Embedded Video Storage (EVS50/EVS70)

Quick Start Guide

V2.1.4

Foreword

General

This User's Manual (hereinafter referred to as "the Manual") introduces the functions and operations of the EVS series (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Models

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

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

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

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

About the Manual

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

Important Safeguards and Warnings

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

Operation Requirements

 WARNING

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

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

Installation Requirements

 WARNING

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

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

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

Maintenance Requirements

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

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

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

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Table of Contents

1 Overview

1.1 Introduction

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

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

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

The contents below are introduced in the example of middle-class 24-HDD single-controller. Functions of other series are similar. Refer to the actual devices when necessary.

1.2 Front Panel

Figure 1-1 Front panel

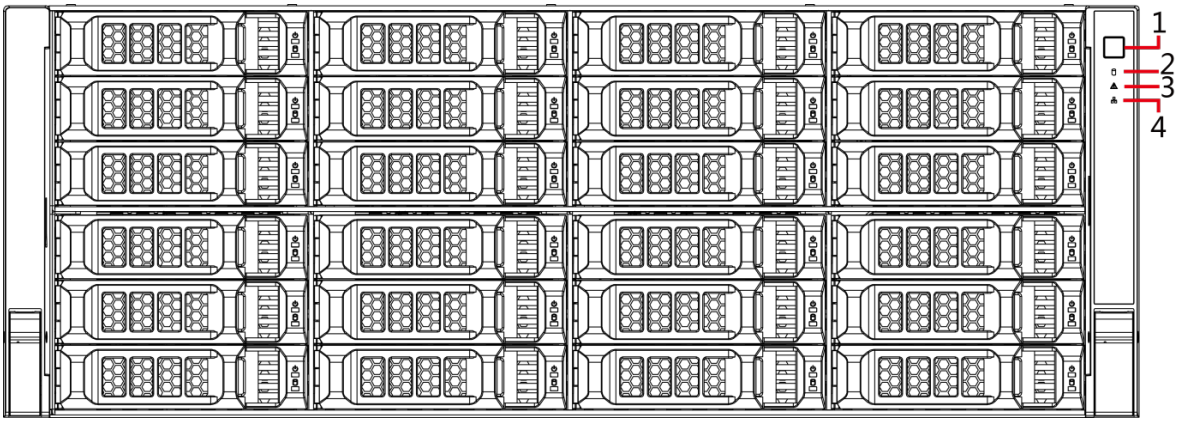


Table 1-1 Front panel description

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

No.	Port/Button	Description
4	Network status indicator	The blue light keeps on if there is network failure, IP conflict or MAC conflict.

1.3 Rear Panel

Figure 1-2 Rear panel (5 Ethernet ports)

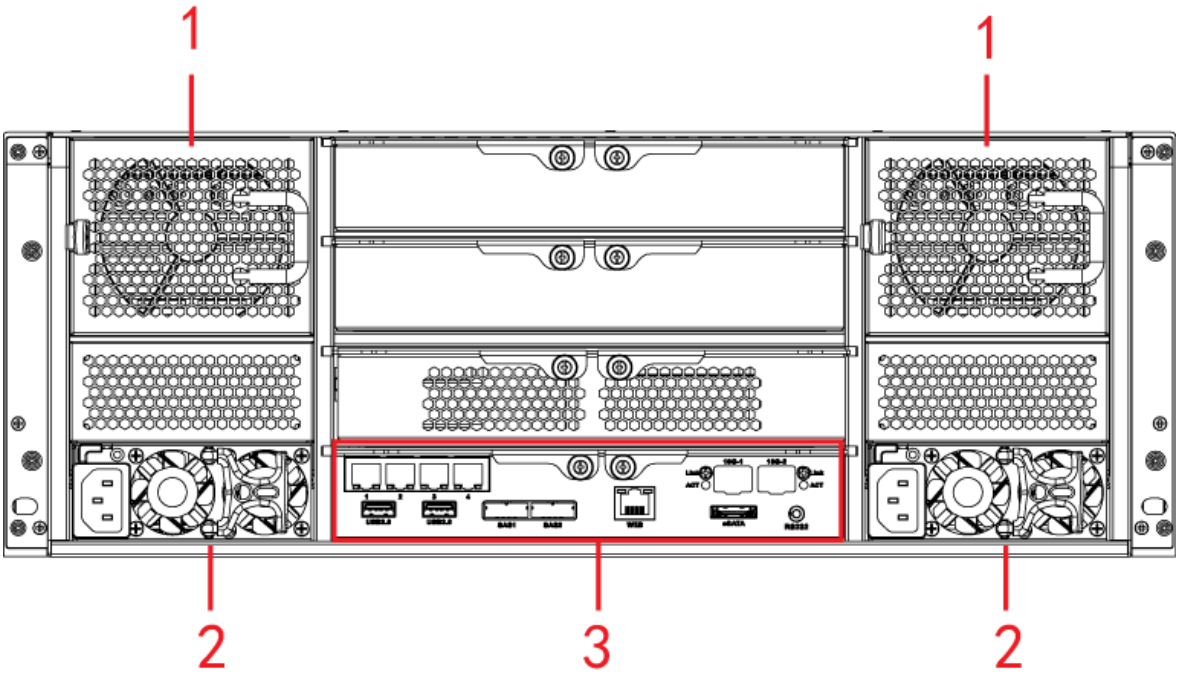


Figure 1-3 Rear panel (7 Ethernet ports)

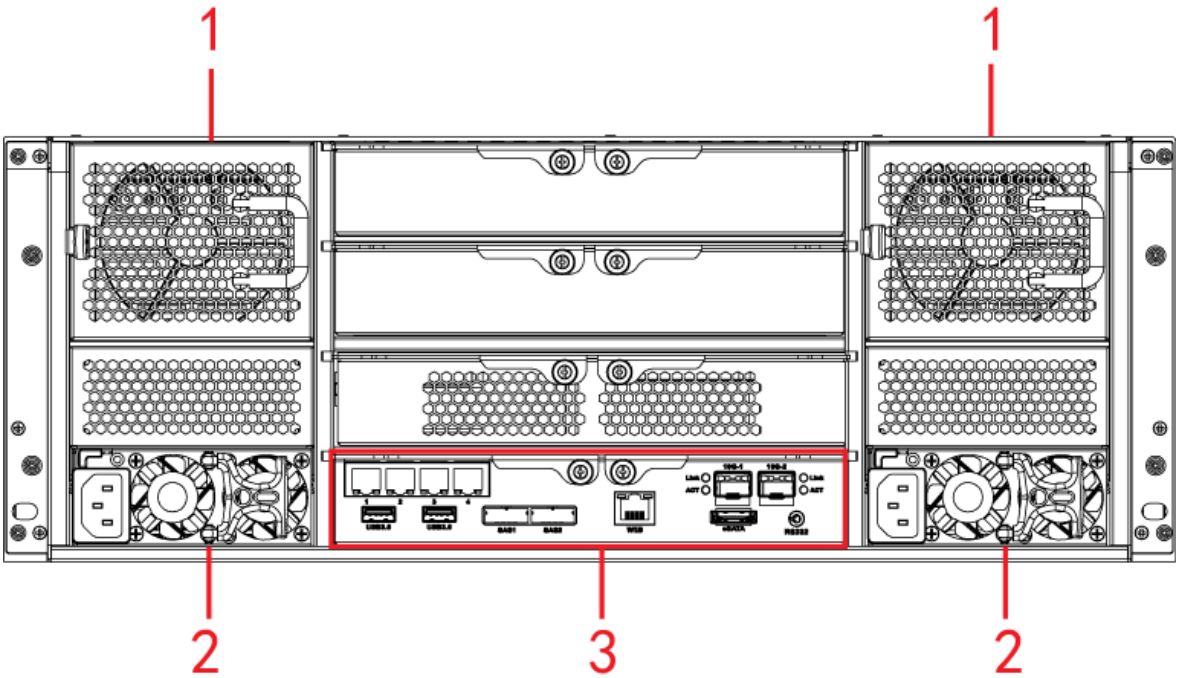


Figure 1-4 Rear panel (9 Ethernet ports)

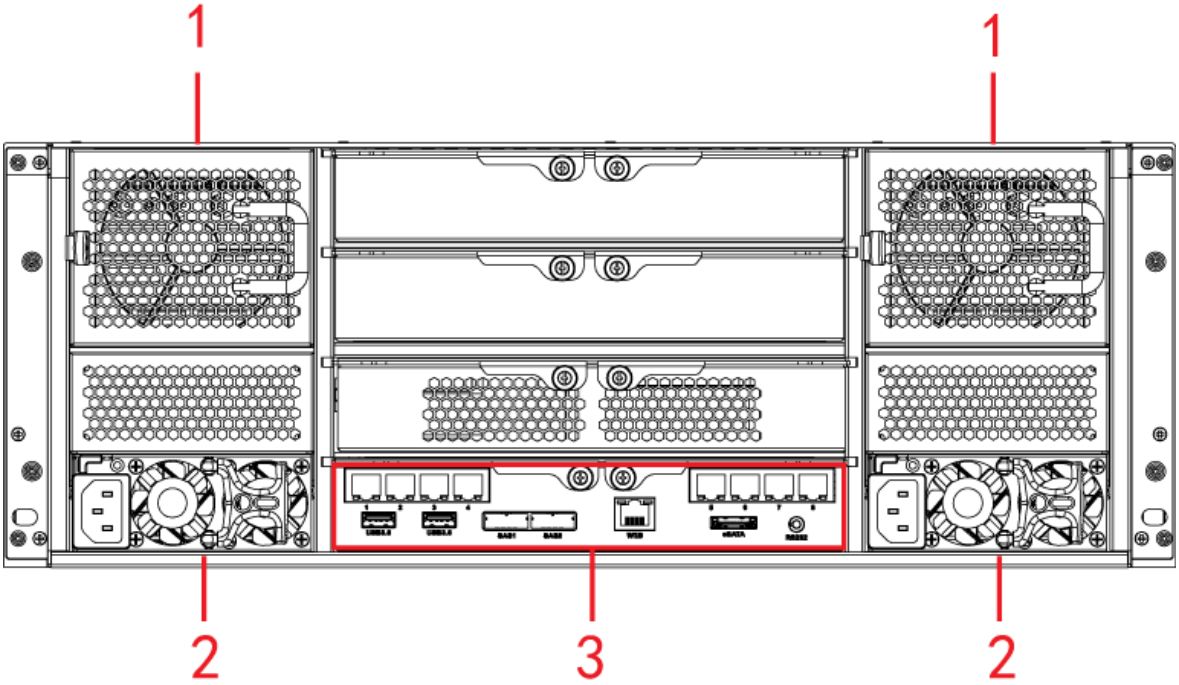


Table 1-2 Rear panel description

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

Table 1-3 Main control module ports

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

2 Installation and Power Up

2.1 Installing HDD

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

WARNING

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

2.1.1 Middle-class 16-HDD Single-controller Series

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

Figure 2-1 Opening the handle

Step 2 Pull out to take the empty HDD box.

Figure 2-2 HDD box

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

Figure 2-3 Fastening the screws

⚠

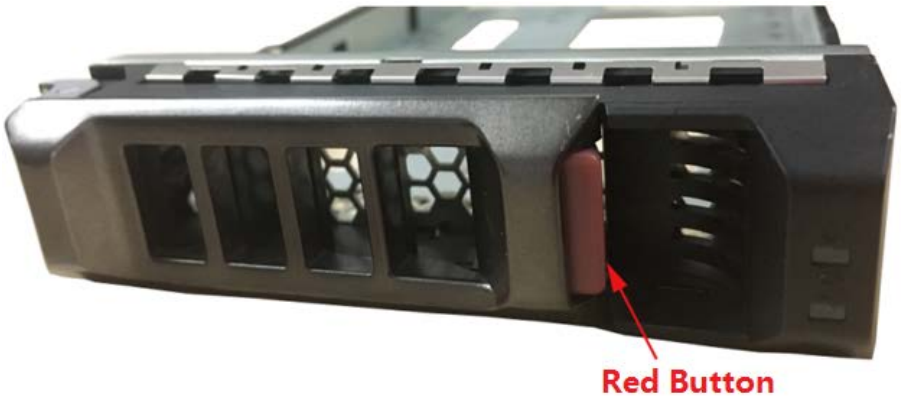
To avoid any damage to the slot, do not close the handle if the HDD box has not been pushed to the bottom.

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

2.1.2 Other Series

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

Figure 2-4 Opening the handle

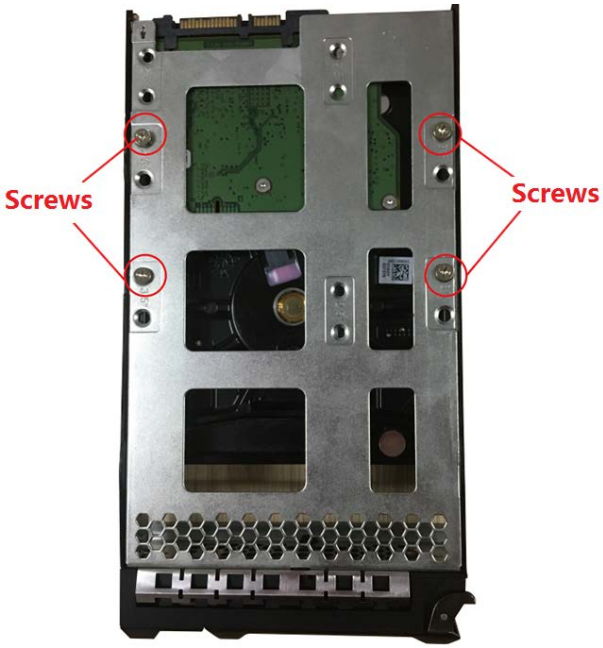


Step 2 Pull out to take the empty HDD box.

Figure 2-5 HDD box

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

Figure 2-6 Locking the screws



⚠

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

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

2.2 Powering Up

2.2.1 Preparation

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

- Make sure that GND is connected correctly.

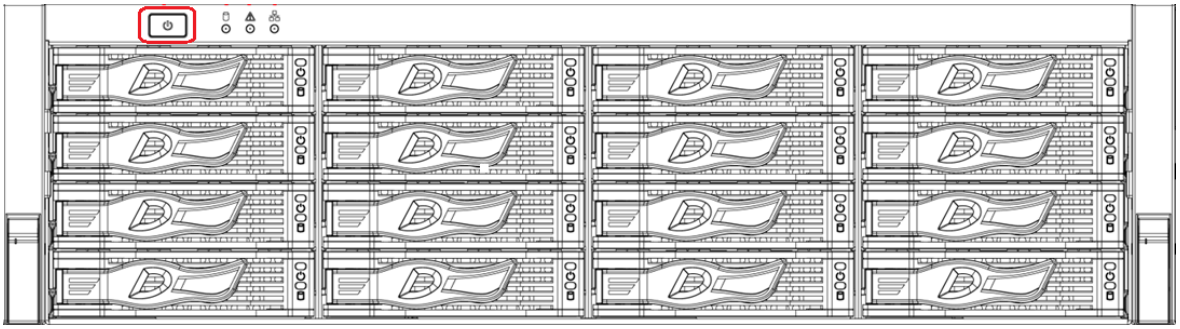
- Different models of devices need different sources of power supplies. Make sure that all power lines are connected correctly.
- Check whether the supplied power voltage complies with the device requirement.
- Check whether the network cables and SAS cables are connected correctly.

2.2.2 Powering Up the Device

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

Press the power button on the front panel.

Figure 2-7 Front panel



See "1.2 Front panel" for the corresponding description table of front panel, and check whether the indicators are normally displayed.

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

3 Web Basic Operations

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

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

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

3.1 Connecting the Network

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

Step 1 Connect the device to the network.

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

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

The Ethernet ports of the Device have different default IP.

