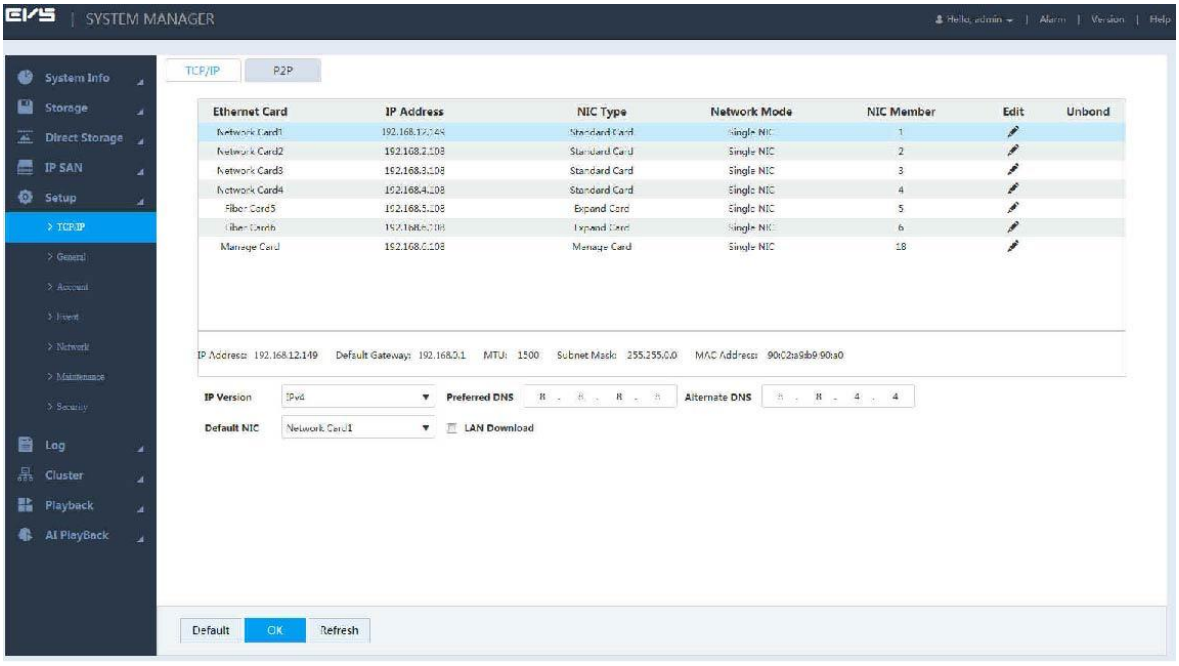
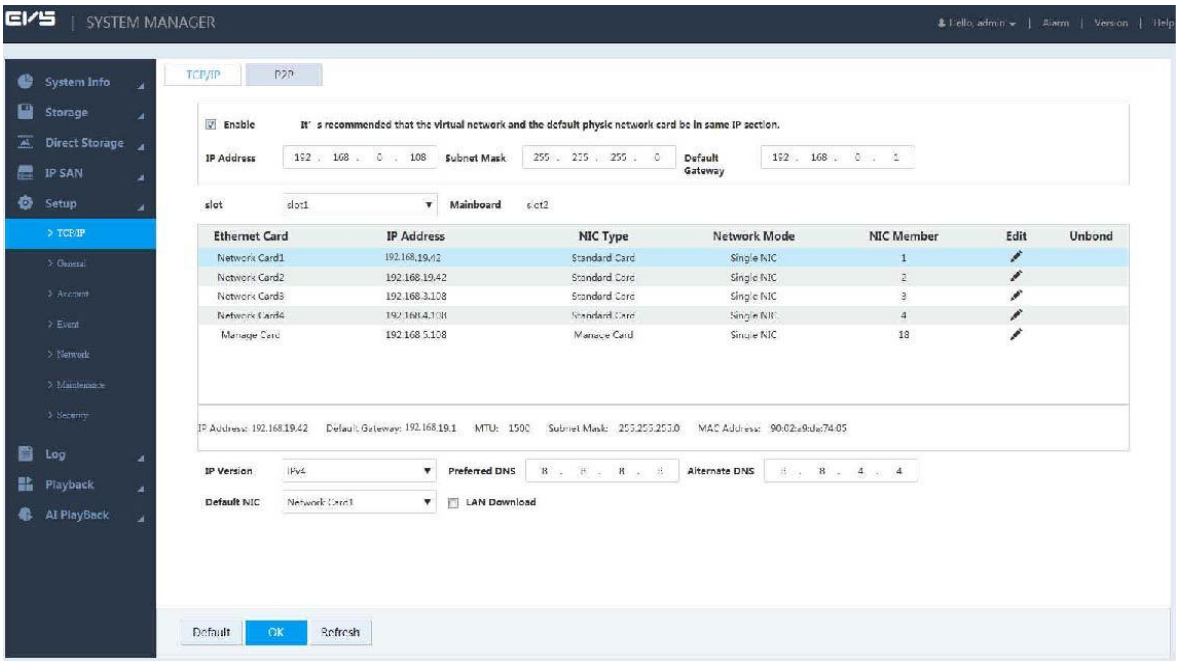


Figure 3-124 TCP/IP settings (dual-control device)



3.14.1.2 Virtual IP

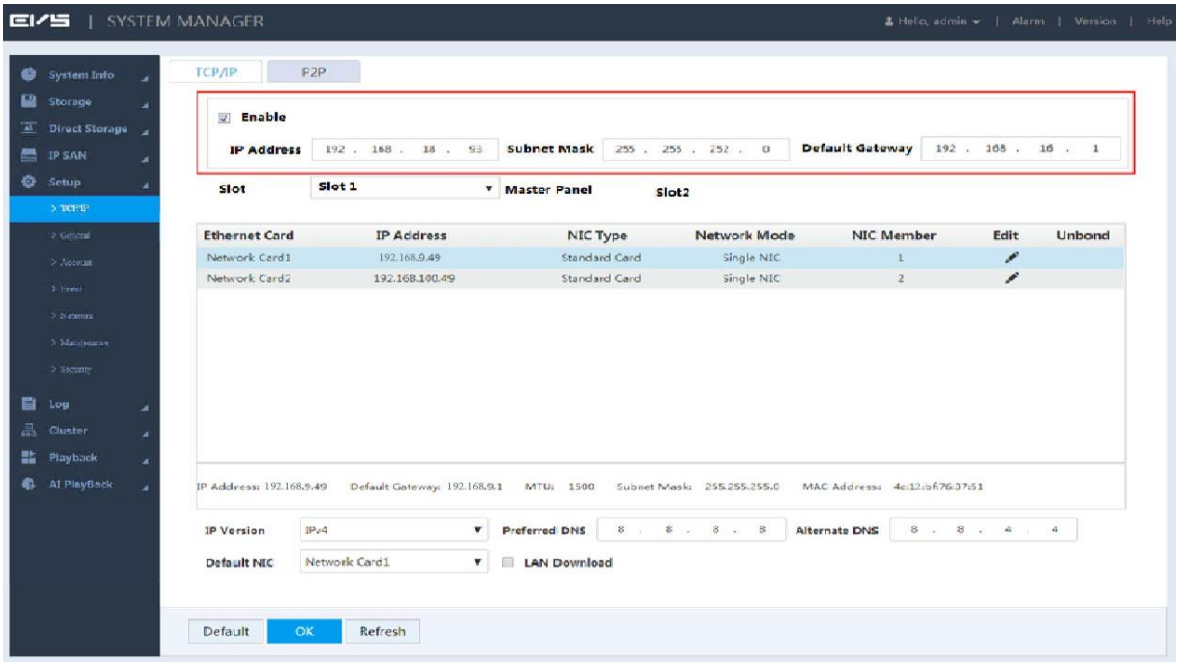
The master control panel and slave control panel have their own physical IP. After setting virtual IP, regardless of switching between master and slave panels, you can log in the web normally.

Only dual-control devices support this function.

Step 1 Select **Setup > TCP/IP > TCP/IP**.

The **TCP/IP** interface is displayed. See Figure 3-125.

Figure 3-125 NIC settings



Step 2 Select the **Enable** check box to open virtual IP.

Step 3 Enter the **IP address**, **Subnet Mask** and **Default Gateway**.

Step 4 Click **OK** to save the configuration.

3.14.1.3 Peer-to-peer (P2P)

P2P is a kind of intranet penetration technology. With P2P, you do not need to apply for dynamic domain name, doing port mapping or deploying transit server. You can add devices through the following method to manage multiple devices at the same time.

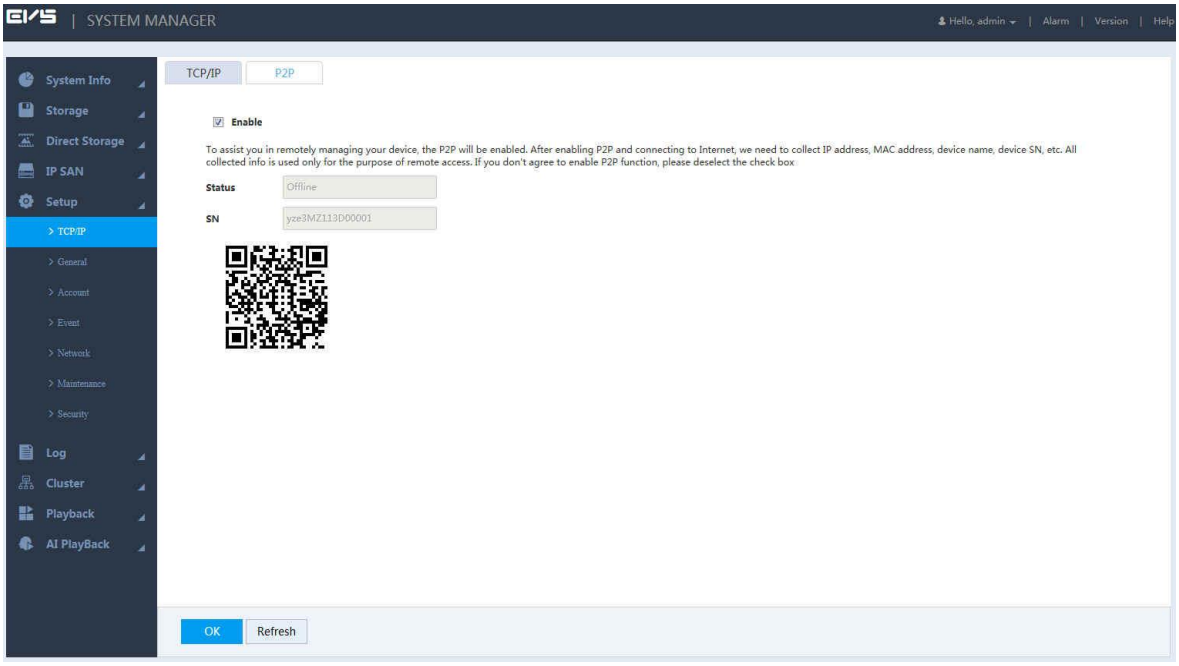
- Scan the QR code, download cell phone app, and then register an account. For details, see *Operations on Cell Phone App*.

You have to connect the Device to the external network when using P2P function.

Step 1 Select **Setup > TCP/IP > P2P**.

The **P2P** interface is displayed. See Figure 3-126.

Figure 3-126 P2P



Step 2 Select **Enable** to enable P2P function.

Step 3 Click **OK** to save the configuration.

After setting, if the **Status** is **Online**, then P2P registration succeeded.

Operations on Cell Phone App

Take the mobile phone client as an example. See the following operations:

Step 1 Use the cell phone to scan the QR code on the interface and then download and install the app.

Step 2 Open the app. Select **Remote Monitor** to enter the main interface.

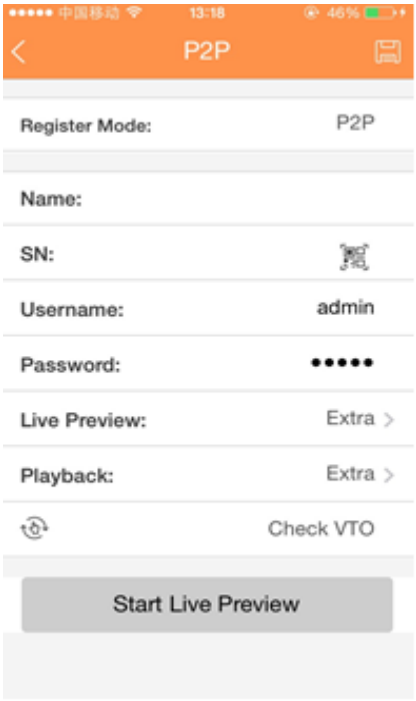
Step 3 Add device on the cell phone app.

1) Tap and select **Device Management**.

2) Tap to enter the QR code scanning interface. Scan the device label or the **SN** QR code shown in Figure 3-127.

After the device is added, its serial number is displayed in **SN**.

Figure 3-127 Adding device



3) Tap **Start Live Preview** to view real-time video.

3.14.2 General Information Settings

Set the general device information such as date, and holiday.

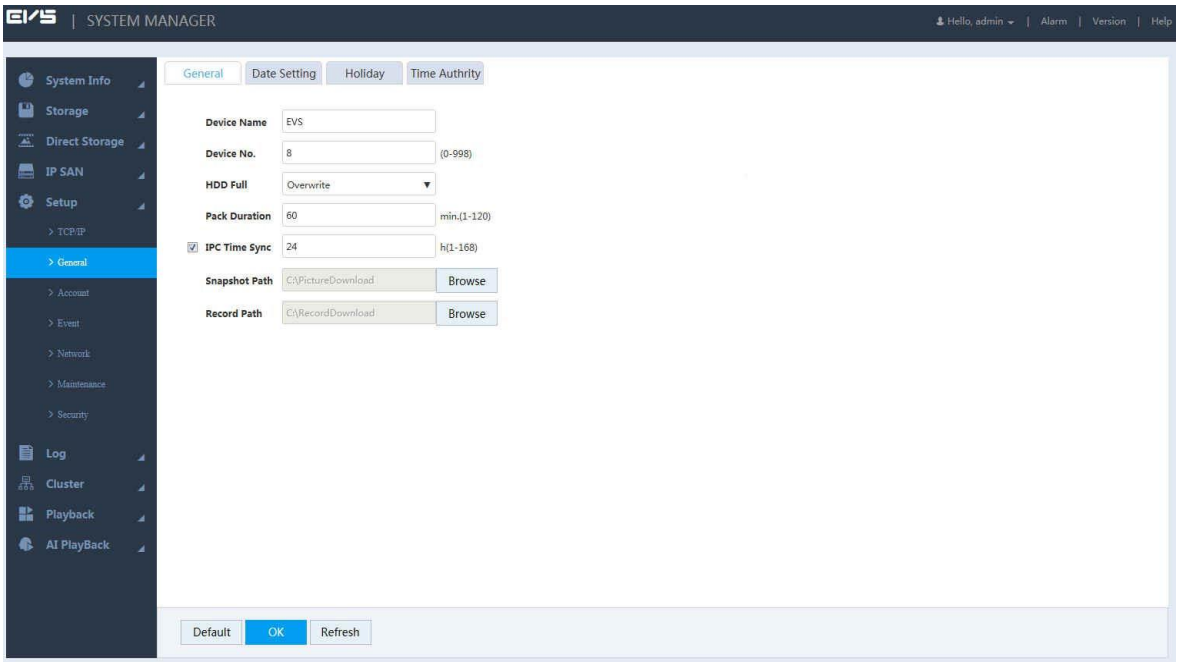
3.14.2.1 Setting General Information

Set information like the device name, number, snapshot, and record storage path.

Step 1 Select **Setup > General > General**.

The **General** interface is displayed. See Figure 3-128.

Figure 3-128 Setting general information



Step 2 Configure the parameters. For details, see Table 3-40.

Table 3-40 General information setting parameters

Parameter	Description
Device Name	Enter the device name.
Device No.	Enter the device number.
HDD Full	Select the record strategy when the HDD is full, including **Stop Record** and **Overwrite**. ● Stop Record: Stop recording when the current working disk is full and there is no extra free disk available. ● Overwritten: Overwriting the earliest records when the current working disk is full and there is no extra free disk available.
Pack Duration	Enter the time duration of each record. The maximum length is 120 minutes.
IPC Time Sync	Select this check box to set the time interval that IPC synchronizes the time with the Device.
Snapshot Path	Click **Browse** at the right side of **Snapshot Path**, and you can set the storage path of manual snapshot. The default path is C:\PictureDownload.
Record Path	Click **Browse** at the right side of **Record Path**, and you can set the storage path of manual record. The default path is C:\ RecordDownload.

Step 3 Click **OK** to save the configuration.

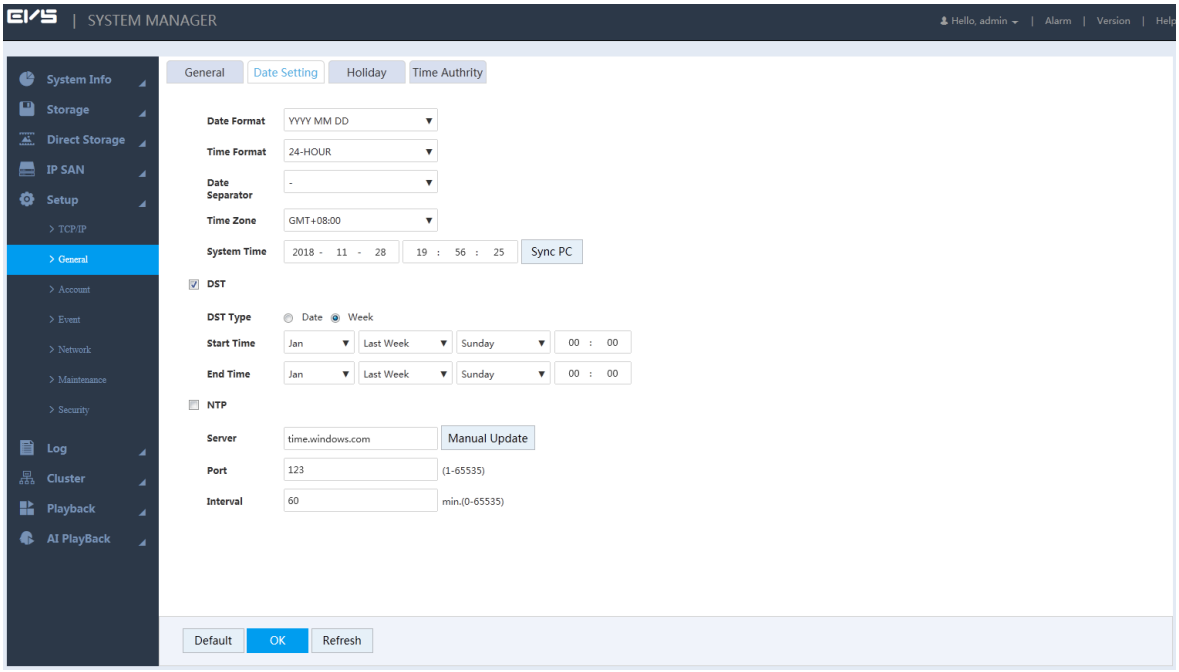
3.14.2.2 Setting Date

Set the system date of the Device. You can also enable Network Time Protocol (NTP) according to your needs. After enabling NTP, the Device automatically synchronizes time with the NTP server.

Step 1 Select **Setup > General > Date Setting**.

The **Date Setting** interface is displayed. See Figure 3-129.

Figure 3-129 Setting date



Step 2 Configure the parameters. For details, see Table 3-41.

Table 3-41 Date setting parameters

Parameter	Description
Date Format	Select the date format of the Device, including YYYY MM DD, MM DD YYYY, DD MM YYYY.
Time Format	Select the time format of the Device, including 24-HOUR and 12-HOUR.
Date Separator	Select the separator between year, month and day.
Time Zone	Select the current time zone that the Device locates in.
System Time	Configure the current system date and time.
Sync PC	Click **Sync PC** and the system automatically synchronizes time with the PC logged in web.
DST	Some countries and regions implement DST (Daylight Saving Time). Enable DST according to actual needs. For steps, see below: 1. Select the **DST** check box to enable DST. 2. Select the DST type, including **Date** and **Week**. 3. Select the **Start Time** and **End Time** of DST.
NTP	The device automatically synchronizes time with the NTP server. For steps, see below: 1. Select the **NTP** check box to enable NTP. 2. Configure the parameters: ● Server: Enter the IP address or domain name of the NTP server. ● Manual Update: Click **Manual Update** and the system synchronizes time with NTP server in real time. ● Port: the system only supports TCP transmission, and the port is limited to 123. ● Interval: the interval that the device synchronizes time to the NTP server. The maximum update period is 65,535 minutes.

Step 3 Click **OK** to save the settings.

3.14.2.3 Setting Holiday

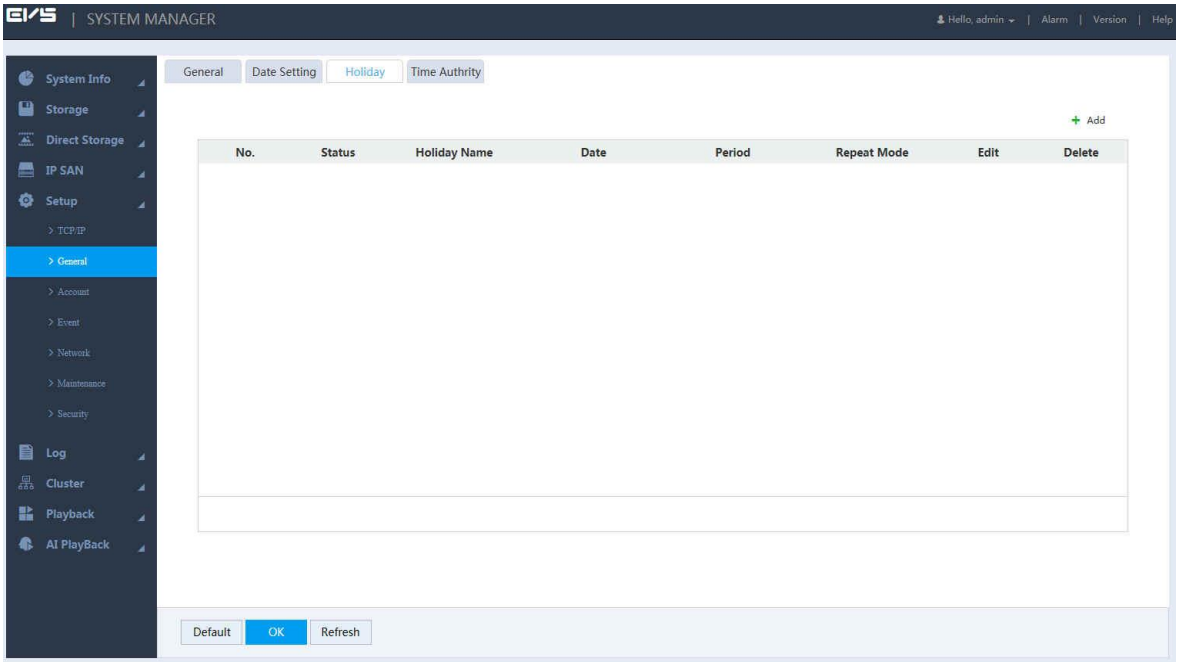
Add, edit and delete holiday information. After setting the holiday, holiday option will appear on the interfaces of setting record and snapshot.

The priority of holiday settings is higher than the settings of normal days. For example, when both of the holiday plan and the normal day plan are set, the system records according to the settings of holiday plan.

Step 1 Select **Setup > General > Holiday**.

The **Holiday** interface is displayed. See Figure 3-130.

