Embedded Video Storage Server (EVS50,EVS70 Series)

Quick Start Guide

V2.0.1

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

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

2. Update Firmware

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

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

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

2. Change Default HTTP and TCP Ports:

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

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

3. Enable HTTPS/SSL:

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

4. Enable IP Filter:

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

5. Change ONVIF Password:

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

6. Forward Only Ports You Need:

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

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

7. Disable Auto-Login on SmartPSS:

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

8. Use a Different Username and Password for SmartPSS:

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

9. Limit Features of Guest Accounts:

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

10. UPnP:

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

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

11. SNMP:

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

12. Multicast:

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

13. Check the Log:

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

14. Physically Lock Down the Device:

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

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

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

16. Isolate NVR and IP Camera Network

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

General

This document introduces the functions and operations of the EVS series devices (hereinafter referred to be "the Device").

Models

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

Safety Instructions

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

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

Privacy Protection Notice

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

About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall govern.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- 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. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Electrical safety

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

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

Transportation security

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

Installation

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

Qualified engineers needed

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

Environment

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

Accessories

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

Lithium battery

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

Table of Contents

1 Overview

1.1 Overview

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

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

This product provides standard network file sharing service and realizes the integrated solution for IPSAN/NAS. It provides centralized storage solution with large capacity, high scalability and high security for all kinds of video monitoring systems.

NOTE

Below contents are introduced in the example of Middle-Class 24-HDD single-controller. Functions of other series are similar. Please refer to the actual situation.

1.2 Front Panel

Figure 1-1 Front panel

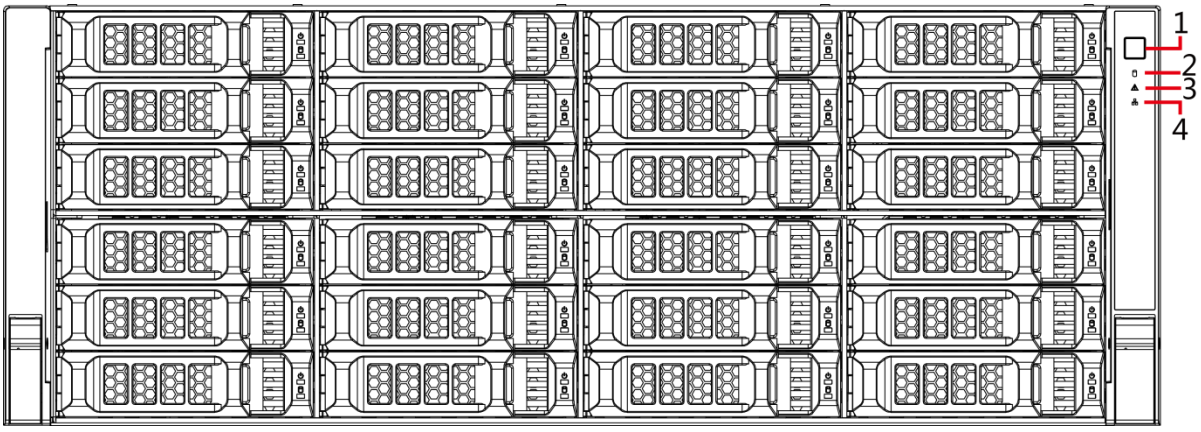


Table 1-1 Description of interfaces on front panel

No.	Indicator Light/Button	Description

No.	Indicator Light/Button	Description
1	Power button	Press the power button to execute operations of device start-up and shutdown. ● Press this button to boot the device when it is shutdown. ● Hold down this button for 5 seconds to force a device shutdown.
2	HDD light	HDD status light. ● The light is out when the HDD is in normal operation. ● The blue light keeps on if no HDD, HDD error or insufficient HDD space.
3	Alarm light	Alarm status light. ● The light is out when the device is running properly. ● The red light keeps on when the power, temperature or fan is abnormal.
4	Network light	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)

