Embedded Video Storage (EVS50/EVS70)

User's Manual

V2.1.4

Foreword

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"). Read carefully before using the device, and keep the manual safe for future reference.

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 signal words 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, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V2.1.4	Added particulate and gaseous contamination specifications.	February 2022
V2.1.3	Deleted the strategy of shortcut RAID creation.	July 2021
V2.1.2	Updated the format according to the latest template.	June 2021
V2.1.1	Update the manual according to the latest template.	May 2019

Version	Revision Content	Release Time
V2.1.0	Update information about GDPR. Add AI playback and routing functions. Update user management and playback functions.	October 2018
V2.0.2	Add FCC information.	September 2018
V2.0.1	Add privacy protection notice.	May 2018
V2.0.0	Baseline switch.	October 2017
V1.0.0	First release.	January 2017

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements

⚠ WARNING

- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The device is heavy and needs to be carried by several persons together to avoid personal injuries.

⚠

- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Operate the device within the rated range of power input and output.
- Use the device under allowed humidity and temperature conditions.
- Do not drip or splash liquid onto the device, make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Do not disassemble the Device.
- The device can only be used with batteries possessing internal protection.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the device during an update.
- Make sure the update file is correct because an incorrect file can result in a device error occurring.
- Do not frequently turn on/off the device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the device.
- Operating temperature: 0 °C to 45 °C (32 °F to 113 °F).
- Salt pray in the operating environment of the device might corrode its electronic components and cables. To ensure the normal operation of the device and prolong its service life, use the device in an indoor environment that is 3 kilometers away from the sea.

Installation Requirements

⚠ WARNING

- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.

- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited for the battery to be thrown into a fire or furnace, and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.

⚠

- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Install the server on a stable surface to prevent it from falling.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements and rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the device casing to reduce the transient voltage to the defined range.
- If you did not push the HDD box to the bottom, then do not close the handle to avoid damage to the HDD slot.
- Install the device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the device securely to the building before use.

Maintenance Requirements

⚠ WARNING

- Make sure to use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly according to the instructions on it.
- Power off the device before maintenance.

⚠

- AI module does not support hot plug. If you need to install or replace the AI module, unplug the device power cord first. Otherwise, it will lead to file damage on the AI module.
- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the device.

- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Transportation Requirements

⚠

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

⚠

Store the device under allowed humidity and temperature conditions.

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 operating 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 & forwarding 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

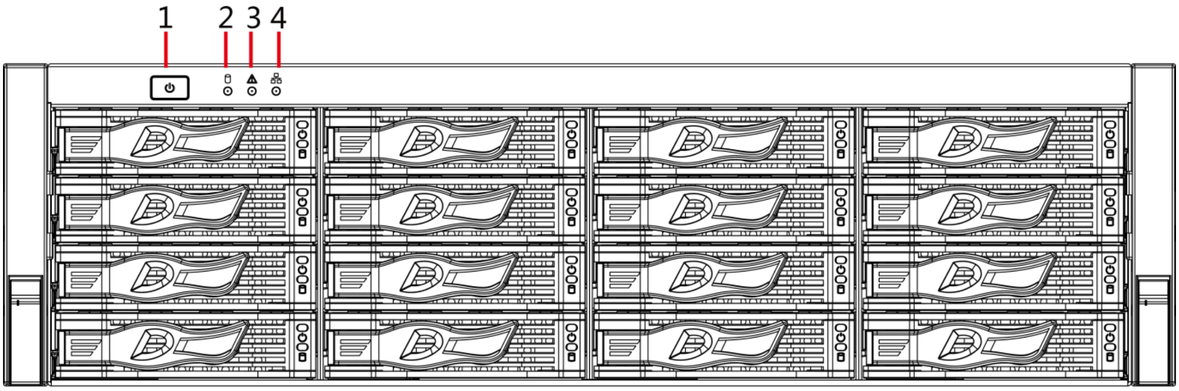


Table 1-1 Front panel description

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the Device is powered 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

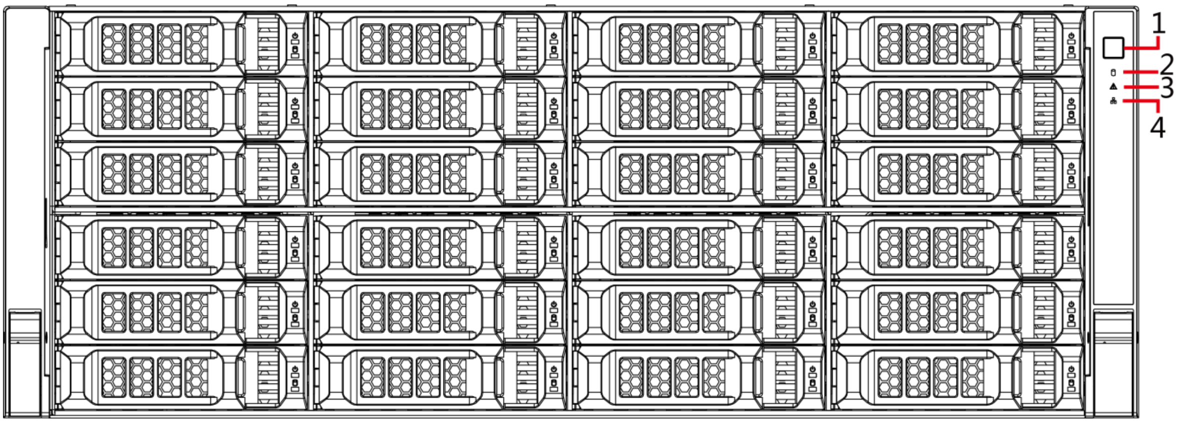


Table 1-2 Front panel description

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the device is powered 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

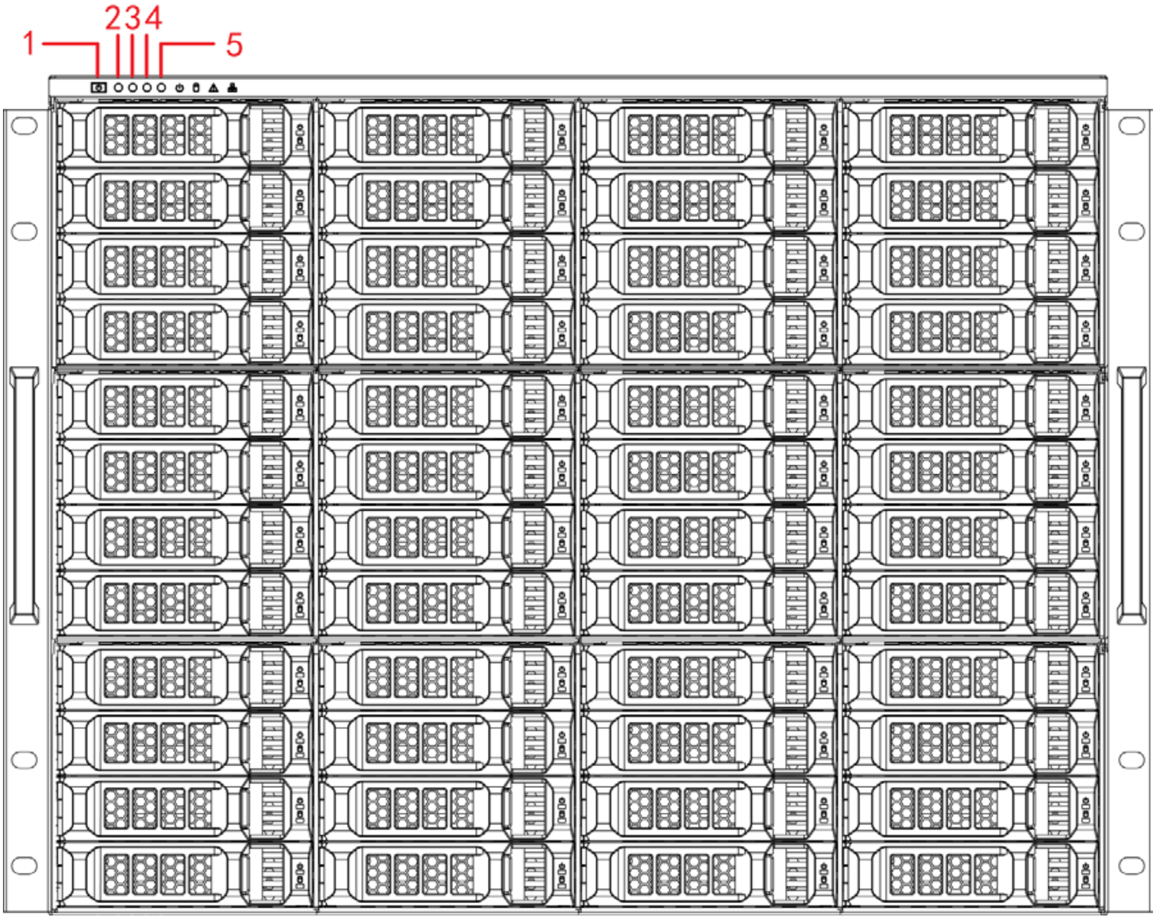


Table 1-3 Front panel description

No.	Indicator/Button	Description
1	Power button	Turns on or off the device. This button keeps blue light on when the device is powered 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

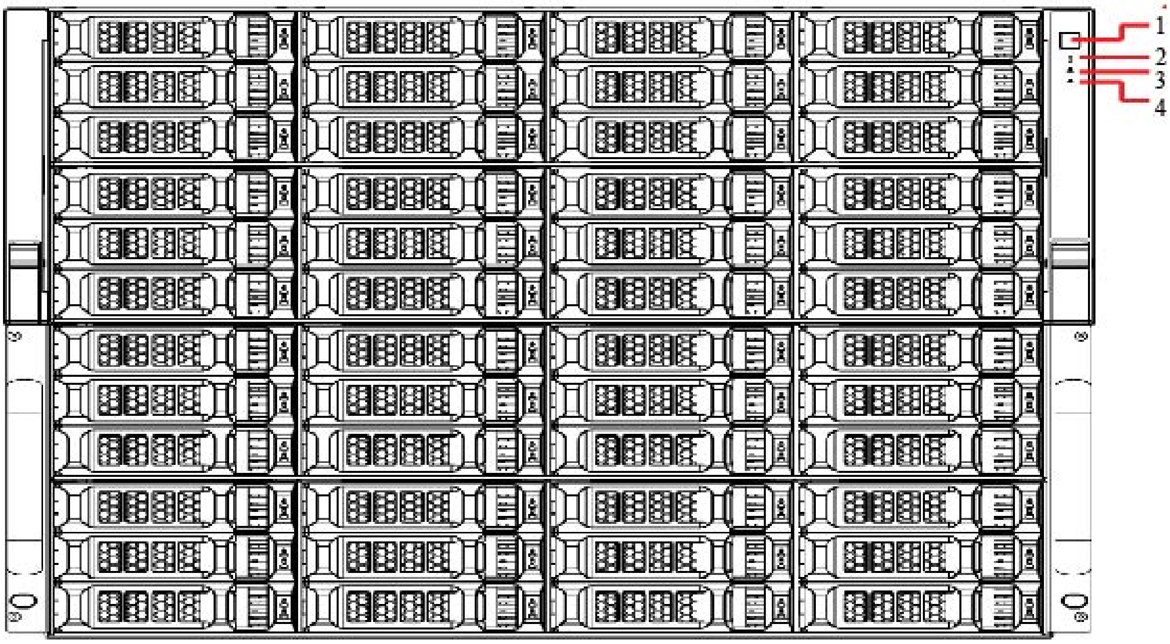


Table 1-4 Front panel description

No.	Indicator /Button	Description
1	Power button	Turns on or off the Device. This button keeps blue light on when the device is powered 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

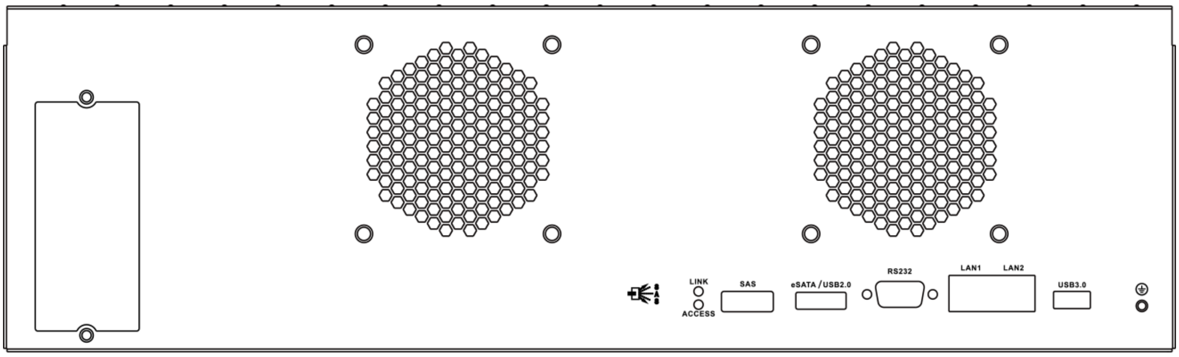


Figure 1-6 Middle-class 16-HDD single-controller with redundant power

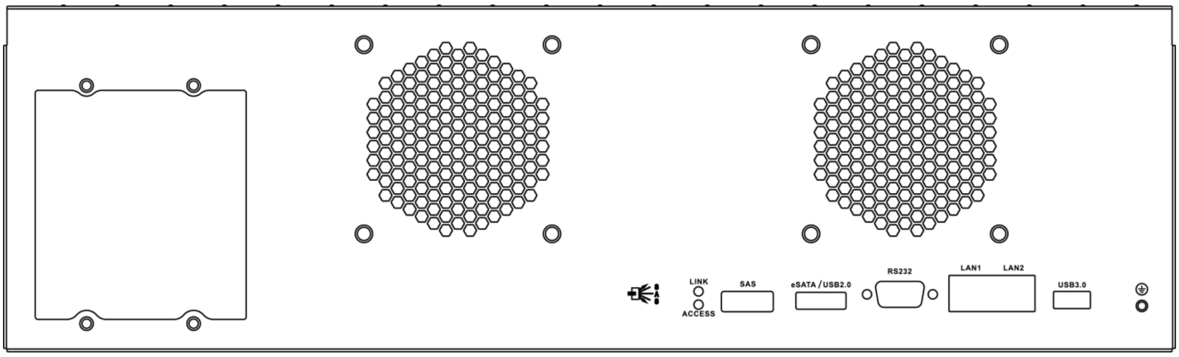


Table 1-5 Rear panel ports

Port/Indicator	Description
USB3.0	Connects the mouse and USB storage devices.
LAN1, LAN2	Gigabit data port. Used for data transmission.
RS-232	RS-232 port.
eSATA, USB2.0	Multiplex port for eSATA and USB2.0.
SAS	Connects the IN port of the expansion drawer.
Link/ACCESS	Status indicator for SAS port.
Power input	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)

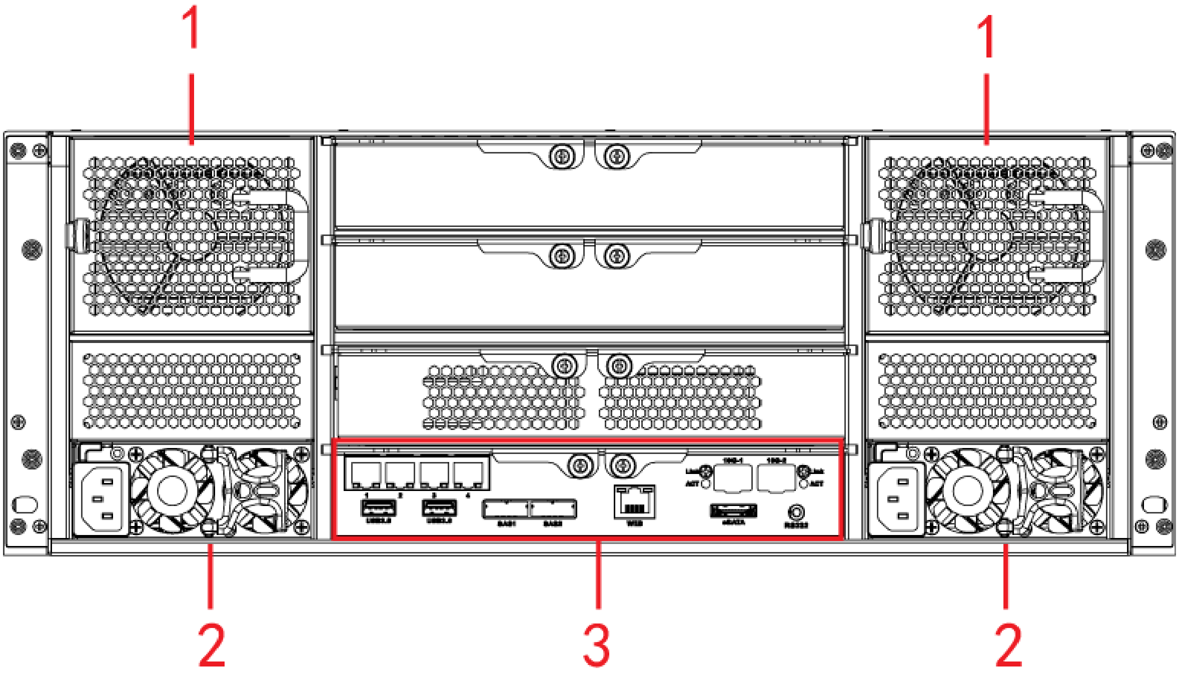


Figure 1-8 Rear panel (7 Ethernet ports)

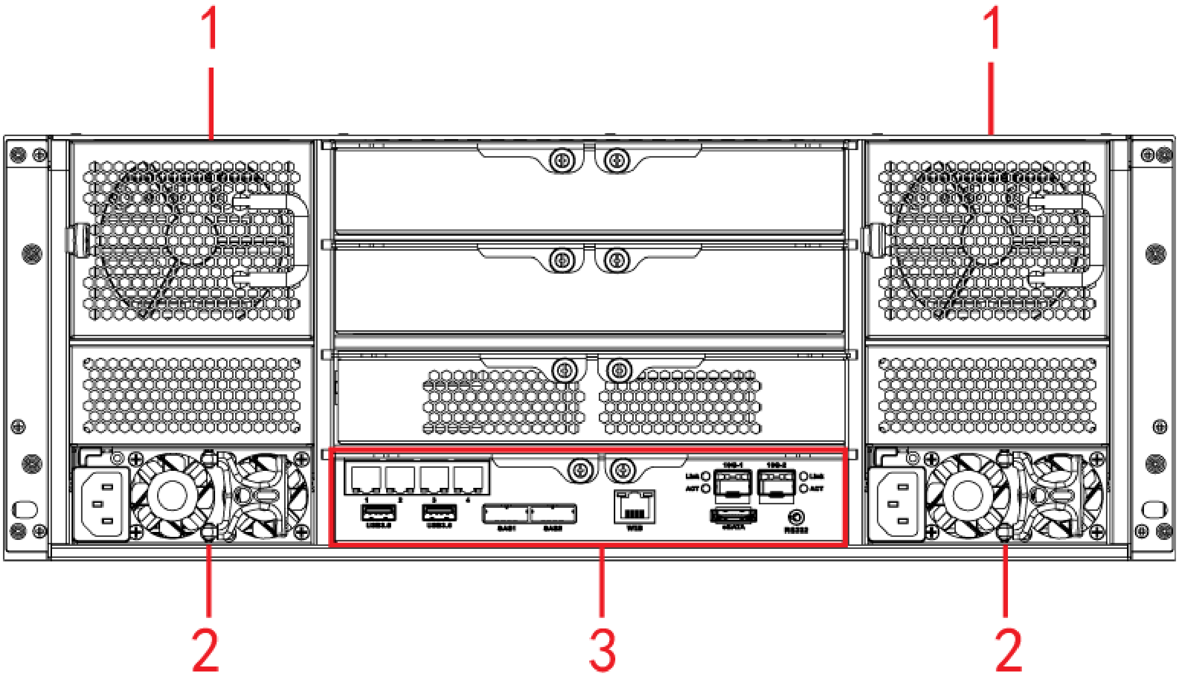


Figure 1-9 Rear panel (9 Ethernet ports)

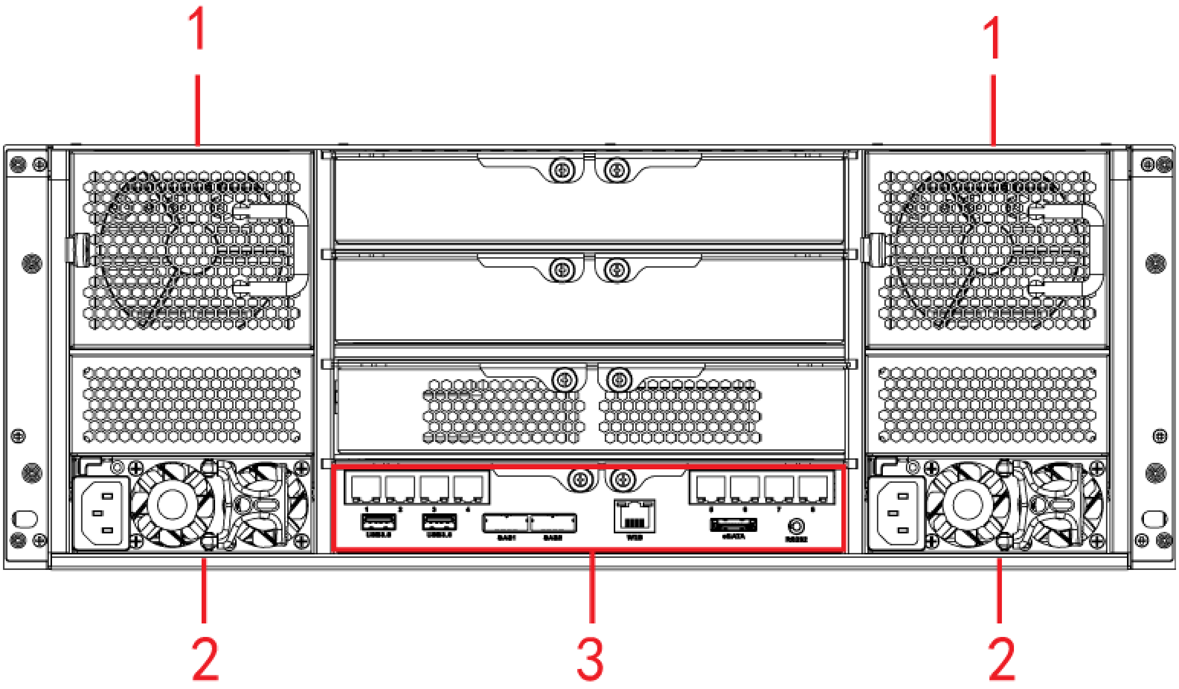


Table 1-6 Rear panel description

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

Table 1-7 Main control module ports

Port/Indicator	Description
1–4/5–8	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA	eSATA port.
SAS1, SAS2	Connects the IN port of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
RS-232	RS-232 port.
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)

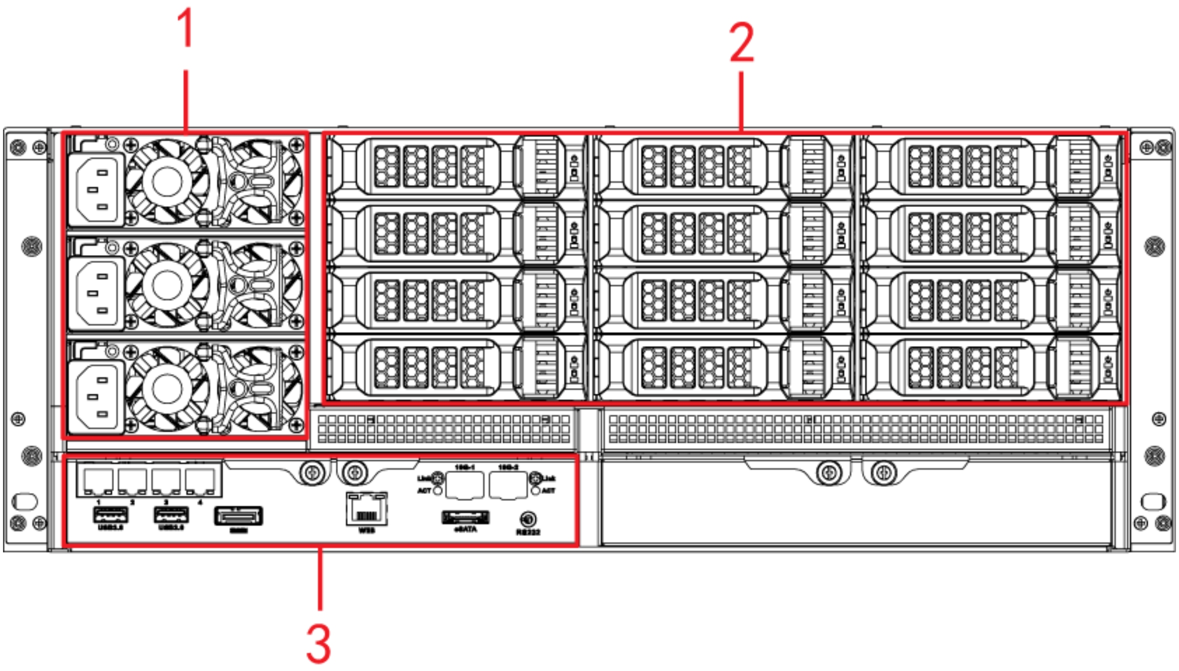


Figure 1-11 Rear panel (7 Ethernet ports)

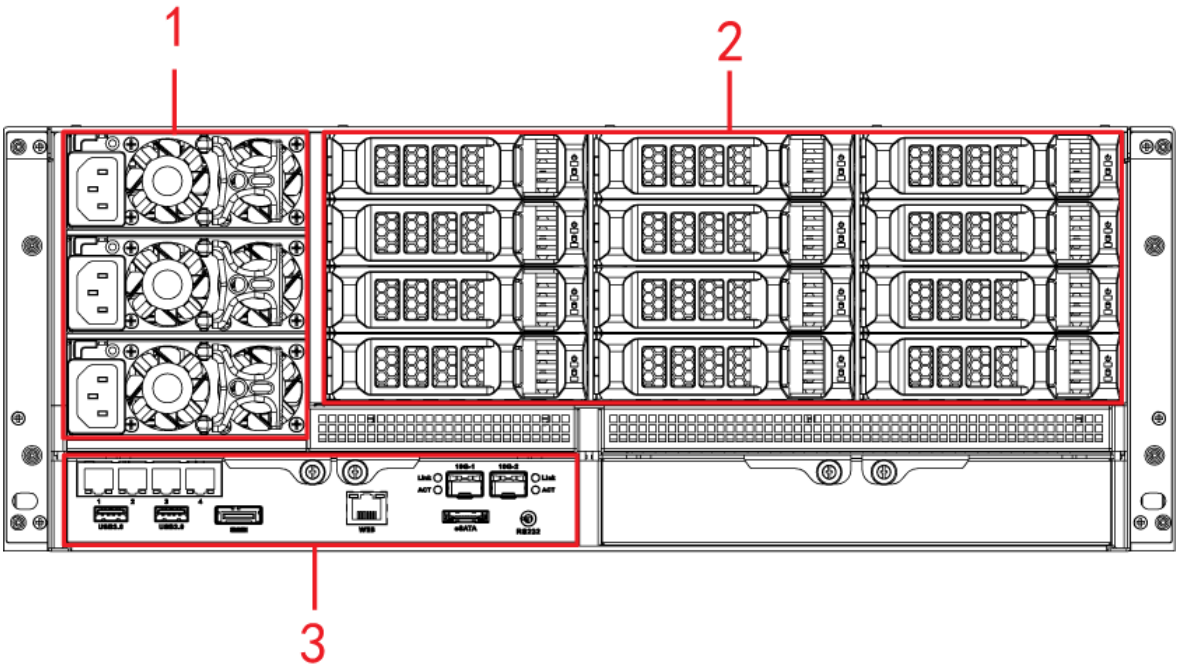


Figure 1-12 Rear panel (9 Ethernet ports)

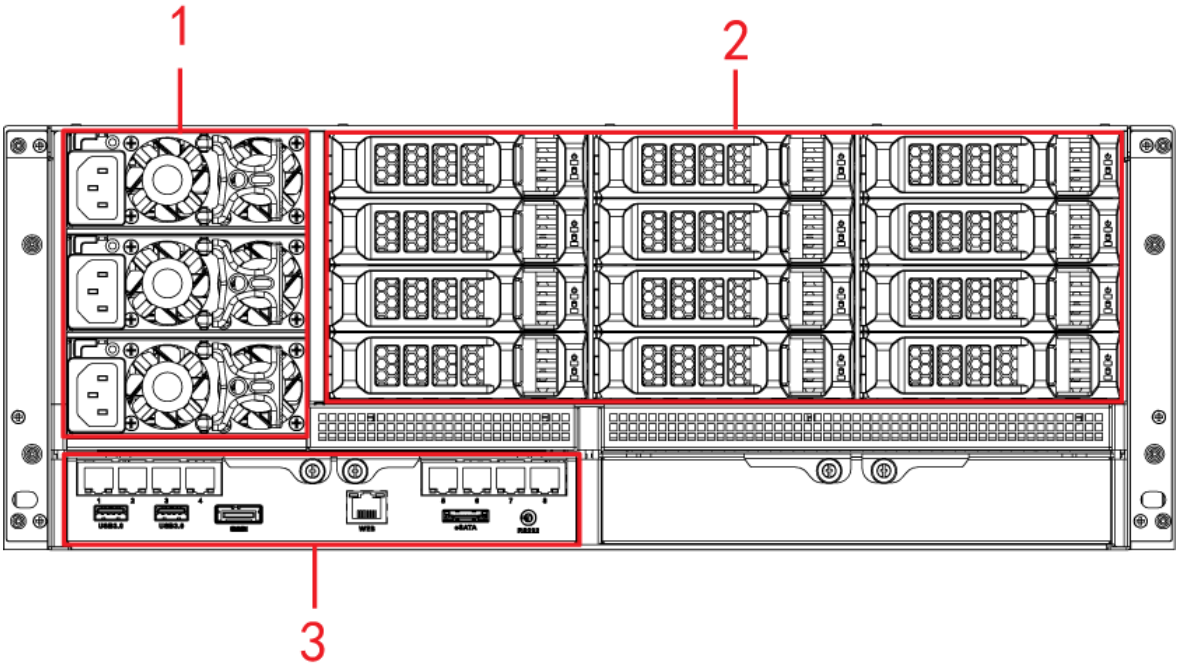


Table 1-8 Rear panel description

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

Table 1-9 Main control module ports

Port/Indicator	Description
1–4/5–8	Gigabit data port. Used for data transmission.
USB3.0	Connects the mouse and USB storage devices.
eSATA	eSATA port.
SAS	Connects the IN port of the expansion drawer.
Web	Gigabit management port. Can be used as data port.
RS-232	RS-232 port.
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

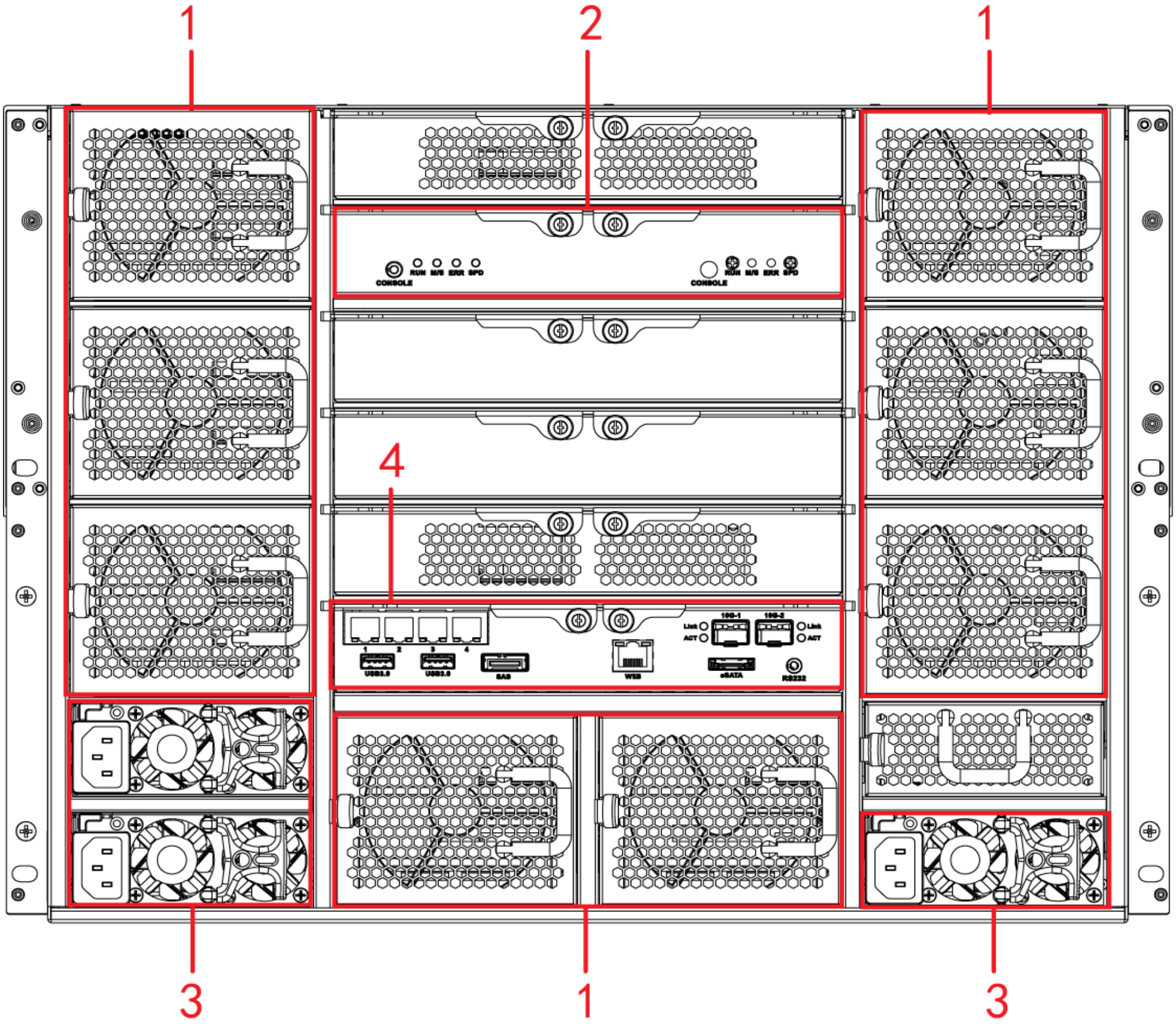


Table 1-10 Rear panel description

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

Table 1-11 Main control module ports

Port	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 port.
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.

Port	Description
RUN	RUN light flickers when the device is powered on and running.
RS-232	RS-232 port.
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 ports

Indicator	Description
CONSOLE	Serial port. It is mainly used for debugging the device and logging in the command line port.
RUN	RUN light flickers when the device is powered 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 6 G and the light goes out if the speed reaches 6 G.

1.3.5 High-end 24-HDD Single-controller

Figure 1-14 Rear panel (5 Ethernet ports)

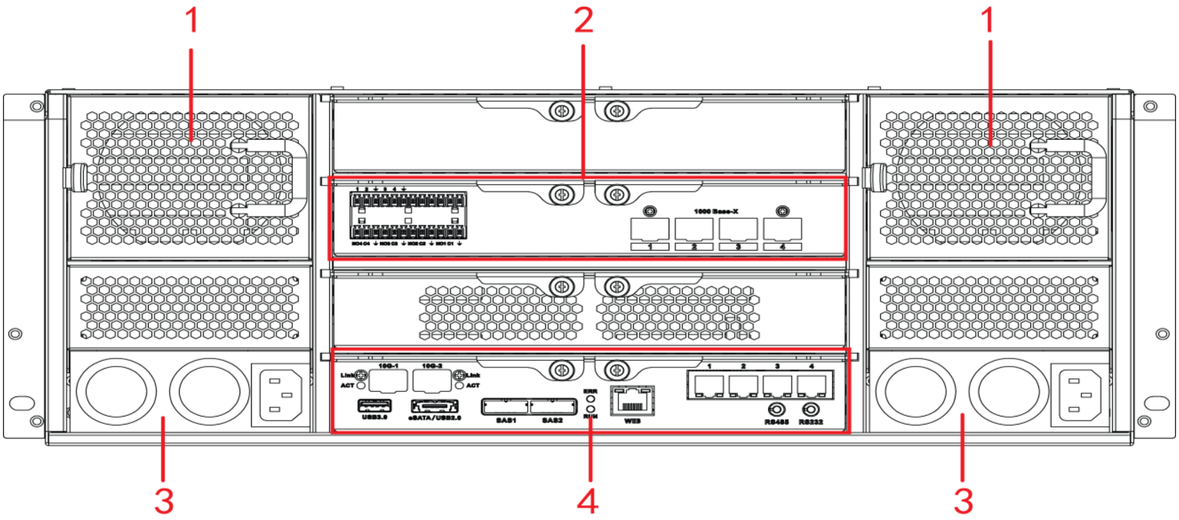


Figure 1-15 Rear panel (7 Ethernet ports)

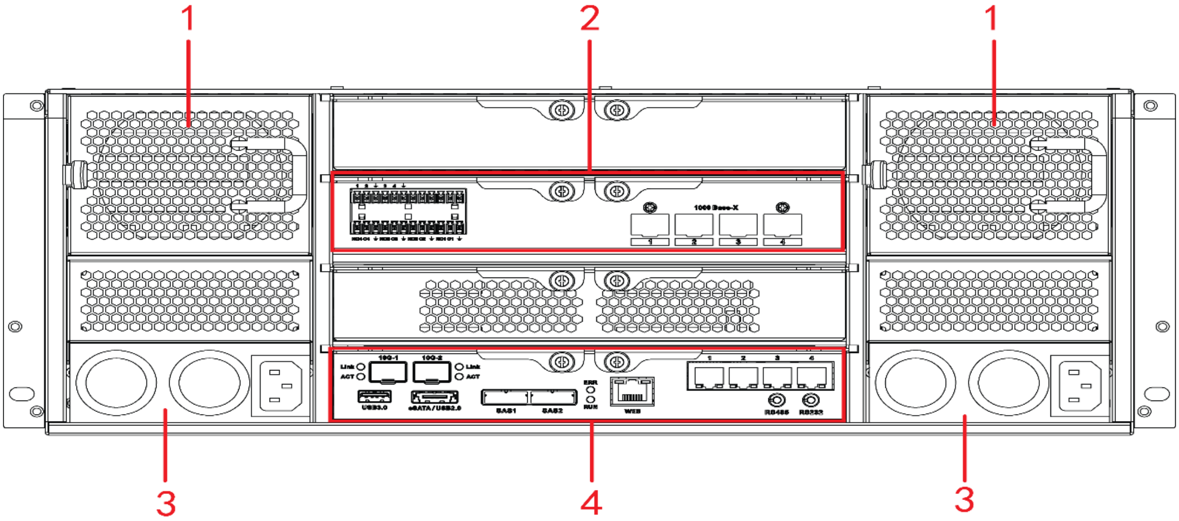


Figure 1-16 Rear panel (9 Ethernet ports)

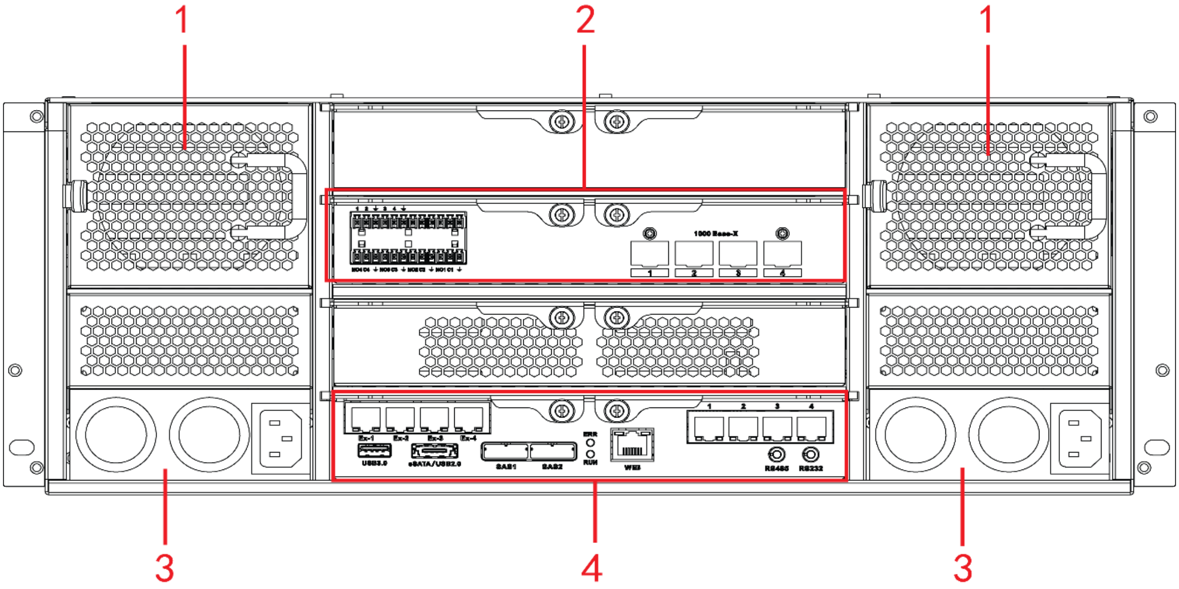


Table 1-13 Rear panel description

No.	Name	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 input	Connects AC power.
4	Main control module	See Table 1-14.

Table 1-14 Main control module ports

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 port for eSATA and USB2.0.
SAS1, SAS2	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.
RUN	RUN light flickers when the device is powered on and running.
RS-232	RS-232 port.
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)

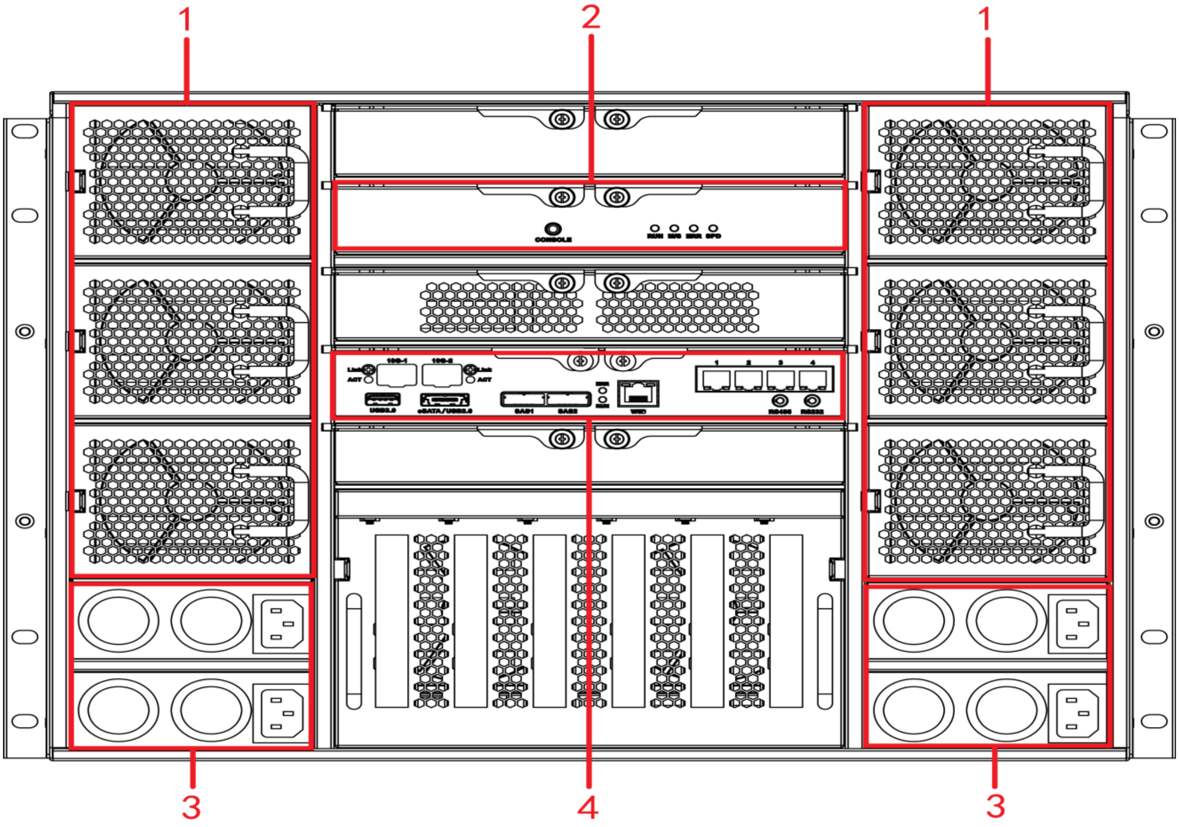


Figure 1-18 Rear panel (7 Ethernet ports)

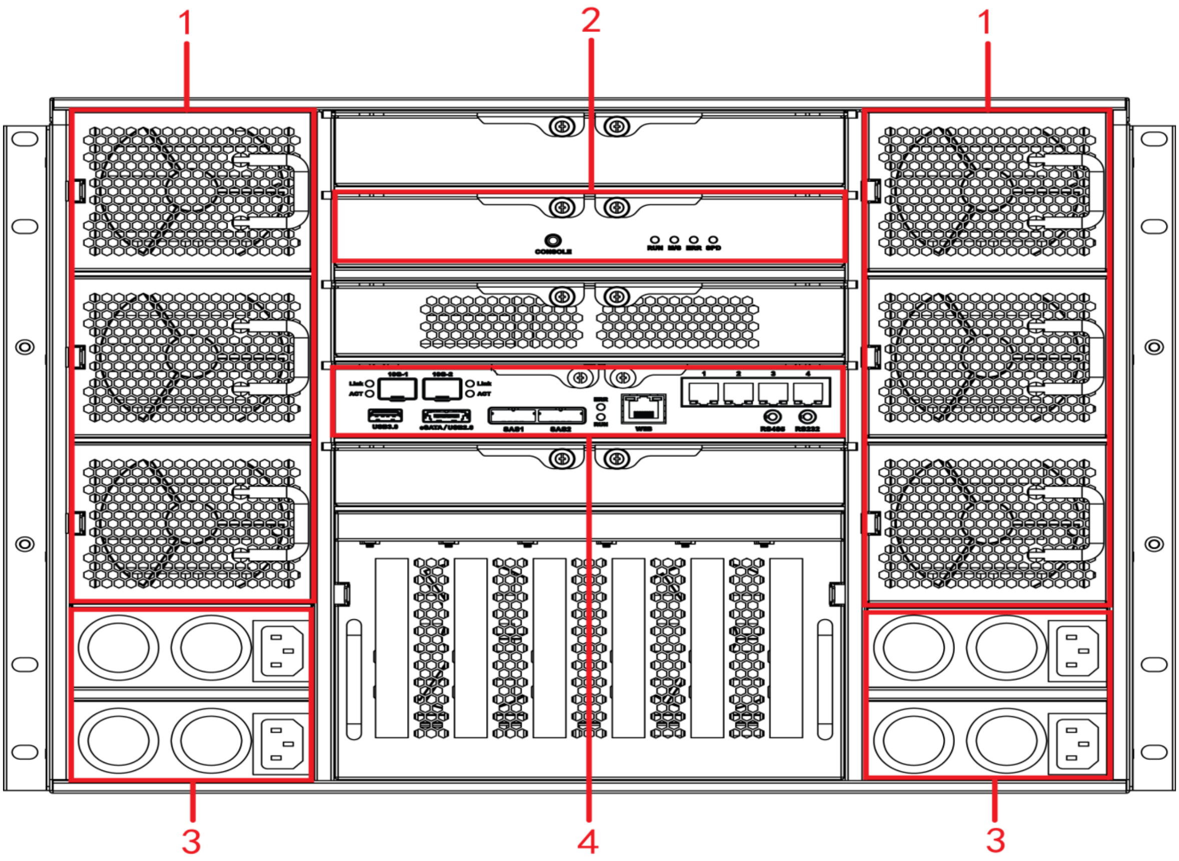


Figure 1-19 Rear panel (9 Ethernet ports)

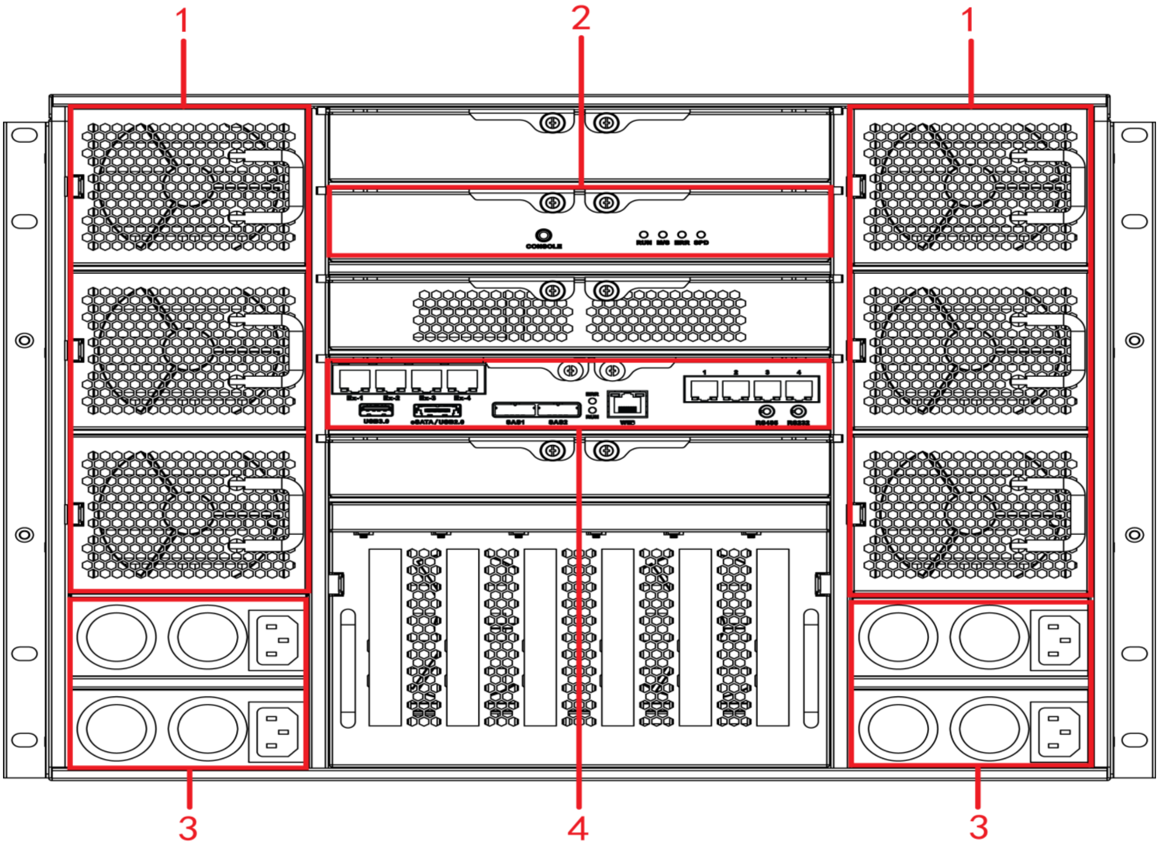


Table 1-15 Rear panel description

No.	Interface	Description
1	Fan	Used for case cooling.

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

Table 1-16 Main control module ports

Port/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 port for eSATA and USB2.0.
SAS1, SAS2	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.
RUN	RUN light flickers when the device is powered on and running.
RS-485	RS-485 port..
RS-232	RS-232 port.
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 description

Port/Indicator	Description
CONSOLE	Serial port. It is mainly used for debugging the device and logging in to the command line interface.
RUN	RUN light flickers when the device is powered 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 6 G, and the light goes out if the speed reaches 6 G.

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.
Refresh	Click this icon to get the latest configuration information.

Icon/Button	Description
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.

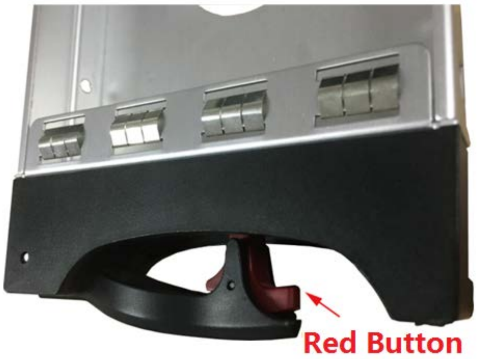
WARNING

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

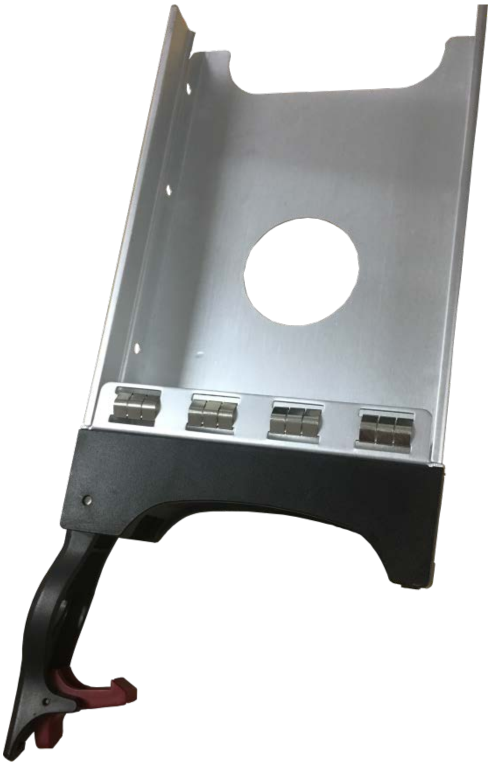
Step 1 Press the red button on the HDD box in the front panel and unlock the handle.

Figure 2-1 Opening the handle



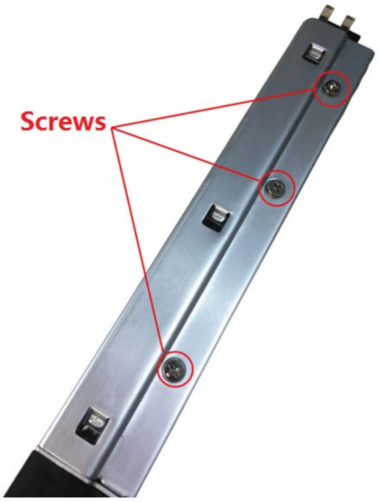
Step 2 Pull out to take the empty HDD box.

Figure 2-2 HDD box



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

Figure 2-3 Fastening the screws



⚠

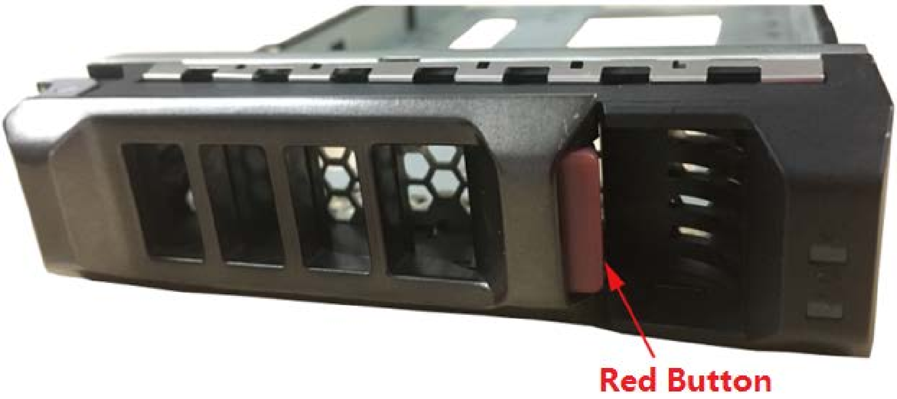
To avoid any damage to the slot, do not close the handle if the HDD box has not been pushed to the bottom.

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

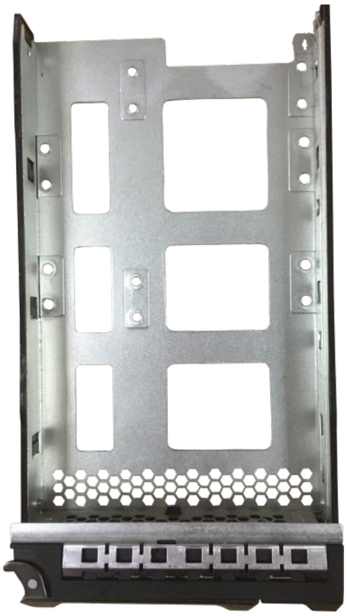
Step 1 Press the red button on the HDD box in the front panel and unlock the handle.

Figure 2-4 Opening the handle



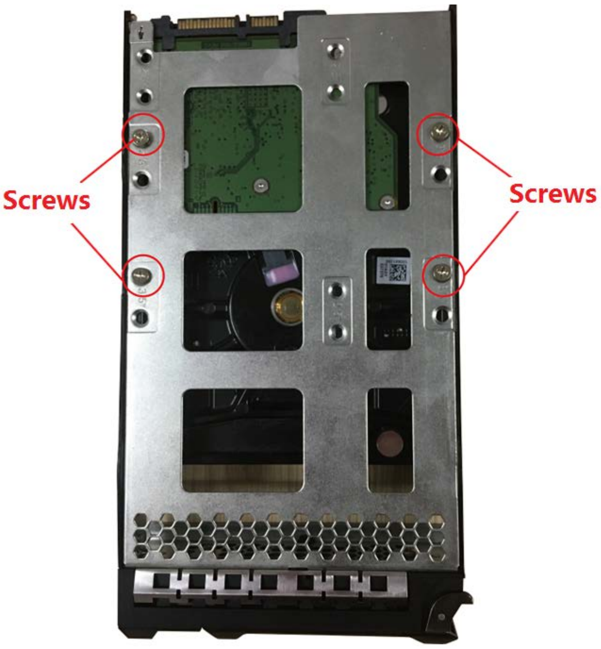
Step 2 Pull out to take the empty HDD box.

Figure 2-5 HDD box



Step 3 Put the HDD into the disk box and fasten the screws at the bottom of the box.

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 Powering Up

2.2.1 Preparation

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

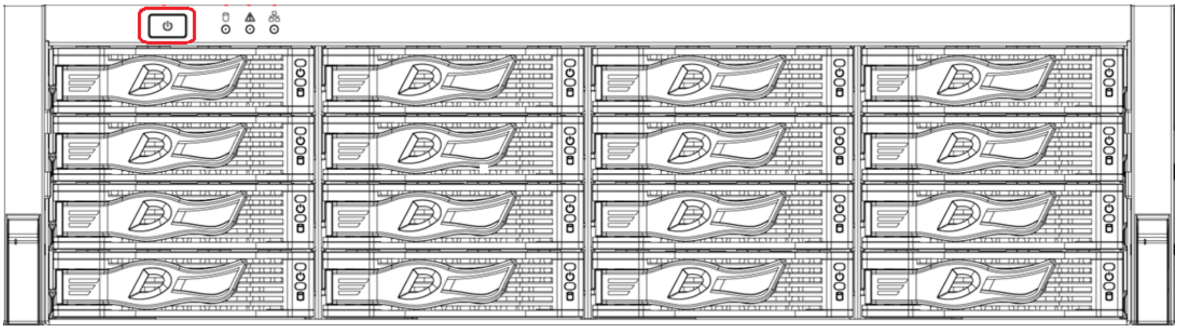
- Make sure that GND is connected correctly.
- Different models of devices need different sources of power supplies. Make sure that all power lines are connected correctly.
- Check whether the supplied power voltage complies with the device requirement.
- Check whether the network cables and SAS cables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

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).

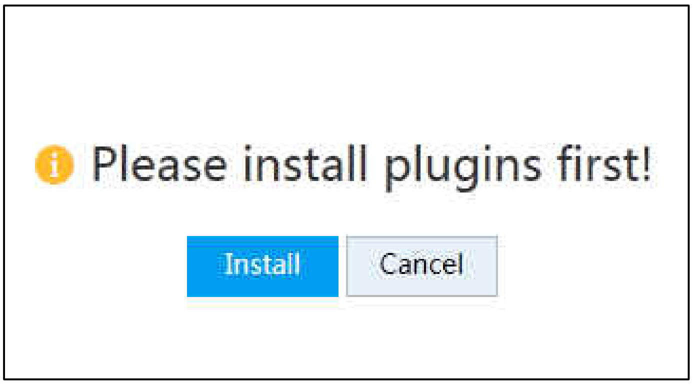
Step 1 Open the browser and enter the IP address in the address bar.

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 the Enter key.

The system prompts you to install plugins.

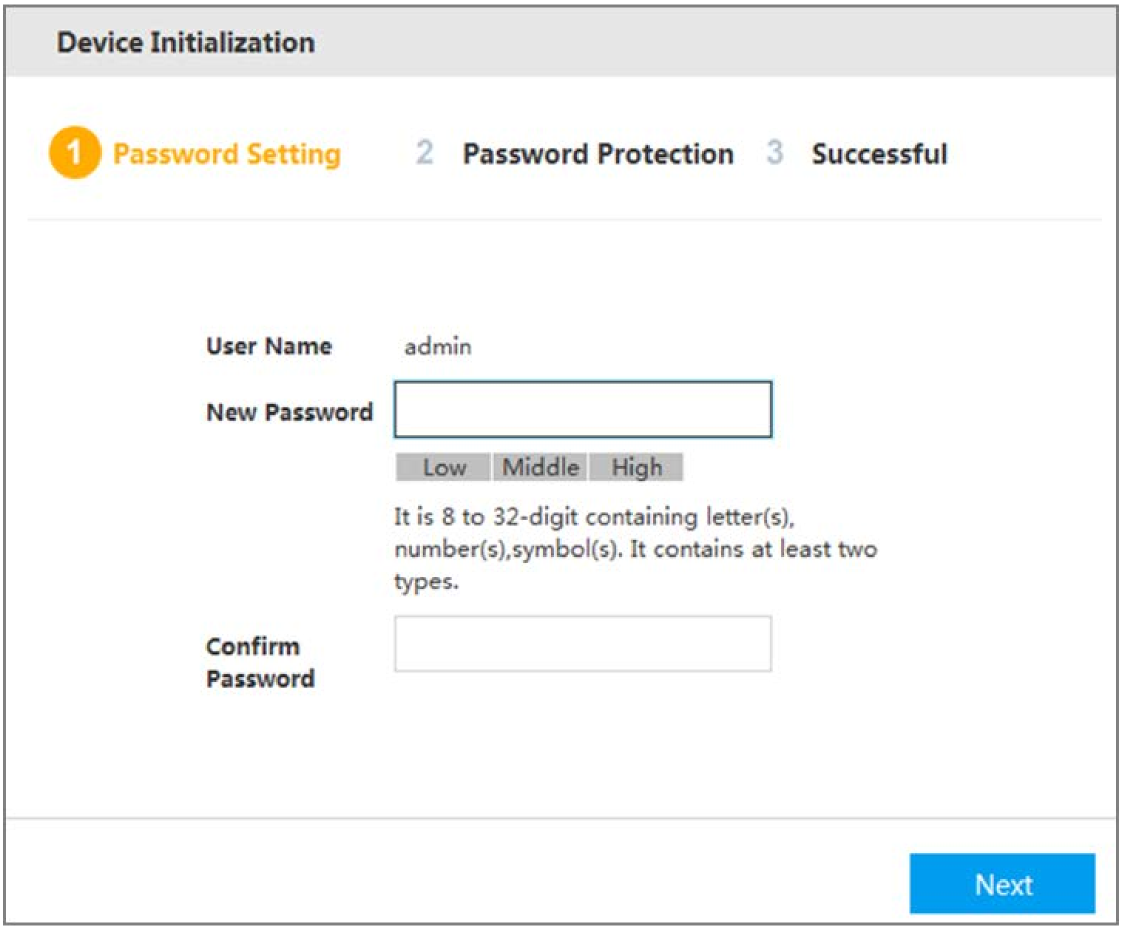
Figure 3-1 Install plugins


Please install plugins first!

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

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

Figure 3-2 Password setting


Device Initialization

User Name admin

New Password

It is 8 to 32-digit containing letter(s), number(s),symbol(s). It contains at least two types.

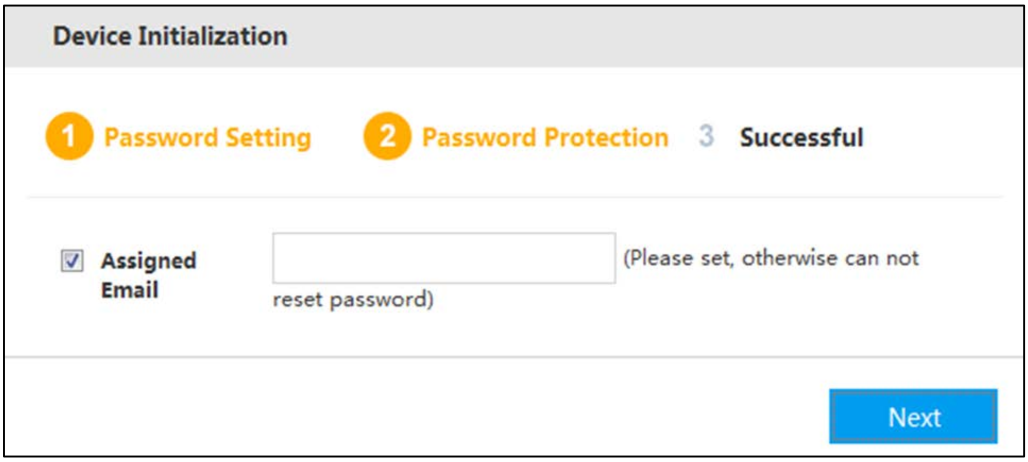
Confirm Password

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**.

Figure 3-3 Password protection



Device Initialization

1 Password Setting 2 Password Protection 3 Successful

☑ Assigned Email (Please set, otherwise can not reset password)

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

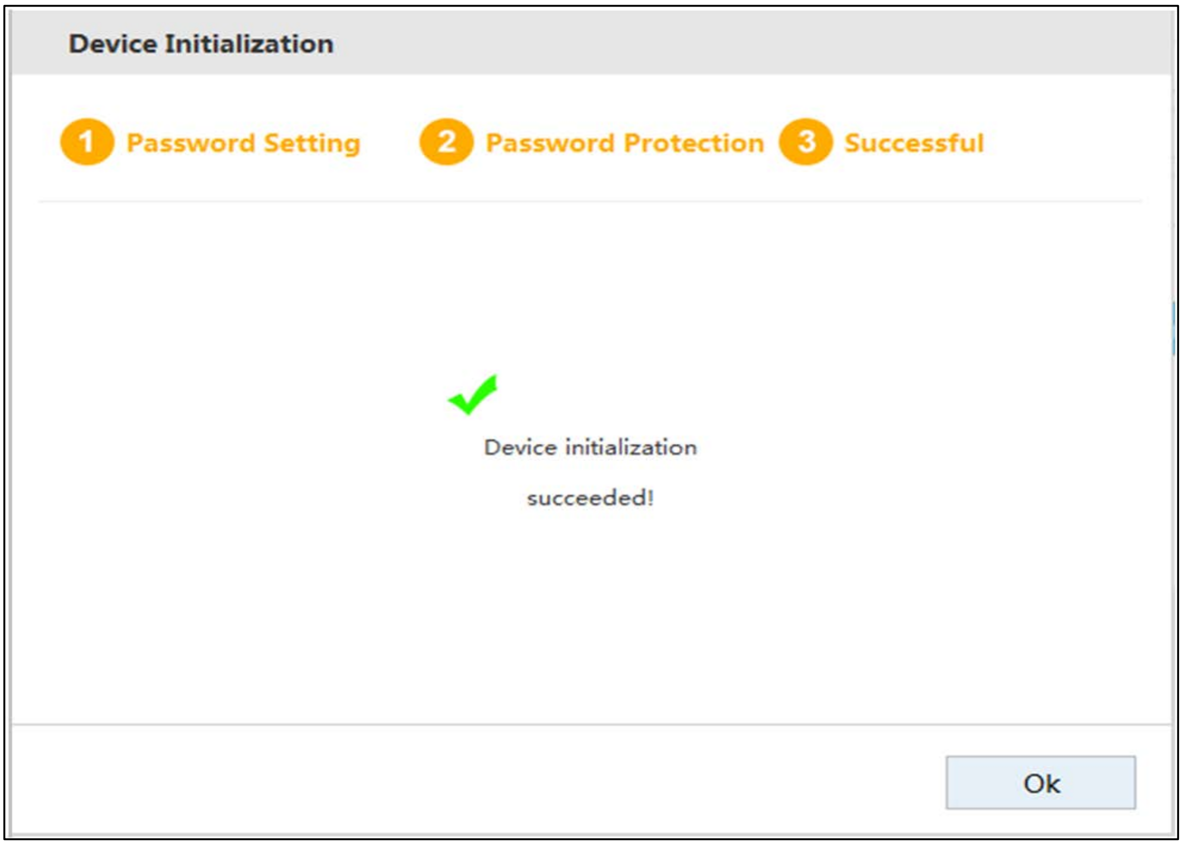
After entering the assigned email, you can reset the admin password through the email. For details, see "3.12.1.3 Resetting Password".

