Embedded Video Storage Server (EVS50, EVS70 Series)

Quick Start Guide

V2.1.1

Foreword

General

This Quick Start Guide (hereinafter referred to as "the Guide") introduces the functions and operations of the EVS series devices (hereinafter referred to as "the Device").

Models

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

Safety Instructions

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

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

Version	Revision Content	Release Time
V2.1.1	Update the manual according to the latest template.	May 2019
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

Privacy Protection Notice

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

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper 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 Guide. 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 Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the Guide are property of their respective owners.
- Go to our website, contact the supplier or customer service if there is any problem occurred when using the Device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Operation Requirement

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

Electrical Safety

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

Table of Contents

1 Overview

1.1 Introduction

The Device is designed for the management, storage and application of high-definition video data. It uses Linux operation system and professional customized hardware platform. It also 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. It can realize 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 solution for IP SAN/NAS. It provides centralized storage solution 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

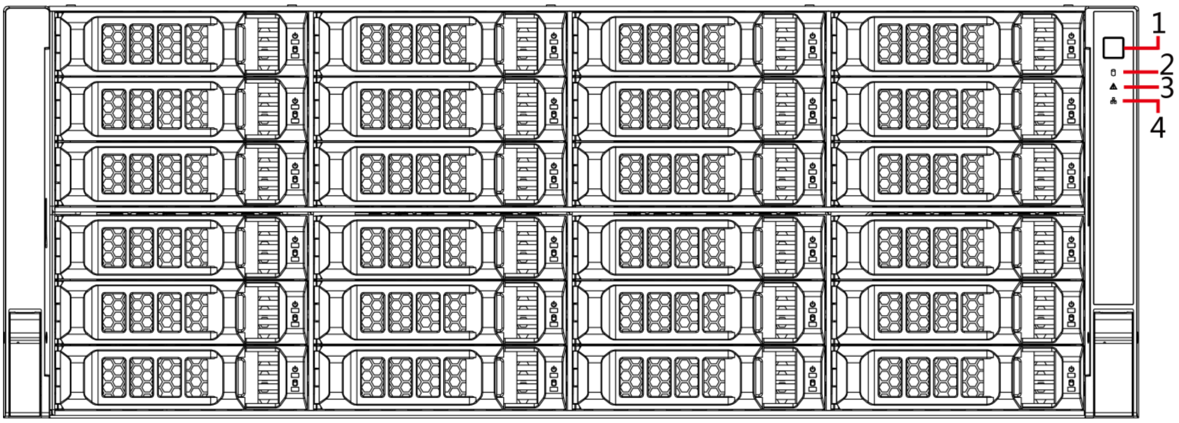


Table 1-1 Front panel interfaces

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

No.	Indicator/Button	Description
3	Alarm status indicator	● The light is out when the Device is running properly. ● The red light keeps on when the power, temperature or fan is abnormal.
4	Network status indicator	The blue light keeps on if there is a network failure, IP conflict or MAC conflict.

1.3 Rear Panel

Figure 1-2 Rear panel (5 Ethernet ports)

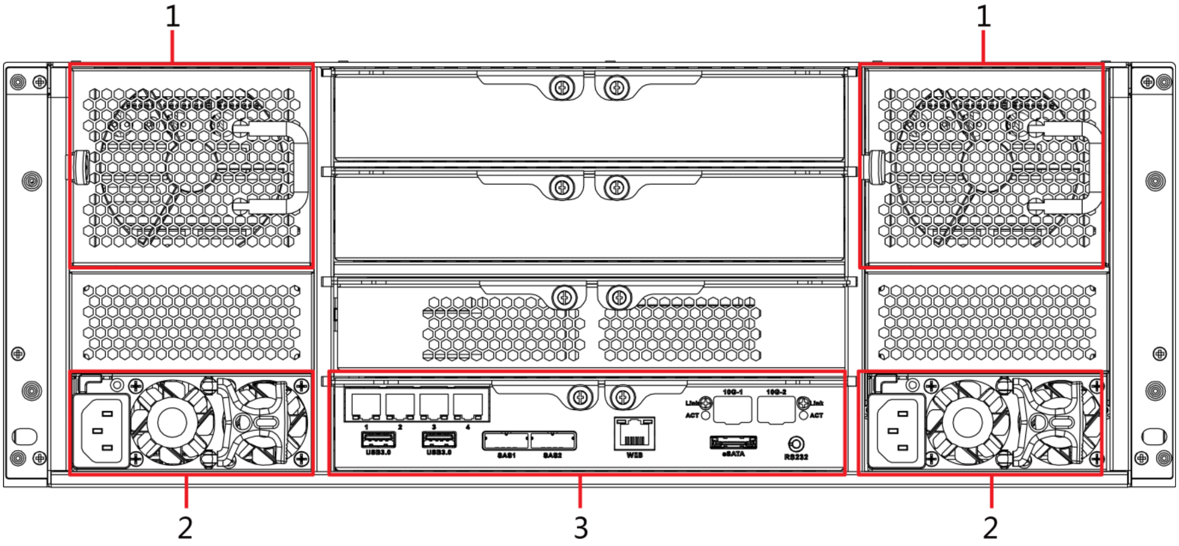


Figure 1-3 Rear panel (7 Ethernet ports)

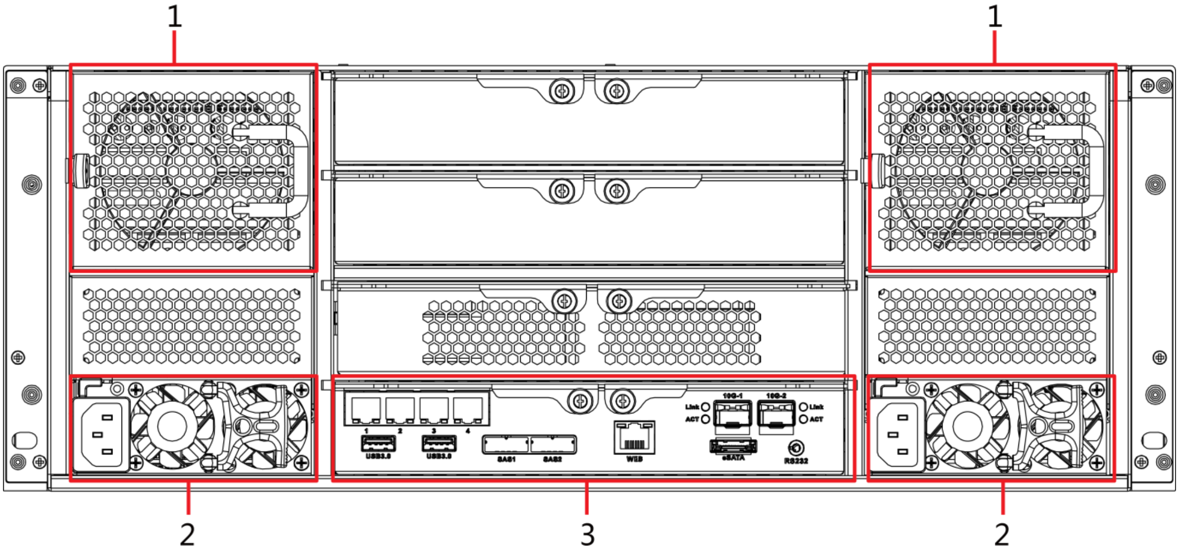


Figure 1-4 Rear panel (9 Ethernet ports)

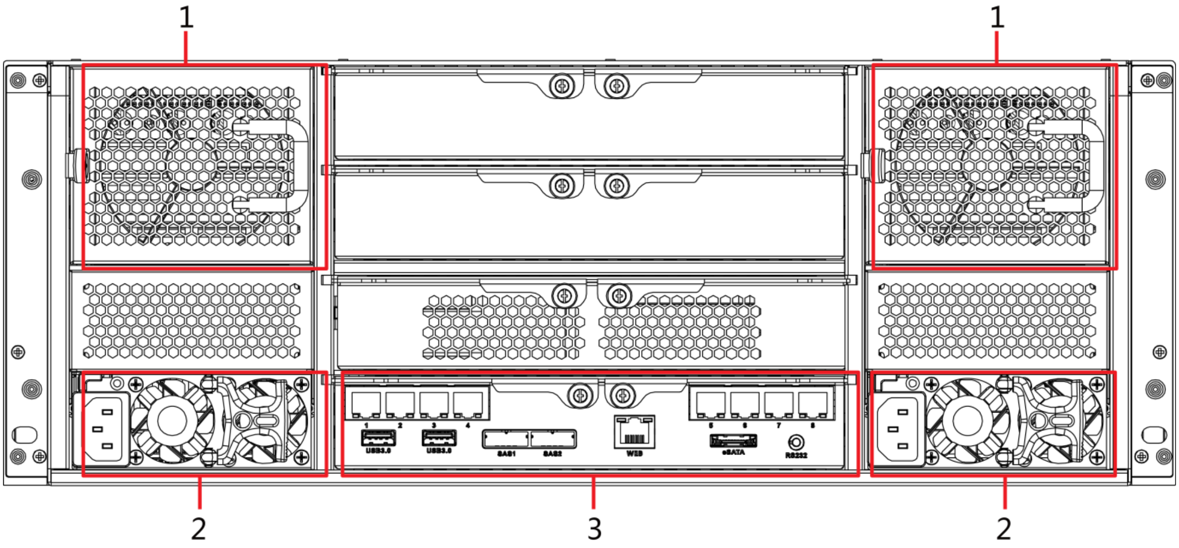


Table 1-2 Rear panel interfaces

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 indicators, see Table 1-3.

Table 1-3 Master control module interfaces

Port/Indicator	Description
1-4/5-8	Gigabit data port. Used for data transmission.
USB 3.0	Connect the mouse and USB storage devices.
eSATA	eSATA interface. For high-end series, it is a 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.
RS-232	RS-232 interface.
10G-1, 10G-2	10 gigabit port. Devices of different models have different numbers of Ethernet ports and 10 gigabit ports. See the actual device.
Link/ACT	Status light 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.

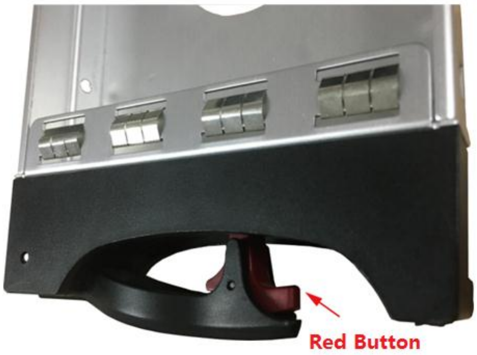
⚠ WARNING

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

2.1.1 Middle-class 16-HDD Single-controller Series

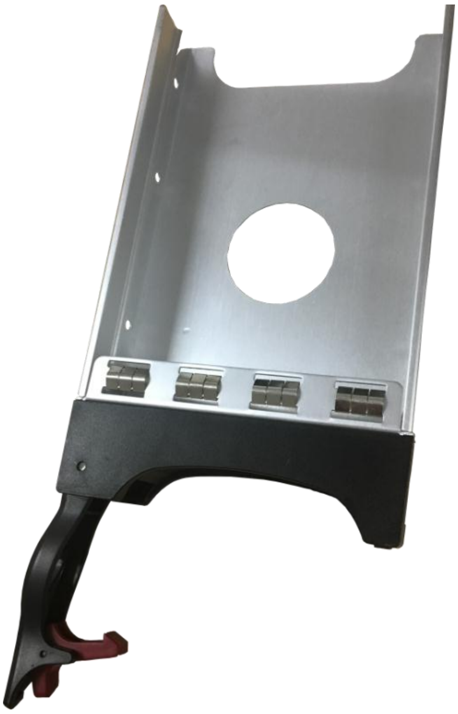
Step 1 Press the red button on the HDD box in the front panel to unlock the handle. See Figure 2-1.

Figure 2-1 Unlocking the handle



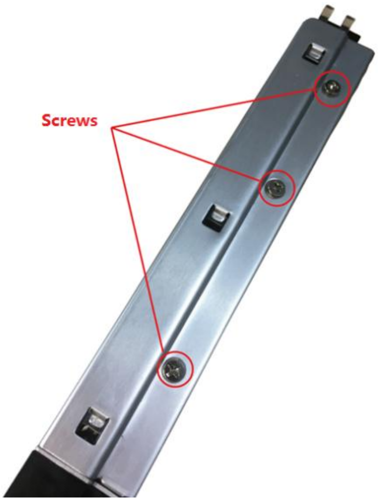
Step 2 Pull out to take the empty HDD box. See Figure 2-2.

Figure 2-2 HDD box



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

Figure 2-3 Fastening the screws



📖

To avoid any damage to the slot, do not lock 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 close the handle.

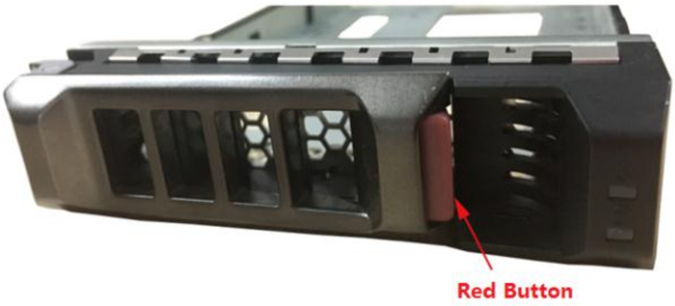
2.1.2 Other Series

⚠

The contents below apply to devices other than the middle-class 16-HDD single-controller series.

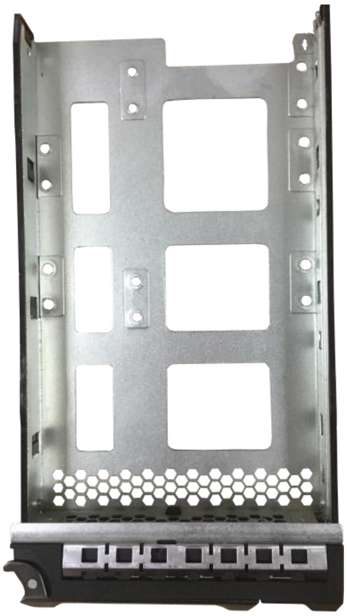
Step 1 Press the red button on the HDD box in the front panel, and unlock open the handle. See Figure 2-4.

Figure 2-4 Opening the handle



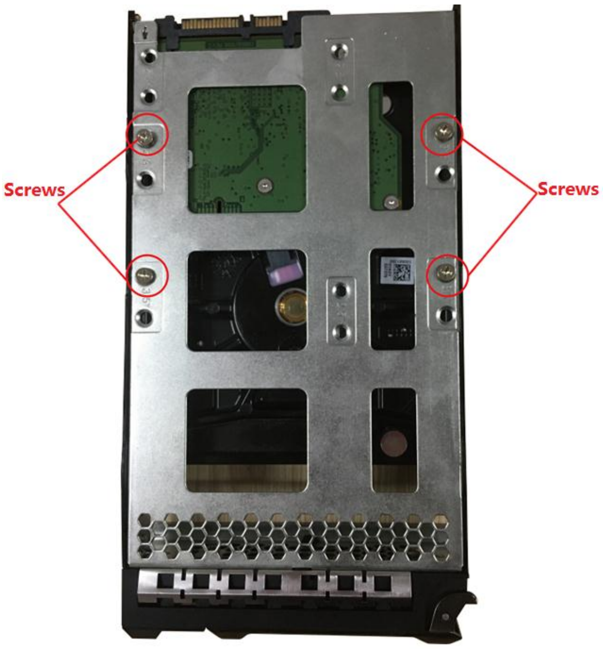
Step 2 Pull out to take the empty HDD box. See Figure 2-5.