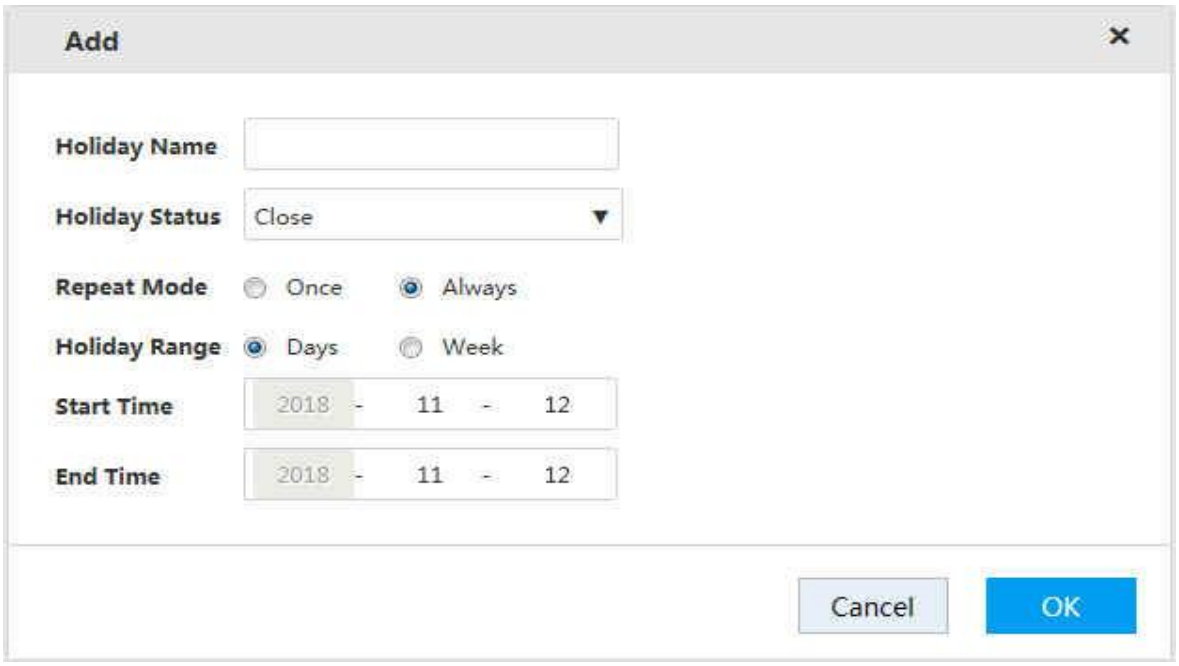
Figure 3-130 Setting holiday (1)



Step 2 Click + .

The **Add** interface is displayed. See Figure 3-131.

Figure 3-131 Adding holiday



Step 3 Configure the parameter. For details, see Table 3-42.

Table 3-42 Holiday setting parameters

Parameter	Description
Holiday Name	Enter the holiday name.
Holiday Status	Select the holiday status, including Open and Close.

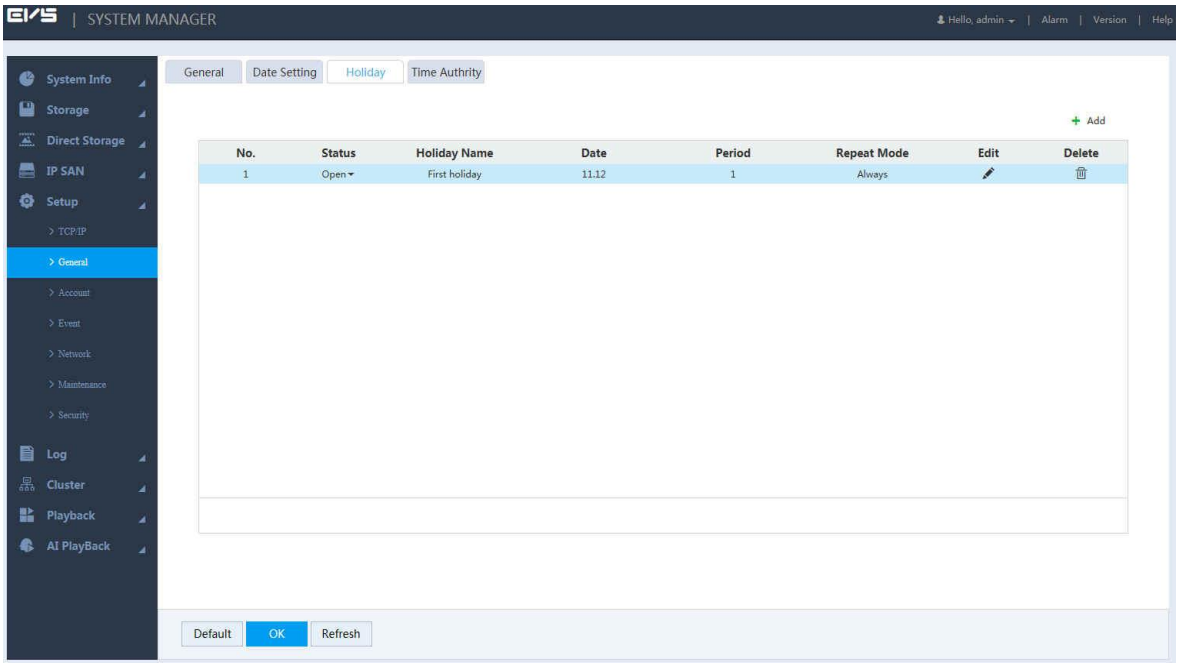
Parameter	Description
Repeat Mode	Select the repeat mode, including Once and Always. ● Once: The holiday takes effect only once. ● Always: The holiday takes effect repeatedly.
Holiday Range	Select the holiday range, including Days and Week.
Start Time	Enter the start time and end time of the holiday.
End Time	

Step 4 Click **OK** to save the settings.

The **Holiday** interface is displayed. See Figure 3-132.

- Click the drop-down list of the corresponding holiday status to open or close the holiday.
- Click to edit the holiday, and click to cancel the holiday.

Figure 3-132 Setting holiday (2)



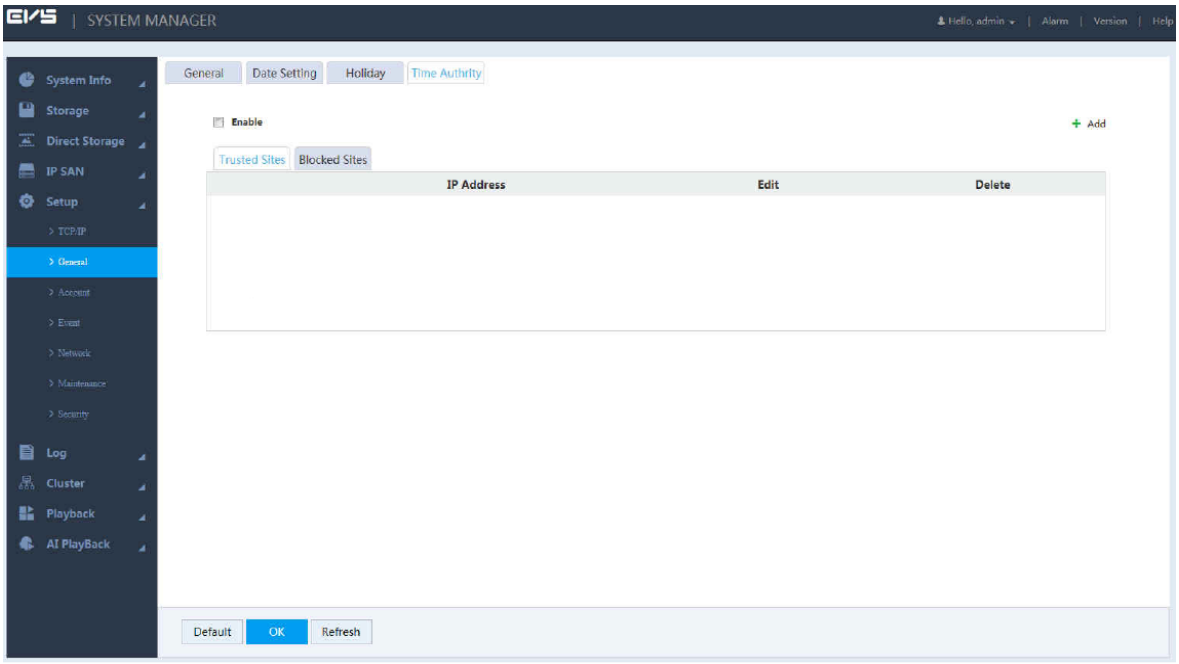
3.14.2.4 Timing Authority

By setting the trusted timing list, it allows the specified IP host to synchronize or modify device time. This helps prevent multiple IP hosts from checking system time with the same device repeatedly.

Step 1 Select **Setup > General > Time Authority**.

The **Time Authority** interface is displayed. See Figure 3-133.

Figure 3-133 Timing authority



Step 2 Select the **Enable** check box to enable this function.

Step 3 Select **Trusted Sites** or **Blocked Sites**.

Step 4 Add IP host.

1) Click **Add**.

The **Add** interface is displayed. See Figure 3-134.

Figure 3-134 Adding IP host

2) Enter the IP address.

3) Click **OK** to save the configuration.

The system returns to the Time Authority interface.

Step 5 Click **OK** to save the configuration.

3.14.3 Network Application

Set the network parameters of the Device to ensure that it can communicate with other devices in the networking.

3.14.3.1 General Settings

General network configuration includes the settings of port, HTTPS, IP filter, and platform server.

3.14.3.1.1 Connection Port

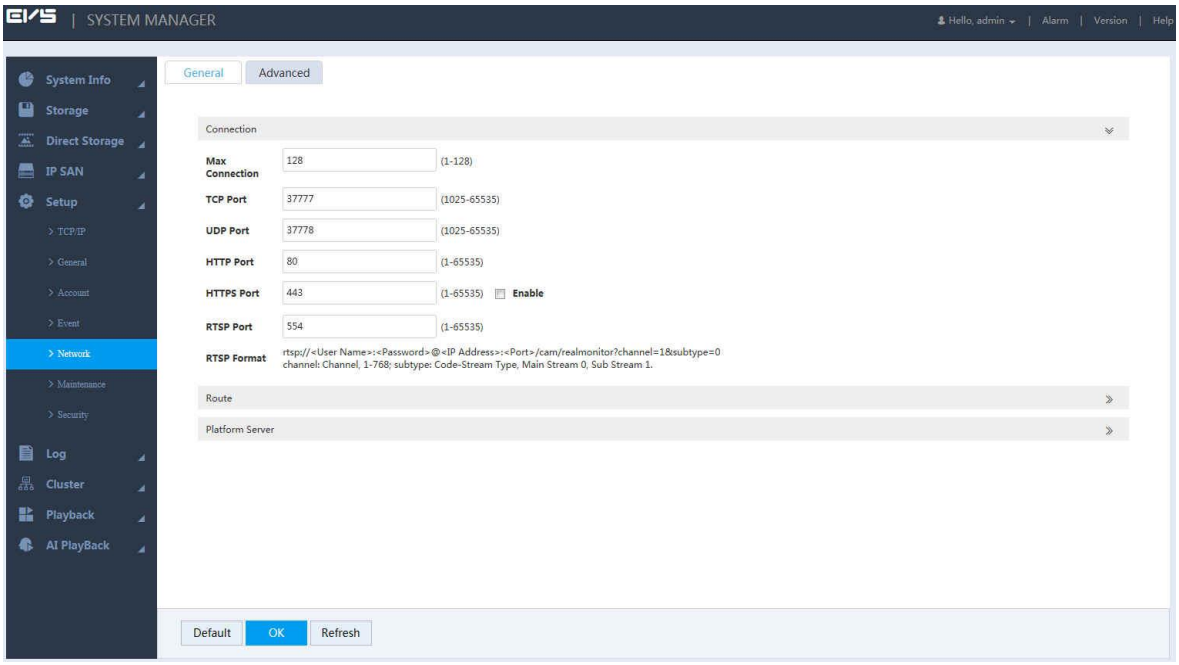
Set the maximum number of connection ports, and their respective port number when multiple clients (such as web client, platform client, mobile phone client) visit the Device at the same time.

Step 1 Select **Setup > Network > General**.

Step 2 Click » corresponding to **Connection**.

The **Connection** interface is displayed. See Figure 3-135.

Figure 3-135 General network settings



Step 3 Configure the parameters. For details, see Table 3-43.

Except Max Connection, if you change the settings of other parameters, they work only after restarting the Device.

Table 3-43 Port parameters

Parameter	Description
Max Connection	The max number of clients logging in the device at the same time (such as web client, platform client, and mobile phone client). It ranges from 0 to 128. The default value is 128.
TCP Port	Provides TCP protocol services. The default value is 37777.
UDP Port	User data packet protocol port. The default value is 37778.
HTTP Port	HTTP communication port. The default value is 80. If you change it to other value, you need to add the port number after the IP address when logging in through browser.

Parameter	Description
HTTPS Port	HTTPS communication port. Select the **Enable** check box and set the port according to actual needs. The default value is 443. The change of HTTPS works only after restarting the Device. Operate with care.
RSTP Port	● The default value is 554, and you do not need to enter the value when using the default. ● When real-time monitoring RTSP media services, you need to specify the channel number and stream type in URL. If verification is required, you also need to provide user name and password. URL format: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 ● User name: Such as admin. ● Password: Such as admin. ● IP: Such as 10.7.8.122. ● Port: The default value is 554. Skip it if using the default. ● Channel: Start from 1. For example, if select 2, then channel=2. ● Subtype: stream type. Main stream is 0 (subtype=0), and sub stream is 1 (subtyoe=1). For example: Request the sub stream of channel 2. URL see below: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If verification is not required, you do not need to specify the user name and password. Format see below: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0

Step 4 Click **OK** to save the configuration.

3.14.3.1.2 Route

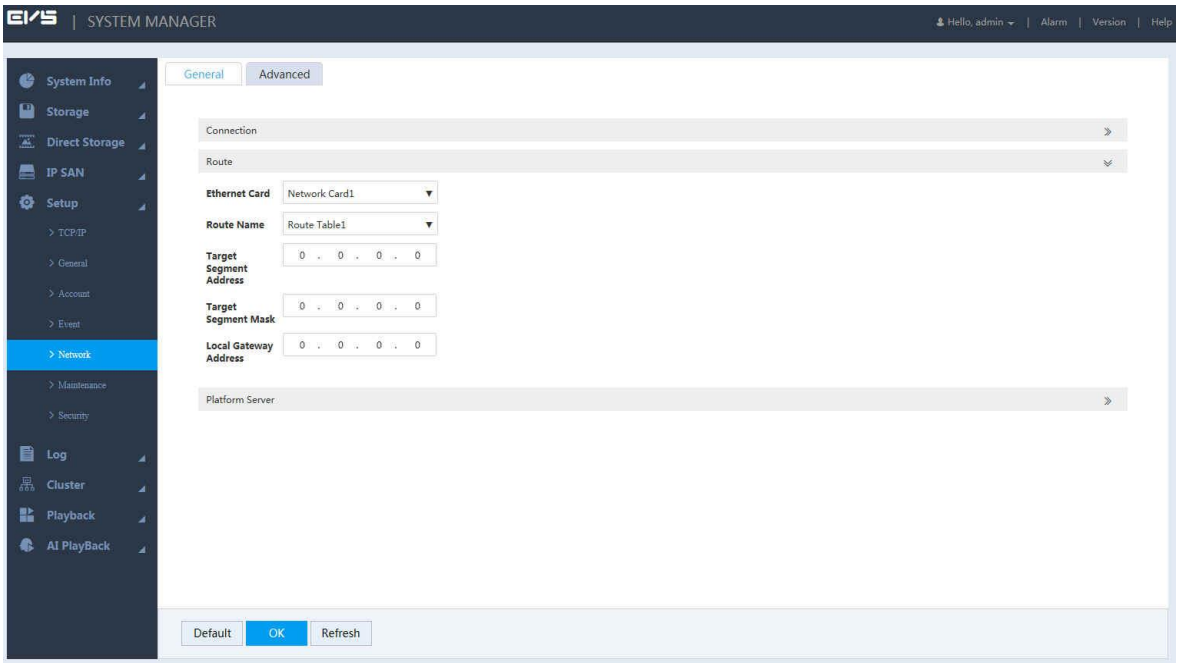
The system supports dual routing table, and permanent static route. Route settings will not lose when restarting the Device.

Step 1 Select **Setup > Network > General**.

Step 2 Click » corresponding to **Route**.

The Route interface is displayed. See Figure 3-136.

Figure 3-136 Route



Step 3 Configure the parameters. For details, see Table 3-44.

Table 3-44 Route parameters

Parameter	Description
Ethernet Card	Select the network card.
Route Name	Select the route table.
Target Segment Address	Enter the target segment address of route, and set the target segment mask and local gateway address corresponding to the target segment address. The target segment address and the local gateway address must be in the same network segment.
Target Segment Mask	
Local Gateway Address	

Step 4 Click **OK** to save the configuration.

3.14.3.1.3 Platform Server

When the platform disconnects with the Device and the pictures in the Device cannot be synchronously uploaded to the platform. After the network is reconnected, the pictures directly stored can be uploaded continuously to the platform through the platform server.

Preparation

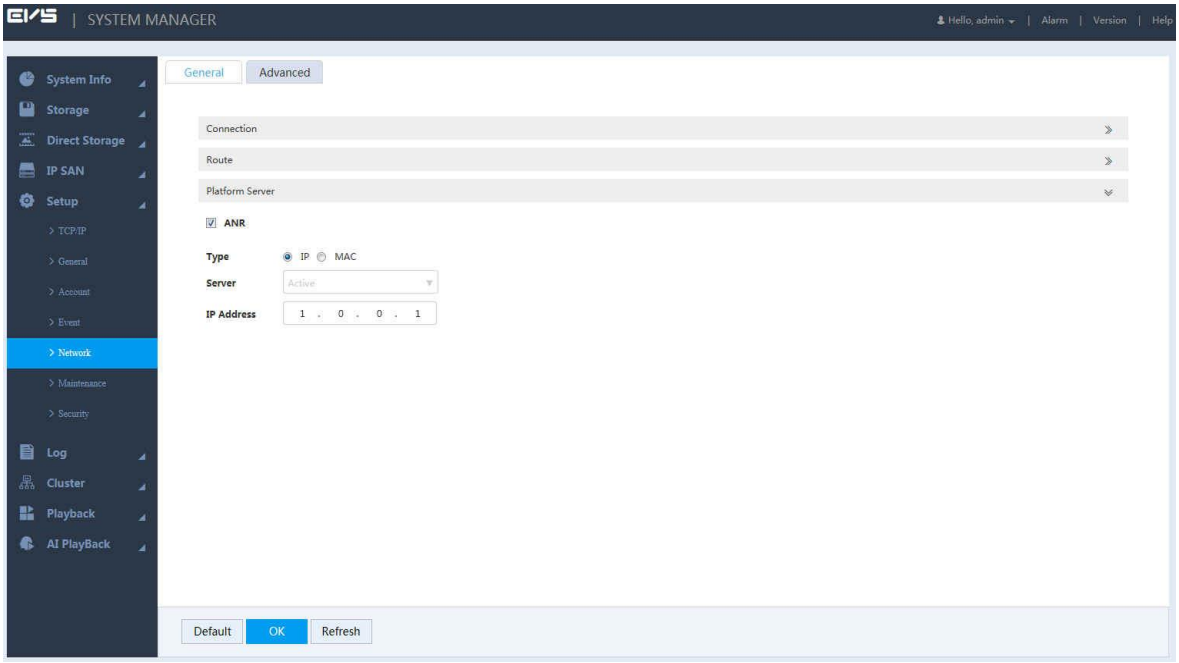
- One or more disk(s) is (are) set as image direct storage disk(s). For details, see "3.13.2.1 Setting Disk Attribute."
- ITC or Smart IPC device is added. For details, see "3.4.2 Adding Remote Device."
- AI playback is enabled. For details, see "3.4.4 Enabling Record Function."

Step 1 Select **Setup > Network > General**.

Step 2 Click » corresponding to **Platform Server**.

The **Platform Server** interface is displayed. See Figure 3-137.

Figure 3-137 Platform server



Step 3 Configure the parameters. For details, see Table 3-45.

Table 3-45 Platform server parameters

Parameter	Description
ANR	Select the check box to enable the function. After the network is reconnected between the platform server and the Device, the Device automatically uploads the directly stored images during network disconnection to the platform server. This helps keep the completeness of images.
Type	Select the address type of the platform server, including IP address and MAC address.
Server	Select the registration mode of the Device and platform server. The default mode is **Active**.
IP Address	Enter the IP address or MAC address of the platform server.
MAC Address	

Step 4 Click **OK** to save the configuration.

3.14.3.2 Advanced Settings

Advanced network configuration includes the settings of PPPoE, DDNS, Email, FTP, UPnP, SNMP, multicast, active registration and bandwidth management.

3.14.3.2.1 DDNS

After setting the parameters of Dynamic Domain Name Server (DDNS), when the IP address of the Device changes frequently, the system can dynamically update the relation between the

domain name and IP address on the DNS server. Instead of recording the frequently changing IP address, you can directly use the domain name to remotely access the device.

Preparation

Before executing configuration, you need to confirm the DNS server type that the Device supports. In addition, you need to register on the website of DDNS service provider, and log in to the WAN PC.

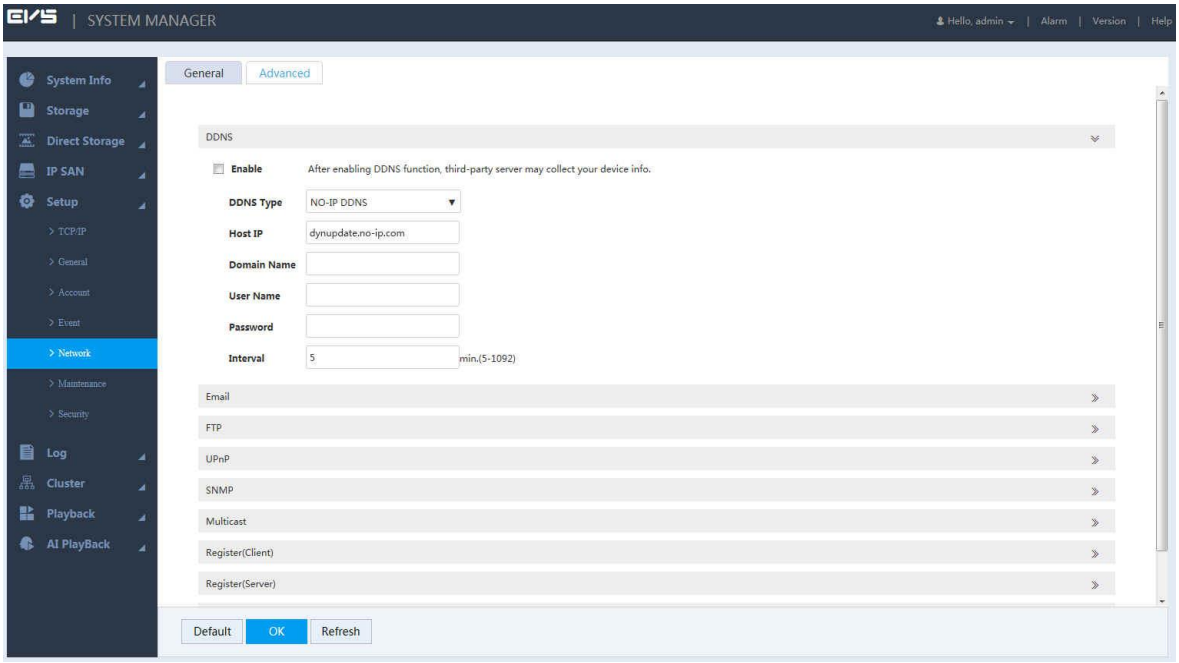
After registering successfully on the DDNS website and logging in, you can view all the information of the connected devices related to your registered account.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **DDNS**.

The **DDNS** interface is displayed. See Figure 3-138.

Figure 3-138 DDNS



Step 3 Select the **Enable** check box.