📖

- If you do not need to set the password protection, you can clear the **Assigned Email** checkbox.
- 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**.

Figure 3-4 Device initialization succeeded



Device Initialization

1 Password Setting 2 Password Protection 3 Successful

Device initialization succeeded!

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

3.3 Logging in to 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.

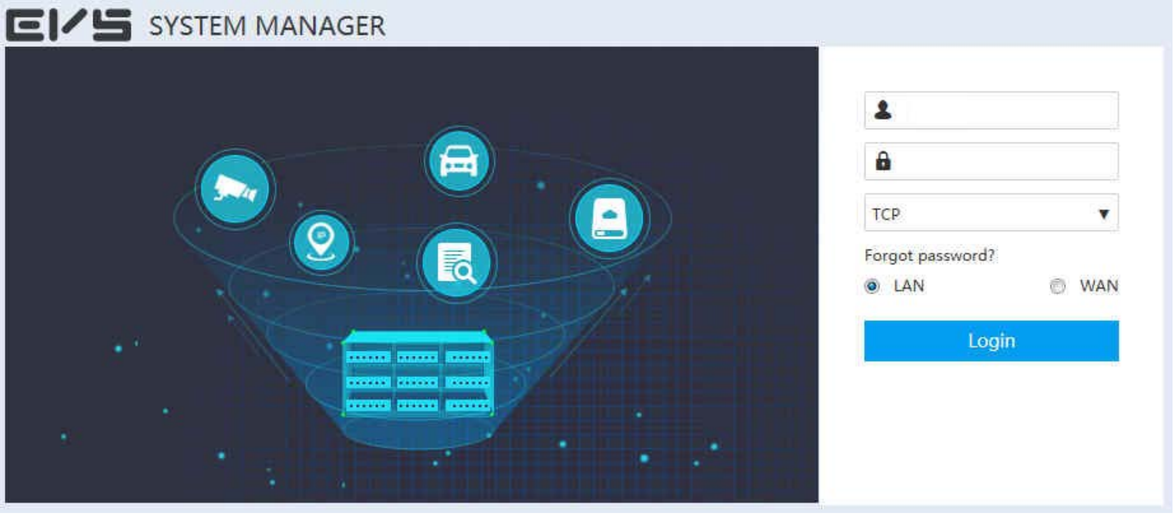
The **Control Installation** page is displayed.

Step 2 Click **Install**.

The system downloads the control automatically. Click **Run** to install the control. The **Web login** page is displayed after successful installation.

- 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

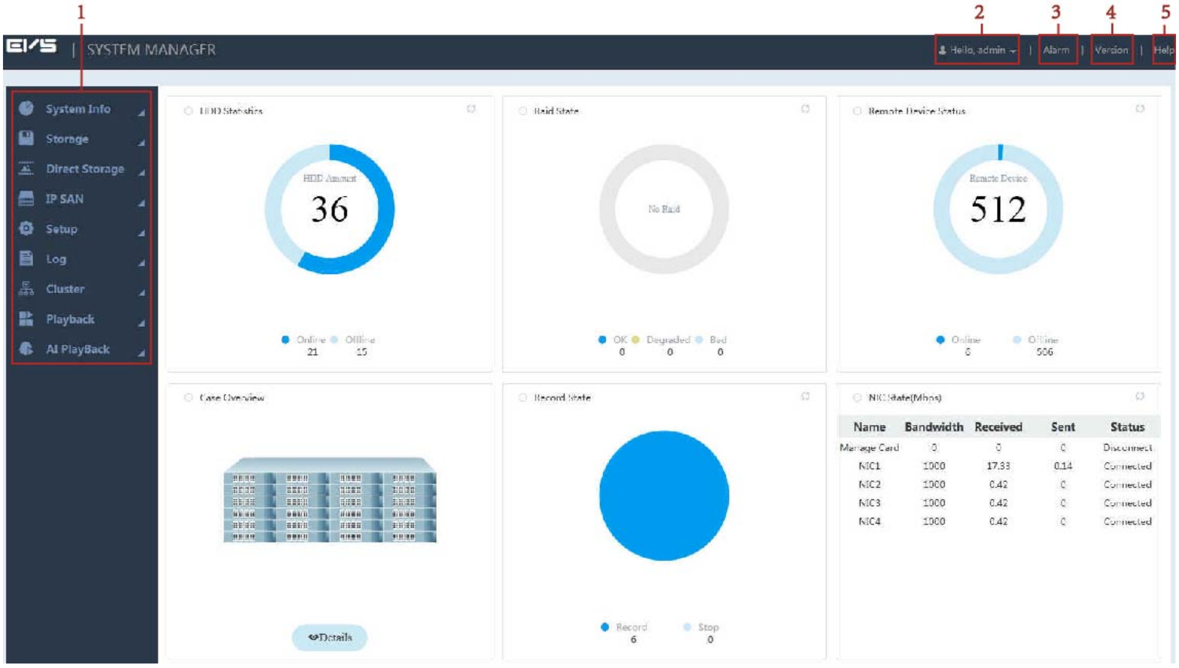


Step 3 Enter the username and password, and then select the network connection type.

- The default username 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**.

Figure 3-6 System manager



NIC State(Mbps)

Name	Bandwidth	Received	Sent	Status
Manage Card	0	0	0	Disconnect
NIC1	1000	17.33	0.14	Connected
NIC2	1000	0.42	0	Connected
NIC3	1000	0.42	0	Connected
NIC4	1000	0.42	0	Connected

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	Username	Displays the current login username. Click ▼ at the right side of the username 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.

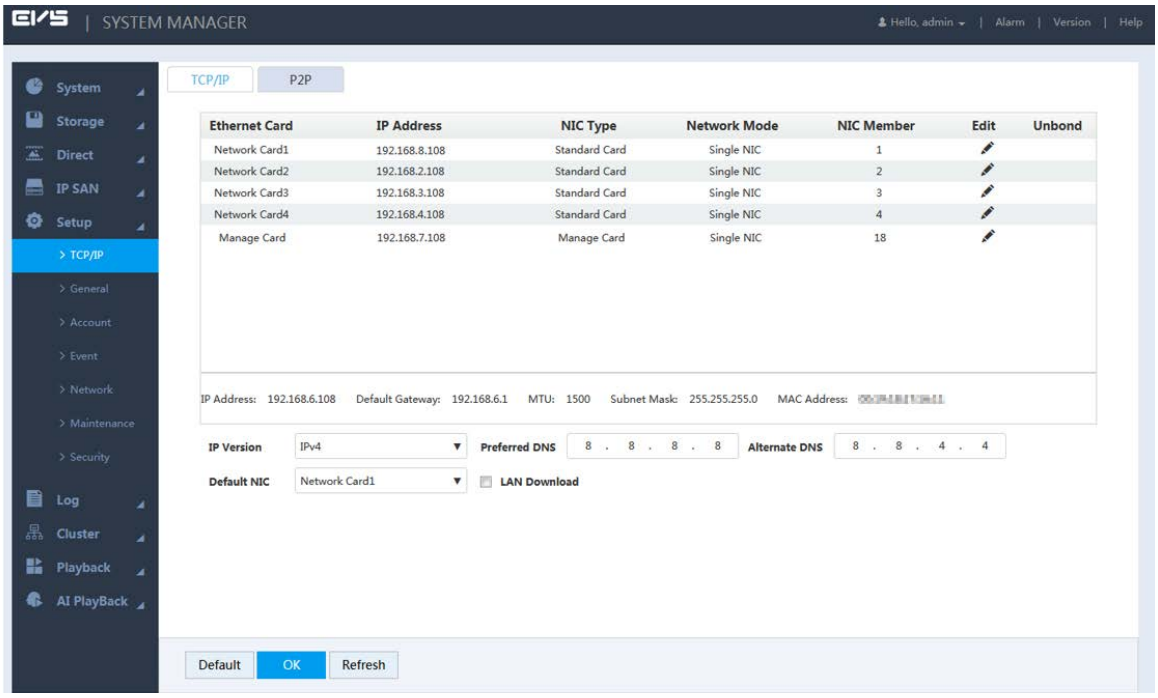
3.4 Initial Configuration

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**.

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



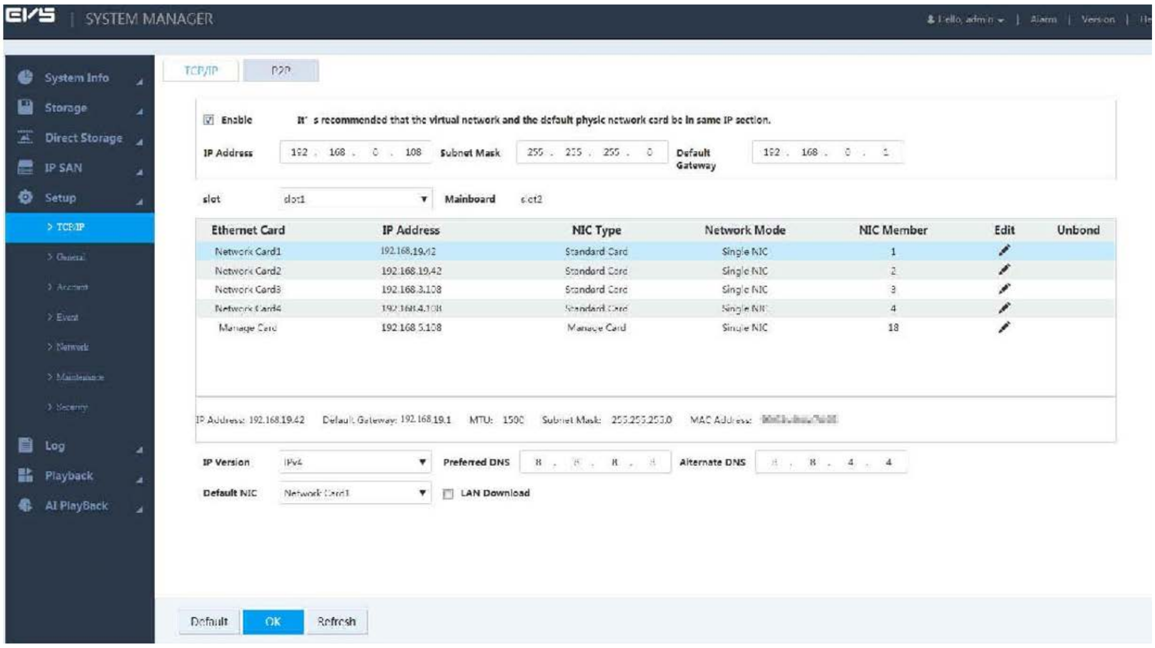
Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.8.108	Standard Card	Single NIC	1	✎	
Network Card2	192.168.2.108	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎	
Manage Card	192.168.7.108	Manage Card	Single NIC	18	✎	

IP Address: 192.168.6.108 Default Gateway: 192.168.6.1 MTU: 1500 Subnet Mask: 255.255.255.0 MAC Address: [redacted]

IP Version: IPv4 Preferred DNS: 8 . 8 . 8 . 8 Alternate DNS: 8 . 8 . 4 . 4

Default NIC: Network Card1 □ LAN Download

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



☑ Enable It' s recommended that the virtual network and the default physic network card be in same IP section.

IP Address: 192 . 168 . 0 . 108 Subnet Mask: 255 . 255 . 255 . 0 Default Gateway: 192 . 168 . 0 . 1

slot: slot1 Mainboard: slot2

Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.19.42	Standard Card	Single NIC	1	✎	
Network Card2	192.168.19.42	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎	
Manage Card	192.168.5.108	Manage Card	Single NIC	18	✎	

IP Address: 192.168.19.42 Default Gateway: 192.168.19.1 MTU: 1500 Subnet Mask: 255.255.255.0 MAC Address: [redacted]

IP Version: IPv4 Preferred DNS: 8 . 8 . 8 . 8 Alternate DNS: 8 . 8 . 4 . 4

Default NIC: Network Card1 □ LAN Download

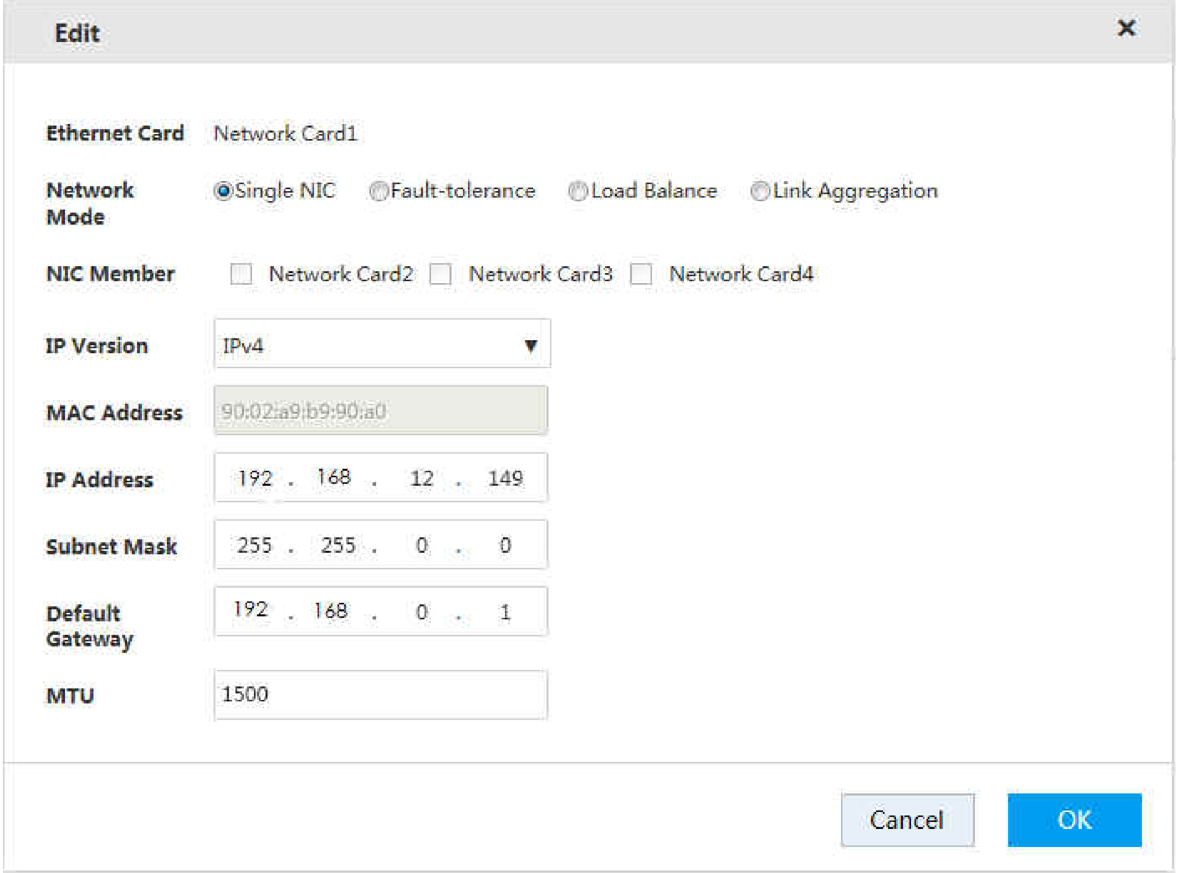
Table 3-2 TCP/IP setting parameters

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 checkbox. If network bandwidth allows, the LAN download speed is 1.5–2 times of the normal download speed.

Step 2 Click ✎.

Figure 3-9 Editing



Ethernet Card	Network Card1
Network Mode	● Single NIC ○ Fault-tolerance ○ Load Balance ○ Link Aggregation
NIC Member	□ Network Card2 □ Network Card3 □ Network Card4
IP Version	IPv4 ▼
MAC Address	90:02:a9:b9:90:a0
IP Address	192 . 168 . 12 . 149
Subnet Mask	255 . 255 . 0 . 0
Default Gateway	192 . 168 . 0 . 1
MTU	1500

Step 3 Configure the parameters.

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 main card. Usually there is only one running card (main card). The system will enable the alternate card when the main 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

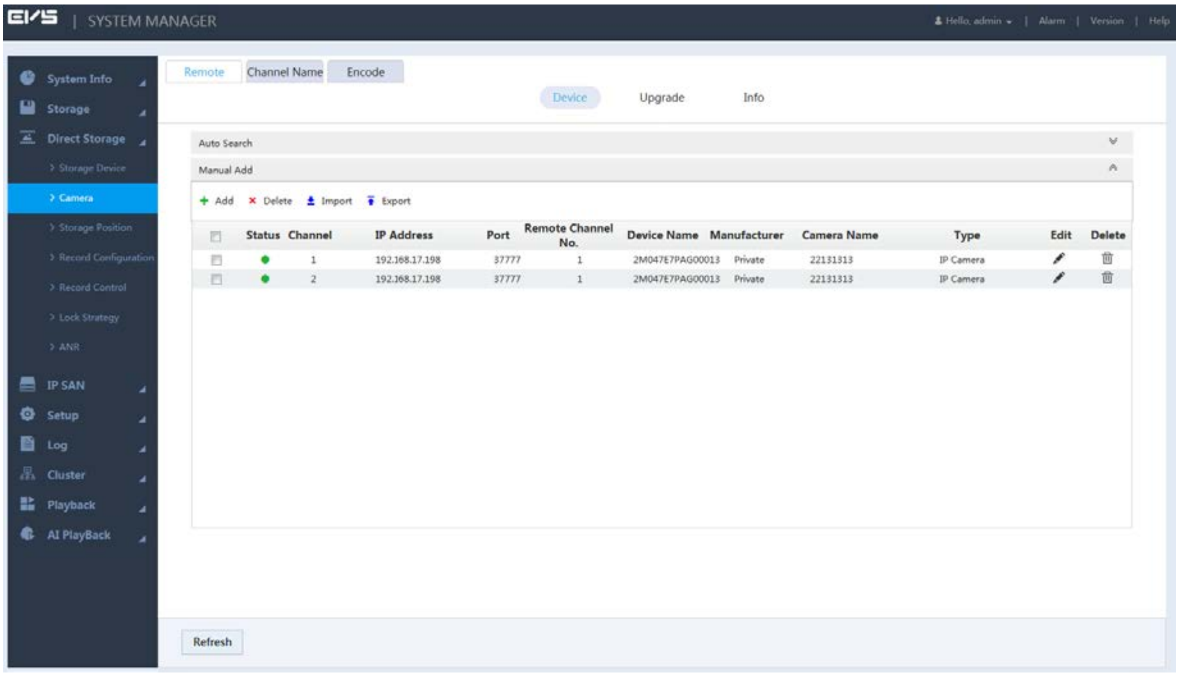
After adding the remote device, the Device can receive, store, and manage the video stream transmitted by the remote device. You can browse, playback, manage, and store several remote devices.

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, username 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 username 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**.

Figure 3-10 Remote device



	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑
□	●	2	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑

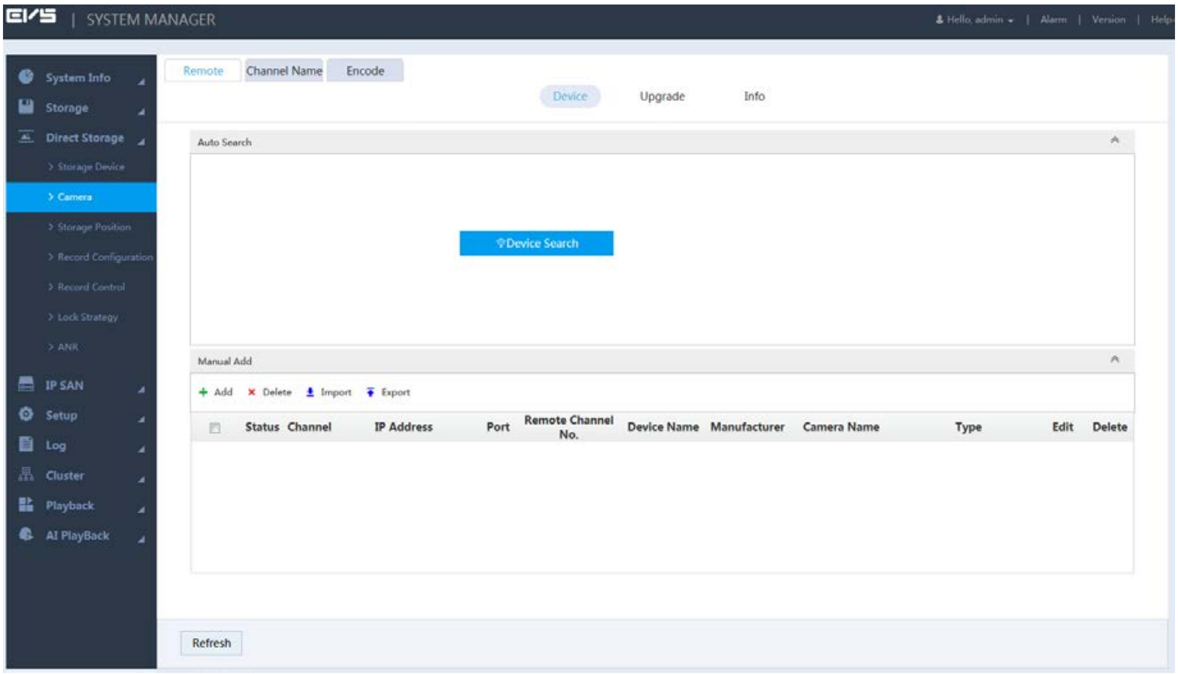
Step 2 Add remote device.

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**.

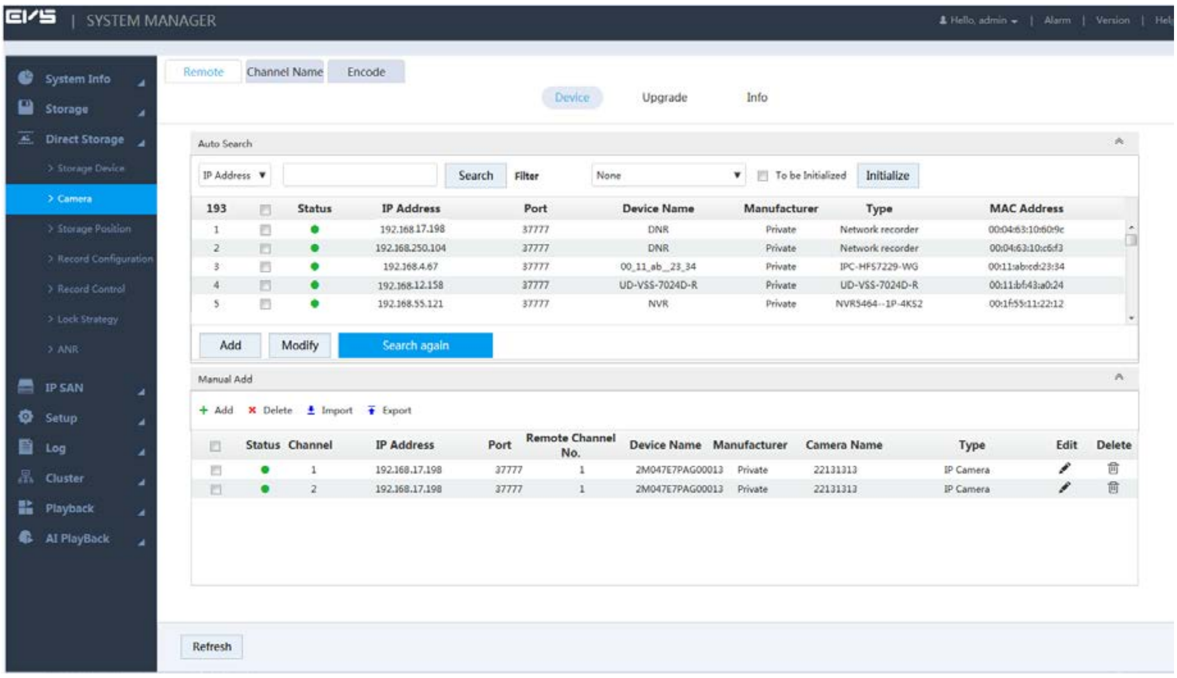
Figure 3-11 Automatic search



2) Click **Device Search**.

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



193	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.17.198	37777	DNR	Private	Network recorder	00:04:63:10:60:9c
2	□	●	192.168.250.104	37777	DNR	Private	Network recorder	00:04:63:10:c6:f3
3	□	●	192.168.4.67	37777	00_11_ab__23_34	Private	IPC-HFS7229-WG	00:11:ab:cd:23:34
4	□	●	192.168.12.158	37777	UD-VSS-7024D-R	Private	UD-VSS-7024D-R	00:11:bf:43:a0:24
5	□	●	192.168.55.121	37777	NVR	Private	NVR5464--1P-4KS2	00:1f:55:11:22:12

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑
□	●	2	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑

Table 3-4 Auto search icons

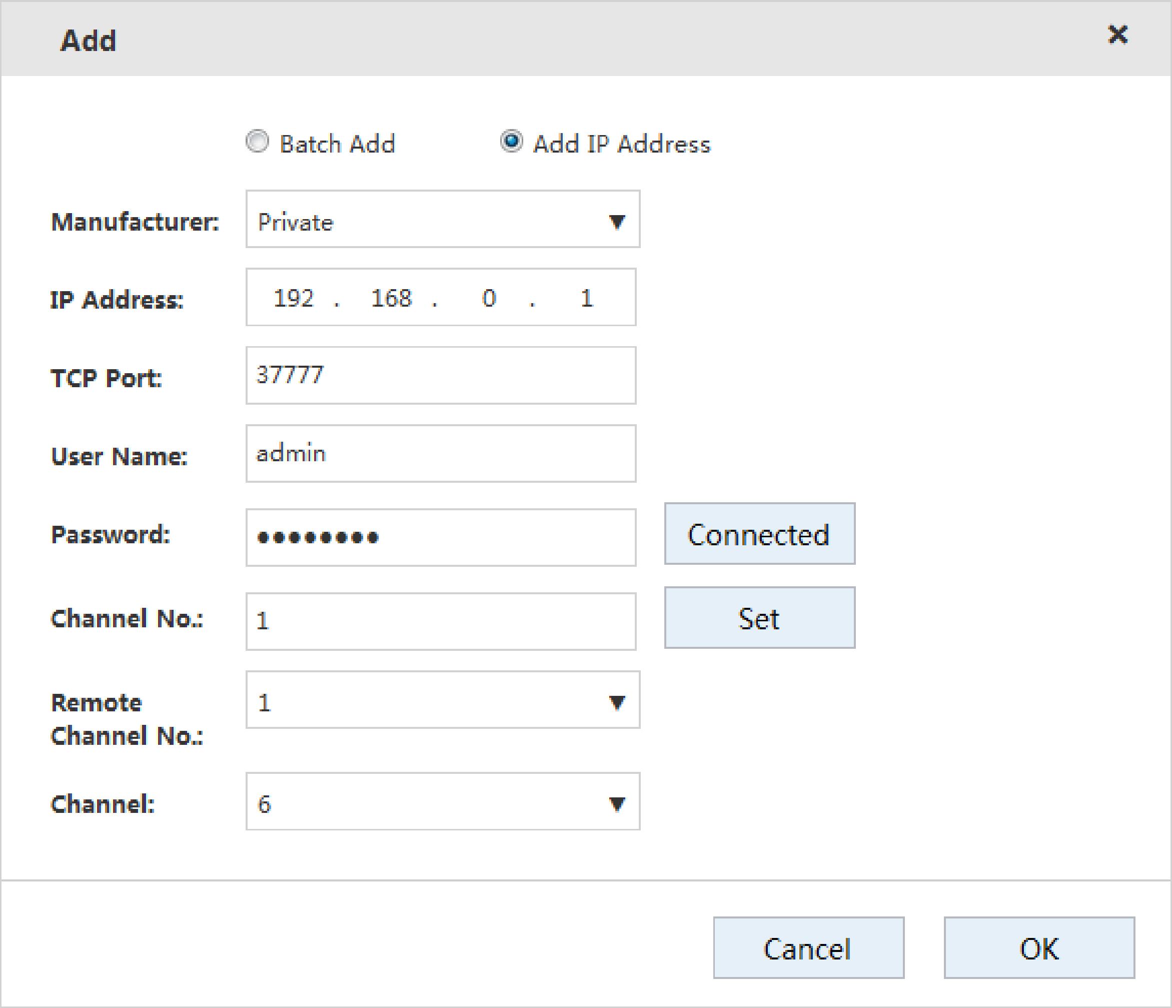
Icon/Parameter	Description
IP Address ▼	Select the remote devices you need to add through IP address or MAC address. 1. Click IP Address ▼ to select IP Address or MAC Address. 2. Enter the IP address or MAC address of the remote device in the text box at the right side of IP Address ▼. 3. Click **Search**.
Initialization	Select the **To Be Initialized** checkbox 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 checkbox 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 checkbox 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**.

Figure 3-13 Adding one device



Add

○ Batch Add ● Add IP Address

Manufacturer: Private

IP Address: 192 . 168 . 0 . 1

TCP Port: 37777

User Name: admin

Password: ••••••••

Channel No.: 1

Remote Channel No.: 1

Channel: 6

2) Configure the parameters.

Table 3-5 Parameters of 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**.
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**.

Parameter	Description
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.
Username/Password	Enter the username 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.
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.

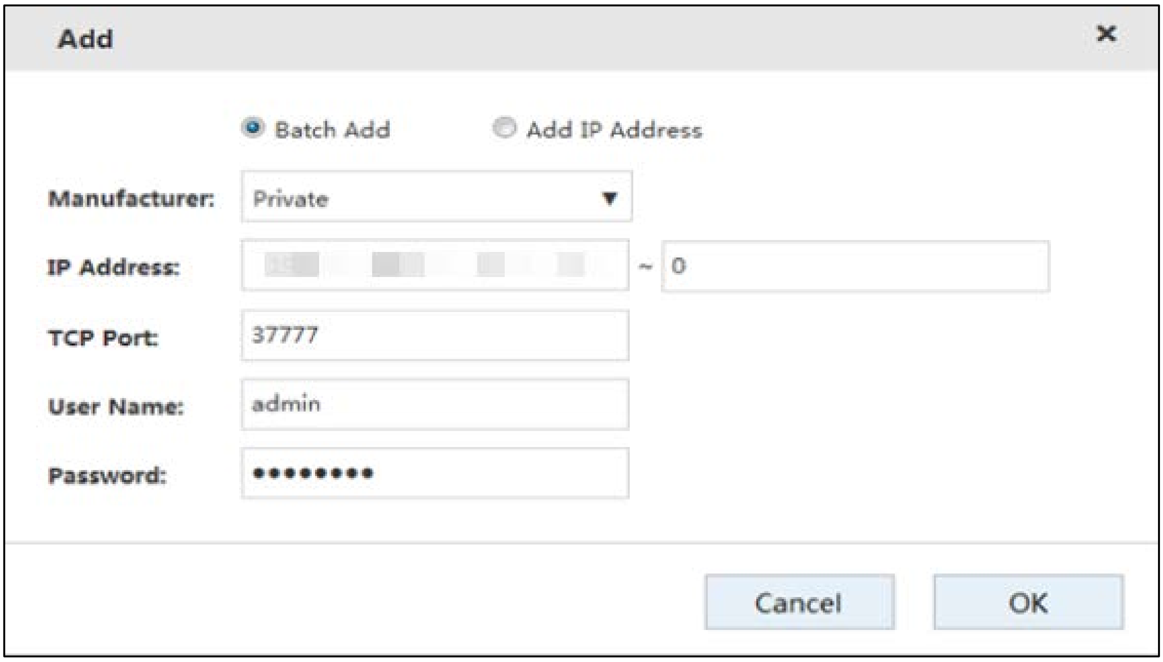
3) Click **OK** to complete adding.

- 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**.

Figure 3-14 Batch add



Add ×

● Batch Add ○ Add IP Address

Manufacturer: Private ▼

IP Address: [redacted] ~ 0

TCP Port: 37777

User Name: admin

Password: •••••••••

Cancel OK

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.

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.

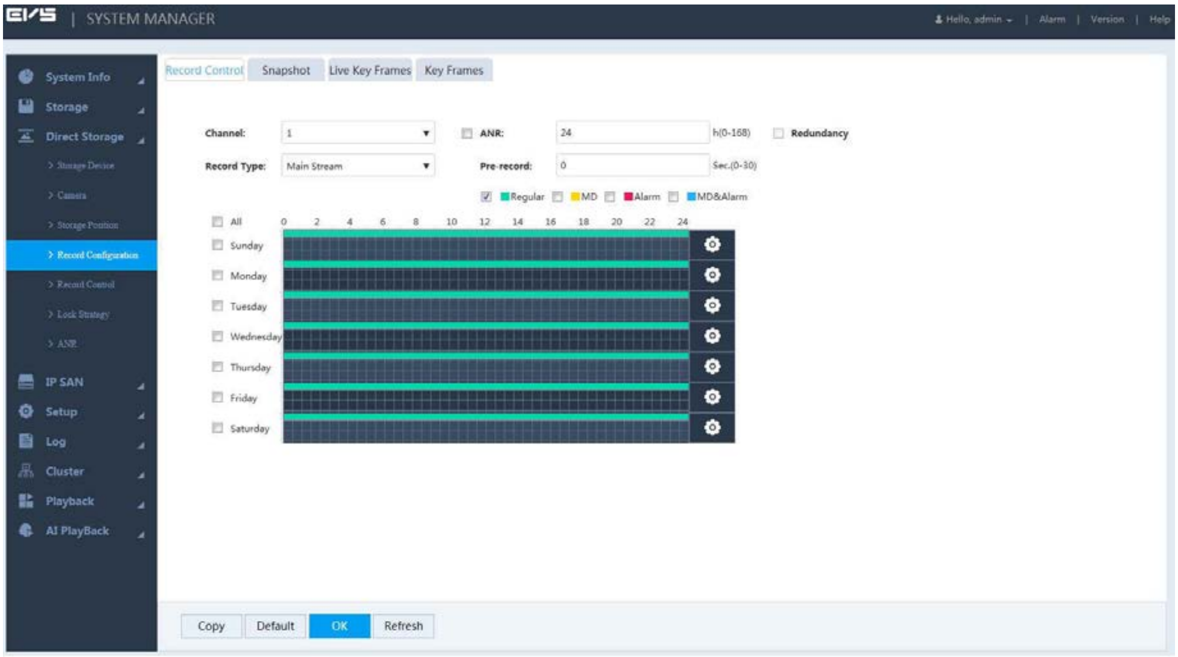
3.4.3.1 Configuring Record Plan

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**.

Figure 3-15 Record plan



Channel: 1

□ ANR: 24 h(0-168)

□ Redundancy

Record Type: Main Stream

Pre-record: 0 Sec.(0-30)

☑ 🟩Regular □ 🟨MD □ 🟥Alarm □ 🟦MD&Alarm

□ All

□ Sunday

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

Step 2 Configure the parameters.

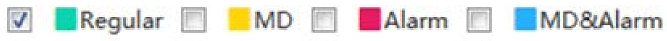
Table 3-6 Record parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** checkbox if you want to perform the same settings for all the channels.
ANR (Automatic Network Replenishment)	Select the checkbox 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 checkbox 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.

Figure 3-16 Alarm type



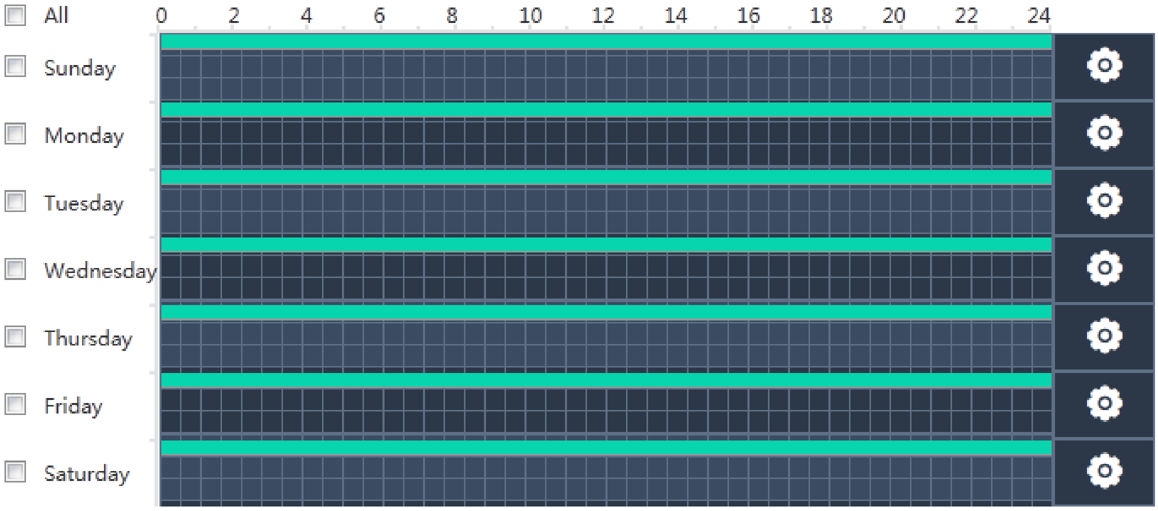
☑ 🟩Regular □ 🟨MD □ 🟥Alarm □ 🟦MD&Alarm

- 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** checkbox and you can synchronously edit or draw the periods for all the weekdays.
- ◇ You can select multiple weekdays to edit at the same time.

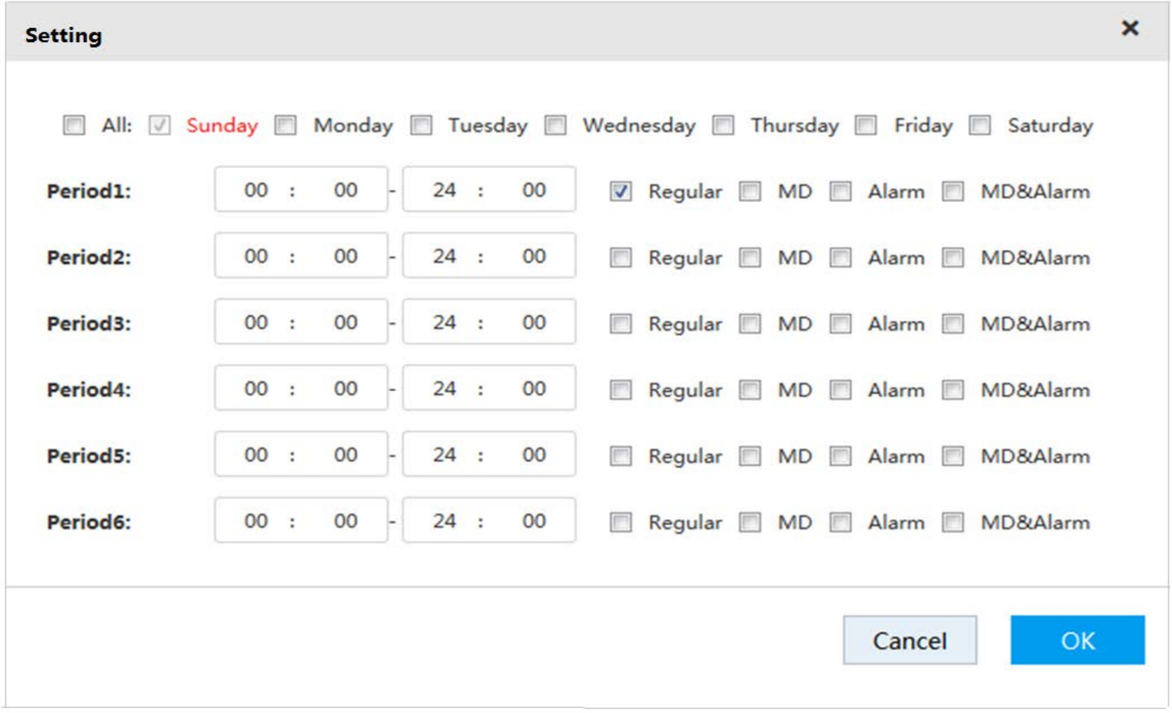
2) Hold the left button of the mouse and move the mouse in the period bar to draw the period.

- ◇ 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 ⚙.

Figure 3-18 Period setting



Setting ×

□ All: ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Period1:	00 : 00	-	24 : 00	☑ Regular	□ MD	□ Alarm	□ MD&Alarm
Period2:	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm
Period3:	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm
Period4:	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm
Period5:	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm
Period6:	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm

2) Select the weekday, record type and period.

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

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

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

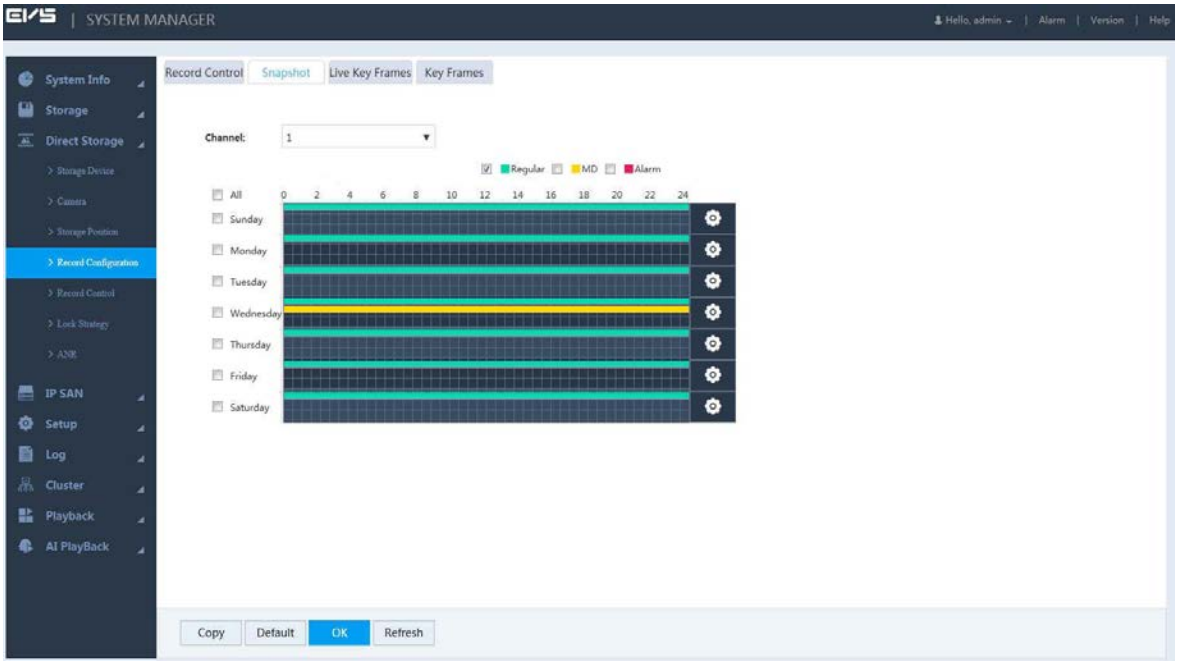
With snapshot plan, the system captures images according to the set time and type. For example, if you set the capture time of Emergency type at 6:00–18:00 of each Monday, the system will automatically capture images of Emergency and of this time period.

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

The **Snapshot** page is displayed.

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



Channel: 1

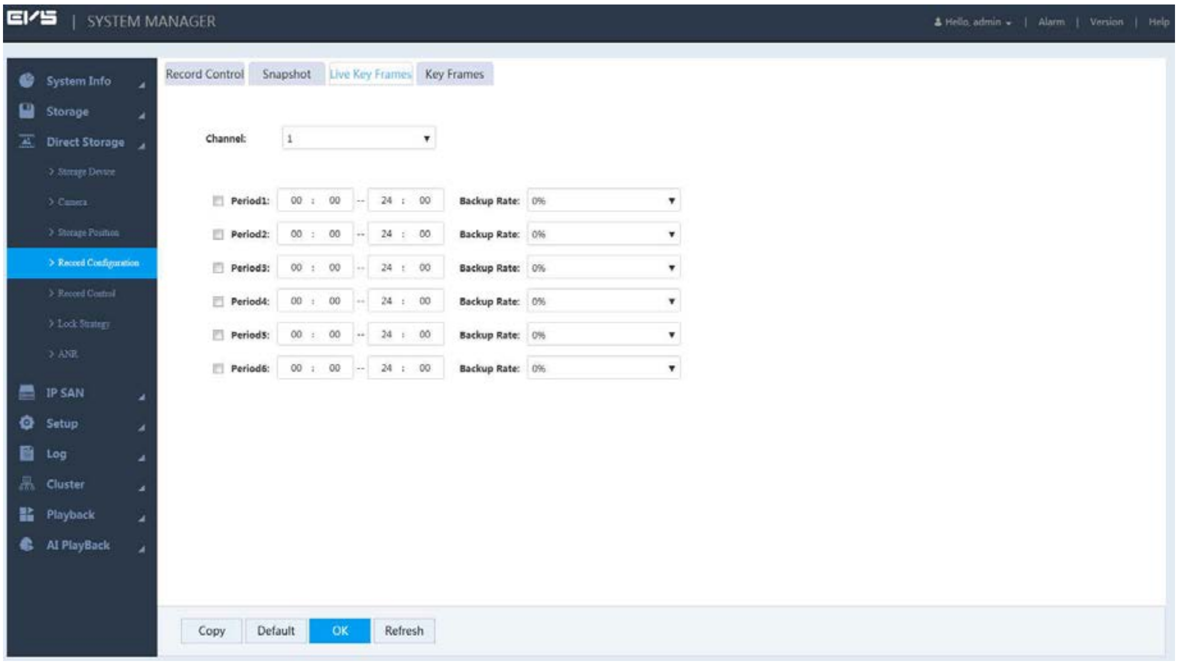
The snapshot plan works after enabling the auto snapshot function. For details of enabling auto snapshot, see "3.4.4 Enabling Record Function".

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**.

Figure 3-20 Live key frames



Channel: 1

□ Period1: 00 : 00 -- 24 : 00 Backup Rate: 0%

□ Period2: 00 : 00 -- 24 : 00 Backup Rate: 0%

□ Period3: 00 : 00 -- 24 : 00 Backup Rate: 0%

□ Period4: 00 : 00 -- 24 : 00 Backup Rate: 0%

□ Period5: 00 : 00 -- 24 : 00 Backup Rate: 0%

□ Period6: 00 : 00 -- 24 : 00 Backup Rate: 0%

Step 2 Configure the parameters.

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** checkbox 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.

⚠

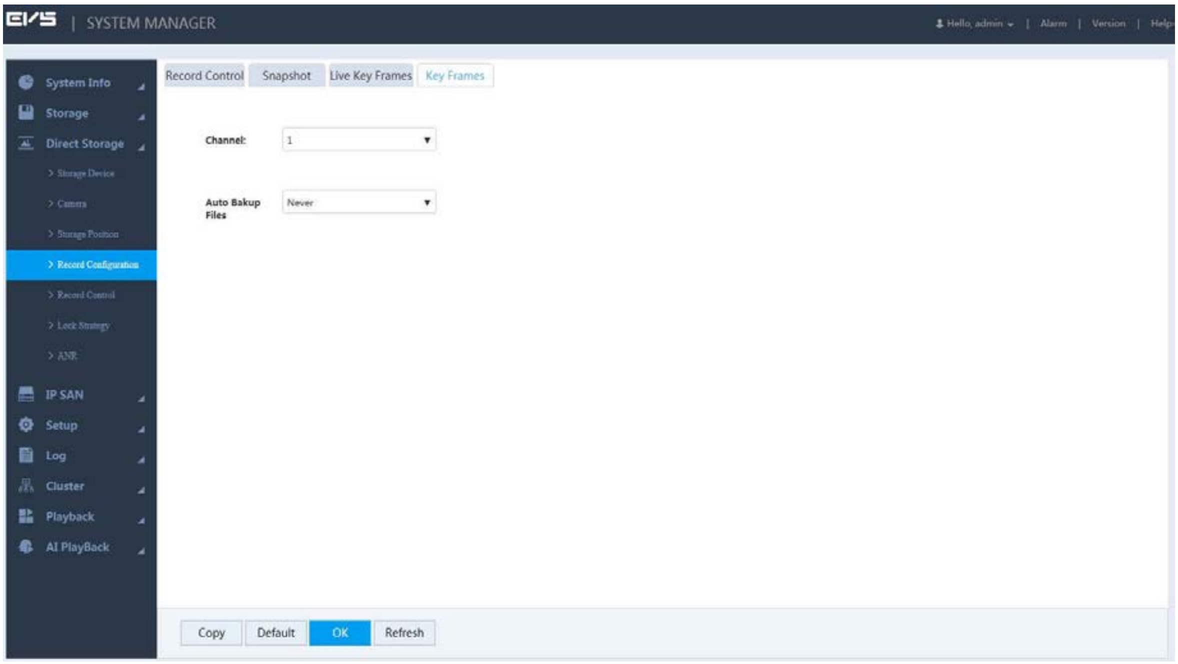
- With key frame settings, part of the record data may be discarded, leaving only the configured key frame data.
- Be cautious with setting key frames, as this operation may influence record fluency and continuity.

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**.

Figure 3-21 Key frames



Channel: 1

Auto Bakup Files: Never

Step 2 Configure the parameters.

Table 3-8 Key frame parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** checkbox 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.

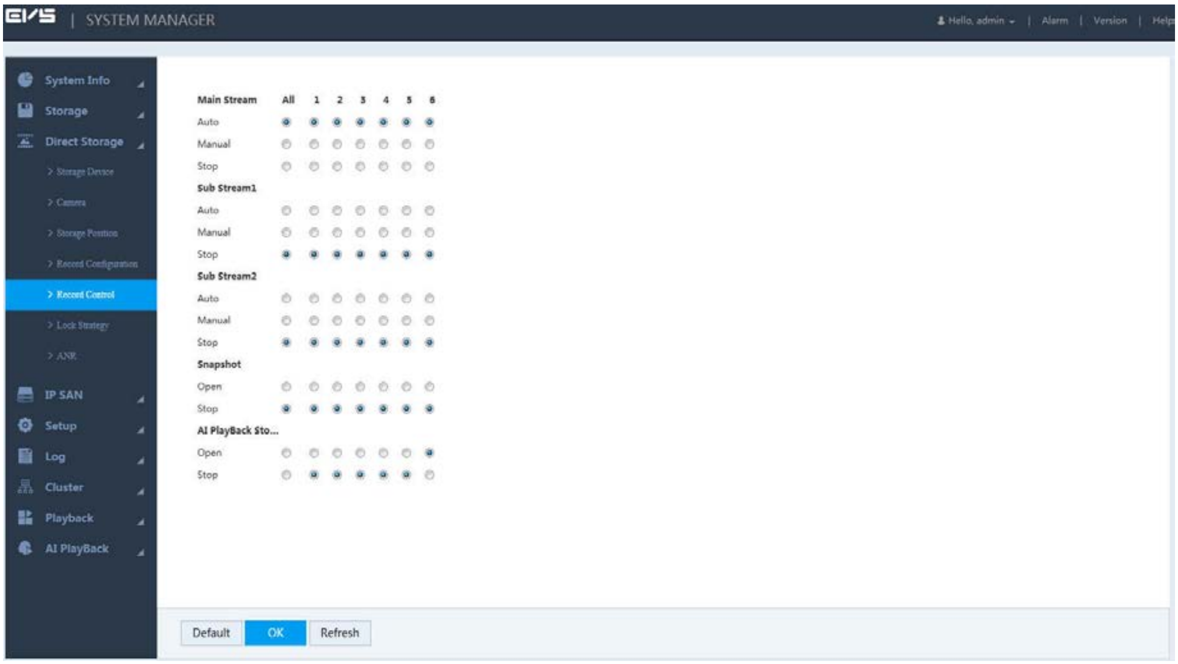
- Auto record: The system automatically takes records according to the set record type and record time.
- Manual record: The system takes 24-hour continuous records in the channel.

⚠

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

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

Figure 3-22 Record control



Main Stream	All	1	2	3	4	5	6
Auto	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○
Sub Stream1							
Auto	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●
Sub Stream2							
Auto	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●
Snapshot							
Open	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●
AI PlayBack Sto...							
Open	○	○	○	○	○	○	●
Stop	○	●	●	●	●	●	○

Step 2 Configure the parameters.

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	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.
Sub Stream	
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.

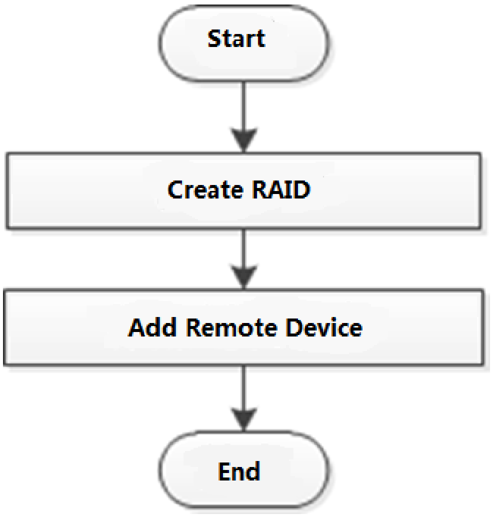
Step 3 Click **OK** to save the configuration.

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.

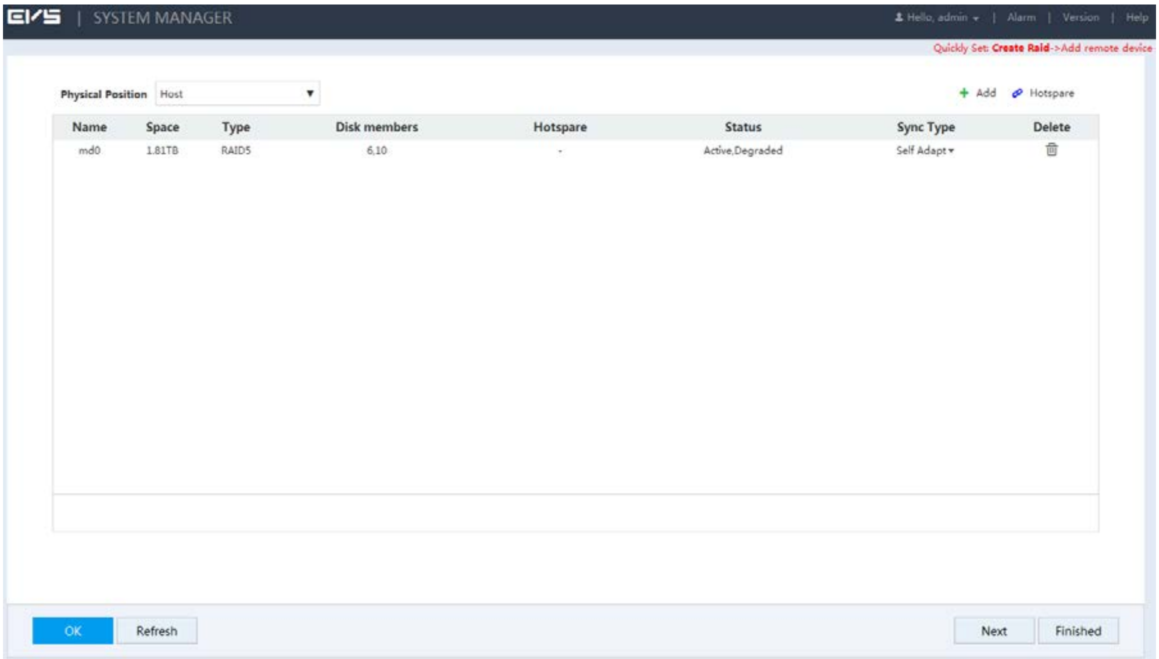
Figure 3-23 Video direct storage



Step 1 Click ▼ at the right side of the username. Select **Quickly Set** > **Video**.

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

Figure 3-24 RAID management

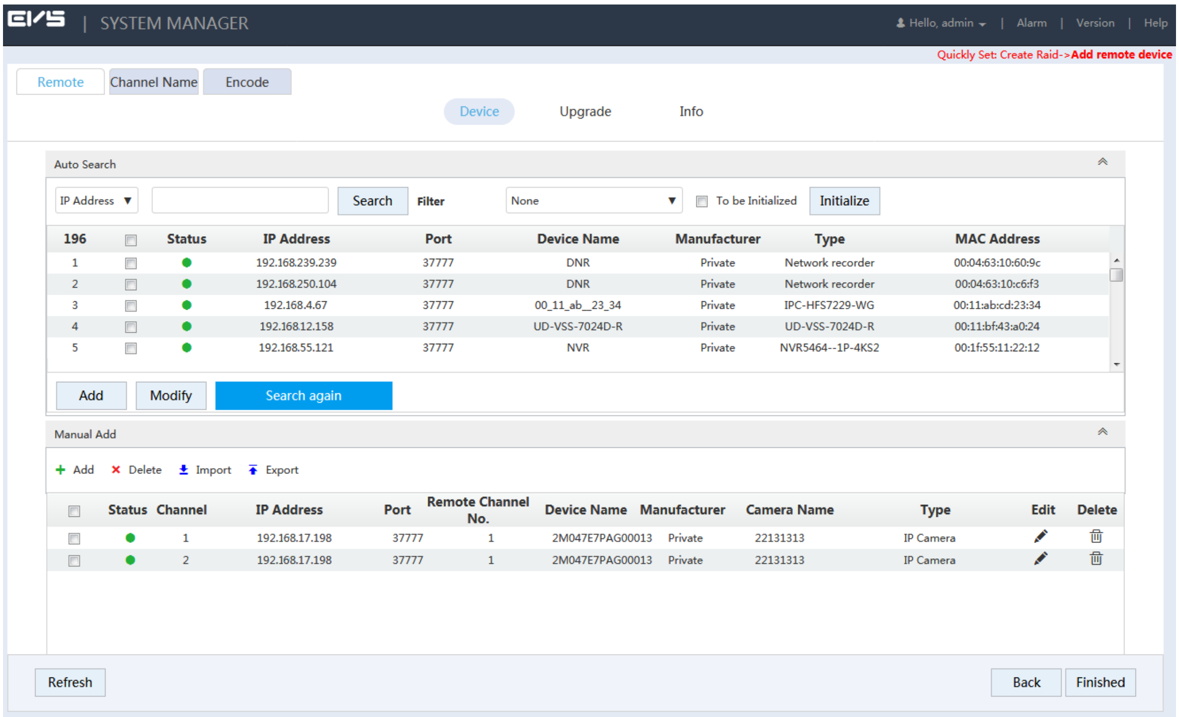


Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	1.81TB	RAID5	6,10	-	Active,Degraded	Self Adapt ▾	🗑

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

Step 3 Click **Next**.

Figure 3-25 Adding remote device



196	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.239.239	37777	DNR	Private	Network recorder	00:04:63:10:60:9c
2	□	●	192.168.250.104	37777	DNR	Private	Network recorder	00:04:63:10:c6:f3
3	□	●	192.168.4.67	37777	00_11_ab__23_34	Private	IPC-HFS7229-WG	00:11:ab:cd:23:34
4	□	●	192.168.12.158	37777	UD-VSS-7024D-R	Private	UD-VSS-7024D-R	00:11:bf:43:a0:24
5	□	●	192.168.55.121	37777	NVR	Private	NVR5464--1P-4KS2	00:1f:55:11:22:12

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑
□	●	2	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑

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

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

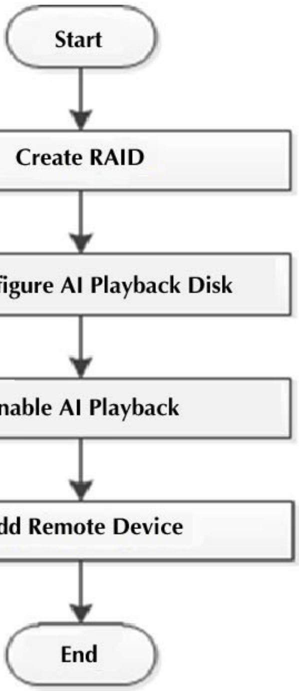
3.6 AI Playback

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

3.6.1 Configuring AI Playback

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

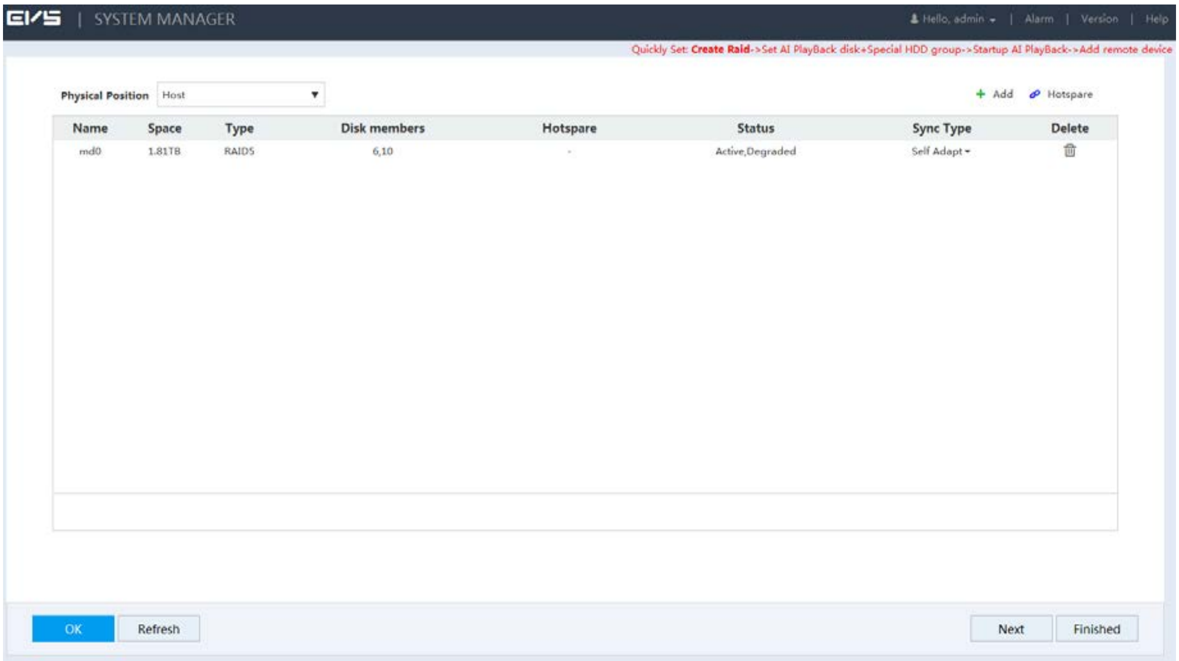
Figure 3-26 AI playback



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

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

Figure 3-27 RAID management



Quickly Set: **Create Raid**->Set AI PlayBack disk+Special HDD group->Startup AI PlayBack->Add remote device

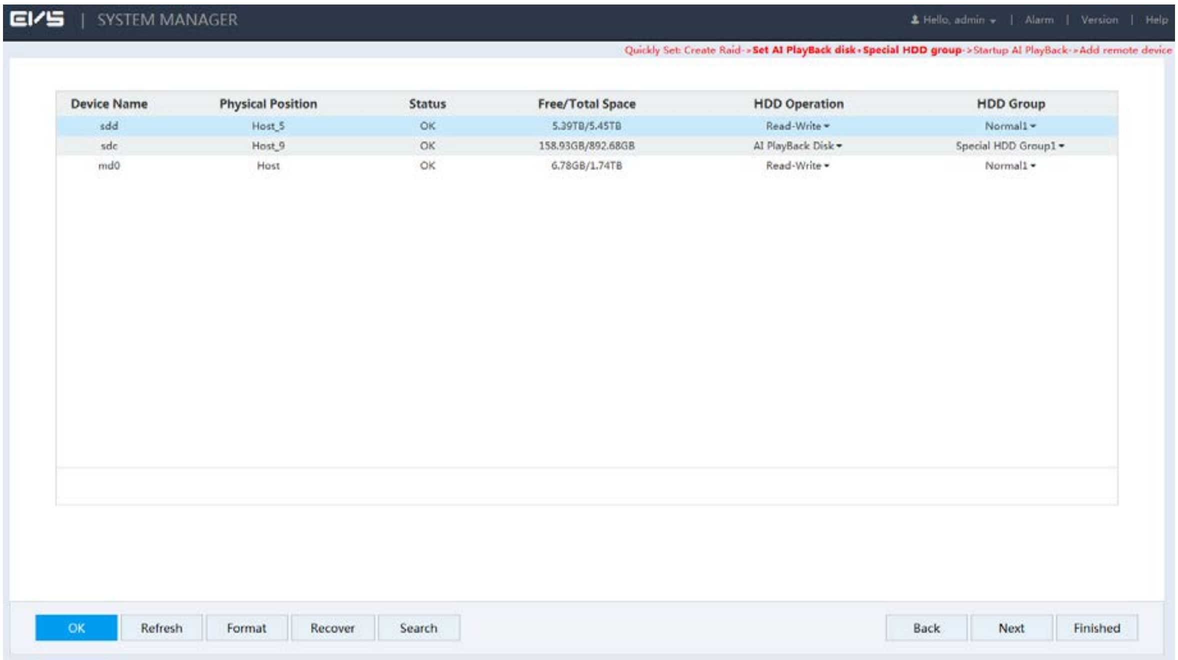
Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	1.81TB	RAID5	6,10	-	Active,Degraded	Self Adapt	🗑

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

Step 3 Click **Next**.

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


SYSTEM MANAGER
Hello, admin
Alarm
Version
Help
Quickly Set: Create Raid->Set AI PlayBack disk+Special HDD group->Startup AI PlayBack->Add remote device
OK
Refresh
Format
Recover
Search
Back
Next
Finished

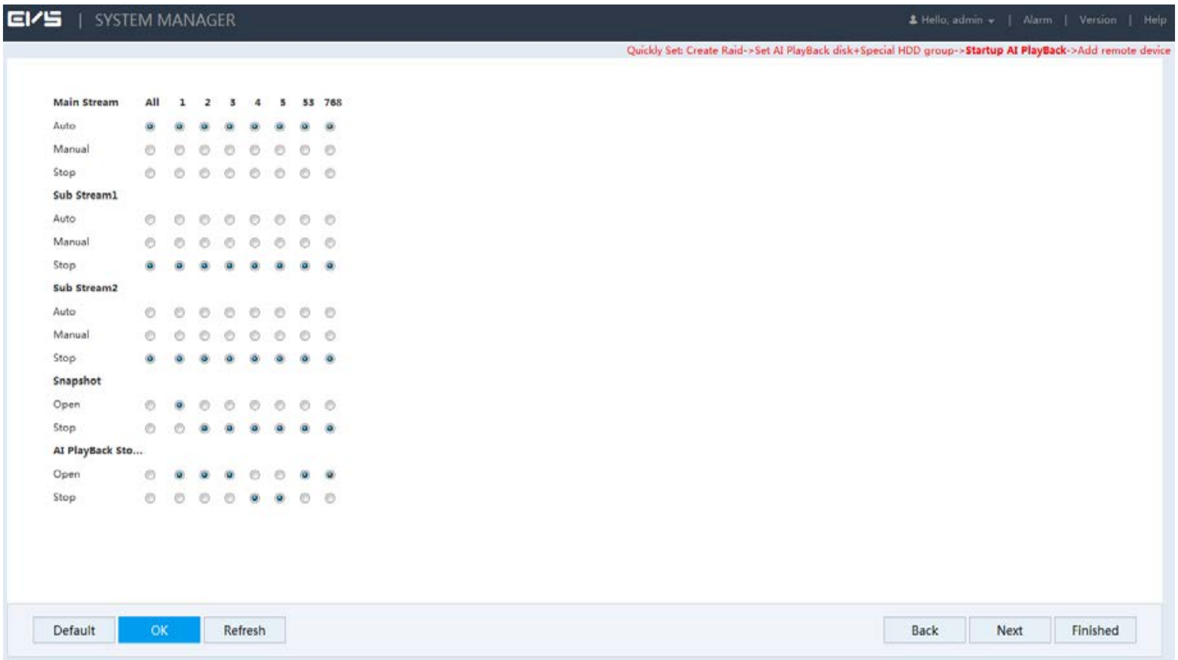
Device Name	Physical Position	Status	Free/Total Space	HDD Operation	HDD Group
sdd	Host_5	OK	5.39TB/5.45TB	Read-Write	Normal1
sdc	Host_9	OK	158.93GB/892.68GB	AI PlayBack Disk	Special HDD Group1
md0	Host	OK	6.78GB/1.74TB	Read-Write	Normal1

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**.

Figure 3-29 AI playback startup


SYSTEM MANAGER
Hello, admin
Alarm
Version
Help
Quickly Set: Create Raid->Set AI PlayBack disk+Special HDD group->Startup AI PlayBack->Add remote device
Default
OK
Refresh
Back
Next
Finished

Main Stream	All	1	2	3	4	5	53	768
Auto	●	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○	○
Sub Stream1								
Auto	○	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●
Sub Stream2								
Auto	○	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●
Snapshot								
Open	○	●	○	○	○	○	○	○
Stop	○	○	●	●	●	●	●	●
AI PlayBack Sto...								
Open	○	●	●	●	○	○	●	●
Stop	○	○	○	○	●	●	○	○

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

Step 7 Click **Next**.

