Embedded Video Storage Server (EVS50, EVS70 Series)

User's Manual

V2.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

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

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

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

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

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

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

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

7. Disable Auto-Login on SmartPSS:

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

8. Use a Different User Name and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different user name and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

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

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.

● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

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

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

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

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Foreword

General

This user's manual (hereinafter referred to be "the Manual") introduces the functions and operations of the EVS series devices (hereinafter referred to be "the Device").

Models

Series	Model
Middle-Class	Middle-Class 16-HDD single-controller, Middle-Class 24-HDD single-controller, Middle-Class 36-HDD single-controller, Middle-Class 48-HDD single-controller
High-End	High-End 24-HDD single-controller, High-End 48-HDD single-controller

Safety Instructions

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

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

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	-
2	V2.0.0	Baseline Switch	October, 2017
3	V2.0.1	Add Privacy Protection Notice	May, 2018

Privacy Protection Notice

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

About the Manual

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

Important Safeguards and Warnings

Electrical safety

- All installation and operation here should conform to your local electrical safety codes.
- The product must be grounded to reduce the risk of electric shock.

We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Transportation security

Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.

Installation

- Keep upwards. Handle with care.
- Do not apply power to the Device before completing installation.
- Do not place objects on the Device.

Qualified engineers needed

All the examination and repair work should be done by the qualified service engineers. We are not liable for any problems caused by unauthorized modifications or attempted repair.

Environment

The Device should be installed in a cool, dry place away from conditions such as direct sunlight, inflammable substances, and explosive substances.

Accessories

- Be sure to use all the accessories recommended by manufacturer.
- Before installation, please open the package and check all the components are included.
- Contact your local retailer ASAP if something is broken in your package.

Lithium battery

- Improper battery use might result in fire, explosion, or personal injury.
- When replacing the battery, please make sure you are using the same type. Risk of explosion if battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.

Table of Contents

1.1 Overview

This product positions in the management, storage and application of high-definition video data. It uses Linux operation system and professional customized hardware platform, owns multiple Hard Disk Drive (HDD) management system, front-end HD device management system, HD video analysis system and large capacity video storage system.

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

This product provides standard network file sharing service and realizes the integrated solution for IPSAN/NAS. It provides centralized storage solution 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

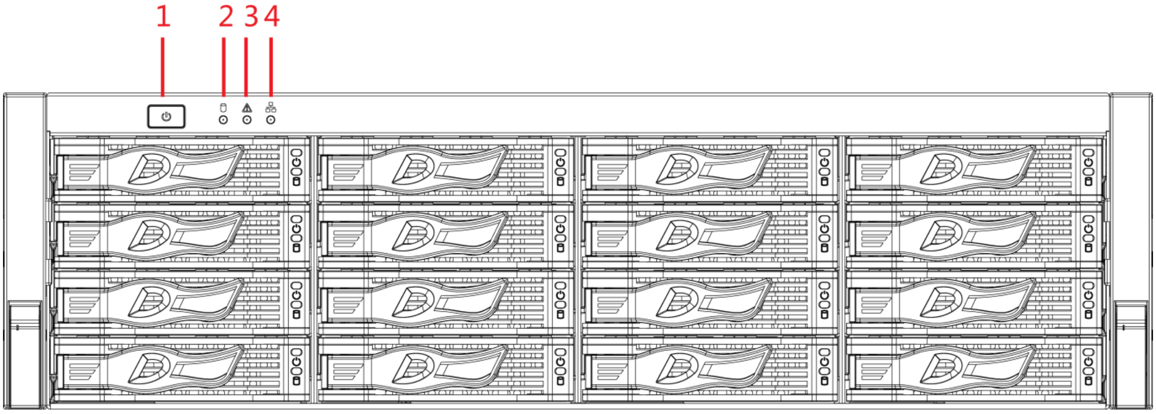


Table 1-1 Description of interfaces on front panel

No.	Indicator Light/Button	Description
1	Power button	Press the power button to execute operations of device start-up and shutdown. This button keeps blue light on when the device is power on. NOTE Hold down this button for 5 seconds to force a device shutdown.

No.	Indicator Light/Button	Description
2	HDD light	HDD status light. ● 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 light	Alarm status light. ● 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 redundant power error.
4	Network light	The blue light keeps on if there is a 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

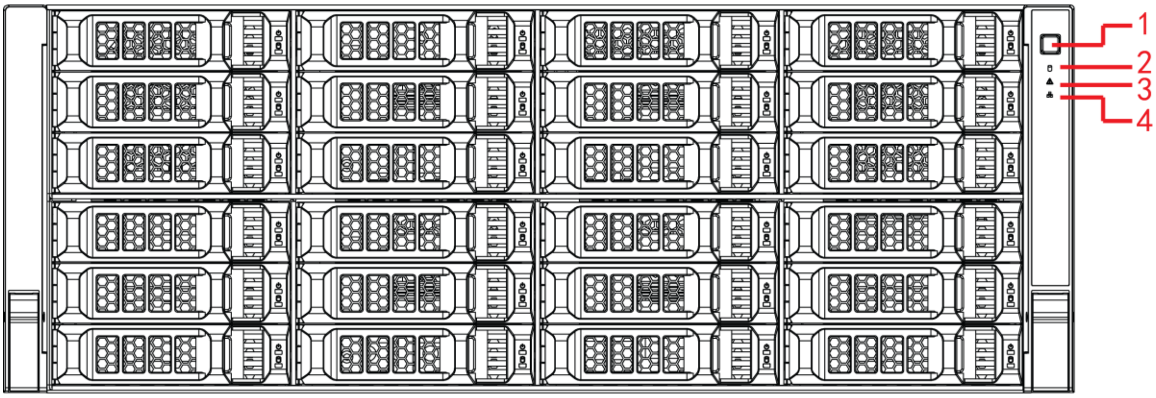


Table 1-2 Description of interfaces on front panel

No.	Indicator Light/Button	Description
1	Power button	Press the power button to execute operations of device start-up and shutdown. NOTE Hold down this button for 5 seconds to force a device shutdown.
2	HDD light	HDD status light. ● 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 light	Alarm status light. ● 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 light	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

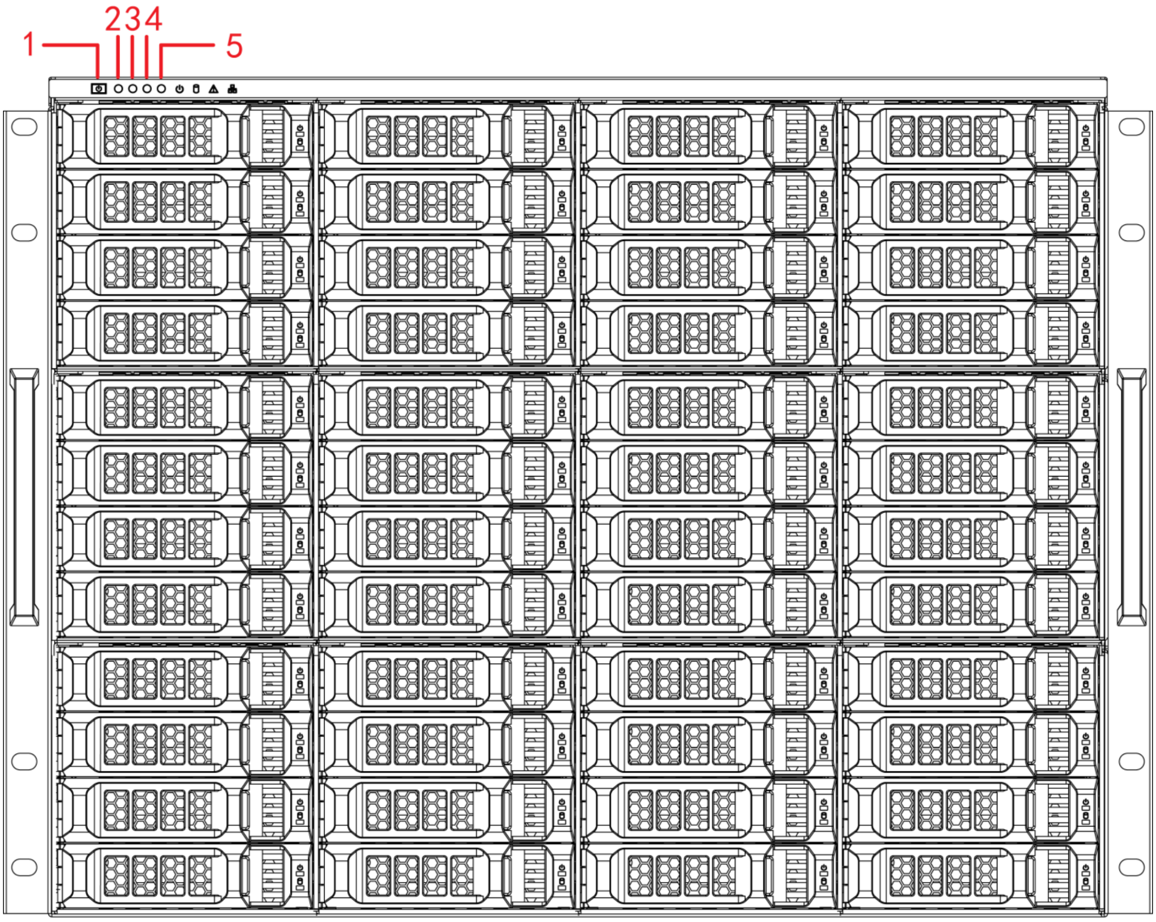


Table 1-3 Description of interfaces on front panel

No.	Indicator Light/Button	Description
1	Power button	Press the power button to execute operations of device start-up and shutdown. NOTE Hold down this button for 5 seconds to force a device shutdown.
2	Power light	Blue light keeps on when the power supply is normal.
3	HDD light	HDD status light. ● 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.
4	Alarm light	Alarm status light. ● 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.
5	Network light	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

1.2.4 Middle-Class 48-HDD Single-Controller

Figure 1-4 Front panel

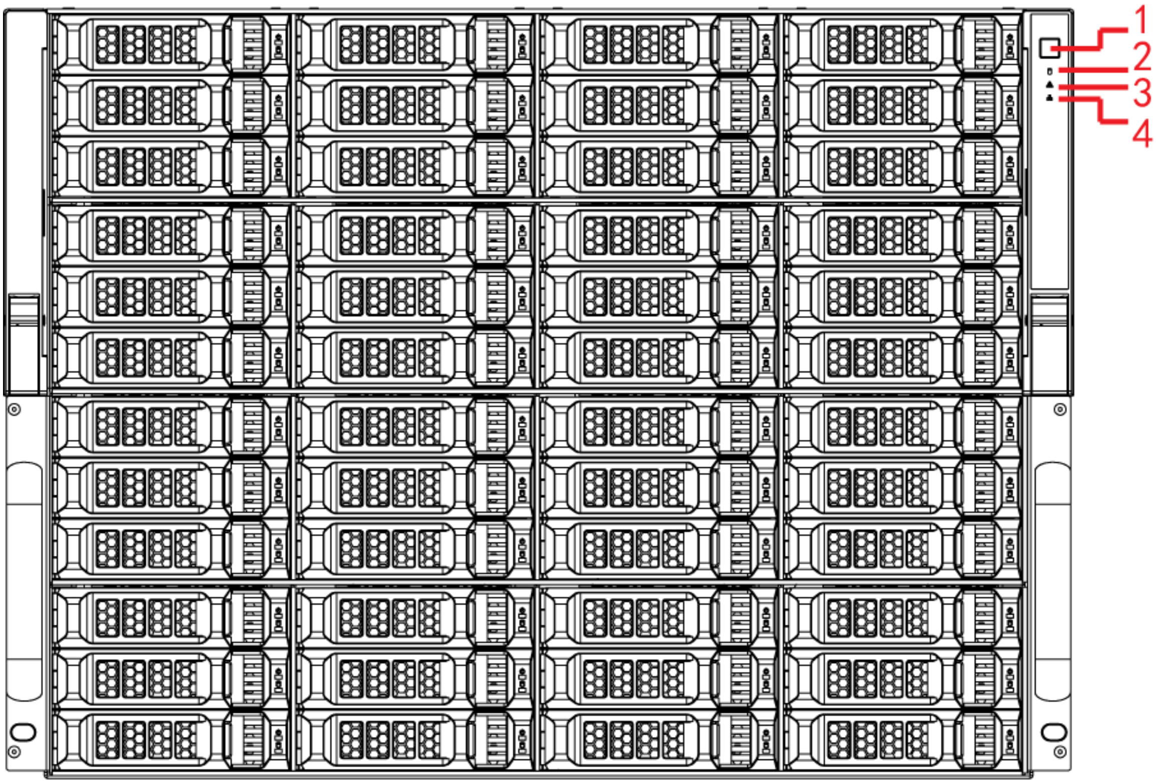


Table 1-4 Description of interfaces on front panel

No.	Indicator Light/Button	Description
1	Power button	Press the power button to execute operations of device start-up and shutdown. This button keeps blue light on when the device is power on. NOTE Hold down this button for 5 seconds to force a device shutdown.
2	HDD light	HDD status light. ● 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 light	Alarm status light. ● 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 light	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

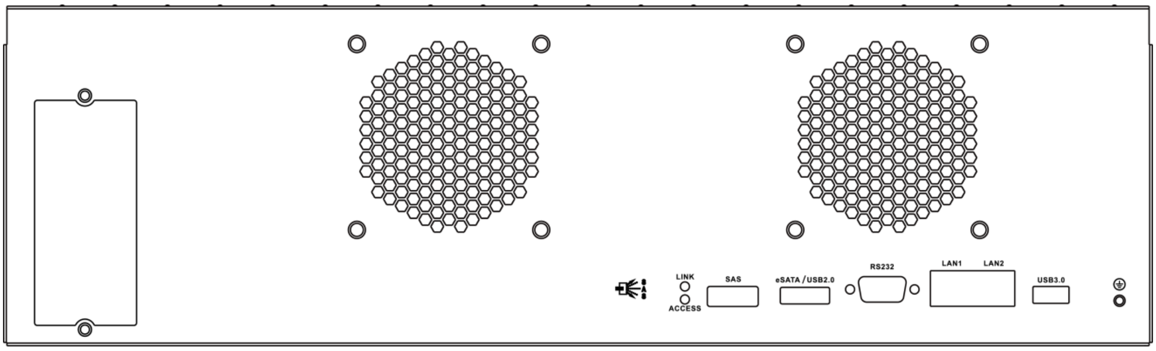


Figure 1-6 Middle-Class 16-HDD Single-Controller with redundant power

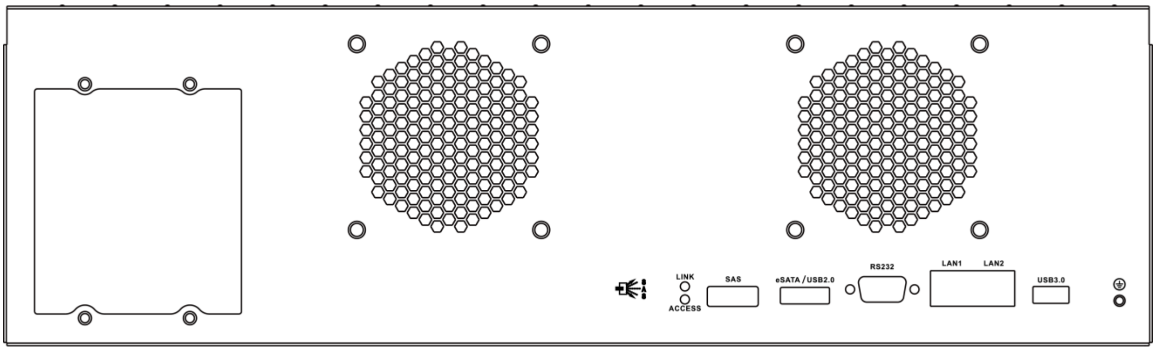


Table 1-5 Description of interfaces on rear panel

Interface	Description
USB3.0	Connect the mouse and USB storage devices.
LAN1, LAN2	Gigabit data port. Used for data transmission.
RS232	RS232 interface.
eSATA, USB2.0	Multiplex interface for eSATA and USB2.0.
SAS	Connect the IN port of the expansion cabinet.
Link/ACCESS	Status light for SAS interface.
Power interface	Connect AC power. NOTE Middle-Class 16-HDD Single-Controller includes devices with single power and devices with dual power.
Power switch	Open or close the device.

1.3.2 Middle-Class 24-HDD Single-Controller

Figure 1-7 Rear panel (5 Ethernet ports)

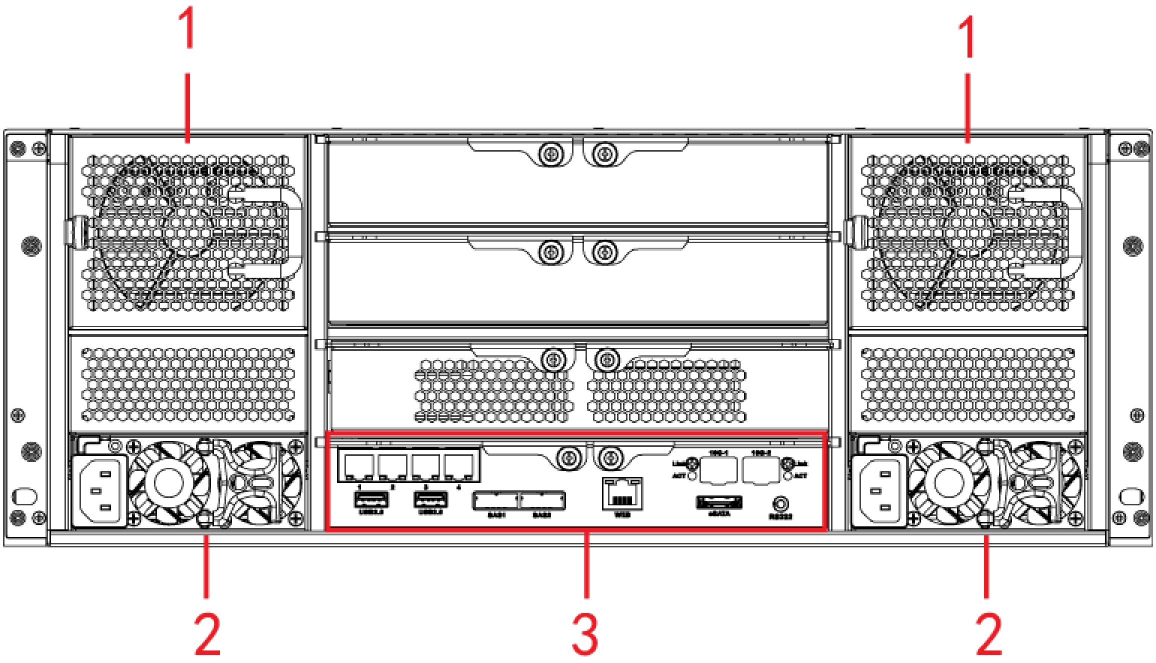


Figure 1-8 Rear panel (7 Ethernet ports)

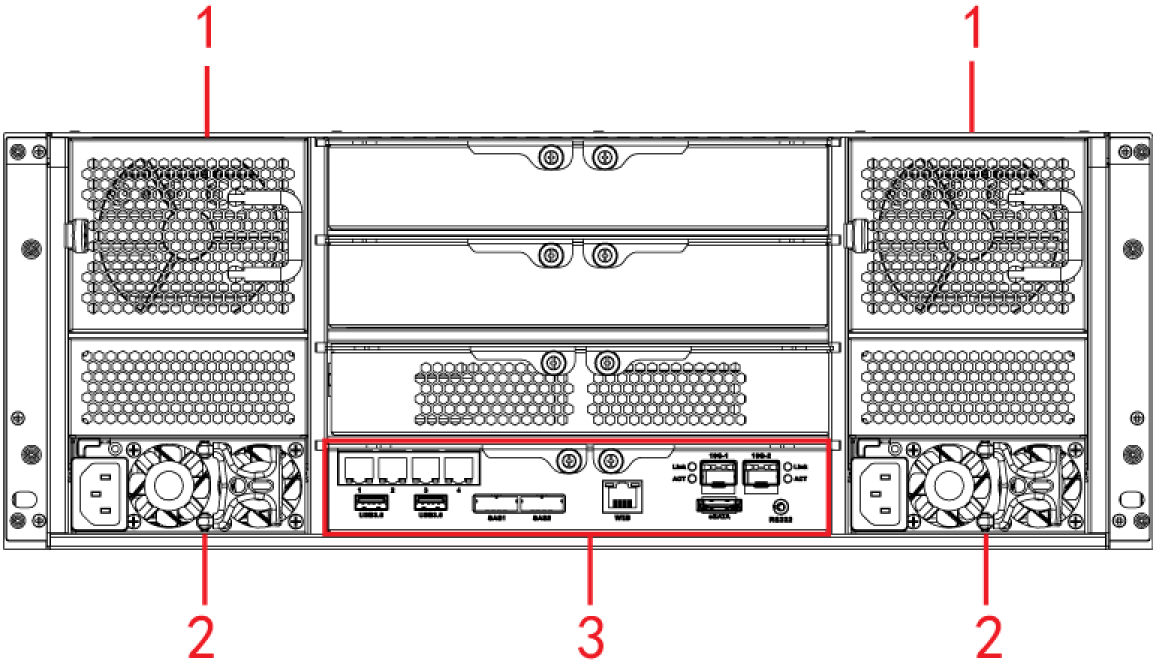


Figure 1-9 Rear panel (9 Ethernet ports)

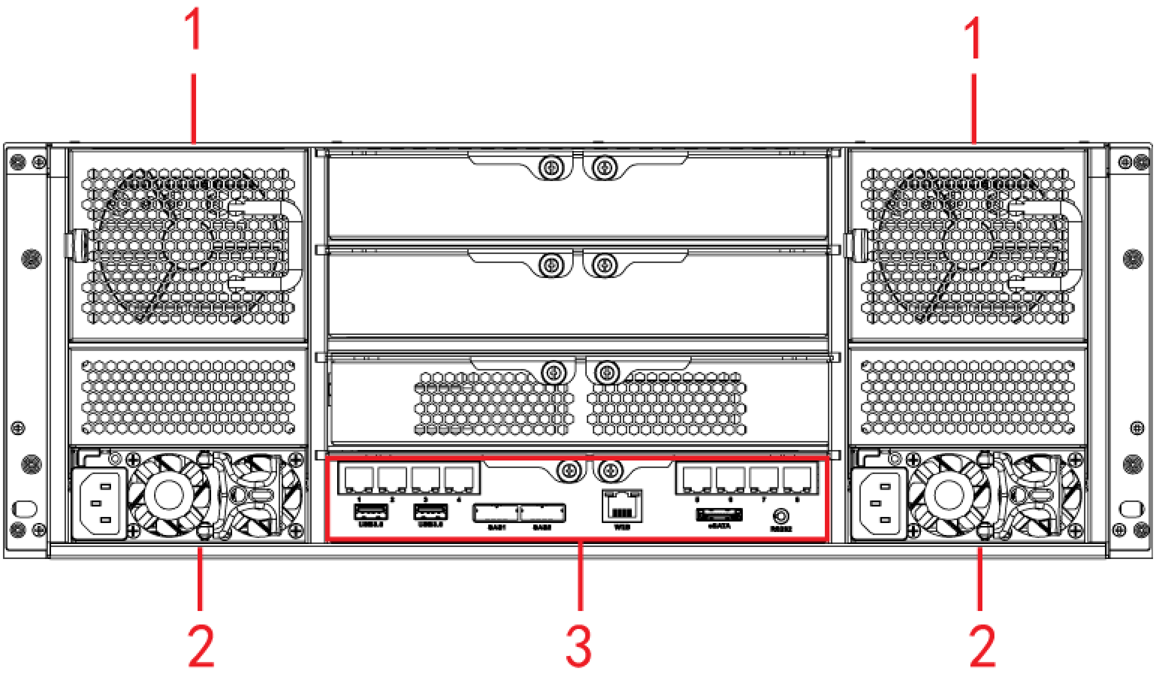


Table 1-6 Description of interfaces on rear panel

No.	Interface	Description
1	Fan	Used for case cooling.
2	Power interface	Connect AC power.
3	Master control module	For description of the interfaces and indicator lights, see Table 1-7.

Table 1-7 Description of interfaces on the master control module

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

1.3.3 Middle-Class 36-HDD Single-Controller

Figure 1-10 Rear panel (5 Ethernet ports)

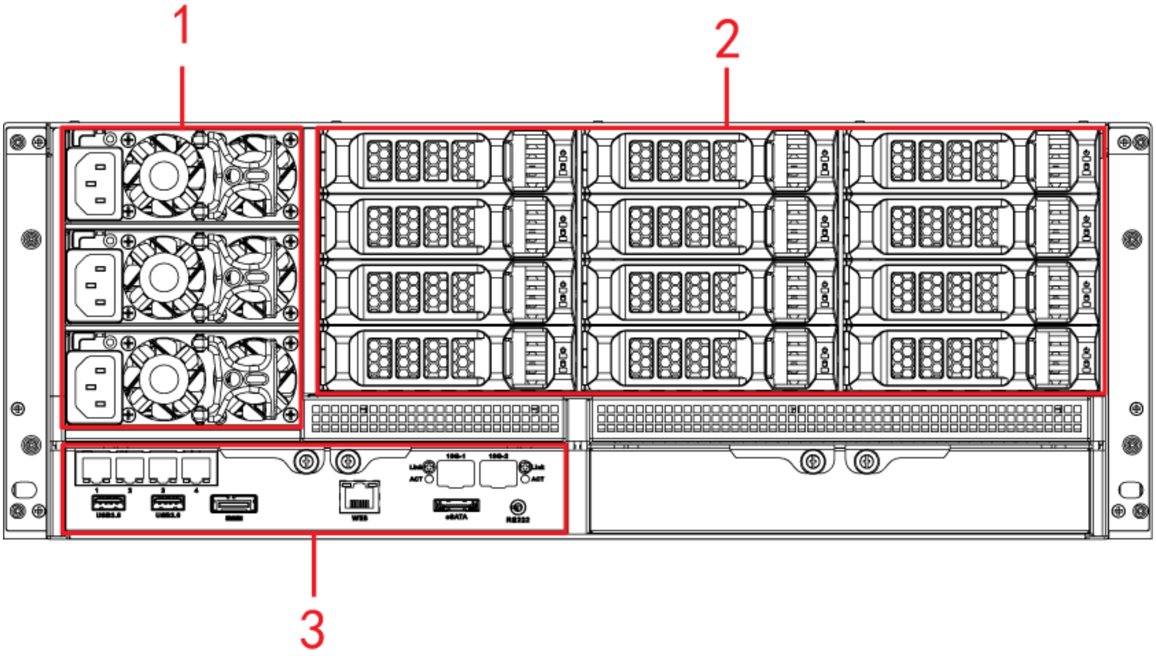


Figure 1-11 Rear panel (7 Ethernet ports)

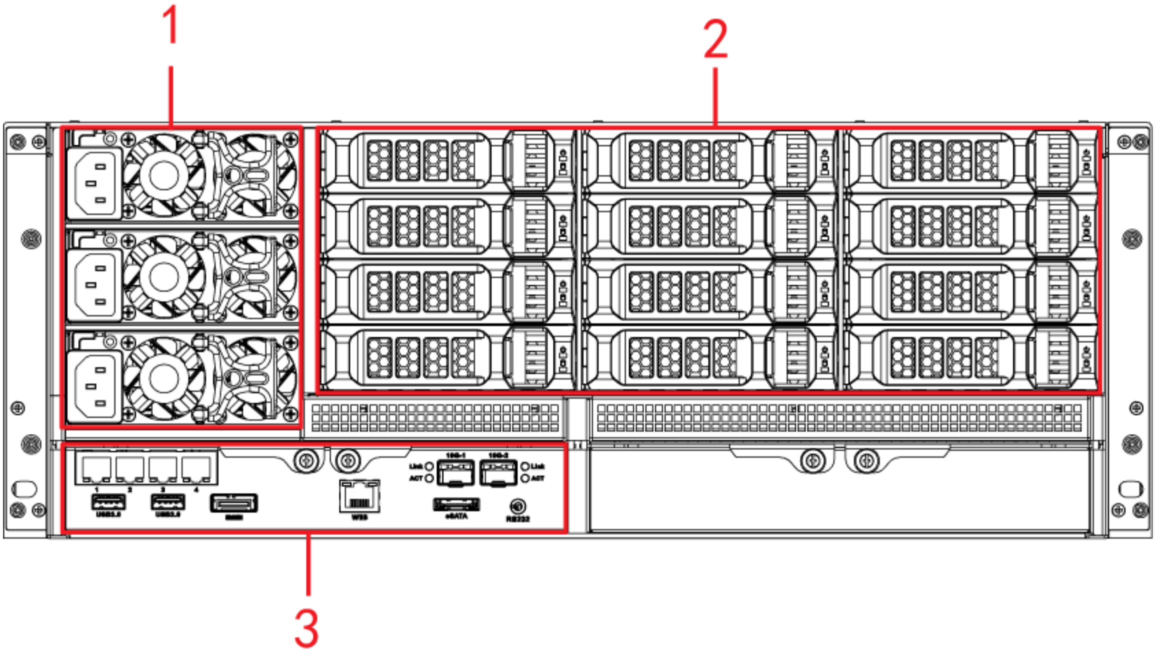


Figure 1-12 Rear panel (9 Ethernet ports)

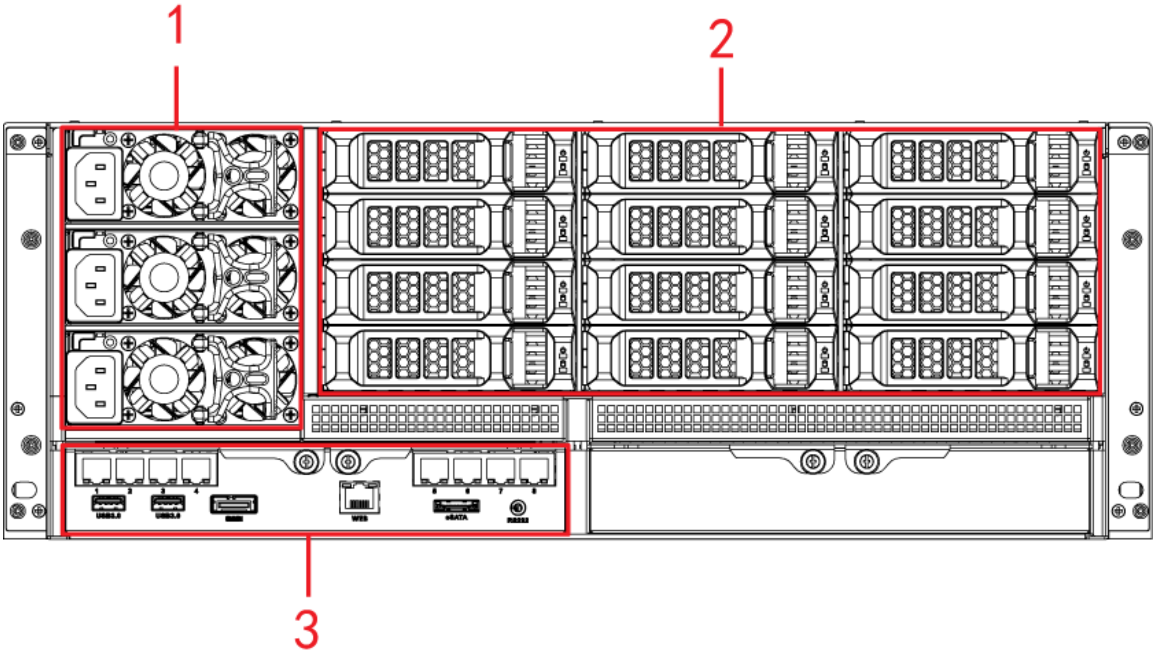


Table 1-8 Description of interfaces on rear panel

No.	Interface	Description
1	Power interface & fan	Connect AC power and cool the case.
2	HDD slot	Install HDD from NO. 25 to No. 36.
3	Master control module	For detailed description of the interfaces and indicator lights, see Table 1-9.

Table 1-9 Description of interfaces on the master control module

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

1.3.4 Middle-Class 48-HDD Single-Controller

Figure 1-13 Rear panel

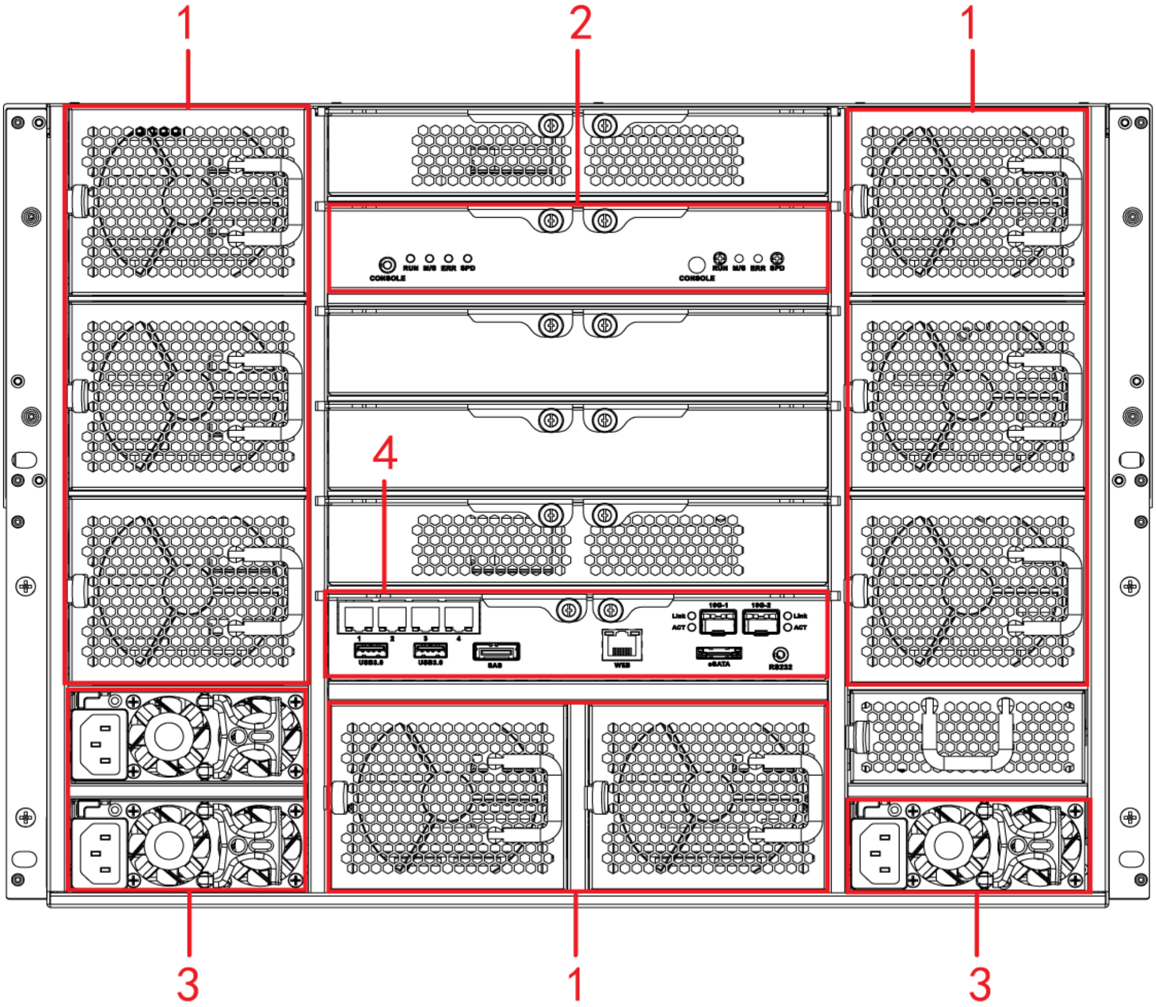


Table 1-10 Description of interfaces on rear panel

No.	Interface	Description
1	Fan	Used for case cooling.
2	SAS expansion controller	For detailed description of the interfaces and indicator lights, see Table 1-12.
3	Power interface	Connect AC power.
4	Master control module	For detailed description of the interfaces and indicator lights, see Table 1-11.

Table 1-11 Description of interfaces on the master control module

Interface	Description
EX-1-EX-4/1-4	Gigabit data port. Used for data transmission.
USB3.0	Connect the mouse and USB storage devices.
eSATA	eSATA interface.
SAS	Connect the IN port of the expansion cabinet.
Web	Gigabit management port. Can be used as data port.
ERR	ERR is on when the system is abnormal. ERR is out when the system is in normal operation.
RUN	RUN light flickers when the device is power on and running.

Interface	Description
RS232	RS232 interface.
10G-1, 10G-2	10 gigabit port. NOTE Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device situation.
Link/ACT	Status light of the 10 gigabit port.

Table 1-12 Description of interfaces on SAS expansion controller

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

1.3.5 High-End 24-HDD Single-Controller

Figure 1-14 Rear panel (5 Ethernet ports)

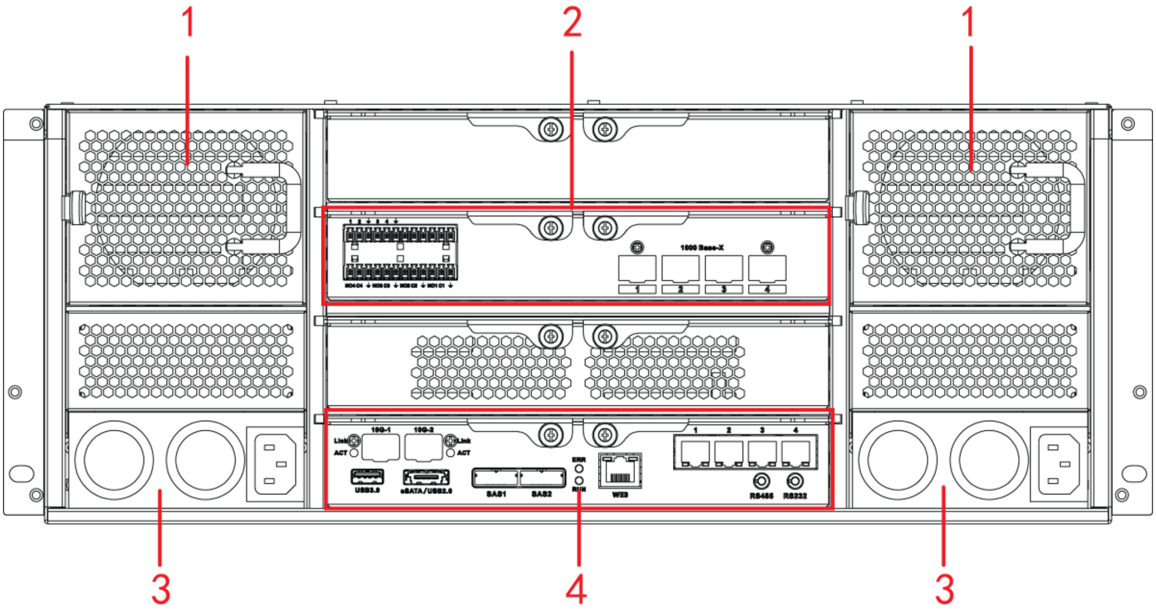


Figure 1-15 Rear panel (7 Ethernet ports)

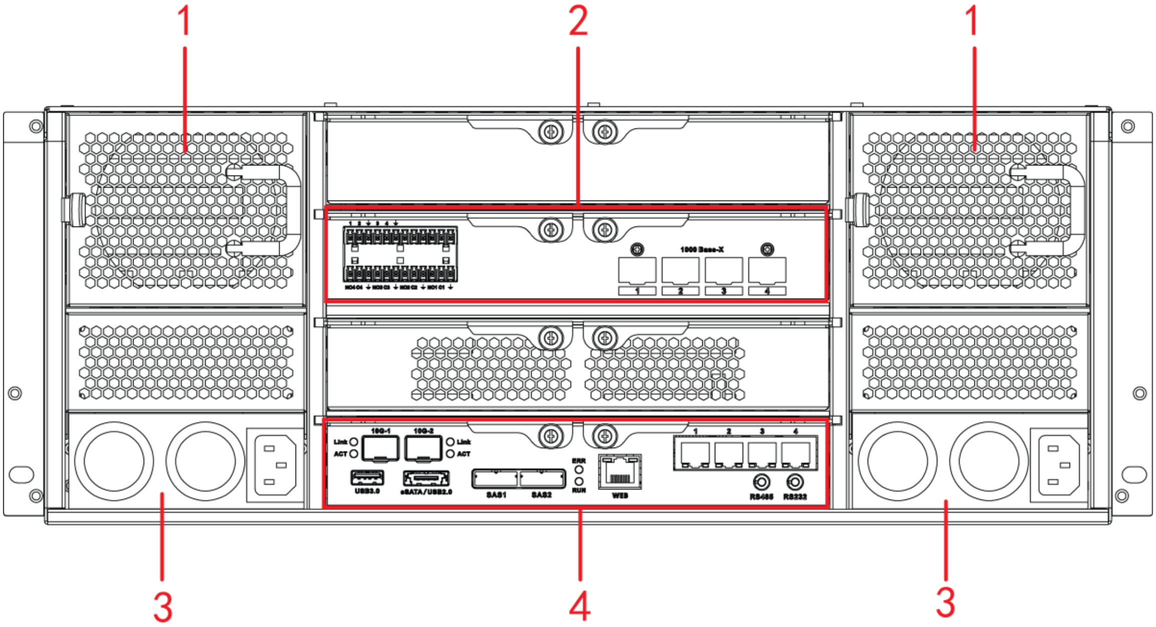


Figure 1-16 Rear panel (9 Ethernet ports)

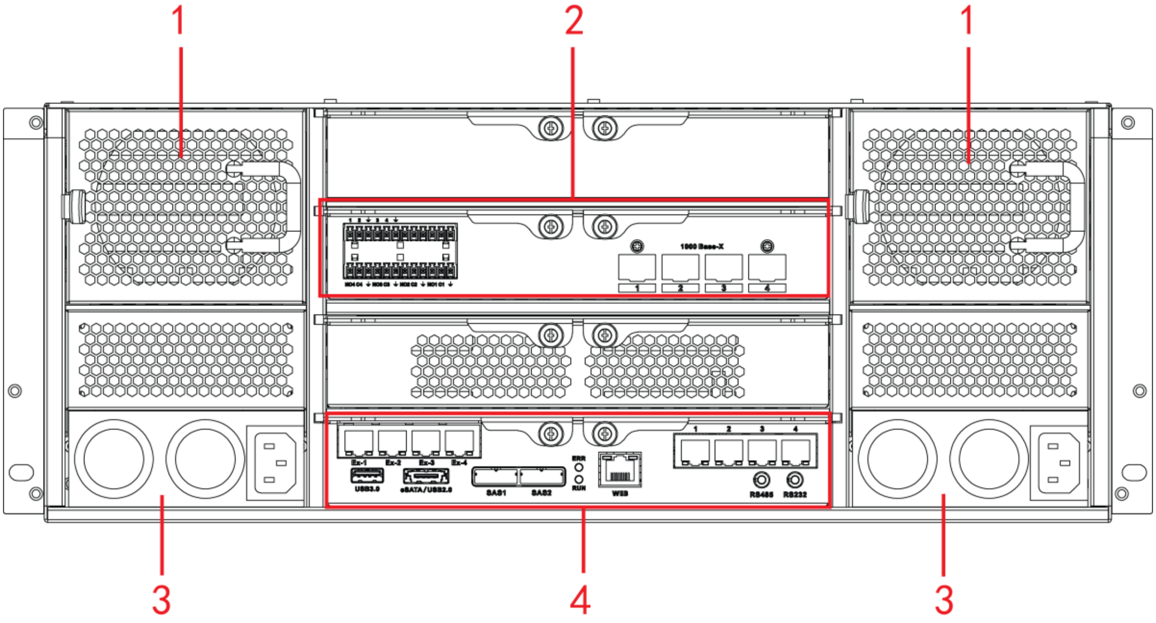


Table 1-13 Description of interfaces on rear panel

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

No.	Interface	Description
4	Master control module	For detailed description of the interfaces and indicator lights, see Table 1-14.

Table 1-14 Description of interfaces on the master control module

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

1.3.6 High-End 48-HDD Single-Controller

Figure 1-17 Rear panel (5 Ethernet ports)

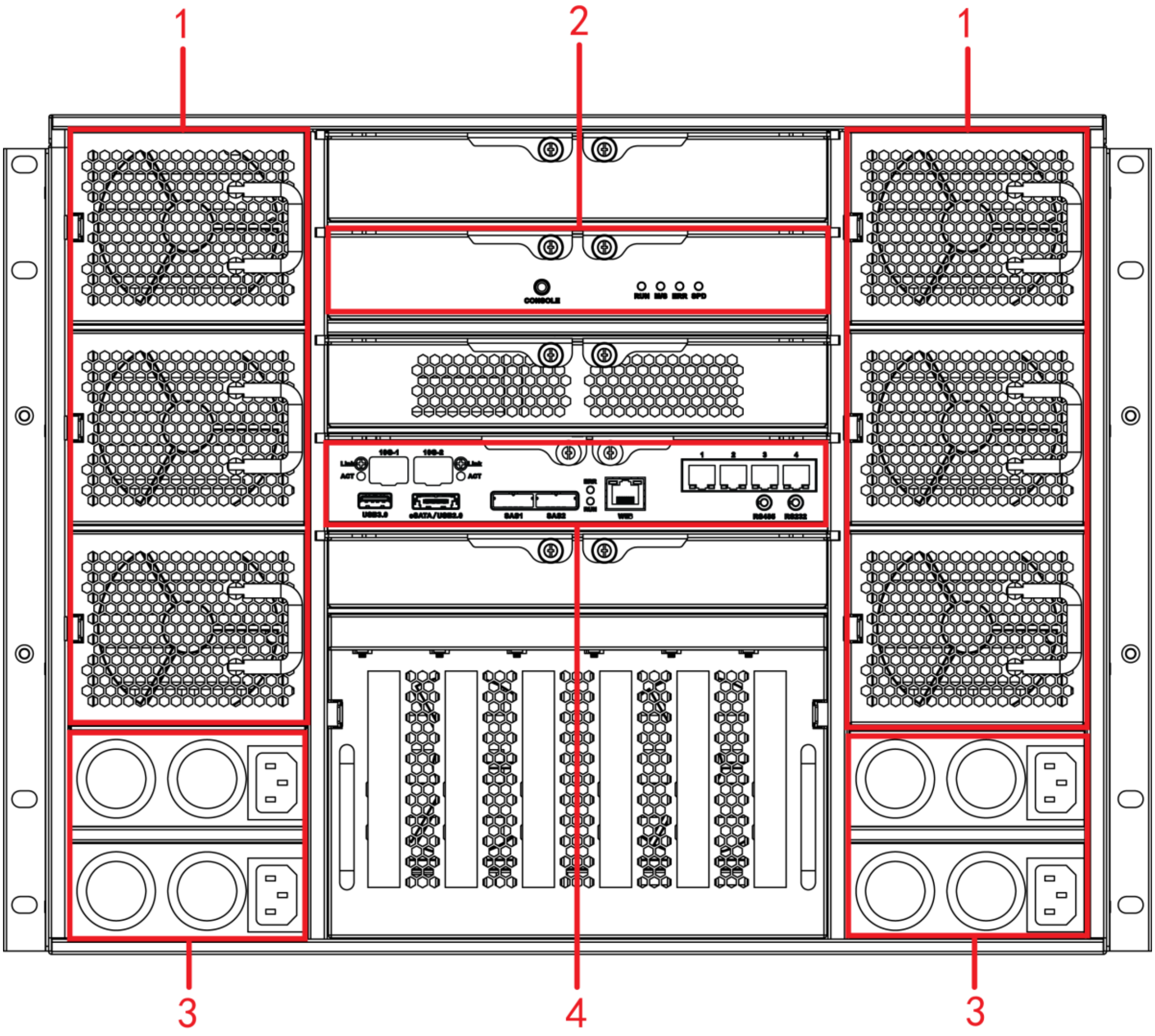


Figure 1-18 Rear panel (7 Ethernet ports)

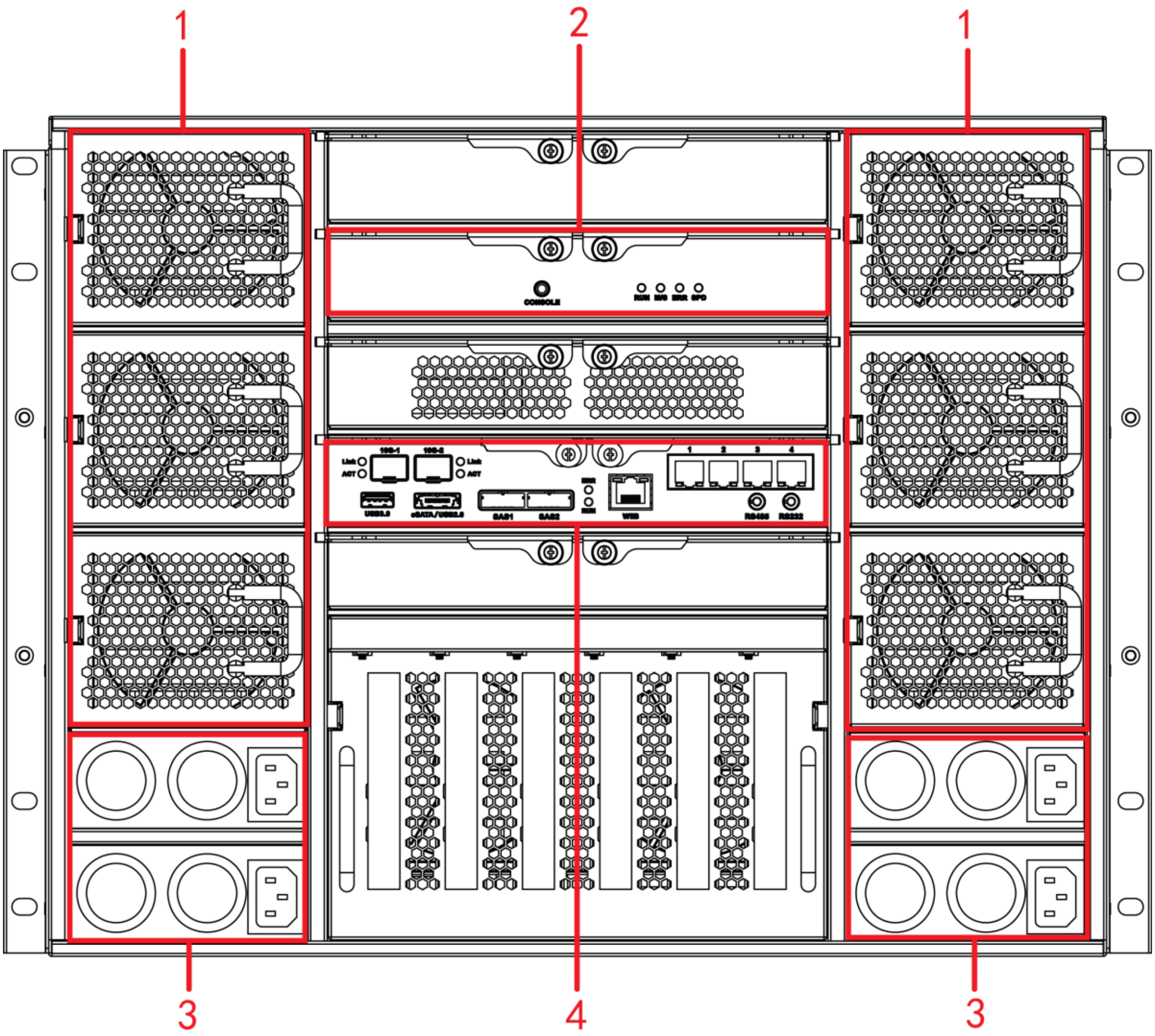


Figure 1-19 Rear panel (9 Ethernet ports)

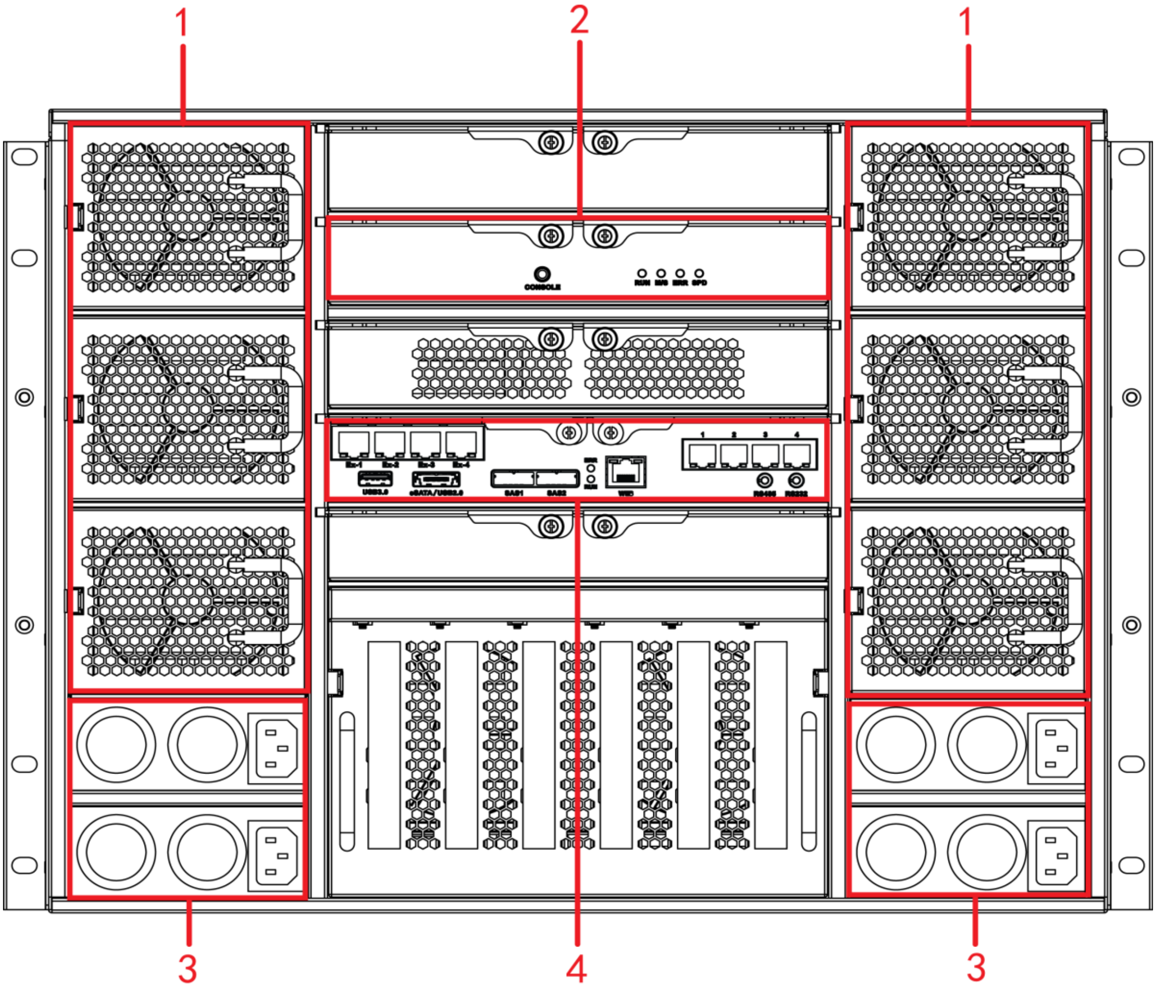


Table 1-15 Description of interfaces on rear panel

No.	Interface	Description
1	Fan	Used for case cooling.
2	SAS expansion controller	For detailed description of the interfaces and indicator lights, see Table 1-17.
3	Power interface	Connect AC power.
4	Master control module	For detailed description of the interfaces and indicator lights, see Table 1-16.

Table 1-16 Description of interfaces on the master control module

Interface	Description
EX-1-EX-4/1-4	Gigabit data port. Used for data transmission.
USB3.0	Connect the mouse and USB storage devices.
eSATA/USB2.0	Multiplex interface for eSATA and USB2.0.
SAS1, SAS2	Connect the IN interface of the expansion cabinet.
Web	Gigabit management port. Can be used as data port.
ERR	ERR is on when the system is abnormal. ERR is out when the system is in normal operation.
RUN	RUN light flickers when the device is power on and running.
RS485	RS485 interface.
RS232	RS232 interface.

Interface	Description
10G-1, 10G-2	10 gigabit port. NOTE Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device situation.
Link/ACT	Status light of the 10 gigabit port.

Table 1-17 Description of interfaces on SAS expansion controller

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

1.4 Description of Menu Items

This section introduces the ions and buttons you will frequently meet when using EVS devices.

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

2 Installing and Powering the Device

2.1 Installing Hard Disk Drive (HDD)

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

⚠ WARNING

Some devices are heavy. Carry them with others to avoid any personnel injury.

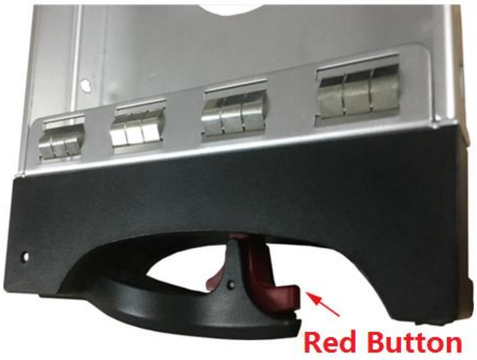
2.1.1 Middle-Class 16-HDD Single-Controller Series

NOTE

The below contents only apply to Middle-Class 16-HDD Single-Controller devices.

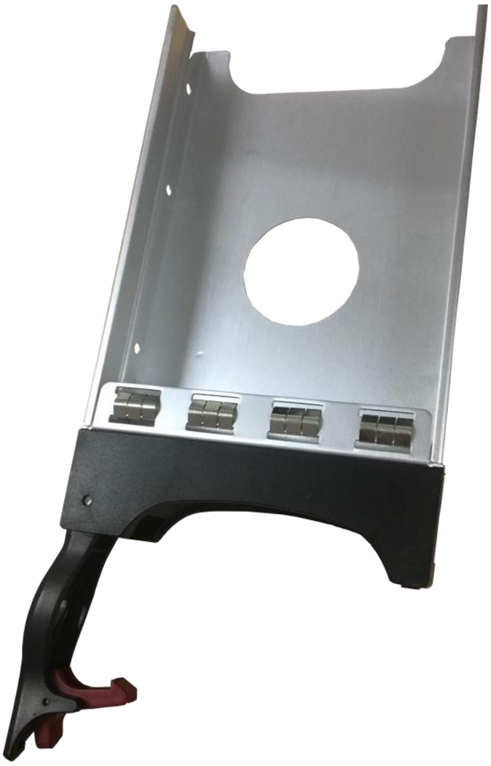
Step 1 Press the red button on the hard disk box in the front panel and open the handle. See Figure 2-1.

Figure 2-1 Opening the handle



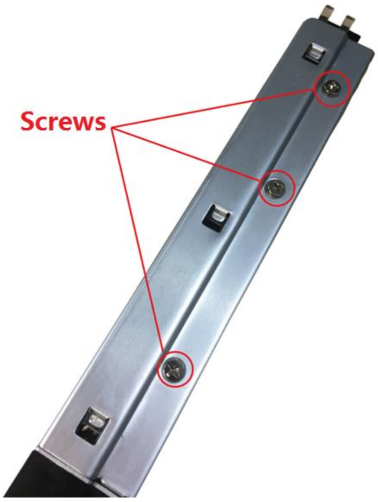
Step 2 Pull out to take the empty hard disk box. See Figure 2-2.

Figure 2-2 Hard disk box



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

Figure 2-3 Locking the screws



Step 4 Insert the hard disk box into the hard disk slot, push it to the bottom, and then close the handle.

⚠ CAUTION

Do not close the handle if the hard disk box has not been pushed to the bottom to avoid any damage to the slot.

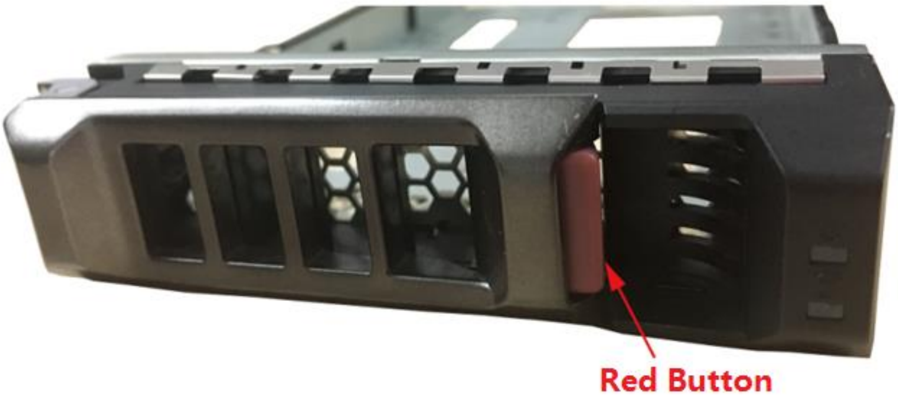
2.1.2 Other Series

NOTE

The below contents apply to devices other than the Middle-Class 16-HDD Single-Controller series.

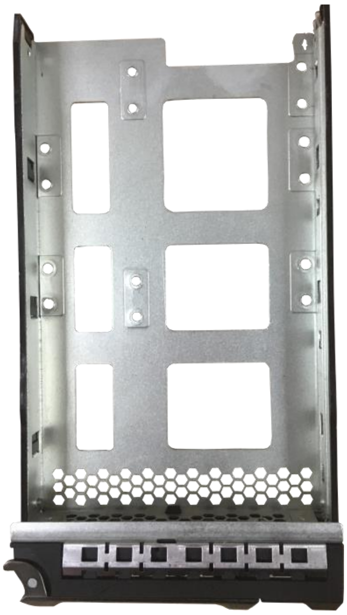
Step 1 Press the red button on the hard disk box in the front panel and open the handle. See Figure 2-4.

Figure 2-4 Opening the handle



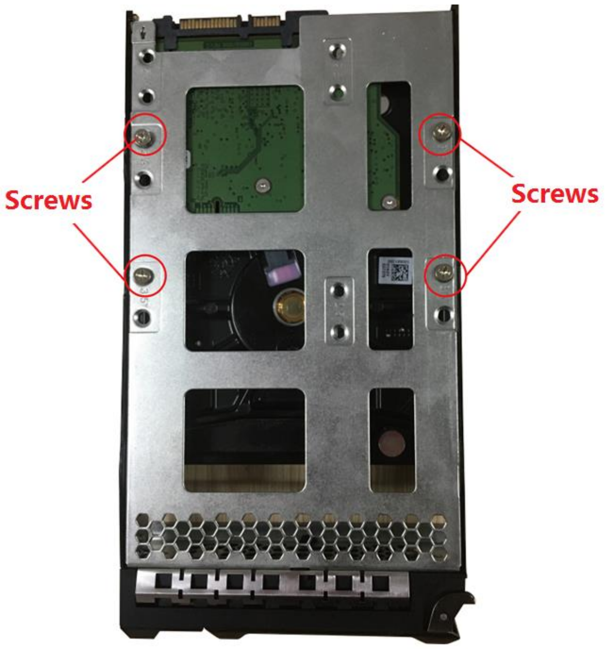
Step 2 Pull out to take the empty hard disk box. See Figure 2-5.

Figure 2-5 Hard disk box



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

Figure 2-6 Locking the screws



Step 4 Insert the hard disk box into the hard disk slot, push it to the bottom and close the handle.

CAUTION

Do not close the handle if the hard disk box has not been pushed to the bottom to avoid any damage to the slot.

2.2 Powering the Device

2.2.1 Preparation

Connect the cables and ensure no error before powering the device. See below for detailed checking items.

- Check that GND is connected correctly.
- Different types of devices need different numbers of power supplies. Check that all power lines are connected correctly.
- Check if the supplied power voltage is consistent with the device requirement.
- Check if the network cables and SAS cables are connected correctly.

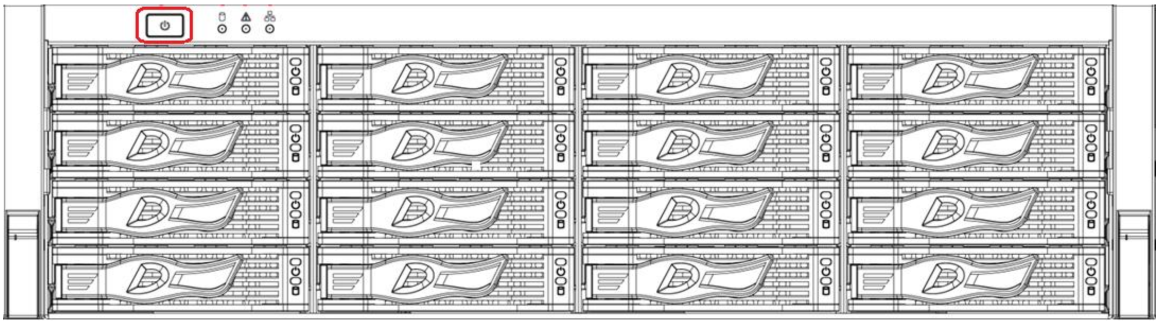
2.2.2 Power on

NOTE

The following contents are introduced in the example of Middle-Class 16-HDD Single-Controller series. You need to see the actual conditions.

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

Figure 2-7 Front panel



See "1.2.1 Middle-Class 16-HDD Single-Controller" for the corresponding description table of the front panel and check if the indicator lights are normally displayed.

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

3 Web Basic Operations

The system supports device access and management through Web at PC (Personal Computer).

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

NOTE

The following contents are only for your reference. Different models have different functions. You need to refer to that displayed actually.

3.1 Connecting the Network

Before logging in Web, check if the network connection between PC and the device 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 routing device in the network, assign IP address of the same network segment for PC and EVS devices.
- If there is routing device in the network, set the corresponding gateway IP and subnet mask for PC and EVS devices respectively.

NOTE

The Ethernet ports of EVS device have different factory default IP.

- Single control device: Network card 1 to network card n corresponds to default IP 192.168.1.108 to 192.168.n.108.
- Double control device: Different slots have different default IP.
  - ◇ Slot 1: Network card 1 to network card n corresponds to default IP 192.168.1.108 to 192.168.n.108.
  - ◇ Slot 2: Network card 1 to network card n corresponds to default IP 192.168.1.109 to 192.168.n.109.
- The port order is standard card, expansion card 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 if 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.

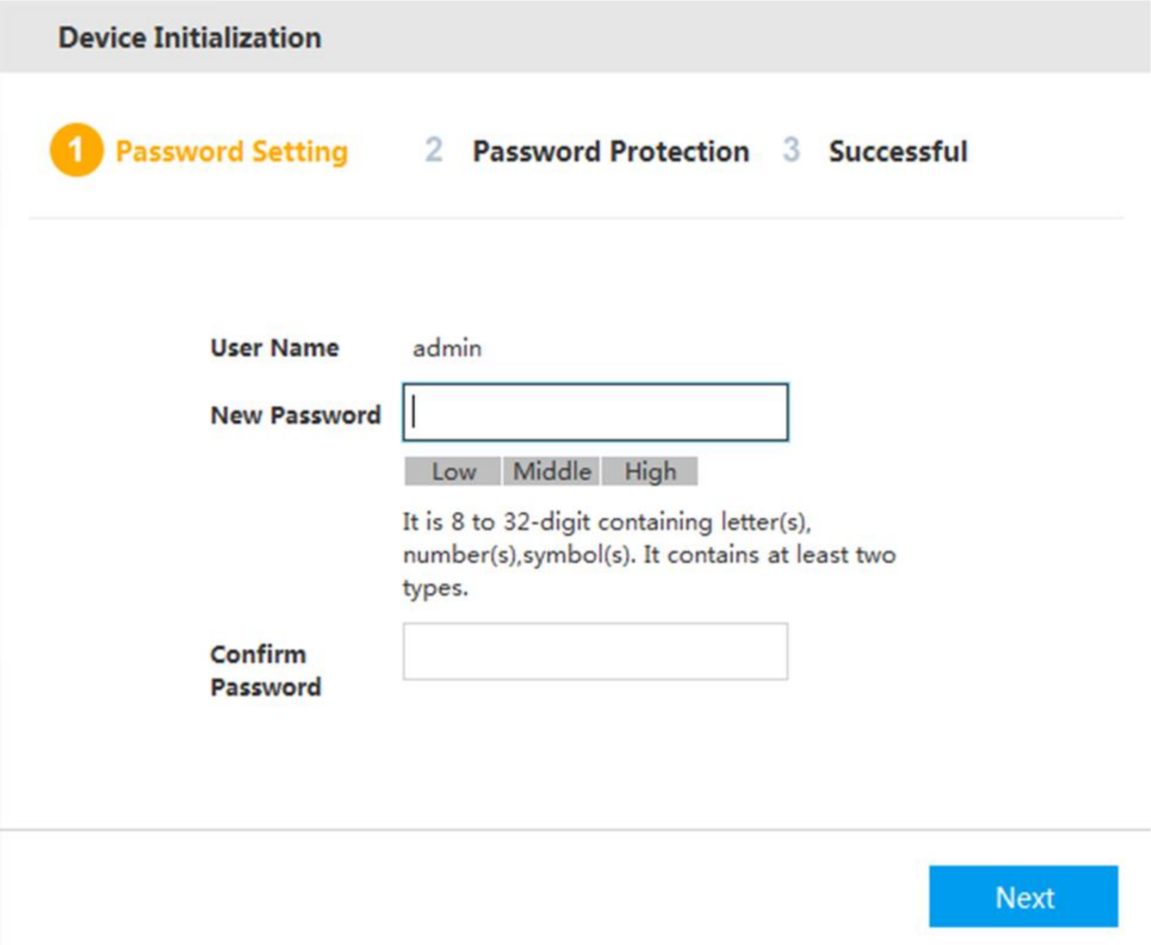
NOTE

The default IP address is 192.168.1.108.

Step 2 Press Enter key.

The **Password Setting** interface is displayed. See Figure 3-1.

Figure 3-1 Password setting



Device Initialization

1 Password Setting 2 Password Protection 3 Successful

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

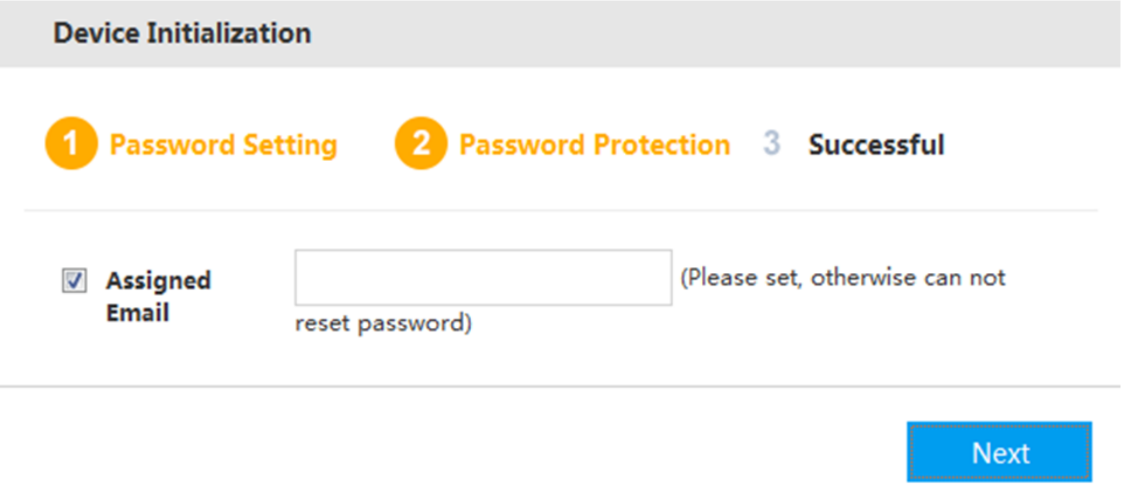
Step 3 In the **New Password** box, enter the new password.

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

Step 4 Click **Next**.

The **Password Protection** interface is displayed. See Figure 3-2.

Figure 3-2 Password protection



Device Initialization

1 Password Setting 2 Password Protection 3 Successful

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

Step 5 Enter the Assigned Email.

After entering the assigned email, you can reset the admin password through the email. For details, see "3.8.3.1.3 Resetting Password."

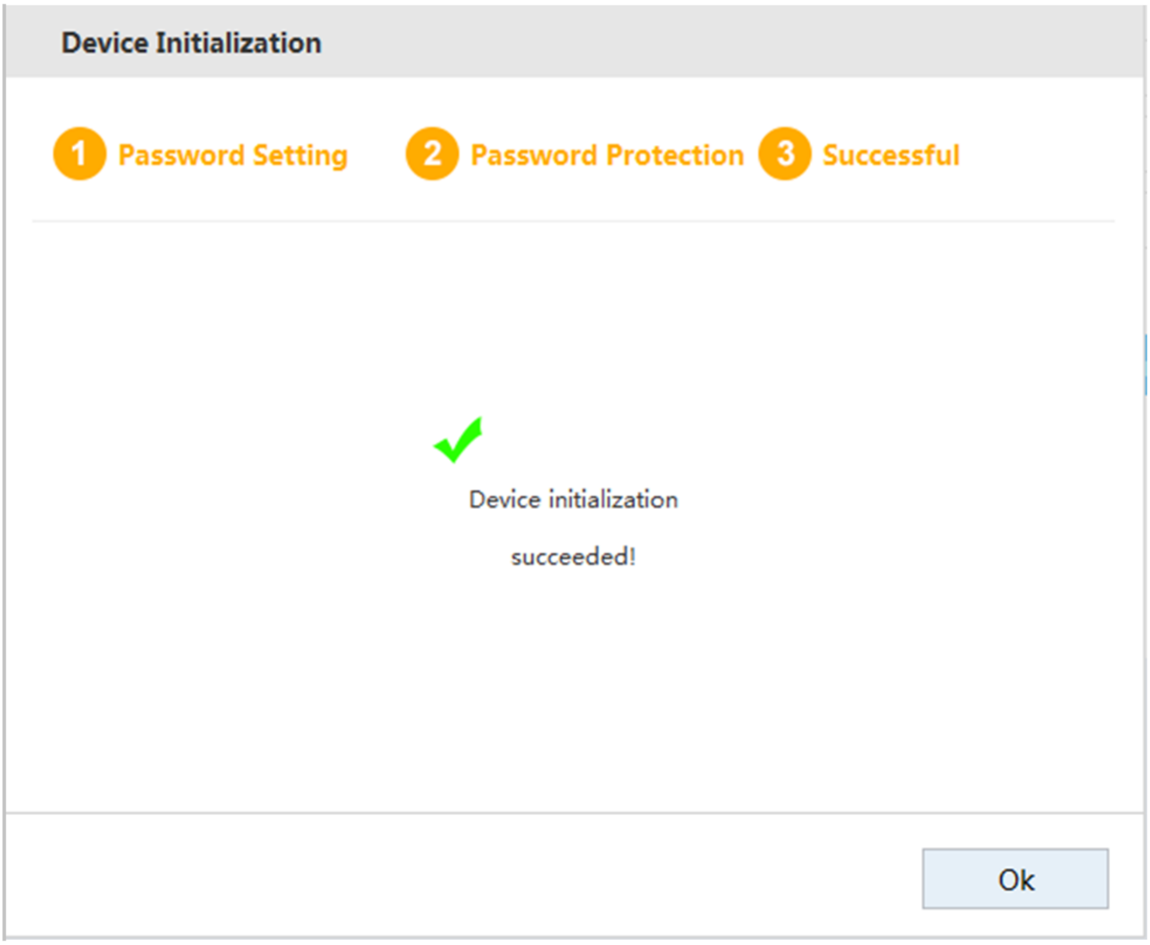
NOTE

- If you do not need to set the password protection, you can clear the **Assigned Email** check box.
- If you have not entered the assigned email, you can enter **SYSTEM MANAGER** > **Account** > **User** to set it after the initialization is completed. For details, see "3.8.3.1.2 Modifying Password."

Step 6 Click **Next**.

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

Figure 3-3 Device initialization completed



Device Initialization

Device initialization succeeded!

Step 7 Click **Ok** to complete the device initialization.

3.3 Logging in Web

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

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

The **Control Installation** interface is displayed.

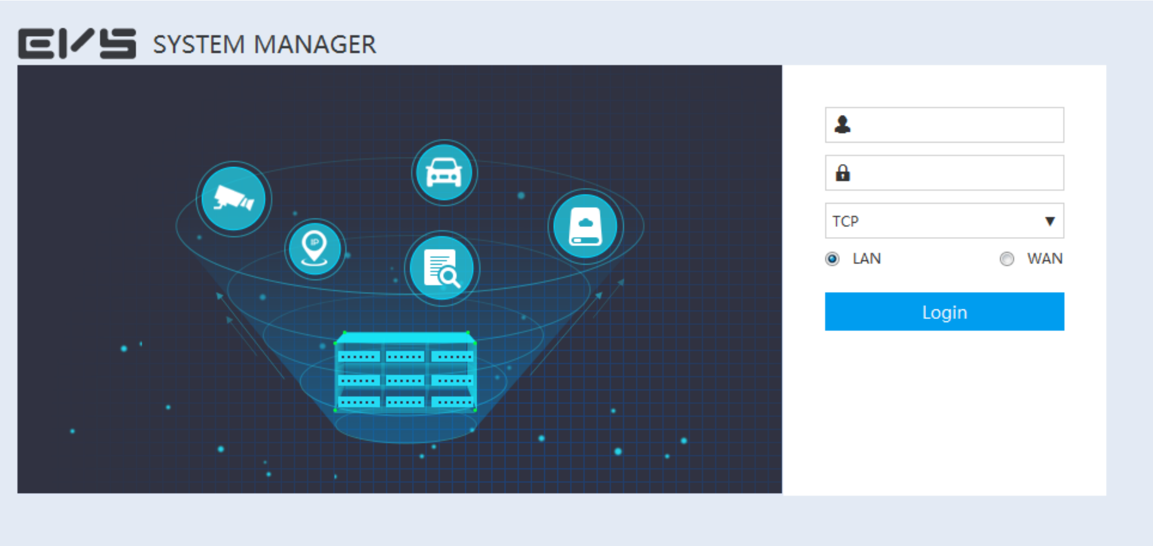
Step 2 Click **Install**.

The system downloads the control automatically. Click **Run** to install the control. The Web login interface is displayed after the installation is successful. See Figure 3-4.

NOTE

- 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 if any other plug-ins are installed which prohibit the control download, and reduce the security level of IE.

Figure 3-4 Web Login interface



Step 3 Enter the user name and password. Select connection type.

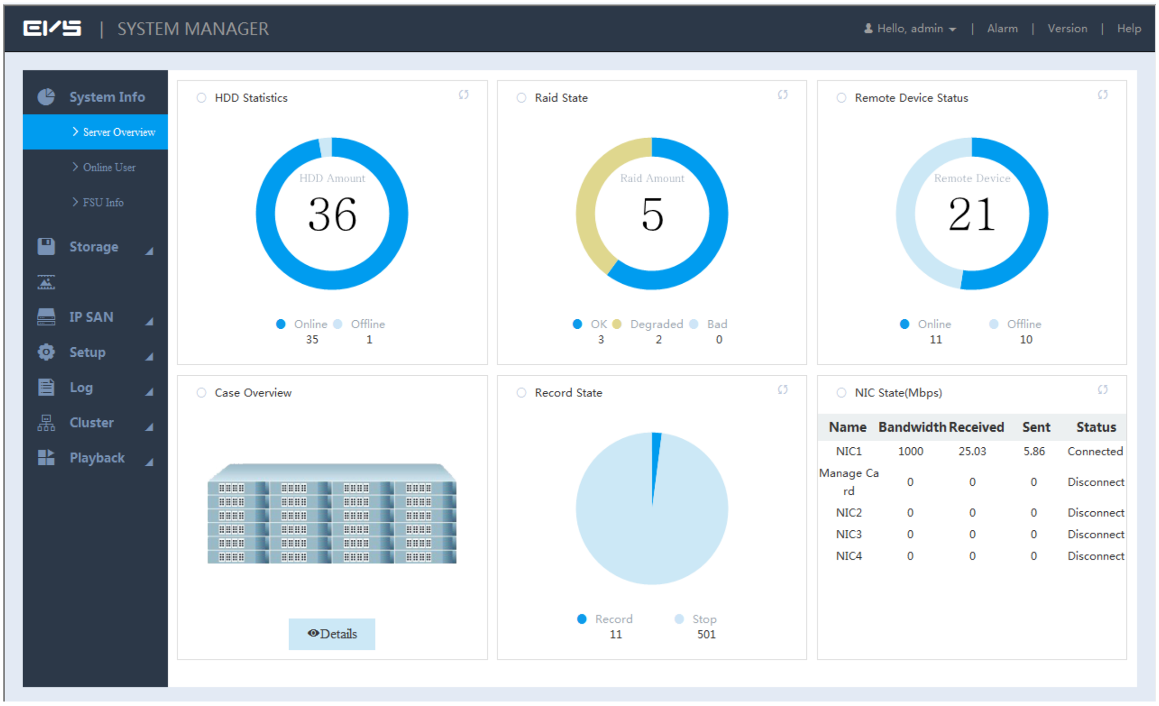
NOTE

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

Step 4 Click **Login**.