Step 4 Configure the parameters. For details, see Table 3-46.

Table 3-46 DDNS parameters

Parameter	Description
DDNS Type	Name of the DDNS server provider.
Host IP	See below for the corresponding addresses of the DDNS server providers: ● NO-IP DDNS: dynupdate.no-ip.com. ● CN99 DDNS: members.3322.org. ● Dyndns DDNS: members.dyndns.org.
Domain Name	The domain name that the user registered on the DDNS provider website.
User Name	Enter the user name and password you got from the DDNS service provider.

Parameter	Description
Password	You need to register an account (including user name and password) on the DDNS provider website.
Interval	The time interval to initiate update requests. The unit is minute.

Step 5 Click **OK** to save the configuration.

Step 6 (Optional) Enter the domain name in the browser address bar of your PC, and press Enter.

If the device web interface is displayed, the configuration succeeded. If not, the configuration failed and you need to check the reason.

3.14.3.2.2 Email Settings

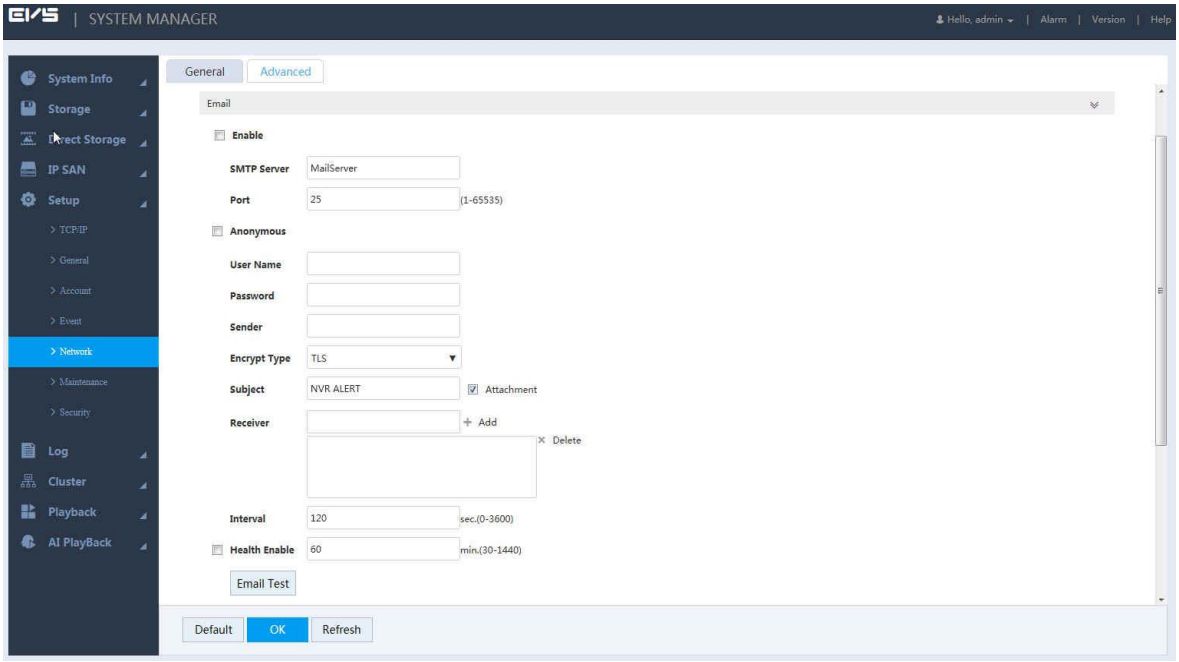
After enabling email alarm linkage, the Device automatically sends email to the user when the corresponding alarm occurs.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **Email**.

The **Email** interface is displayed. See Figure 3-139.

Figure 3-139 Email settings



Step 3 Select the **Enable** check box.

Step 4 Configure the parameters. For details, see Table 3-47.

Table 3-47 Email setting parameters

Parameter	Description
SMTP Server	Enter the server address of Simple Mail Transfer Protocol (SMTP).
Port	Enter the SMTP server port number.
Anonymous	Select the check box to allow anonymous login.
User Name	Enter the user name and password of the SMTP server.
Password	
Sender	Enter the Email address of the sender.

Parameter	Description
Encryption Type	Select the encryption type, including NONE, Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
Subject	Enter the subject of the Email. It supports to enter both Chinese and English characters, and Arabic numbers. You can enter 63 characters at most.
Receiver	Enter the email address of the receiver. Click + to add a receiver. You can set three receivers at most. ● It supports adding no more than email addresses of three receivers at the same time. Separate the addresses with ":". ● Select the added receiver address and click **Delete** to delete the receiver.
Interval	After entering the **interval**, when an alarm or an abnormal event is triggered, instead of sending an email immediately, the system will send an email according to the time interval of previous similar events. ● By entering **Interval**, it can avoid frequent abnormal alarms or events which produce a large number of emails, and lead to large stress of the email server. ● You can enter 0–3,600 seconds in the **Interval**. Setting 0 means no time interval.
Health Enable	Select this check box to set the sending interval of health email. The system sends email test information according to the set interval to check whether the email connection is successful. You can enter 30–1,440 minutes for health email interval.
Email Test	Test if the email function work. The email box can receive test emails if the configuration is correct. Before email test, you need to click **OK** to save the email configuration.

Step 5 Click **OK** to save the configuration.

3.14.3.2.3 FTP

Set the FTP server and you can store the records and images in the server.

Preparation

You need to purchase or download FTP service tools and install the tools in your PC.

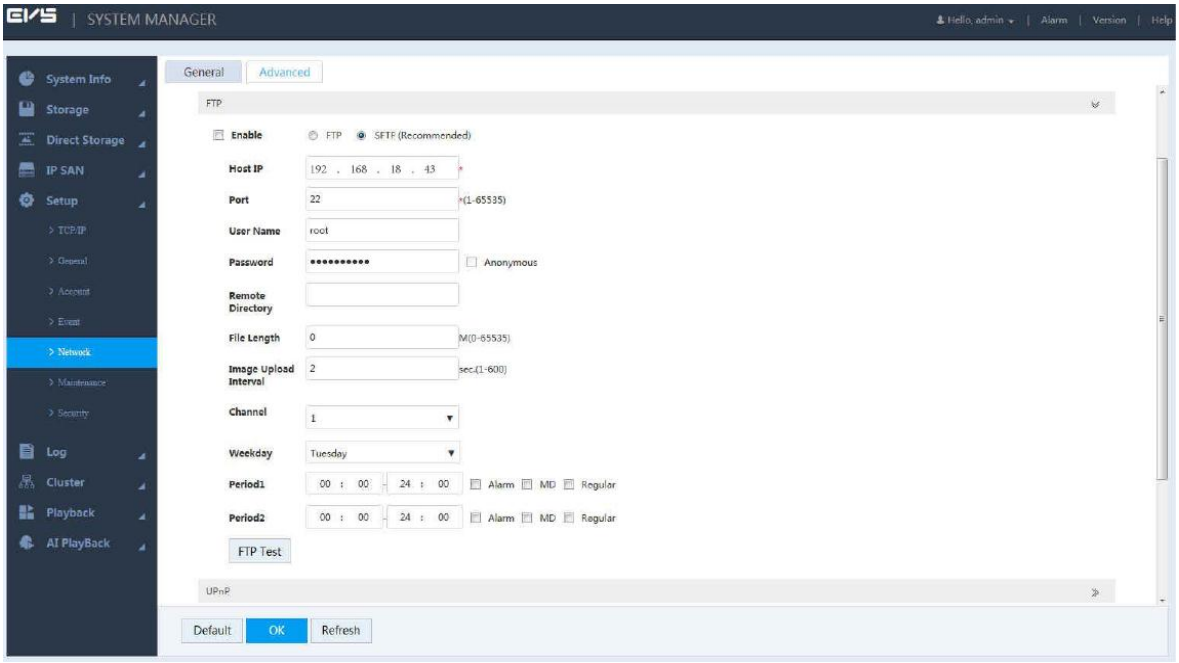
When creating a FTP user, you need to set the write permission of FTP folder. Otherwise, you cannot upload the file.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **FTP**.

The **FTP** interface is displayed. See Figure 3-140.

Figure 3-140 FTP



Step 3 Select the **Enable** check box.

Step 4 Configure the parameters. For details, see Table 3-48.

Table 3-48 FTP parameters

Parameter	Description
Host IP	Enter the IP address of the host which has installed the FTP service.
Port	Enter the port number to connect FTP server. The default number is 21.
User Name	The username and password to access FTP server. Select the **Anonymous** check box and it supports anonymous access to FTP server.
Password	
Remote Directory	Create folders according to the rules in the root directory of FTP account. ● When the remote directory is empty, the system automatically creates different folders according to IP, time and channel. ● Enter the remote directory name. The system creates a folder in the root directory of FTP, and then creates different folders according to IP, time and channel.

Parameter	Description
File Length	Enter the size of the uploaded record files. ● When the set length is smaller than the record length, only a part of the record within the set length is uploaded. ● When the set length is larger than the record length, the whole record is uploaded. ● When the length is set as zero, it uploads the whole record file.
Image Upload Interval	Enter the time interval to upload images. ● When the image upload interval is larger than the snapshot frequency, the system uploads the latest image. For example, when the image upload interval is five seconds, and the snapshot frequency is two seconds per image, the system uploads a latest snapshot image every five seconds. ● When the image upload interval is smaller than the snapshot frequency, the system uploads images according to the snapshot frequency. For example, when the upload interval is five seconds, and the snapshot frequency is ten seconds per image, the system uploads an image every ten seconds.  You can modify the snapshot frequency. For details, see "Setting Image Stream."
Channel	Select the channel to upload records.  **All** means all the channels can upload records and images.
Weekday	Select the weekday and alarm type, and enter the periods. The system uploads records and images according to the set time period. You can set two periods for each weekday.
Period	
FTP Test	Click **FTP Test** to check whether the FTP connection succeeded. ● Succeeded: The system prompts that FTP test succeeded. ● Failed: The system prompts that FTP test failed. You need to check whether the network connection or configuration is correct.

Step 5 Click **OK** to save the configuration.

3.14.3.2.4 UPnP

After establishing mapping relation between internal and external network through UPnP Protocol, users in the external network can access the devices in the internal network directly with the external IP address.

Preparation

- Log in the router, and set the IP address of the WAN port to access external network.
- UPnP function of the router is enabled.
- Connect the Device to the LAN port of the router to access private network.

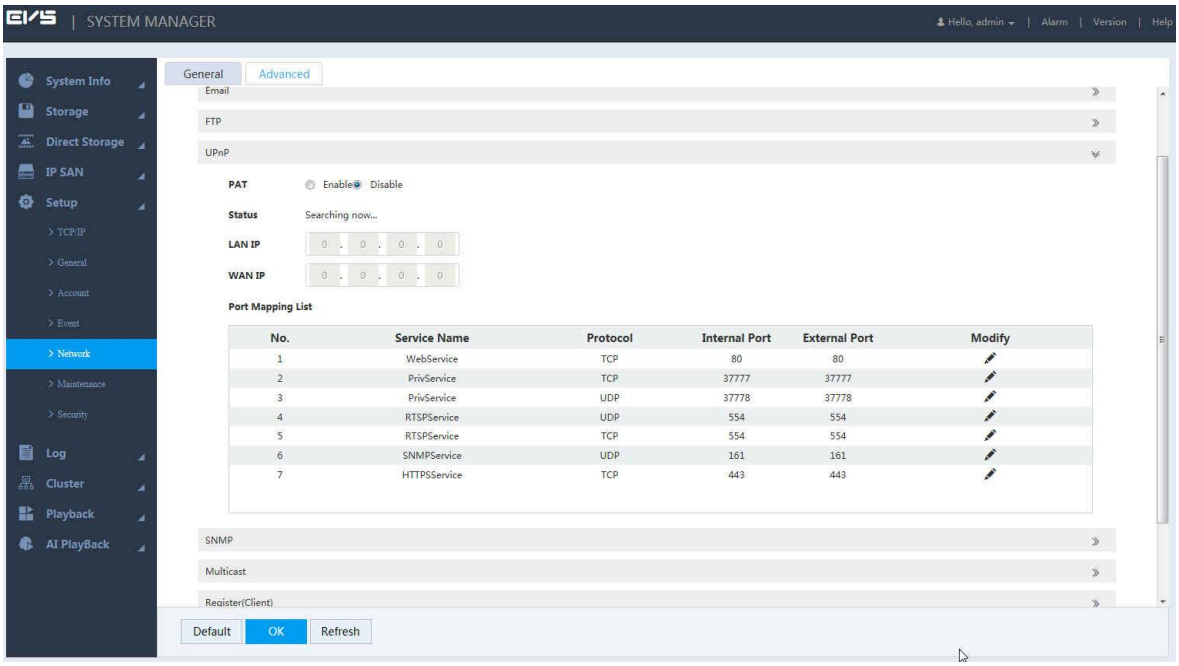
- Set the IP address of the Device to the private IP of the router (e.g. 192.168.1.101). For details, see "3.14.1.1 Setting IP."

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **UPnP**.

THE **UPnP** interface is displayed. See Figure 3-141.

Figure 3-141 UPnP



Step 3 Configure the parameters. For details, see Table 3-49.

Table 3-49 UPnP parameters

Parameter	Description
PAT	Select the **Enable** check box to enable UPnP function.
Status	Displays the UPnP status. ● Displays **Disabled** when the mapping failed. ● Displays **Enabled** when the mapping succeeded.
LAN IP	LAN port address of the router. After mapping successfully, the system automatically obtains IP address.
WAN IP	WAN port address of the router. After mapping successfully, the system automatically obtains the IP address.

Parameter	Description
Port Mapping List	It corresponds to the UPnP mapping list on the router. ● **Service Name**: Name of the network server. ● **Protocol**: Protocol type. ● **Internal Port**: Local ports needed to be mapped. ● **External Port**: External ports which are mapped on the router.  ● When setting the external ports of router mapping ports, use ports from 1,024 to 5,000. Avoid using the known ports from 1 to 255 and system ports from 256 to 1023 to avoid any conflict. ● When deploying multiple devices in the same LAN, plan the port mapping to avoid mapping multiple devices to the same external port. ● Before mapping the port, make sure the port is not occupied or restricted. ● Keep the internal ports of TCP and UDP consistent with their external ports. They are unchangeable.
	Click this icon to change the external port number of the corresponding service.

Step 4 Click **OK** to save the configuration.

3.14.3.2.5 SNMP

After setting Simple Network Management Protocol (SNMP) and connecting the Device with relevant software tools (such as MIB Builder and MG-SOFT MIB Browser), you can directly manage and monitor the Device information on the software tools.

Preparation

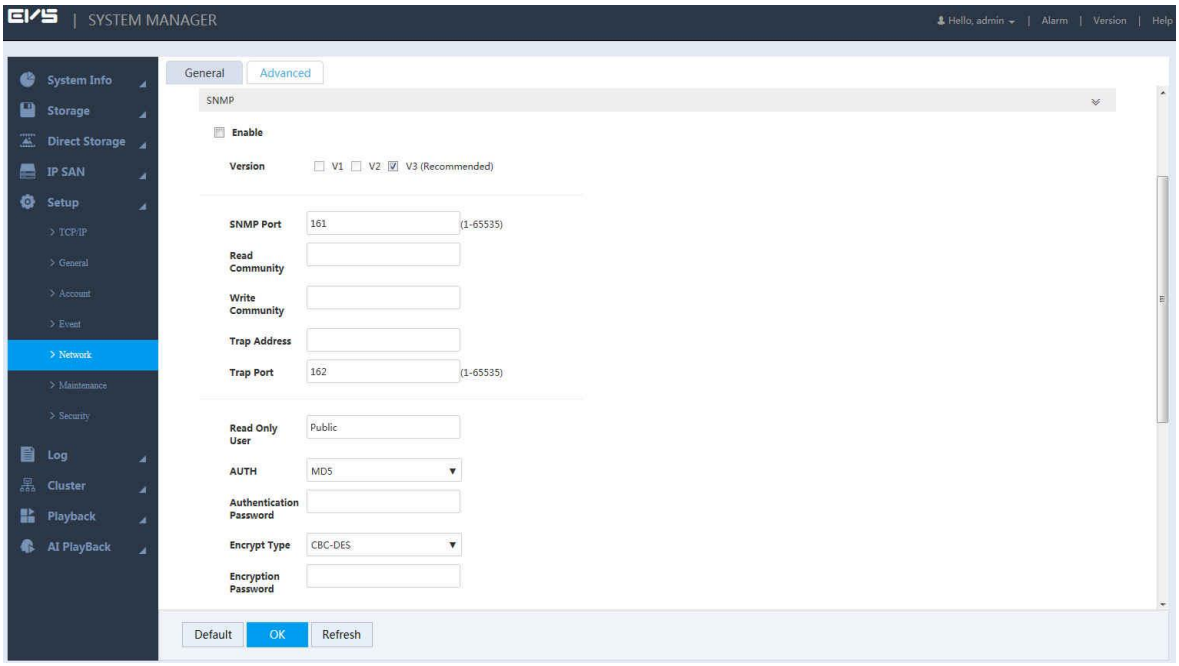
- SNMP monitoring and management tools, such as MIB Builder and MG-SOFT MIB Browser, are installed.
- MIB files corresponding to the current version are obtained from technical supports.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click  corresponding to **SNMP**.

The **SNMP** interface is displayed. See Figure 3-142.

Figure 3-142 SNMP



Step 3 Select the **Enable** check box.

Step 4 Configure the parameters. For details, see Table 3-50.

Table 3-50 SNMP parameters

Parameter	Description
Version	Select the version number, and the device only processes the information of the corresponding version.
SNMP Port	Enter the port number of monitoring in the device. The default value is 161.
Read Community	It is the read/write community strings supported by the agent program.
Write Community	
Trap Address	Enter the IP address of PC that has installed MG-SOFT MIB Browser. It is the target address to which the agent program sends traps.
Trap Port	The target port to which the agent program sends traps. The default value is 162.
Read Only User	Set the name of read only user that accesses the Device.
AUTH	Includes MD5 and SHA modes. The system will automatically recognize the mode after AUTH is enabled.
Authentication Password	Set authentication password.
Encrypt Type	Set encrypt type. The system selects CBC-DES by default.
Read/Write User	Set the name of read/write user.

Step 5 Click **OK** to save the configuration.

Step 6 (Optional) View the Device information.

1) Run MIB Builder and MG-SOFT MIB Browser on PC.
2) Compile MIB files with MIB Builder.
3) Run MG-SOFT MIB Browser to load the compiled module into the tool.

4) Enter the IP of the Device you need to manage into MG-SOFT MIB Browser, and then select the version number to search.
5) Extend the tree list displayed on the MG-SOFT MIB Browser to get the configuration information of the Device, such as video/audio channel number, and program version.

3.14.3.2.6 Multicast Settings

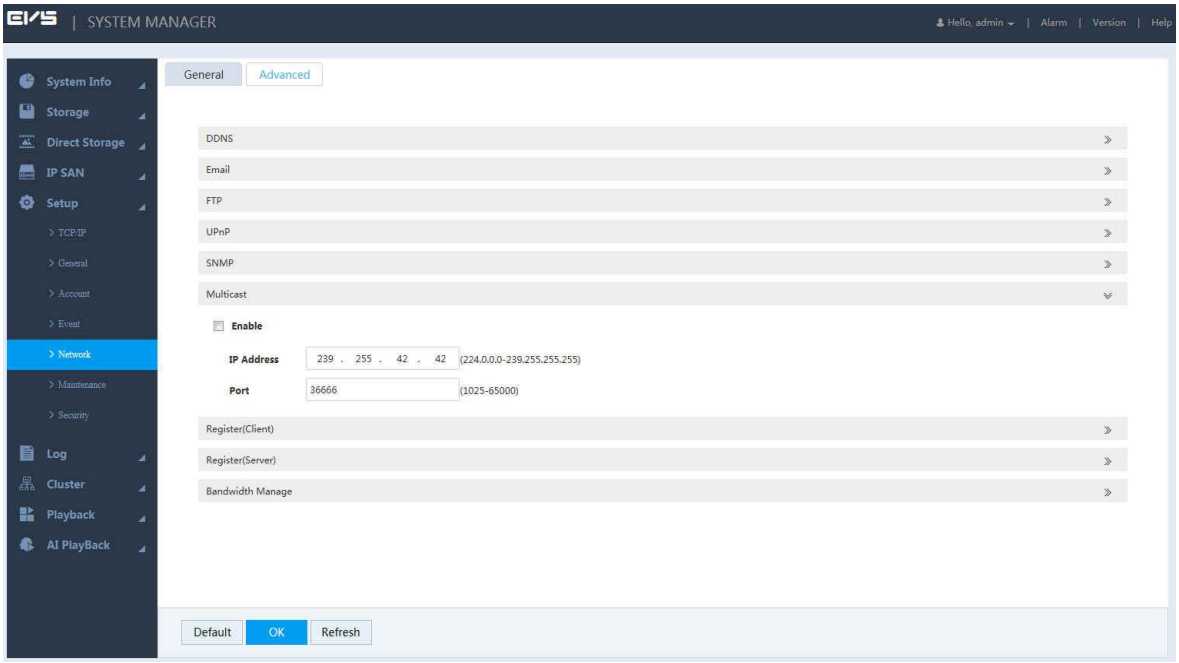
When multiple users want to preview video of the same channel at the same time, they might be unable to preview due to bandwidth limitation. You can set a multicast IP for the Device (224.0.0.0–238.255.255.255). In this way, you can solve this problem by accessing with the multicast protocol.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **Multicast**.

The **Multicast** interface is displayed. See Figure 3-143.

Figure 3-143 Multicast



Step 3 Select the **Enable** check box.

Step 4 Enter the parameters. For details, see Table 3-51.

Table 3-51 Multicast parameters

Parameter	Description
IP Address	Enter the multicast IP address to access the Device.
Port	Enter the port number to access the Device. The default value is 36666.

Step 5 Click **OK** to save the configuration.

Step 6 (Optional) Using multicast to log in the web.

Enter the login interface of the Device, and select Multicast as the login type. See Figure 3-144.

After logging in, the Device automatically obtains the multicast address and joins the multicast group, so that the monitoring screen can be viewed in real time through multicast.

Figure 3-144 Multicast

3.14.3.2.7 Active Register (Client)

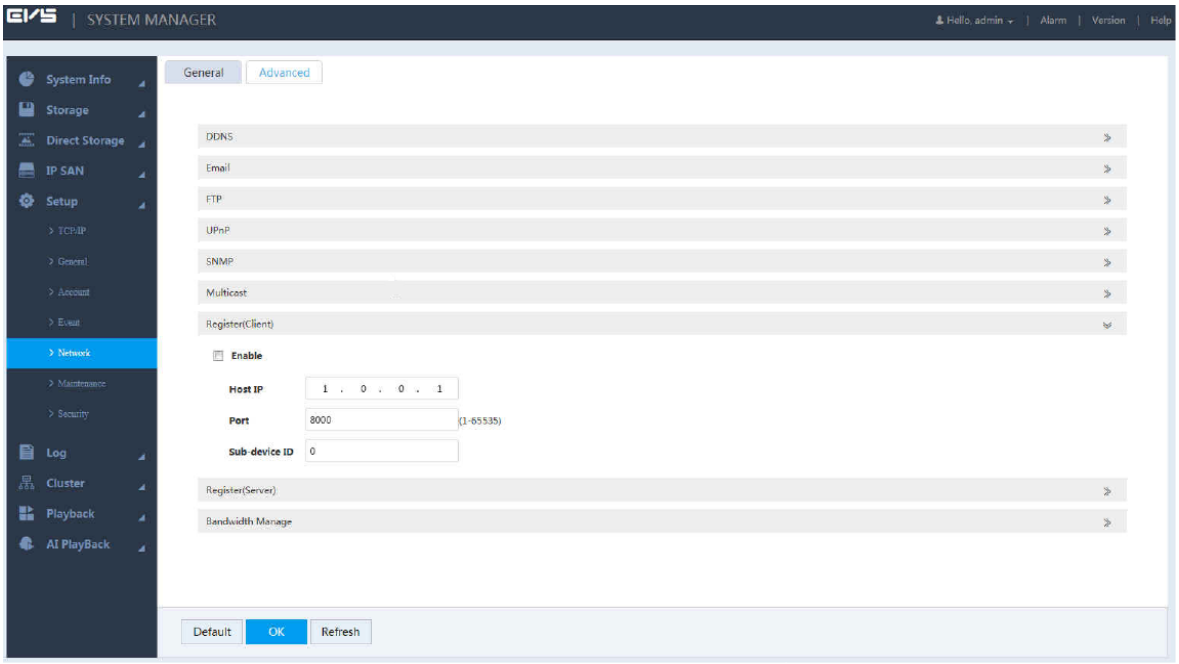
After accessing the external network, the Device automatically reports the current position to the specified server. This facilitates the server to access the Device for preview and surveillance.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **Register(Client)**.