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

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

3.2 Initializing the Device

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

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

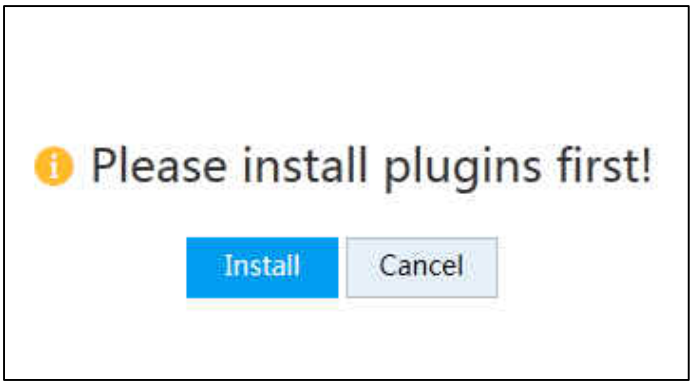
The default IP address of single-control device is 192.168.1.108.

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

Step 2 Press Enter.

The system prompts you to install plugins.

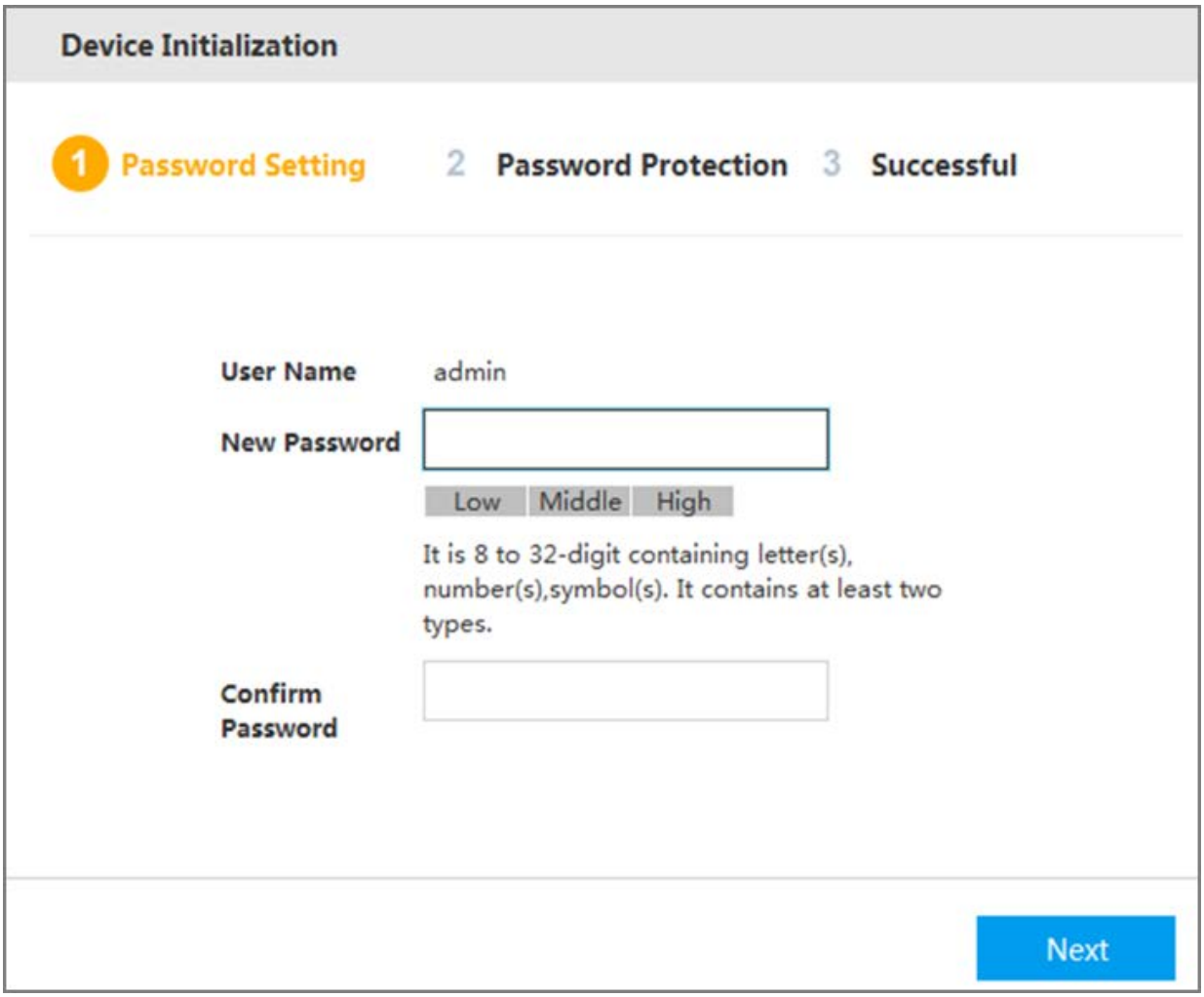
Figure 3-1 Install plugins



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

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

Figure 3-2 Password setting

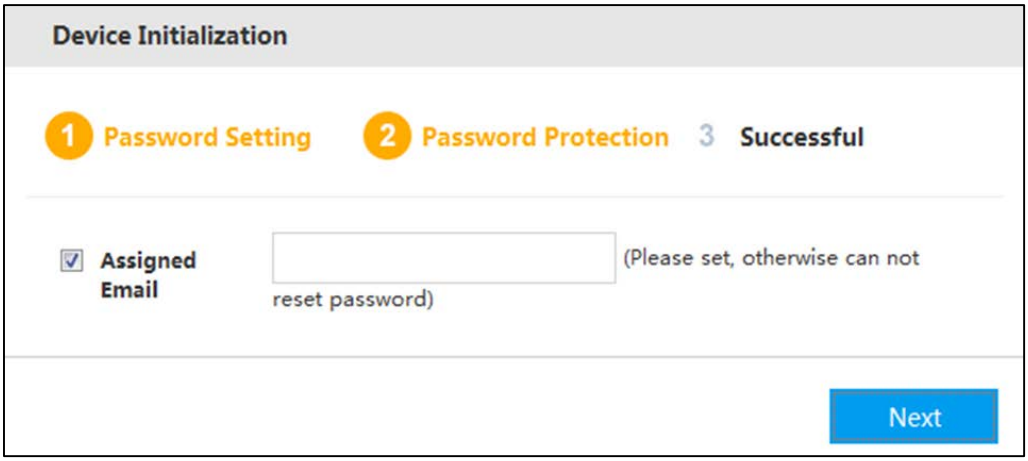


Step 4 In the **New Password** box, enter the new password.

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

Step 5 Click **Next**.

Figure 3-3 Password protection



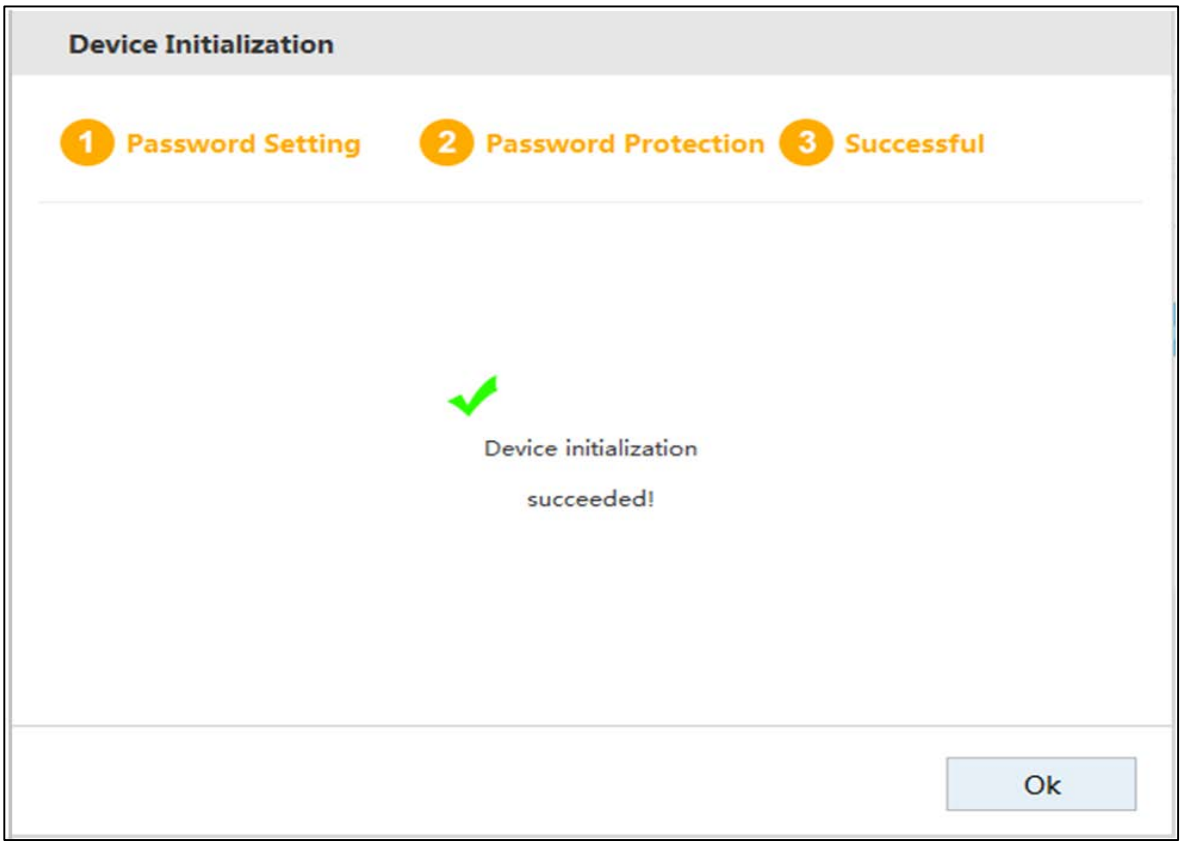
Step 6 In the **Assigned Email** box, enter the assigned email.

After entering the assigned email, you can reset the admin password through the email.

- If you do not need to set the password protection, you can clear the **Assigned Email** checkbox.
- If you have not entered the assigned email, you can enter **Setup > Account > User** to set it after the initialization is completed.

Step 7 Click **Next**.

Figure 3-4 Device initialization succeeded



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

3.3 Logging in to Web

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

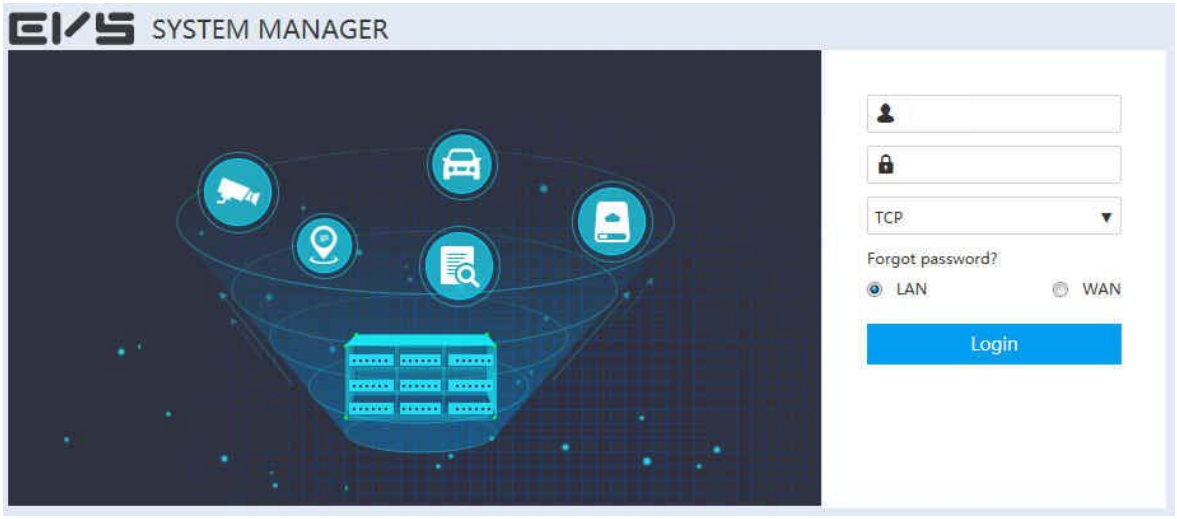
Step 1 Open the browser, enter the IP address in the address bar, and then press Enter.

Step 2 Click **Install**.

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

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

Figure 3-5 Web login



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

The default user name of the administrator is admin, and the password is the one you set in device initialization. To ensure security, it is recommended that you change the password regularly and keep it properly.

Step 4 Click **Login**.

Figure 3-6 System manager

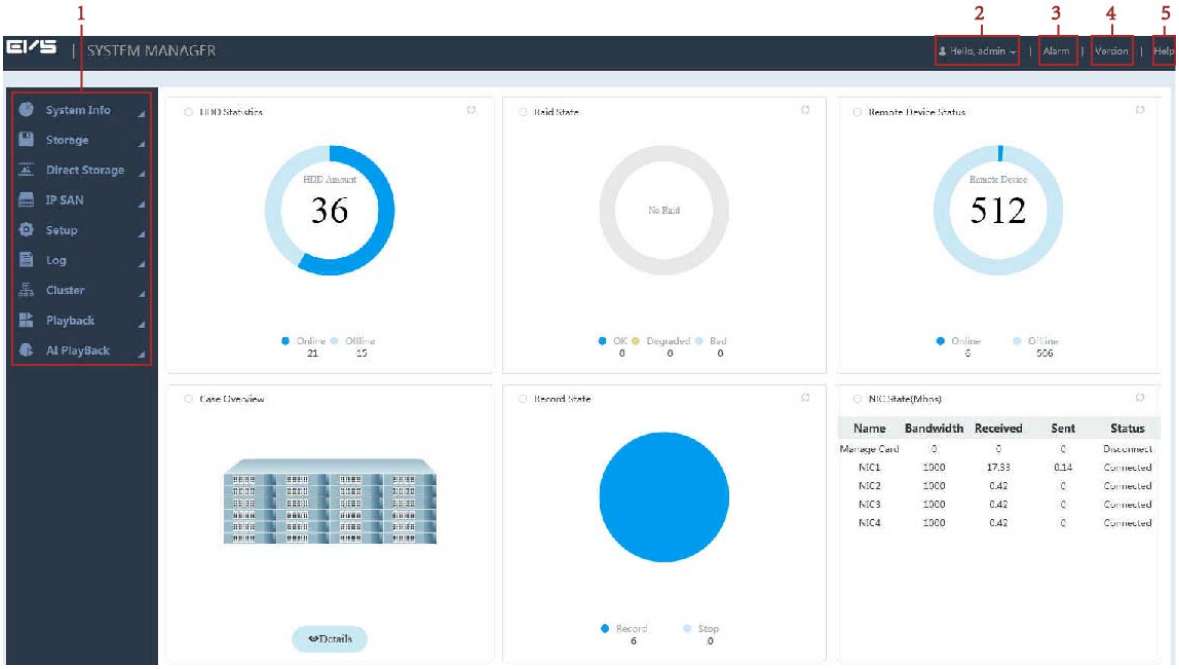


Table 3-1 System manager

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

3.4 Initial Configuration

3.4.1 Setting IP

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

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

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

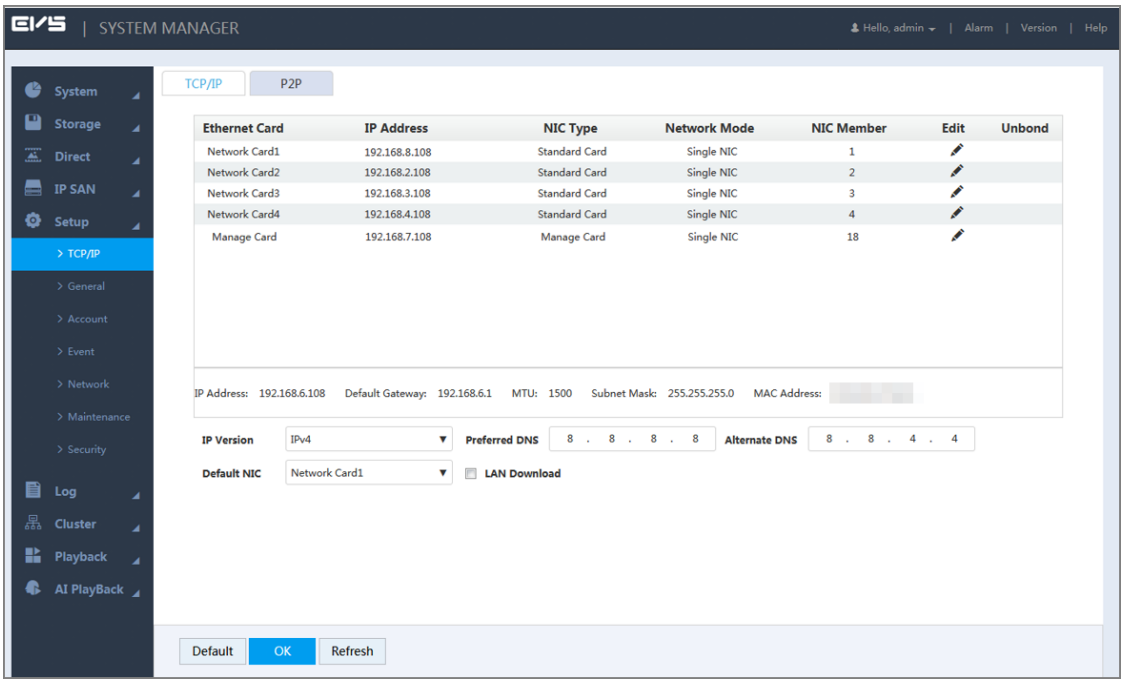


Figure 3-8 Setting TCP/IP (dual-control device)