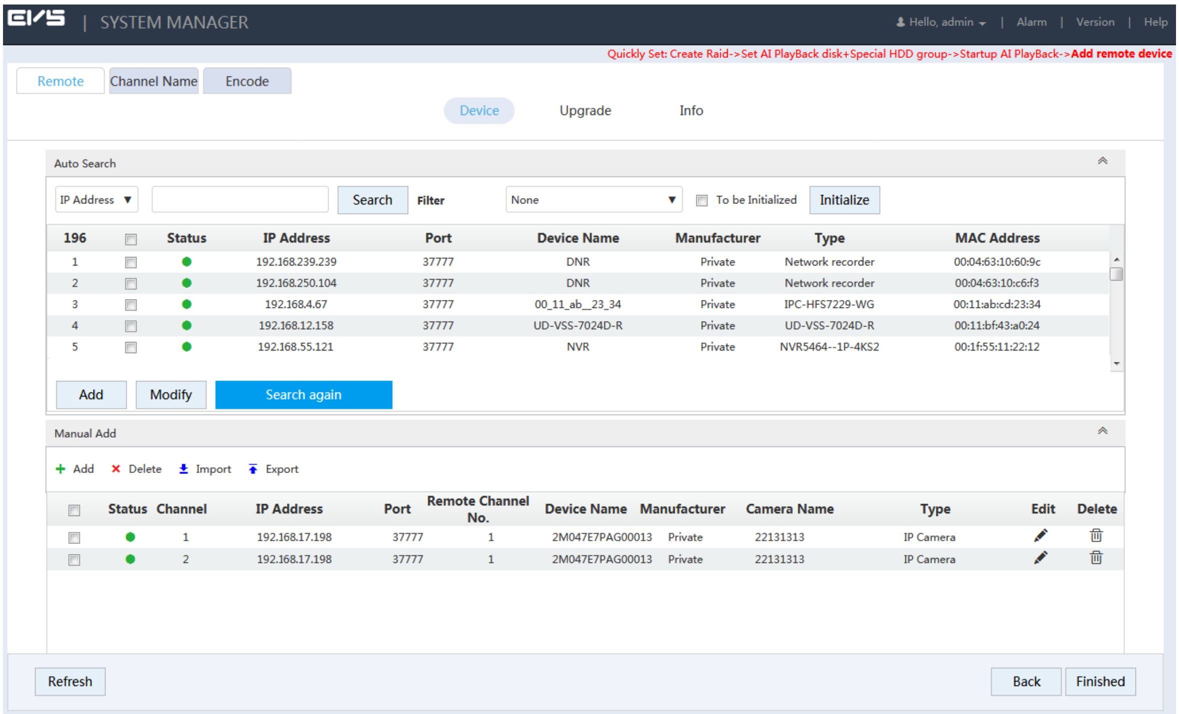


Figure 3-30 Adding remote device

196	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.239.239	37777	DNR	Private	Network recorder	00:04:63:10:60:9c
2	□	●	192.168.250.104	37777	DNR	Private	Network recorder	00:04:63:10:c6:f3
3	□	●	192.168.4.67	37777	00_11_ab__23_34	Private	IPC-HFS7229-WG	00:11:ab:cd:23:34
4	□	●	192.168.12.158	37777	UD-VSS-7024D-R	Private	UD-VSS-7024D-R	00:11:bf:43:a0:24
5	□	●	192.168.55.121	37777	NVR	Private	NVR5464--1P-4KS2	00:1f:55:11:22:12

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑
□	●	2	192.168.17.198	37777	1	2M047E7PAG00013	Private	22131313	IP Camera	✎	🗑

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 for or downloading AI records, including records of IVS analytics, 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.

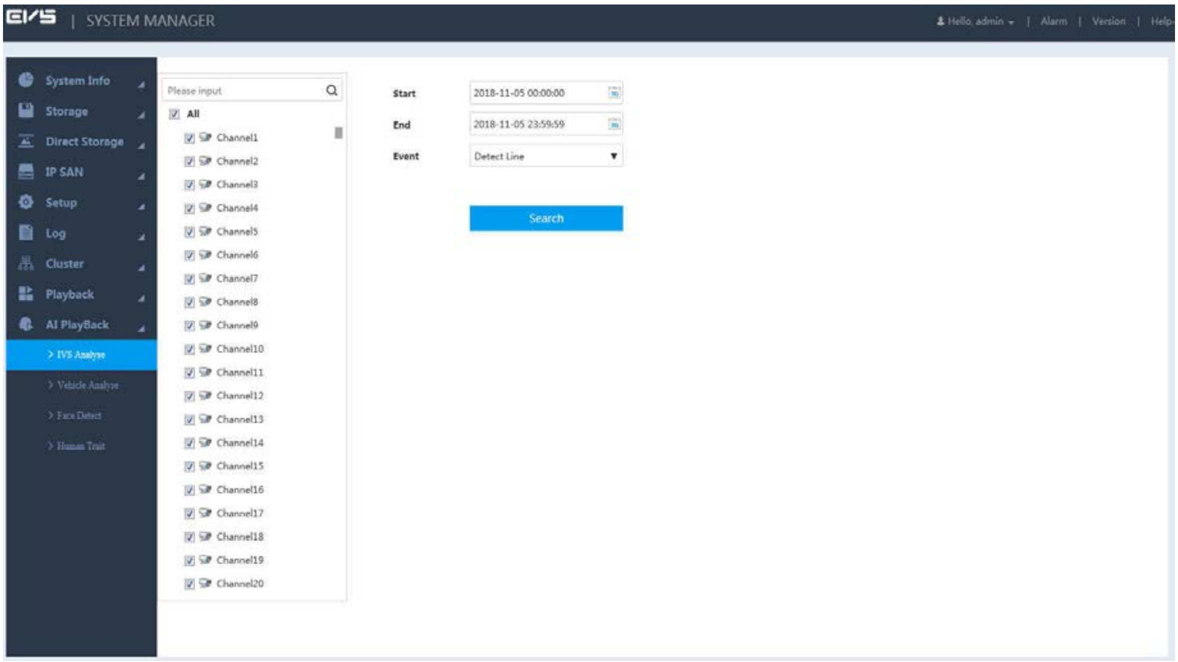
3.6.2.1 IVS Analyse

IVS analytics 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 analytics 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**.

Figure 3-31 IVS analyse



Start 2018-11-05 00:00:00

End 2018-11-05 23:59:59

Event Detect Line

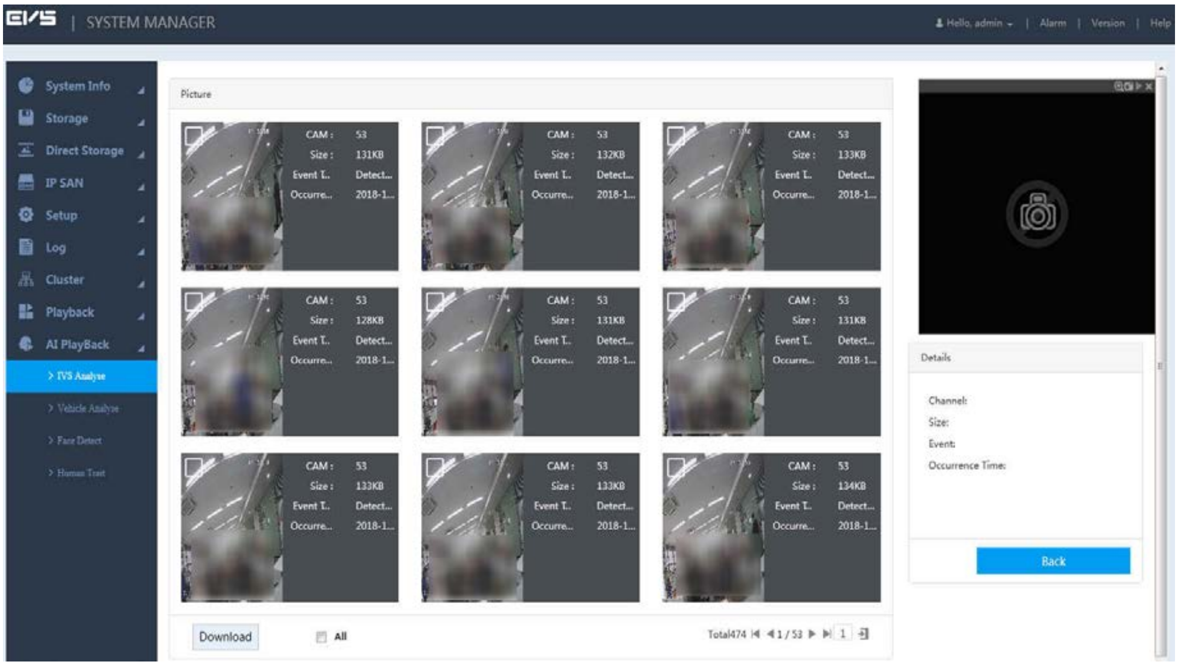
Step 2 Select the parameters.

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**.

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 10 s before and after the picture in the upper right window. For play details, see Table 3-11.

  You can double-click the play page 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.

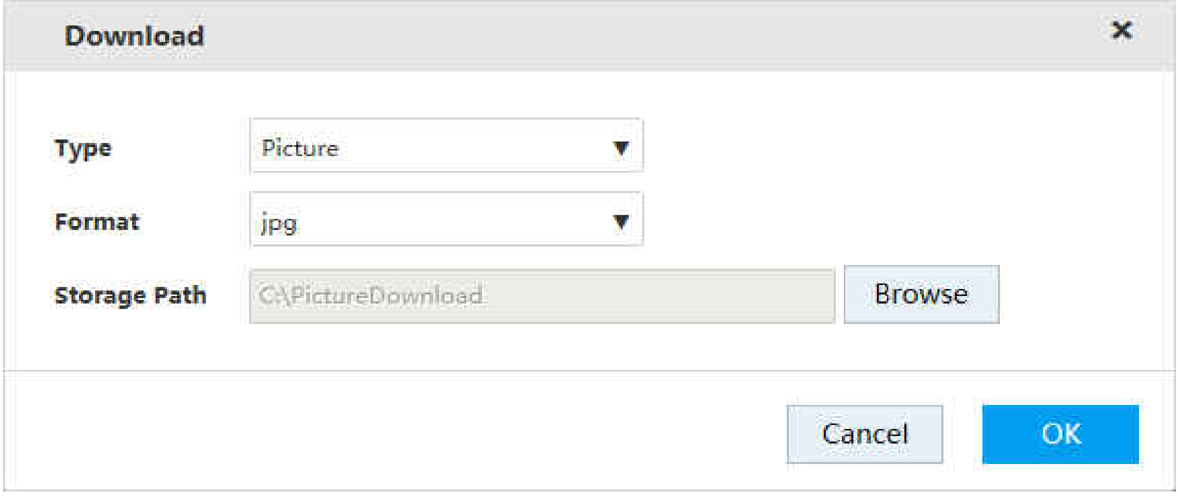
Download

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

The **Download** page is displayed.

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

Figure 3-33 Download



Download

Type: Picture

Format: jpg

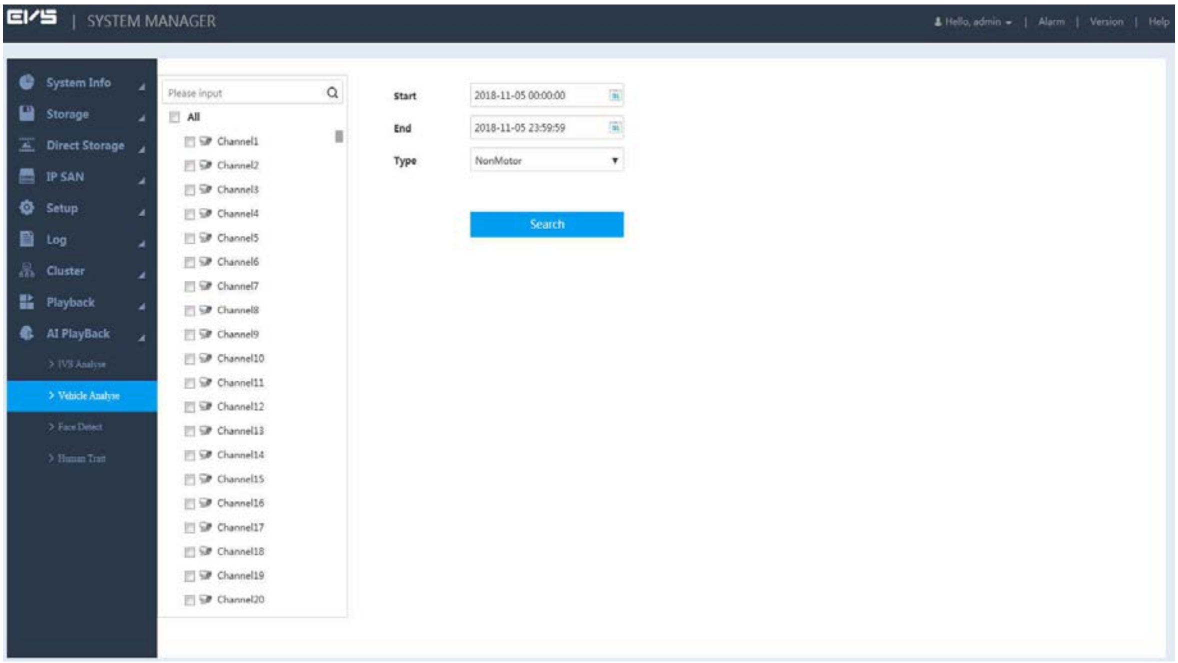
Storage Path: C:\PictureDownload

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**.

Figure 3-34 Vehicle analyse



Start 2018-11-05 00:00:00

End 2018-11-05 23:59:59

Type NonMotor

Step 2 Configure the parameters.

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.
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**.

Parameter	Description
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 10 s before and after the picture in the upper right window. For play details, see Table 3-11.

  📖

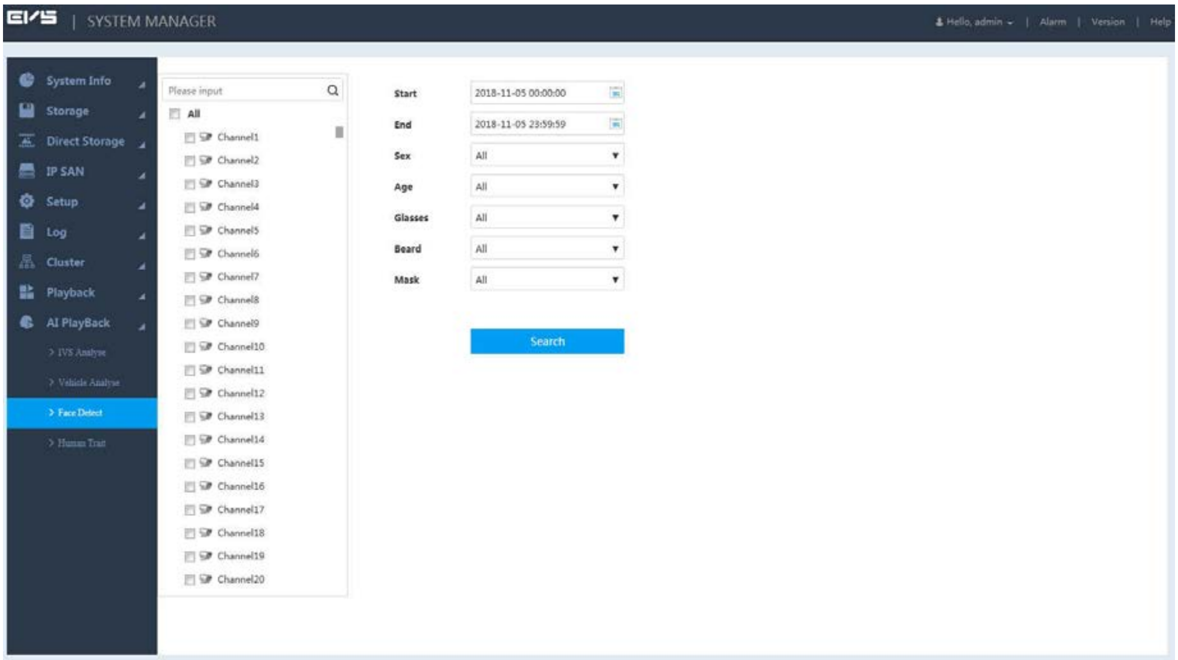
  You can double-click the play page to switch between full-screen and small-screen play.

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**.

Figure 3-35 Face detect



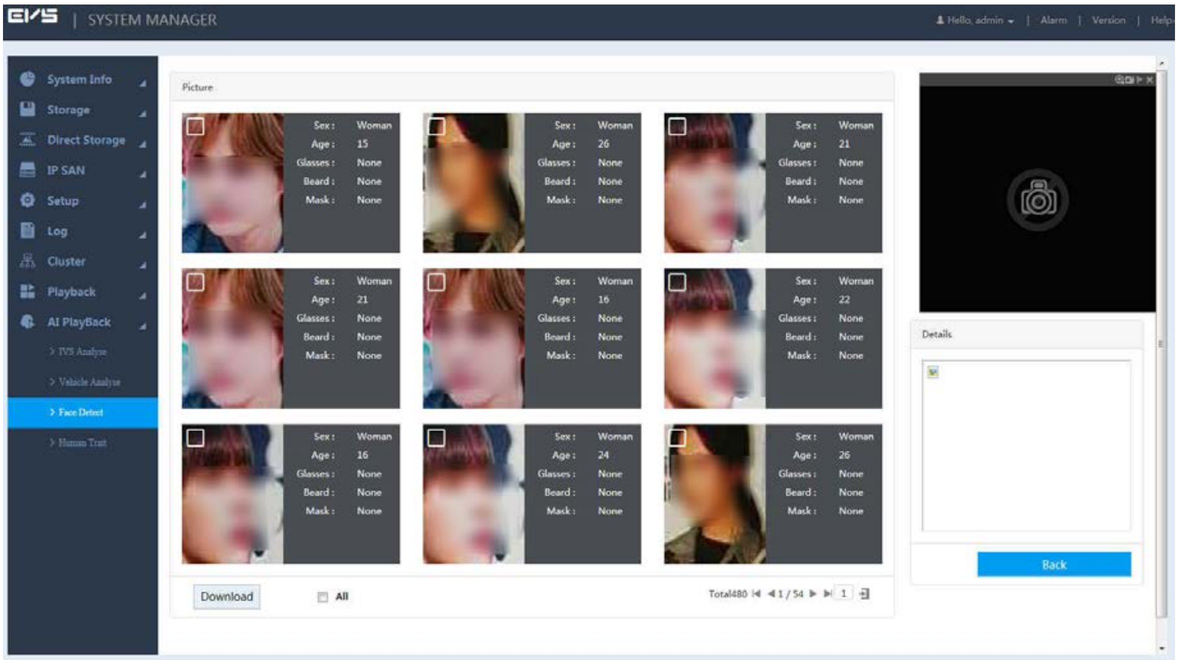
Start: 2018-11-05 00:00:00
End: 2018-11-05 23:59:59
Sex: All
Age: All
Glasses: All
Beard: All
Mask: All

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.

Figure 3-36 Face detect results



Sex :	Age :	Glasses :	Beard :	Mask :
Woman	15	None	None	None
Woman	26	None	None	None
Woman	21	None	None	None
Woman	21	None	None	None
Woman	16	None	None	None
Woman	22	None	None	None
Woman	16	None	None	None
Woman	24	None	None	None
Woman	26	None	None	None

Total480 1 / 54 1

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 10 s before and after the picture in the upper right window. For play details, see Table 3-11.

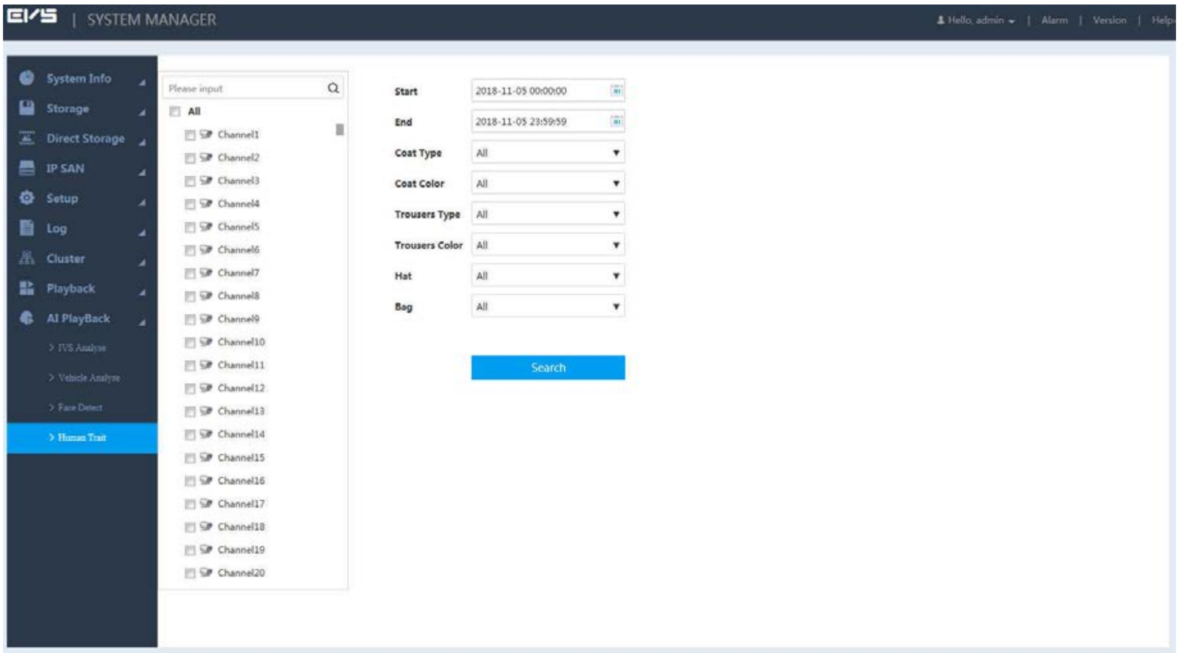
You can double-click the play page to switch between full-screen and small-screen play.

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**.

Figure 3-37 Human trait



Start 2018-11-05 00:00:00

End 2018-11-05 23:59:59

Coat Type All

Coat Color All

Trousers Type All

Trousers Color All

Hat All

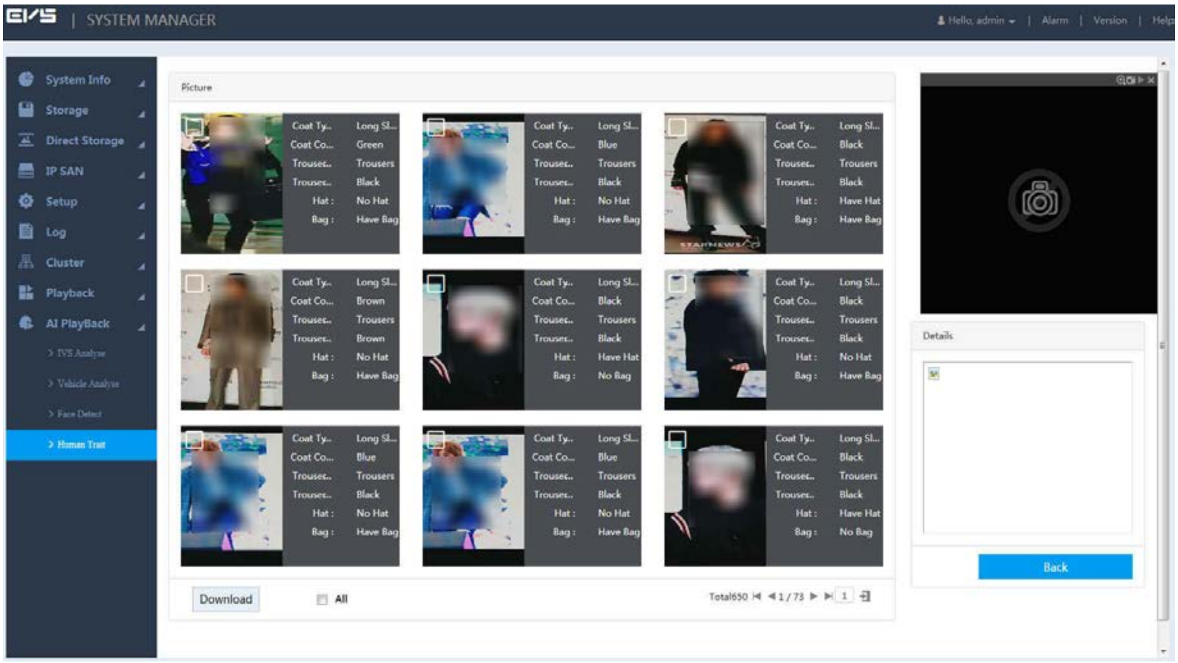
Bag All

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.

Figure 3-38 Human trait results



Coat Ty.. Long Sl...
Coat Co... Green
Trouses... Trousers
Trouses... Black
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Blue
Trouses... Trousers
Trouses... Black
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Black
Trouses... Trousers
Trouses... Black
Hat : Have Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Brown
Trouses... Trousers
Trouses... Brown
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Black
Trouses... Trousers
Trouses... Black
Hat : Have Hat
Bag : No Bag

Coat Ty.. Long Sl...
Coat Co... Black
Trouses... Trousers
Trouses... Black
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Blue
Trouses... Trousers
Trouses... Black
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Blue
Trouses... Trousers
Trouses... Black
Hat : No Hat
Bag : Have Bag

Coat Ty.. Long Sl...
Coat Co... Black
Trouses... Trousers
Trouses... Black
Hat : Have Hat
Bag : No Bag

Total650 1 / 73 1

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 10 s before and after the picture in the upper right window. For play details, see Table 3-11.

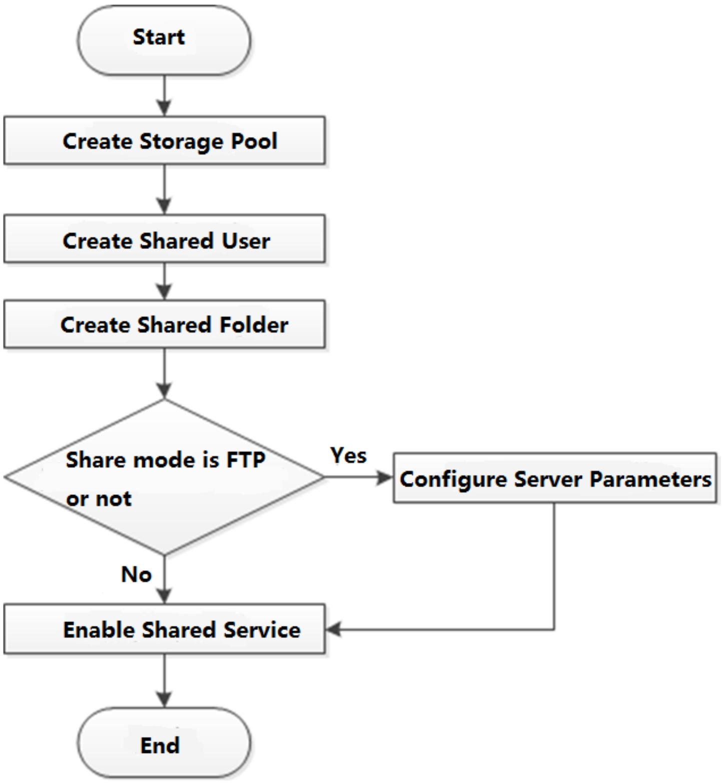
You can double-click the play page to switch between full-screen and small-screen play.

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



3.7.1 Creating Storage Pool

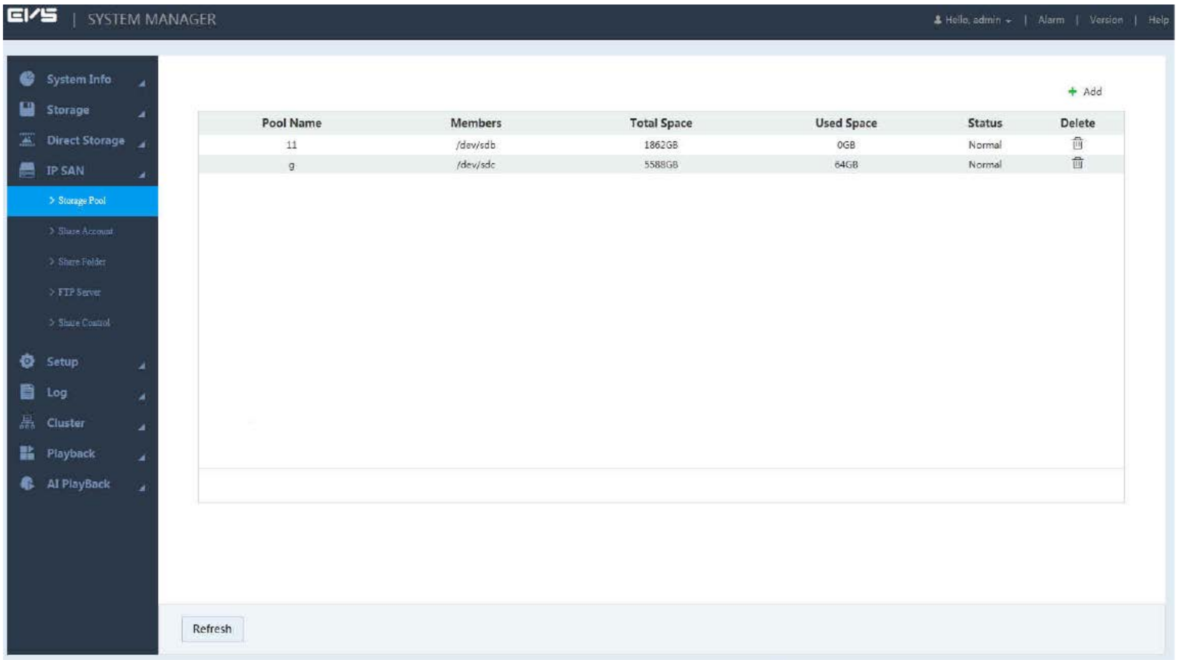
Storage pool is a logical device that is virtualized by the storage devices, which is managed by the system and can be composed of multiple actual disks or RAID. It is one of the main means to realize virtual storage.

⚠

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

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

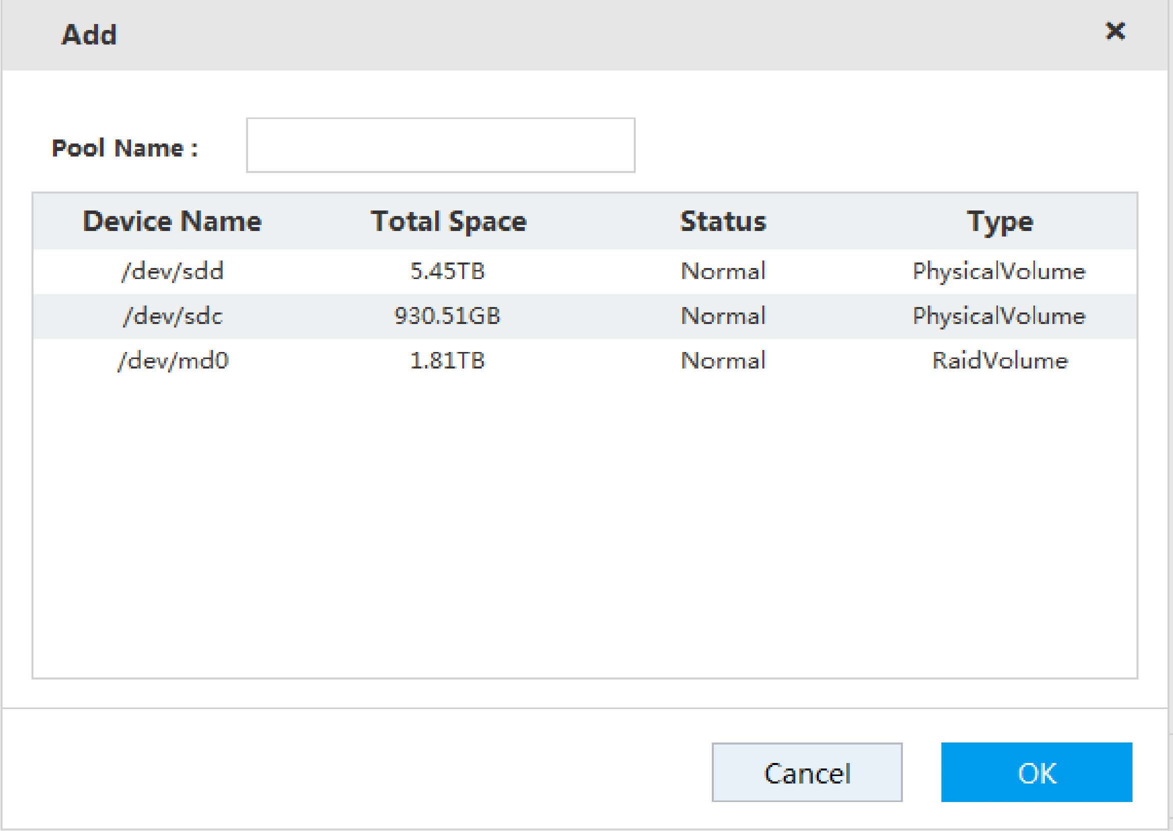
Figure 3-40 Storage pool



Pool Name	Members	Total Space	Used Space	Status	Delete
11	/dev/sdb	1862GB	0GB	Normal	🗑
g	/dev/sdc	5588GB	64GB	Normal	🗑

Step 2 Click +.

Figure 3-41 Adding storage pool



Pool Name :

Device Name	Total Space	Status	Type
/dev/sdd	5.45TB	Normal	PhysicalVolume
/dev/sdc	930.51GB	Normal	PhysicalVolume
/dev/md0	1.81TB	Normal	RaidVolume

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**.

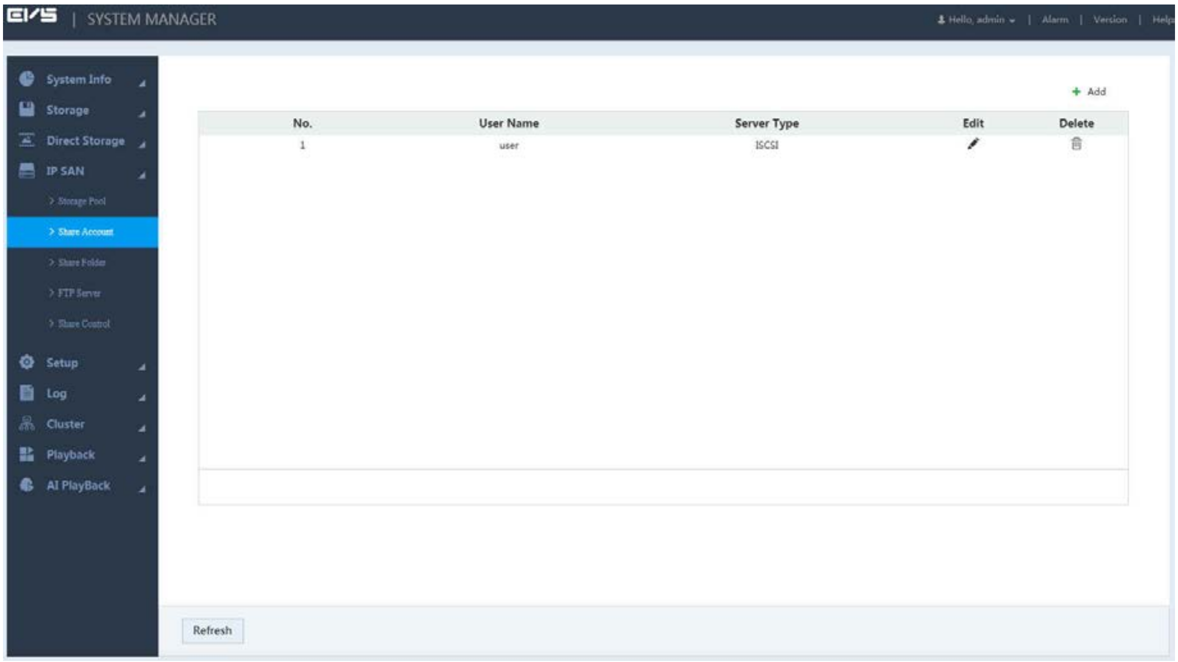
The system starts to create the storage pool. After the creation, the system returns to the **Storage Pool** page. You can view the new pool information here.

3.7.2 Managing Share Account

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

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

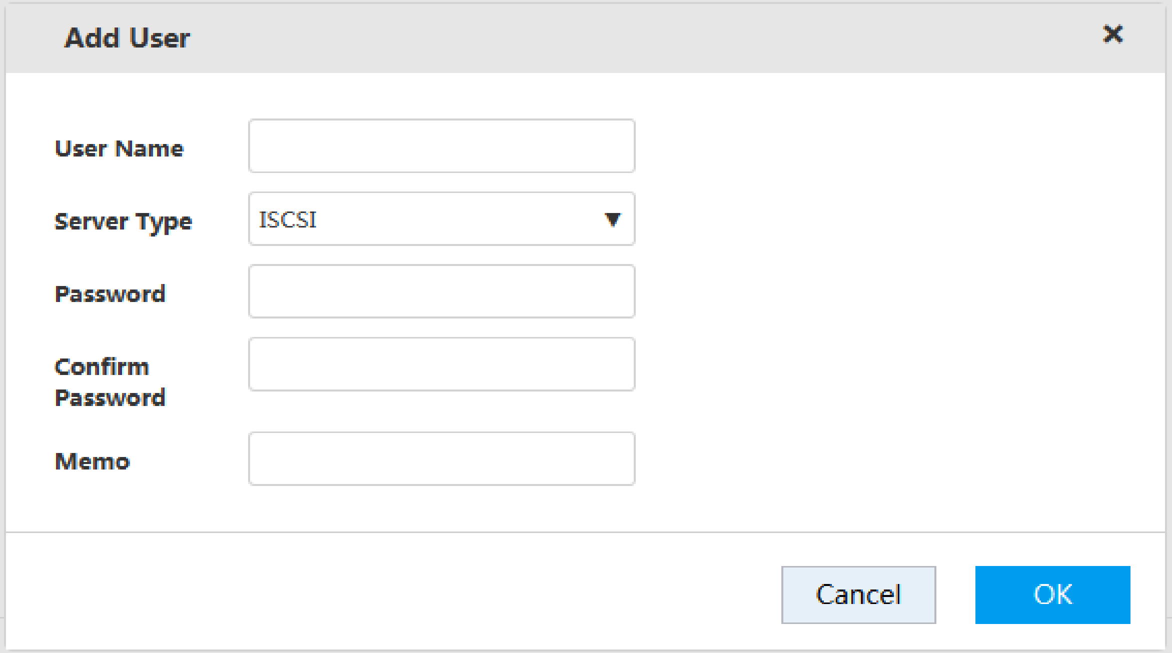
Figure 3-42 Share account management



No.	User Name	Server Type	Edit	Delete
1	user	ISCSI	✎	🗑

Step 2 Click + .

Figure 3-43 Adding shared user



User Name	
Server Type	ISCSI ▼
Password	
Confirm Password	
Memo	

Step 3 Configure the parameters.

Table 3-13 Adding user parameters

Parameter	Description
Username	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.

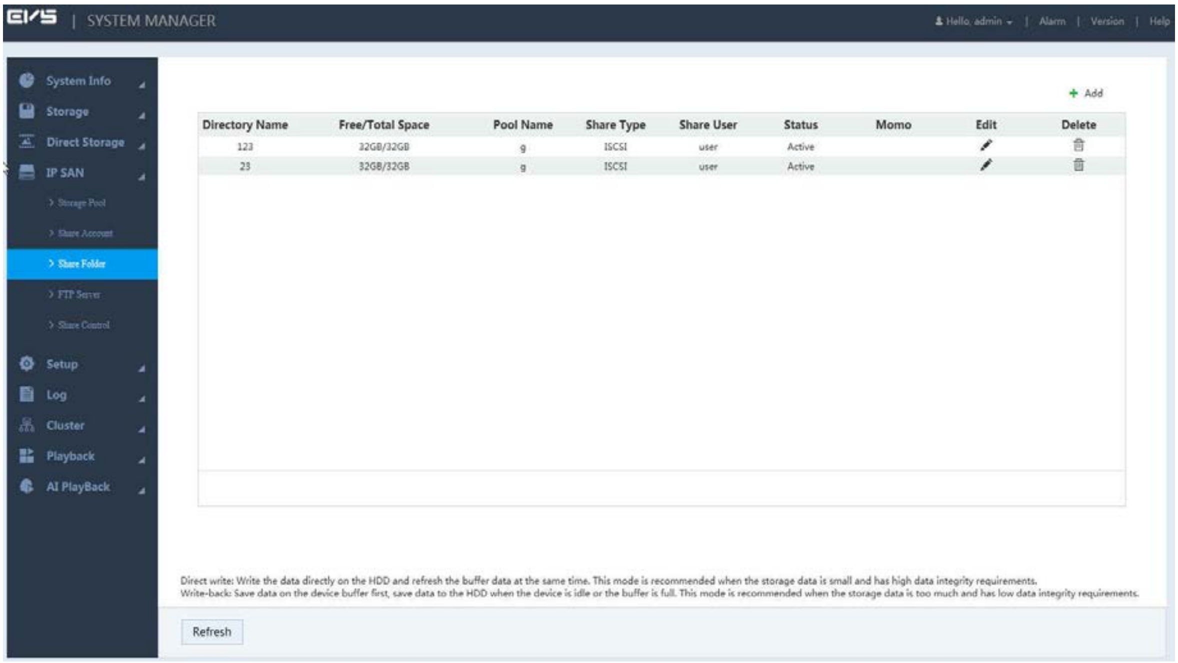
The system returns to the **Share Account** page. You can view the new account information here.

3.7.3 Setting Share Folder

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

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

Figure 3-44 Share folder

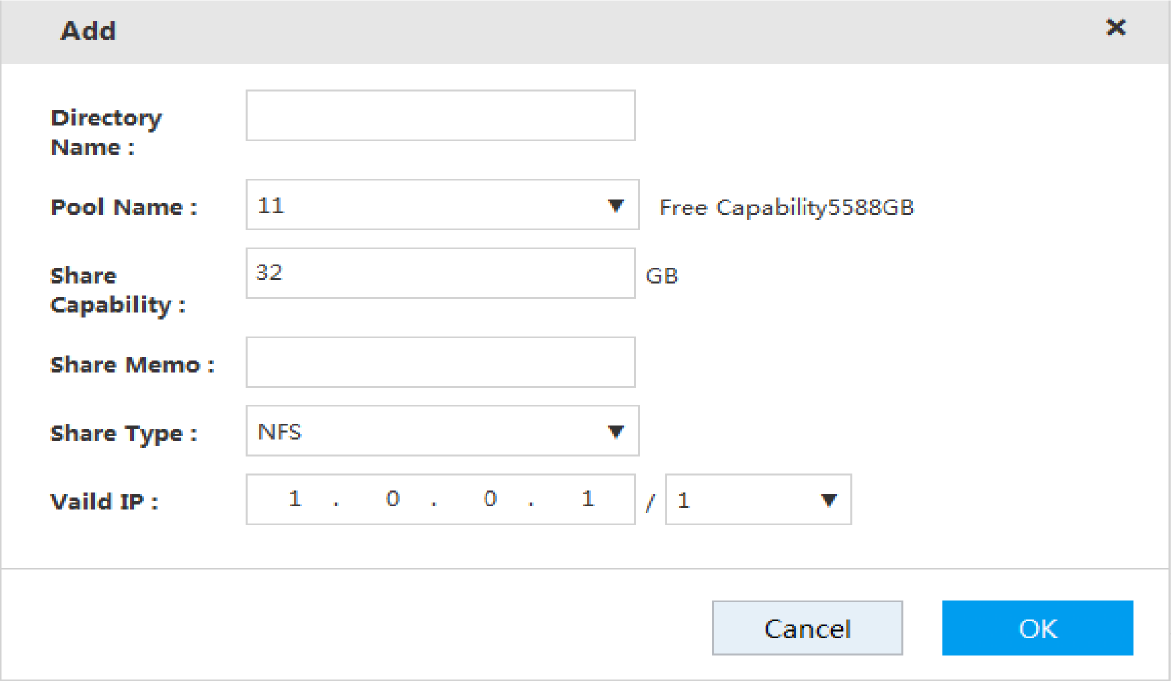


Directory Name	Free/Total Space	Pool Name	Share Type	Share User	Status	Momo	Edit	Delete
123	32GB/32GB	g	ISCSI	user	Active		✎	🗑
23	32GB/32GB	g	ISCSI	user	Active		✎	🗑

Direct write: Write the data directly on the HDD and refresh the buffer data at the same time. This mode is recommended when the storage data is small and has high data integrity requirements.
Write-back: Save data on the device buffer first, save data to the HDD when the device is idle or the buffer is full. This mode is recommended when the storage data is too much and has low data integrity requirements.

Step 2 Click + .

Figure 3-45 Adding share folder (NFS)



Add

Directory Name :

Pool Name : 11 Free Capability5588GB

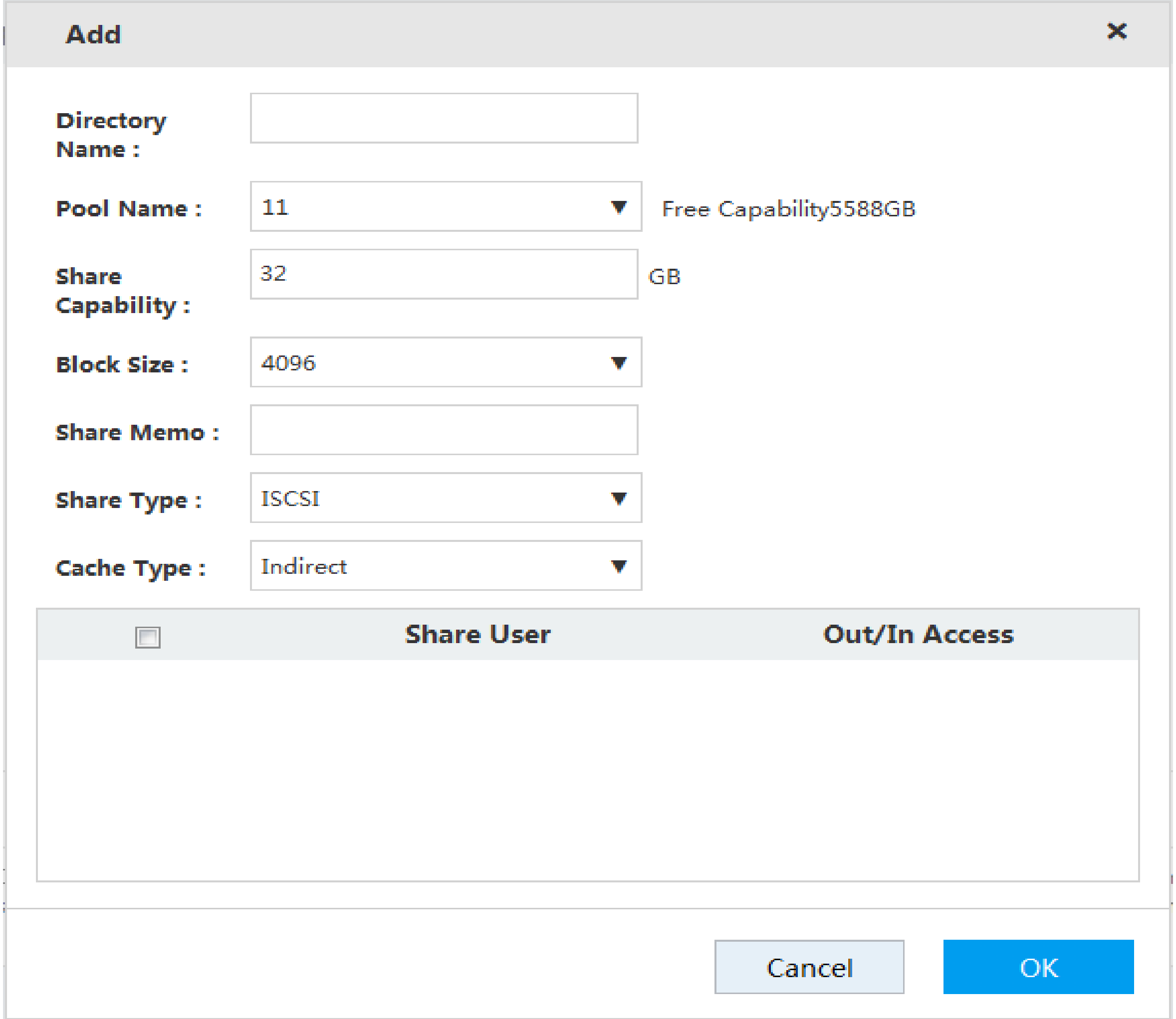
Share Capability : 32 GB

Share Memo :

Share Type : NFS

Vaild IP : 1 . 0 . 0 . 1 / 1

Figure 3-46 Adding share folder (iSCSI)



Add

Directory Name :

Pool Name : 11 Free Capability5588GB

Share Capability : 32 GB

Block Size : 4096

Share Memo :

Share Type : ISCSI

Cache Type : Indirect

□	Share User	Out/In Access

Step 3 Configure the parameters.

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.
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 512 bytes, 1024 bytes, 2048 bytes and 4096 bytes. 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** page. 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.

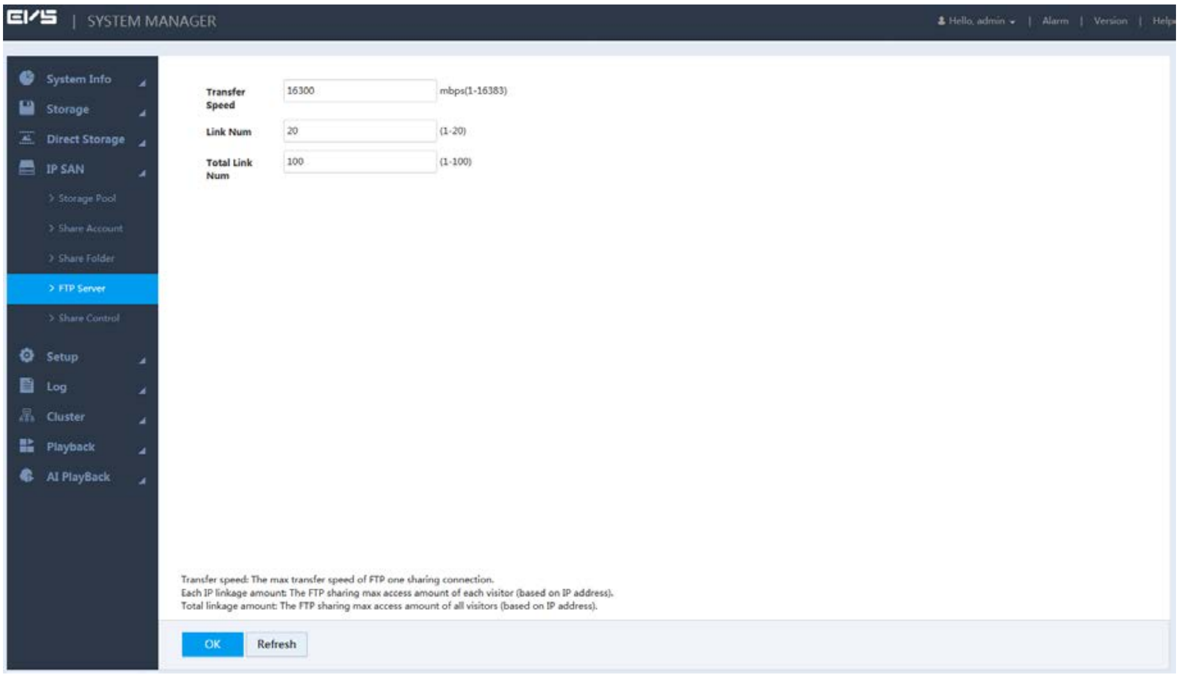
3.7.4 Setting FTP Parameters

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**.

Figure 3-47 FTP Parameters



Transfer Speed 16300 mbps(1-16383)

Link Num 20 (1-20)

Total Link Num 100 (1-100)

Transfer speed: The max transfer speed of FTP one sharing connection.
Each IP linkage amount: The FTP sharing max access amount of each visitor (based on IP address).
Total linkage amount: The FTP sharing max access amount of all visitors (based on IP address).

Step 2 Enter the parameters.

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.

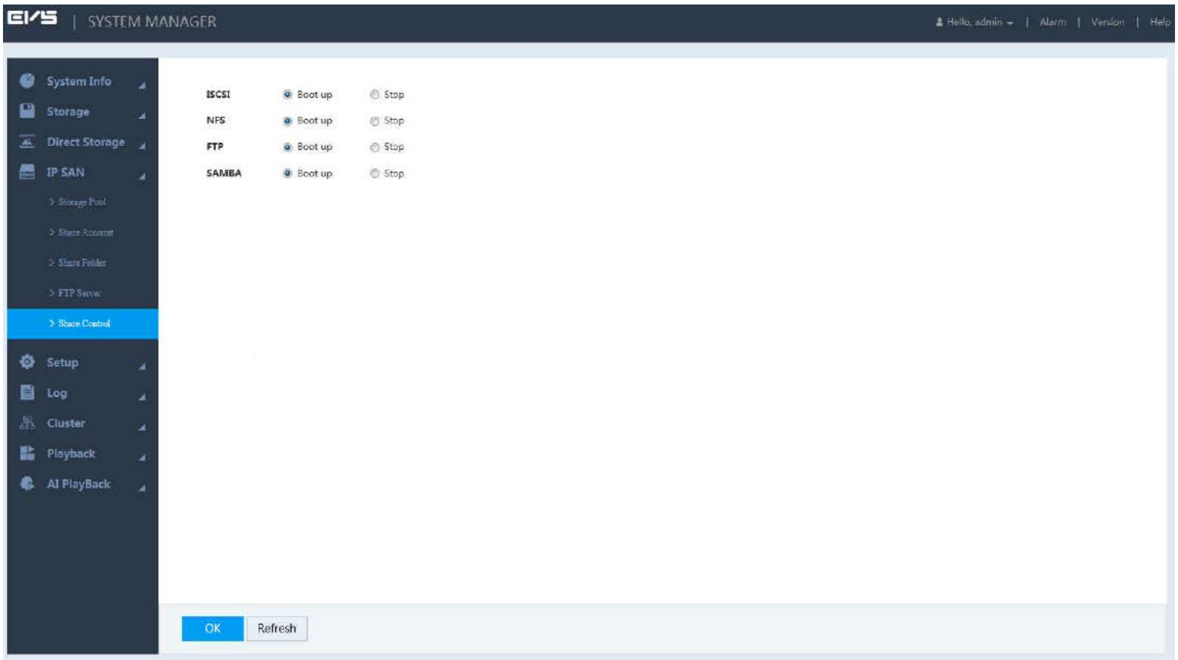
Step 3 Click **OK** to save the configuration.

3.7.5 Opening Share Services

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

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

Figure 3-48 Share control



ISCSI	● Boot up	○ Stop
NFS	● Boot up	○ Stop
FTP	● Boot up	○ Stop
SAMBA	● Boot up	○ Stop

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

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

3.8 Remote Device

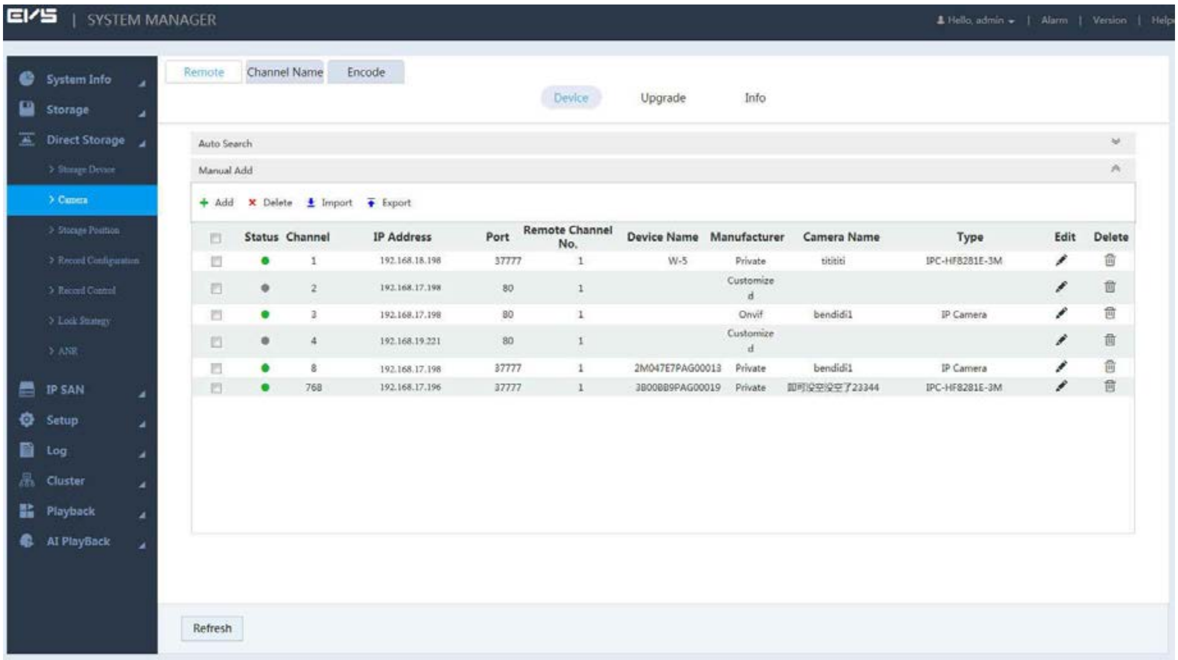
You can add, edit and upgrade your remote device. In addition, you can set the channel name and stream parameters of your remote device.

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**.

Figure 3-49 Device

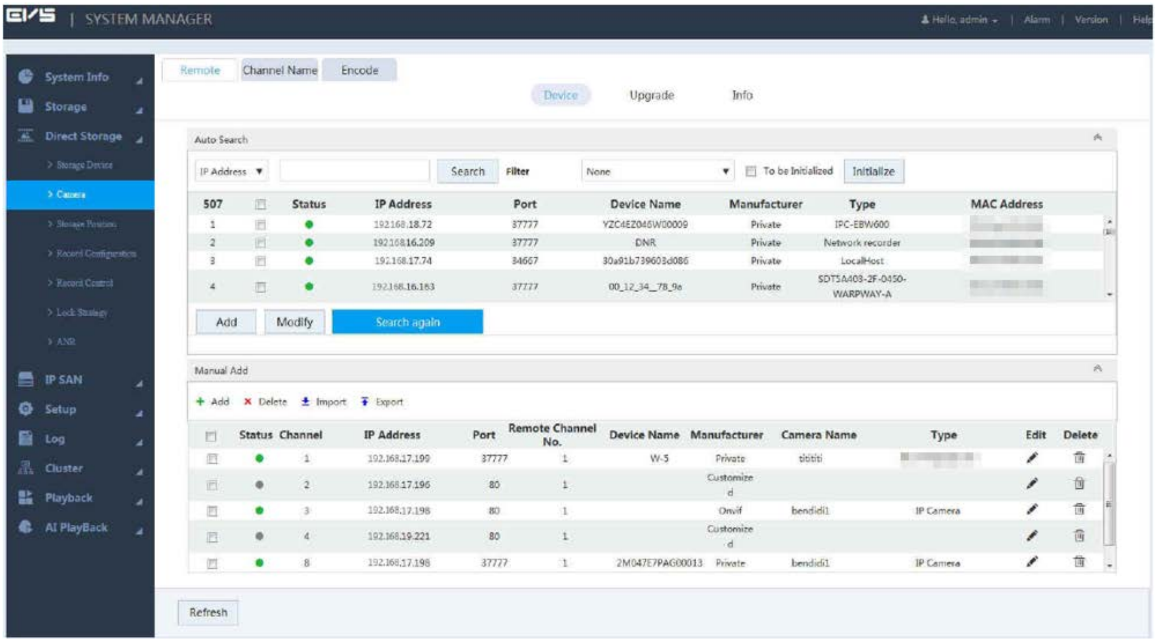


□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.18.198	37777	1	W-5	Private	titititi	IPC-HF8281E-3M	✎	🗑
□	●	2	192.168.17.198	80	1		Customized			✎	🗑
□	●	3	192.168.17.198	80	1		Onvif	bendidi1	IP Camera	✎	🗑
□	●	4	192.168.19.221	80	1		Customized			✎	🗑
□	●	8	192.168.17.198	37777	1	2M047E7PAG00013	Private	bendidi1	IP Camera	✎	🗑
□	●	768	192.168.17.196	37777	1	3B00BB9PAG00019	Private	即可没空没空了23344	IPC-HF8281E-3M	✎	🗑

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.

Figure 3-50 Search result



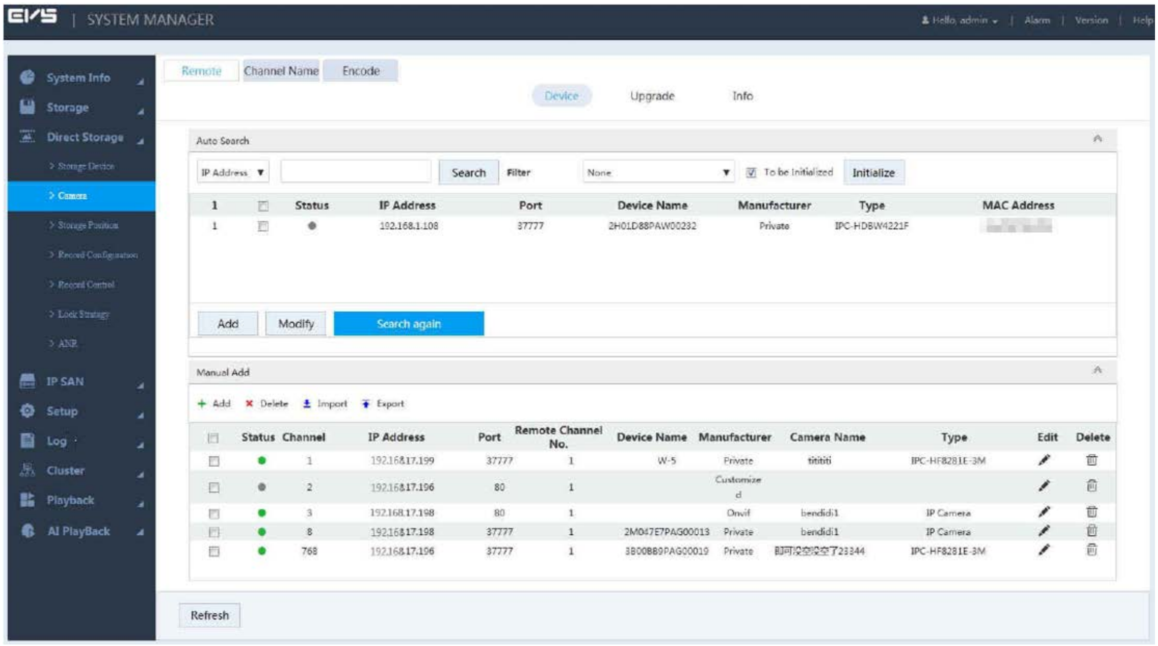
507	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.18.72	37777	YZC4EZ046W00009	Private	IPC-EBW600	[redacted]
2	□	●	192.168.16.209	37777	DNR	Private	Network recorder	[redacted]
3	□	●	192.168.17.74	34667	30a91b739603d086	Private	LocalHost	[redacted]
4	□	●	192.168.16.163	37777	00_12_34__78_9a	Private	SDT5A403-2F-0450-WARPWAY-A	[redacted]

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.199	37777	1	W-5	Private	tititi	[redacted]	✎	🗑
□	●	2	192.168.17.196	80	1		Customized			✎	🗑
□	●	3	192.168.17.198	80	1		Onvif	bendidi1	IP Camera	✎	🗑
□	●	4	192.168.19.221	80	1		Customized			✎	🗑
□	●	8	192.168.17.198	37777	1	2M047E7PAG00013	Private	bendidi1	IP Camera	✎	🗑

Step 3 Select **To be initialized**.

The system displays device that needs to be initialized.

Figure 3-51 Device needs to be initialized



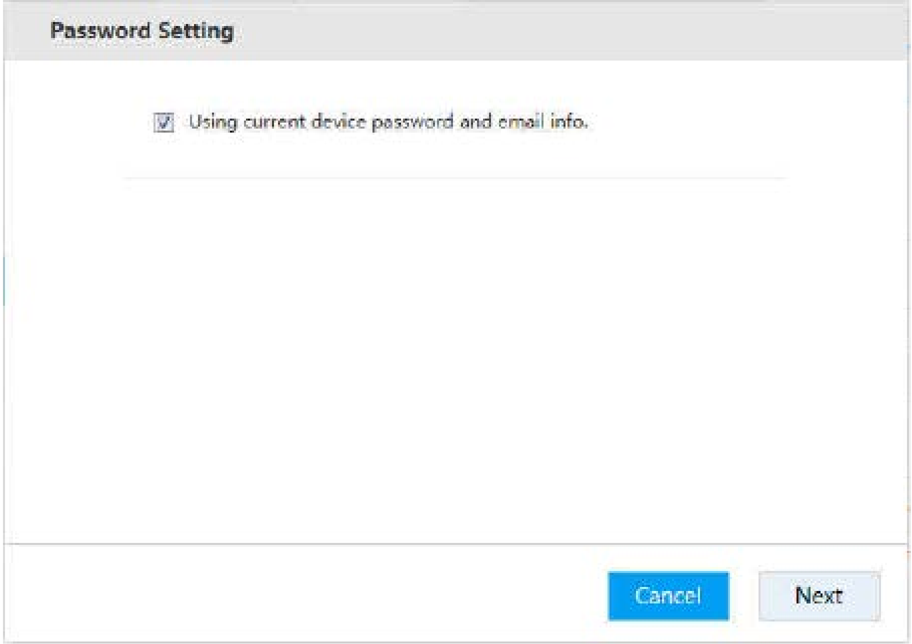
1	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.1.108	37777	2H01D88PAW00232	Private	IPC-HDBW4221F	[redacted]

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.17.199	37777	1	W-5	Private	titititi	IPC-HF8281E-3M	✎	🗑
□	●	2	192.168.17.196	80	1		Customized			✎	🗑
□	●	3	192.168.17.198	80	1		Onvif	bendidi1	IP Camera	✎	🗑
□	●	8	192.168.17.198	37777	1	2M047E7PAG00013	Private	bendidi1	IP Camera	✎	🗑
□	●	768	192.168.17.196	37777	1	3B00B89PAG00019	Private	即可没空没空了23344	IPC-HF8281E-3M	✎	🗑

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

The system displays **Password Setting** page.

Figure 3-52 Password setting (1)



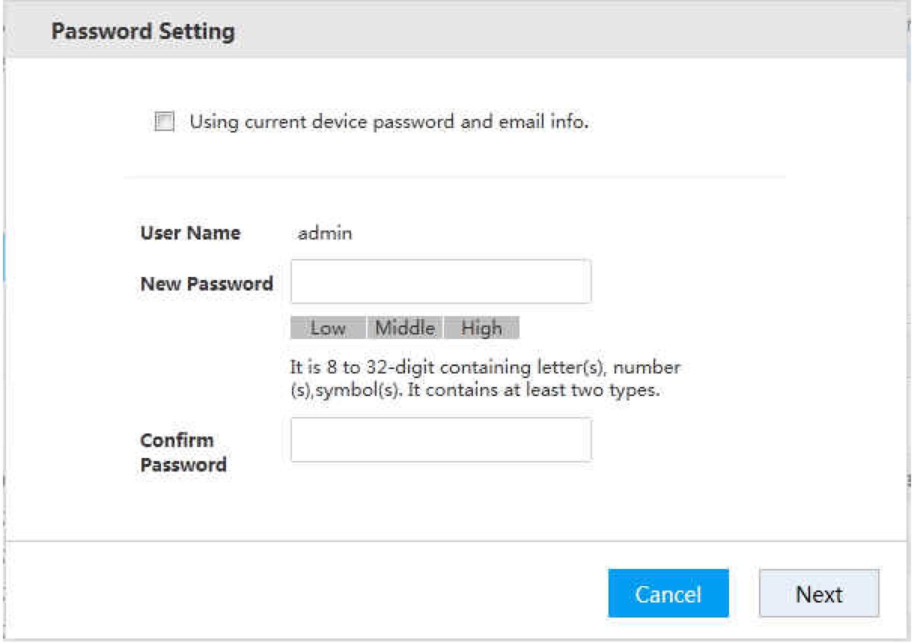
Password Setting

☑ Using current device password and email info.

Step 5 Set the password of the remote device.