The **Register(Client)** interface is displayed. See Figure 3-145.

Figure 3-145 Active register (client)



Step 3 Select the **Enable** check box.

Step 4 Enter the parameters. For details, see Table 3-52.

Table 3-52 Active register parameters

Parameter	Description
Host IP	Enter the IP address of the server you want to register.
Port	Enter the port number for active register. The default value is 8000.

Parameter	Description
Sub-device ID	The device ID distributed by the server-side. It is used to distinguish with other devices.

Step 5 Click **OK** to save the configuration.

3.14.3.2.8 Active Register (Server)

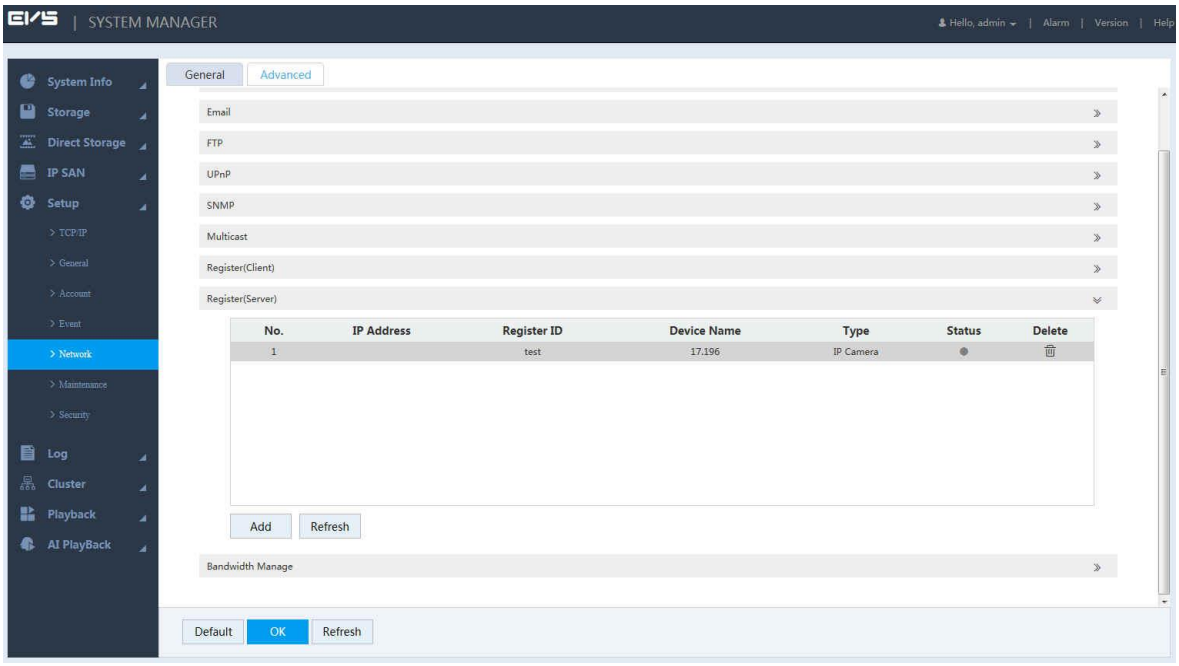
After setting the joint parameters in active register server, you can configure the joint parameters in the web of remote device (such as IPC) and register the remote device to the Device.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **Register(Server)**.

The **Register(Server)** interface is displayed. See Figure 3-146.

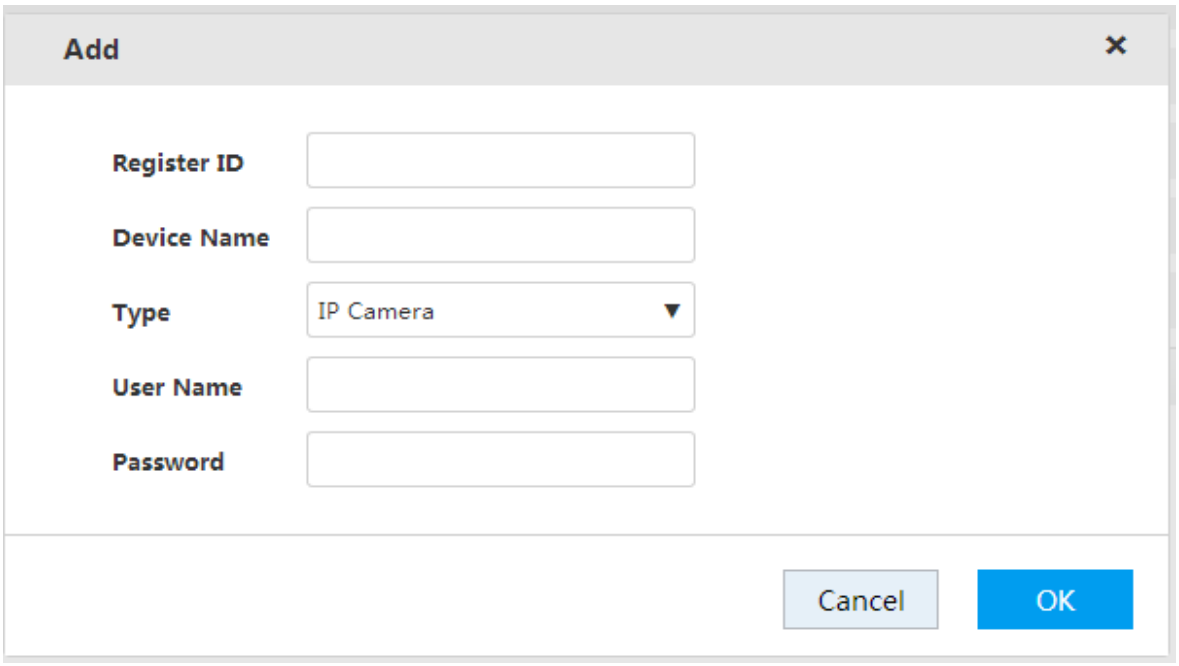
Figure 3-146 Active register (server)



Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 3-147.

Figure 3-147 Adding register (server)



Step 4 Configure the parameters. For details, see Table 3-53.

Table 3-53 Adding register (server) parameters

Parameter	Description
Register ID	Enter the register ID.
Device Name	Enter the device name.
Type	Select the device type. The default type is IP Camera.
User Name	Enter the user name and password of the remote device.
Password	

Step 5 Click **OK** to save the configuration.

After the configuration, the parameter settings in the web interface of the remote device must be the same as the settings here. Otherwise, the register will fail.

3.14.3.2.9 Bandwidth Management

Control different users to have different bandwidth.

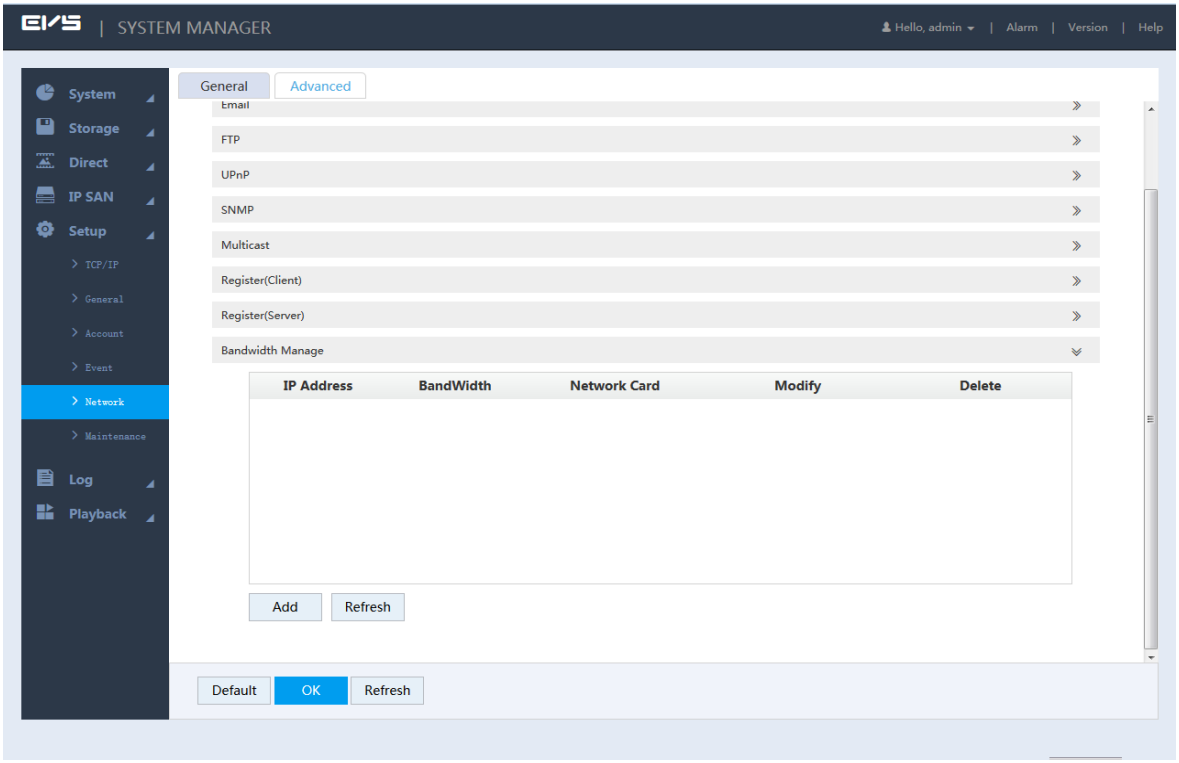
Bandwidth refers to the max bandwidth of NIC. For example: NIC of the Device has a max bandwidth of 1 GB.

Step 1 Select **Setup > Network > Advanced**.

Step 2 Click » corresponding to **Bandwidth Management**.

The **Bandwidth Management** interface is displayed. See Figure 3-148.

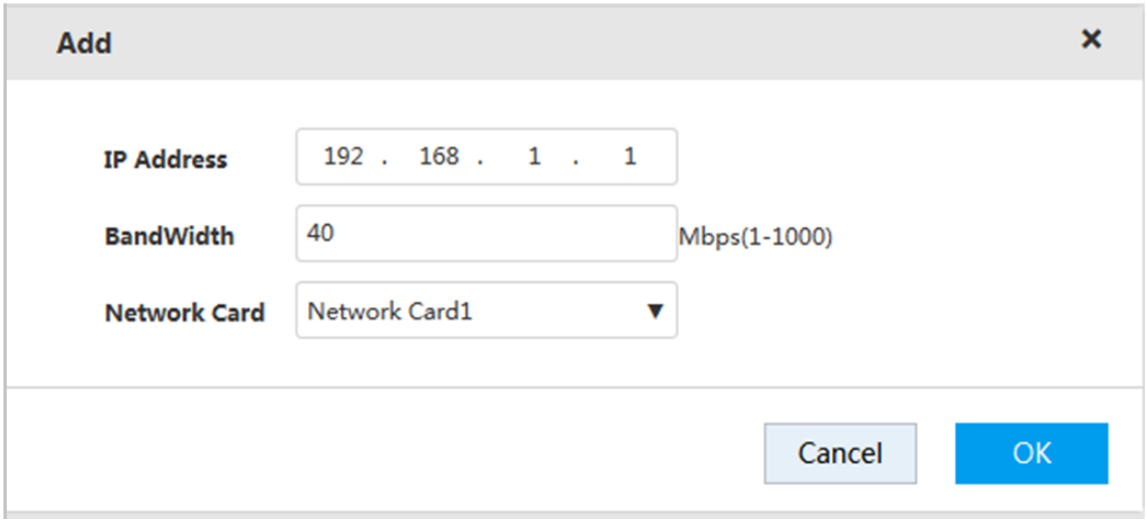
Figure 3-148 Bandwidth Management



Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 3-149.

Figure 3-149 Adding Bandwidth



Step 4 Configure the parameters. For details, see Table 3-54.

Table 3-54 Bandwidth management parameters

Parameter	Description
IP Address	Enter the IP address of the user you want to restrict the bandwidth.
Bandwidth	Enter the bandwidth ceiling value.
Network Card	Select the network card you want to restrict the bandwidth.

Step 5 Click **OK** to save the configuration.

3.14.4 Security Management

To ensure security of network and data, it is necessary to set the access permission of IP host (PC or server with IP) and password reset function.

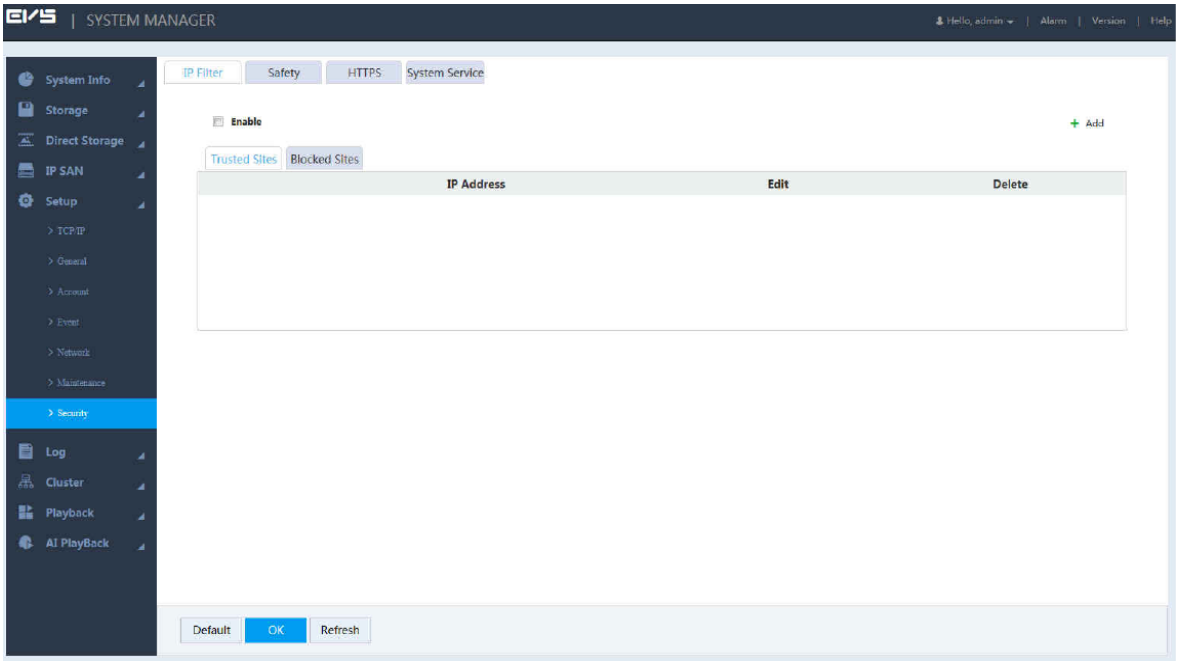
3.14.4.1 IP Filter

Set the IP host that accesses the Device. After setting, only IP hosts in the Trusted Sites can log in to the web. Hosts in the Blocked Sites will not be able to do the same. This ensures the security of network and data in the Device.

Step 1 Select **Setup > Security > IP Filter**.

The **IP Filter** interface is displayed. See Figure 3-150.

Figure 3-150 IP filter



Step 2 Select the **Enable** check box to enable IP filter function.

The **Trusted Sites** and **Blocked Sites** boxes are displayed.

Step 3 Add Trusted Sites/Blocked Sites.

1) Select **Trusted Sites** or **Blocked Sites**.
2) Click ✚.

The **Add** interface is displayed. See Figure 3-151.

Figure 3-151 Add interface

3) Configure the parameters. For details, see Table 3-55.

Table 3-55 Add parameters

Parameter	Description
IP Address	Click the drop-down list to select the way of adding Trusted Sites/Blocked Sites. ● IP Address: Enter the IP address of trusted site/blocked site to add. ● IP Section: Enter the IP section of trusted site/blocked site to add. You can add multiple hosts at the same time. ● MAC Address: Enter the MAC address of trusted site/blocked site to add. The system does not support adding blocked sites through MAC address.
IPv4	Click the drop-down list to select IP address protocol. ● IPv4: the IP address is in the form of IPv4. For example, 192.168.5.10. ● IPv6: the IP address is in the form of IPv6. For example, aa:aa:aa:aa:aa:aa:aa:aa.

4) Click **OK**.

Step 4 Click **OK**.

Click the **Trusted Sites** tab or **Blocked Sites** tab to view the IP host information in corresponding list.

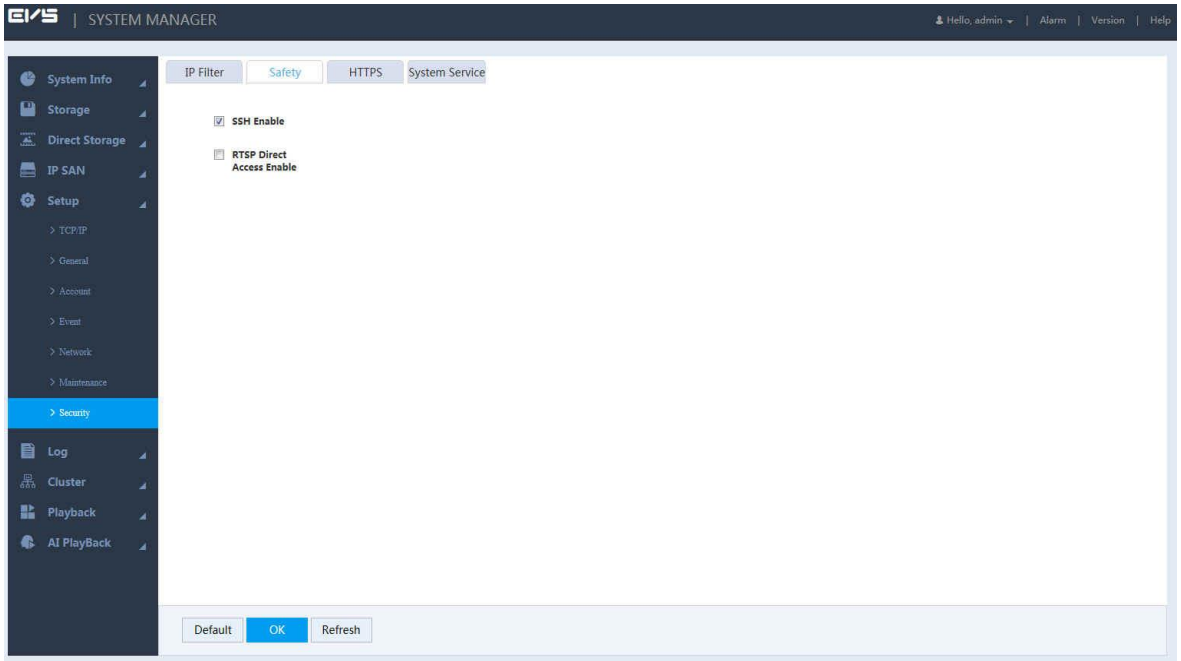
3.14.4.2 Safety

Set parameters of SSH enable and RTSP direct access enable to ensure network and data safety.

Step 1 Select **Setup > Security > Safety**.

The **Safety** interface is displayed. See Figure 3-152.

Figure 3-152 Safety



Step 2 Select the **SSH Enable** check box and **RTSP Direct Access Enable** check box.

- The system selects SSH Enable by default. It supports SSH backend.
- RTSP Direct Access Enable is used when the Device accessing the platform.

Step 3 Click **OK** to save the configuration.

3.14.4.3 HTTPS

On the HTTPS interface, by creating server certificate or downloading root certificate and setting the port number, your PC can log in properly through HTTPS. This helps guarantee information and device security.

Preparation

Only after enabling HTTPS port can you create server certificate and download root certificate. For detailed operations to enable HTTPS, see "3.14.3.1.1 Connection Port."

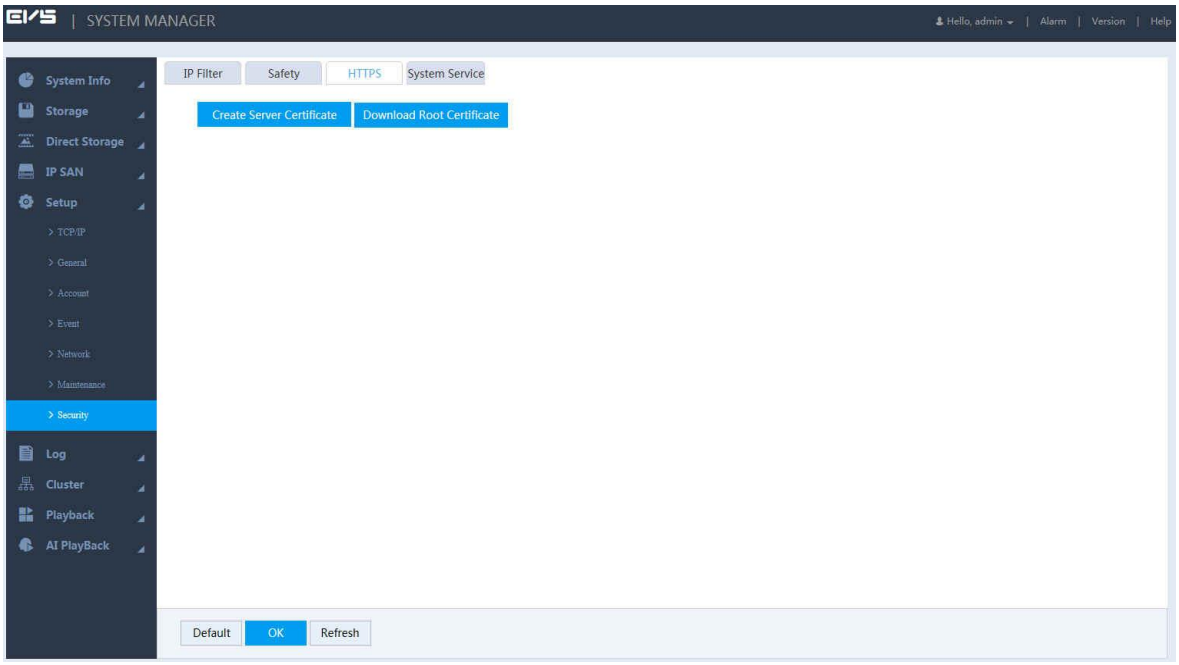
Create Server Certificate

If you use this function for the first time, or you have changed the IP address, you need to create server certificate.

Step 1 Select **Setup > Security > HTTPS**.

The **HTTPS** interface is displayed. See Figure 3-153.