The **SYSTEM MANAGER** interface is displayed. See Figure 3-5. For details, see Table 3-1.

Figure 3-5 System manager



Name	Bandwidth	Received	Sent	Status
NIC1	1000	25.03	5.86	Connected
Manage Card	0	0	0	Disconnect
NIC2	0	0	0	Disconnect
NIC3	0	0	0	Disconnect
NIC4	0	0	0	Disconnect

Table 3-1 System manager description

No.	Name	Description
1	Function bar	You can view the basic system information, configure system parameters and play monitoring images and videos.
2	User name	Display the current login user name. Click ▼ on the right side of the user name and you can perform quick guide configuration and user logout. ● Quick guide: You can configure video/image direct storage and IPSAN. For details, see "3.4 Quick Guide." ● Exit: Log out the current user.
3	Alarm	Click **Alarm** and you can search the alarm logs of the EVS device. For details, see "3.7 Alarm."
4	Version	Click **Version** and you can view the version information of the EVS device, including video channel, S/N, Web version, system version, Bios version and Onvif Client version.
5	Help	Click **Help** and you can get the Quick Start Guide for EVS devices.

3.4 Quick Guide

The device provides quick guide setting functions, which facilitate users to quickly configure video/image direct storage and IPSAN according to different use scenarios.

3.4.1 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 which reduces the operating pressure of the management server.

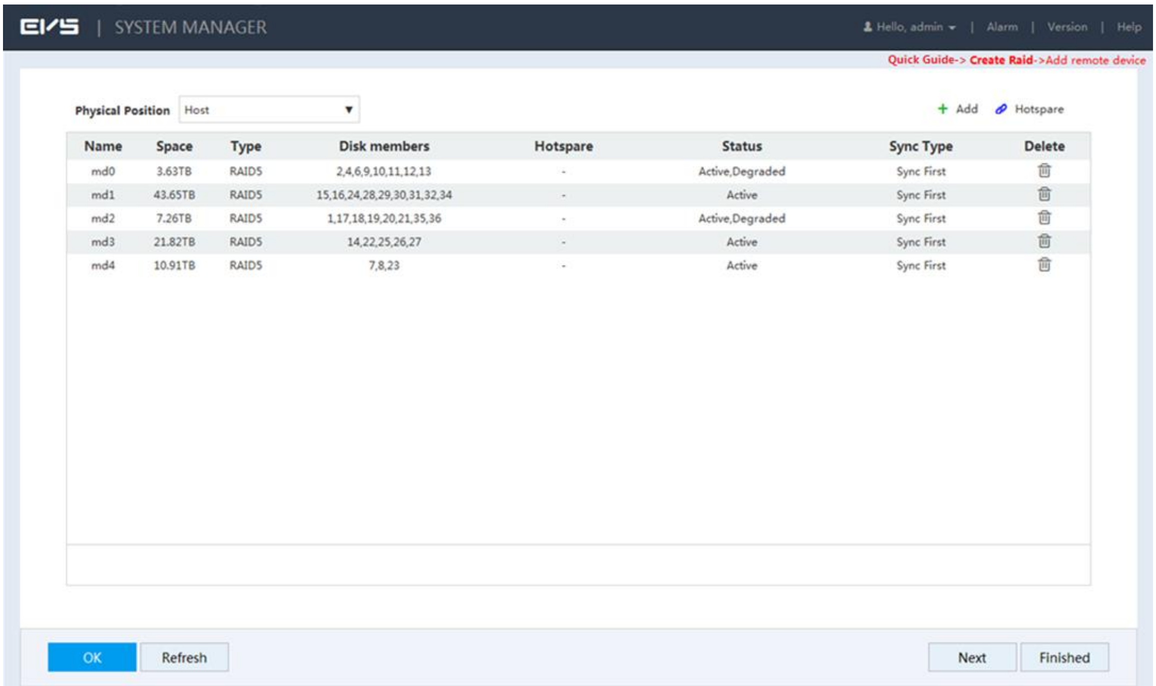
Step 1 Click ▼ on the right side of the user name. Select **Quick Guide** > **Video Direct Storage**.

The **Create Raid** interface is displayed. See Figure 3-6.

NOTE

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

Figure 3-6 RAID management


EVS | SYSTEM MANAGER
Hello, admin | Alarm | Version | Help
Quick Guide-> Create Raid->Add remote device
+ Add
Hotspare
OK
Refresh
Next
Finished

Physical Position: Host

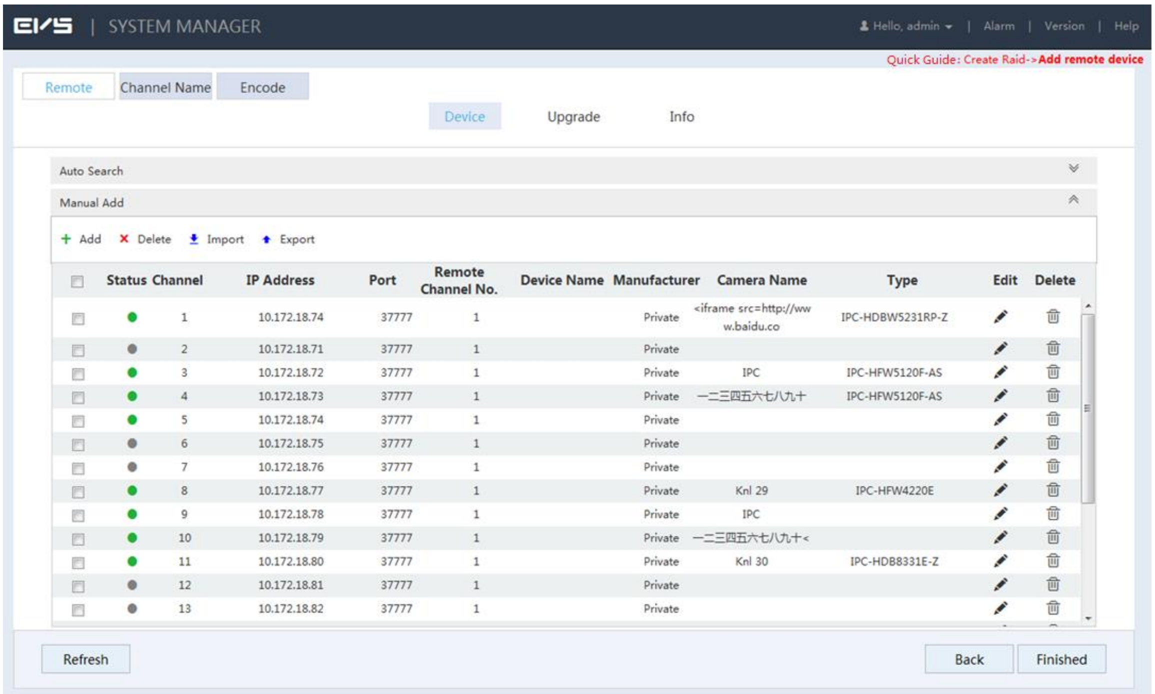
Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	3.63TB	RAID5	2,4,6,9,10,11,12,13	-	Active,Degraded	Sync First	🗑
md1	43.65TB	RAID5	15,16,24,28,29,30,31,32,34	-	Active	Sync First	🗑
md2	7.26TB	RAID5	1,17,18,19,20,21,35,36	-	Active,Degraded	Sync First	🗑
md3	21.82TB	RAID5	14,22,25,26,27	-	Active	Sync First	🗑
md4	10.91TB	RAID5	7,8,23	-	Active	Sync First	🗑

Step 2 Create RAID. For details, see "3.9.3 RAID Management."

Step 3 Click **Next**.

The **Add remote device** interface is displayed. See Figure 3-7.

Figure 3-7 Adding remote device



☐	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
☐	🟢	1	10.172.18.74	37777	1		Private	<iframe src=http://www.baidu.co	IPC-HDBW5231RP-Z	✎	🗑
☐	⚫	2	10.172.18.71	37777	1		Private			✎	🗑
☐	🟢	3	10.172.18.72	37777	1		Private	IPC	IPC-HFW5120F-AS	✎	🗑
☐	🟢	4	10.172.18.73	37777	1		Private	一二三四五六七八九十	IPC-HFW5120F-AS	✎	🗑
☐	🟢	5	10.172.18.74	37777	1		Private			✎	🗑
☐	⚫	6	10.172.18.75	37777	1		Private			✎	🗑
☐	⚫	7	10.172.18.76	37777	1		Private			✎	🗑
☐	🟢	8	10.172.18.77	37777	1		Private	Knl 29	IPC-HFW4220E	✎	🗑
☐	🟢	9	10.172.18.78	37777	1		Private	IPC		✎	🗑
☐	🟢	10	10.172.18.79	37777	1		Private	一二三四五六七八九十<		✎	🗑
☐	🟢	11	10.172.18.80	37777	1		Private	Knl 30	IPC-HDB8331E-Z	✎	🗑
☐	⚫	12	10.172.18.81	37777	1		Private			✎	🗑
☐	⚫	13	10.172.18.82	37777	1		Private			✎	🗑

Step 4 Add remote device. For details, see "3.5 Adding Remote Device."

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

3.4.2 Image Direct Storage

Image direct storage refers to the automatic storage of images snapped in the intelligent events into the direct memory disk, which can reduce the intermediate forwarding links of the system and make the system more efficient, stable and reliable.

Before using the image direct storage function, you need to set a disk for the image direct memory.

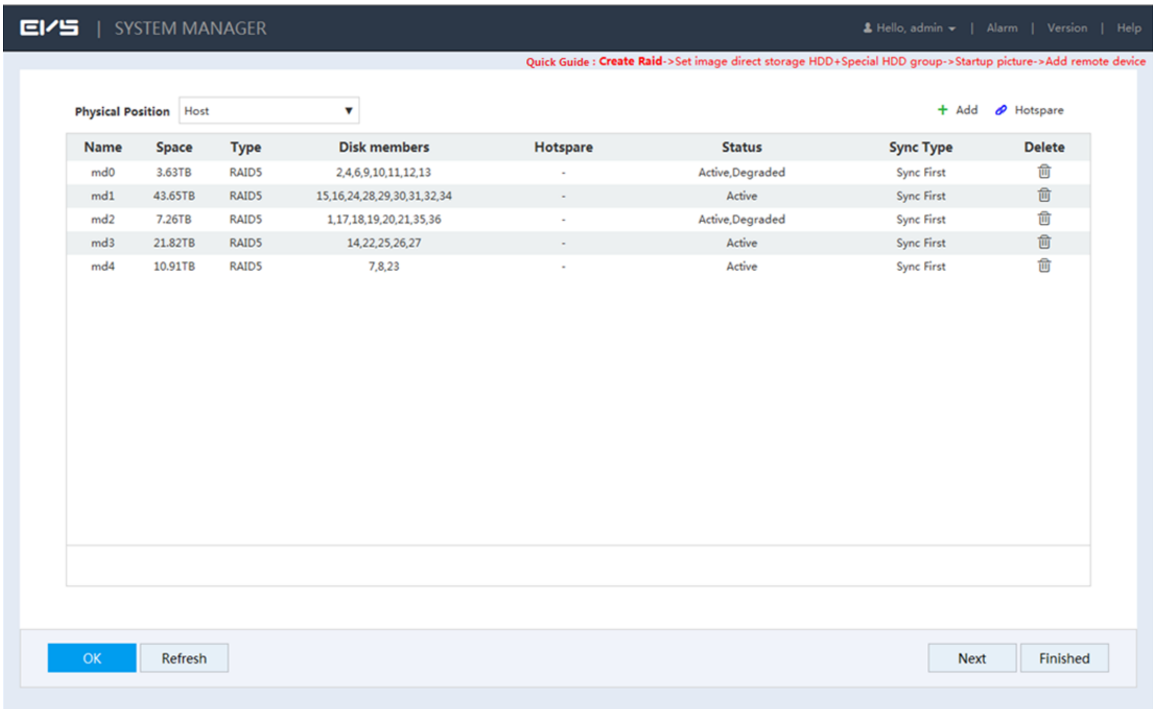
Step 1 Click ▼ on the right side of the user name. Select **Quick Guide** > **Image Direct Storage**.

The **Create Raid** interface is displayed. See Figure 3-8.

NOTE

The steps to quick configure the image direct storage scenario are displayed on the top right corner of the screen.

Figure 3-8 RAID management



Quick Guide : **Create Raid**->Set image direct storage HDD+Special HDD group->Startup picture->Add remote device

Physical Position: Host

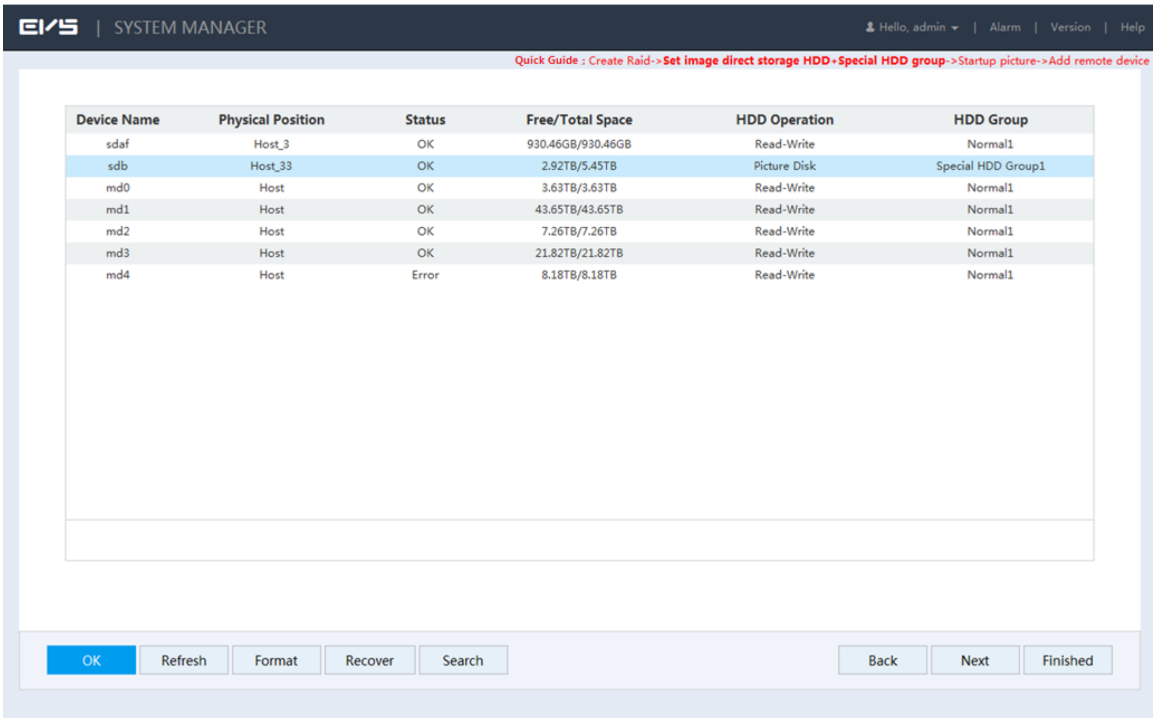
Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	3.63TB	RAID5	2,4,6,9,10,11,12,13	-	Active,Degraded	Sync First	🗑
md1	43.65TB	RAID5	15,16,24,28,29,30,31,32,34	-	Active	Sync First	🗑
md2	7.26TB	RAID5	1,17,18,19,20,21,35,36	-	Active,Degraded	Sync First	🗑
md3	21.82TB	RAID5	14,22,25,26,27	-	Active	Sync First	🗑
md4	10.91TB	RAID5	7,8,23	-	Active	Sync First	🗑

Step 2 Create RAID. For details, see "3.9.3 RAID Management."

Step 3 Click **Next**.

The **Set image direct storage HDD + Special HDD group** interface is displayed. See Figure 3-9.

Figure 3-9 Setting image direct storage HDD and special HDD group



Quick Guide : Create Raid->**Set image direct storage HDD+Special HDD group**->Startup picture->Add remote device

Device Name	Physical Position	Status	Free/Total Space	HDD Operation	HDD Group
sdaf	Host_3	OK	930.46GB/930.46GB	Read-Write	Normal1
sdb	Host_33	OK	2.92TB/5.45TB	Picture Disk	Special HDD Group1
md0	Host	OK	3.63TB/3.63TB	Read-Write	Normal1
md1	Host	OK	43.65TB/43.65TB	Read-Write	Normal1
md2	Host	OK	7.26TB/7.26TB	Read-Write	Normal1
md3	Host	OK	21.82TB/21.82TB	Read-Write	Normal1
md4	Host	Error	8.18TB/8.18TB	Read-Write	Normal1

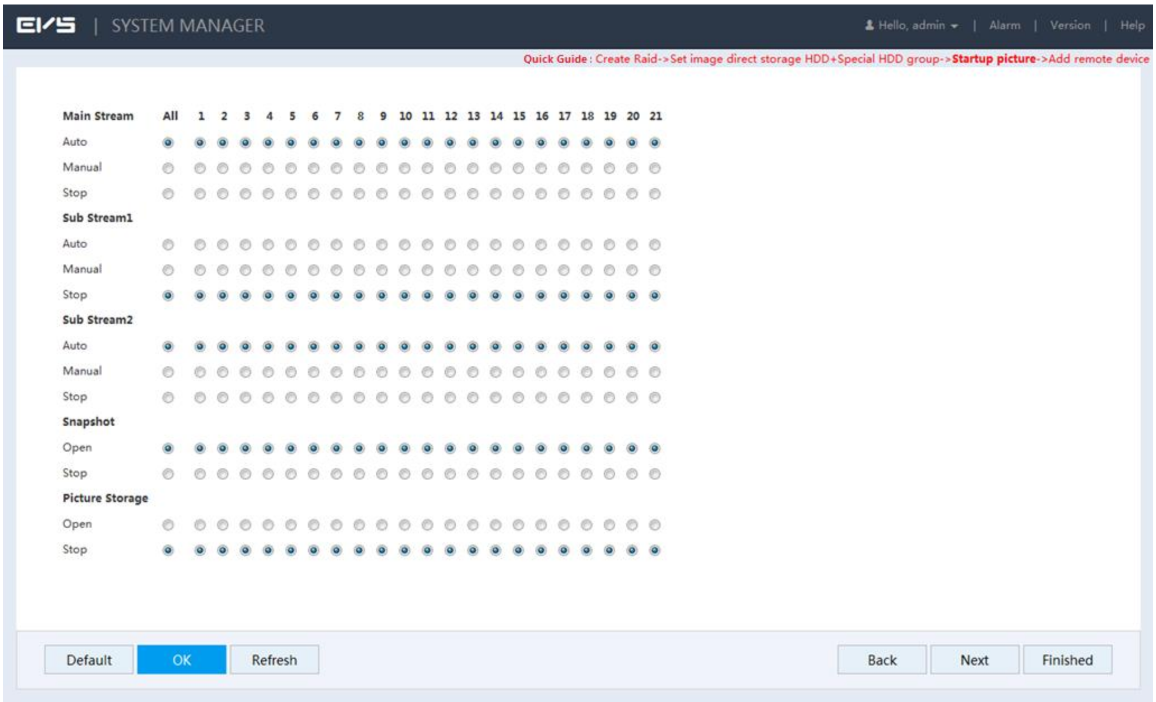
Step 4 Set the image direct storage HDD and HDD group.

1) Set the **HDD Operation** of one or several disks to **Image Direct Storage**.
2) Set the **HDD Group** of the image direct storage disk to **Special HDD Group**.
3) Click **OK** to save the configuration.

Step 5 Click **Next**.

The **Startup picture** interface is displayed. See Figure 3-10.

Figure 3-10 Picture startup



Quick Guide : Create Raid->Set image direct storage HDD+Special HDD group->**Startup picture**->Add remote device

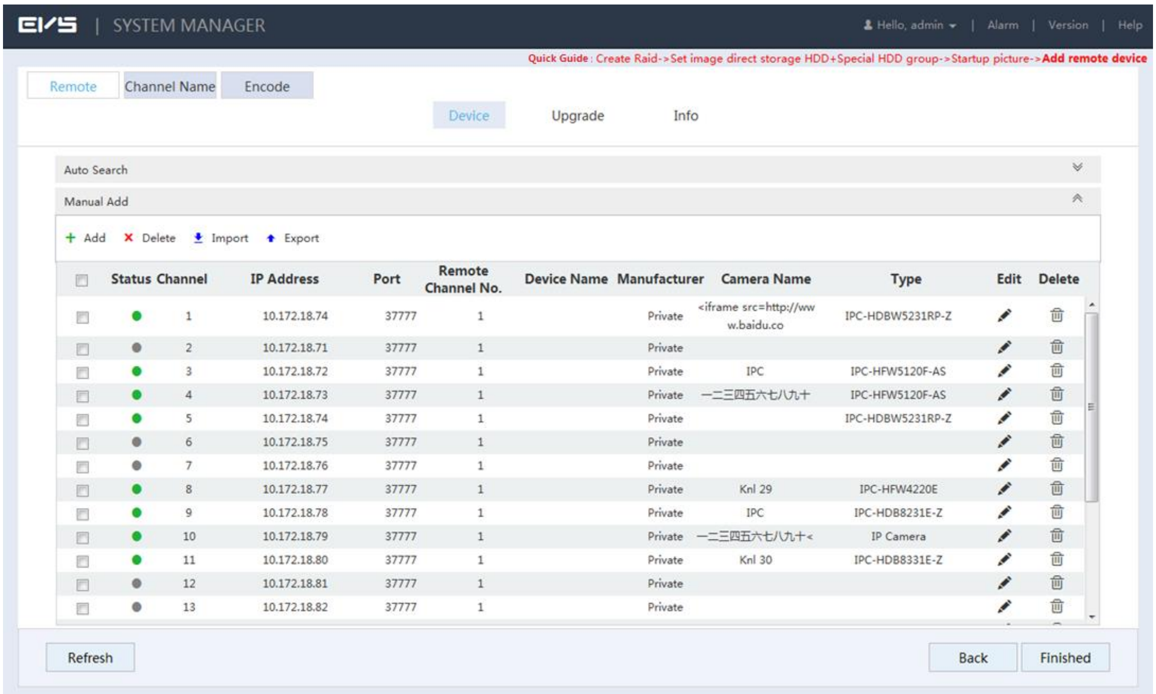
Main Stream	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Sub Stream1																						
Auto	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Sub Stream2																						
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Snapshot																						
Open	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Stop	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Picture Storage																						
Open	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

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

Step 7 Click **Next**.

The **Add remote device** interface is displayed. See Figure 3-11.

Figure 3-11 Remote device



Quick Guide : Create Raid->Set image direct storage HDD+Special HDD group->Startup picture->**Add remote device**

□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	10.172.18.74	37777	1		Private	<iframe src=http://www.baidu.co	IPC-HDBW5231RP-Z	✎	🗑
□	●	2	10.172.18.71	37777	1		Private			✎	🗑
□	●	3	10.172.18.72	37777	1		Private	IPC	IPC-HFW5120F-AS	✎	🗑
□	●	4	10.172.18.73	37777	1		Private	一二三四五六七八九十	IPC-HFW5120F-AS	✎	🗑
□	●	5	10.172.18.74	37777	1		Private		IPC-HDBW5231RP-Z	✎	🗑
□	●	6	10.172.18.75	37777	1		Private			✎	🗑
□	●	7	10.172.18.76	37777	1		Private			✎	🗑
□	●	8	10.172.18.77	37777	1		Private	Knl 29	IPC-HFW4220E	✎	🗑
□	●	9	10.172.18.78	37777	1		Private	IPC	IPC-HDB8231E-Z	✎	🗑
□	●	10	10.172.18.79	37777	1		Private	一二三四五六七八九十<	IP Camera	✎	🗑
□	●	11	10.172.18.80	37777	1		Private	Knl 30	IPC-HDB8331E-Z	✎	🗑
□	●	12	10.172.18.81	37777	1		Private			✎	🗑
□	●	13	10.172.18.82	37777	1		Private			✎	🗑

Step 8 Add remote device. For details, see "3.5 Adding Remote Device."

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

NOTE

After the configuration, you can search the direct stored images. For details, see "3.6.3 Image Direct Storage."

3.4.3 IPSAN

Internet Protocol Storage Area Network (IPSAN) is a kind of network storage technology based on IP network. It builds disks and Redundant Array of Independent Disks (RAID) into a virtual logic device (i.e. storage pool), and shares the storage path with other devices through Network File System (NFS), Internet Small Computer System Interface (iSCSI), File Transfer Protocol (FTP) and SAMBA to enable other devices to store data into the shared path.

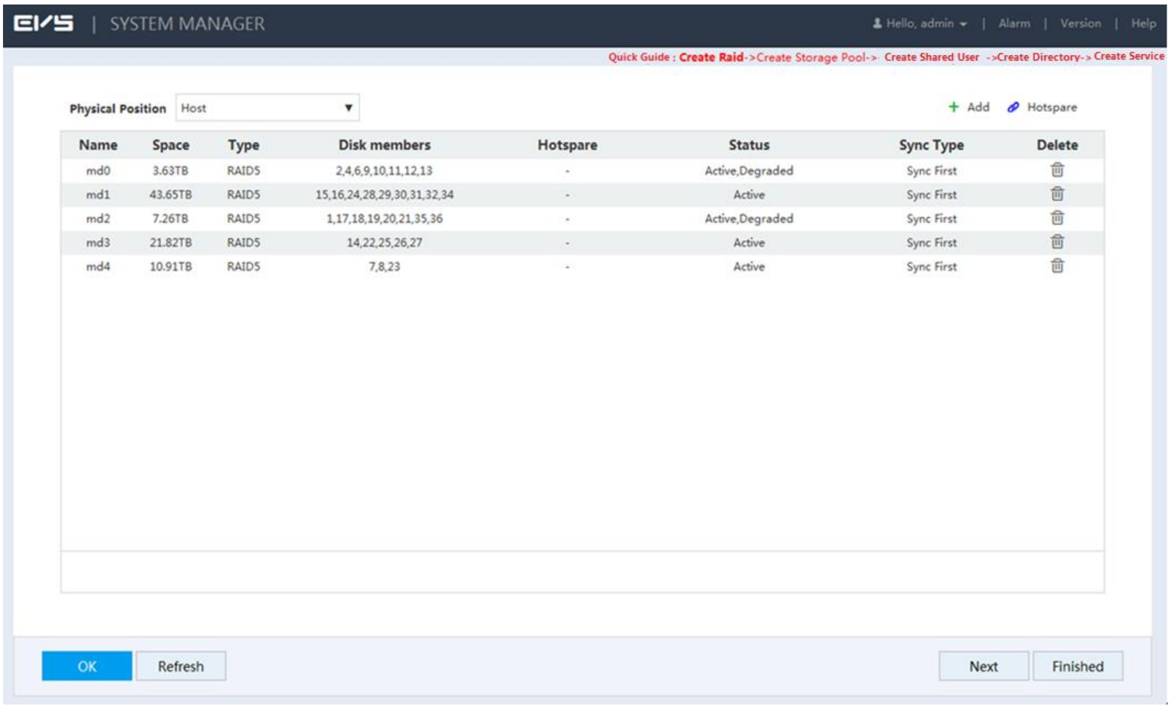
Step 1 Click ▼ on the right side of the user name. Select **Quick Guide** > **IPSAN**.

The **Create Raid** interface is displayed. See Figure 3-12.

NOTE

The steps to quick configure IPSAN are displayed on the top right corner of the screen.

Figure 3-12 RAID management



SYSTEM MANAGER
Hello, admin
Alarm
Version
Help
Quick Guide : Create Raid->Create Storage Pool-> Create Shared User ->Create Directory-> Create Service
+ Add
Hotspare
OK
Refresh
Next
Finished

Physical Position: Host

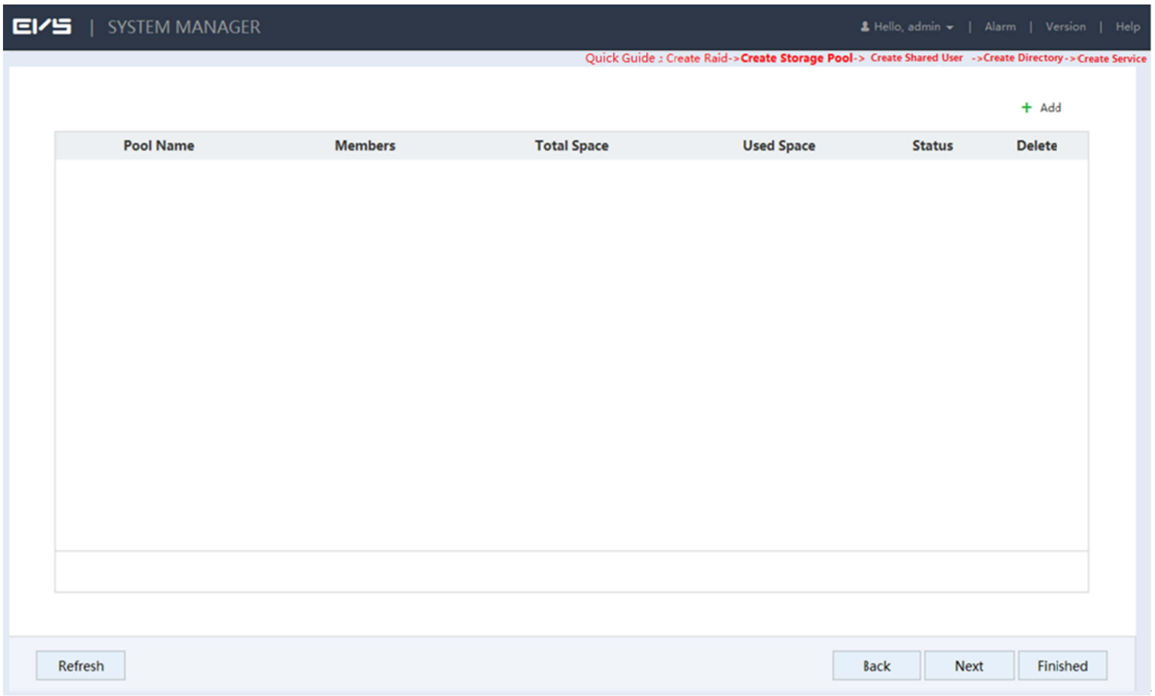
Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	3.63TB	RAID5	2,4,6,9,10,11,12,13	-	Active,Degraded	Sync First	🗑
md1	43.65TB	RAID5	15,16,24,28,29,30,31,32,34	-	Active	Sync First	🗑
md2	7.26TB	RAID5	1,17,18,19,20,21,35,36	-	Active,Degraded	Sync First	🗑
md3	21.82TB	RAID5	14,22,25,26,27	-	Active	Sync First	🗑
md4	10.91TB	RAID5	7,8,23	-	Active	Sync First	🗑

Step 2 Create RAID. For details, see "3.9.3 RAID Management."

Step 3 Click **Next**.

The **Create Storage Pool** interface is displayed. See Figure 3-13.

Figure 3-13 Storage pool

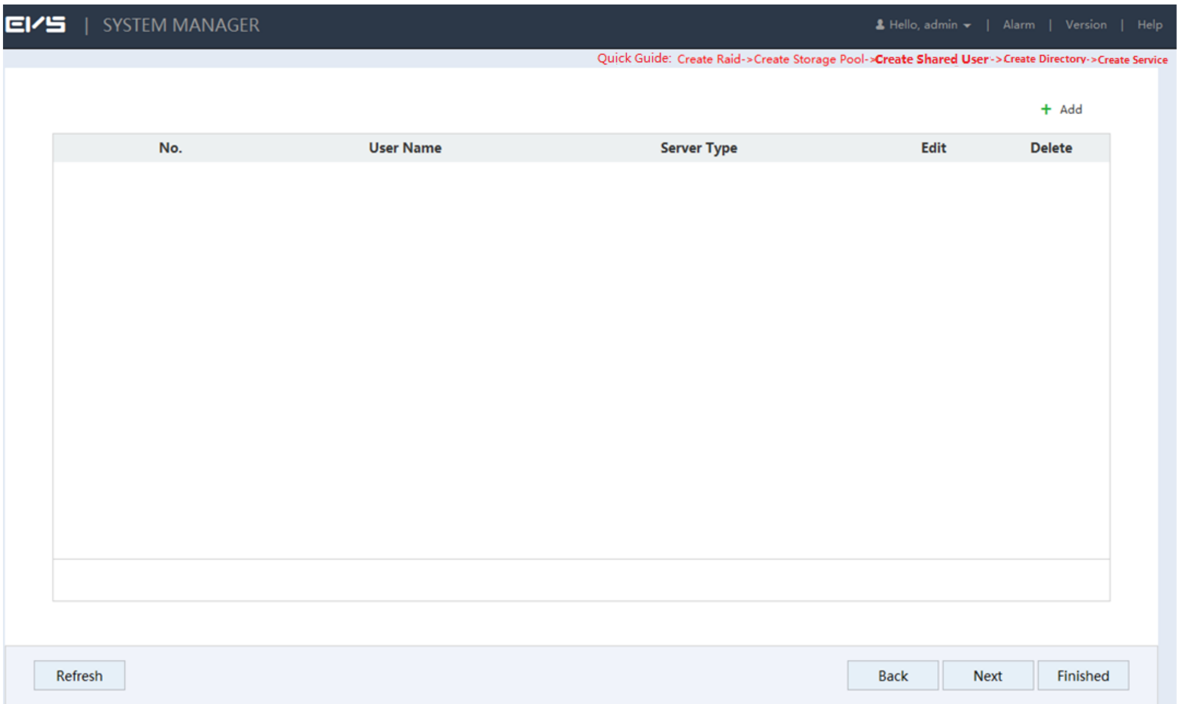

SYSTEM MANAGER
Hello, admin | Alarm | Version | Help
Quick Guide : Create Raid->Create Storage Pool-> Create Shared User ->Create Directory->Create Service
Add
Pool Name
Members
Total Space
Used Space
Status
Delete
Refresh
Back
Next
Finished

Step 4 Create storage pool. For details, see "3.11.1 Creating Storage Pool."

Step 5 Click **Next**.

The **Create Shared User** interface is displayed. See Figure 3-14.

Figure 3-14 Creating shared user

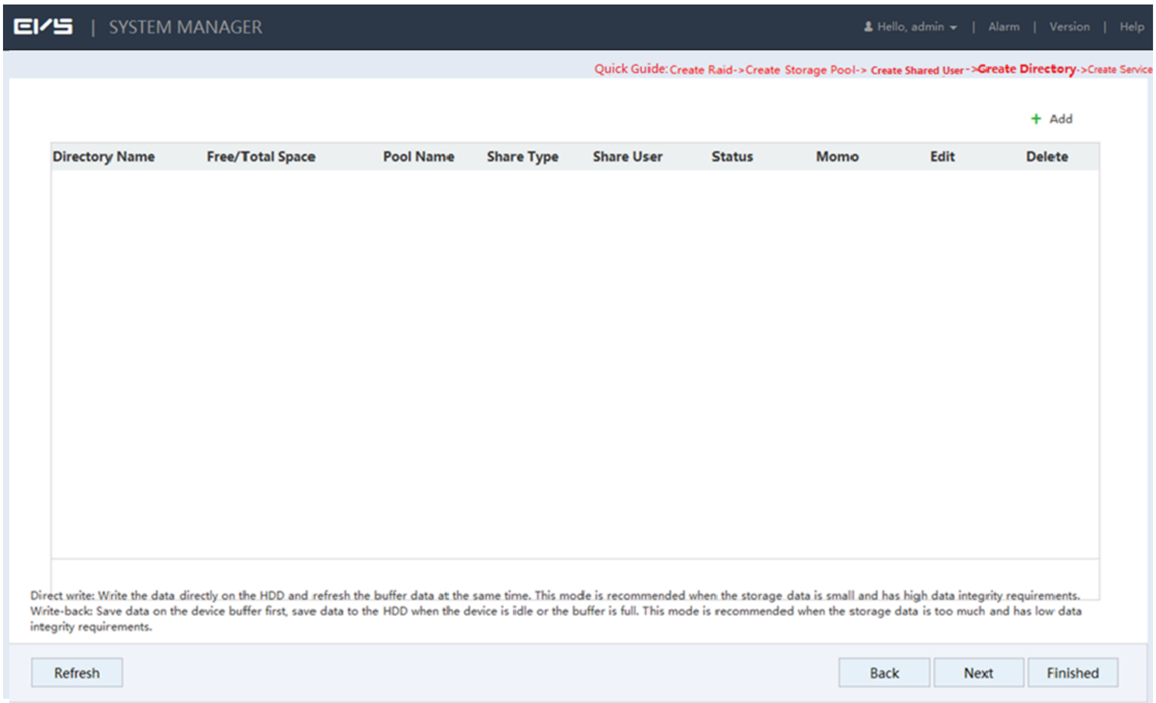

SYSTEM MANAGER
Hello, admin | Alarm | Version | Help
Quick Guide: Create Raid->Create Storage Pool->Create Shared User->Create Directory->Create Service
Add
No.
User Name
Server Type
Edit
Delete
Refresh
Back
Next
Finished

Step 6 Create shared user. For details, see "3.11.2 Shared Account Management."

Step 7 Click **Next**.

The **Create Directory** interface is displayed. See Figure 3-15.

Figure 3-15 Creating shared directory


SYSTEM MANAGER
Hello, admin
Alarm
Version
Help
Quick Guide: Create Raid->Create Storage Pool-> Create Shared User->Create Directory->Create Service
+ Add
Refresh
Back
Next
Finished

Directory Name	Free/Total Space	Pool Name	Share Type	Share User	Status	Momo	Edit	Delete

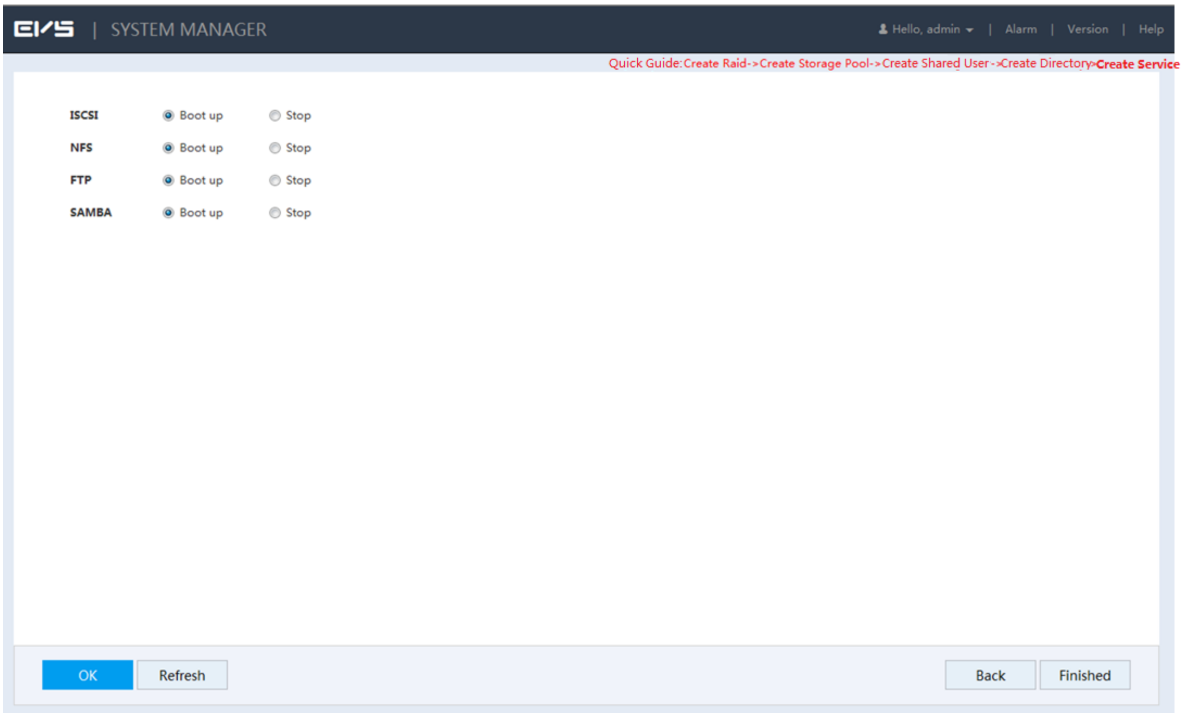
Direct write: Write the data directly on the HDD and refresh the buffer data at the same time. This mode is recommended when the storage data is small and has high data integrity requirements.
Write-back: Save data on the device buffer first, save data to the HDD when the device is idle or the buffer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

Step 8 Create shared folder. For details, see "3.11.3 Shared Folder."

Step 9 Click **Next**.

The **Create Service** interface is displayed. See Figure 3-16.

Figure 3-16 Creating shared service


SYSTEM MANAGER
Hello, admin
Alarm
Version
Help
Quick Guide: Create Raid->Create Storage Pool->Create Shared User->Create Directory>Create Service
OK
Refresh
Back
Finished

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

Step 10 Select the shared service(s) you want to enable. Click **OK** to save the setting.

Step 11 Click **Finished** to save the configuration.

3.5 Adding Remote Device

After adding the remote device, the device can receive, store and manage the video stream transmitted by the remote device, so as to realize the distributed advantage of the network. You can browse, replay, manage and store several remote devices.

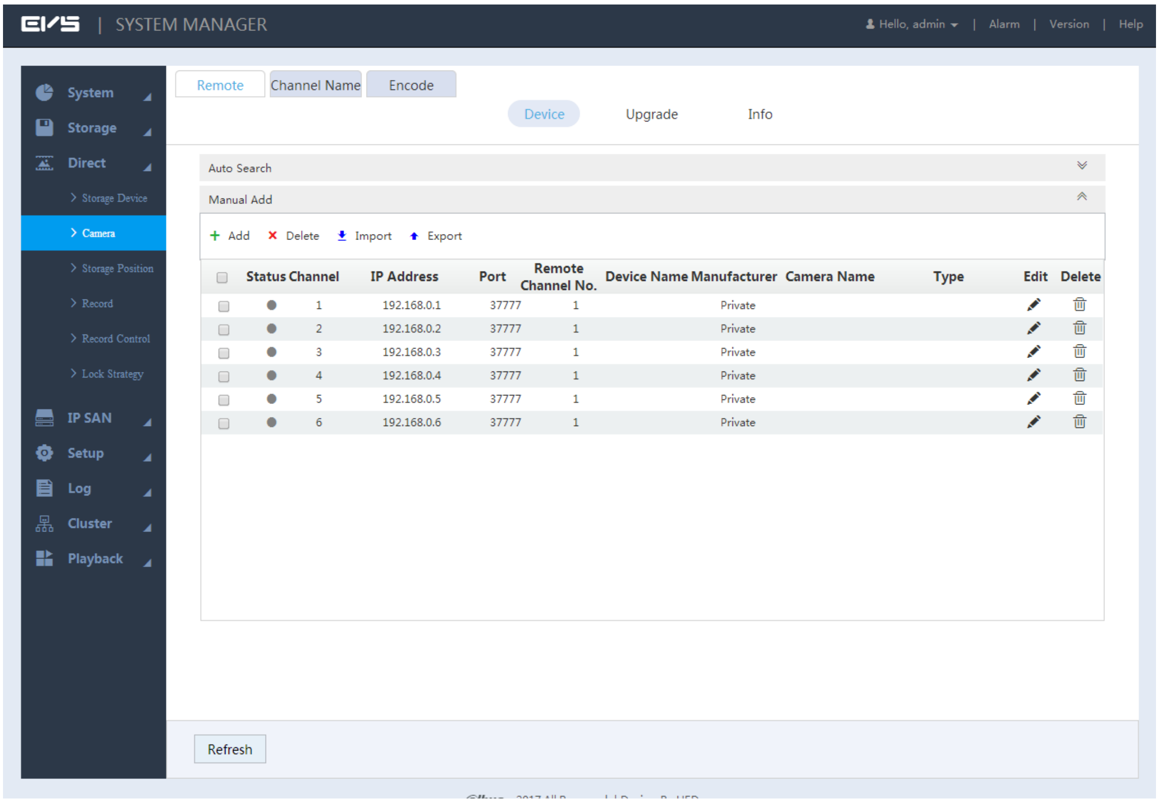
The system supports adding remote devices in three ways: searching add, single add and batch add.

- Searching add: 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.
- Single add: Add a few remote devices and you know the IP address, user name and password of the device.
- Batch add: When the first three sections of the remote device IP addresses are the same (e.g. 192.168.1.1-192.168.1.255), and the user name and password of the devices are also the same, this method is recommended to improve the speed of addition.
- Template import: Import remote devices in batch through the template file.

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

The **Device** interface is displayed. See Figure 3-17.

Figure 3-17 Remote device



□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.0.1	37777	1		Private			✎	🗑
□	●	2	192.168.0.2	37777	1		Private			✎	🗑
□	●	3	192.168.0.3	37777	1		Private			✎	🗑
□	●	4	192.168.0.4	37777	1		Private			✎	🗑
□	●	5	192.168.0.5	37777	1		Private			✎	🗑
□	●	6	192.168.0.6	37777	1		Private			✎	🗑

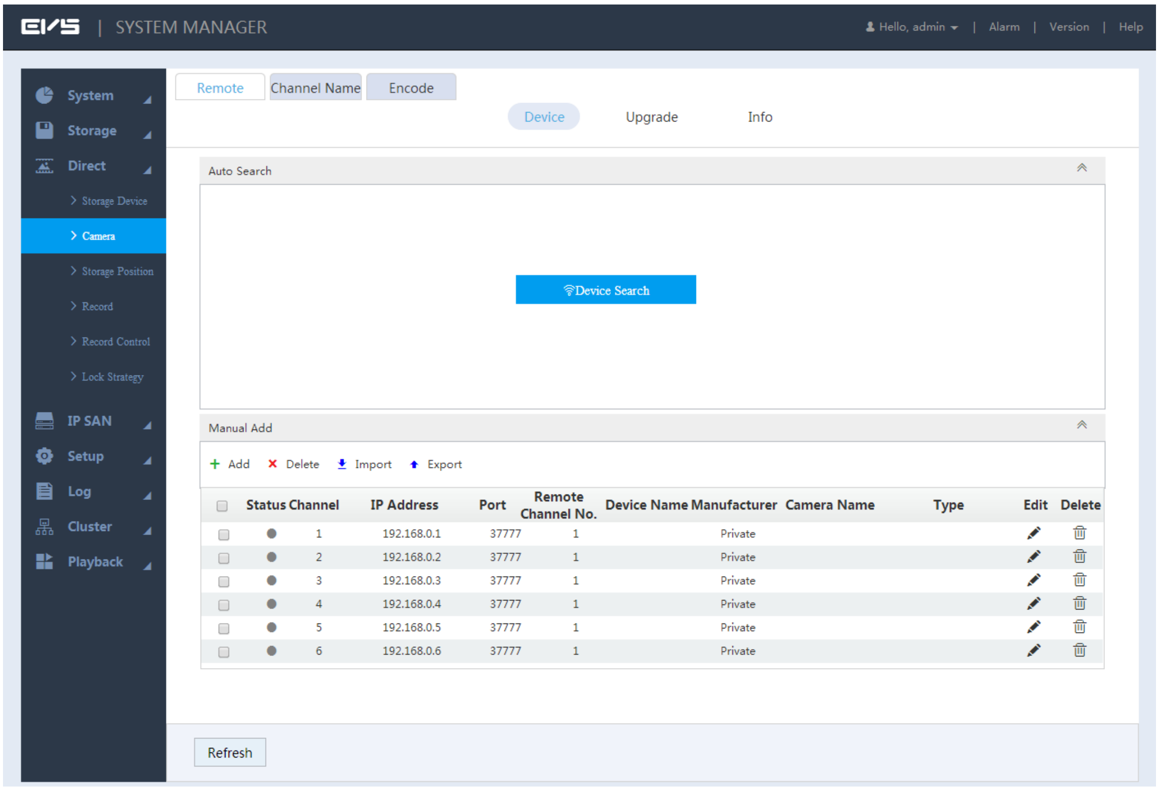
Step 2 Add remote device.

You can use searching add, single add or batch add.

- Searching add

1) Click ︾ on the right side of **Auto Search**.

The **Auto Search** interface is displayed. See Figure 3-18.



□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.0.1	37777	1		Private			✎	🗑
□	●	2	192.168.0.2	37777	1		Private			✎	🗑
□	●	3	192.168.0.3	37777	1		Private			✎	🗑
□	●	4	192.168.0.4	37777	1		Private			✎	🗑
□	●	5	192.168.0.5	37777	1		Private			✎	🗑
□	●	6	192.168.0.6	37777	1		Private			✎	🗑

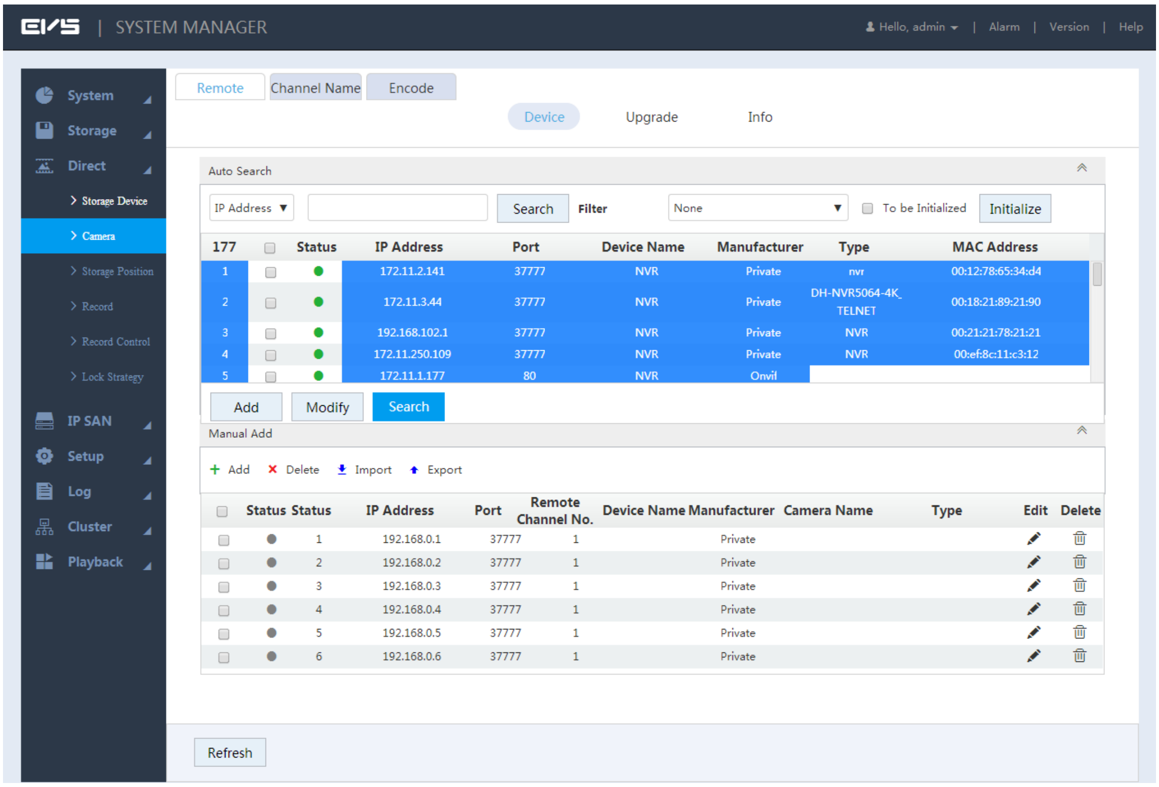
Figure 3-18 Automatic search

2) Click **Device Search**.

The results are displayed. See Figure 3-19. For details, see Table 3-2.

NOTE

The IP address of the added device will not appear in the search result list.



IP Address ▼ Filter None ▼ □ To be Initialized

177	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	172.11.2.141	37777	NVR	Private	nvr	00:12:78:65:34:d4
2	□	●	172.11.3.44	37777	NVR	Private	DH-NVR5064-4K_ TELNET	00:18:21:89:21:90
3	□	●	192.168.102.1	37777	NVR	Private	NVR	00:21:21:78:21:21
4	□	●	172.11.250.109	37777	NVR	Private	NVR	00:ef:8c:11:c3:12
5	□	●	172.11.1.177	80	NVR	Onvil		

□	Status	Status	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	192.168.0.1	37777	1		Private			✎	🗑
□	●	2	192.168.0.2	37777	1		Private			✎	🗑
□	●	3	192.168.0.3	37777	1		Private			✎	🗑
□	●	4	192.168.0.4	37777	1		Private			✎	🗑
□	●	5	192.168.0.5	37777	1		Private			✎	🗑
□	●	6	192.168.0.6	37777	1		Private			✎	🗑

Figure 3-19 Search results

Table 3-2 Description of auto search icons

Icon/Parameter	Description

Icon/Parameter	Description
IP Address ▼	Screen out the remote devices you need to add through IP address or MAC address. Steps see below: Click IP Address ▼ to select **IP Address** or **MAC Address**. Enter the IP address or MAC address of the remote device in the text box on the right of IP Address ▼. Click Search. The results are displayed.
Initialization	Select the **To Be Initialized** check box and click **Initialize**, you can modify the login password and IP address. For details, see "3.10.2.1.2 Initializing the Remote Device."
Filter	Set filter conditions according to device model. The system only displays the remote device information that meets the filter conditions, so as to facilitate the users to search for devices they need to add.
Modify	Select the check box in front of the remote device and click **Modify** to change the IP address of the device. NOTE ● 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	Click this icon to search the remote devices again.

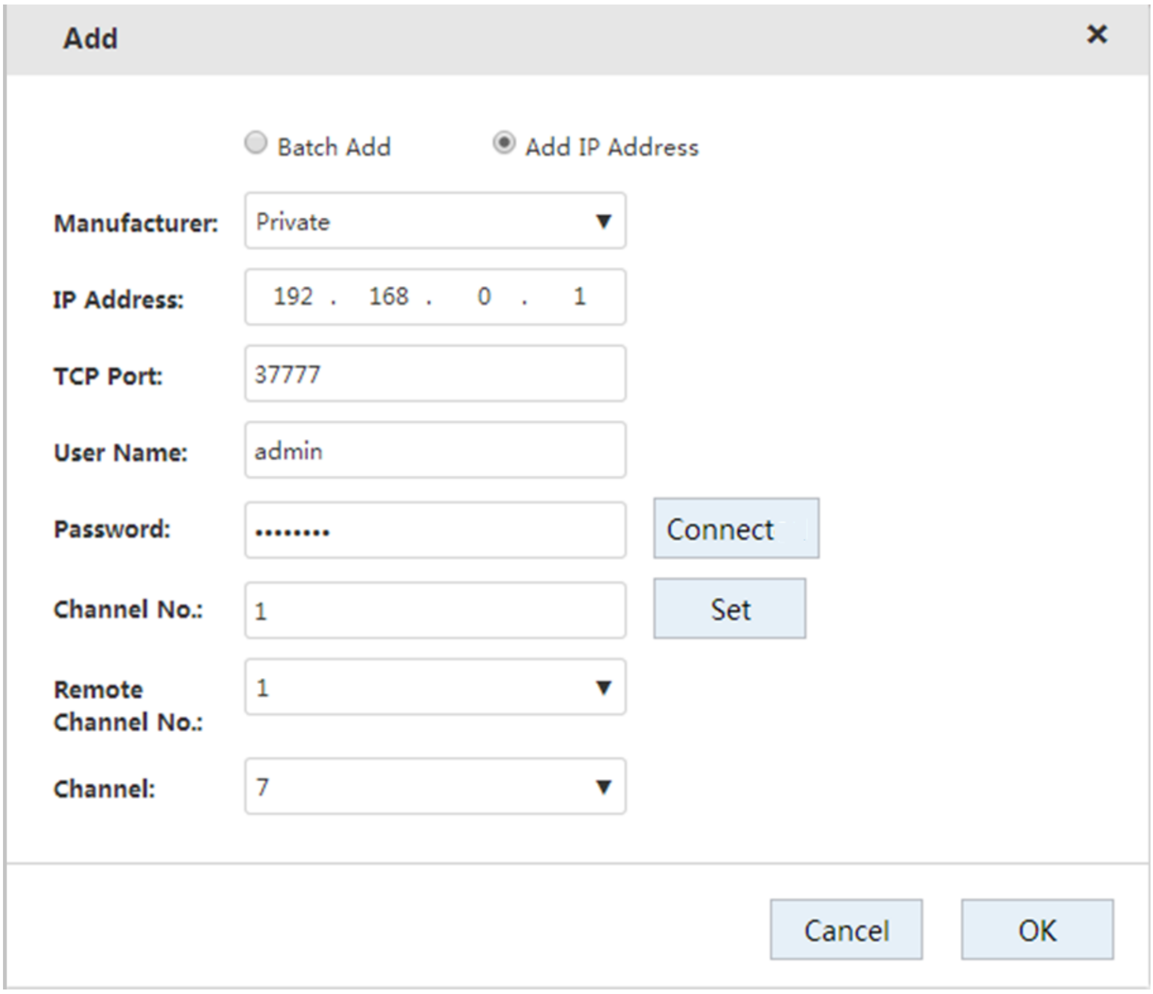
3) Double-click the remote device, or select the check box in front of the device and click **Add**, the system adds this remote device to the added list.

- Single add

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

The **Add** interface is displayed. See Figure 3-20.

Figure 3-20 Single add



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: 7

2) Select/Enter the parameters. For details, see Table 3-3.

Table 3-3 Parameter description for adding

Parameter	Description
Manufacturer	Select the manufacturer in the drop-down box according to the actual situation. NOTE 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 according to actual needs. The default is 37777. NOTE You neet to set it when the **Manufacturer** is set to **Private**.

Parameter	Description
RTSP Port	Set the RTSP port No. of the remote device. The default is 554. NOTE You do not need to configure it when the **Manufacturer** is set to **Private** or **Custom**.
HTTP Port	Set the HTTP port of the remote device. The default is 80. NOTE You do not need to configure it when the **Manufacturer** is set to **Private** or **Custom**.
User Name/Password	Enter the user name and password to log in the remote device.
Channel No.	Enter the **Channel No.** or click **Connect** to get the total channel number of the front-end device. NOTE 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 confirm 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.
Service Type	Set the corresponding service type of the remote device. NOTE ● Different manufacturers support different service types. See the actual interface. ● When the remote device is connected through private protocol, the default connection type is TCP.

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

- Batch add

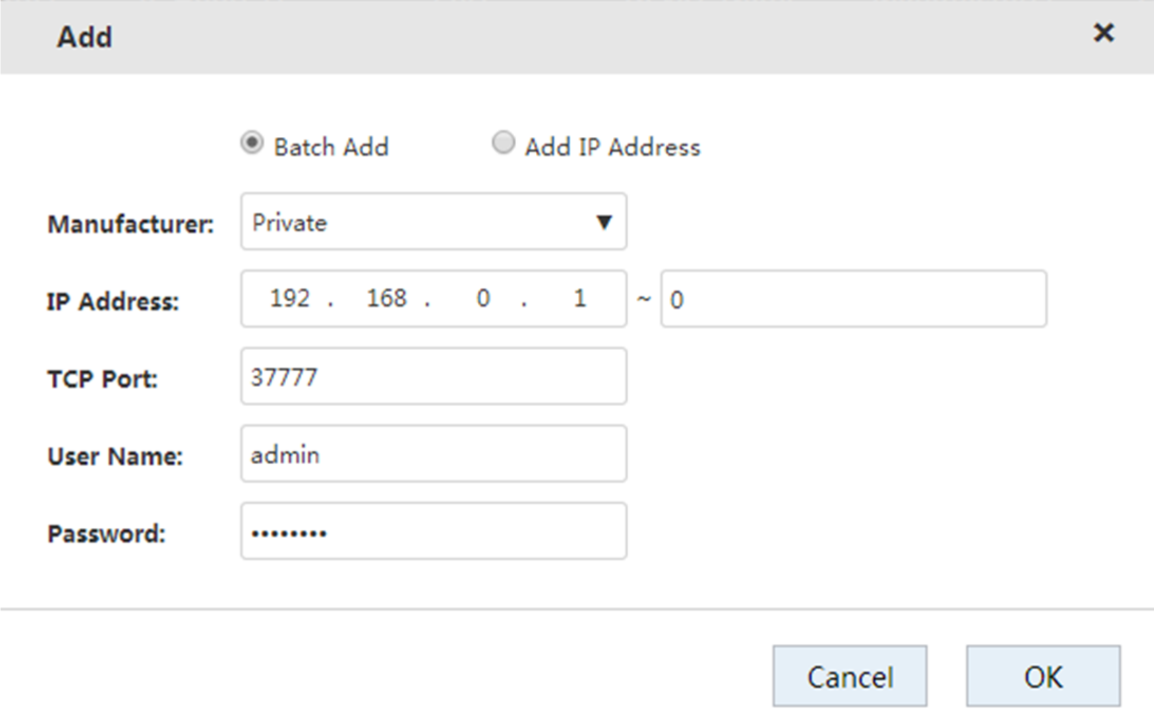
NOTE

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

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

The **Add** interface is displayed. See Figure 3-21.

Figure 3-21 Batch add



Add ×

● Batch Add ○ Add IP Address

Manufacturer: Private ▼

IP Address: 192 . 168 . 0 . 1 ~ 0

TCP Port: 37777

User Name: admin

Password: ••••••••

Cancel OK

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

NOTE

Batch add only supports devices of which the first three segments of the IP address are the same. Enter the search range of the fourth segment. For example: 192.168.1.1-192.168.1.255.

3) Set other parameters. For details, see Table 3-3.

4) Click **OK** to complete the adding.

- Template Import

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

◇ The default naming rule is RemoteConfig_*2016-12-13*.csv. *2016-12-13* is the date to export 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.

CAUTION

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

3) Click ⬇ to select template file.

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

NOTE

After adding, if the **Status** shows ● , the connection is successful. If the **Status** shows ● , the connection fails. Check the reason.

3.6 Monitoring Playback

Check the real-time monitoring images of the remote devices, play back record files and query direct-stored images.

3.6.1 Real-Time Monitoring

Select **Playback** > **Preview**. The **Preview** interface is displayed. See Figure 3-22. For details, see Table 3-4.

Figure 3-22 Real-time monitoring

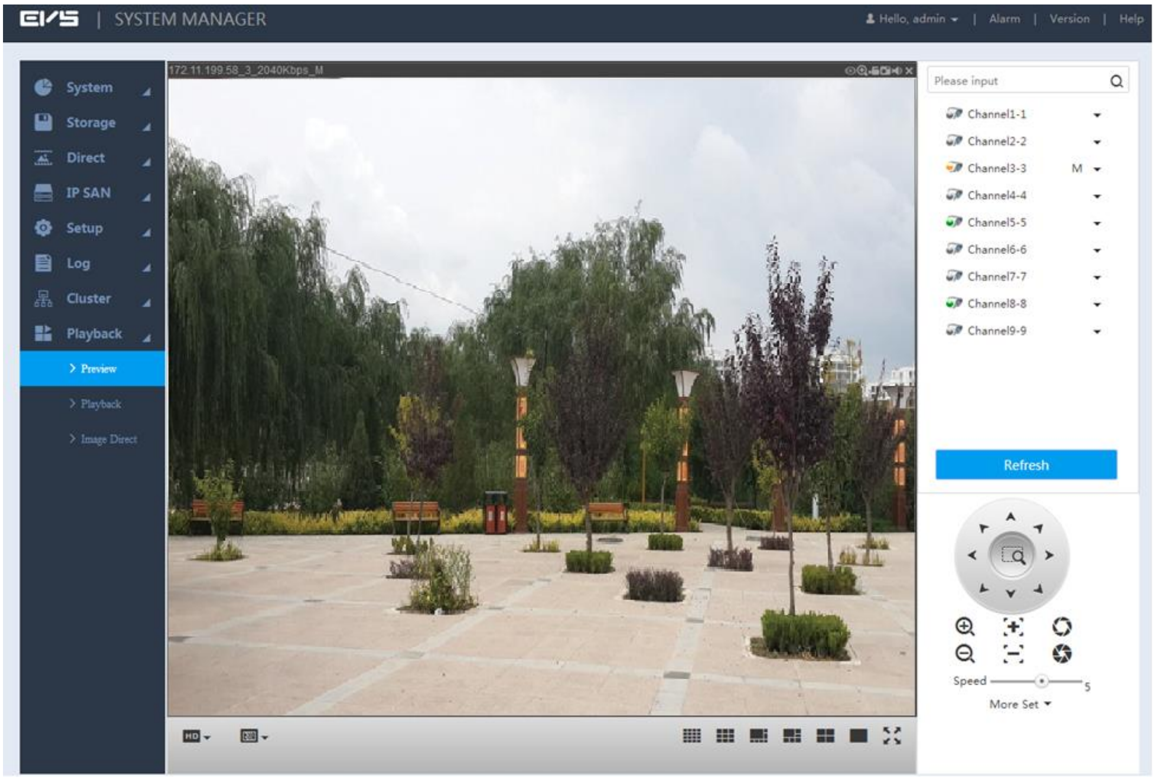


Table 3-4 Description of real-time monitoring

No.	Description
1	Real-time monitoring window. For details, see "3.6.1.1 Real-Time Monitoring Window."
2	Monitoring channel list. For details, see "3.6.1.2 Monitoring Channel List."
3	PTZ console. For details, see "3.6.1.3 PTZ Console."
4	Switch the number of real-time monitoring windows. Icons from left to right in sequence: 16 windows, nine windows, eight windows, six windows, four windows, single window and full-screen.
5	Set the fluency and quality of the real-time monitoring images. Real-time monitoring can flexibly adjust the priority of image fluency or video real-time. 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.

3.6.1.1 Real-Time Monitoring Window

Click the on-line remote device in the monitoring channel list to open the real-time monitoring screen of this device. For the picture of real-time monitoring window, see Figure 3-23. For details, see Table 3-5.

NOTE

- Click the drop-down box of the remote device in the monitor channel list to select the main stream or sub stream of the remote device for real-time monitoring.
- When select the sub stream for real-time monitoring, the sub stream shall be open and supported by the remote device.

Figure 3-23 Real-time monitoring window

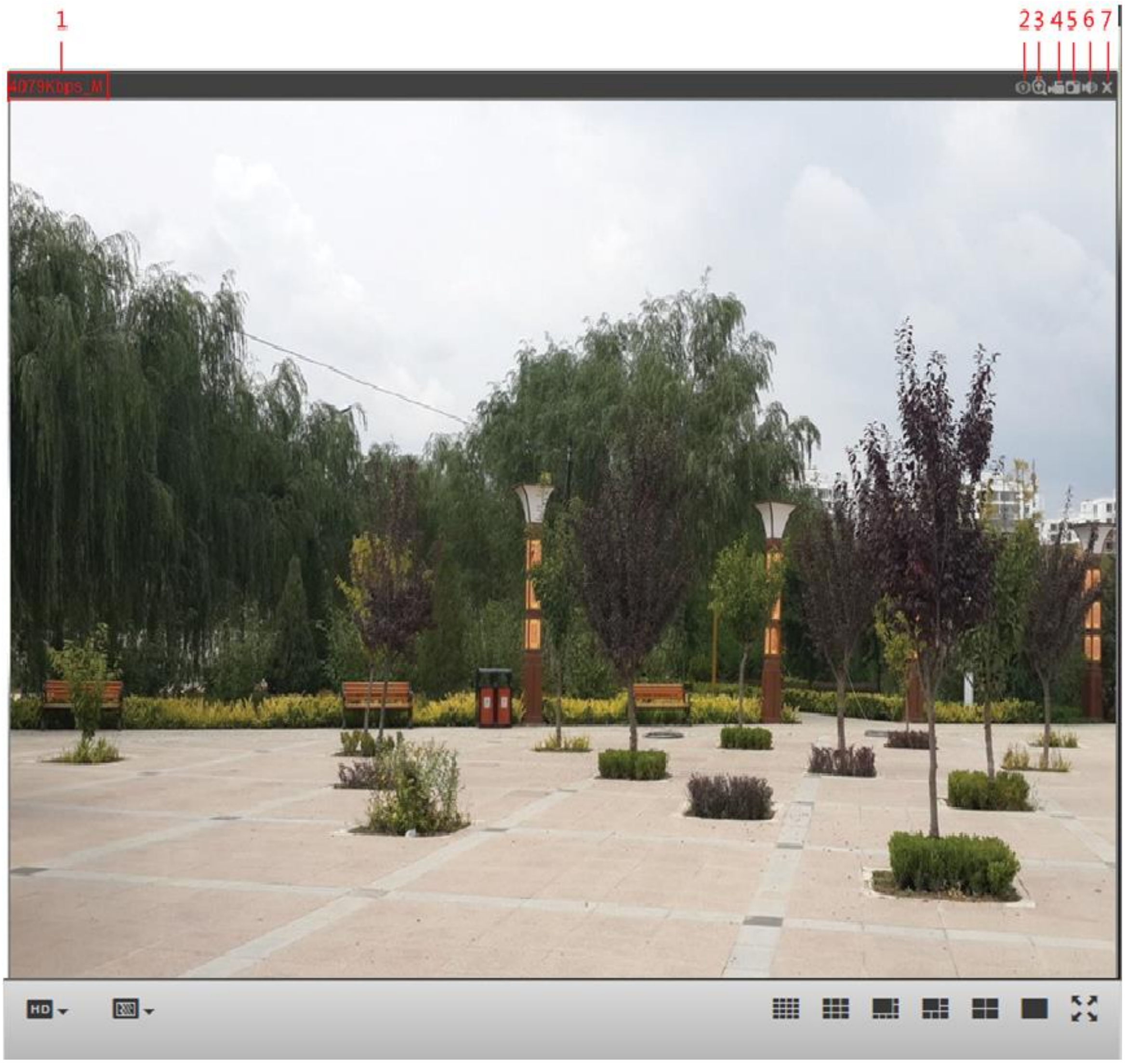


Table 3-5 Description of real-time monitoring window icons

No.	Description
1	Display the current stream value and decoding mode. NOTE M-main stream. S-sub stream.
2	Fish-eye Setting. Click this icon to adjust the mounting mode and display mode of the fish-eye camera. For details, see "3.6.1.4 Fish-Eye."

No.	Description
3	Partial enlargement. Click the icon and drag the left mouse button in the video window to select any area that will zoom in. Click this icon again or right-click to restore the original state.
4	Local record. Click this icon to start recording and click the icon again to stop it. 📖 NOTE The default storage path: C:\RecordDownload. For detailed operations to modify the default storage path, see "3.8.2.1 Local Settings."
5	Picture snapshot. Click this icon to start snapshot and click again to stop it. 📖 NOTE The default storage path: C:\PictureDownload. For detailed operations to modify the default storage path, see "3.8.2.1 Local Settings."
6	Audio settings. Click this icon to open/close audio. If the audio is closed, there is no sound in monitoring.
7	Close the video. Click this icon to close the current video.

3.6.1.2 Monitoring Channel List

For the monitoring channel list, see Figure 3-24. For details, see Table 3-6.

Figure 3-24 Monitoring channel list

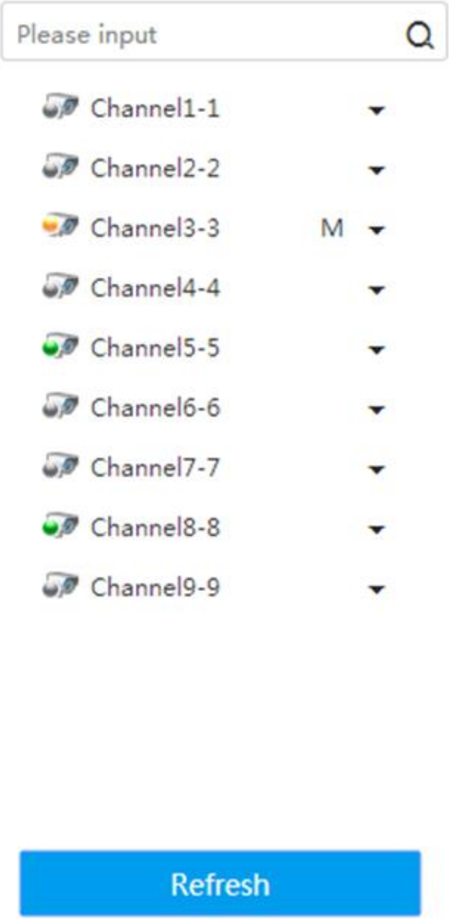
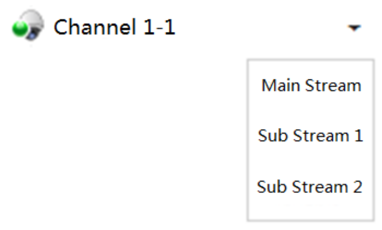


Table 3-6 Description of icons in the monitoring channel list

Icon/Parameter	Description
Please input 🔍	Enter the channel name in the text box and click 🔍 or press Enter key. The system displays the items meeting the condition. 📖 NOTE Support fuzzy queries. That is, enter any character of the channel name and the channel can be searched.
Channel state icon 🟢 ⚪ 🟠	Display the state of the remote device corresponding to the current channel. ● 🟢 Remote device is online. ● ⚪ Remote device is offline. ● 🟠 Remote device is playing real-time monitoring images.

Icon/Parameter	Description
 Channel 1-1 Main Stream Sub Stream 1 Sub Stream 2	Click the drop-down box after the channel name to select the main stream or sub stream for play. NOTE When select the sub stream for real-time monitoring, the sub stream shall be open and supported by the fron-end camera.
Refresh	Click this icon to refresh the list.

3.6.1.3 PTZ Console

Through the PTZ console, you can set the PTZ direction, step, zoom, iris, preset point, tour, pattern, scan boundary, light, wiper and horizontal rotation. See Figure 3-25.

- PTZ rotation supports 8 directions: Up, down, left, right, upper left, upper right, lower left and lower right.
- Click 🔍 and click any position of the monitor screen, and the screen will be adjusted automatically centering on the mouse click.
- The larger the step size, the faster it rotates. For example, the speed of step 8 is much faster than that of step 1.
- Click **More Set** to configure the scan, preset point, tour and other auxiliary functions. For details, see Table 3-7.

Figure 3-25 PTZ Console

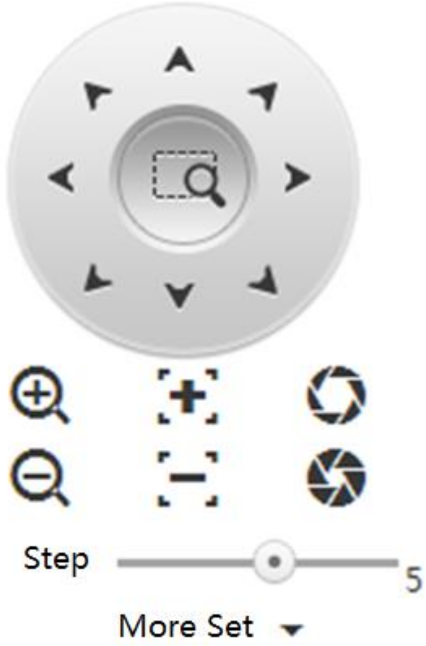


Table 3-7 Description of PTZ parameters

Parameter	Description

Parameter	Description
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.
Preset	Set the preset points of the camera including viewing, adding and delete. ● Add Turn the camera to the needed position, enter preset value in the **Preset** text box, and then click **Add** to add the preset point. ● View Enter the preset value in the **Preset** text box and click **View**. The camera automatically turns to the preset position. ● Delete Enter the preset value in the **Preset** text box and click **Delete** to delete this preset point.
Tour	The camera turns between the multiple preset points. ● Setting In the **Tour** interface, enter the value of tour path and click **Add**. Enter the value of preset, click **Add** or **Delete**, and then you can add or delete preset points in the path. NOTE You can repeatedly click **Add** or **Delete** to add or delete preset points in this point path. ● Delete In the **Tour** interface, enter the value of tour path and click **Delete** to delete this tour path. ● Start In the **Tour** interface, enter the value of tour path, click **Start**, and then the camera starts rotation according to the path.
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 the other settings on the main interface, such as zoom, focus, iris and direction. Return to the pattern interface and click **Stop** to complete the setting. 3. Click **Start**. The camera starts rotation according to the set pattern.
Horizontal Rotation	Select **Horizontal Rotation** in the drop-down list and click **Start**. The camera rotates 360° corresponding to the original position. Click **Stop** to end the rotation.
Aux	Enter value into the **Aux** box. Click **Aux on** to open the corresponding auxiliary function and click **Aux off** to close the function.
Light/wiper	Control the light/wiper switch of the external device through RS485. This function shall be supported by the external device.

Parameter	Description
Flip	Select **Flip** in the drop-down list and click **Flip**. The camera can vertically turn 180° corresponding to the original position.
Reset	Select **Reset** in the drop-down list and click **Reset** to turn the camera back to the default position.

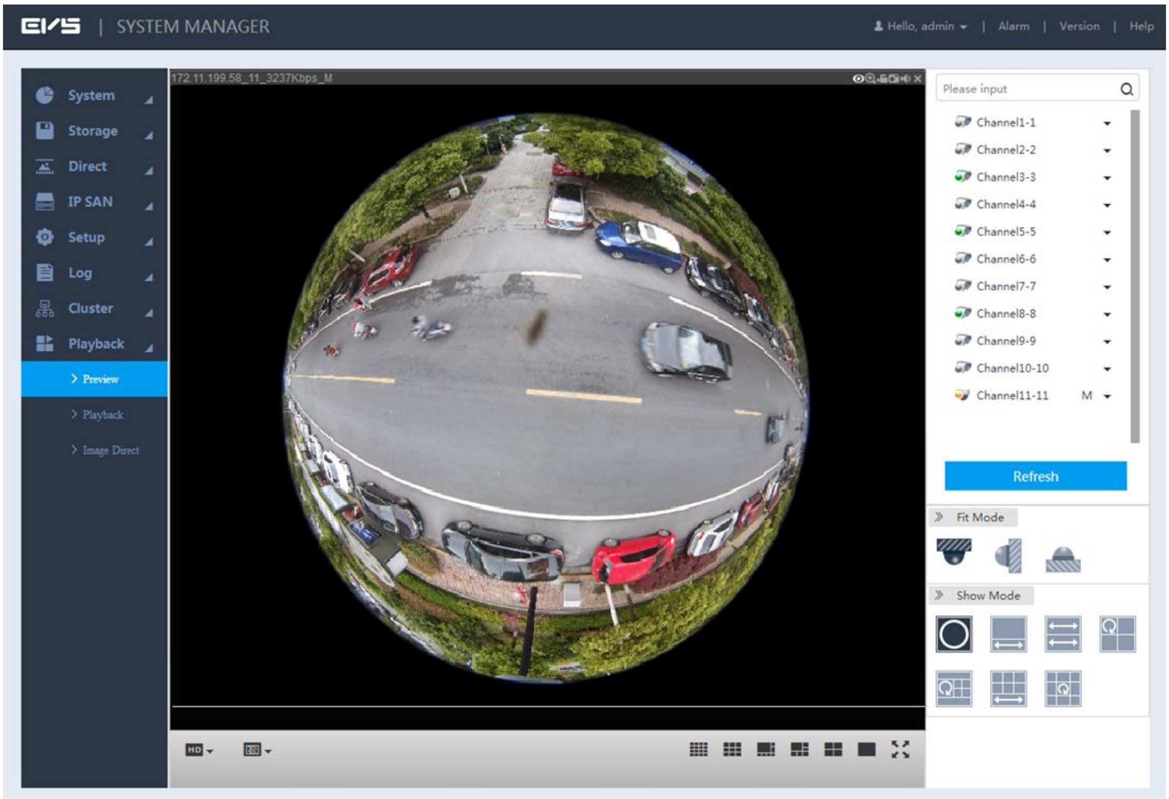
3.6.1.4 Fish-Eye

After opening the real-time monitoring screen, click ◉ on the upper right corner of the window and the fisheye interface is displayed. See Figure 3-26. You can adjust the **Fit Mode** and **Show Mode.**

NOTE

Fisheye setting only supports fisheye channel. If the current channel is not a fisheye channel, the system prompts that the channel does not support correction.