If you do not select **Using current device password and email info**, and the page 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)



Password Setting

□ Using current device password and email info.

User Name admin

New Password

Low Middle High

It is 8 to 32-digit containing letter(s), number (s),symbol(s). It contains at least two types.

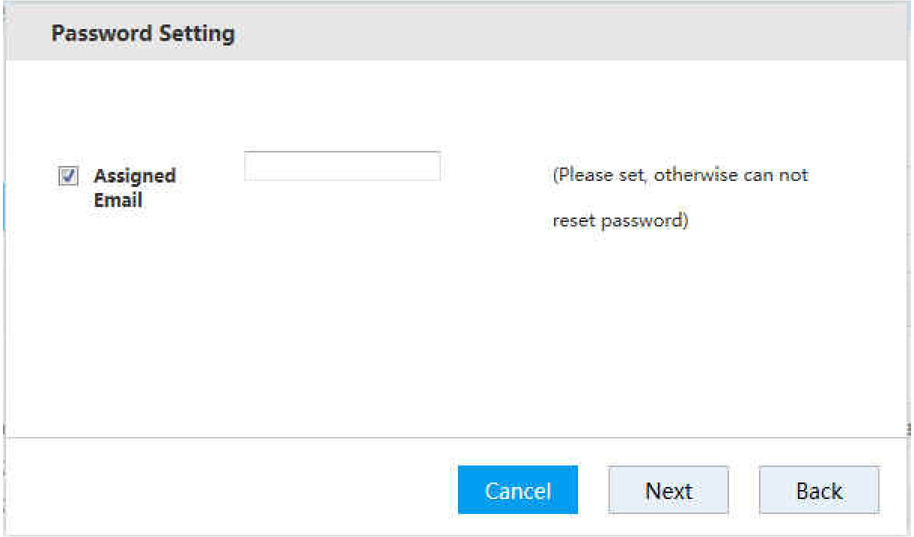
Confirm Password

- 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 page 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 prompt you to enter the assigned email.

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

Figure 3-54 Password setting (3)

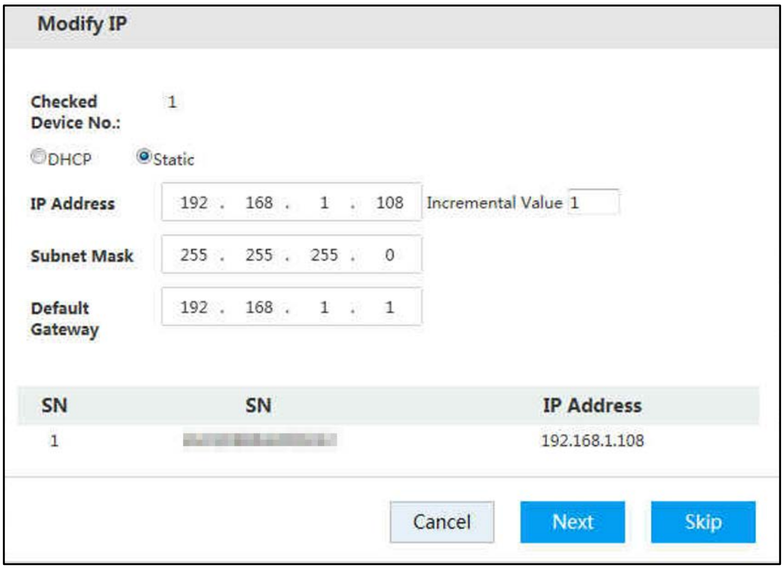

Password Setting

☑ Assigned Email

(Please set, otherwise can not reset password)

Step 7 The **Modify IP** page is displayed.

Figure 3-55 Modify IP


Modify IP

Checked Device No.: 1

○DHCP ●Static

IP Address 192 . 168 . 1 . 108 Incremental Value 1

Subnet Mask 255 . 255 . 255 . 0

Default Gateway 192 . 168 . 1 . 1

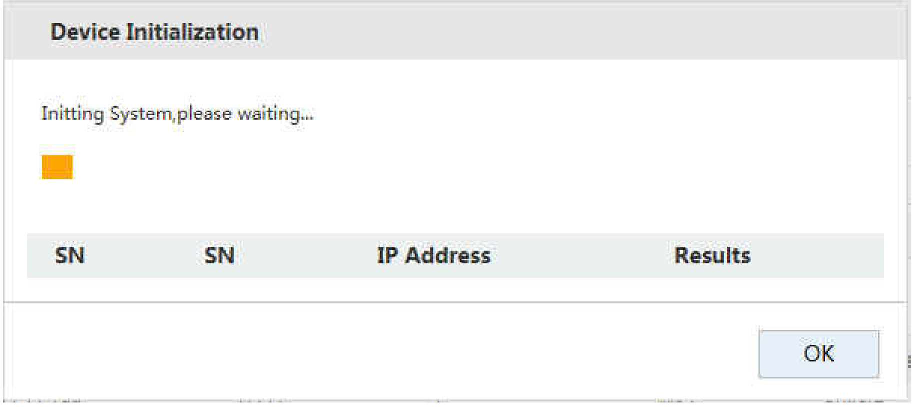
SN	SN	IP Address
1	[redacted]	192.168.1.108

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.

Figure 3-56 Device initialization



Device Initialization

Initting System,please waiting...

SN	SN	IP Address	Results

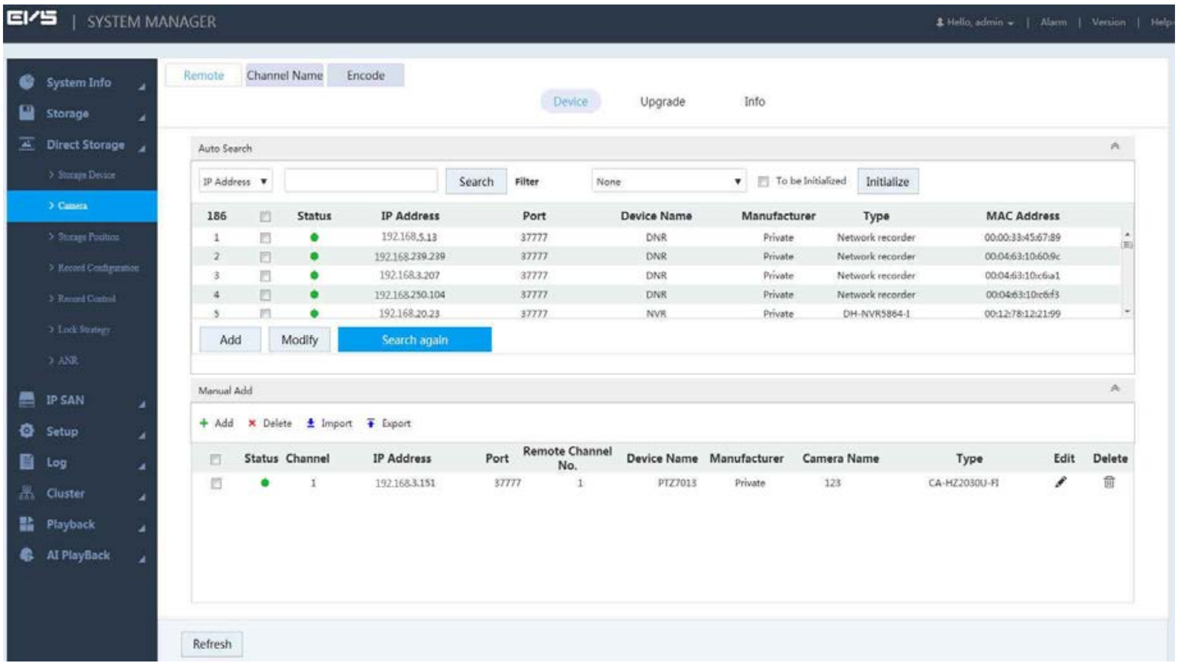
3.8.2 Modifying IP address

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

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

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

Figure 3-57 Device

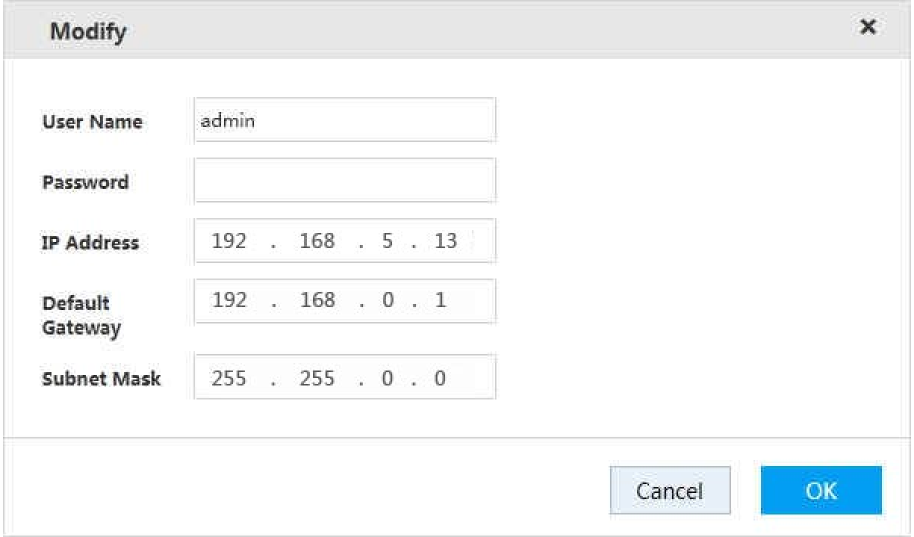


186	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	192.168.5.13	37777	DNR	Private	Network recorder	00:00:33:45:67:89
2	□	●	192.168.239.239	37777	DNR	Private	Network recorder	00:04:63:10:60:9c
3	□	●	192.168.3.207	37777	DNR	Private	Network recorder	00:04:63:10:c6:a1
4	□	●	192.168.250.104	37777	DNR	Private	Network recorder	00:04:63:10:c6:f3
5	□	●	192.168.20.23	37777	NVR	Private	DH-NVR5864-I	00:12:78:12:21:99

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.3.151	37777	1	PTZ7013	Private	123	CA-HZ2030U-FI	✎	🗑

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

Figure 3-58 Modify



Modify

User Name: admin

Password:

IP Address: 192 . 168 . 5 . 13

Default Gateway: 192 . 168 . 0 . 1

Subnet Mask: 255 . 255 . 0 . 0

Step 4 Enter the **Username** 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** page 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

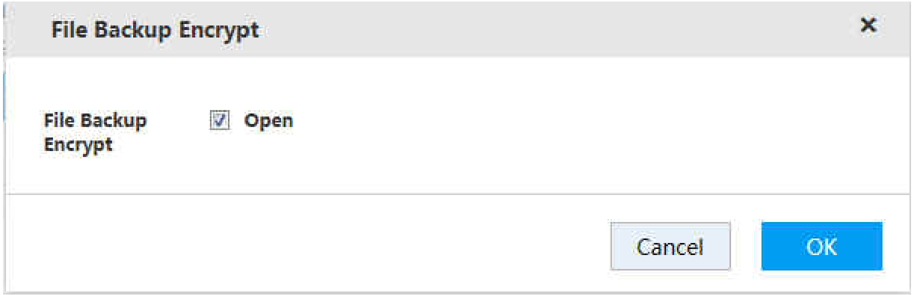
The system supports exporting the entire list of devices added, and save it in the PC.

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

The **Device** page is displayed.

Step 2 Click ⬆. The **File Backup Encrypt** page is displayed.

Figure 3-59 File Backup Encrypt

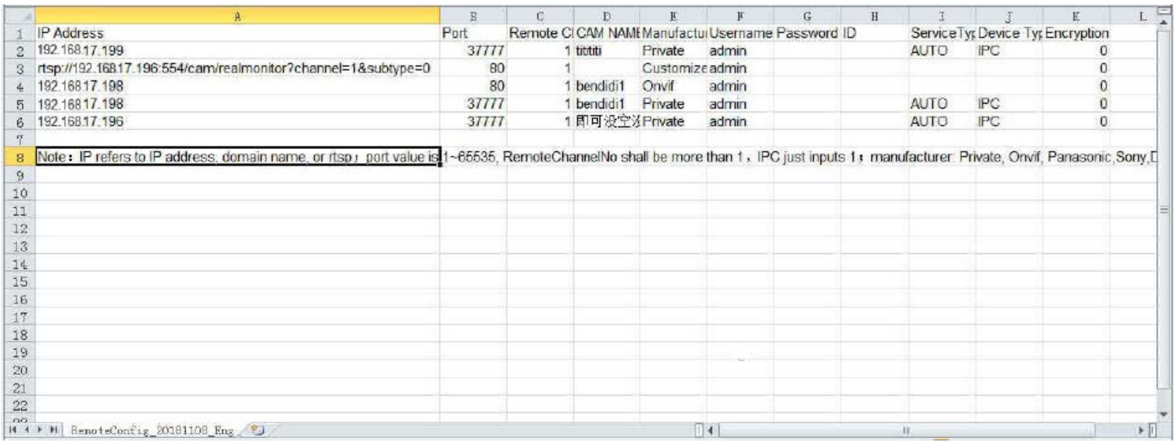


File Backup Encrypt

File Backup Encrypt ☑ Open

- 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	Manufactu	Username	Password	ID	ServiceTy	Device Ty	Encryption
192.168.17.199	37777	1	tititi	Private	admin			AUTO	IPC	0
rtsp://192.168.17.196:554/cam/realmonitor?channel=1&subtype=0	80	1		Customize	admin					0
192.168.17.198	80	1	bendidi1	Onvif	admin					0
192.168.17.198	37777	1	bendidi1	Private	admin			AUTO	IPC	0
192.168.17.196	37777	1	即可没空㳌	Private	admin			AUTO	IPC	0

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.

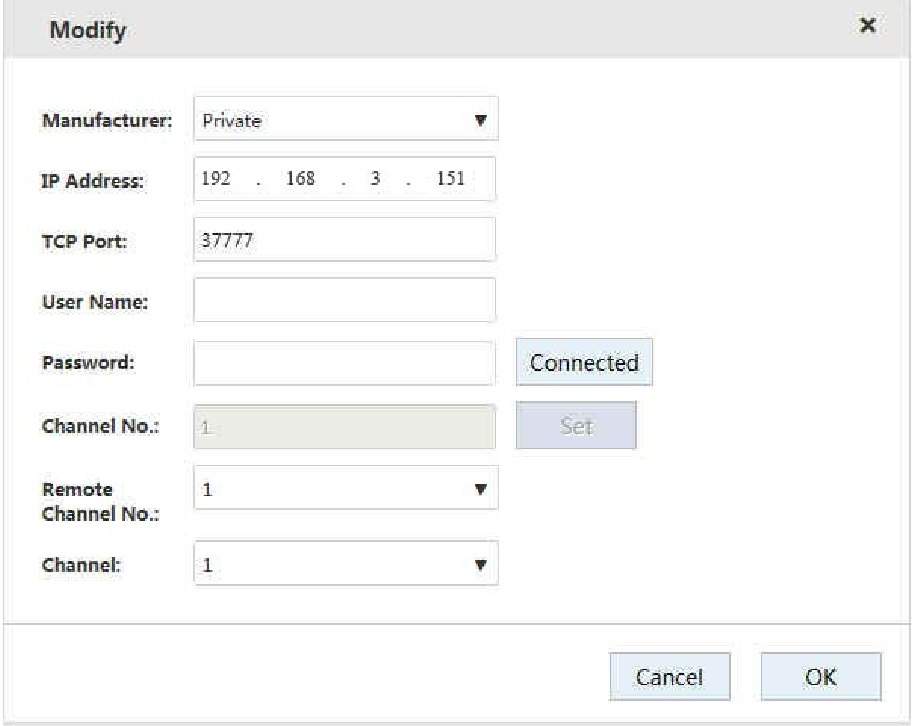
3.8.4 Editing Remote Device

You can modify or delete remote devices added.

- Click ✎, the **Modify** page is displayed.

  You can modify the information of the remote device.

Figure 3-61 Modify



Modify

Manufacturer: Private

IP Address: 192 . 168 . 3 . 151

TCP Port: 37777

User Name:

Password:

Channel No.: 1

Remote Channel No.: 1

Channel: 1

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

3.8.5 Upgrading Remote Device

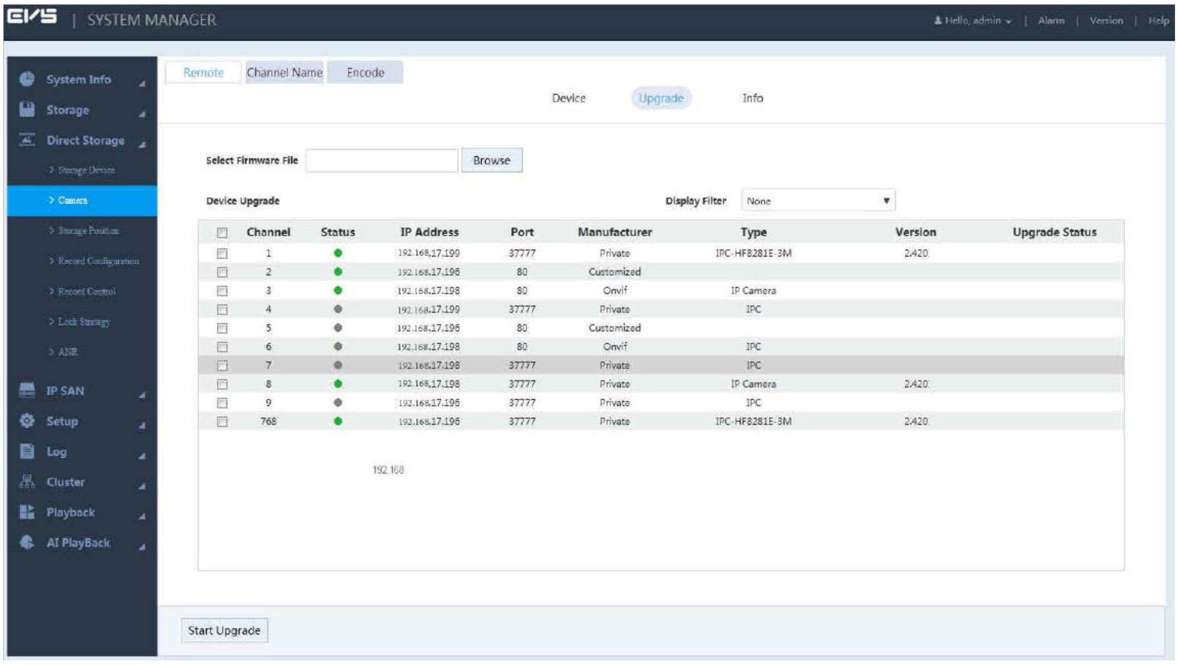
The system supports upgrading the remote device on web interface.

Preparation

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

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

Figure 3-62 Upgrade



Select Firmware File

Device Upgrade

Display Filter: None

□	Channel	Status	IP Address	Port	Manufacturer	Type	Version	Upgrade Status
□	1	●	192.168.17.199	37777	Private	IPC-HF8281E-3M	2.420	
□	2	●	192.168.17.196	80	Customized			
□	3	●	192.168.17.198	80	Onvif	IP Camera		
□	4	●	192.168.17.199	37777	Private	IPC		
□	5	●	192.168.17.196	80	Customized			
□	6	●	192.168.17.198	80	Onvif	IPC		
□	7	●	192.168.17.198	37777	Private	IPC		
□	8	●	192.168.17.198	37777	Private	IP Camera	2.420	
□	9	●	192.168.17.196	37777	Private	IPC		
□	768	●	192.168.17.196	37777	Private	IPC-HF8281E-3M	2.420	

192.168

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

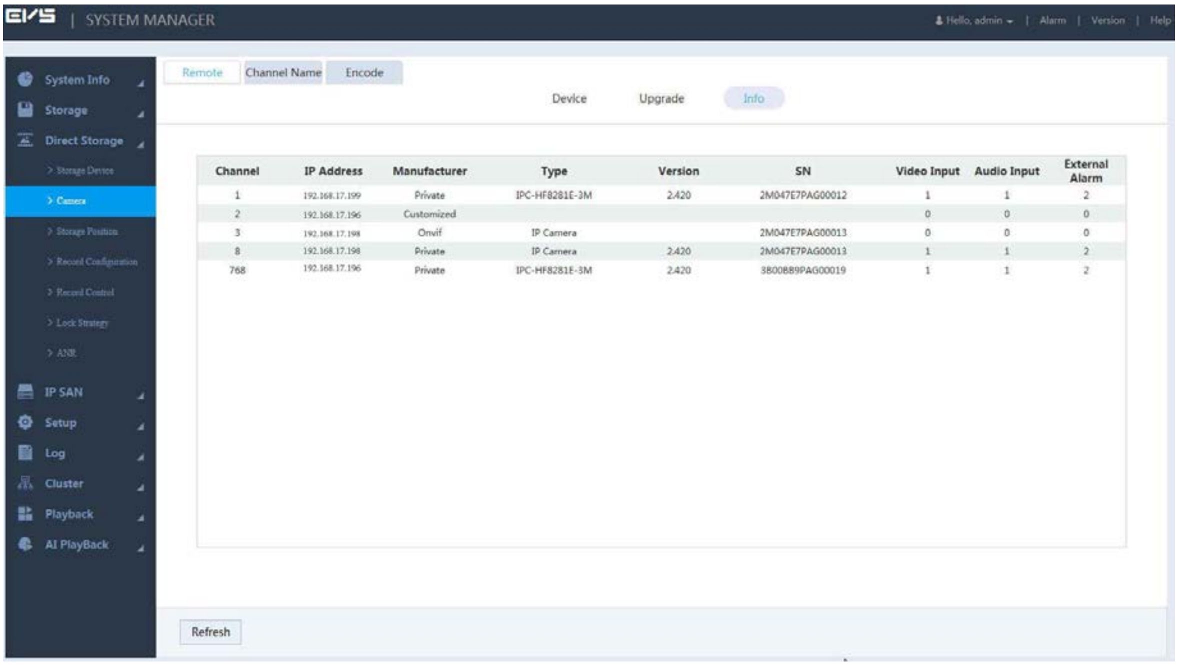
View the information of the remote device, such as channel, IP address, manufacturer, type, version, SN, video input, audio output, and external alarm.

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

The **Info** page is displayed.

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

Figure 3-63 Info



Channel	IP Address	Manufacturer	Type	Version	SN	Video Input	Audio Input	External Alarm
1	192.168.17.199	Private	IPC-HF8281E-3M	2.420	2M047E7PAG00012	1	1	2
2	192.168.17.196	Customized				0	0	0
3	192.168.17.198	Onvif	IP Camera		2M047E7PAG00013	0	0	0
8	192.168.17.198	Private	IP Camera	2.420	2M047E7PAG00013	1	1	2
768	192.168.17.196	Private	IPC-HF8281E-3M	2.420	3B00BB9PAG00019	1	1	2

3.8.7 Setting Channel Name

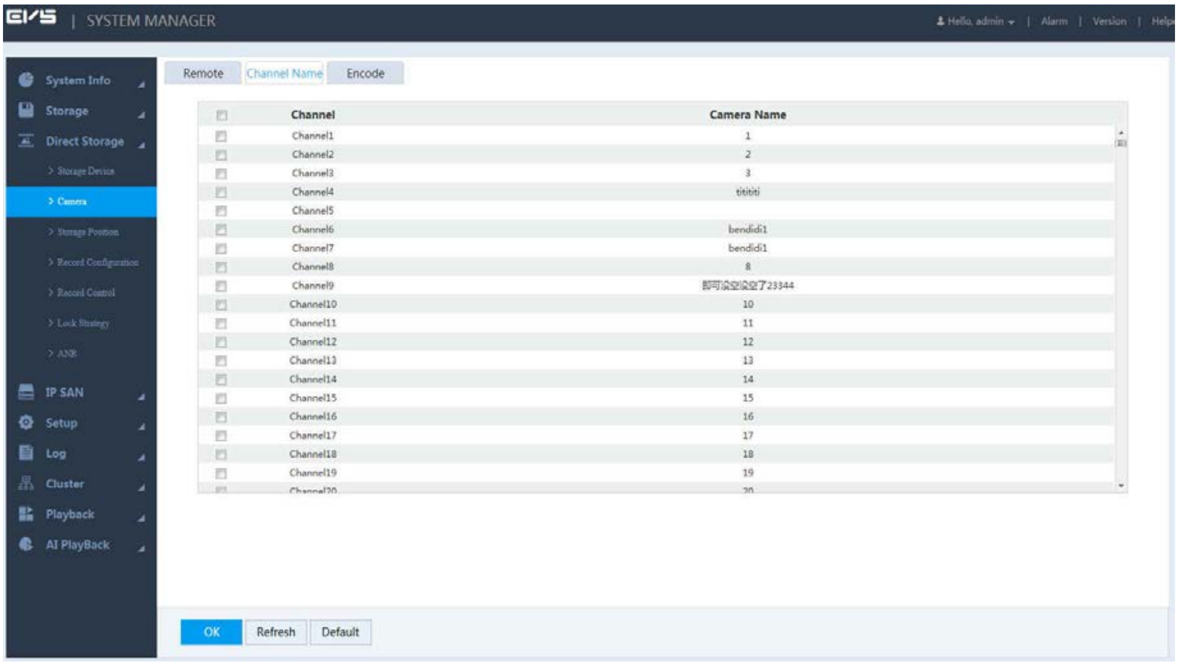
The system supports setting the channel name of remote device.

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

The **Channel Name** page is displayed.

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

Figure 3-64 Channel name



□	Channel	Camera Name
□	Channel1	1
□	Channel2	2
□	Channel3	3
□	Channel4	tititi
□	Channel5	
□	Channel6	bendidi1
□	Channel7	bendidi1
□	Channel8	8
□	Channel9	即可设空设空了23344
□	Channel10	10
□	Channel11	11
□	Channel12	12
□	Channel13	13
□	Channel14	14
□	Channel15	15
□	Channel16	16
□	Channel17	17
□	Channel18	18
□	Channel19	19
□	Channel20	20

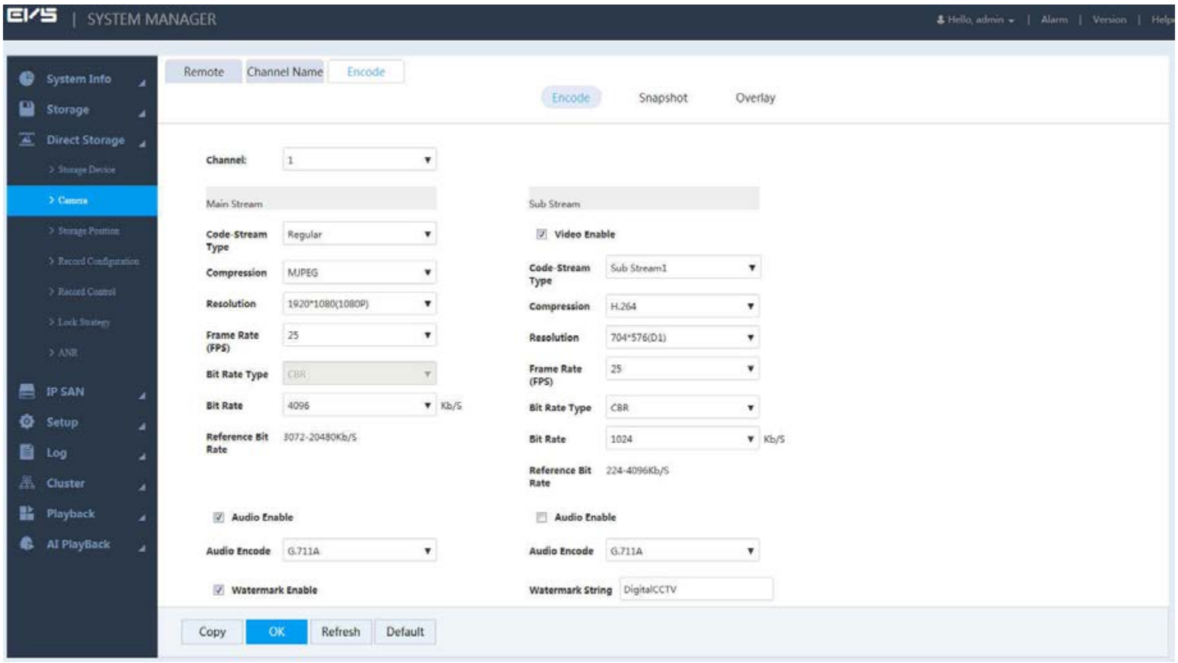
3.8.8 Setting Encoding Parameters

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**.

Figure 3-65 Encode



Channel: 1

Main Stream

Code-Stream Type: Regular

Compression: MJPEG

Resolution: 1920*1080(1080P)

Frame Rate (FPS): 25

Bit Rate Type: CBR

Bit Rate: 4096 Kb/S

Reference Bit Rate: 3072-20480Kb/S

☑ Audio Enable

Audio Encode: G.711A

☑ Watermark Enable

Sub Stream

☑ Video Enable

Code-Stream Type: Sub Stream1

Compression: H.264

Resolution: 704*576(D1)

Frame Rate (FPS): 25

Bit Rate Type: CBR

Bit Rate: 1024 Kb/S

Reference Bit Rate: 224-4096Kb/S

□ Audio Enable

Audio Encode: G.711A

Watermark String: DigitalCCTV

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** checkbox 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 checkbox, and then the record is a file that combines video and audio streams.
Audio Encoding	Select the audio encoding format.
Watermark Enable	Select the checkbox 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.

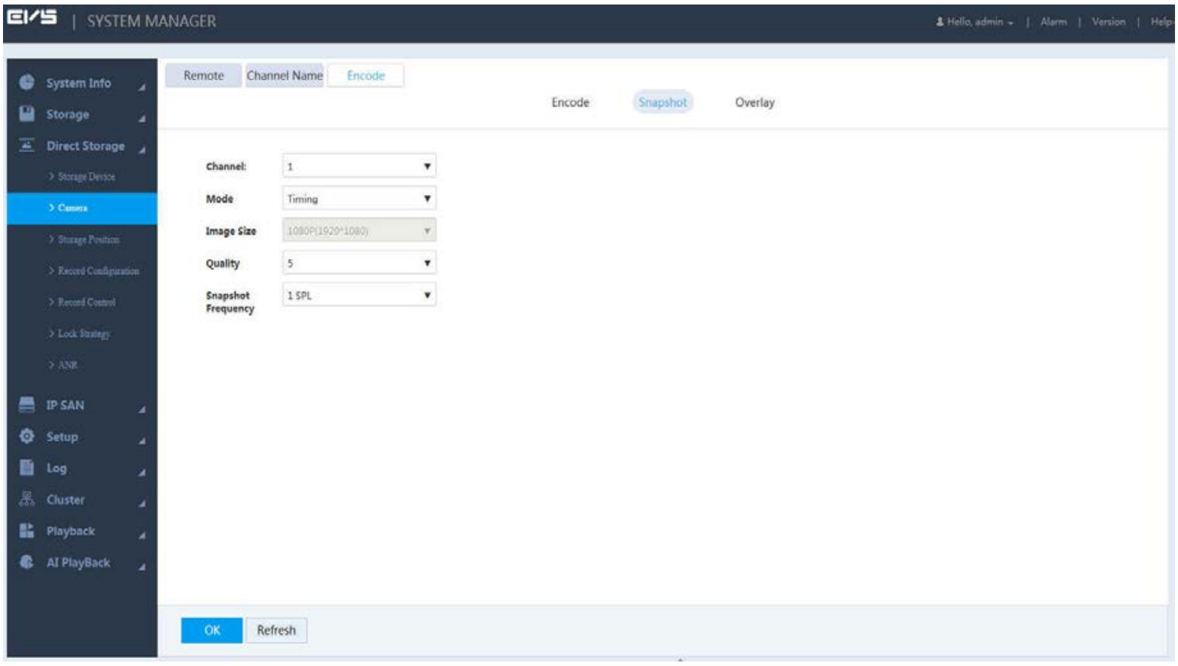
Step 3 Click **OK** to save the configuration.

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**.

Figure 3-66 Image stream



Channel: 1
Mode: Timing
Image Size: 1080P(1920*1080)
Quality: 5
Snapshot Frequency: 1 SPL

Step 2 Configure the parameters.

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.

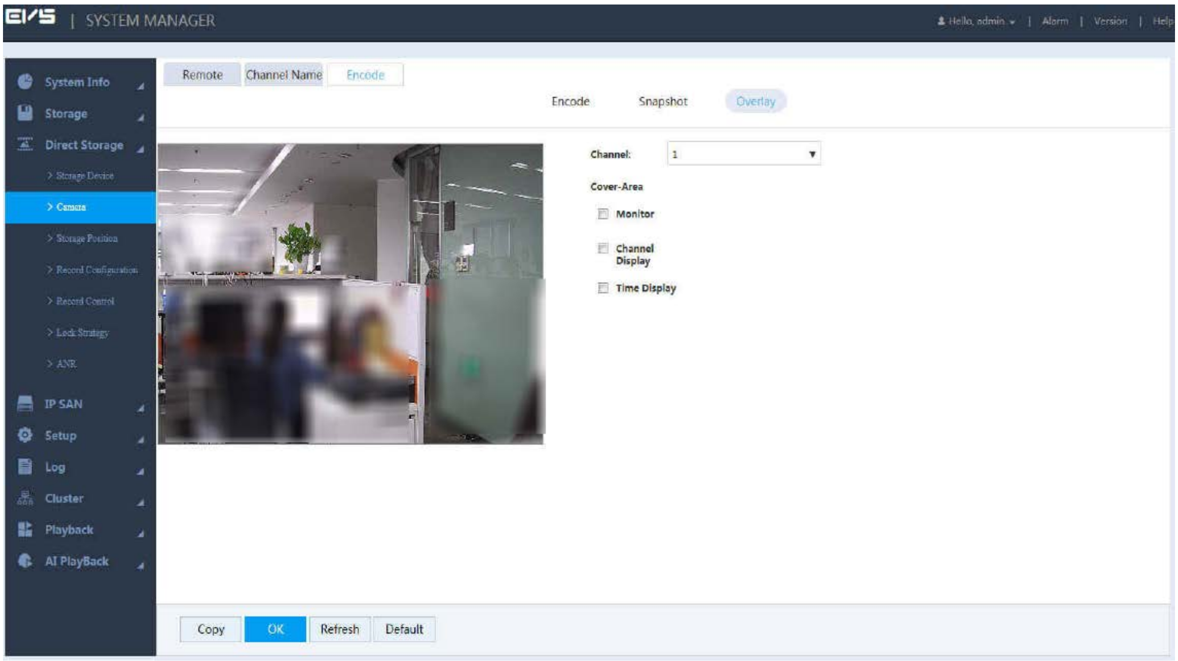
Step 3 Click **OK** to save the configuration.

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**.

Figure 3-67 Overlay



Channel: 1

Cover-Area

□ Monitor

□ Channel Display

□ Time Display

Step 2 Configure the parameters.

Table 3-18 Video overlay parameters

Parameter	Description
Channel	Select the channel number.

Parameter	Description
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** checkbox. 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	Displays the time or channel in the video screen. 1. Select **Channel Display** or **Time Display** checkbox. 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.
Time Display	

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

3.9 Configuring Events

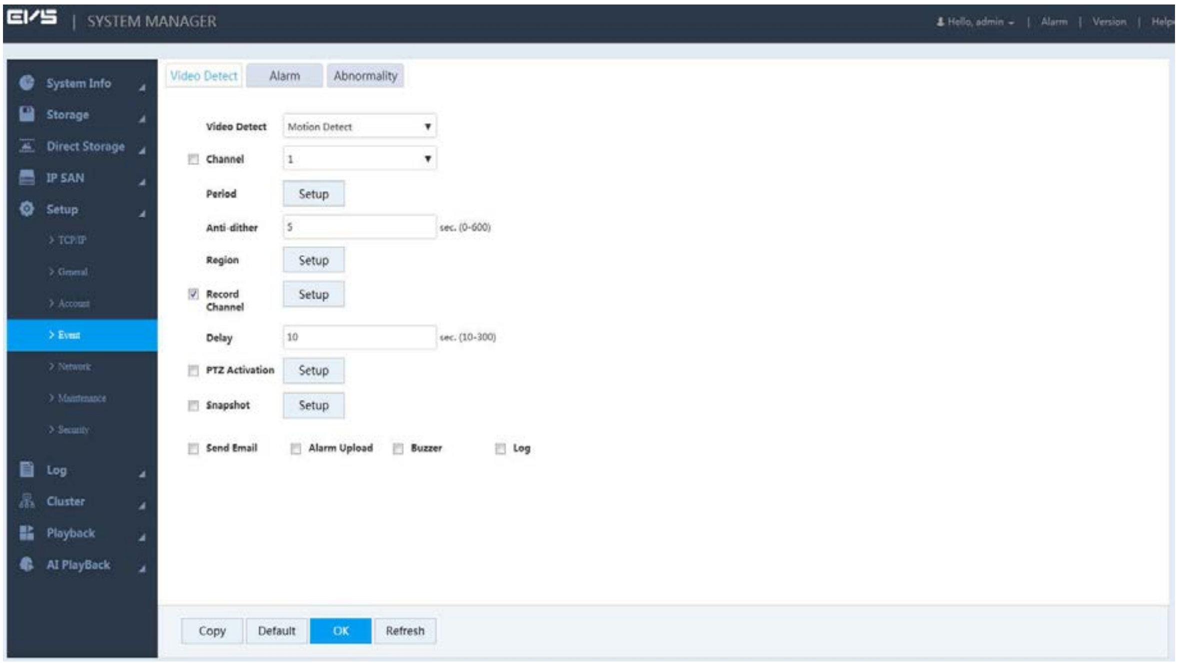
You can configure the linkages of video detection, alarm events, and abnormal events. When the alarm is triggered, the Device automatically performs the pre-set linked actions.

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**.

Figure 3-68 Video detect



Video Detect: Motion Detect

□ Channel: 1

Period: Setup

Anti-dither: 5 sec. (0-600)

Region: Setup

☑ Record Channel: Setup

Delay: 10 sec. (10-300)

□ PTZ Activation: Setup

□ Snapshot: Setup

□ Send Email □ Alarm Upload □ Buzzer □ Log

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.

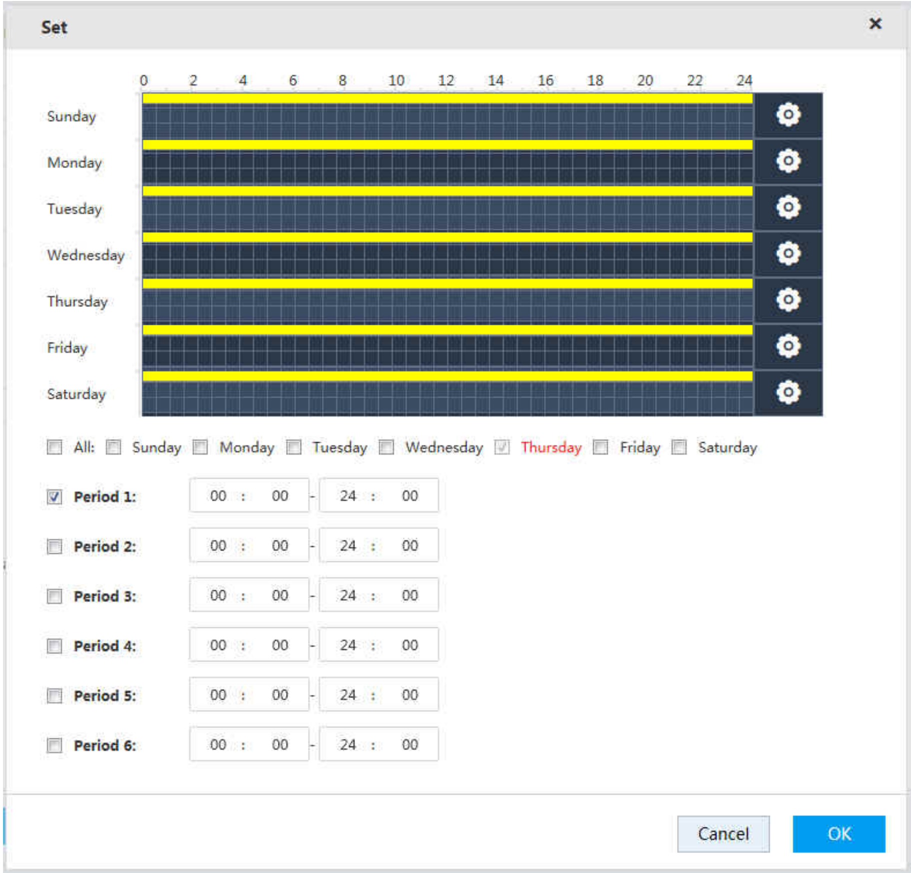
Step 3 Select the checkbox at the left side of **Channel**, and choose the channel number to enable video detection function.

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 page is displayed.

Figure 3-69 Period setup



□ All: □ Sunday □ Monday □ Tuesday □ Wednesday ☑ Thursday □ Friday □ Saturday

☑ **Period 1:** 00 : 00 - 24 : 00

□ **Period 2:** 00 : 00 - 24 : 00

□ **Period 3:** 00 : 00 - 24 : 00

□ **Period 4:** 00 : 00 - 24 : 00

□ **Period 5:** 00 : 00 - 24 : 00

□ **Period 6:** 00 : 00 - 24 : 00

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 checkbox of the corresponding period, and then enter the time value. Six periods are available for each day.

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

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

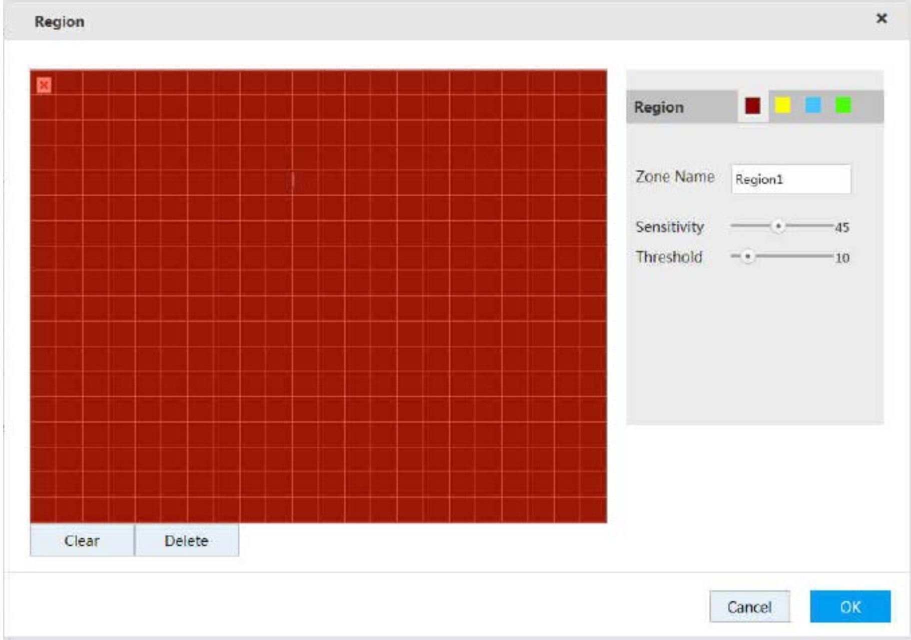
Step 5 Set the video detect region.

Only **Motion Detect** supports this function.

1) Click **Setup** at the right side of **Region**.

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

Figure 3-70 Region



Zone Name: Region1

Sensitivity: 45

Threshold: 10

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

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

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.

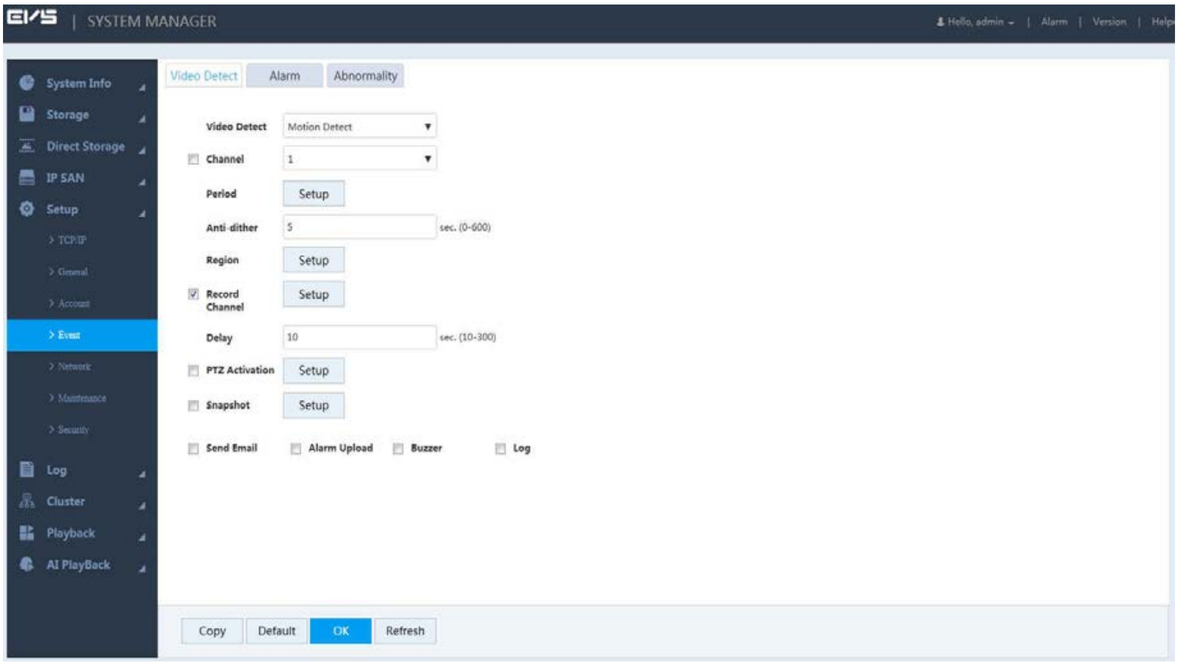
Table 3-19 Region setting parameters

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.

Figure 3-71 Video detect



Video Detect: Motion Detect

□ Channel: 1

Period: Setup

Anti-dither: 5 sec. (0-600)

Region: Setup

☑ Record Channel: Setup

Delay: 10 sec. (10-300)

□ PTZ Activation: Setup

□ Snapshot: Setup

□ Send Email □ Alarm Upload □ Buzzer □ Log

Table 3-20 Video detect parameters

Parameter	Description
Period	Alarm linkage works only in the set time period.
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 checkbox, 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 checkbox, 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".
Snapshot	Select the checkbox, 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".

Parameter	Description
Send Email	Select the checkbox 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 checkbox. 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 checkbox. The buzzer bleats when an alarm occurs.
Log	Select the checkbox. When an alarm occurs, the Device records the alarm information and saves it to the log.

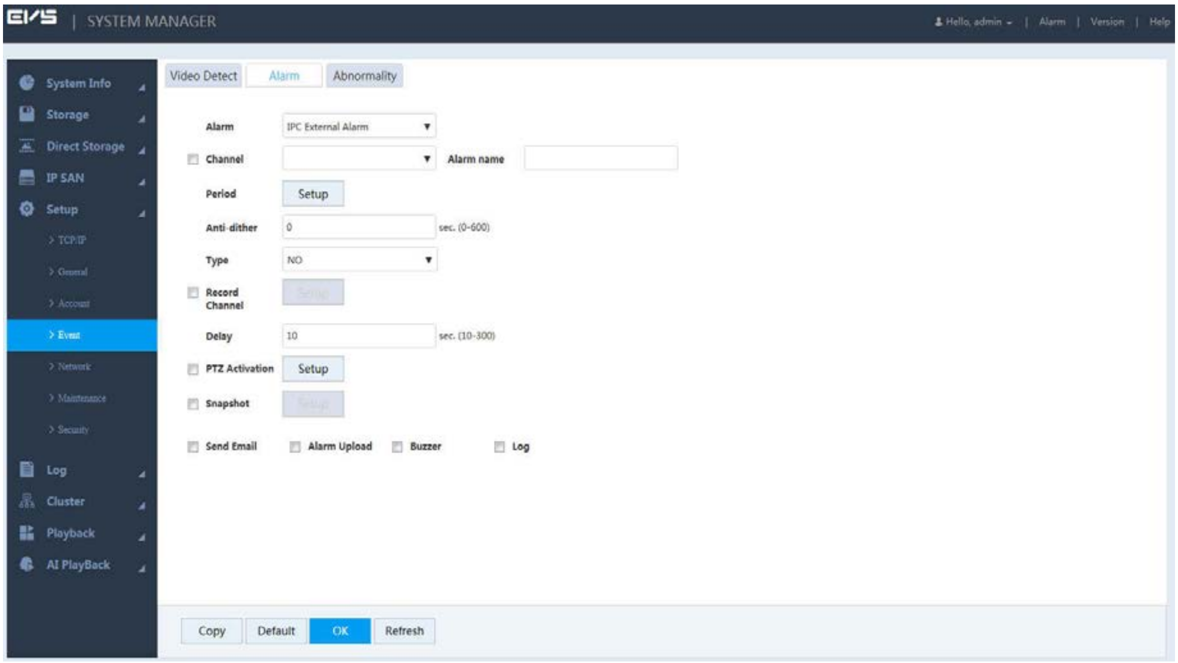
Step 7 Click **OK** to save the configuration.

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**.

Figure 3-72 Set alarm



Alarm: IPC External Alarm

□ Channel: Alarm name:

Period: Setup

Anti-dither: 0 sec. (0-600)

Type: NO

□ Record Channel: Setup

Delay: 10 sec. (10-300)

□ PTZ Activation: Setup

□ Snapshot: Setup

□ Send Email □ Alarm Upload □ Buzzer □ Log

Step 2 Configure the parameters.

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.

Parameter	Description
Channel	Select the checkbox, 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 checkbox, 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 checkbox, 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 checkbox, 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 checkbox 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 checkbox. When an alarm occurs, the device uploads the alarm signal to **Alarm** at the top right of the web interface. Only some models support this function. See the actual device.
Buzzer	Select the checkbox. The buzzer bleats when an alarm occurs.
Log	Select the checkbox. When an alarm occurs, the Device records the alarm information and saves it to the log.

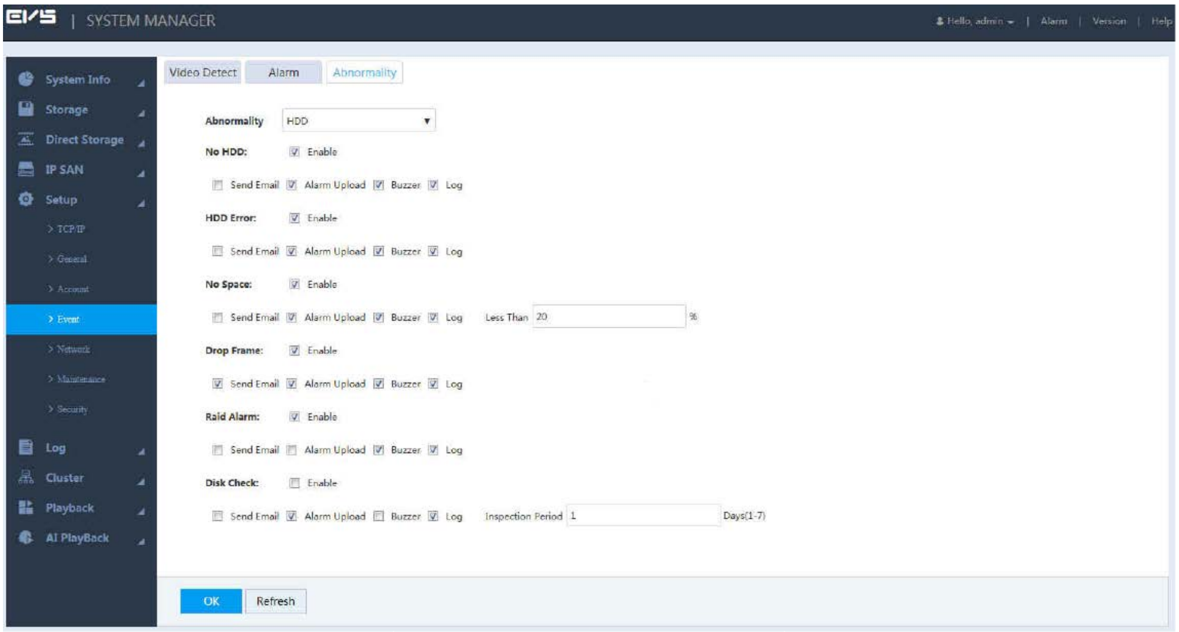
Step 3 Click **OK** to save the configuration.

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**.

Figure 3-73 Abnormality handling



Abnormality: HDD

No HDD: ☑ Enable

☐ Send Email ☑ Alarm Upload ☑ Buzzer ☑ Log

HDD Error: ☑ Enable

☐ Send Email ☑ Alarm Upload ☑ Buzzer ☑ Log

No Space: ☑ Enable

☐ Send Email ☑ Alarm Upload ☑ Buzzer ☑ Log Less Than 20 %

Drop Frame: ☑ Enable

☑ Send Email ☑ Alarm Upload ☑ Buzzer ☑ Log

Raid Alarm: ☑ Enable

☐ Send Email ☐ Alarm Upload ☑ Buzzer ☑ Log

Disk Check: ☐ Enable

☐ Send Email ☑ Alarm Upload ☐ Buzzer ☑ Log Inspection Period 1 Days(1-7)

Step 2 Configure the parameters.

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 checkbox to enable the corresponding abnormal event.
Send Email	Select the checkbox 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".

Parameter	Description
Alarm Upload	Select the checkbox. When an alarm occurs, the device uploads the alarm signal to **Alarm** at the top right of the web interface. 📖 Only some models support this function. See the actual device.
Buzzer	Select the checkbox. The buzzer bleats when an alarm occurs.
Log	Select the checkbox. 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 checkbox 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 checkbox 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 checkbox 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** page is displayed.

Figure 3-74 Real-time monitoring

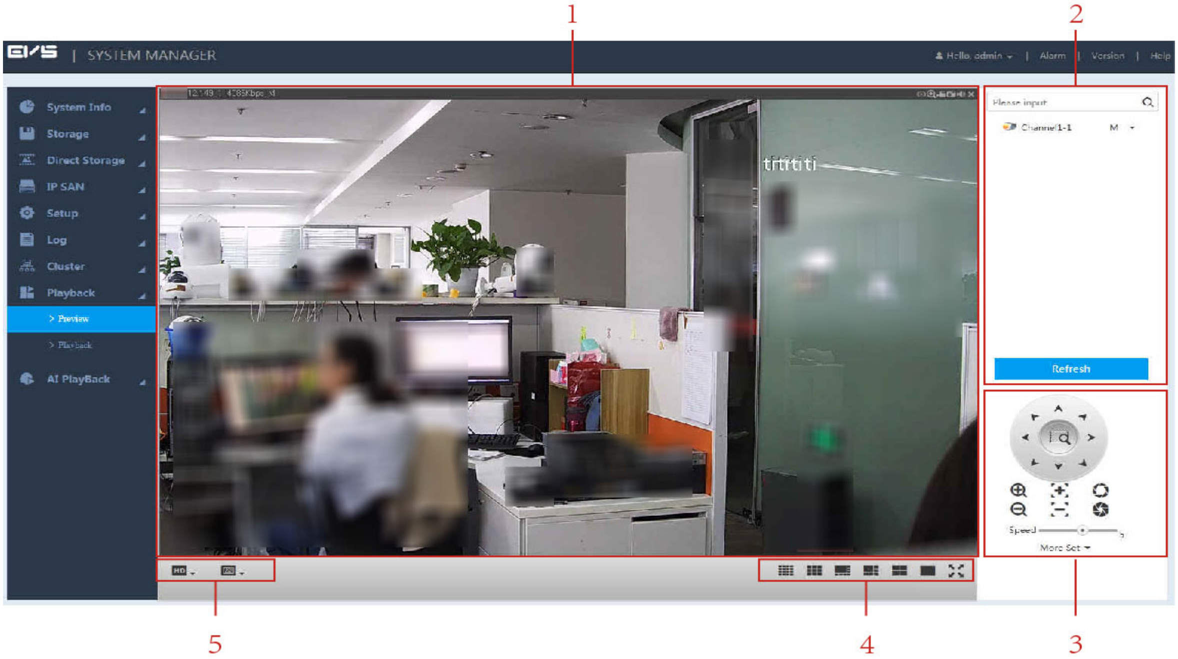


Table 3-23 Real-time monitoring

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.

- 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

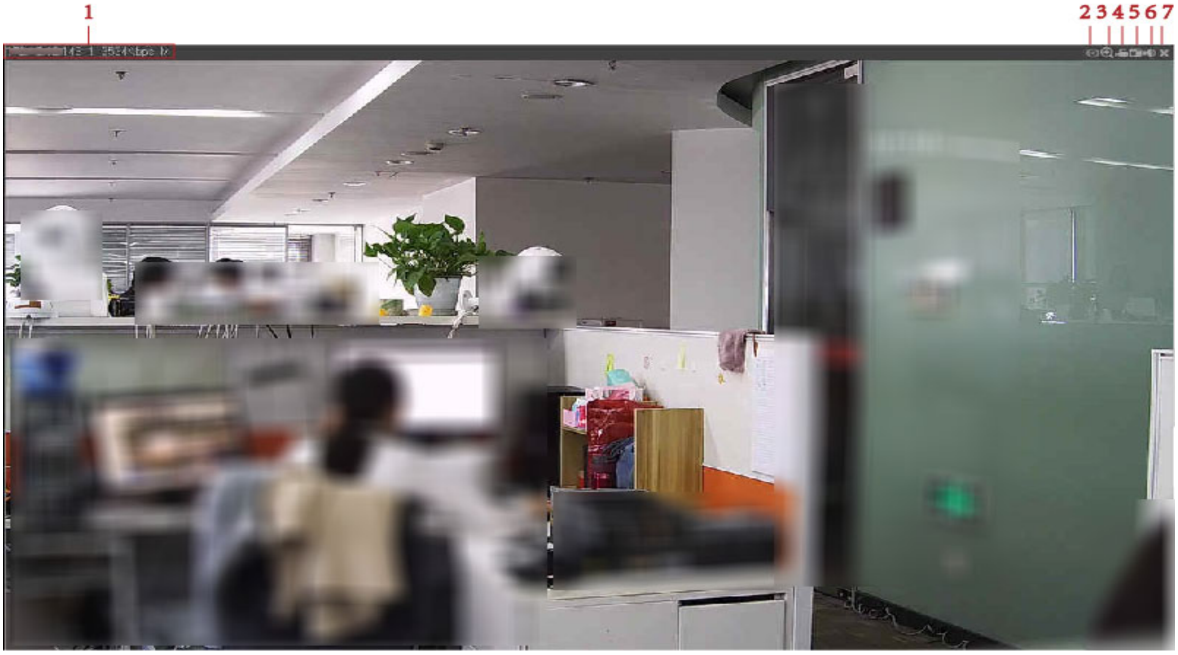


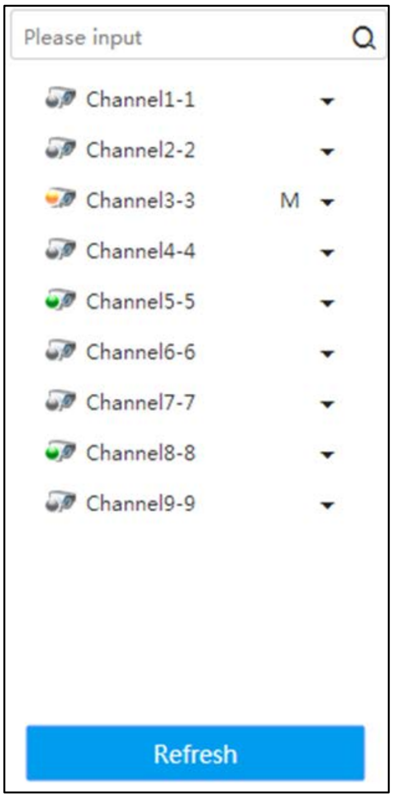
Table 3-24 Real-time monitoring window icons

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.

Figure 3-76 Monitoring channel list



Please input

Channel1-1

Channel2-2

Channel3-3 M

Channel4-4

Channel5-5

Channel6-6

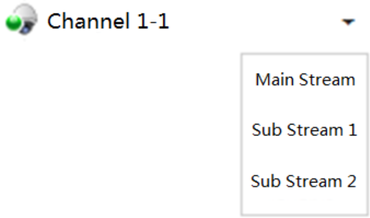
Channel7-7

Channel8-8

Channel9-9

Refresh

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.
 Channel 1-1 Main Stream Sub Stream 1 Sub Stream 2	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.

- 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.

Figure 3-77 PTZ console

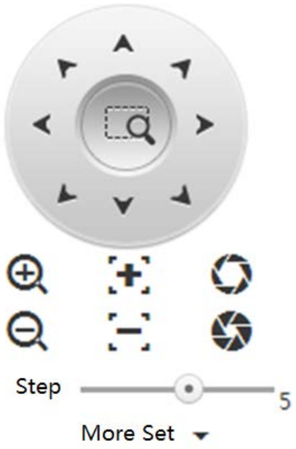


Table 3-26 PTZ parameters

No.	Parameter	Description
1	Preset	Set the preset points of the camera including details, add and delete. ● Add preset Turn the camera to the needed position, enter preset value in the **Preset** text box, and then click **Add** to add the preset point. ● Set value Enter the preset value in the **Preset** text box and click **Details**. The camera automatically turns to the preset position. ● Delete preset Enter the preset value in the **Preset** text box and click **Del** to delete this preset point.

No.	Parameter	Description
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** page, 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** page, enter the value of tour path and click **Del** to delete this tour path. ● Start On the **Tour** page, 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 home page, such as zoom, focus, iris and direction. Return to the pattern page 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.
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 RS-485. 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.

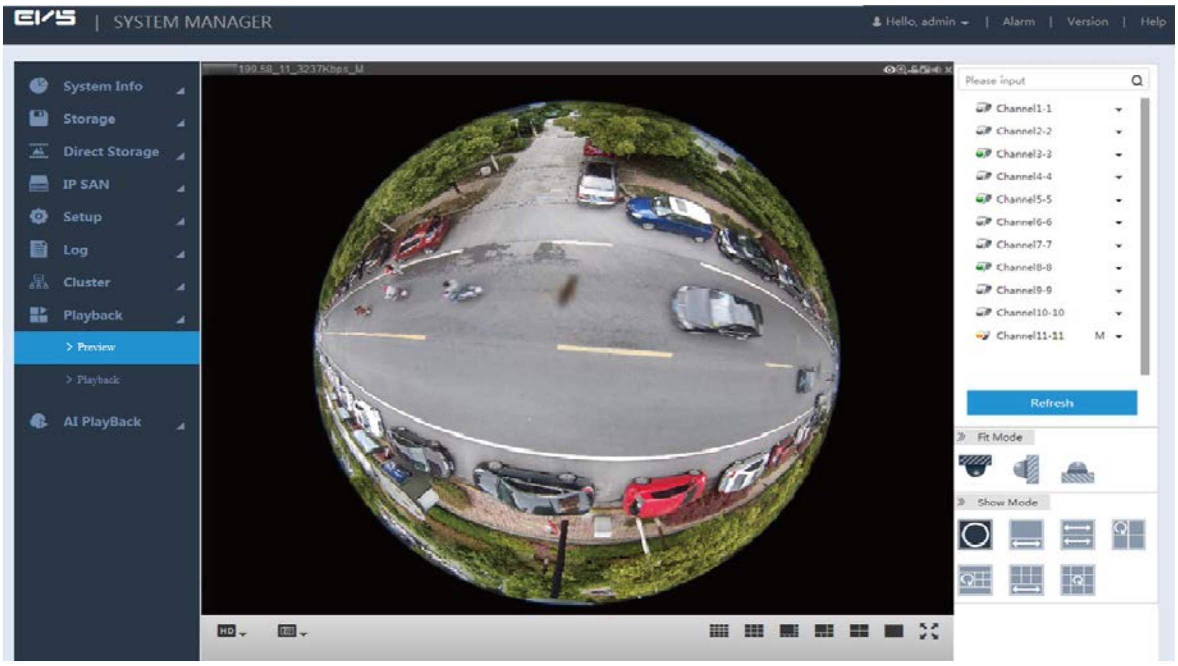
3.10.4 Fisheye

After opening the real-time monitoring screen, click on the upper right corner of the window. The **Fisheye** page is displayed.

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 mode.

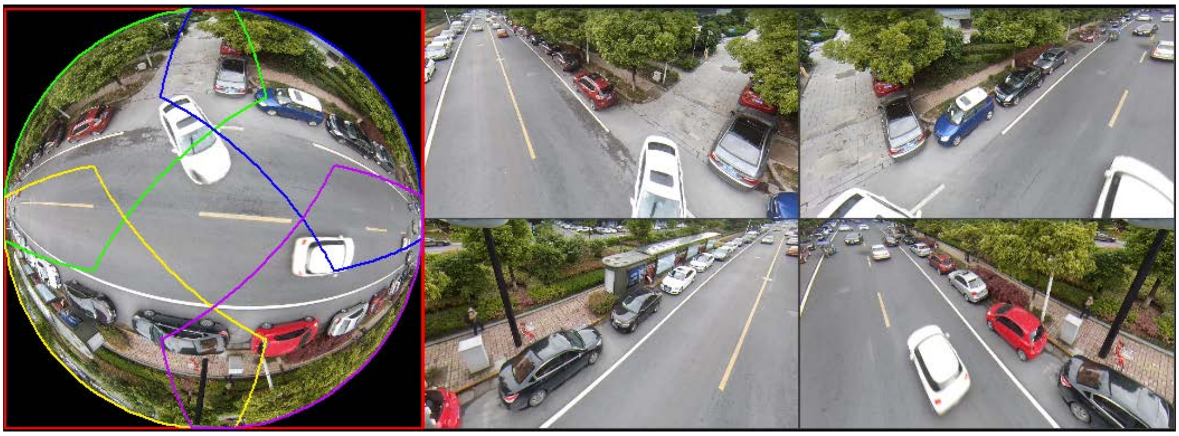
Table 3-27 Fisheye mounting modes

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

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**.

Figure 3-80 Playback

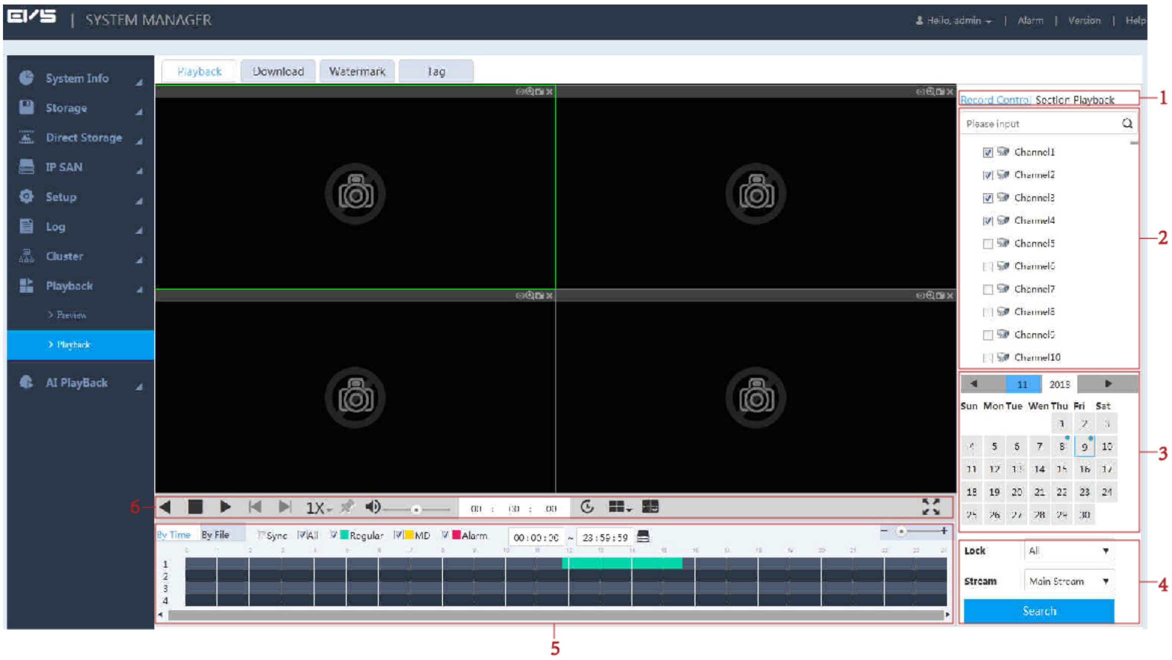


Table 3-28 Playback parameters

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".

No.	Name	Description
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** page.