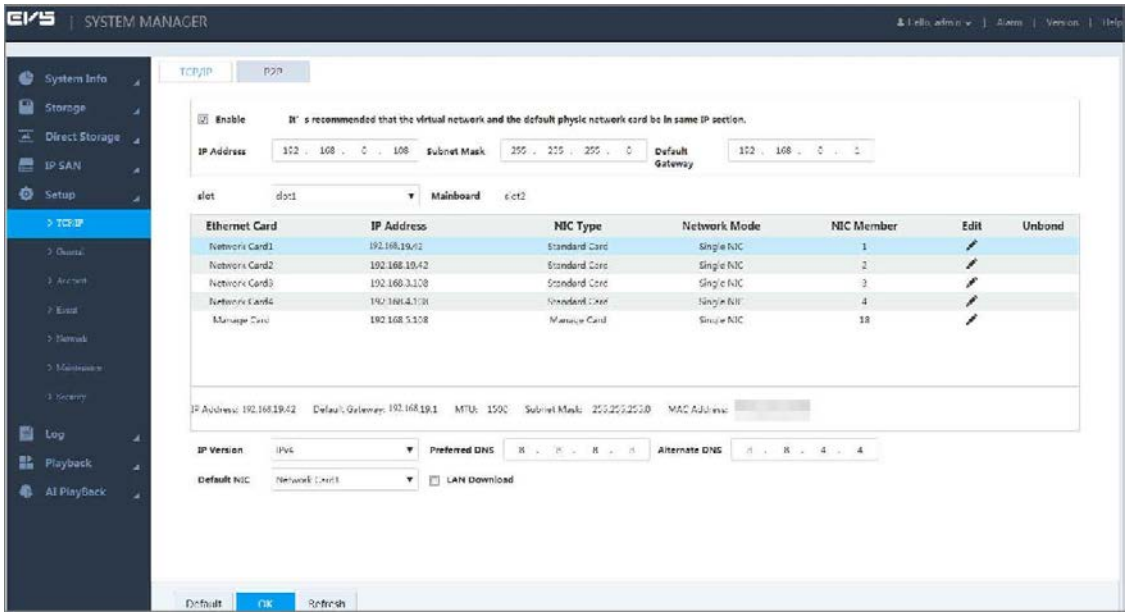
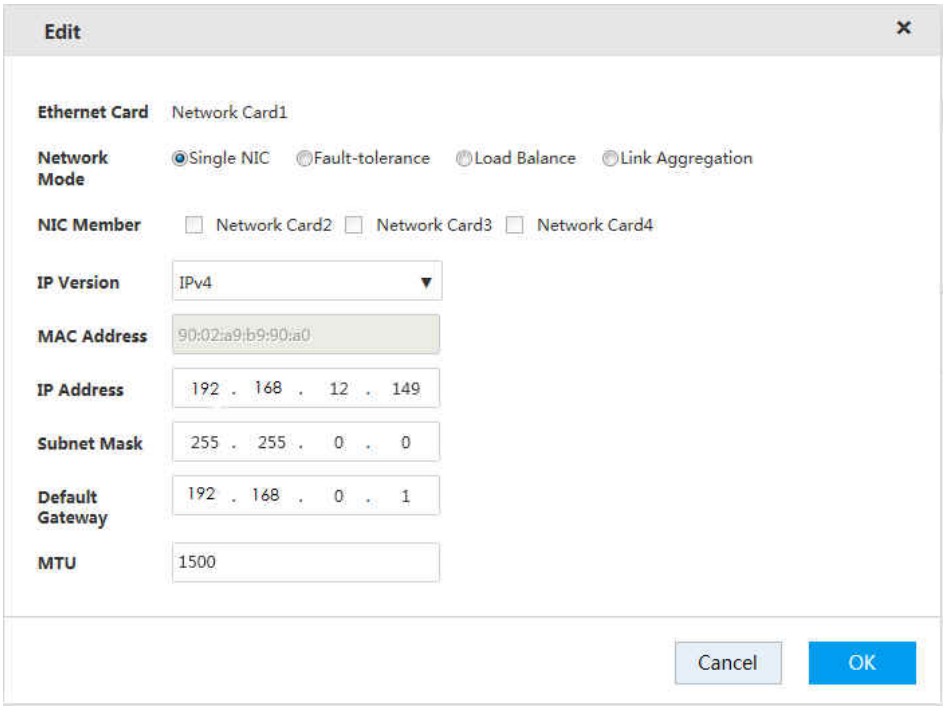


Table 3-2 TCP/IP setting parameters

Parameter	Description
Enable	Enter the virtual IP address of the dual-control device. The main control board and sub control board of dual-control device have their respective physical IP. After setting the virtual IP, in spite of switching between the main and sub control boards, the user can always log in web normally with the virtual IP.
IP Address	
Subnet Mask	
Default Gateway	
Slot	Select the slot of the dual-control device. The corresponding NIC information is displayed in the list. Only dual-control device supports this function.
IP Version	Select the IP version, including IPv4 and IPv6 formats.
Preferred DNS	Enter the IP address of preferred DNS server.
Alternate DNS	Enter the IP address of alternate DNS server.
Default NIC	Select the default NIC of the Device.
LAN Download	Select the checkbox. If network bandwidth allows, the LAN download speed is 1.5–2 times of the normal download speed.

Step 2 Click .

Figure 3-9 Editing



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

Table 3-3 NIC editing parameters

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

Parameter	Description
NIC	When the **Network Mode** is set as **Single NIC**, you can bond the current NIC to any other one. Management NIC does not support this function.
IP Version	You can select IPv4 or IPv6 Format. Currently both IP addresses are supported.
MAC Address	Displays the MAC address of the Device.
IP Address	Set the IP address, subnet mask and default gateway of the Device according to the actual network planning.
Subnet Mask	
Default Gateway	
MTU	Enter the MTU (Maximum Transmission Unit) value of the NIC. The default value is 1,500 bytes. The suggested value is 1,500 or 1,492. ● 1,500: The maximum and default value of the Ethernet packet. It is a typical network connection setting without PPPoE and VPN. It is the default setting of some routers, network adapters and switches. ● 1,492: Optimum value of PPPoE. ● Modifying MTU will lead to NIC restart and network interruption. This will affect the running operations. Operate with care. ● It is recommended to view the MTU value of the gateway first, and set the MTU value of the Device to be the same or slightly smaller than that of the gateway. This will reduce sub package and improve network transmission efficiency.

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

3.4.2 Adding Remote Device

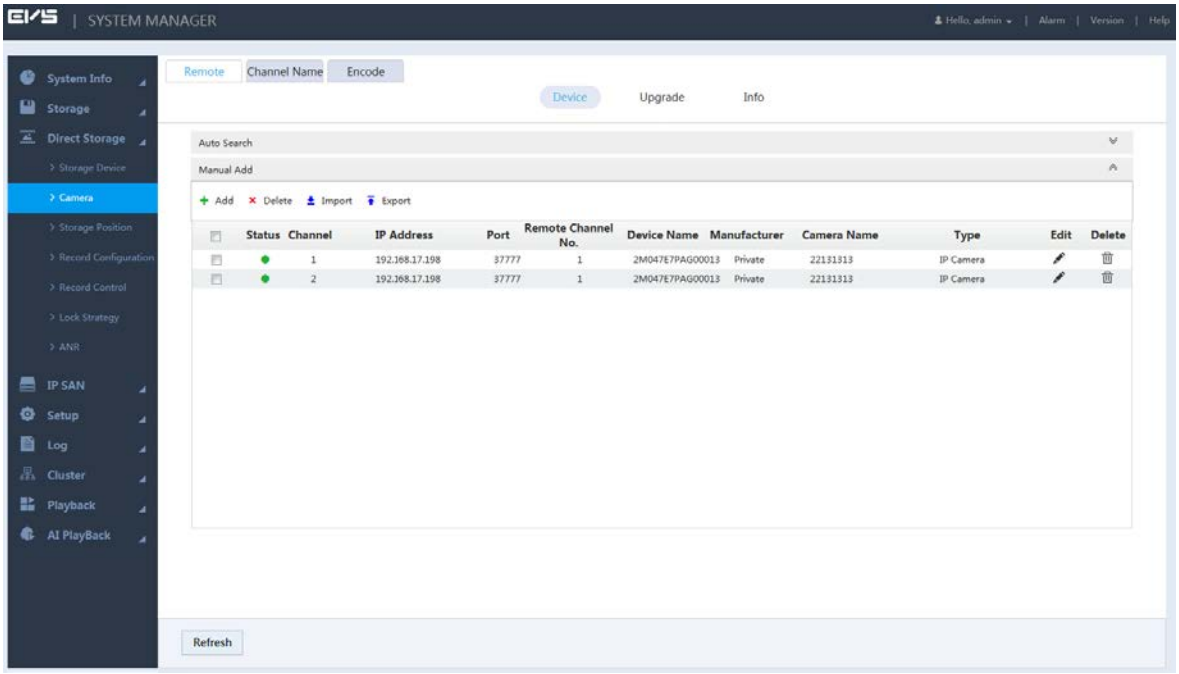
After adding the remote device, the Device can receive, store, and manage the video stream transmitted by the remote device. You can browse, playback, manage, and store several remote devices.

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

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

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

Figure 3-10 Remote device



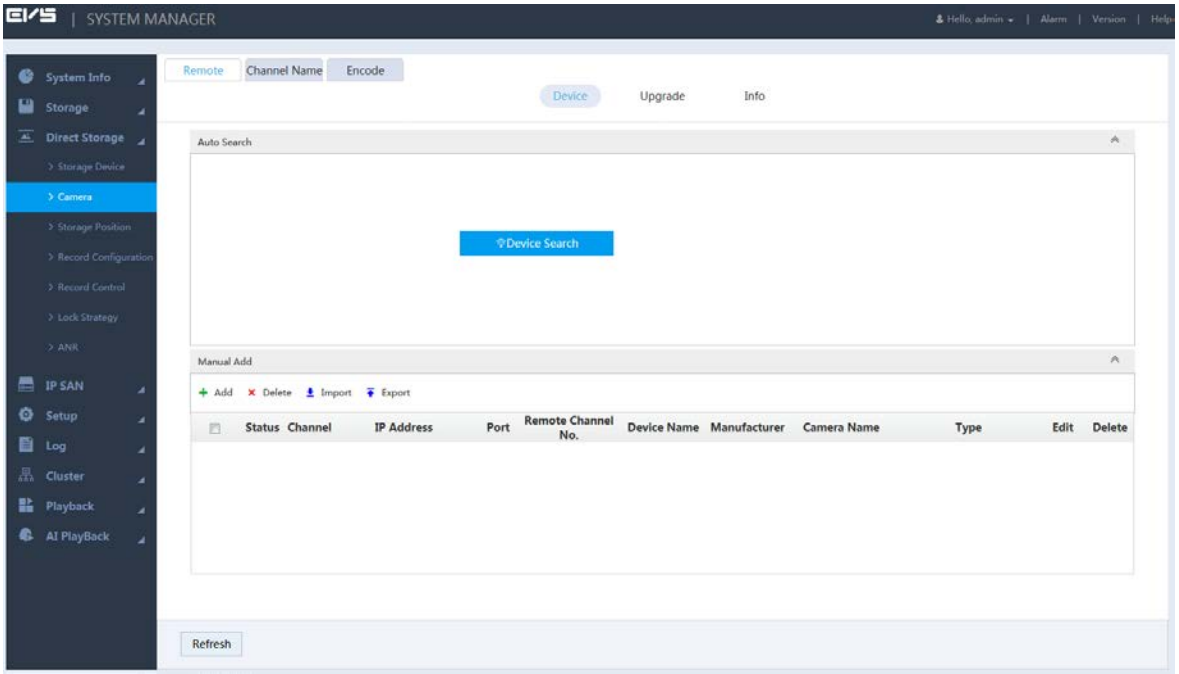
Step 2 Add remote device.

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

- Adding by search

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

Figure 3-11 Automatic search



2) Click **Device Search**.

The results are displayed.