Figure 3-26 Fisheye settings



Mounting mode includes top, wall and ground. Different mounting modes support different display mode. For details, see Table 3-8.

Table 3-8 Description of fisheye mounting modes

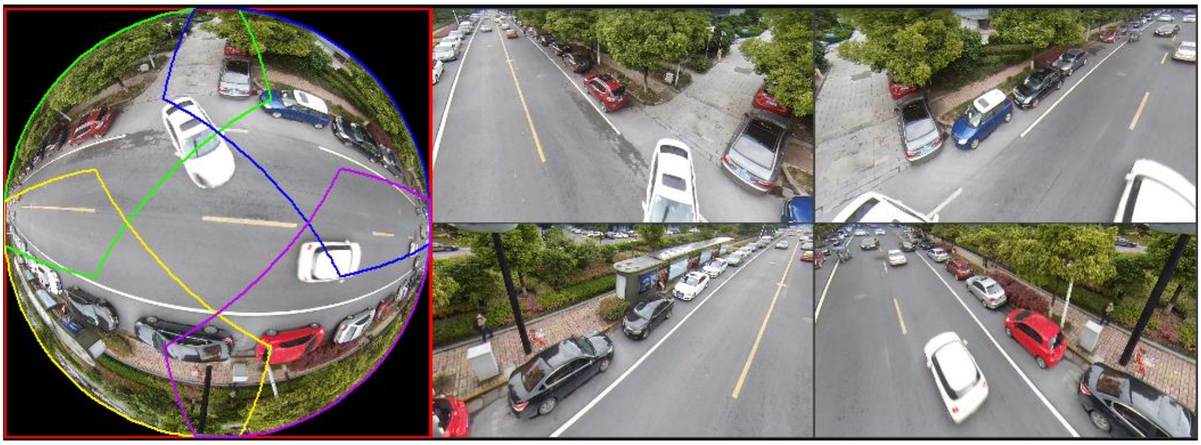
Mounting Mode	Display Mode
Top/Ground Mounting	360° panoramic original image.
	One correction window+ one panoramic drawing.
	Two panoramic drawings.
	One 360° panoramic image + three correction windows.
	One 360° panoramic image + four correction windows.
	Four correction windows + one panoramic drawing.

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

Top-mounting one 360° panoramic image + four correction windows: you can do correction for the colorful area in the left panoramic image, or move the position of the small images on the right. See Figure 3-27.

Method: Zoon in, zoom out, move and rotate the images with the mouse.

Figure 3-27 Fisheye correction



3.6.2 Playback

The system supports replay, download and manage record files.

3.6.2.1 Record Playback

Select **Playback** > **Playback** > **Playback**. The **Playback** interface is displayed. See Figure 3-28. For details, see Table 3-9.

Figure 3-28 Playback

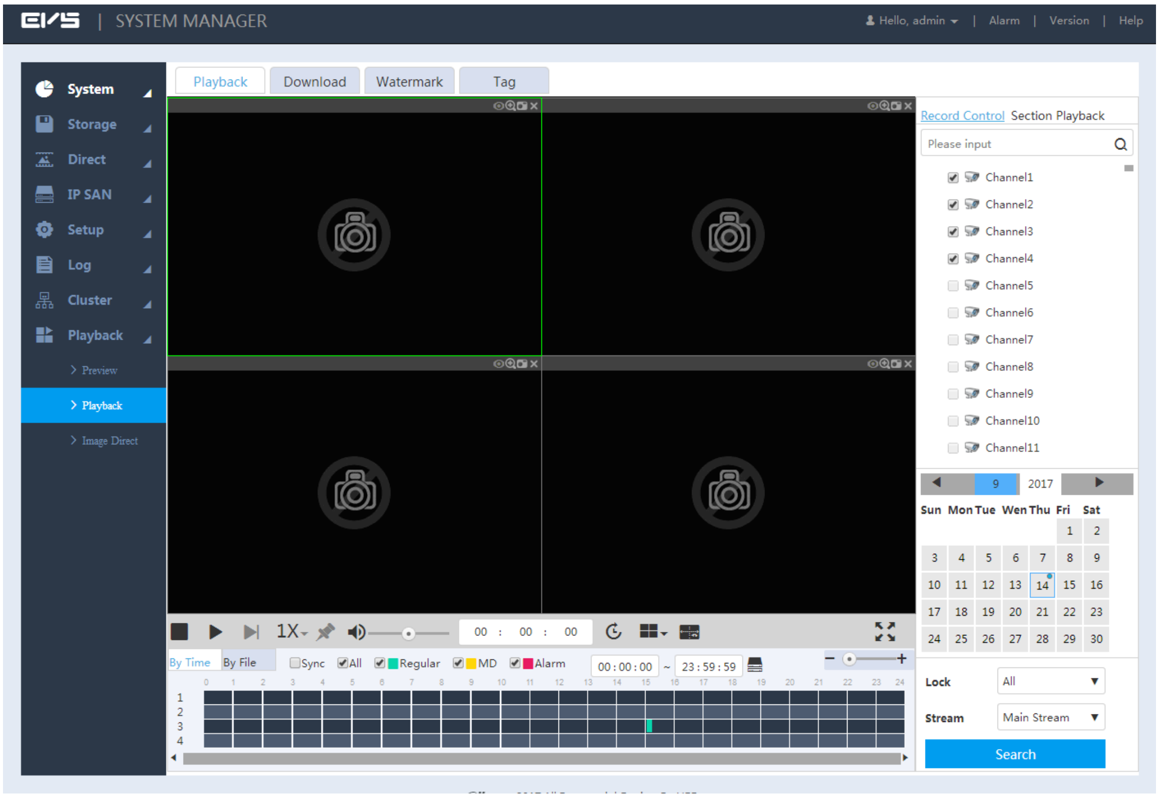


Table 3-9 Description of playback parameters

No.	Description
1	Playback type includes record playback and section playback. ● Record: Replay according to the stored record files. ● Section playback: Synchronous play of multiple sections from the record file to improve the speed. For details, see "3.6.2.1.1 Section Playback."
2	Channel list of the remote device. NOTE Enter the channel name into the text box, click 🔍 or press **Enter**, and then the system displays the channels meeting the 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 record file is available on that day.
4	Set the record query conditions. ● Lock: Includes all, lock and tag. ● Stream: Includes main stream and sub stream.
5	The record display list supports listing by time or by file and it supports record clip backup. For details, see "3.6.2.1.2 Record Display List."
6	Record playback control bar. For details, see "3.6.2.1.3 Record Playback Control Bar."

3.6.2.1.1 Section Playback

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

NOTE

The minimum section shall be no less than five minutes. Play five minutes if the section is less than five minutes. For example: an eight minute record is divided into two sections: five minutes and three minutes. The window ends first keeps black until all the windows finish the play, and then go on to play the next file.

Step 1 Click **Section Playback** on the upper-right corner of the **Playback** interface.

Step 2 Click ■▾ and select the split window number. For description of window split, see Table 3-10.

NOTE

■▾No window split. When you select different split numbers, the icons are different. See that displayed actually.

Table 3-10 Description of window split icons

Icon	Description
■	No split.
⊞	Four split windows.
▦	Eight split windows.
▦	16 split windows.

Step 3 Select the channel needed for playback. Click ▶.

Section playback starts.

NOTE

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

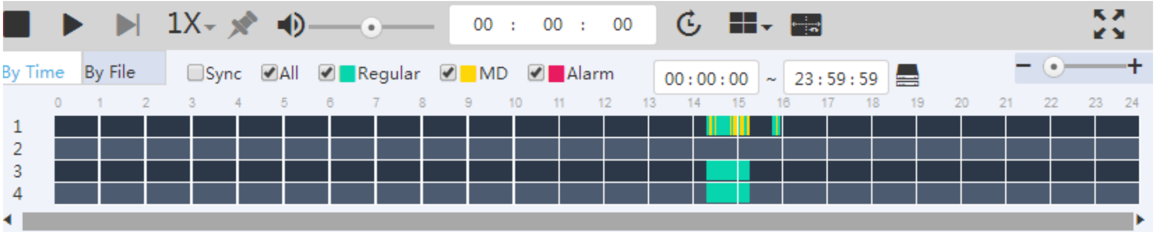
3.6.2.1.2 Record Display List

Select the date with record and the system can display record file by time and by file. See Figure 3-29 and Figure 3-30. For details, see Table 3-11.

NOTE

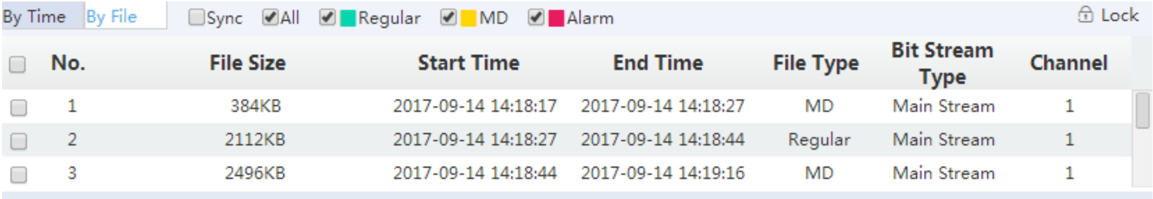
Records of different types are displayed in different colors on the timeline. 🟩 Regular, 🟨 Motion detection (MD), 🟥 Alarm.

Figure 3-29 Display by time



By Time By File ☐Sync ☑All ☑🟩Regular ☑🟨MD ☑🟥Alarm 00 : 00 : 00 ~ 23 : 59 : 59

Figure 3-30 Display by file



By Time | By File □Sync ☑All ☑🟩Regular ☑🟨MD ☑🟥Alarm 🔒 Lock

□	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 3-11 Description of parameters in the record display list

Icon	Description
By Time | By File	Set the record display type: ● By time: Display record by timeline. See Figure 3-29. ● By file: Display record in file list. See Figure 3-30.
☑All ☑🟩Regular ☑🟨MD ☑🟥Alarm	Select the check box and only the corresponding record files are displayed.
00 : 00 : 00 ~ 23 : 59 : 59 💾	Clip a record and save it in PC. 1. Select a record file. 2. Select the start time on the timeline. Click 🟩 to start clip. 3. Select the end time on the timeline. Click 🟩 to end the clip. 4. Click 💾, select storage path, and then store the clipped record.
− ● +	Adjust the time unit of the timeline.
🔒 Lock	Lock a file to avoid overwritten. For details, see "3.6.2.1.4 Locking and Unlocking Files." 📖 NOTE Lock is supported only when displayed by file.

3.6.2.1.3 Record Playback Control Bar

For the record playback control bar, see Figure 3-31. For details, see Figure 3-12.

Figure 3-31 Record playback control bar

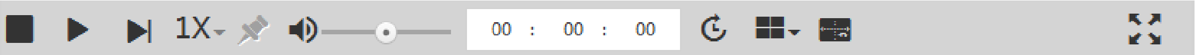


Table 3-12 Description of icons on the record playback control bar

Icon	Description
■	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.

Icon	Description
▶|	Display the next frame. ● When the record is paused, click ▶| to replay single frames. ● During the single-frame play, click ▶ or ❚❚ to enter the normal playback state.
1X▾	Set the play speed, including 1×, 2×, 4×, 8× and 16×.
📌	Add a tag. During the playback, click this icon, enter the tag name, and then click **OK** to mark the record file. You can search the record through the marked time and key and replay it. For details, see "3.6.2.4 Tag Management."
🔊 ──●──	Adjust the record playback volume.
00 : 00 : 00 ↻	Positioning. Set a time point and click ↻ to position the record.
⊞▾	Window split. Click this icon to set the window split number, including 16, nine, four and single. 📖 NOTE Different models support different split numbers. See the interface displayed actually.
▬	Smart rule. Click this icon and the smart rules of remote device painting are displayed.
⛶	Full-screen display.

3.6.2.1.4 Locking and Unlocking Files

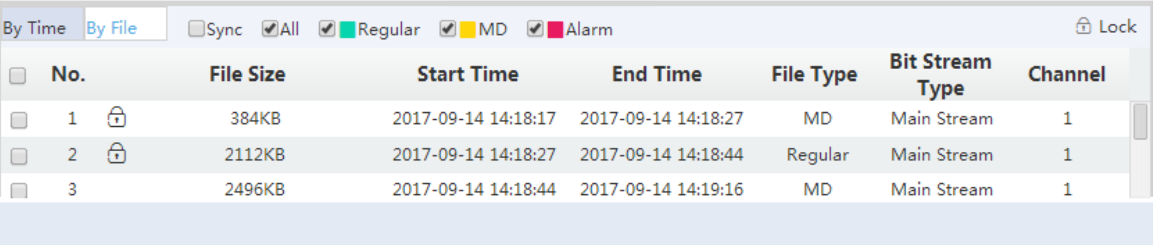
The system supports locking and unlocking record files. The locked file cannot be overwritten.

Locking Files

Step 1 Select the channel, date, lock and stream on the **Playback** interface.

Step 2 Click **Search** and Click **By File**. The record file list is displayed. See Figure 3-32.

Figure 3-32 Record file list



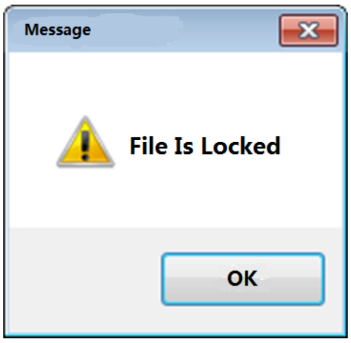
By Time | By File ☐Sync ☑All ☑🟩Regular ☑🟨MD ☑🟥Alarm 🔒 Lock

☐	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

Step 3 Select the file needed to be locked and click **Lock**.

The system prompts a success message. See Figure 3-33.

Figure 3-33 Prompt



Message

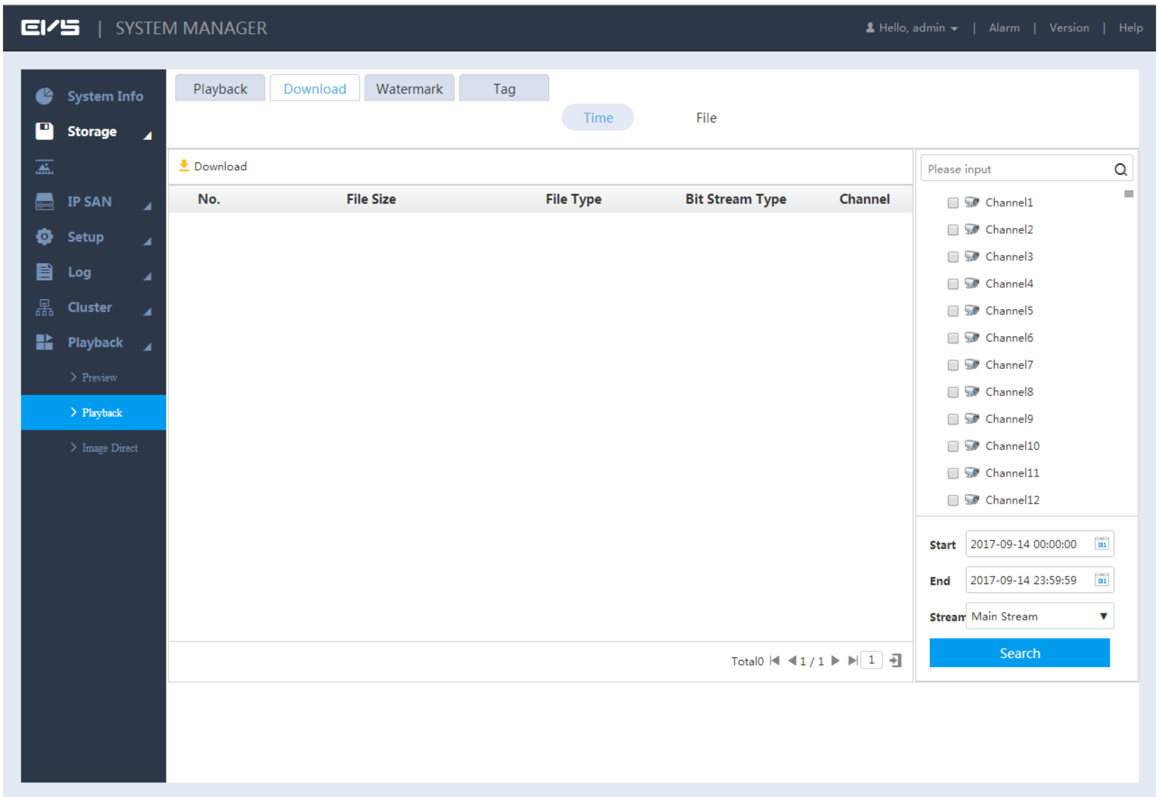
File Is Locked

Unlocking Files

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

The **File** interface is displayed. See Figure 3-34.

Figure 3-34 File



Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Stream Main Stream

Step 2 Select the channel. Select the **Start**, **End** and **Stream**.

Step 3 Lock the record.

Step 4 Click **Search**.

The locked record list is displayed.

Step 5 Select the file and click 🔓 to unlock it.

3.6.2.2 Download

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

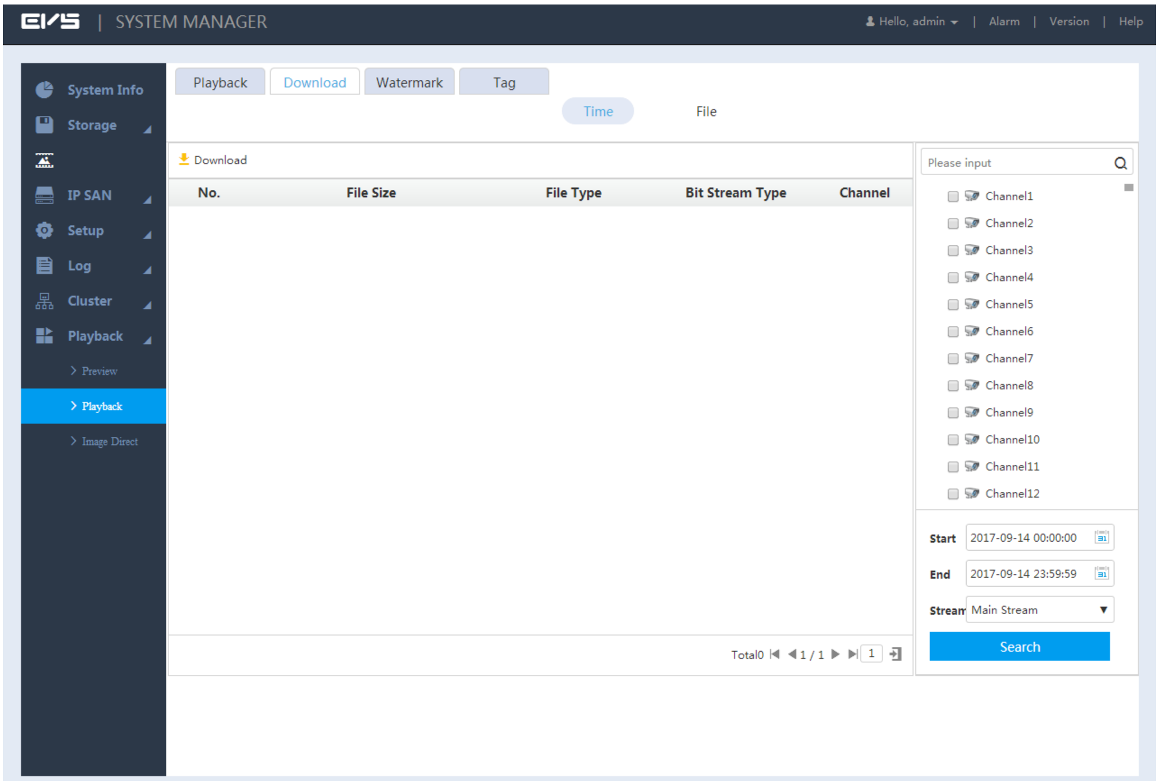
3.6.2.2.1 Download by Time

According to the set record period and other filter conditions like channel and stream type, you can locally download the video files.

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

The **Time** interface is displayed. See Figure 3-35.

Figure 3-35 Time



Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Stream Main Stream

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

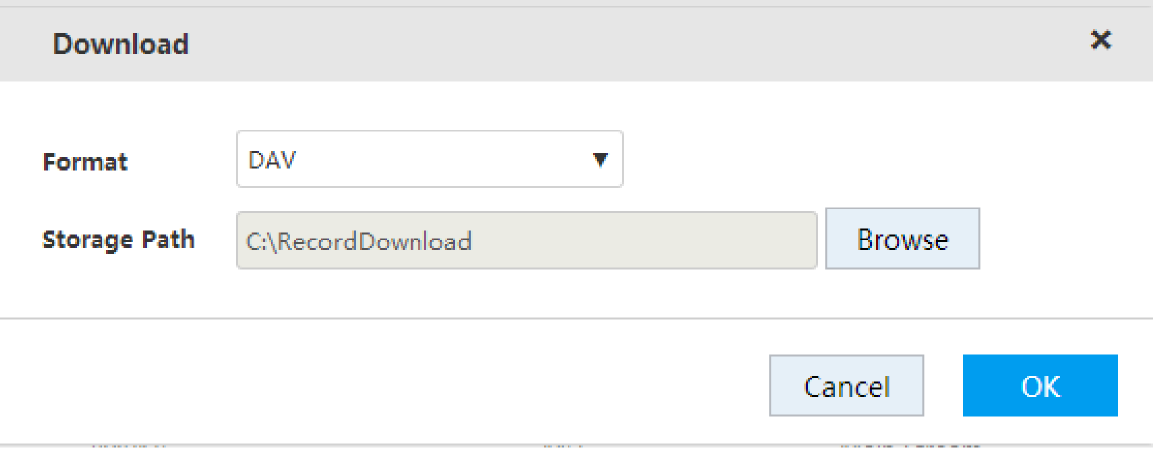
Step 3 Click **Search**.

The record files meeting the conditions are displayed.

Step 4 Select the file and click ⭳ .

The **Download** interface is displayed. See Figure 3-36.

Figure 3-36 Download



Format DAV

Storage Path C:\RecordDownload

Step 5 Select Format and Storage Path.

NOTE

The default storage path is C:\RecordDownload. For details to modify the path, see "3.8.2.1 Local Settings."

Step 6 Click **OK**.

The system starts to download the record file.

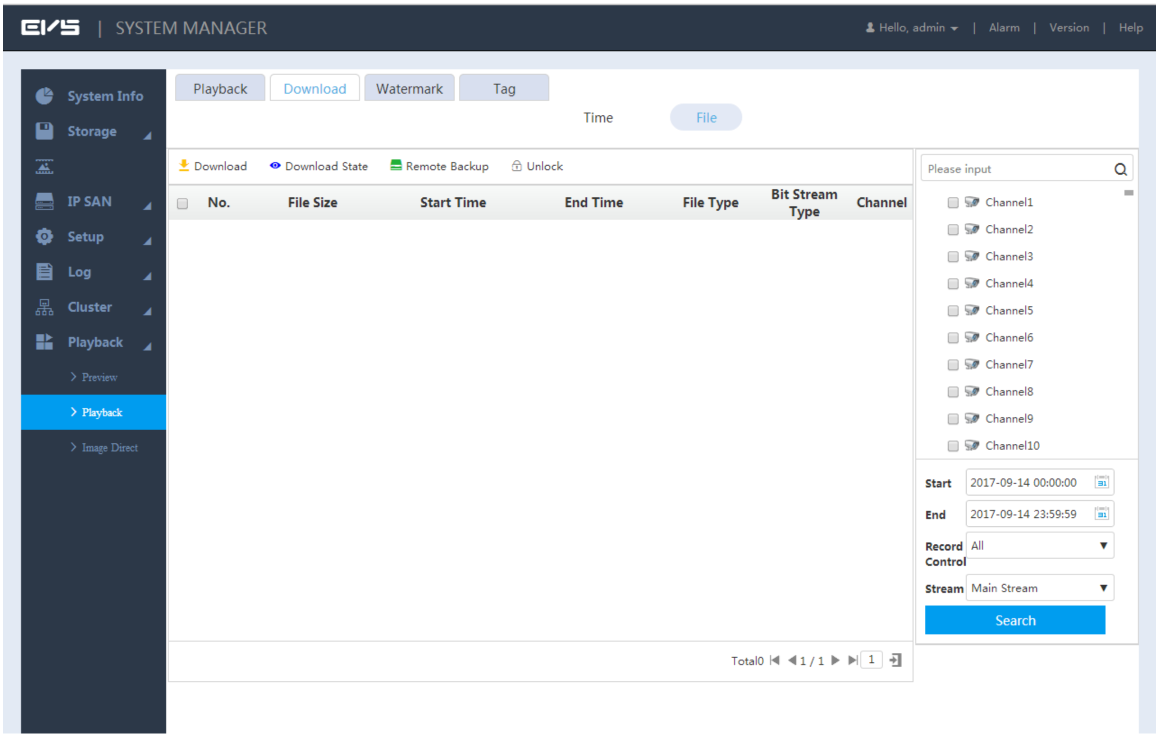
3.6.2.2.2 Download by File

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

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

The **File** interface is displayed. See Figure 3-37.

Figure 3-37 File



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

Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Record Control All

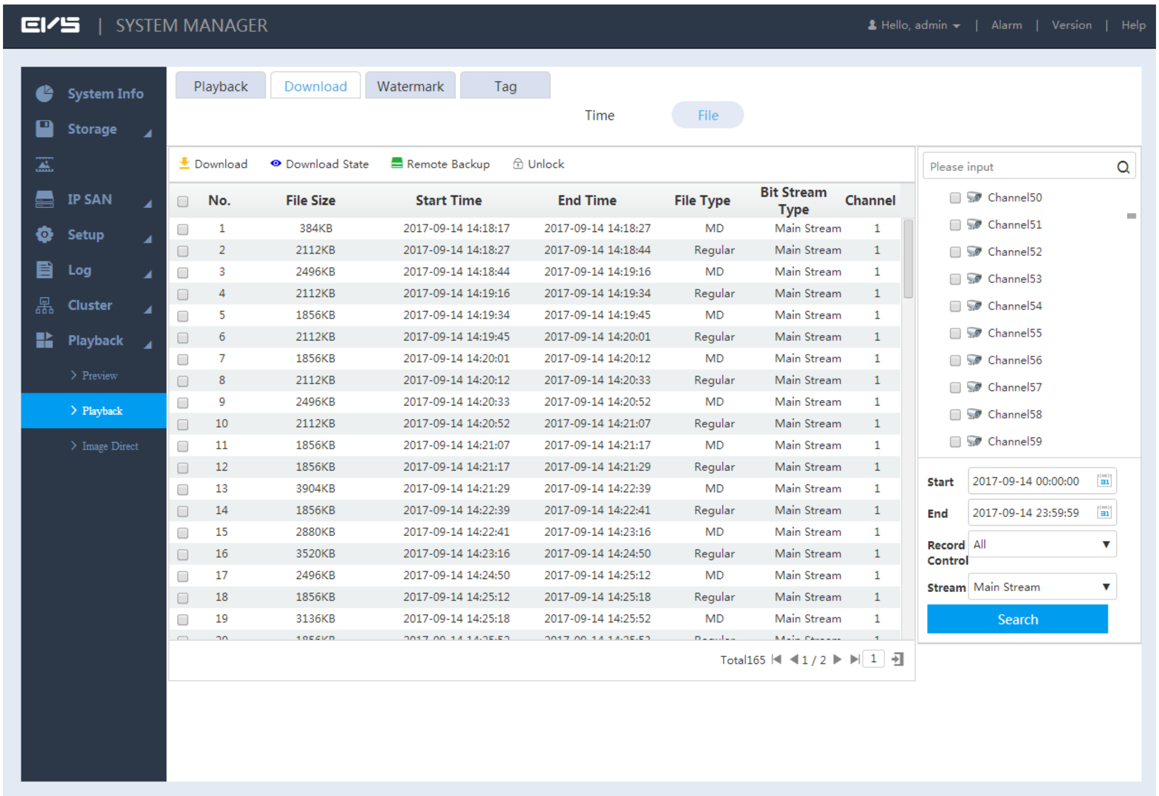
Stream Main Stream

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

Step 3 Click Search.

The record files meeting the conditions are displayed.

Figure 3-38 Search results



□	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
□	4	2112KB	2017-09-14 14:19:16	2017-09-14 14:19:34	Regular	Main Stream	1
□	5	1856KB	2017-09-14 14:19:34	2017-09-14 14:19:45	MD	Main Stream	1
□	6	2112KB	2017-09-14 14:19:45	2017-09-14 14:20:01	Regular	Main Stream	1
□	7	1856KB	2017-09-14 14:20:01	2017-09-14 14:20:12	MD	Main Stream	1
□	8	2112KB	2017-09-14 14:20:12	2017-09-14 14:20:33	Regular	Main Stream	1
□	9	2496KB	2017-09-14 14:20:33	2017-09-14 14:20:52	MD	Main Stream	1
□	10	2112KB	2017-09-14 14:20:52	2017-09-14 14:21:07	Regular	Main Stream	1
□	11	1856KB	2017-09-14 14:21:07	2017-09-14 14:21:17	MD	Main Stream	1
□	12	1856KB	2017-09-14 14:21:17	2017-09-14 14:21:29	Regular	Main Stream	1
□	13	3904KB	2017-09-14 14:21:29	2017-09-14 14:22:39	MD	Main Stream	1
□	14	1856KB	2017-09-14 14:22:39	2017-09-14 14:22:41	Regular	Main Stream	1
□	15	2880KB	2017-09-14 14:22:41	2017-09-14 14:23:16	MD	Main Stream	1
□	16	3520KB	2017-09-14 14:23:16	2017-09-14 14:24:50	Regular	Main Stream	1
□	17	2496KB	2017-09-14 14:24:50	2017-09-14 14:25:12	MD	Main Stream	1
□	18	1856KB	2017-09-14 14:25:12	2017-09-14 14:25:18	Regular	Main Stream	1
□	19	3136KB	2017-09-14 14:25:18	2017-09-14 14:25:52	MD	Main Stream	1
□	20	1856KB	2017-09-14 14:25:52	[illegible]	Regular	Main Stream	1

Total165 1 / 2 1

Start 2017-09-14 00:00:00

End 2017-09-14 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. The system starts record download.

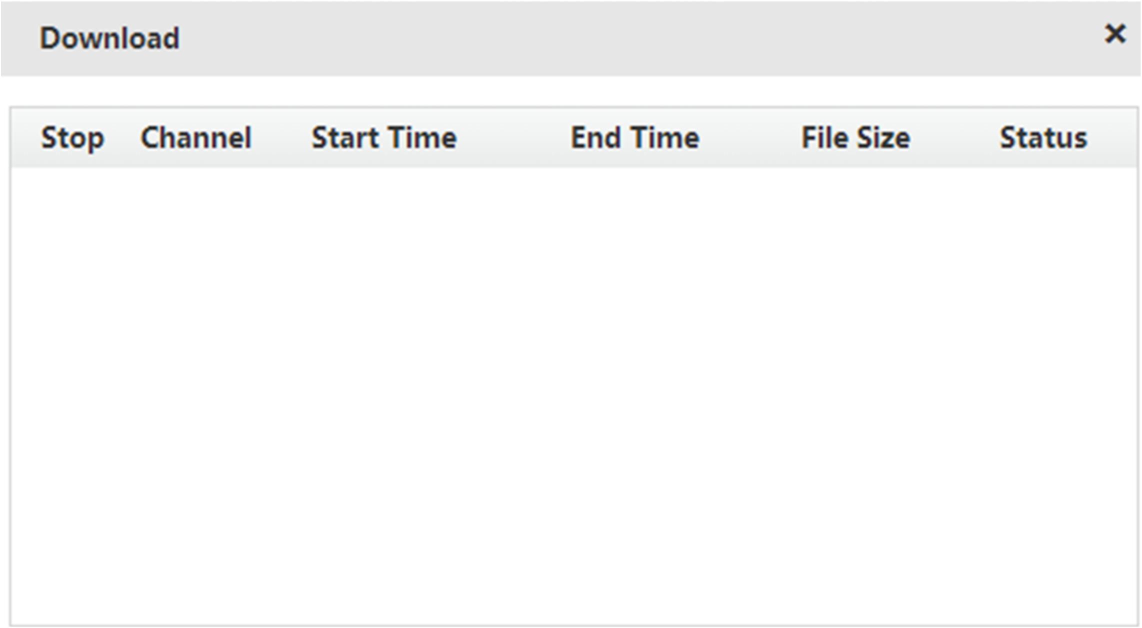
- Remote backup

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

Step 5 (Optional) Click .

The **Download** interface is displayed. See Figure 3-39. You can view the download progress. Click 🟩 to stop the record download.

Figure 3-39 Download



Download

Stop	Channel	Start Time	End Time	File Size	Status

3.6.2.3 Watermark Verification

You can check if the downloaded record file is tampered with through the function of watermark verification.

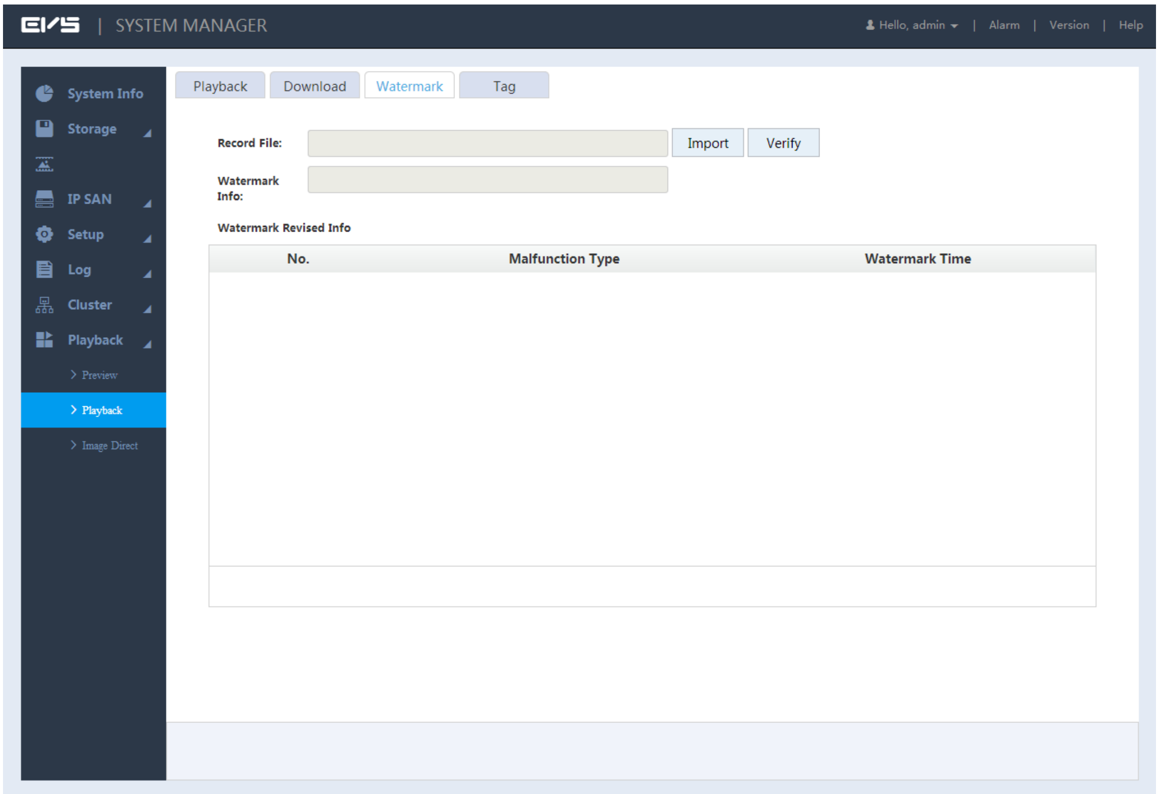
Preparation

The watermark verification function is open on the EVS device. For details, see "3.10.2.3.1 Stream Parameter Settings."

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

The **Watermark** interface is displayed. See Figure 3-40.

Figure 3-40 Watermark verification



Record File:

Watermark Info:

Watermark Revised Info

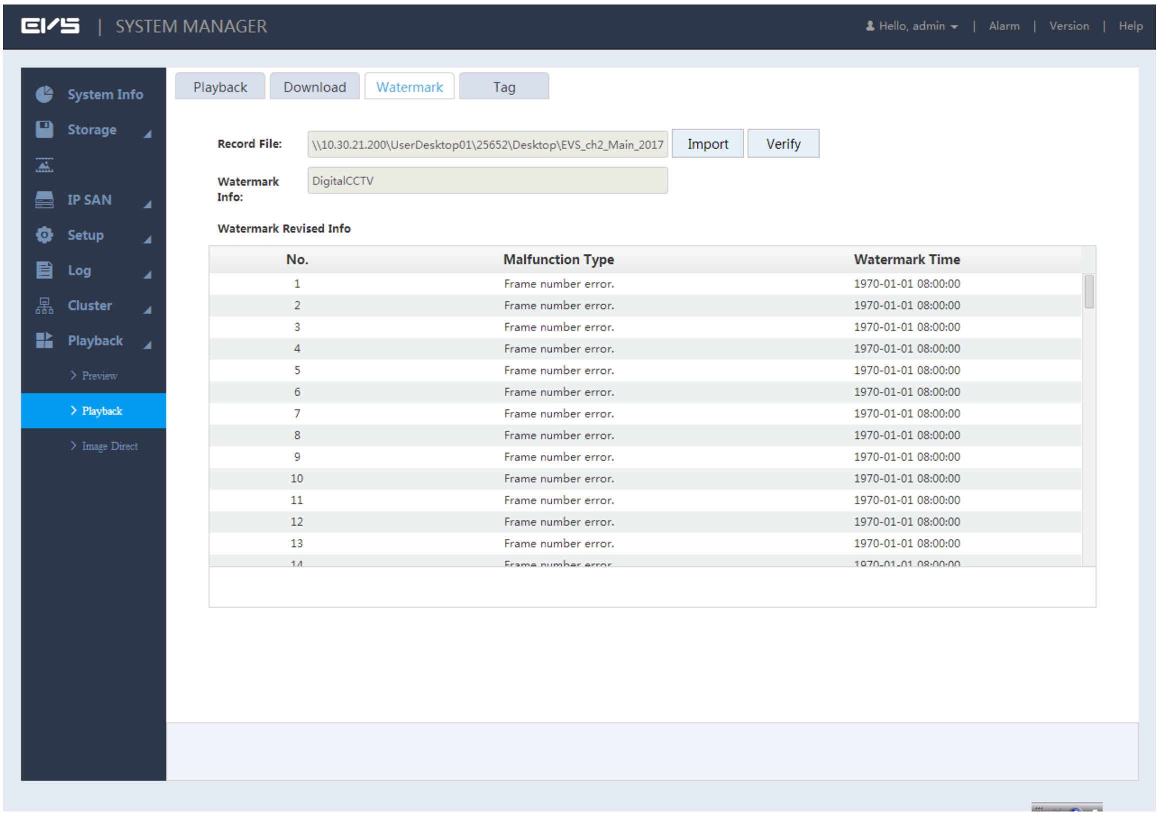
No.	Malfunction Type	Watermark Time

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. See Figure 3-41.

Figure 3-41 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

3.6.2.4 Tag Management

In record playback, you can add tags to the records with importation information. After adding the tag, you can search by the marked time and key words and replay the related records, so as to enable the users to obtain needed video information quickly.

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

The **Tag** interface is displayed.

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

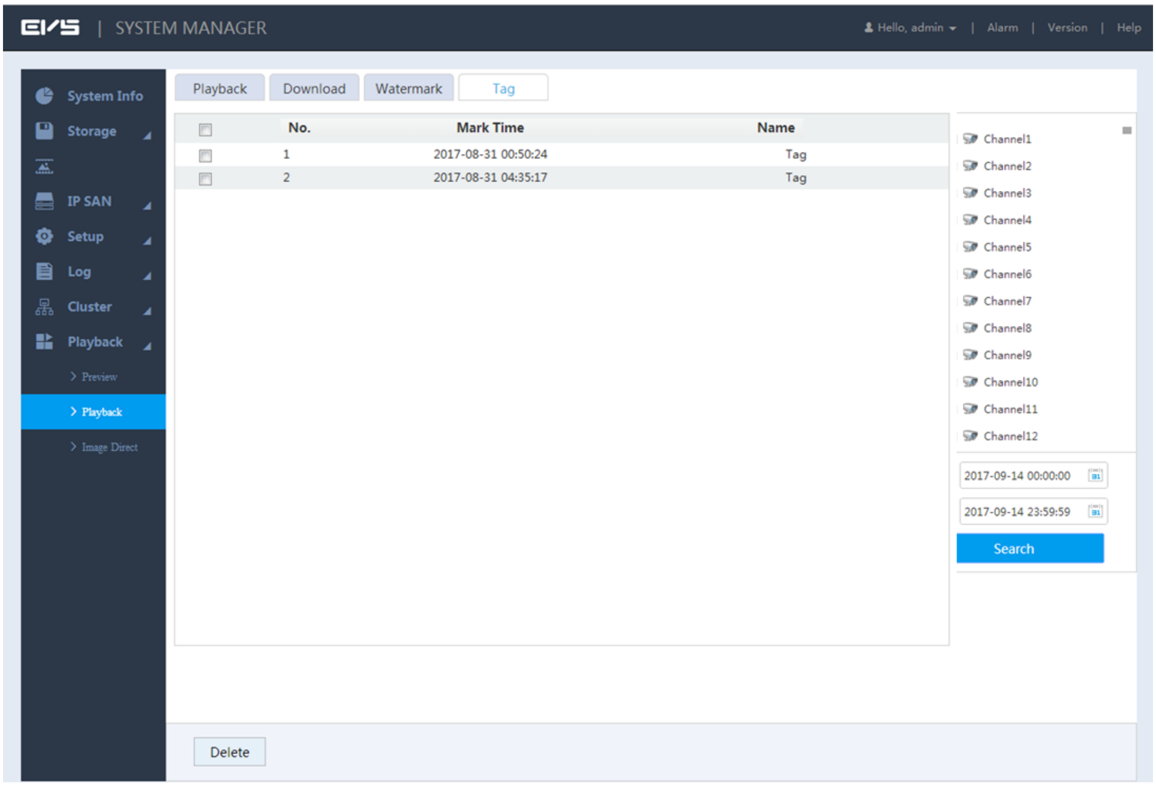
Step 3 Click Search.

The files with the searched tag are displayed. See Figure 3-42.

NOTE

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

Figure 3-42 Tag management



□	No.	Mark Time	Name
□	1	2017-08-31 00:50:24	Tag
□	2	2017-08-31 04:35:17	Tag

2017-09-14 00:00:00

2017-09-14 23:59:59

3.6.3 Image Direct Storage

The system supports to search and download the images stored in IVS and intelligent transportation events.

Preparation

Have done the image direct storage configuration.

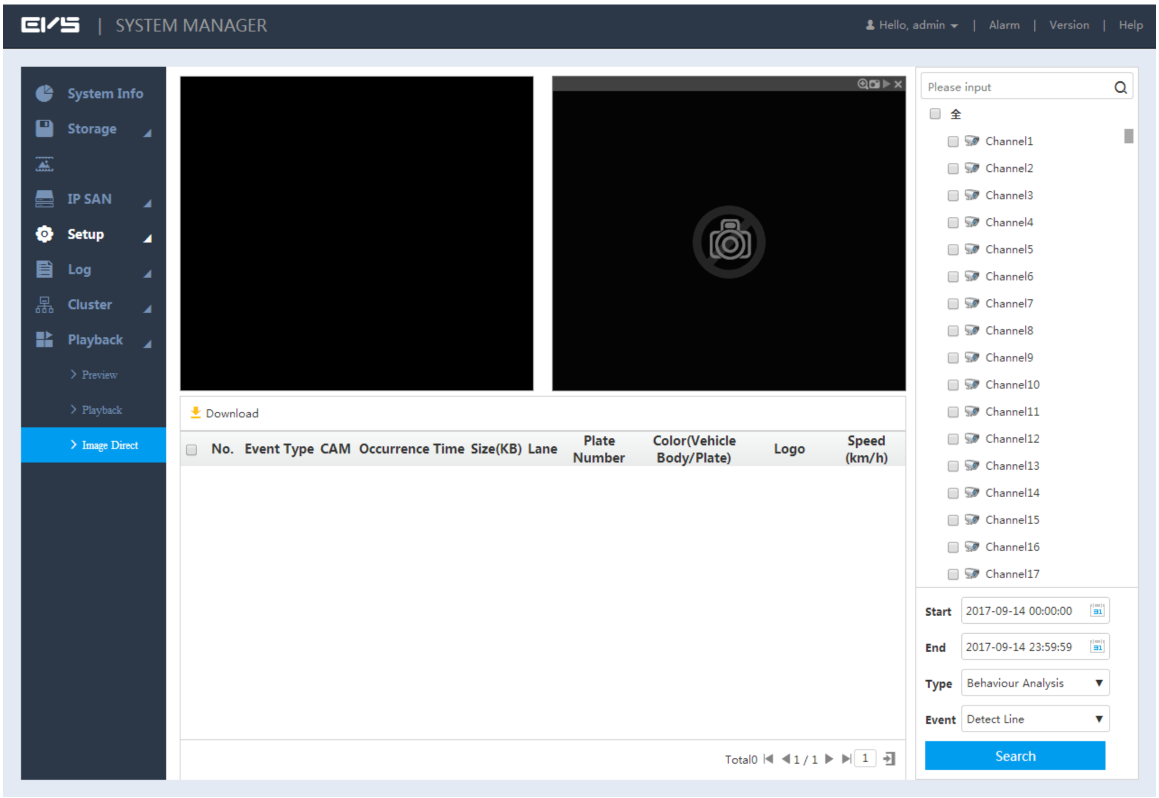
- Have reserved one or several HDDs for image direct storage. For details, see "3.10.1 Storage Device."
- Have added ITC or Smart IPC devices. For details, see "3.5 Adding Remote Device."
- Have enabled image direct storage. For details, see "3.10.5 Record Control."

3.6.3.1 Searching Image/Record

Step 1 Select **Playback** > **Image Direct**.

The **Image Direct** interface is displayed. See Figure 3-43.

Figure 3-43 Image direct storage (IVS)



□	No.	Event Type	CAM	Occurrence Time	Size(KB)	Lane	Plate Number	Color(Vehicle Body/Plate)	Logo	Speed (km/h)

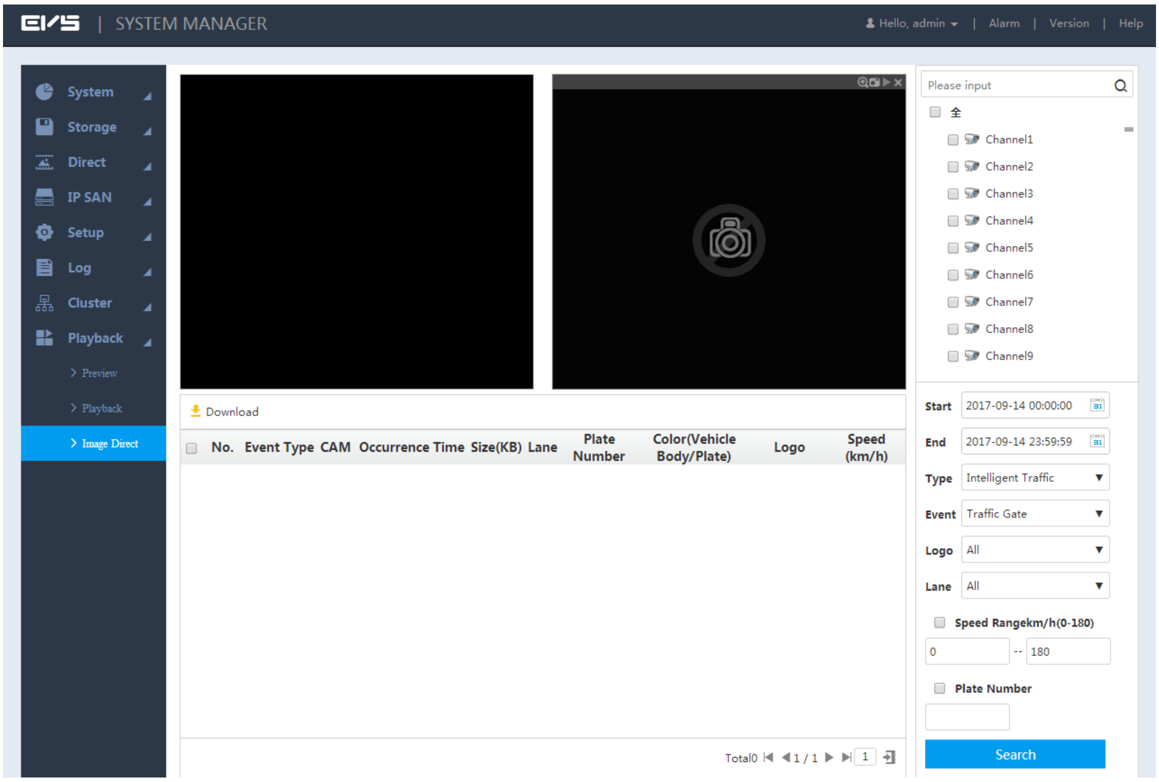
Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Type Behaviour Analysis

Event Detect Line

Figure 3-44 Image direct storage (intelligent transportation)



□	No.	Event Type	CAM	Occurrence Time	Size(KB)	Lane	Plate Number	Color(Vehicle Body/Plate)	Logo	Speed (km/h)

Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Type Intelligent Traffic

Event Traffic Gate

Logo All

Lane All

□ Speed Rangekm/h(0-180)

0 -- 180

□ Plate Number

Step 2 Select/Enter the parameters. For details, see Table 3-13.

Table 3-13 Description of image direct storage parameters

Parameter	Description
Channel	Select the channel you need to search for directly stored images. NOTE Select **All** to search for directly stored images in all the channels.
Start	Select the start time and end time of the images you need to search.
End	
Type	Select search type, including IVS and intelligent transportation. NOTE IVS corresponds to images in Smart IPC and intelligent transportation corresponds to images in ITC.
Event	Select the event type of the directly stored images needed to search.
Logo	Select/enter the logo, lane, speed range and plate number of the car you need to search. NOTE This needs to be set when the type is intelligent transportation.
Lane	
Speed Range	
Plate Number	

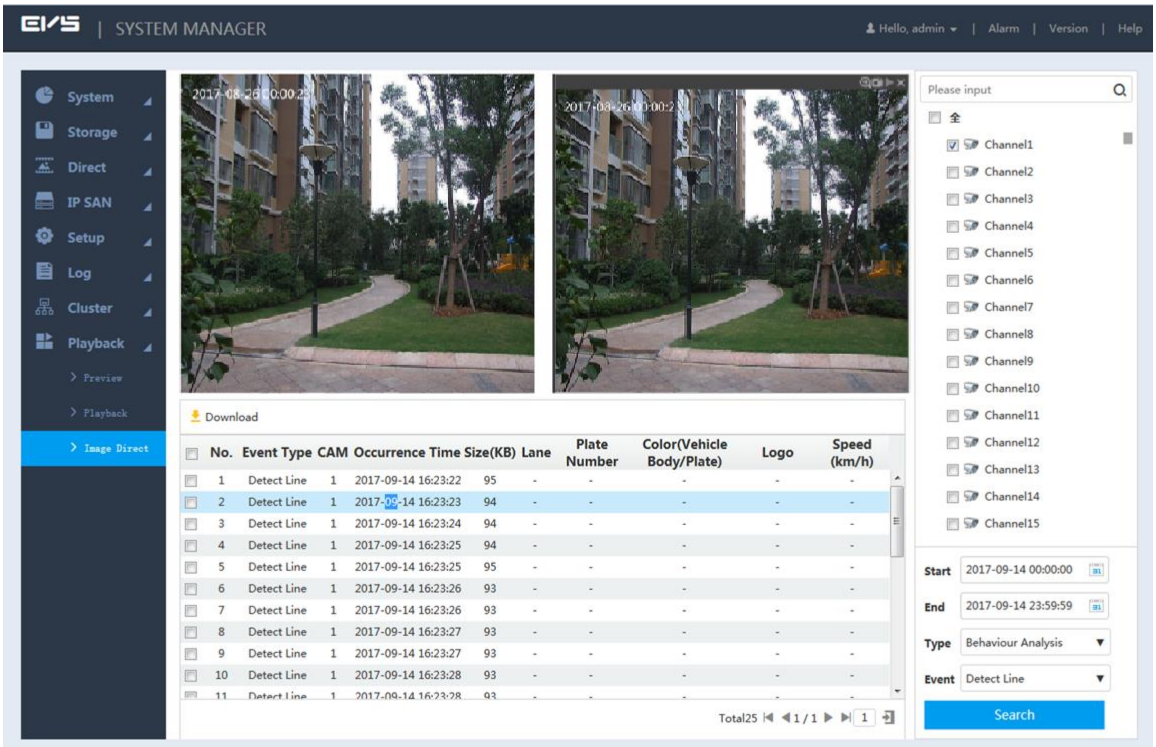
Step 3 Click **Search**.

The results are displayed. Double-click the record in the list and the system displays the corresponding image. Meanwhile, the main stream record about 10 seconds before and after the image is played in the window on the right side. See Figure 3-45.

NOTE

The records can be viewed only when the system time of EVS device is the same as the time of Smart IPC or ITC device.

Figure 3-45 Search results of image direct storage



Start 2017-09-14 00:00:00

End 2017-09-14 23:59:59

Type Behaviour Analysis

Event Detect Line

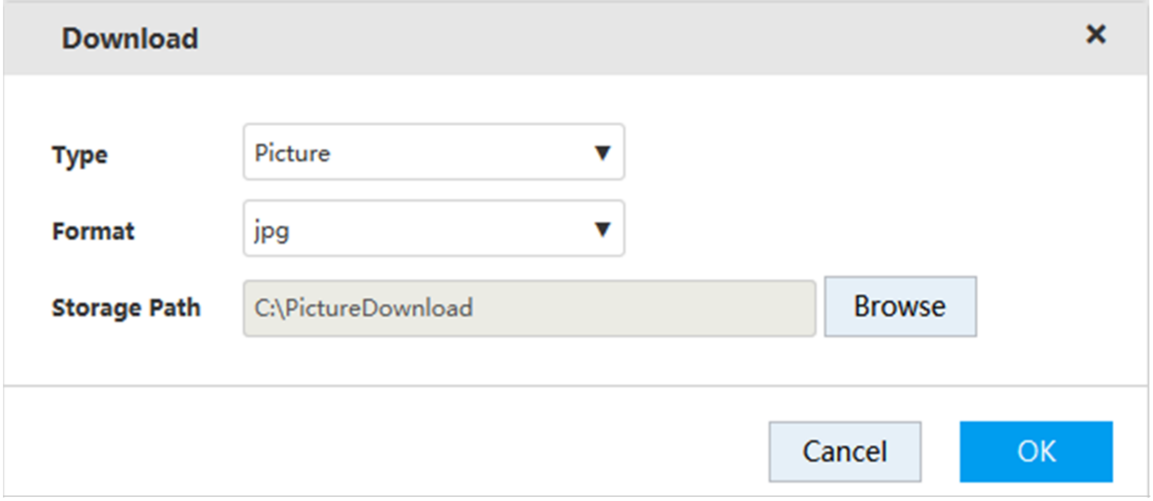
□	No.	Event Type	CAM	Occurrence Time	Size(KB)	Lane	Plate Number	Color(Vehicle Body/Plate)	Logo	Speed (km/h)
□	1	Detect Line	1	2017-09-14 16:23:22	95	-	-	-	-	-
□	2	Detect Line	1	2017-09-14 16:23:23	94	-	-	-	-	-
□	3	Detect Line	1	2017-09-14 16:23:24	94	-	-	-	-	-
□	4	Detect Line	1	2017-09-14 16:23:25	94	-	-	-	-	-
□	5	Detect Line	1	2017-09-14 16:23:25	95	-	-	-	-	-
□	6	Detect Line	1	2017-09-14 16:23:26	93	-	-	-	-	-
□	7	Detect Line	1	2017-09-14 16:23:26	93	-	-	-	-	-
□	8	Detect Line	1	2017-09-14 16:23:27	93	-	-	-	-	-
□	9	Detect Line	1	2017-09-14 16:23:27	93	-	-	-	-	-
□	10	Detect Line	1	2017-09-14 16:23:28	93	-	-	-	-	-
□	11	Detect Line	1	2017-09-14 16:23:28	93	-	-	-	-	-

Total25 1 / 1 1

3.6.3.2 Image/Record Download

Select one or several image records in the search result list (see Figure 3-45), click ⬇, and then the **Download** interface is displayed. See Figure 3-46. You can download the corresponding image or record to the local PC.

Figure 3-46 Download



Type: Picture
Format: jpg
Storage Path: C:\PictureDownload

3.7 Alarm

View the triggering time, channel number, alarm type and processing state of the alarm logs.

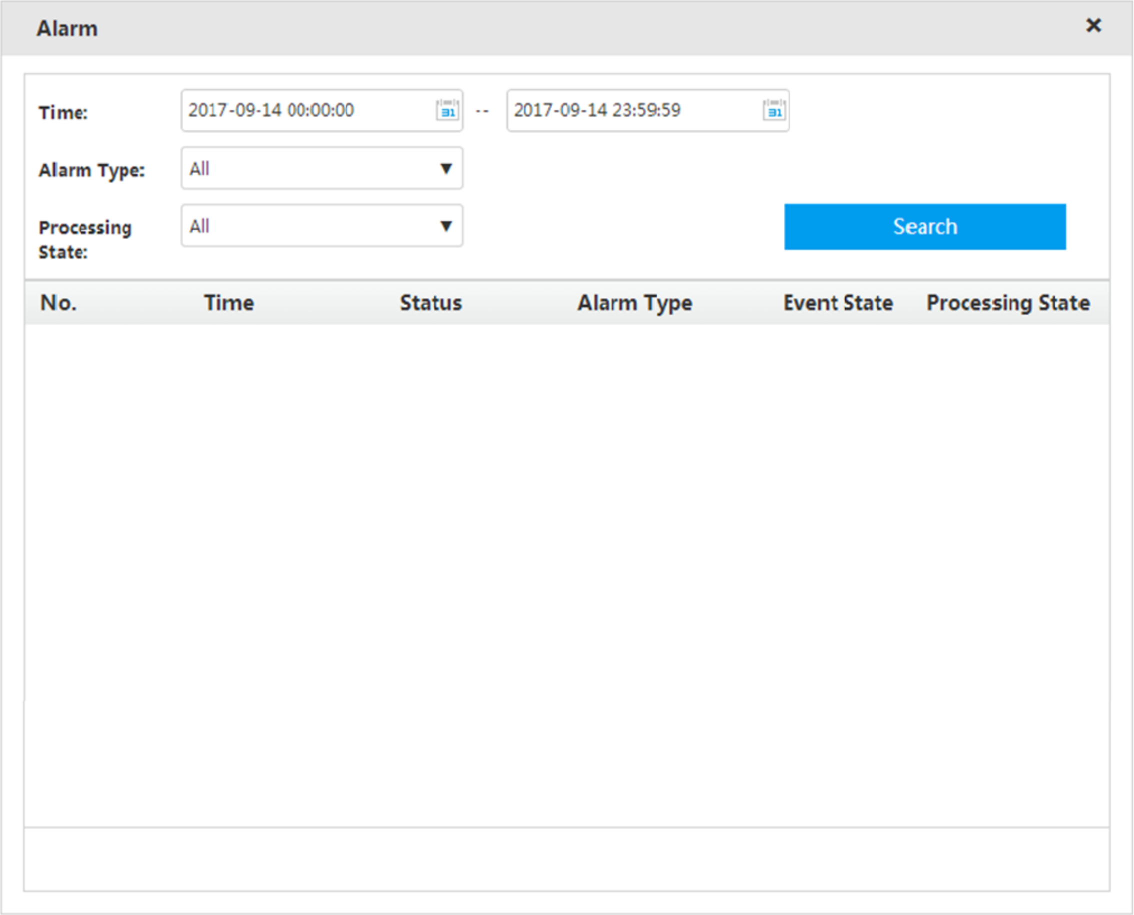
⚠ CAUTION

The alarm information on the **Alarm** interface is valid for the current login state. They will be cleared when log in again.

Step 1 Click **Alarm** on the upper right corner.

The **Alarm** interface is displayed. See Figure 3-47.

Figure 3-47 Alarm



Time: 2017-09-14 00:00:00 -- 2017-09-14 23:59:59

Alarm Type: All

Processing State: All

Step 2 Select the search conditions. For details, see Table 3-14.

Table 3-14 Description of alarm search parameters

Parameter	Description
Time	Select the time range of alarm search.
Alarm Type	Select the alarm type to search. NOTE ● Only when you have enabled the alarm function and this alarm type is triggered, you can search for the corresponding alarm log. For details to enable alarm, see "3.8.4 Configuring Events." ● Different models support different alarm types. See the interface actually displayed.
Processing State	Select the alarm processing state, including all, unsolved, solved, processing, false and ignored.

Step 3 Click **Search**.

The results are displayed.

3.8 Configuring the System

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

3.8.1 TCP/IP Settings

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

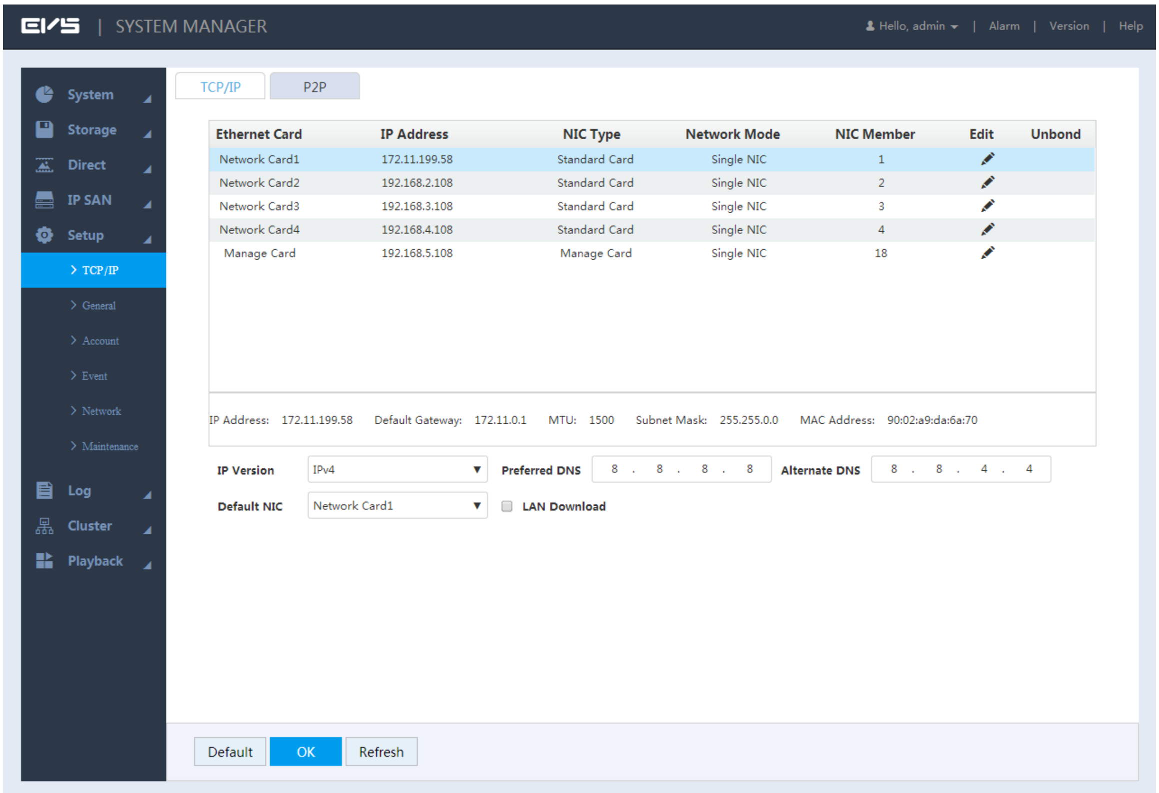
3.8.1.1 IP Settings

According to network plan, set the EVS device information such as the IP address and DNS server.

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

The **TCP/IP** interface is displayed. See Figure 3-48 and Figure 3-49. For details, see Table 3-15.

Figure 3-48 TCP/IP settings (single-control device)



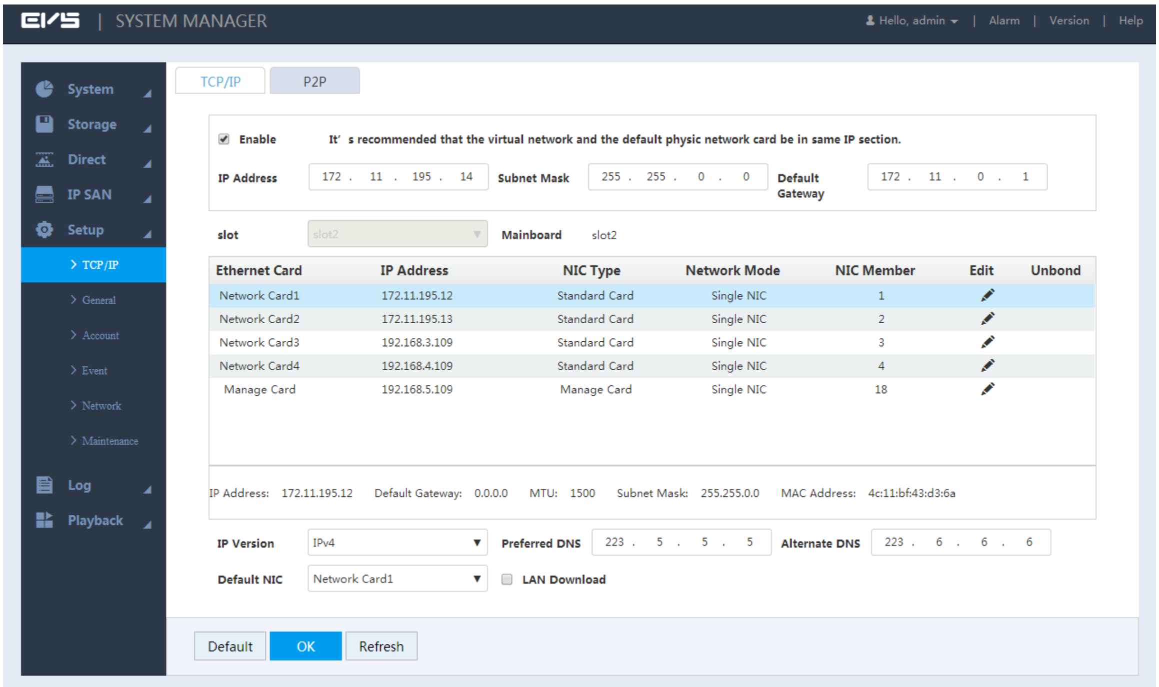
Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	172.11.199.58	Standard Card	Single NIC	1	✎	
Network Card2	192.168.2.108	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎	
Manage Card	192.168.5.108	Manage Card	Single NIC	18	✎	

IP Address: 172.11.199.58 Default Gateway: 172.11.0.1 MTU: 1500 Subnet Mask: 255.255.0.0 MAC Address: 90:02:a9:da:6a:70

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

Default NIC: Network Card1 □ LAN Download

Figure 3-49 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 172 . 11 . 195 . 14 Subnet Mask 255 . 255 . 0 . 0 Default Gateway 172 . 11 . 0 . 1

slot slot2 Mainboard slot2

Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	172.11.195.12	Standard Card	Single NIC	1	✎	
Network Card2	172.11.195.13	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.109	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.109	Standard Card	Single NIC	4	✎	
Manage Card	192.168.5.109	Manage Card	Single NIC	18	✎	

IP Address: 172.11.195.12 Default Gateway: 0.0.0.0 MTU: 1500 Subnet Mask: 255.255.0.0 MAC Address: 4c:11:bf:43:d3:6a

IP Version IPv4 Preferred DNS 223 . 5 . 5 . 5 Alternate DNS 223 . 6 . 6 . 6

Default NIC Network Card1 □ LAN Download

Default OK Refresh

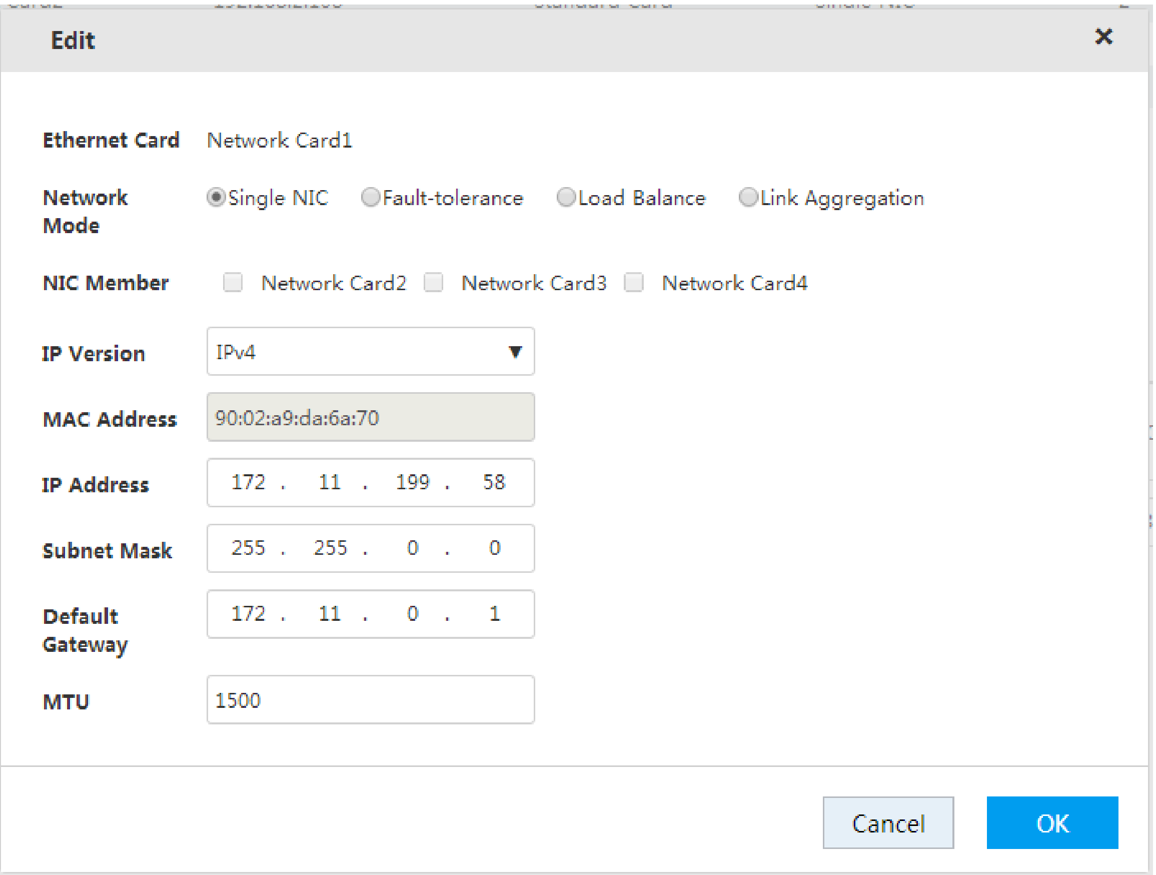
Table 3-15 Description of TCP/IP setting parameters

Parameter	Description
Slot	Select the slot of the dual-control device. The corresponding NIC information is displayed in the list. NOTE 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.
Alternate DNS	Enter the IP address of alternate DNS.
Default NIC	Select the default NIC of EVS device.
LAN Download	Select the check box. Under the condition of network bandwidth allowed, the LAN download speed is 1.5-2 times of the normal download speed.

Step 2 Click ✎.

The **Edit** interface is displayed. See Figure 3-50.

Figure 3-50 Editing



Edit

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:da:6a:70

IP Address: 172 . 11 . 199 . 58

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 172 . 11 . 0 . 1

MTU: 1500

Step 3 Select/Enter the parameters. For details, see Table 3-16.

Table 3-16 Description of NIC editing parameters

Parameter	Description
Ethernet Card	Display the current NIC name.

Parameter	Description
Network Mode	Select the network mode of the EVS device. ● Single NIC: The Network card can be used alone. You can select one Network card to provide the HTTP or RTSP service. You need to set one default Network card (default is eth1) to request the network service started by Email and FTP. Once the card is offline, the whole network is offline. ● Fault-tolerance: In this mode, device uses bonding NIC to communicate with the external devices. You can focus on one host IP address. At the same time, you need to set one master card. Usually there is only one running card (master card).System can enable alternate card when the master card is malfunction. The system is shown as offline once all cards are offline. Notice that all cards shall be in the same LAN. ● Load balance: In this mode, device uses bonding NIC to communicate with the external device. All cards are working now and bearing the network load. Their network loads are general the same. The system is shown as offline once all cards are offline. Notice that all cards shall be in the same LAN. ● Link aggregation: System uses bonding NIC to realize communication function. All binding NICs are working together and bearing the network load. System allocates the corresponding ports to the specified switches according to the port load setting. Once one port link is malfunction, system stops sending out data from current port. System can calculate the new load and specify the new port(s) to send out data. System calculates again to specify the port(s) once the malfunction port becomes available. 📖 NOTE ● EVS device only supports LACP link aggregation. ● When the switch supports link aggregation and is equipped with link aggregation, you can set the network mode to link aggregation.
NIC Member	When the **Network Mode** is set to **Single NIC**, you can bond the current NIC to any other one. 📖 NOTE Management NIC does not support this function.
IP Version	You can select IPv4 or IPv6 Format. Currently both IP addresses are supported.
MAC Address	Display the MAC address of the EVS device.
IP Address	Set the IP address, subnet mask and default gateway of the EVS 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 the 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. NOTE ● Modifying the MTU will lead to NIC restart and network interruption to affect the running business. Be careful to perform it. ● It is recommended to view the MTU value of the gateway first, and set the MTU value of EVS device to be the same or slightly smaller than that of the gateway, so as to reduce sub package and improve network transmission efficiency.

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

3.8.1.2 Virtual IP

The master control panel and slave control panel have their own real IP. After setting the virtual IP, regardless of the switch of master and slave panels, the user can log in Web normally.

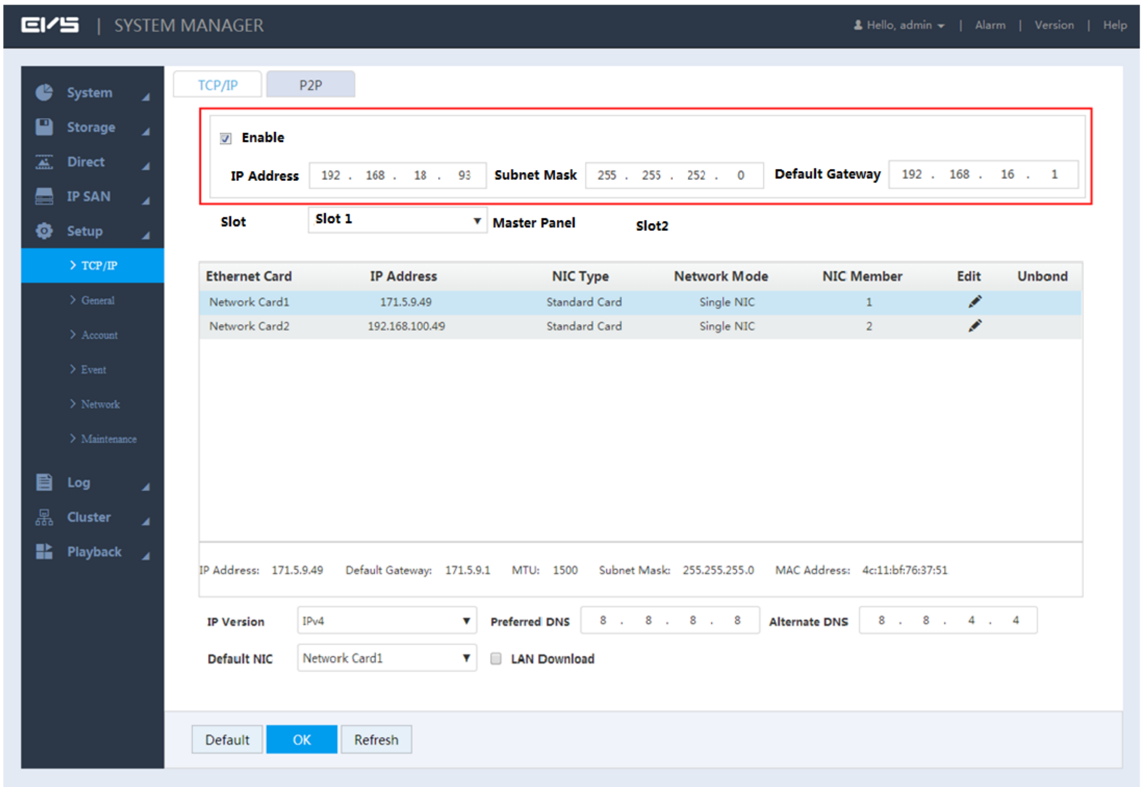
NOTE

Only dual-control devices support this function.

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

The **TCP/IP** interface is displayed. See Figure 3-51.

Figure 3-51 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	171.5.9.49	Standard Card	Single NIC	1	✎	
Network Card2	192.168.100.49	Standard Card	Single NIC	2	✎	

IP Address: 171.5.9.49 Default Gateway: 171.5.9.1 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** check box to open virtual IP.

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

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

3.8.1.3 P2P

P2P is a kind of convenient private network penetration technology. You do not need to apply for dynamic domain name, doing port mapping or deploying transit server. You can add EVS devices through the below way to achieve the purpose of managing multiple EVS devices at the same time.

- Scan the QR code, download cell phone app, and then register an account. For details, see Operations on Cell Phone App.
- Log in the platform at address www.gotop2p.com, register an account, and then add device through the serial number. For details, see Introduction of P2P Operations which is available in the disk delivered with the device.

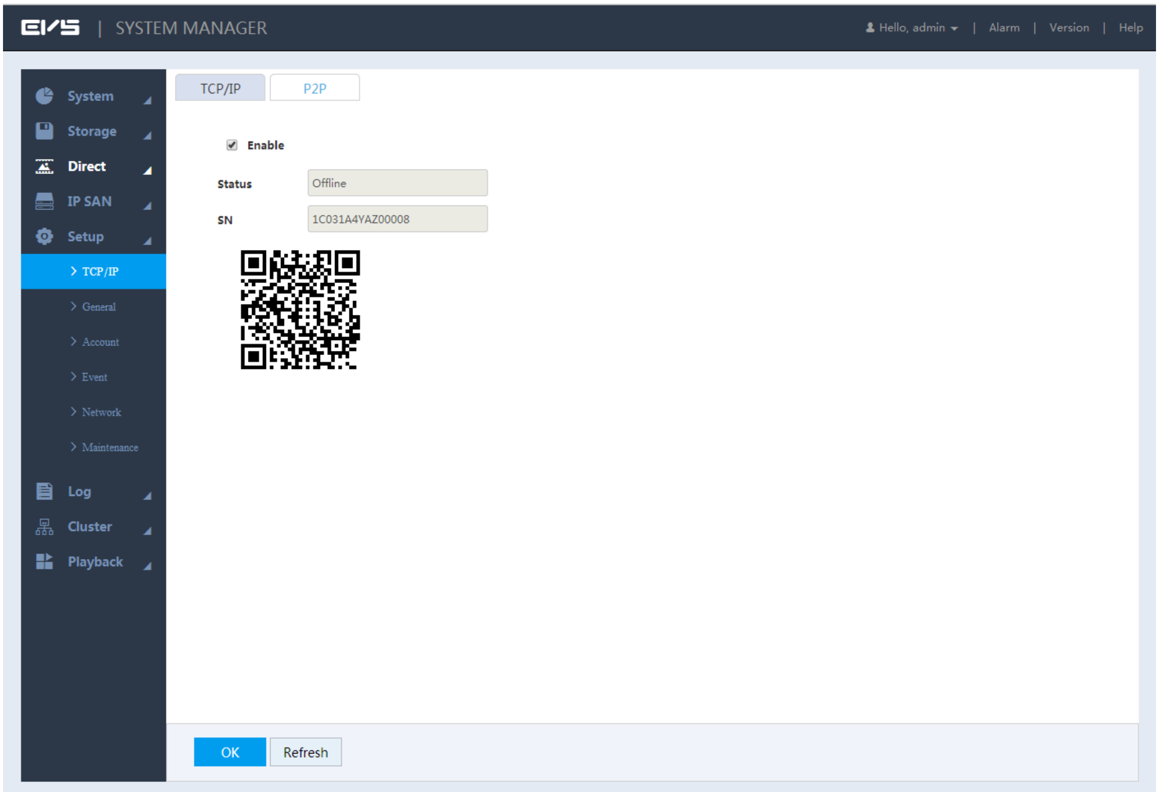
⚠ CAUTION

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

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

The **P2P** interface is displayed. See Figure 3-52.