Figure 2-5 HDD box



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

Figure 2-6 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 close 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:

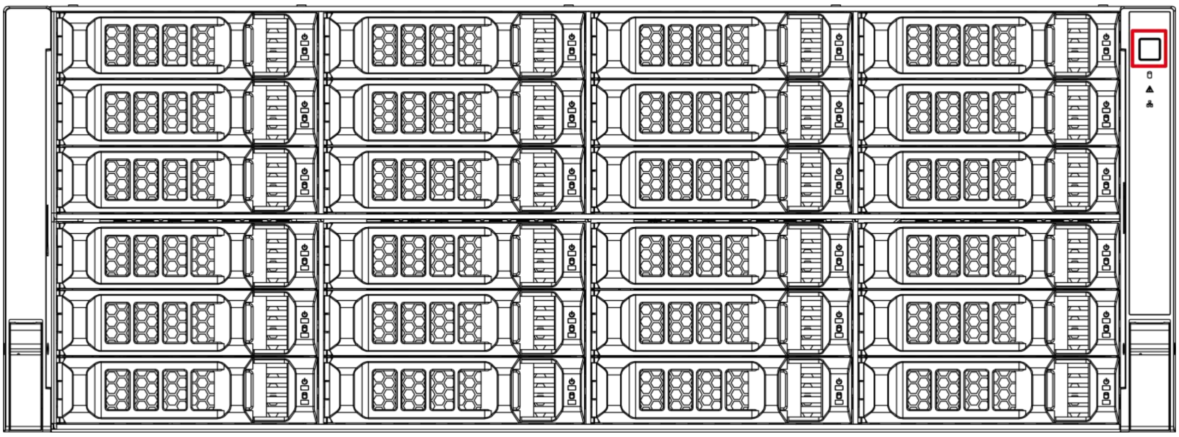
- Make sure that GND is connected correctly.
- Different models of devices need different sources of power supplies. Make sure that all power lines are connected correctly.
- Check whether the supplied power voltage complies with device requirements.
- Check whether the network cables and SAS cables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

2.2.2 Powering Up the Device

This section takes middle-class 24-HDD single-controller series as an example, and the actual product shall prevail.

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

Figure 2-7 Front panel



See Table 1-1 to check whether the indicators are normally displayed.

- When 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 the Device again.

3 Web Basic Operations

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

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

The following contents are only for your reference. See the actual models for the functions you need.

3.1 Connecting the Network

Before logging in web on PC, connect your PC and the Device to the same network and make sure the network 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 NIC. You need to confirm the default IP according to the actual device condition.

Step 3 On PC, execute the command of **ping** *192.168.1.108 (192.168.1.108* is the IP address of the Device) 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 (the default user name is admin).

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

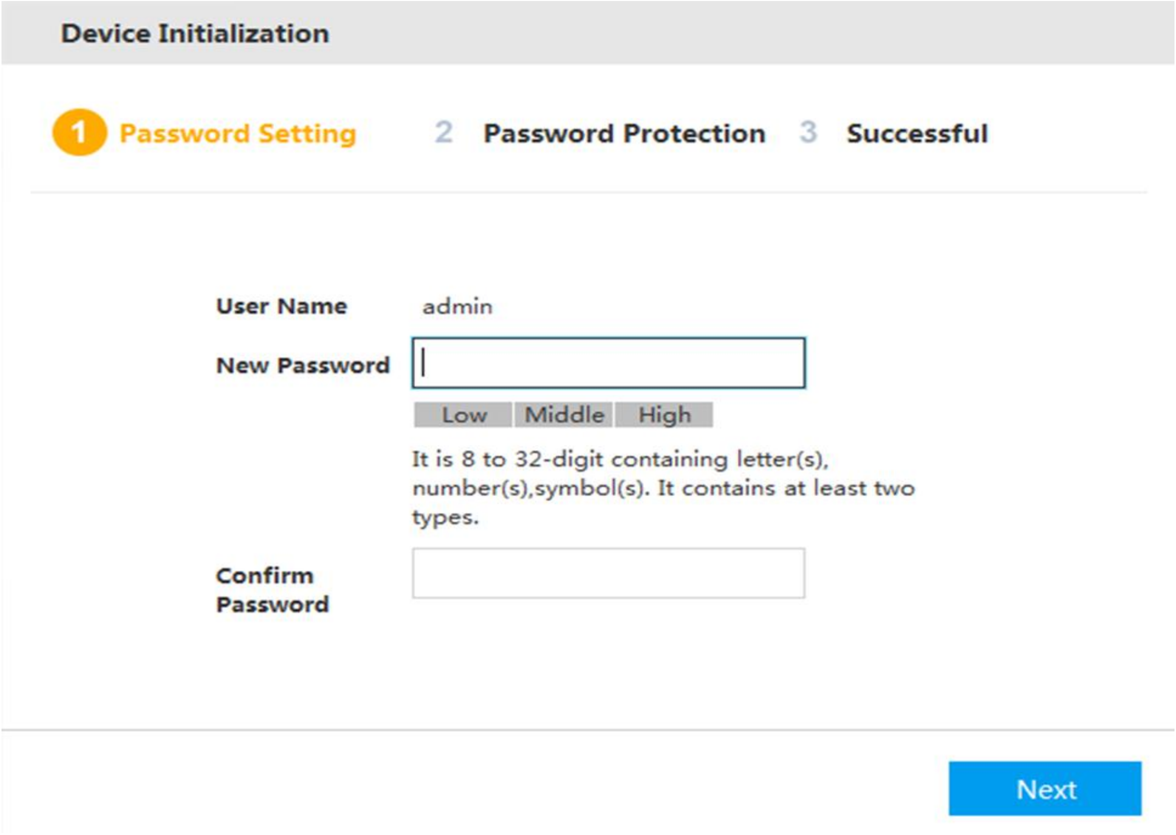
- Single-control device: Default IP is 192.168.1.108.

- Dual-control device: Default IP is 192.168.0.108.

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

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

Confirm Password

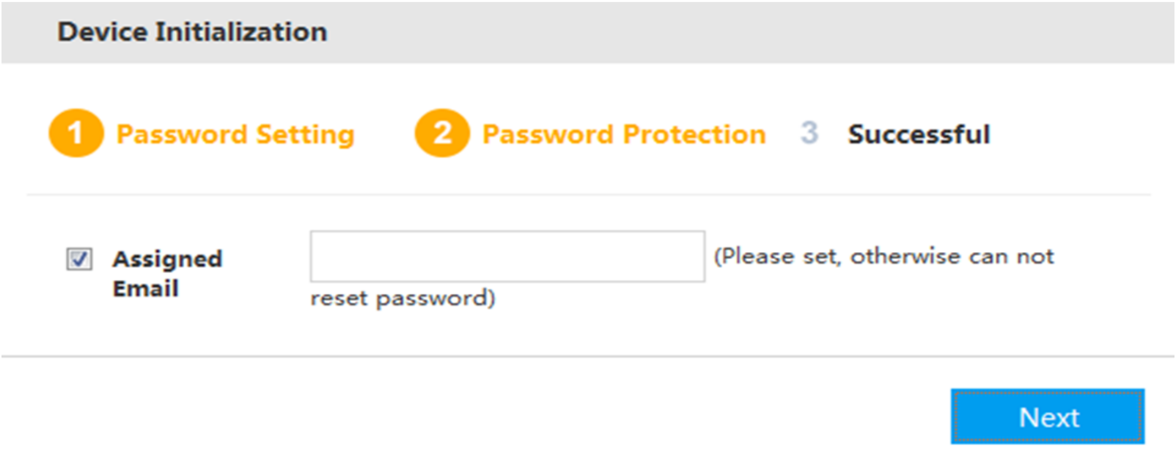
Step 3 In the **New Password** box, enter the new password.

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

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 In the Assigned Email box, enter the **Assigned Email**.

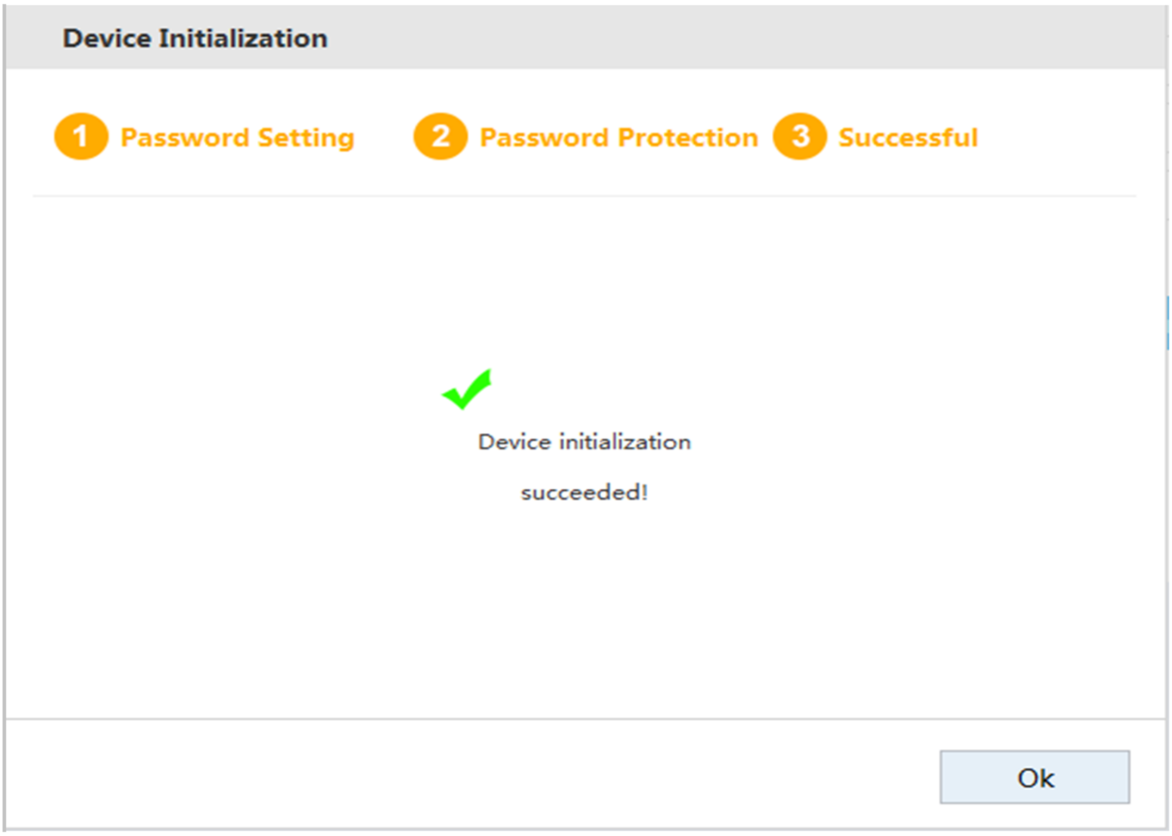
After entering the assigned email, you can reset the admin password through the email. For details, see *User's Manual*.

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

Step 6 Click **Next**.

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

Figure 3-3 Device initialization succeeded



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.

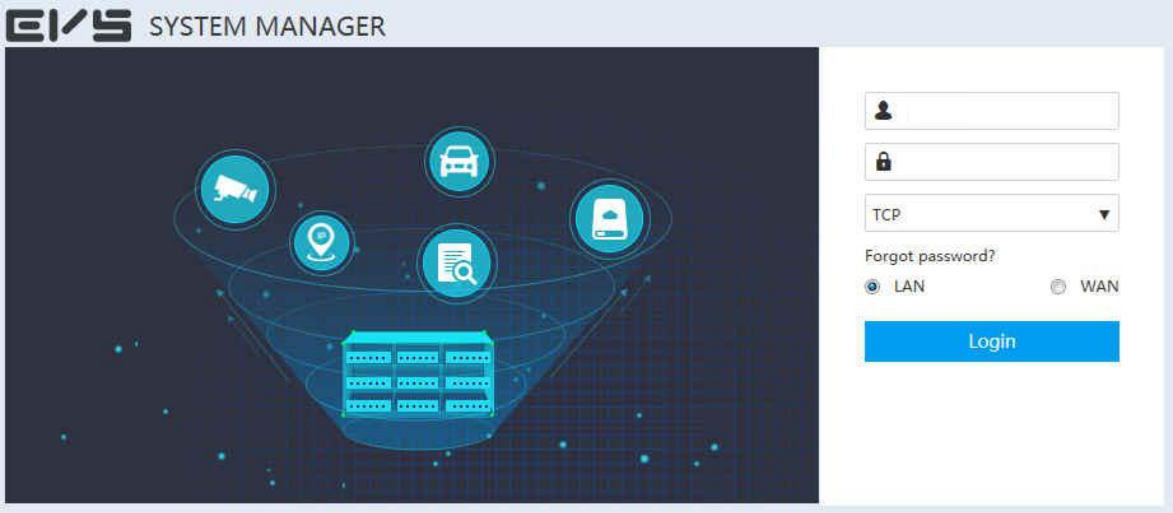
Step 1 Open the browser, enter the IP address in the address bar, and then press Enter.

Step 2 Install the control.

When you log in the Device for the first time on PC, the control installation interface is displayed. After the installation is successful, the web login interface is displayed. See Figure 3-4.

If the system does not allow to download the plug-ins, check whether any other plug-ins are installed. These plug-ins might prohibit the download and reduce the security level of IE.

Figure 3-4 Web login interface



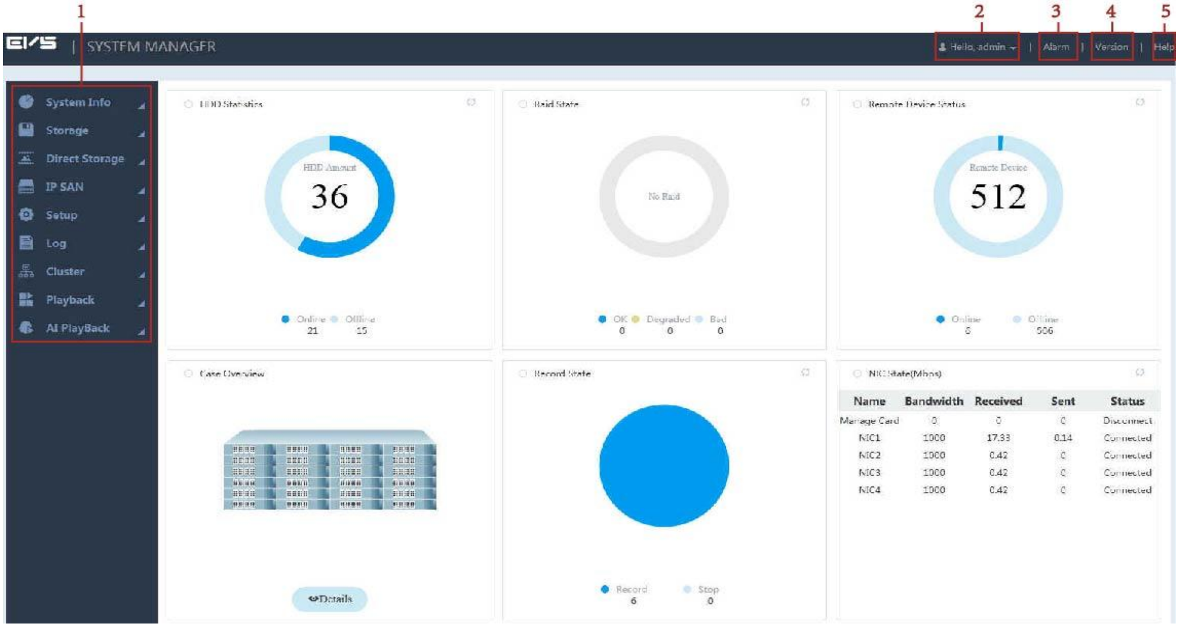
Step 3 Enter the user name and password, and then select the network connection type.

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

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
Manage Card	0	0	0	Disconnect
NIC1	1000	17.33	0.14	Connected
NIC2	1000	0.42	0	Connected
NIC3	1000	0.42	0	Connected
NIC4	1000	0.42	0	Connected

Table 3-1 System manager description

No.	Name	Description
1	Function bar	You can view the basic system information, configure system parameters and play monitoring images and videos.

No.	Name	Description
2	User name	Display the current login user name. Click ▾ at the right side of the user name and you can perform quickly set and logout. ● Quickly set: You can configure video, AI playback and IP SAN according to different applications. ● Logout: Log out the current user.
3	Alarm	Click **Alarm** and you can search the alarm logs of the Device. For details, see *User's Manual*.
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 of the Device.