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

Figure 3-12 Search results

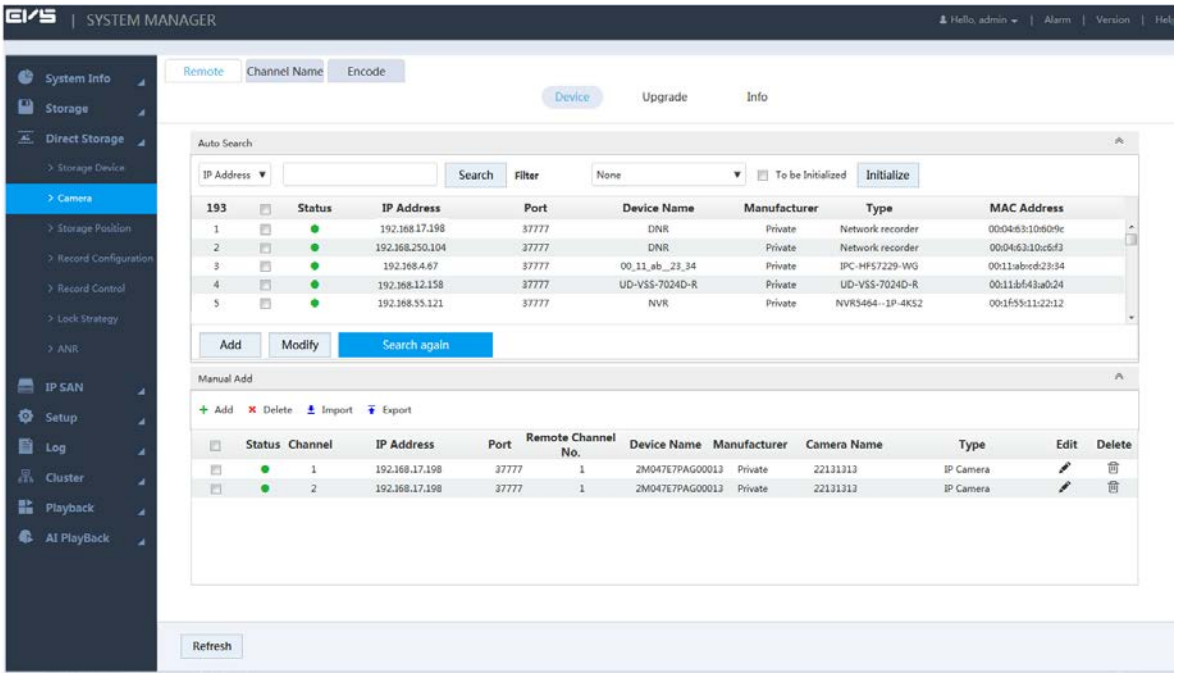


Table 3-4 Auto search icons

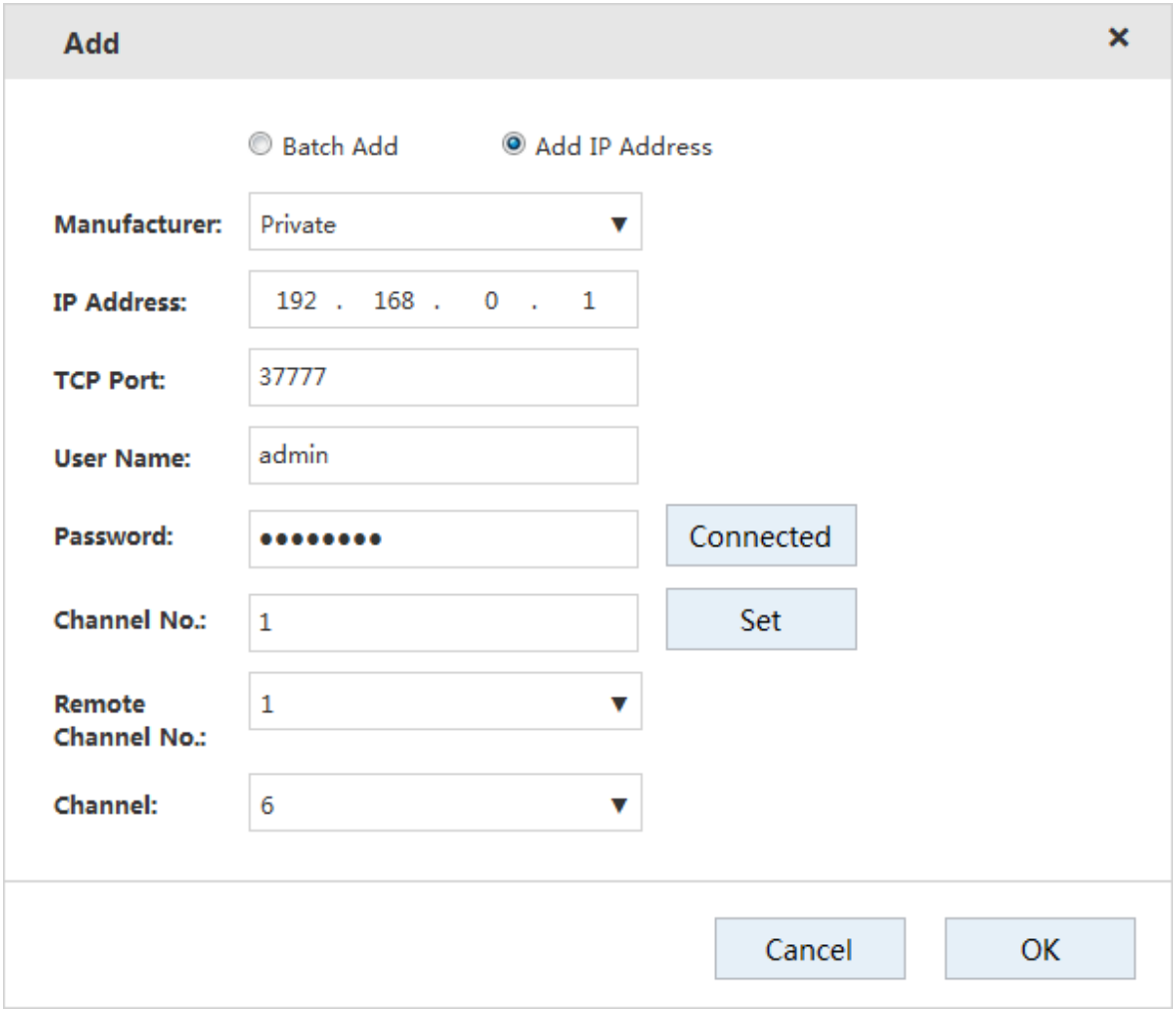
Icon/Parameter	Description
IP Address ▼	Select the remote devices you need to add through IP address or MAC address. 1. Click IP Address ▼ to select IP Address or MAC Address. 2. Enter the IP address or MAC address of the remote device in the text box at the right side of IP Address ▼. 3. Click **Search**.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

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

- Single add

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

Figure 3-13 Adding one device



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

Table 3-5 Adding device

Parameter	Description
Manufacturer	Select the manufacturer in the drop-down box according to the actual situation. Different models support different manufacturer protocols. You need to refer to the actual situation.
IP Address	Set the IP address of the remote device.
TCP Port	Provides services with TCP protocol. You can set the port according to actual needs. The default is 37777. You need to set it when the **Manufacturer** is set as **Private**.
RTSP Port	Set the RTSP port No. of the remote device. The default is 554. You do not need to configure it when the **Manufacturer** is set as **Private** or **Custom**.

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

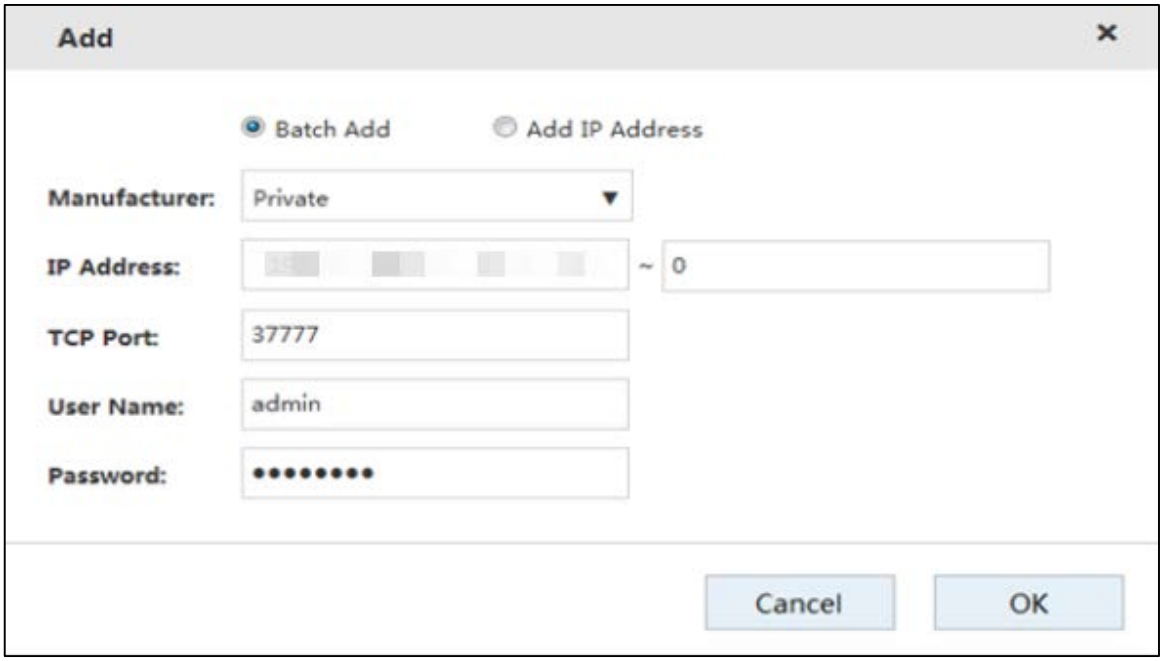
3) Click **OK** to complete adding.

- Batch add

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

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

Figure 3-14 Batch add



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

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

3) Set other parameters. For details, see Table 3-5.

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

- Importing from template

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

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

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

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

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

3) Click to select the template file.

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

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

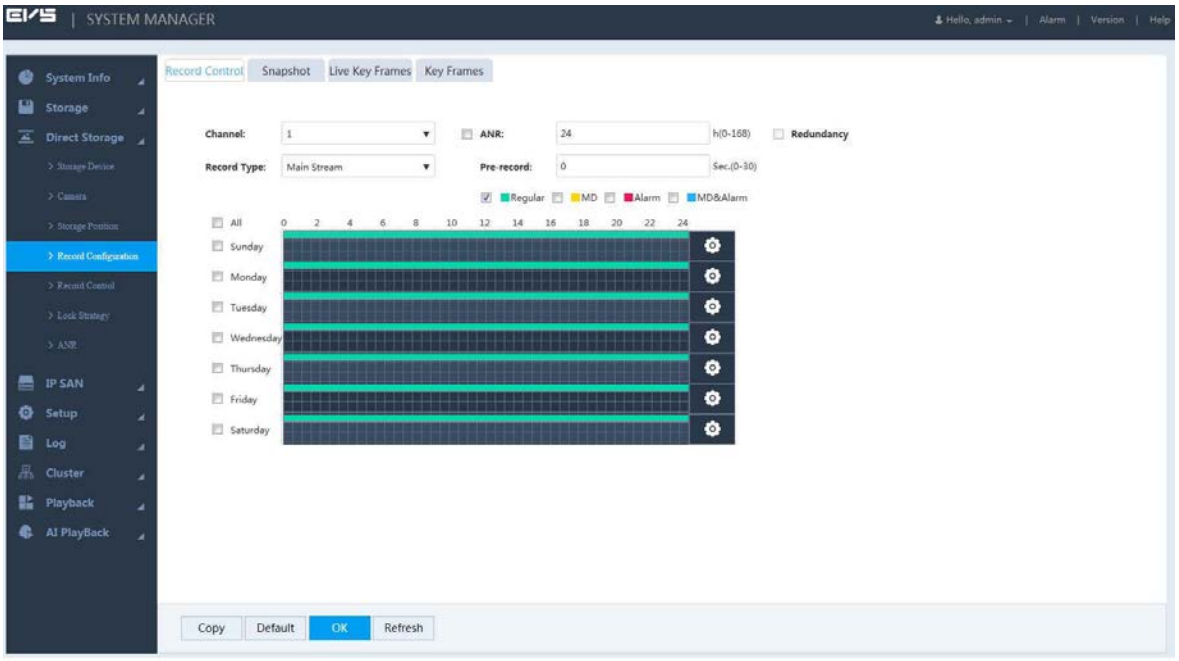
3.4.3 Configuring Record Plan

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

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

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

Figure 3-15 Record plan



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

Table 3-6 Record parameters

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

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

Step 3 Select the alarm type.

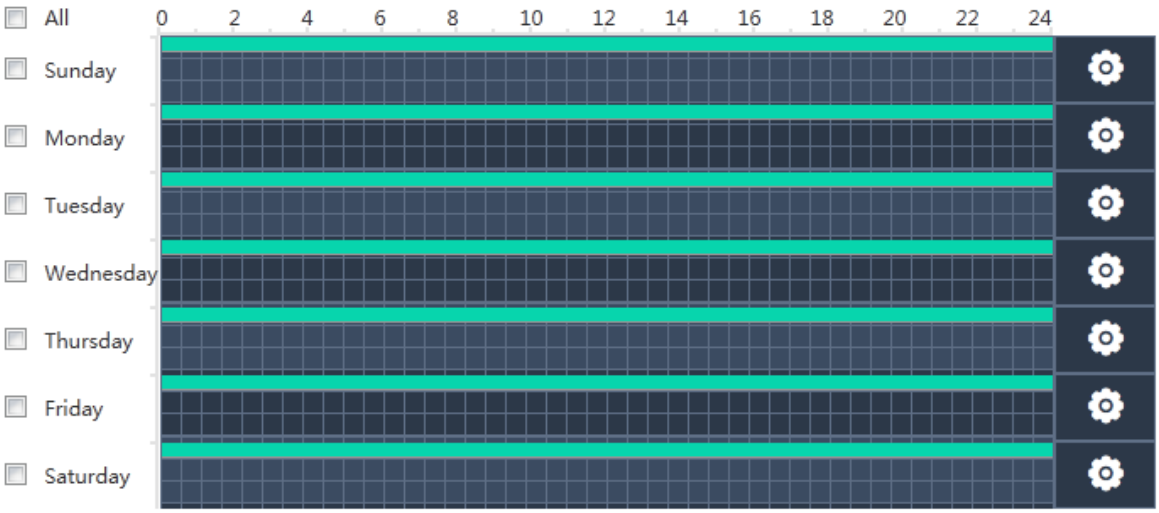
Figure 3-16 Alarm type

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

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

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

Figure 3-17 Time period setting



- Drawing:

1) Select the weekday.

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

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

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

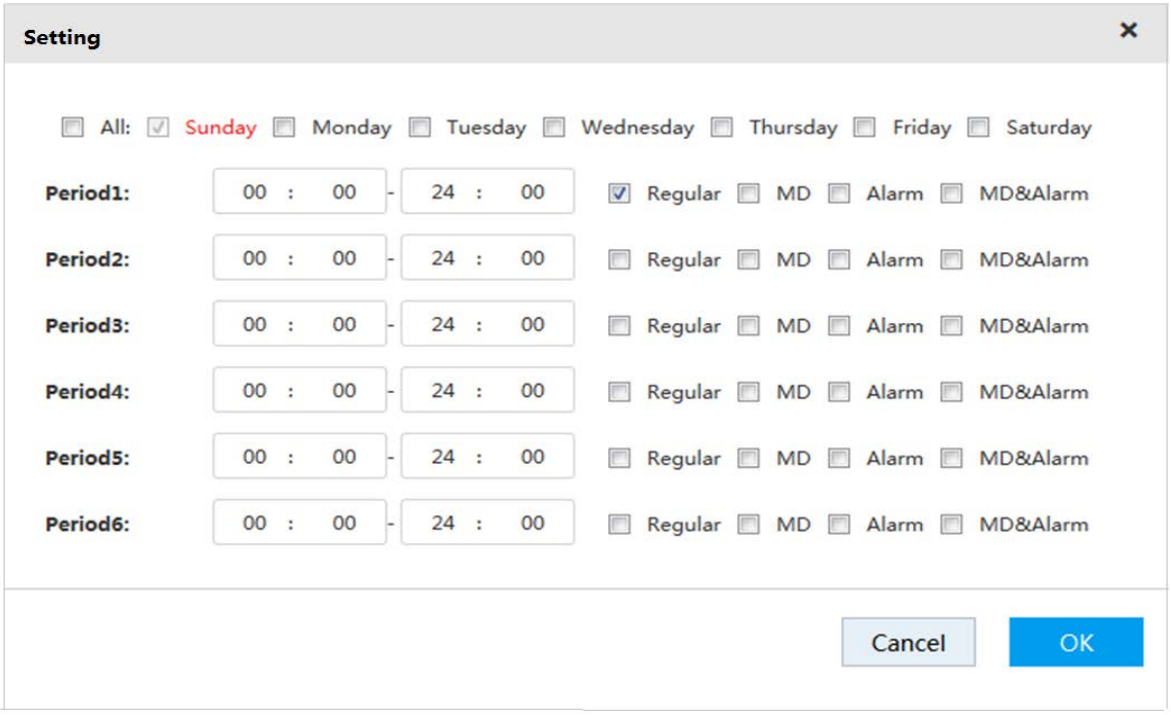
◇ You can set six periods for each day. The Device performs recording in the corresponding period.

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

- Editing:

1) Select the corresponding weekday and click .

Figure 3-18 Period setting



2) Select the weekday, record type and period.