Figure 3-52 P2P



☑ Enable

Status: Offline

SN: 1C031A4YAZ00008

Step 2 Select **Enable** to open the P2P function.

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

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

Operations on Cell Phone App

Taking the mobile phone client as an example, operations see below:

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

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

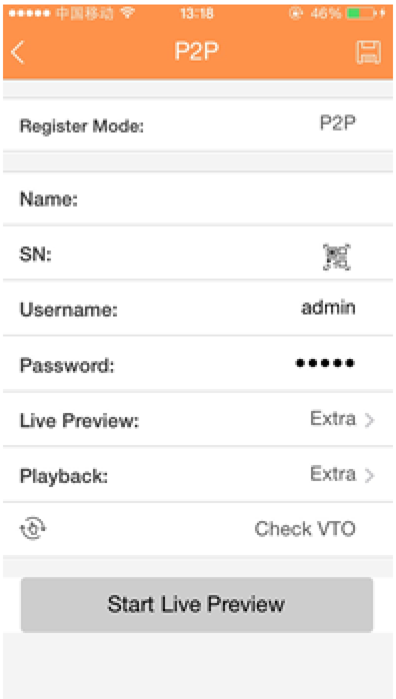
Step 3 Add device on the cell phone app.

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

2) Tap + to enter the QR code scanning interface. Scan the device label or the **SN** QR code shown in Figure 3-53.

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

Figure 3-53 Adding device



Register Mode: P2P

Name:

SN:

Username: admin

Password: ●●●●●

Live Preview: Extra >

Playback: Extra >

Check VTO

Start Live Preview

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

3.8.2 General Settings

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

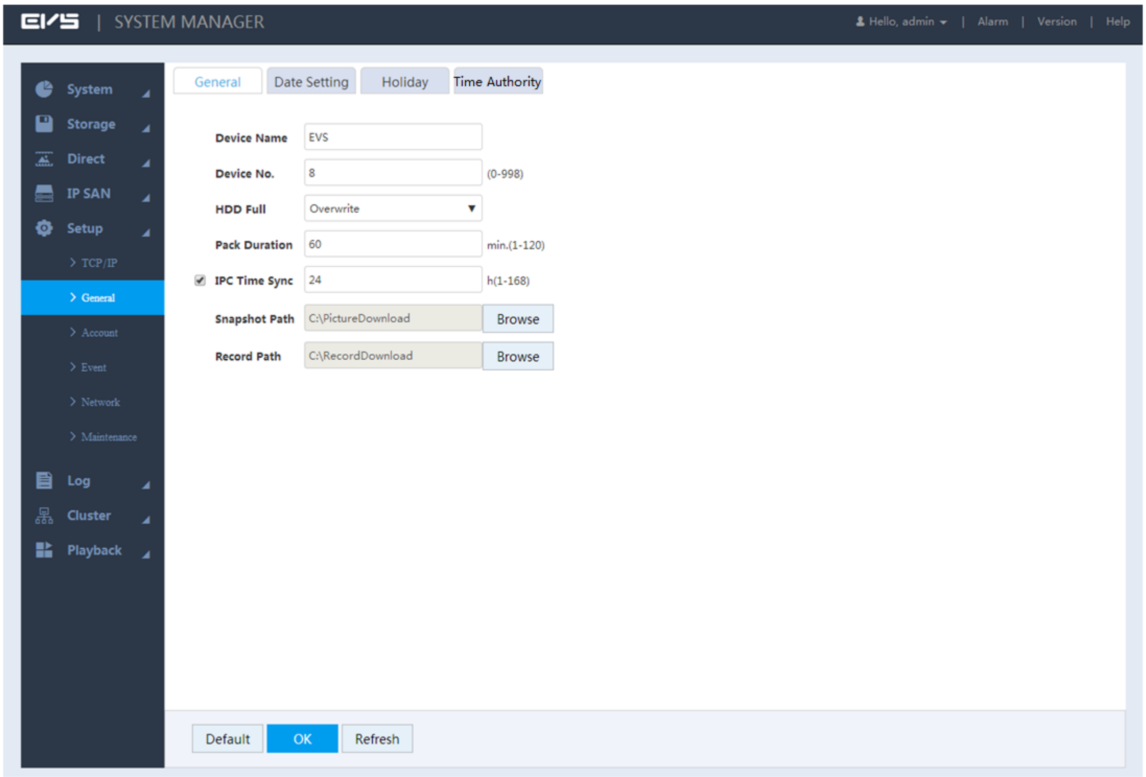
3.8.2.1 Local Settings

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

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

The **General** interface is displayed. See Figure 3-54.

Figure 3-54 Local settings



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 Select/Enter the parameters. For details, see Table 3-17.

Table 3-17 Description of local 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** and **Overwrite**. ● Condition of record stop: The current working disk is full and there is no extra free disk available, stop recording. ● Condition of record overwritten: The current working disk is full and there is no extra free disk available, overwrite the earliest records in cycle.
Pack Duration	Enter the time duration of each record. The maximum length can be 120 minutes.
IPC Time Sync	Select this check box to set the time interval that IPC synchronize the time with the EVS device.
Snapshot Path	Click the **Browse** on 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 the **Browse** on 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.

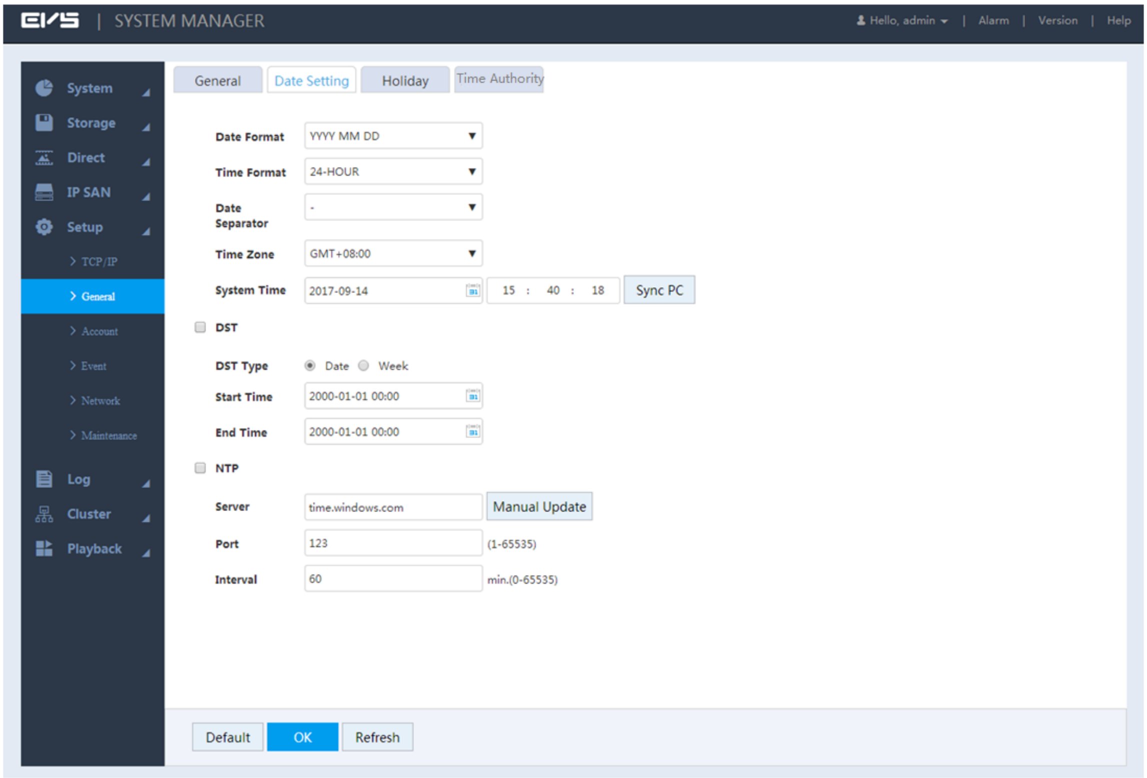
3.8.2.2 Date Settings

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

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

The **Date Setting** interface is displayed. See Figure 3-55.

Figure 3-55 Date Settings



Date Format: YYYY MM DD

Time Format: 24-HOUR

Date Separator: -

Time Zone: GMT+08:00

System Time: 2017-09-14 15 : 40 : 18

□ DST

DST Type: ● Date ○ Week

Start Time: 2000-01-01 00:00

End Time: 2000-01-01 00:00

□ NTP

Server: time.windows.com

Port: 123 (1-65535)

Interval: 60 min.(0-65535)

Step 2 Select/Enter the parameters. For details, see Table 3-18.

Table 3-18 Description of date setting parameters

Parameter	Description
Date Format	Select the date format of the EVS device, including YYYY MM DD, MM DD YYYY, DD MM YYYY.
Time Format	Select the time format of the EVS device, including 24-hour and 12-hour.
Date Separator	Select the separator between the year, month and date.
Time Zone	Select the current time zone that EVS device locates.
System Time	Select/Enter the current system date and time. ⚠ CAUTION The modified system time shall be out of the time period which record exists in the HDD, otherwise you might fail to search the record. For example, if there is a record available from 10:00-12:00 in HDD and you change the system time to 11:00, you might be unable to view the record from 11:00-12:00.
Sync PC	Click **Sync PC** and the system automatically synchronizes time with the PC logged in Web.
DST	Some countries and districts implement DST (Daylight Saving Time). Enable DST according to actual needs. For steps, see below: 1. Select the **DST** check box to enable it. 2. Select the DST type, including **Date** and **Week**. 3. Select the **Start Time** and **End Time** of DST.

Parameter	Description
NTP	The device automatically synchronizes time with the NTP server. For steps, see below: 1. Select the **NTP** check box to enable it. 2. Select/Enter 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 at 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.

3.8.2.3 Holiday Settings

Add, edit and delete holiday information. After setting the holiday, holiday option will appear in the time period displayed on the record setting and snapshot setting interfaces.

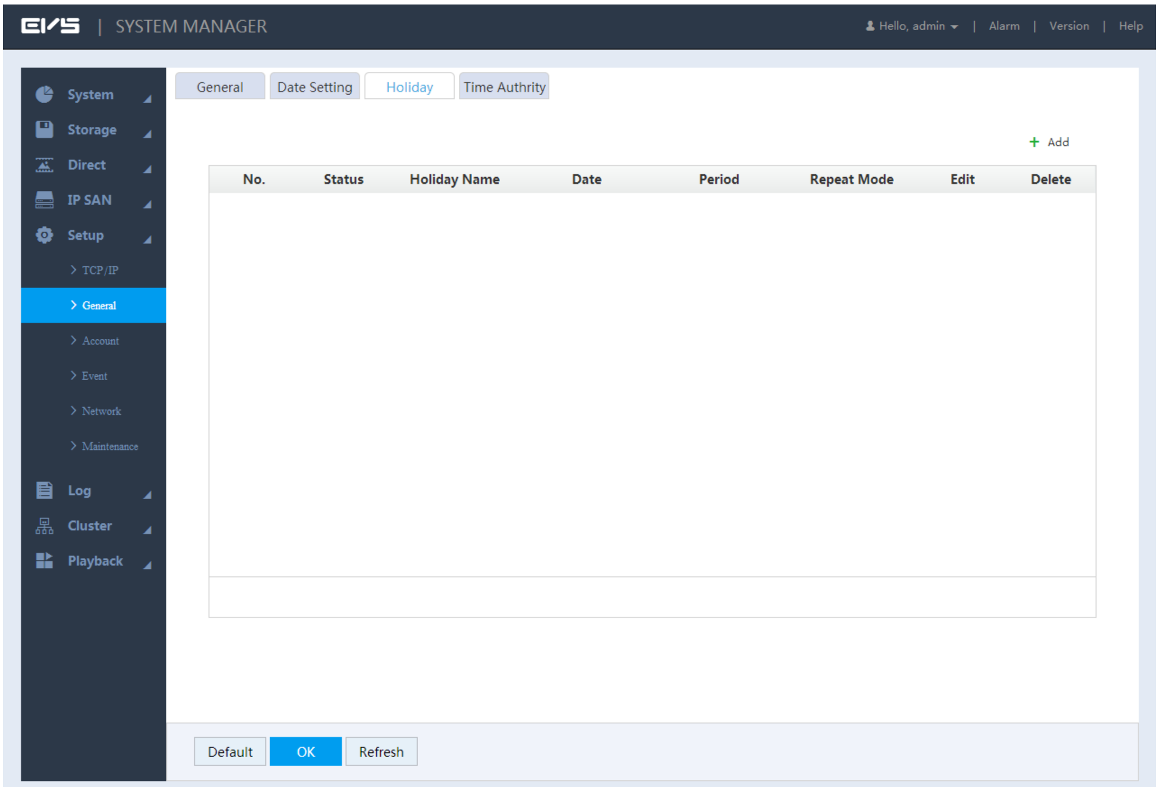
NOTE

The priority of holiday setting is higher than the general one. For example, both the holiday plan and general plan are open on a holiday, the system starts recording according to the holiday plan.

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

The **Holiday** interface is displayed. See Figure 3-56.

Figure 3-56 Holiday settings (1)

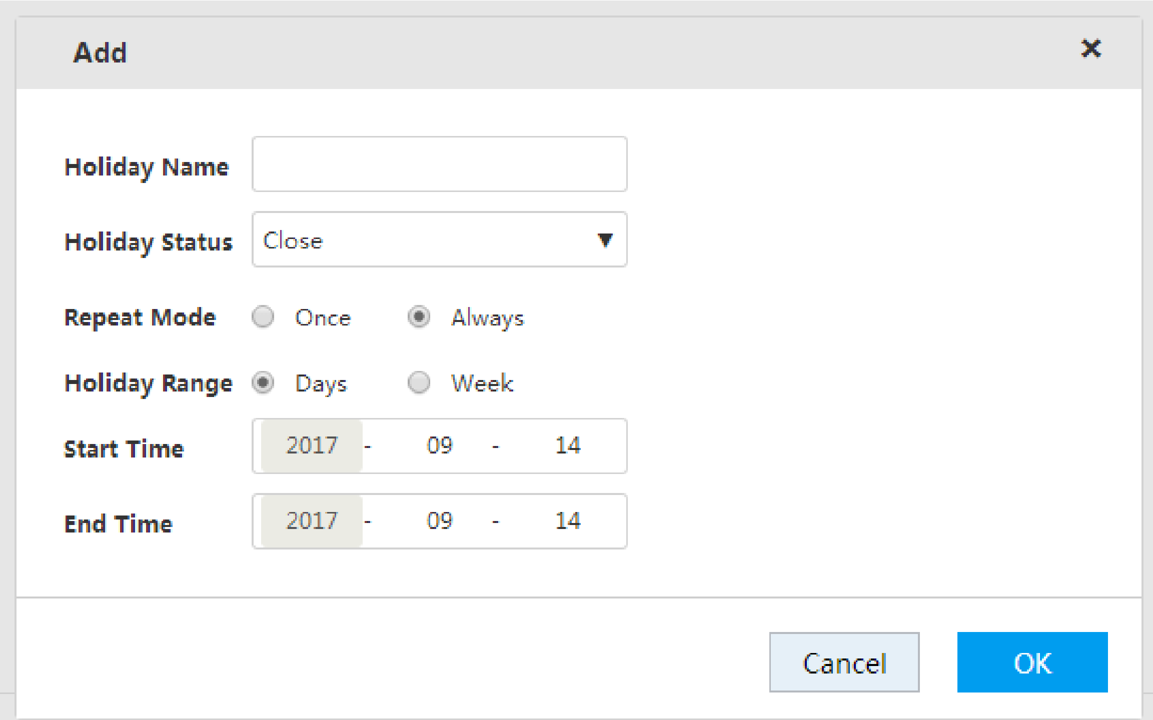


No.	Status	Holiday Name	Date	Period	Repeat Mode	Edit	Delete

Step 2 Click + .

The **Add** interface is displayed. See Figure 3-57.

Figure 3-57 Adding holiday



Add

Holiday Name

Holiday Status: Close

Repeat Mode: ○ Once ● Always

Holiday Range: ● Days ○ Week

Start Time: 2017 - 09 - 14

End Time: 2017 - 09 - 14

Step 3 Configure the parameter. For details, see Table 3-19.

Table 3-19 Description of 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 for once. ● **Always**: The holiday takes effect repeatedly.
Holiday Range	Select the holiday range, including **Days** and **Week**.
Start Time	Enter the start time and end time of the holiday.
End Time	

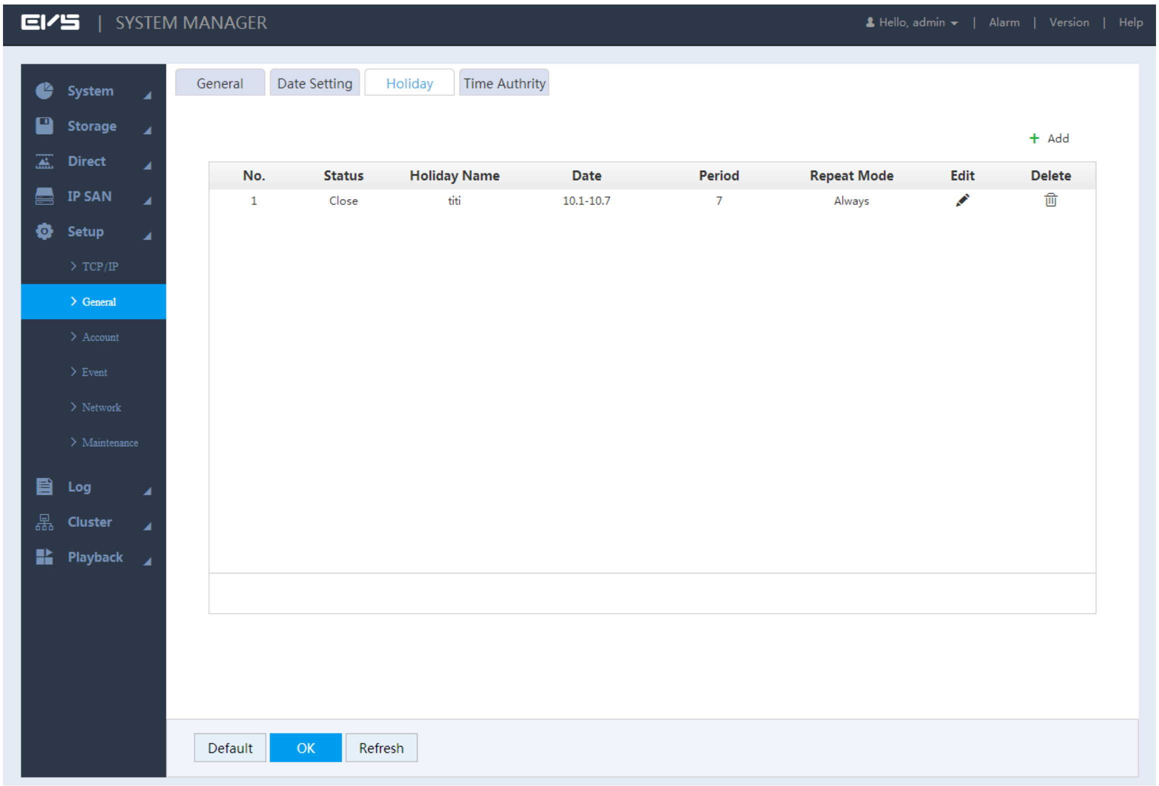
Step 4 Click **OK** to save the settings.

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

NOTE

- Double-click the corresponding status of the holiday, you can open or close the holiday.
- Click ✎ to edit the holiday and click 🗑 to cancel the holiday.

Figure 3-58 Holiday settings (2)



No.	Status	Holiday Name	Date	Period	Repeat Mode	Edit	Delete
1	Close	titi	10.1-10.7	7	Always	✎	🗑

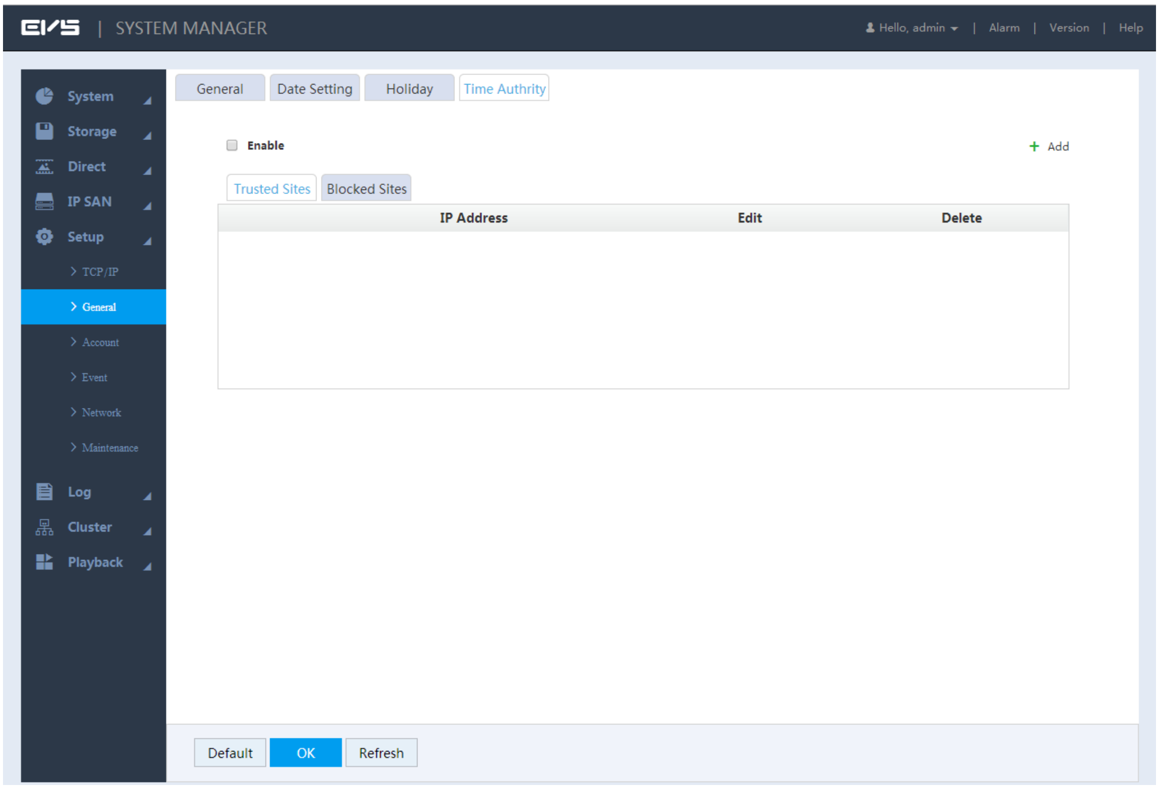
3.8.2.4 Timing Authority

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

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

The **Time Authority** interface is displayed. See Figure 3-59.

Figure 3-59 Timing authority



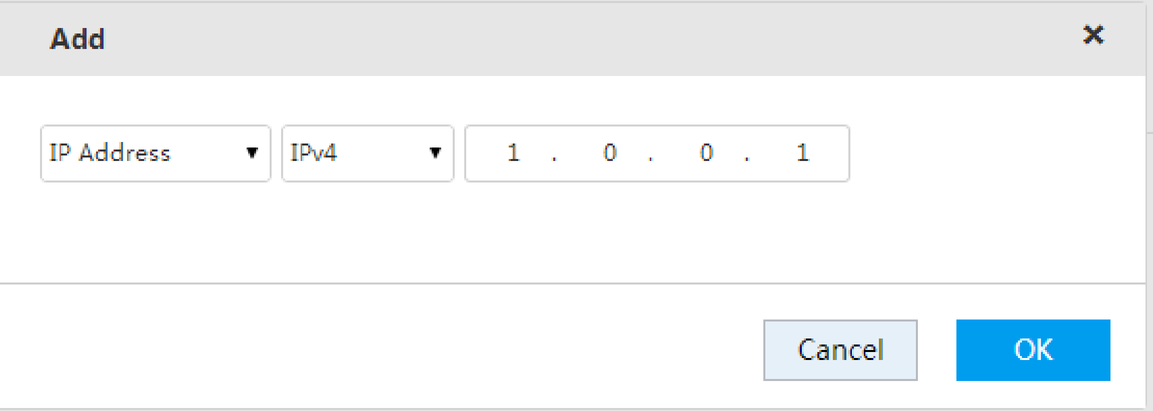
Step 2 Select the **Enable** check box to open this function.

Step 3 Add IP host.

1) Click **Add**.

The **Add** interface is displayed. See Figure 3-60.

Figure 3-60 Adding IP host



2) Select/Enter the IP address information. For details, see Table 3-20.

NOTE

The system supports 64 IP addresses at most.

Table 3-20 Description of IP address parameters

Parameter	Description
IP Address	Click the drop-down box to select the way to add trusted/blocked sites. ● IP address: Enter the IP address you want to add to the trusted/blocked list. ● IP network segment: Enter the range of the network segment you want to add to the trusted/blocked list. You can add multiple hosts at the same time. ● MAC address: Enter the MAC address you want to add to the trusted/blocked list.

Parameter	Description
IPv4	Click the drop-down box to select the IP protocol. ● IPv4: The IP address adopts IPv4 format, like 192.168.5.10. ● IPv6: The IP address adopts IPv6 format, like aa:aa:aa:aa:aa:aa:aa:aa.

3) Click **OK**.

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

3.8.3 User Management

User management adopts both user group and user levels. Each user name and group name is unique and cannot by repeated.

- The factory default user name is admin. The default password is the same as the user name.
- You can set up to 64 users or 20 user groups.
- Factory default includes both user and admin groups, and the admin group cannot be deleted.
- Users in the group can modify its authority in the group authority. To facilitate the user management, the recommended authority of common users shall be lower than that of advanced users.
- Each user must belong to and can only belong to one group. When selecting a group to which the user belongs to, the user's authority can only be a subset of the group's authorities and cannot exceed the authority attribute of the group.
- The user name and group name is a string of 1-31 bytes, which can only be made up of letter(s), number(s), underscore(s) and connection(s).

3.8.3.1 User

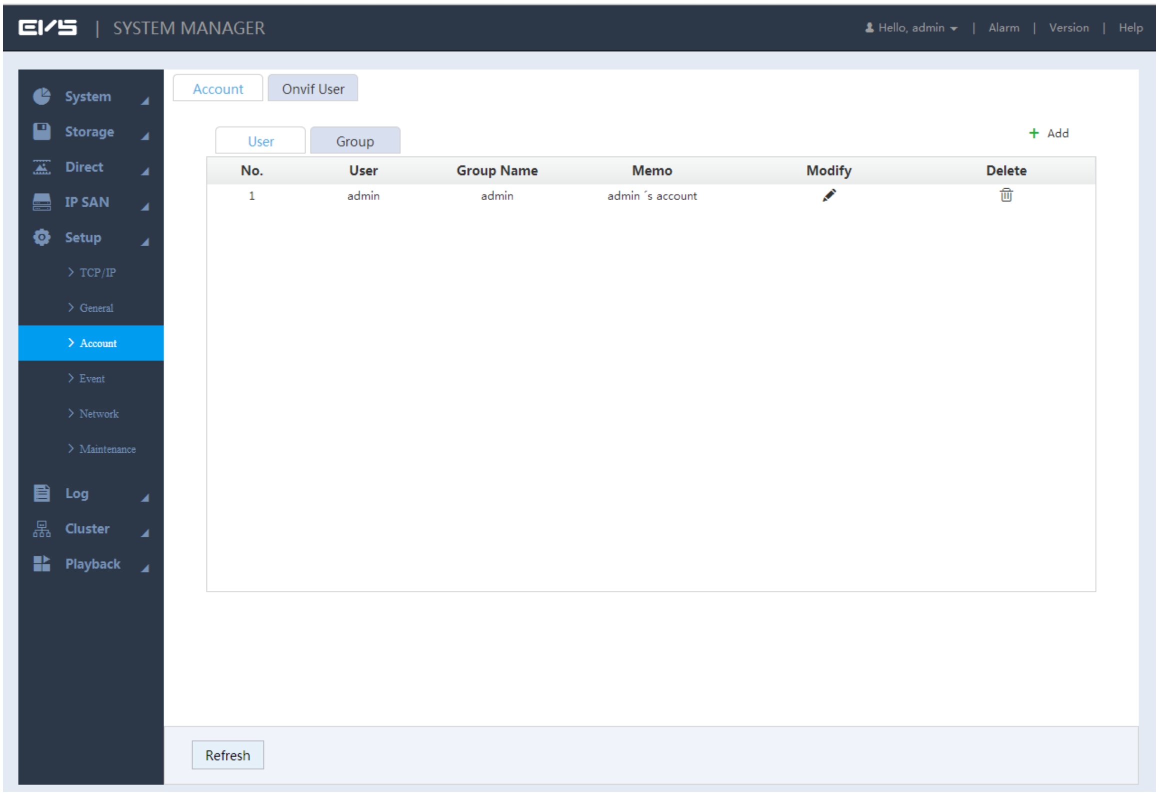
User information management includes adding, deleting and modifying users, adding users to a group and set the user authority.

3.8.3.1.1 Adding Users

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

The **User** interface is displayed. See Figure 3-61.

Figure 3-61 User

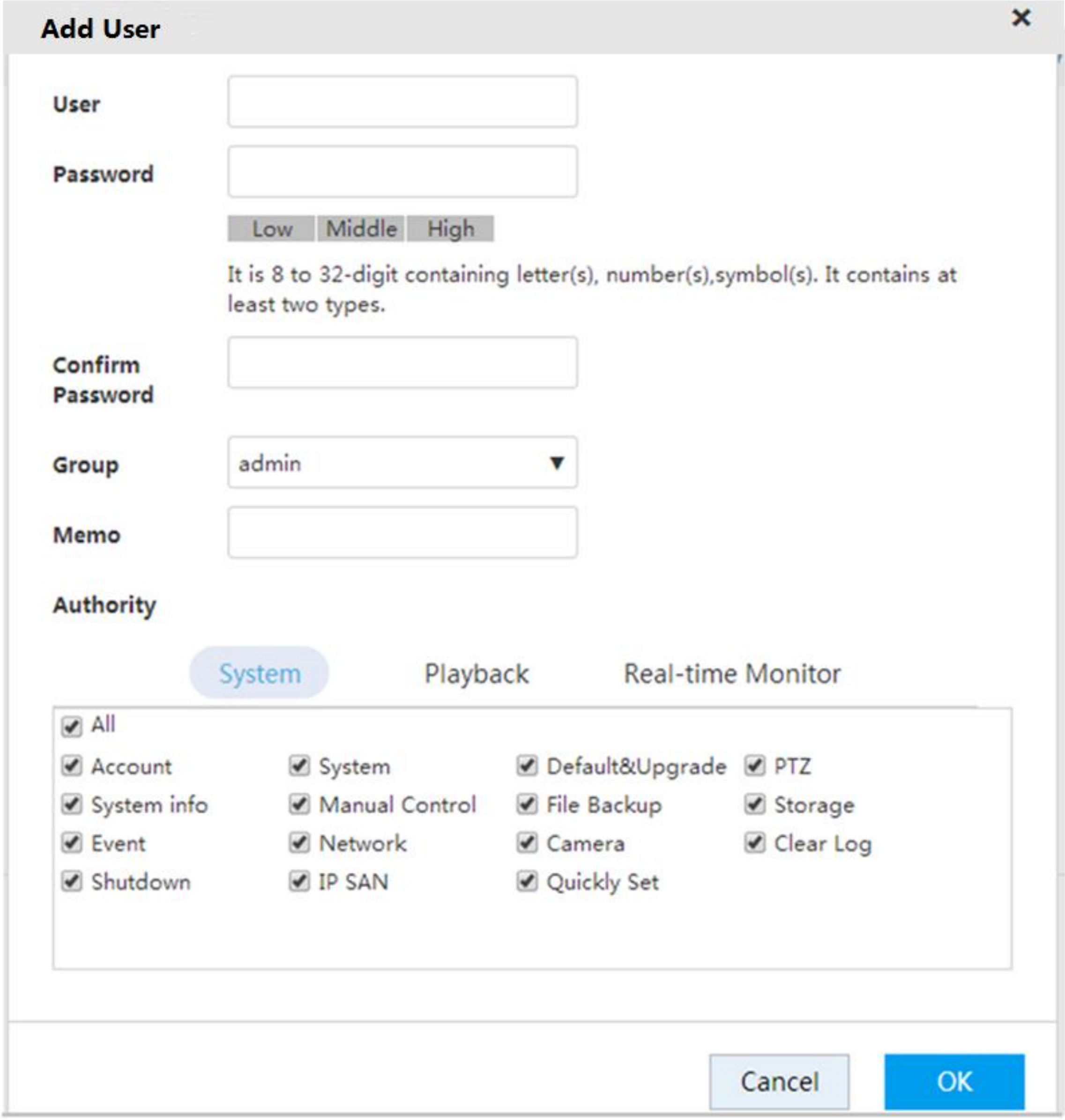


No.	User	Group Name	Memo	Modify	Delete
1	admin	admin	admin ´s account	✎	🗑

Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-62.

Figure 3-62 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

System | Playback | Real-time Monitor

☑ All

☑ Account	☑ System	☑ Default&Upgrade	☑ PTZ
☑ System info	☑ Manual Control	☑ File Backup	☑ Storage
☑ Event	☑ Network	☑ Camera	☑ Clear Log
☑ Shutdown	☑ IP SAN	☑ Quickly Set	

Step 3 Select/Enter the parameters. For details, see Table 3-21.

Table 3-21 Description of adding user parameters

Parameter	Description
User	Enter the user name.
Password	Enter and confirm the password. It is an 8-digit to 32-digit string containing letter(s), number(s) and symbol(s). It contains at least 2 types. 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. NOTE For detailed description of adding groups, see "3.8.3.2 User Group."
Memo	Enter memo information to help user recognition and management.

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

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

NOTE

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

3.8.3.1.2 Modifying Password

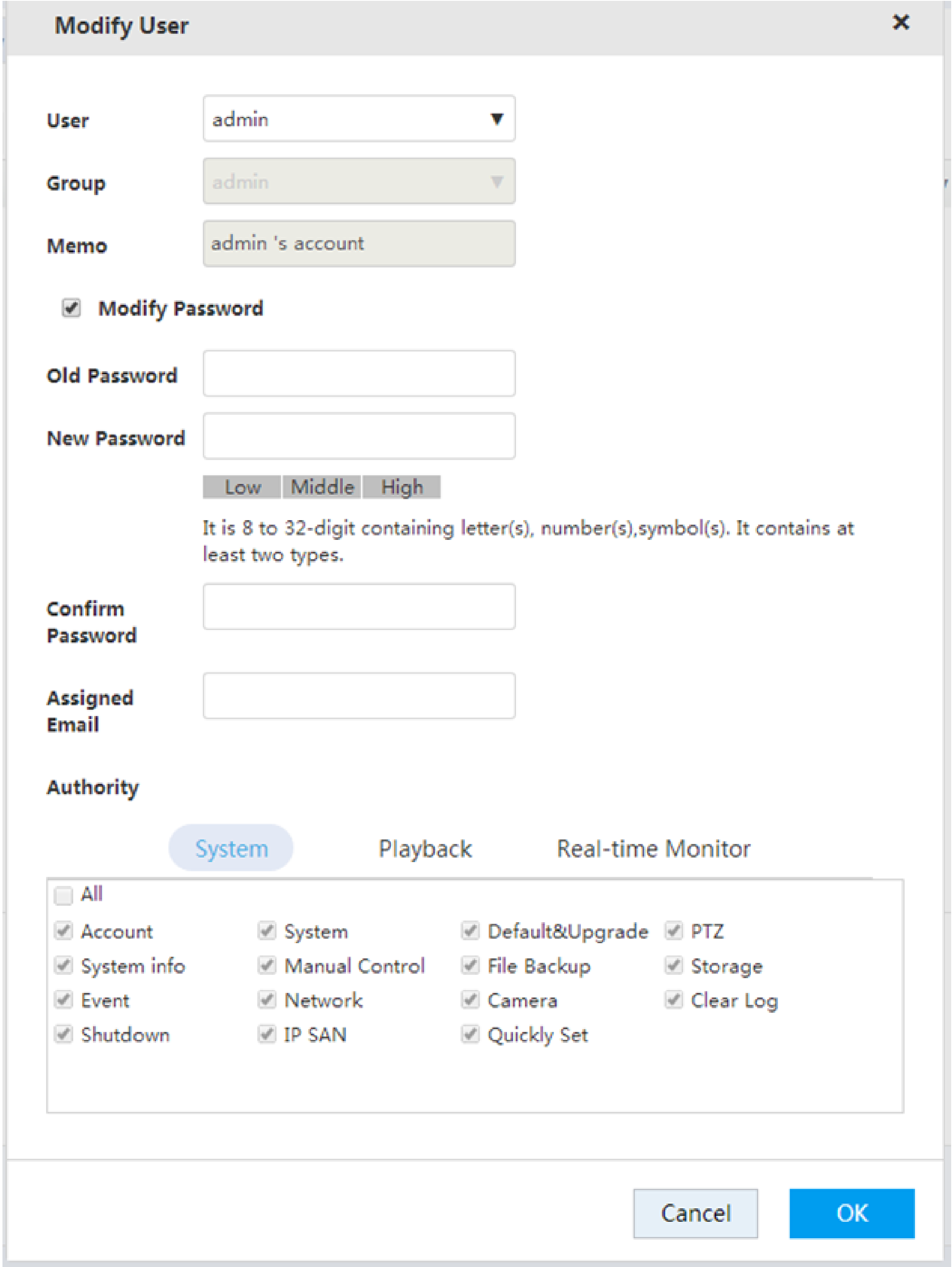
Users with user management authority can modify the password of themselves and other users.

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

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

The **Modify User** interface is displayed. See Figure 3-63.

Figure 3-63 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	☑ Default&Upgrade	☑ PTZ
☑ System info	☑ Manual Control	☑ File Backup	☑ Storage
☑ Event	☑ Network	☑ Camera	☑ Clear Log
☑ Shutdown	☑ IP SAN	☑ Quickly Set	

Step 3 Enter Old Password, New Password and Confirm Password.

NOTE

It is an 8-digit to 32-digit string containing letter(s), number(s) and symbol(s). It contains at least 2 types.

Step 4 Assign email.

After entering the assigned email, you can reset the password through the email if you forgot the password for admin account.

NOTE

Only the admin account supports assigned email. See the interface displayed actually.

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

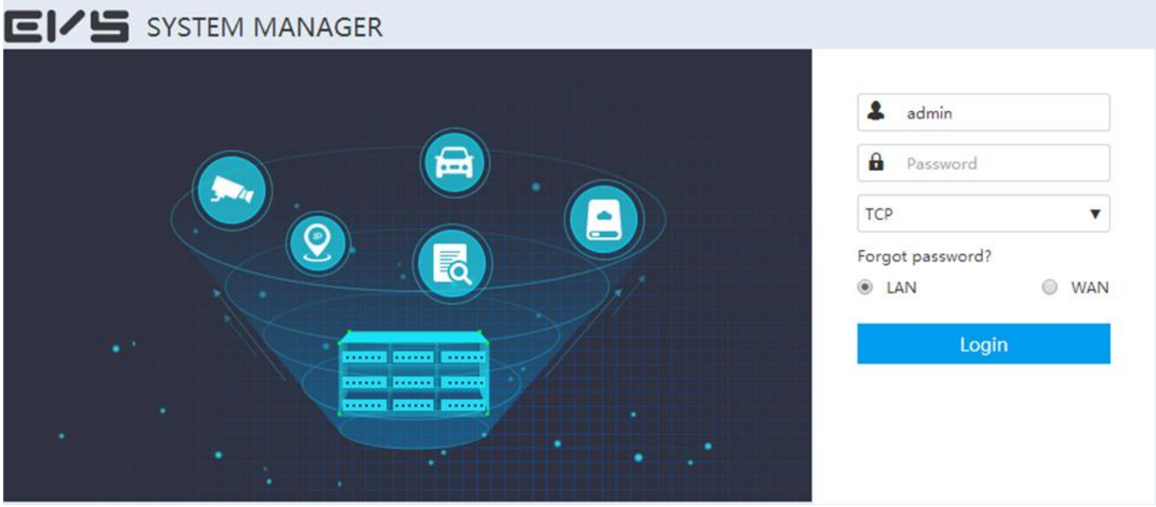
3.8.3.1.3 Resetting Password

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 EVS device into the address bar. Press Enter key.

The login interface is displayed. See Figure 3-64.

Figure 3-64 Login



EVS SYSTEM MANAGER

admin

Password

TCP

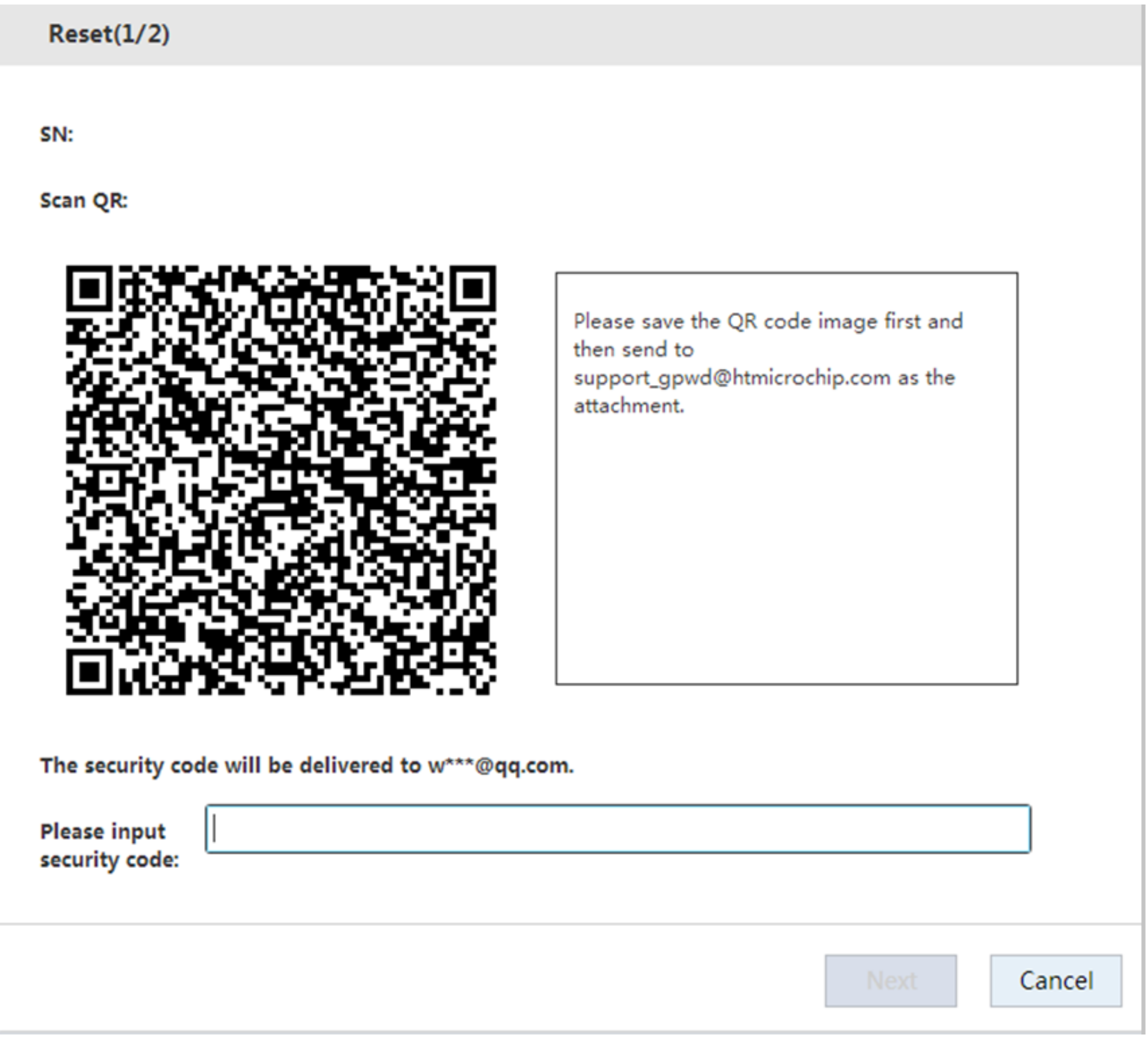
Forgot password?

● LAN ○ WAN

Step 2 Click Forgot password.

The **Reset (1/2)** interface is displayed. See Figure 3-65.

Figure 3-65 Resetting password (1)



Reset(1/2)

SN:

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 w***@qq.com.

Please input security code:

Step 3 Send the QR code according to the notice to obtain the security code.

CAUTION

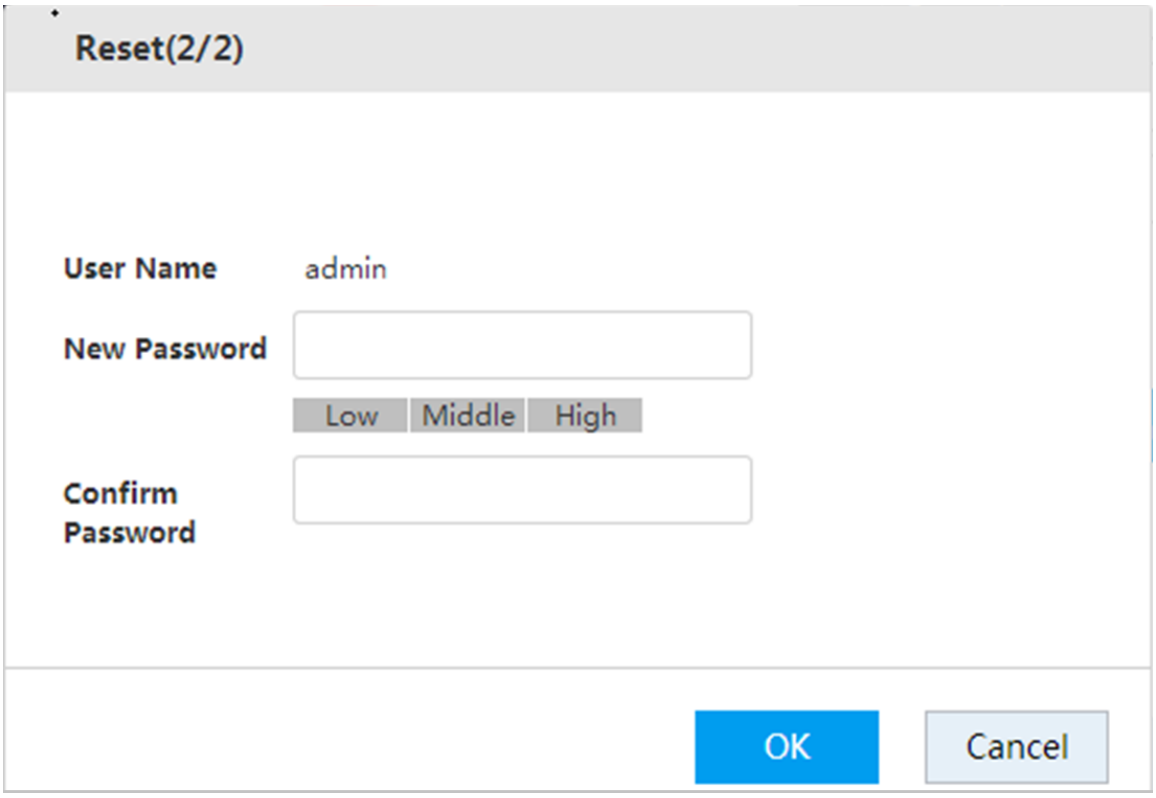
- You can obtain the security code for twice at most by sending the same QR code. If you need more times, refresh the QR interface.
- Use the security code to reset the password within 24 hours, otherwise it will be invalid.

Step 4 Enter the security code into the **Please input security code** text box.

Step 5 Click **Next**.

The **Reset (2/2)** interface is displayed. See Figure 3-66.

Figure 3-66 Resetting password (2)


Reset(2/2)

User Name admin

New Password

Confirm Password

Step 6 Enter the New Password and Confirm Password.

It is an 8-digit to 32-digit string containing letter(s), number(s) and symbol(s). It contains at least 2 types. It is recommended to set a high security password according to the strength prompt.

Step 7 Click **OK** to complete the password reset.

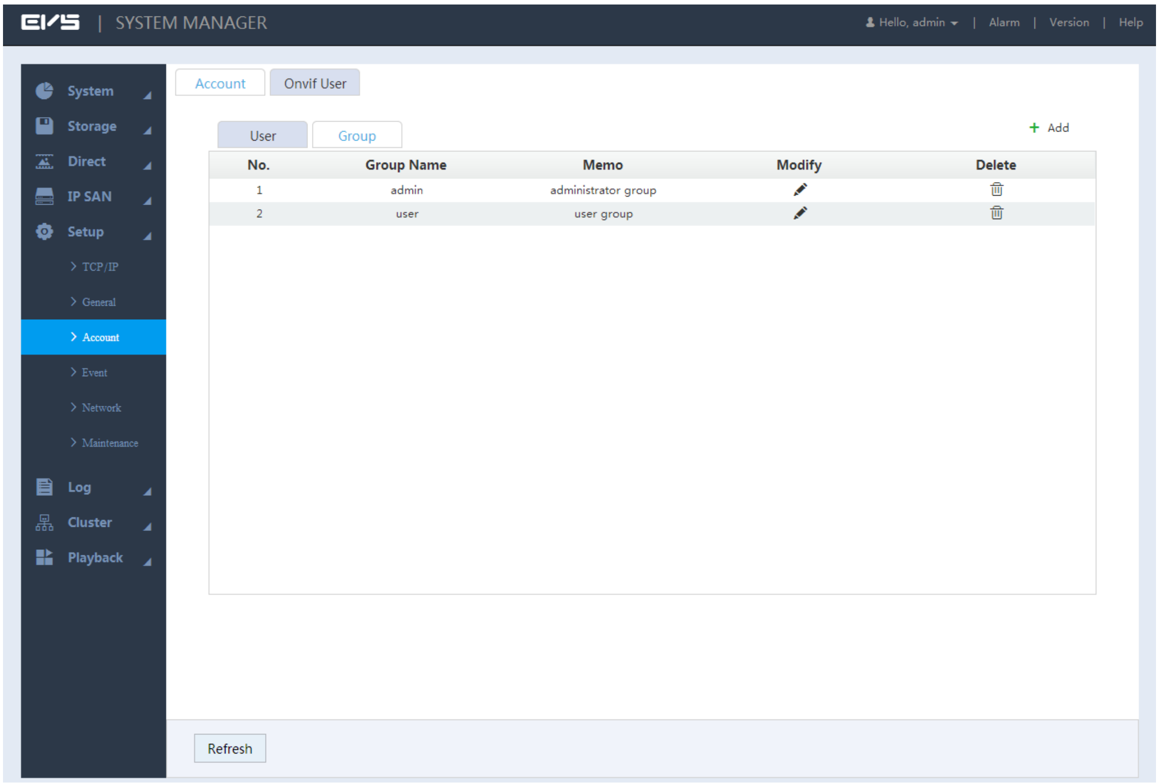
3.8.3.2 User Group

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

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

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

Figure 3-67 Group

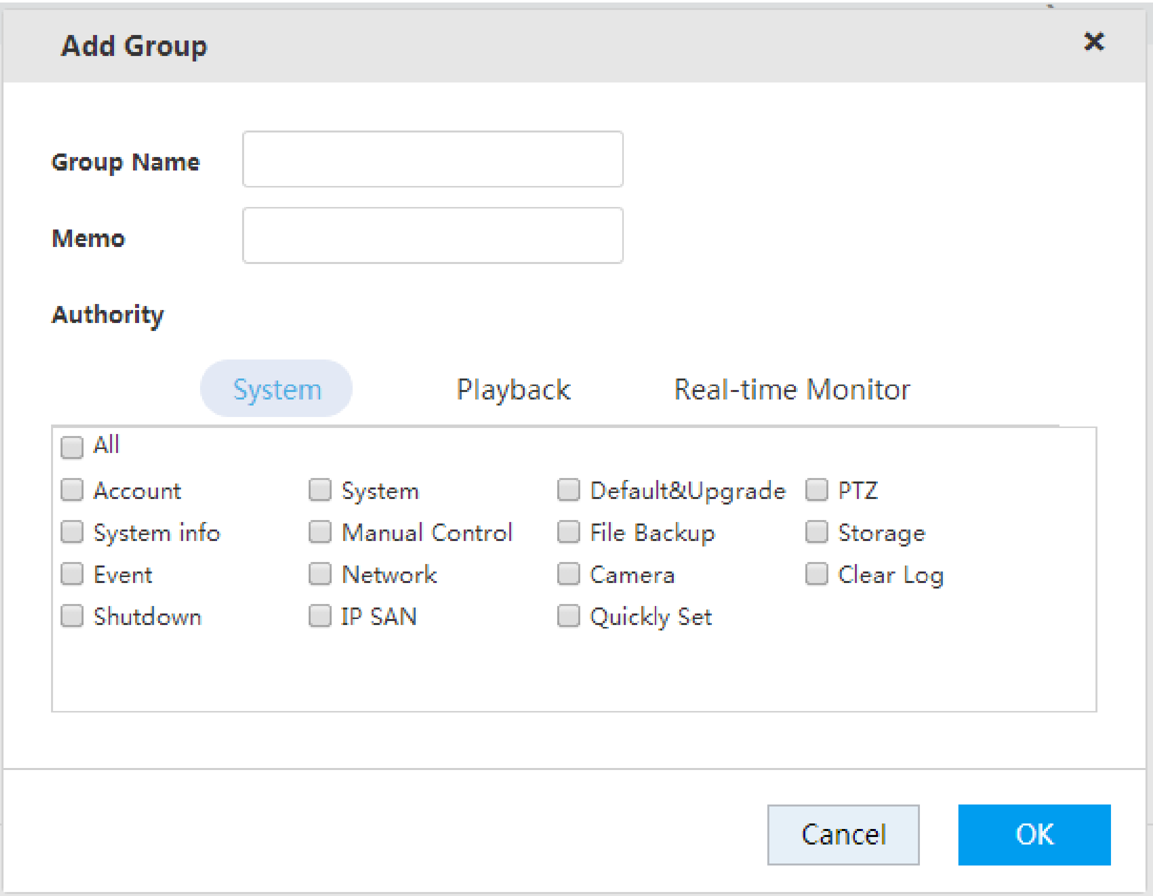


No.	Group Name	Memo	Modify	Delete
1	admin	administrator group	✎	🗑
2	user	user group	✎	🗑

Step 2 Click + .

The **Add Group** interface is displayed. See Figure 3-68.

Figure 3-68 Adding Group



Group Name

Memo

Authority

☐ All

☐ Account ☐ System ☐ Default&Upgrade ☐ PTZ

☐ System info ☐ Manual Control ☐ File Backup ☐ Storage

☐ Event ☐ Network ☐ Camera ☐ Clear Log

☐ Shutdown ☐ IP SAN ☐ Quickly Set

Step 3 Select/Enter the parameters. For details, see

Table 3-22 Description of adding group parameters

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

NOTE

Click ✎ to edit group information and click 🗑 to delete the group.

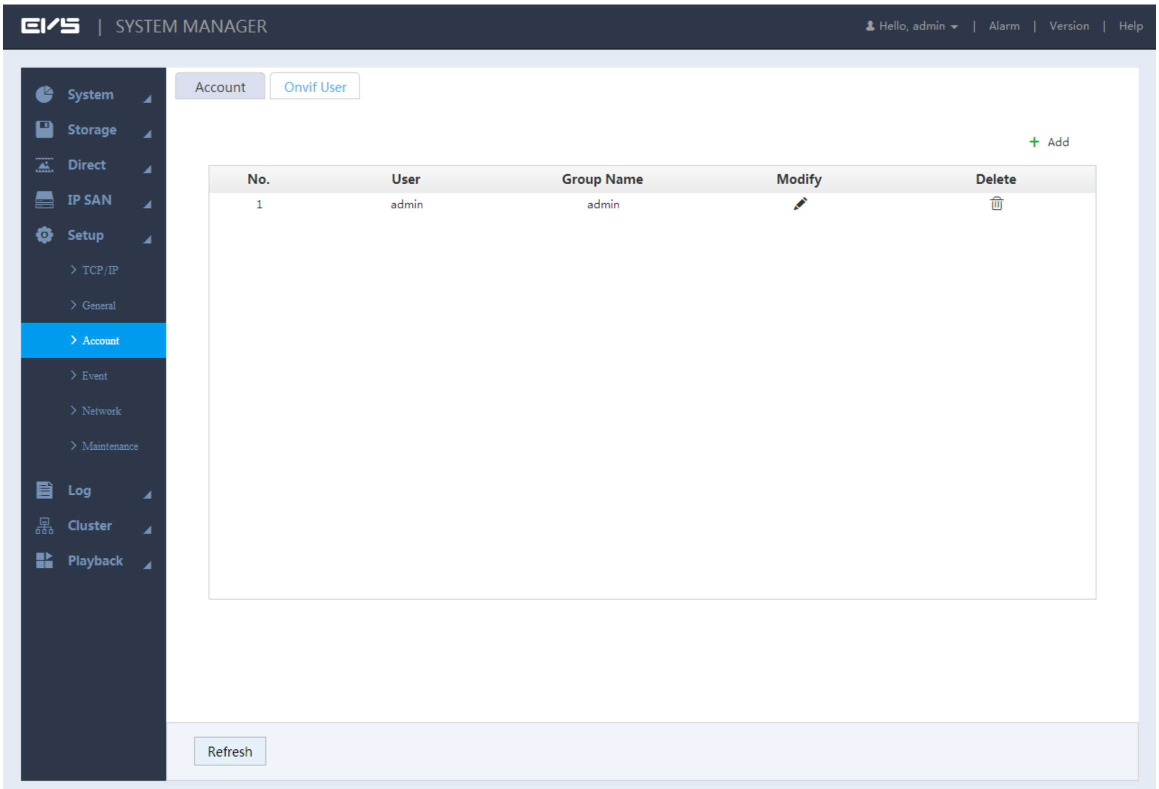
3.8.3.3 Onvif User

When devices of other manufacturers access EVS device through the Onvif protocol, the Onvif account needs to be verified. You can manage Onvif user information in this interface.

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

The **Onvif User** interface is displayed. See Figure 3-69.

Figure 3-69 Onvif user

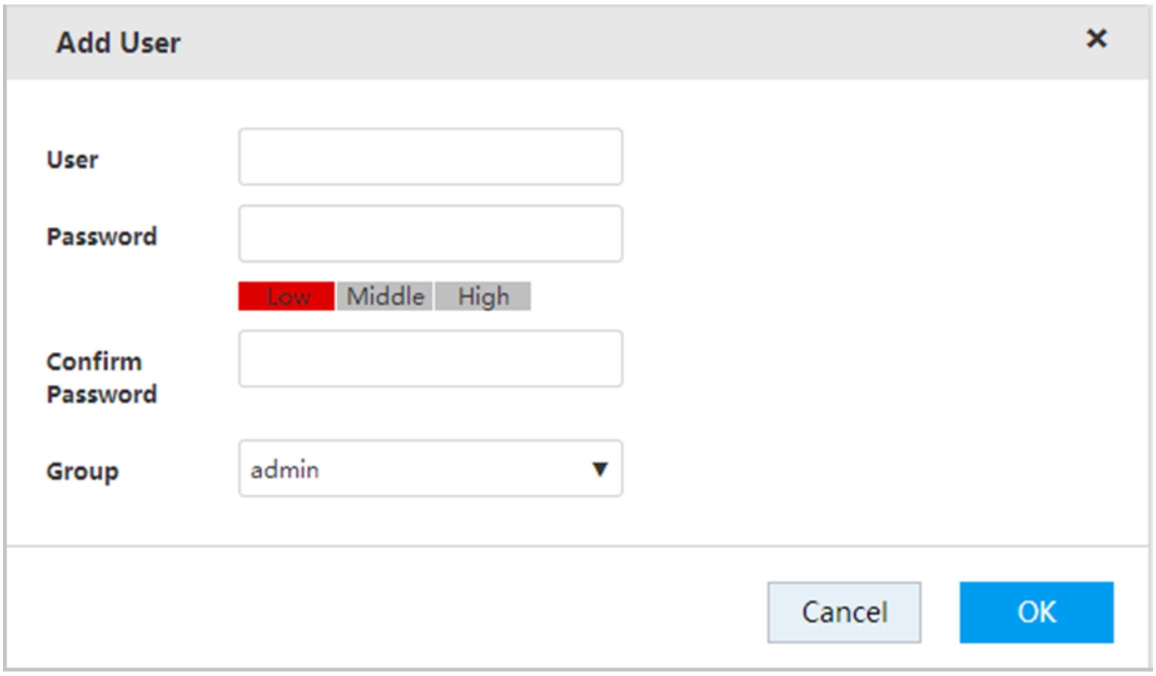


No.	User	Group Name	Modify	Delete
1	admin	admin	✎	🗑

Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-70.

Figure 3-70 Adding user



Group: admin

Step 3 Select/Enter the parameters. For details, see Table 3-23.

Table 3-23 Description of adding user parameters

Parameter	Description
User	Enter the user name.
Password	Enter and confirm the password. The new password can be set from 8 characters through 32 characters and contain at least two types from 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. NOTE For detailed description of adding groups, see "3.8.3.2 User Group."

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

NOTE

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

3.8.4 Configuring Events

Configure the linkages of video detection, alarm events and abnormal events. When the alarm is triggered, the EVS device automatically performs the pre-set linked actions.

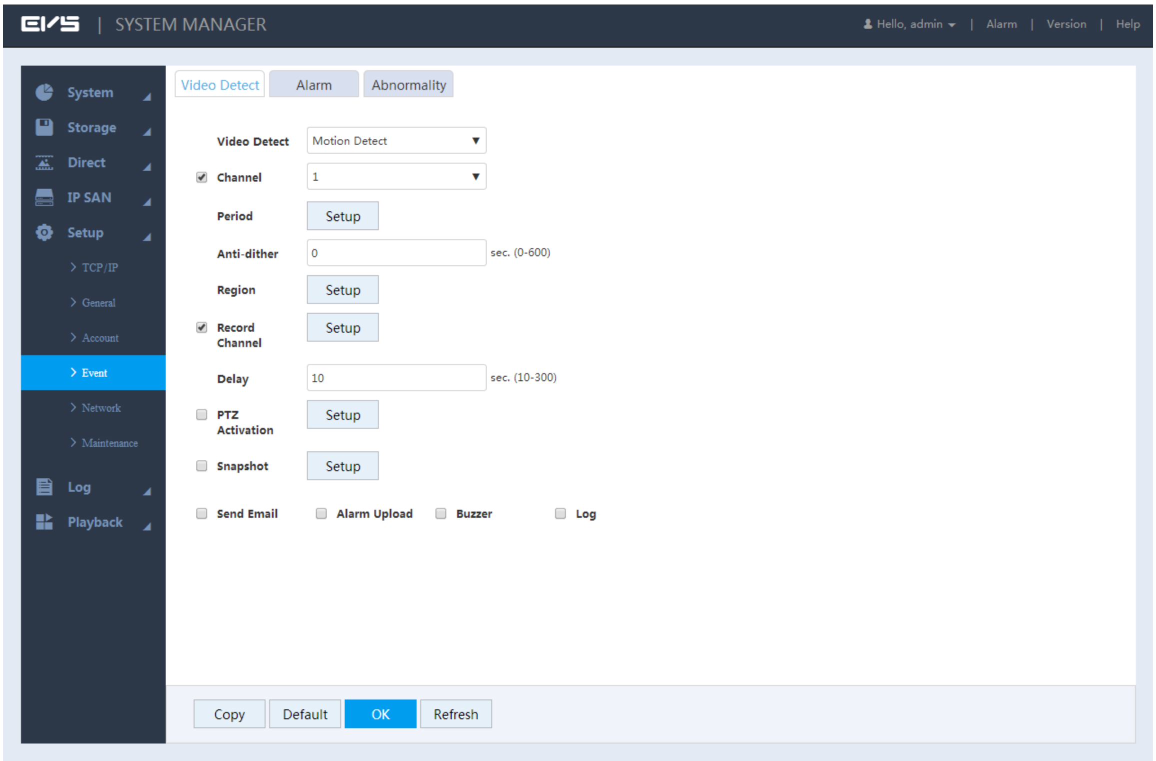
3.8.4.1 Video Detect

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

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

The **Video Detect** interface is displayed. See Figure 3-71.

Figure 3-71 Video detect



Video Detect: Motion Detect

☑ Channel: 1

Period: Setup

Anti-dither: 0 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.
- Video block: When the monitoring screen is blocked by some object, resulting in the output of a single color image, the system executes the alarm linkage.

Step 3 Select the **Channel** check box and choose the channel number to enable the video detection function.

Step 4 Set the **Period** of deployment and withdrawal.

Step 5 Set the video detect region.

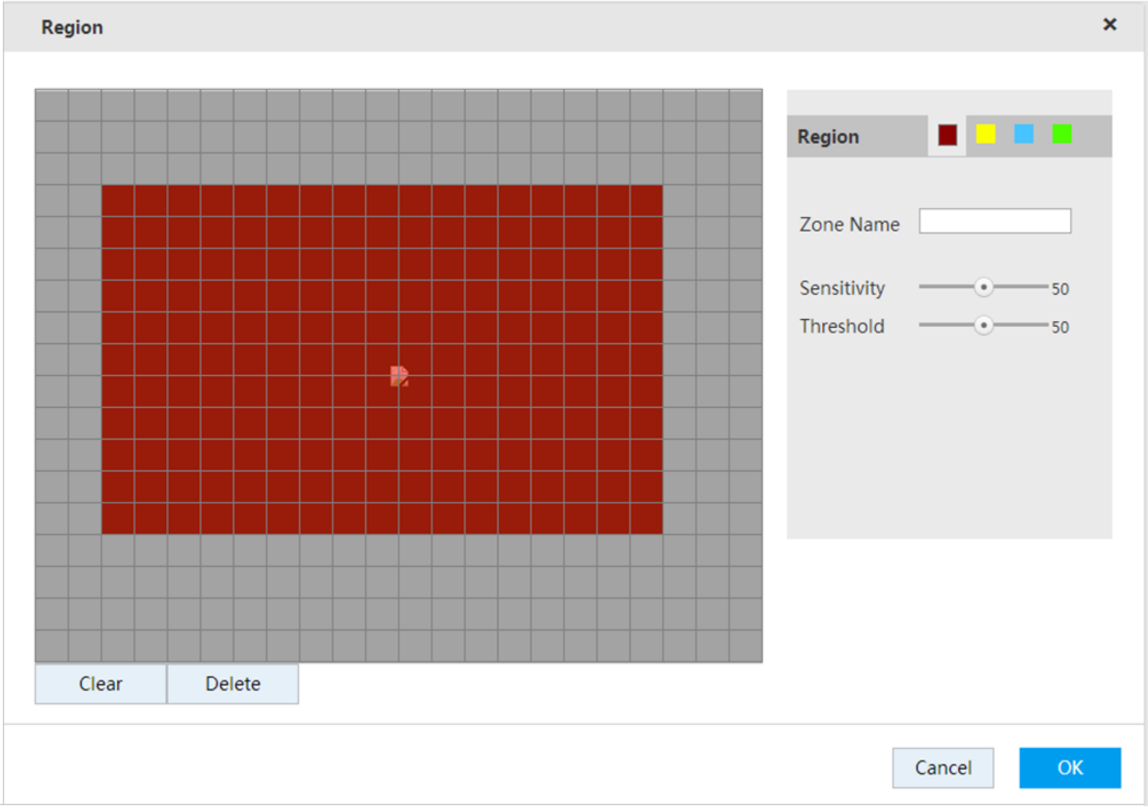
1) Click **Setup** on the right side of **Region**.

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

NOTE

The region is composed of 22*18(PAL) and 22*15(NTSC) small regions.

Figure 3-72 Region settings



Zone Name

Sensitivity 50

Threshold 50

2) Select a region in the Region. Different regions are marked with different colors.

NOTE

Different front device supports different number of regions. See the interface actually displayed.

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

NOTE

- You can draw multiple detect areas until the whole monitoring screen is filled.
- Channel alarm condition: if any one of the four regions triggers the alarm, the channel in which the area is located triggers the alarm.

4) Select/Enter the parameters. For details, see Table 3-24.

Table 3-24 Description of region setting parameters

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

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

Step 6 Select/Enter the parameters. For details, see Table 3-25.

Table 3-25 Description of video detection parameters

Parameter	Description

Parameter	Description
Period	Alarm linkage takes effect only in the set time period. For details, see "Period Settings."
Anti-dither	Only record alarm event for once during the set anti-dither time period. NOTE Only motion detection supports this function.
Record Channel	Select the check box, click **Setup** on the right side, and then select the channels as needed (multiple choices available). When an alarm occurs, the EVS device links to the selected channel for video recording. NOTE Firstly you need to open the motion detection and auto record functions. For details, see "3.10.4.1 Record Plan Settings" and "3.10.5 Record Control."
Post Record	At the end of the alarm, the record is extended for a period of time. The extended time range is 10-300 seconds.
Alarm Out	Connect the alarm device to the alarm out port (like light, siren). The device transmits alarm information to the alarm device when an alarm occurs. NOTE Only High-End 24-HDD Single-Controller supports this function.
Delay	At the end of the alarm information, the alarm extends for a period of time. The extended time range is 0-300 seconds. NOTE Only High-End 24-HDD Single-Controller supports this function.
PTZ Activation	Select the check box, click the **Setup** on 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. NOTE ● Motion detection only supports PTZ pre-set point linkage. ● The corresponding PTZ actions shall be set first. For details, see "3.6.1.3 PTZ Console."
Snapshot	Select the check box, click the **Setup** on the right side, and then select the channel. When an alarm occurs, the device links to the selected channel for snapshot. NOTE Firstly you need to open the motion detect snapshot and auto snapshot functions. For details, see "3.10.4.2 Snapshot Plan Settings" and "3.10.5 Record Control."
Prompt	Select the check box. When an alarm occurs, alarm information pops up on the screen of the local host.
Send Email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. NOTE You need to set the Email first. For details, see "3.8.5.2.2 Email Settings."

Parameter	Description
Alarm Upload	Select the check box. The device uploads the alarm signal to the network (including alarm center) when an alarm occurs. NOTE Only some models support this function. See the actual situation.
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.

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

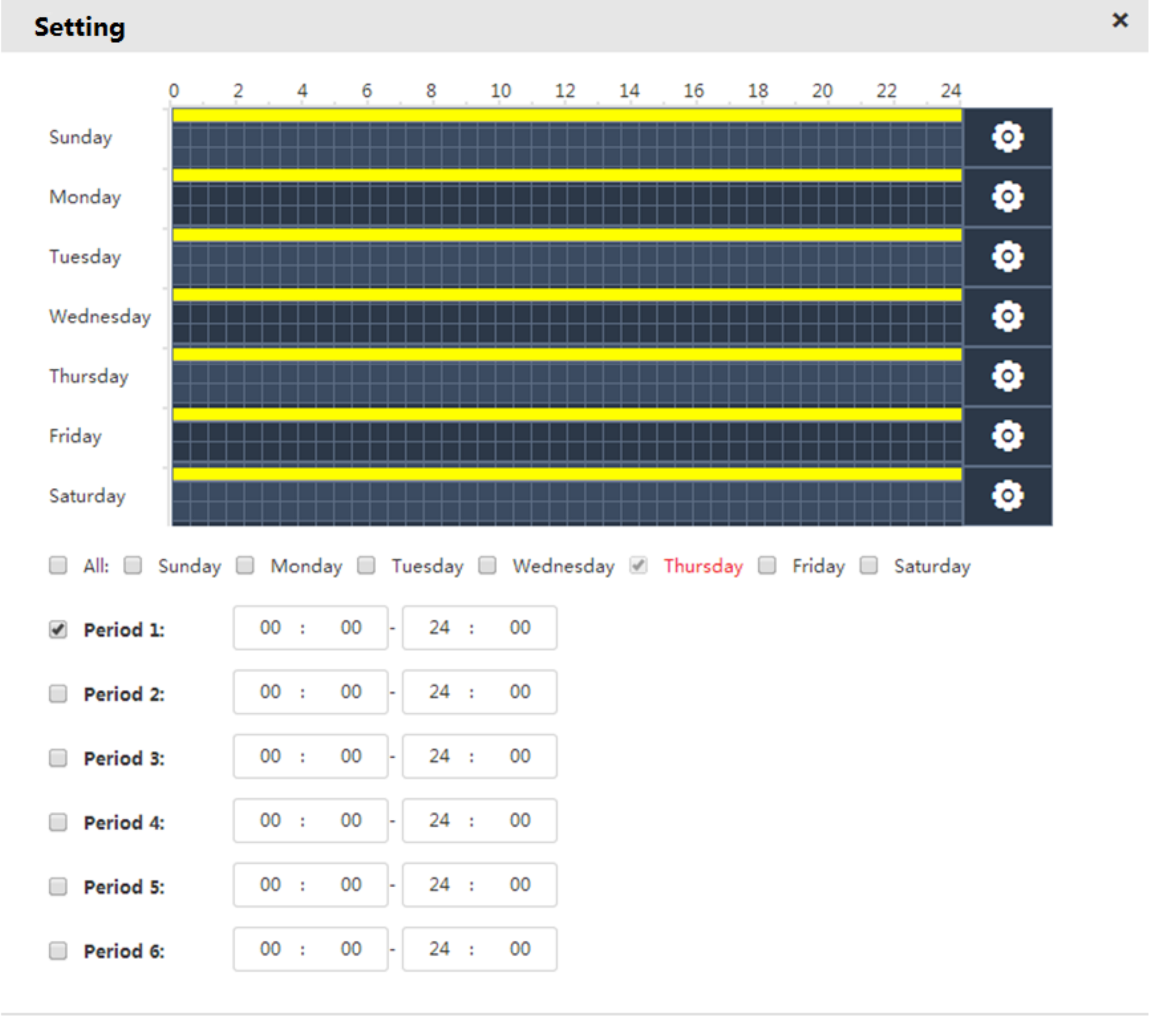
Period Settings

Only within the set time period, the corresponding configuration item will start alarm linkage.

Step 1 Click **Setup** on the right side of **Period**.

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

Figure 3-73 Period Setting



□ 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

Step 2 Set the period, including drawing method and editing method.

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

NOTE

Select the check box in front of the day and you can set the period for multiple or all the days.

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

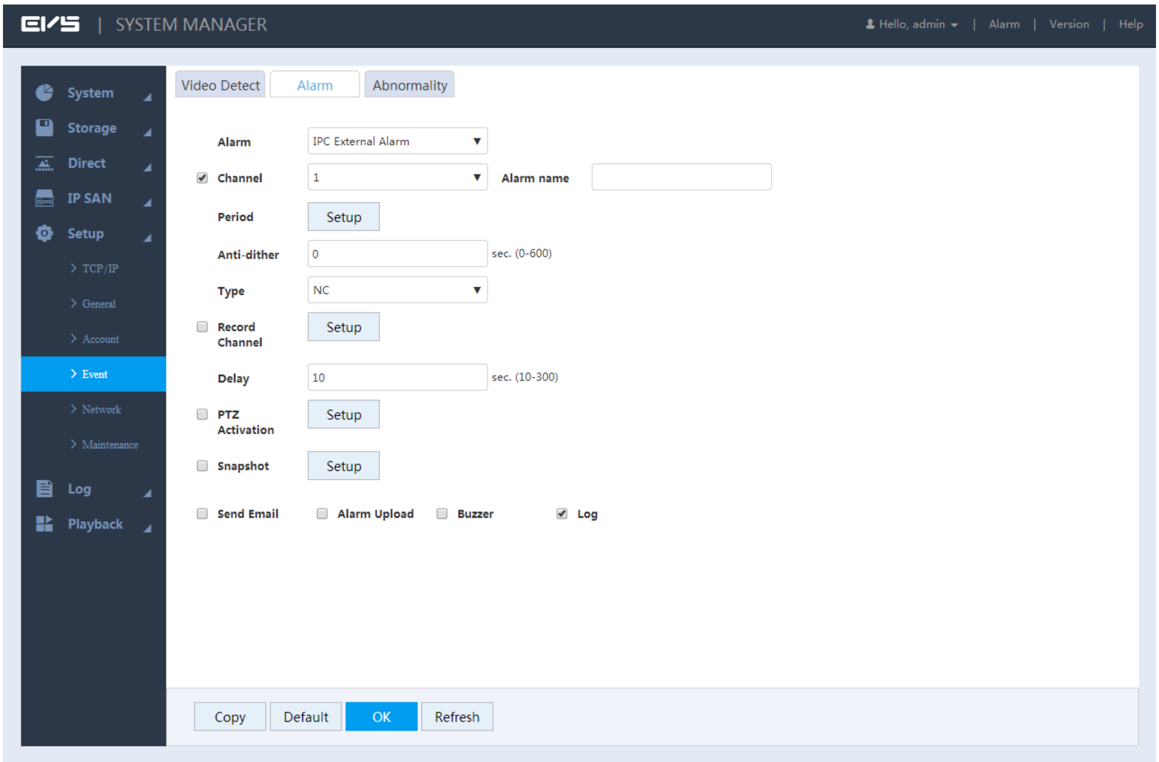
3.8.4.2 Alarm Settings

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

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

The **Alarm** interface is displayed. See Figure 3-74.

Figure 3-74 Alarm settings



Alarm: IPC External Alarm

☑ Channel: 1 Alarm name:

Period: Setup

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

Type: NC

□ Record Channel: Setup

Delay: 10 sec. (10-300)

□ PTZ Activation: Setup

□ Snapshot: Setup

□ Send Email □ Alarm Upload □ Buzzer ☑ Log

Step 2 Select/Enter the parameters. For details, see Table 3-26.

Table 3-26 Description of alarm setting parameters

Parameter	Description
Alarm	Select the alarm setting type: ● Local alarm: Connect alarm device to the alarm input port of the EVS device. When alarm signal is transmitted to the EVS device, the system executes the alarm linkage. ● IPC external alarm: When the IPC external alarm device is triggered, it uploads alarm signal to the EVS device through the network and the system executes alarm linkage. ● IPC off-line alarm: When the network connection between EVS device and IPC are broken, the system executes the alarm linkage. NOTE Only High-End 24-HDD Single-Controller supports local alarm.
Channel	Select the channel for video detect in the drop-down box.

Parameter	Description
Period	Alarm linkage takes effect only in the set time period. For details, see "Period Settings."
Anti-dither	Only record alarm event for once during the set anti-dither time period.
Type	Select the type of the remote device, including NO and NC.
Record Channel	Select the check box, click **Setup** on the right side, and then select the channels as needed (multiple choices available). When an alarm occurs, the EVS device links to the selected channel for video recording. 📖 NOTE Firstly you need to open the motion detection and auto record functions. For details, see "3.10.4.1 Record Plan Settings" and "3.10.5 Record Control."
Post Record	At the end of the alarm, the record is extended for a period of time. The extended time range is 10 seconds to 300 seconds.
Alarm Out	Connect the alarm device to the alarm out port (like light, siren). The device transmits alarm information to the alarm device when an alarm occurs. 📖 NOTE Only High-End 24-HDD Single-Controller supports this function.
Delay	At the end of the alarm information, the alarm extends for a period of time. The extended time range is 0-300 seconds. 📖 NOTE Only High-End 24-HDD Single-Controller supports this function.
PTZ Activation	Select the check box, click the **Setup** on 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. 📖 NOTE ● Motion detection only supports PTZ pre-set point linkage. ● The corresponding PTZ actions shall be set first. For details, see "3.6.1.3 PTZ Console."
Snapshot	Select the check box, click the **Setup** on the right side, and then select the channel. When an alarm occurs, the device links to the selected channel for snapshot. 📖 NOTE Firstly you need to open the motion detect snapshot and auto snapshot functions. For details, see "3.10.4.2 Snapshot Plan Settings" and "3.10.5 Record Control."
Prompt	Select the check box. When an alarm occurs, alarm information pops up on the screen of the local host.
Send Email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. 📖 NOTE You need to set the Email first. For details, see "3.8.5.2.2 Email Settings."
Alarm Upload	Select the check box. The device uploads the alarm signal to the network (including alarm center) when an alarm occurs. 📖 NOTE Only some models support this function. See the actual situation.