3.4 Initial Configuration

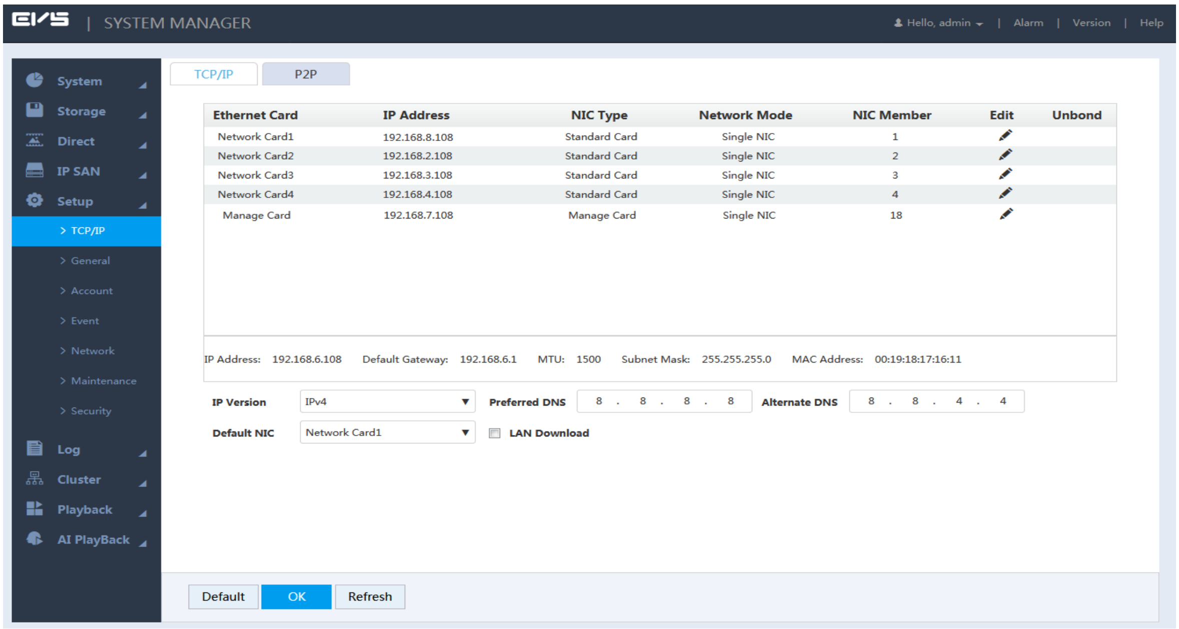
3.4.1 Setting IP

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

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

The **TCP/IP** interface is displayed. See Figure 3-6 and Figure 3-7. For details, see Table 3-2.

Figure 3-6 Setting TCP/IP (single-control device)



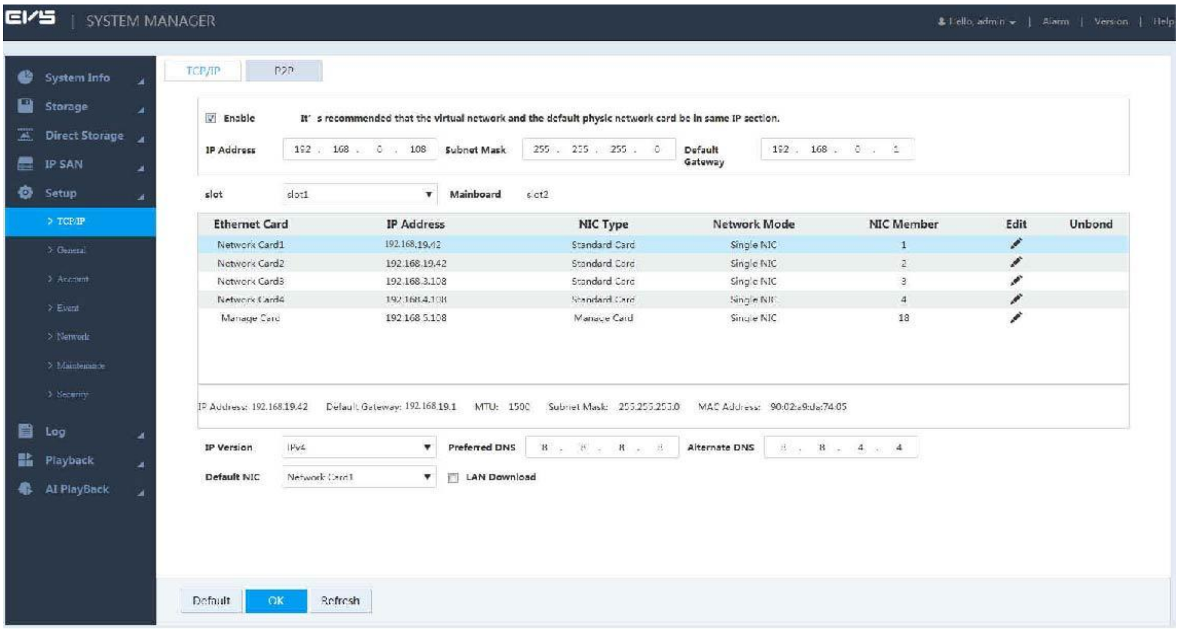
Ethernet Card	IP Address	NIC Type	Network Mode	NIC Member	Edit	Unbond
Network Card1	192.168.8.108	Standard Card	Single NIC	1	✎	
Network Card2	192.168.2.108	Standard Card	Single NIC	2	✎	
Network Card3	192.168.3.108	Standard Card	Single NIC	3	✎	
Network Card4	192.168.4.108	Standard Card	Single NIC	4	✎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

IP Address: 192.168.6.108 Default Gateway: 192.168.6.1 MTU: 1500 Subnet Mask: 255.255.255.0 MAC Address: 00:19:18:17:16:11

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

Default NIC: Network Card1 □ LAN Download

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



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

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

slot: slot1 Mainboard: slot2

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

IP Address: 192.168.19.42 Default Gateway: 192.168.19.1 MTU: 1500 Subnet Mask: 255.255.253.0 MAC Address: 90:02:a9:da:74:05

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

Default NIC: Network Card1 □ LAN Download

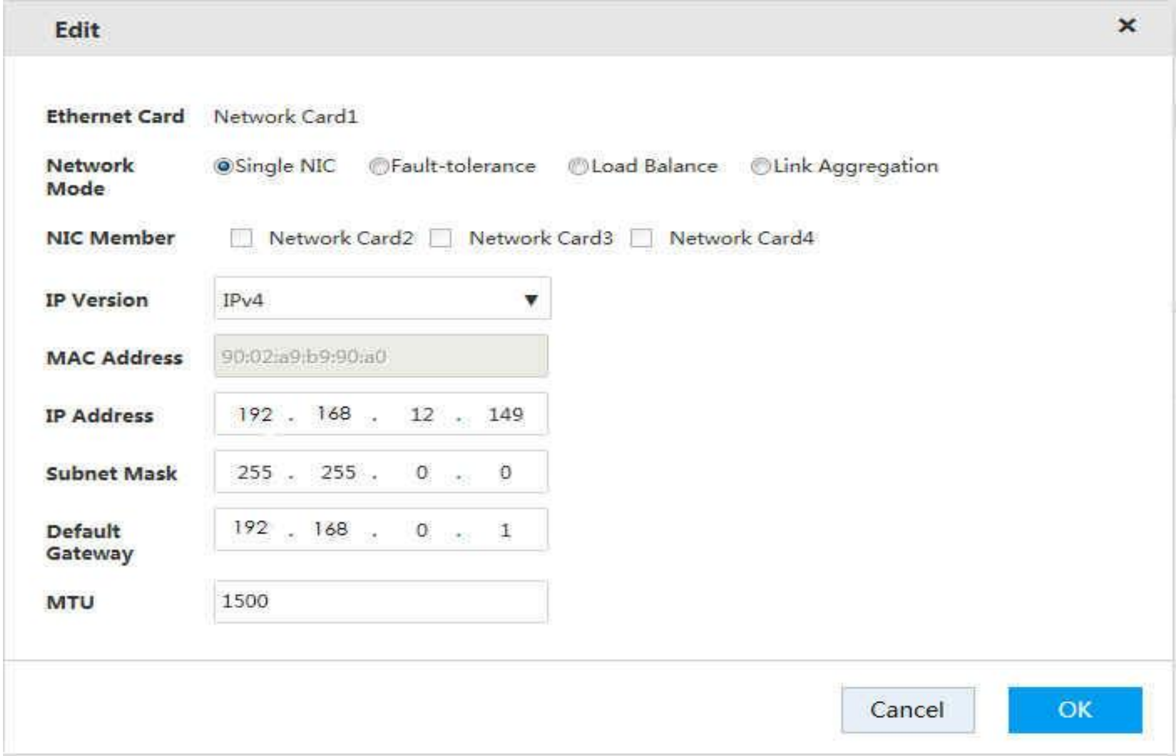
Table 3-2 TCP/IP setting parameters

Parameter	Description
Enable	Enter the virtual IP address of the dual-control device. For details, see *User's Manual*. 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 switch 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 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 3-8.

Figure 3-8 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:b9:90:a0

IP Address: 192 . 168 . 12 . 149

Subnet Mask: 255 . 255 . 0 . 0

Default Gateway: 192 . 168 . 0 . 1

MTU: 1500

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

Table 3-3 NIC editing parameters

Parameter	Description
Ethernet Card	Displays the current NIC name.

Parameter	Description
Network Mode	Displays the network mode of the Device. ● Single NIC: The NIC can be 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 FTP. Once the card is offline, the system triggers a disconnection alarm. ● 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. ● The 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	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	Display the MAC address of the Device.
IP Address	Set the IP address, subnet mask and default gateway of the Device according to the actual network planning.
Subnet Mask	
Default Gateway	

Parameter	Description
MTU	Enter the MTU (Maximum Transmission Unit) value of the NIC. The default value is 1,500 bytes. The suggested value is 1,500 or 1,492. ● 1,500: The maximum and default value of the Ethernet packet. It is 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. ● Modifying the MTU will lead to NIC restart and network interruption to affect the running business. 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, so as to 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, so as to realize the distributed advantage of the network. You can browse, replay, manage, and store several remote devices.

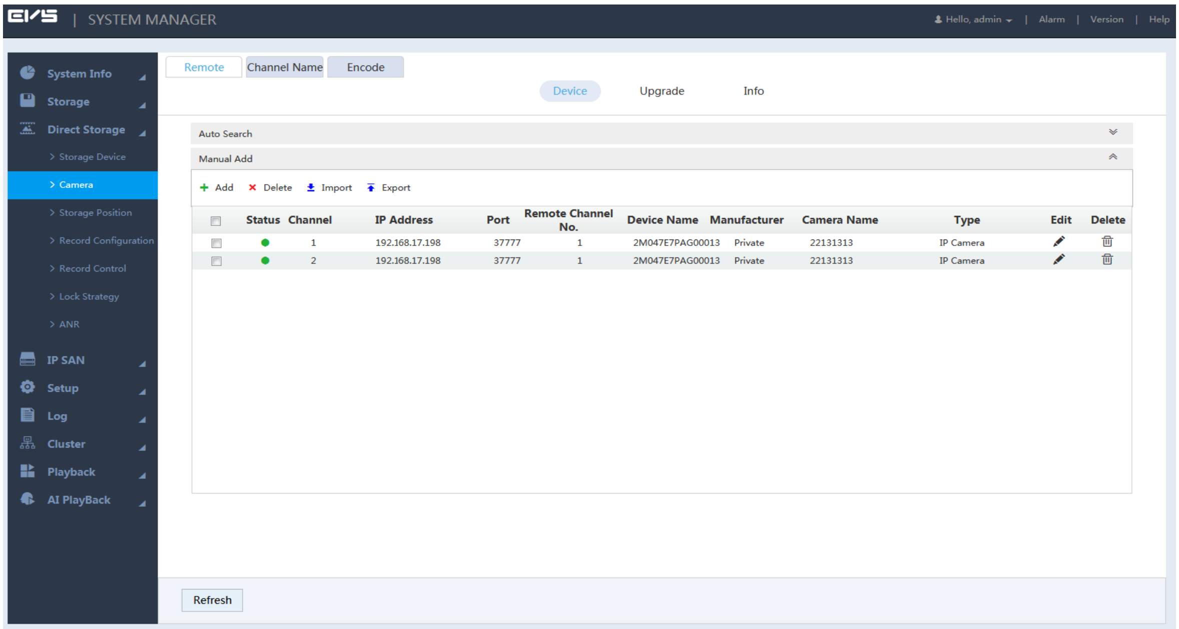
The system supports adding remote devices in three ways: Adding by search, adding one device add, and batch add.

- 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, 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 Storage > Camera > Remote > Device**.

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

Figure 3-9 Remote device



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

Step 2 Add remote device.

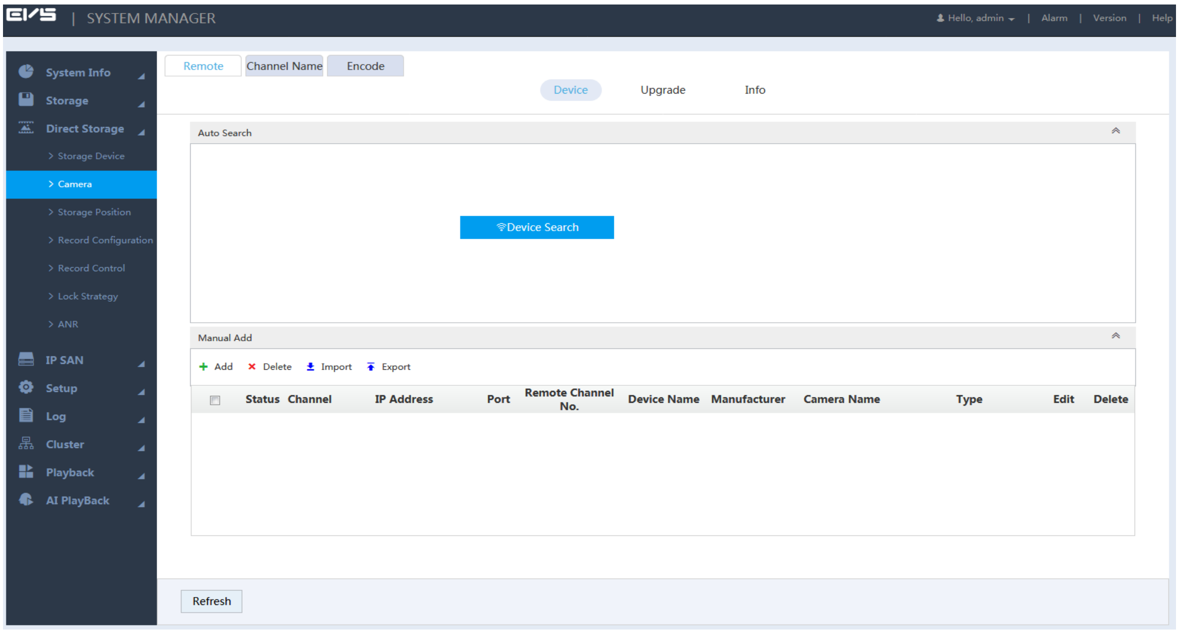
You can use adding by search, adding one device, batch add or importing from template.

- Adding by search

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

The **Auto Search** interface is displayed. See Figure 3-10.