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

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

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

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

3.4.4 Enabling Record Function

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

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

- Auto record: The system automatically takes records according to the set record type and record

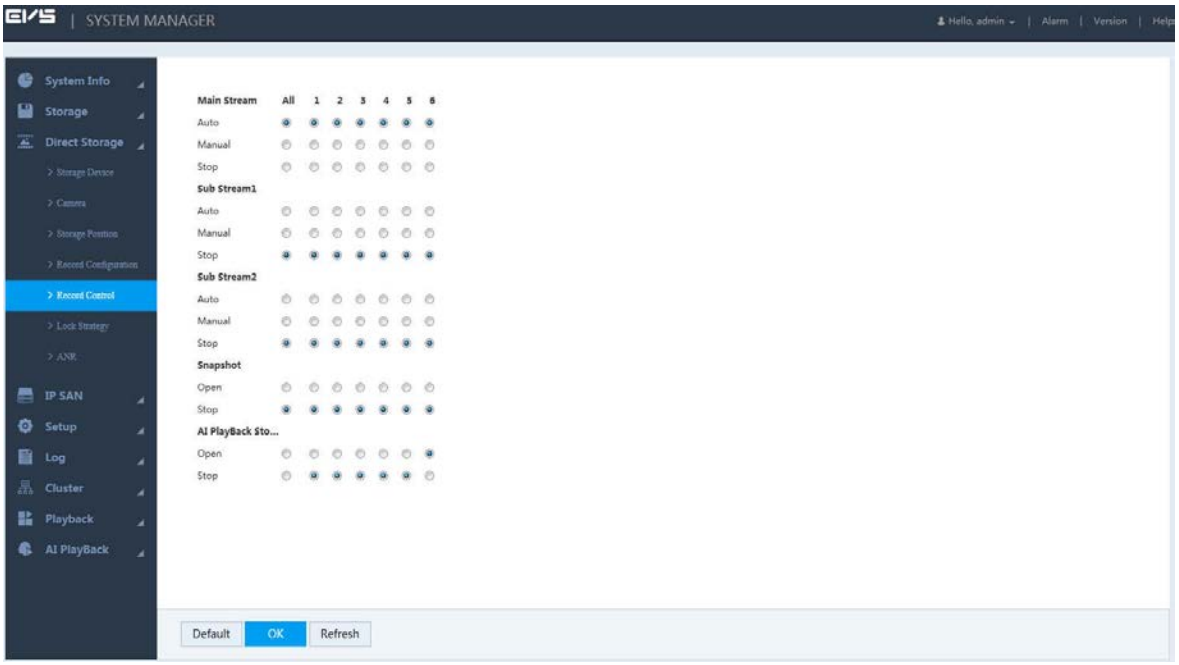
time.

- Manual record: The system takes 24-hour continuous records in the channel.

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

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

Figure 3-19 Record control



Step 2 Configure the parameters. For details, see Table 3-7.

Table 3-7 Record control parameters

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

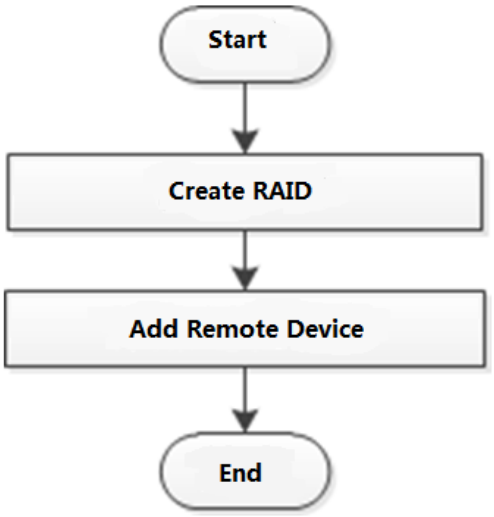
Step 3 Click **OK** to save the configuration.

3.5 Video Direct Storage

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

For the procedure to configure video direct storage, see Figure 3-20.

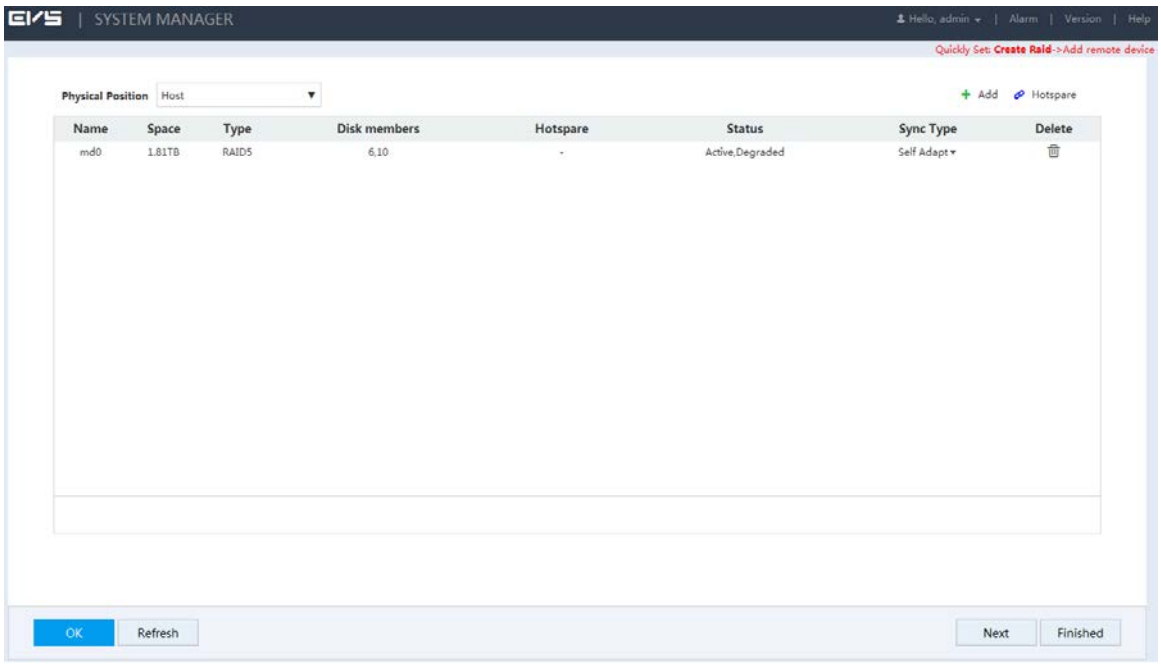
Figure 3-20 Video direct storage



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

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

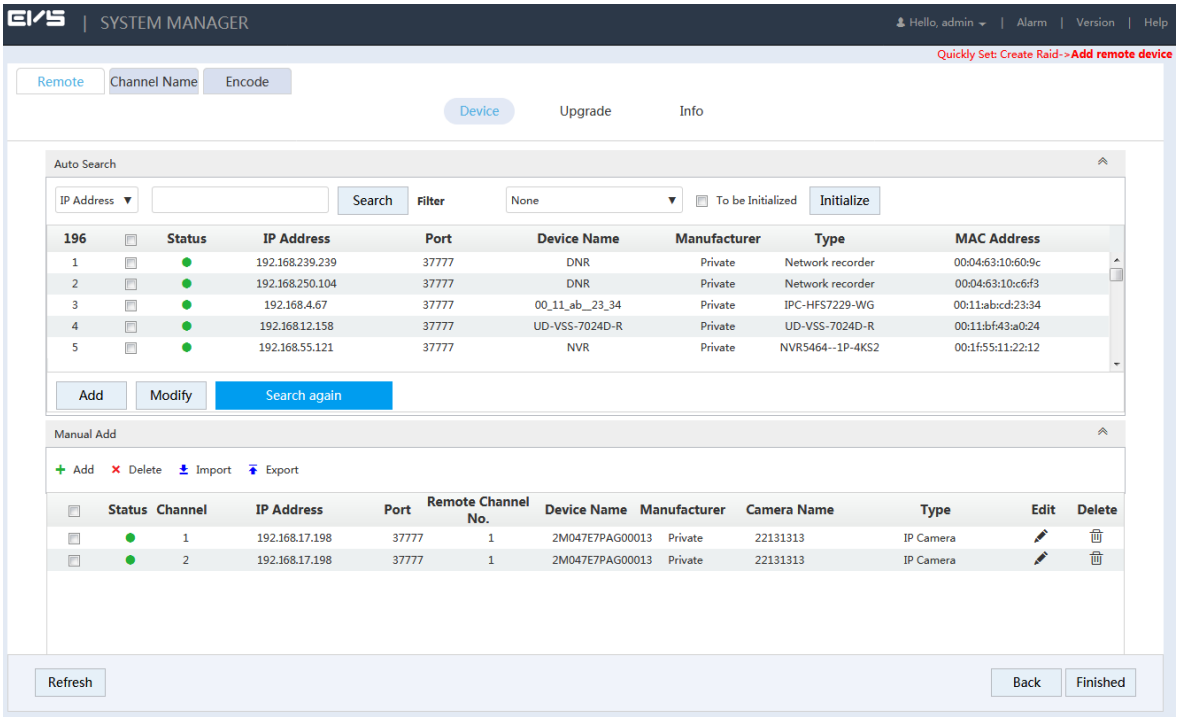
Figure 3-21 RAID management



Step 2 Create RAID. For details, see "3.8.1 Creating RAID."

Step 3 Click **Next**.

Figure 3-22 Adding remote device



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

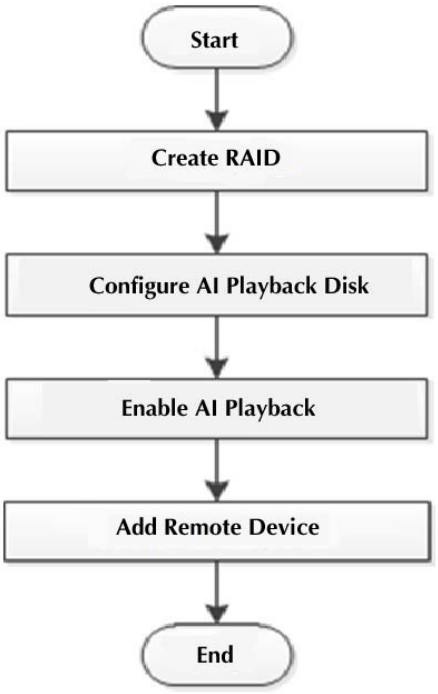
Step 5 Click **Finished** to save the configuration.

3.6 AI Playback

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

For the procedure to configure AI playback, see Figure 3-23.

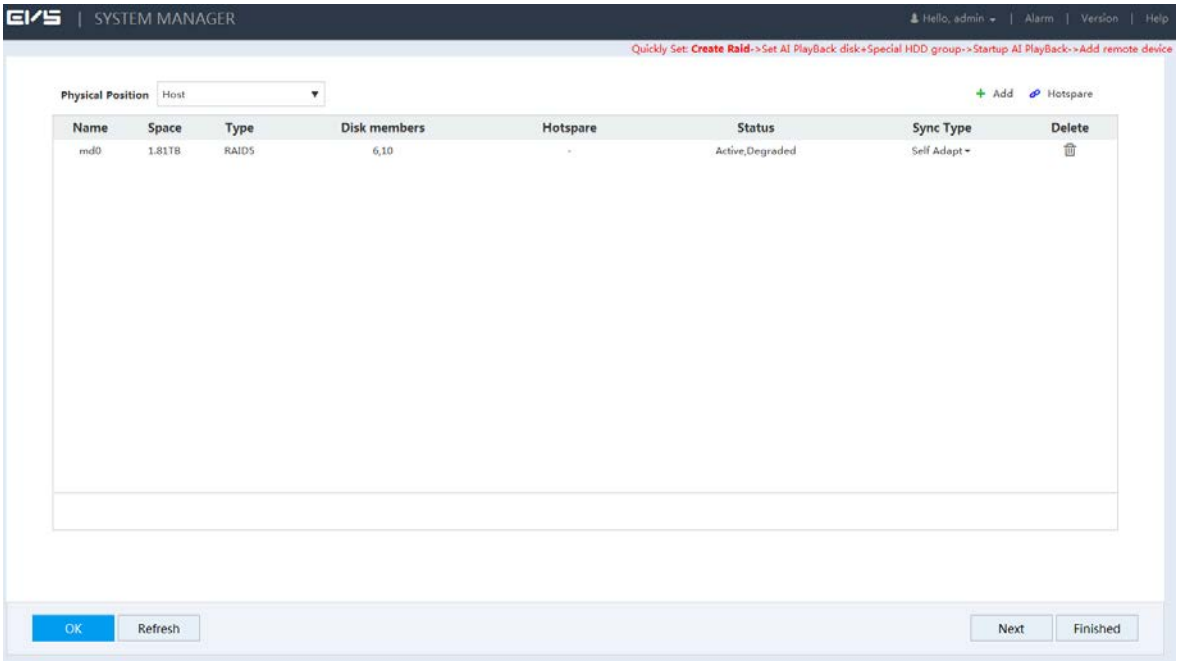
Figure 3-23 AI playback



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

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

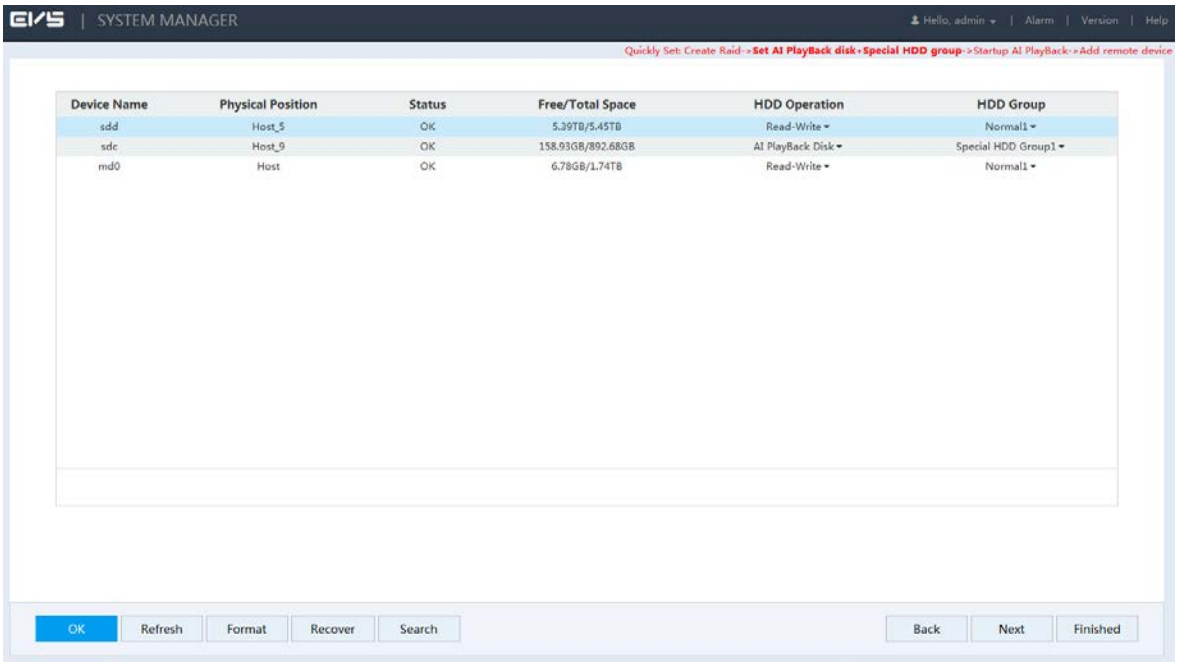
Figure 3-24 RAID management



Step 2 Create RAID. For details, see "3.8.1 Creating RAID."

Step 3 Click **Next**.

Figure 3-25 Setting AI playback HDD and special HDD group

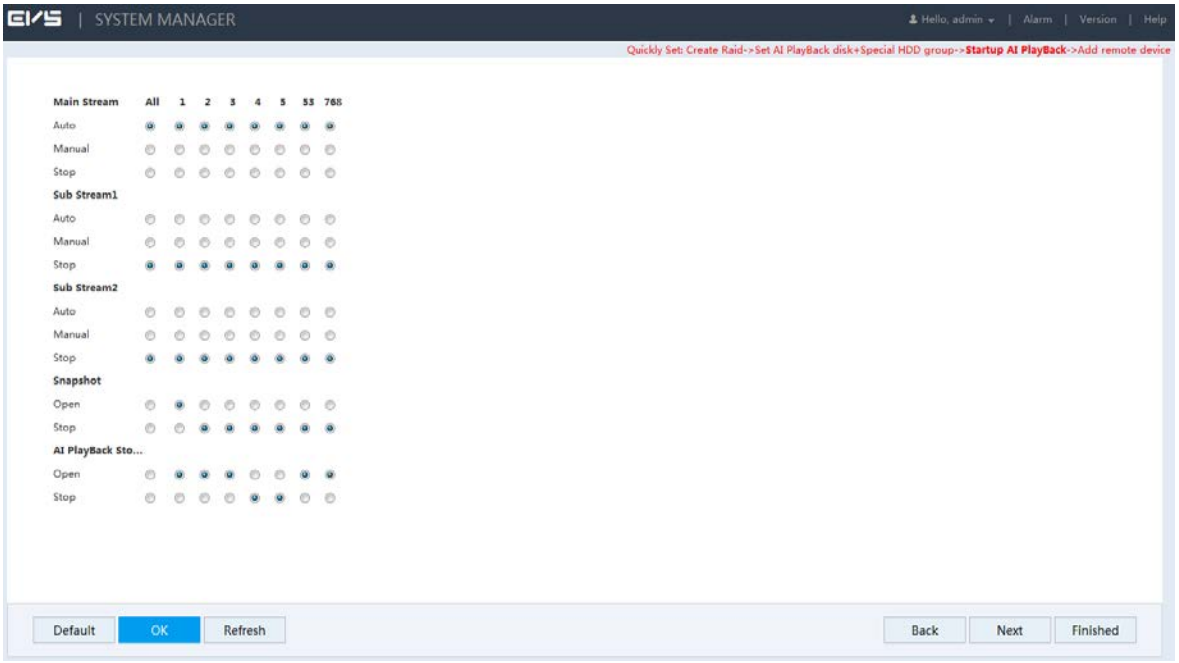


Step 4 Set AI playback HDD and HDD group.