Parameter	Description
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.

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

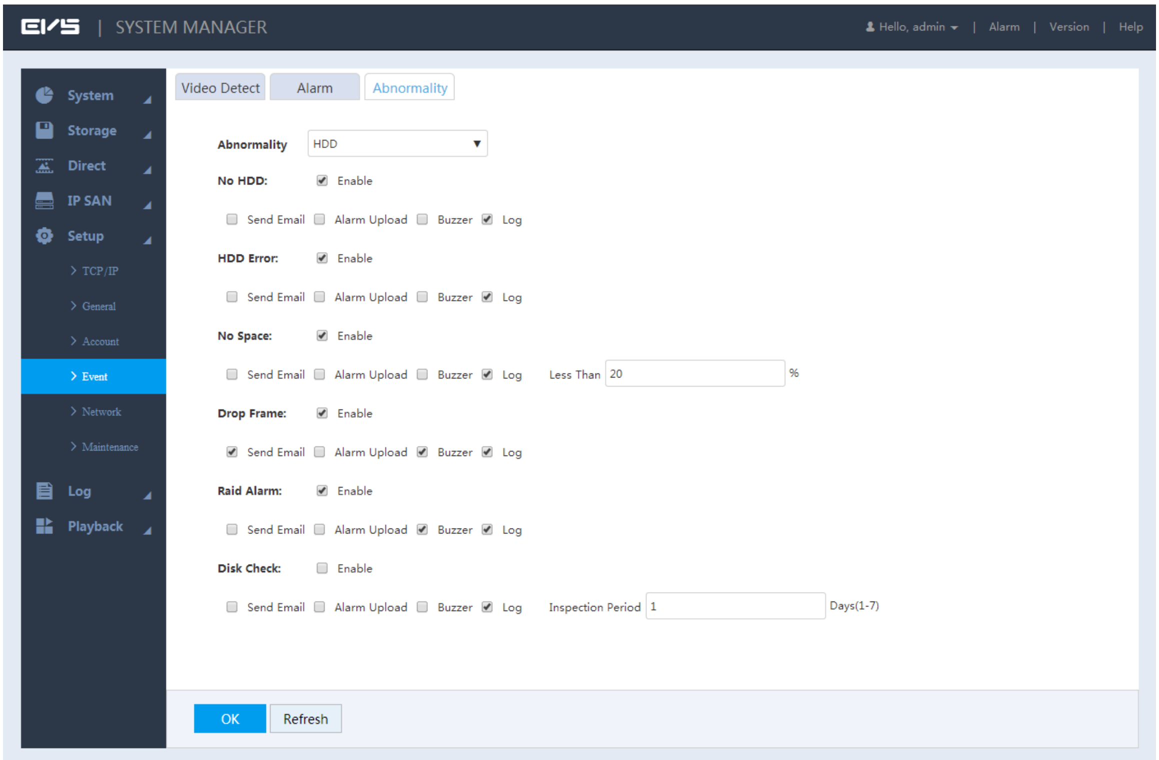
3.8.4.3 Handling Abnormality

Set the alarm mode of abnormal events. When abnormal events occur during the operation of the EVS device, the system executes the alarm linkage.

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

The Abnormality interface is displayed. See Figure 3-75.

Figure 3-75 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 Select/Enter the parameters. For details, see Table 3-27.

Table 3-27 Description of abnormality handling parameters

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. ● **Network**: Configure the type and alarm way of network abnormal events, including off-line alarm, IP conflict and MAC conflict. ● **Shared service**: Configure the type and alarm way of shared service abnormal events, including shared services and storage pool abnormality. ● **Other**: Configure the type and alarm way of other abnormal events, including fan, temperature and redundant power. NOTE The **Other** abnormal events of dual-control devices also support the alarm of abnormal version.

Parameter	Description
Enable	Select the check box to enable the corresponding abnormal event.
Alarm out	Connect the alarm device to the alarm out port (like light, siren). The device transmits alarm information to the alarm device when an alarm occurs. NOTE Only High-End 24-HDD Single-Controller supports this function.
Delay	At the end of the alarm information, the alarm extends for a period of time. The extended time range is 0-300 seconds. NOTE Only High-End 24-HDD Single-Controller supports this function.
Space	When the actual remaining space of the hard disk is lower than the set value, the system generates alarm. NOTE Only **No Space** events support this function.
Inspection period	The time period of disk inspection. The range is 1-7 days. NOTE Only **Disk Check** events support this function.
Prompt	Select the check box. When an alarm occurs, alarm information pops up on the screen of the local host.
Send email	Select the check box and the device sends an email to the assigned email box when an alarm occurs. NOTE You need to set the Email first. For details, see "3.8.5.2.2 Email Settings."
Alarm upload	Select the check box. The device uploads the alarm signal to the network (including alarm center) when an alarm occurs. NOTE Only some models support this function. See the actual situation.
Buzzer	Select the check box. The buzzer bleats when an alarm occurs.
Log	Select the check box. When the alarm occurs, the device records the alarm information into the log.

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

3.8.5 Network Application

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

3.8.5.1 General Settings

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

3.8.5.1.1 Connection Port

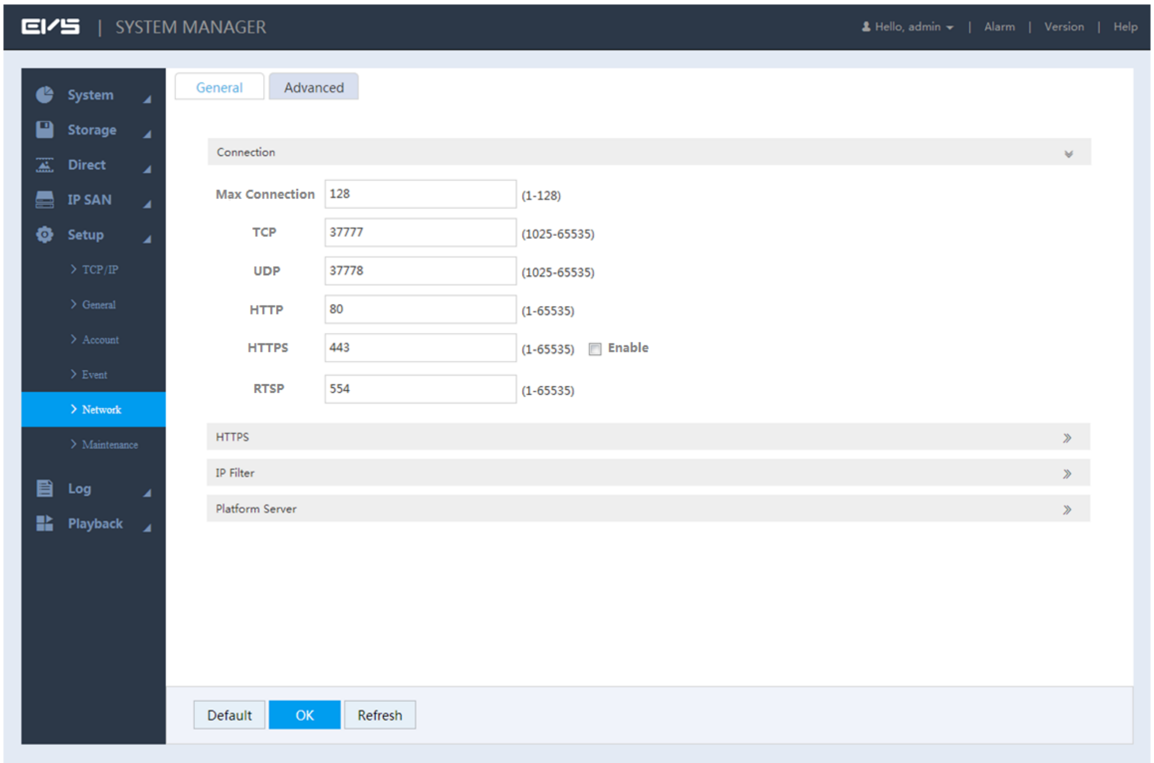
Set the maximum number of connection ports and their respective port number when multiple clients (such as Web client and platform client) visit the EVS device at the same time.

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

Step 2 Click » corresponding to the connection.

The **Connection** interface is displayed. See Figure 3-76.

Figure 3-76



Connection

Max Connection 128 (1-128)

TCP 37777 (1025-65535)

UDP 37778 (1025-65535)

HTTP 80 (1-65535)

HTTPS 443 (1-65535) □ Enable

RTSP 554 (1-65535)

HTTPS

IP Filter

Platform Server

Step 3 Select/Enter the parameters. For details, see Table 3-28.

NOTE

Except the max connection, if you change the settings of other parameters, they can come into effect only after restarting the EVS device.

Table 3-28 Description of port parameters

Parameter	Description
Max connection	The max number of clients logging in the device at the same time (such as Web client and platform client). It ranges from 0 to 128(default).
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 login through the browser.
HTTPS port	HTTPS communication port. Select the **Enable** check box and set the port according to the actual needs. The default value is 443. NOTE The change of HTTPS comes into effect only after device restart. Be careful to change it.

Parameter	Description
RSTP port	● The default value is 554 and you might not enter this item when using the default. ● When real-time monitoring RTSP media services, you shall clarify the channel number and stream type in URL. Provide user name and password if required. URL format: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 ● User name: Such as admin. ● Password: Such as admin. ● Ip: Such as 10.7.8.122. ● Port: The default value is 554. Skip it if using the default. ● Channel: Start from 1. For example, select 2 for channel 2. ● Subtype: stream type. Main stream is 0 (subtype=0) and sub stream is 1 (subtyoe=1). For example: Request the sub stream of channel 2. URL see below: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1 If verification is not required, you do not need to specify the user name and password. Format see below: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0

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

3.8.5.1.2 HTTPS

In the HTTPS interface, by creating server certificate or downloading root certificate and setting the port number, it enables PC to log in properly through HTTPS, providing guarantee for user information and device security through the reliable and stable technologies.

Preparation

Only after you have enabled the HTTPS port, you can create server certificate and download root certificate. For detailed operations to enable HTTPS, see "3.8.5.1.1 Connection Port."

Create Server Certificate

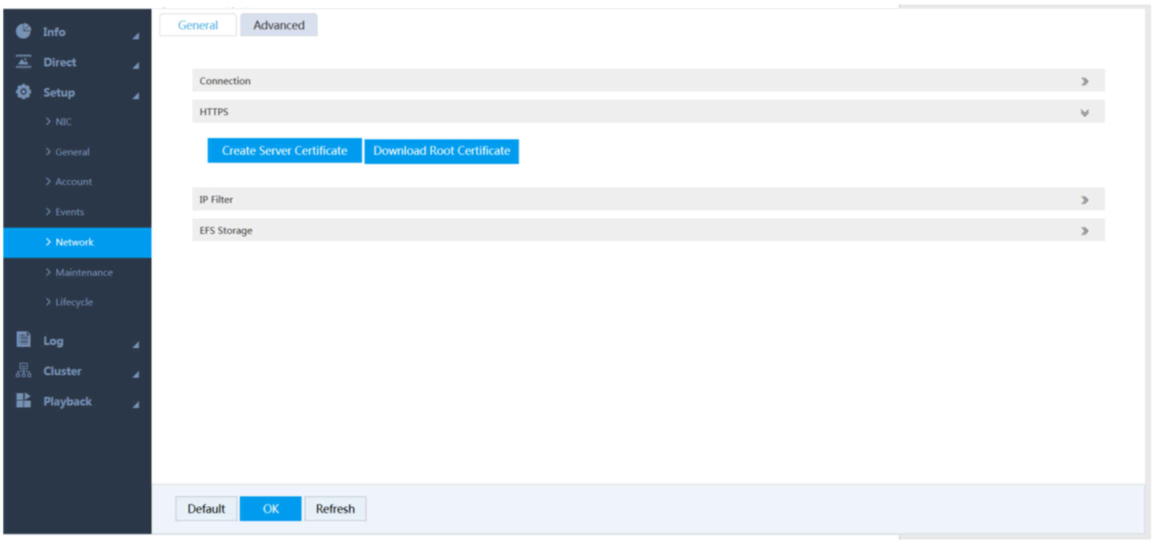
If you use this function for the first time or you changed the IP address, you need to create the server certificate.

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

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

The **HTTPS** port interface is displayed. See Figure 3-77.

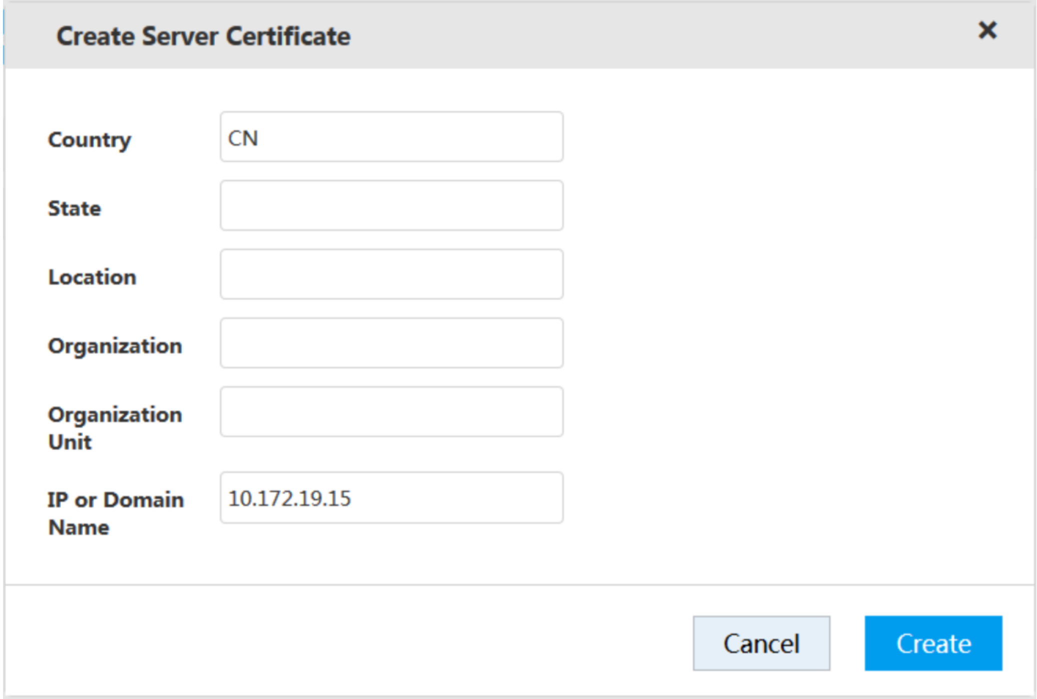
Figure 3-77 HTTPS



Step 3 Click **Create Server Certificate**.

The **Create Server Certificate** interface is displayed. See Figure 3-78.

Figure 3-78 Creating server certificate


Create Server Certificate

Country	CN
State	
Location	
Organization	
Organization Unit	
IP or Domain Name	10.172.19.15

Step 4 Enter the information like country and state.

NOTE

IP or Domain Name shall be the same as the device IP and domain name.

Step 5 Click Create.

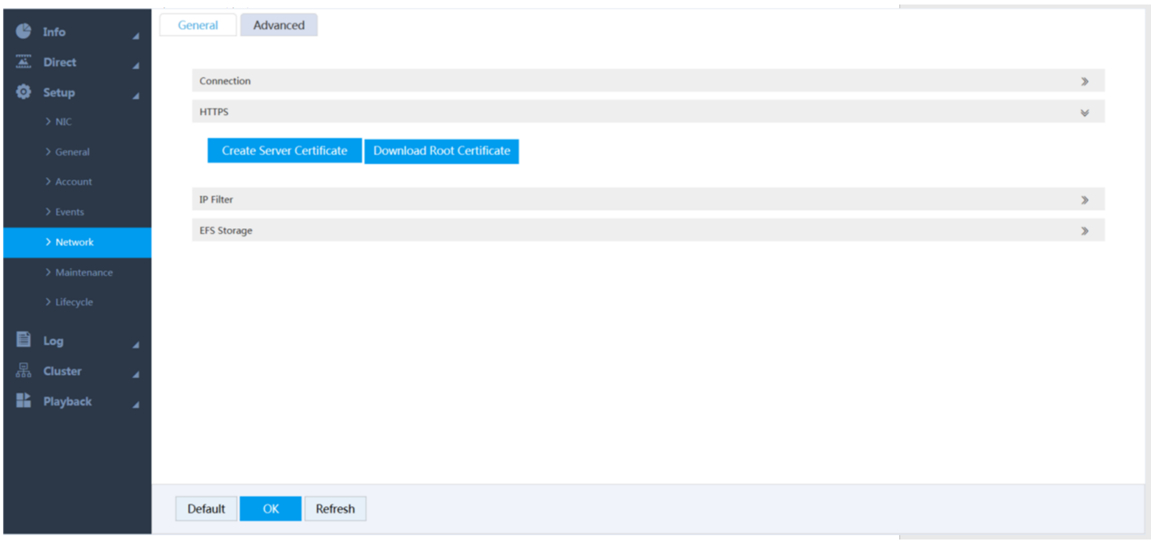
The system prompts **Creation Succeed** when it is done successfully.

Downloading Root Certificate

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

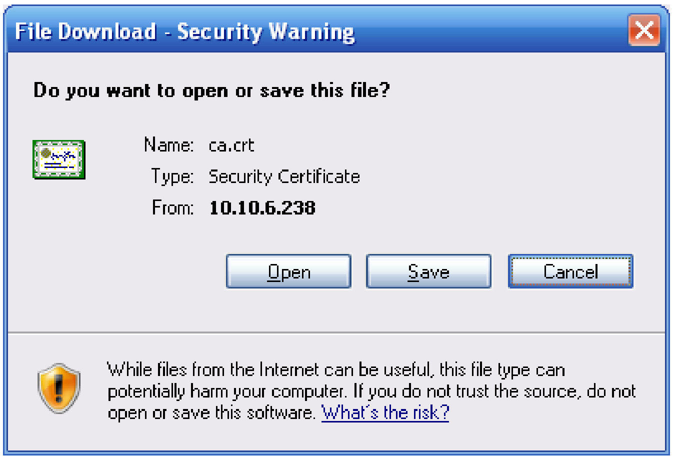
The **HTTPS** port interface is displayed. See Figure 3-79.

Figure 3-79 HTTPS



Step 2 Click **Download Root Certificate**, and the **File Download-Security Warning** dialogue box pops up. See Figure 3-80.

Figure 3-80 File Download



Do you want to open or save this file?

Name: ca.crt

Type: Security Certificate

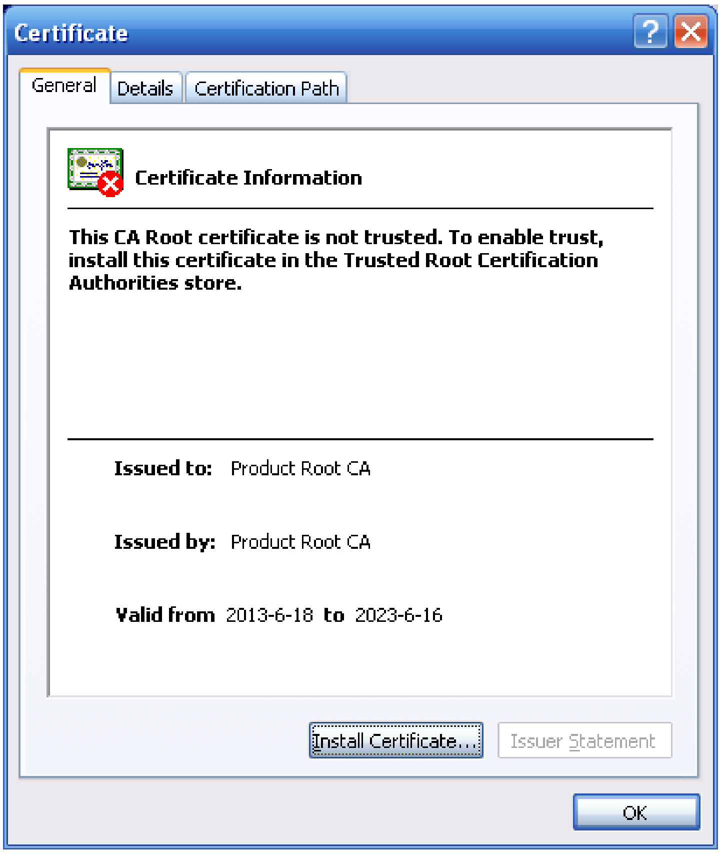
From: **10.10.6.238**

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**.

The **Certificate Information** interface is displayed. See Figure 3-81.

Figure 3-81 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

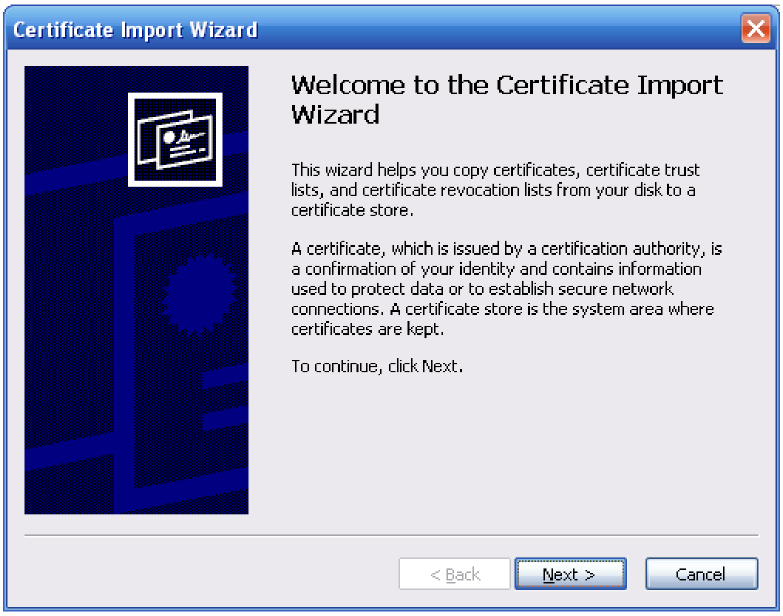
Issued by: Product Root CA

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

Step 4 Click **Install Certificate**.

The **Certificate Import Wizard** is displayed. See Figure 3-82.

Figure 3-82 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.

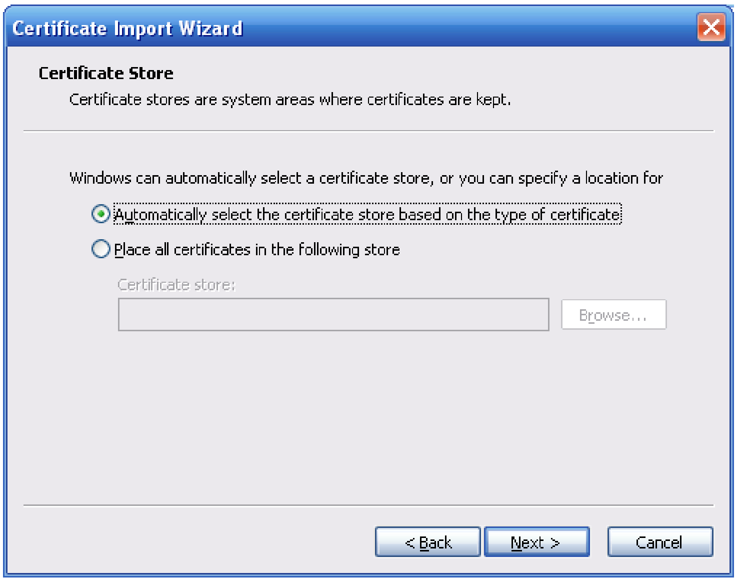
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Step 5 Click **Next**.

The **Certificate Store** interface is displayed. See Figure 3-83.

Figure 3-83 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

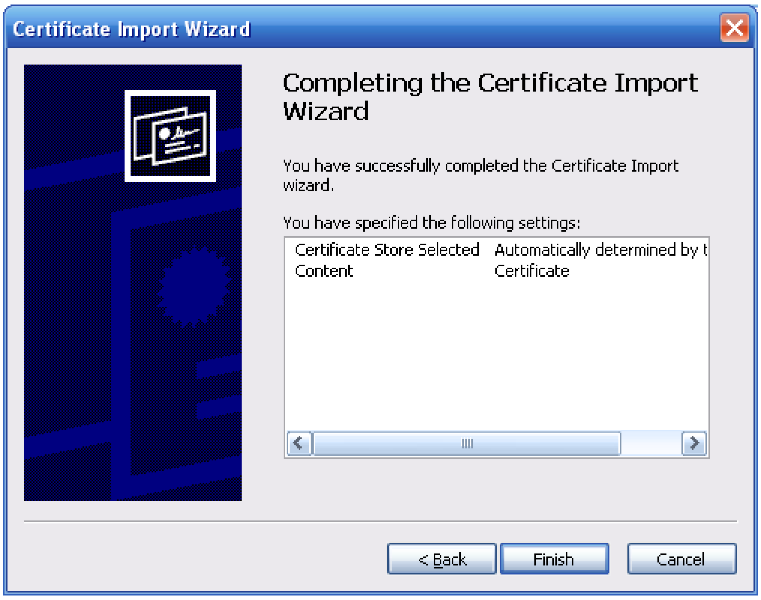
○ Place all certificates in the following store

Certificate store:

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

The **Completing the Certificate Import Wizard** interface is displayed. See Figure 3-84.

Figure 3-84 Completing certificate import


Certificate Import Wizard

Completing the Certificate Import Wizard

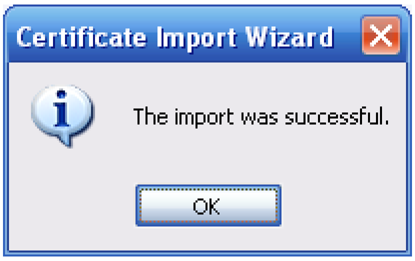
You have successfully completed the Certificate Import wizard.

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**. See Figure 3-85.

Figure 3-85 Success


Certificate Import Wizard

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 "3.8.5.1.1 Connection Port."

After the settings, enter https://xx.xx.xx.xx:port into the browser and you can log in EVS device via HTTPS.

NOTE

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

3.8.5.1.3 IP Authority

Set the IP hosts (here refers to devices with IP address) accessing NVR device. After the setting, only IP hosts in the white-list can log in Web and those in the black-list will be blocked, thus enhancing the security of EVS network and data.

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

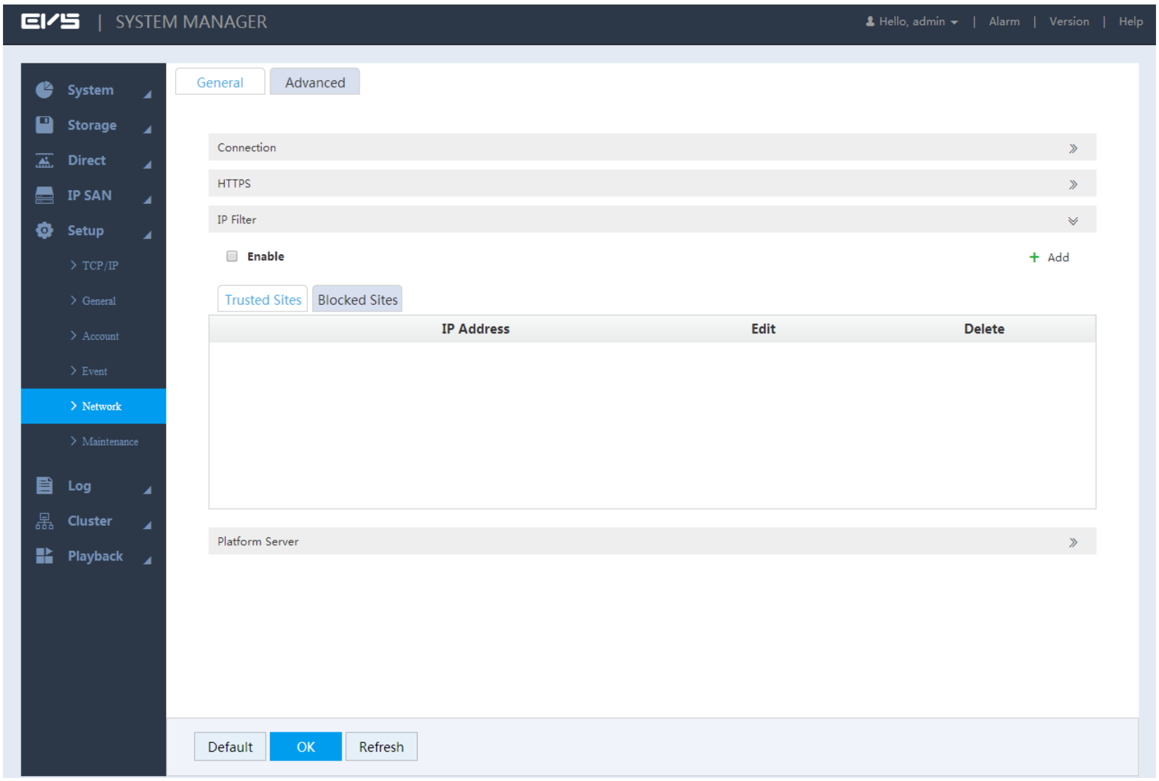
Step 2 Click » corresponding to **IP Filter**.

The **IP Filter** interface is displayed.

Step 3 Select the **Enable** check box to open this function.

The tabs of **Trusted Sites** and **Blocked Sites** are displayed. See Figure 3-86.

Figure 3-86 IP Authority



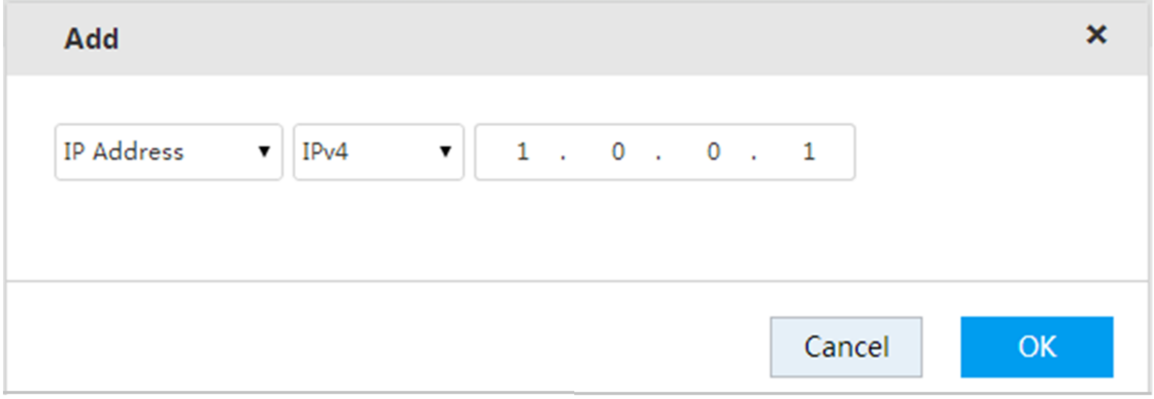
Step 4 Add trusted sites or blocked sites.

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

2) Click + .

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

Figure 3-87 Adding trusted sites/blocked sites


Add

IP Address ▼ IPv4 ▼ 1 . 0 . 0 . 1

Cancel OK

3) Select/Enter the parameters. For details, see Table 3-29.

Table 3-29 Description of IP filter parameters

Parameter	Description
IP Address	Click the drop-down box to select the way to add trusted/blocked sites. ● IP address: Enter the IP address you want to add to the trusted or blocked sites. ● IP Segment: Enter the IP segment range you want to add to the trusted/blocked sites. You can add multiple hosts at the same time. ● MAC address: Enter the MAC address you want to add to the trusted sites. NOTE The system does not support to add blocked sites via MAC address.
IPv6	Click the drop-down box to select the IP address protocol. ● IPv4: IP address adopts IPv4 format, like 192.168.5.10. ● IPv6: IP address adopts IPv6 format, like aa:aa:aa:aa:aa:aa:aa:aa.

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

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

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

3.8.5.1.4 Platform Server

When the platform disconnects with the EVS device and the pictures in the EVS 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

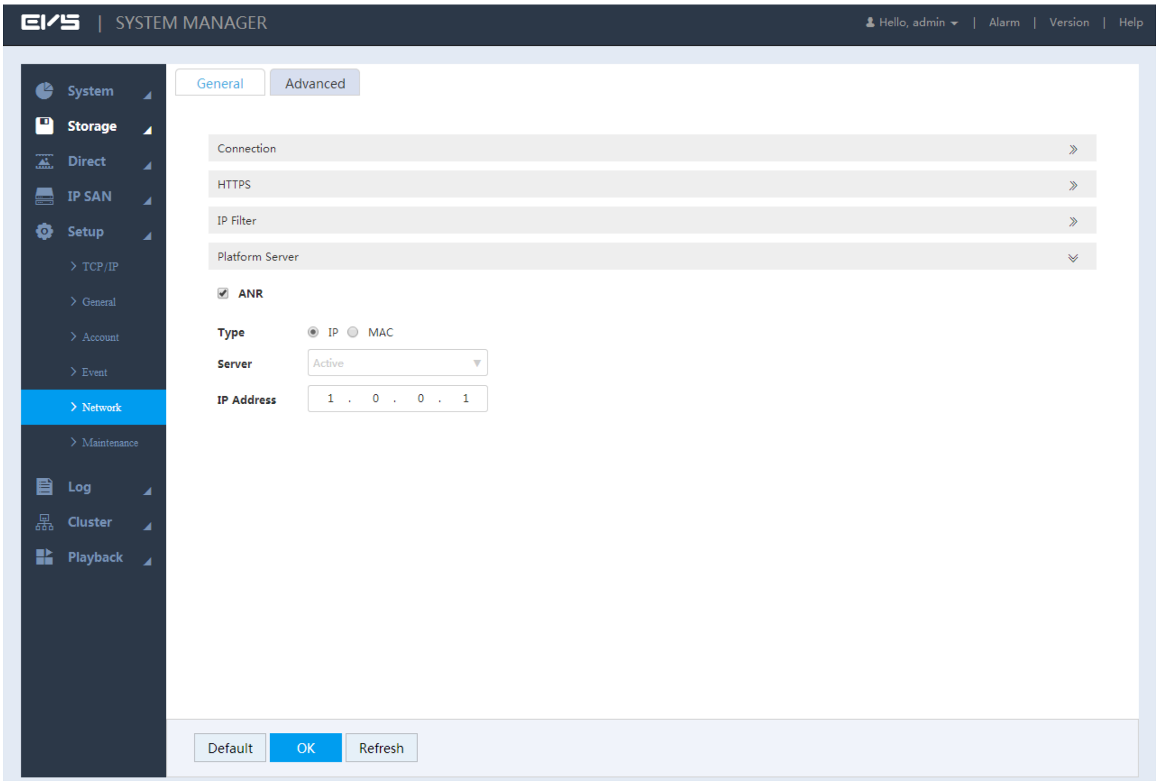
- Have set one or several disks as the image direct storage disk. For details, see "3.10.1 Storage Device."
- Have added ITC or Smart IPC device. For details, see "3.5 Adding Remote Device."
- Have enabled the image direct storage function. For details, see "3.10.5 Record Control."

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

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

The **Platform Server** interface is displayed. See Figure 3-88.

Figure 3-88 Platform server



☑ ANR

Type ● IP ○ MAC

Server Active

IP Address 1 . 0 . 0 . 1

Step 3 Select/Enter the parameters. For details, see Table 3-30.

Table 3-30 Description of platform server parameters

Parameter	Description
ANR	Select the check box to enable the function. After the network is reconnected between the platform server and EVS device, the EVS device automatically uploads the directly stored images during the network broken to the platform server, so as to keep the integrity of the images.
Type	Select the address type of the platform server, including IP address and MAC address.
Server	Select the registration mode of EVS 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.

3.8.5.2 Advanced Settings

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

3.8.5.2.1 DDNS

After setting the DDNS (Dynamic Domain Name Server) parameters, 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 remote access the device.

Preparation

Before the configuration, you need to confirm the DNS server type that the EVS device supports and you have registered on the DDNS service provider website and logged in on the WAN PC.

NOTE

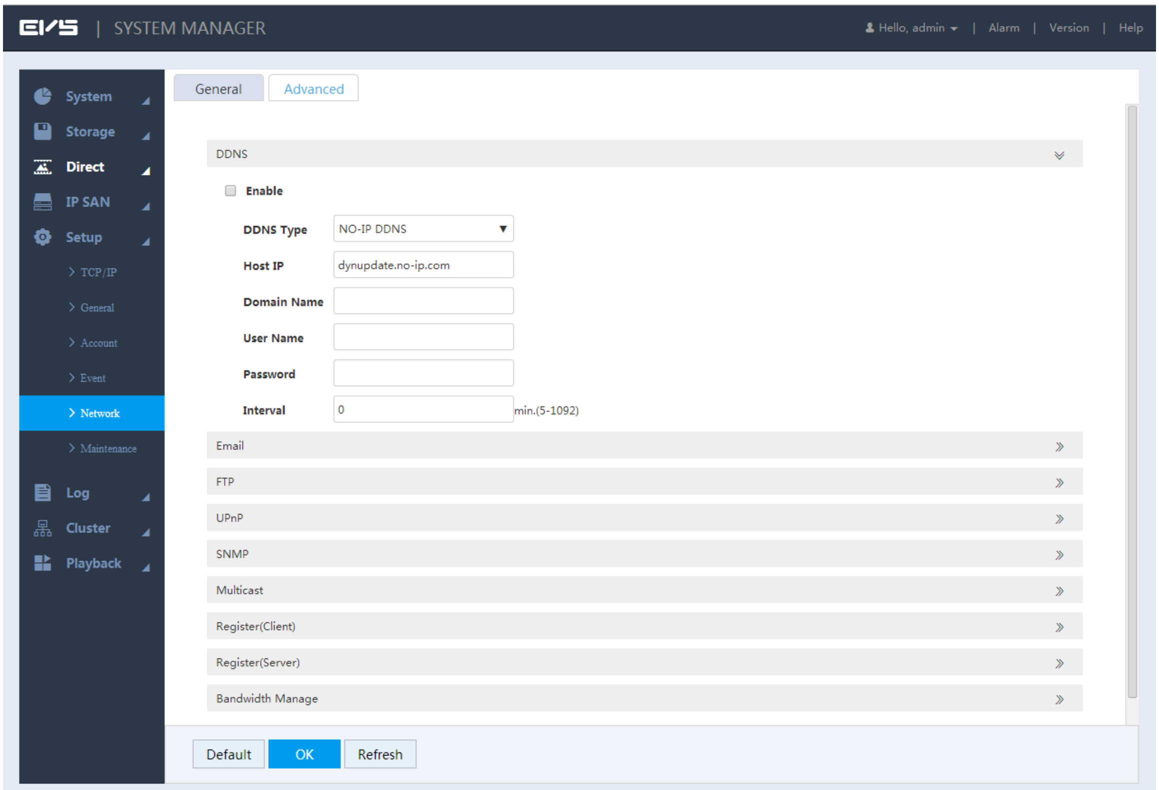
After registering successfully on the DDNS website and logging in, the user can view all the information of the connected devices under this registered user.

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

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

The **DDNS** interface is displayed. See Figure 3-89.

Figure 3-89 DDNS



DDNS

□ Enable

DDNS Type: NO-IP DDNS

Host IP: dynupdate.no-ip.com

Domain Name:

User Name:

Password:

Interval: 0 min.(5-1092)

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

Step 4 Select/Enter the parameters. For details, see Table 3-31.

Table 3-31 Description of DDNS parameters

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

Parameter	Description
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 PC browser and press Enter key.

If the device Web interface is displayed, the configuration is successful. If it is not shown, the configuration failed and you need to check the reason.

3.8.5.2.2 Email Settings

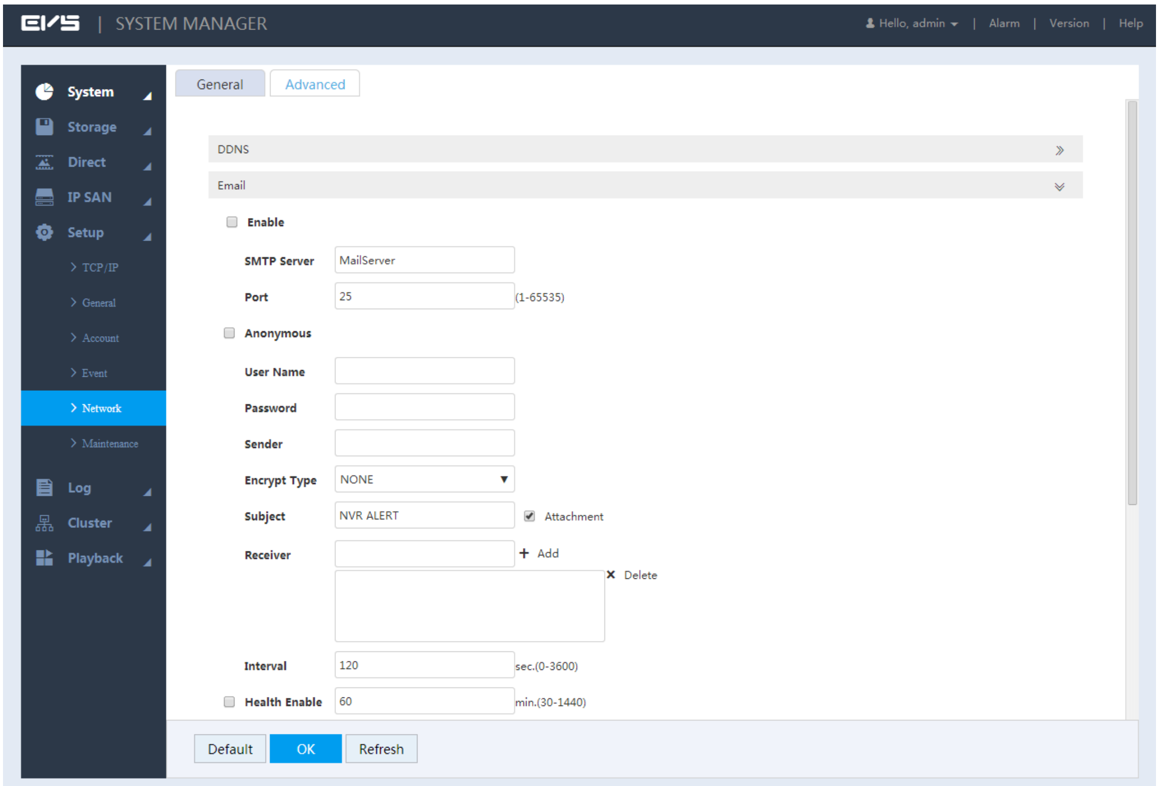
After enabling the email alarm linkage, the EVS device automatically sends email to the user when the corresponding alarm occurs.

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

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

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

Figure 3-90 Email settings



☐ Enable

SMTP Server: MailServer

Port: 25 (1-65535)

☐ Anonymous

User Name:

Password:

Sender:

Encrypt Type: NONE

Subject: NVR ALERT ☑ Attachment

Receiver: + Add ✕ Delete

Interval: 120 sec.(0-3600)

☐ Health Enable: 60 min.(30-1440)

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

Step 4 Select/Enter the parameters. For details, see Table 3-32.

Table 3-32 Description of Email setting parameters

Parameter	Description
SMTP Server	Enter the server address of SMTP (Simple Mail Transfer Protocol). For details, see Table 3-33.
Port	Enter the SMTP server port number. For details, see Table 3-33.
Anonymous	Select the check box to allow anonymous login.
User Name	Enter the user name and password of the SMTP server. For details, see Table 3-33.
Password	
Sender	Enter the Email address of the sender.

Parameter	Description
Encryption Type	Select the encryption type, including NONE, SSL (Secure Sockets Layer) and TLS (Transport Layer Security). For details, see Table 3-33.
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 an receiver. You can set three receivers at most. NOTE ● It supports to add no more than three receiver Email addresses at the same time. Use ":" to separate the addresses. ● Select the added receiver address and click **Delete** to delete the receiver.
Interval	After entering the **interval**, when the alarm or abnormal event is triggered, instead of sending an email immediately according the triggering of the alarm signal, the system will send an email according to the time interval of the previous similar events. NOTE ● By entering the **Interval**, it can avoid frequent abnormal alarms or evens which produces a large number of Emails and leads to large stress of the Email server. ● You can enter 0-3,600 seconds in the **Interval**. Zero means no time interval before sending the Email.
Health Enable	Select this check box and enter the time interval. The system sends Email test information according to the set interval to check if the Email connection is successful. NOTE You can enter 30-1,440 minutes in the health Email interval.
Email Test	Test if the email function is normal. The Email box can receive test emails if the configuration is correct. NOTE Before the Email test, you need to click **OK** to save the Email configuration.

Table 3-33 Parameter reference for common email configuration

Email Type	SMTP Server	Encryption Mode	Port	Description
QQ	smtp.qq.com	SSL	465	● You cannot select **NONE** for the encryption type. ● The mailbox shall open SMTP service. ● The password must be the authorized code. QQ and Email login passwords are invalid. NOTE Authorized code is obtained when the mailbox enables SMTP service.
		TLS	587	
163	smtp.163.com	SSL	465/994	● Mailbox shall enable SMTP service. ● The password must be the
		TLS	25	

Email Type	SMTP Server	Encryption Mode	Port	Description
		NONE	25	authorized code. QQ and Email login passwords are invalid. NOTE Authorized code is obtained when the mailbox enables SMTP service.
Sina	smtp.sina.com	SSL	465	Mailbox shall enable SMTP service.
		NONE	25	
126	smtp.126.com	NONE	25	Mailbox shall enable SMTP service.

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

3.8.5.2.3 FTP

Set the FTP(File Transfer Protocol) server and you can store the records and images in the FTP server.

Preparation

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

NOTE

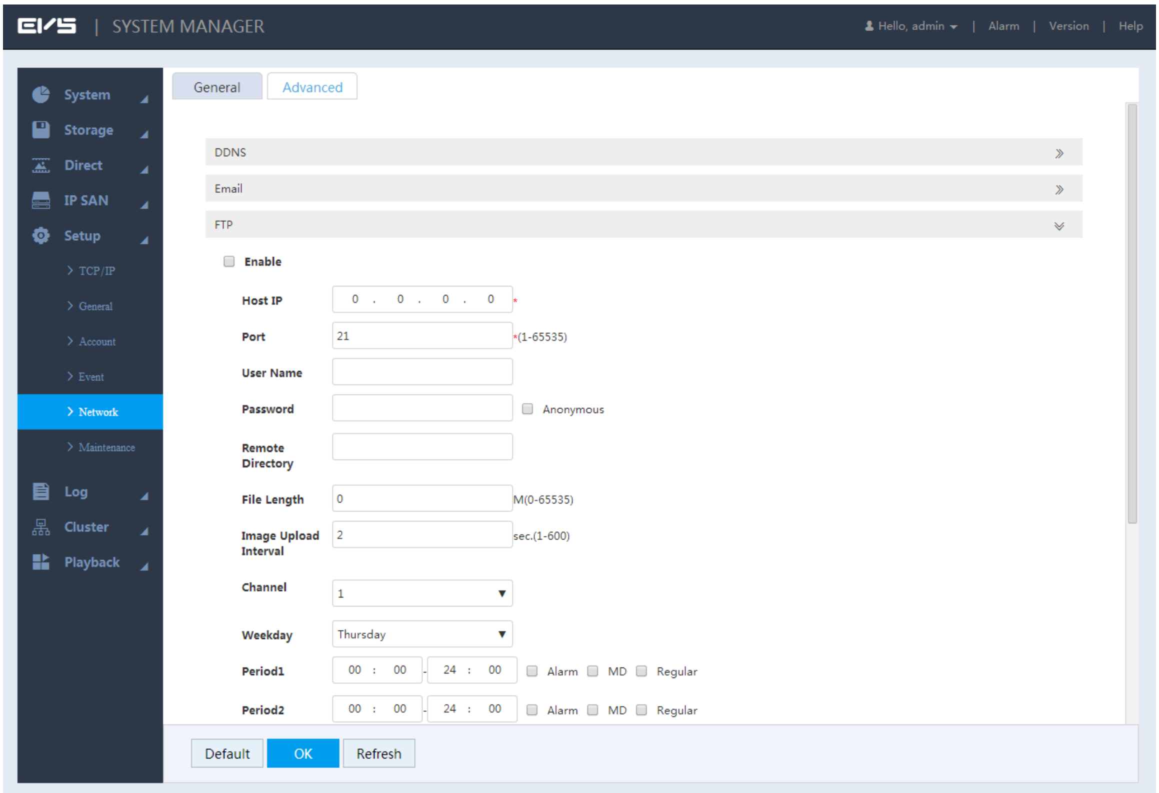
When creating a FTP user, you need to set the write permission of FTP folder. Otherwise, you cannot upload the file.

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

Step 2 Click » corresponding to FTP.

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

Figure 3-91 FTP



□ Enable

Host IP 0 . 0 . 0 . 0 *

Port 21 *(1-65535)

User Name

Password □ Anonymous

Remote Directory

File Length 0 M(0-65535)

Image Upload Interval 2 sec.(1-600)

Channel 1

Weekday Thursday

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

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

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

Step 4 Select/Enter the parameters. For details, see Table 3-34.

Table 3-34 Description of FTP parameters

Parameter	Description
Host IP	Enter the IP address of the host which has installed the FTP service.
Port	Enter the port number to connect FTP server. The default number is 21.
User Name	The username and password to access FTP server. NOTE Select the **Anonymous** check box and it supports to access FTP server in anonymous way.
Password	
Remote Directory	Create folders according to the rules in the root directory of the 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 to zero, it uploads the whole record file.
Image Upload Interval	Enter the time interval to upload images. ● When the image upload interval is larger than the snapshot frequency, the system uploads the latest image. For example: when the image upload interval is five seconds and the snapshot frequency is two seconds per image, the system uploads a latest snapshot image every five seconds. ● When the image upload interval is smaller than the snapshot frequency, the system uploads images according to the snapshot frequency. For example, when the upload interval is five seconds and the snapshot frequency is ten seconds per image, the system uploads an image every ten seconds. NOTE You can modify the **Snapshot Frequency**. For details, see "3.10.2.3.2 Image Stream Settings."
Channel	Select the channel to upload records. NOTE **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 if the FTP connection is successful. ● Succeeded: The system prompts that FTP test succeeded. ● Failed: The system prompts that FTP test failed. You need to check if the network connection or configuration is correct.

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

3.8.5.2.4 UPnP

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

Preparation

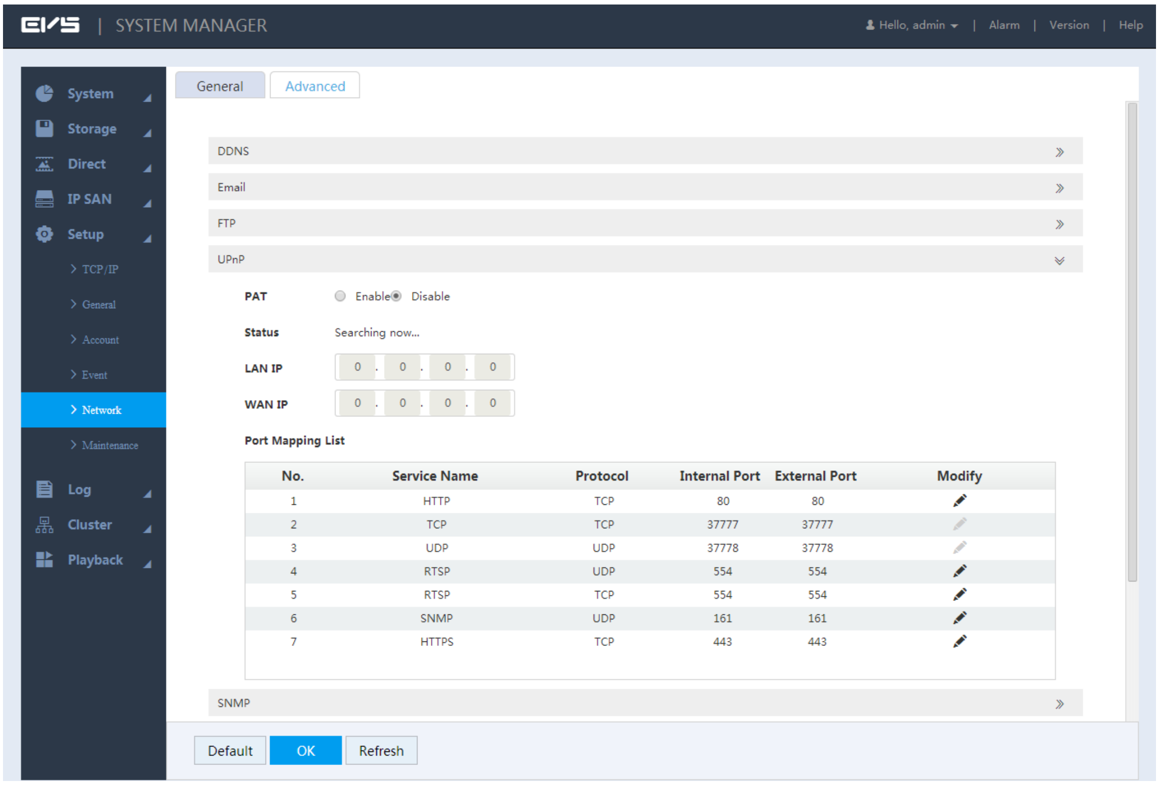
- Log in the router and set the IP address of the WAN port to access external network.
- Enable the UPnP function of the router.
- Connect the EVS device to the LAN port of the router to access private network.
- Set the IP address of the EVS device to the private IP of the router (e.g. 192.168.1.101). For details, see "3.8.1.1 IP Settings."

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

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

THE **UPnP** interface is displayed. See Figure 3-92.

Figure 3-92 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	HTTP	TCP	80	80	✎
2	TCP	TCP	37777	37777	✎
3	UDP	UDP	37778	37778	✎
4	RTSP	UDP	554	554	✎
5	RTSP	TCP	554	554	✎
6	SNMP	UDP	161	161	✎
7	HTTPS	TCP	443	443	✎

Step 3 Select/Enter the parameters. For details, see Table 3-35.

Table 3-35 Description of UPnP parameters

Parameter	Description
PAT	Select the **Enable** check box to open the UPnP function.
Status	Display the UPnP status. ● Display **Disabled** when the mapping failed. ● Display **Enabled** when the mapping succeeded.

Parameter	Description
LAN IP	LAN port address of the router. After mapping successfully, the system automatically obtains the 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. NOTE ● When setting the external ports of the router mapping ports, use ports from 1,024 to 5,000 and avoid using the known ports from 1 to 255 and system ports from 256 to 1023, so as 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 doing the port mapping, make sure that the mapped 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.

3.8.5.2.5 SNMP

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

Preparation

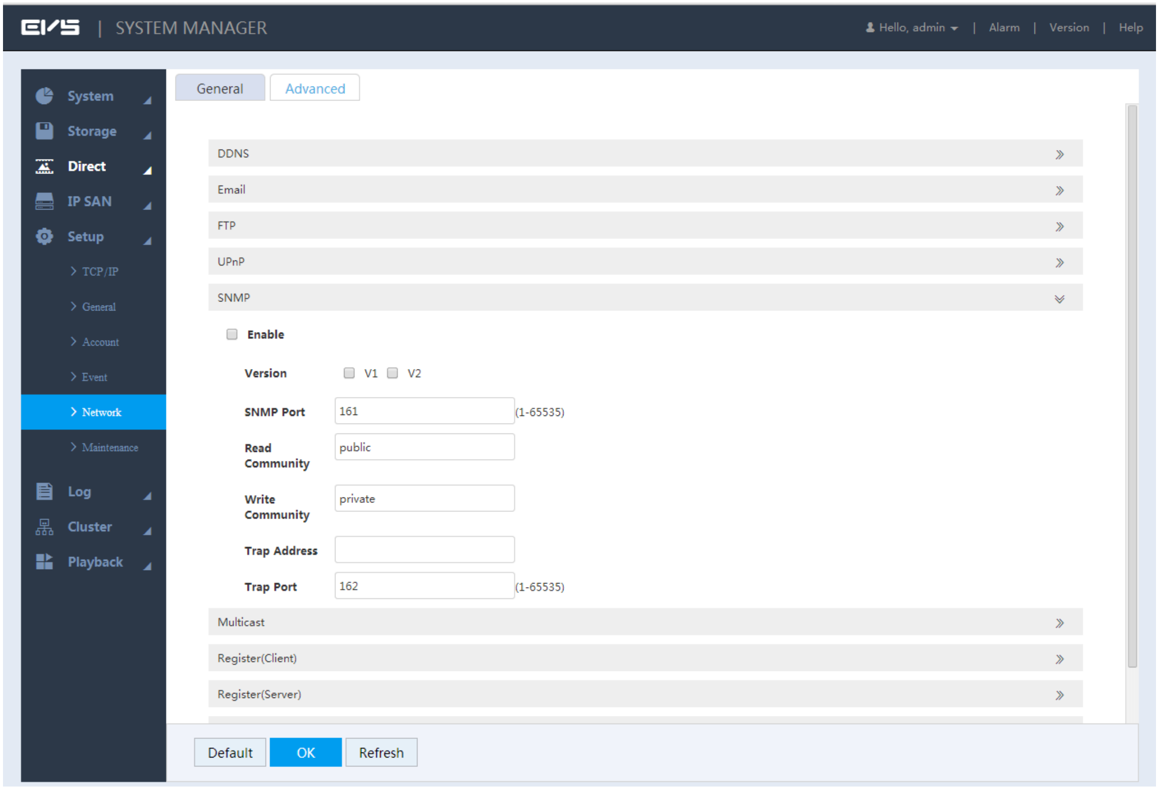
- Have installed the SNMP monitoring and management tools, such as MIB Builder and MG-SOFT MIB Browser.
- Have got the MIB files corresponding to the current version from the technical supporters.

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

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

The **SNMP** interface is displayed. See Figure 3-93.

Figure 3-93 SNMP



□ Enable

Version □ V1 □ V2

SNMP Port 161 (1-65535)

Read Community public

Write Community private

Trap Address

Trap Port 162 (1-65535)

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

Step 4 Select/Enter the parameters. For details, see Table 3-36.

Table 3-36 Description of 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 the PC that has installed MG-SOFT MIB Browser. It is the target address to which the agent program sends traps.
Trap Port	It is the target port to which the agent program sends traps. The default value is 162.

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

Step 6 (Optional) View the EVS device information.

1) Run MIB Builder and MG-SOFT MIB Browser in 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 EVS device you need to manage into MG-SOFT MIB Browser, and then select the version number to search.
5) Expand the tree list displayed on the MG-SOFT MIB Browser to get the configuration information of the EVS device, such as the video/audio channel number and program version.

3.8.5.2.6 Multicast Settings

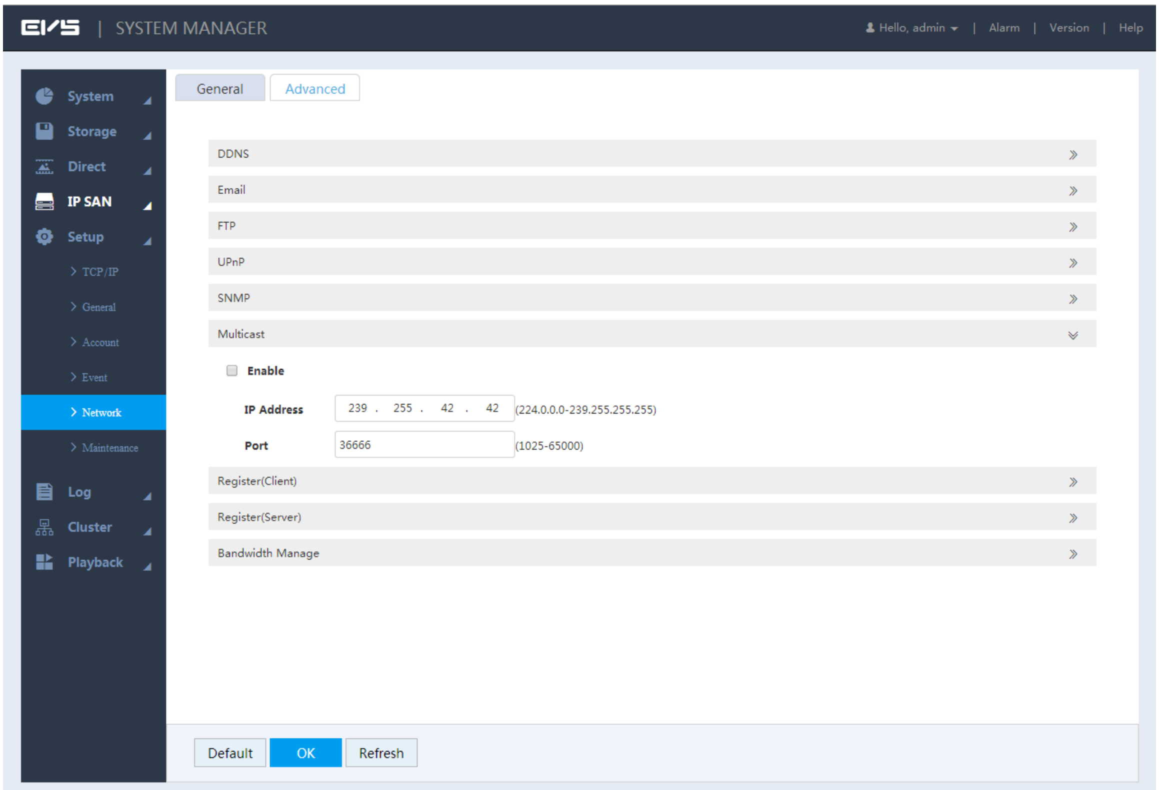
When multiple users want to preview video of the same channel at the same time, they might be unable to preview due to the bandwidth limitation. You can set a multicast IP for the EVS device (224.0.0.0-238.255.255.255) and the users can solve this problem by accessing with the multicast protocol.

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

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

The **Multicast** interface is displayed. See Figure 3-94.

Figure 3-94 Multicast



□ Enable

IP Address 239 . 255 . 42 . 42 (224.0.0.0-239.255.255.255)

Port 36666 (1025-65000)

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

Step 4 Enter the parameters. For details, see Table 3-37.

Table 3-37 Description of multicast parameters

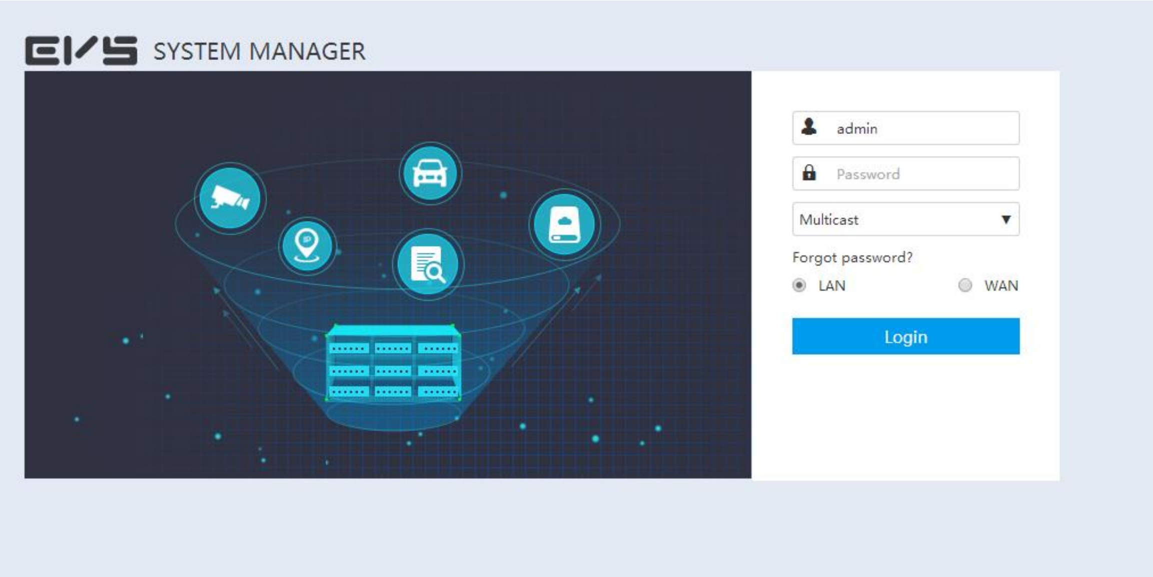
Parameter	Description
IP Address	Enter the multicast IP address to access the EVS device.
Port	Enter the port number to access the EVS device. The default value is 36666.

Step 5 Click OK to save the configuration.

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

Enter the login interface of the EVS device and select Multicast as the login type. See Figure 3-95. After logging in, the EVS device automatically obtains the multicast address and joins the multicast group, so that the monitoring screen can be viewed through the multicast form in real time.

Figure 3-95 Multicast



EVS SYSTEM MANAGER

admin

Password

Multicast ▼

Forgot password?

● LAN ○ WAN

Login

3.8.5.2.7 Active Register (Client)

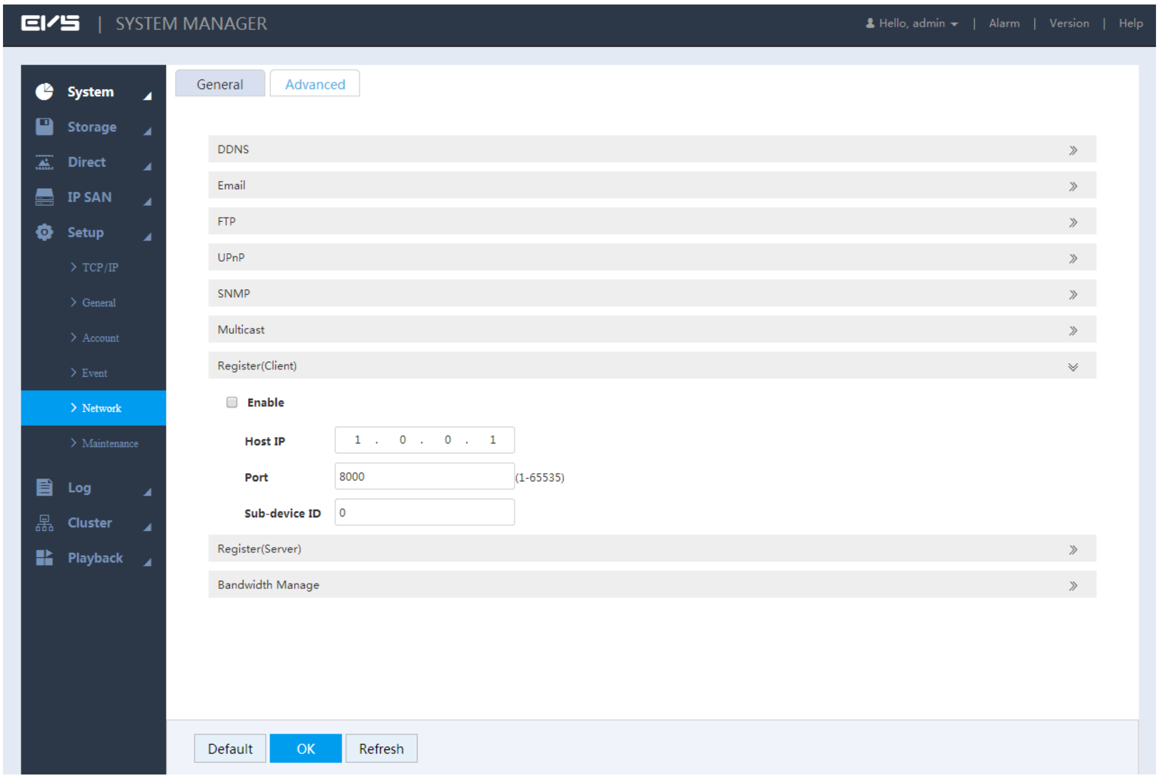
After accessing the external network, the EVS device actively reports the current position to the specified server, so as to facilitate the server to access the EVS device for preview and surveillance.

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

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

The **Register (Client)** interface is displayed. See Figure 3-96.

Figure 3-96 Active register (client)



EVS | SYSTEM MANAGER

Hello, admin ▾ | Alarm | Version | Help

System
Storage
Direct
IP SAN
Setup
> TCP/IP
> General
> Account
> Event
> Network
> Maintenance
Log
Cluster
Playback

General | Advanced

DDNS »
Email »
FTP »
UPnP »
SNMP »
Multicast »
Register(Client) ⌄

□ Enable

Host IP: 1 . 0 . 0 . 1

Port: 8000 (1-65535)

Sub-device ID: 0

Register(Server) »
Bandwidth Manage »

Default | OK | Refresh

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

Step 4 Enter the parameters. For details, see Table 3-38.

Table 3-38 Description of active register parameters

Parameter	Description
Host IP	Enter the IP address of the server you want to register to.
Port	Enter the port number for active register. The default value is 8000.
Sub-device ID	The device ID distributed by the server-end. It is used to distinguish with other devices.

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

3.8.5.2.8 Active Register (Server)

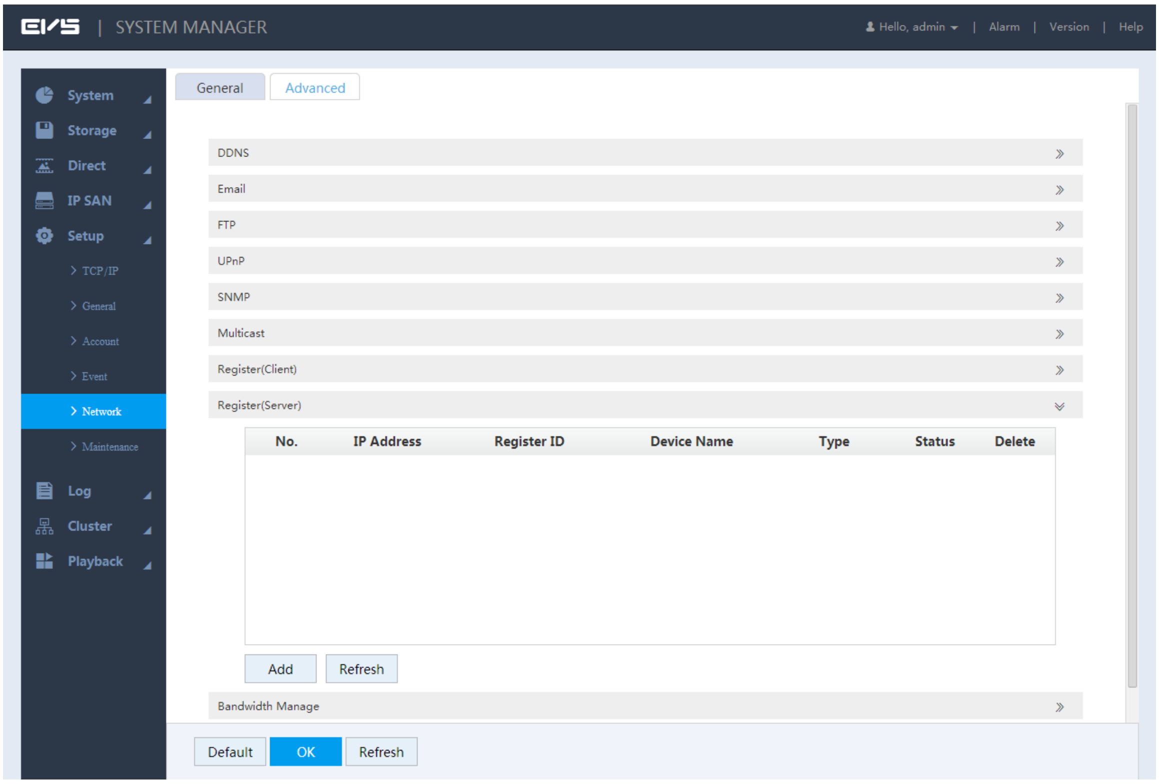
After setting the joint parameters in active register server, you can configure the joint parameters in the Web of remote device (such as IPC) and register the remote device to EVS device.

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

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

The **Register (Server)** interface is displayed. See Table 3-39

Figure 3-97 Active register (server)

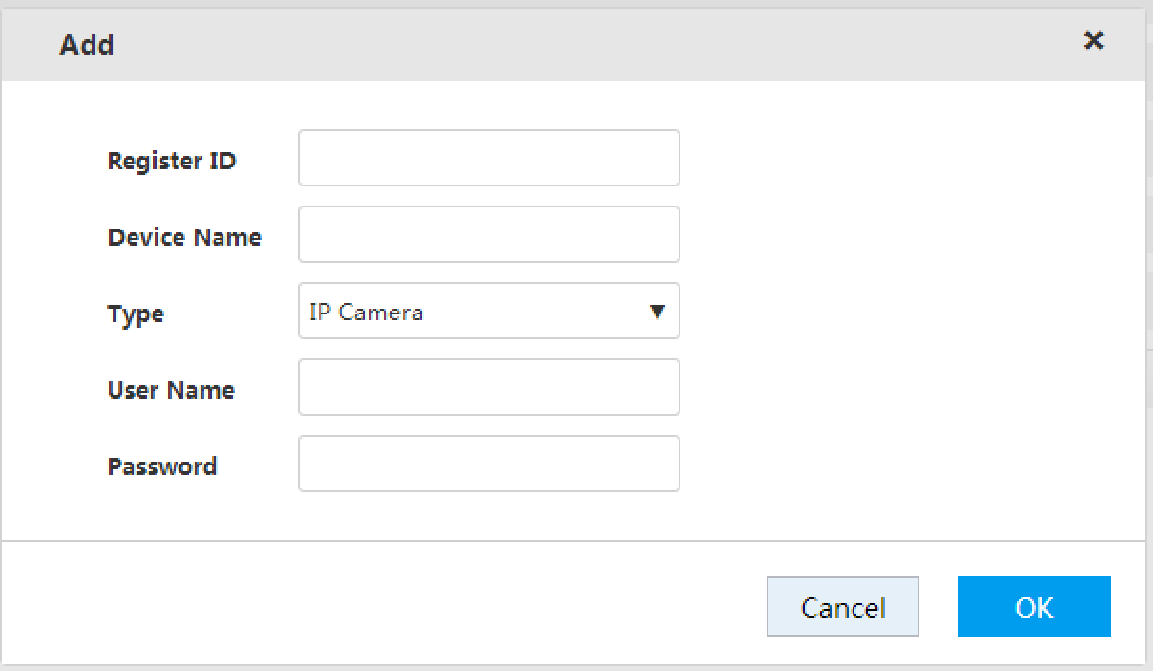


No.	IP Address	Register ID	Device Name	Type	Status	Delete

Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 3-98.

Figure 3-98 Adding register (server)



Add

Register ID

Device Name

Type: IP Camera

User Name

Password

Step 4 Select/Enter the parameters. For details, see Table 3-39.

Table 3-39 Description of adding register (server) parameters

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

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

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

3.8.5.2.9 Bandwidth Management

Control different users to have different bandwidth.

NOTE

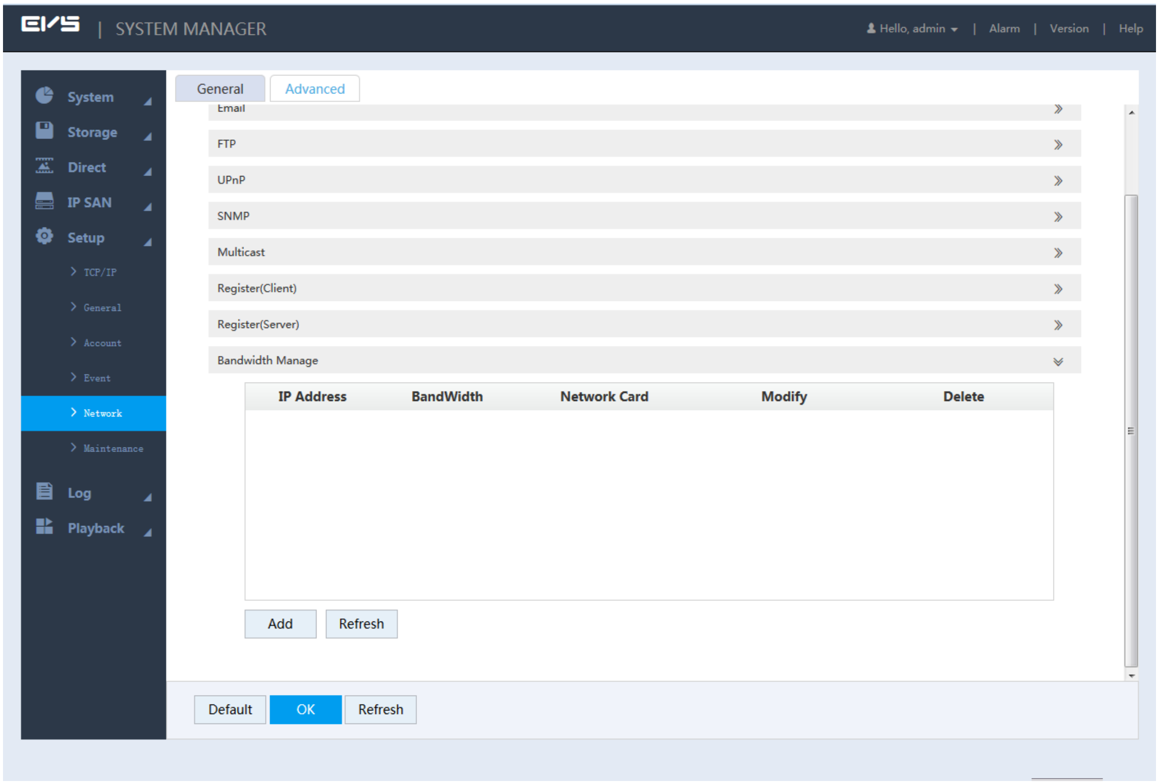
Bandwidth refers to the max bandwidth of the network card. For example: NIC of EVS device has a max bandwidth of 1 GB.

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

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

The **Bandwidth Management** interface is displayed. See Figure 3-99.

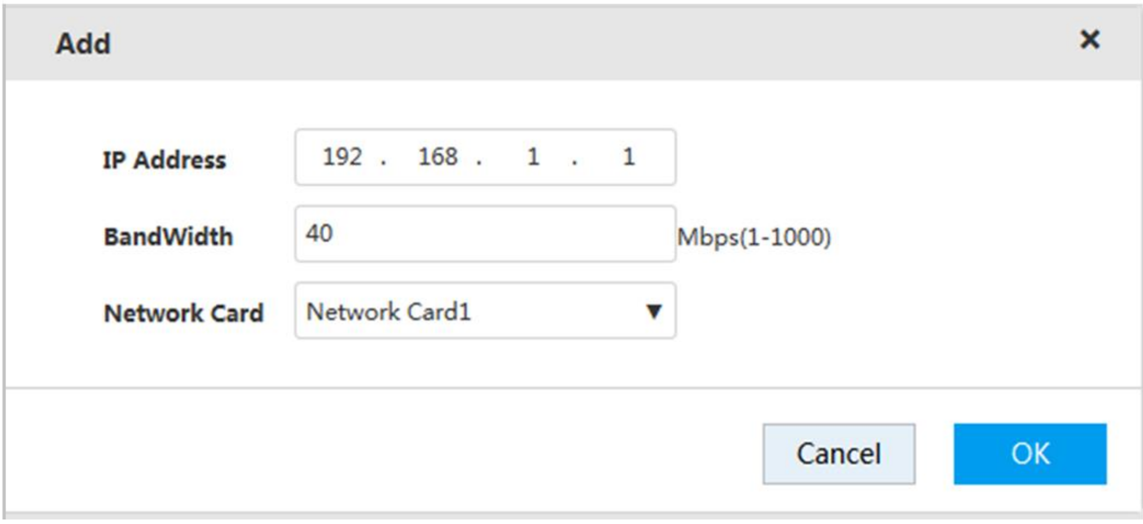
Figure 3-99 Bandwidth Management



Step 3 Click **Add**.