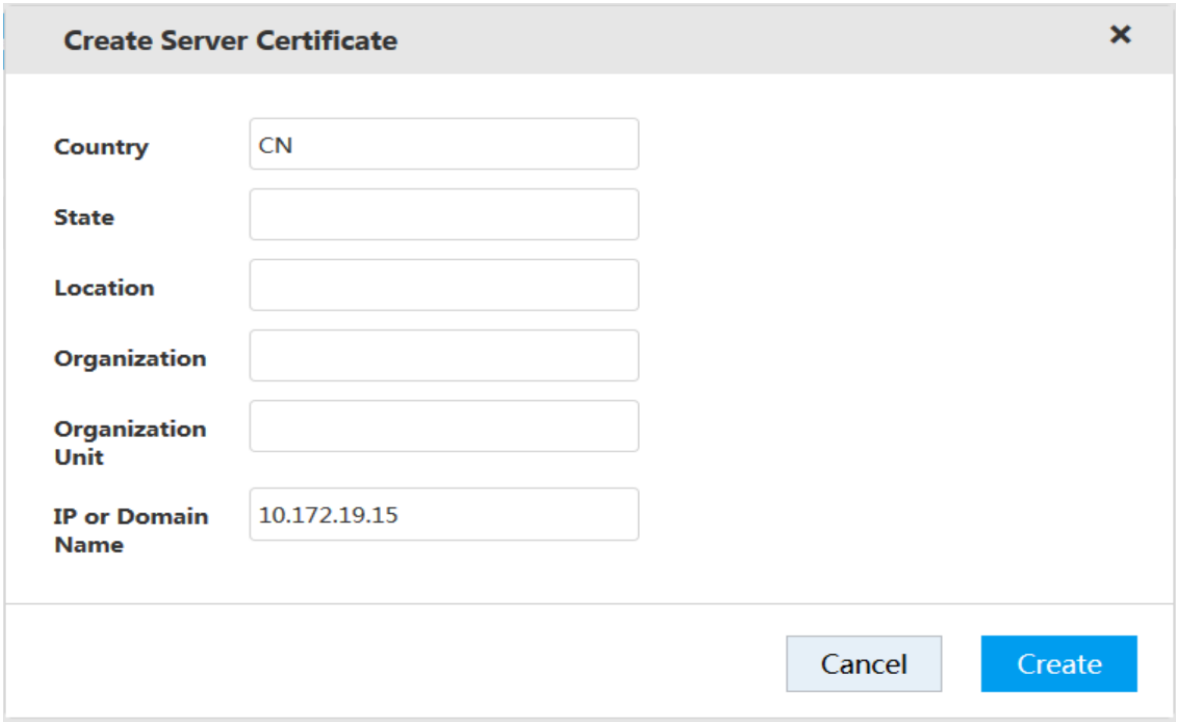
Figure 3-153 HTTPS



Step 2 Click **Create Server Certificate**.

The **Create Server Certificate** interface is displayed. See Figure 3-154.

Figure 3-154 Creating server certificate



Step 3 Enter the information like country and state.

IP or Domain Name must be the same as the IP or domain name of the Device.

Step 4 Click **Create**.

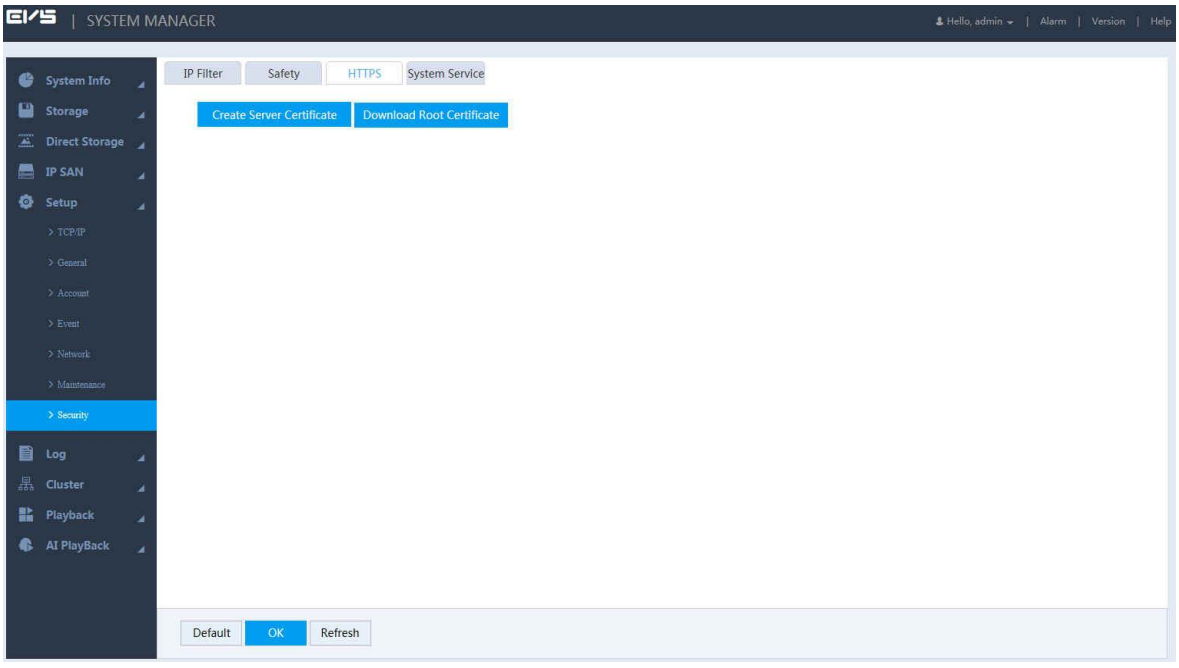
The system prompts **Creation Succeed** when it is done successfully.

Download Root Certificate

Step 1 Select **Setup > Security > HTTPS**.

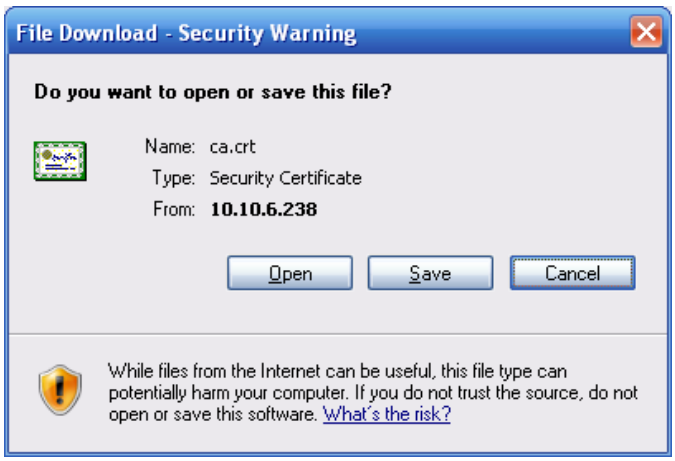
The **HTTPS** interface is displayed. See Figure 3-155.

Figure 3-155 HTTPS



Step 2 Click **Download Root Certificate**, and the **File Download-Security Warning** dialogue box pops up. See Figure 3-156.

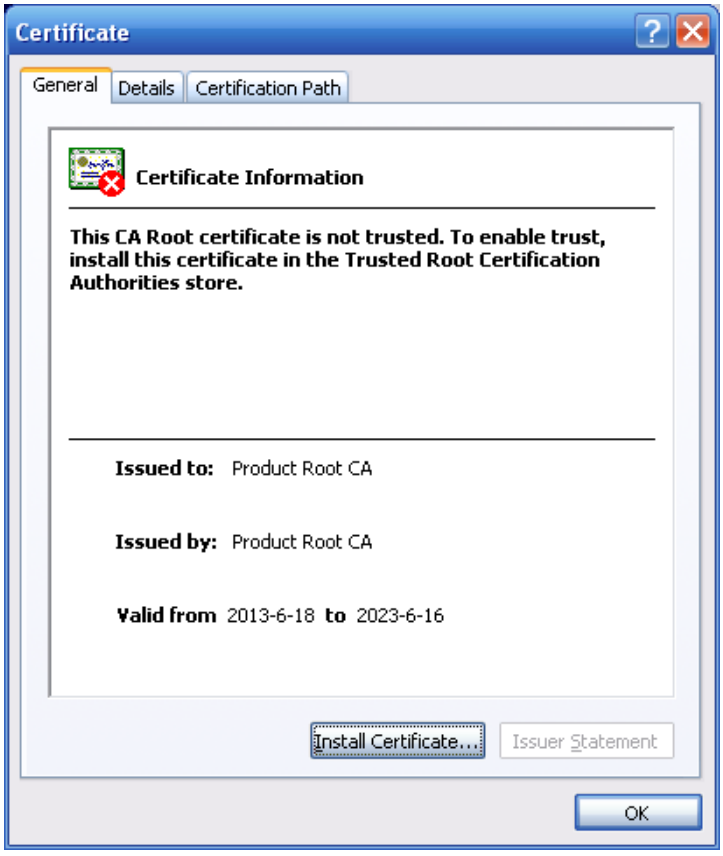
Figure 3-156 File download



Step 3 Click **Open**.

The **Certificate Information** interface is displayed. See Figure 3-157.

Figure 3-157 Certificate information



Step 4 Click **Install Certificate**.

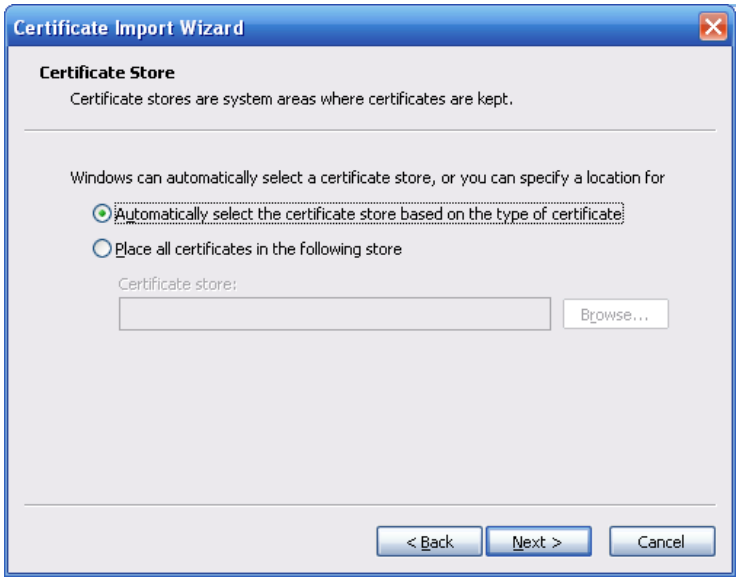
The **Certificate Import Wizard** interface is displayed. See Figure 3-158.

Figure 3-158 Certificate import wizard

Step 5 Click **Next**.

The **Certificate Store** interface is displayed. See Figure 3-159.

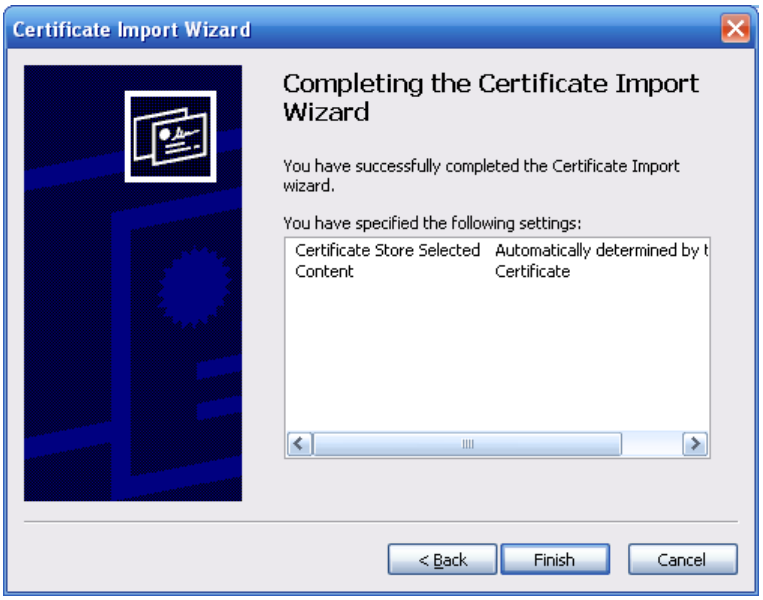
Figure 3-159 Certificate storage



Step 6 Select the storage location and click **Next**.

The **Completing the Certificate Import Wizard** interface is displayed. See Figure 3-160.

Figure 3-160 Completing certificate import



Step 7 Click **Finish** and a dialogue box pops up showing **The import was successful**. See Figure 3-161.

Figure 3-161 Success

HTTPS Login

After creating server certificate or downloading root certificate, you need to set the HTTPS port number. For details, see "3.14.3.1.1 Connection Port."

After setting, enter https://xx.xx.xx.xx:port in the browser and you can log in the Device through HTTPS.

- **xx.xx.xx.xx** refers to the IP address or domain name of the Device.
- **Port** corresponds to the HTTPS port number. You can enter https://xx.xx.xx.xx directly if using the default port number 443.

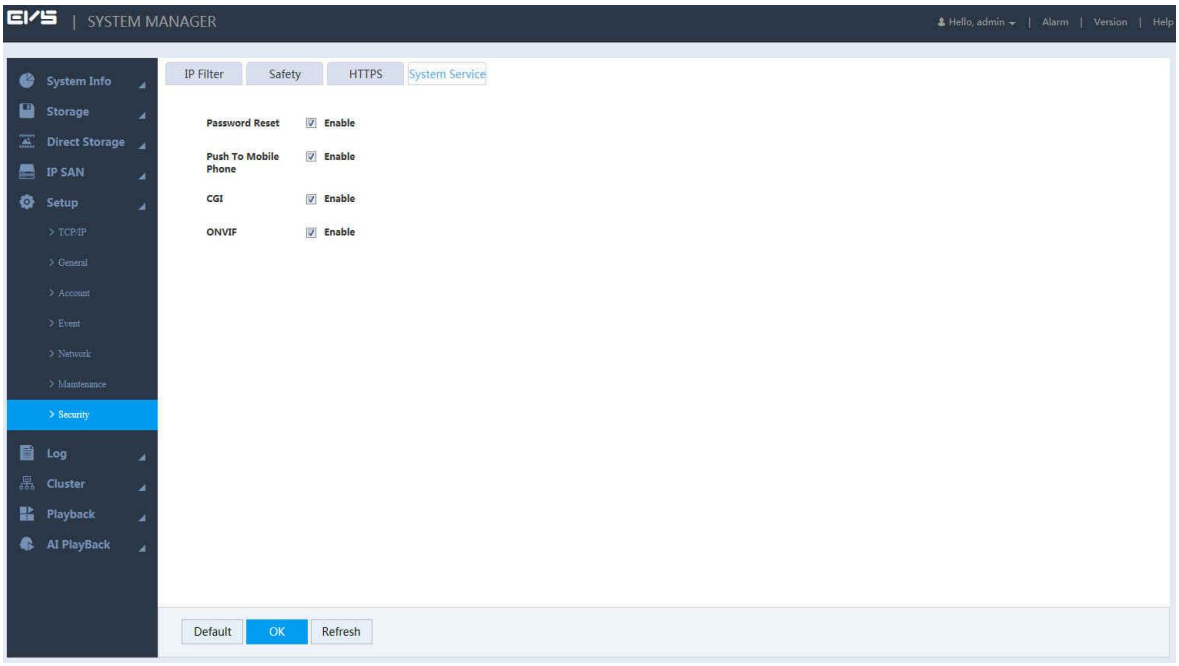
3.14.4.4 System Service

You can enable and disable system services of the Device.

Step 1 Select **Setup > Security > System Service**.

The **System Service** interface is displayed. See Figure 3-162.

Figure 3-162 System service



Step 2 Configure the parameters. For details, see Table 3-56.

Table 3-56 System service

Parameter	Description
Password Reset	Enable or disable the function of resetting password. The system selects **Enable** by default.
Push To Mobile Phone	By enabling this function, the alarm triggered on the Device will be pushed to the phone. The system selects **Enable** by default.
CGI	By enabling this function, the Device can be connected through this protocol. The system selects **Enable** by default.
ONVIF	By enabling this function, the Device can be connected through this protocol. The system selects **Enable** by default.

Step 3 Click **OK** to save the configuration.

3.14.5 System Maintenance

System maintenance includes operations of restarting the Device, deleting old files, restoring factory default, and upgrading the system. It helps clear the faults and errors during system operation, and improves the operation efficiency of the Device.

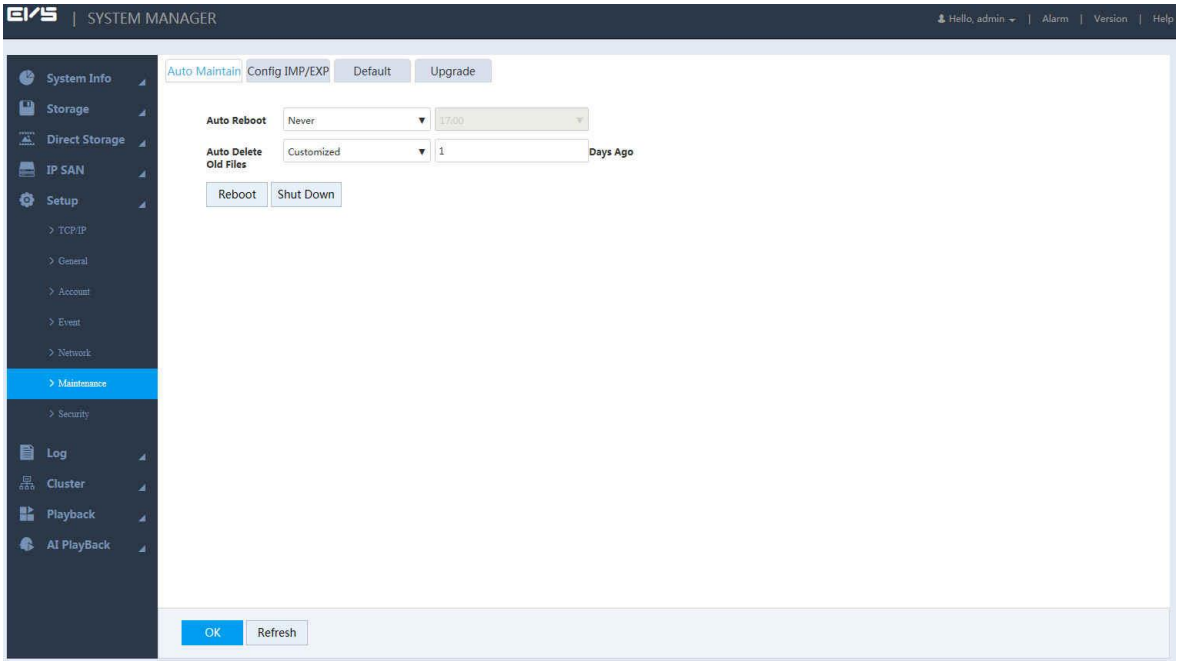
3.14.5.1 Automatic Maintenance

If the Device has run for a long time, there might be many old files left. You can set the Device for automatic restart or deleting the old files during spare time.

Step 1 Select **Setup > Maintenance > Auto Maintain**.

The **Auto Maintain** interface is displayed. See Figure 3-163.

Figure 3-163 Auto maintenance



Step 2 Select time for **Auto Reboot** and **Auto Delete Old Files**.

Step 3 Click **OK** to save the configuration.

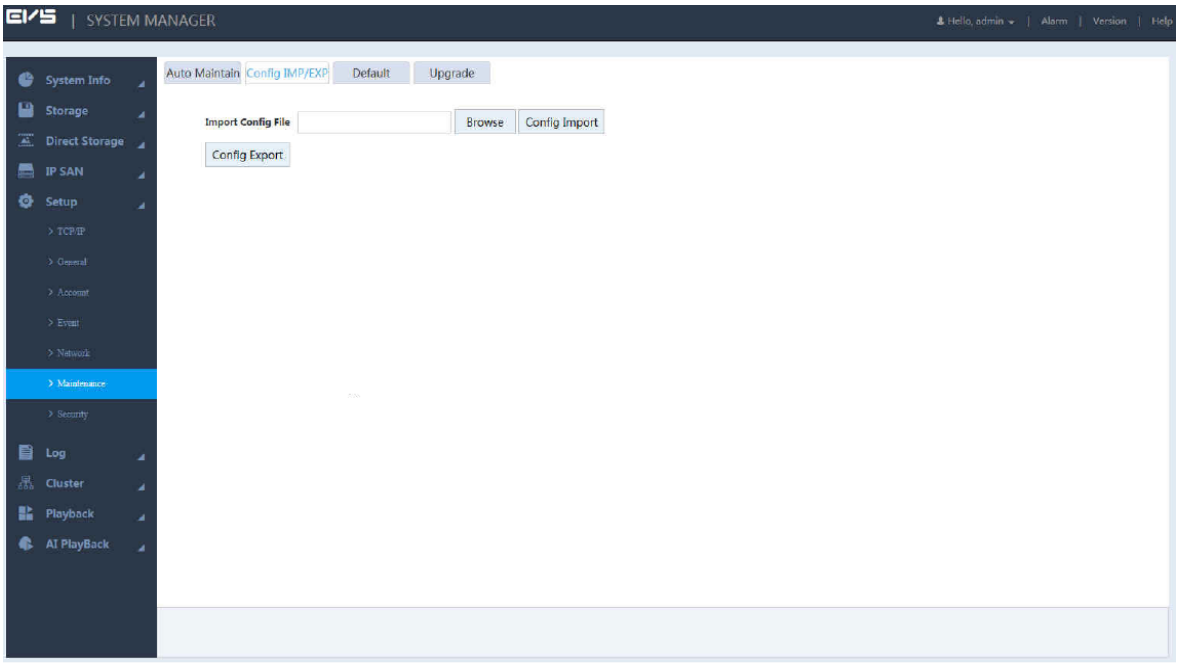
3.14.5.2 Configuring Import and Export

By configuring backup, the system exports the configuration information in the Device to PC. If there is any error in the Device, such information can be imported to the Device. This helps restore the original configuration of the Device.

Step 1 Select **Setup > Maintenance > Config IMP/EXP**.

The **Config IMP/EXP** interface is displayed. See Figure 3-164.

Figure 3-164 Configuration backup



Step 2 Import or export configuration information.

- Configuration export: Click **Browse** to select the config file to export, click **Config Export**, and then you can export the config information to PC.
- Configuration import: Click **Browse** to select the config file to import, click **Config Import**, and then you can import the stored config information.

3.14.5.3 Restoring Defaults

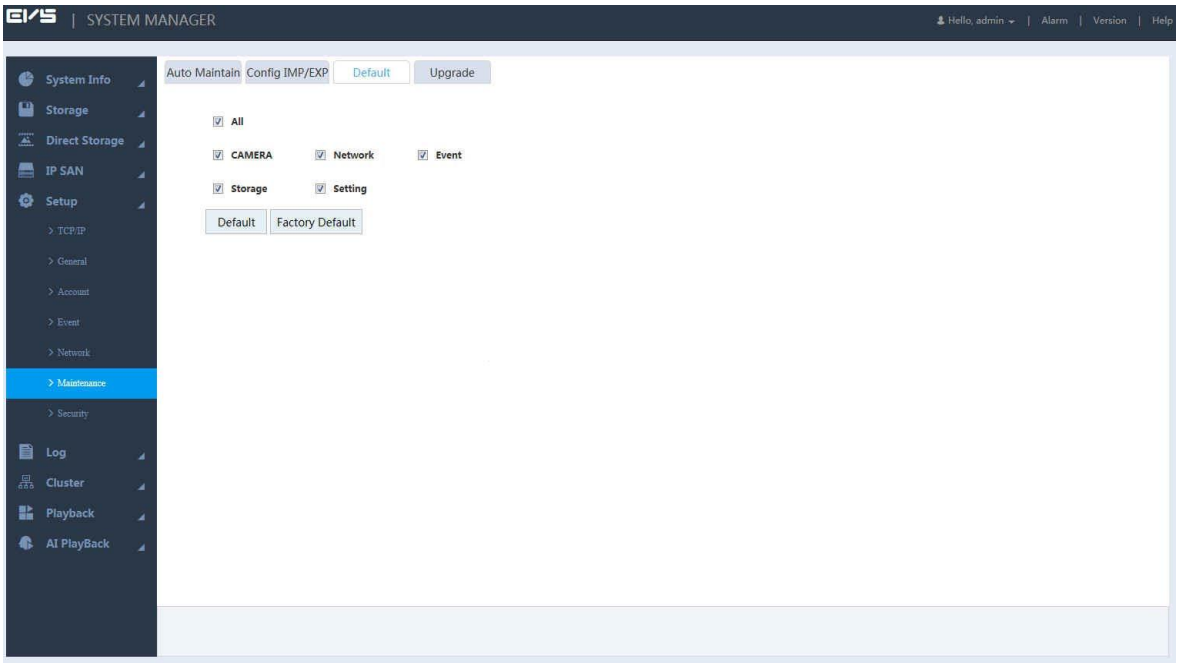
When the Device is running slowly or there is configuration error, you can try to solve the problem by restoring defaults.