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

Step 5 Click **Next**.

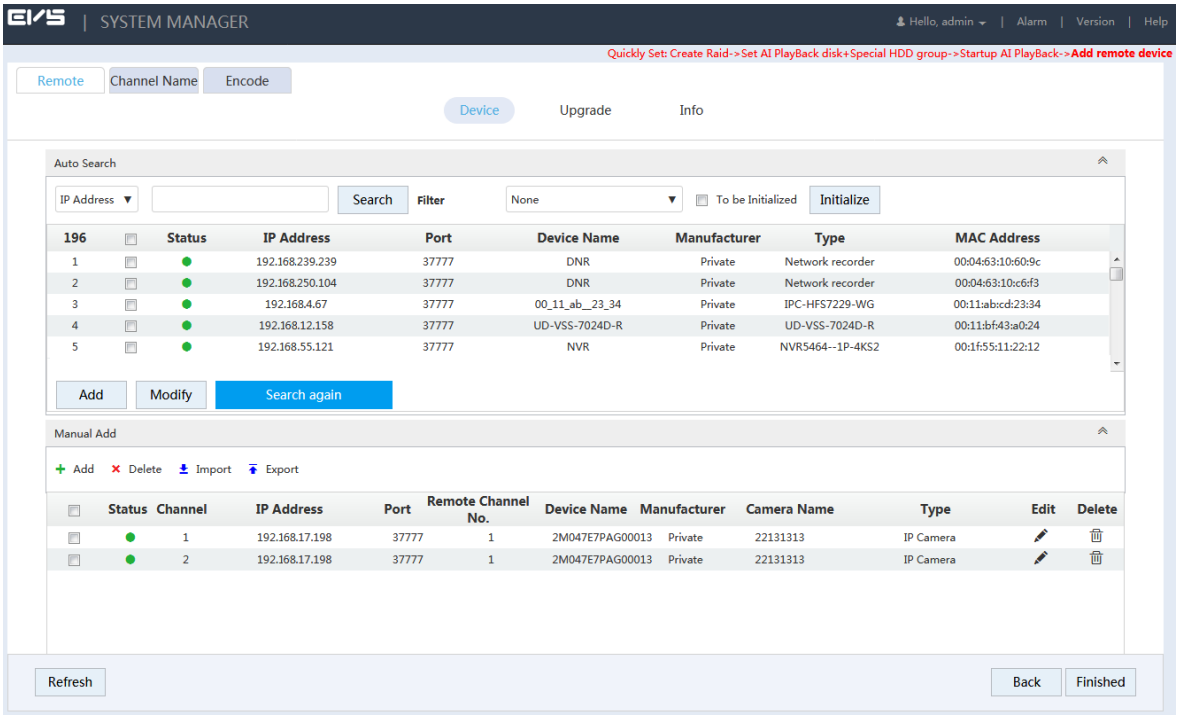
Figure 3-26 AI playback startup



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

Step 7 Click **Next**.

Figure 3-27 Adding remote device



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

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

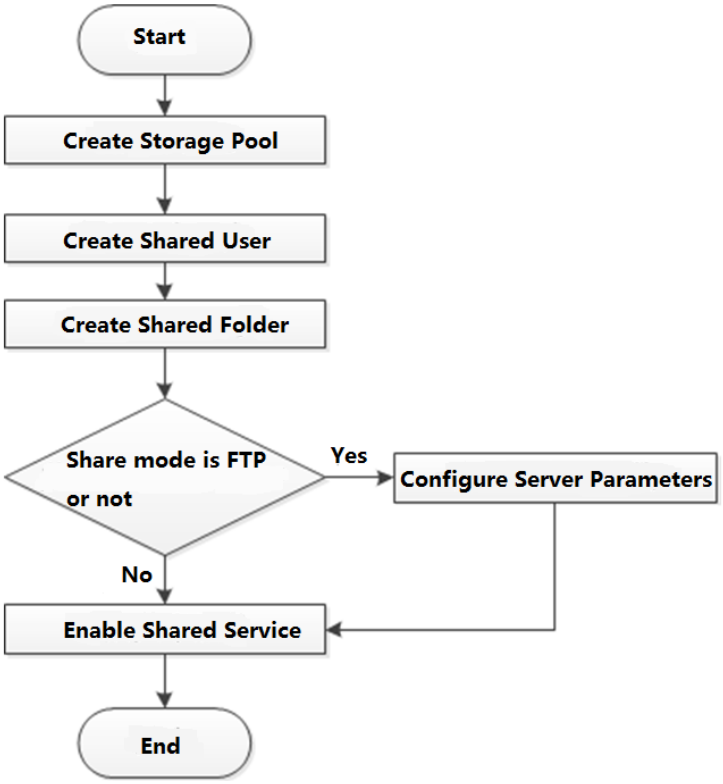
After the configuration, you can search the AI playback video.

3.7 IP SAN

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

For the procedure to configure IP SAN, see Figure 3-28.

Figure 3-28 Configuring IP SAN



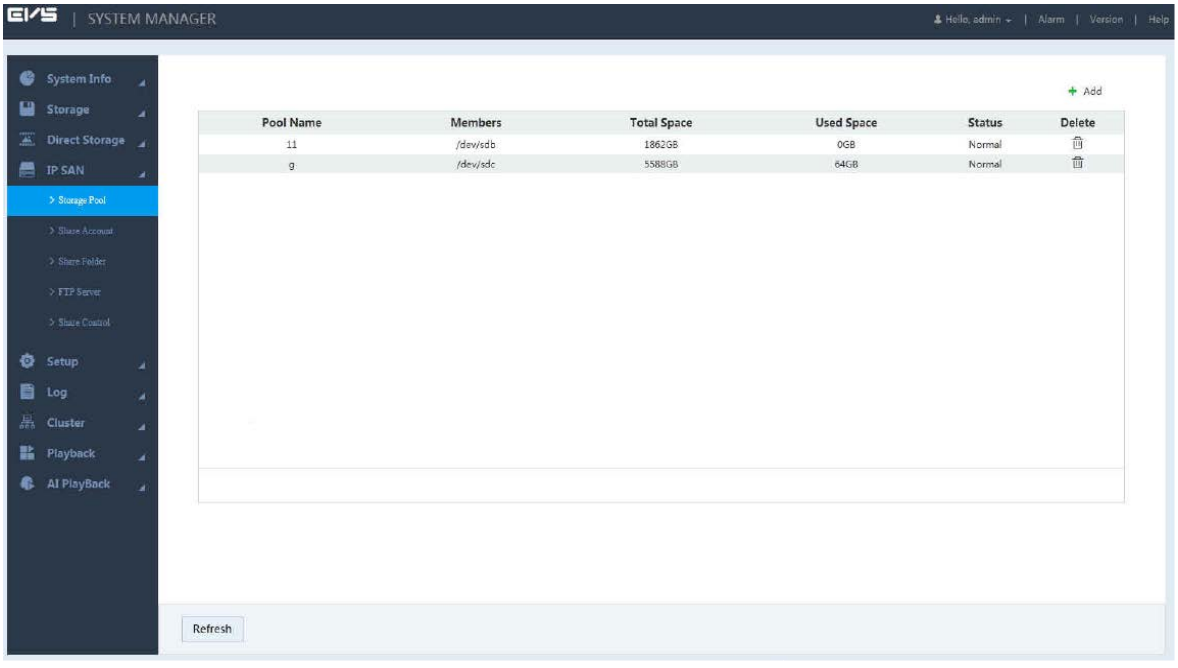
3.7.2 Creating Storage Pool

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

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

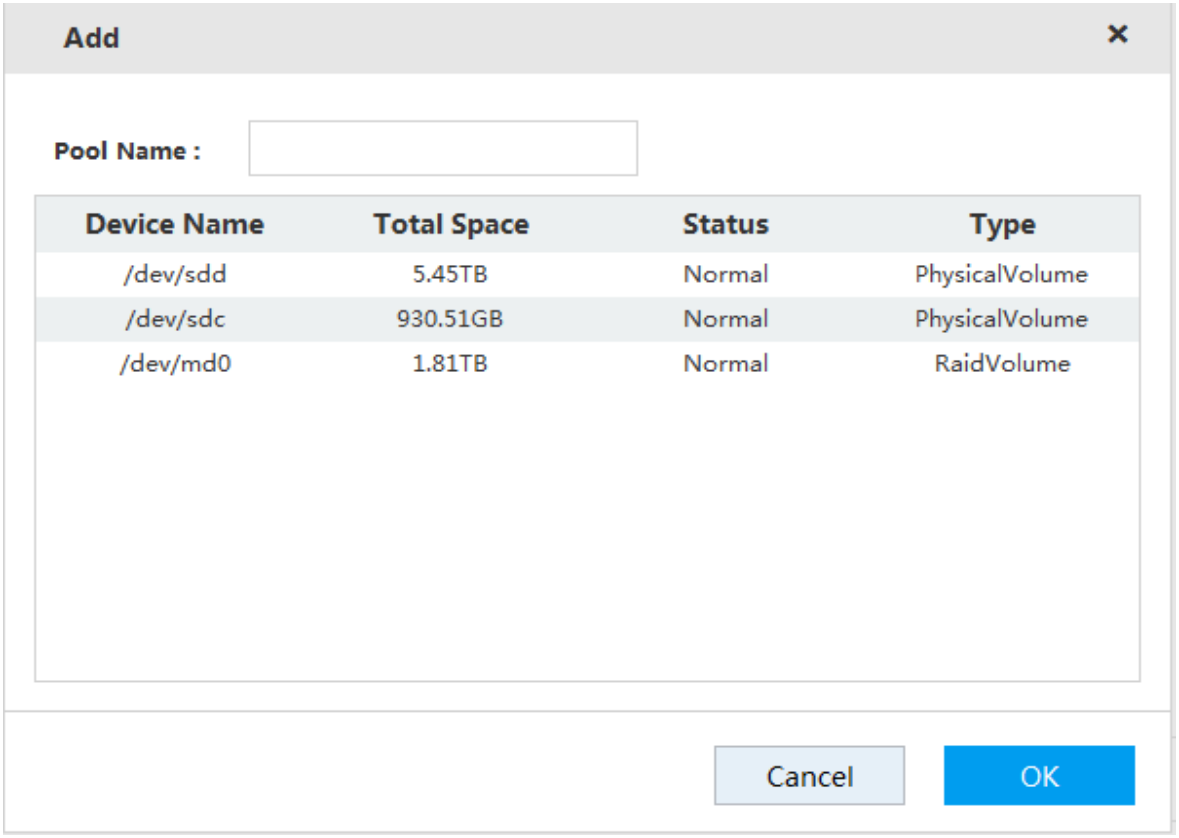
Step 1 Select **IP SAN > Storage Pool**.

Figure 3-29 Storage pool



Step 2 Click + .

Figure 3-30 Adding storage pool



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

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

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

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

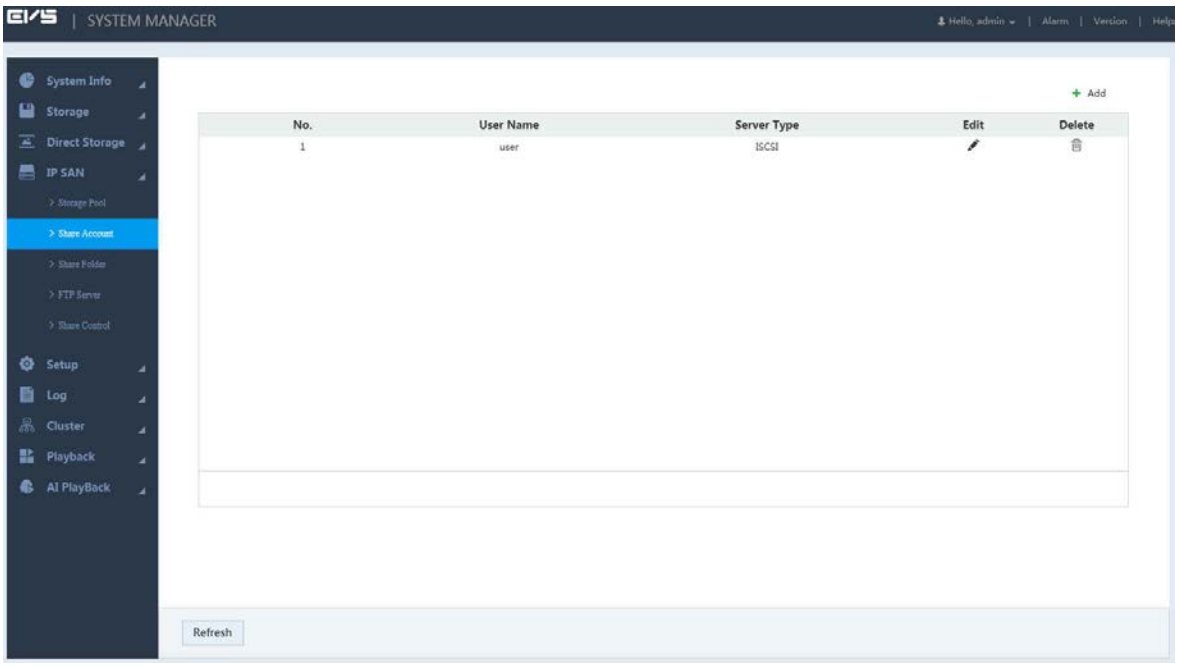
The system starts to create the storage pool. After the creation, the system returns to the **Storage Pool** page. You can view the new pool information here.

3.7.3 Managing Share Account

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

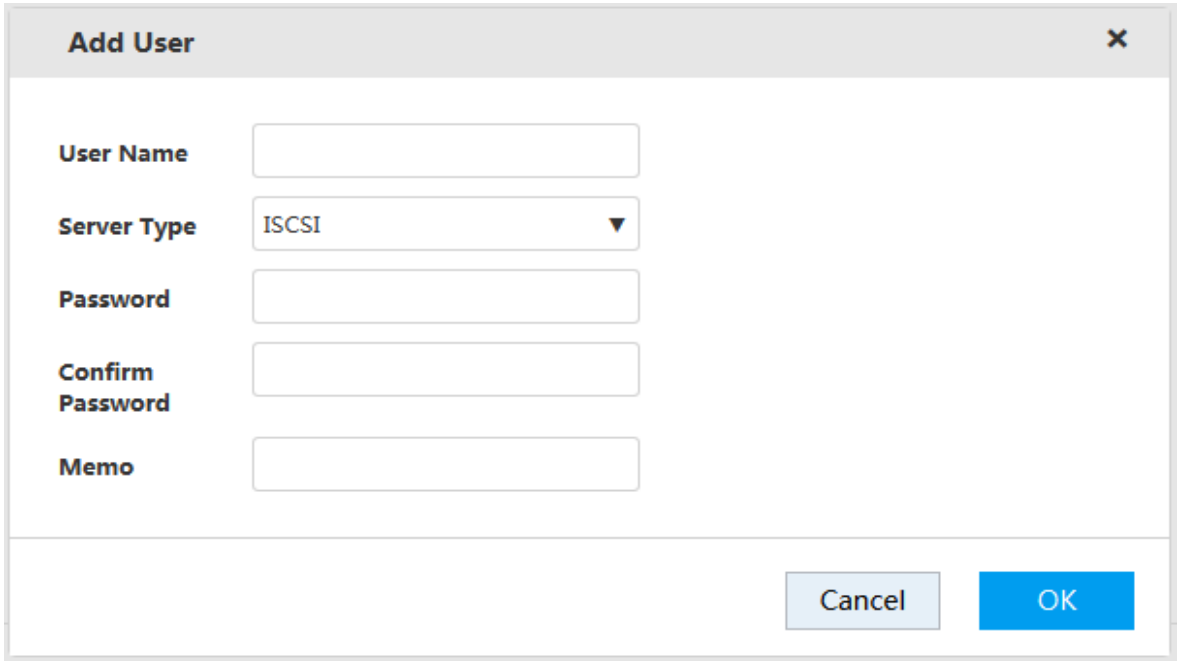
Step 1 Select **IP SAN > Share Account**.