The **Add** interface is displayed. See Figure 3-100.

Figure 3-100 Adding Bandwidth



IP Address: 192 . 168 . 1 . 1

BandWidth: 40 Mbps(1-1000)

Network Card: Network Card1

Step 4 Select/Enter the parameters. For details, see

Table 3-40 Description of 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.

3.8.6 System Maintenance

System maintenance refers to restart the EVS device, delete old files, restore factory defaults or upgrade the system. It clears the faults and errors during the system operation and improves the operation efficiency of the EVS device.

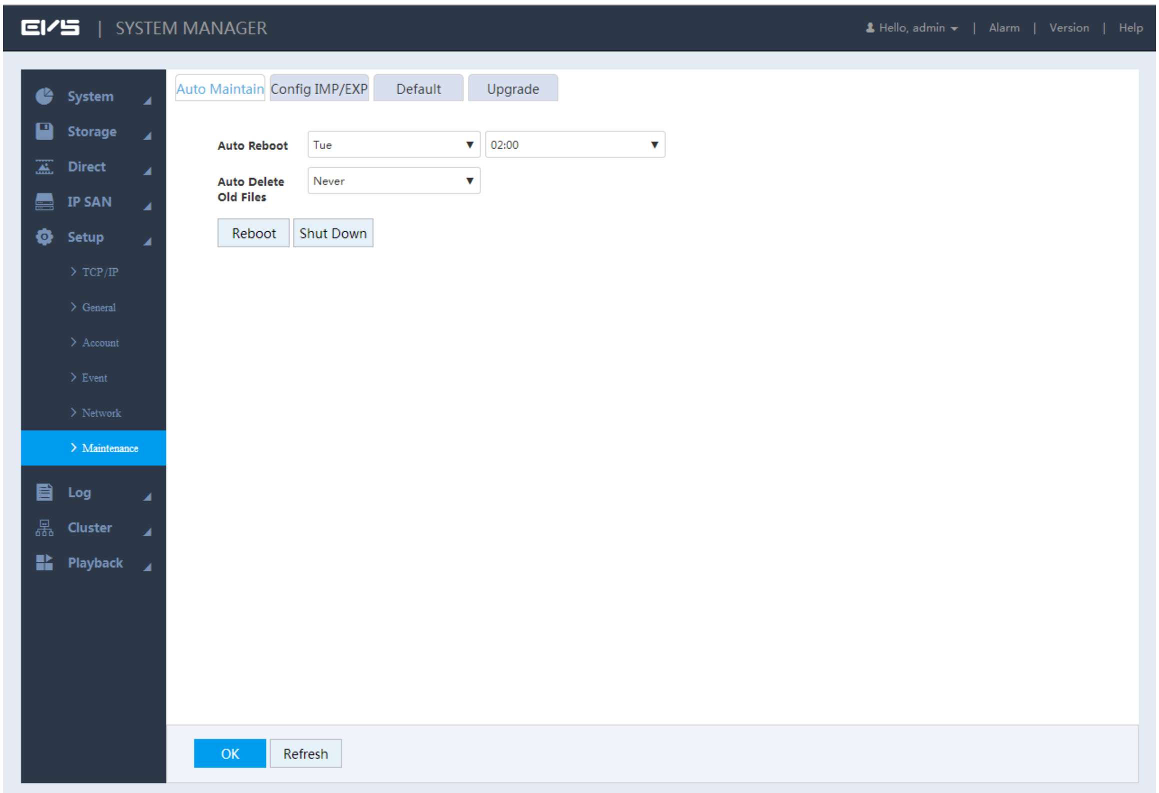
3.8.6.1 Automatic Maintenance

When the device has run for a long time and there might be many old files remained. You can set the device to automatically restart itself or delete the old files during spare time.

Step 1 Select **Setup** > **Maintenance** > **Auto Maintain**.

The **Auto Maintain** interface is displayed. See Figure 3-101.

Figure 3-101 Auto maintenance



Auto Reboot: Tue, 02:00

Auto Delete Old Files: Never

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

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

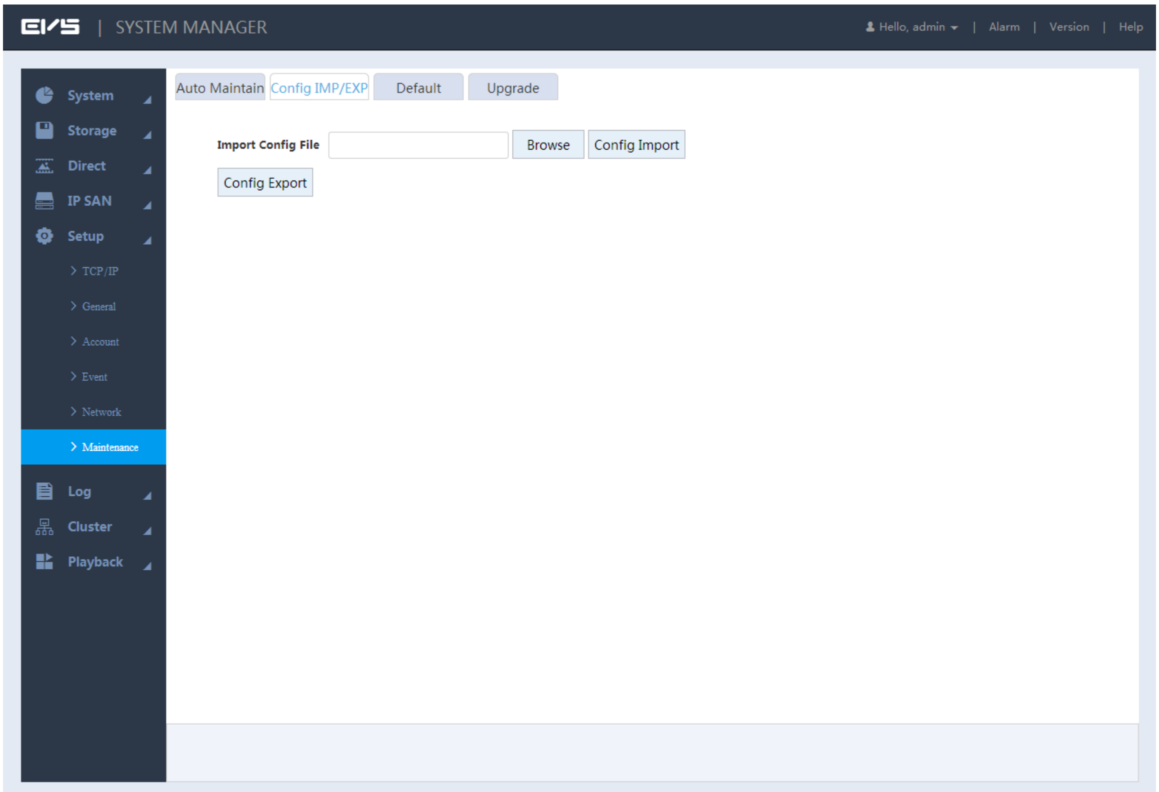
3.8.6.2 Backing up Configuration

By backing up configuration, the system can export and store the configuration in EVS device to the PC. When the EVS device is abnormal, the stored configuration information can be imported back to restore original configuration of the EVS device.

Step 1 Select **Setup** > **Maintenance** > **Config IMP/EXP**.

The **Config IMP/EXP** interface is displayed. See Figure 3-102.

Figure 3-102 Configuration backup



Step 2 Import or export config information.

- Config export: Click **Browse** to select the config file needed to be exported, click **Config Export**, and then you can export the EVS config information to the PC.
- Config import: Click **Browse** to select the config file needed to be imported, click **Config Ixport**, and then you can import the stored config information.

3.8.6.3 Restoring Defaults

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

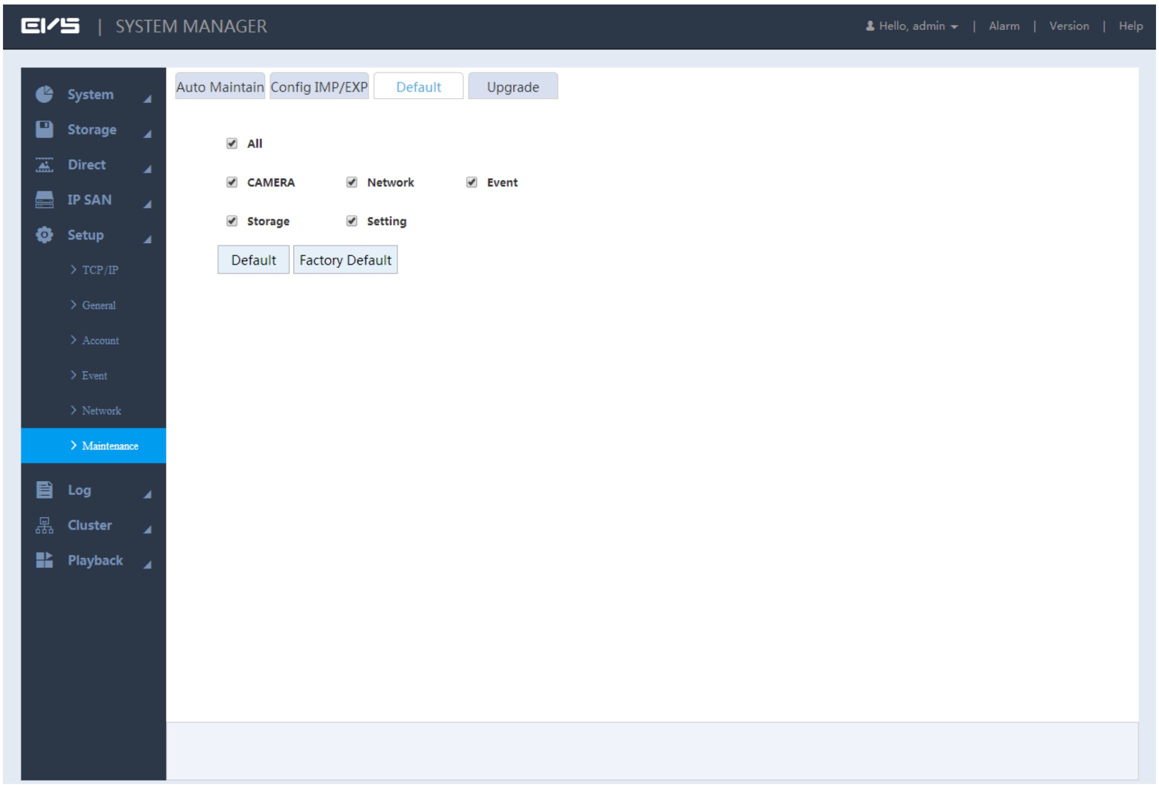
CAUTION

After restoring defaults, the existing system configuration will be lost. Be careful to perform it.

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

The **Default** interface is displayed. See Figure 3-103.

Figure 3-103 Restoring defaults



☑ All

☑ CAMERA ☑ Network ☑ Event

☑ Storage ☑ Setting

Step 2 Restoring defaults or factory defaults.

- Restoring defaults: Select the configuration item and click **Default**. The system deletes all existing configurations and restores the default status.
- Restoring factory defaults: Click **Factory Default** and all the EVS configurations are restored to factory default status.

3.8.6.4 System Upgrade

Upgrade the system of EVS device by importing upgrade files. Upgrade files are marked with *.bin.

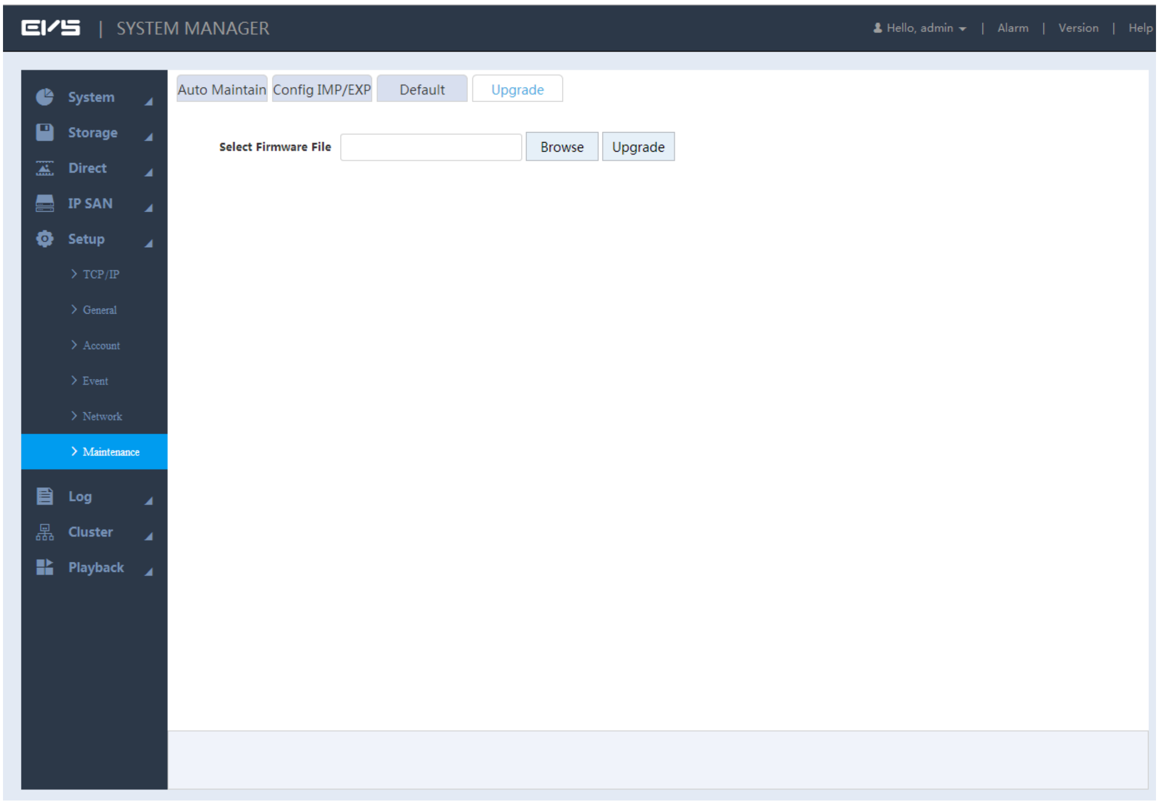
⚠ CAUTION

- In the process of upgrading, do not cut down the power/network, restart or shutdown the device.
- Upgrading error might lead to device fault. Make sure that the imported upgrade file is correct.

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

The **Upgrade** interface is displayed. See Figure 3-104.

Figure 3-104 System upgrade



Select Firmware File

Step 2 Click **Browse** to select the upgrade file.

Step 3 Click **Upgrade** and the system starts upgrading.

3.9 Storage Management

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

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

3.9.1 Physical HDD

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

Select **Storage** > **Physical HDD**. The **Physical HDD** interface is displayed. See Figure 3-105.

- 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.

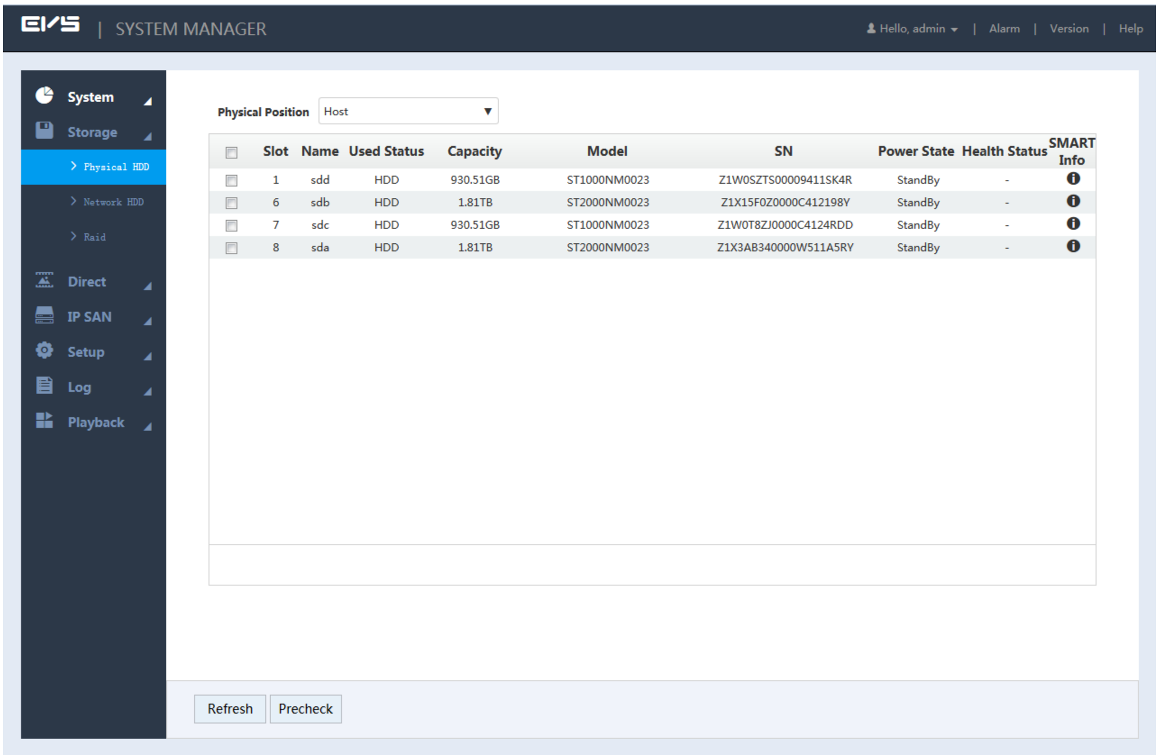
- Select the physical HDD and click **Precheck**. The system can check the operation status of the disk to help users understand disk performance and upgrade disk errors timely.

- Click ⓘ and the **SMART Info** interface is displayed. See Figure 3-106.

NOTE

SMART (Self-Monitoring Analysis and Reporting Technology) is a kind of automatic HDD status monitoring and forewarning technology. SMART monitors and records the HDD with the monitoring orders in the disk and compares the results with the safe values preset by the manufacturer. If the monitored value is approaching or exceeding the security scope, the system sends warning to the user and performs slight repair, so that to guarantee the data security in the HDD.

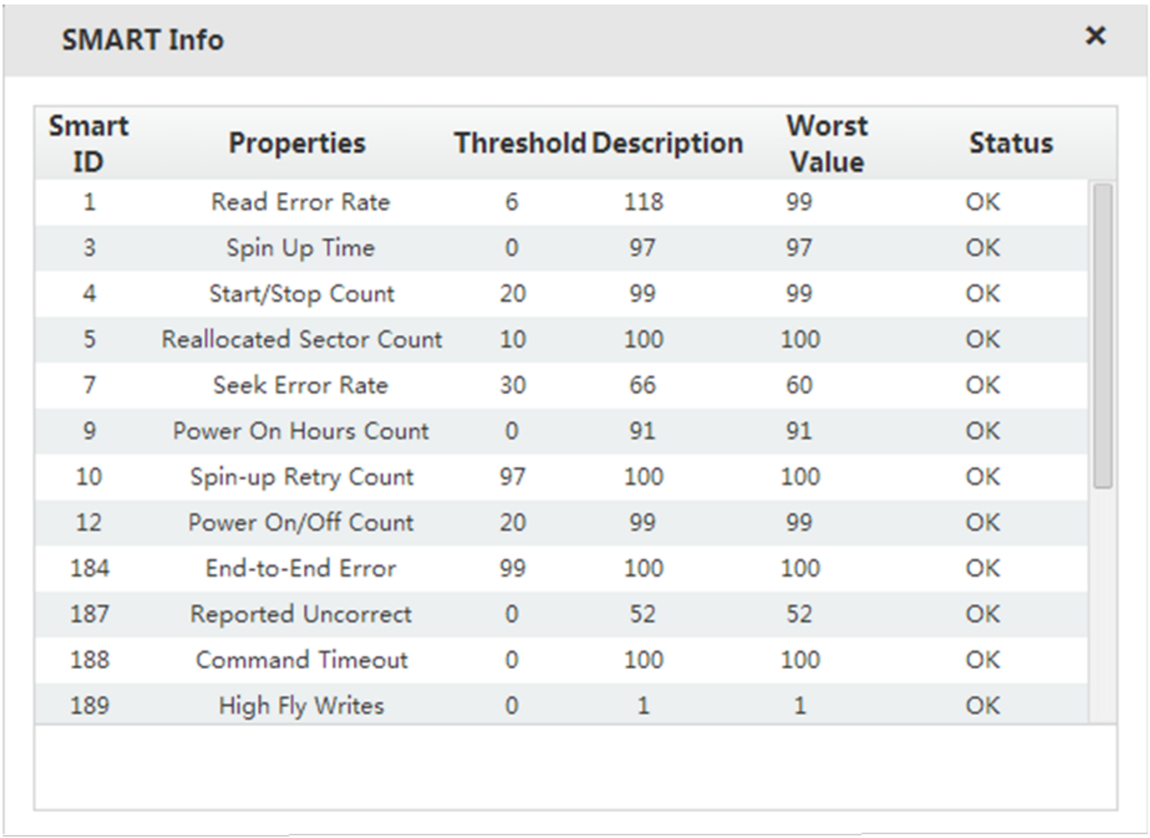
Figure 3-105 Physical HDD



Physical Position: Host

□	Slot	Name	Used Status	Capacity	Model	SN	Power State	Health Status	SMART Info
□	1	sdd	HDD	930.51GB	ST1000NM0023	Z1W0SZTS00009411SK4R	StandBy	-	ⓘ
□	6	sdb	HDD	1.81TB	ST2000NM0023	Z1X15F0Z0000C412198Y	StandBy	-	ⓘ
□	7	sdc	HDD	930.51GB	ST1000NM0023	Z1W0T8ZJ0000C4124RDD	StandBy	-	ⓘ
□	8	sda	HDD	1.81TB	ST2000NM0023	Z1X3AB340000W511A5RY	StandBy	-	ⓘ

Figure 3-106 SMART information



SMART Info

Smart ID	Properties	Threshold	Description	Worst Value	Status
1	Read Error Rate	6	118	99	OK
3	Spin Up Time	0	97	97	OK
4	Start/Stop Count	20	99	99	OK
5	Reallocated Sector Count	10	100	100	OK
7	Seek Error Rate	30	66	60	OK
9	Power On Hours Count	0	91	91	OK
10	Spin-up Retry Count	97	100	100	OK
12	Power On/Off Count	20	99	99	OK
184	End-to-End Error	99	100	100	OK
187	Reported Uncorrect	0	52	52	OK
188	Command Timeout	0	100	100	OK
189	High Fly Writes	0	1	1	OK

3.9.2 Network HDD

Set the network HDD with iSCSI and then map the network HDD to the EVS device, so that the EVS device can store data through the network HDD.

NOTE

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

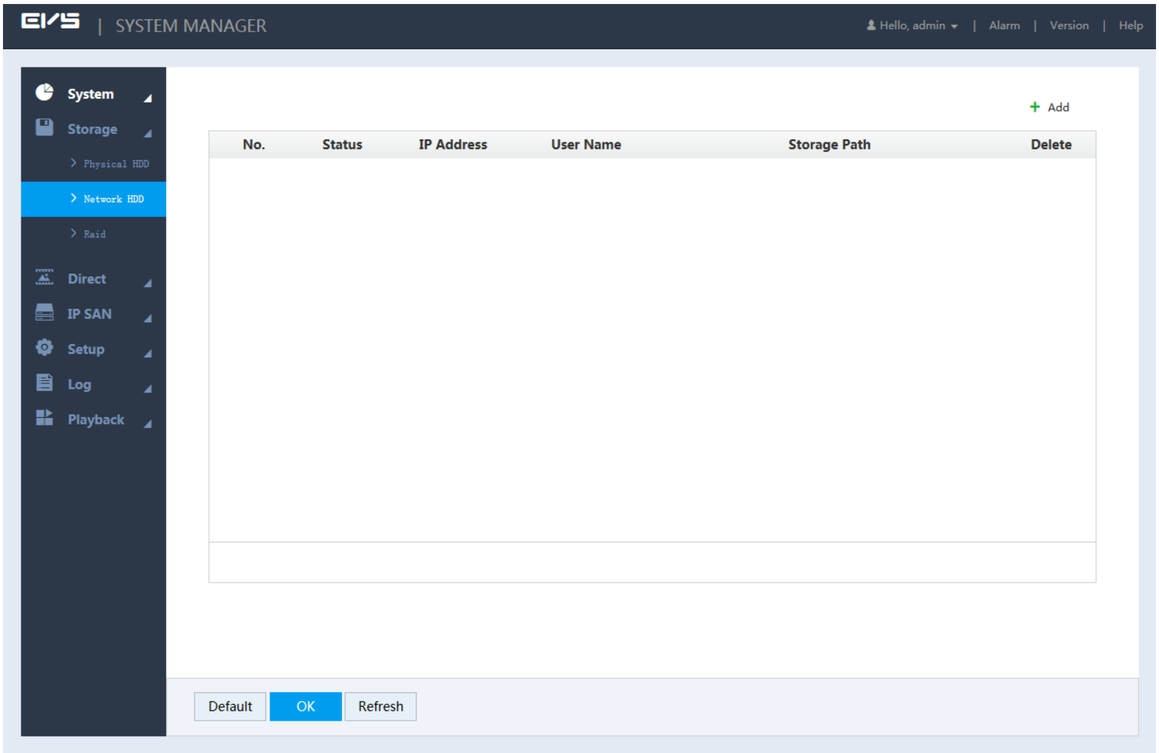
Preparation

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

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

The **Network HDD** interface is displayed. See Figure 3-107.

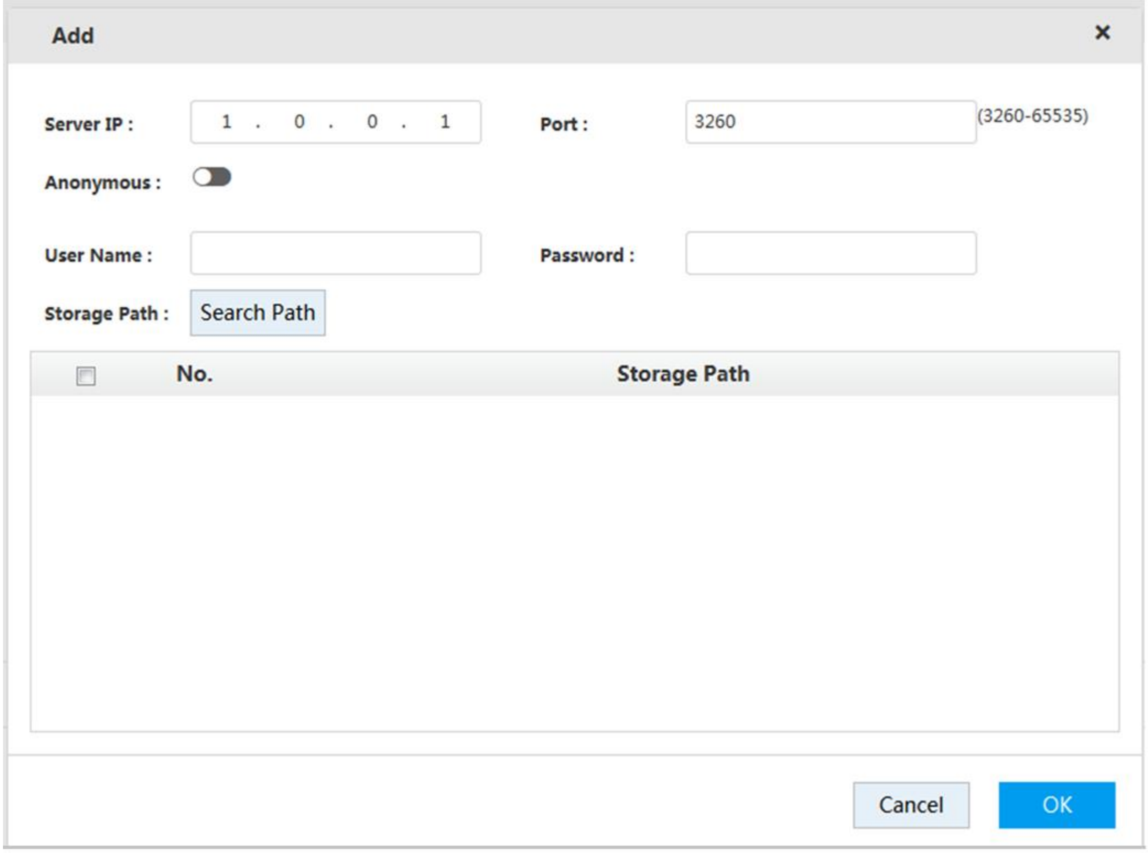
Figure 3-107 Network HDD



Step 2 Click + .

The **Add** interface is displayed. See Figure 3-108.

Figure 3-108 Adding network HDD



Step 3 Select/Enter the parameters. For details, see Table 3-41.

Table 3-41 Description of network HDD parameters

Parameter	Description

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. ● Disable anonymous login. ● Enable anonymous login. You do not need to enter the user name and password.
User Name	If the iSCSI server has set access permission when it created the shared file list, you need to enter the user name and password.
Password	
Storage Path	Click Search Path to select the stored path of the network disk. NOTE iSCSI server has generated the corresponding path when it created the shared file list. Each path represents a iSCSI shared disk.

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

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

NOTE

- Click 🗑 to delete a network disk. Click **Refresh** to update the disk list.
- In the **Storage** interface, you can set the disk group of network HDDs. For details, see "3.10.1 Storage Device."

3.9.3 RAID Management

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

NOTE

- The disk set for image direct storage cannot be used to create RAID.
- Currently the following RAID types are supported: RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60. For details, see "Appendix 1 RAID Introduction."

3.9.3.1 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 the practical needs.

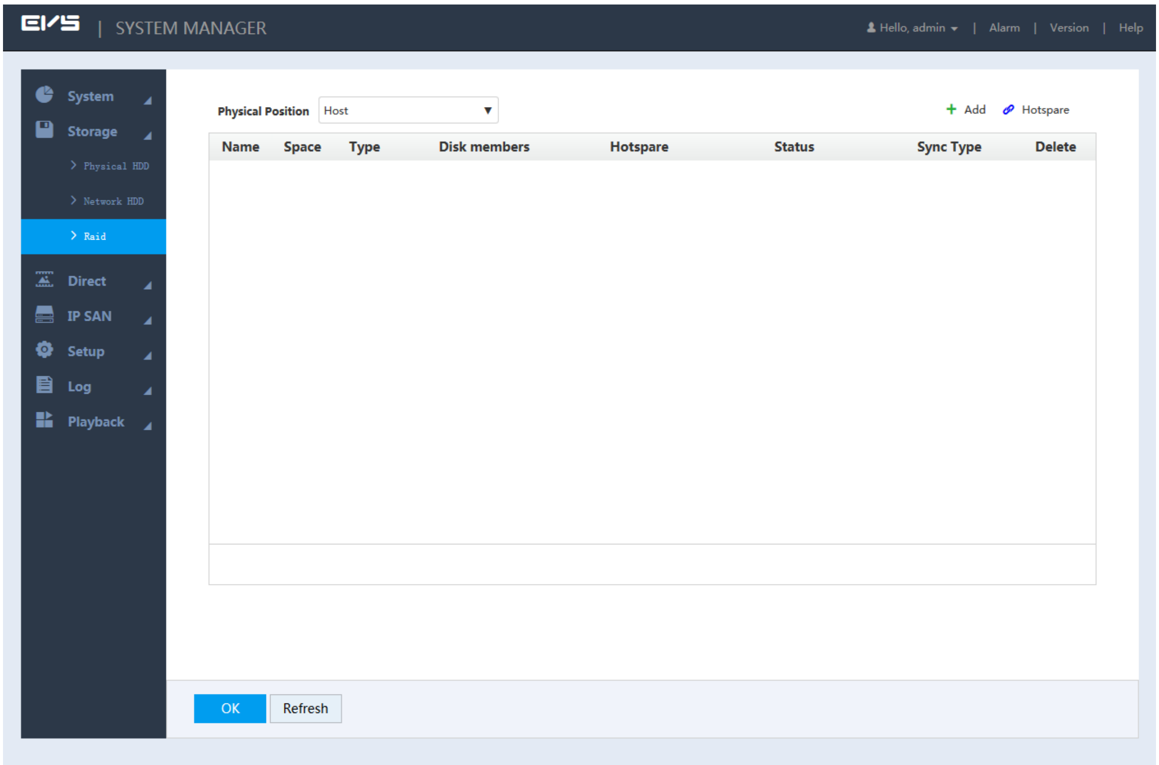
⚠ CAUTION

The system will clear the original data in the disk when creating RAID. Be careful to perform it.

Step 1 Select **Storage** > **Raid**.

The **Raid** interface is displayed. See Figure 3-109.

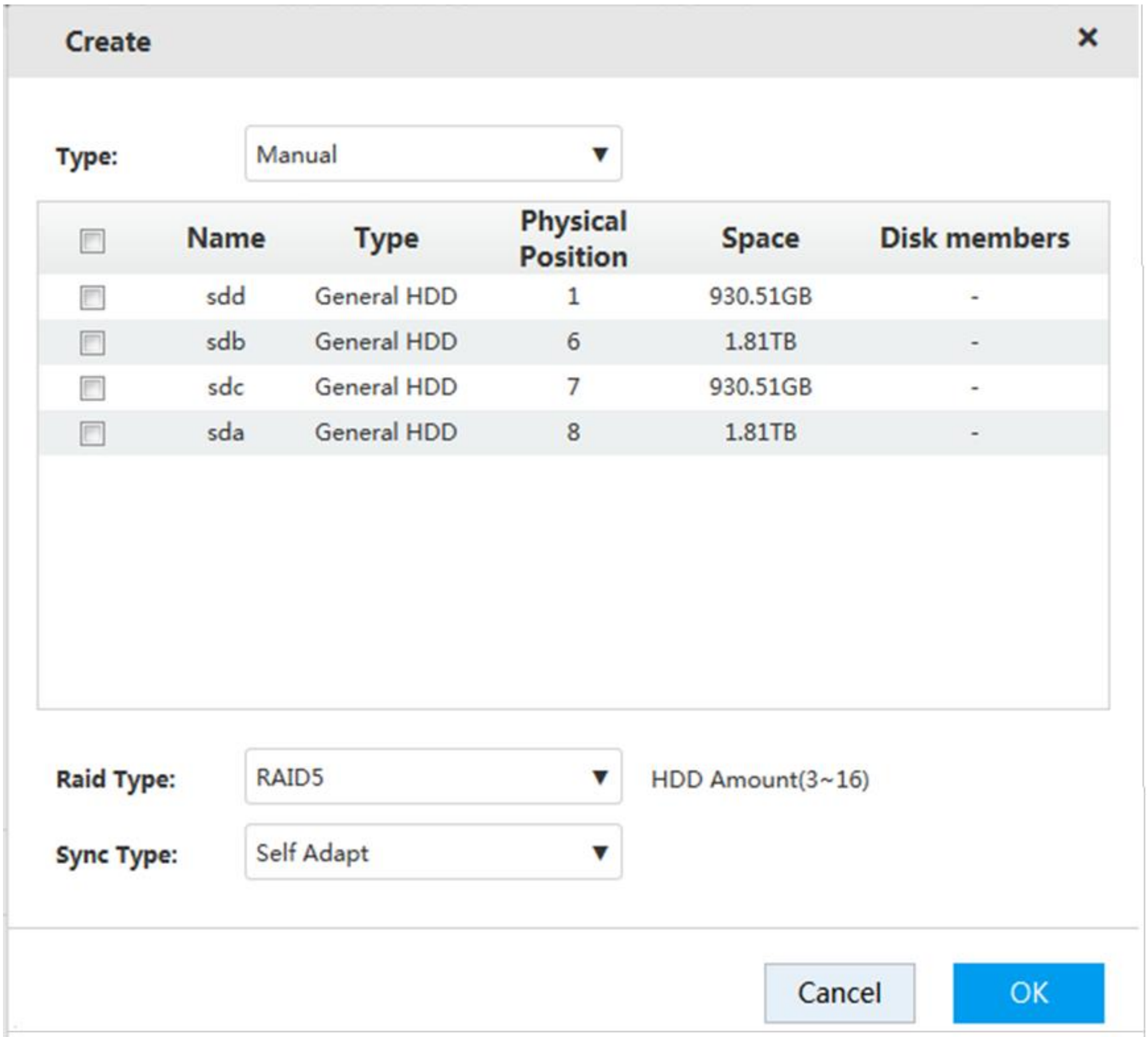
Figure 3-109 Raid management



Step 2 Click + .

The **Create** interface is displayed. See Figure 3-110.

Figure 3-110 Creating RAID



Create

Type: Manual

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

Raid Type: RAID5 HDD Amount(3~16)

Sync Type: Self Adapt

Step 3 Select the parameters. For details, see Table 3-42.

Table 3-42 Description of RAID creation parameters

Parameter	Description
Type	Select the RAID creation type, including manual and one-click. NOTE When you choose the one-click RAID creation, the system automatically creates RAID 5 according to the one-click RAID creation strategy. For details, see Table 3-43.
HDD	Select the HDD you want to use to create RAID. NOTE Different RADI type needs different number of disks. See the actual situation.
Raid Type	Select the RAID type you want to create.

Parameter	Description
Sync Type	Select the sync mode of the business resources allocation. ● Self-adaption: Automatically adjust the RAID sync speed according to the current business loads. NOTE 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 priority: Resource priority is assigned to RAID sync. ● Business priority: Resource priority is assigned to business operations. ● Balance: Resource is evenly distributed to RAID sync and business operations.

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

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

NOTE

- 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.

One-Click RAID Creation Strategy

When the disks are fully installed, the system creates RAID 5 at one-click according to the policy in Table 3-43.

NOTE

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

Table 3-43 One-click RAID creation strategy

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

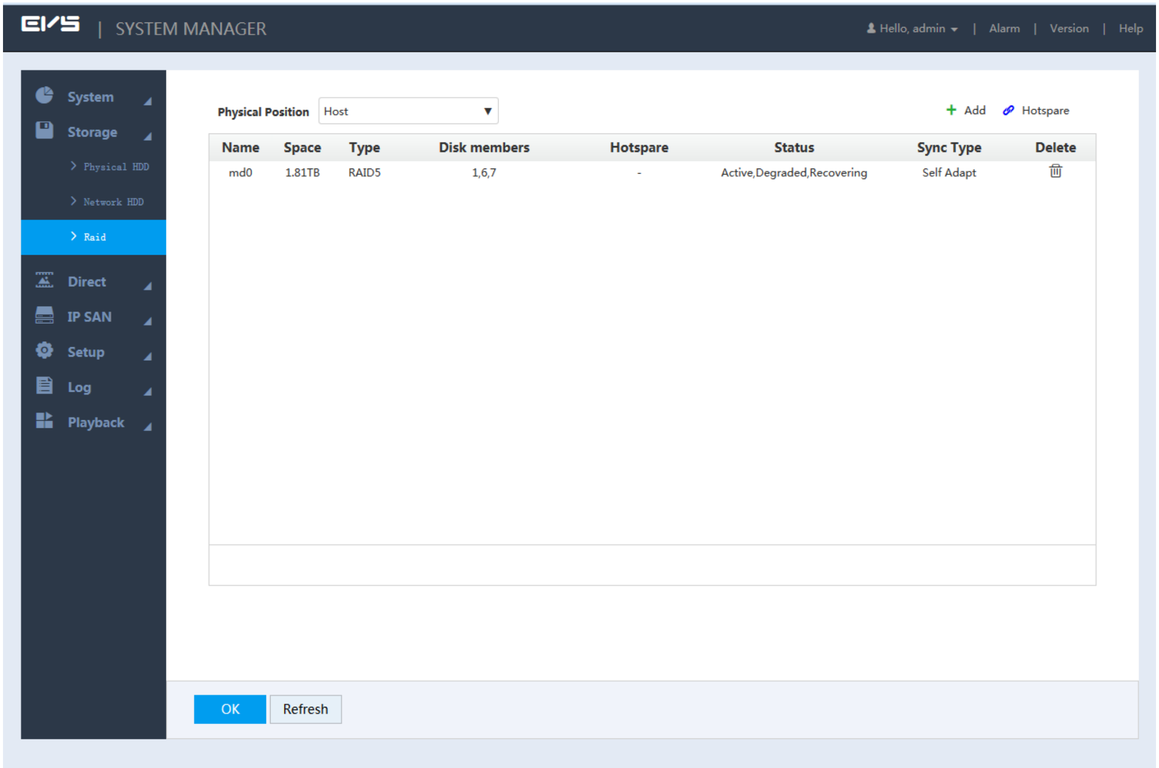
3.9.3.2 Hotspare Management

When a member disk of the RAID group is fault or abnormal, the hotspare disk replaces it to work, so as to avoid data loss and guarantee the reliability of the storage system.

Step 1 Select **Storage** > **Raid**.

The **Raid** interface is displayed. See Figure 3-111.

Figure 3-111 RAID management



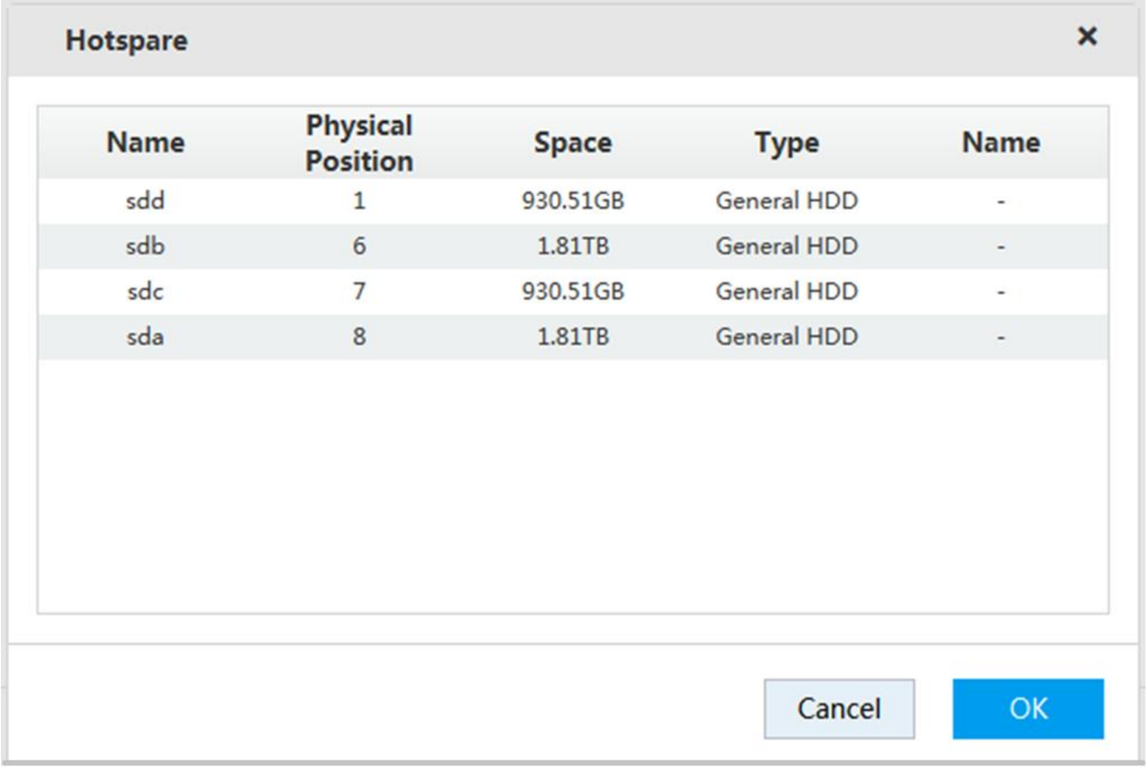
Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	1.81TB	RAID5	1,6,7	-	Active,Degraded,Recovering	Self Adapt	🗑

Step 2 Click 🔗 .

The **Hotspare** interface is displayed. See Figure 3-112.

Figure 3-112 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 hotspare or general hotspare.

- General HDD: A general disk member in the RAID.
- Private hotspare: Double-click the corresponding **Name**, select the RAID group,

and then this HDD is used as a hotspare only for the corresponding RAID.

- General hotspare: It is used as a hotspare for all the RAID groups.

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

3.10 Direct Storage Mode

3.10.1 Storage Device

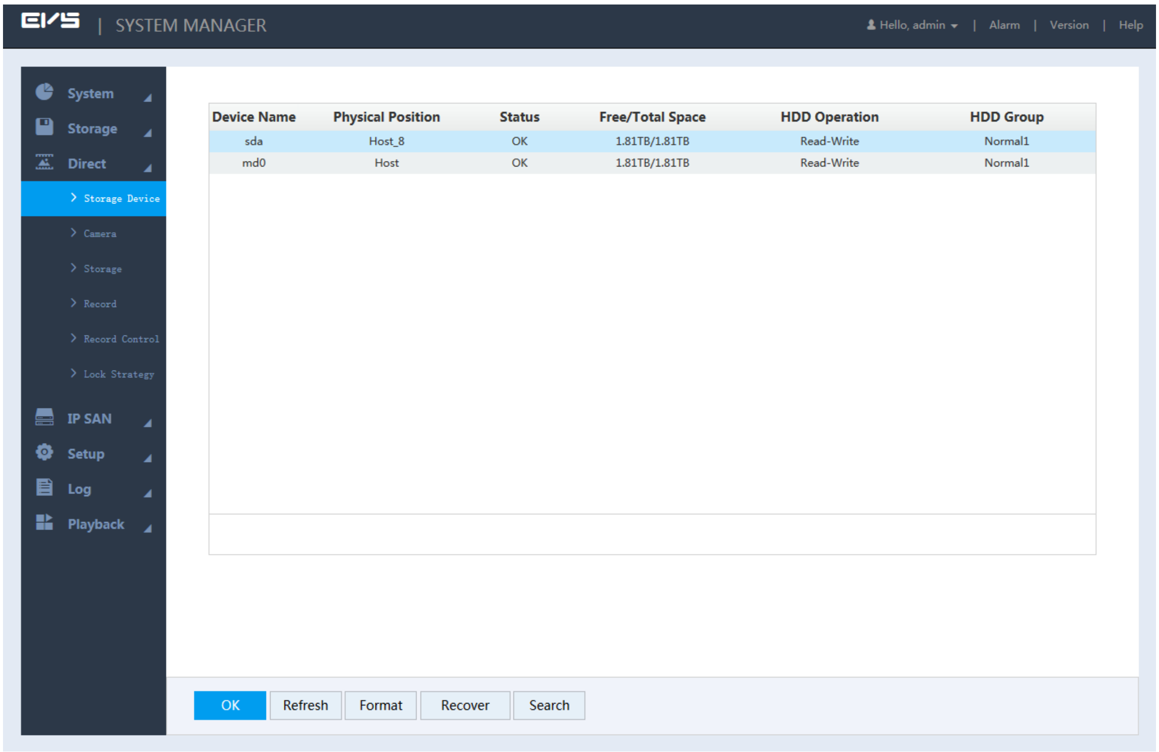
View the disk information, format the disk, recover the image library and search the records.

3.10.1.1 HDD Property Settings

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

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

Figure 3-113 Storage device



Device Name	Physical Position	Status	Free/Total Space	HDD Operation	HDD Group
sda	Host_8	OK	1.81TB/1.81TB	Read-Write	Normal1
md0	Host	OK	1.81TB/1.81TB	Read-Write	Normal1

Step 2 Select/Enter the parameters. For details, see Table 3-44.

Table 3-44 Description of storage device parameters

Parameter	Description
Device Name	Display the HDD or RAID name.
Physical Position	Display the physical position of the HDD or RAID.
Status	Display the current running status of the HDD or RAID.
Free/Total Space	Display the free space and total space of the HDD or RAID.

Parameter	Description
HDD Operation	Double-click the corresponding **HDD Operation** to set the HDD or RAID properties. ● Read-write disk: Used to read and store data. ● Read-only disk: Only used to read data. Not support data storage. ● Redundant disk: Used to store redundant records and images. ● Frame disk: Only used to store the records after frame extracting. ● Image direct-storage disk: Only used to store images.
HDD Group	Double-click the corresponding **HDD Group** to set the HDD group. Image direct storage disk corresponds to special group and read-write disk corresponds to normal group. Other disks do not need to set the group.

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

3.10.1.2 Formatting HDD

Select the HDD and click **Format** to clear all the data in the disk.

⚠ CAUTION

- HDD formatting will clear all the data in the disk. Be careful to perform it.
- You need to restart the EVS device after the formatting to make the configuration effective.

3.10.1.3 Restore Image Library

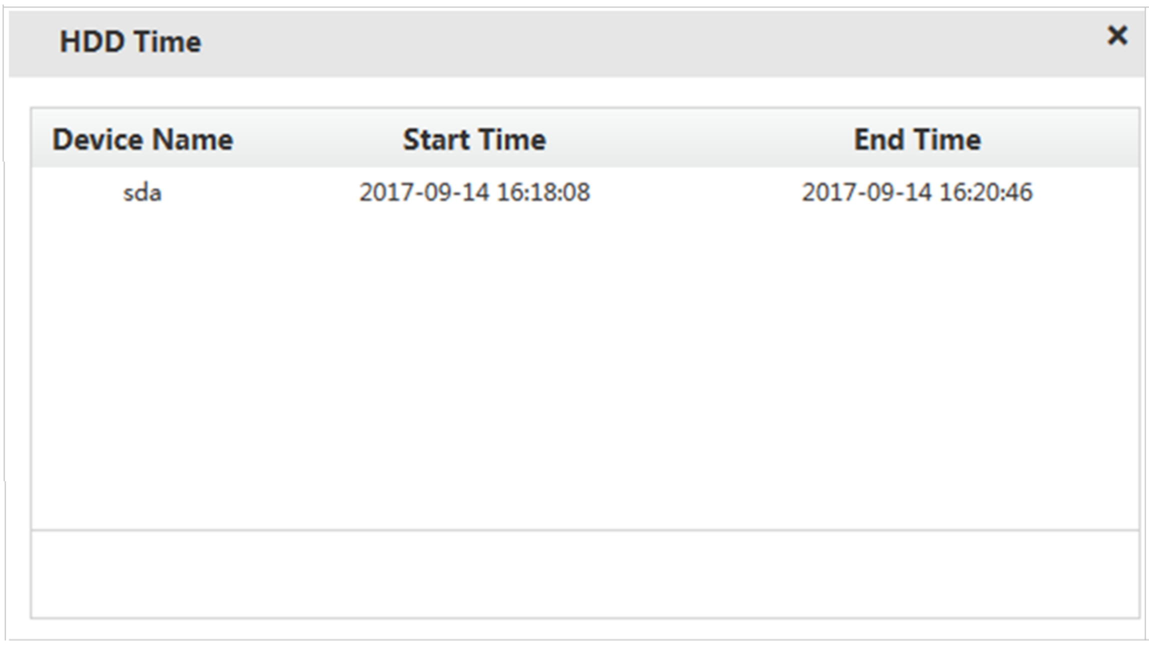
You can perform the image library recovery for the image direct storage disk when the library is abnormal.

Select the corresponding image direct storage disk and click **Image Library Recovery** to restore it.

3.10.1.4 Search Records

Select the disk and click **Search Record**. The **HDD Time** interface is displayed. See Figure 3-114. You can view the record time in the specified HDD.

Figure 3-114 HDD record time period



HDD Time

Device Name	Start Time	End Time
sda	2017-09-14 16:18:08	2017-09-14 16:20:46

3.10.2 Camera

3.10.2.1 Remote Device Management

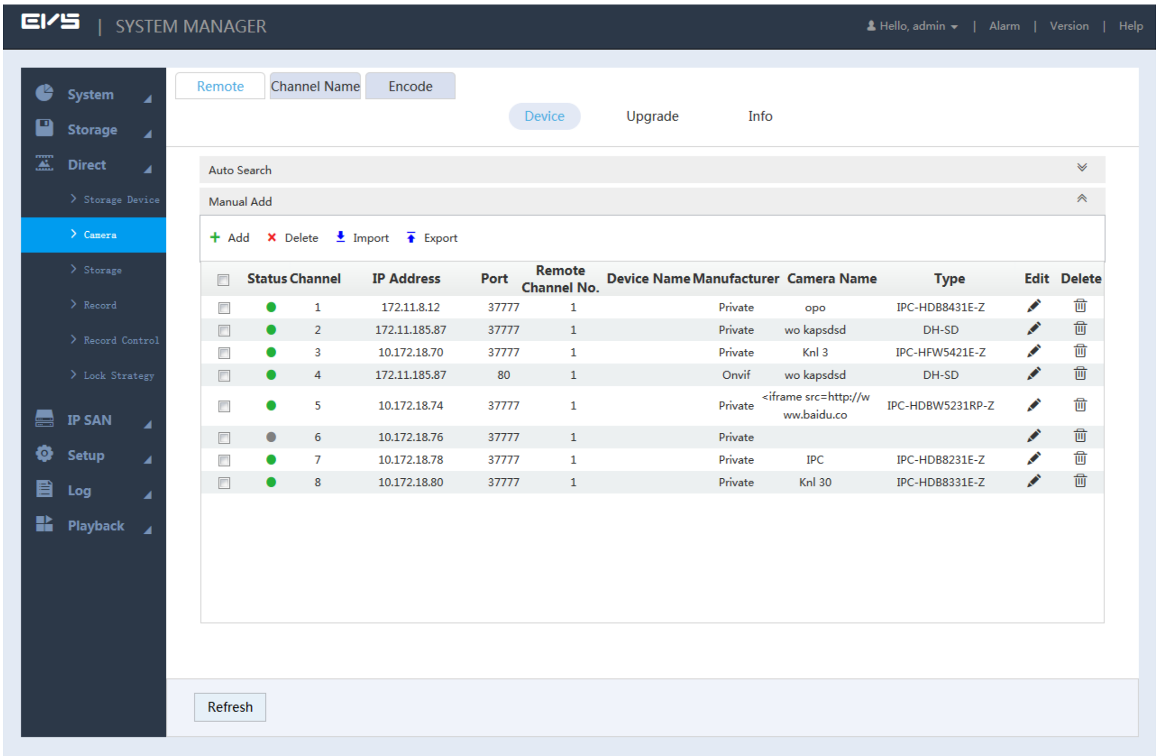
Remote device management includes adding, editing and upgrading remote device and setting the channel name and stream parameters of the device.

3.10.2.1.1 Adding Remote Device

Select **Direct** > **Camera** > **Remote** > **Device**. The **Device** interface is displayed. See Figure 3-115.

The system supports to add remote device and import/export remote device information. For details, see "3.5 Adding Remote Device."

Figure 3-115 Adding remote device



□	Status	Channel	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	172.11.8.12	37777	1		Private	opo	IPC-HDB8431E-Z	✎	🗑
□	●	2	172.11.185.87	37777	1		Private	wo kapsdsd	DH-SD	✎	🗑
□	●	3	10.172.18.70	37777	1		Private	Knl 3	IPC-HFW5421E-Z	✎	🗑
□	●	4	172.11.185.87	80	1		Onvif	wo kapsdsd	DH-SD	✎	🗑
□	●	5	10.172.18.74	37777	1		Private	<iframe src=http://www.baidu.co	IPC-HDBW5231RP-Z	✎	🗑
□	●	6	10.172.18.76	37777	1		Private			✎	🗑
□	●	7	10.172.18.78	37777	1		Private	IPC	IPC-HDB8231E-Z	✎	🗑
□	●	8	10.172.18.80	37777	1		Private	Knl 30	IPC-HDB8331E-Z	✎	🗑

3.10.2.1.2 Initializing the Remote Device

You can modify the login password and IP address of the remote device through the initialization.

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

The **Device** interface is displayed. See Figure 3-115.

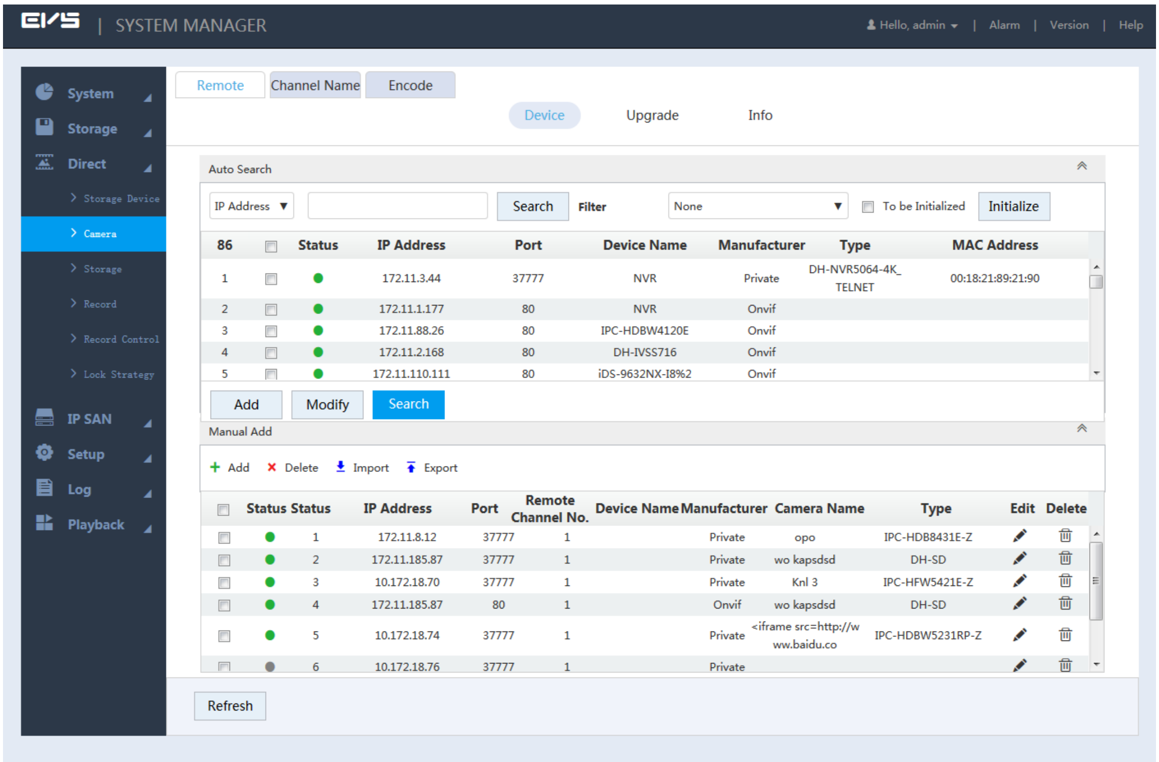
Step 2 Click ︾ on the right side of **Auto Search** and click **Search**.

The system searches the remote devices in the LAN and displays the results.

Step 3 Select the **To be Initialized** check box.

The uninitialized devices are displayed. See Figure 3-116.

Figure 3-116 Auto search results



Auto Search

IP Address ▼ | Search | Filter | None ▼ | □ To be Initialized | Initialize

86	□	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
1	□	●	172.11.3.44	37777	NVR	Private	DH-NVR5064-4K_TELNET	00:18:21:89:21:90
2	□	●	172.11.1.177	80	NVR	Onvif		
3	□	●	172.11.88.26	80	IPC-HDBW4120E	Onvif		
4	□	●	172.11.2.168	80	DH-IVSS716	Onvif		
5	□	●	172.11.110.111	80	iDS-9632NX-I8%2	Onvif		

Add | Modify | Search

Manual Add

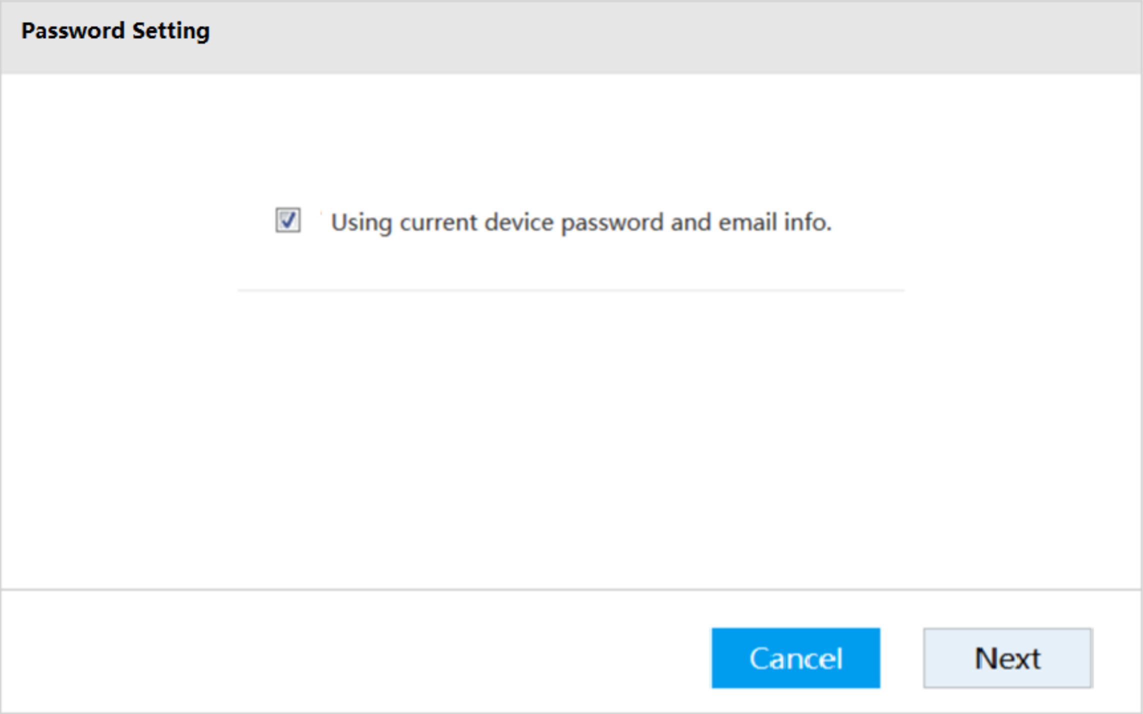
Add | Delete | Import | Export

□	Status	Status	IP Address	Port	Remote Channel No.	Device Name	Manufacturer	Camera Name	Type	Edit	Delete
□	●	1	172.11.8.12	37777	1		Private	opo	IPC-HDB8431E-Z	✎	🗑
□	●	2	172.11.185.87	37777	1		Private	wo kapsdsd	DH-SD	✎	🗑
□	●	3	10.172.18.70	37777	1		Private	Knl 3	IPC-HFW5421E-Z	✎	🗑
□	●	4	172.11.185.87	80	1		Onvif	wo kapsdsd	DH-SD	✎	🗑
□	●	5	10.172.18.74	37777	1		Private	<iframe src=http://www.baidu.co	IPC-HDBW5231RP-Z	✎	🗑
□	●	6	10.172.18.76	37777	1		Private			✎	🗑

Step 4 Select the uninitialized device and click **Initialize**.

The Password Setting interface is displayed. See Figure 3-117.

Figure 3-117 Password setting (1)



Password Setting

☑ Using current device password and email info.

Cancel | Next

Step 5 Set the password of the remote device.

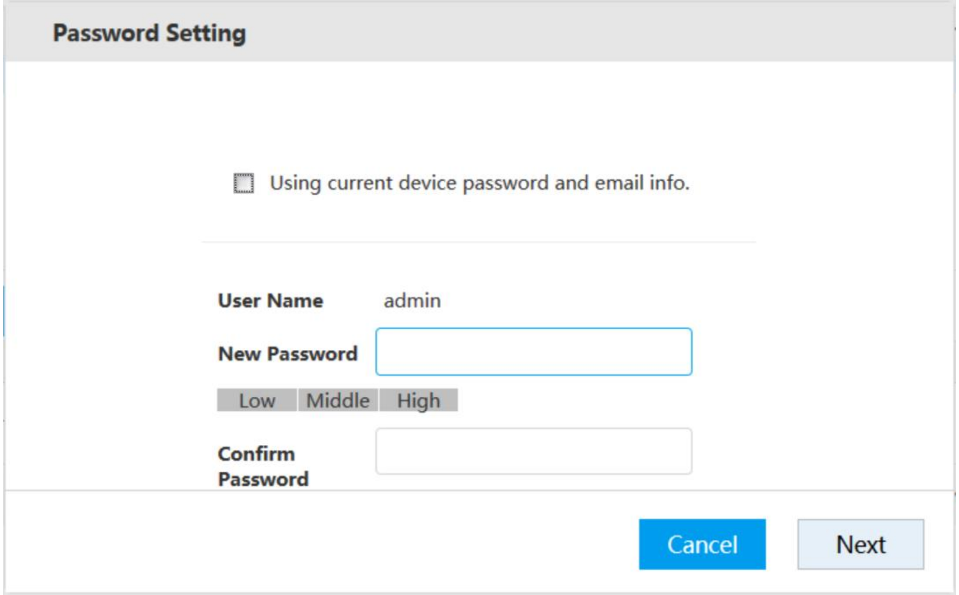
Clear the **Using current device password and email info** check box. The **Password Setting** interface is displayed. See Figure 3-118. You need to set the remote device password manually.

NOTE

- When you select the **Using current device password and email info** check box, the remote device automatically use the password of the current admin account. You do not need to set the password and can directly go forward to Step 6.

- The password consists of 8 to 32 characters containing letter(s), number(s) and symbol(s). It contains at least two types.

Figure 3-118 Password setting (2)



Password Setting

□ Using current device password and email info.

User Name admin

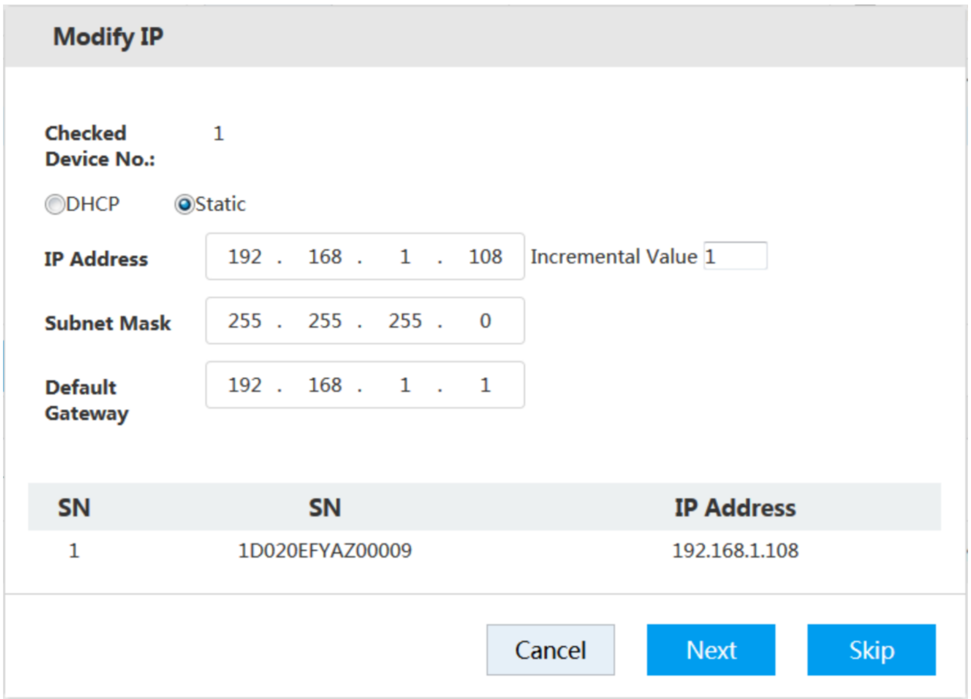
New Password

Confirm Password

Step 6 Click **Next**.

The **Modify IP** interface is displayed. See Figure 3-119.

Figure 3-119 Modifying 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	1D020EFYAZ00009	192.168.1.108

Step 7 Set the IP address of the remote device.

- If you select **DHCP**, you do not need to enter the **IP Address**, **Subnet Mask** and **Default Gateway**. The system distributes the IP address automatically.
- If you select **Static**, you need to enter the **IP Address**, **Subnet Mask**, **Default Gateway** and **Incremental Value**. The system assigns IP address for remote devices in an increasing sequence of the fourth section in the IP address.

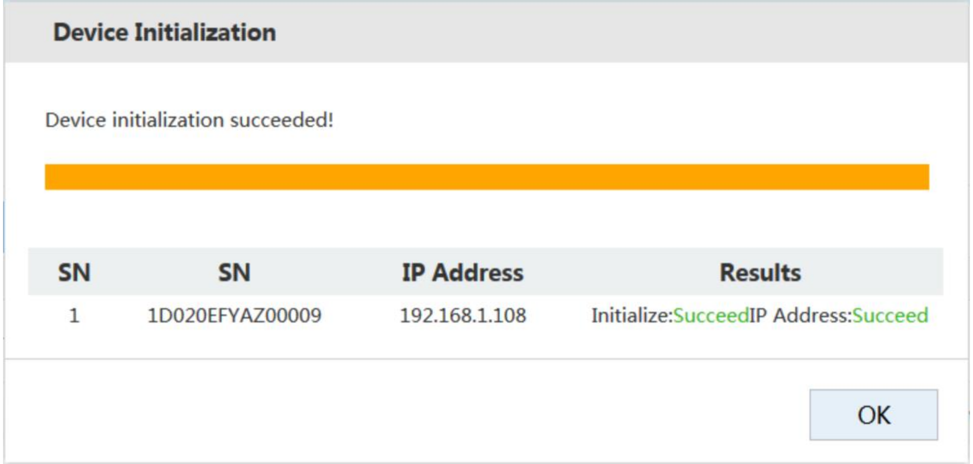
NOTE

- When modifying multiple remote devices, the system will change the IP addresses into the same network segment if they were different previously.
- When modifying the static IP, if there is IP conflict, the system will prompt a notice. If the IP addresses are modified in batch, the system will skip the conflicted IP and go on distributing IP in an increasing sequence.
- If you do not set the IP address, click **Skip**. The system starts to initialize the device. See Figure 3-120.

Step 8 Click **Next**.

The system starts to initialize the remote device. See Figure 3-120.

Figure 3-120 Device initialization



Device Initialization

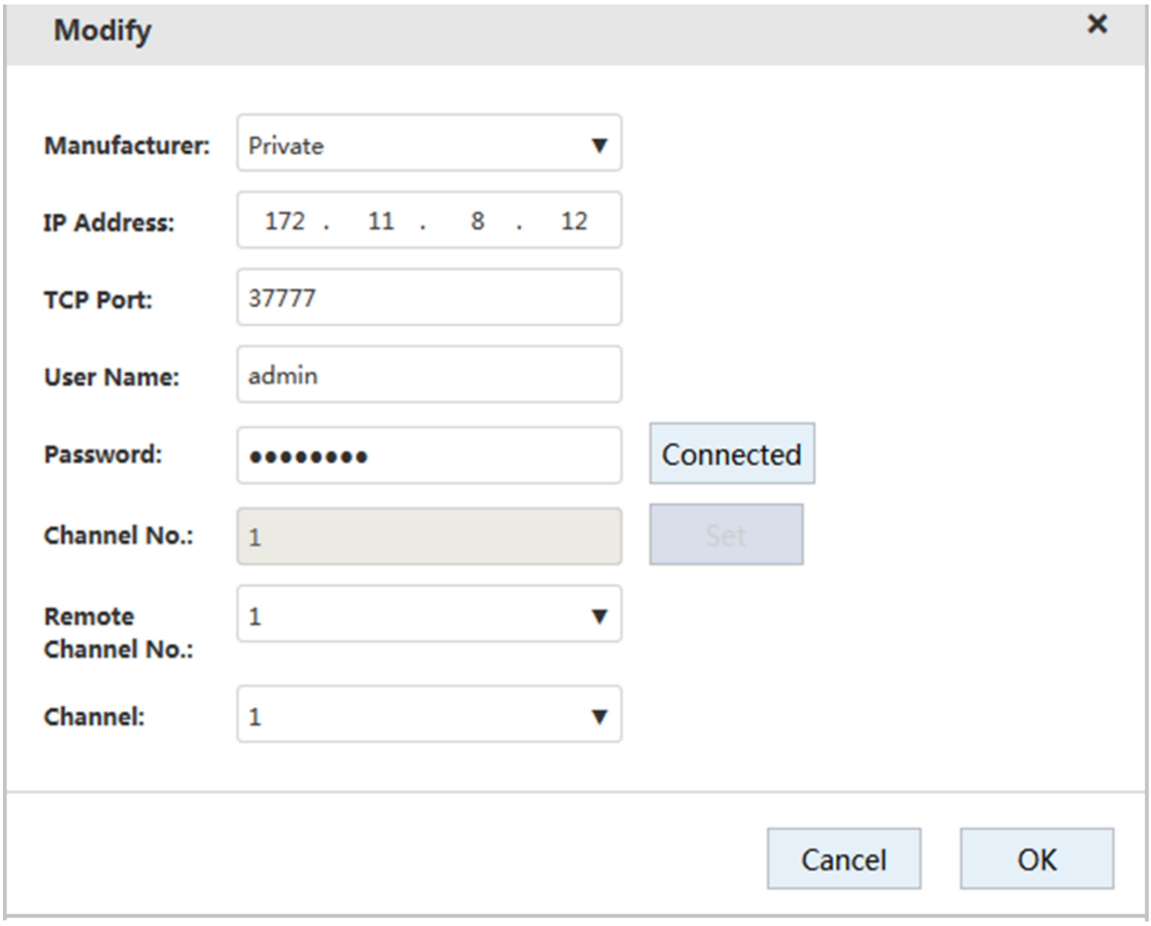
Device initialization succeeded!

SN	SN	IP Address	Results
1	1D020EFYAZ00009	192.168.1.108	Initialize:SucceedIP Address:Succeed

3.10.2.1.3 Editing Remote Device

- Click ✎ and the **Modify** interface is displayed. See Figure 3-121. You can modify the remote device information, such as the IP address.
- Click 🗑 or select the check box of the remote device and click ✕ to delete the device.
- Click **Refresh** to update the device list.

Figure 3-121 Modifying remote device



Modify

Manufacturer: Private

IP Address: 172 . 11 . 8 . 12

TCP Port: 37777

User Name: admin

Password: ••••••••

Channel No.: 1

Remote Channel No.: 1

Channel: 1

3.10.2.1.4 Upgrading Remote Device

The system supports to upgrade the remote device in the Web interface.

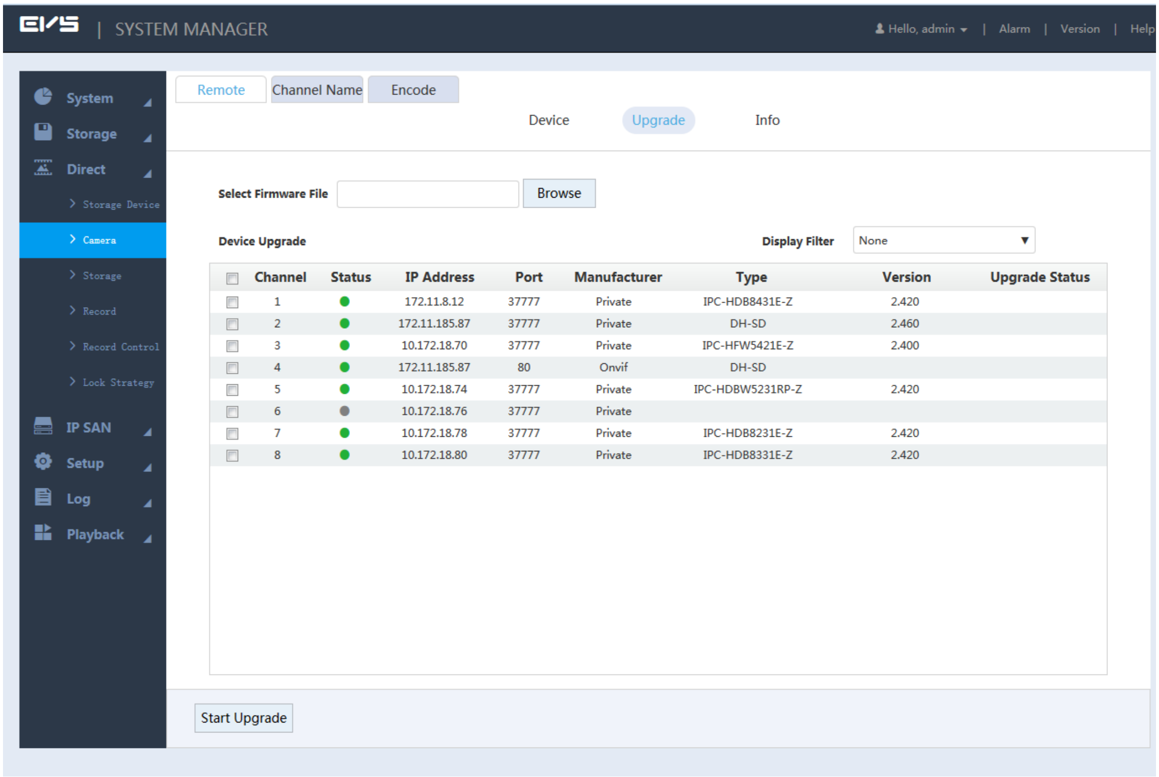
Preparation

You have got the corresponding upgrade file of the remote device.

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

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

Figure 3-122 Upgrading remote device



Select Firmware File

Device Upgrade

Display Filter: None

□	Channel	Status	IP Address	Port	Manufacturer	Type	Version	Upgrade Status
□	1	●	172.11.8.12	37777	Private	IPC-HDB8431E-Z	2.420	
□	2	●	172.11.185.87	37777	Private	DH-SD	2.460	
□	3	●	10.172.18.70	37777	Private	IPC-HFW5421E-Z	2.400	
□	4	●	172.11.185.87	80	Onvif	DH-SD		
□	5	●	10.172.18.74	37777	Private	IPC-HDBW5231RP-Z	2.420	
□	6	●	10.172.18.76	37777	Private			
□	7	●	10.172.18.78	37777	Private	IPC-HDB8231E-Z	2.420	
□	8	●	10.172.18.80	37777	Private	IPC-HDB8331E-Z	2.420	

Step 2 Select the device needed for upgrade.

NOTE

- It only supports to upgrade the devices whose **Status** is ●.
- When there are a large number of remote devices, you can select the type in the drop-down box of **Display Filter**.

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

Step 4 Click **Start Upgrade** and the system starts to upgrade the device.

3.10.2.1.5 Viewing Information

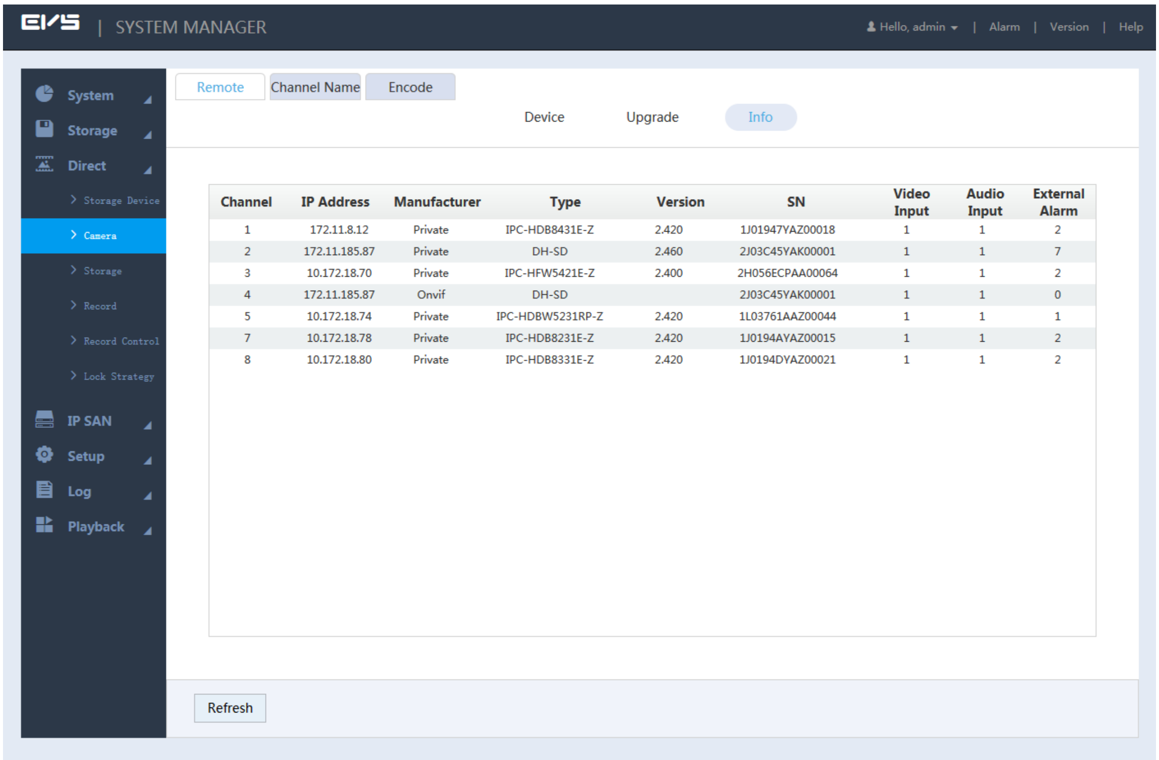
You can view the information of the remote devices, including channel, IP address, manufacturer, type, version, SN, video/audio input and external alarm.