After restoring defaults, the existing system configuration will be lost. Operate with care.

Step 1 Select **Setup > Maintenance > Default**.

The **Default** interface is displayed. See Figure 3-165.

Figure 3-165 Restoring defaults



Step 2 Restoring default or factory default.

- Restoring default: Select the configuration item and click **Default**. The system restores all the selected configurations to default status.
- Restoring factory default: Click **Factory Default**, and all the configurations of the Device are restored to factory default status.

3.14.5.4 Upgrading the System

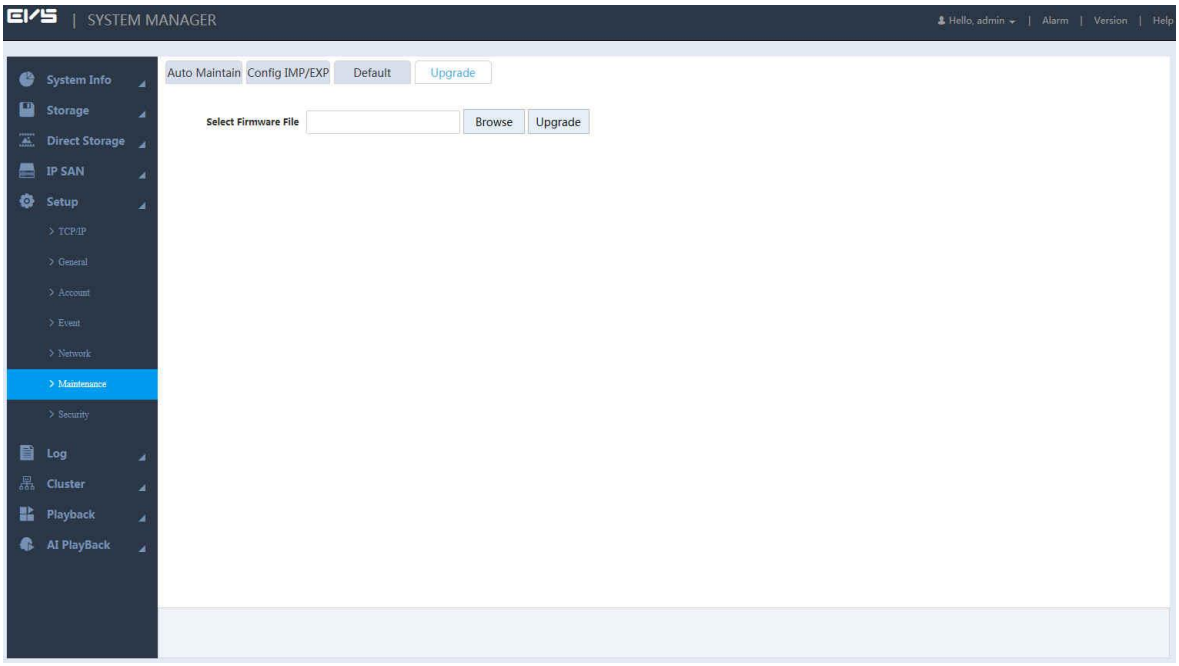
Upgrade the system of the Device by importing upgrade files. Upgrade files are files with *.bin.

- In the process of upgrading, do not cut down the power/network, or restart/shutdown the Device.
- Upgrading error might lead to device fault. Make sure that the imported upgrade file is correct.

Step 1 Select **Setup > Maintenance > Upgrade**.

The **Upgrade** interface is displayed. See Figure 3-166.

Figure 3-166 System upgrade



Step 2 Click **Browse** to select the upgrade file.

Step 3 Click **Upgrade** and the system starts upgrading.

3.15 Cluster Service

Cluster function, also known as cluster redundancy function, is a way that can improve device reliability.

Create N master devices and M backup devices in the cluster (N+M cluster), and provide virtual IP address (cluster IP) for unified login and management. Normally, the master devices are working. If the master device breaks down, the backup device not working will replace it to work according to the configuration of the master one and the cluster IP. After the master one is restored, the backup one transmits back the configuration, cluster IP and records during the breakdown, and the master one goes on working.

There is a management server called dispatching console (DSC) in the N+M cluster. DSC performs timely dispatching for the master devices and backup devices. When cluster is created in the Device, the Device is used as a DCS by default.

Dual-control device does not support cluster.

3.15.1 Configuring Cluster

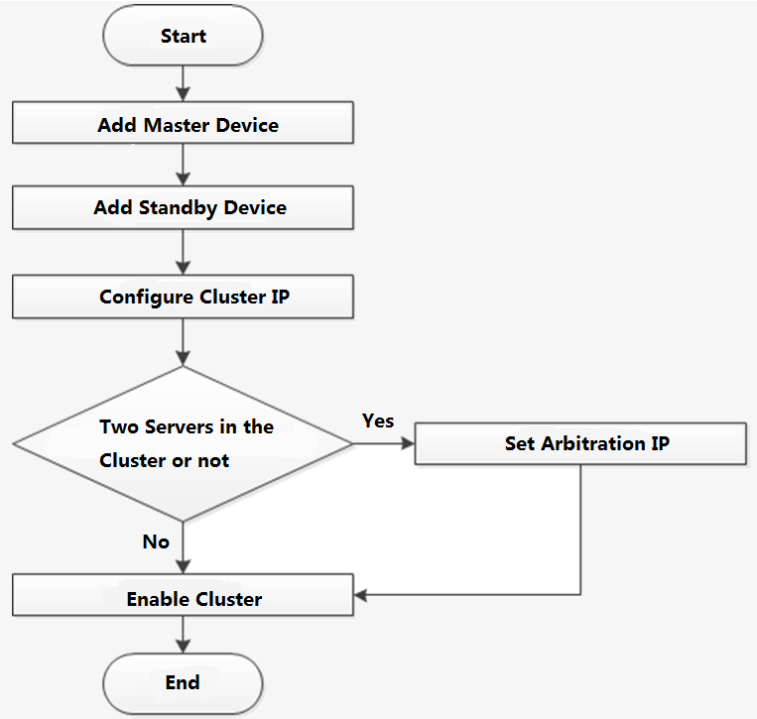
You can create cluster, view cluster information, restore master device and set arbitration IP.

3.15.1.1 Creating Cluster

Creating cluster requires organizing multiple devices into a cluster. For the creation flow, see Figure 3-167.

When creating a cluster, the first standby device works as DCS by default. The priority of the rest standby devices is defined by the adding sequence. The earlier the device is added, the higher its priority is.

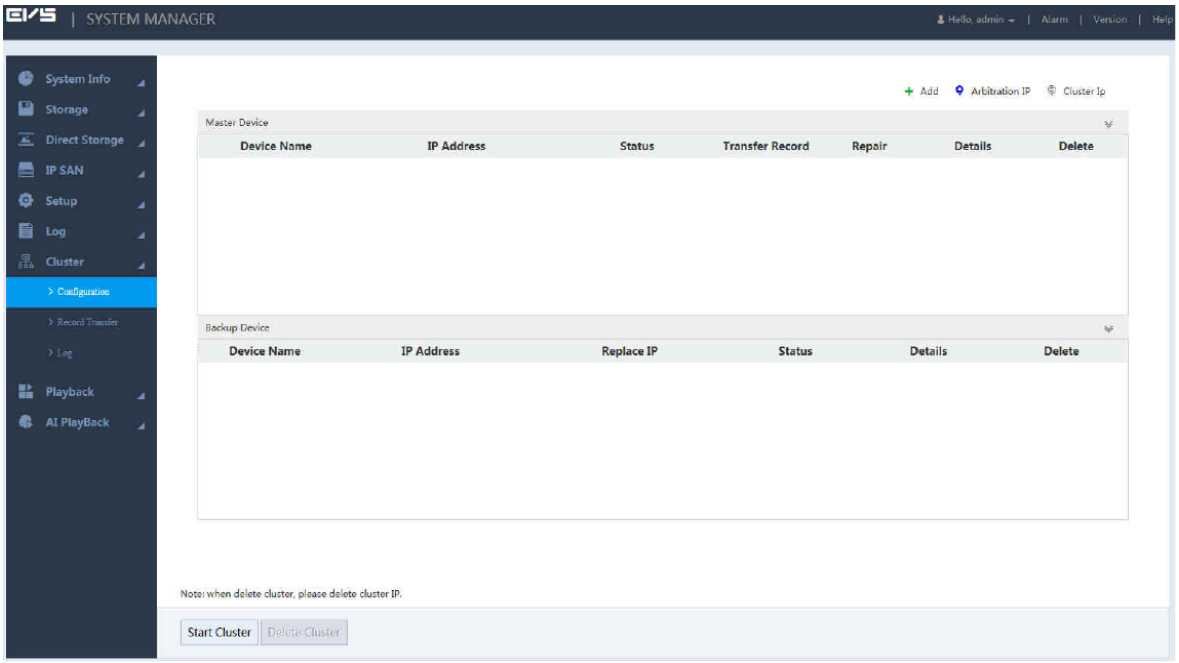
Figure 3-167 Creating cluster



Step 1 Select **Cluster > Configuration**.

The **Configuration** interface is displayed. See Figure 3-168.

Figure 3-168 Cluster configuration

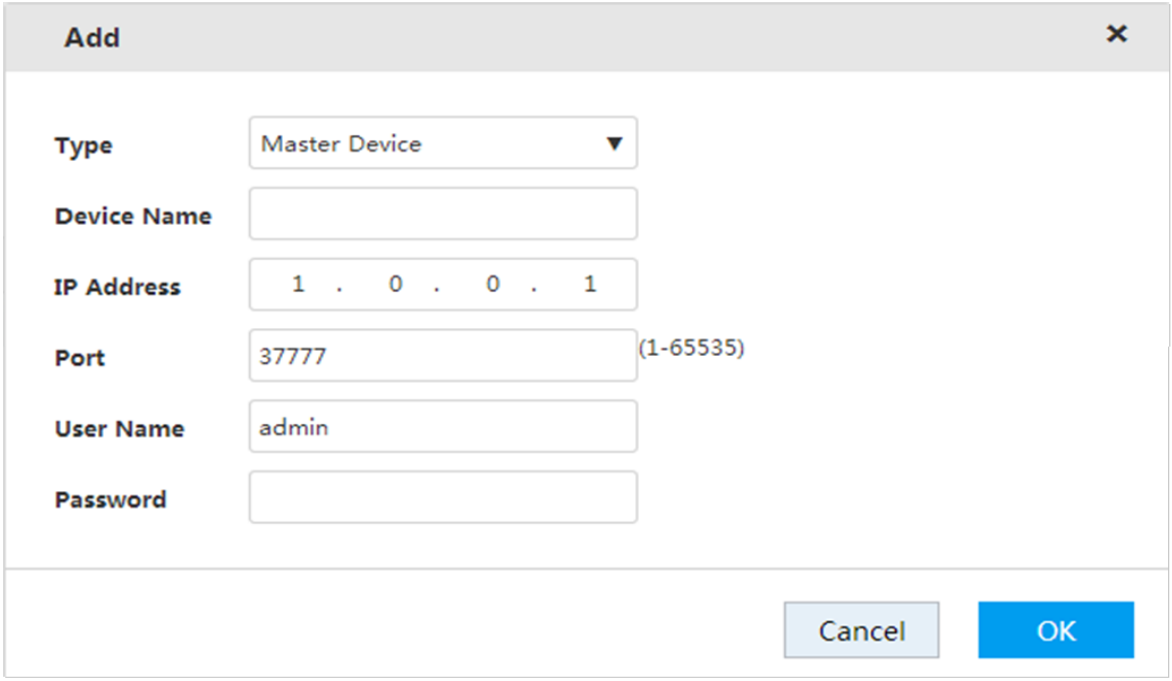


Step 2 Adding master device or backup device.

1) Click + .

The **Add** interface is displayed. See Figure 3-169.

Figure 3-169 Adding master/backup device



2) Configure the parameters. For details, see Table 3-57.

Table 3-57 Server parameters

Parameter	Description
Type	Select the device type, including master device and backup device.
Device Name	Enter the device name.
IP Address	Enter the IP address of the master or backup device. You do not need to enter the IP address when adding the first backup device. The system takes this device as the first backup device for cluster by default.
Port	The default value is 37777.
User Name	Enter the user name and password of the master device or backup device. That is, the user name and password to access the web of the Device.
Password	

3) Click **OK** to save the configuration.

The system returns to the **Configuration** interface.

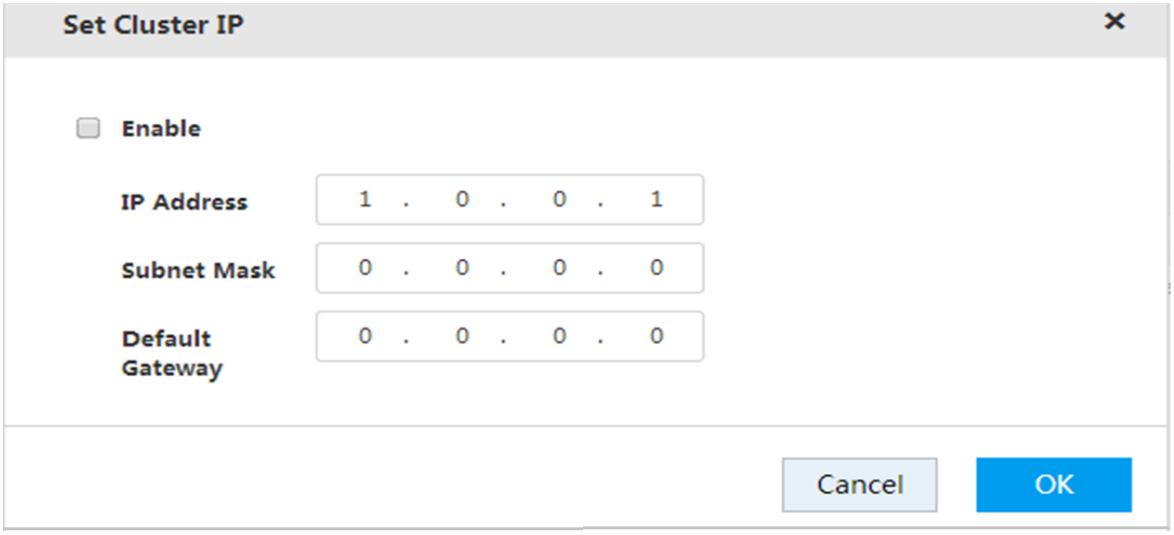
Step 3 Setting cluster IP.

Configuring cluster IP requires creating a virtual IP address, and you can access and manage the master and backup devices in the cluster through this virtual IP. If logging in with the virtual IP, you can still view real-time monitoring when the master device fails and the backup device is used.

1) Click .

The **Set Cluster IP** interface is displayed. See Figure 3-170.

Figure 3-170 Setting cluster IP



2) Select the **Enable** check box. Enter the **IP Address**, **Subnet Mask** and **Default Gateway**.
3) Click **OK** to save the configuration.
The system returns to the **Configuration** interface.

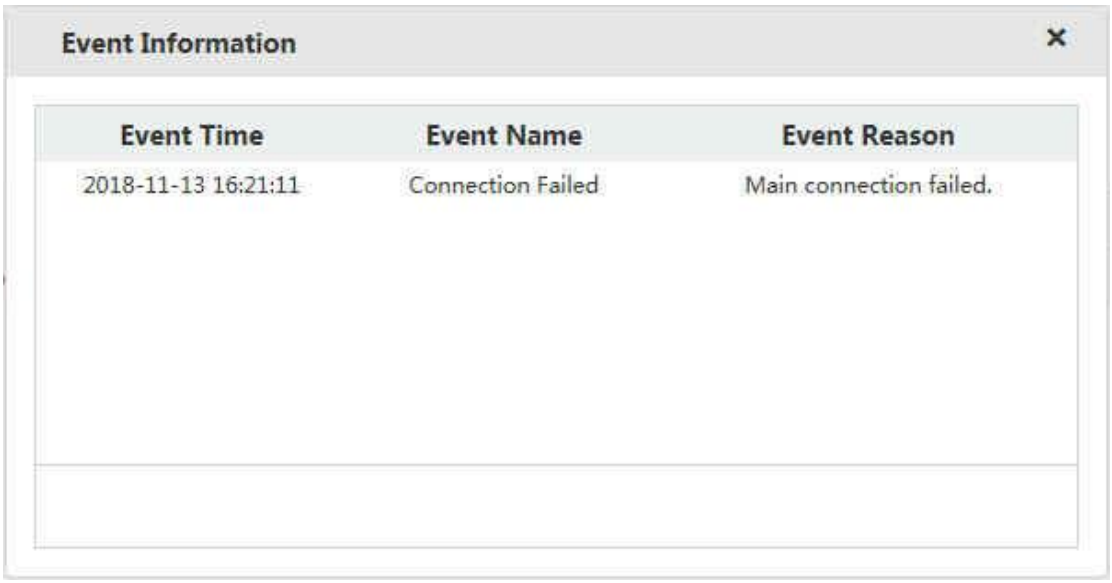
Step 4 Click **Start Cluster** to enable cluster function.

- If there are only two devices in the cluster, you have to set arbitration IP to make the cluster switch normally. For details of setting arbitration IP, see "3.15.1.4 Setting Arbitration IP."
- Click to delete a master or backup device. Click **Delete Cluster** to delete a cluster.

3.15.1.2 Viewing Information

Click corresponding to the master device or backup device. You can view its log information, including event time, name and reason.

Figure 3-171 Event information



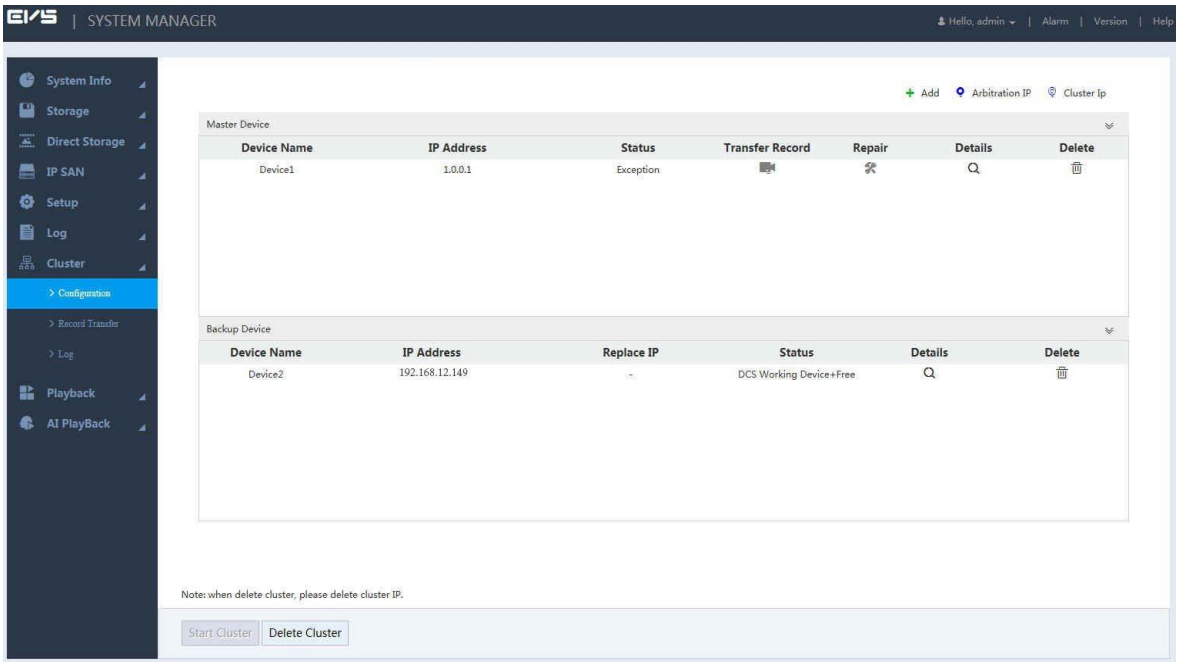
3.15.1.3 Restoring Master Device

When the master device breaks down, the backup device replaces it to work. The status of the backup device changes from free to working. After the master device is repaired, you need to restore the master device manually.

Step 1 Select **Cluster > Configuration**.

The **Configuration** interface is displayed. See Figure 3-172.

Figure 3-172 Cluster configuration



Step 2 Click  .

The **Record Transfer** interface is displayed.

Step 3 Enable auto record transfer according to actual needs.

- Click **OK**. The system starts to restore the master device and transfer records automatically.

- Click **Cancel**. The system starts to restore the master device, but records will not be transferred. If you need to transfer the records, do it manually. For details, see "3.15.2 Record Transfer."

3.15.1.4 Setting Arbitration IP

When there are only two Devices in the cluster, a third-party device is needed to define if the master device is breakdown. That is, you have to set an arbitration IP to make the cluster perform switching normally. The arbitration IP can be the IP address of device, PC or network gateway connected with the Device.

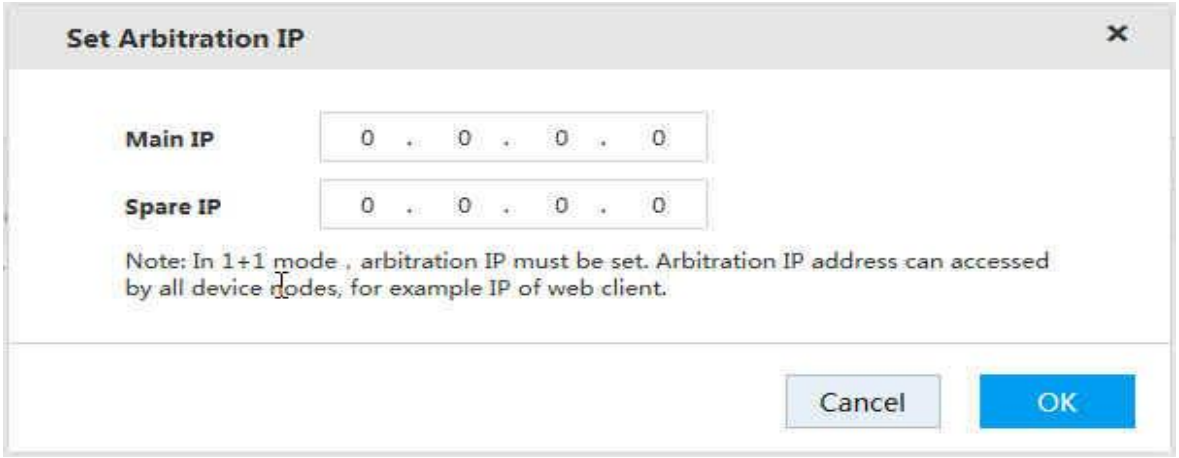
Step 1 Select **Cluster > Configuration**.

The **Configuration** interface is displayed. See Figure 3-172.

Step 2 Click .

The **Set Arbitration IP** interface is displayed. See Figure 3-173.

Figure 3-173 Setting arbitration IP



Step 3 Enter the Main IP and Spare IP.

Step 4 Click **OK** to save the configuration.

3.15.2 Record Transfer

After the master device is repaired, the records on the backup device must be transferred back to the master device.