Figure 3-10 Automatic search

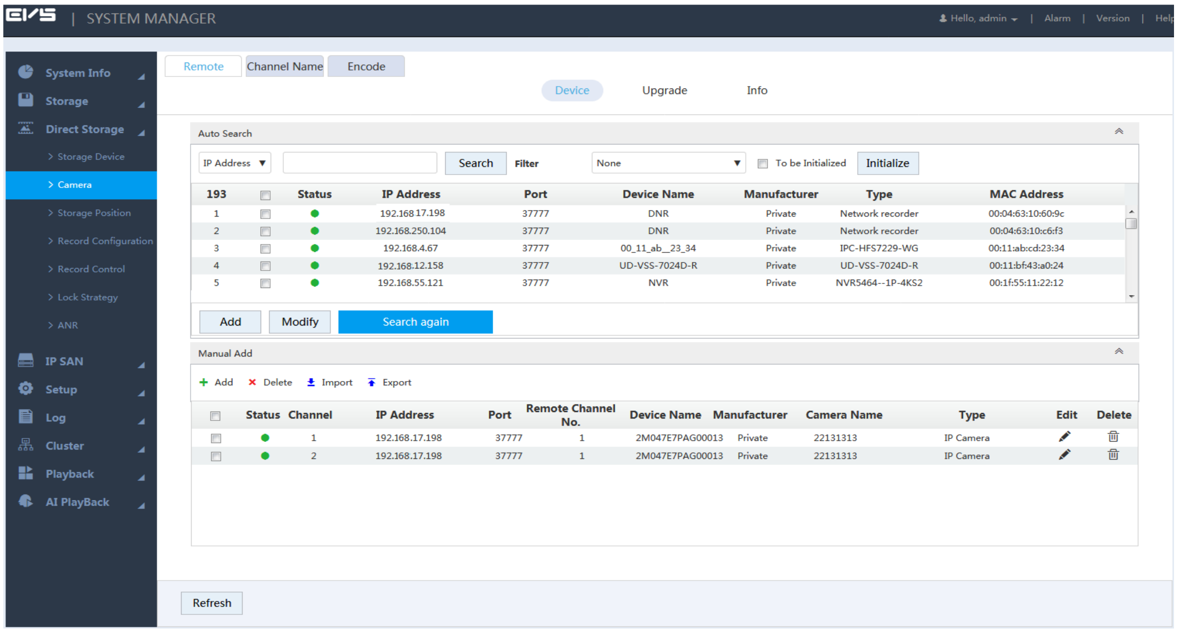


2) Click **Device Search**.

The results are displayed. See Figure 3-11. For details, see Table 3-4.

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

Figure 3-11 Search results



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

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

Table 3-4 Auto search icons

Icon/Parameter	Description
IP Address ▼	Select the remote devices you need to add through IP address or MAC address. 1. Click IP Address ▼ to select IP Address or MAC Address. 2. Enter the IP address or MAC address of the remote device in the text box at the right side of IP Address ▼. 3. Click **Search**. 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 *User's Manual*.
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. ● The IP address of the remote device can be modified only when the **Manufacturer** is **Private**. ● You can only modify one IP address at a time.
Search again	Click this icon to search the remote devices again.

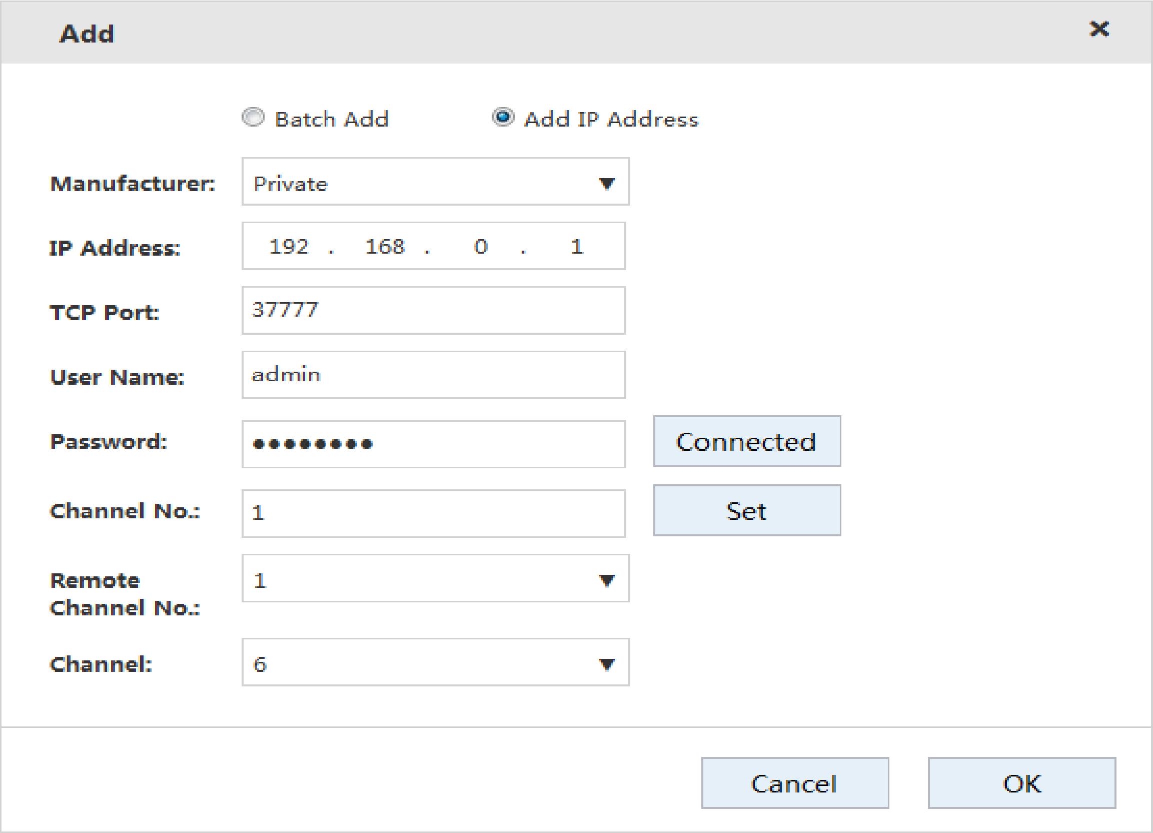
3) Double-click the remote device, or select the check box in front of the device and click **Add**, the system adds this remote device to the added list.

- Adding one device

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

The **Add** interface is displayed. See Figure 3-12.

Figure 3-12 Adding one device



Add

○ Batch Add ● Add IP Address

Manufacturer: Private

IP Address: 192 . 168 . 0 . 1

TCP Port: 37777

User Name: admin

Password: •••••••••

Channel No.: 1

Remote Channel No.: 1

Channel: 6

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

Table 3-5 Description of adding device

Parameter	Description
Manufacturer	Select the manufacturer in the drop-down list 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 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 via 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 remote device to be connected through Onvif.
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. These modes include: 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.

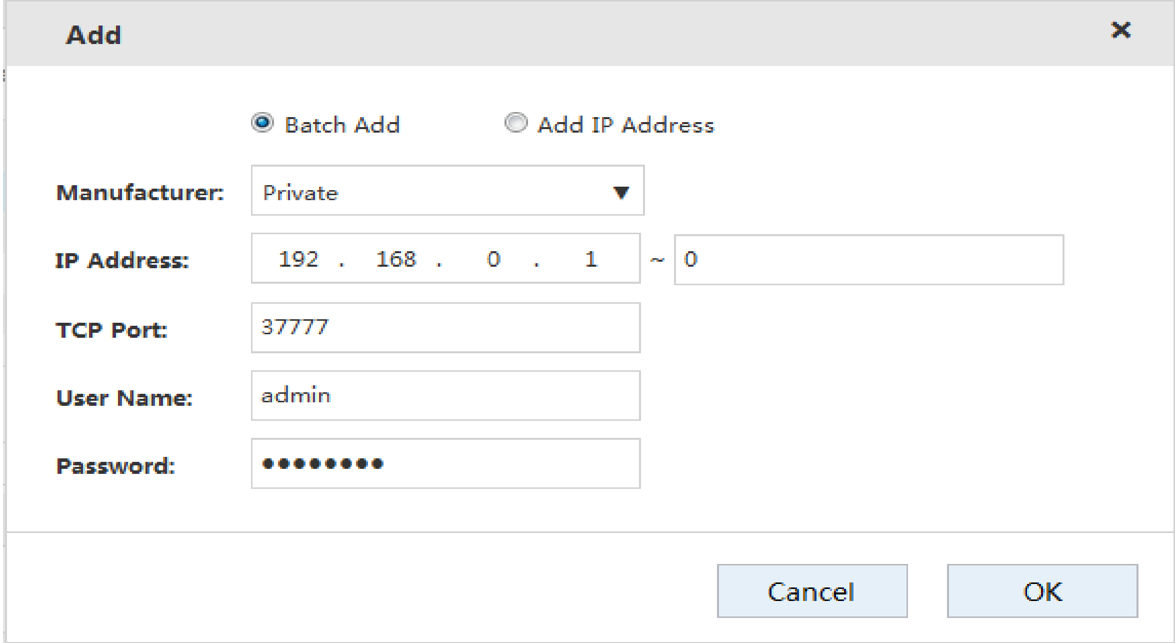
- Batch add

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

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

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

Figure 3-13 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.

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 3-5.
4) Click **OK** to complete the 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.* "*.cs*" 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, it will fail to import the file.

3) Click ⬇ to select template file.

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

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

3.4.3 Configuring Record Plan

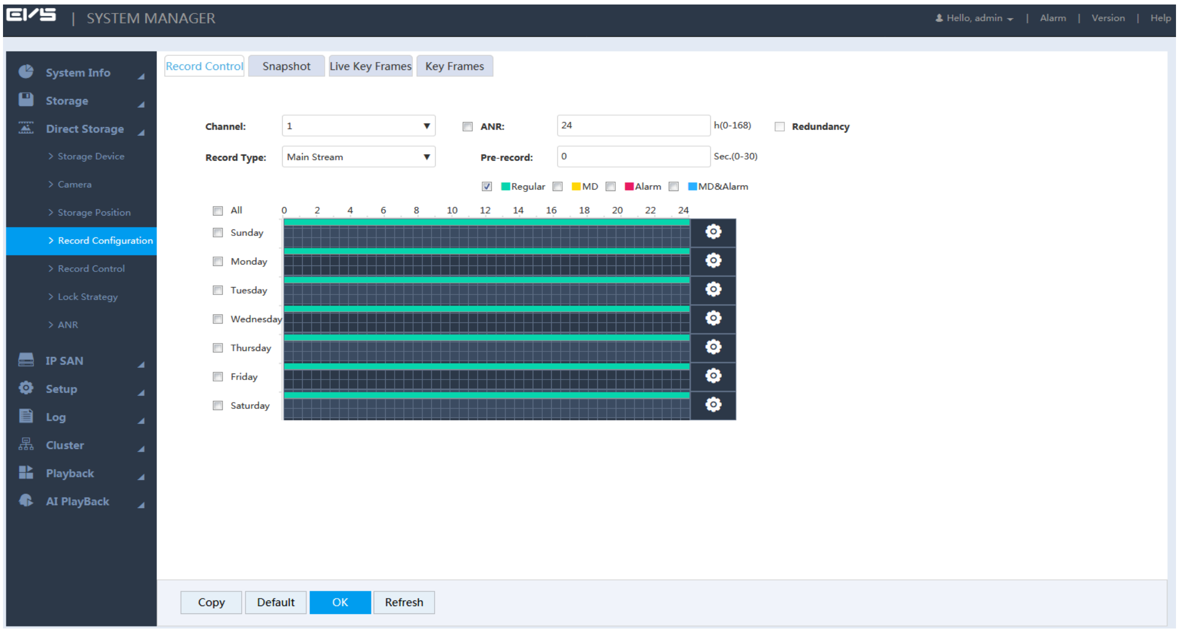
The system performs the corresponding video recording according to the set record plan. For example, when you set the time period of alarm videos to 6:00–18:00, the system automatically takes records if any alarm occurs during this period.

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 Storage > Record Configuration > Record Control**.

The **Record Control** interface is displayed. See Figure 3-14.

Figure 3-14 Record plan



Channel: 1

Record Type: Main Stream

□ ANR: 24 h(0-168)

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

□ Redundancy

☑ 🟩Regular □ 🟨MD □ 🟥Alarm □ 🟦MD&Alarm

□ All

□ Sunday

□ Monday

□ Tuesday

□ Wednesday

□ Thursday

□ Friday

□ Saturday

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

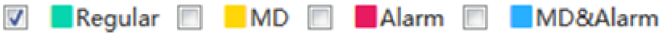
Table 3-6 Record parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.

Parameter	Description
ANR	Select the check box to enable the function. ● When the network connection between the Device and IPC is broken, 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 is available for IPC that has installed the SD card.
Redundancy	When multiple disks are available in the 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. Set a redundant disk. For detailed operations, see *User's Manual*. 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. The recording in the redundant disk corresponds to a backup of recording in the read-write disk. Images are not backed up.
Record Type	Select the record type, including main stream and sub stream.
Pre-record	Start to record 0–30 seconds (according to the stream size and status) before the preset action.

Step 3 Select the alarm type. See Figure 3-15.

Figure 3-15 Alarm type

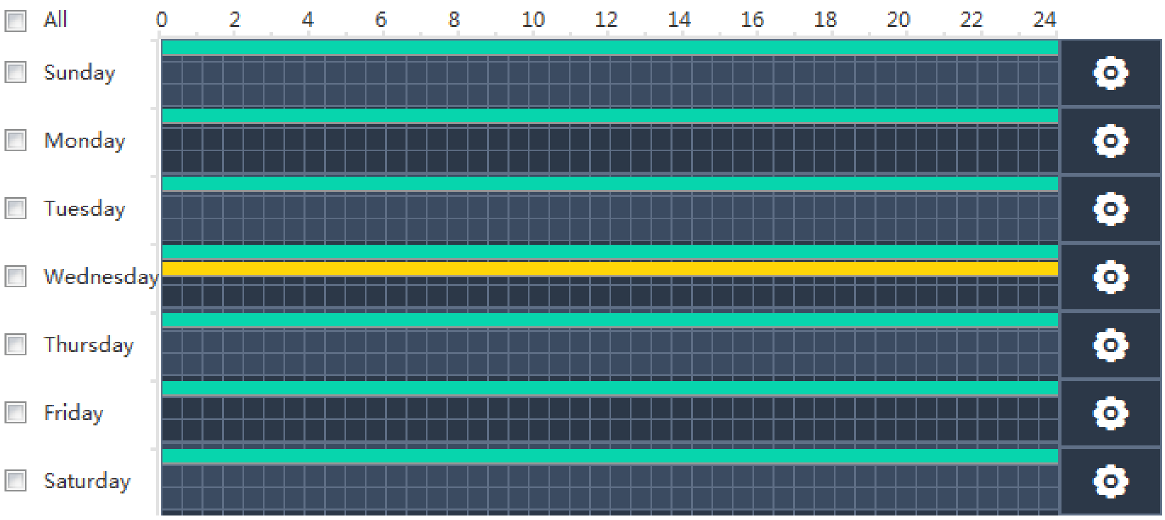


- When you select the **MD**, **Alarm** or **MD & Alarm**, you need to enable the alarm record linkage for the corresponding channel. For details, see *User's Manual*.
- The color bar in Figure 3-16 indicates the record type of the corresponding time period.

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

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

Figure 3-16 Time period setting



- Drawing:

1) Select the weekday.

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

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

2) Hold 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. The Device performs recording in the corresponding period.

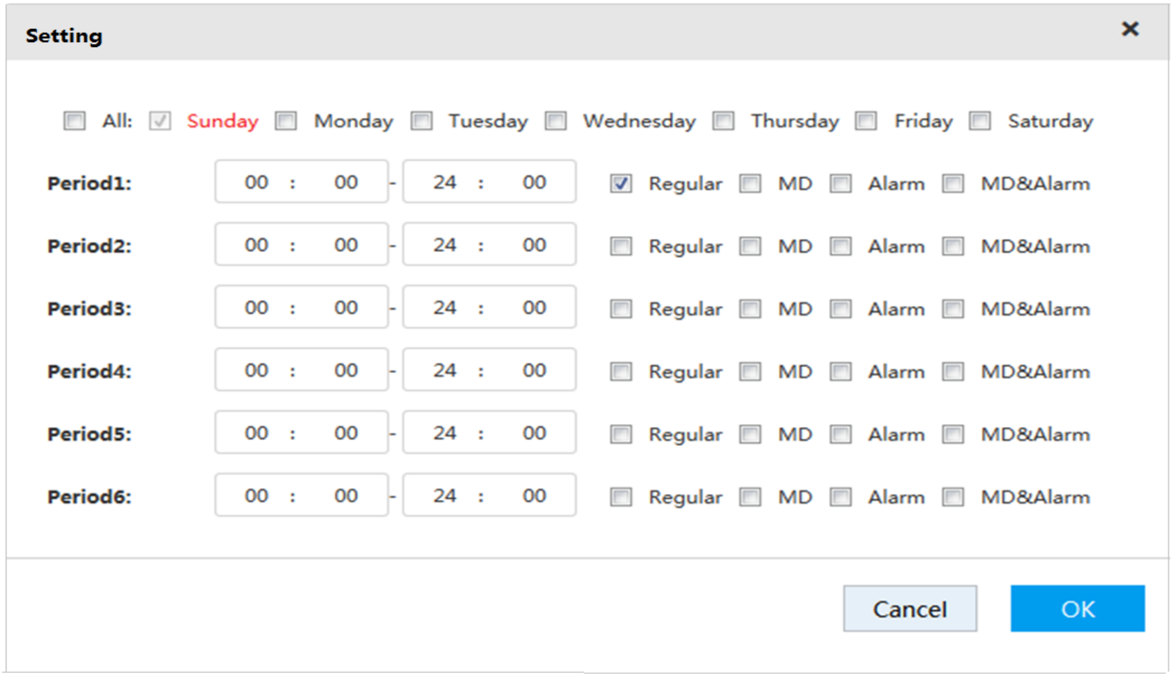
   ◇ When the record time is overlapped, refer to this record priority: MD & alarm > alarm > MD > regular.