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

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

Figure 3-81 Display by time

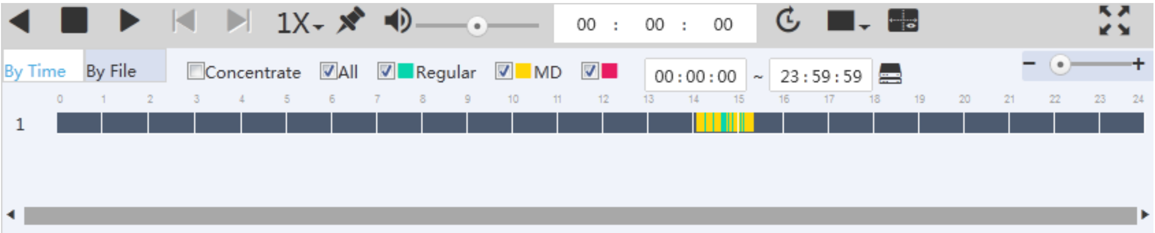
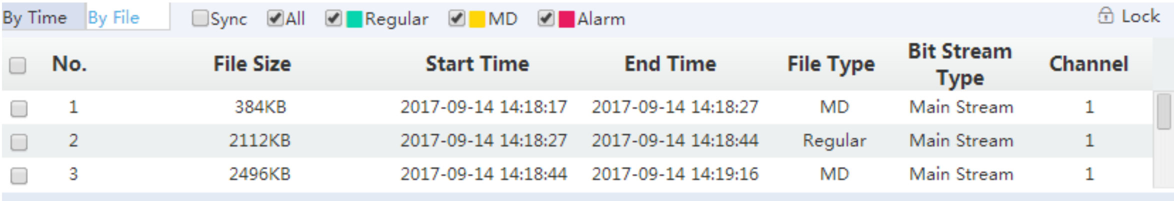


Figure 3-82 Display by file



☐	No.	File Size	Start Time	End Time	File Type	Bit Stream Type	Channel
☐	1	384KB	2017-09-14 14:18:17	2017-09-14 14:18:27	MD	Main Stream	1
☐	2	2112KB	2017-09-14 14:18:27	2017-09-14 14:18:44	Regular	Main Stream	1
☐	3	2496KB	2017-09-14 14:18:44	2017-09-14 14:19:16	MD	Main Stream	1

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 checkbox and only the corresponding record files are displayed.

Icon	Description
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.
🔒 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.

Figure 3-83 Record playback control bar

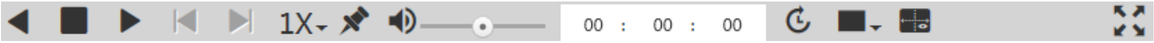


Table 3-31 Icons on the record playback control bar

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×.

Icon	Description
📌	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.
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 page 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.

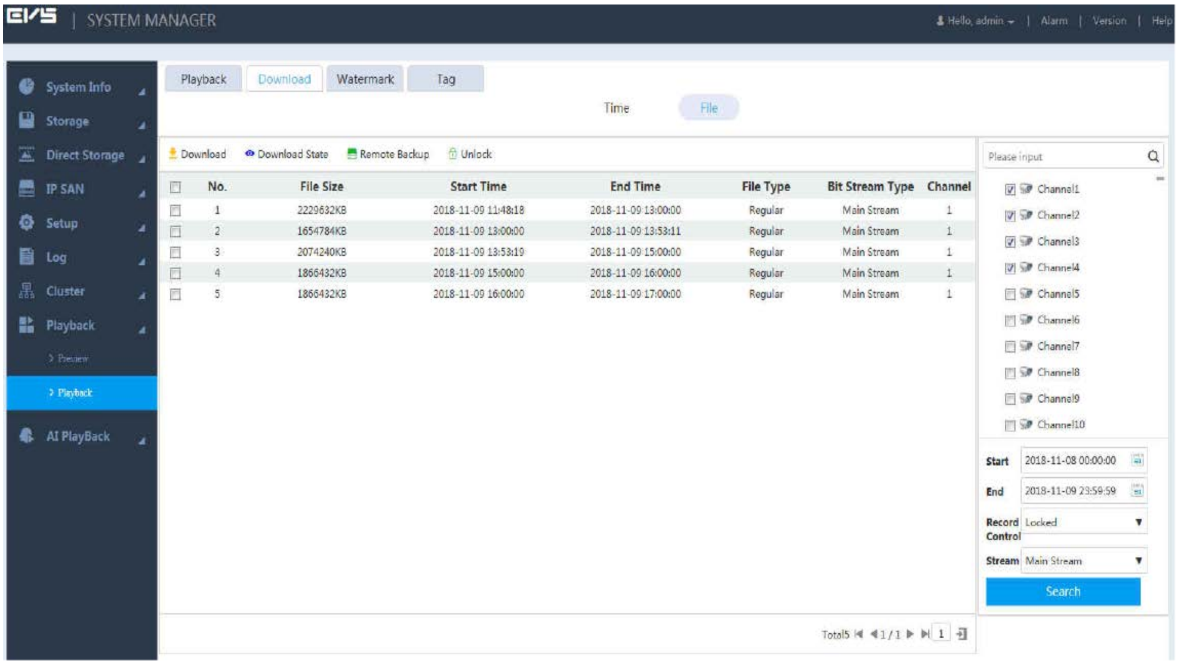
3.11.1.4 Locking and Unlocking Files

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**.

Figure 3-84 Files to unlock



□	No.	File Size	Start Time	End Time	File Type	Bit Stream Type	Channel
□	1	2229632KB	2018-11-09 11:48:18	2018-11-09 13:00:00	Regular	Main Stream	1
□	2	1654784KB	2018-11-09 13:00:00	2018-11-09 13:53:11	Regular	Main Stream	1
□	3	2074240KB	2018-11-09 13:53:19	2018-11-09 15:00:00	Regular	Main Stream	1
□	4	1866432KB	2018-11-09 15:00:00	2018-11-09 16:00:00	Regular	Main Stream	1
□	5	1866432KB	2018-11-09 16:00:00	2018-11-09 17:00:00	Regular	Main Stream	1

☑ Channel1
☑ Channel2
☑ Channel3
☑ Channel4
□ Channel5
□ Channel6
□ Channel7
□ Channel8
□ Channel9
□ Channel10

Start 2018-11-08 00:00:00
End 2018-11-09 23:59:59
Record Control Locked
Stream Main Stream

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

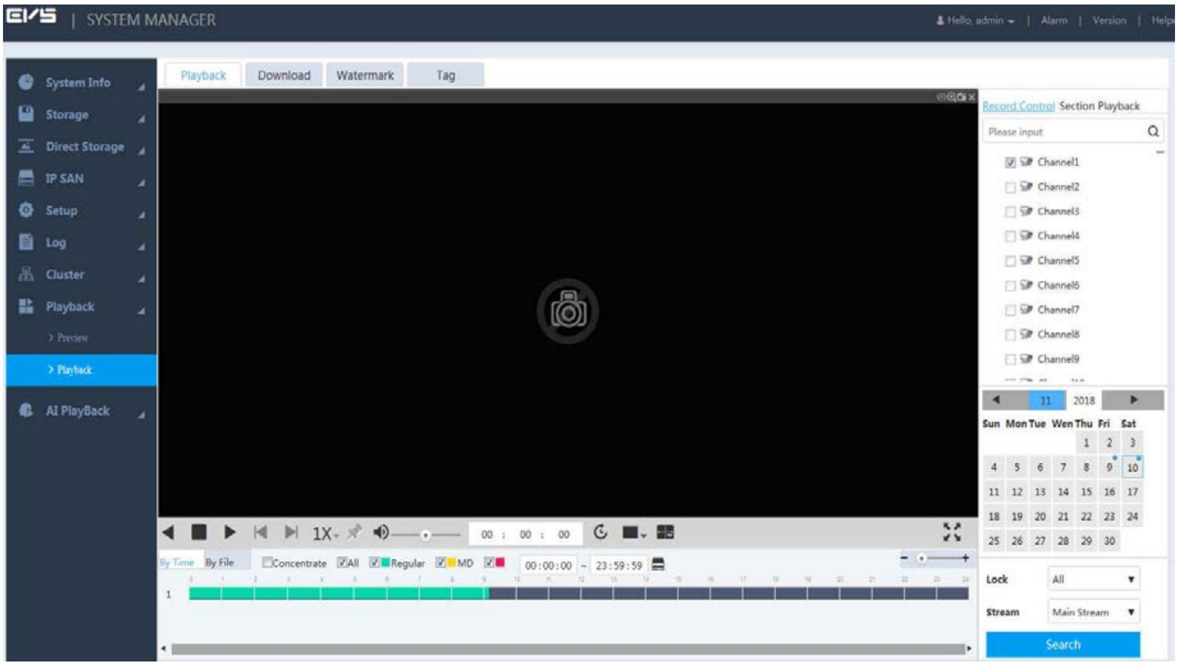
3.11.1.5 Concentrated Playback

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**.

Figure 3-85 Playback



☑ Channel1
□ Channel2
□ Channel3
□ Channel4
□ Channel5
□ Channel6
□ Channel7
□ Channel8
□ Channel9

Lock All
Stream Main Stream

Step 2 On the **Playback** page, 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

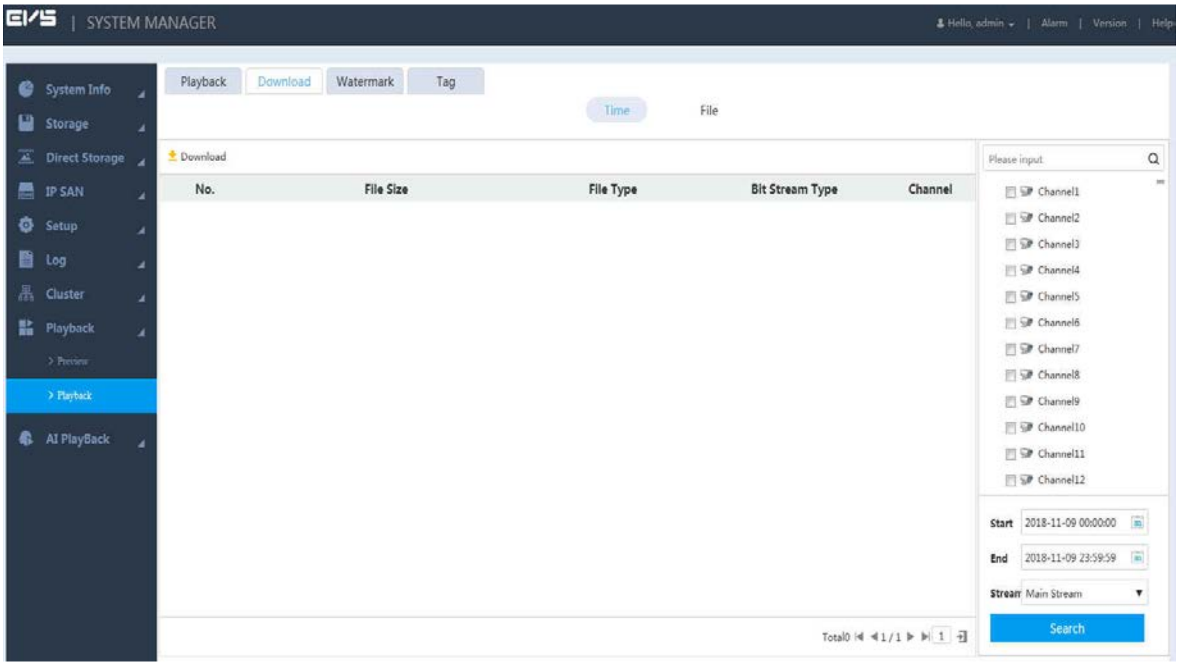
The system supports downloading record by file or by time and stores it to PC or external USB.

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**.

Figure 3-86 Time



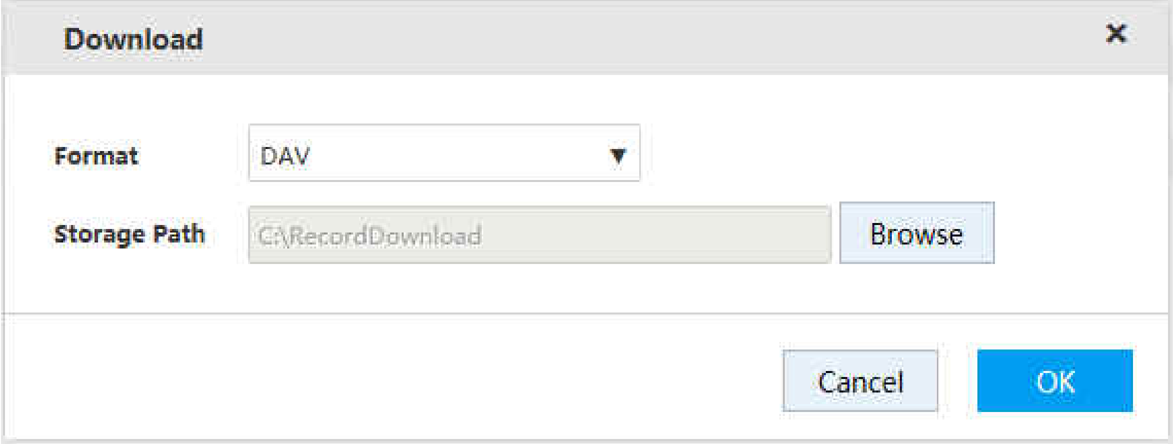
Step 2 Select **Channel**, and configure **Start**, **End** and **Stream**.

Step 3 Click **Search**.

The record files meeting the conditions are displayed.

Step 4 Select the file and click ⬇ .

Figure 3-87 Download


Download

Format: DAV

Storage Path: C:\RecordDownload

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**.

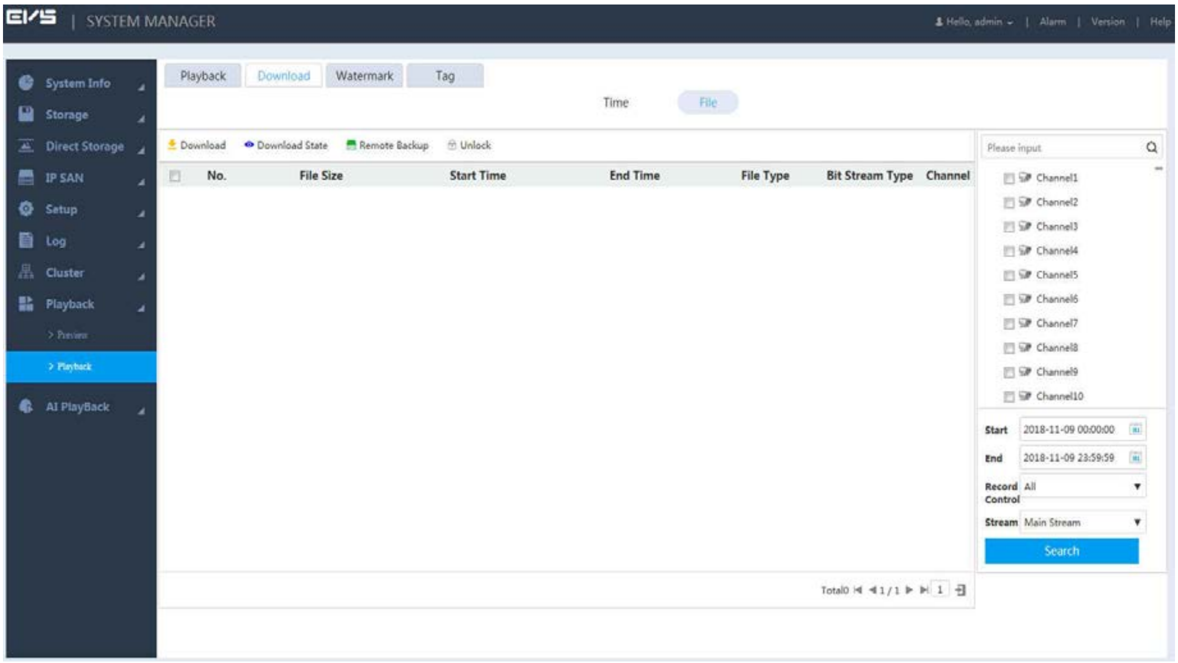
The system starts to download the record file.

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**.

Figure 3-88 File


□	No.	File Size	Start Time	End Time	File Type	Bit Stream Type	Channel

□ Channel1
□ Channel2
□ Channel3
□ Channel4
□ Channel5
□ Channel6
□ Channel7
□ Channel8
□ Channel9
□ Channel10

Start: 2018-11-09 00:00:00

End: 2018-11-09 23:59:59

Record Control: All

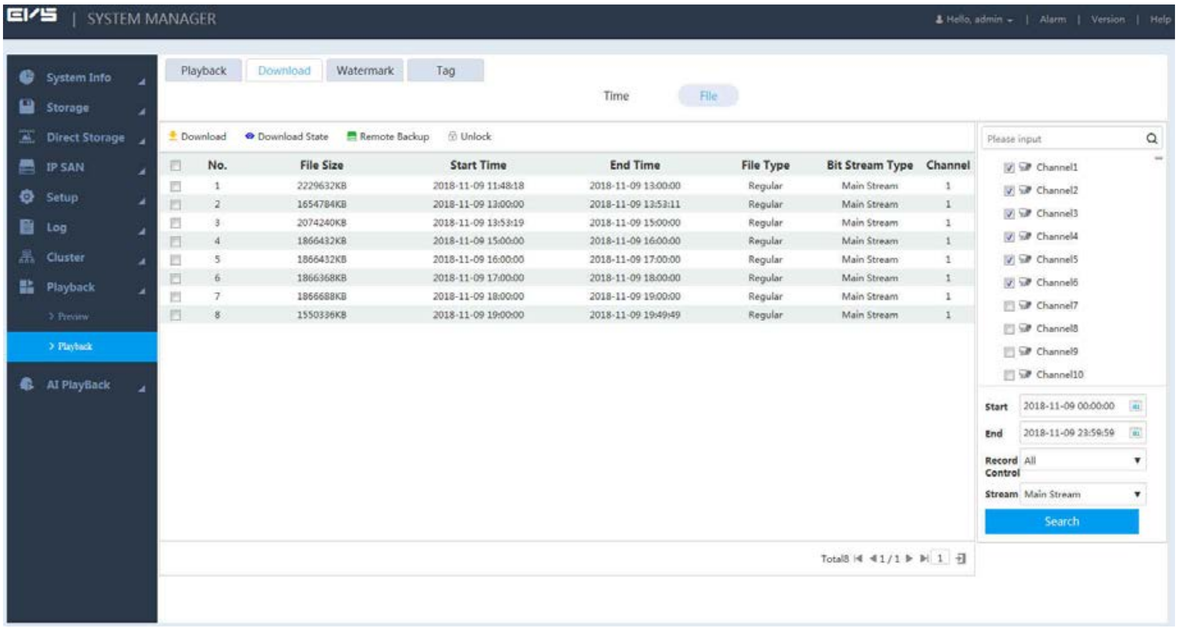
Stream: Main Stream

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



□	No.	File Size	Start Time	End Time	File Type	Bit Stream Type	Channel
□	1	2229632KB	2018-11-09 11:48:18	2018-11-09 13:00:00	Regular	Main Stream	1
□	2	1654784KB	2018-11-09 13:00:00	2018-11-09 13:53:11	Regular	Main Stream	1
□	3	2074240KB	2018-11-09 13:53:19	2018-11-09 15:00:00	Regular	Main Stream	1
□	4	1866432KB	2018-11-09 15:00:00	2018-11-09 16:00:00	Regular	Main Stream	1
□	5	1866432KB	2018-11-09 16:00:00	2018-11-09 17:00:00	Regular	Main Stream	1
□	6	1866368KB	2018-11-09 17:00:00	2018-11-09 18:00:00	Regular	Main Stream	1
□	7	1866688KB	2018-11-09 18:00:00	2018-11-09 19:00:00	Regular	Main Stream	1
□	8	1550336KB	2018-11-09 19:00:00	2018-11-09 19:49:49	Regular	Main Stream	1

- ☑ Channel1
- ☑ Channel2
- ☑ Channel3
- ☑ Channel4
- ☑ Channel5
- ☑ Channel6
- □ Channel7
- □ Channel8
- □ Channel9
- □ Channel10

Start 2018-11-09 00:00:00

End 2018-11-09 23:59:59

Record Control All

Stream Main Stream

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

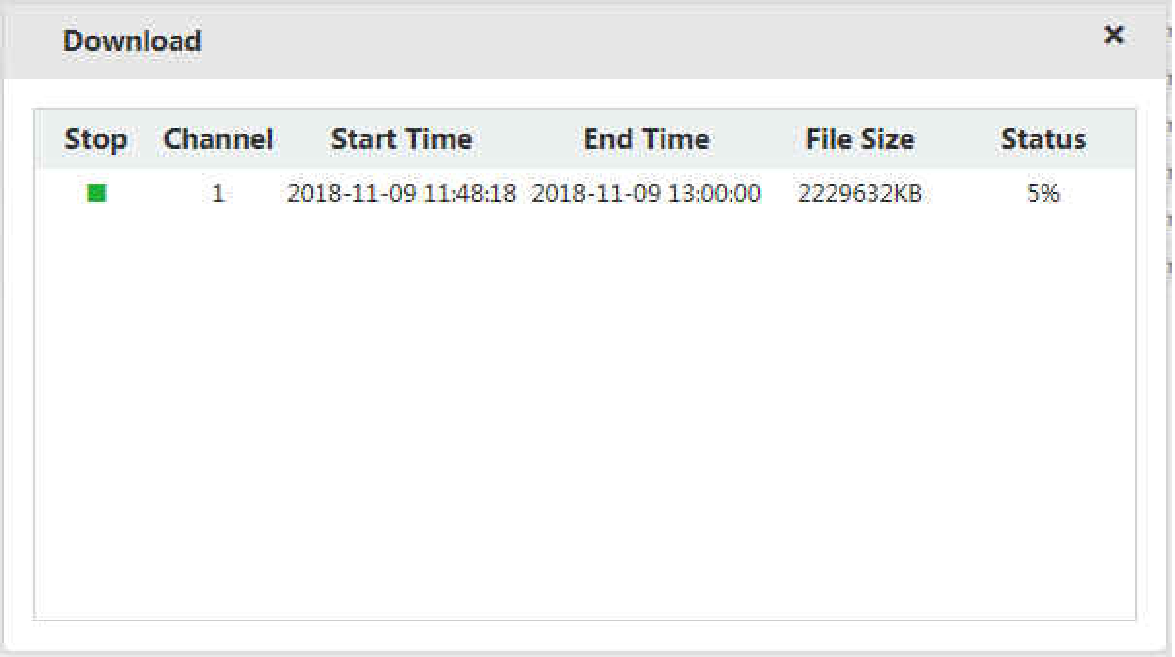
  Connect the USB to the USB port of PC, select the record, and then click 🟩. The system starts to back up the file to external USB device.

Step 5 (Optional) Click 👁.

You can view the download progress.

Click 🟩 to stop download.

Figure 3-90 Download



Stop	Channel	Start Time	End Time	File Size	Status
🟩	1	2018-11-09 11:48:18	2018-11-09 13:00:00	2229632KB	5%

3.11.3 Record Verification

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

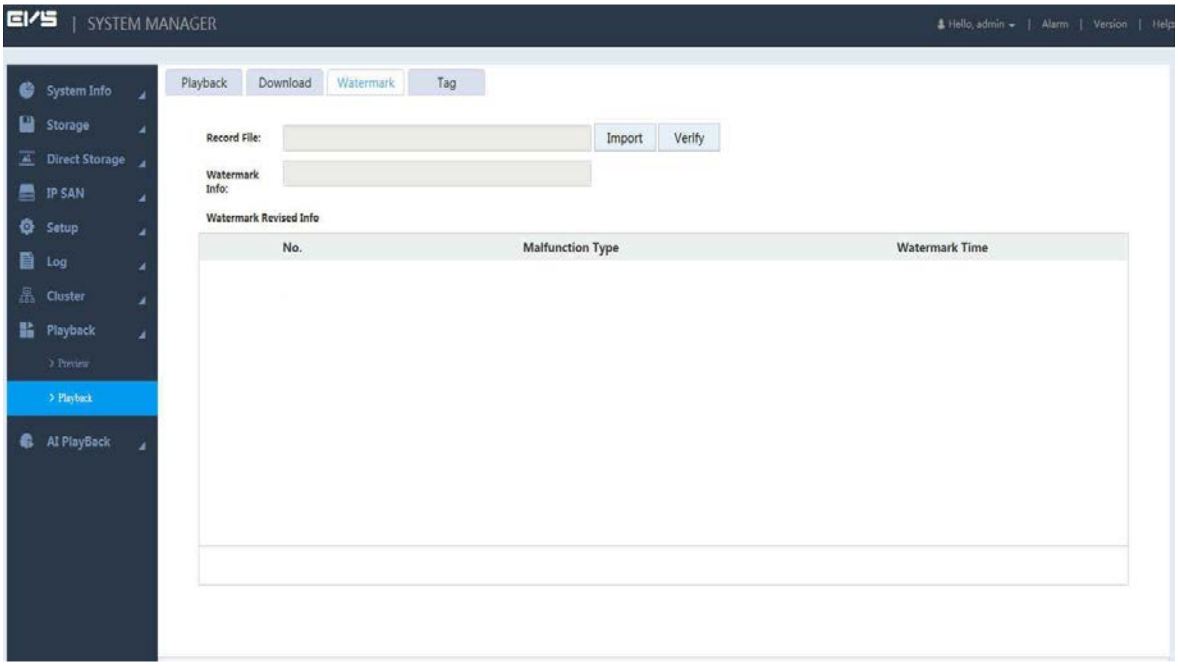
Preparation

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

Procedure

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

Figure 3-91 Watermark verification



Record File:

Watermark Info:

Watermark Revised Info

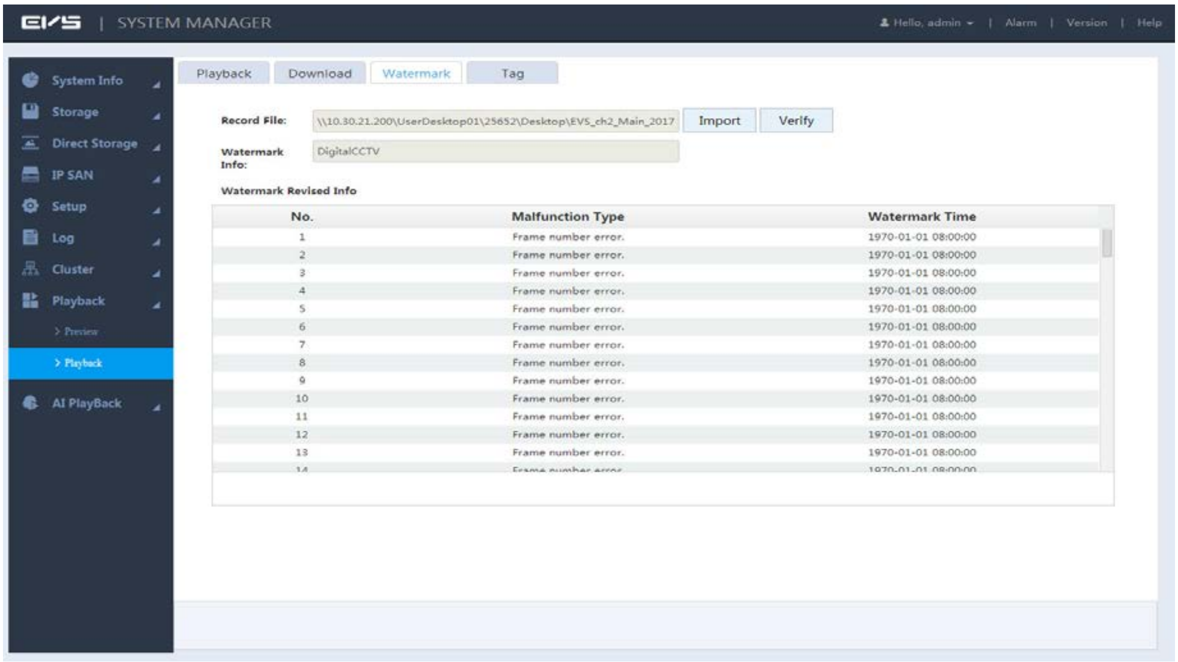
No.	Malfunction Type	Watermark Time

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.

Figure 3-92 Verification results



Record File: \\10.30.21.200\UserDesktop01\25652\Desktop\EVS_ch2_Main_2017

Watermark Info: DigitalCCTV

Watermark Revised Info

No.	Malfunction Type	Watermark Time
1	Frame number error.	1970-01-01 08:00:00
2	Frame number error.	1970-01-01 08:00:00
3	Frame number error.	1970-01-01 08:00:00
4	Frame number error.	1970-01-01 08:00:00
5	Frame number error.	1970-01-01 08:00:00
6	Frame number error.	1970-01-01 08:00:00
7	Frame number error.	1970-01-01 08:00:00
8	Frame number error.	1970-01-01 08:00:00
9	Frame number error.	1970-01-01 08:00:00
10	Frame number error.	1970-01-01 08:00:00
11	Frame number error.	1970-01-01 08:00:00
12	Frame number error.	1970-01-01 08:00:00
13	Frame number error.	1970-01-01 08:00:00
14	Frame number error.	1970-01-01 08:00:00

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.

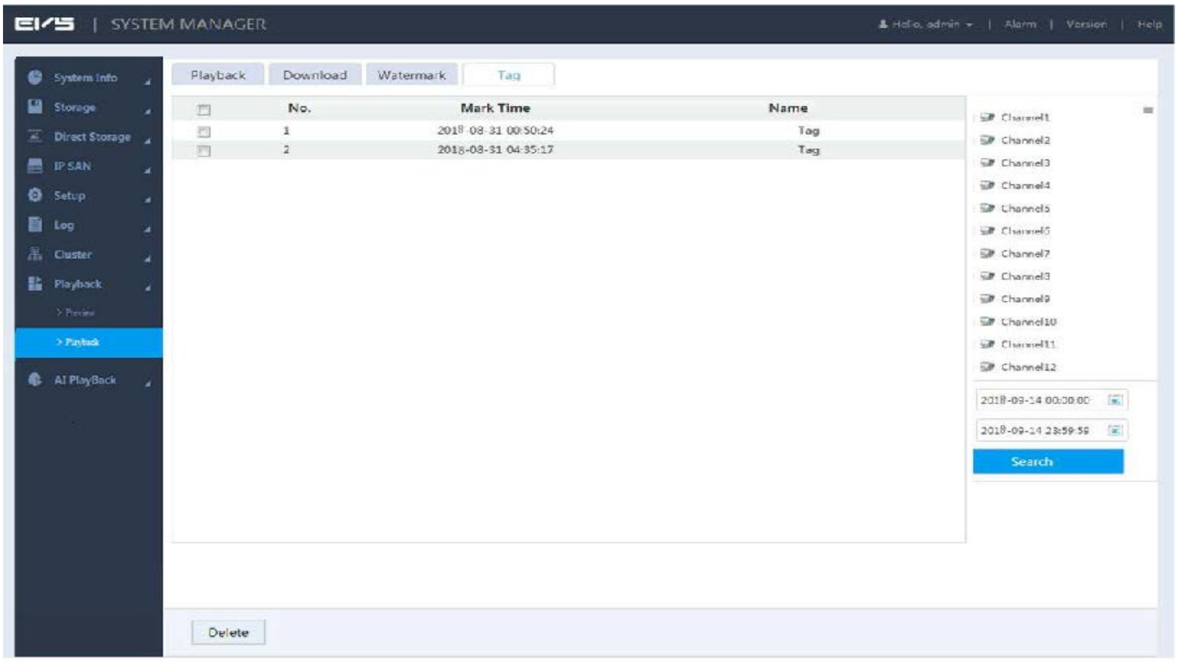
Step 1 Select **Playback** > **Playback** > **Tag**.

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

Step 3 Click **Search**.

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

Figure 3-93 Tag management



□	No.	Mark Time	Name
□	1	2018-08-31 00:50:24	Tag
□	2	2018-08-31 04:35:17	Tag

2018-09-14 00:00:00

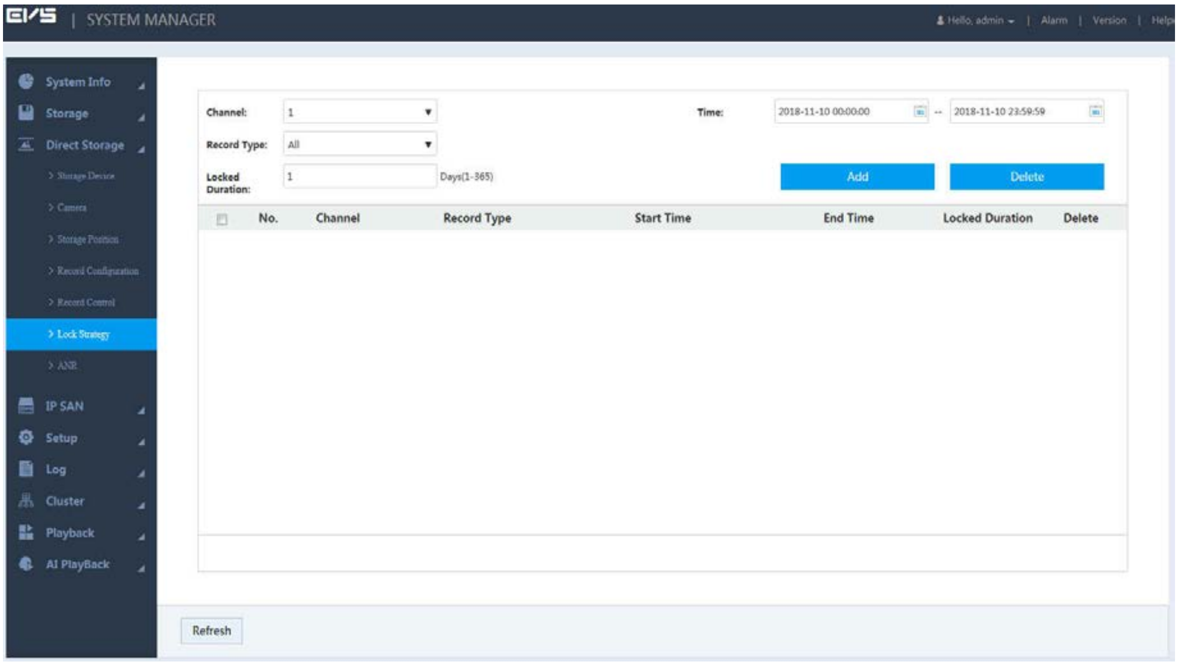
2018-09-14 23:59:59

3.11.5 Setting Lock Strategy

Lock the video record to prevent it from being deleted.

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

Figure 3-94 Lock strategy



Channel: 1

Record Type: All

Locked Duration: 1 Days(1-365)

Time: 2018-11-10 00:00:00 -- 2018-11-10 23:59:59

□	No.	Channel	Record Type	Start Time	End Time	Locked Duration	Delete

Step 2 Configure parameters.

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.

Parameter	Description
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.

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.

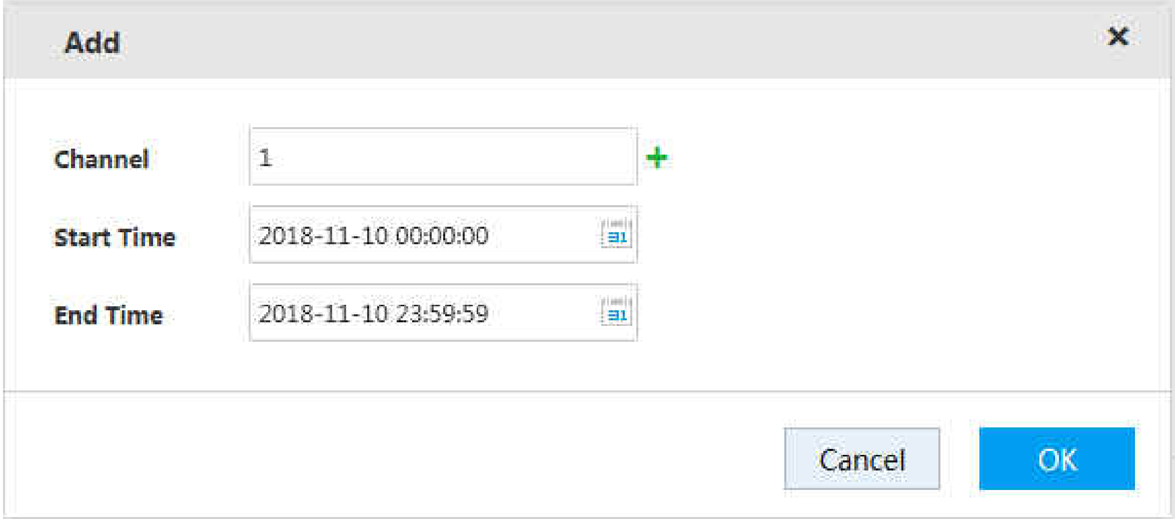
Two ANR modes are available: Automatic and Manual.

- 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 download 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.

Figure 3-95 Adding backup record



Add

Channel: 1

Start Time: 2018-11-10 00:00:00

End Time: 2018-11-10 23:59:59

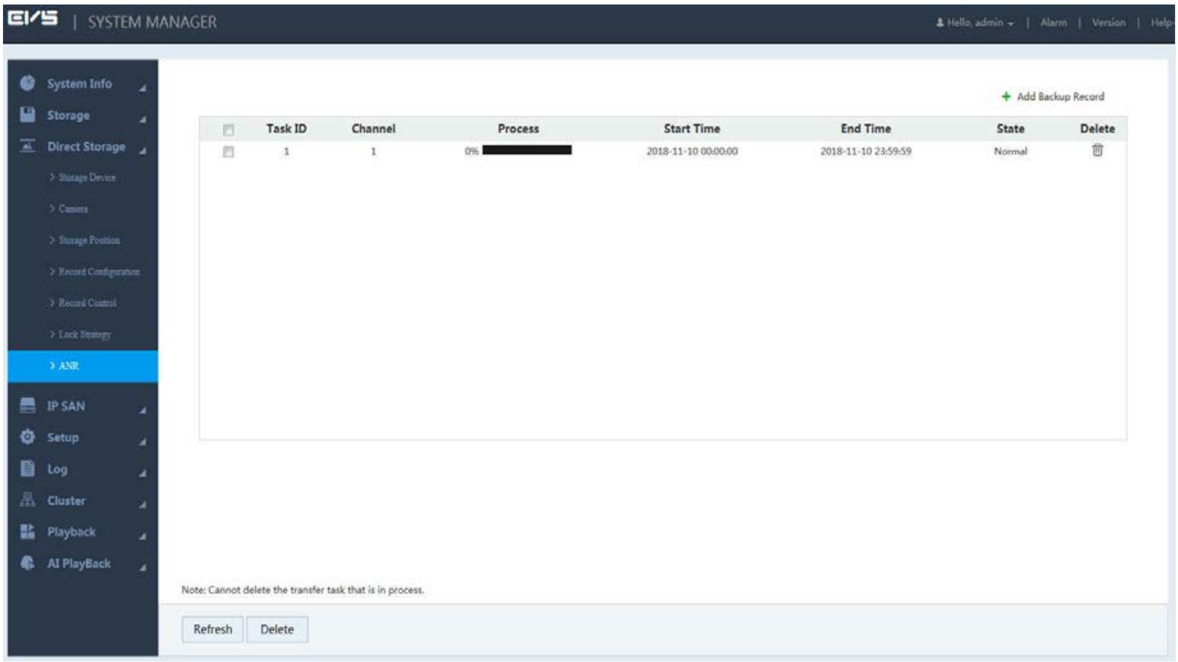
Step 3 Select channel, set start time and end time.

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** page.

You can view the upload progress of record on this page.

Figure 3-96 Upload progress



□	Task ID	Channel	Process	Start Time	End Time	State	Delete
□	1	1	0%	2018-11-10 00:00:00	2018-11-10 23:59:59	Normal	🗑

Note: Cannot delete the transfer task that is in process.

Task(s) in progress cannot be deleted.

3.12 User Management

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

- The factory default username 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 username 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).

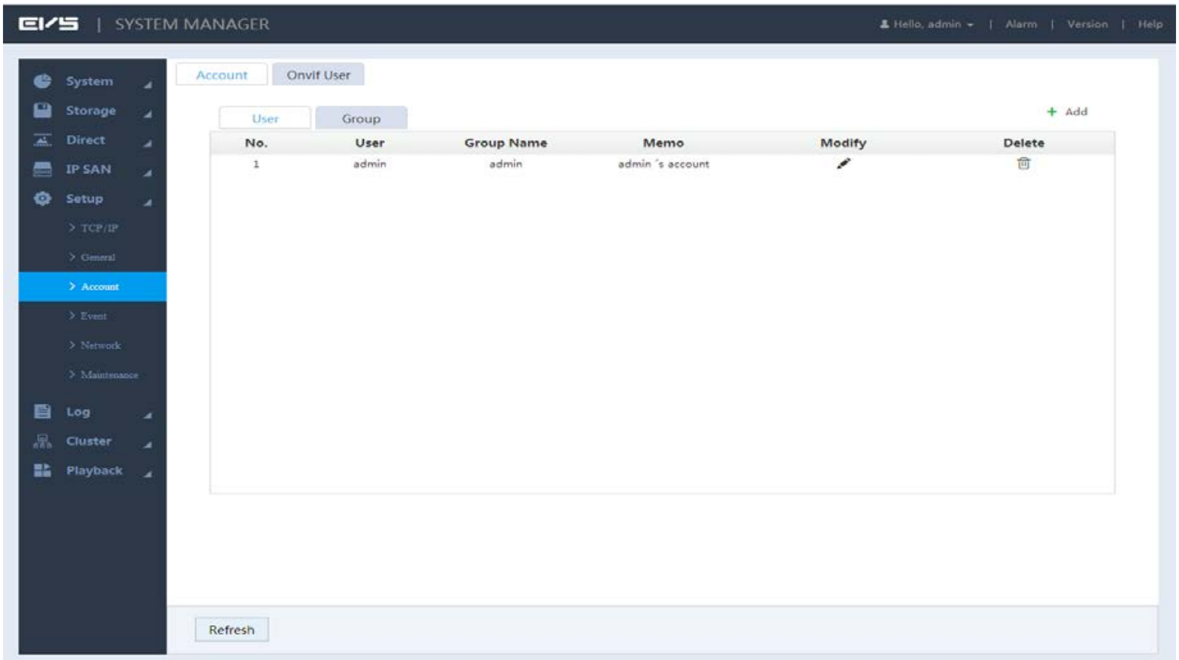
3.12.1 User

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**.

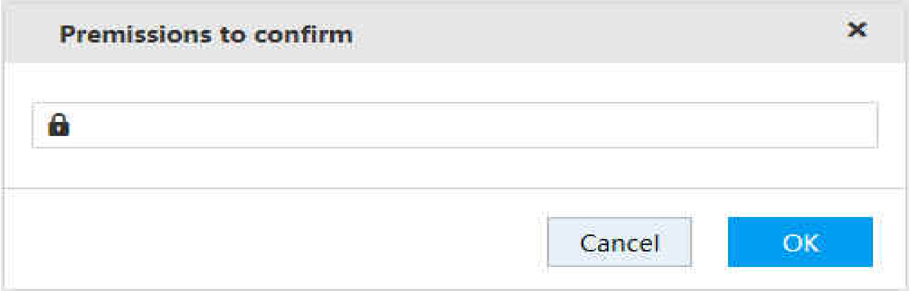
Figure 3-97 User



No.	User	Group Name	Memo	Modify	Delete
1	admin	admin	admin´s account	✎	🗑

Step 2 Click + .

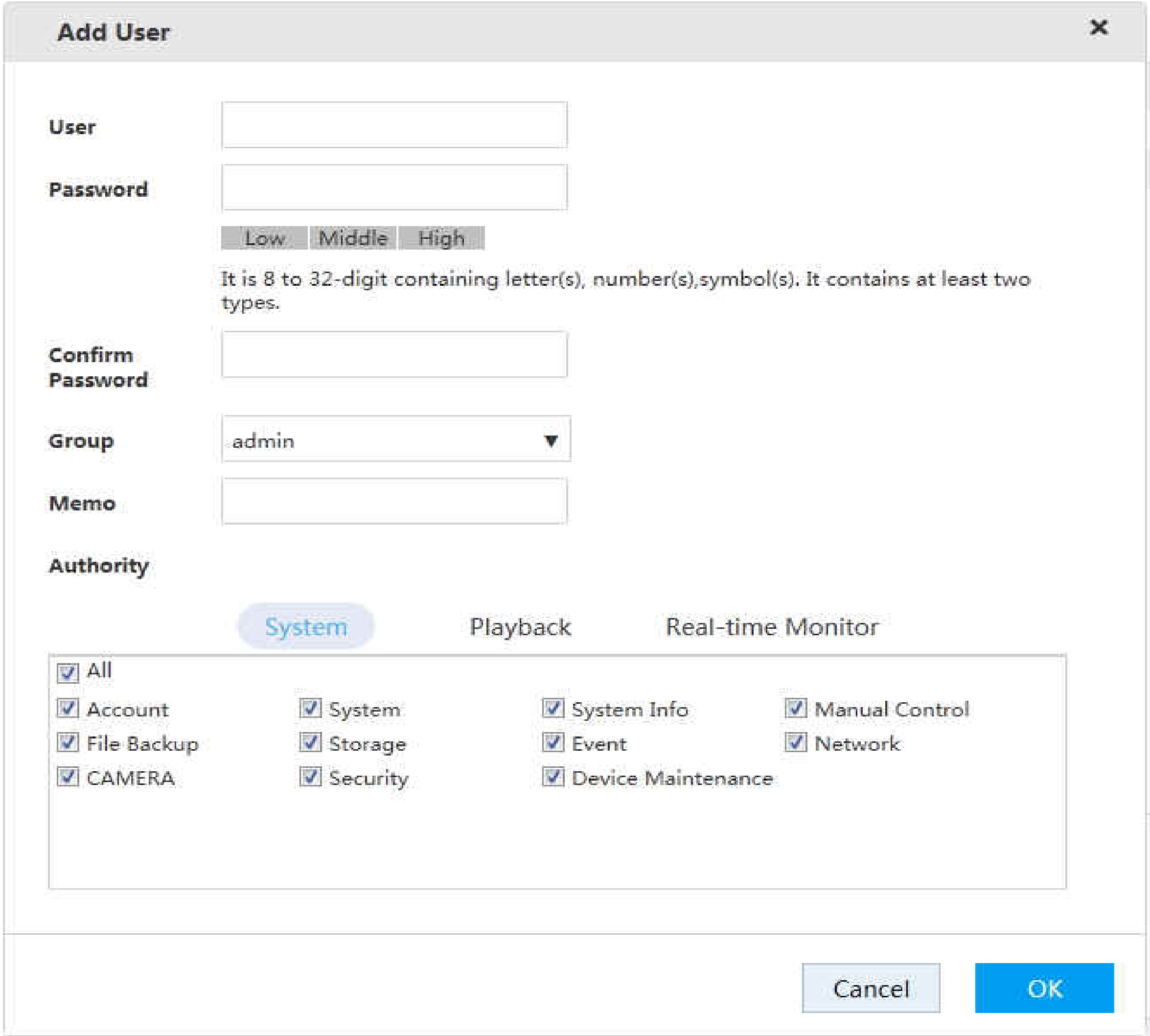
Figure 3-98 Permissions to confirm



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

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

Figure 3-99 Adding user



Add User

User

Password

Low Middle High

It is 8 to 32-digit containing letter(s), number(s),symbol(s). It contains at least two types.

Confirm Password

Group: admin

Memo

Authority

Step 4 Configure the parameters.

Table 3-33 Parameters of adding user

Parameter	Description
User	Enter the username.
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.
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.

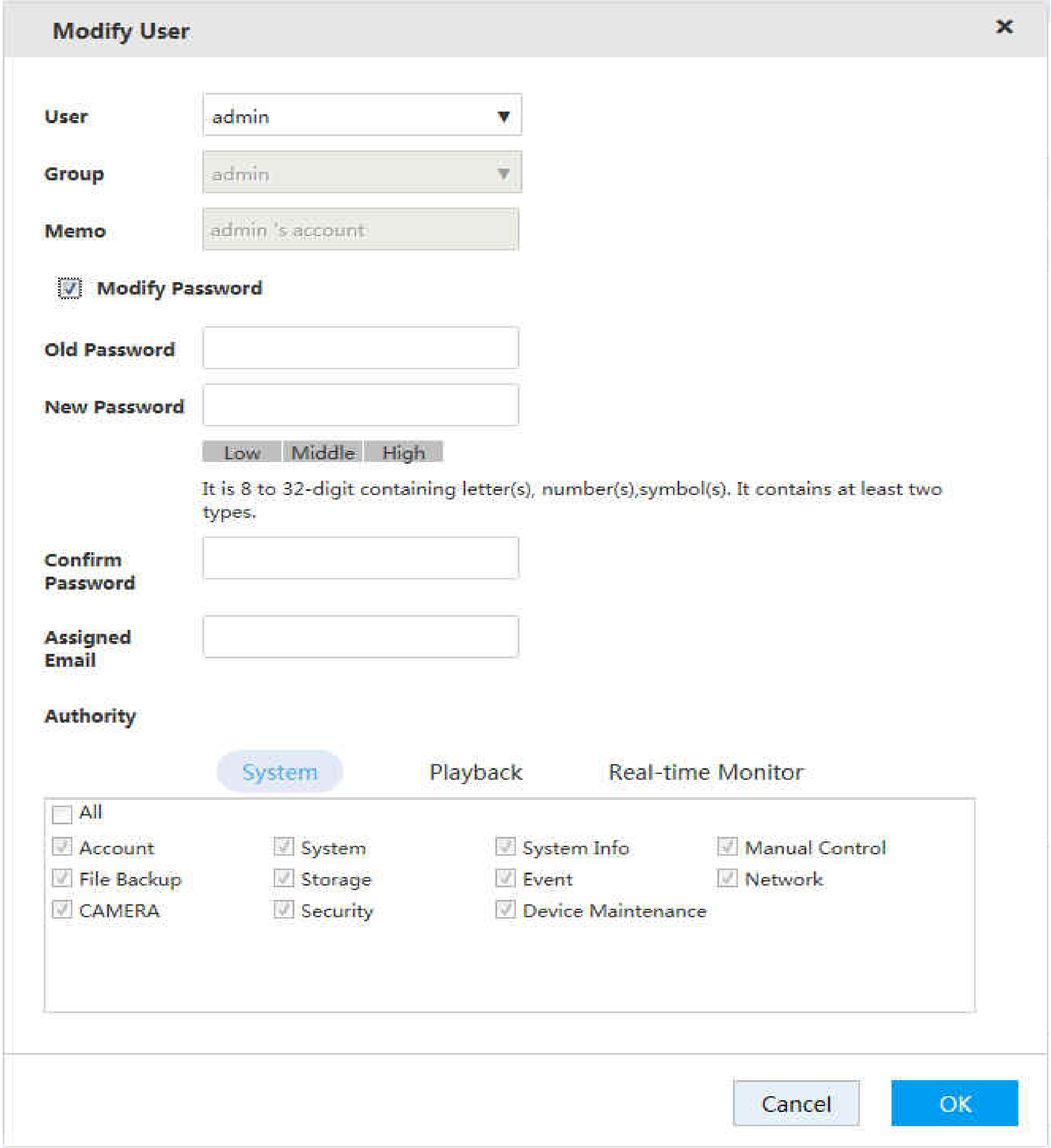
3.12.1.2 Changing Password

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

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

Step 2 Select the **Modify Password** checkbox.

Figure 3-100 Modifying user



Modify User ×

User	admin ▼
Group	admin ▼
Memo	admin 's account

☑ Modify Password

Old Password	
New Password	

Low Middle High

It is 8 to 32-digit containing letter(s), number(s),symbol(s). It contains at least two types.

Confirm Password	
Assigned Email	

Authority

System Playback Real-time Monitor

□ All

☑ Account	☑ System	☑ System Info	☑ Manual Control
☑ File Backup	☑ Storage	☑ Event	☑ Network
☑ CAMERA	☑ Security	☑ Device Maintenance	

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 page.

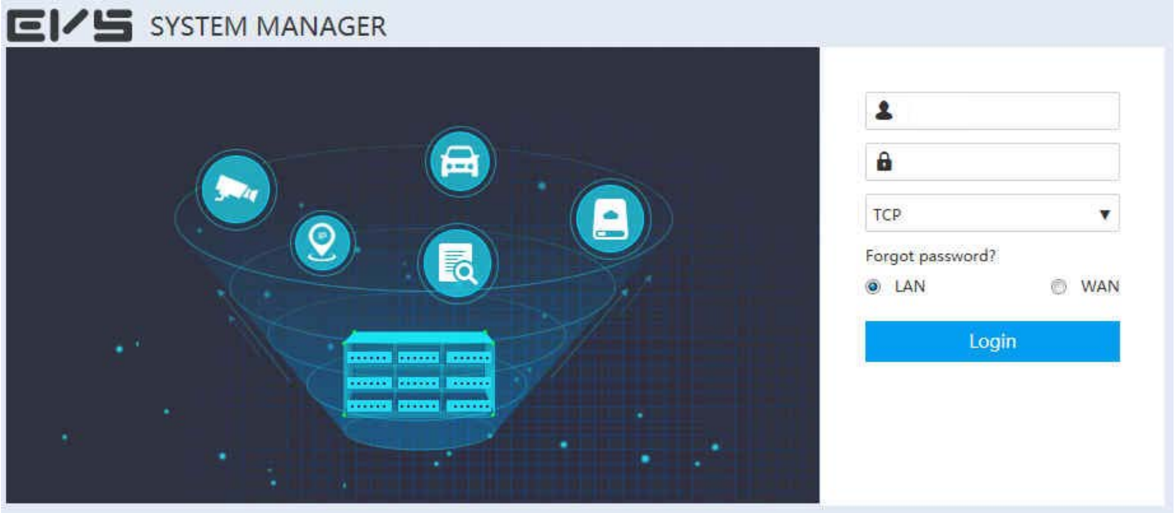
Step 5 Click **OK** to save the configuration.

3.12.1.3 Resetting Password

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

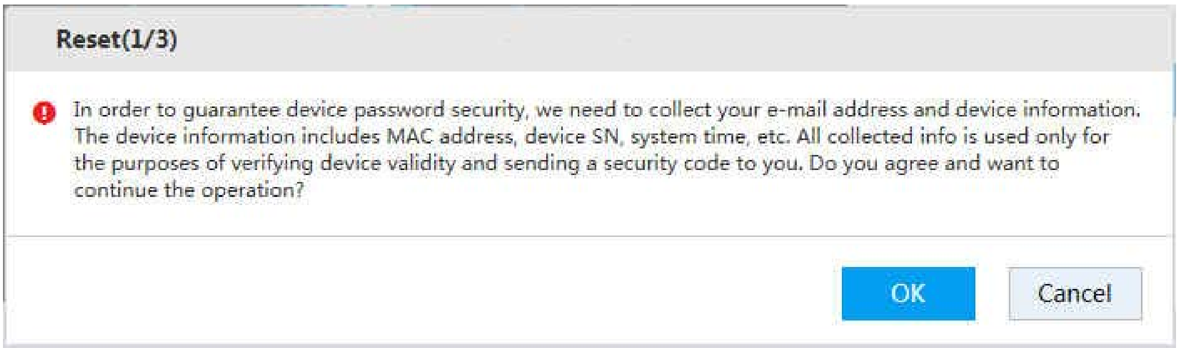
Step 1 Open the browser, and enter the IP address of the Device in the address bar. Press Enter.

Figure 3-101 Login



Step 2 Click **Forgot password?**

Figure 3-102 Resetting password (1)



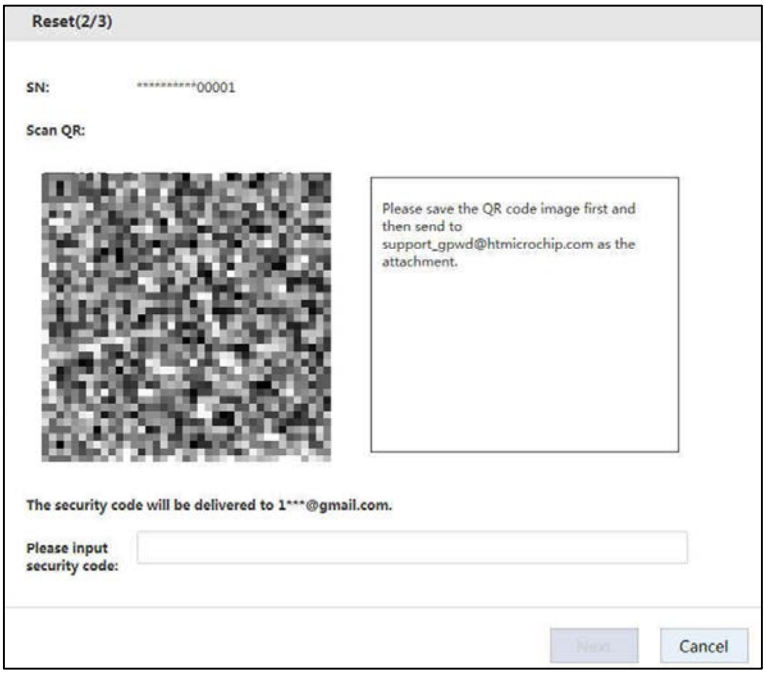
Reset(1/3)

In order to guarantee device password security, we need to collect your e-mail address and device information. The device information includes MAC address, device SN, system time, etc. All collected info is used only for the purposes of verifying device validity and sending a security code to you. Do you agree and want to continue the operation?

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**.

Figure 3-103 Resetting password (2)



Reset(2/3)

SN: **********00001

Scan QR:

Please save the QR code image first and then send to support_gpwd@htmicrochip.com as the attachment.

The security code will be delivered to 1***@gmail.com.

Please input security code:

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

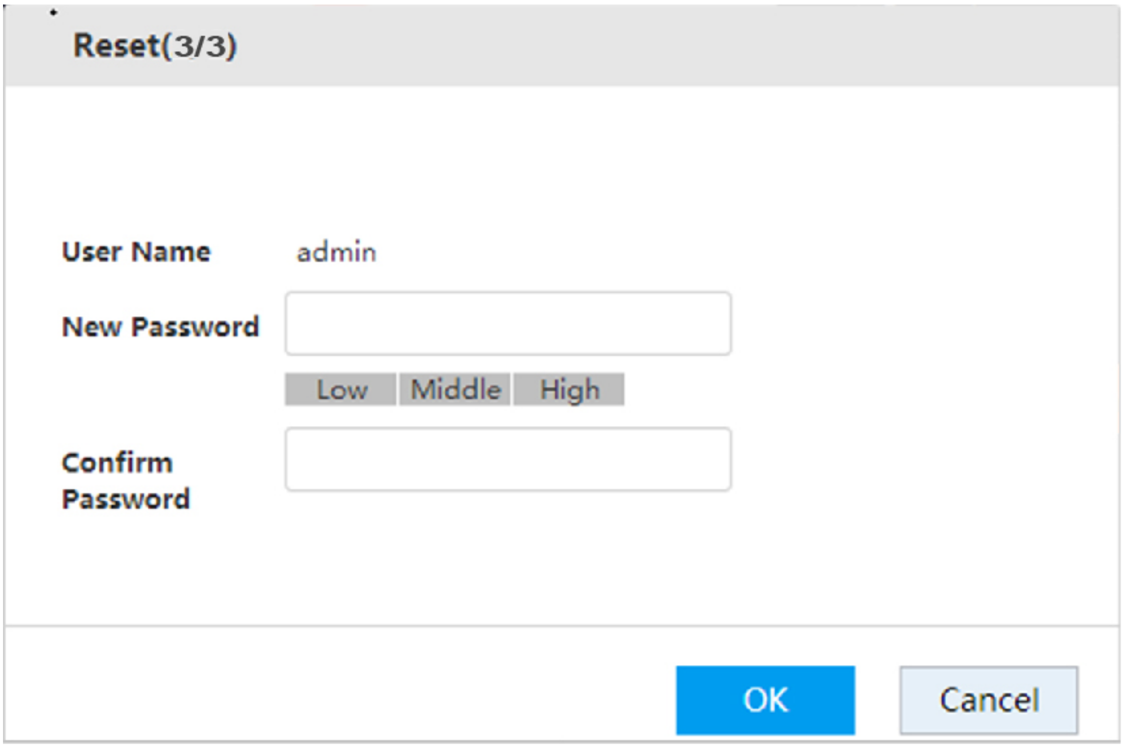
⚠

- You can obtain the security code for twice at most by scanning the same QR code. If you need more times, refresh the QR page.
- 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**.

Figure 3-104 Resetting password (2)



Reset(3/3)

User Name admin

New Password

Low Middle High

Confirm Password

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.

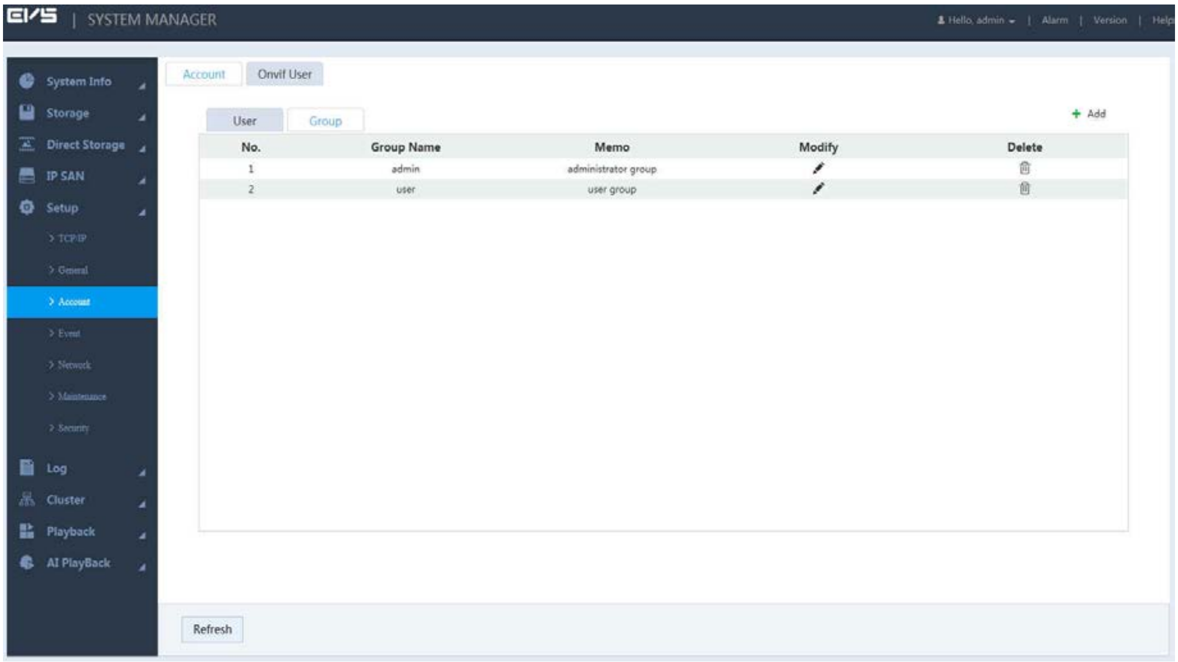
Step 8 Click **OK** to complete password reset.

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**.

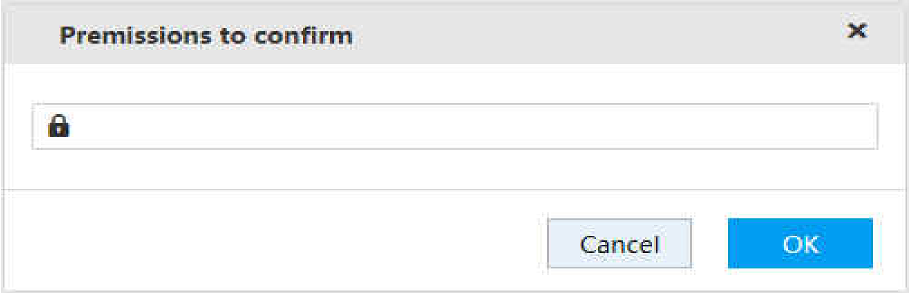
Figure 3-105 Group



No.	Group Name	Memo	Modify	Delete
1	admin	administrator group	✎	🗑
2	user	user group	✎	🗑

Step 2 Click + .

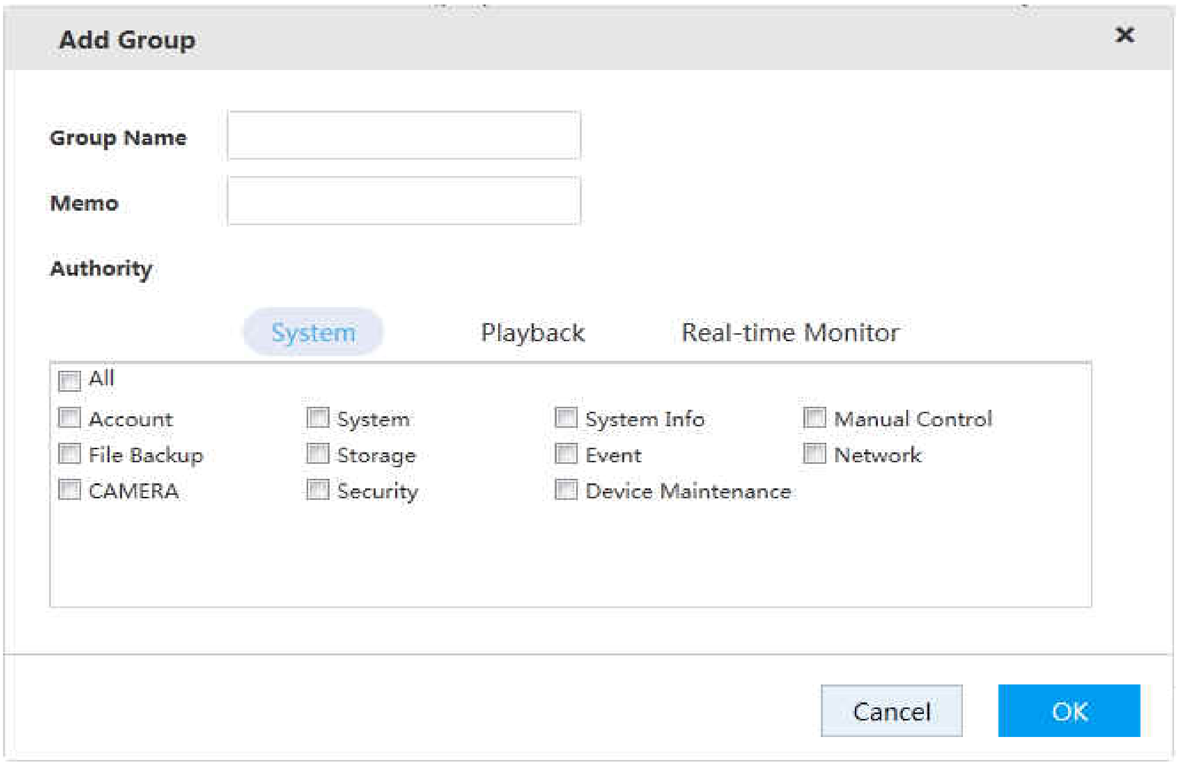
Figure 3-106 Permissions to confirm



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

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

Figure 3-107 Adding group


Add Group

Group Name

Memo

Authority

System Playback Real-time Monitor

□ All

□ Account □ System □ System Info □ Manual Control

□ File Backup □ Storage □ Event □ Network

□ CAMERA □ Security □ Device Maintenance

Cancel OK

Step 4 Configure the parameters.

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.

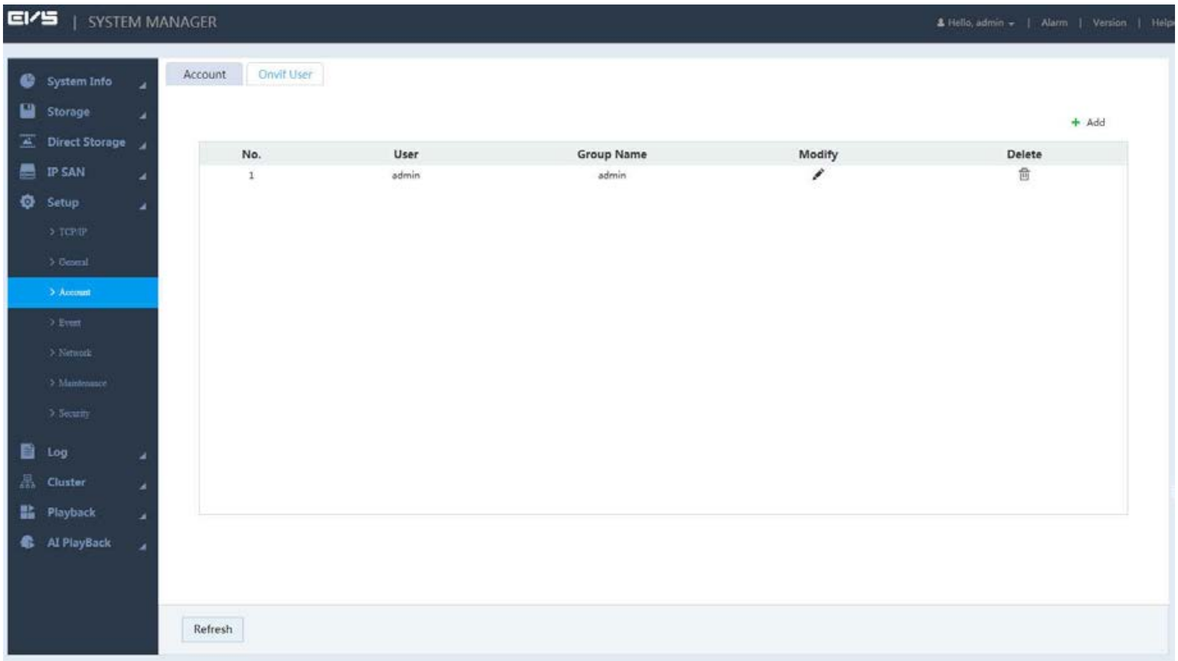
3.12.3 ONVIF User

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**.