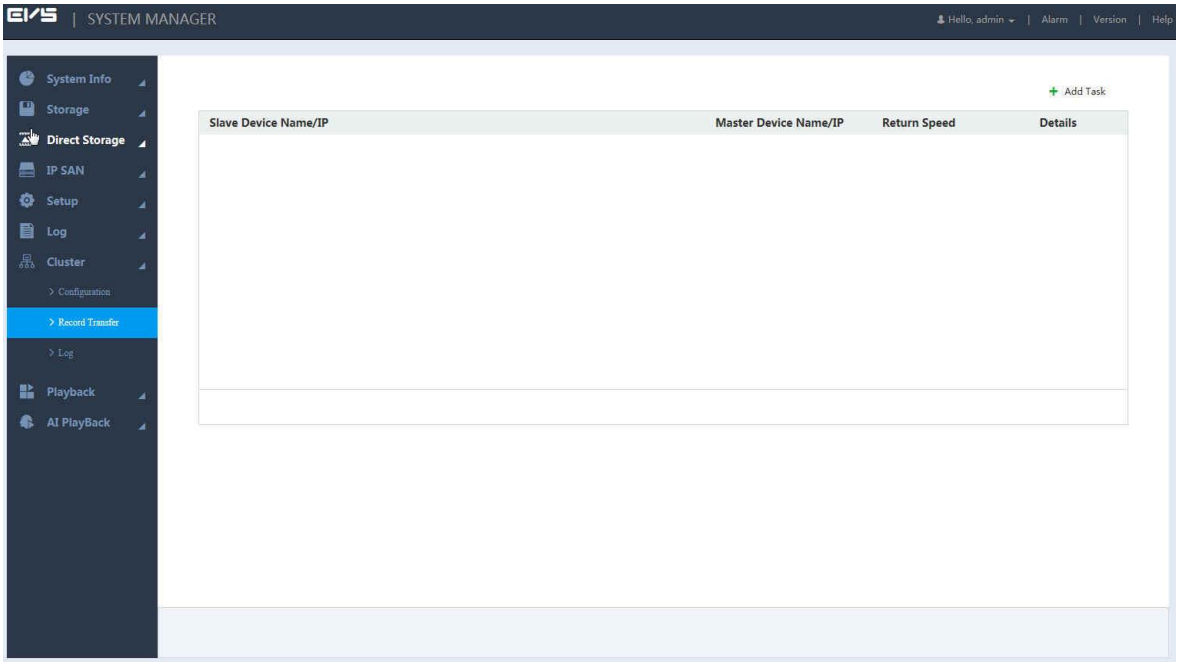
Preparation

The master device is restored. For details, see "3.15.1.3 Restoring Master Device."

Step 1 Select **Cluster > Record Transfer**.

The **Record Transfer** interface is displayed. See Figure 3-174.

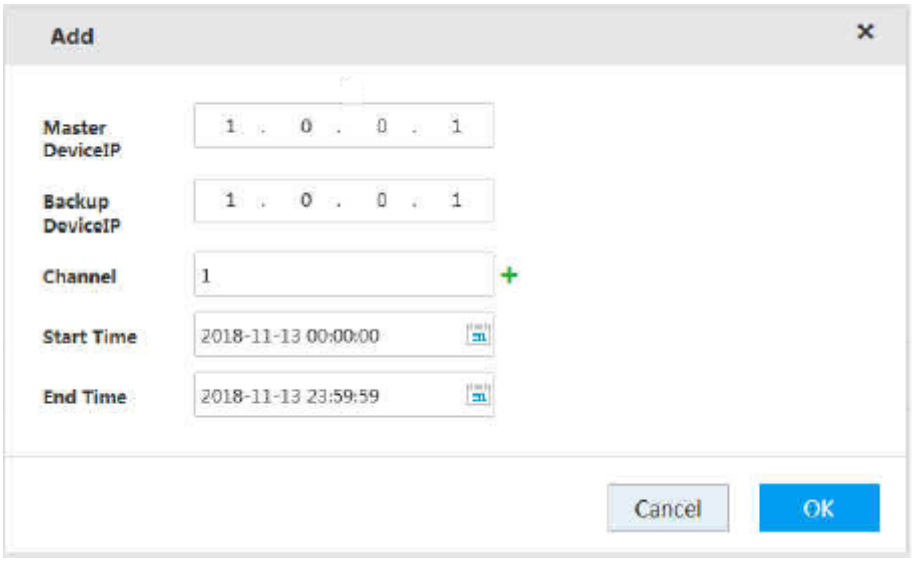
Figure 3-174 Record transfer



Step 2 Click + .

The **Add** interface is displayed. See Figure 3-175.

Figure 3-175 Adding record transfer



Step 3 Configure the parameters. For details, see Table 3-58.

Table 3-58 Record transfer parameters

Parameter	Description
Master Device IP	Enter the IP address of master device.
Backup Device IP	Enter the IP address of backup device.
Channel	Enter the channel number you need to transfer records. Click + to set the channel range.
Start Time	Select the time period of records that you need to transfer.

Parameter	Description
End Time	

Step 4 Click **OK** to save the configuration.

The system returns to the **Record Transfer** interface. You can view the detailed information like transfer speed.

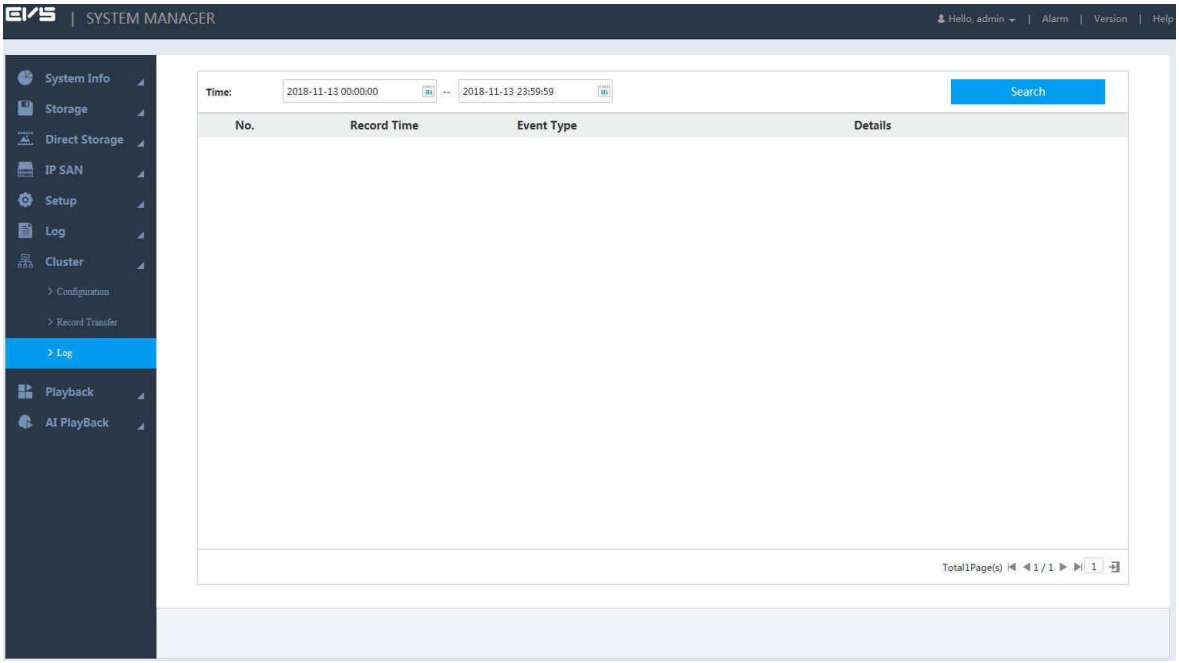
3.15.3 Cluster Log

The system supports searching and viewing cluster logs.

Step 1 Select **Cluster > Log**.

The **Log** interface is displayed. See Figure 3-176.

Figure 3-176 Cluster log



Step 2 Select the time period of recorded cluster logs.

Step 3 Click **Search**.

The search results are displayed. You can view the relative log information.

3.16 System Information

You can view the Device information such as the current status, online users, device information and system logs.

3.16.1 Server Overview

View the HDD statistics, RAID status, device online, case, record status and NIC status.

Select **System Info > Server Overview**.

The **Server Overview** interface is displayed. See Figure 3-177.

- Click to get the latest status or information of the Device.
- Click Details, and the **Case Overview** interface is displayed. See Figure 3-178. You

can view the information of HDD, power, and interface status.

Figure 3-177 Server overview

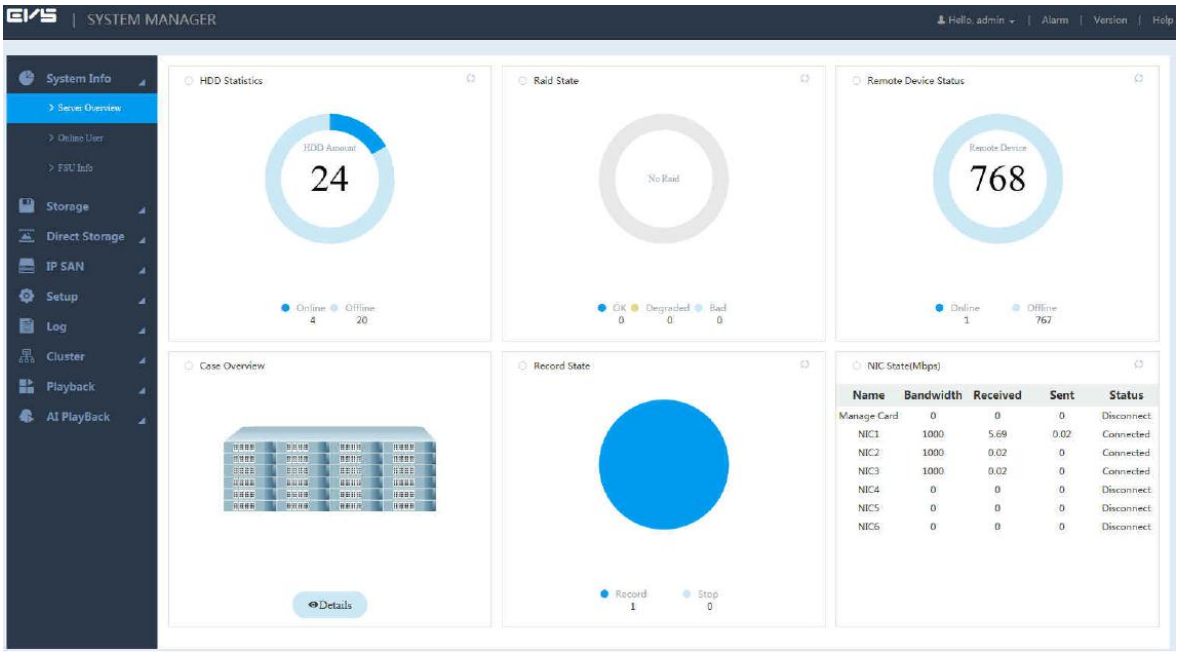
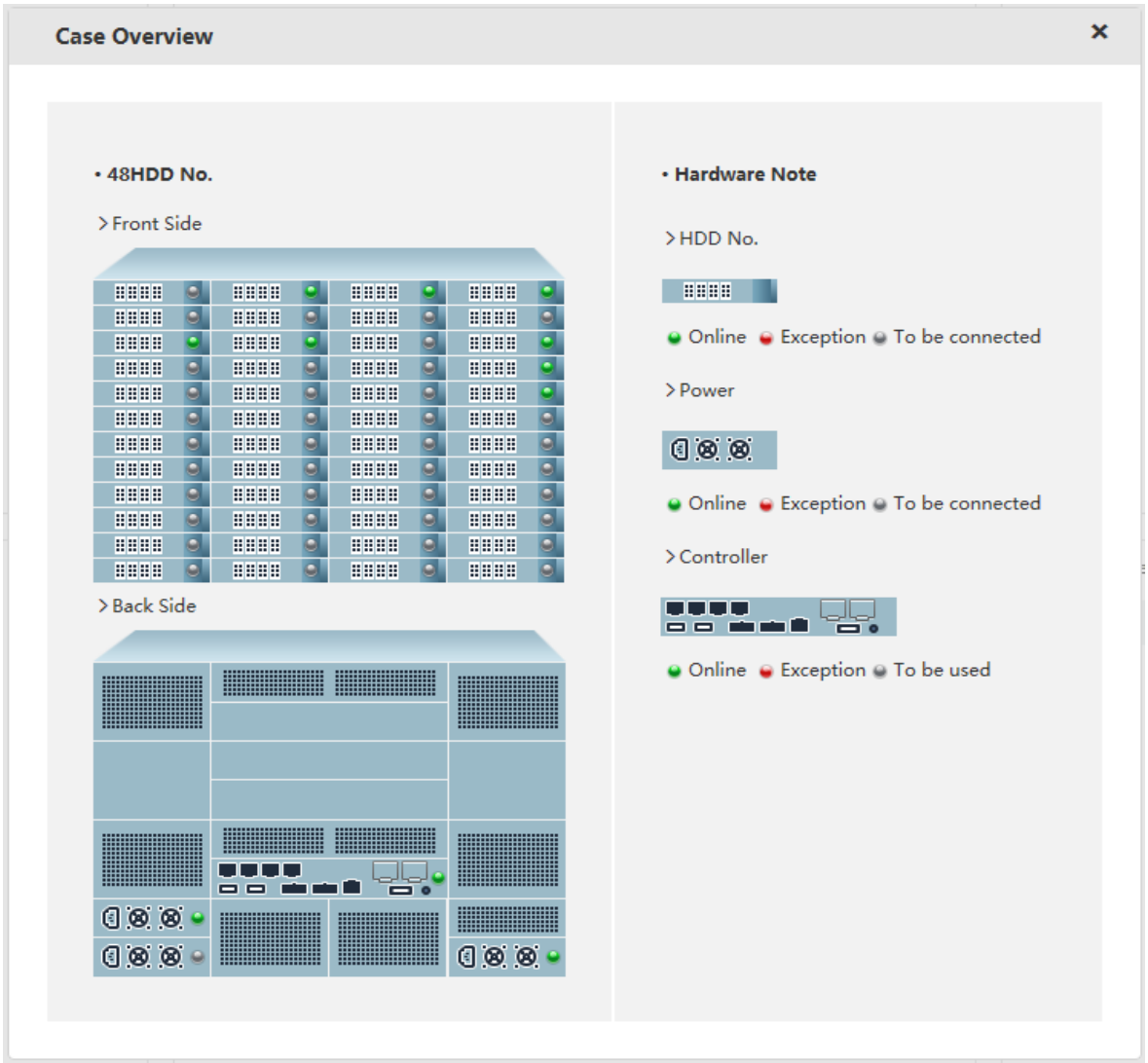


Figure 3-178 Case overview



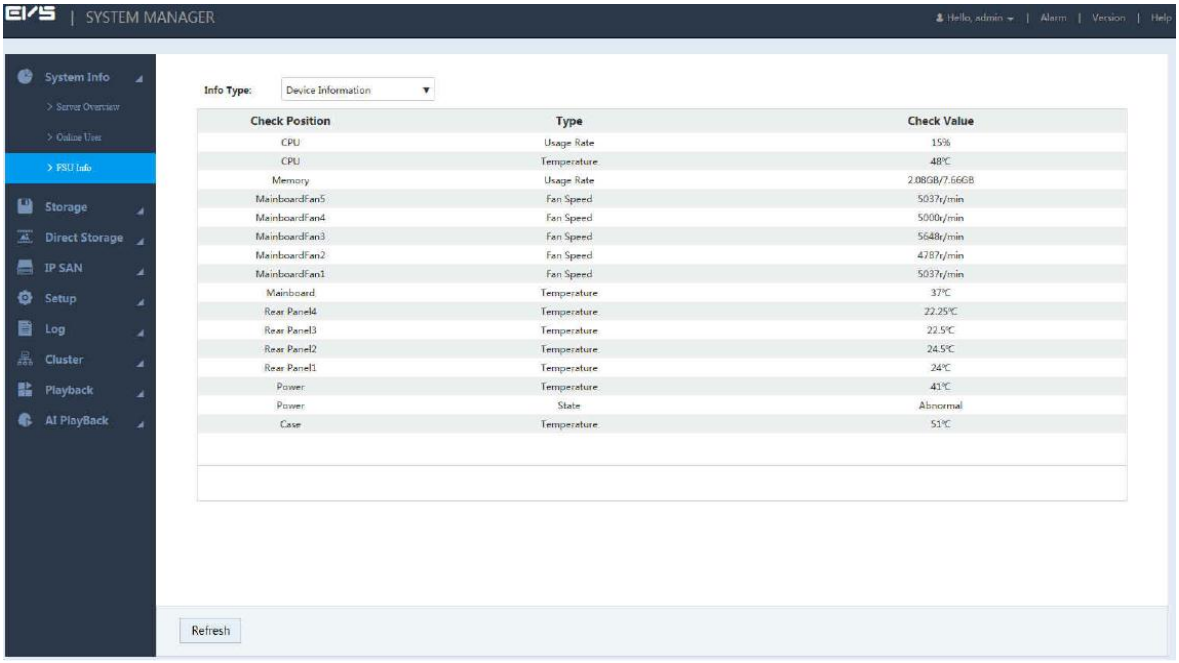
3.16.2 FSU Information

View the field surveillance unit (FSU) information, including information of master and backup devices, and all the expansion drawers.

Select **System > FSU Info**. The **FSU Info** interface is displayed. See Figure 3-179.

Click **Refresh** to get the latest device information.

Figure 3-179 FSU Information



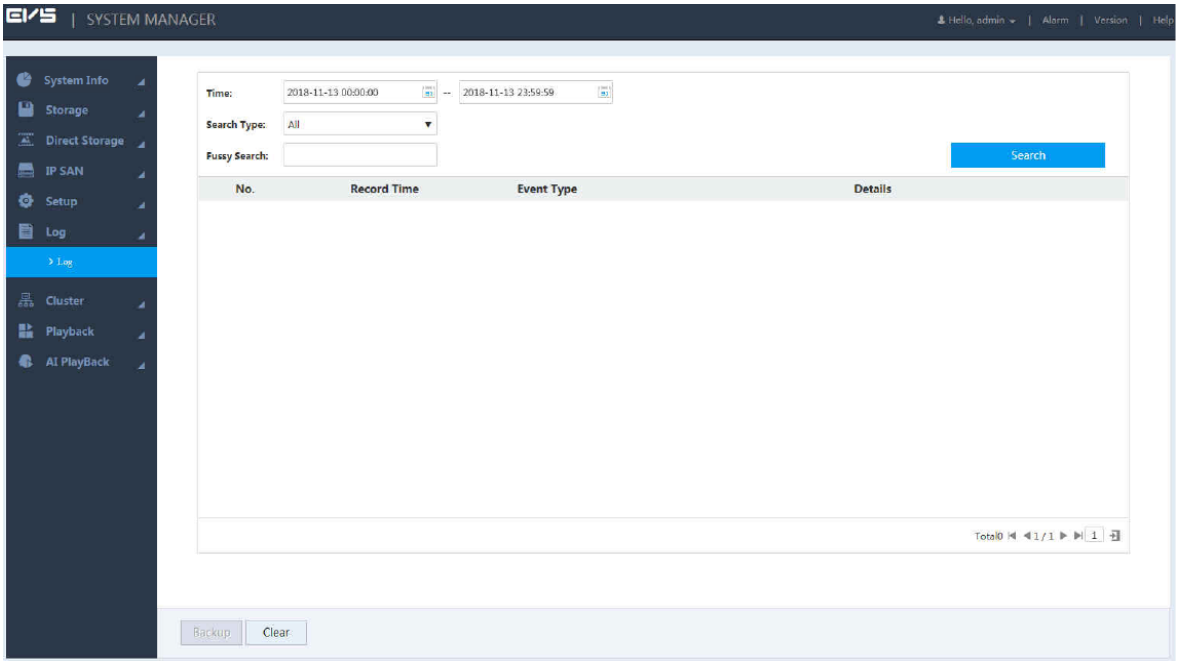
3.16.3 System Log

You can search and view the system logs or back up system logs to local PC.

Step 1 Select **Log > Log**.

The **Log** interface is displayed. See Figure 3-180.

Figure 3-180 Log (1)



Step 2 Configure the parameters. For details, see Table 3-59.

Table 3-59 Log parameters

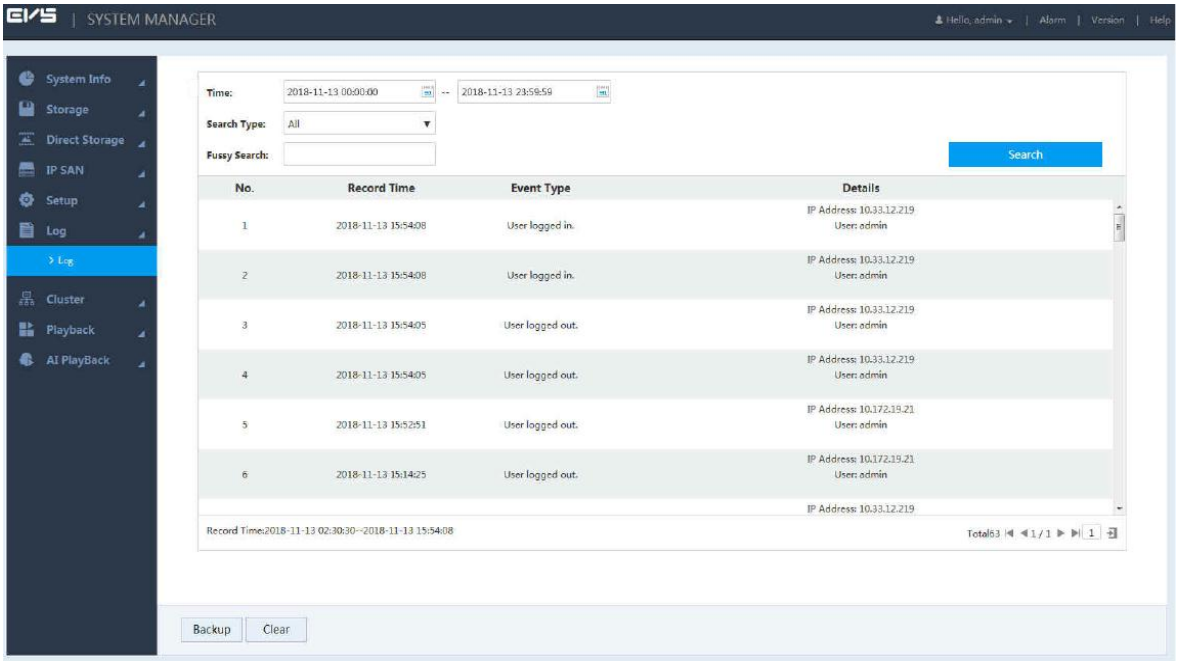
Parameter	Description
Time	Select the time period within which to search for logs.
Search Time	Select the type of the logs to search for, including all, system, config operation, storage, alarm, record operation, account, clear log, playback and connection log.
Fuzzy Search	You can enter the keyword of the log to search if you are not sure about the log type.

Step 3 Click **Search**.

The results are displayed. See Figure 3-181.

- Click **Clear** and the system deletes all the logs. Operate with care.
- Only admin user has the authority to clear the logs.

Figure 3-181 Log (2)



Step 4 (Optional) Log backup.

Click **Backup**, select the storage path, and then click **Save**. You can back up the logs to local PC. The suffix of the backup file name is .txt.