- Editing:

1) Select the corresponding weekday and click ⚙.

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

Figure 3-17 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.

The record plan comes into effect after enabling the auto record function. For details of enabling auto record, see "3.4.4 Enabling Record Function."

3.4.4 Enabling Record Function

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 stream.

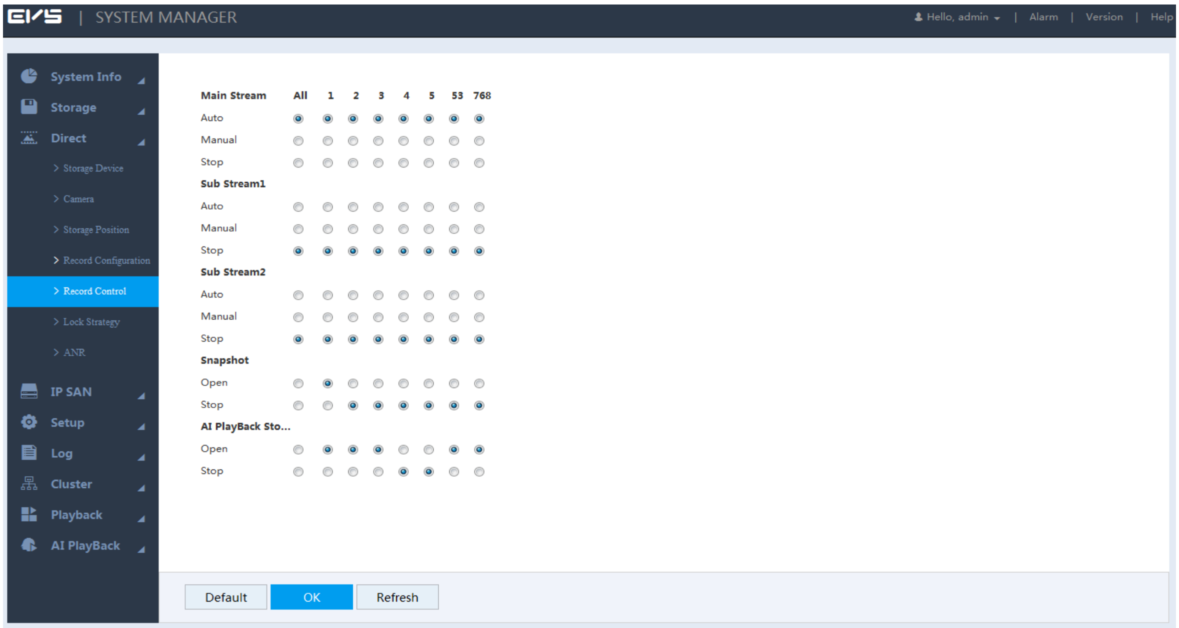
- Auto record: The system automatically takes records according to the set record type and record time.
- Manual record: The system takes 24-hour continuous records in the channel.

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

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

The **Record Control** interface is displayed. See Figure 3-18.

Figure 3-18 Record control



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

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

Table 3-7 Record control parameters

Parameter	Description

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 "3.4.3 Configuring Record Plan." ● Stop: All the channels stop recording.
Sub Stream	
Snapshot	Select a single channel or multiple channels, and open/close the snapshot of the corresponding channel.
AI Playback Storage	Select a single channel or multiple channels, and open/close AI playback in the corresponding channel.

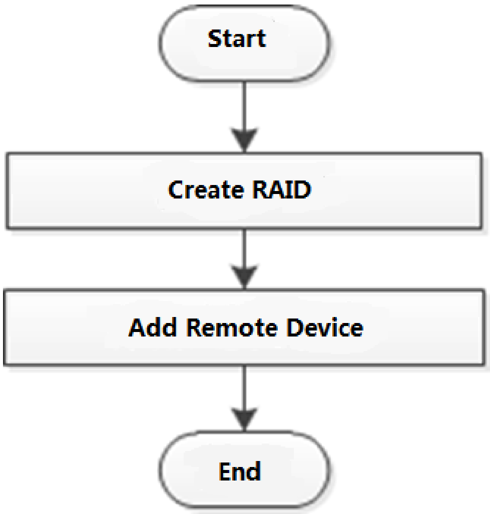
Step 3 Click **OK** to save the configuration.

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 which reduces the operating pressure of the management server.

For the procedure to configure video direct storage, see Figure 3-19.

Figure 3-19 Video direct storage

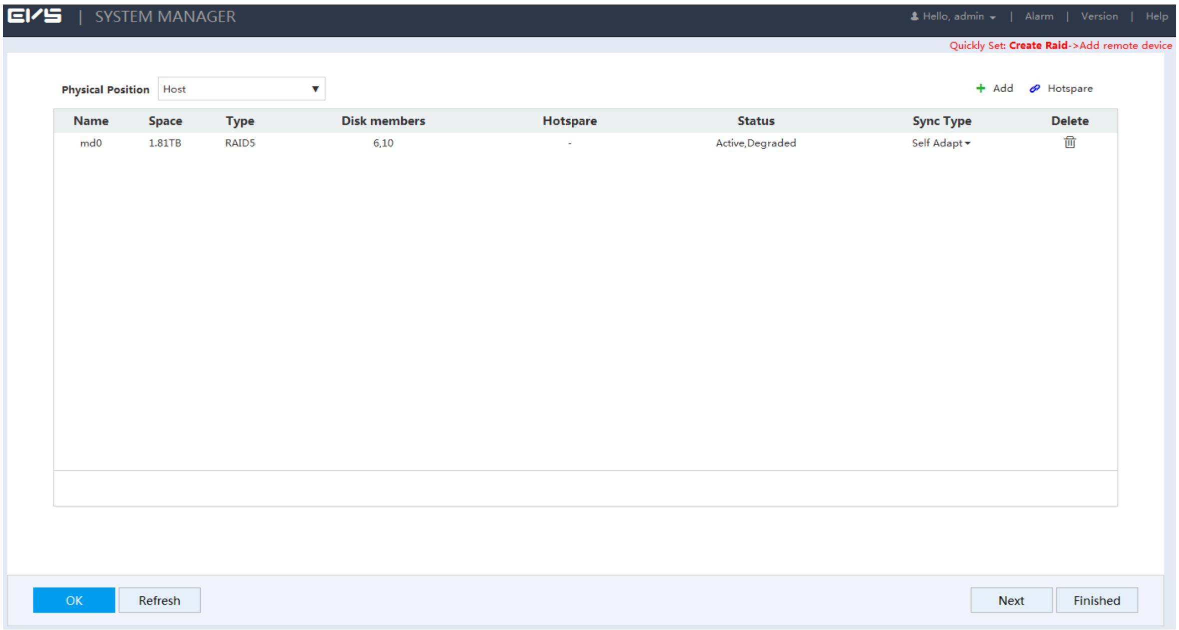


Step 1 Click ▾ at the right side of the user name. Select **Quickly Set > Video**.

The **Create Raid** interface is displayed. See Figure 3-20.

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

Figure 3-20 RAID management


SYSTEM MANAGER
Hello, admin | Alarm | Version | Help
Quickly Set: Create Raid->Add remote device
Physical Position
Host
+ Add
Hotspare
OK
Refresh
Next
Finished

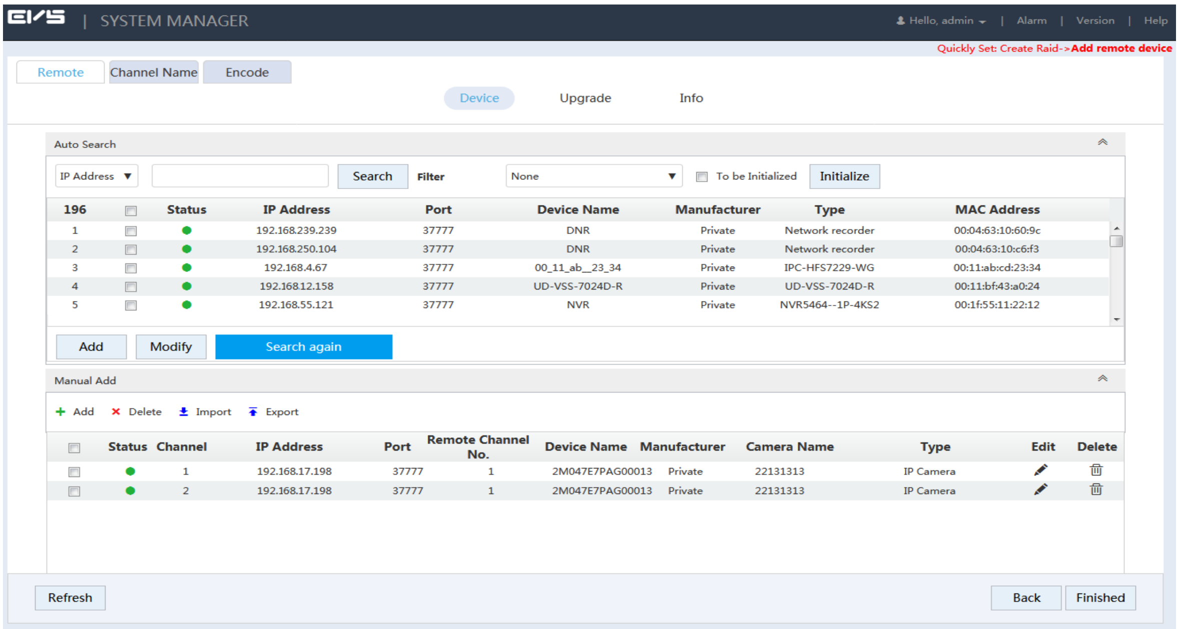
Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	1.81TB	RAID5	6,10	-	Active,Degraded	Self Adapt	🗑

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

Step 3 Click **Next**.

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

Figure 3-21 Adding remote device



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

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

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

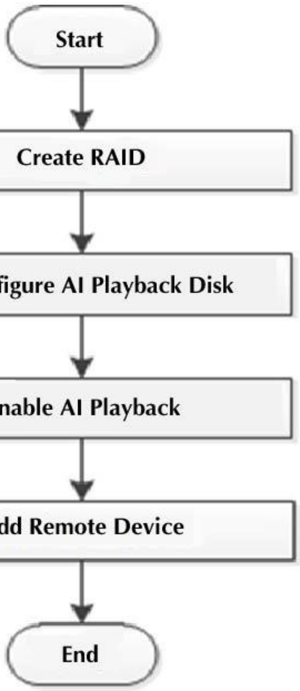
Step 5 Click **Finished** to save the configuration.

3.6 AI Playback

AI playback is an intelligent function for you to check and play back the results of general behavior analysis, vehicle detection, face detection and face matching.

For the procedure to configure AI playback, see Figure 3-22.

Figure 3-22 AI playback



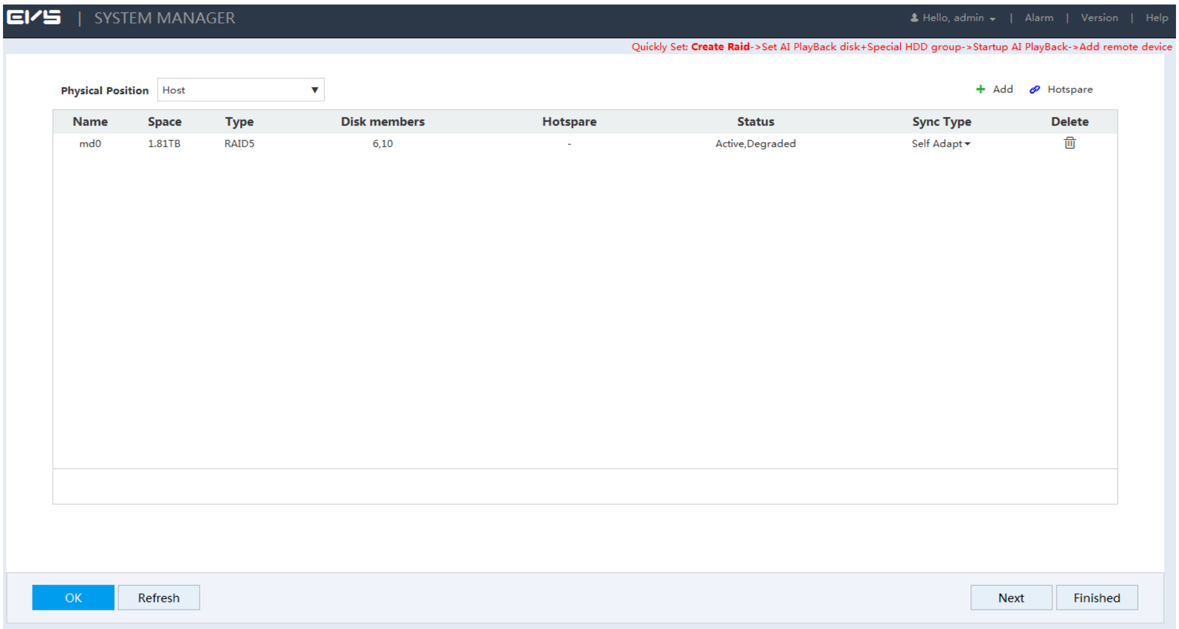
Step 1 Click ▾ at the right side of the user name. Select **Quickly Set > AI PlayBack**.

The **Create Raid** interface is displayed. See Figure 3-23.

📖

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

Figure 3-23 RAID management



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

Physical Position: Host

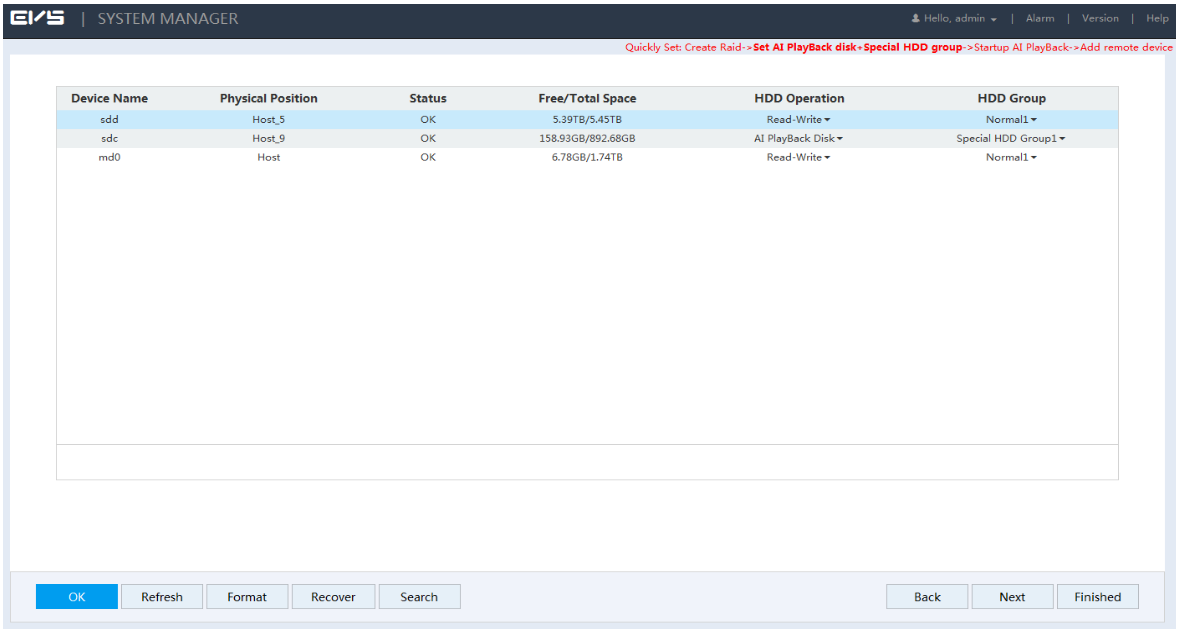
Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete
md0	1.81TB	RAID5	6,10	-	Active,Degraded	Self Adapt ▾	🗑

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

Step 3 Click **Next**.