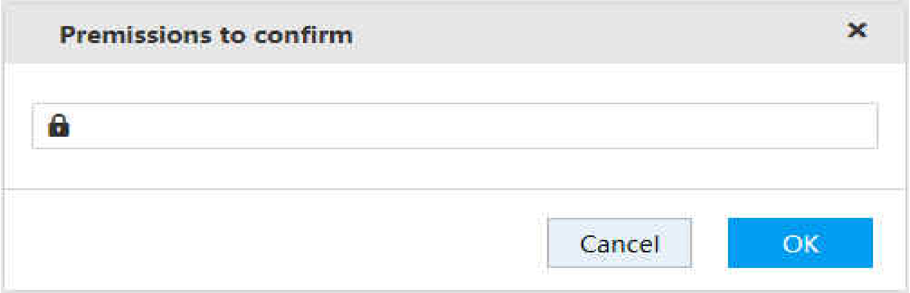
Figure 3-108 ONVIF user



No.	User	Group Name	Modify	Delete
1	admin	admin	✎	🗑

Step 2 Click + .

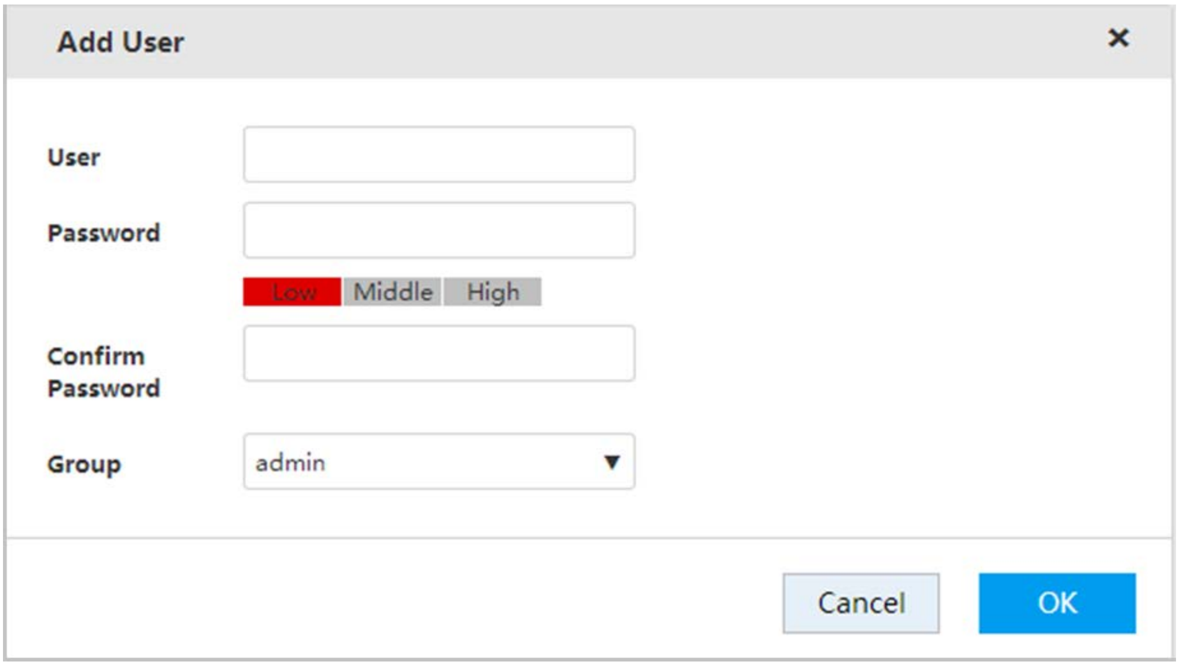
Figure 3-109 Permissions to confirm



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

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

Figure 3-110 Adding user



Group: admin

Step 4 Configure the parameters.

Table 3-35 Adding user parameters

Parameter	Description
User	Enter the username.
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.

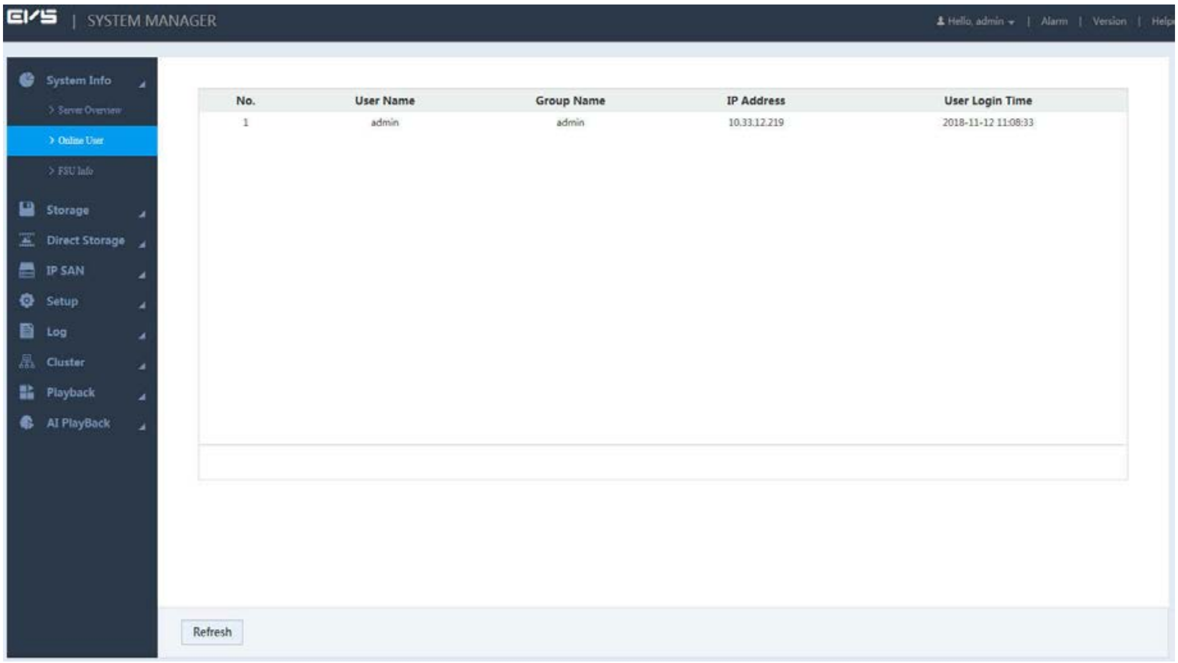
Click ✎ to edit user information, and click 🗑 to delete the user.

3.12.4 Online User

Select **System Info** > **Online User**, and then you can view the information of the current online users connected with the Device.

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



No.	User Name	Group Name	IP Address	User Login Time
1	admin	admin	10.33.12.219	2018-11-12 11:08:33

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.

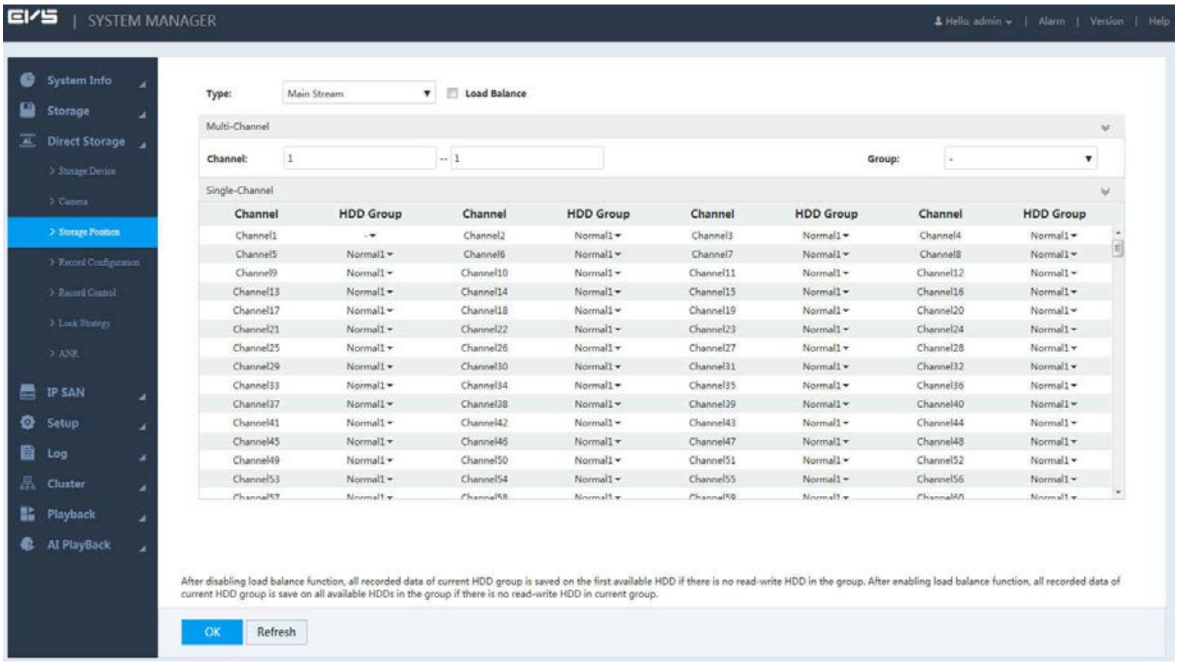
- Physical HDD: Disks directly installed in the Device.
- Network HDD: The virtual storage space mapped to the Device through network.
- RAID: Organize multiple independent physical disks into disk arrays. RAID provides higher storage performance and data redundancy.

3.13.1 Setting 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**.

Figure 3-112 Storage position



Type: Main Stream ▼ □ Load Balance

Multi-Channel

Channel: 1 -- 1 Group: - ▼

Single-Channel

Channel	HDD Group	Channel	HDD Group	Channel	HDD Group	Channel	HDD Group
Channel1	-	Channel2	Normal1	Channel3	Normal1	Channel4	Normal1
Channel5	Normal1	Channel6	Normal1	Channel7	Normal1	Channel8	Normal1
Channel9	Normal1	Channel10	Normal1	Channel11	Normal1	Channel12	Normal1
Channel13	Normal1	Channel14	Normal1	Channel15	Normal1	Channel16	Normal1
Channel17	Normal1	Channel18	Normal1	Channel19	Normal1	Channel20	Normal1
Channel21	Normal1	Channel22	Normal1	Channel23	Normal1	Channel24	Normal1
Channel25	Normal1	Channel26	Normal1	Channel27	Normal1	Channel28	Normal1
Channel29	Normal1	Channel30	Normal1	Channel31	Normal1	Channel32	Normal1
Channel33	Normal1	Channel34	Normal1	Channel35	Normal1	Channel36	Normal1
Channel37	Normal1	Channel38	Normal1	Channel39	Normal1	Channel40	Normal1
Channel41	Normal1	Channel42	Normal1	Channel43	Normal1	Channel44	Normal1
Channel45	Normal1	Channel46	Normal1	Channel47	Normal1	Channel48	Normal1
Channel49	Normal1	Channel50	Normal1	Channel51	Normal1	Channel52	Normal1
Channel53	Normal1	Channel54	Normal1	Channel55	Normal1	Channel56	Normal1
Channel57	Normal1	Channel58	Normal1	Channel59	Normal1	Channel60	Normal1

After disabling load balance function, all recorded data of current HDD group is saved on the first available HDD if there is no read-write HDD in the group. After enabling load balance function, all recorded data of current HDD group is save on all available HDDs in the group if there is no read-write HDD in current group.

OK Refresh

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.

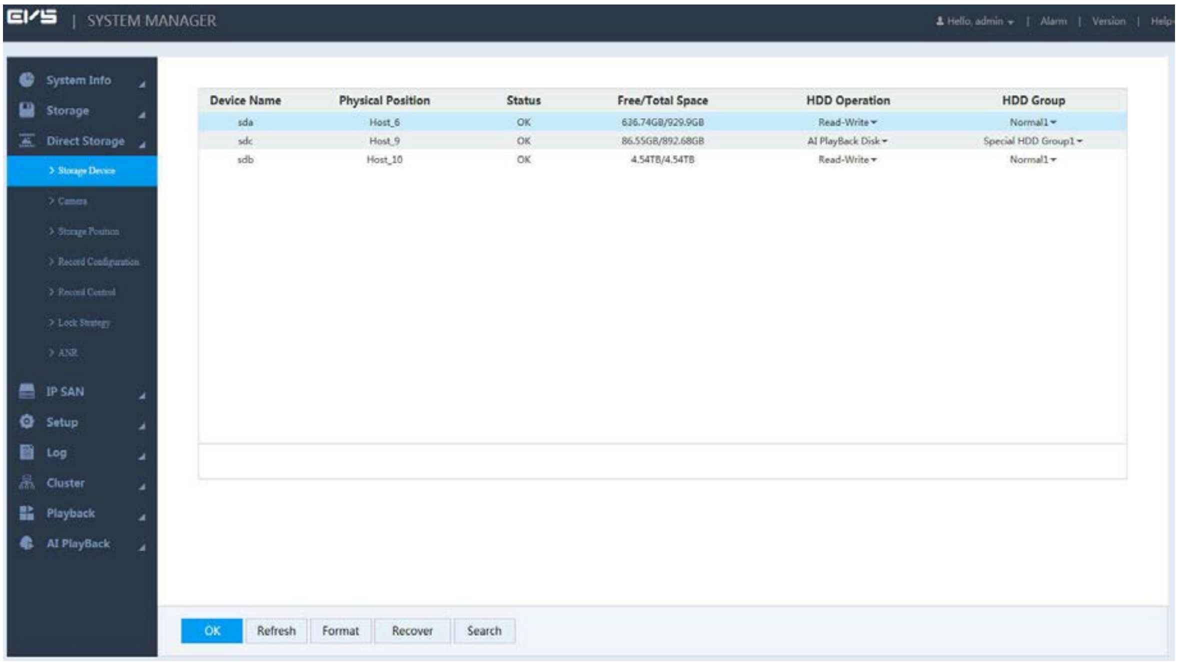
3.13.2 Managing Storage Device

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**.

Figure 3-113 Storage position



Device Name	Physical Position	Status	Free/Total Space	HDD Operation	HDD Group
sda	Host_6	OK	636.74GB/929.9GB	Read-Write	Normal1
sdc	Host_9	OK	86.55GB/892.68GB	AI PlayBack Disk	Special HDD Group1
sdb	Host_10	OK	4.54TB/4.54TB	Read-Write	Normal1

Step 2 Configure the parameters.

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** page, 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.

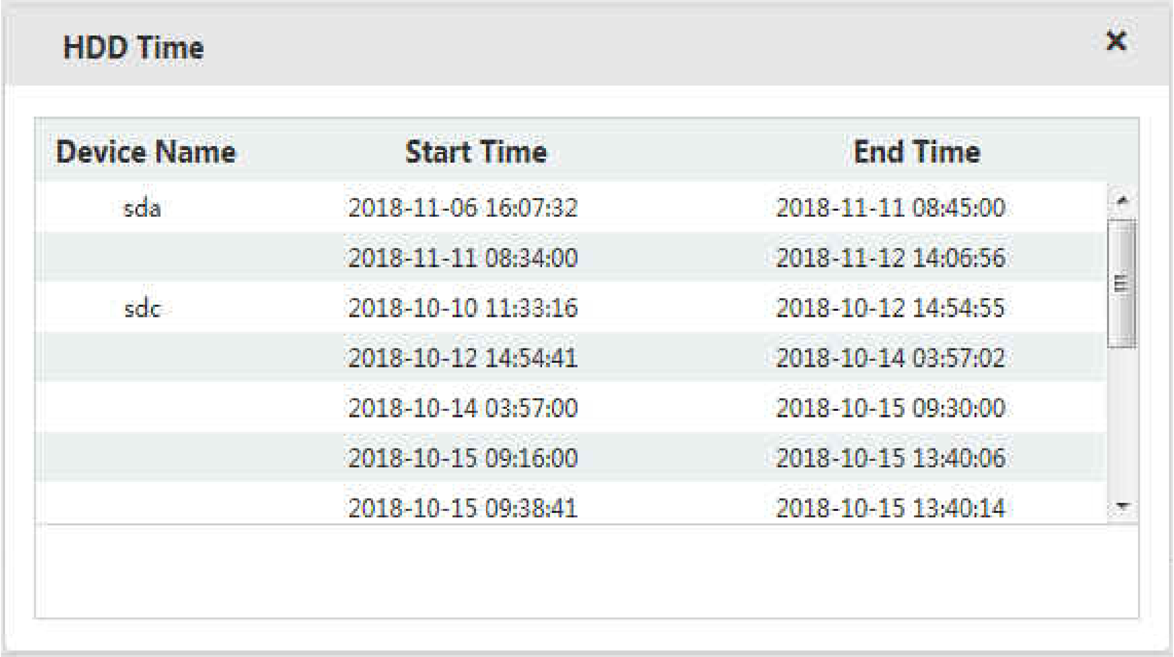
On the **Storage Device** page, select the corresponding disk, and click **Recover** to recover the picture database.

3.13.2.4 Searching record

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

The **HDD Time** page is displayed. On this page, you can check the time of record in specified disks.

Figure 3-114 HDD Time



HDD Time

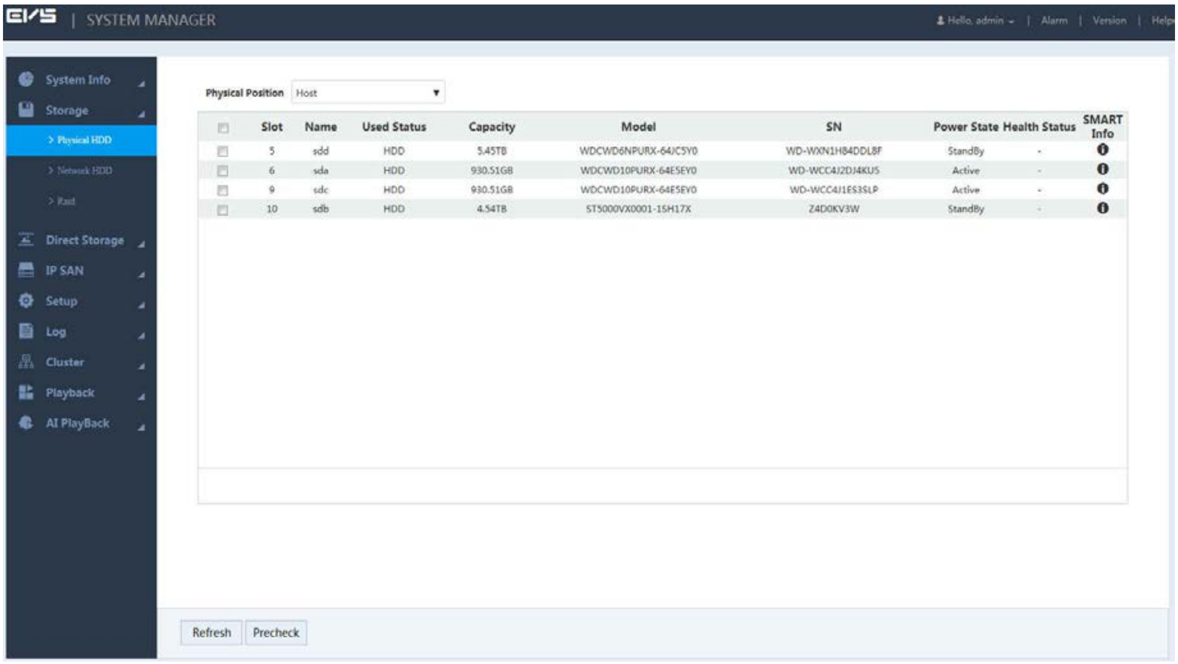
Device Name	Start Time	End Time
sda	2018-11-06 16:07:32	2018-11-11 08:45:00
	2018-11-11 08:34:00	2018-11-12 14:06:56
sdc	2018-10-10 11:33:16	2018-10-12 14:54:55
	2018-10-12 14:54:41	2018-10-14 03:57:02
	2018-10-14 03:57:00	2018-10-15 09:30:00
	2018-10-15 09:16:00	2018-10-15 13:40:06
	2018-10-15 09:38:41	2018-10-15 13:40:14

3.13.3 Managing 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**.

Figure 3-115 Physical HDD

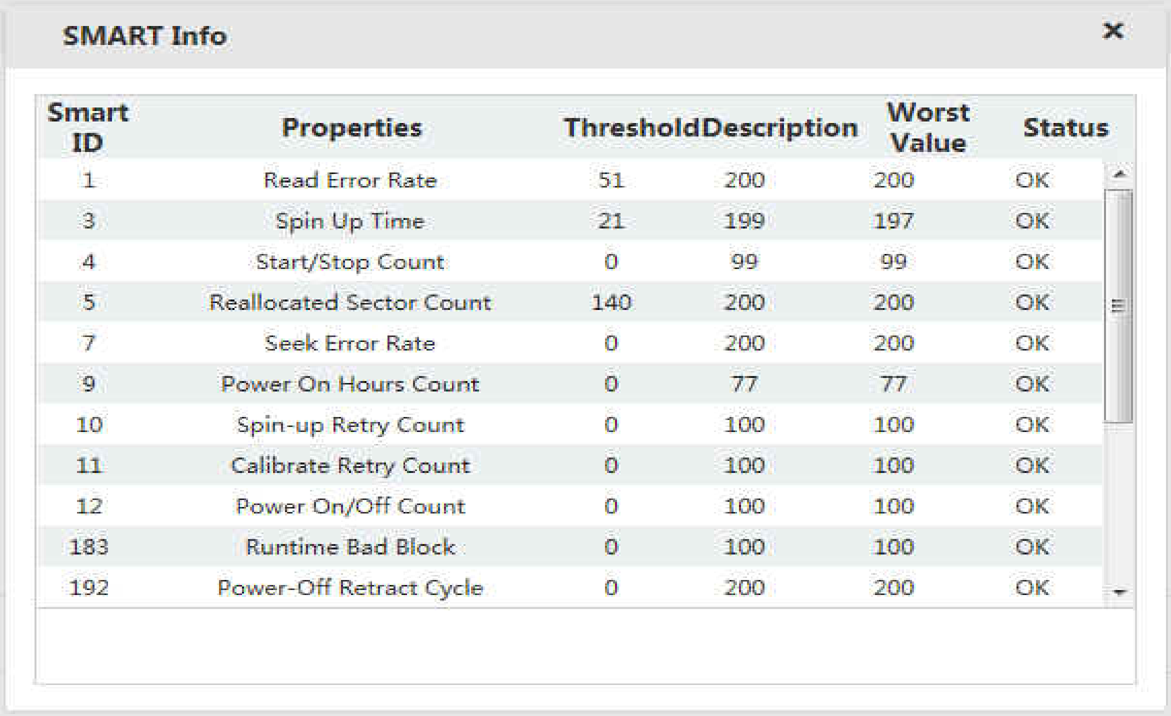


Physical Position: Host

□	Slot	Name	Used Status	Capacity	Model	SN	Power State	Health Status	SMART Info
□	5	sdd	HDD	5.45TB	WDCWD6NPURX-64JC5Y0	WD-WXN1H84DDL8F	StandBy	-	●
□	6	sda	HDD	930.51GB	WDCWD10PURX-64E5EY0	WD-WCC4J2DJ4KUS	Active	-	●
□	9	sdc	HDD	930.51GB	WDCWD10PURX-64E5EY0	WD-WCC4J1ES3SLP	Active	-	●
□	10	sdb	HDD	4.54TB	ST5000VX0001-1SH17X	Z4D0KV3W	StandBy	-	●

- 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** page is displayed.

Figure 3-116 SMART information



SMART Info

Smart ID	Properties	Threshold	Description	Worst Value	Status
1	Read Error Rate	51	200	200	OK
3	Spin Up Time	21	199	197	OK
4	Start/Stop Count	0	99	99	OK
5	Reallocated Sector Count	140	200	200	OK
7	Seek Error Rate	0	200	200	OK
9	Power On Hours Count	0	77	77	OK
10	Spin-up Retry Count	0	100	100	OK
11	Calibrate Retry Count	0	100	100	OK
12	Power On/Off Count	0	100	100	OK
183	Runtime Bad Block	0	100	100	OK
192	Power-Off Retract Cycle	0	200	200	OK

3.13.4 Adding 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.

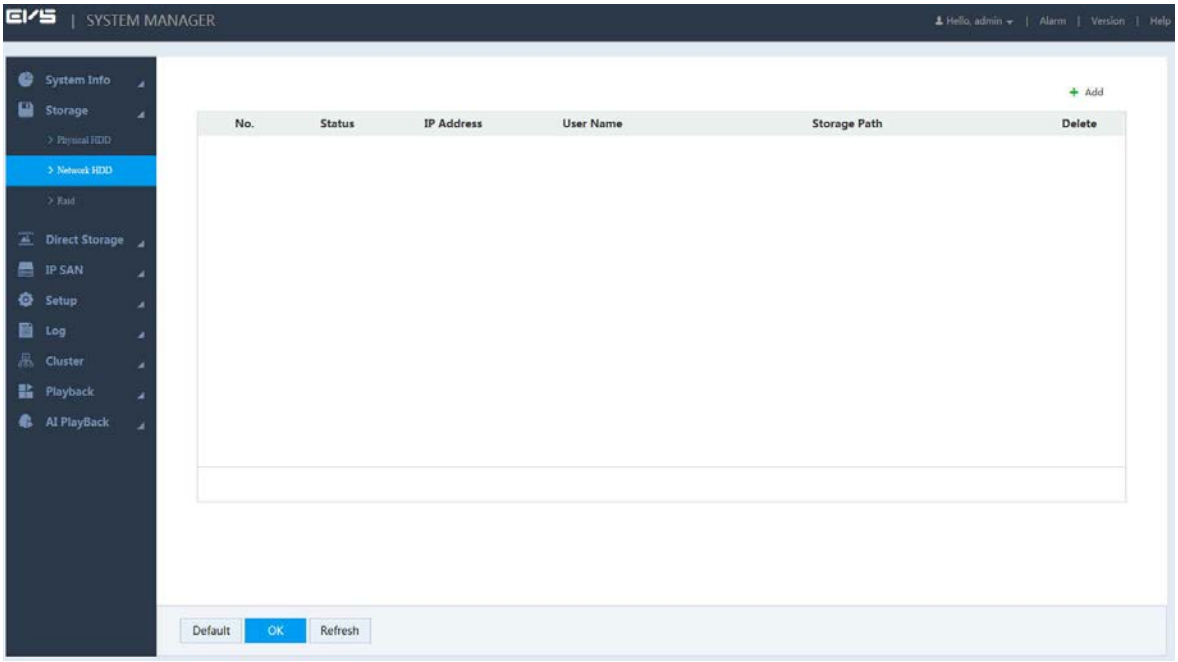
Preparation

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

Procedure

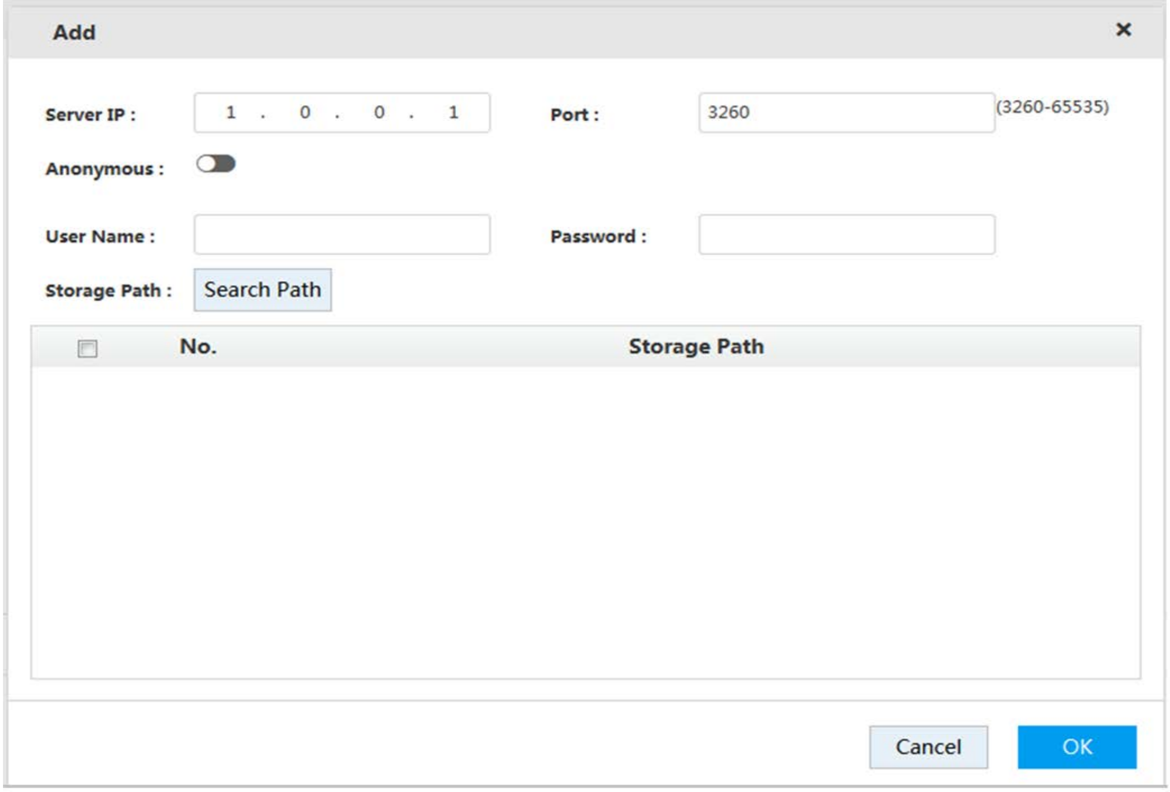
Step 1 Select **Storage** > **Network HDD**.

Figure 3-117 Network HDD



Step 2 Click + .

Figure 3-118 Adding network HDD



Step 3 Configure the parameters.

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 username and password. ● ○: Anonymous login disabled.
Username	If the iSCSI server has set access permission when it creates the share file list, you need to enter the username and password.
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** page. You can view the added disk information on this page.

- 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** page. 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

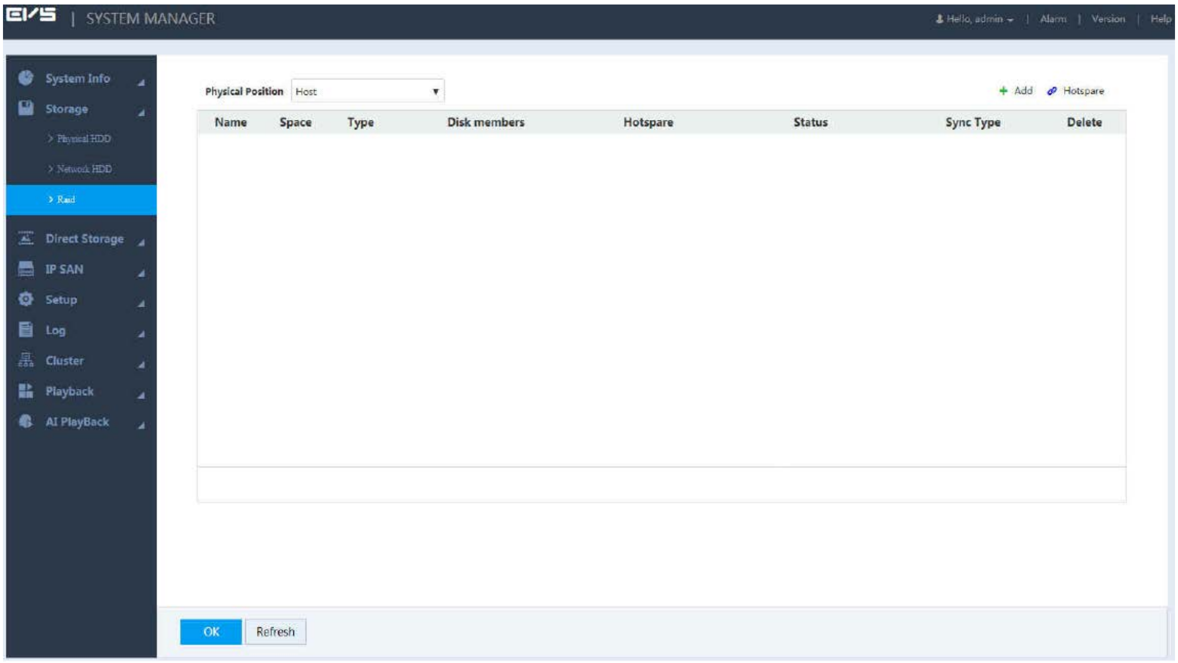
RAID has different levels (such as RAID5, RAID6), and each level has its own data protection, data availability and performance level. You can create RAID according to actual needs.

⚠

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

Step 1 Select **Storage > Raid**.

Figure 3-119 Raid management

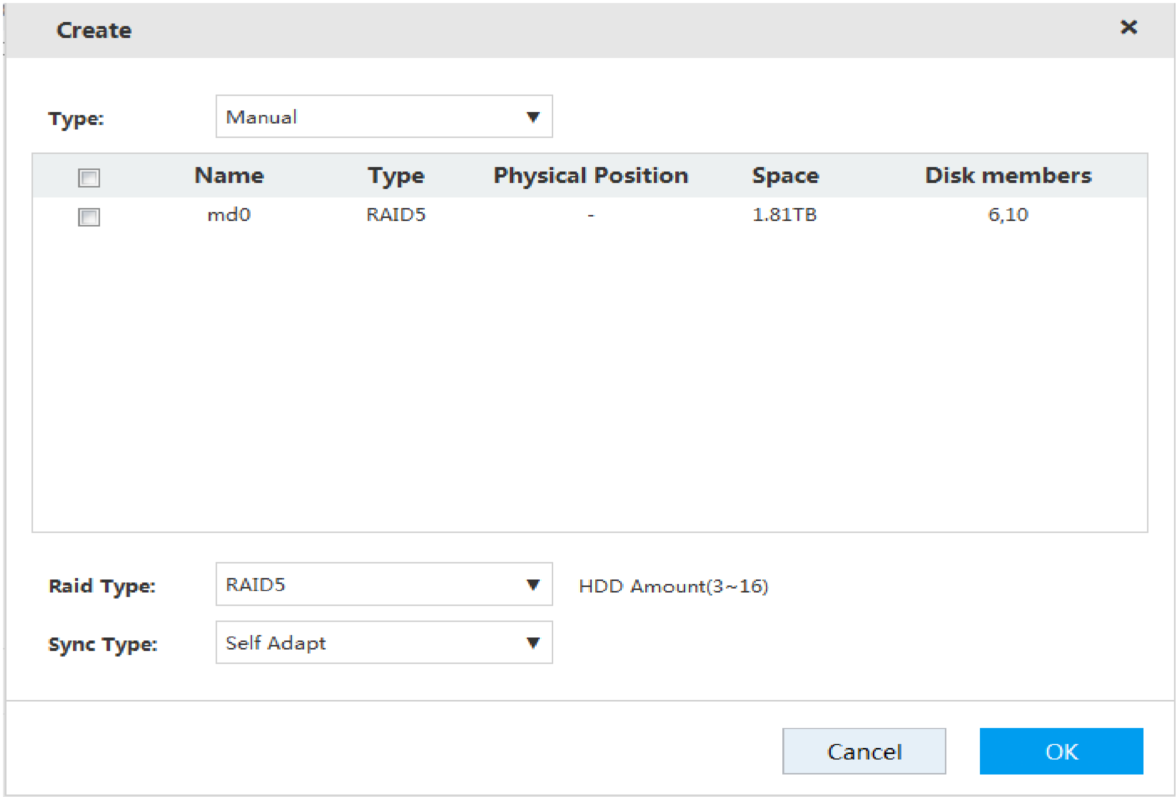


Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete

Step 2 Click + .

Figure 3-120 Creating RAID



Create ×

Type: Manual

☐	Name	Type	Physical Position	Space	Disk members
☐	md0	RAID5	-	1.81TB	6,10

Raid Type: RAID5 HDD Amount(3~16)

Sync Type: Self Adapt

Step 3 Select the parameters.

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. ● 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.
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.

Parameter	Description
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** page. You can view the added RAID information on this page.

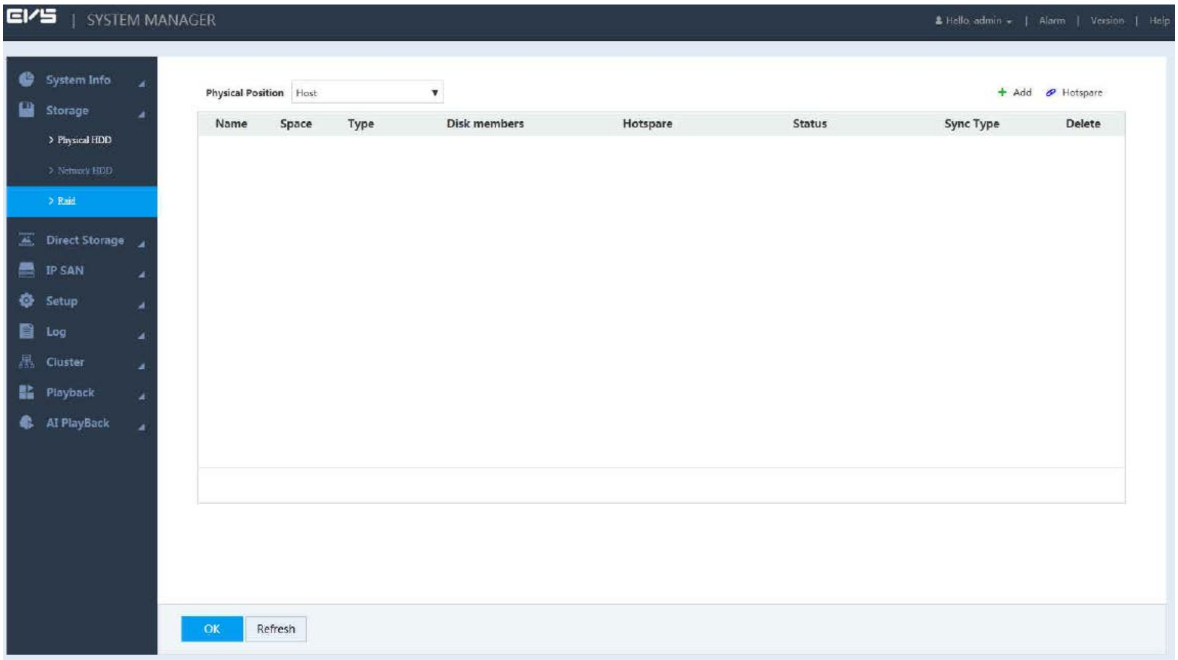
- Click 🗑 to delete a RAID, and click **Refresh** to update the RAID list.
- Double-click the RAID line, and you can view the detailed information.

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**.

Figure 3-121 RAID management

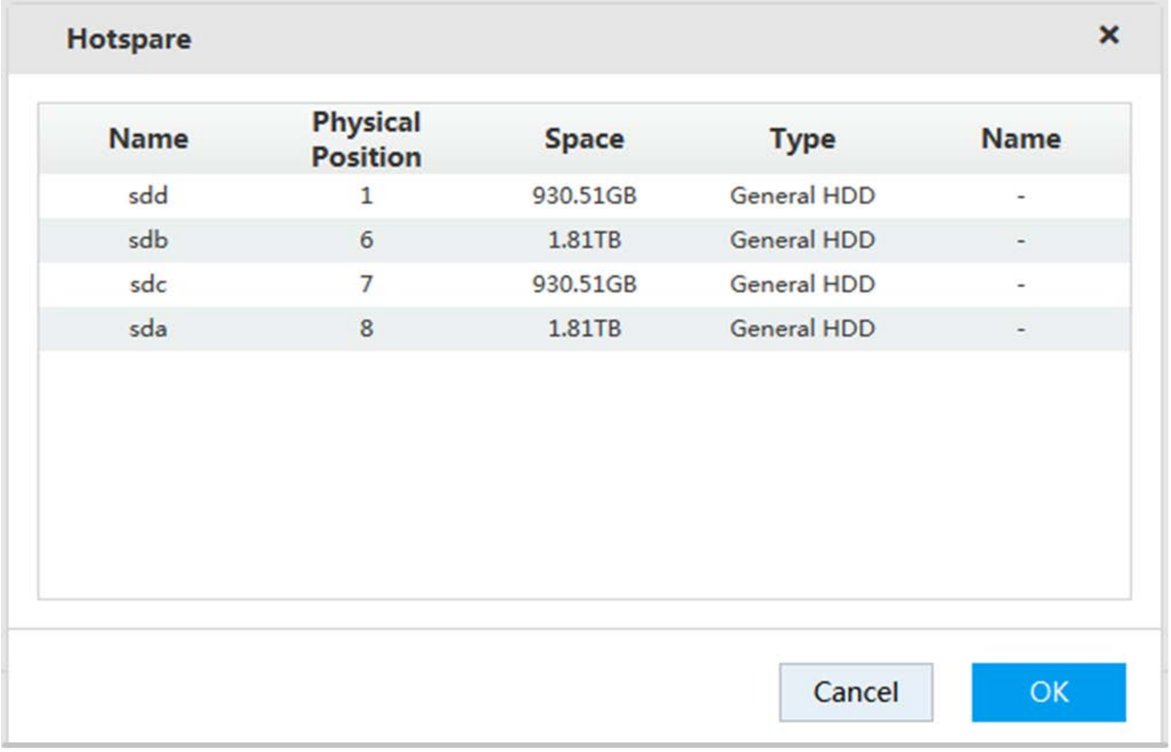


Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete

Step 2 Click 🔗 .

Figure 3-122 Hotspare management



Name	Physical Position	Space	Type	Name
sdd	1	930.51GB	General HDD	-
sdb	6	1.81TB	General HDD	-
sdc	7	930.51GB	General HDD	-
sda	8	1.81TB	General HDD	-

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.

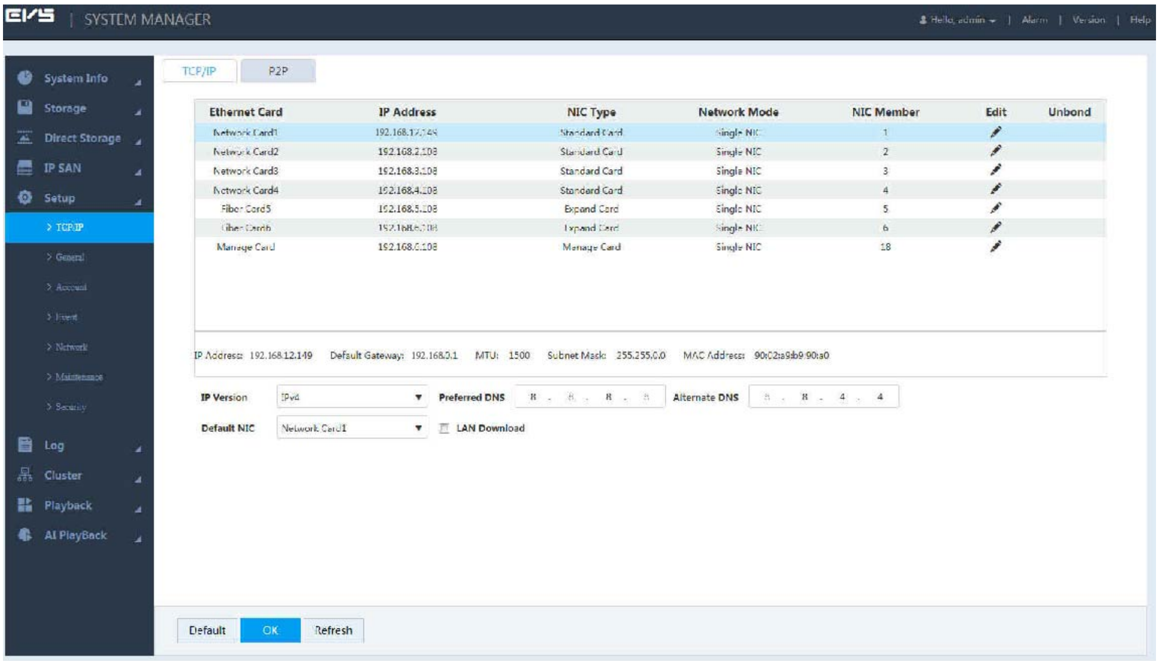
3.14.1.1 Setting IP

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** page is displayed. For details on setting IP, see "3.4.1 Setting IP".

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



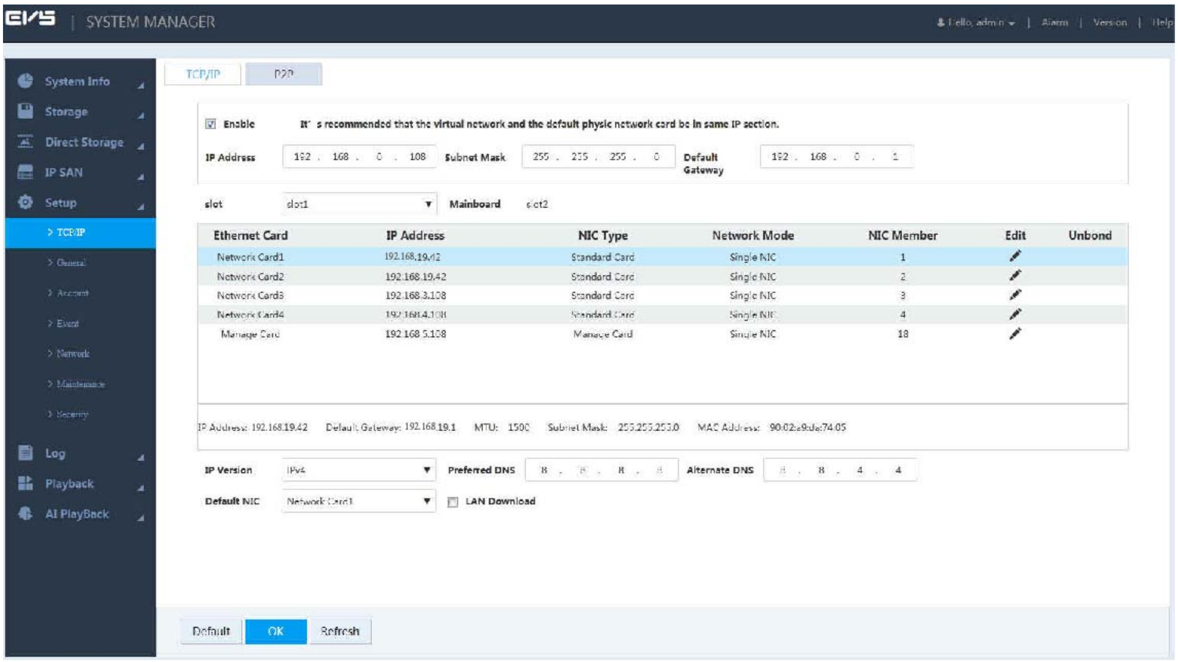
Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.12.149	Standard Card	Single NIC	1	✎	
Network Card2	192.168.2.108	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎	
Fiber Card5	192.168.5.108	Expand Card	Single NIC	5	✎	
Fiber Card6	192.168.6.108	Expand Card	Single NIC	6	✎	
Manage Card	192.168.0.108	Manage Card	Single NIC	18	✎	

IP Address: 192.168.12.149 Default Gateway: 192.168.0.1 MTU: 1500 Subnet Mask: 255.255.0.0 MAC Address: 90:02:a9:b9:90:a0

IP Version: IPv4 ▼ Preferred DNS: 8 . 8 . 8 . 8 Alternate DNS: 8 . 8 . 4 . 4

Default NIC: Network Card1 ▼ □ LAN Download

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



☑ Enable It' s recommended that the virtual network and the default physic network card be in same IP section.

IP Address 192 . 168 . 0 . 108 Subnet Mask 255 . 255 . 255 . 0 Default Gateway 192 . 168 . 0 . 1

slot slot1 Mainboard slot2

Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.19.42	Standard Card	Single NIC	1	✎	
Network Card2	192.168.19.42	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎	
Manage Card	192.168.5.108	Manage Card	Single NIC	18	✎	

IP Address: 192.168.19.42 Default Gateway: 192.168.19.1 MTU: 1500 Subnet Mask: 255.255.255.0 MAC Address: 90:02:a9:da:74:05

IP Version IPv4 Preferred DNS 8 . 8 . 8 . 8 Alternate DNS 8 . 8 . 4 . 4

Default NIC Network Card1 □ LAN Download

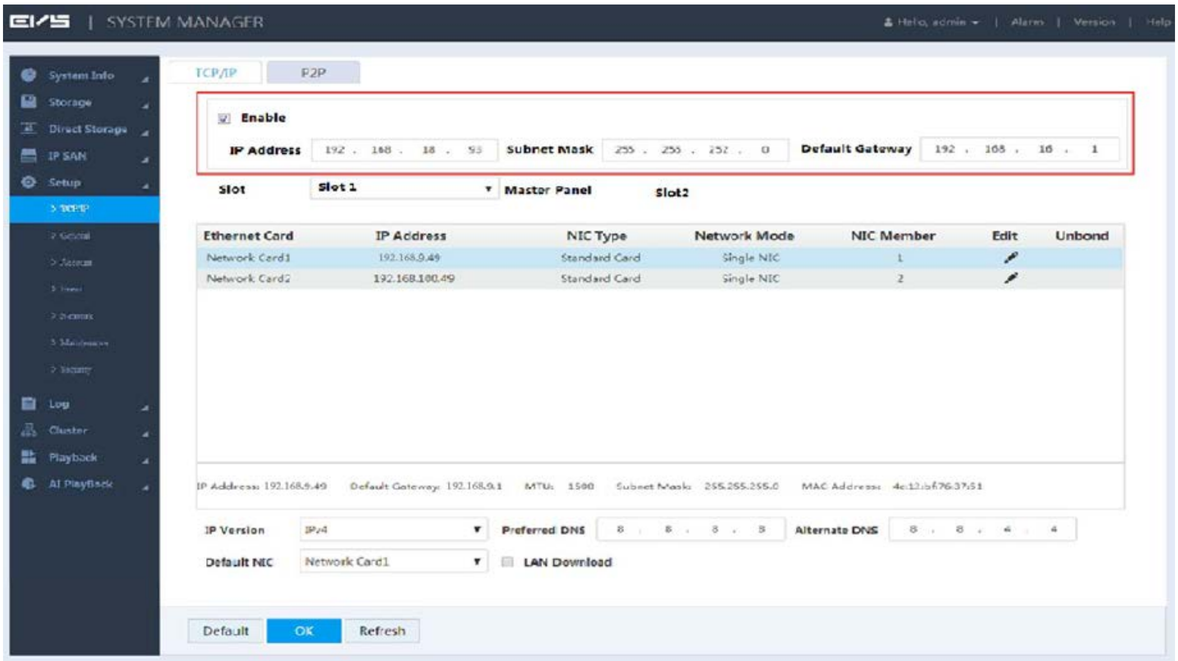
3.14.1.2 Virtual IP

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

Only dual-control devices support this function.

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

Figure 3-125 NIC settings



☑ Enable

IP Address 192 . 168 . 18 . 93 Subnet Mask 255 . 255 . 252 . 0 Default Gateway 192 . 168 . 16 . 1

Slot Slot 1 Master Panel Slot2

Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.9.49	Standard Card	Single NIC	1	✎	
Network Card2	192.168.100.49	Standard Card	Single NIC	2	✎	

IP Address: 192.168.9.49 Default Gateway: 192.168.9.1 MTU: 1500 Subnet Mask: 255.255.255.0 MAC Address: 4c:11:bf:76:37:51

IP Version IPv4 Preferred DNS 8 . 8 . 8 . 8 Alternate DNS 8 . 8 . 4 . 4

Default NIC Network Card1 □ LAN Download

Step 2 Select the **Enable** checkbox 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.

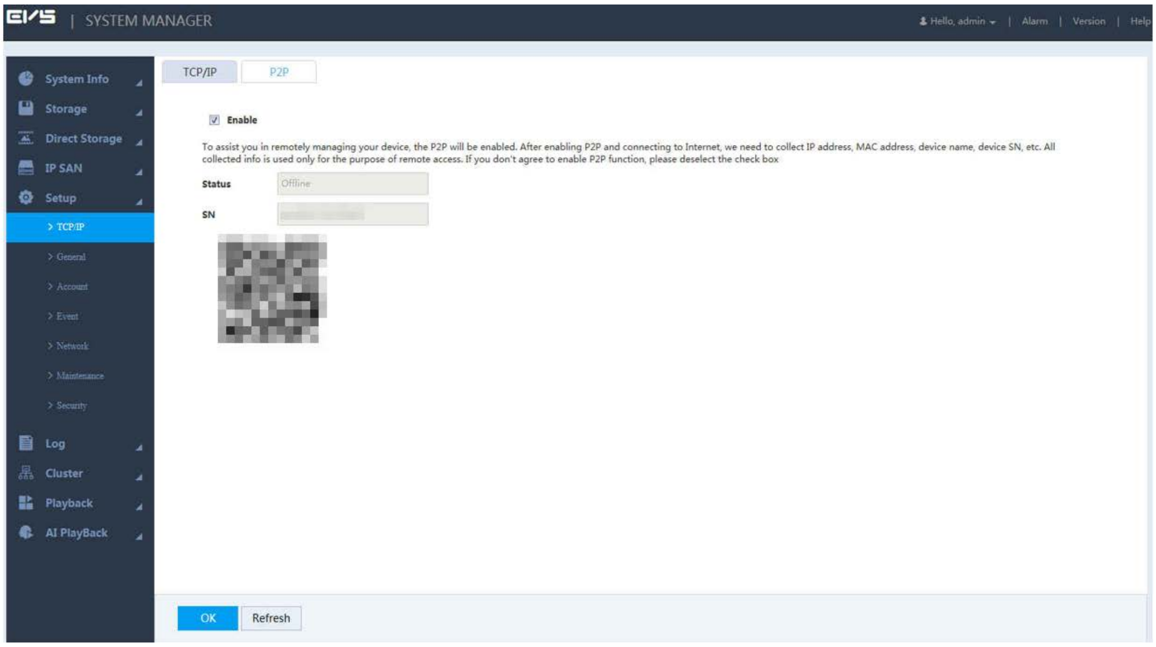
- Scan the QR code, download cell phone app, and then register an account. For details, see the corresponding user's manual.

⚠

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

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

Figure 3-126 P2P



☑ Enable

To assist you in remotely managing your device, the P2P will be enabled. After enabling P2P and connecting to Internet, we need to collect IP address, MAC address, device name, device SN, etc. All collected info is used only for the purpose of remote access. If you don't agree to enable P2P function, please deselect the check box

Status: Offline

SN: [redacted]

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 page and then download and install the app.

Step 2 Open the app. Select **Remote Monitor** to enter the home page.

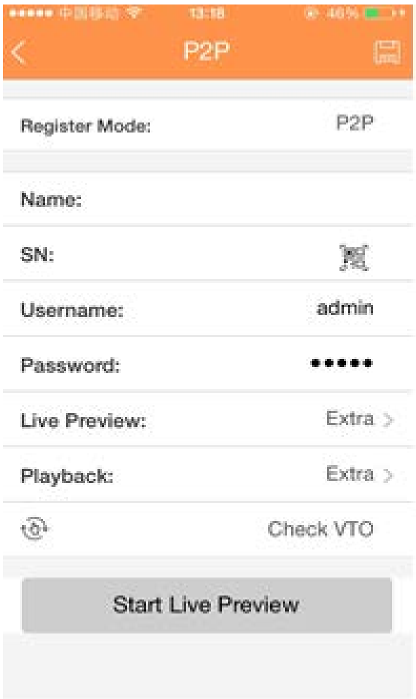
Step 3 Add device on the cell phone app.

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

2) Tap + to enter the QR code scanning page. 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



Register Mode: P2P

Name:

SN:

Username: admin

Password: •••••

Live Preview: Extra

Playback: Extra

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

3.14.2 General Information Settings

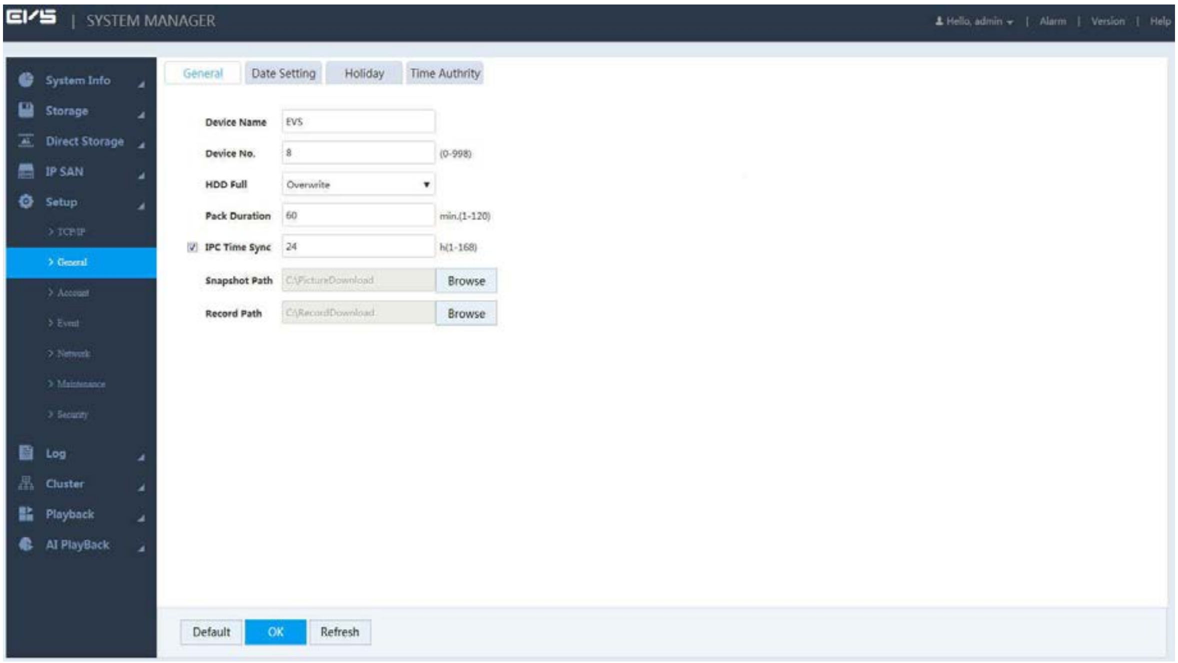
Set the general device information such as date, and holiday.

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**.

Figure 3-128 Setting general information



Device Name: EVS

Device No.: 8 (0-998)

HDD Full: Overwrite

Pack Duration: 60 min.(1-120)

☑ IPC Time Sync: 24 h(1-168)

Snapshot Path: C:\PictureDownload

Record Path: C:\RecordDownload

Step 2 Configure the parameters.

Table 3-39 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 checkbox 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.

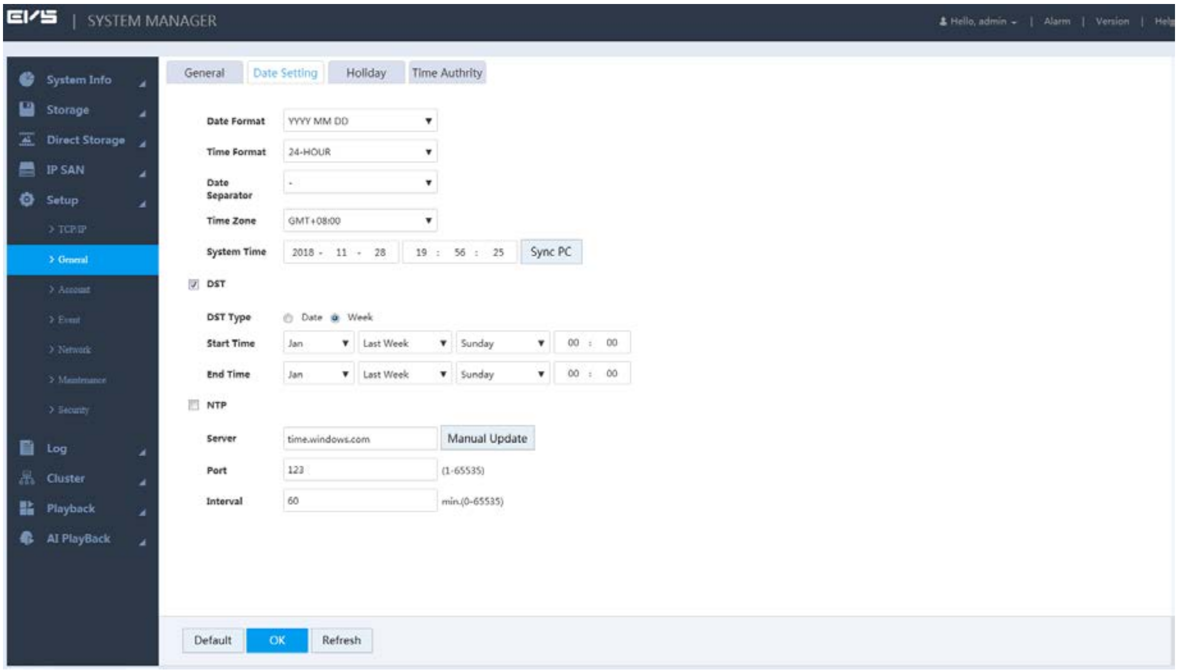
Step 3 Click **OK** to save the configuration.

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**.

Figure 3-129 Setting date



Date Format: YYYY MM DD

Time Format: 24-HOUR

Date Separator: -

Time Zone: GMT+08:00

System Time: 2018 - 11 - 28 19 : 56 : 25

☑ DST

DST Type: ○ Date ● Week

Start Time: Jan Last Week Sunday 00 : 00

End Time: Jan Last Week Sunday 00 : 00

□ NTP

Server: time.windows.com

Port: 123 (1-65535)

Interval: 60 min.(0-65535)

Step 2 Configure the parameters.

Table 3-40 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** checkbox 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** checkbox 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.

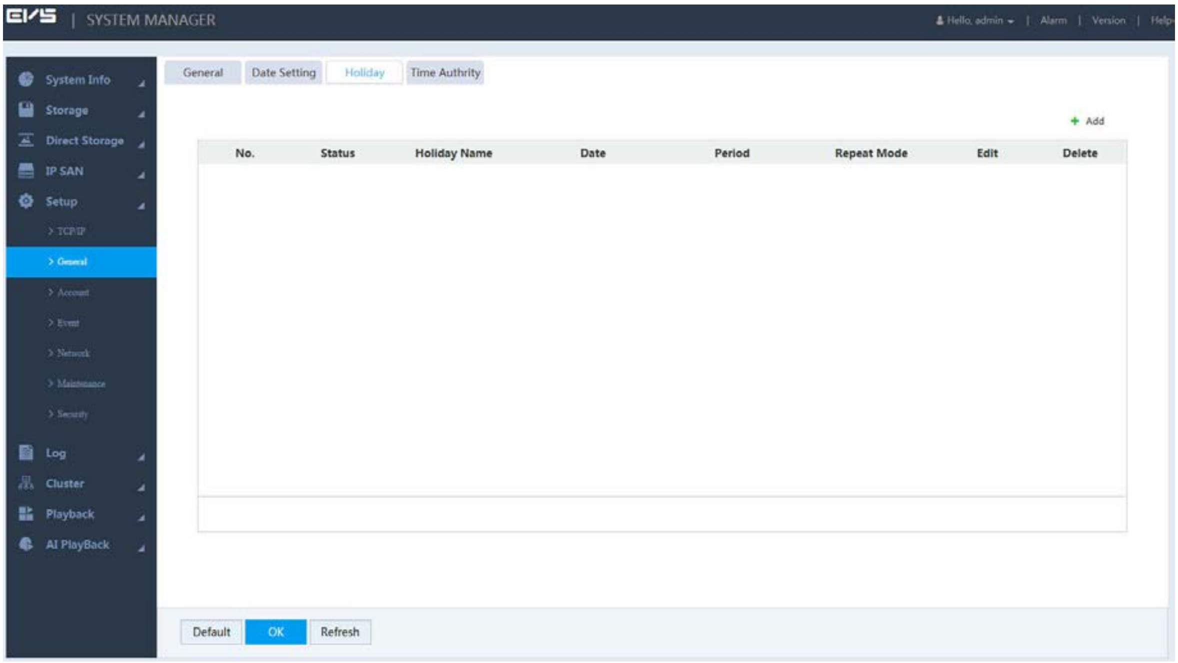
3.14.2.3 Setting Holiday

Add, edit and delete holiday information. After setting the holiday, holiday option will appear on the pages 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.

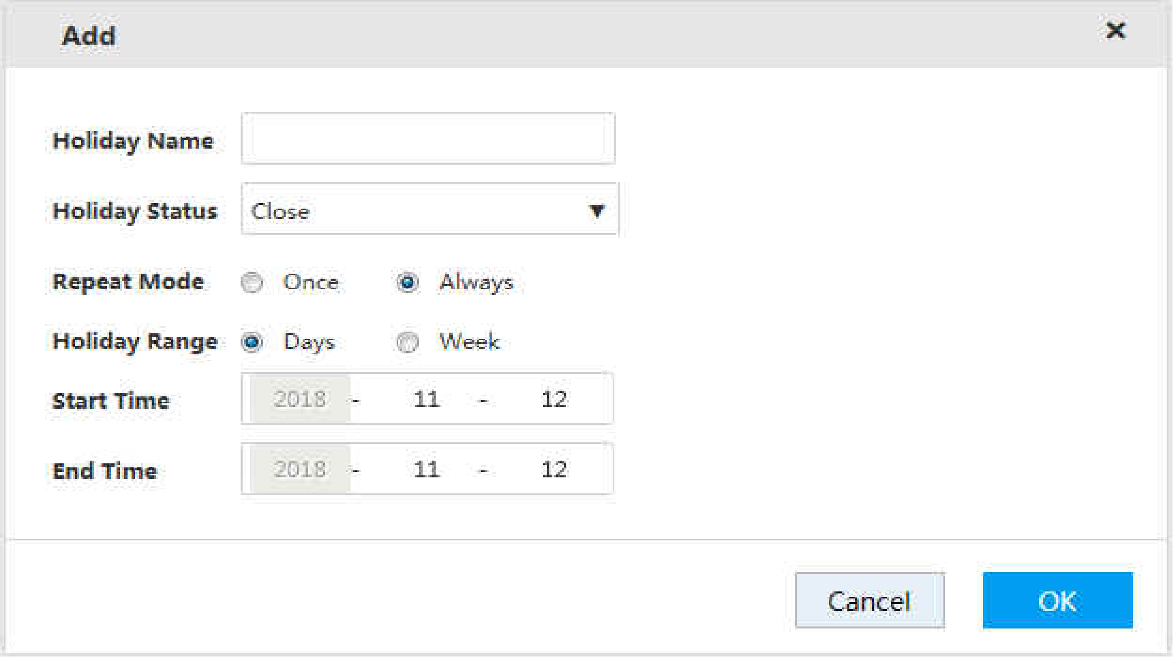
Step 1 Select **Setup > General > Holiday**.

Figure 3-130 Setting holiday (1)



Step 2 Click + .

Figure 3-131 Adding holiday



Holiday Name

Holiday Status: Close

Repeat Mode: ○ Once ● Always

Holiday Range: ● Days ○ Week

Start Time: 2018 - 11 - 12

End Time: 2018 - 11 - 12

Step 3 Configure the parameter.