Figure 3-31 Share account management



Step 2 Click + .

Figure 3-32 Adding shared user



Step 3 Configure the parameters. For details, see Table 3-8.

Table 3-8 Adding user parameters

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

Parameter	Description
Memo	Enter memo to help recognize and manage the account.

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

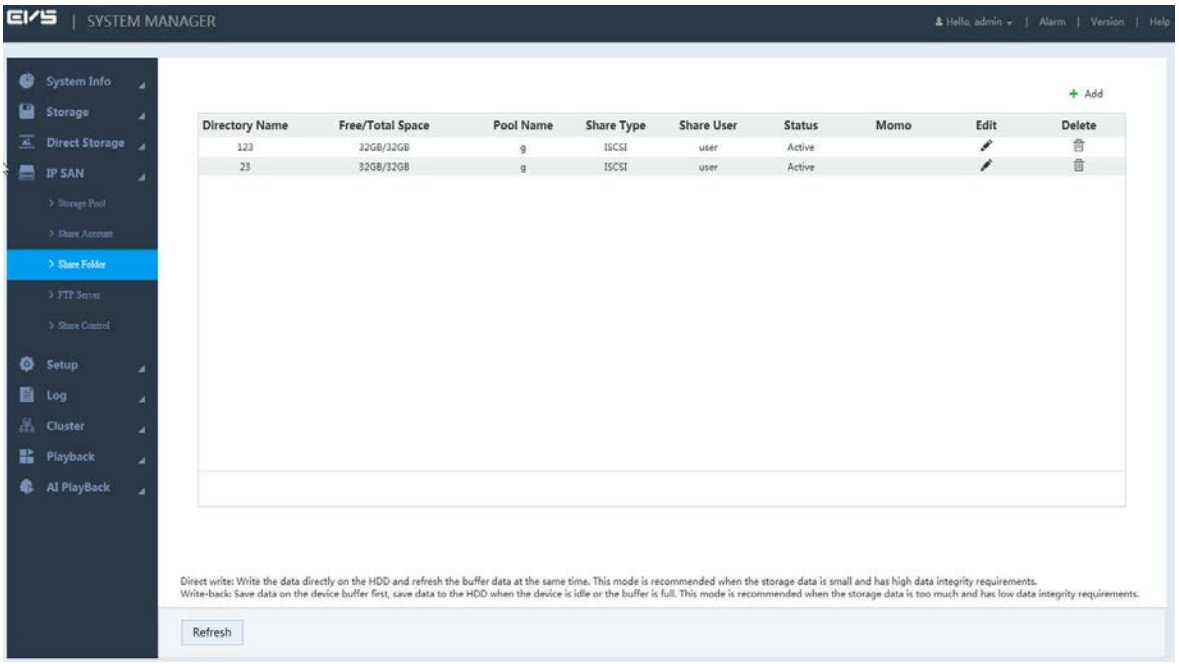
The system returns to the **Share Account** page. You can view the new account information here.

3.7.4 Setting Share Folder

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

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

Figure 3-33 Share folder



Step 2 Click + .

Figure 3-34 Adding share folder (NFS)

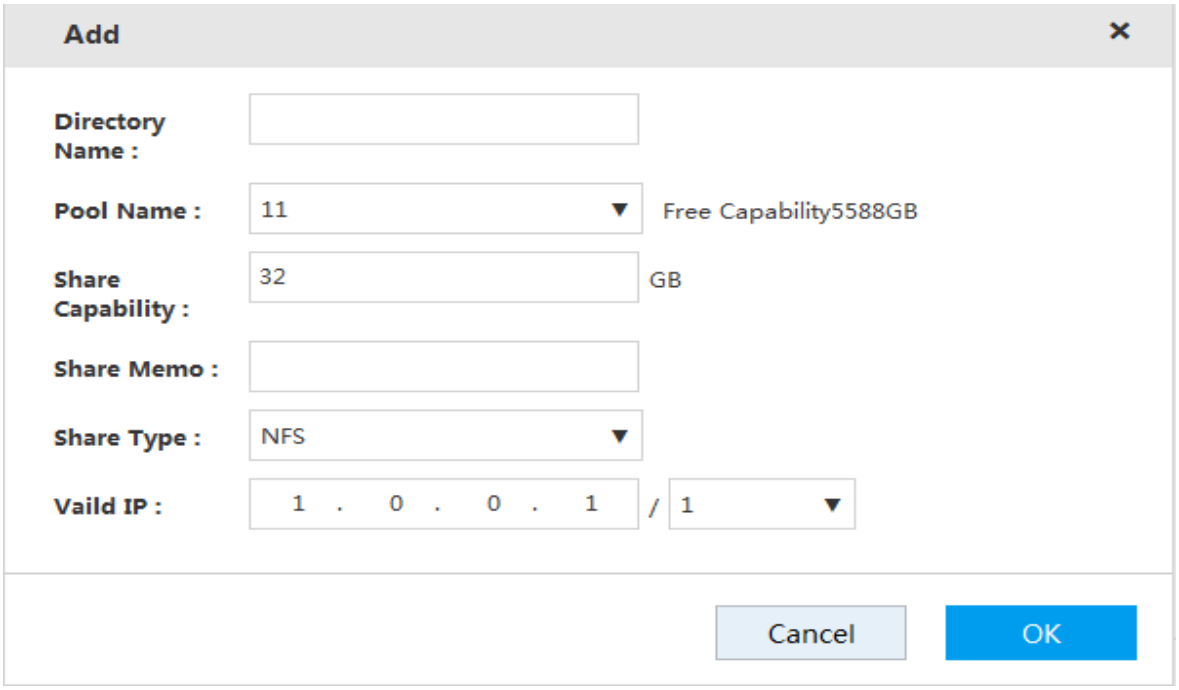
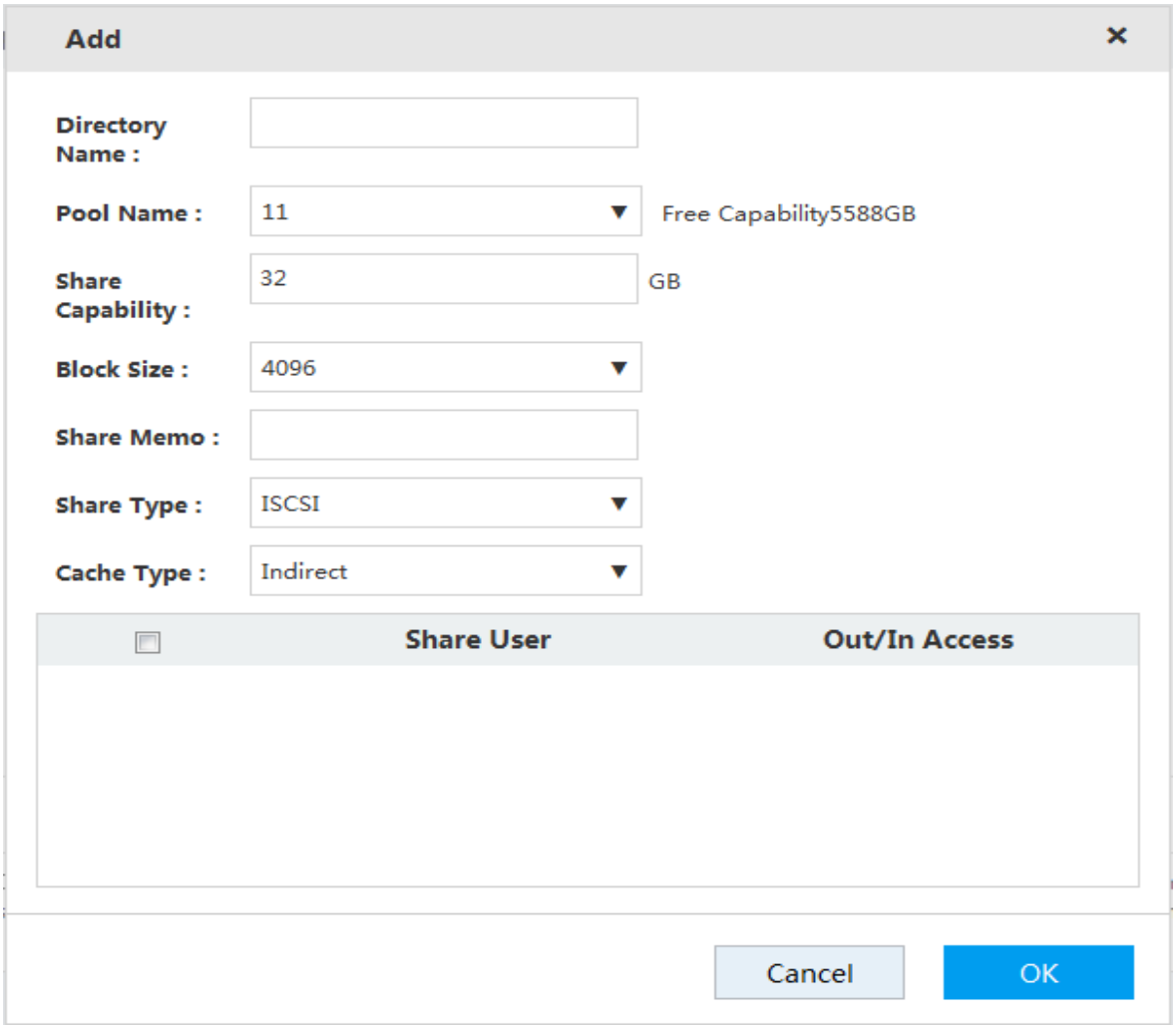


Figure 3-35 Adding share folder (iSCSI)



Step 3 Configure the parameters.

Table 3-9 Share folder parameters

Parameter	Description
Directory Name	Enter the name of the share folder.
Pool Name	Select the pool in which you need to create the share folder. Free capability refers to the max available volume of the storage pool.
Share Capability	Enter the available space of the share folder.
Share Memo	(Optional) It helps to recognize and manage the share folder.
Share Type	Select the **Share Type**: ● NFS: Provides share services to Linux users. ● FTP: Provides share services to Windows and Linux users at the same time. ● SAMBA: Provides share services to Windows users. ● iSCSI: Provides share services to iSCSI users.

Parameter	Description
Valid IP	Set the IP address and subnet mask of the hosts allowed to access this share folder. For example: When the valid IP is 192.168.10.108/24, it means the IP address is 192.168.10.108 and the subnet mask is 255.255.255.0. All the IP hosts in this segment can access the share folder. This parameter needs to be configured when the **Share Type** is set as NFS.
Valid User	Select the shared user and set its out/in access authority. ● When the **Share Type** is set as FTP and SAMBA and no valid user is selected, only the admin account has the access permission. Other accounts do not have the authority. ● When the **Share Type** is set as iSCSI and no valid user is selected, all the users have the access permission. ● You need to select the valid user when select FTP, SAMBA or iSCSI as the share type. ● FTP default admin account: ftpuser; default password: 111111111111. SAMBA default admin account: admin; default password: 888888888888.
Cache Type	It includes **Direct** and **Indirect**. ● Direct: Store the data directly into the disk and update the data in cache. When you have little data but high integrity request, direct strategy is recommended. ● Indirect: Store data in the cache first and transfer it to the disk when the system is free or the cache is full. When you have a large amount of data and the data integrity request is low, indirect strategy is recommended. You need to configure this item when the share type is iSCSI.
Block Size	Select the block size of share folder, including 512Byte, 1024Byte, 2048Byte and 4096Byte. You need to configure this item when the share type is iSCSI.

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

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

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

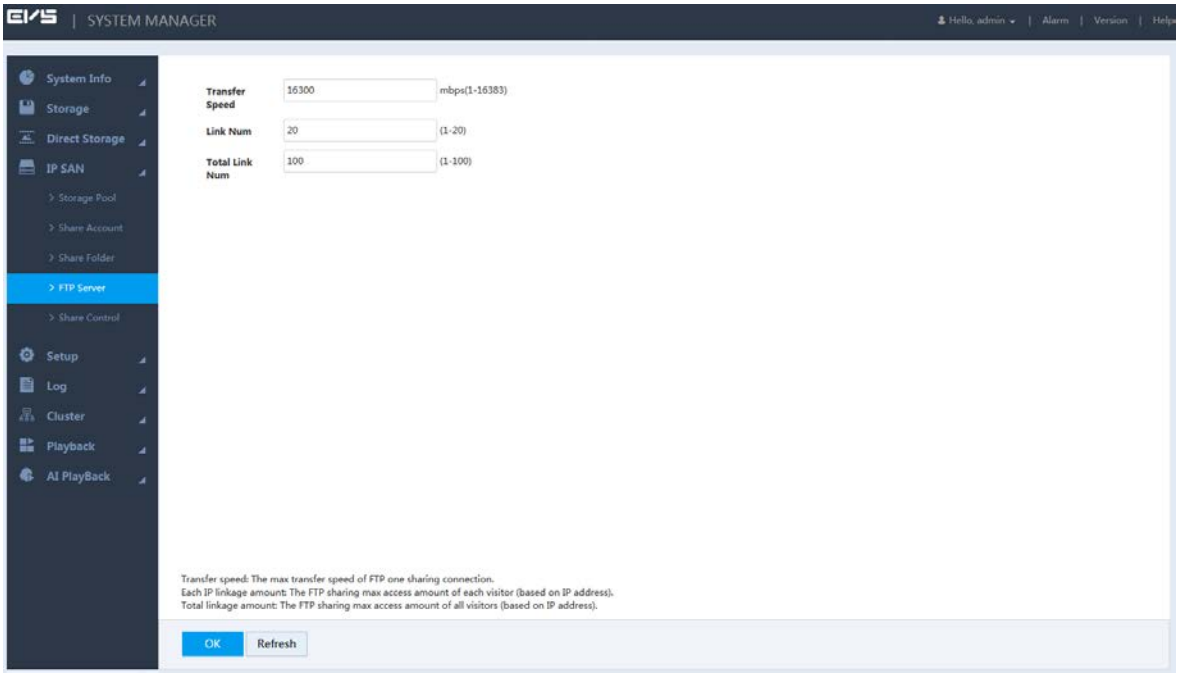
3.7.5 Setting FTP Parameters

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

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

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

Figure 3-36 FTP Parameters



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

Table 3-10 FTP server parameters

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

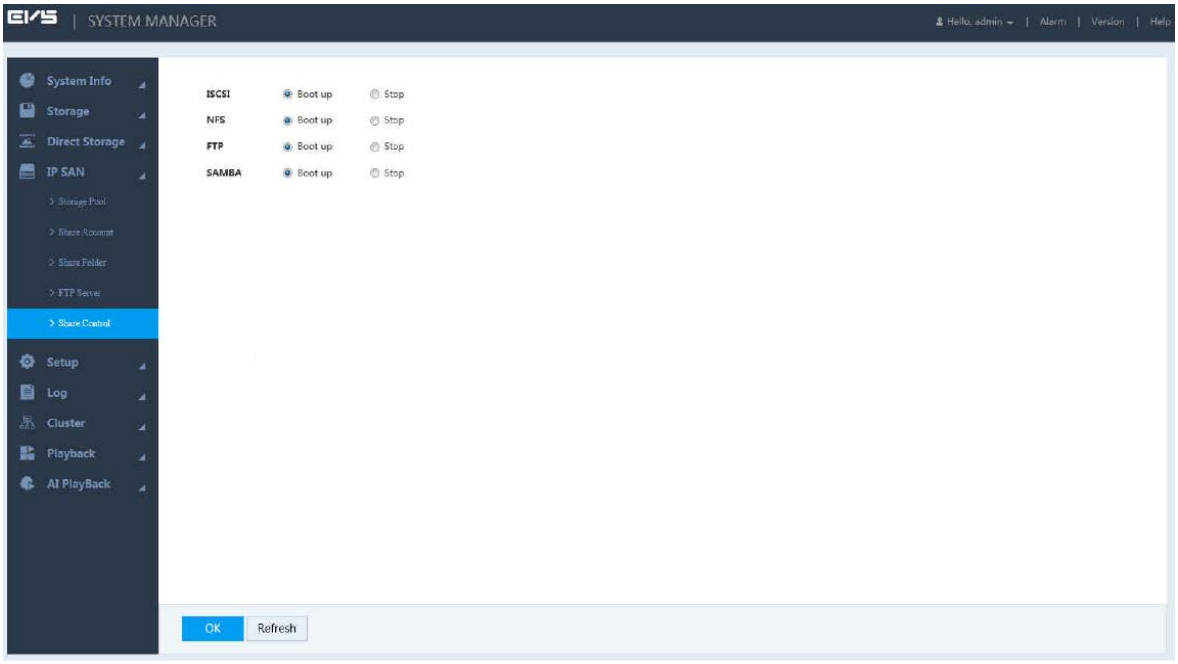
Step 3 Click **OK** to save the configuration.