3.16.4 Alarm Log

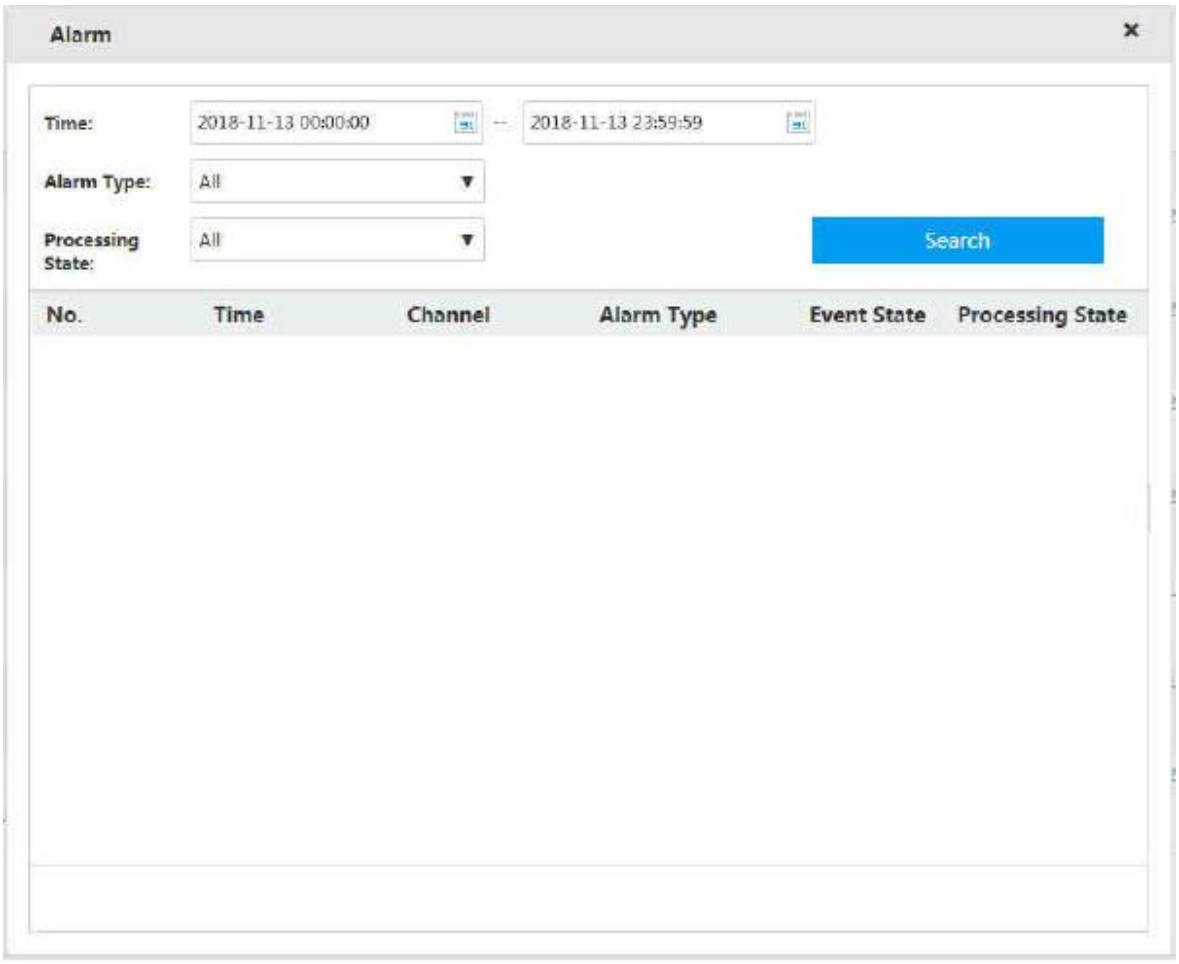
You can view the time of alarm, channel number, alarm type, and processing state.

Step 1 Click **Alarm** at the top right corner of the web.

The **Alarm** interface is displayed. See Figure 3-182.

- The alarm information on this **Alarm** interface is only valid for the current login. When login again, the system clears all the previous alarm information.
- Alarm upload must be enabled. For details, see "3.9 Configuring Events."

Figure 3-182 Alarm



Step 2 Configure alarm searching conditions. For details, see Table 3-60.

Table 3-60 Alarm searching parameters

Parameter	Description
Time	Set the time period of alarm you want to search.
Alarm Type	Set the alarm type. ● Alarm log only can be searched when alarm is enabled and alarm event is triggered. For details of enable alarm, see "3.9 Configuring Events." ● Different models of devices support different alarm types. See the actual interface of the Device.
Processing State	Set the processing state of alarm type, including all, pending, fixed, processing, false alarm, and ignored.

Appendix 1 RAID Introduction

RAID is an abbreviation of Redundant Array of Independent Disks. It combines several independent HDDs (physical HDD) to form a HDD group (logic HDD) to provide more storage capacity and data redundancy.

RAID Level

RAID level refers to the way that the disk array is organized. Different RAID levels have different data protection, availability and performance.

RAID Level	Description	Least Disk No.
RAIDJ	RAIDJ is a data protection method. With erasure codes, you can freely set the number of redundant HDD. Considering the actual scenario, the system provides redundancy of up to 8 HDDs. That is to say, the erasure code RAID can make sure the data will not lose when the 8 HDDs are broken. The security is greatly improved compared with other RAID levels.	3
RAID0	RAID0 consists of striping. Because striping distributes the contents of each file among all HDDs, reads and writes can be done concurrently. Its read and write speed is N times of single HDD (N is the number of disk that consists of RAID0). RAID0 provides no redundancy, and if one HDD fails then all data in the array is lost.	2
RAID1	RAID1 is also called mirroring. Data is written identically to two HDDs, thus improving the system reliability and performance. Its read throughput approaches the sum of throughputs of every HDD in the set, and the write throughput is limited by the slowest HDD. At the same time, RAID has the lowest disk usage, only 50%.	2
RAID2.0	Raid2.0 provides different storage strategies for the same RAID based on your data security requirements. For example, for data of the file system, it offers data security as high as RAID1; for data of ordinary files, it ensures the same security and space utilization of RAID5.	12
RAID5	It distributes data and parity information among the HDDs, and parity information and corresponding data are respectively backed up on different HDDs. Upon failure of a single HDD, subsequent data and parity information can be used to reconstruct the failed data to ensure data integrity.	3

RAID Level	Description	Least Disk No.
SRAID	Also called super RAID, it is an improved RAID configuration on the basis of RAID5. ● SRAID can be used immediately after being created. This helps improve security. ● The reconstruction and write operations are related. ● If SRAID is disconnected thus unavailable, when the connection restores, it can directly come back to work, with no need of restarting the Device. ● If one HDD is broken, the system copies the data on this HDD to a new one before deleting it. ● Read still work if SRAID fails, but part of the data may be lost.	3
RAID6	A parity information HDD is added on the basis of RAID5. The two independent parity systems use different algorithms for enhanced reliability. No data will be lost when the two HDDs fail. But compared with RAID5, it needs to distribute larger space for parity information, so it performs worse in respect of write.	4
RAID10	RAID10 is a combination of RAID1 and RAID0. It owns high read and write capabilities of RAID0, as well as high data protection and restorability of RAID1. But its HDD utilization is as low as RAID1.	4
RAID50	RAID50 is a combination of the RAID5 and RAID0. It has higher fault-tolerance. There is no data loss even one HDD in the set malfunctions.	6
RAID60	RAID60 is a combination of the RAID6 and RAID0. It has higher fault-tolerance and read performance. There is no data loss even two HDDs in one set malfunctions.	8

RAID Capacity Calculation

CapacityN refers to the HDD with the minimum capacity in the set. The capacity shall be subject to the value on the web.

Parameter	Total Capacity of N HDDs
RAIDJ	(N-M) × min (capacityN) M: Select M check disk(s) on the interface.
SRAID	(N-1) × min (capacityN)
RAID60	(N-4) × min (capacityN)
RAID50	(N-2) × min (capacityN)
RAID10	(N/2) × min (capacityN)
RAID6	(N-2) × min (capacityN)
RAID5	(N-1) × min (capacityN)

Parameter	Total Capacity of N HDDs
RAID1	Min (capacityN)
RAID0	Total capacity of the HDDs in the set

Appendix 2 Glossary

FTP	File Transfer Protocol (FTP) is a protocol of the TCP/IP protocol group. It transfers file from one PC to another, without consideration of the location, connection type, and operation system of the PC.
IP SAN	Internet Protocol Storage Area Network (IP SAN) is an IP-based network storage technology.
iSCSI	Internet Small Computer System Interface (iSCSI) is an internet protocol standard in Ethernet, and an SCSI instruction set for hardware to be used in IP protocol layer. Briefly, iSCSI can realize SCSI protocol in the IP network, so router option is available in high-speed 1000M Ethernet.
LAN	Local Area Network (LAN) is a computer network that interconnects computers within a limited area (such as an office building or a school).
NFS	Network File System (NFS) is a distributed file system protocol. It allows a client computer to access files or peripheral devices of another PC. It is mainly used in UNIX-like platforms.
MTU	Maximum Transmission Unit (MTU) is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
SAMBA	It is a free software that can realize Server Messages Block (SMB) on Linux and Unix systems. It consists of server and client.
SATA	Serial Advanced Technology Attachment (SATA) is a serial HDD interface that can realize serial data transmission. The current released Serial ATA 2.0 enjoys maximum theoretical transfer speed of 300MB/s.
SATA HDD	HDD that adopts SATA standard. Some leading manufacturers such as Seagate, Western Digital, and Hitachi are offering SATA HDDs.
SMART	Self-Monitoring Analysis and Reporting Technology (SMART) is an automatic monitoring and alarming system of HDD status. It monitors and records the HDD through monitoring instructions in the HDD, and compares the monitoring results with the preset security value of the manufacturer. If the monitoring situation is about to exceed or already exceeded the preset value, an alarm will be triggered, and small-scale repair will be initiated. This helps ensure the security of HDD data.
TCP	Transmission Control Protocol (TCP) is a transmission-layer communication protocol that provides reliable and ordered delivery of a stream of bytes.
UDP	User Datagram Protocol (UDP) is a connectionless communication protocol used for processing data packets.
WAN	Wide Area Network (WAN) is a computer network that extends over a large geographical distance. It connects physically disparate LANs and computer systems for the purpose of resource sharing.
Storage Pool	It is a virtual logic device. It can consist of several HDDs and RAID groups. It is a main way to realize virtual storage.

Synchronization	After creating RAID1 or RAID5, and before using it, the system needs to read and write the HDD at a fixed speed and adopts an algorithm to calculate. This process is called synchronization. During synchronization, the system performance speed is very low.
Shared Directory	Local PC access the top path of the shared storage space. You can create, remove, authenticate and set valid user at the storage device. User is only allowed to operate folder and file performance in the under-layer. According to different share protocols, it can be divided into SAMBA share folder, NFS share folder and FTP share folder.
Working Status	It is for RAID6/RAID5/RAID1. It is the RAID status after it completes synchronization operation. When the RAID group is in working status, on the **Storage > RAID** interface, the RAID device status is "clean."
Degraded Status	It is a status after you remove one disk from RAID1/RAID5 (working status) or remove two disks from RAID6. The status shows "degraded."
Manageable Status	It is a device status when controller configure device by web. Actually, when there is no error or damage, the device shall always be in manageable status.
Ready Status	It is a device status when controller access HDD by network. The system is ready to use after you configure correctly in accordance with the Manual. Some non-device error (such as configuration error, hot swap error) may result in device failure. You can configure again to boot up the Device. But data loss may occur during this process.

Appendix 3.1 Middle-class 16-HDD Single-controller Series

Model		**Middle-Class 16-HDD Single-Controller**
OS	Main processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/iSCSI/ SMB/NFS/FTP
	Media protocol	ONVIF, etc.
HDD	HDD amount	16 SATA HDDs (Max 8T/HDD) Support SATA/SSD HDD Does not support SAS HDD
	SAS port	1 SAS port
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60, SRAID, RAID2.0, JRAID. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is created
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety
	HDD roaming	HDD or RAID group can be removed from one device

Model		Middle-Class 16-HDD Single-Controller
		and then installed on another. Data is safe
	Logic volume Manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 320-channel (640Mbps) front-end connection and storage, 160-channel (320Mbps) transfer, 32-channel (64Mbps) network playback
	Record playback	WEB. Search unit is second Various playback speeds
	IP SAN mode	IP SAN direct storage
	Snapshot	Support snapshot function. Create logic volume to backup data
	Volume clone	Support clone function. Create logic volume to back up the whole data
	Frame extracting	Support frame extracting and storage function. Support time and the frame setup
	Cluster service	Support N+M cluster service
	Auto transfer after power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK
Port	USB interface	One USB 3.0 port, one eSATA/USB2.0 hybrid port
	Network connection	Two 1000Mbps data ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	RS232	One RS232 port
Others	Power	100V–240V, 47–63Hz One series has single power supplying one series has redundant power supply Support hot swap
	Total power consumption	< 200W (with HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–2000m
	Dimensions (L*W*H)	473.6mm*484.6mm*133.2mm (with handle)
	Weight	11kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation

Appendix 3.2 Middle-class 24-HDD Single-controller Series

Model		Middle-Class 24-HDD Single-Controller
OS	Main processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media protocol	ONVIF, etc.
HDD	HDD amount	24 SATA HDDs (Max 6T/HDD) Support SSD HDD Support 2.5-inch HDD
	SAS port	2 SAS ports
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60, SRAID, RAID2.0, JRAID. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is created
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety
	HDD roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe
	Logic volume manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 320-channel (640Mbps) front-end connection and storage, 160-channel (320Mbps) transfer, 32-channel

Model		Middle-Class 24-HDD Single-Controller
		(64Mbps) network playback
	Record playback	WEB Search unit is second Various playback speeds
	IP SAN mode	IP SAN direct storage
	Snapshot	Support snapshot function. Create logic volume to backup data
	Volume clone	Support clone function. Create logic volume to back up the whole data
	Frame extracting	Support frame extracting and storage function. Support time and the frame setup
	Cluster service	Support N+M cluster service
	Auto transfer after power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK
Port	USB interface	Two USB 3.0 ports
	Network connection	Default mode: five 100/1000Mbps Ethernet ports (one 100/1000Mbps Ethernet management port + four 100/1000Mbps Ethernet data ports) Extension mode: five 100/1000Mbps Ethernet ports + two 10000Mbps optical ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	RS232	One RS232 port
Others	Power	100V–240V, 47–63Hz 2 redundant power supplying Support hot swap
	Fan	DC12V 1.5A Fan diameter: 80mm Hot swap
	Total power consumption	200–400W (with HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–3000m
	Dimensions (W*H*D)	483mm*175mm*494mm (with handle)
	Weight	27kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation

Appendix 3.3 Middle-class 36-HDD Single-controller Series

Model		Middle-Class 36-HDD Single-Controller
OS	Main processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media protocol	ONVIF, etc.
HDD	HDD amount	36 SATA HDDs (max 6T/HDD) Support SSD HDD Support 2.5-inch HDD
	SAS port	1 SAS port
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60, SRAID, RAID2.0, JRAID. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is created
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety
	HDD roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe
	Logic volume manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 320-channel (640Mbps) front-end connection, storage, 160-channel (320Mbps) transfer, 32-channel

Model		Middle-Class 36-HDD Single-Controller
		(64Mbps) network playback
	Record playback	WEB Search unit is second Various playback speeds
	IP SAN mode	IP SAN direct storage
	Snapshot	Support snapshot function. Create logic volume to backup data
	Volume clone	Support clone function. Create logic volume to back up the whole data
	Frame extracting	Support frame extracting and storage function. Support time and the frame setup
	Cluster service	Support N+M cluster service
	Auto transfer after power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK
Port	USB interface	Two USB 3.0 ports
	Network connection	Default mode: five 100/1000Mbps Ethernet ports (one 100/1000Mbps Ethernet management port + four 100/1000Mbps Ethernet data ports) Extension mode: five 100/1000Mbps Ethernet ports + two 10000Mbps optical ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	RS232	One RS232 port
Others	Power	100V–240V, 47–63Hz 2+1 redundant power supplying Support hot swap
	Fan	DC12V 1.5A Fan diameter: 80mm Hot swap
	Total power consumption	200–400W (with HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–3000m
	Dimensions (W*H*D)	483mm*175mm*670.5mm (with handle)
	Weight	35kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation

Appendix 3.4 Middle-class 48-HDD Single-controller Series

Model		Middle-Class 48-HDD Single-Controller
OS	Main processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media protocol	ONVIF, etc.
HDD	HDD amount	48 SATA HDDs (Max 6T/HDD) Support SSD HDD Support 2.5-inch HDD
	SAS port	2 SAS ports
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60, SRAID, RAID2.0, JRAID. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is created
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety
	HDD roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe
	Logic volume manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 320-channel (640Mbps) front-end connection, storage, 160-channel (320Mbps) transfer, 32-channel (64Mbps) network playback
	Record playback	WEB

Model		Middle-Class 48-HDD Single-Controller
		Search unit is second Various playback speeds
	IP SAN mode	IP SAN direct storage
	Snapshot	Support snapshot function. Create logic volume to backup data
	Volume clone	Support clone function. Create logic volume to back up the whole data
	Frame extracting	Support frame extracting and storage function. Support time and the frame setup
	Cluster service	Support N+M cluster service
	Auto transfer after power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK
Port	USB interface	Two USB 3.0 ports
	Network connection	Default mode: five 100/1000Mbps Ethernet ports (one 100/1000Mbps Ethernet management port + four 100/1000Mbps Ethernet data ports) Extension mode: five 100/1000Mbps Ethernet ports + two 10000Mbps optical ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	RS232	One RS232 port
Others	Power	100V–240V, 50–60Hz 3 redundant power supplying. Support hot swap
	Fan	DC12V 1.5A, Fan diameter:80mm, Hot swap
	Total power consumption	175–950W (With HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–3000m
	Dimensions(W*H*D)	482.6mm×347.8mm×558.55mm (with handle)
	Weight	50kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation

Appendix 3.5 High-end 24-HDD Single-controller

Model		**High-End 24-HDD Single-Controller**
OS	Main processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	Default 8G Max support 16G
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP, RTSP, UDP, HTTP, NTP, SNMP protocol
	Media protocol	ONVIF, etc.
HDD	HDD amount	24 SATA/SAS HDDs (Max 6T/HDD) SAS/SATA HDD composite connection Support SSD, 2.5-inch HDD
	SAS port	2 SAS ports
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID10, RAID5, RAID6, RAID50, RAID60, SRAID, RAID2.0, JRADI. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is create
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety
	HDD roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe
	Logic volume manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
	Cluster service	N+M cluster service
	ANR	After diconnection, system can download the record file from the SD card on the network camera to maintain the full record file
Record and Playback	Record mode	Manual recording, motion detection recording, schedule recording and alarm recording Priority: manual recording > alarm recording >

Model		High-End 24-HDD Single-Controller
		detection recording > schedule recording Support event pre-record
	Record schedule	Main stream/sub stream storage by period I frame storage by period
	Record search	Various search engines such as time, type and channel, front-end position information
	Record protection	Record protection function to prevent vicious modification. Protection time is adjustable
	Record backup	Flash disk, portable HDD, eSATA
	Record download	WEB
	Record playback	WEB Search unit is second Various playback speeds
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 512-channel (1024Mbps) front-end connection and storage, 256-channel (512Mbps) transfer, 32-channel (64Mbps) network playback
	Transfer mode performance	4096Mbps front-end connection, 4096Mbps network transfer
	IP SAN mode	IP SAN direct storage
	IP SAN performance	IP SAN working mode: Storage bandwidth shall not be less than 3.6Gbps
Port	USB interface	One USB 2.0 port and one USB 3.0 port The USB 2.0 port can also be used as eSATA port
	Network connection	Default mode: five 100/1000Mbps Ethernet ports (one 100/1000Mbps Ethernet management port + four 100/1000Mbps Ethernet data ports) Extension mode: five 100/1000Mbps Ethernet ports + two 10000Mbps optical ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	Alarm port	4 input/4 output
	RS232 RS485	One RS232 port One RS485 port
Others	Power	100V–240V, 47–63Hz 2 redundant power supply Support hot swap
	Fan	Redundant dual ball bearing fan MTBF > 100 thousand hours Hot swap
	Total power consumption	200–400W (with HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)

Model		High-End 24-HDD Single-Controller
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–3000m
	Dimensions (W*H*D)	483mm*175mm*494mm (with handle)
	Weight	27kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation

Appendix 3.6 High-end 48-HDD Single-controller

Model		High-end 48-HDD Single-controller
OS	Main processor	64-bit high-performance multiple-core processor
	Controller	Single controller
	Operation system	Embedded LINUX system
	Memory	8GB (default). Max 16G
	Case	1.2mm extra-thickness hot-dip galvanized steel High accuracy aluminum alloy slider Self-developed patent removable HDD bracket
	User interface	WEB
	Network protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/iSCSI/SMB/NFS/FTP
	Media protocol	ONVIF, etc.
HDD	HDD amount	48 HDDs (Max 6T/HDD) SAS/SATA HDD composite connection
	SAS port	2 SAS ports
	HDD installation	Additional HDD bracket, support HDD hot swap, online replacement
	HDD mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID10, RAID5, RAID6, RAID50, RAID60, SRAID, RAID2.0, JRAID. JBOD, hot spare
	HDD manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span
	HDD process	HDD bad track mapping to enhance HDD life span
	HDD status detect	Pre-detect before HDD use, schedule detect when the HDD is in use
	RAID plug and play	RAID becomes available once it is created
	RAID rebuild	Dynamically adjust RAID rebuild speed to guarantee system

Model		High-end 48-HDD Single-controller
		load balance
	RAID sync-write	RAID Sync-write technology to guarantee data safety.
	HDD roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic volume manager	Support iSCSI volume management, NAS (SMB\NFS\FTP) volume management
	Snapshot	Support snapshot function, create user volume to backup data
	Volume clone	Support clone function. Create user volume to backup the complete data
	Extract frame	Support extracting P frame function. Customizied extracting period and backup rate setup
	ANR	After diconnection, system can download the record file from the SD card on the network camera to maintain the full record file
	Shortcut RAID creation	Click one button to create RAID conveniectly
Record and Playback	Record mode	Manual recording, motion detection recording, schedule recording and alarm recording Priority: manual recording > alarm recording > detection recording > schedule recording Support event pre-record
	Record schedule	Main stream/sub stream storage by period I frame storage by period
	Record search	Various search engines such as time, type and channel, front-end position information
	Record protection	Record protection function to prevent vicious modification. Protection time is adjustable
	Record backup	Flash disk, portable HDD, eSATA
	Record download	WEB
	Record playback	WEB Search unit is second Various playback speeds
Performance	Video stream mode	Video stream direct storage
	Video stream storage mode	Max 768-channel (1536Mbps) front-end connection, storage and transfer, 64-channel (128Mbps) network playback
	Transfer Mode	4096Mbps front-end connection, 4096Mbps network transfer

Model		High-end 48-HDD Single-controller
	Performance	
	IP SAN mode	IP SAN direct storage
	IP SAN performance	IP SAN working mode: storage bandwidth shall not be less than 3.6Gbps
Port	USB interface	One USB 2.0 port and one USB 3.0 port The USB 2.0 port can be reused as the eSATA port
	Network connection	Default mode: five 100/1000Mbps Ethernet ports (one 100/1000Mbps Ethernet management port + four 100/1000Mbps Ethernet data ports) Extension mode: five 100/1000Mbps Ethernet ports + two 10000Mbps optical ports
	Ethernet port	Support load balance, fault-tolerance, etc.
	RS232 RS485	One RS232 port One RS485 port
Others	Power	100V–240V, 47–63Hz 2+2 redundant power supply Support hot swap
	Fan	DC12V, 1.5A Hot swap Fan diameter: 80mm
	Total power consumption	1000W (with HDD)
	Working temperature	0°C–40°C
	Working humidity	10%–80% (non-condensing)
	Storage temperature	-20°C–70°C
	Storage humidity	5%–90% (non-condensing)
	Working altitude	-60m–5000m
	Dimensions (W*H*D)	444.4mm*352.8mm*494mm (with handle) 444.4mm*352.8mm*532mm (without handle)
	Weight	49.92kg (excluding package or HDD)
	Installation mode	Standard 19-inch rack installation