Select **Direct** > **Camera** > **Remote** > **Info**. The **Info** interface is displayed. See Figure 3-123.

NOTE

Click **Refresh** to update the information.

Figure 3-123 Viewing device information



Channel	IP Address	Manufacturer	Type	Version	SN	Video Input	Audio Input	External Alarm
1	172.11.8.12	Private	IPC-HDB8431E-Z	2.420	1J01947YAZ00018	1	1	2
2	172.11.185.87	Private	DH-SD	2.460	2J03C45YAK00001	1	1	7
3	10.172.18.70	Private	IPC-HFW5421E-Z	2.400	2H056ECPAA00064	1	1	2
4	172.11.185.87	Onvif	DH-SD		2J03C45YAK00001	1	1	0
5	10.172.18.74	Private	IPC-HDBW5231RP-Z	2.420	1L03761AAZ00044	1	1	1
7	10.172.18.78	Private	IPC-HDB8231E-Z	2.420	1J0194AYAZ00015	1	1	2
8	10.172.18.80	Private	IPC-HDB8331E-Z	2.420	1J0194DYAZ00021	1	1	2

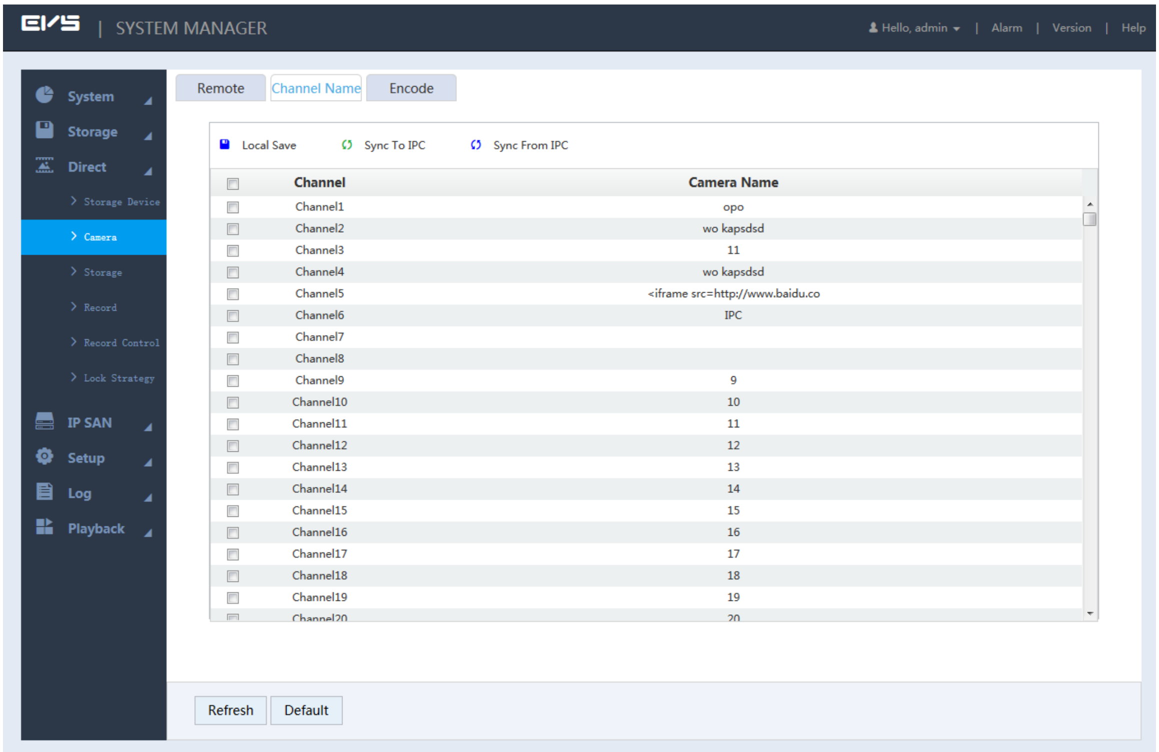
3.10.2.2 Channel Name Settings

EVS device supports to set the channel name of the remote device and locally store, front-end sync or front-end obtain the channel name.

Select **Direct** > **Camera** > **Channel Name**. The **Channel Name** interface is displayed. See Figure 3-124. For details, see Table 3-45.

Double-click the name of any channel and you can modify it.

Figure 3-124 Channel name



□	Channel	Camera Name
□	Channel1	opo
□	Channel2	wo kapsdsd
□	Channel3	11
□	Channel4	wo kapsdsd
□	Channel5	<iframe src=http://www.baidu.co
□	Channel6	IPC
□	Channel7	
□	Channel8	
□	Channel9	9
□	Channel10	10
□	Channel11	11
□	Channel12	12
□	Channel13	13
□	Channel14	14
□	Channel15	15
□	Channel16	16
□	Channel17	17
□	Channel18	18
□	Channel19	19
□	Channel20	20

Table 3-45 Description of channel name parameters

Parameter	Description
Local Store	Modify the channel name, select the corresponding channel, and then click 💾 . It only changes the channel name of the remote device in the Web interface and the device name will not be changed.
Sync To IPC	Modify the channel name, select the corresponding channel, and then click ⟳ . It changes both the channel name on the Web interface and the device name.
Sync From IPC	Select the channel and click ⟳ to get the name of the remote device.

3.10.2.3 Encoding Parameter Settings

Set the video encoding parameters, including the video stream, image stream and video overlay.

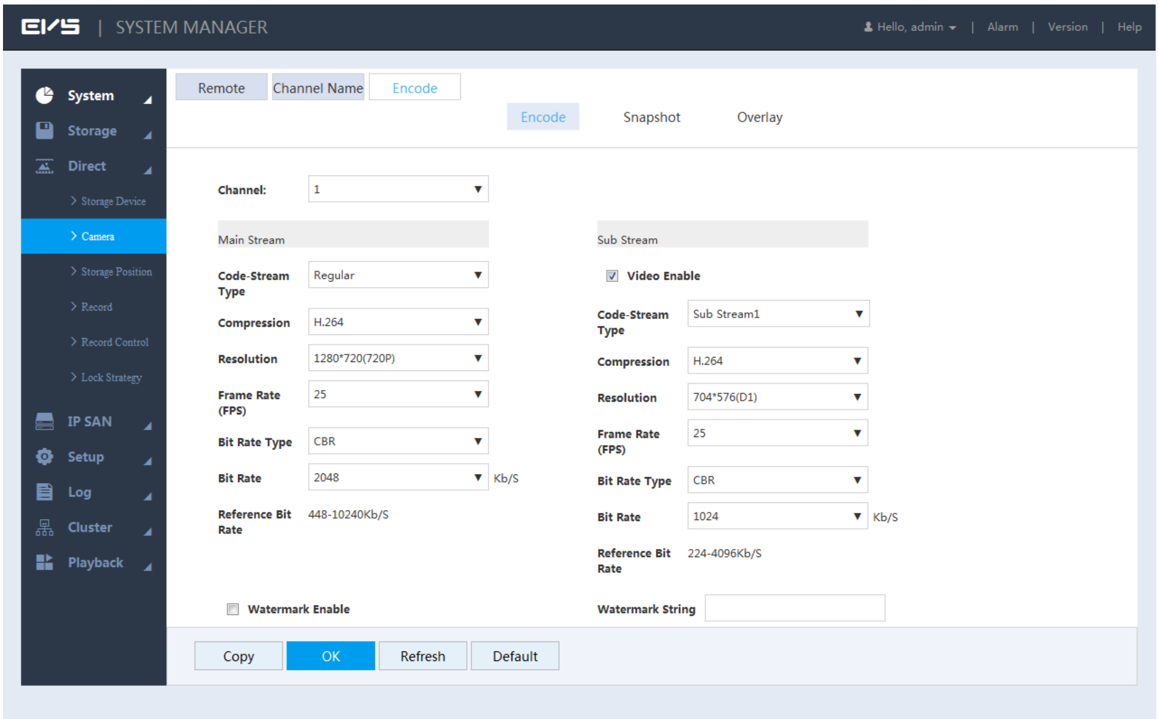
3.10.2.3.1 Stream Parameter Settings

Select/Enter the video stream parameters (such as stream type, encoding mode and resolution) according to the actual bandwidth situation.

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

The **Encode** interface is displayed. See Figure 3-125.

Figure 3-125 Encoding setting



Channel: 1

Main Stream

Code-Stream Type: Regular

Compression: H.264

Resolution: 1280*720(720P)

Frame Rate (FPS): 25

Bit Rate Type: CBR

Bit Rate: 2048 Kb/S

Reference Bit Rate: 448-10240Kb/S

□ 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

Watermark String:

Step 2 Select/Enter the parameters. For details, see Table 3-46.

Table 3-46 Description of encoding parameters

Parameter	Description
Channel	Select the channel number.
Video Enable	Select the Video Enable check box to open 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 vivid and smooth the image. FPS varies with the resolution.
Bit Rate Type	Select the stream control type of the video. ● CBR: The bit rate changes slightly near the set value. ● VBR: The bit rate varies with the monitoring scenario. NOTE ● It is recommend the select CBR when the monitoring scenario changes little and select VBR when the scenario changes much. ● MJPEG only corresponds to CBR.
Image Quality	Select the quality level (level 1-level 6). The larger the value, the better the quality. NOTE You can set this item only when selecting the VBR.

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 a best range. ● Sub stream: In CBR, the bit rate changes slightly near the set value. In VBR, the bit rate automatically changes with the image and keeps the max value near the set number.
Reference Bit Rate	The system recommends the best bit rate range according to the configured resolution and FPS.
Audio Enable	Select this check box and the record file is a combined flow of video and audio.
Audio Encoding	Select the audio encoding format.
Watermark Enable	Select this check box to confirm if the record was tempered with. NOTE For detailed introduction of watermark verification, see "3.6.2.3 Watermark Verification."
Watermark String	Enter the string for watermark verification. The default string is DigitalCCTV. NOTE The watermark string can only be composed of number(s), letter(s), underline and line-through. It contains 128 characters at most.
Apply to	After setting a channel, click **Apply to** and you can apply the settings to other channels.

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

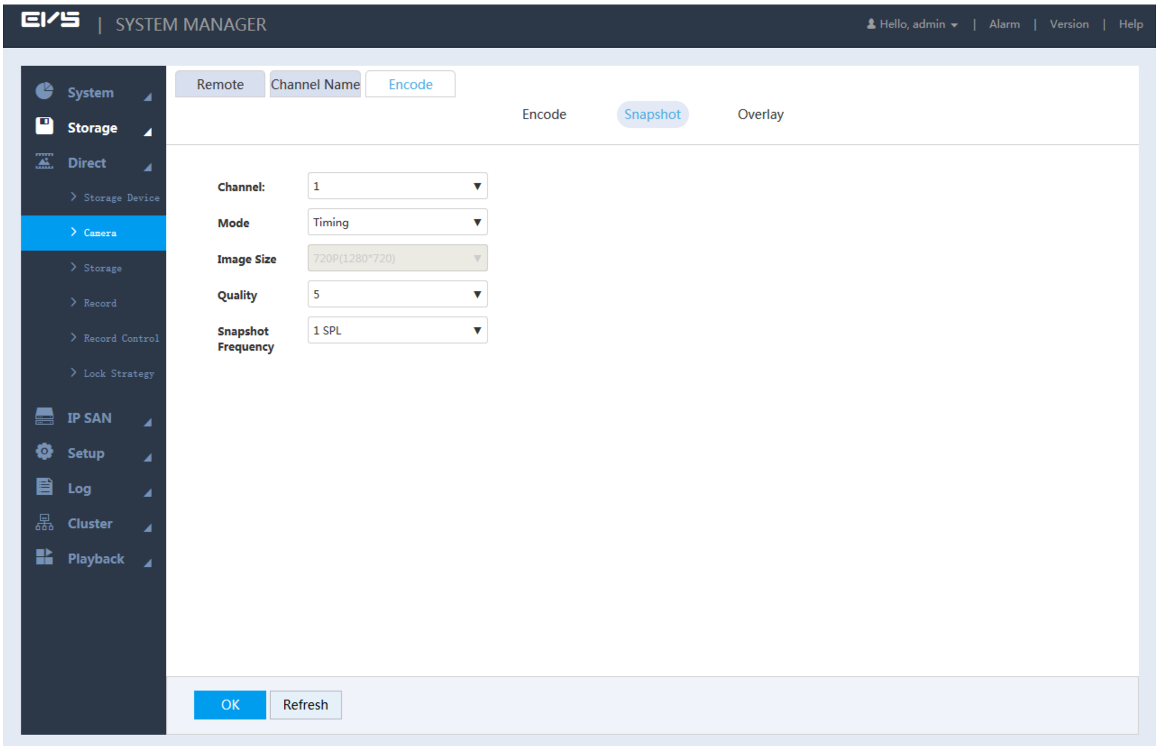
3.10.2.3.2 Image Stream Settings

Set the image stream parameters, including snapshot type, image size, image quality and snapshot frequency.

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

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

Figure 3-126 Image Stream



Channel: 1

Mode: Timing

Image Size: 720P(1280*720)

Quality: 5

Snapshot Frequency: 1 SPL

Step 2 Select the parameters. For details, see Table 3-47.

Table 3-47 Description of image stream parameters

Parameter	Description
Channel	Select the channel number.
Mode	Select the snapshot mode, including **Timing** and **Event**. ● Timing: Snapshot according to the set plan. For details, see "3.10.4.2 Snapshot Plan Settings." ● Event: Snapshot according to the set triggering events. For details, see "3.8.4 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 second/image to 7 second/image. Select **Custom** to define the frequency by yourself. You can set up to 3600 seconds/image.

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

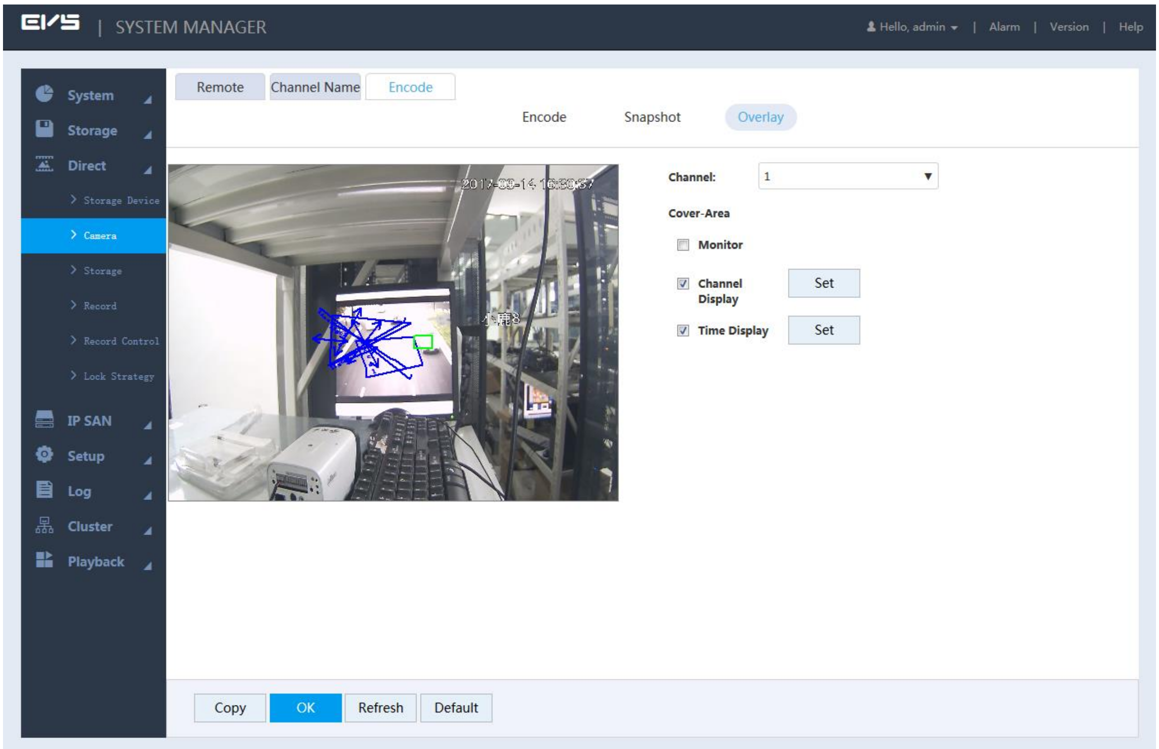
3.10.2.3.3 Video Overlay Settings

Configure the headline information of video overlay.

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

The **Overlay** interface is displayed. See Figure 3-127.

Figure 3-127 Video Overlay



Channel: 1

Cover-Area

□ Monitor

☑ Channel Display Set

☑ Time Display Set

Step 2 Select/Enter the parameters. For details, see Table 3-48.

Table 3-48 Description of video overlay parameters

Parameter	Description
Channel	Select the channel number.
Cover-Area	Select an area in the monitor screen as the cover-area which is blocked and unavailable to view. 1. Select the **Monitor** check box. 2. Select a cover-area in the monitor screen. You can drag the border to change the position and size of the area. 3. Click **OK** to save the configuration. NOTE Each channel supports up to four cover-areas.
Channel Display	Display the time headline or channel headline in the preview or monitor screen. 1. Select the **Channel Display** to **Time Display** check box. 2. Click the **Set** on the right side. 3. Drag the headline in the screen to the proper position. 4. Click **OK** to save the configuration.
Time Display	

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

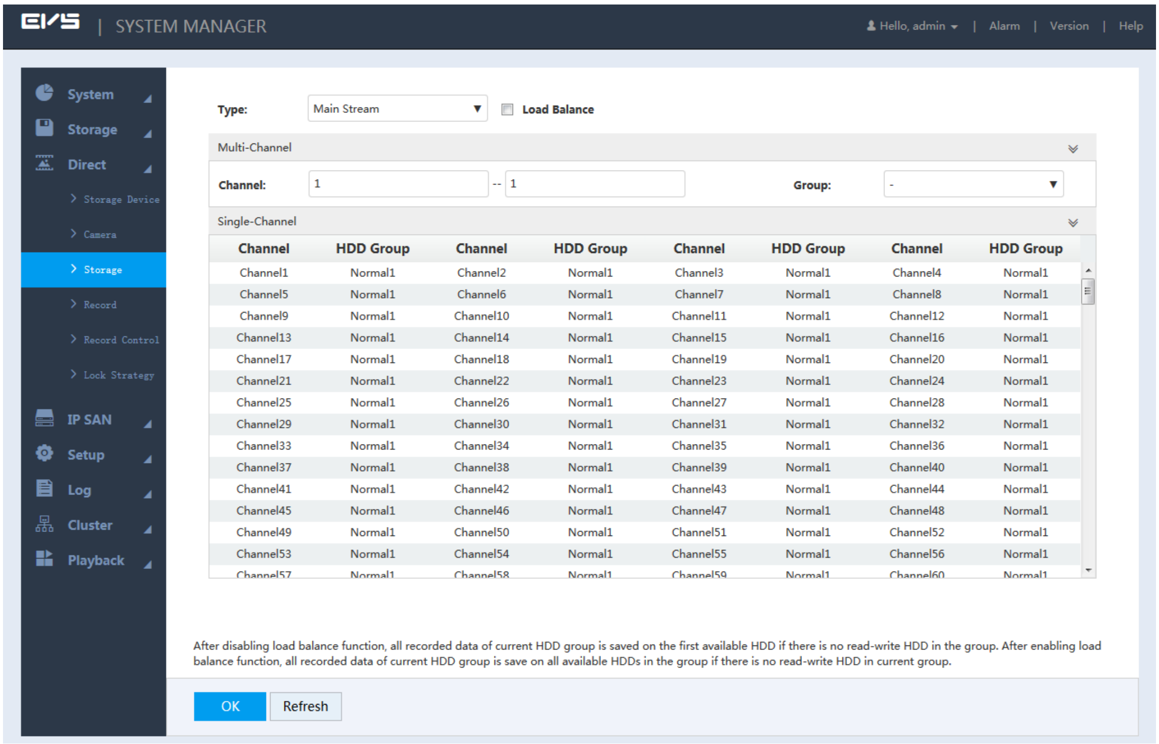
3.10.3 Storage Path Settings

Through HDD grouping, you can save the main stream, sub stream and images of the specified channel to the specified group.

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

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

Figure 3-128 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	Normal1	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 the record or image, including main stream, sub stream, image and image direct.

Step 3 (Optional) Select the **Load Balance** check box.

- Enabled load balance: If there is no read-write disk available in the group, records of all the channels from this group will be stored in one available group.
- Disabled load balance: If there is no read-write disk available in the group, records of all the channels from this group will be distributed to all the other available groups.

Step 4 Set the disk group of each channel.

You can choose to set the group for a single channel or set the group for multiple channels.

- Multiple-channel: Enter the channel range, such as 1-100, and set the group.
- Single-channel: Double-click the group corresponding to the channel and set it.

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

3.10.4 Record Plan Settings

You can select different channels and dates to do video recording during different periods. The system supports up to six periods. By configuring the real-time key frames and historical key frames, it can reduce the space that the records take.

3.10.4.1 Record Plan Settings

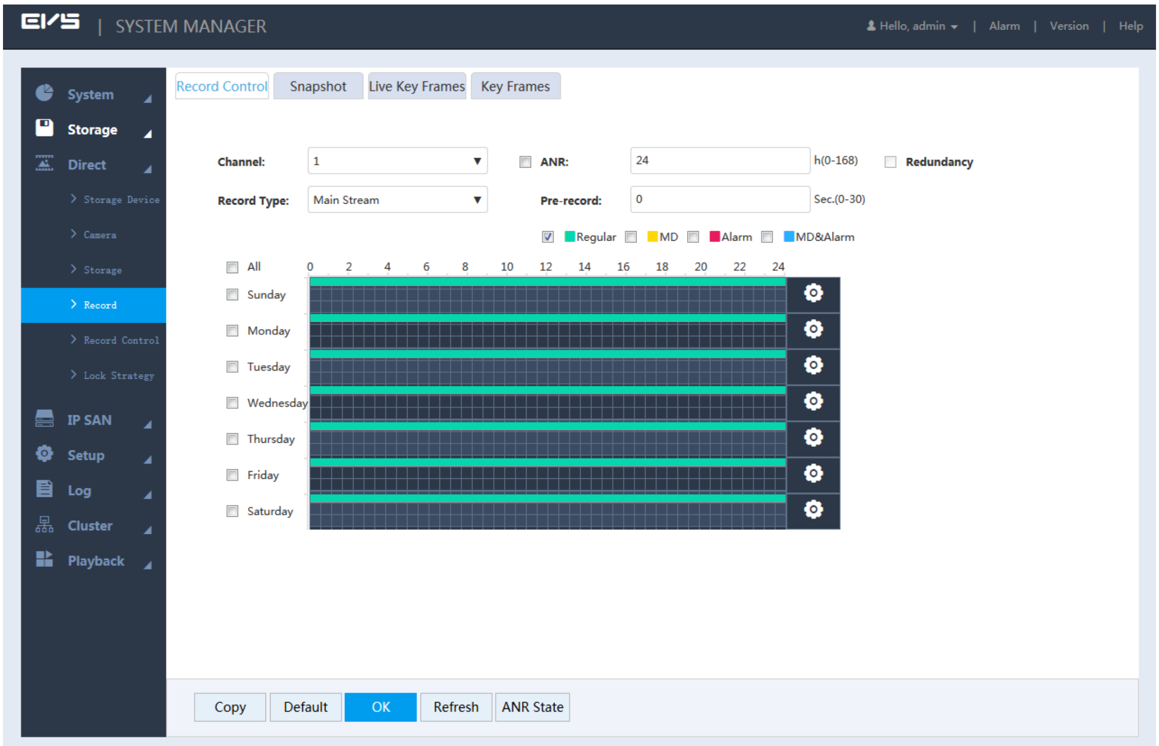
The system performs the corresponding video recording according to the set record plan. For example, when you set the time period of alarm videos to 6:00-18:00, the system automatically takes records if any alarm occurs during this period.

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** > **Record** > **Record Control**.

The **Record Control** interface is displayed. See Figure 3-129.

Figure 3-129 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

Step 2 Select/Enter the parameters. For details, see Table 3-49.

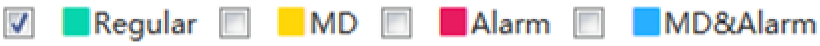
Table 3-49 Description of record parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.
ANR	Select the check box to open the function. ● When the network connection between the EVS device and IPC is broken, IPC keeps on recording. After the network recovery, the EVS 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. NOTE This function is available for IPC that has installed the SD card.

Parameter	Description
Redundancy	When multiple disks are available in the EVS device, select one disk to be the redundancy to realize the double backup of records. The records are stored in different disks at the same time to guarantee the data security. 1. For operations to set a redundant disk, see "3.10.1 Storage Device." 2. Select the check box to enable redundancy. ◇ If the selected channel is not recording a video, redundancy comes into effect 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. NOTE 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 record type. See Figure 3-130 Alarm type.

Figure 3-130 Alarm type



☑ 🟩Regular □ 🟨MD □ 🟥Alarm □ 🟦MD&Alarm

NOTE

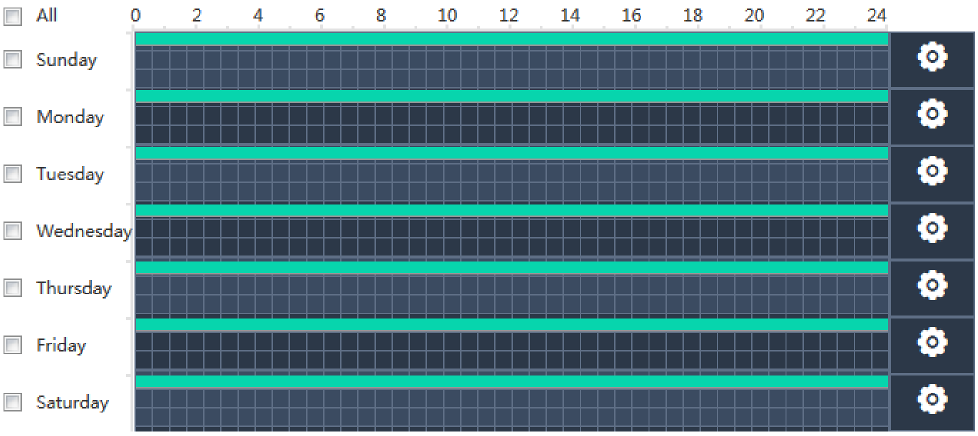
- When you select the **MD**, **Alarm** or **MD & Alarm**, you need to enable the alarm record linkage for the corresponding channel. For details, see "3.8.4 Configuring Events."
- The color bar in Figure 3-131 indicates the record type of the corresponding time period.

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

NOTE

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

Figure 3-131 Time period setting



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

- Drawing:

1) Select the weekday.

◇ Select the **All** check box and you can synchronously edit or draw the periods for all the weekdays.

◇ You can select multiple weekdays to edit at the same time.

2) Hold down 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. EVS device performs recording in the corresponding period.

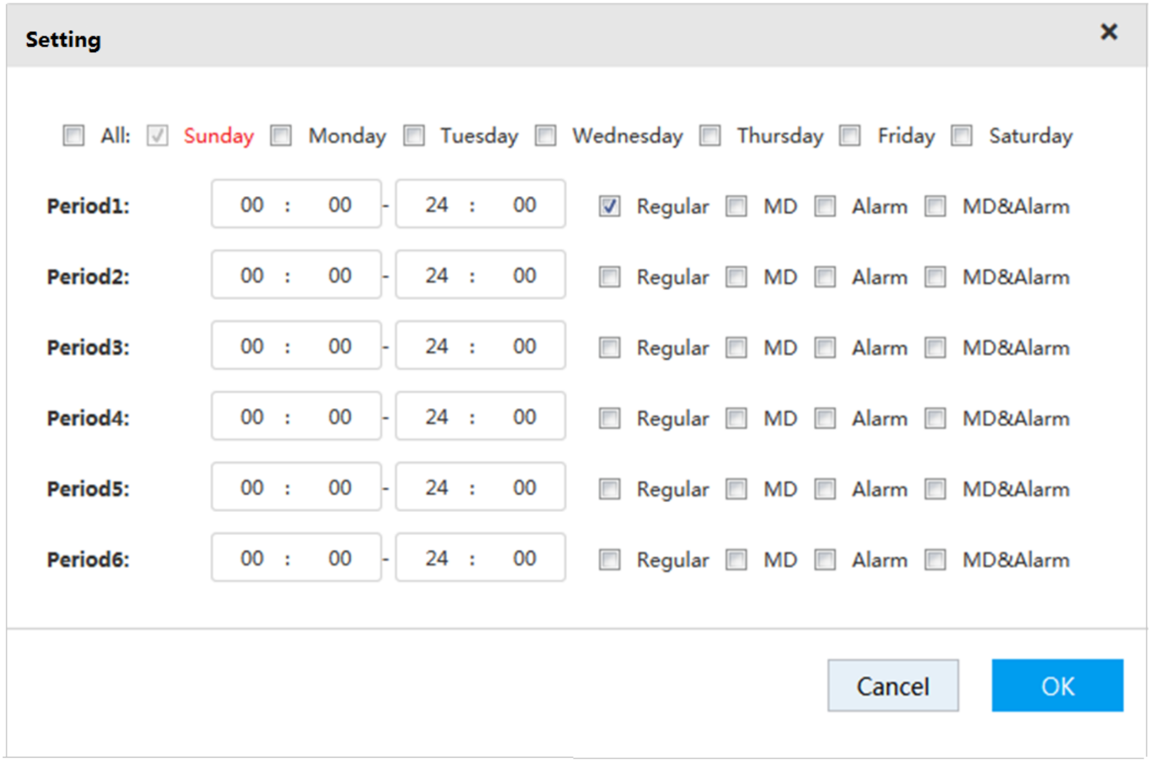
◇ When the record time is overlapped, see following for the record priority: MD & alarm > alarm > MD > regular.

- Editing:

1) Select the corresponding weekday and click ⚙.

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

Figure 3-132 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** interface.

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

NOTE

The record plan comes into effect after enabling the auto record function. For details to enabling auto record, see "3.10.5 Record Control."

3.10.4.2 Snapshot Plan Settings

The system performs the corresponding snapshot according to the set snapshot plan. For example, when you set the time period of snapshot to 6:00-18:00, the system automatically performs snapshot if any alarm occurs during this period.

Select **Direct** > **Record** > **Snapshot**.

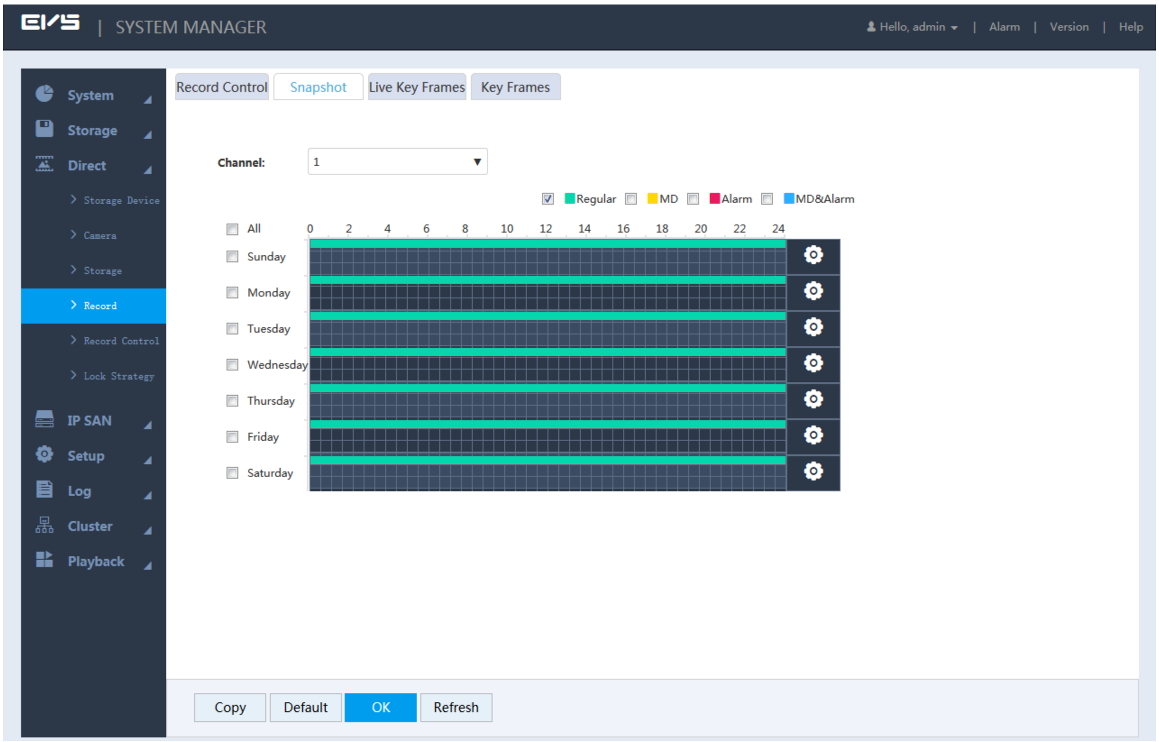
The **Snapshot** interface is displayed. See Figure 3-133.

The steps to set snapshot plan is the same as that of setting record plan. For details, see "3.10.4.1 Record Plan Settings."

NOTE

The snapshot plan comes into effect after enabling the auto snapshot function. For details to enabling auto snapshot, see "3.10.5 Record Control."

Figure 3-133 Snapshot



Channel: 1

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

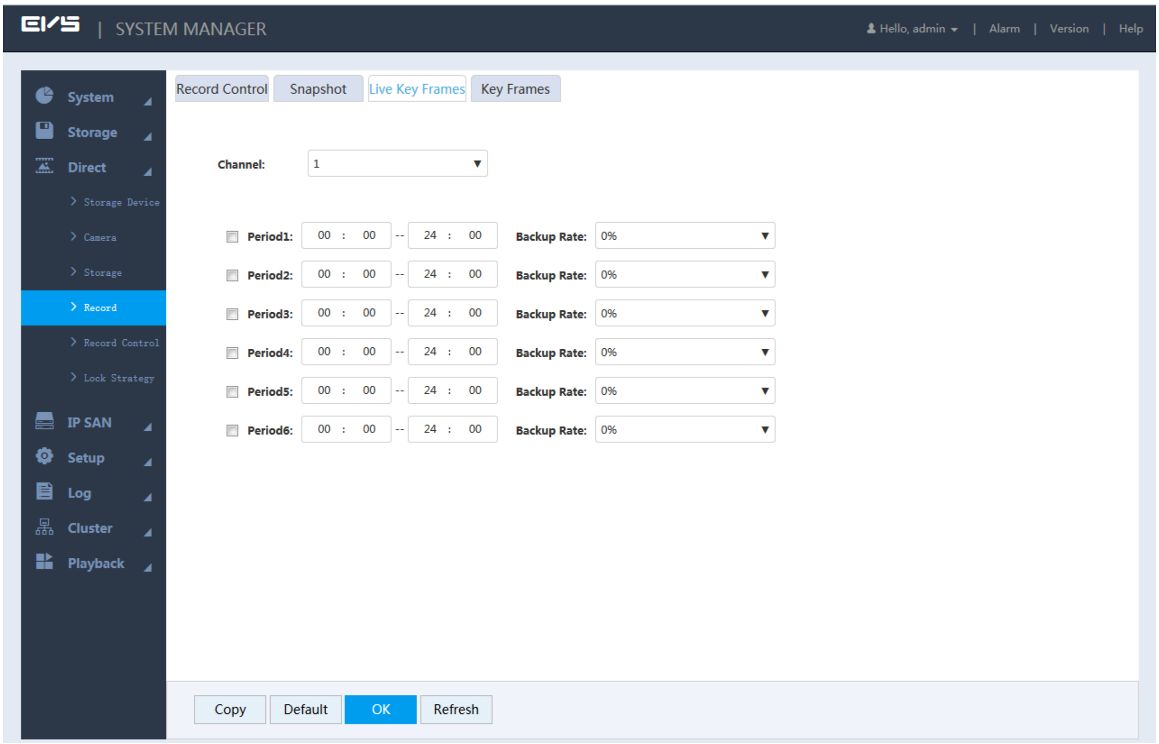
3.10.4.3 Real-Time Key Frame Settings

The system deletes some or all the non-key frames according to the backup rate, so as to reduce the space occupied by the records.

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

The **Live Key Frame** interface is displayed. See Figure 3-134.

Figure 3-134 Real-time 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 Select/Enter the parameters. For details, see Table 3-50.

Table 3-50 Description of real-time key frame parameters

Parameter	Description
Channel	Select the channel number. Select **All** to do the same setting for all the channels.
Period	You can set six periods at most.
Backup Rate	Select the backup rate of each period. NOTE Backup rate means the retention rate of non-key frames. For example, when the backup rate is 0%, all the non-key frames will be extracted. When the backup rate is 100%, all the non-key frames will be retained.

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

3.10.4.4 Historical Key Frame Settings

When the storage space is limited and you want to keep long-time records, you can use the historical frames to delete the non-key frames in the stored records and only keep the key frames, so as to release storage space and improve space utilization rate. But the smoothness and continuity of the record will be affected.

CAUTION

- After enabling the historical key frames, part of the record data will be deleted and only the key frame data will be kept.
- Frame extract will affect the record smoothness and continuity. Be careful to perform it.

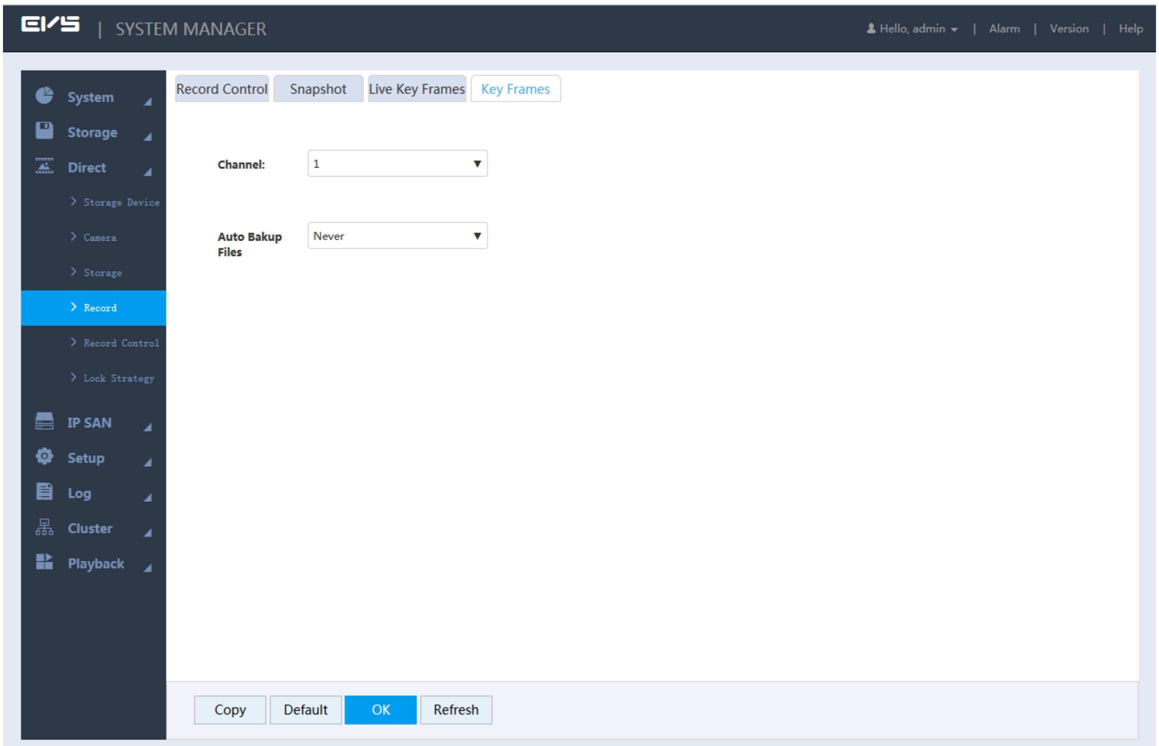
Preparation

You need to set an independent disk to store the record files after extracting. The original records in the disk will be deleted. For details, see "3.10.1 Storage Device."

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

The **Key Frames** interface is displayed. See Figure 3-135.

Figure 3-135 Historical key frames



Channel: 1

Auto Bakup Files: Never

Step 2 Select the parameters. For details, see Table 3-51.

Table 3-51 Description of historical key frame parameters

Parameter	Description
Channel	Select the channel number. Select **All** to do the same setting for all the channels.
Auto Backup File	Select the way to back up files automatically. ● Never: Do not extract any frame. ● Custom: You can select to extract frames for records three days to 30 days ago, and store the key records in the independent disk.

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

3.10.5 Record Control

After setting the record plan and snapshot plan, you need to enable the auto record and auto snapshot function so that the system can perform automatically.

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

- 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.

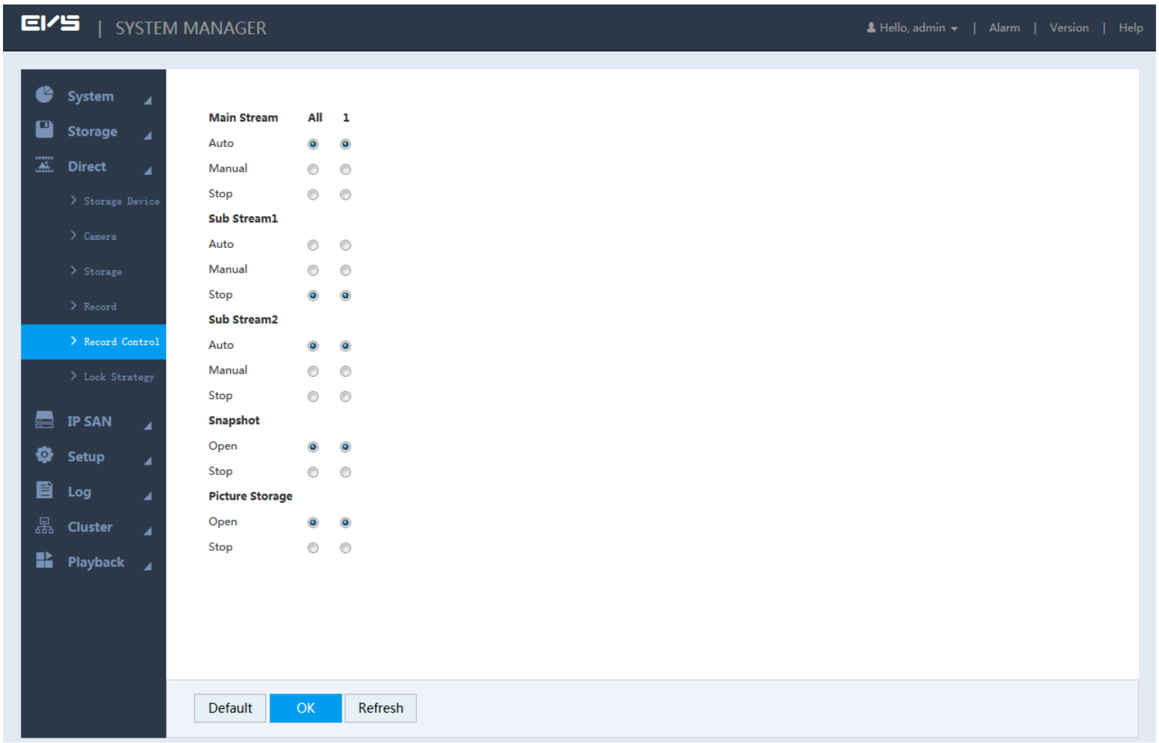
CAUTION

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

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

The **Record Control** interface is displayed. See Figure 3-136.

Figure 3-136 Record control



Main Stream	All	1
Auto	●	●
Manual	○	○
Stop	○	○
Sub Stream1		
Auto	○	○
Manual	○	○
Stop	●	●
Sub Stream2		
Auto	●	●
Manual	○	○
Stop	○	○
Snapshot		
Open	●	●
Stop	○	○
Picture Storage		
Open	●	●
Stop	○	○

Step 2 Select the parameters. For details, see Table 3-52.

Table 3-52 Description of record control parameters

Parameter	Description
Channel	Display all the channels with remote devices added. You can select a single channel or multiple channels or select **All** for all the channels.
Status	Display 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 the **Manual**. ● Auto: Taking records according to the set record plan (regular, MD and alarm). For details, see "3.10.4.1 Record Plan Settings." ● Stop: All the channels stop recording.
Sub Stream	
Snapshot	Select single or multiple channels and open/close the snapshot of the corresponding channel.
Picture Storage	Select single or multiple channels and open/close the image direct storage in the corresponding channel.

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

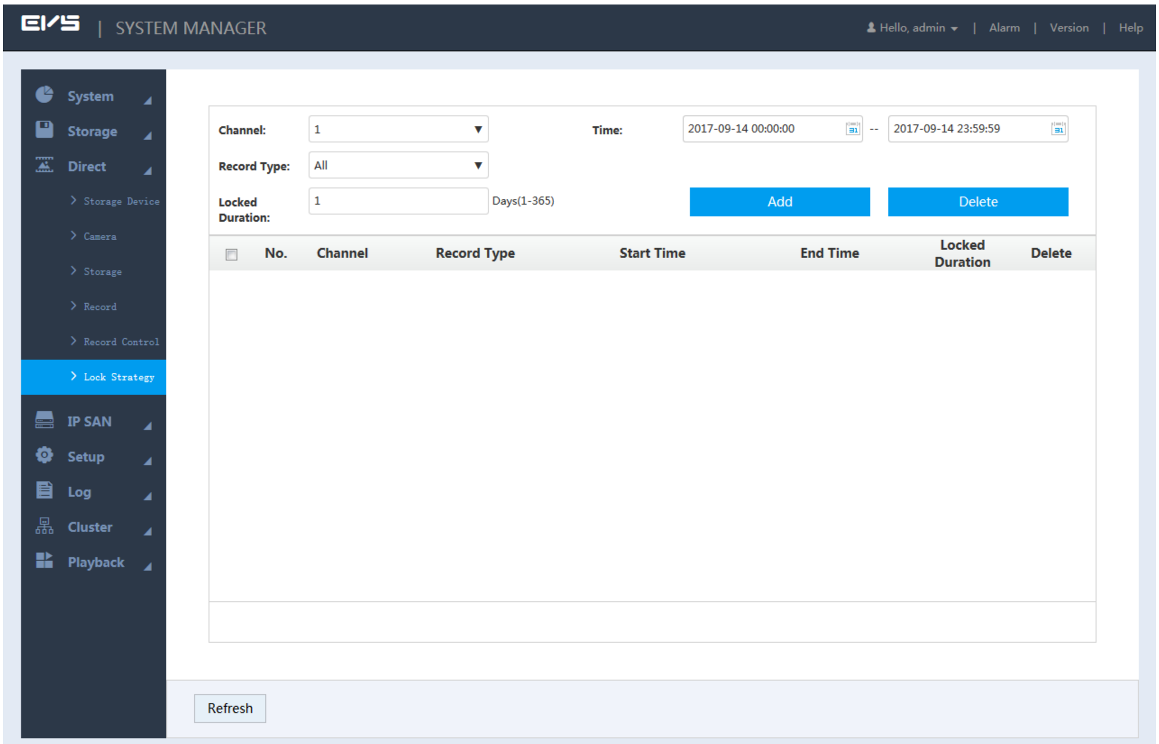
3.10.6 Lock Strategy

Lock the record to avoid being deleted.

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

The **Lock Strategy** interface is displayed. See Figure 3-137.

Figure 3-137 Lock strategy



Channel: 1

Time: 2017-09-14 00:00:00 -- 2017-09-14 23:59:59

Record Type: All

Locked Duration: 1 Days(1-365)

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

Step 2 Select/Enter the parameters. For details, see Table 3-53.

Table 3-53 Description of lock strategy parameters

Parameter	Description
Channel	Select the channel number. Select **All** to do the same setting for all the channels.
Time	Select the time period to lock the record.
Record Type	Select the record type to be locked, including all, regular, external and MD.
Locked Duration	Enter the duration of the lock during which the locked record will not be deleted.

Step 3 Click **Add**.

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

NOTE

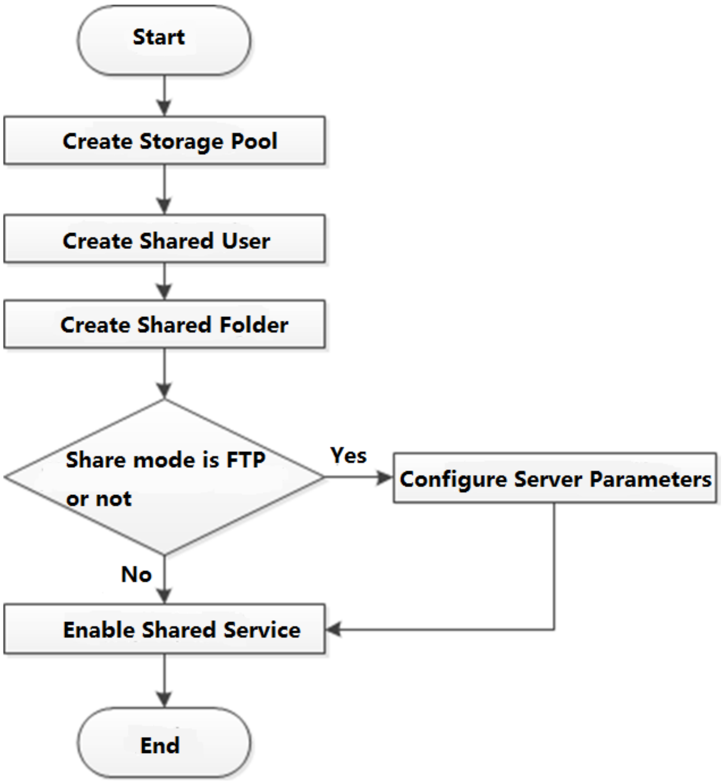
Click 🗑 to unlock the record file.

3.11 IPSAN

Internet Protocol Storage Area Network (IPSAN) 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 flow to configure the IPSAN, see Figure 3-138.

Figure 3-138 Configuring IPSAN



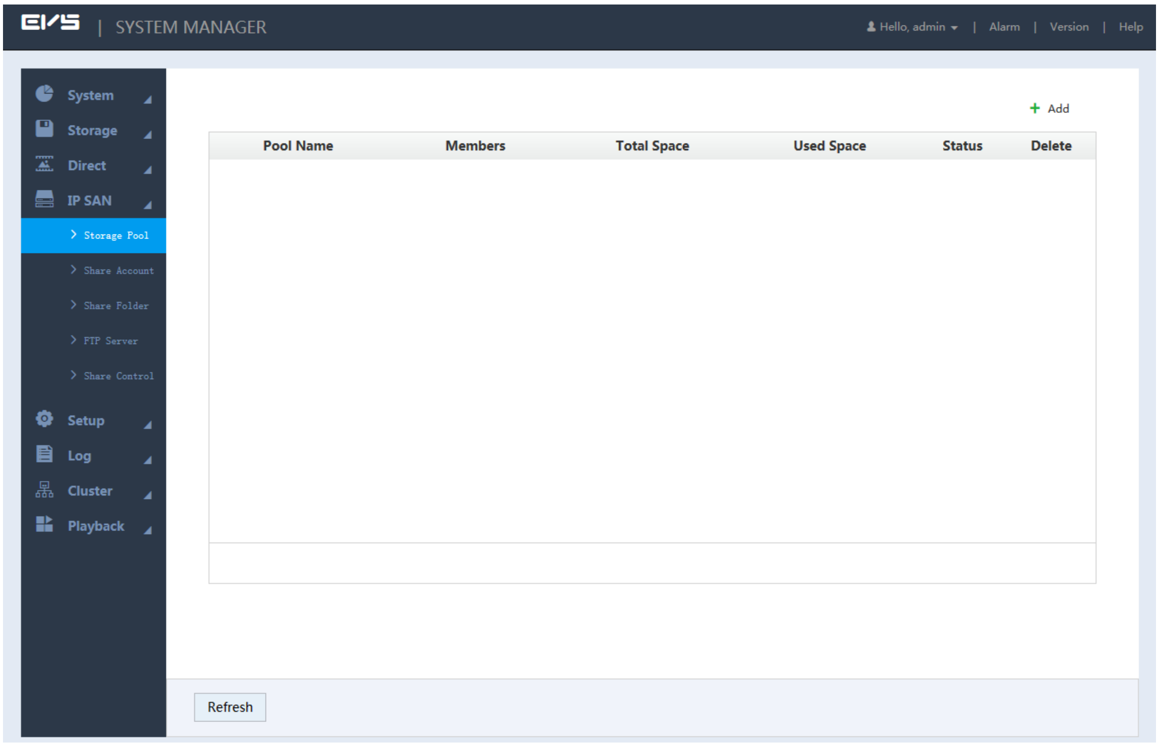
3.11.1 Creating Storage Pool

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.

Step 1 Select **IPSAN** > **Storage Pool**.

The **Storage Pool** interface is displayed. See Figure 3-139.

Figure 3-139 Storage pool

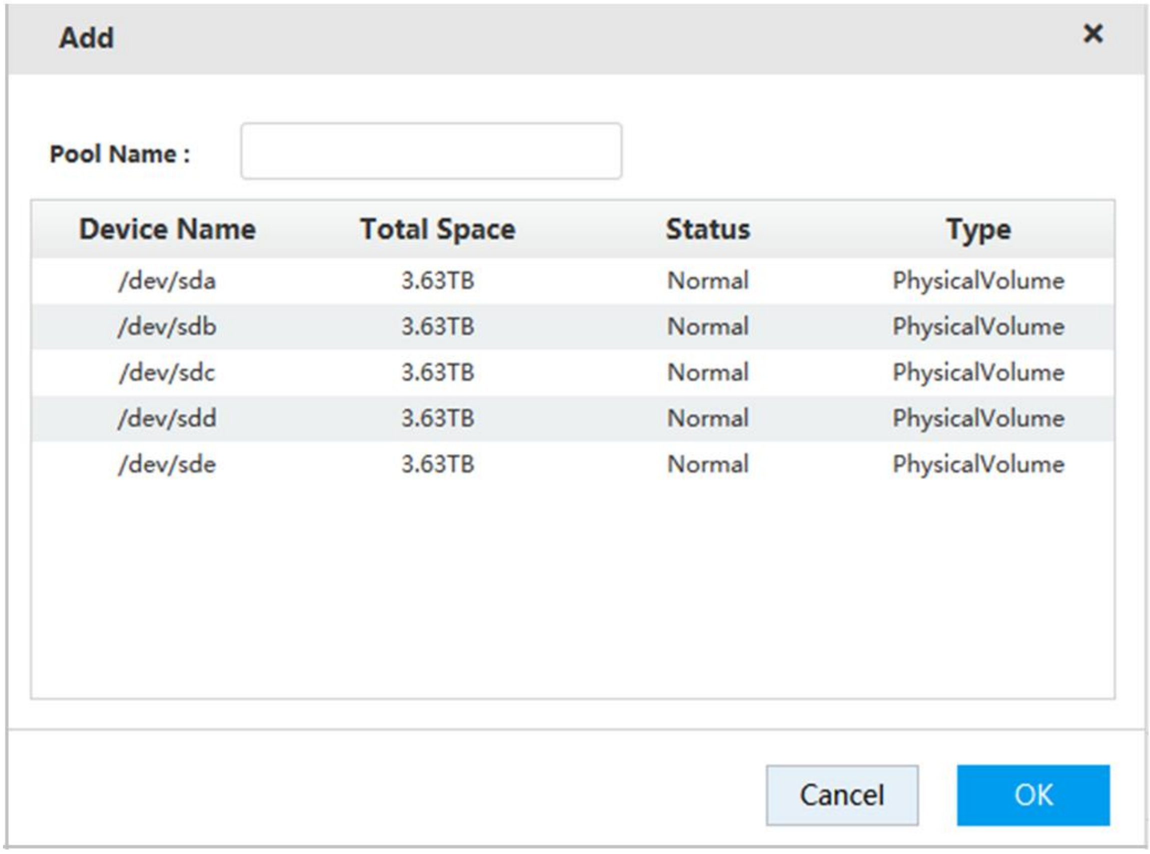


Pool Name	Members	Total Space	Used Space	Status	Delete

Step 2 Click + .

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

Figure 3-140 Adding storage pool



Pool Name :

Device Name	Total Space	Status	Type
/dev/sda	3.63TB	Normal	PhysicalVolume
/dev/sdb	3.63TB	Normal	PhysicalVolume
/dev/sdc	3.63TB	Normal	PhysicalVolume
/dev/sdd	3.63TB	Normal	PhysicalVolume
/dev/sde	3.63TB	Normal	PhysicalVolume

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

NOTE

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

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

The system returns to the **Storage Pool** interface. You can view the new pool information here.

NOTE

Click 🗑 to delete the pool. Click **Refresh** to get the latest configuration.

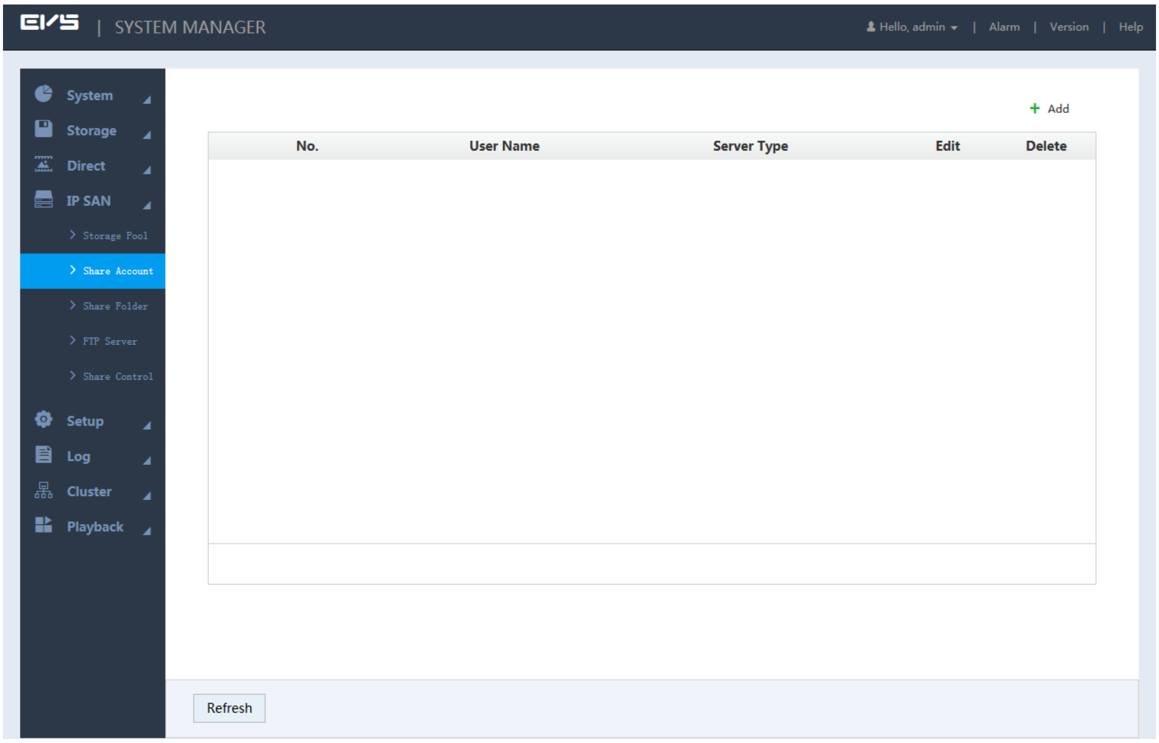
3.11.2 Shared Account Management

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

Step 1 Select **IPSAN** > **Shared Account**.

The **Shared Account** interface is displayed. See Figure 3-141.

Figure 3-141 Shared account management

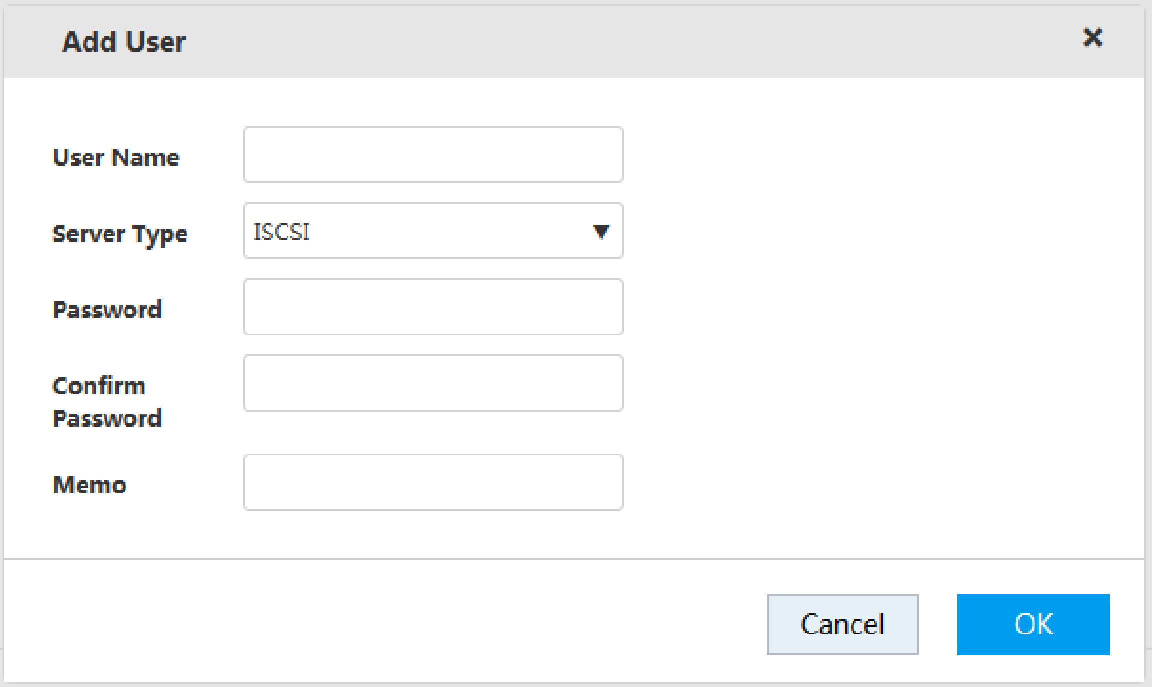


No.	User Name	Server Type	Edit	Delete

Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-142.

Figure 3-142 Adding shared user


Add User

User Name	
Server Type	ISCSI
Password	
Confirm Password	
Memo	

Step 3 Select/Enter the parameters. For details, see Table 3-54.

Table 3-54 Description of adding user parameters

Parameter	Description
User Name	Enter the name of the shared account.
Server Type	Select the corresponding service type of the shared account.
Password	Enter and confirm the password of the shared account. NOTE 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 **Shared Account** interface. You can view the new account information here.

NOTE

Click 🗑 to delete the account. Click ✎ to edit the account. Click **Refresh** to get the latest stored information.

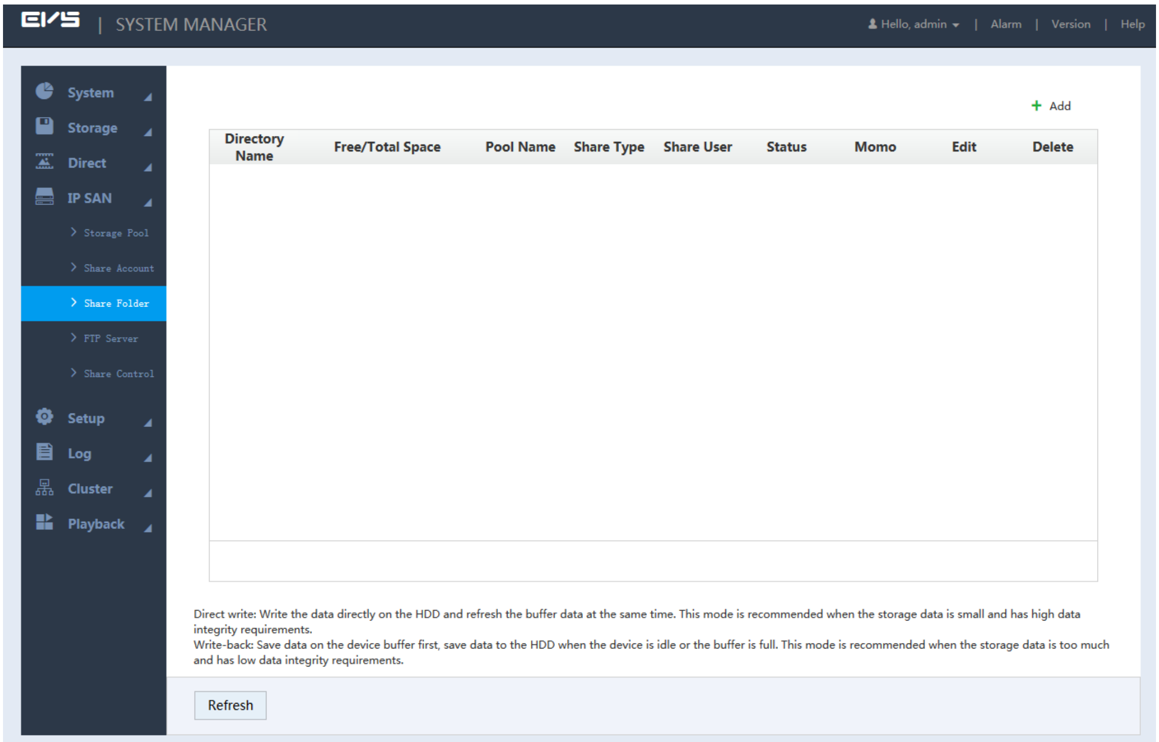
3.11.3 Shared Folder Settings

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

Step 1 Select **IPSAN** > **Shared Folder**.

The **Shared Folder** interface is displayed. See Figure 3-143.

Figure 3-143 Shared folder



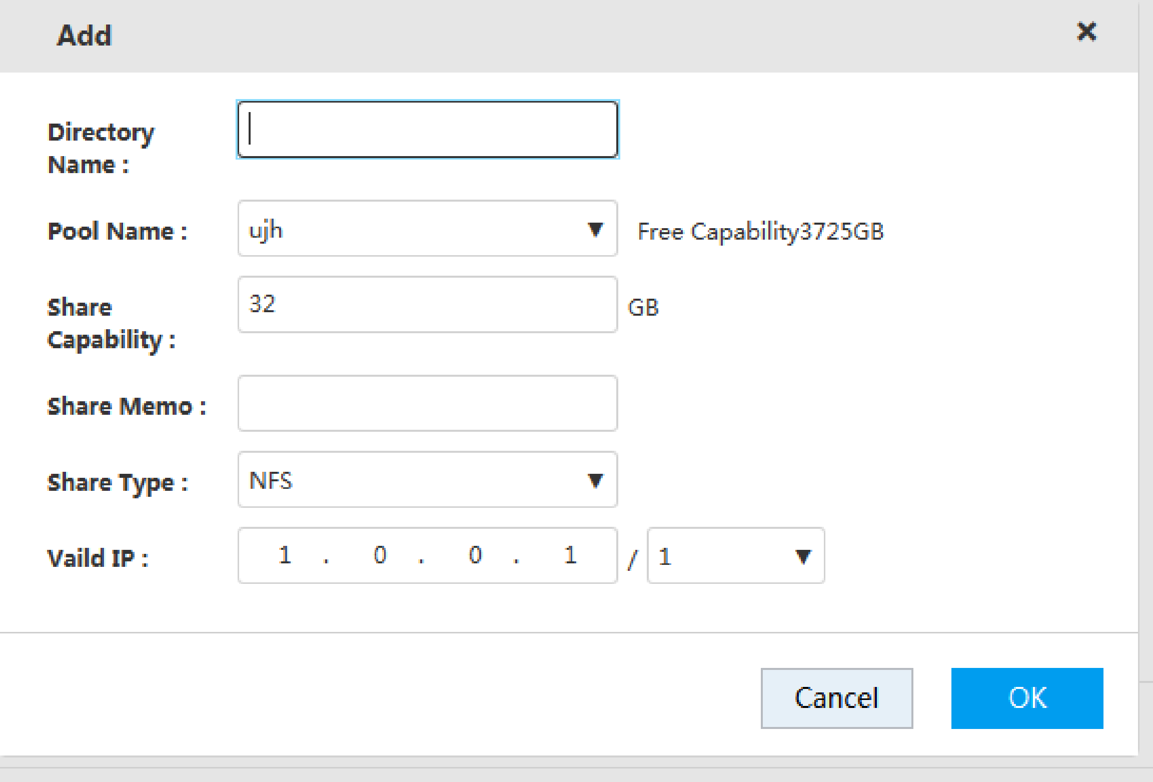
Directory Name	Free/Total Space	Pool Name	Share Type	Share User	Status	Momo	Edit	Delete

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 **+** .

The **Add** interface is displayed. See Figure 3-144 or Figure 3-145.

Figure 3-144 Adding shared folder (1)



Directory Name :

Pool Name : ujh Free Capability3725GB

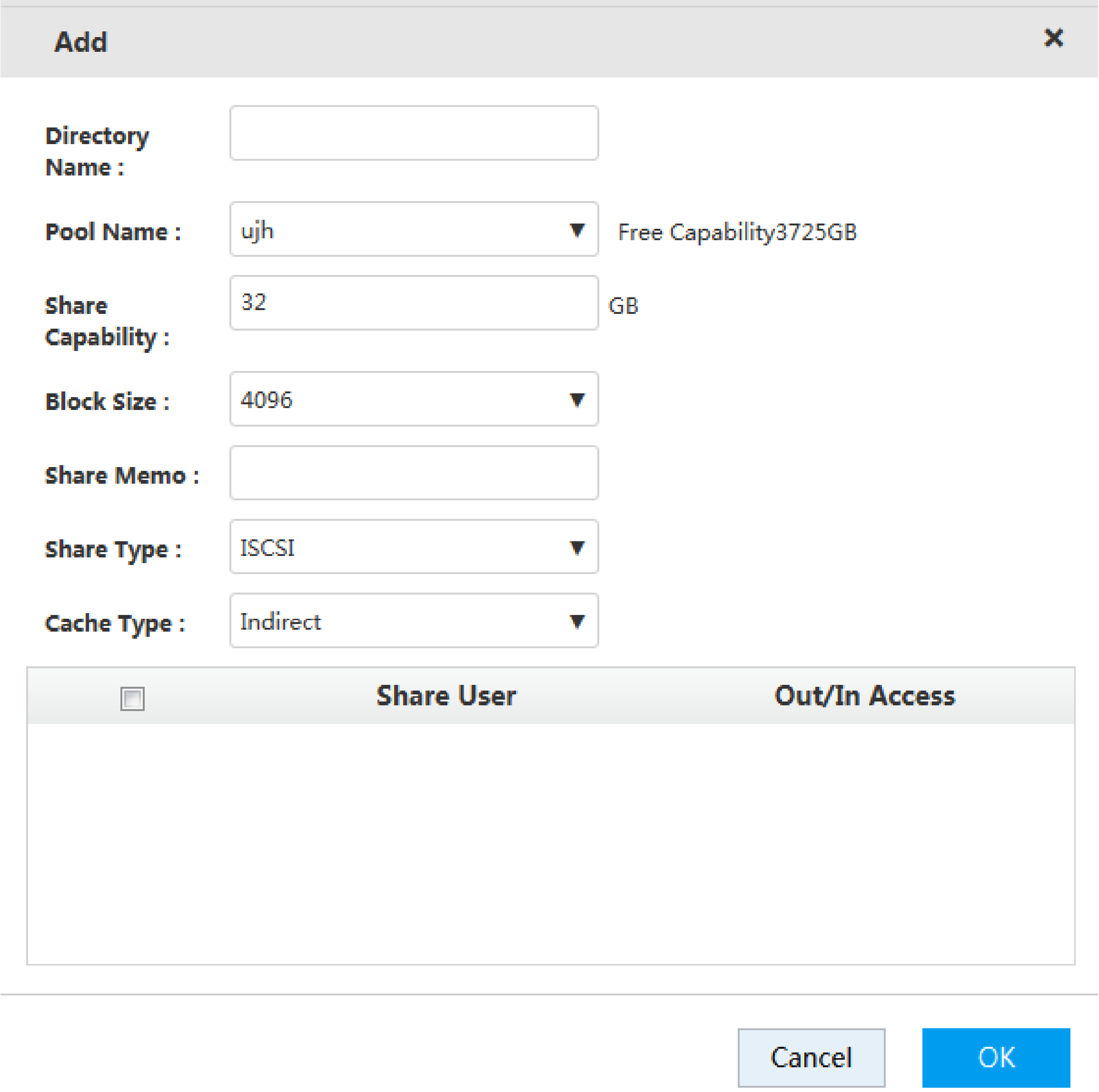
Share Capability : 32 GB

Share Memo :

Share Type : NFS

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

Figure 3-145 Adding shared folder (2)



Add

Directory Name :	
Pool Name :	ujh ▼ Free Capability3725GB
Share Capability :	32 GB
Block Size :	4096 ▼
Share Memo :	
Share Type :	ISCSI ▼
Cache Type :	Indirect ▼

□	Share User	Out/In Access

Step 3 Select/Enter the parameters. For details, see Table 3-55.

Table 3-55 Description of shared folder parameters

Parameter	Description
Directory Name	Enter the name of the shared folder.
Pool Name	Select the pool in which you need to create the shared folder. NOTE Free capability refers to the max available volume of the storage pool.
Share Capability	Enter the available space of the shared folder.
Share Memo	(Optional)It helps to recognize and manage the shared 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.

Parameter	Description
Valid IP	Select the IP range of the host authorized to access the shared folder. It supports 32 IPs at most. NOTE This needs to be set when the share type is NFS.
Valid User	Select the shared user and set its out/in access authority. ● When the **Share Type** is set to 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 to iSCSI and no valid user is selected, all the users have the access permission. NOTE ● 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. NOTE You need to configure this item when the share type is iSCSI.
Block Size	Select the block size of the shared folder, including 512Byte, 1024Byte, 2048Byte and 4096Byte. NOTE 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 **Shared Folder** interface. You can view the new shared folder information here.

NOTE

- When you create the shared folder for the first time or create shared folder under the condition of system auto maintenance, the system will force off the auto maintenance. After configuring the IPSAN, you can enable auto maintenance manually. For details, see "3.8.6.1 Automatic Maintenance."
- Click 🗑 to delete shared folder. Click ✎ to edit the folder. Click **Refresh** to get the latest configuration.
- In the process of iSCSI shared folder editing, you need to restart the EVS device to enable the switch of cache type.

3.11.4 FTP Parameter Settings

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

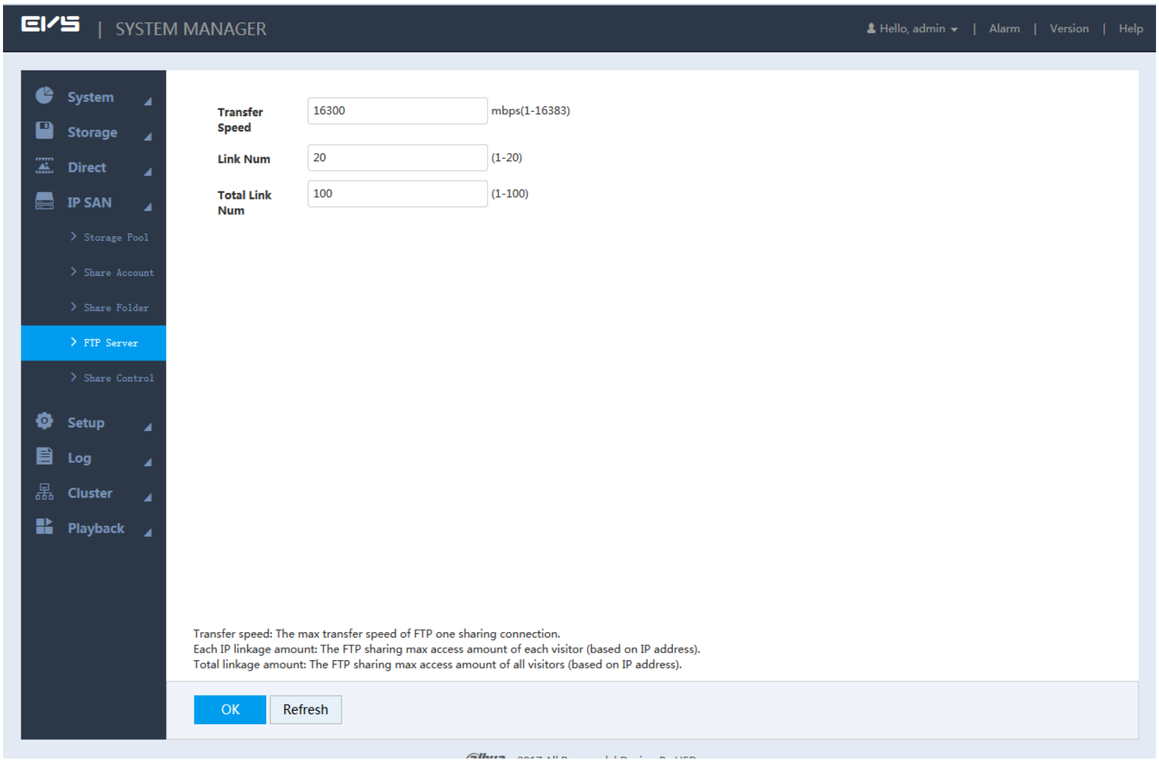
NOTE

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

Step 1 Select **IPSAN** > **FTP Server**.

The **FTP Server** interface is displayed. See Figure 3-146.

Figure 3-146 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. For details, see Table 3-56.

Table 3-56 Description of 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 connection number 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.

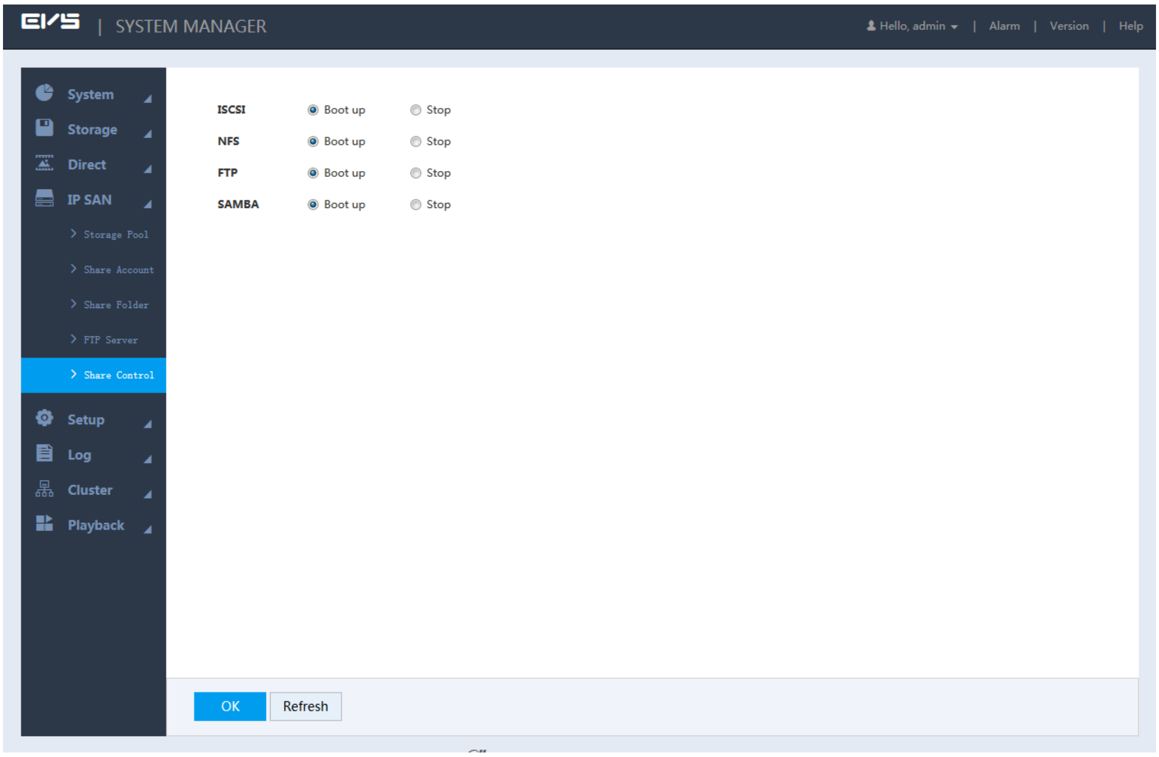
3.11.5 Opening Shared Services

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

Step 1 Select **IPSAN** > **Share Control**.