The **Set AI PlayBack disk + Special HDD group** interface is displayed. See Figure 3-24.

Figure 3-24 Setting AI playback HDD and special HDD group



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

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

Step 4 Set AI playback HDD and HDD group.

1) Set the **HDD Operation** of one or several disks to **AI PlayBack Disk**.

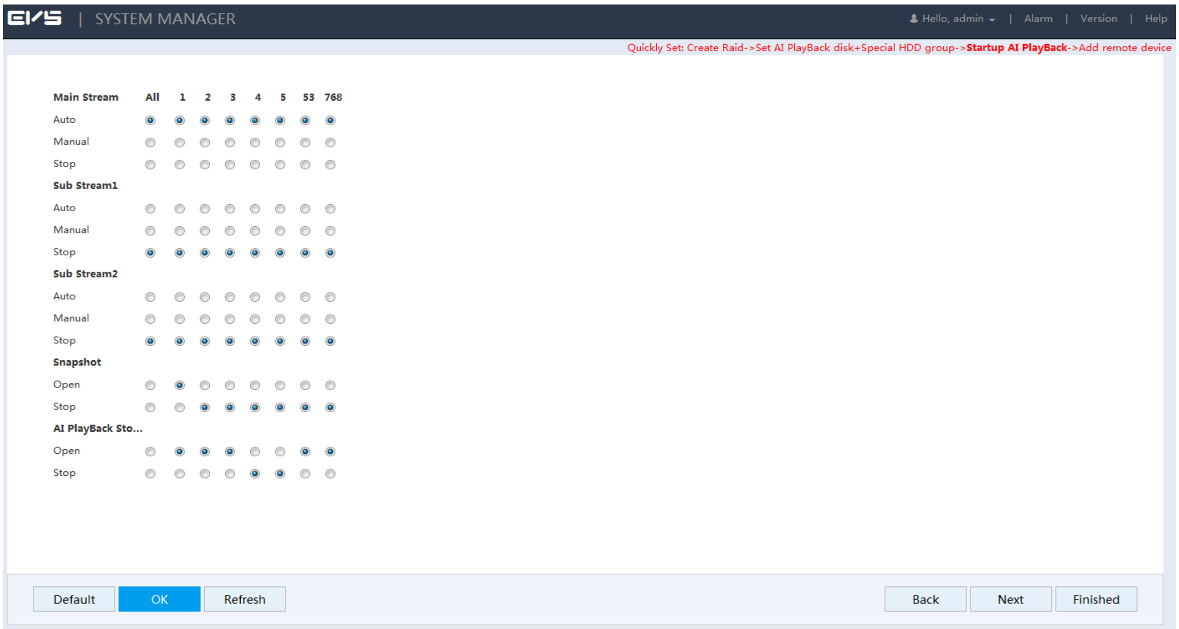
1) Set the **HDD Group** of the AI playback disk to **Special HDD Group**.

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

Step 5 Click **Next**.

The **Startup AI PlayBack** interface is displayed. See Figure 3-25.

Figure 3-25 AI playback startup



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

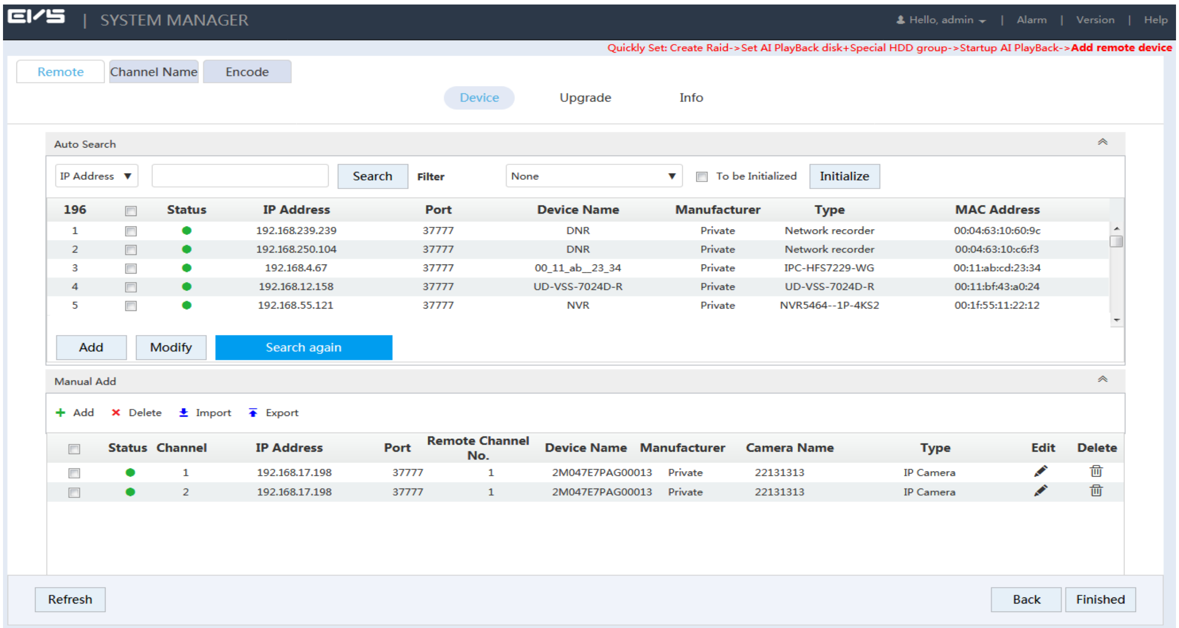
Main Stream	All	1	2	3	4	5	53	768
Auto	●	●	●	●	●	●	●	●
Manual	○	○	○	○	○	○	○	○
Stop	○	○	○	○	○	○	○	○
Sub Stream1								
Auto	○	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●
Sub Stream2								
Auto	○	○	○	○	○	○	○	○
Manual	○	○	○	○	○	○	○	○
Stop	●	●	●	●	●	●	●	●
Snapshot								
Open	○	●	○	○	○	○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

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

Step 7 Click **Next**.

The **Add remote device** interface is displayed. See Figure 3-26.

Figure 3-26 Adding remote device



EVS | SYSTEM MANAGER
Hello, admin | Alarm | Version | Help
Quickly Set: Create Raid->Set AI PlayBack disk+Special HDD group->Startup AI PlayBack->Add remote device
Remote
Channel Name
Encode
Device
Upgrade
Info
Auto Search
IP Address
Search
Filter
None
To be Initialized
Initialize

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

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

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

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

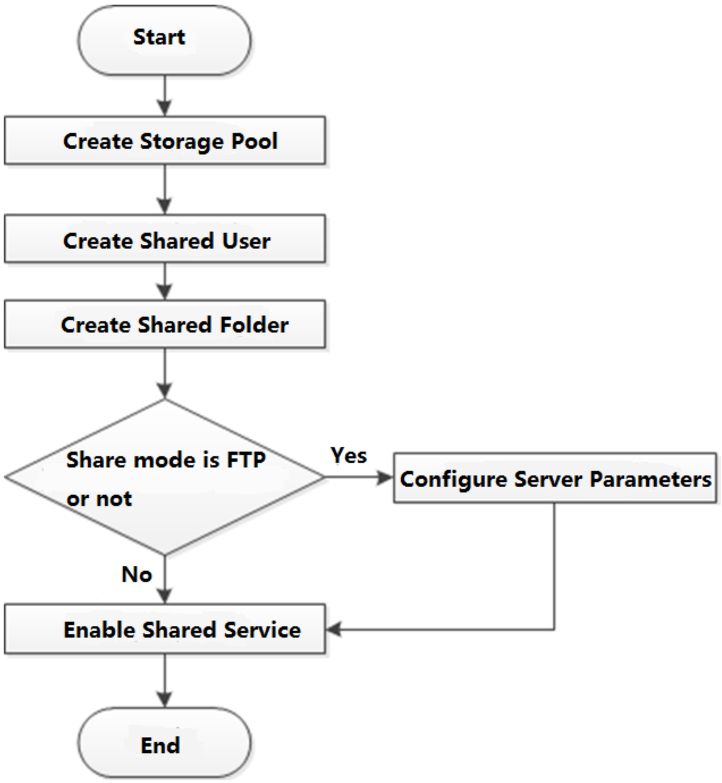
After the configuration, you can search the direct stored images. For details, see *User’s Manual*.

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 3-27.

Figure 3-27 Configuring IP SAN



3.7.1 Creating Storage Pool

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

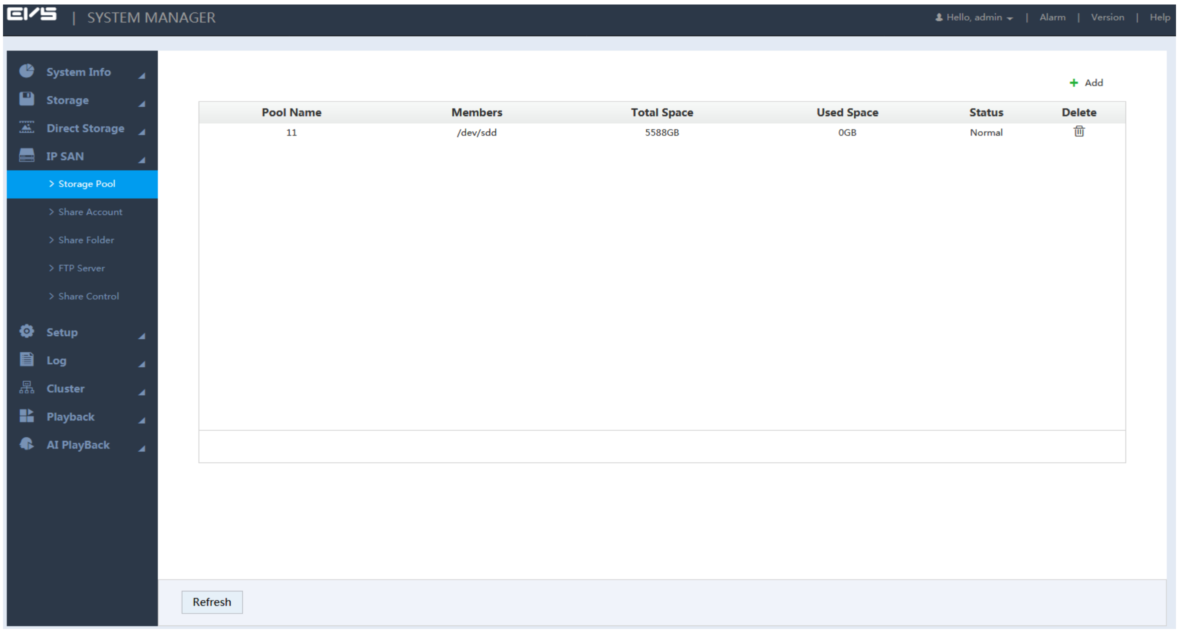
⚠

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

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

The **Storage Pool** interface is displayed. See Figure 3-28.

Figure 3-28 Storage pool

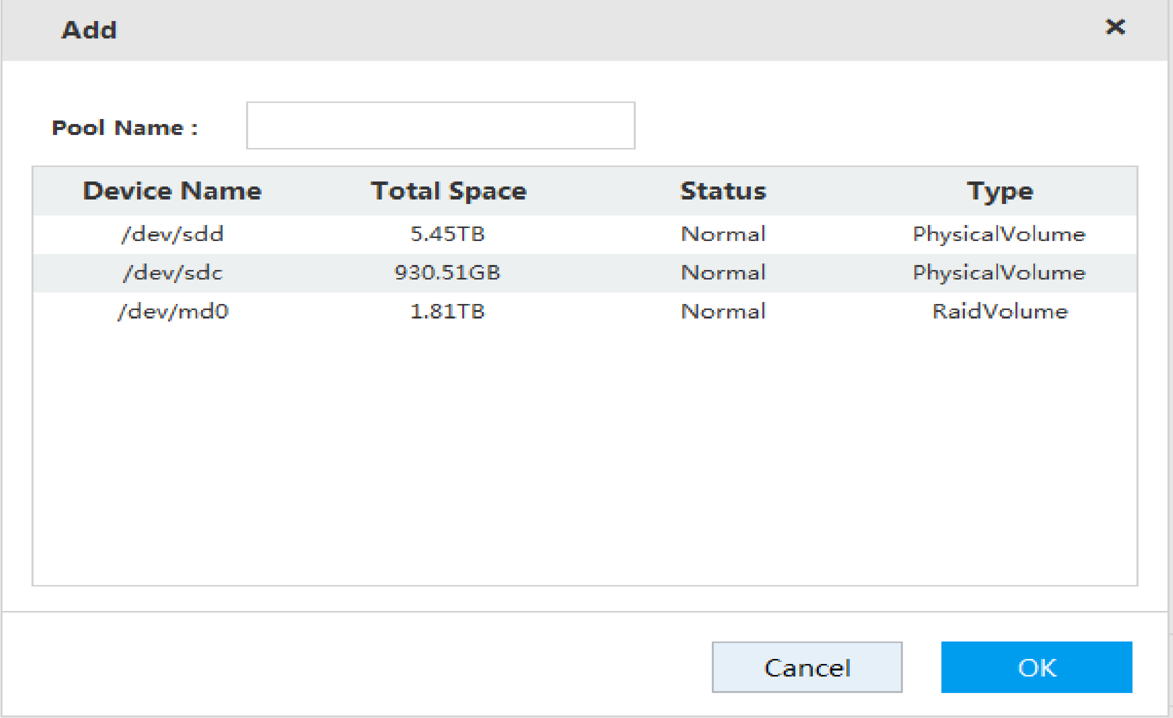


Pool Name	Members	Total Space	Used Space	Status	Delete
11	/dev/sdd	5588GB	0GB	Normal	🗑

Step 2 Click + .

The **Add** interface is displayed. See Figure 3-29.

Figure 3-29 Adding storage pool



Pool Name :

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

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

By default, 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.

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

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

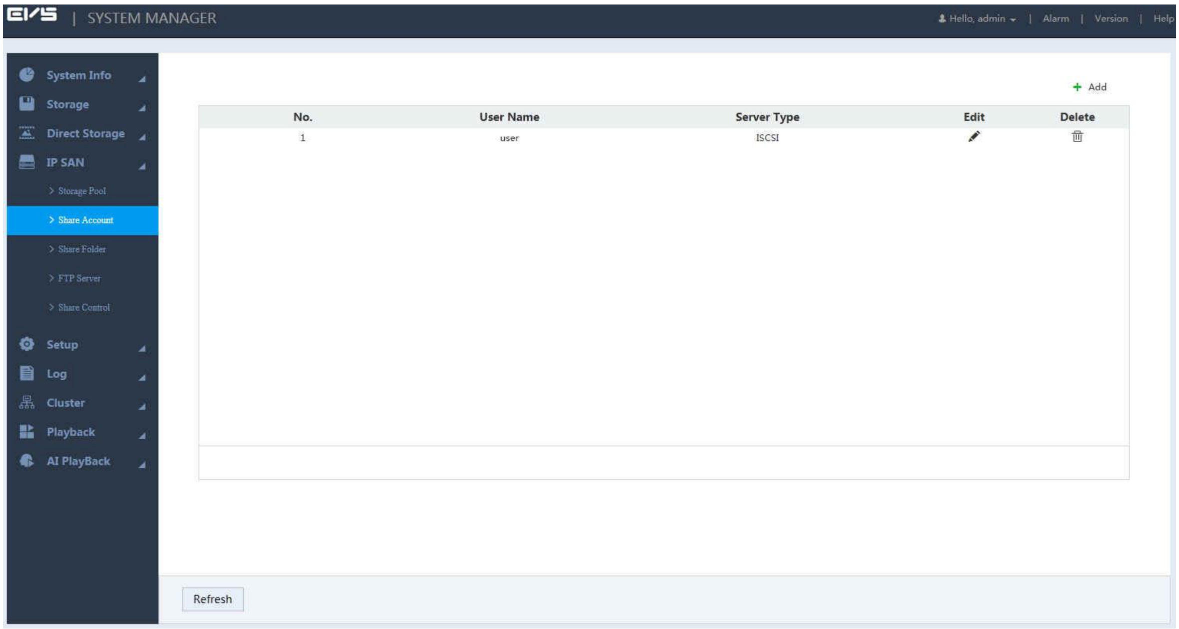
3.7.2 Managing Share Account

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

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

The **Share Account** interface is displayed. See Figure 3-30.