Table 3-41 Holiday setting parameters

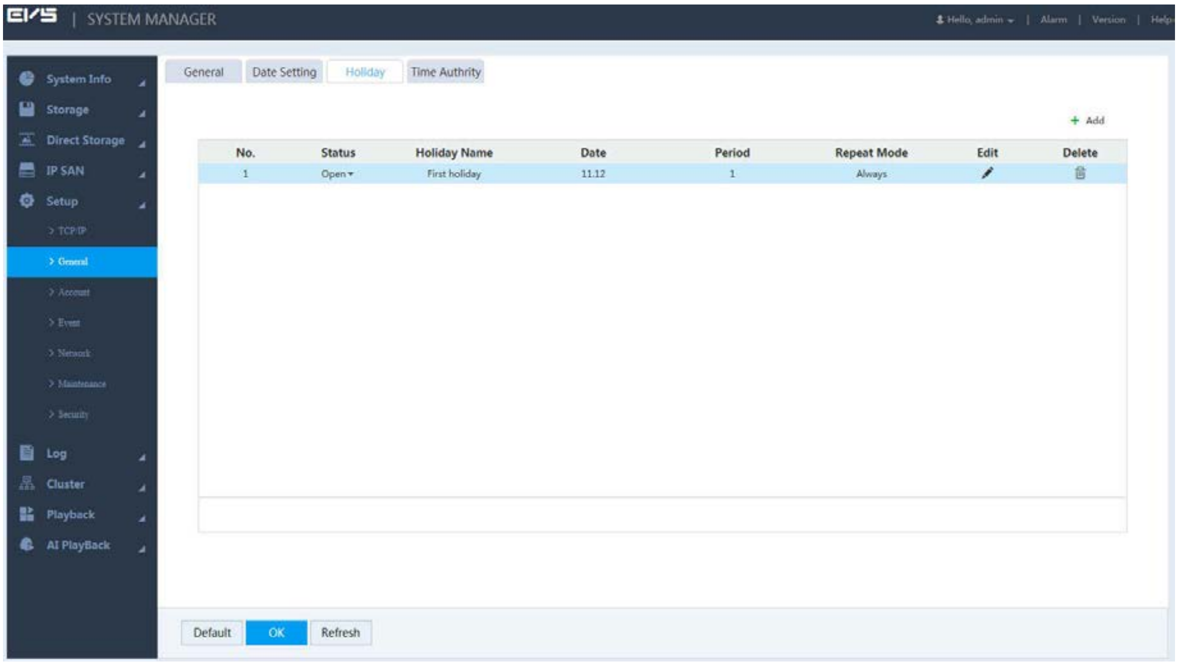
Parameter	Description
Holiday Name	Enter the holiday name.
Holiday Status	Select the holiday status, including Open and Close.
Repeat Mode	Select the repeat mode, including Once and Always. ● Once: The holiday takes effect only once. ● Always: The holiday takes effect repeatedly.

Parameter	Description
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.

- 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)



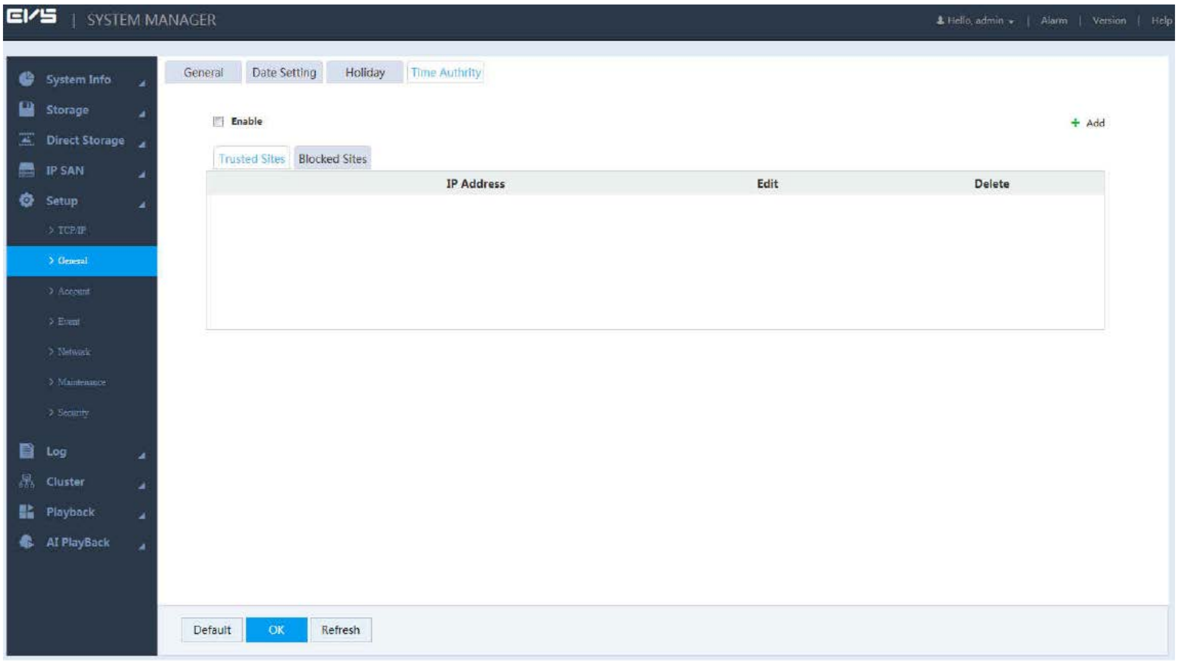
No.	Status	Holiday Name	Date	Period	Repeat Mode	Edit	Delete
1	Open ▾	First holiday	11.12	1	Always	✎	🗑

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**.

Figure 3-133 Timing authority



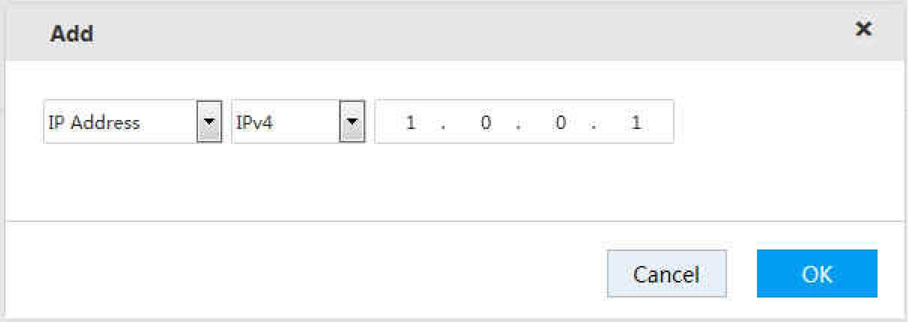
Step 2 Select the **Enable** checkbox to enable this function.

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

Step 4 Add IP host.

1) Click **Add**.

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** page.

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.

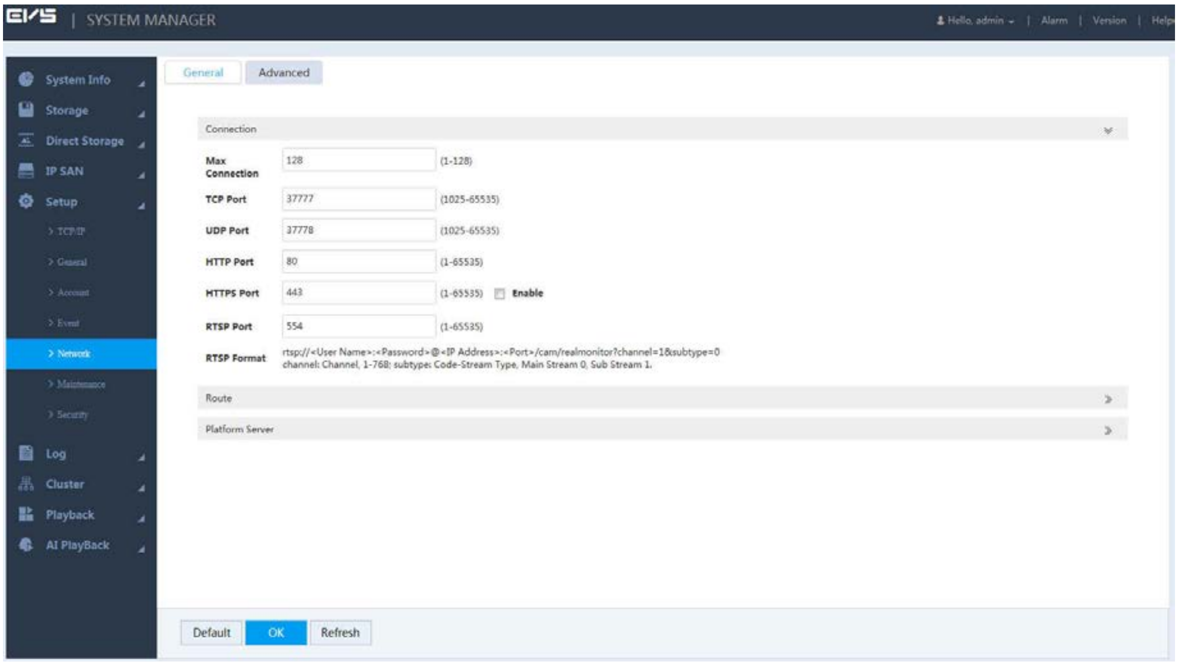
3.14.3.1.1 Connection Port

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**.

Figure 3-135 General network settings



Connection

Max Connection 128 (1-128)

TCP Port 37777 (1025-65535)

UDP Port 37778 (1025-65535)

HTTP Port 80 (1-65535)

HTTPS Port 443 (1-65535) □ Enable

RTSP Port 554 (1-65535)

RTSP Format rtsp://<User Name>:<Password>@<IP Address>:<Port>/cam/realmonitor?channel=1&subtype=0
channel: Channel, 1-768; subtype: Code-Stream Type, Main Stream 0, Sub Stream 1.

Step 3 Configure the parameters.

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

Table 3-42 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.
HTTPS Port	HTTPS communication port. Select the **Enable** checkbox 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.

Parameter	Description
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 username and password. URL format: *rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0* ● Username: 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 username and password. Format see below: *rtsp://ip:port/cam/realmonitor?channel=1&subtype=0*

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

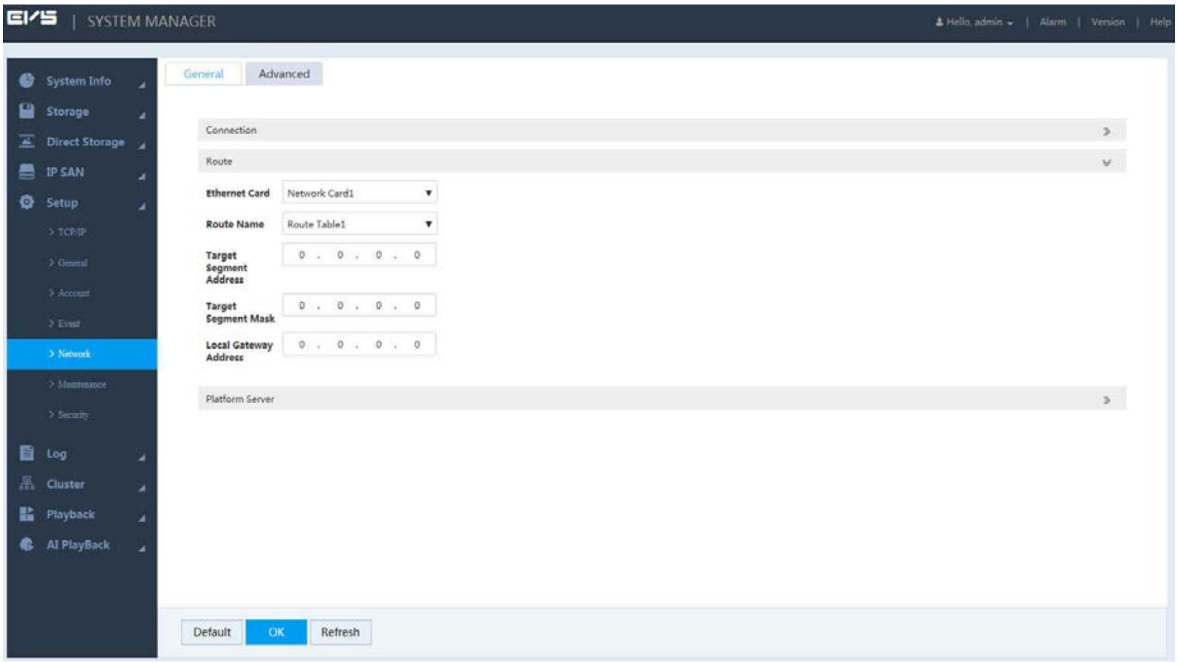
3.14.3.1.2 Route

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**.

Figure 3-136 Route



Ethernet Card: Network Card1

Route Name: Route Table1

Target Segment Address: 0 . 0 . 0 . 0

Target Segment Mask: 0 . 0 . 0 . 0

Local Gateway Address: 0 . 0 . 0 . 0

Step 3 Configure the parameters.

Table 3-43 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.

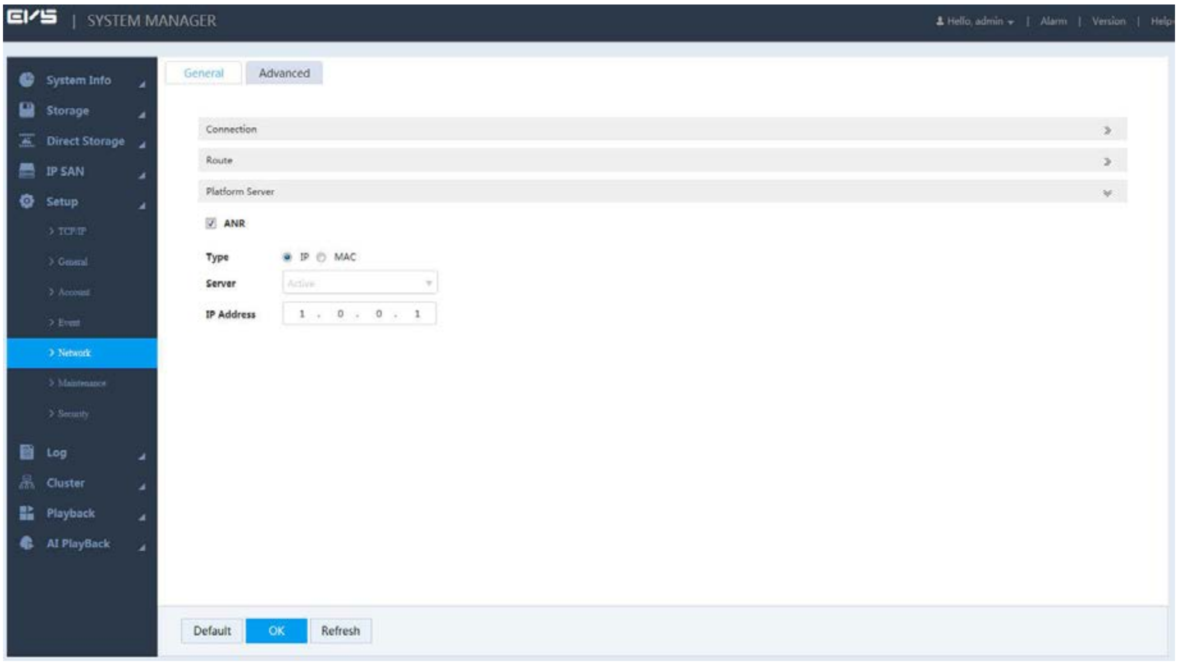
Preparation

- 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**.

Figure 3-137 Platform server



☑ ANR

Type ● IP ○ MAC

Server Active

IP Address 1 . 0 . 0 . 1

Step 3 Configure the parameters.

Table 3-44 Platform server parameters

Parameter	Description
ANR	Select the checkbox 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

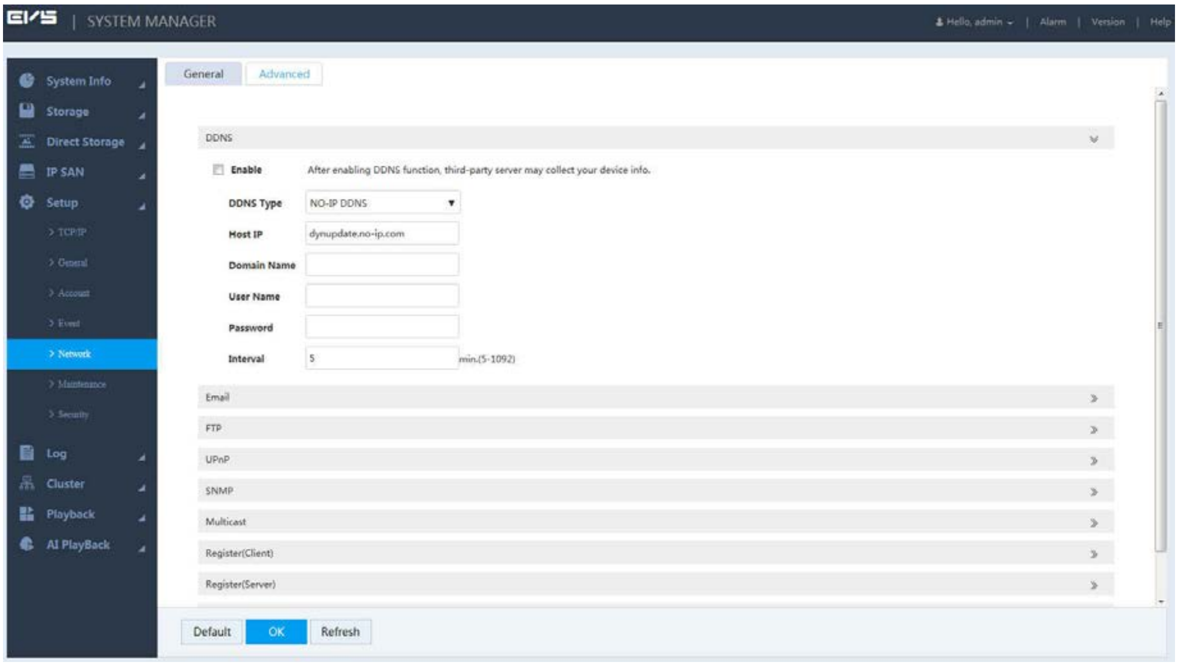
Before executing configuration, you need to confirm the DNS server type that the Device supports. In addition, you need to register on the website of DDNS service provider, and log in to the WAN PC.

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**.

Figure 3-138 DDNS



□ Enable After enabling DDNS function, third-party server may collect your device info.

DDNS Type: NO-IP DDNS

Host IP: dynupdate.no-ip.com

Domain Name:

User Name:

Password:

Interval: 5 min.(5-1092)

Step 3 Select the **Enable** checkbox.

Step 4 Configure the parameters.

Table 3-45 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.
Username	Enter the username and password you got from the DDNS service provider. You need to register an account (including username and password) on the DDNS provider website.
Password	
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.

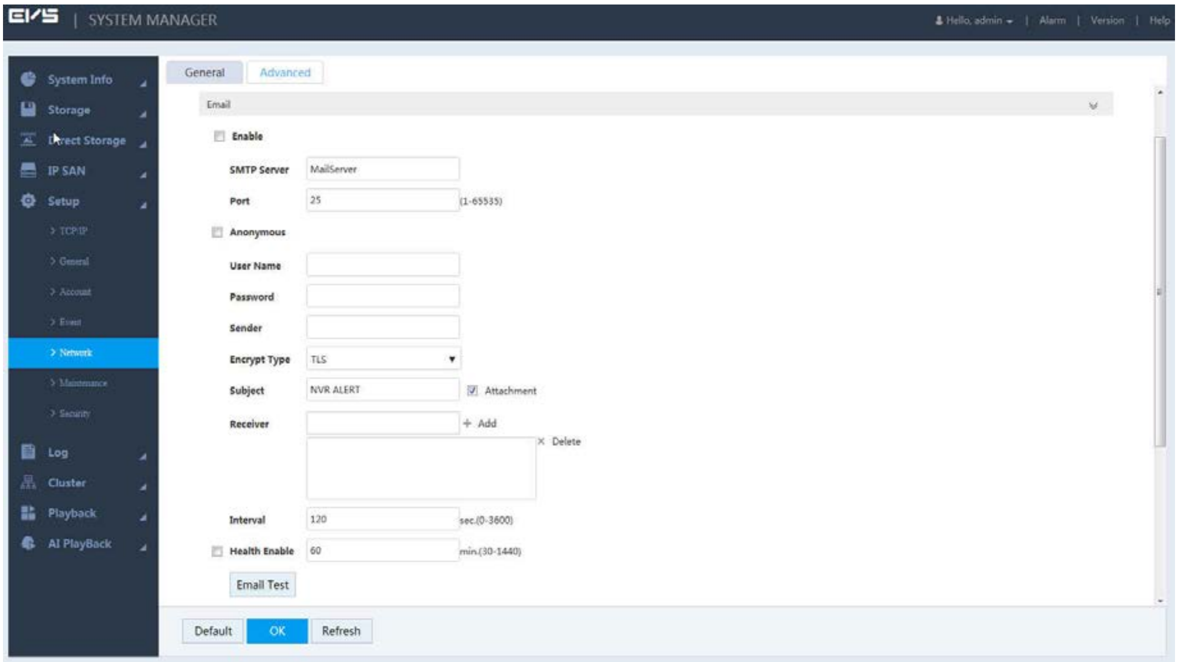
3.14.3.2.2 Email Settings

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**.

Figure 3-139 Email settings



□ Enable

SMTP Server: MailServer

Port: 25 (1-65535)

□ Anonymous

User Name:

Password:

Sender:

Encrypt Type: TLS

Subject: NVR ALERT ☑ Attachment

Receiver:

Interval: 120 sec.(0-3600)

□ Health Enable: 60 min.(30-1440)

Step 3 Select the **Enable** checkbox.

Step 4 Configure the parameters.

Table 3-46 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 checkbox to allow anonymous login.
Username	Enter the username and password of the SMTP server.
Password	
Sender	Enter the Email address of the sender.
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.

Parameter	Description
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 checkbox 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.

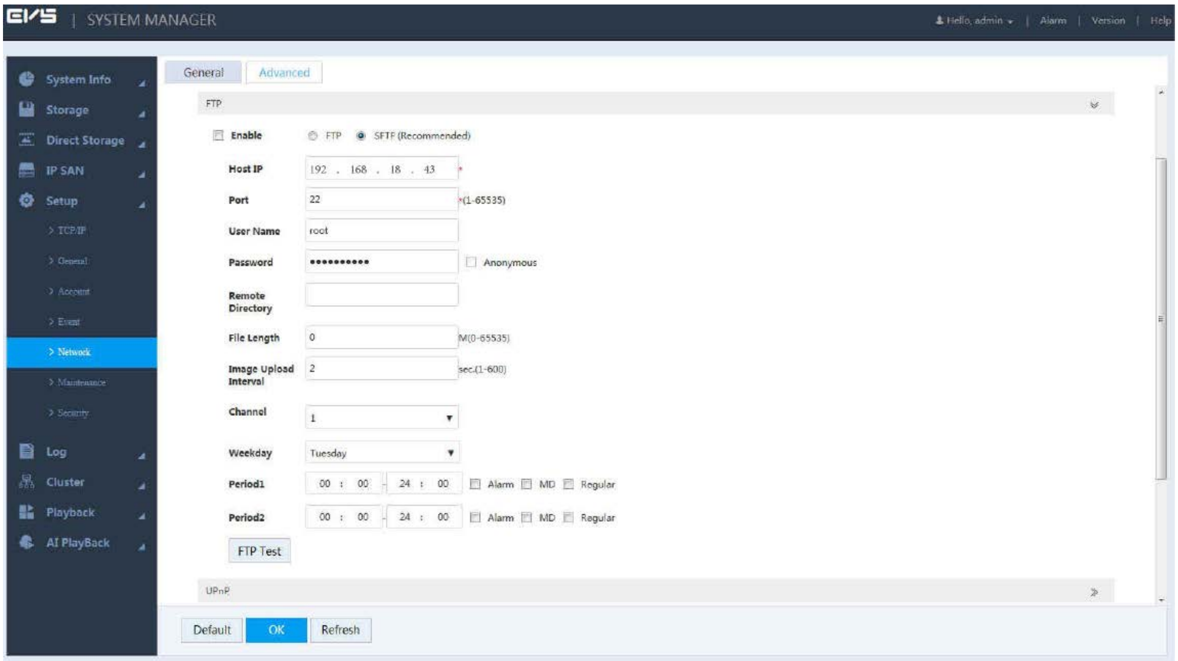
📖

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**.

Figure 3-140 FTP



FTP

□ Enable ○ FTP ● SFTF (Recommended)

Host IP: 192 . 168 . 18 . 43 *

Port: 22 *(1-65535)

User Name: root

Password: •••••••••• □ Anonymous

Remote Directory:

File Length: 0 M(0-65535)

Image Upload Interval: 2 sec.(1-600)

Channel: 1

Weekday: Tuesday

Period1: 00 : 00 - 24 : 00 □ Alarm □ MD □ Regular

Period2: 00 : 00 - 24 : 00 □ Alarm □ MD □ Regular

FTP Test

Step 3 Select the **Enable** checkbox.

Step 4 Configure the parameters.

Table 3-47 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.
Username	The username and password to access FTP server. Select the **Anonymous** checkbox 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.
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.

Parameter	Description
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 "3.8.8.2 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.

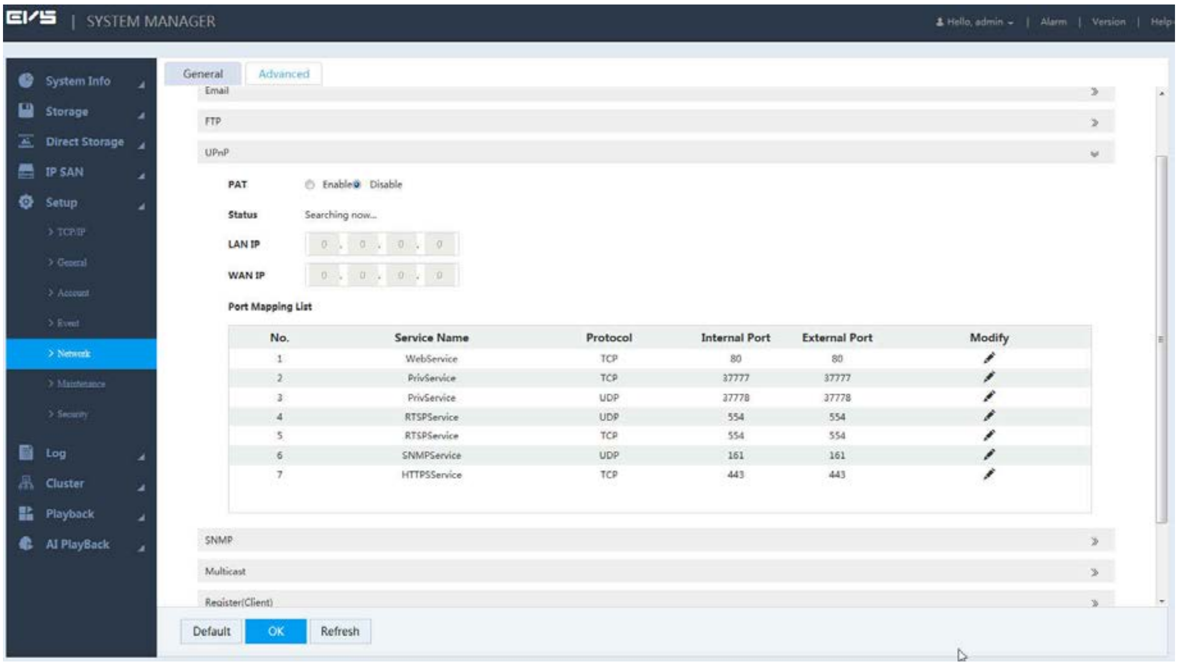
Preparation

- 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**.

Figure 3-141 UPnP



PAT ○ Enable ● Disable

Status Searching now...

LAN IP 0 . 0 . 0 . 0

WAN IP 0 . 0 . 0 . 0

Port Mapping List

No.	Service Name	Protocol	Internal Port	External Port	Modify
1	WebService	TCP	80	80	✎
2	PrivService	TCP	37777	37777	✎
3	PrivService	UDP	37778	37778	✎
4	RTSPService	UDP	554	554	✎
5	RTSPService	TCP	554	554	✎
6	SNMPService	UDP	161	161	✎
7	HTTPSService	TCP	443	443	✎

Step 3 Configure the parameters.

Table 3-48 UPnP parameters

Parameter	Description
PAT	Select the **Enable** checkbox 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.
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.

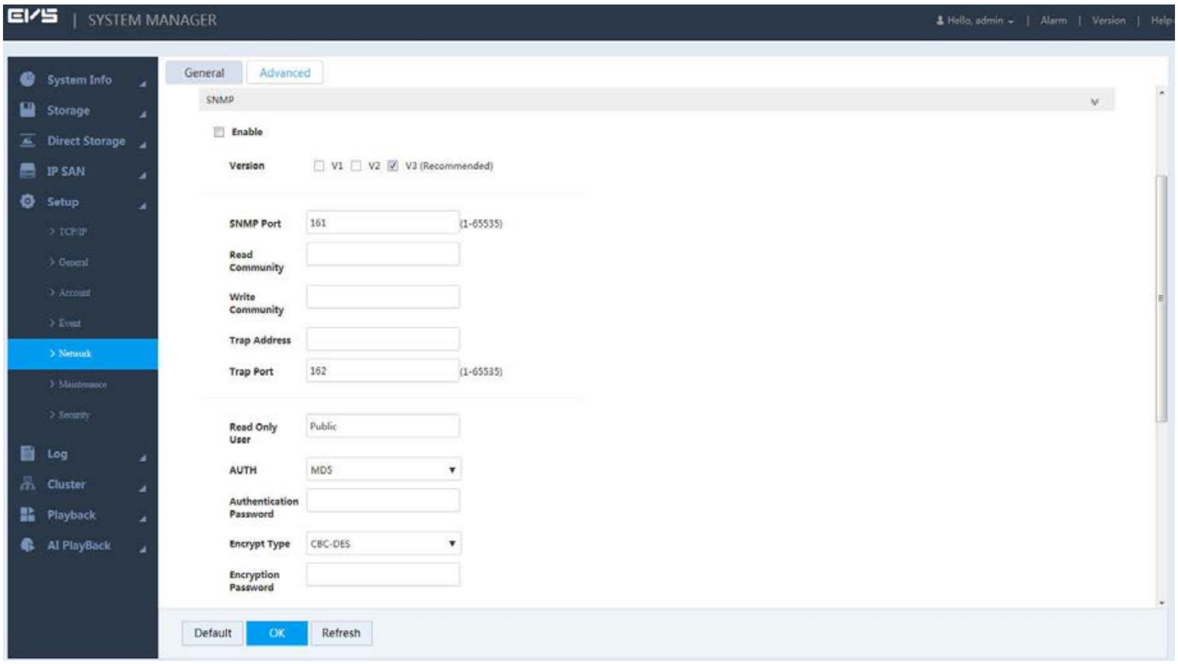
Preparation

- 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**.

Figure 3-142 SNMP



□ Enable

Version □ V1 □ V2 ☑ V3 (Recommended)

SNMP Port 161 (1-65535)

Read Community

Write Community

Trap Address

Trap Port 162 (1-65535)

Read Only User Public

AUTH MD5 ▾

Authentication Password

Encrypt Type CBC-DES ▾

Encryption Password

Step 3 Select the **Enable** checkbox.

Step 4 Configure the parameters.

Table 3-49 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.

Parameter	Description
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.

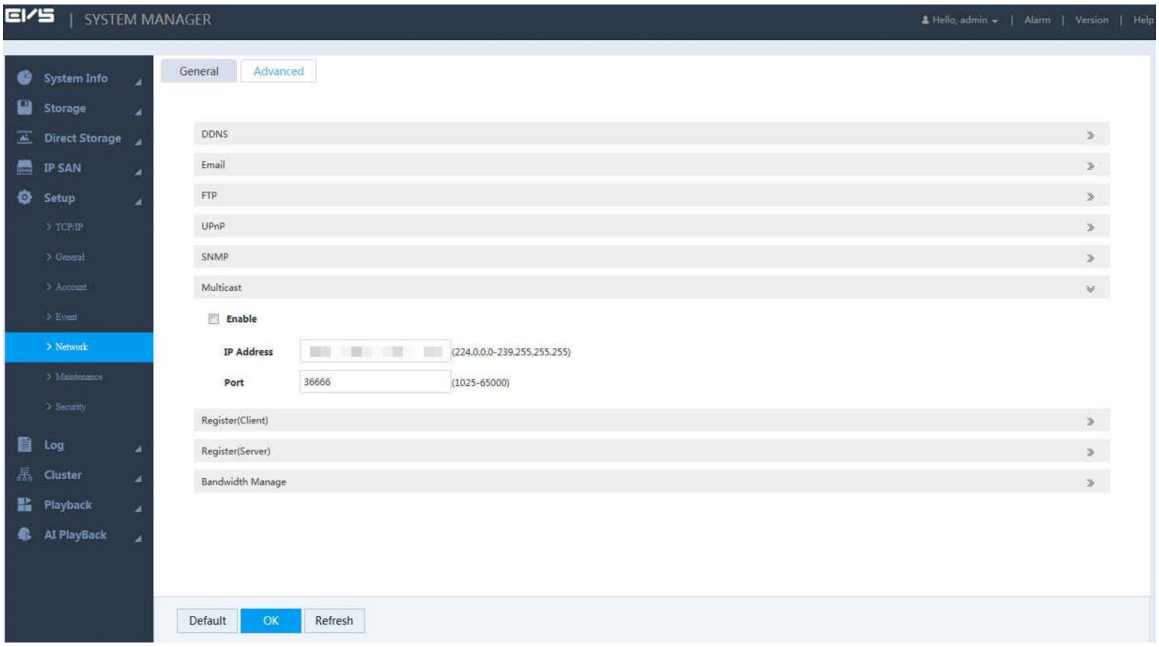
3.14.3.2.6 Multicast Settings

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**.

Figure 3-143 Multicast



☐ Enable

IP Address [redacted] (224.0.0.0-239.255.255.255)

Port 36666 (1025-65000)

Step 3 Select the **Enable** checkbox.

Step 4 Enter the parameters.

Table 3-50 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.

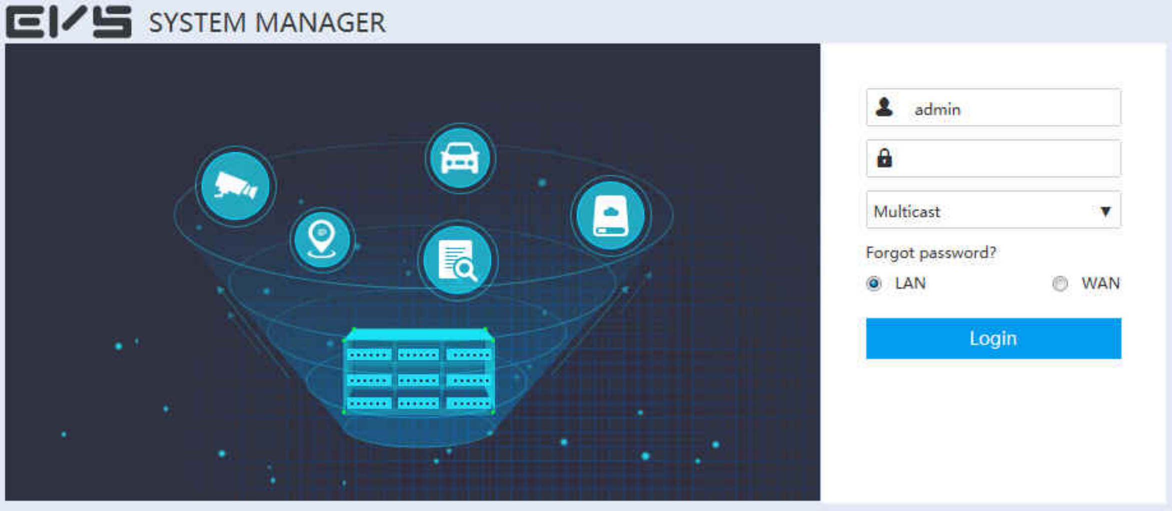
Step 5 Click **OK** to save the configuration.

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

Enter the login page of the Device, and select Multicast as the login type.

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



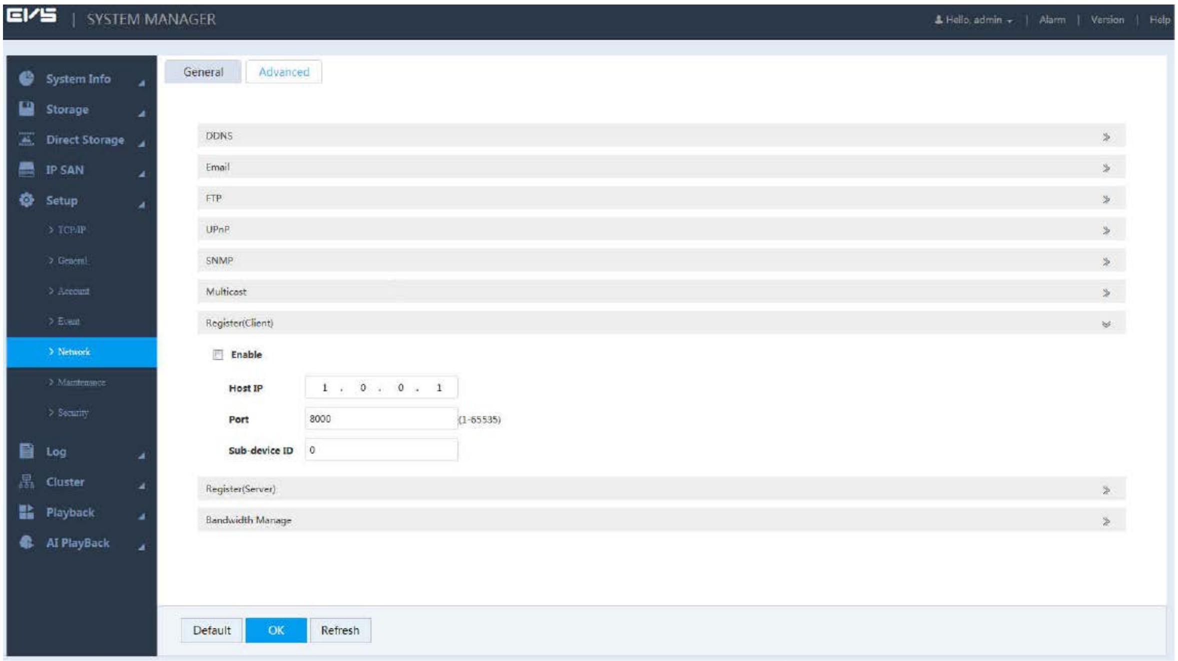
3.14.3.2.7 Active Register (Client)

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)**.

Figure 3-145 Active register (client)



□ Enable

Host IP: 1 . 0 . 0 . 1

Port: 8000 (1-65535)

Sub-device ID: 0

Step 3 Select the **Enable** checkbox.

Step 4 Enter the parameters.

Table 3-51 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.
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.

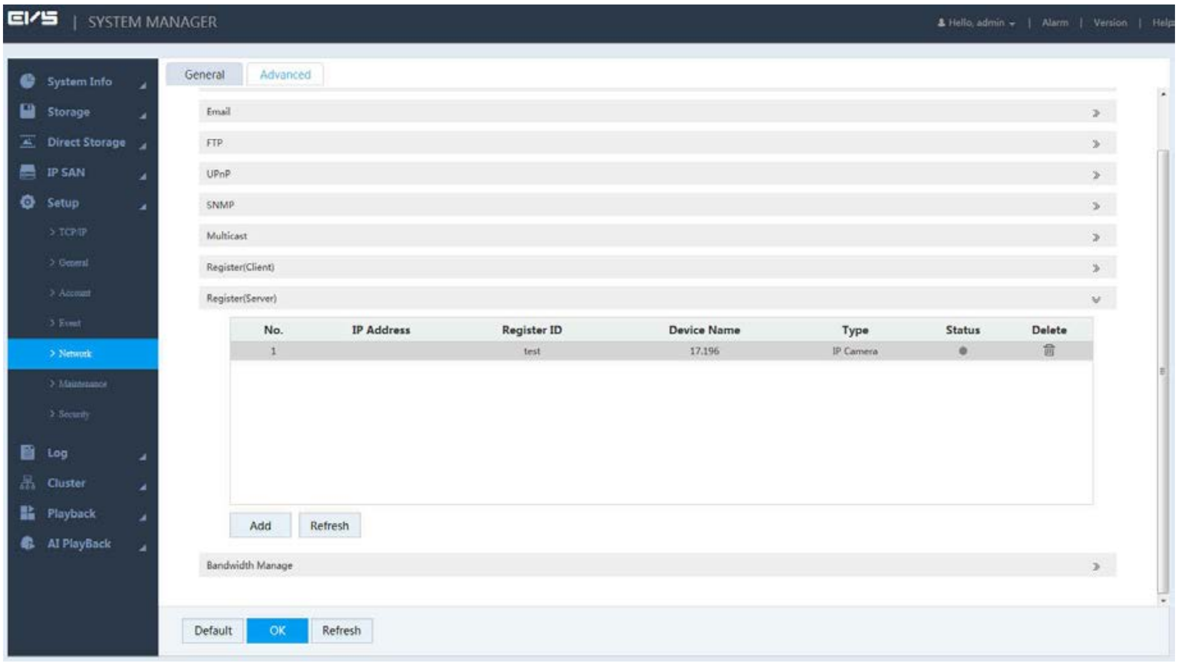
3.14.3.2.8 Active Register (Server)

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)**.

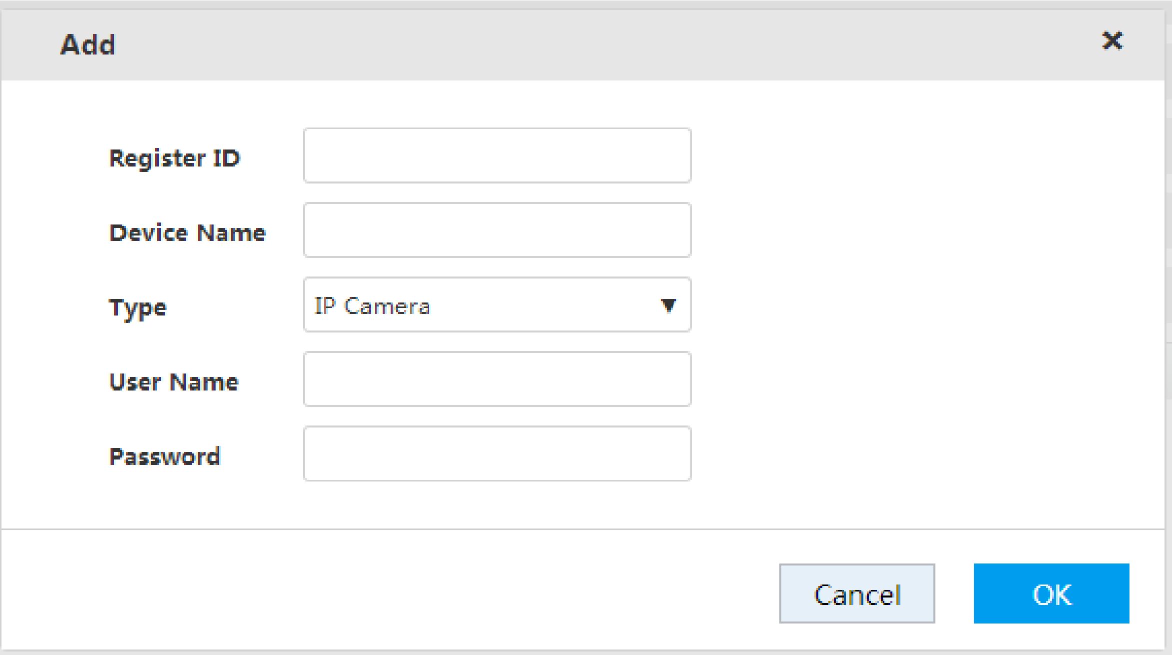
Figure 3-146 Active register (server)



No.	IP Address	Register ID	Device Name	Type	Status	Delete
1		test	17.196	IP Camera	●	🗑

Step 3 Click **Add**.

Figure 3-147 Adding register (server)



Register ID

Device Name

Type: IP Camera

User Name

Password

Step 4 Configure the parameters.

Table 3-52 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.
Username	Enter the username 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

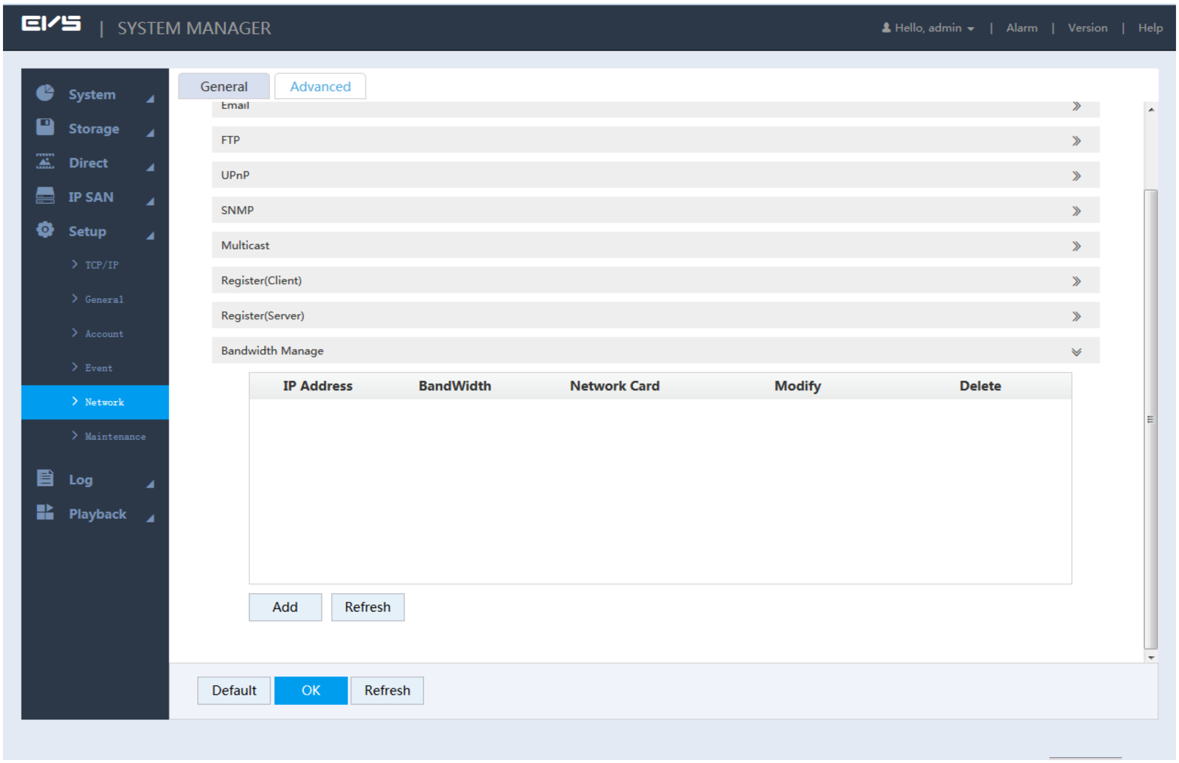
Control different users to have different bandwidth.

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**.

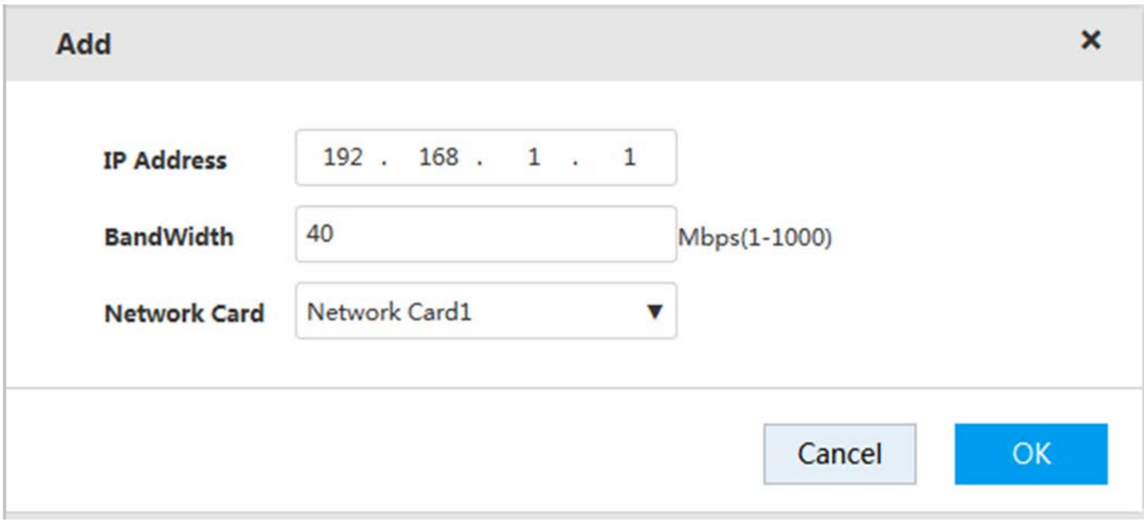
Step 2 Click » corresponding to **Bandwidth Management**.

Figure 3-148 Bandwidth Management



Step 3 Click **Add**.

Figure 3-149 Adding Bandwidth



IP Address: 192 . 168 . 1 . 1

BandWidth: 40 Mbps(1-1000)

Network Card: Network Card1

Step 4 Configure the parameters.

Table 3-53 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

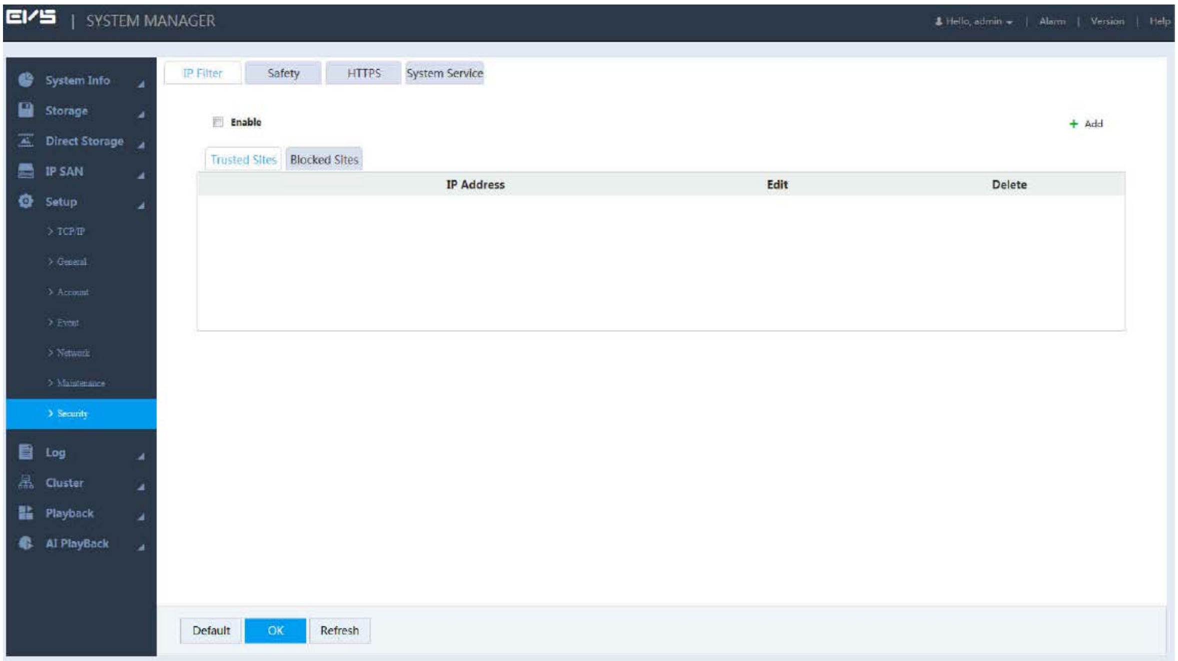
To ensure security of network and data, it is necessary to set the access permission of IP host (PC or server with IP) and password reset function.

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**.

Figure 3-150 IP filter



Step 2 Select the **Enable** checkbox to enable IP filter function.

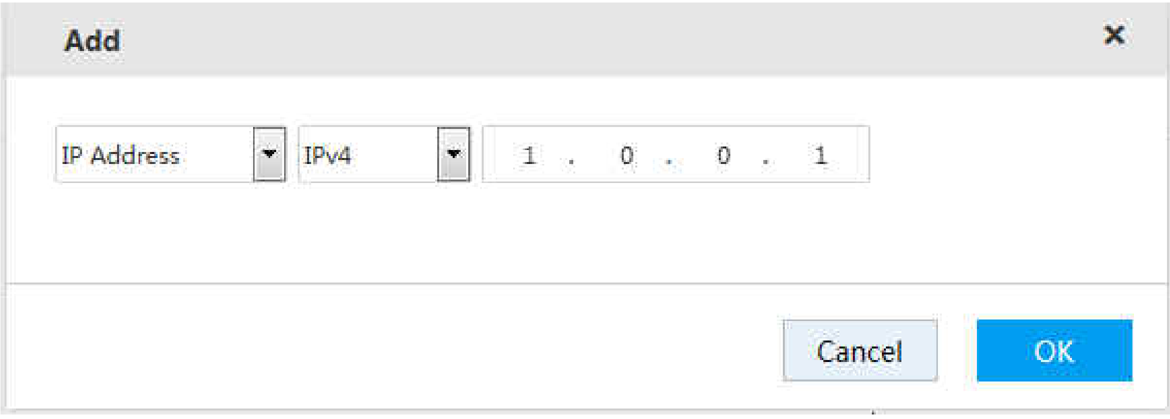
The **Trusted Sites** and **Blocked Sites** boxes are displayed.

Step 3 Add trusted or blocked sites.

1) Select **Trusted Sites** or **Blocked Sites**.

2) Click +.

Figure 3-151 Add



3) Configure the parameters.

Table 3-54 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**.

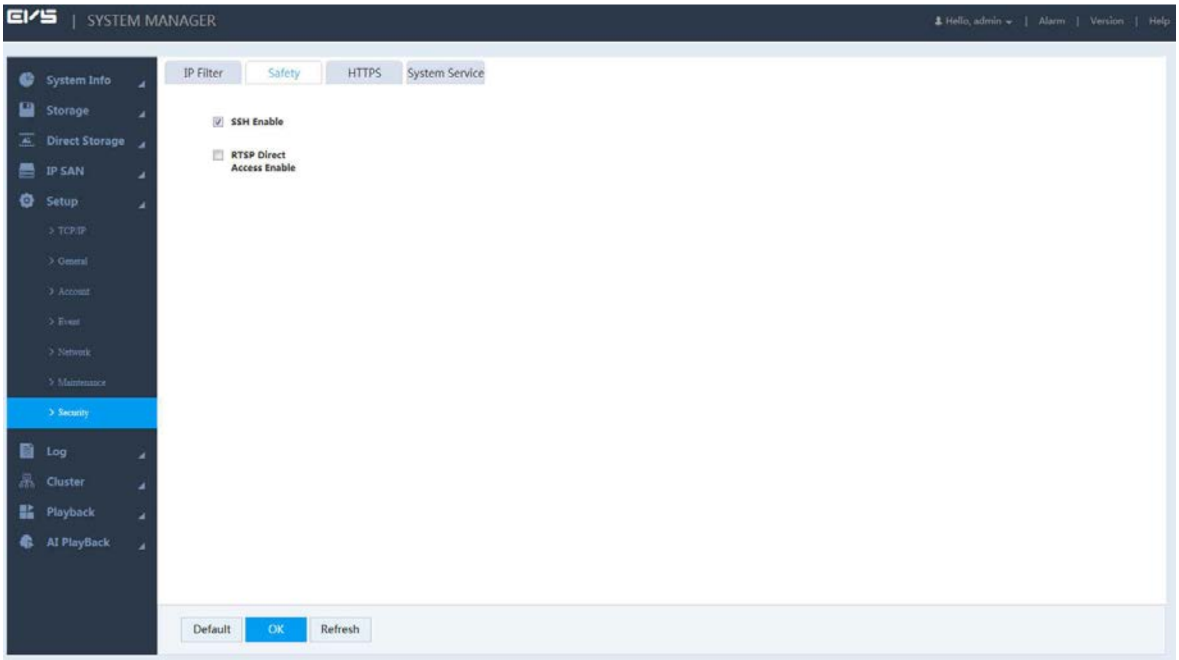
Click the **Trusted Sites** tab or **Blocked Sites** tab to view the IP host information in corresponding list.

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**.

Figure 3-152 Safety


☑ SSH Enable

□ RTSP Direct Access Enable

Step 2 Select the **SSH Enable** checkbox and **RTSP Direct Access Enable** checkbox.

- 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 page, 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

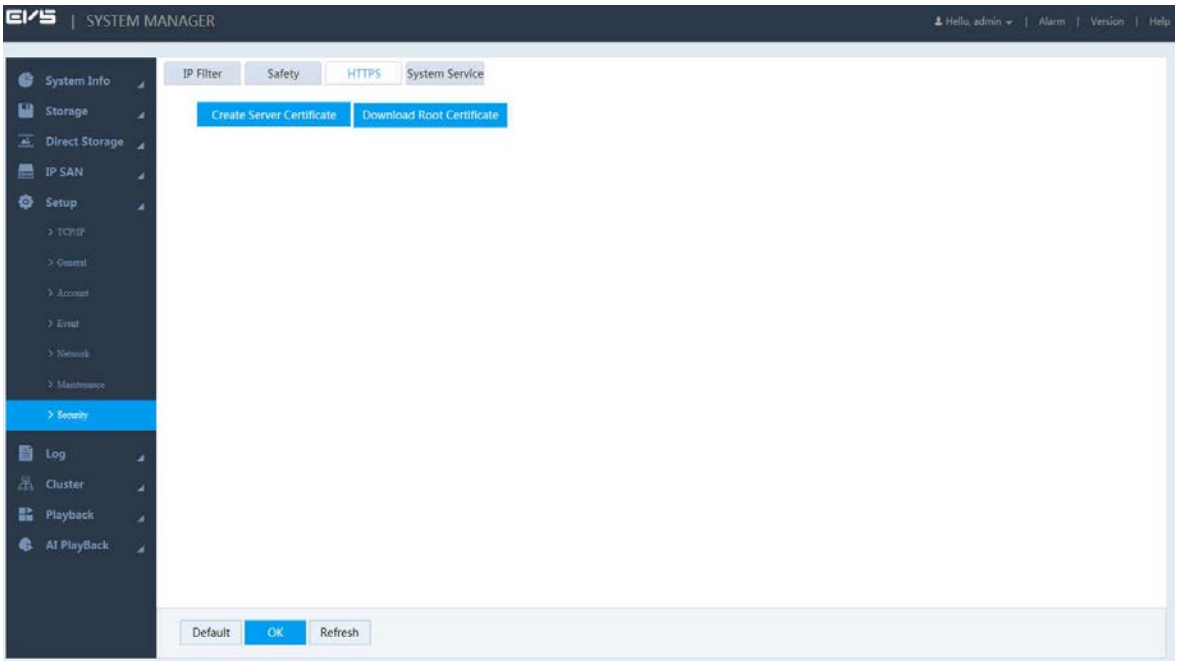
Only after enabling HTTPS port can you create server certificate and download root certificate. For detailed operations to enable HTTPS, see "3.14.3.1.1 Connection Port".

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.

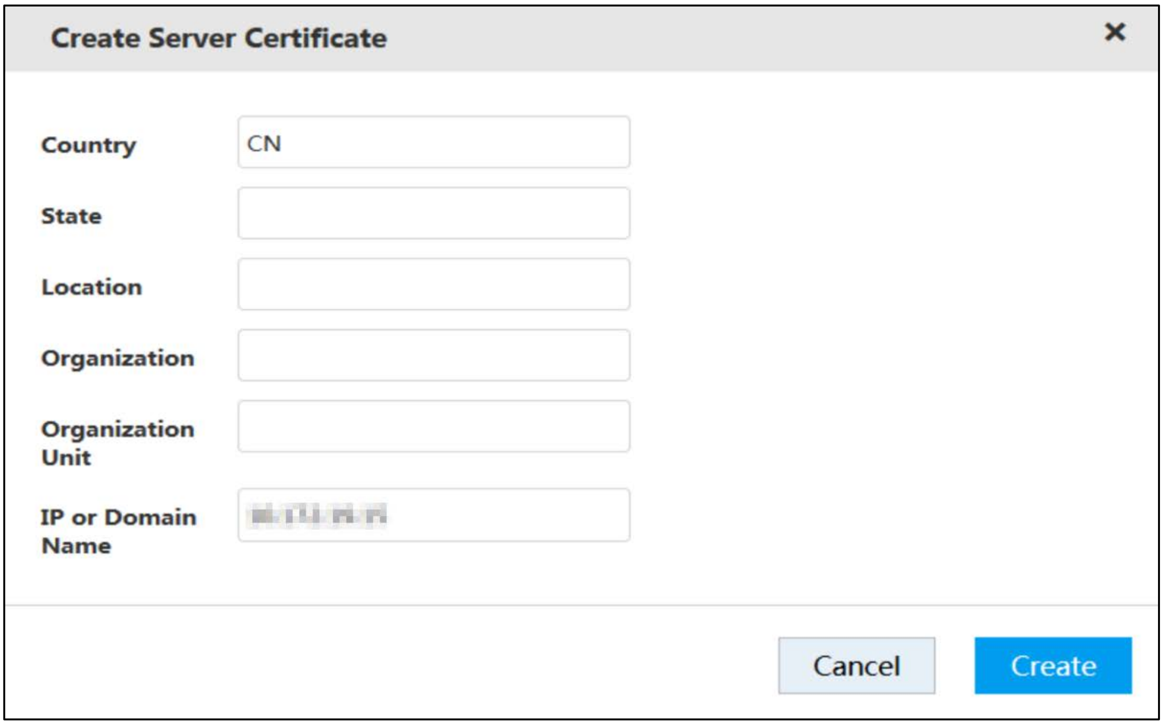
Step 1 Select **Setup** > **Security** > **HTTPS**.

Figure 3-153 HTTPS



Step 2 Click **Create Server Certificate**.

Figure 3-154 Creating server certificate



Create Server Certificate ×

Country: CN

State:

Location:

Organization:

Organization Unit:

IP or Domain Name: [redacted]

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.

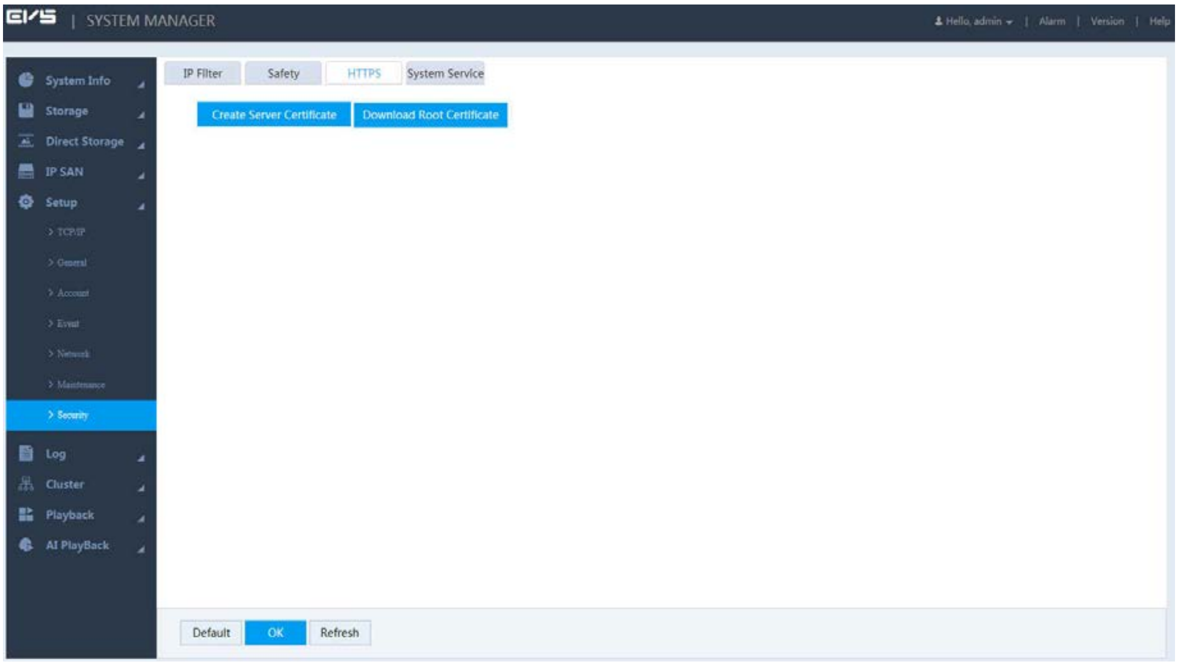
Step 4 Click **Create**.

The system prompts **Creation Succeed** when it is done successfully.

Download Root Certificate

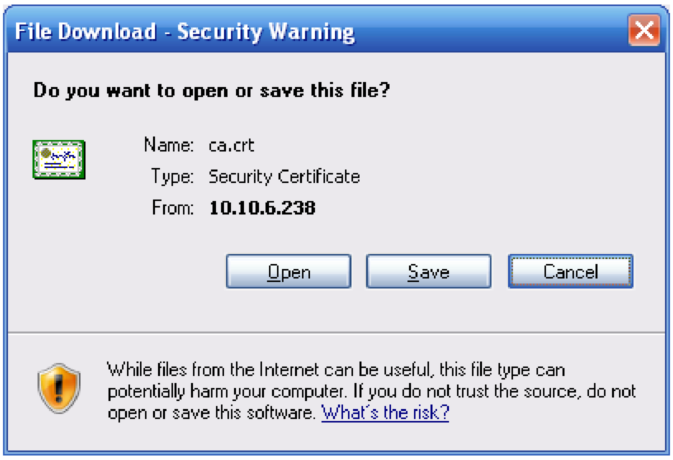
Step 1 Select **Setup** > **Security** > **HTTPS**.

Figure 3-155 HTTPS



Step 2 Click **Download Root Certificate**, and the **File Download-Security Warning** dialogue box pops up.

Figure 3-156 File download



File Download - Security Warning

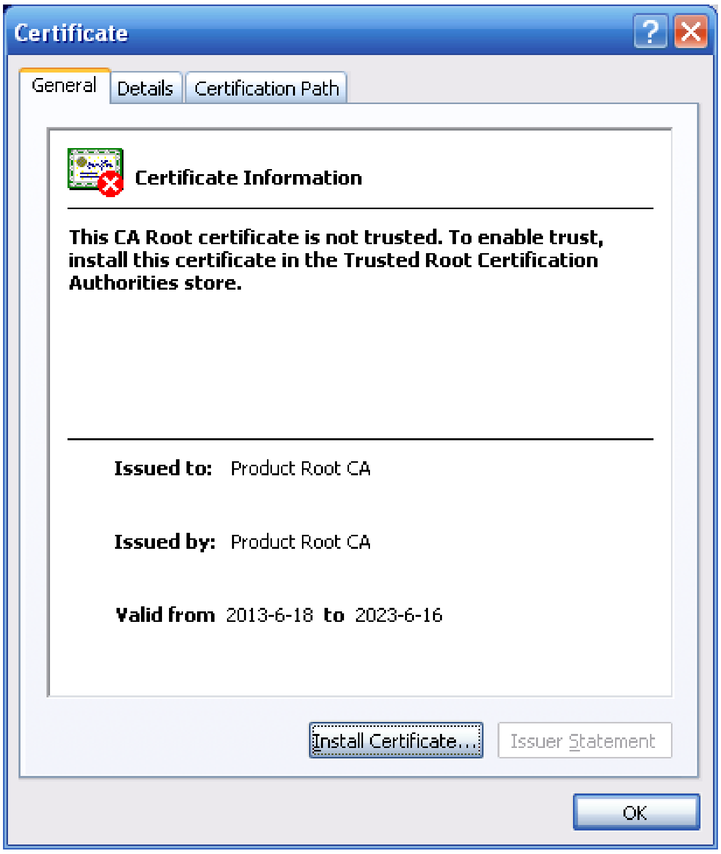
Do you want to open or save this file?

Name: ca.crt
Type: Security Certificate
From: 10.10.6.238

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Step 3 Click **Open**.

Figure 3-157 Certificate information



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

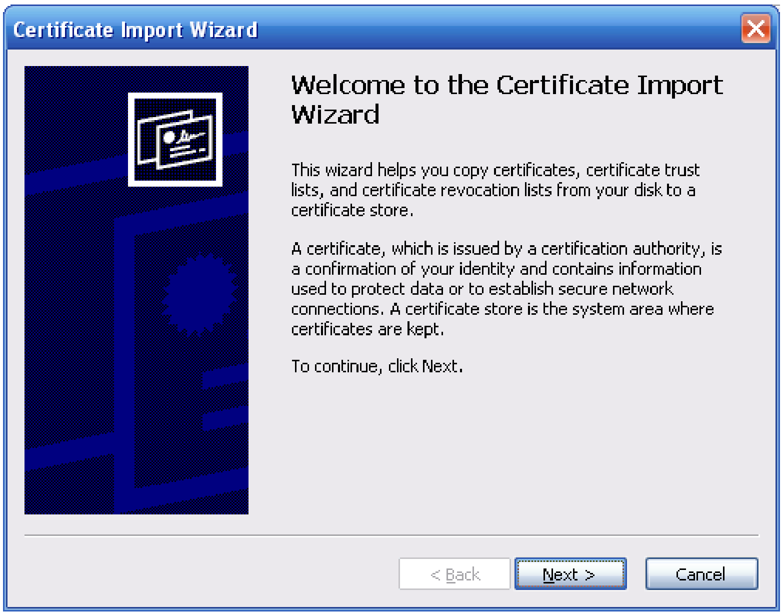
Issued to: Product Root CA

Issued by: Product Root CA

Valid from 2013-6-18 to 2023-6-16

Step 4 Click **Install Certificate**.