3.7.6 Opening Share Services

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

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

Figure 3-37 Share control



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

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

3.8 RAID Management

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

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

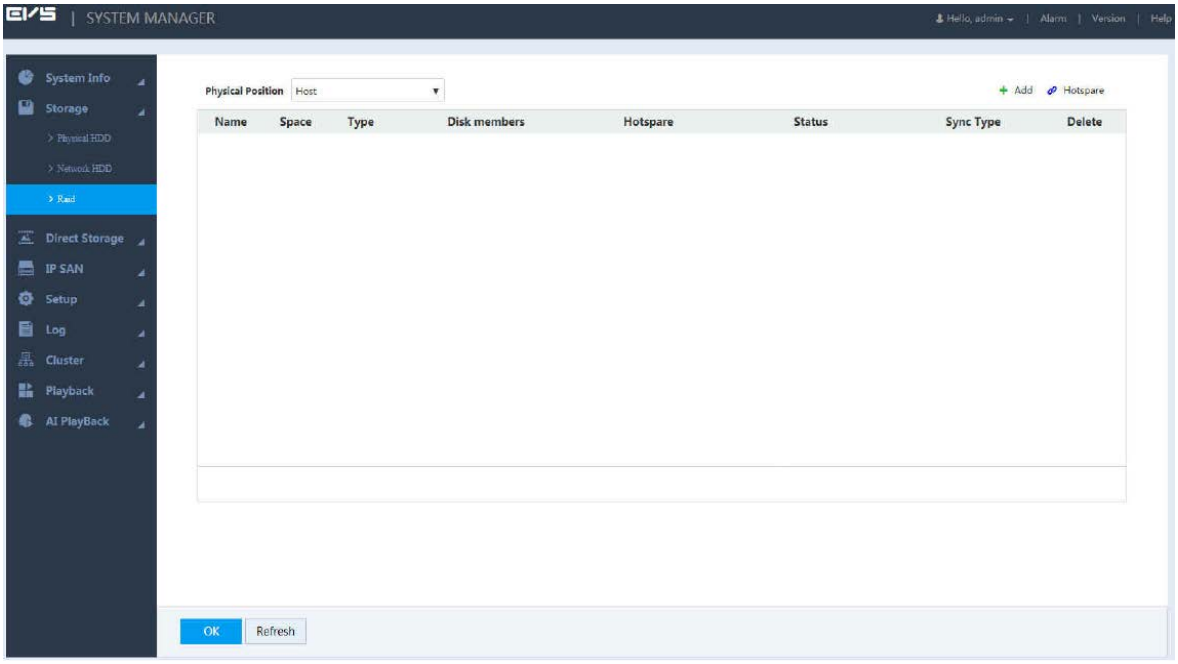
3.8.1 Creating RAID

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

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

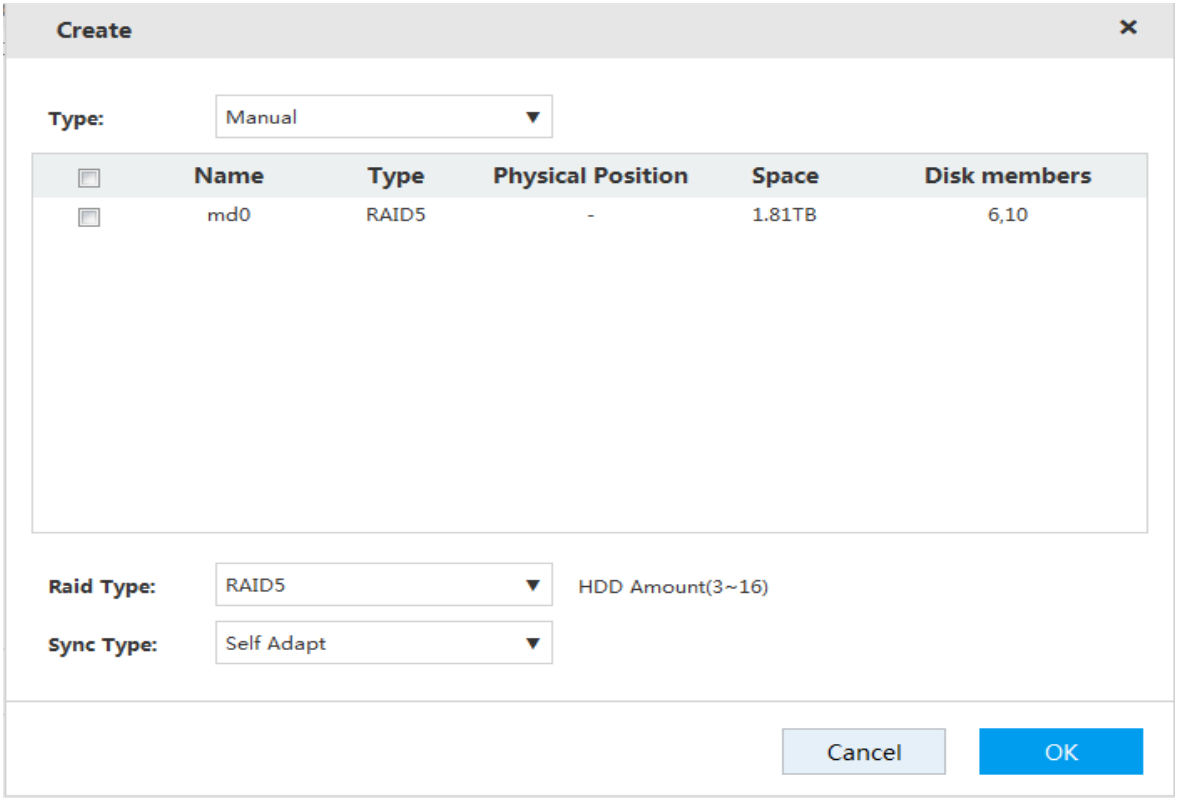
Step 1 Select **Storage > Raid**.

Figure 3-38 Raid management



Step 2 Click + .

Figure 3-39 Creating RAID



Step 3 Select the parameters. For details, see Table 3-11.

Table 3-11 RAID creation parameters

Parameter	Description
Type	Select the RAID creation type, including manual, shortcut and Raid2.0. ● When you choose shortcut RAID creation, the system automatically creates RAID 5. ● Raid2.0 provides different storage strategies for the same RAID based on your data security requirements. For example, for data of the file system, it offers data security as high as RAID1; for data of ordinary files, it ensures the same security and space utilization of RAID5.
HDD	Select the HDD you want to use to create RAID. Different RAID types need different numbers of disks, depends on the actual situation.
RAID Type	Select the RAID type you want to create.
Check Disk	If you select RAIDJ as the Raid type, you need to set the check disk. The number of check disk is limited to 1–8. RAIDJ cannot be created if there is no check disk, the number of check disks is more than 8, or the number of data disk is less than 2 or more than 8.
Raid Strategy	Select Raid strategy. ● If Raid5 is selected as the Raid type, the system supports 2D+1P, 4D+1P and 8D+1P. ● If Raid6 is selected as the Raid type, the system supports 2D+2P, 4D+2P, and 8D+2P. Only when selecting **Raid2.0** as the **Type** will the system support this function.
Hot Spare Strategy	Select hot spare strategy. Three types of strategies are supported: low, middle and high. Only when selecting Raid2.0 as the Type will the system support this function.
Sync Type	Select the sync mode of the business resources allocation. ● Self Adapt: Automatically adjust the RAID sync speed according to the current business loads. When there is no external business, sync is performed at a high speed. When there is external business, sync is performed at a low speed. ● Sync First: Resource priority is assigned to RAID sync. ● Business First: Resource priority is assigned to business operations. ● Balance: Resource is evenly distributed to RAID sync and business operations. Only when selecting **Manual** as the **Type** and **Raid 5** as the **Raid Type** will the system support this function.

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

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

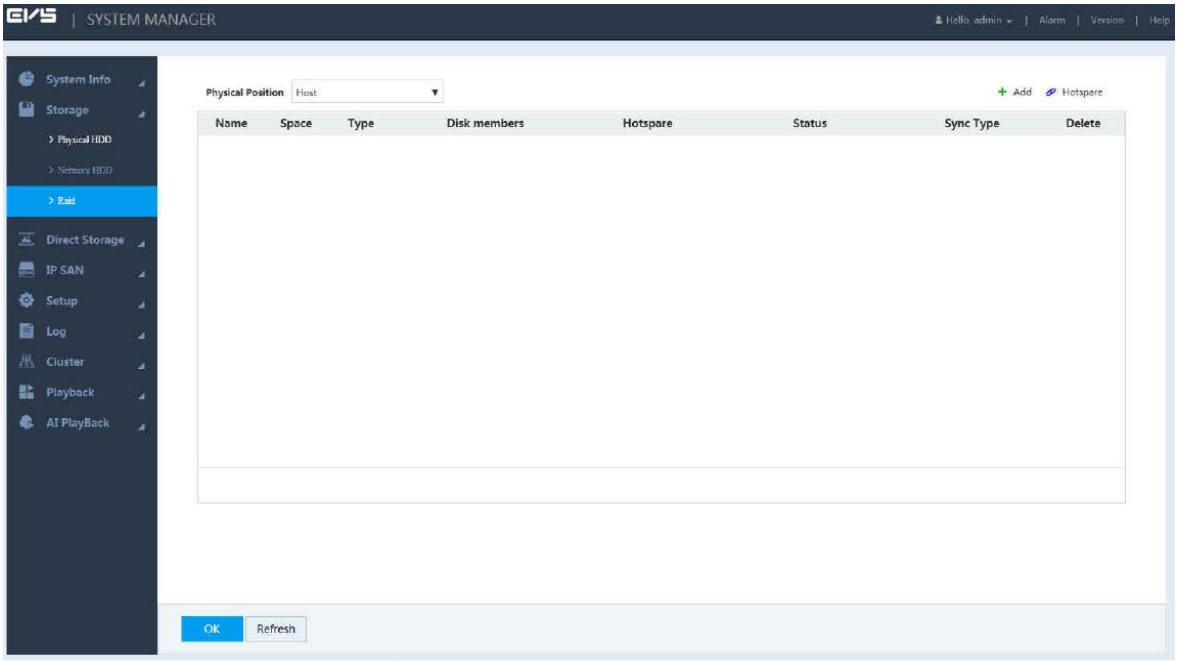
- Click to delete a RAID, and click **Refresh** to update the RAID list.
- Double-click the RAID line, and you can view the detailed information.

3.8.2 Hotspare Management

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

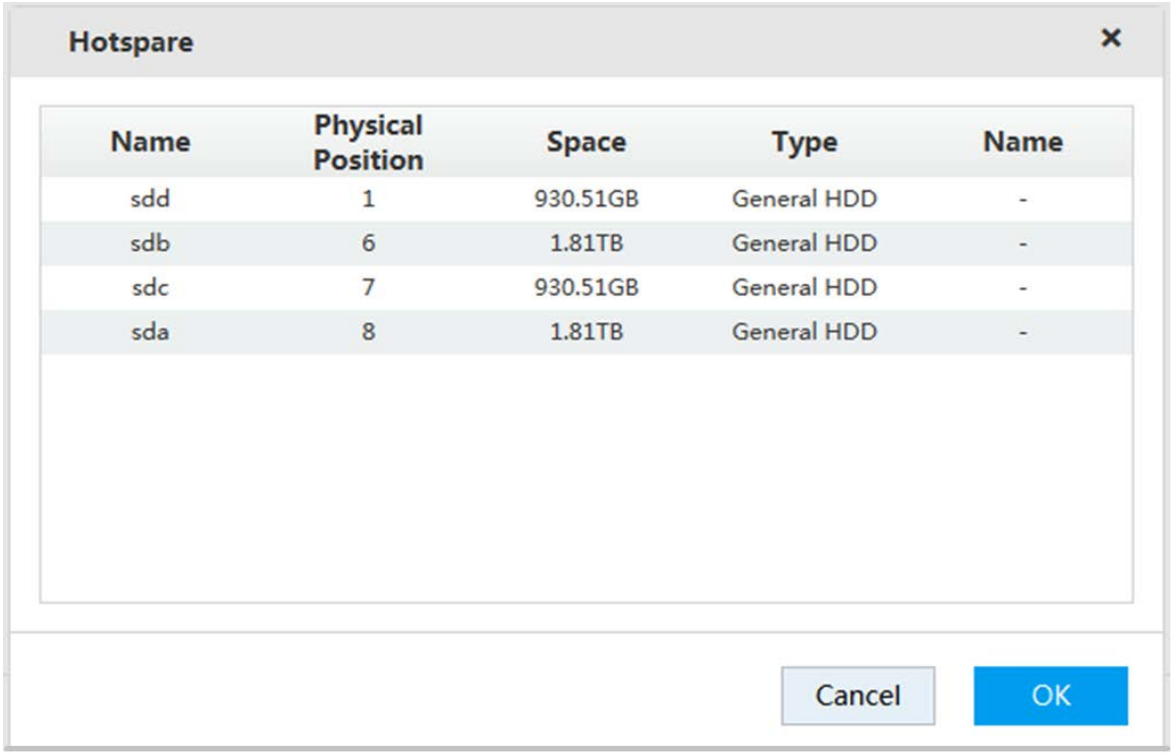
Step 1 Select **Storage > Raid**.

Figure 3-40 RAID management



Step 2 Click .

Figure 3-41 Hotspare management



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

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

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

Appendix 1 Particulate and Gaseous Contamination Specifications

Appendix 1.1 Particulate Contamination Specifications

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

Appendix Table 1-1 Particulate contamination specifications

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

Appendix Table 1-2 ISO 14644-1 cleanroom classification

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

Appendix 1.2 Gaseous Contamination Specifications

Usually indoor and outdoor atmospheric environments contain a small amount of common corrosive gas pollutants. When these mixed or single corrosive gas pollutants react with other environmental factors such as temperature or relative humidity in the long term, the device might suffer from a risk

of corrosion and failure. The following table defines the limitations of the gaseous contamination in the operating environment of the device.

Appendix Table 1-3 Gaseous contamination specifications

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

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

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

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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