Figure 3-30 Share account management

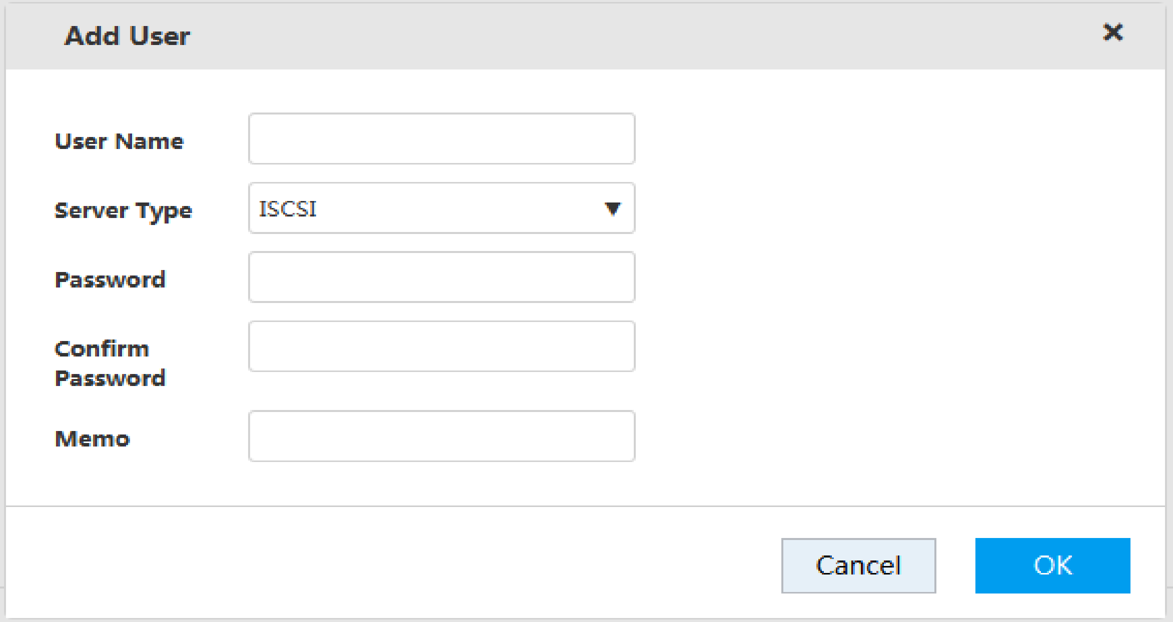


No.	User Name	Server Type	Edit	Delete
1	user	ISCSI	✎	🗑

Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-31.

Figure 3-31 Adding shared user



User Name	
Server Type	ISCSI ▼
Password	
Confirm Password	
Memo	

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

Table 3-8 Parameters of adding user

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

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

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

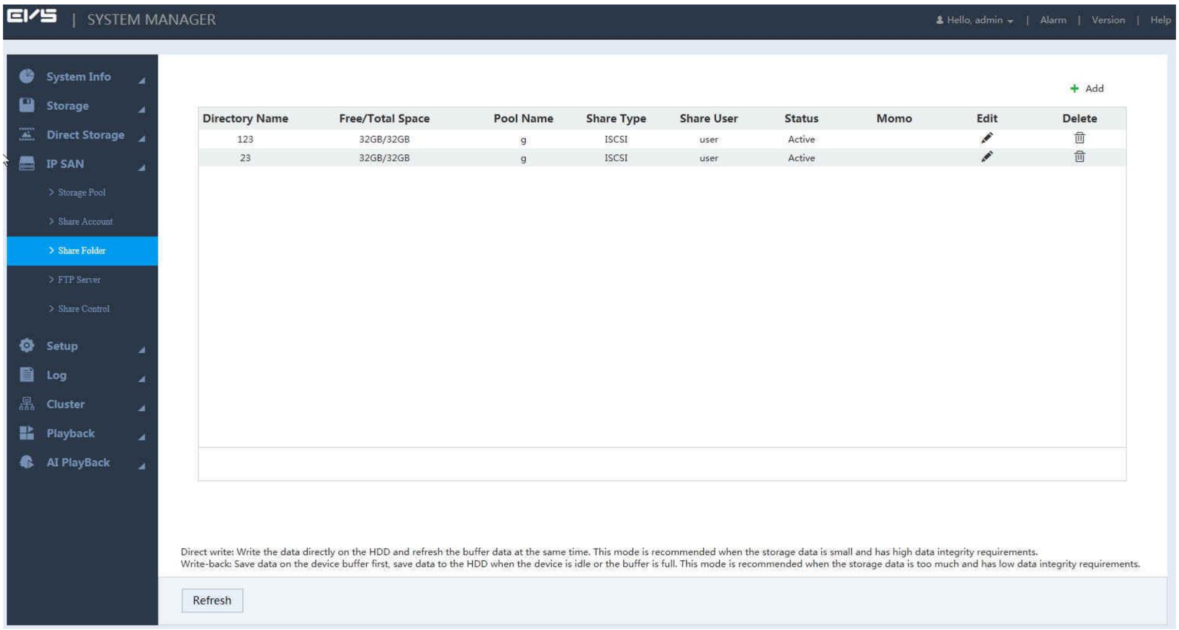
3.7.3 Setting Share Folder

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

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

The **Share Folder** interface is displayed. See Figure 3-32.

Figure 3-32 Share folder



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

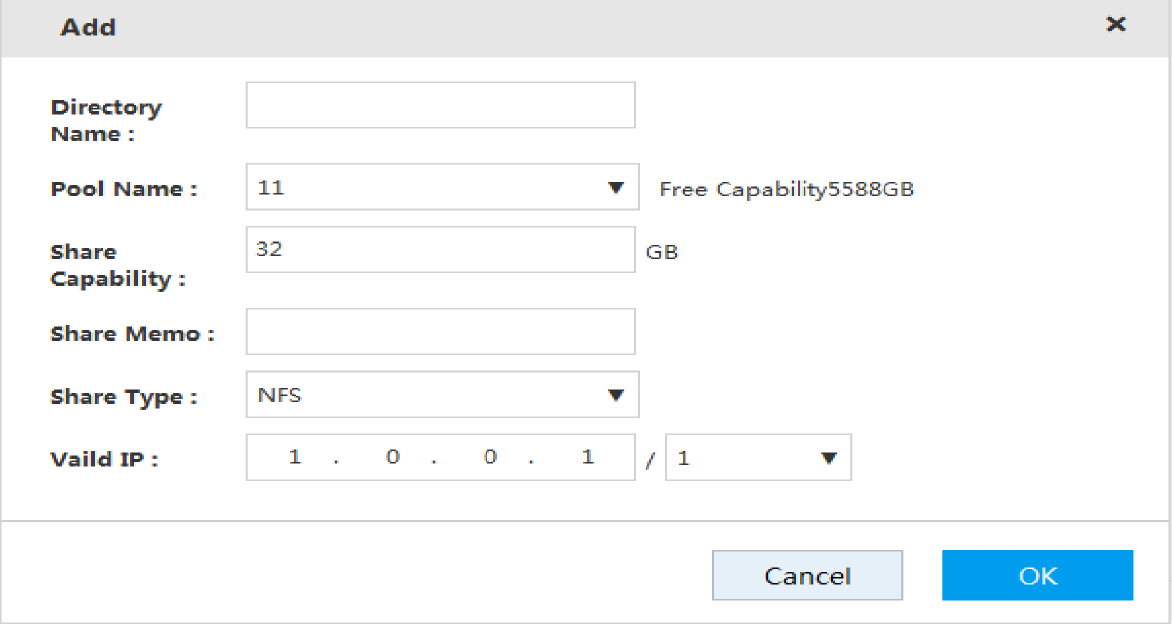
Direct write: Write the data directly on the HDD and refresh the buffer data at the same time. This mode is recommended when the storage data is small and has high data integrity requirements.

Write-back: Save data on the device buffer first, save data to the HDD when the device is idle or the buffer is full. This mode is recommended when the storage data is too much and has low data integrity requirements.

Step 2 Click + .

The Add interface is displayed. See Figure 3-33 or Figure 3-34.

Figure 3-33 Adding share folder (NFS)


Add

Directory Name :

Pool Name : 11 Free Capability5588GB

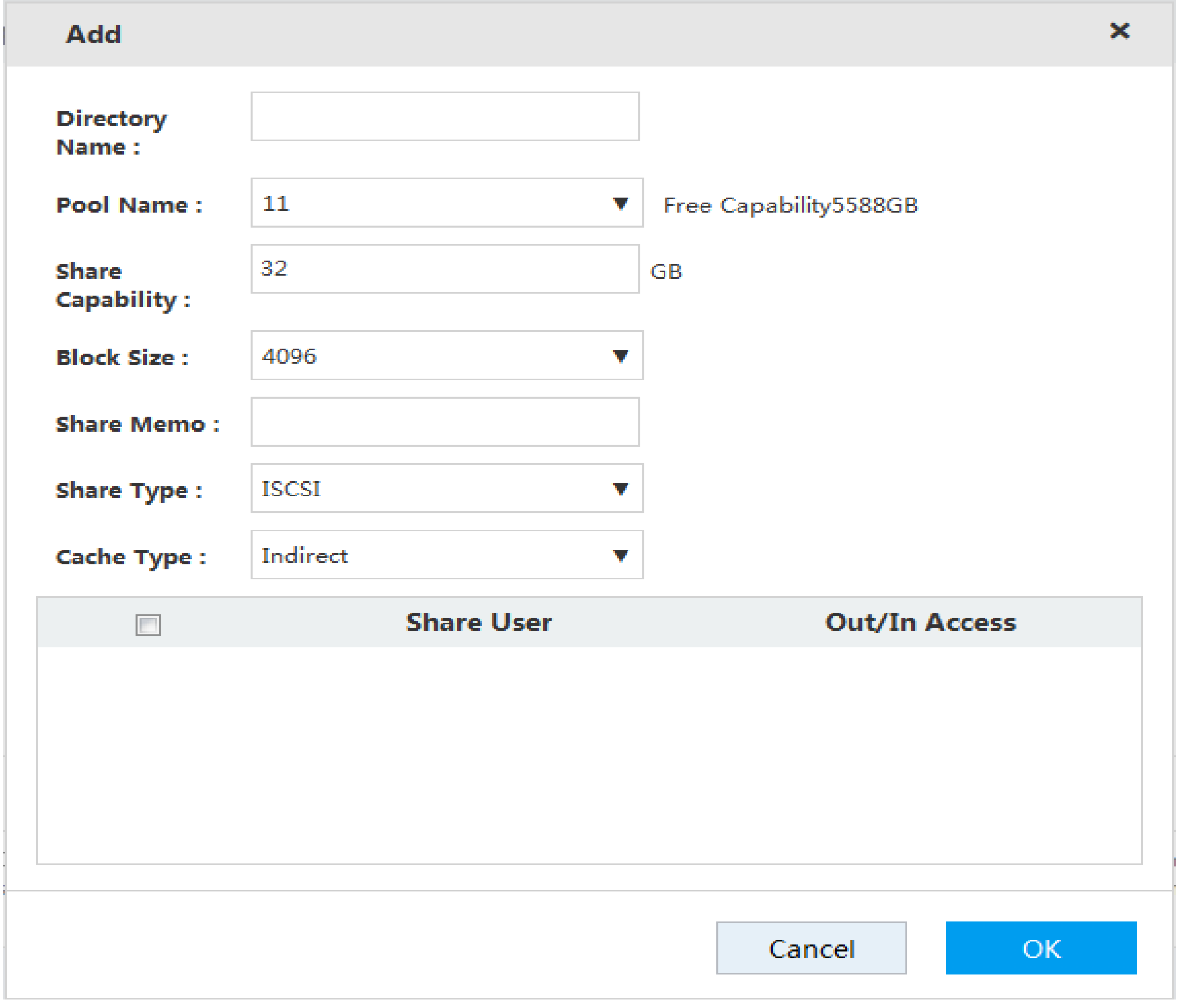
Share Capability : 32 GB

Share Memo :

Share Type : NFS

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

Figure 3-34 Adding share folder (iSCSI)


Add

Directory Name :

Pool Name : 11 Free Capability5588GB

Share Capability : 32 GB

Block Size : 4096

Share Memo :

Share Type : ISCSI

Cache Type : Indirect

□	Share User	Out/In Access

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

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.
Valid IP	Set the IP address and subnet mask of the hosts allowed to access this share folder. For example: When the valid IP is 192.168.10.108/24, it means the IP address is 192.168.10.108 and the subnet mask is 255.255.255.0. All the IP hosts in this segment can access the share folder. 📖 This parameter needs to be configured when the **Share Type** is set as NFS.
Valid User	Select the shared user and set its out/in access authority. ● When the **Share Type** is set as FTP and SAMBA and no valid user is selected, only the admin account has the access permission. Other accounts do not have the authority. ● When the **Share Type** is set as iSCSI and no valid user is selected, all the users have the access permission. 📖 ● You need to select the valid user when select FTP, SAMBA or iSCSI as the share type. ● FTP default admin account: ftpuser; default password: 111111111111. SAMBA default admin account: admin; default password: 888888888888.

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

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

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

When you create the share folder for the first time or create share folder under the condition of system auto maintenance, the system will force off the auto maintenance. After configuring the IP SAN, you can enable auto maintenance manually. For details, see *User's Manual*.

3.7.4 Setting FTP Parameters

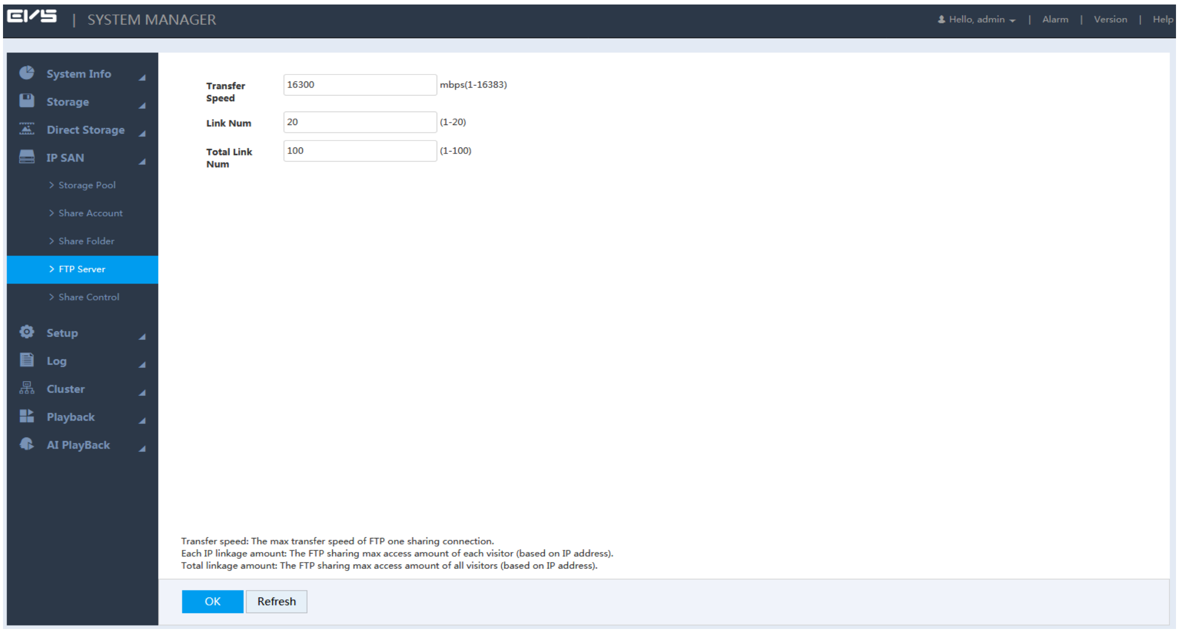
Set the transmission speed and max connection number in FTP share.