Figure 3-158 Certificate import wizard



Certificate Import Wizard

Welcome to the Certificate Import Wizard

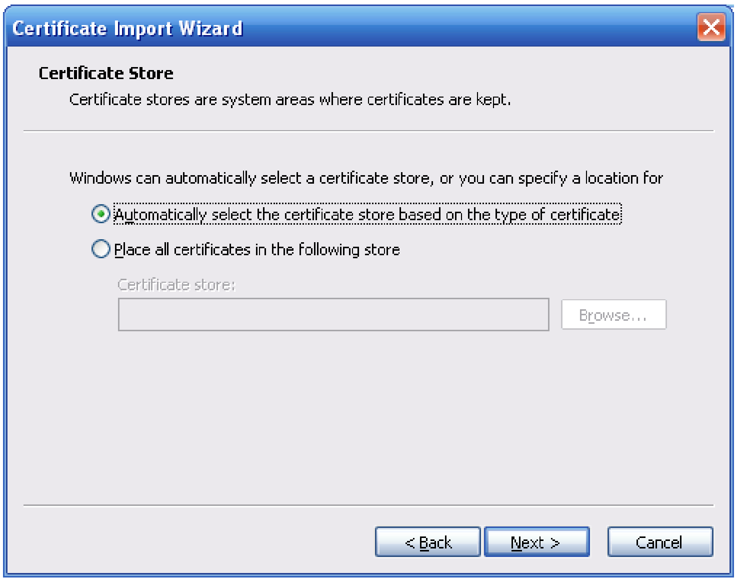
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 5 Click **Next**.

Figure 3-159 Certificate storage



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

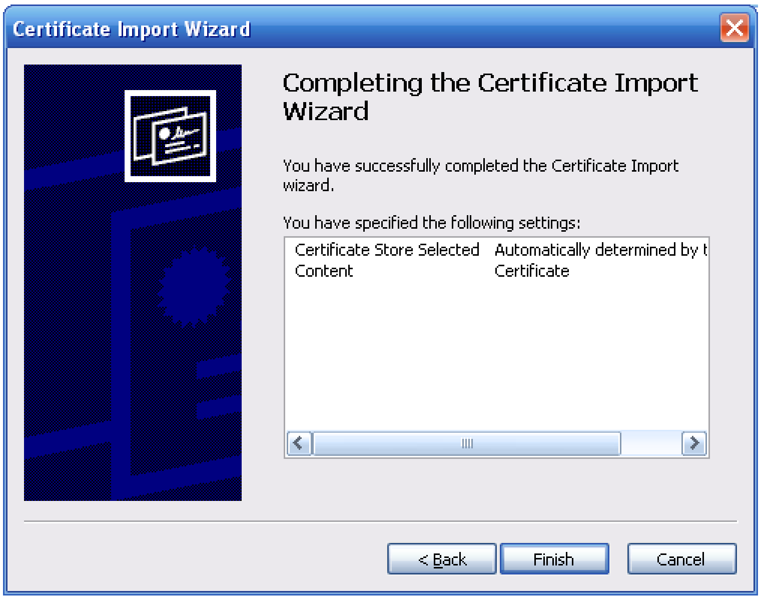
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Step 6 Select the storage location and click **Next**.

Figure 3-160 Completing certificate import



Completing the Certificate Import Wizard

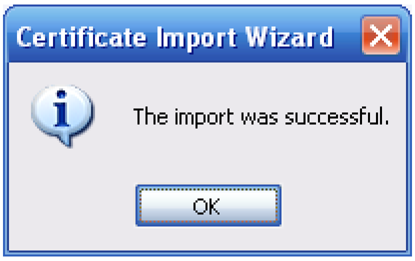
You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

Step 7 Click **Finish** and a dialogue box pops up showing **The import was successful**.

Figure 3-161 Success



The import was successful.

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.

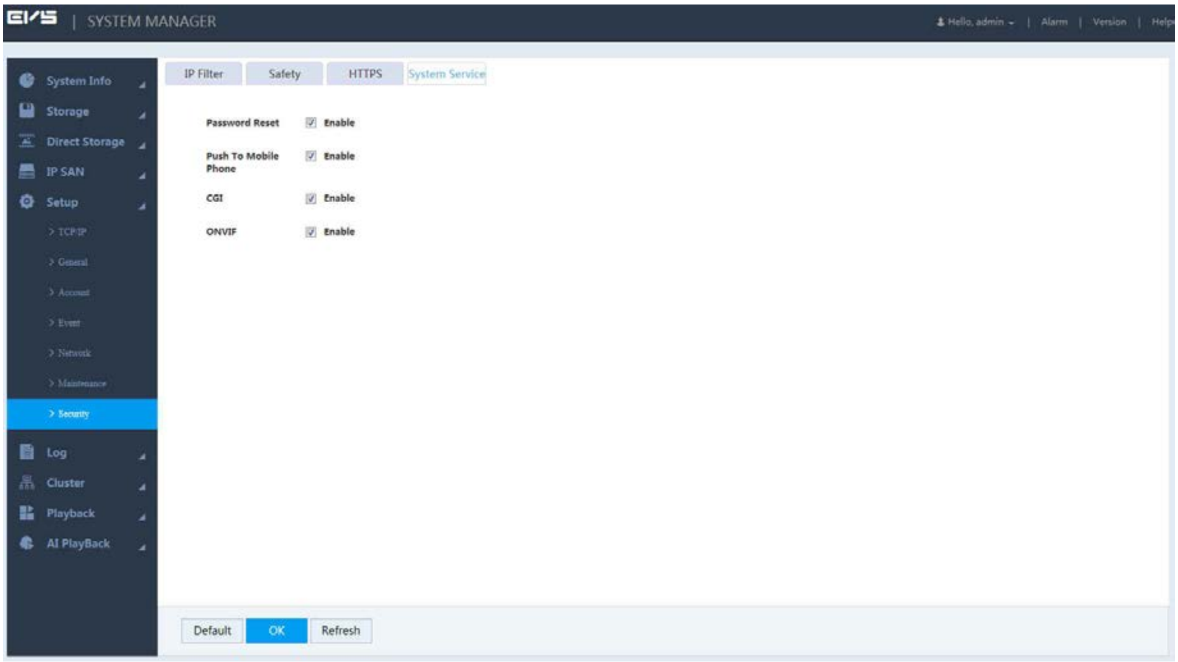
- *xx.xx.xx.xx* refers to the IP address or domain name of the Device.
- *Port* corresponds to the HTTPS port number. You can enter https://xx.xx.xx.xx directly if using the default port number 443.

3.14.4.4 System Service

You can enable and disable system services of the Device.

Step 1 Select **Setup > Security > System Service**.

Figure 3-162 System service



Password Reset ☑ Enable

Push To Mobile Phone ☑ Enable

CGI ☑ Enable

ONVIF ☑ Enable

Step 2 Configure the parameters.

Table 3-55 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

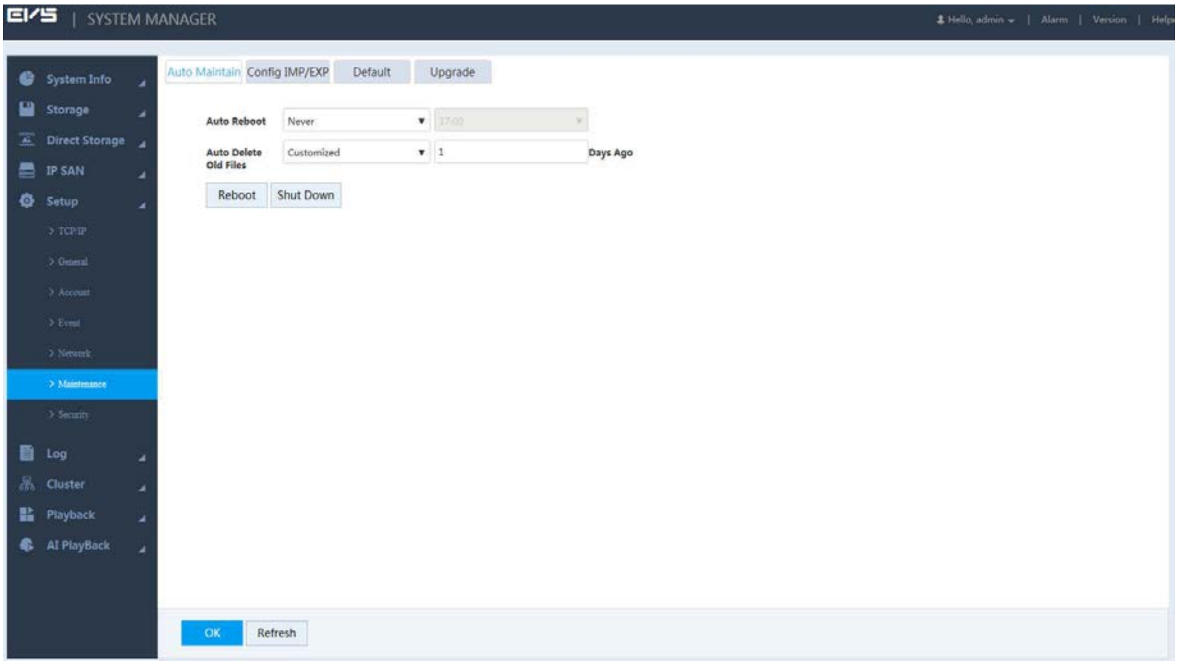
System maintenance includes operations of restarting the Device, deleting old files, restoring factory default, and upgrading the system. It helps clear the faults and errors during system operation, and improves the operation efficiency of the Device.

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**.

Figure 3-163 Auto maintenance



Auto Reboot: Never

Auto Delete Old Files: Customized 1 Days Ago

Step 2 Select time for **Auto Reboot** and **Auto Delete Old Files**.

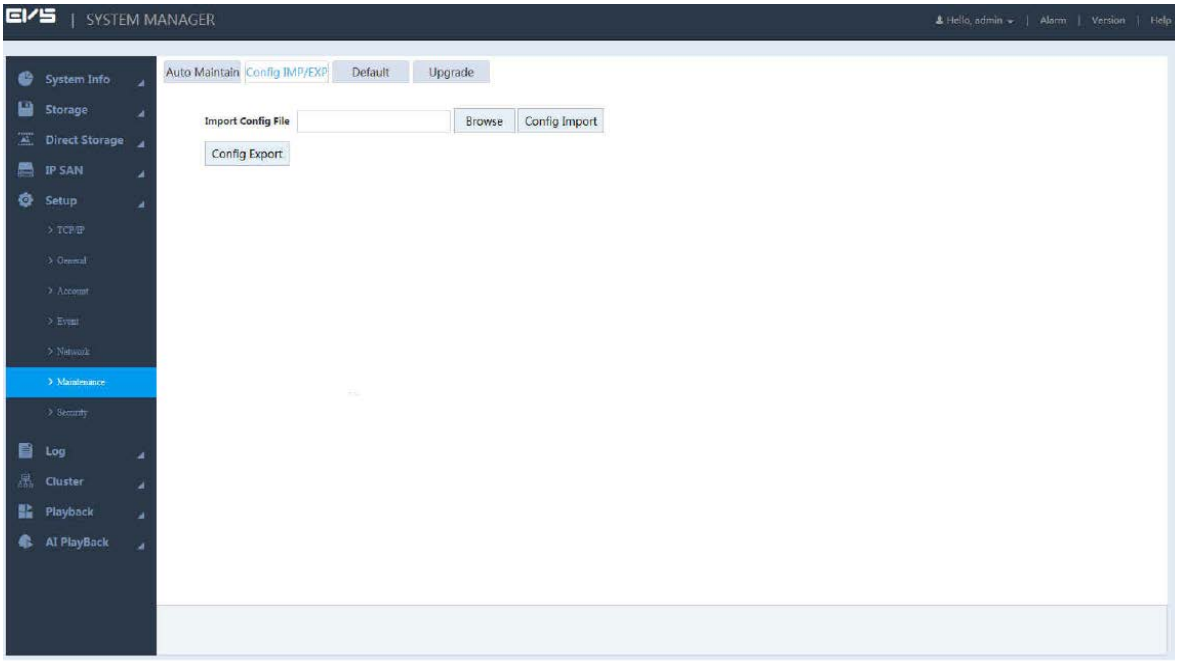
Step 3 Click **OK** to save the configuration.

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**.

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

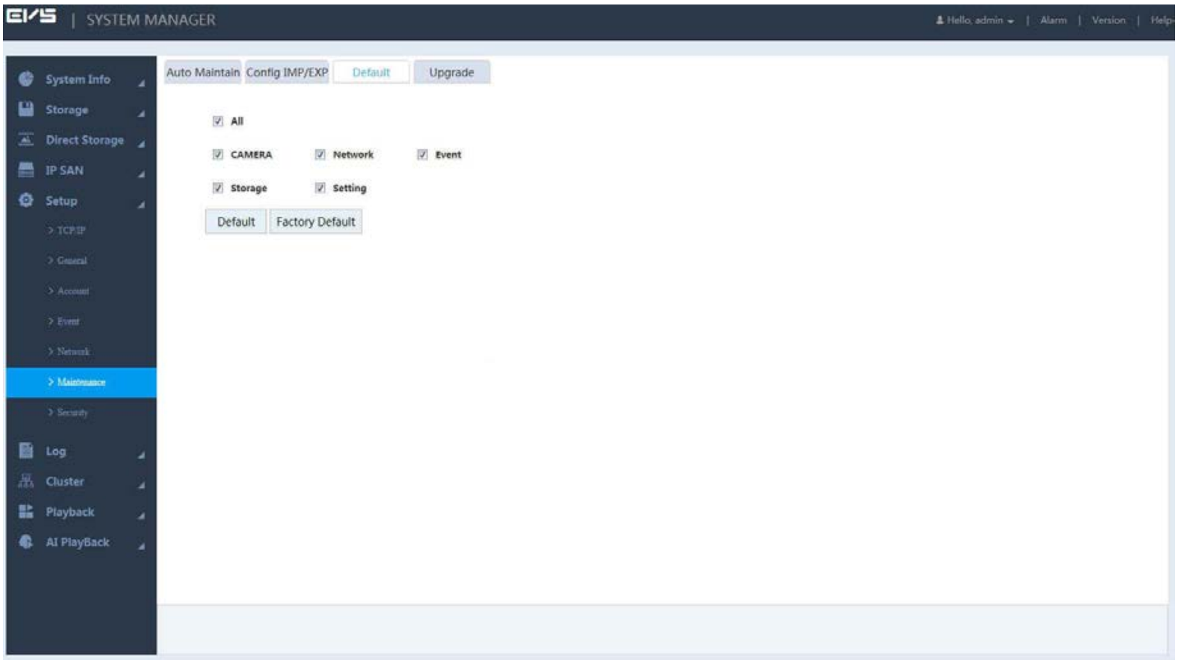
When the Device is running slowly or there is configuration error, you can try to solve the problem by restoring defaults.

⚠

After restoring defaults, the existing system configuration will be lost. Operate with care.

Step 1 Select **Setup** > **Maintenance** > **Default**.

Figure 3-165 Restoring defaults



☑ All

☑ CAMERA ☑ Network ☑ Event

☑ Storage ☑ Setting

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

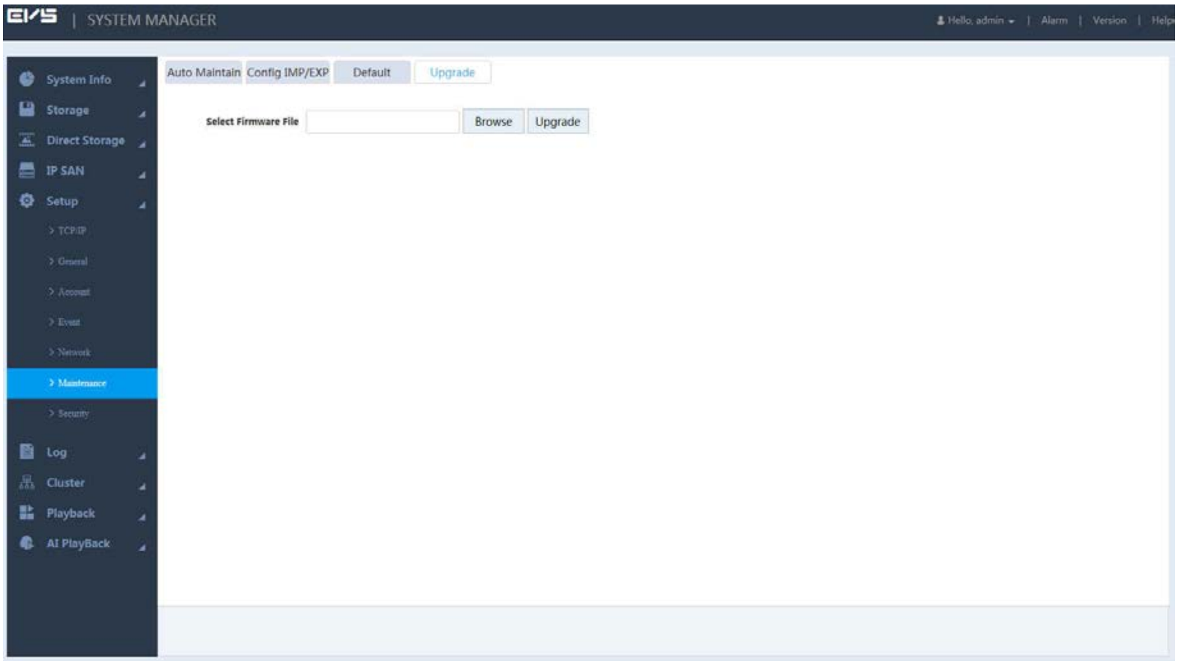
Upgrade the system of the Device by importing upgrade files. Upgrade files are files with *.bin.

⚠

- 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**.

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 main 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 main devices are working. If the main device breaks down, the backup device not working will replace it to work according to the configuration of the main one and the cluster IP. After the main one is restored, the backup one transmits back the configuration, cluster IP and records during the breakdown, and the main one goes on working.

There is a management server called dispatching console (DSC) in the N+M cluster. DSC performs timely dispatching for the main 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

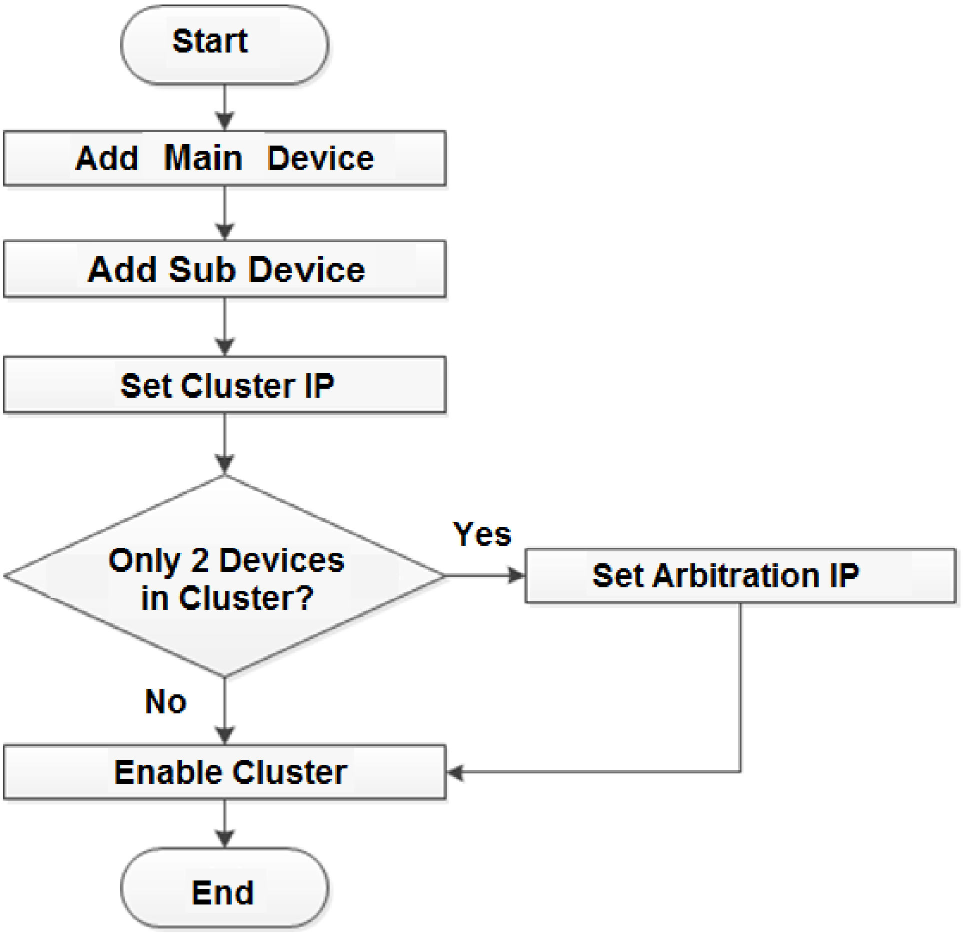
You can create cluster, view cluster information, restore main device and set arbitration IP.

3.15.1.1 Creating Cluster

Creating cluster requires organizing multiple devices into a cluster. For the creation flow, see Figure 3-167.

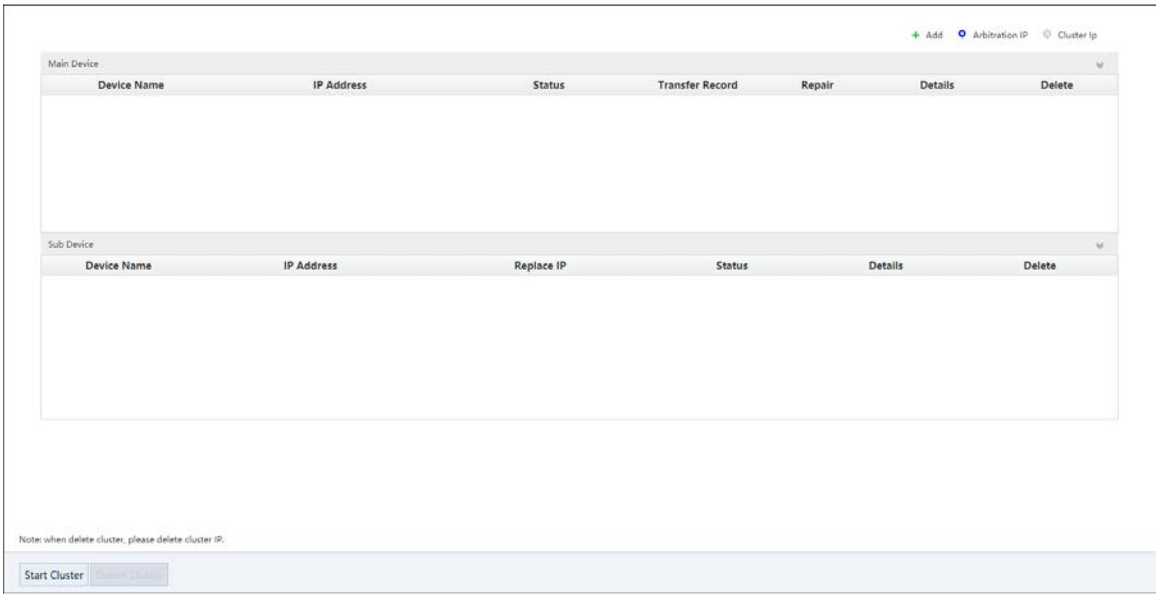
When creating a cluster, the first standby device works as DCS by default. The priority of the rest standby devices is defined by the adding sequence. The earlier the device is added, the higher its priority is.

Figure 3-167 Creating cluster



Step 1 Select **Cluster > Configuration**.

Figure 3-168 Cluster configuration



Main Device

Device Name	IP Address	Status	Transfer Record	Repair	Details	Delete

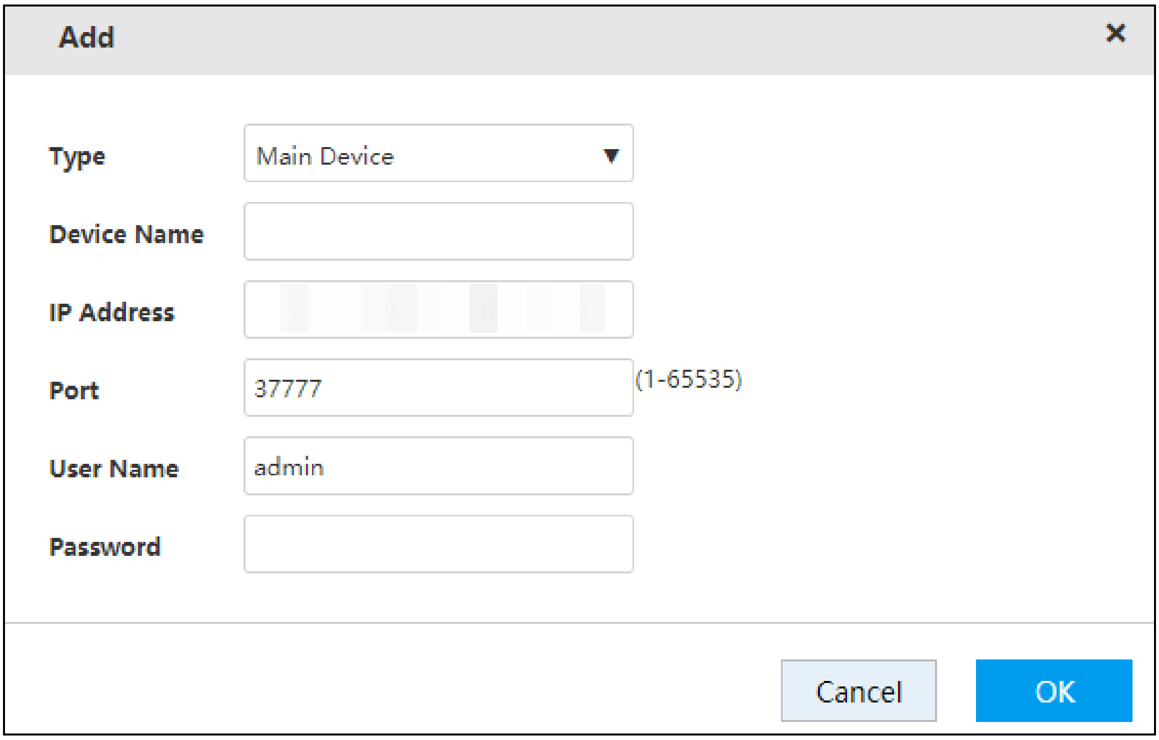
Sub Device

Device Name	IP Address	Replace IP	Status	Details	Delete

Note: when delete cluster, please delete cluster IP.

Step 2 Adding main device or backup device.

1) Click + .


Add

Type: Main Device ▼

Device Name:

IP Address:

Port: 37777 (1-65535)

User Name: admin

Password:

Figure 3-169 Adding main/backup device

2) Configure the parameters.

Table 3-56 Server parameters

Parameter	Description
Type	Select the device type, including main device and backup device.
Device Name	Enter the device name.
IP Address	Enter the IP address of the main 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.
Username	Enter the username and password of the main device or backup device. That is, the username and password to access the web of the Device.
Password	

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

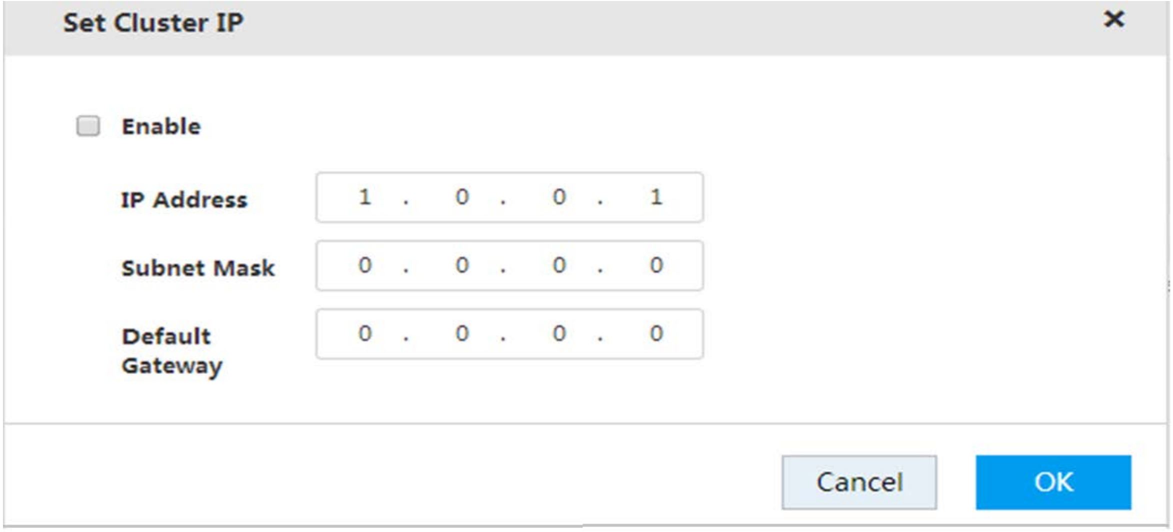
The system returns to the **Configuration** page.

Step 3 Setting cluster IP.

Configuring cluster IP requires creating a virtual IP address, and you can access and manage the main 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 main device fails and the backup device is used.

1) Click .

Figure 3-170 Setting cluster IP



Set Cluster IP

□ Enable

IP Address: 1 . 0 . 0 . 1

Subnet Mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

2) Select the **Enable** checkbox. Enter the **IP Address**, **Subnet Mask** and **Default Gateway**.

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

The system returns to the **Configuration** page.

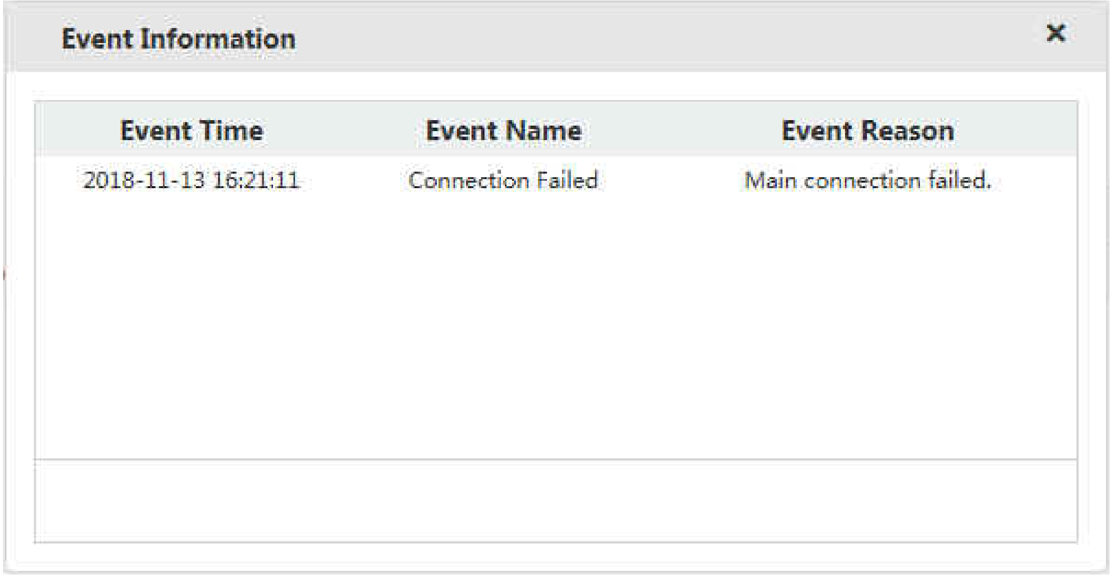
Step 4 Click **Start Cluster** to enable cluster function.

- 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 main or backup device. Click **Delete Cluster** to delete a cluster.

3.15.1.2 Viewing Information

Click 🔍 corresponding to the main device or backup device. You can view its log information, including event time, name and reason.

Figure 3-171 Event information



Event Information

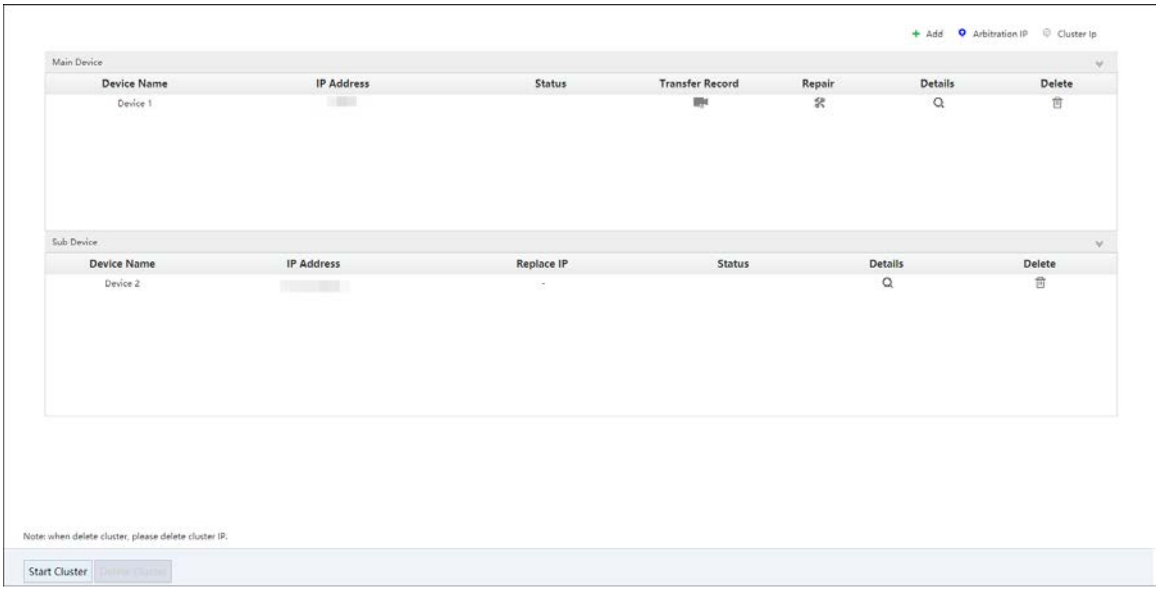
Event Time	Event Name	Event Reason
2018-11-13 16:21:11	Connection Failed	Main connection failed.

3.15.1.3 Restoring Main Device

When the main device breaks down, the backup device replaces it to work. The status of the backup device changes from free to working. After the main device is repaired, you need to restore the main device manually.

Step 1 Select **Cluster > Configuration**.

Figure 3-172 Cluster configuration



Main Device

Device Name	IP Address	Status	Transfer Record	Repair	Details	Delete
Device 1	[redacted]					

Sub Device

Device Name	IP Address	Replace IP	Status	Details	Delete
Device 2	[redacted]	-			

Note: when delete cluster, please delete cluster IP.

Step 2 Click .

Step 3 Enable auto record transfer according to actual needs.

- Click **OK.** The system starts to restore the main device and transfer records automatically.
- Click **Cancel**. The system starts to restore the main 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".

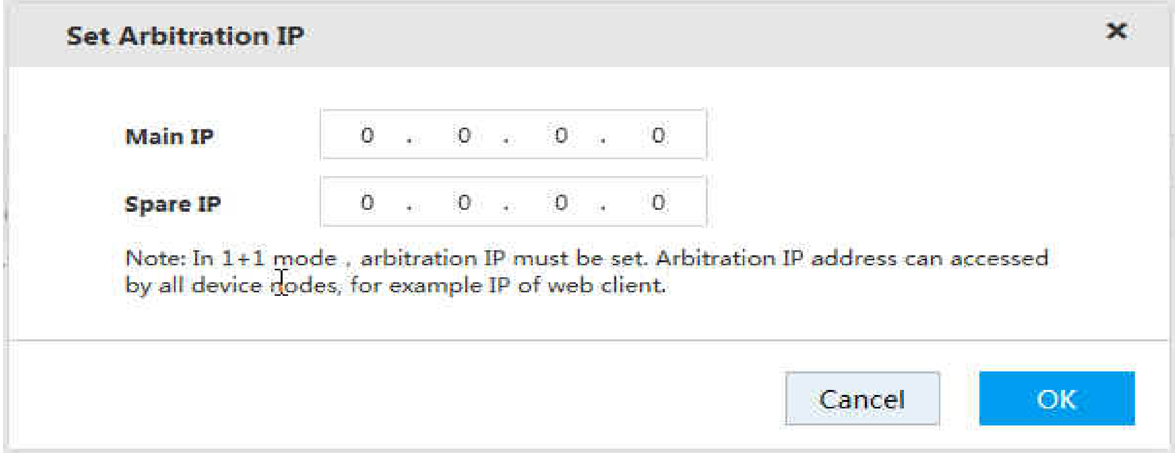
3.15.1.4 Setting Arbitration IP

When there are only two Devices in the cluster, a third-party device is needed to define if the main 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**.

Step 2 Click .

Figure 3-173 Setting arbitration IP



Set Arbitration IP

Main IP 0 . 0 . 0 . 0

Spare IP 0 . 0 . 0 . 0

Note: In 1+1 mode , arbitration IP must be set. Arbitration IP address can accessed by all device nodes, for example IP of web client.

Step 3 Enter the Main IP and Spare IP.

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

3.15.2 Record Transfer

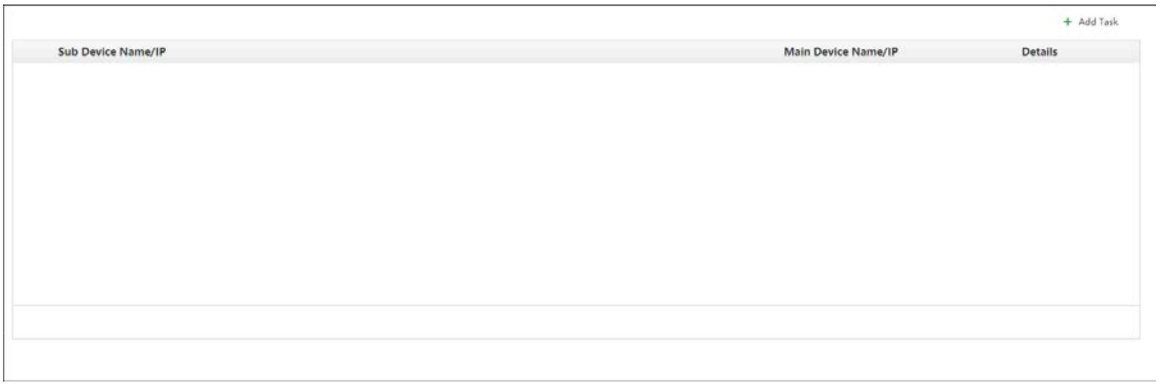
After the main device is repaired, the records on the backup device must be transferred back to the main device.

Preparation

The main device is restored. For details, see "3.15.1.3 Restoring Main Device".

Step 1 Select **Cluster > Record Transfer**.

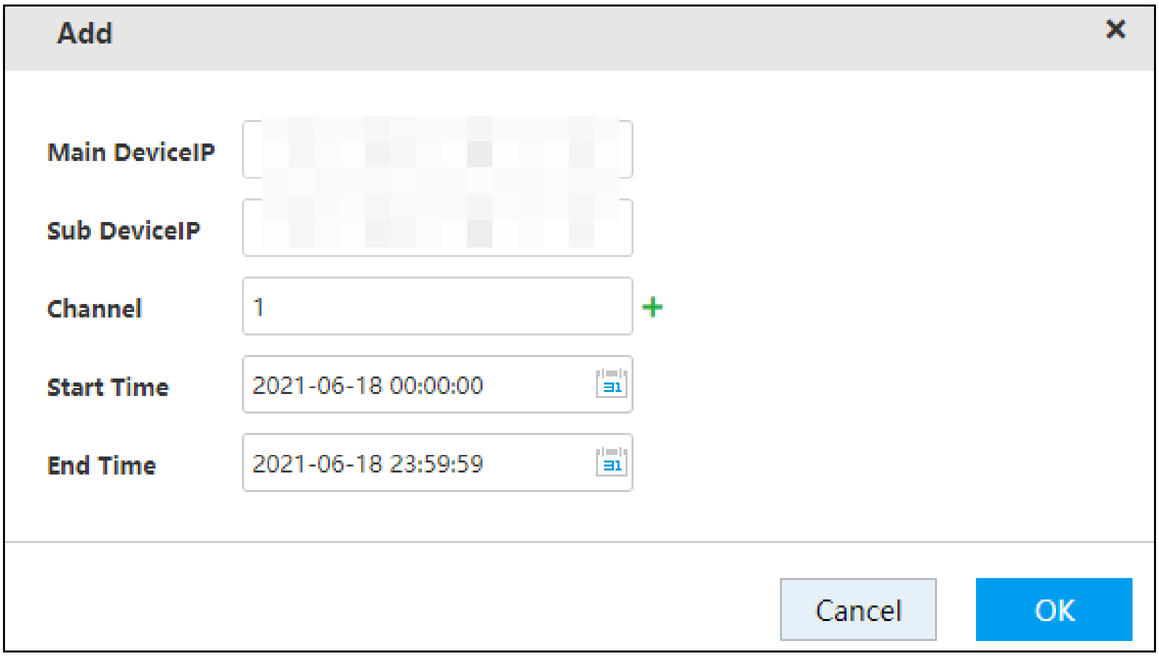
Figure 3-174 Record transfer



Sub Device Name/IP	Main Device Name/IP	Details

Step 2 Click + .

Figure 3-175 Adding record transfer



Main DeviceIP

Sub DeviceIP

Channel: 1 +

Start Time: 2021-06-18 00:00:00

End Time: 2021-06-18 23:59:59

Step 3 Configure the parameters.

Table 3-57 Record transfer parameters

Parameter	Description
Main Device IP	Enter the IP address of main 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.
End Time	

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

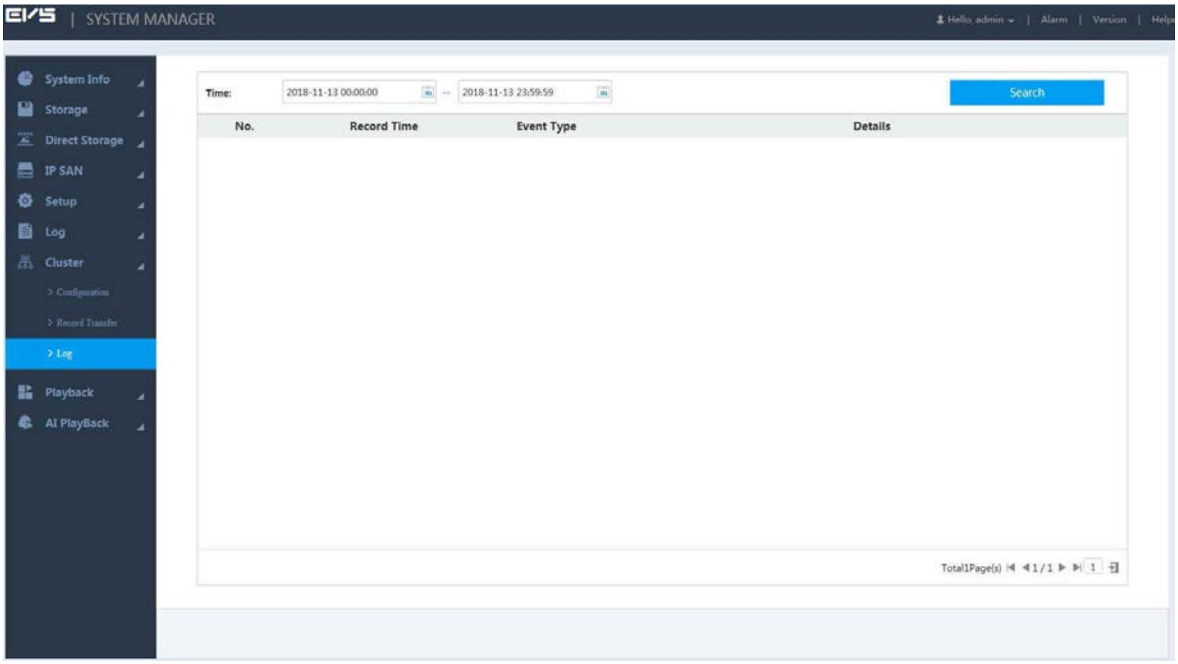
The system returns to the **Record Transfer** page. You can view the detailed information like transfer speed.

3.15.3 Cluster Log

The system supports searching and viewing cluster logs.

Step 1 Select **Cluster > Log**.

Figure 3-176 Cluster log



Time: 2018-11-13 00:00:00 -- 2018-11-13 23:59:59

No.	Record Time	Event Type	Details

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

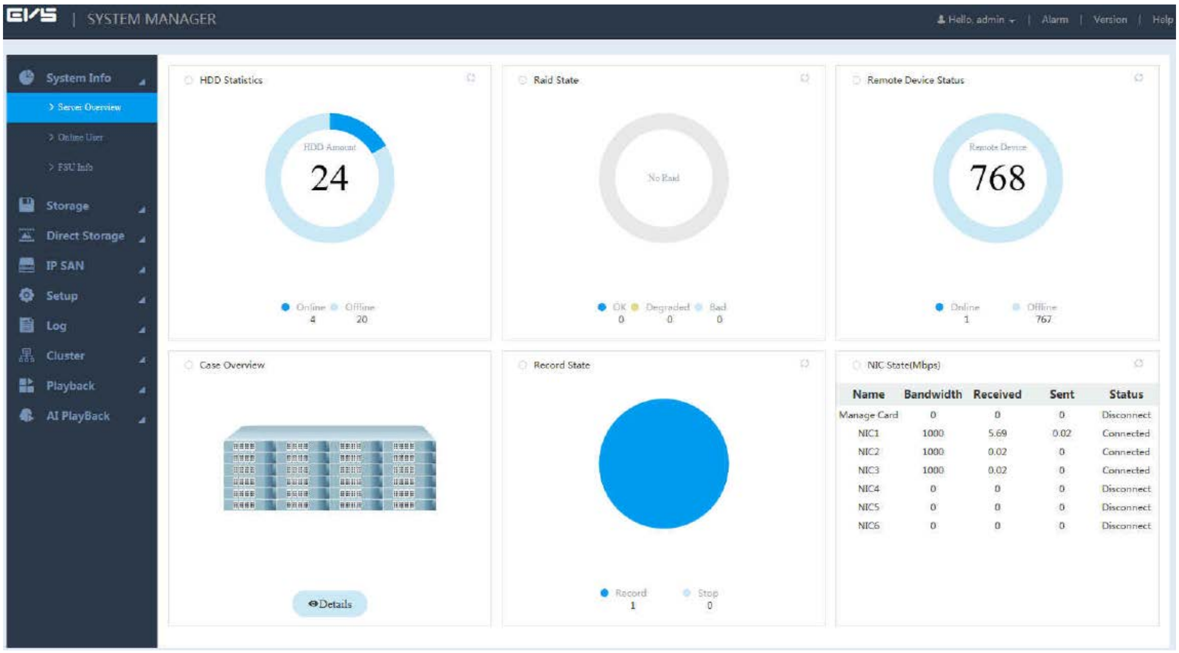
View the HDD statistics, RAID status, device online, case, record status and NIC status.

Select **System Info** > **Server Overview**.

The **Server Overview** page is displayed. See Figure 3-177.

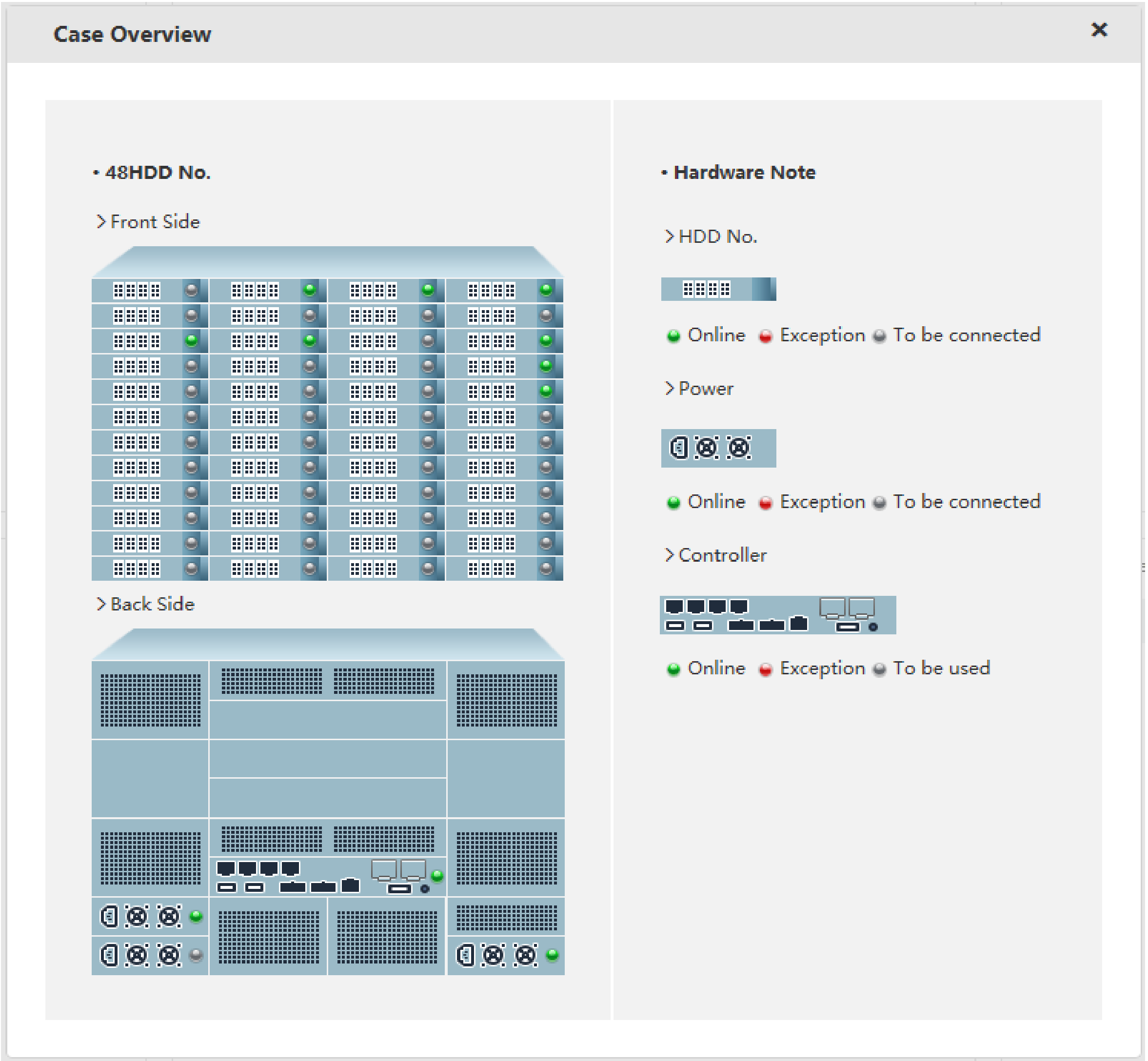
- Click ⟳ to get the latest status or information of the Device.
- Click 👁Details, and the **Case Overview** page is displayed. See Figure 3-178. You can view the information of HDD, power, and port status.

Figure 3-177 Server overview



Name	Bandwidth	Received	Sent	Status
Manage Card	0	0	0	Disconnect
NIC1	1000	5.69	0.02	Connected
NIC2	1000	0.02	0	Connected
NIC3	1000	0.02	0	Connected
NIC4	0	0	0	Disconnect
NIC5	0	0	0	Disconnect
NIC6	0	0	0	Disconnect

Figure 3-178 Case overview


Case Overview
• 48HDD No.
> Front Side
> Back Side
• Hardware Note
> HDD No.
● Online ● Exception ● To be connected
> Power
● Online ● Exception ● To be connected
> Controller
● Online ● Exception ● To be used

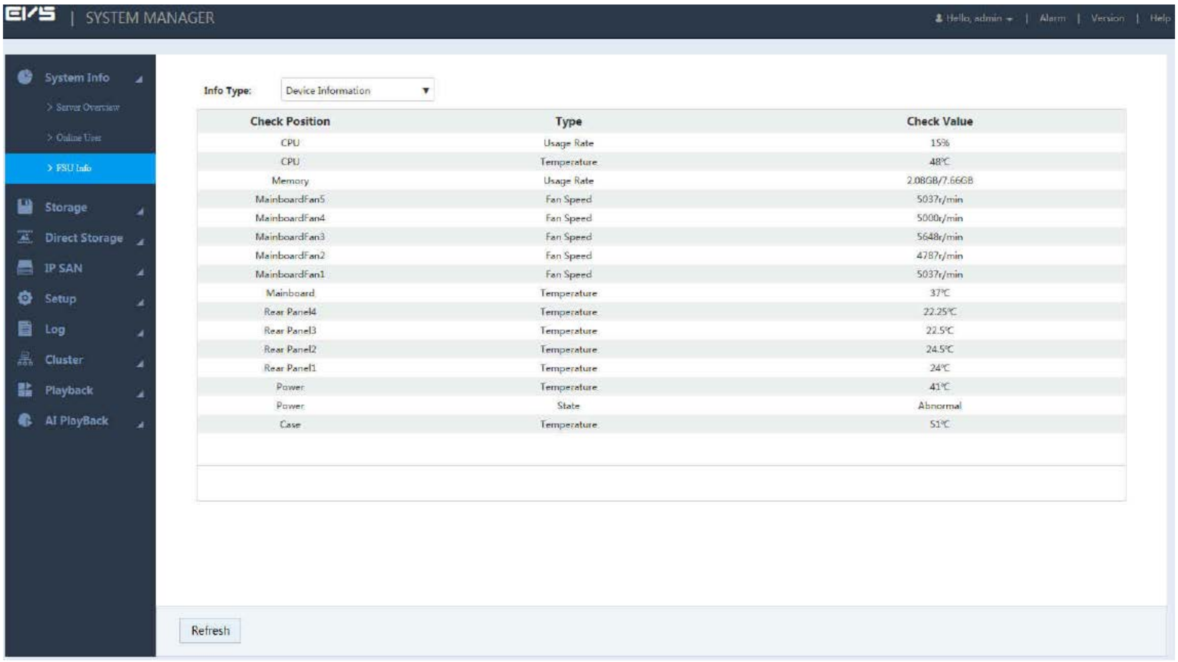
3.16.2 FSU Information

View the field surveillance unit (FSU) information, including information of main and backup devices, and all the expansion drawers.

Select **System** > **FSU Info**. The **FSU Info** page is displayed.

Click **Refresh** to get the latest device information.

Figure 3-179 FSU Information



Info Type: Device Information

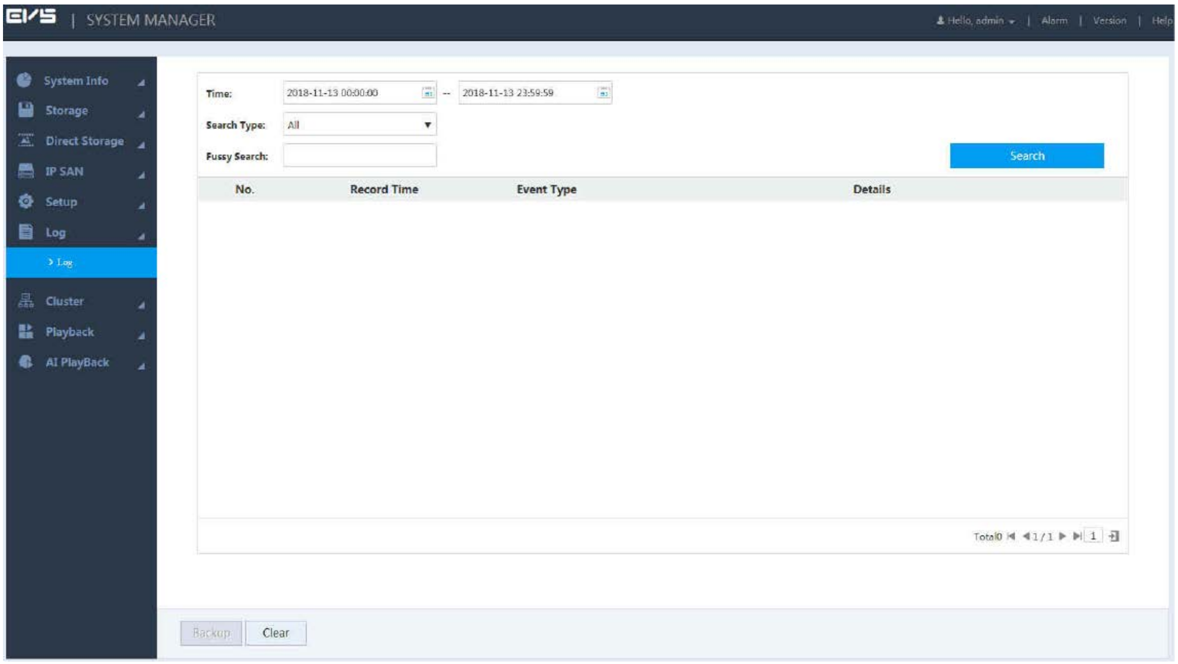
Check Position	Type	Check Value
CPU	Usage Rate	15%
CPU	Temperature	48℃
Memory	Usage Rate	2.08GB/7.66GB
MainboardFan5	Fan Speed	5037r/min
MainboardFan4	Fan Speed	5000r/min
MainboardFan3	Fan Speed	5648r/min
MainboardFan2	Fan Speed	4787r/min
MainboardFan1	Fan Speed	5037r/min
Mainboard	Temperature	37℃
Rear Panel4	Temperature	22.25℃
Rear Panel3	Temperature	22.5℃
Rear Panel2	Temperature	24.5℃
Rear Panel1	Temperature	24℃
Power	Temperature	41℃
Power	State	Abnormal
Case	Temperature	51℃

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**.

Figure 3-180 Log (1)



Time: 2018-11-13 00:00:00 -- 2018-11-13 23:59:59

Search Type: All

Fussy Search:

No.	Record Time	Event Type	Details

Step 2 Configure the parameters.

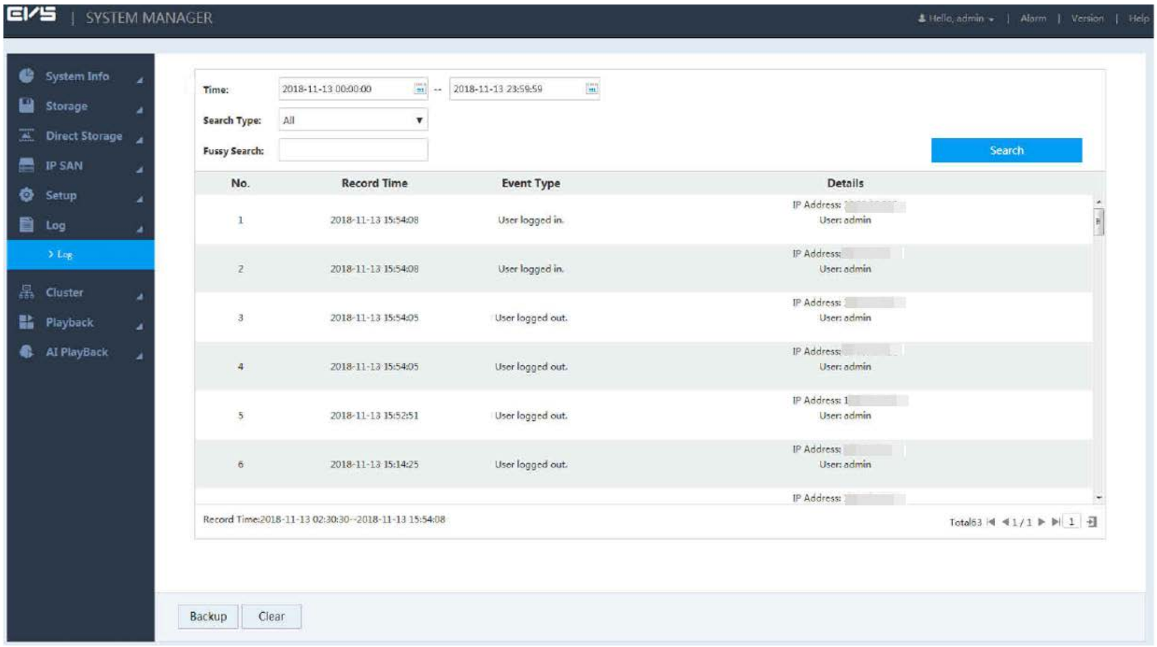
Table 3-58 Log parameters

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**.

⚠

- Click **Clear** and the system deletes all the logs. Operate with care.
- Only admin user has the authority to clear the logs.



Time: 2018-11-13 00:00:00 -- 2018-11-13 23:59:59

Search Type: All

Fussy Search:

No.	Record Time	Event Type	Details
1	2018-11-13 15:54:08	User logged in.	IP Address: [redacted] User: admin
2	2018-11-13 15:54:08	User logged in.	IP Address: [redacted] User: admin
3	2018-11-13 15:54:05	User logged out.	IP Address: [redacted] User: admin
4	2018-11-13 15:54:05	User logged out.	IP Address: [redacted] User: admin
5	2018-11-13 15:52:51	User logged out.	IP Address: [redacted] User: admin
6	2018-11-13 15:14:25	User logged out.	IP Address: [redacted] User: admin
			IP Address: [redacted]

Record Time:2018-11-13 02:30:30--2018-11-13 15:54:08

Total63 1/1 1

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

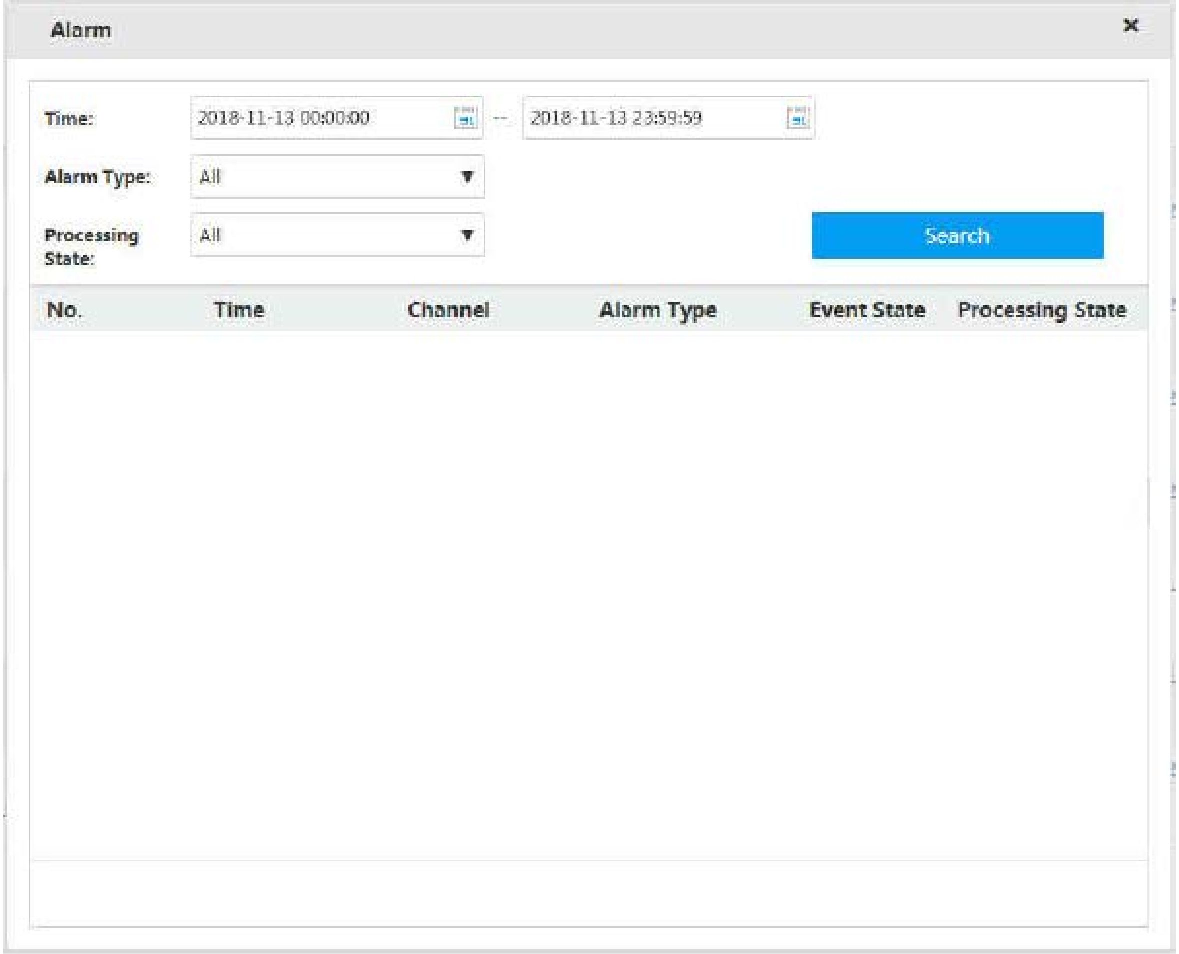
You can view the time of alarm, channel number, alarm type, and processing state.

Step 1 Click **Alarm** at the top right corner of the web.

⚠

- The alarm information on this **Alarm** page 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


Alarm

Time: 2018-11-13 00:00:00 -- 2018-11-13 23:59:59

Alarm Type: All

Processing State: All

Step 2 Configure alarm searching conditions.

Table 3-59 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 page of the Device.
Processing State	Set the processing state of alarm type, including all, pending, fixed, processing, false alarm, and ignored.

Appendix 1 Particulate and Gaseous Contamination Specifications

Appendix 1.1 Particulate Contamination Specifications

The following table defines the limitations of the particulate contamination in the operating environment of the device. If the level of particulate contamination exceeds the specified limitations and result in device damage or failure, you need to rectify the environmental conditions.

Appendix Table 1-1 Particulate contamination specifications

Particulate contamination	Specifications
Air filtration	Class 8 as defined by ISO 14644-1.
Conductive dust	Air must be free of conductive dust, zinc whiskers, or other conductive particles.
Corrosive dust	Air must be free of corrosive dust. Residual dust present in the air must have a deliquescent point less than 60% relative humidity.

Appendix Table 1-2 ISO 14644-1 cleanroom classification

Class	Maximum particles/m³					
-	≥ 0.1 μm	≥ 0.2 μm	≥ 0.3 μm	≥ 0.5 μm	≥ 1 μm	≥ 5 μm
Class 1	10	2	-	-	-	-
Class 2	100	24	10	4	-	-
Class 3	1000	237	102	35	8	-
Class 4	10000	2370	1020	352	83	-
Class 5	100000	23700	10200	3520	832	29
Class 6	1000000	237000	102000	35200	8320	293
Class 7	-	-	-	352000	83200	2930
Class 8	-	-	-	3520000	832000	29300
Class 9	-	-	-	-	8320000	293000

Appendix 1.2 Gaseous Contamination Specifications

Usually indoor and outdoor atmospheric environments contain a small amount of common corrosive gas pollutants. When these mixed or single corrosive gas pollutants react with other environmental factors such as temperature or relative humidity in the long term, the device might suffer from a risk of corrosion and failure. The following table defines the limitations of the gaseous contamination in the operating environment of the device.

Appendix Table 1-3 Gaseous contamination specifications

Gaseous contamination	Specifications
Copper coupon corrosion rate	< 300 Å/month per Class G1 as defined by ANSI/ISA71.04-2013
Silver coupon corrosion rate	< 200Å/month per Class G1 as defined by ANSI/ISA71.04-2013

Appendix Table 1-4 ANSI/ISA-71.04-2013 classification of reactive environments

Class	Copper Reactivity	Silver Reactivity	Description
G1 (mild)	< 300 Å/month	< 200 Å/month	Corrosion is not a factor in determining equipment reliability.
G2 (moderate)	< 1000 Å/month	< 1000 Å/month	Corrosion effects are measurable and corrosion might be a factor.
G3 (harsh)	< 2000 Å/month	< 2000 Å/month	High probability that corrosive attack will occur.
GX (severe)	≥ 2000 Å/month	≥ 2000 Å/month	Only specially designed and packaged devices are expected to survive.

Appendix 2 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)
RAID1	Min (capacityN)
RAID0	Total capacity of the HDDs in the set

Appendix 3 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 operating 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 4 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
   - Do not contain the account name or the account name in reverse order;
   - Do not use continuous characters, such as 123, abc, etc.;
   - Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Time**

   - According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
   - We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. **Physical Protection**

   We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

   We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. **Set and Update Passwords Reset Information Timely**

   The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. **Enable Account Lock**

   The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

   We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

    Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

    Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. **Construct a Safe Network Environment**

    In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.