The **Share Control** interface is displayed. See Figure 3-147.

Figure 3-147 Share control



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

Step 2 Boot up or stop the shared service according to actual needs.

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

3.12 Cluster Service

Cluster function, also known as cluster redundancy function, is a way to improve the reliability of the device.

Create N master devices and M backup devices in the cluster (N + M mode) and provide virtual IP address (cluster IP) for unified login and management. Normally, the master devices are working. When the master device breaks down, the backup device will replace it to work according to the configuration of the master one and the cluster IP. After the master one is restored, the backup one transmits back the configuration, cluster IP and records during the breakdown, and the master one goes on working.

There is a management server called DSC (Dispatching Console) in the N + M cluster, which performs timely dispatching for the master devices and backup devices. When the cluster is created in EVS device, the EVS device is used as the DCS by default.

NOTE

Dual-control device does not support cluster.

3.12.1 Configuring Cluster

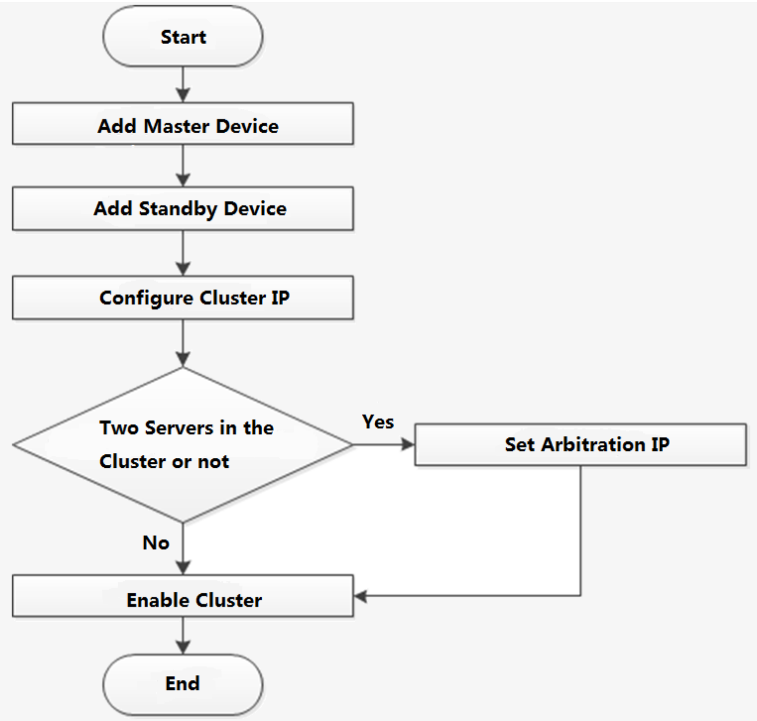
It includes creating cluster, viewing cluster information, restoring master device and setting arbitration IP.

3.12.1.1 Creating Cluster

Creating cluster refers to organizing multiple EVS devices into a cluster. For the creation flow, see Figure 3-148.

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

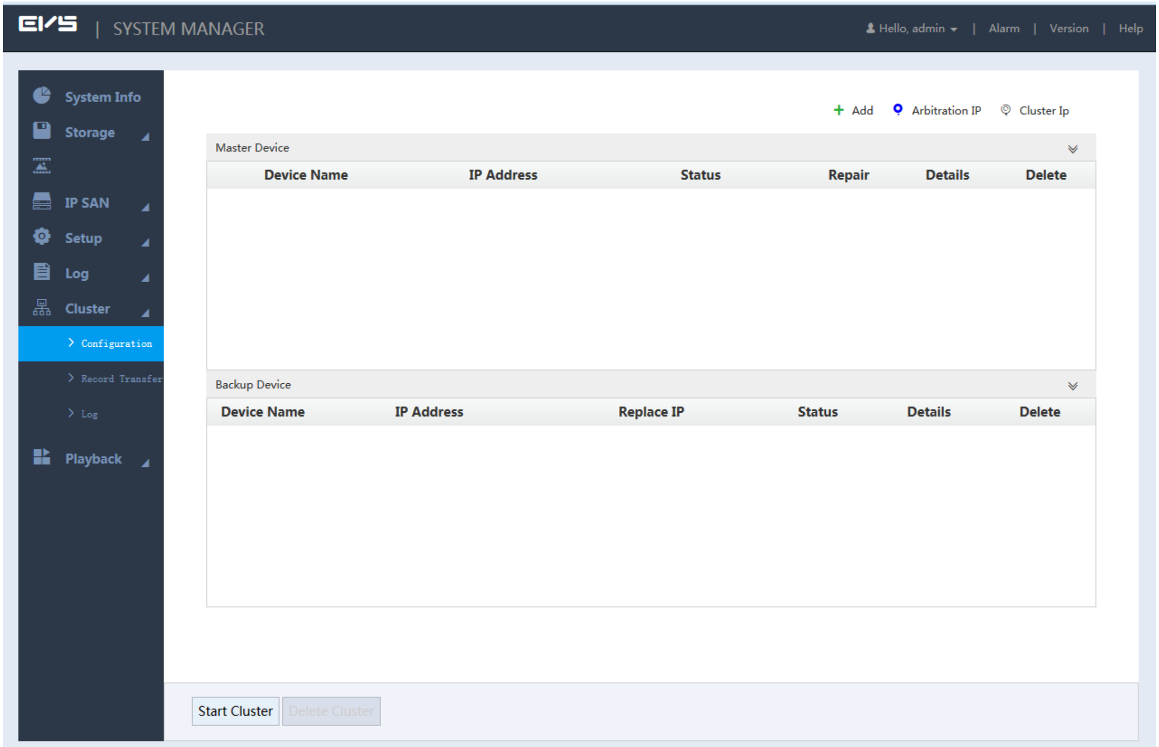
Figure 3-148 Creating cluster



Step 1 Select **Cluster** > **Configuration**.

The **Configuration** interface is displayed. See Figure 3-149.

Figure 3-149 Cluster configuration

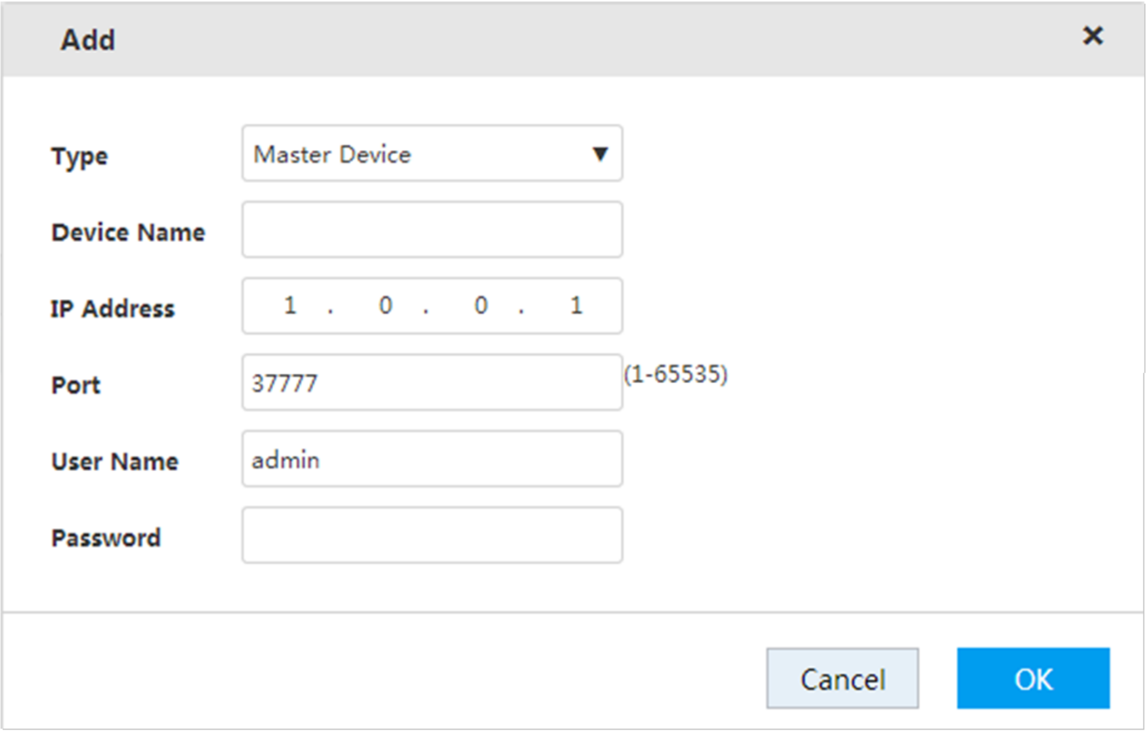


Step 2 Adding master device or backup device.

1) Click + .

The **Add** interface is displayed. See Figure 3-150.

Figure 3-150 Adding master/backup device



Type: Master Device ▼

Device Name:

IP Address: 1 . 0 . 0 . 1

Port: 37777 (1-65535)

User Name: admin

Password:

2) Select/Enter the parameters. For details, see Table 3-57.

Table 3-57 Description of server parameters

Parameter	Description
Type	Select the device type, including master device and backup device.

Parameter	Description
Device Name	Enter the device name.
IP Address	Enter the IP address of the master or backup device. That is, the IP address of the EVS device. 📖 NOTE You do not need to enter the IP address of the first backup device. The system takes the current EVS device as the first backup device by default.
Port	The default value is 37777.
User Name	Enter the user name and password of the master device or backup device. That is, the user name and password you use to access the Web of EVS device.
Password	

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

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

Step 3 Setting cluster IP.

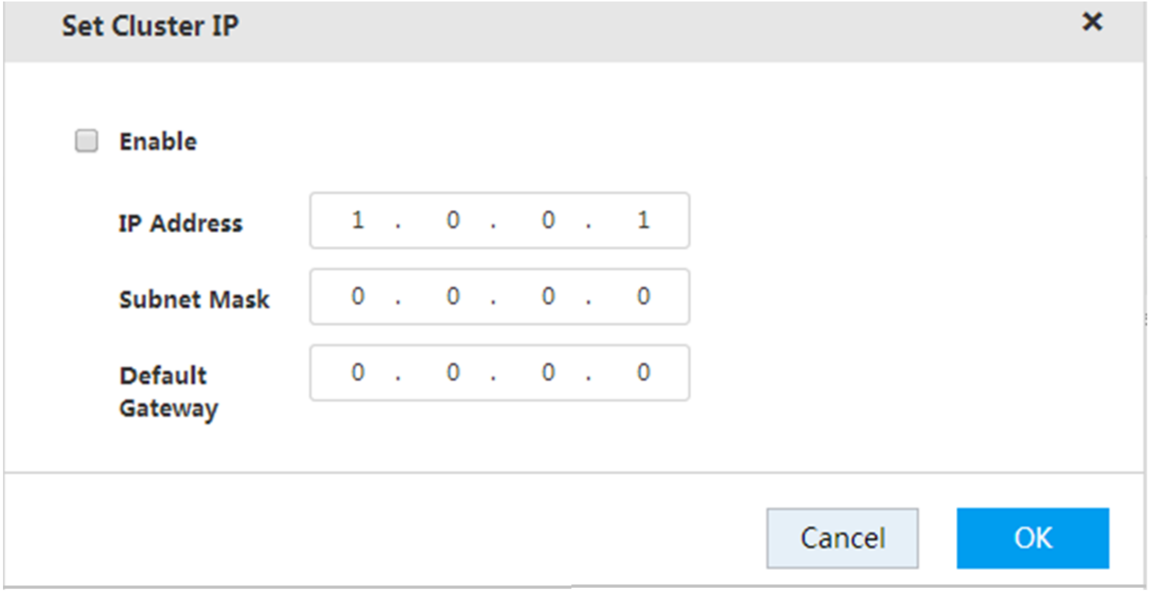
📖 NOTE

Cluster IP configuration refers to creating a virtual IP address and you can access and manage the master and backup devices in the cluster through this virtual IP. Logging in with the virtual IP, you can still view real-time monitoring when the backup device replaces the fault master device.

1) Click .

The **Set Cluster IP** interface is displayed. See Figure 3-151.

Figure 3-151 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** check box. Enter the **IP Address**, **Subnet Mask** and **Default Gateway**.

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

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

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

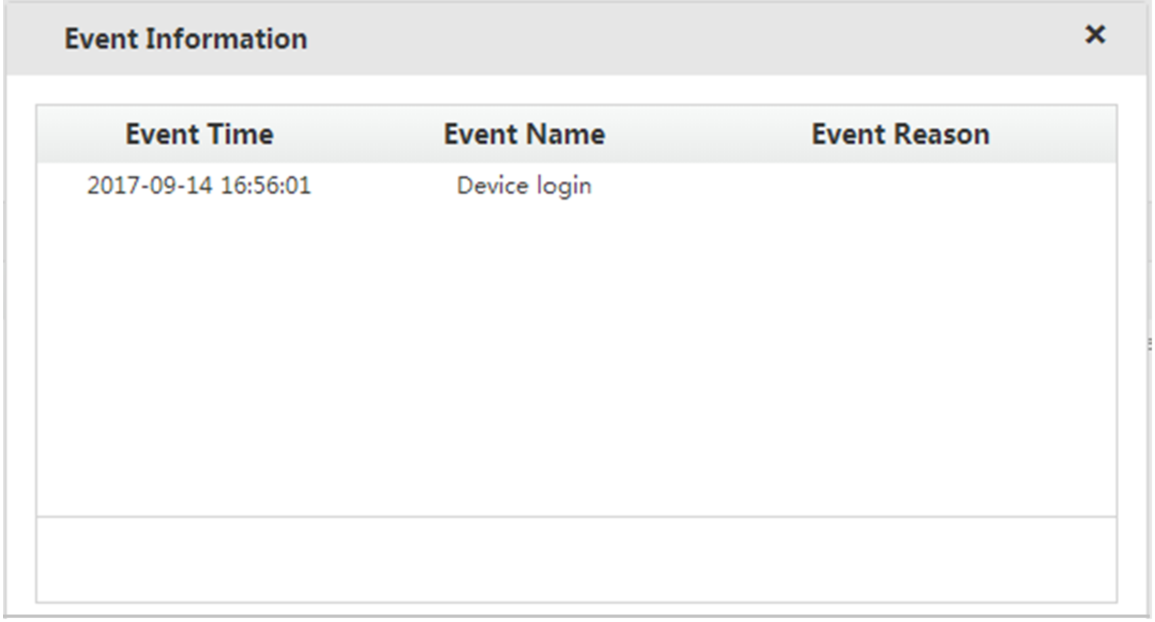
NOTE

- If there are only two EVS devices in the cluster, you have to set the arbitration IP to make the cluster switch normally. For details to setting arbitration IP, see "3.12.1.4 Arbitration IP Settings."
- Click 🗑 to delete a master or backup device. Click **Delete Cluster** to delete a cluster.

3.12.1.2 Viewing Information

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

Figure 3-152 Event information



Event Time	Event Name	Event Reason
2017-09-14 16:56:01	Device login	

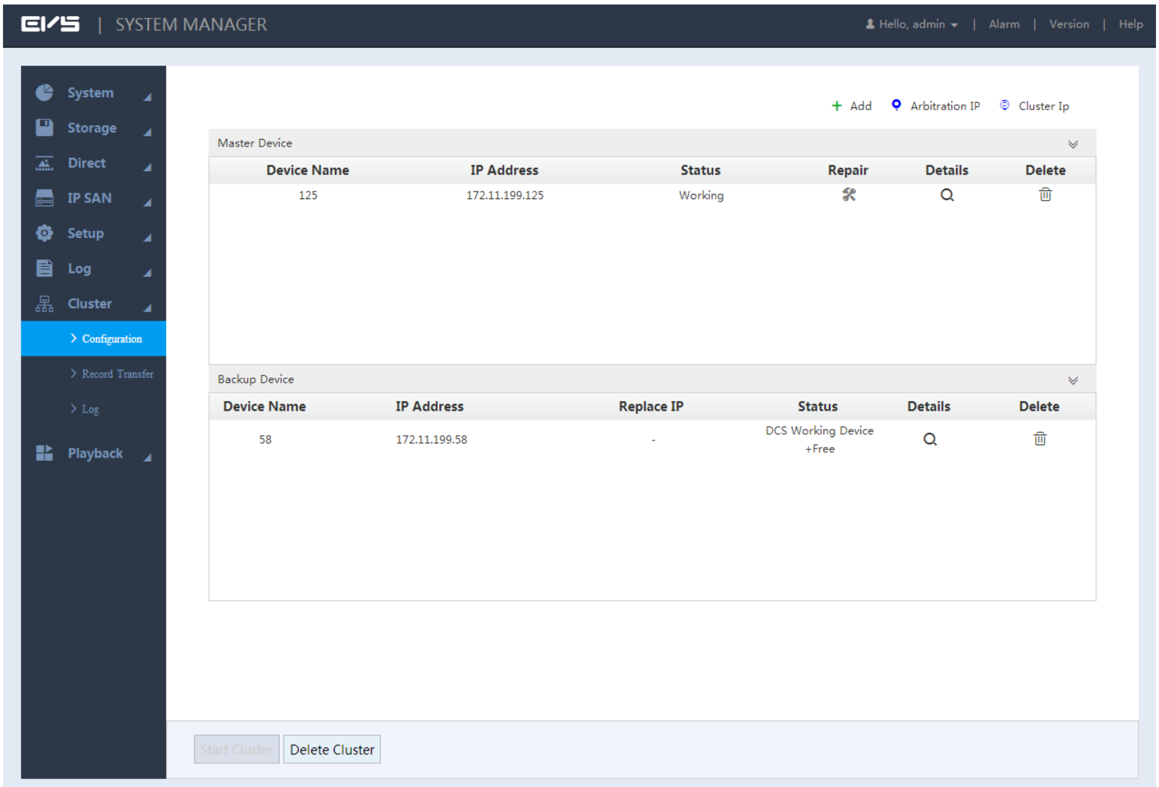
3.12.1.3 Restoring Master Device

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

Step 1 Select **Cluster** > **Configuration**.

The **Configuration** interface is displayed. See Figure 3-153.

Figure 3-153 Cluster configuration



Master Device

Device Name	IP Address	Status	Repair	Details	Delete
125	172.11.199.125	Working	🛠	🔍	🗑

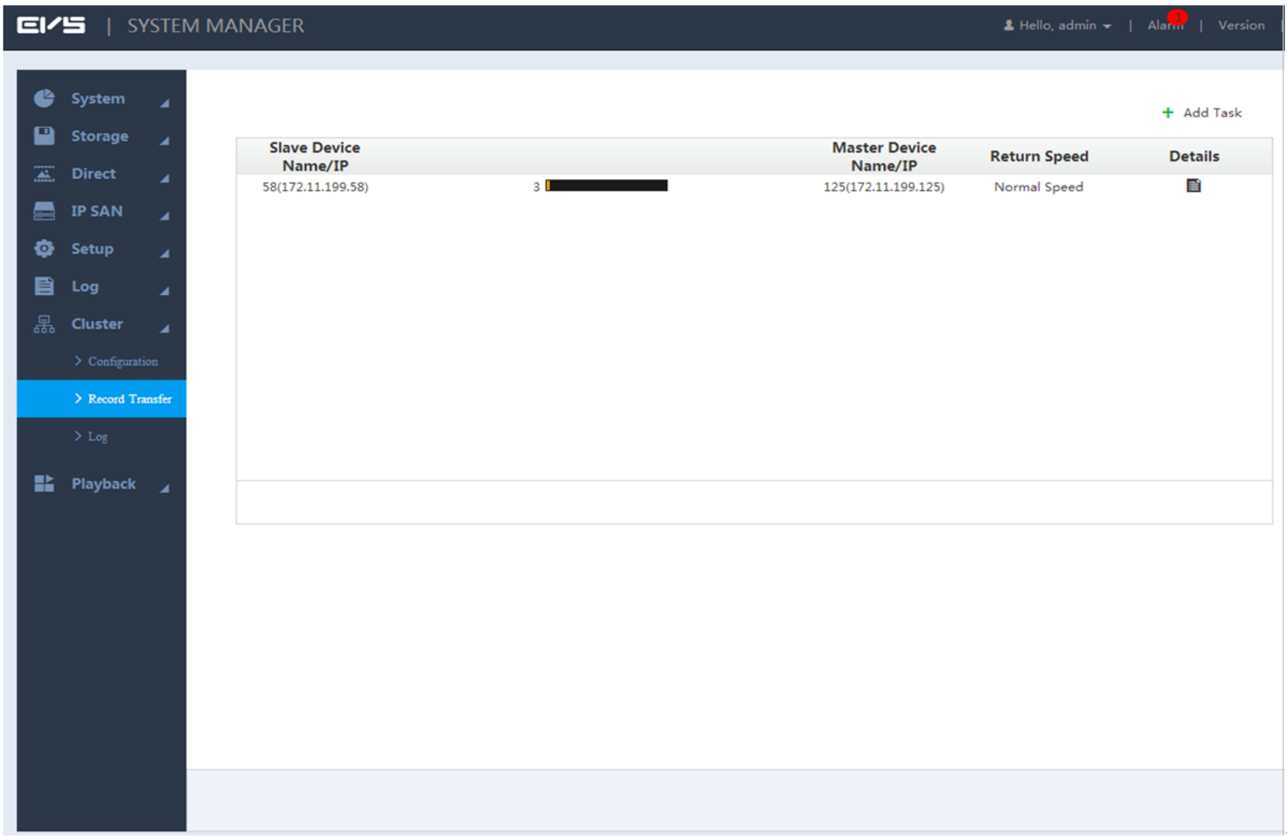
Backup Device

Device Name	IP Address	Replace IP	Status	Details	Delete
58	172.11.199.58	-	DCS Working Device +Free	🔍	🗑

Step 2 Click 🛠 .

The **Record Transfer** interface is displayed. See Figure 3-154.

Figure 3-154 Record transfer



Slave Device Name/IP		Master Device Name/IP	Return Speed	Details
58(172.11.199.58)	3	125(172.11.199.125)	Normal Speed	📄

Step 3 Enable auto record transfer according to the actual needs.

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

- Click Cancel. The system starts to restore the master device, but records will not be transferred. If you need to transfer the records, do manually. For details, see "3.12.2 Record Transfer."

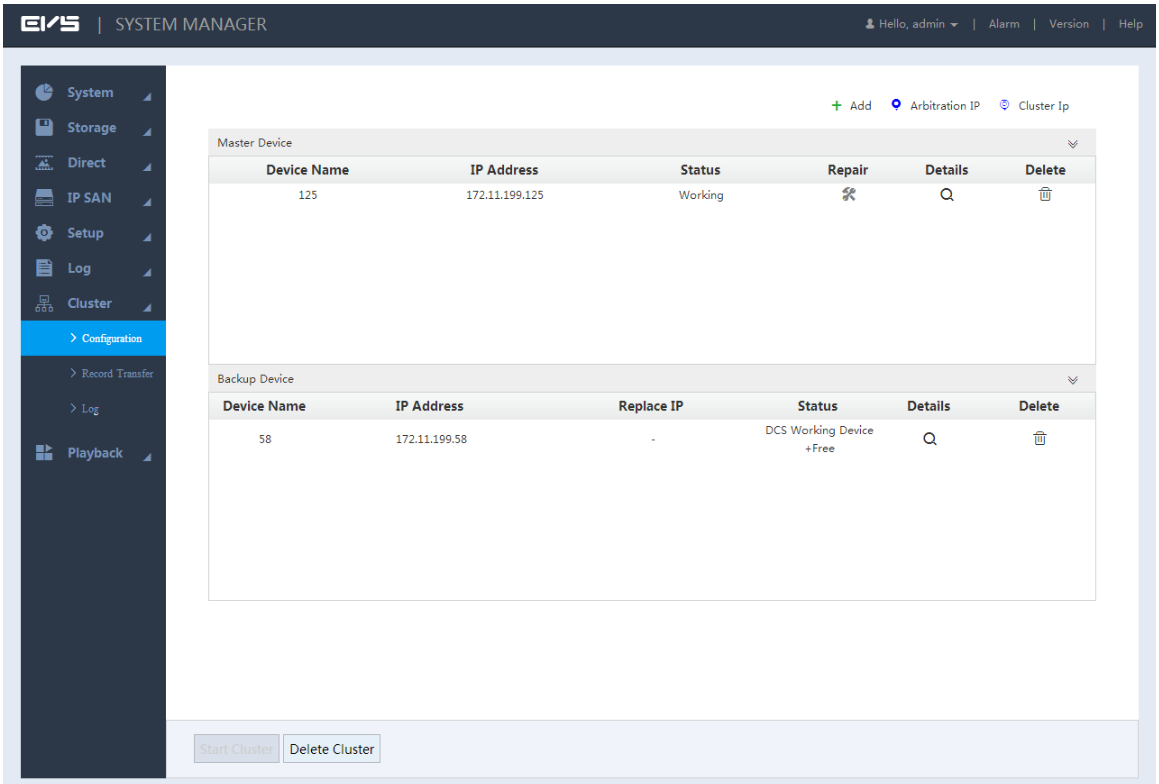
3.12.1.4 Arbitration IP Settings

When there are only two EVS devices in the cluster, a third-party device is needed to define if the master device is breakdown. That is, you have to set an arbitration IP to make the cluster perform switching normally. The arbitration IP can be the IP address of the device, PC or network gateway connected with the EVS device.

Step 1 Select **Cluster** > **Configuration**.

The Configuration interface is displayed. See Figure 3-155.

Figure 3-155 Cluster configuration



Master Device

Device Name	IP Address	Status	Repair	Details	Delete
125	172.11.199.125	Working			

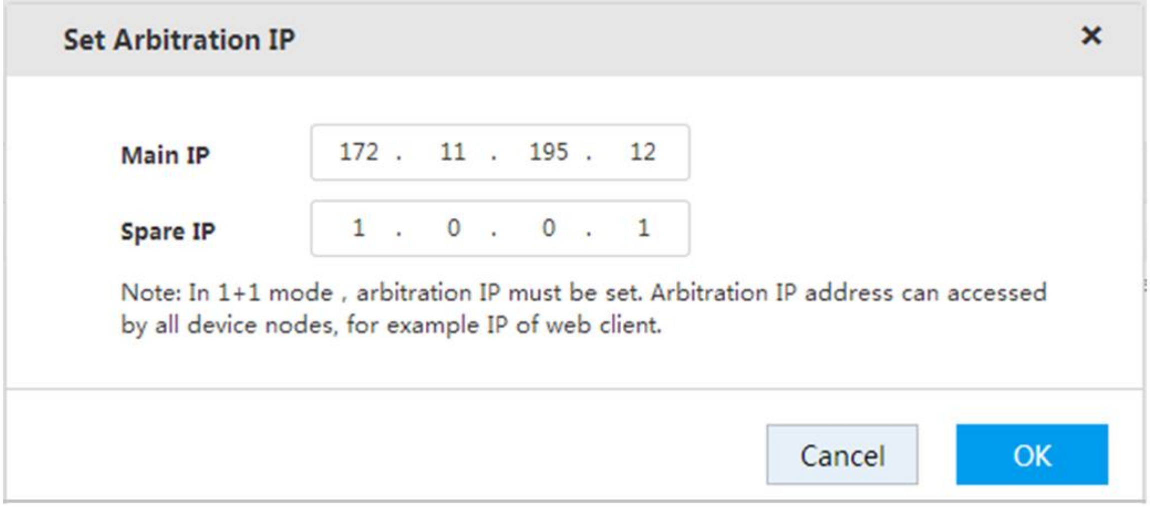
Backup Device

Device Name	IP Address	Replace IP	Status	Details	Delete
58	172.11.199.58	-	DCS Working Device +Free		

Step 2 Click 📍 .

The **Set Arbitration IP** interface is displayed. See Figure 3-156.

Figure 3-156 Setting arbitration IP



Set Arbitration IP

Main IP 172 . 11 . 195 . 12

Spare IP 1 . 0 . 0 . 1

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.

3.12.2 Record Transfer

After the master device is repaired, the records on the backup device shall be transferred back to the master device.

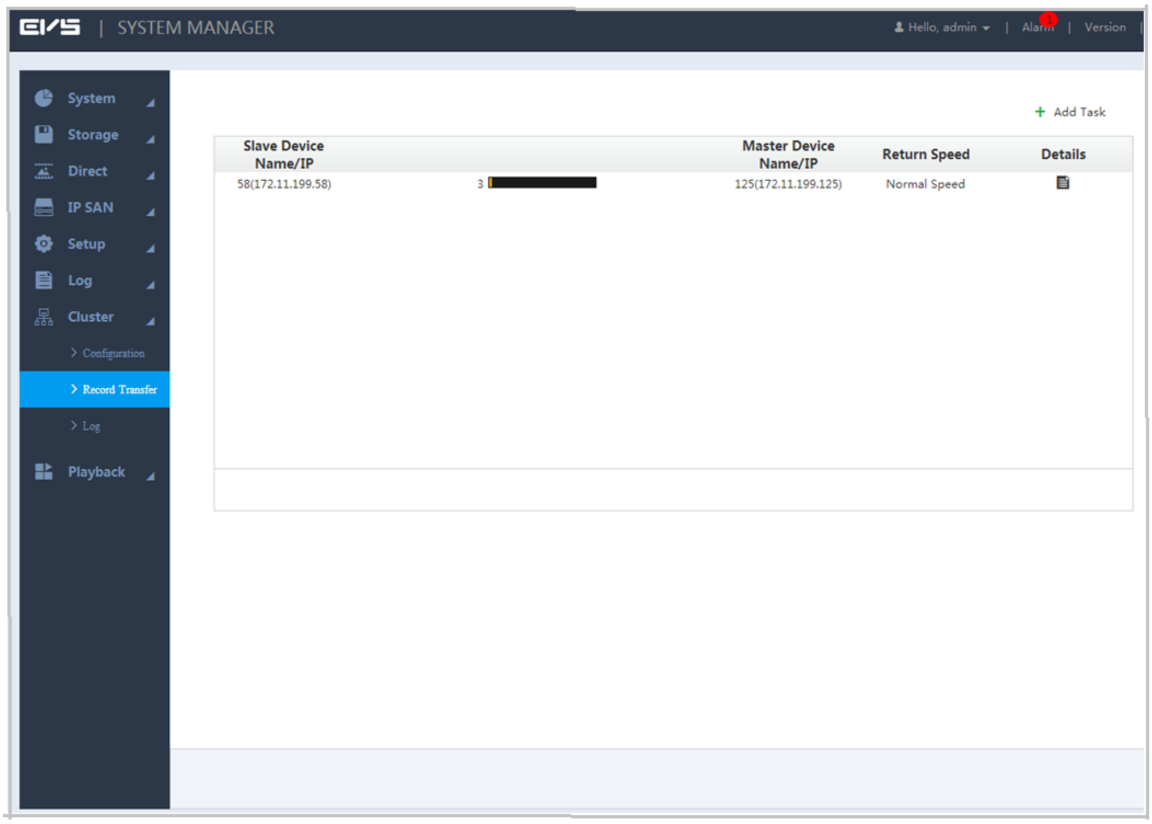
Preparation

The master device is restored. For details, see "3.12.1.3 Restoring Master Device."

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

The **Record Transfer** interface is displayed. See Figure 3-157.

Figure 3-157 Record transfer



EVS | SYSTEM MANAGER

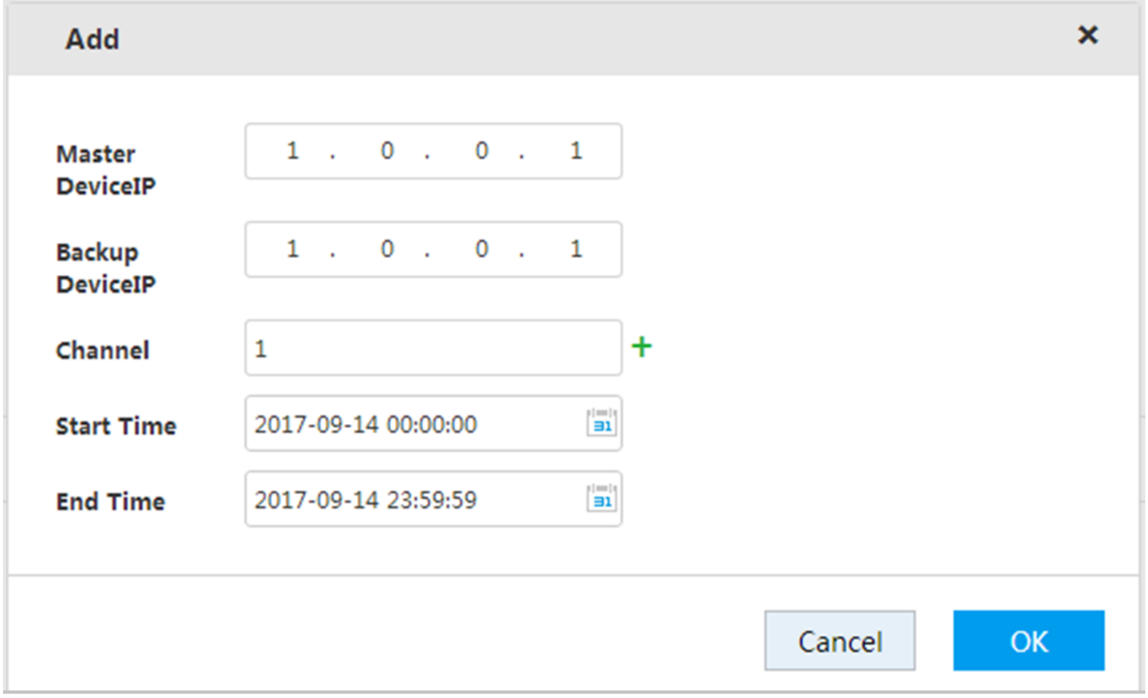
Hello, admin | Alarm | Version

Slave Device Name/IP		Master Device Name/IP	Return Speed	Details
58(172.11.199.58)	3 [redacted]	125(172.11.199.125)	Normal Speed	

Step 2 Click + .

The **Add** interface is displayed. See Figure 3-158.

Figure 3-158 Adding record transfer



Add

Master DeviceIP	1 . 0 . 0 . 1
Backup DeviceIP	1 . 0 . 0 . 1
Channel	1 +
Start Time	2017-09-14 00:00:00
End Time	2017-09-14 23:59:59

Step 3 Select/Enter the parameters. For details, see Table 3-58.

Table 3-58 Description of record transfer parameters

Parameter	Description
Master Device IP	Enter the IP address of the master device.

Parameter	Description
Backup Device IP	Enter the IP address of the backup device.
Channel	Enter the channel number you need to transfer records. Click + to set the channel range.
Start Time	Select the time period to transfer records.
End Time	

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

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

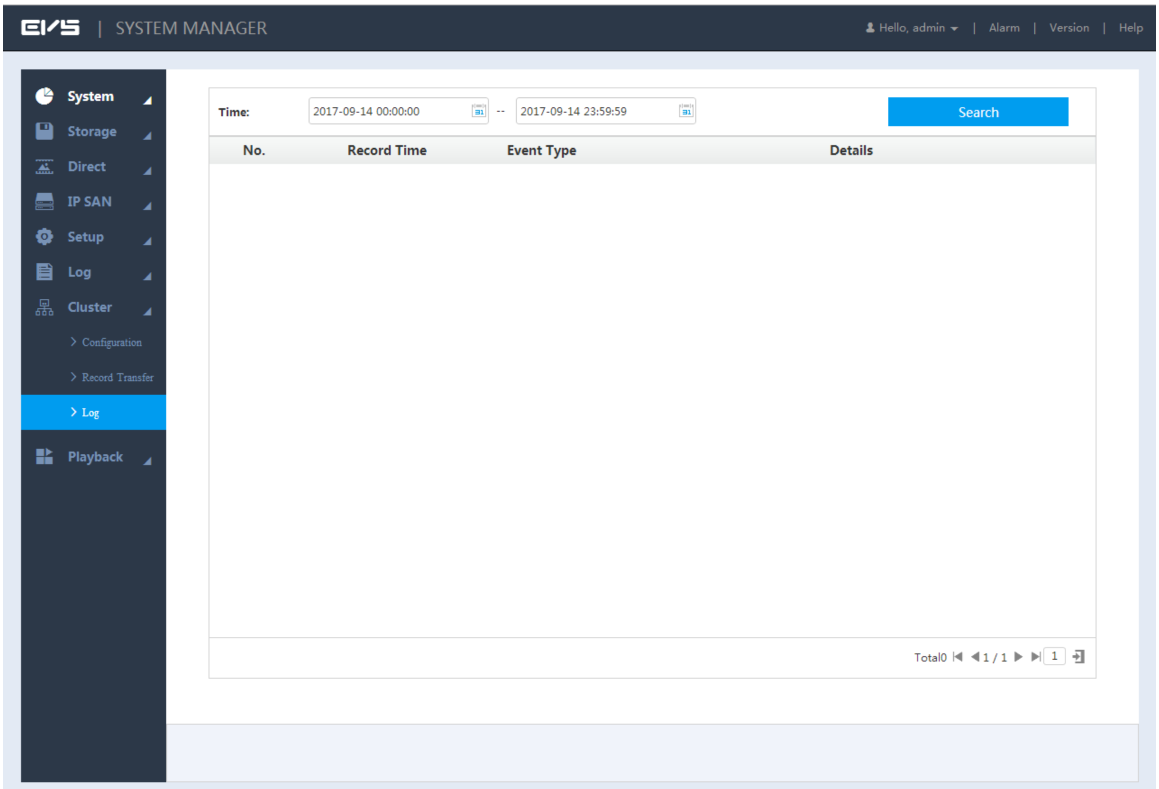
3.12.3 Cluster Log

The system supports to search and view the cluster logs.

Step 1 **Select Cluster** > **Log**.

The **Log** interface is displayed. See Figure 3-159.

Figure 3-159 Cluster log



Time: 2017-09-14 00:00:00 -- 2017-09-14 23:59:59

No.	Record Time	Event Type	Details

Step 2 Select the time period to record cluster logs.

Step 3 Click **Search**.

The search results are displayed. You can view the relative log information here.

3.13 System Information

You can view the EVS device information such as the current status, online users, device information and system logs.

3.13.1 Server Overview

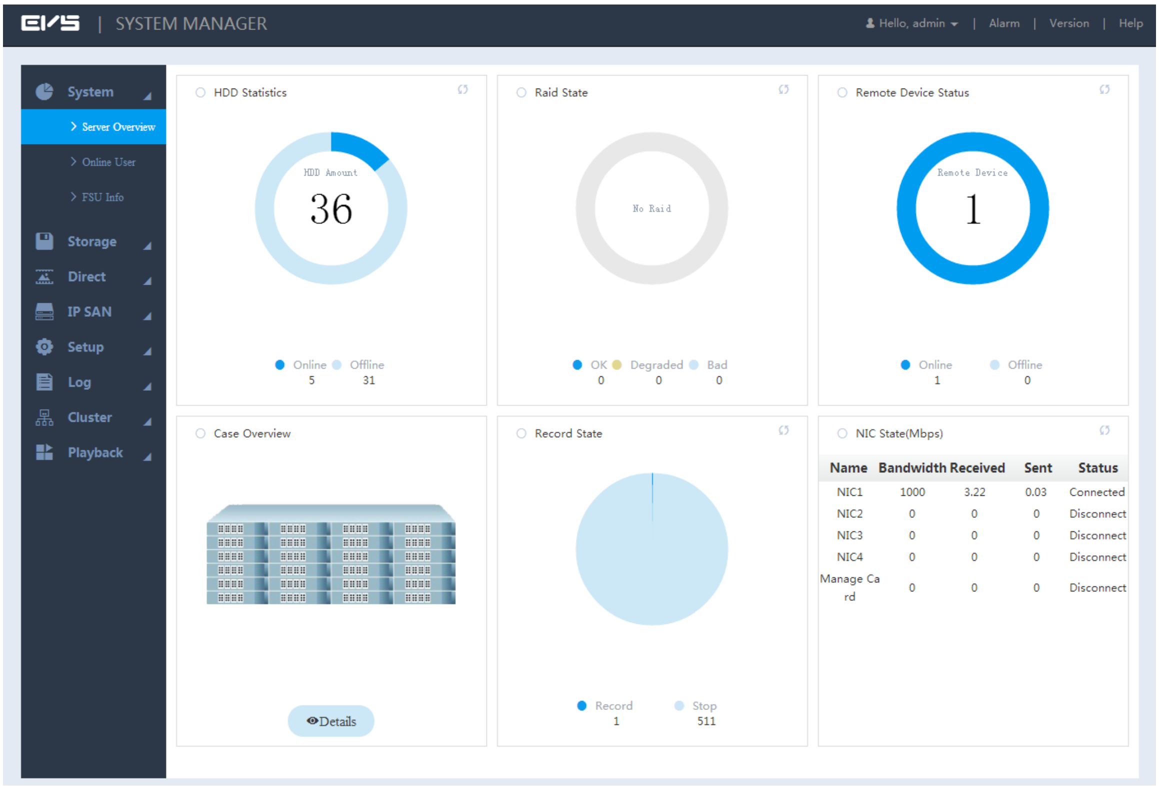
View the HDD statistics, RAID status, device online, case, record status and NIC status here.

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

The **Server Overview** interface is displayed. See Figure 3-160.

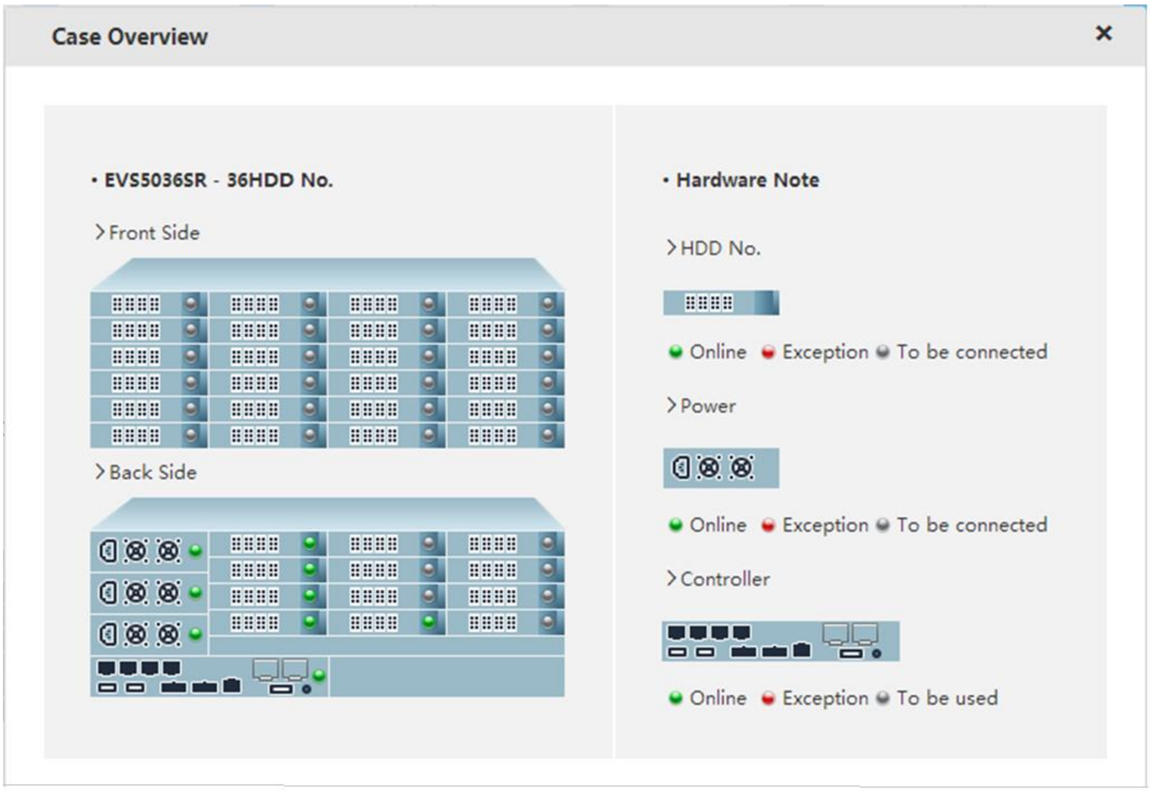
- Click ⟳ to get the latest status or information of the EVS device.
- Click Details and the **Case Overview** interface is displayed. See Figure 3-161. You can view the HDD, power and interface status here.

Figure 3-160 Server overview



Name	Bandwidth	Received	Sent	Status
NIC1	1000	3.22	0.03	Connected
NIC2	0	0	0	Disconnect
NIC3	0	0	0	Disconnect
NIC4	0	0	0	Disconnect
Manage Card	0	0	0	Disconnect

Figure 3-161 Case overview


Case Overview
×
• EVS5036SR - 36HDD 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

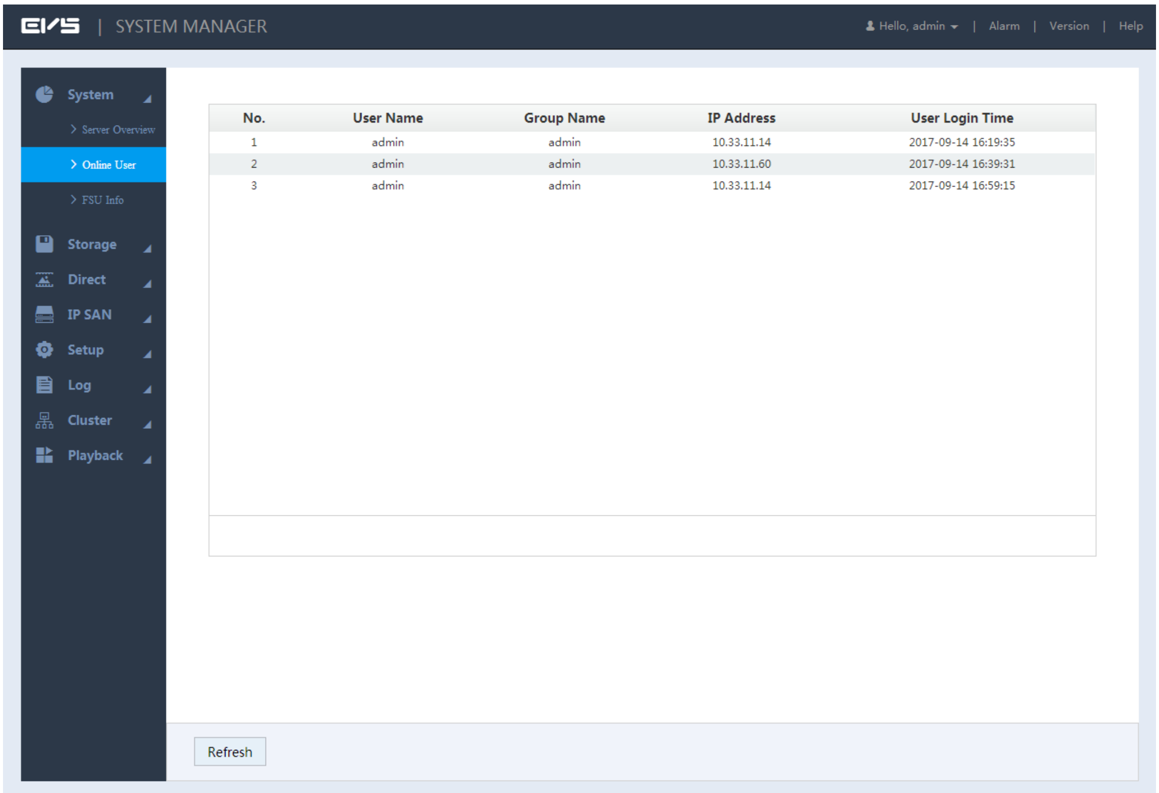
3.13.2 Online User

View the information of the current online users connected with the EVS device.

Select **System**>**Online User**. The Online User interface is displayed. See Figure 3-162.

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

Figure 3-162 Online User



No.	User Name	Group Name	IP Address	User Login Time
1	admin	admin	10.33.11.14	2017-09-14 16:19:35
2	admin	admin	10.33.11.60	2017-09-14 16:39:31
3	admin	admin	10.33.11.14	2017-09-14 16:59:15

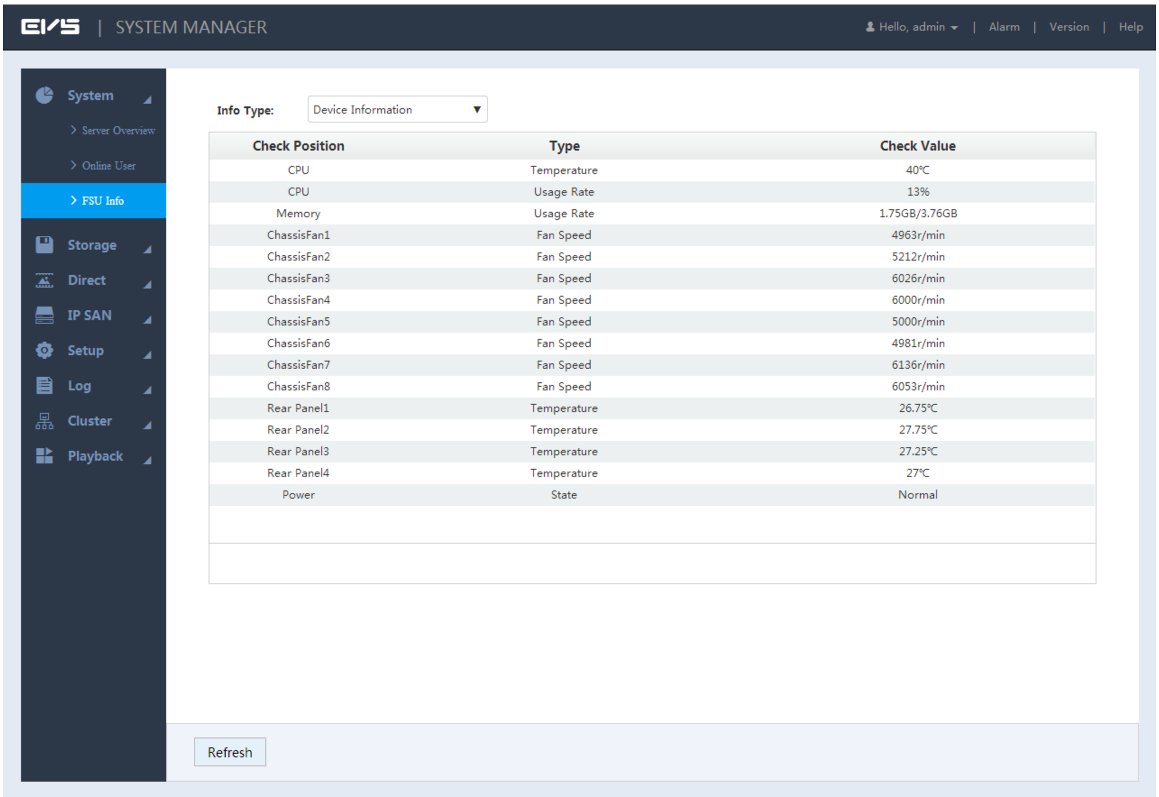
3.13.3 FSU Information

View the information of the master/backup devices and all the expansion cases here.

Select **System** > **FSU Info**. The **FSU Info** interface is displayed. See Figure 3-163.

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

Figure 3-163 FSU Information



Info Type: Device Information

Check Position	Type	Check Value
CPU	Temperature	40℃
CPU	Usage Rate	13%
Memory	Usage Rate	1.75GB/3.76GB
ChassisFan1	Fan Speed	4963r/min
ChassisFan2	Fan Speed	5212r/min
ChassisFan3	Fan Speed	6026r/min
ChassisFan4	Fan Speed	6000r/min
ChassisFan5	Fan Speed	5000r/min
ChassisFan6	Fan Speed	4981r/min
ChassisFan7	Fan Speed	6136r/min
ChassisFan8	Fan Speed	6053r/min
Rear Panel1	Temperature	26.75℃
Rear Panel2	Temperature	27.75℃
Rear Panel3	Temperature	27.25℃
Rear Panel4	Temperature	27℃
Power	State	Normal

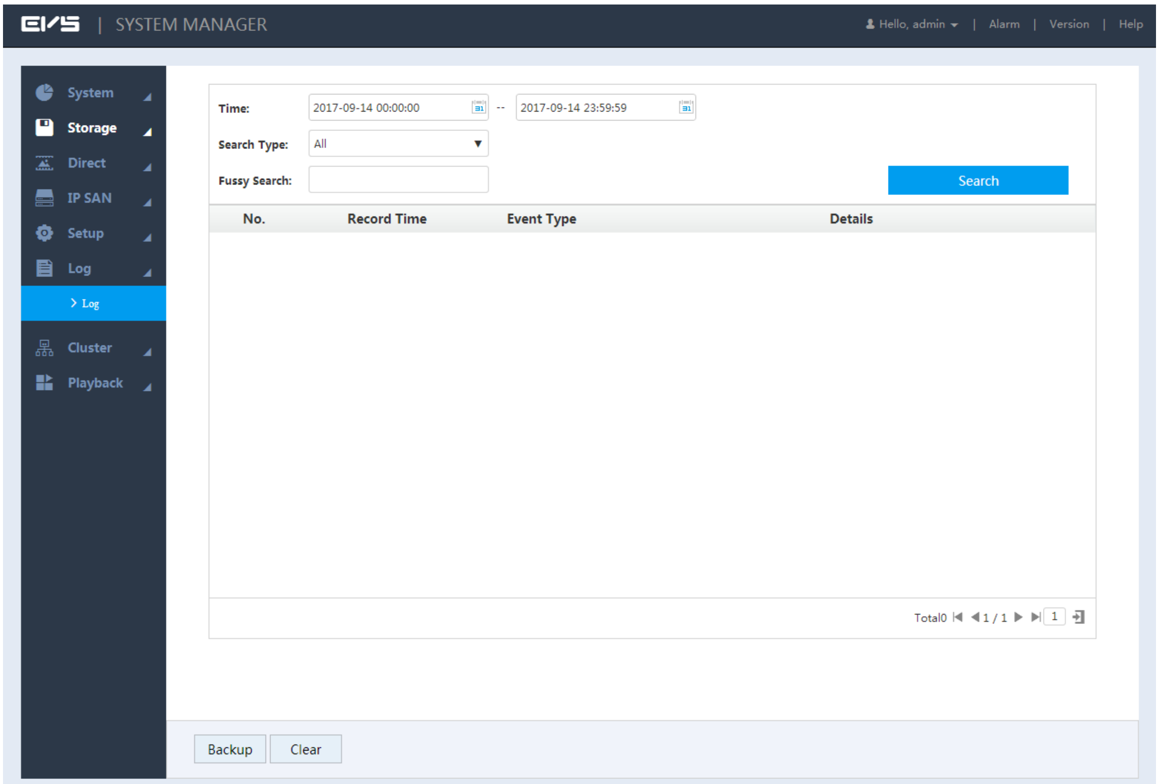
3.13.4 Log

You can search and view the system logs or back up system logs to local PC.

Step 1 Select **Log** > **Log**.

The **Log** interface is displayed. See Figure 3-164.

Figure 3-164 Log (1)



Time: 2017-09-14 00:00:00 -- 2017-09-14 23:59:59

Search Type: All

Fussy Search:

Step 2 Select/Enter the parameters. For details, see Table 3-59.

Table 3-59 Description of 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, configuration, data, alarm, record, user, log clear, file operation and connection log.
Fuzzy Search	You can enter the key word of the log to search for if you are not sure about the log type.

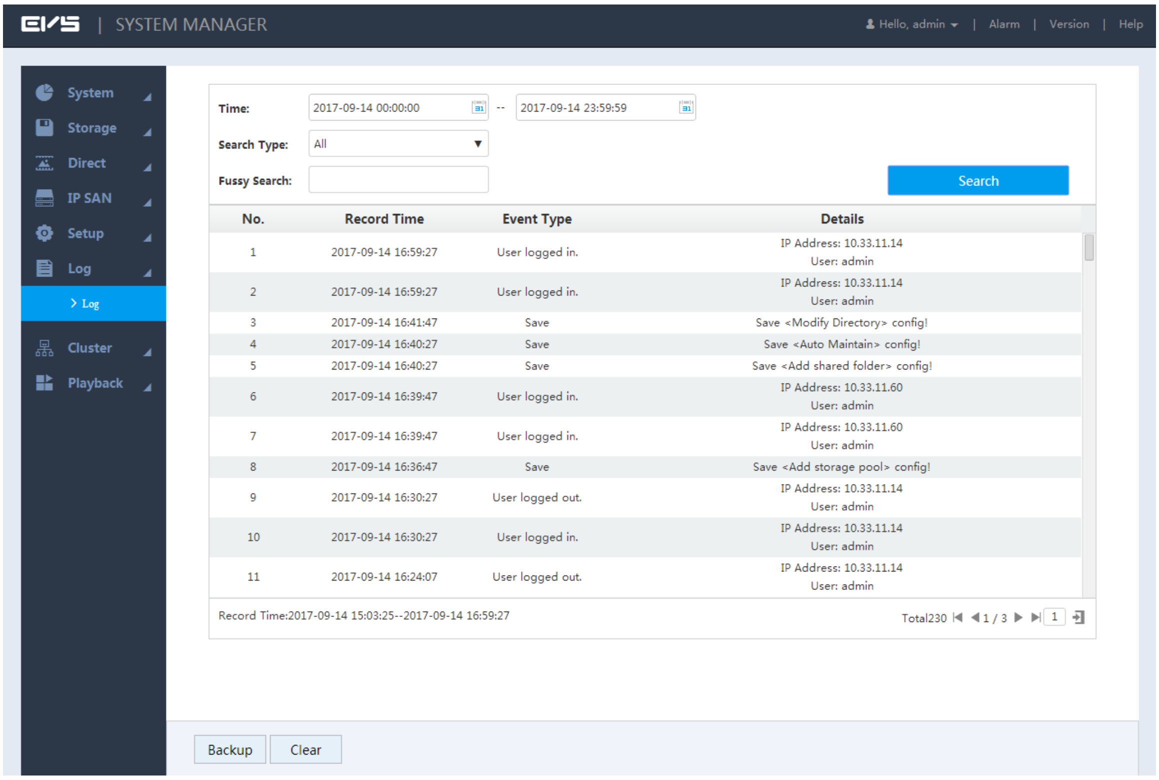
Step 3 Click **Search**.

The results are displayed. See Figure 3-165.

⚠ CAUTION

Click **Clear** and the system deletes all the logs. Be careful to perform it.

Figure 3-165 Log (2)



Time: 2017-09-14 00:00:00 -- 2017-09-14 23:59:59

Search Type: All

Fussy Search:

No.	Record Time	Event Type	Details
1	2017-09-14 16:59:27	User logged in.	IP Address: 10.33.11.14 User: admin
2	2017-09-14 16:59:27	User logged in.	IP Address: 10.33.11.14 User: admin
3	2017-09-14 16:41:47	Save	Save <Modify Directory> config!
4	2017-09-14 16:40:27	Save	Save <Auto Maintain> config!
5	2017-09-14 16:40:27	Save	Save <Add shared folder> config!
6	2017-09-14 16:39:47	User logged in.	IP Address: 10.33.11.60 User: admin
7	2017-09-14 16:39:47	User logged in.	IP Address: 10.33.11.60 User: admin
8	2017-09-14 16:36:47	Save	Save <Add storage pool> config!
9	2017-09-14 16:30:27	User logged out.	IP Address: 10.33.11.14 User: admin
10	2017-09-14 16:30:27	User logged in.	IP Address: 10.33.11.14 User: admin
11	2017-09-14 16:24:07	User logged out.	IP Address: 10.33.11.14 User: admin

Record Time:2017-09-14 15:03:25--2017-09-14 16:59:27

Total230 1 / 3 1

Step 4 (Optional) Log backup.

Click **Backup**, select the storage path, and then click **Save**. You can back up the logs to the local PC. The suffix of the backup file name is .txt.

Appendix 1 RAID Introduction

RAID is an abbreviation of Redundant Array of Independent Disks.

It is to combine 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.
RAID0	RAID0 is also called Striped Disk Array without Fault Tolerance. It represents the highest storage performance in RAID level. RAID0 is to read-write continue data in several HDDs. System data query will be performed in several HDDs at the same time.	2
RAID1	It is also called Mirror or mirroring. Its aim is to maximally guarantee data safety and restorability. RAID1 is to automatically copy user data fully to other RAID1 HDDs.	2
RAID5	RAID5 does not backup the storage data. Instead, it will memorize data and corresponding verification information to HDDs of RAID5. The data and verification information will be backed up in different HDDs respectively. When data in one of the HDDs is damaged, system can use the rest data and corresponding verification information to restore the lost data.	3
RAID6	Based on the RAID 5, the verification disk is two. The data and verification information will be backed up in different HDDs respectively. When data in two of the HDDs is damaged, system can still use the rest data and corresponding verification information to restore the lost data.	4
RAID10	RAID10 is a combination of RAID 1 and RAID 0. It owns the high read-write capability of RAID 0 and the high data protection and restorability of RAID 1. But its disk utilization is as low as RAID 1.	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 one group is malfunction.	6
RAID60	RAID60 is a combination of the RAID6 and RAID0. It has higher fault-tolerance. There is no data loss even two HDDs in one group is malfunction. It has higher read capability.	8

RAID Capacity Calculation

NOTE

capacityN refers to the disk with the minimum capacity in the disk group. The capacity shall be subject to the value on the Web.

Parameter	Total Capacity of the N Disks
RAID60	(N-4) × min (capacity)
RAID50	(N-2) × min (capacity)
RAID10	(N/2) × min (capacity)
RAID6	(N-2) × min (capacity)
RAID5	(N-1) × min (capacity)
RAID1	Min (capacity)
RAID0	Total capacity of the disks in the group.

Appendix 2 Glossary

NAS	It is an abbreviation of Network Attached System. It provides user file service via network.
SATA	It is an abbreviation of Serial Advanced Technology Attachment. In current released Serial ATA 2.0, data transmission speed can reach 300MB/second.
SATA HDD	HDD adopts SATA standard. Some leading manufacturers such as Seagate, Hitachi have already released SATA HDD.
SAMBA	It is MS network communication protocol software suitable for UNIX. Its core is SMB (server message block) protocol. SMB is a client /server protocol. User can access shared file system, printer and other resources in the server via this protocol.
NFS	It is an abbreviation of Network File System. It is a distributed file system. It allows the local PC to use the file or peripheral devices of another PC. It is mainly used in UNIX platform.
iSCSI	It is an abbreviation of Internet Small Computer System Interface. It is an internet protocol standard in Ethernet. It is an SCSI instruction set for hardware to be used in IP protocol layer. Generally speaking, iSCSI can realize SCSI protocol in the IP network to realize router option in high-speed 1000M Ethernet.
FTP	It is an abbreviation of File Transfer Protocol. It is a protocol of the TCP/IP protocol group. It is to transfer file from one PC to another while it has no relationship with PC OS, location and connection type.
CIFS	It is an abbreviation of Common Internet File System. CIFS is an open and cross-platform running mechanism for the user to ask for file or print service from the server. It is a standard server message block (SMB) protocol widely used in personnel PC and work station
Synchronization	After creating RAID 1 or RAID 5, before using, 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 the synchronization, system performance speed is very low.
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.
Shared directory	Local PC access the top path of the share 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.
Manageable status	It is a device status when controller configure device via web. Actually, when there is no error or damage, device shall be always in manageable status.

Ready status	It is a device status when controller access HDD via network. System is ready to use after you configure correctly in accordance with this user's 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.
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 WEB interface, from Disk -> RAID, the RAID device status is "clean".
Degraded status	It is a status after you remove one disk from the RAID1/RAID5 (working status) or remove two disks from RAID6.

Appendix 3 Specifications

Appendix 3.1 Middle-Class 16-HDD Single-Controller Series

Model		**Middle-Class 16-HDD Single-Controller**
OS	Main Processor	64-bit high performance multiple-core processor.
	Controller	Single controller.
	Operation System	Embedded LINUX system.
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel. High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB.
	Network Protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/iSCSI/ SMB/NFS/FTP
	Media Protocol	ONVIF and etc.
HDD	HDD Amount	16 SATA HDDs (Max 8T/HDD) Support SATA/SSD HDD. Does not support SAS HDD.
	SAS Port	1 SAS port.
	HDD Installation	Additional HDD bracket, support HDD hot swap, online replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60.RAID,JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP） volume management.
Performance	Video Stream Mode	Video stream direct storage.
	Video Stream	Max 512-channel (1024Mbps) front-end connection, storage,

Model		Middle-Class 16-HDD Single-Controller
	Storage Mode	256(512Mbps)transfer,64-channel (128Mbps) network playback.
	Record Playback	WEB. Search unit is second. Various playback speeds.
	IPSAN Mode	IPSAN direct storage.
	Snapshot	Support snapshot function. Create logic volume to backup data.
	Volume Clone	Support clone function. Create logic volume to backup the whole data.
	Frame Extracting	Support frame extracting and storage function. Support time and the frame setup.
	Cluster Service	Support N+M cluster service
	Auto Transfer after Power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK.
Port	USB Interface	One USB 3.0 port, one eSATA/USB2.0 hybrid port.
	Network connection	Two 1000Mbps data ports.
	Ethernet Port	Support load balance, fault-tolerance and etc.
	RS232	One RS232 port.
Others	Power	100V～240V, 47～63Hz One series has single power supplying one series has redundant power supplying. Support hot swap
	Total Power Consumption	< 200W (With HDD)
	Working Temperature	0℃~40℃
	Working Humidity	10%~80%（Non-condense）
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）
	Working Altitude	-60m~2000m
	Dimensions(L*W*H)	473.6mm×484.6mm×133.2mm (With handle)
	Weight	11KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation.

Appendix 3.2 Middle-Class 24-HDD Single-Controller Series

Model		Middle-Class 24-HDD Single-Controller
OS	Main Processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation System	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel.

Model		Middle-Class 24-HDD Single-Controller
		High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB
	Network Protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media Protocol	ONVIF and etc.
HDD	HDD Amount	24 SATA HDDs (Max 6T/HDD) Support SSD HDD. Support 2.5-inch HDD.
	SAS Port	2 SAS ports.
	HDD Installation	Additional HDD bracket, support HDD hot swap, online replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60.RAID,JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP）volume management.
Performance	Video Stream Mode	Video stream direct storage.
	Video Stream Storage Mode	Max 512-channel (1024Mbps) front-end connection, storage, 256(512Mbps)transfer,64-channel (128Mbps) network playback.
	Record Playback	WEB. Search unit is second. Various playback speeds.
	IPSAN Mode	IPSAN direct storage.
	Snapshot	Support snapshot function. Create logic volume to backup data.
	Volume Clone	Support clone function. Create logic volume to backup the whole data.
	Frame Extracting	Support frame extracting and storage function. Support time and the frame setup.
	Cluster Service	Support N+M cluster service
	Auto Transfer after	When the network camera is offline, the video is storage on

Model		Middle-Class 24-HDD Single-Controller
	Power failure	the SD card. It can transfer the video to the device once the network connection is OK.
Port	USB Interface	Two USB 3.0 ports.
	Network connection	Default mode : Five 100/1000Mbps Ethernet ports （One 100/1000Mbps Ethernet management port+ Four 100/1000Mbps Ethernet data ports） The extension mode: Five 100/1000Mbps Ethernet ports+Two 10000Mbps optical ports
	Ethernet Port	Support load balance, fault-tolerance and etc.
	RS232	One RS232 port
Others	Power	100V～240V, 47～63Hz 2 redundant power supplying. Support hot swap
	Fan	DC12V 1.5A, Fan diameter:80mm, Hot swap
	Total Power Consumption	200～400W (With HDD)
	Working Temperature	0℃~40℃
	Working Humidity	10%~80%（Non-condense）
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）
	Working Altitude	-60m~3000m
	Dimensions(W*H*D)	483mm×175mm×494mm (With handle)
	Weight	27KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation

Appendix 3.3 Middle-Class 36-HDD Single-Controller Series

Model		Middle-Class 36-HDD Single-Controller
OS	Main Processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation System	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel. High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB
	Network Protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media Protocol	ONVIF and etc.

Model		Middle-Class 36-HDD Single-Controller
HDD	HDD Amount	36 SATA HDDs (Max 6T/HDD) Support SSD HDD. Support 2.5-inch HDD.
	SAS Port	1 SAS ports
	HDD Installation	Additional HDD bracket, support HDD hot swap, online replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60.JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP）volume management.
Performance	Video Stream Mode	Video stream direct storage.
	Video Stream Storage Mode	Max 512-channel (1024Mbps) front-end connection, storage, 256(512Mbps) transfer, 64-channel (128Mbps) network playback.
	Record Playback	WEB. Search unit is second. Various playback speeds.
	IPSAN Mode	IPSAN direct storage
	Snapshot	Support snapshot function. Create logic volume to backup data.
	Volume Clone	Support clone function. Create logic volume to backup the whole data.
	Frame Extracting	Support frame extracting and storage function. Support time and the frame setup.
	Cluster Service	Support N+M cluster service
	Auto Transfer after Power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK.
Port	USB Interface	Two USB 3.0 ports.
	Network connection	Default mode : Five 100/1000Mbps Ethernet ports （One 100/1000Mbps Ethernet management port+ Four 100/1000Mbps Ethernet data ports）

Model		Middle-Class 36-HDD Single-Controller
		The extension mode: Five 100/1000Mbps Ethernet ports+Two 10000Mbps optical ports
	Ethernet Port	Support load balance, fault-tolerance and etc.
	RS232	One RS232 port
Others	Power	100V～240V, 47～63Hz 2+1 redundant power supplying. Support hot swap
	Fan	DC12V 1.5A, Fan diameter:80mm, Hot swap
	Total Power Consumption	200～400W (With HDD)
	Working Temperature	0℃~40℃
	Working Humidity	10%~80%（Non-condense）
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）
	Working Altitude	-60m~3000m
	Dimensions(W*H*D)	483mm×175mm×670.5mm (With handle)
	Weight	35KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation

Appendix 3.4 Middle-Class 48-HDD Single-Controller Series

Model		Middle-Class 48-HDD Single-Controller
OS	Main Processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation System	Embedded LINUX system
	Memory	Default 4GB
	Case	1.2mm extra-thickness hot-dip galvanized steel. High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB
	Network Protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/ iSCSI/SMB/NFS/FTP
	Media Protocol	ONVIF and etc.
HDD	HDD Amount	48 SATA HDDs (Max 6T/HDD) Support SSD HDD. Support 2.5-inch HDD.
	SAS Port	2 SAS ports
	HDD Installation	Additional HDD bracket, support HDD hot swap, online

Model		Middle-Class 48-HDD Single-Controller
		replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID5, RAID6, RAID10, RAID50, RAID60.JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP）volume management.
Performance	Video Stream Mode	Video stream direct storage.
	Video Stream Storage Mode	Max 512-channel (1024Mbps) front-end connection, storage, transfer, 96-channel (192Mbps) network playback.
	Record Playback	WEB. Search unit is second. Various playback speeds.
	IPSAN Mode	IPSAN direct storage.
	Snapshot	Support snapshot function. Create logic volume to backup data.
	Volume Clone	Support clone function. Create logic volume to backup the whole data.
	Frame Extracting	Support frame extracting and storage function. Support time and the frame setup.
	Cluster Service	Support N+M cluster service
	Auto Transfer after Power failure	When the network camera is offline, the video is storage on the SD card. It can transfer the video to the device once the network connection is OK.
Port	USB Interface	Two USB 3.0 ports.
	Network connection	Default mode : Five 100/1000Mbps Ethernet ports （One 100/1000Mbps Ethernet management port+ Four 100/1000Mbps Ethernet data ports） The extension mode: Five 100/1000Mbps Ethernet ports+Two 10000Mbps optical ports
	Ethernet Port	Support load balance, fault-tolerance and etc.
	RS232	One RS232 port
Others	Power	100V～240V, 50～60Hz 3 redundant power supplying.

Model		Middle-Class 48-HDD Single-Controller
		Support hot swap
	Fan	DC12V 1.5A, Fan diameter:80mm, Hot swap
	Total Power Consumption	175～950W (With HDD)
	Working Temperature	0℃~40℃
	Working Humidity	10%~80%（Non-condense）
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）
	Working Altitude	-60m~3000m
	Dimensions(W*H*D)	482.6mm×347.8mm×558.55mm (With handle)
	Weight	50KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation

Appendix 3.5 High-End 24-HDD Single-Controller

Model		High-End 24-HDD Single- Controller
OS	Main Processor	64-bit high performance multiple-core processor
	Controller	Single controller
	Operation System	Embedded LINUX system
	Memory	Default 8GB Max support 16G
	Case	1.2mm extra-thickness hot-dip galvanized steel. High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB
	Network Protocol	RTP/RTCP, RTSP, UDP, HTTP, NTP, SNMP protocol
	Media Protocol	ONVIF and etc.
HDD	HDD Amount	24 SATA/SAS HDDs (Max 6T/HDD) SAS/SATA HDD composite connection. Support SSD, 2.5-inch HDD.
	SAS Port	2 SAS ports
	HDD Installation	Additional HDD bracket, support HDD hot swap, online replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID10, RAID5, RAID6, RAID50, RAID60.JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.

Model		High-End 24-HDD Single- Controller
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP）volume management.
	Cluster Service	N+M cluster service
	ANR	After diconnection, system can download the record file from the SD card on the network camera to maintain the full record file.
Record and Playback	Record Mode	Manual recording, motion detection recording, schedule recording and alarm recording Priority: Manual recording > alarm recording > detection recording > schedule recording. Support event pre-record.
	Record Schedule	Main stream/sub stream storage by period. I frame storage by period.
	Record Search	Various search engines such as time, type and channel, front-end position info.
	Record Protection	Record protection function to prevent vicious modification. Protection time is adjustable.
	Record Backup	Flash disk, portable HDD, eSATA.
	Record Download	WEB
	Record Playback	WEB. Search unit is second. Various playback speeds.
Performance	Video Stream Mode	Video stream direct storage.
	Video Stream Storage Mode	Max 768-channel (1536Mbps) front-end connection, storage, transfer, 64-channel (128Mbps) network playback.
	Transfer Mode Performance	4096Mbps front-end connection, 4096Mbps network transfer.
	IPSAN Mode	IPSAN direct storage.
	IPSAN performance	IPSAN working mode: Storage bandwidth shall not be less than 3.6Gbps.
Port	USB Interface	One USB 2.0 port and one USB 3.0 port. The USB 2.0 port can be reused as the eSATA port.

Model		**High-End 24-HDD Single- Controller**
	Network Connection	Default mode : Five 100/1000Mbps Ethernet ports （One 100/1000Mbps Ethernet management port+ Four 100/1000Mbps Ethernet data ports） The extension mode: Five 100/1000Mbps Ethernet ports+Two 10000Mbps optical ports
	Ethernet Port	Support load balance, fault-tolerance and etc.
	Alarm Port	4 input/4 output
	RS232 RS485	One RS232 port One RS485 port
Others	Power	100V～240V, 47～63Hz 2 redundant power supplying. Support hot swap
	Fan	Redundant dual ball bearing fan MTBF > 100 thousand hours Hot swap
	Total Power Consumption	200～400W (With HDD)
	Working Temperature	0℃~40℃
	Working Humidity	10%~80%（Non-condense）
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）
	Working Altitude	-60m~3000m
	Dimensions(W*H*D)	483mm×175mm×494mm (With handle)
	Weight	27KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation

Appendix 3.6 High-End 48-HDD Single-Controller

Model		**High-End 48-HDD Single- Controller**
OS	Main Processor	64-bit high-performance multiple-core processor.
	Controller	Single controller.
	Operation System	Embedded LINUX system.
	Memory	8GB (default). Max 16G.
	Case	1.2mm extra-thickness hot-dip galvanized steel. High accuracy aluminum alloy slider. Self-developed patent removable HDD bracket.
	User Interface	WEB.
	Network Protocol	RTP/RTCP/RTSP/UDP/HTTP/NTP/SNMP/iSCSI/SMB/NFS/FTP
	Media Protocol	ONVIF and etc.
HDD	HDD Amount	48 HDDs (Max 6T/HDD.) SAS/SATA HDD composite connection.

Model		High-End 48-HDD Single- Controller
	SAS Port	2 SAS ports
	HDD Installation	Additional HDD bracket, support HDD hot swap, online replacement.
	HDD Mode	Single HDD, RAID0, RAID1, RAID3, RAID4, RAID10, RAID5, RAID6, SRAID,RAID50, RAID60.JBOD, hotspare.
	HDD Manager	Non-working HDD hibernation to guarantee sound ventilation, reduce power consumption and enhance HDD life span.
	HDD Process	HDD bad track mapping to enhance HDD life span.
	HDD Status Detect	Pre-detect before HDD use, schedule detect when the HDD is in use.
	RAID Plug and Play	RAID becomes available once it is created.
	RAID Rebuild	Dynamically adjust RAID rebuild speed to guarantee system load balance.
	RAID Sync-Write	RAID Sync-write technology to guarantee data safety.
	HDD Roaming	HDD or RAID group can be removed from one device and then installed on another. Data is safe.
	Logic Volume Manager	Support iSCSI volume management, NAS（SMB\NFS\FTP） volume management.
	Snapshot	Support snapshot function, create user volume to backup data.
	Volume Clone	Support clone function. Create user volume to backup the complete data.
	Extract Frame	Support extracting P frame function. Customizied extracting period and frame rate setup.
	ANR	After diconnection, system can download the record file from the SD card on the network camera to maintain the full record file.
	Shortcut RAID Creation	Click one button to create RAID conveniectly.
Record and Playback	Record Mode	Manual recording, motion detection recording, schedule recording and alarm recording Priority: Manual recording > alarm recording > detection recording > schedule recording. Support event pre-record.
	Record Schedule	Main stream/sub stream storage by period. I frame storage by period.
	Record Search	Various search engines such as time, type and channel, front-end position info.
	Record Protection	Record protection function to prevent vicious modification. Protection time is adjustable.
	Record Backup	Flash disk, portable HDD, eSATA.
	Record Download	WEB.
	Record Playback	WEB. Search unit is second. Various playback speeds.
Performance	Video Stream Mode	Video stream direct storage

Model		High-End 48-HDD Single- Controller
	Video Stream Storage Mode	Max 768-channel (1536Mbps) front-end connection, storage, transfer, 64-channel (128Mbps) network playback.
	Transfer Mode Performance	4096Mbps front-end connection, 4096Mbps network transfer.
	IPSAN Mode	IPSAN direct storage
	IPSAN performance	IPSAN working mode: Storage bandwidth shall not be less than 3.6Gbps.
Port	USB Interface	One USB 2.0 port and one USB 3.0 port. The USB 2.0 port can be reused as the eSATA port.
	Network connection	Default mode : Five 100/1000Mbps Ethernet ports（One 100/1000Mbps Ethernet management port+ Four 100/1000Mbps Ethernet data ports） The extension mode: Five 100/1000Mbps Ethernet ports+Two 10000Mbps optical ports.
	Ethernet Port	Support load balance, fault-tolerance and etc.
	RS232 RS485	One RS232 port One RS485 port
Others	Power	100V～240V，47～63Hz 2+2 redundant power supplying. Support hot swap.
	Fan	DC12V,1.5A Hot swap Fan diameter:80mm
	Total Power Consumption	1000W (With HDD)
	Working Temperature	0℃~40℃.
	Working Humidity	10%~80%（Non-condense）.
	Storage Temperature	-20℃~70℃
	Storage Humidity	5%~90%（Non-condense）.
	Working Altitude	-60m~5000m
	Dimensions(W*H*D)	444.4mm×352.8mm×494mm (No handle)， 444.4mm×352.8mm×532mm（With handle）
	Weight	49.92KG (Excluding package or HDD)
	Installation Mode	Standard 19-inch rack installation.