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

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

The **FTP Server** interface is displayed. See Figure 3-35.

Figure 3-35 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 Configure 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 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.

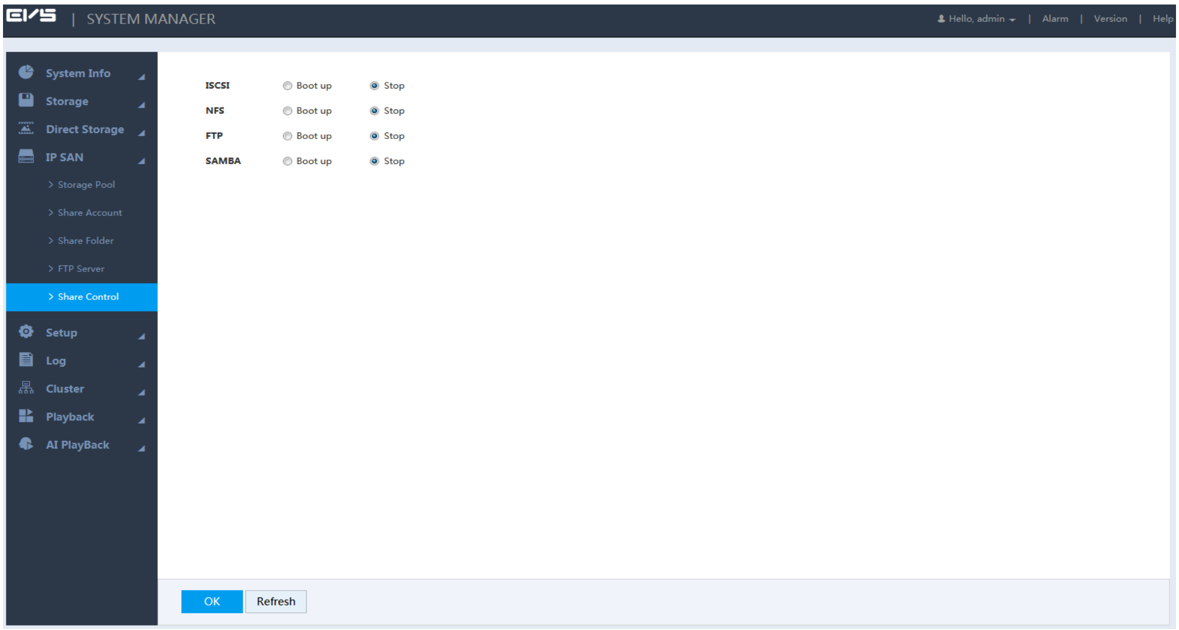
3.7.5 Opening Share Services

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

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

The **Share Control** interface is displayed. See Figure 3-36.

Figure 3-36 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 share service according to actual needs.

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

3.8 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.

- The disk set for AI playback 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, RAID2.0 and RAIDJ. For details, see *User's Manual*.

3.8.1 Creating RAID

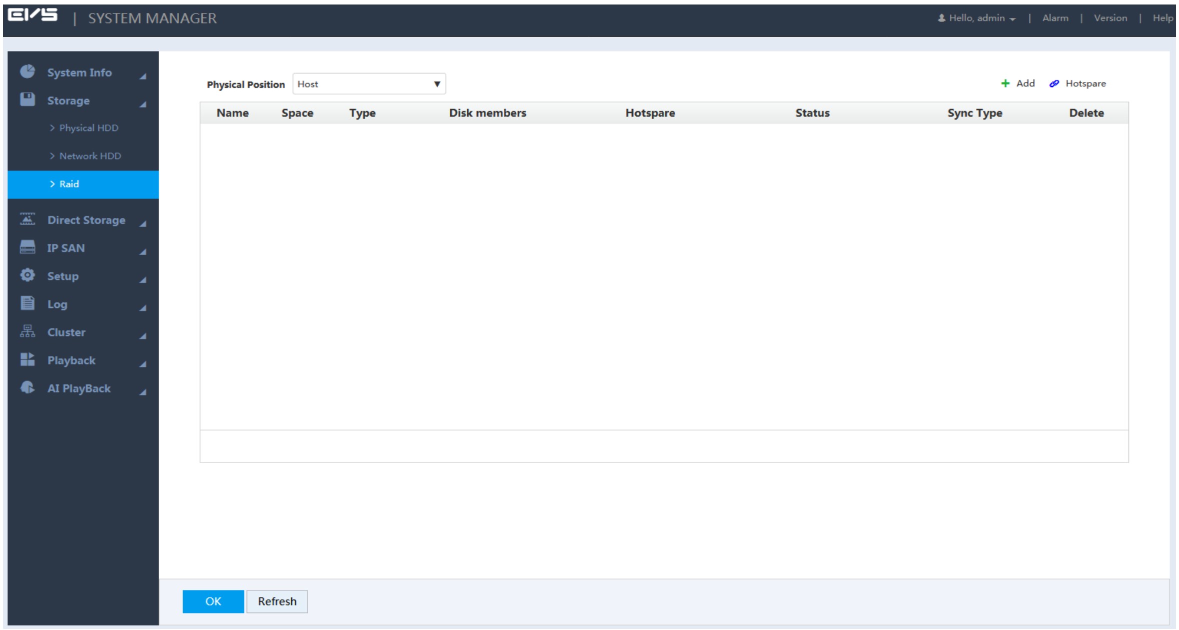
RAID has different levels (such as RAID5, RAID6) and each level has its own data protection, data availability and performance level. You can create RAID according to the practical needs.

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

Step 1 Select **Storage > Raid**.

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

Figure 3-37 Raid management



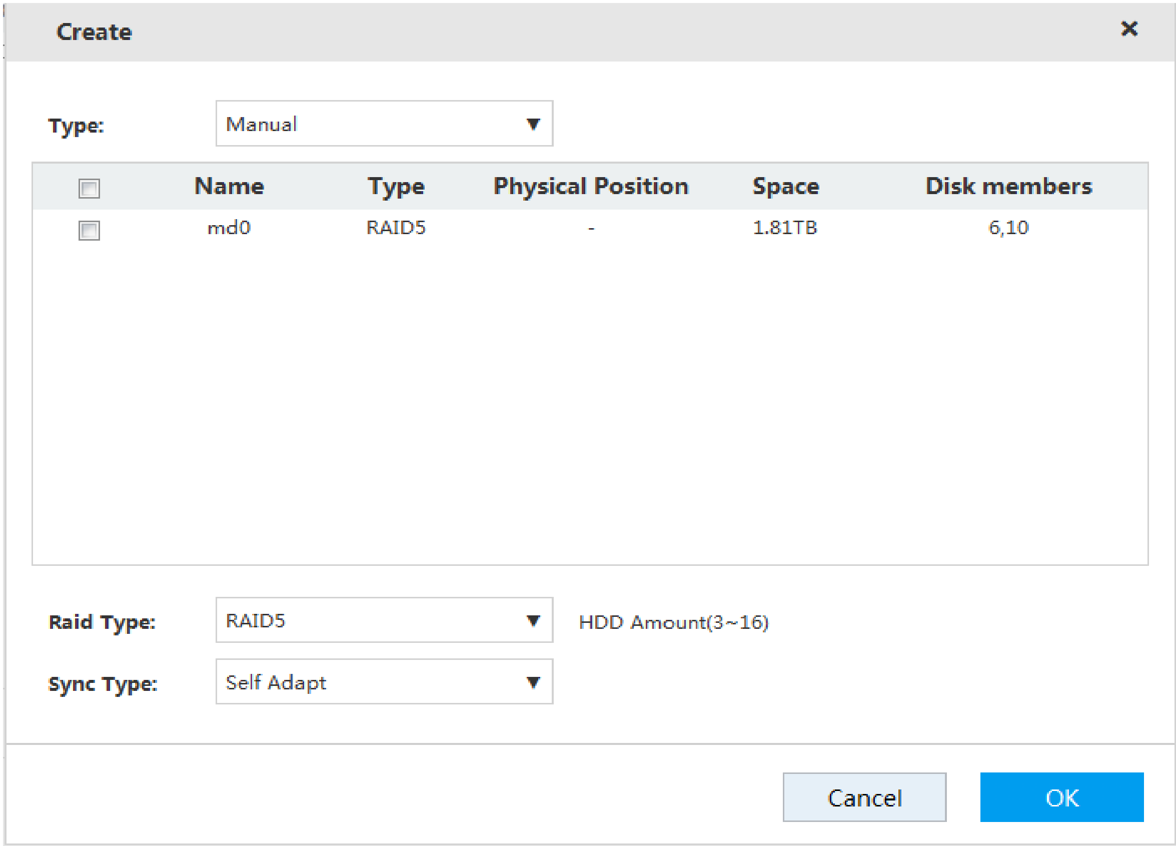
Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete

Step 2 Click + .

The **Create** interface is displayed. See Figure 3-38.

Figure 3-38 Creating RAID



Type: Manual

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

Raid Type: RAID5 HDD Amount(3~16)

Sync Type: Self Adapt

Step 3 Configure 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 according to the shortcut RAID creation strategy. For details, see Table 3-12. Raid2.0 provides different storage strategies for the same RAID based on your data security requirements.
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 are supported: low, middle and high. 📖 Only when selecting "Raid2.0" as the Type will the system support this function.

Parameter	Description
Sync Type	Select the sync mode of the business resources allocation. Self Adapt: Automatically adjust the RAID sync speed according to the current business loads. When there is no external business, sync is performed at a high speed. When there is external business, sync is performed at a low speed. Sync First: Resource priority is assigned to RAID sync. Business First: Resource priority is assigned to business operations. Balance: Resource is evenly distributed to RAID sync and business operations. Only when selecting "Manual" as the Type and "Raid 5" as the Raid Type will the system support this function.

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

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

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

Shortcut RAID Creation Strategy

When the disks are fully installed, the system creates RAID 5 according to the policy in Table 3-12.

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

Table 3-12 Shortcut RAID creation strategy

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

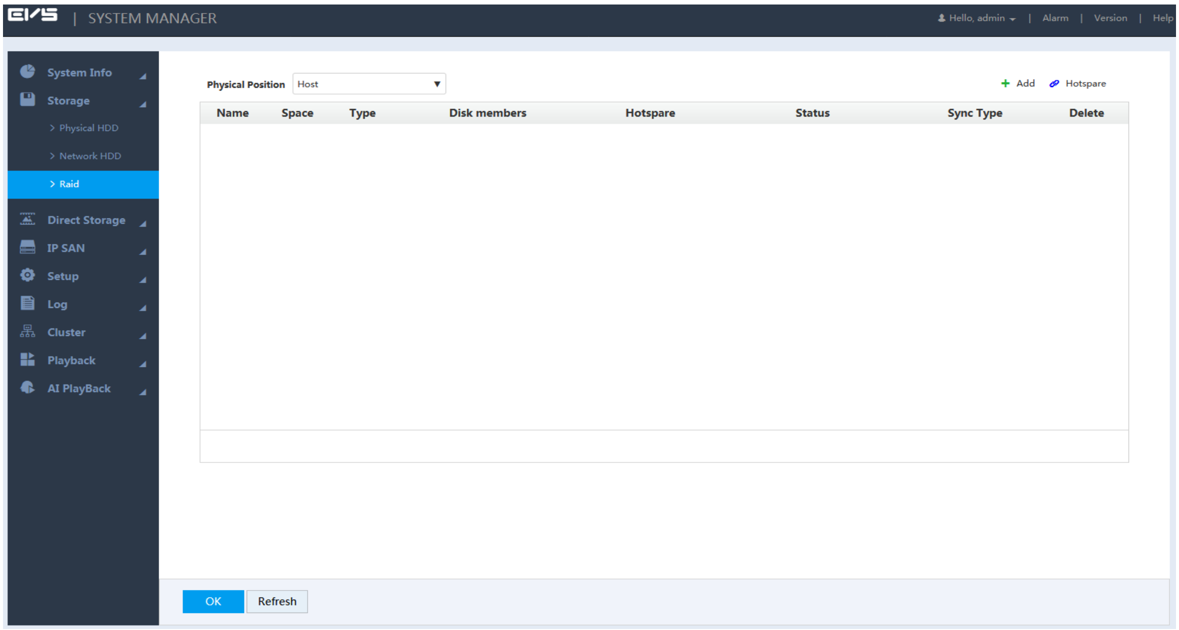
3.8.2 Hot Spare Management

When a member disk of the RAID group is fault or abnormal, the hot spare 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 3-39.

Figure 3-39 Raid management



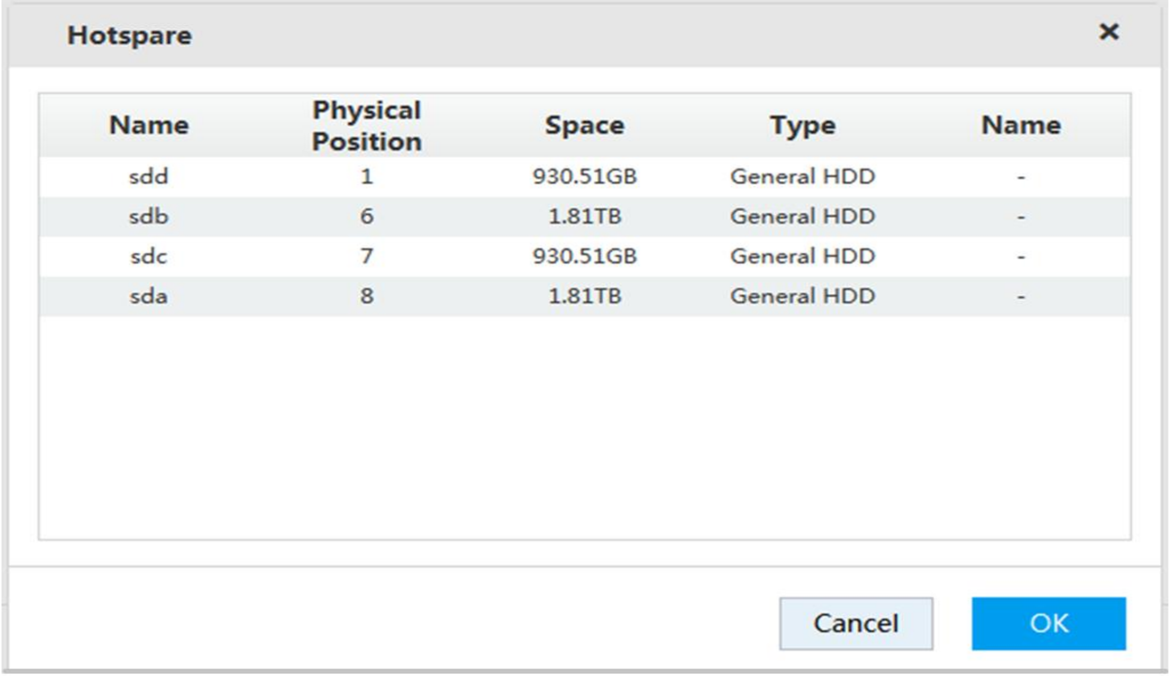
Physical Position: Host

Name	Space	Type	Disk members	Hotspare	Status	Sync Type	Delete

Step 2 Click 🔗 .

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

Figure 3-40 Hot spare management



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

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

- General HDD: A general disk member in the RAID.

- Private hot spare: Double-click the corresponding **Name**, select the RAID group, and then this HDD is used as a hot spare only for the corresponding group.
- 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 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**

   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

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

9. **Assign Accounts and Privileges Reasonably**

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

10. **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.

11. **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.

12. **Secure Auditing**

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

13. **Network Log**

    Due to the limited storage capacity of the equipment, 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.

14. **Construct a Safe Network Environment**

    In order to better ensure the safety of equipment 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.