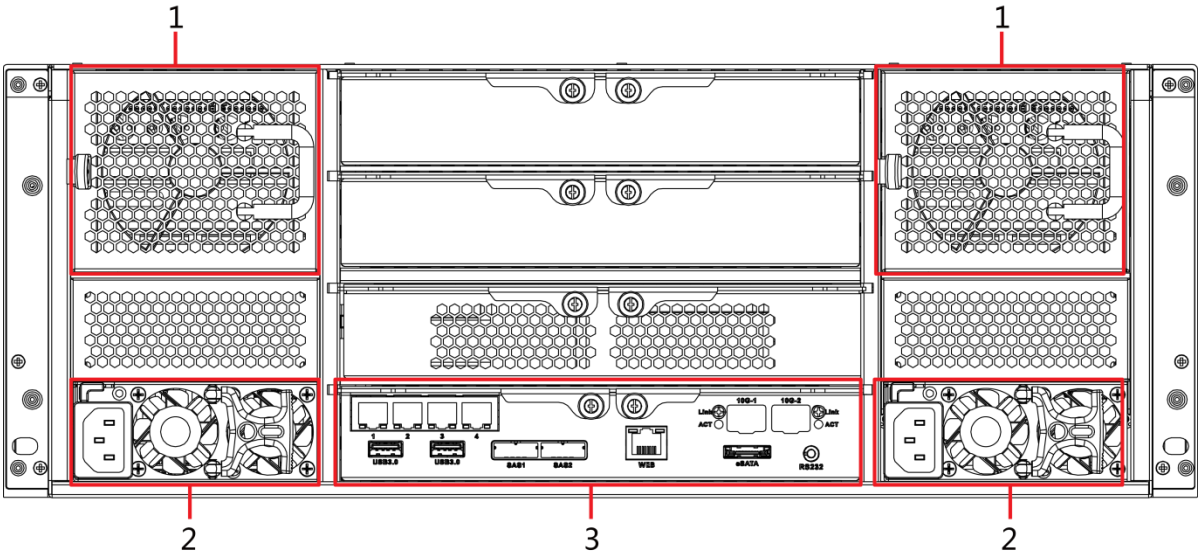


Figure 1-3 Rear panel (7 Ethernet ports)

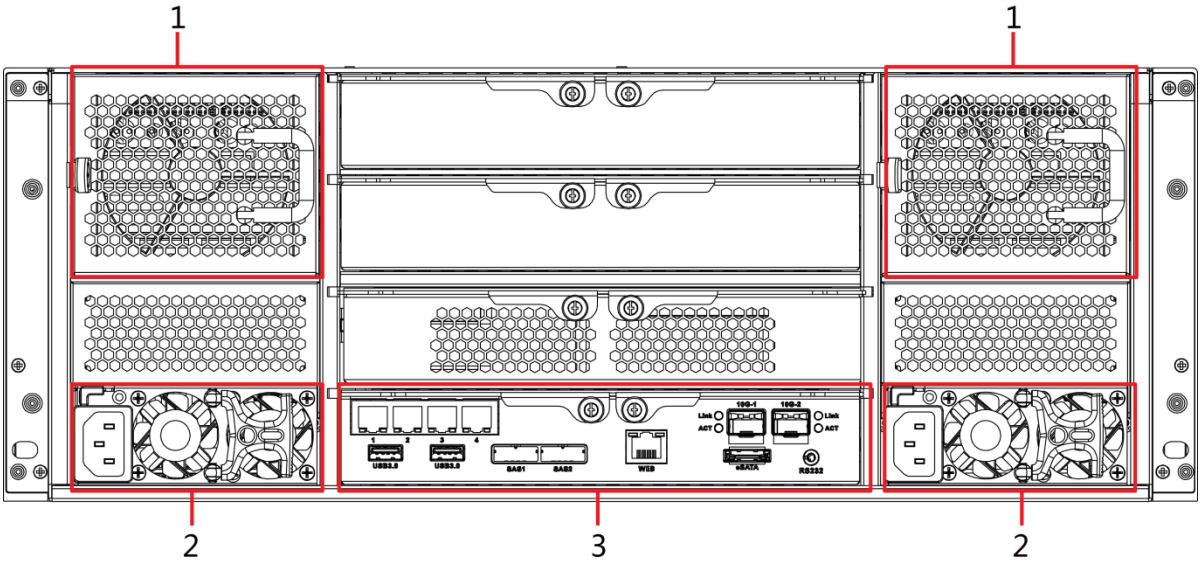


Figure 1-4 Rear panel (9 Ethernet ports)

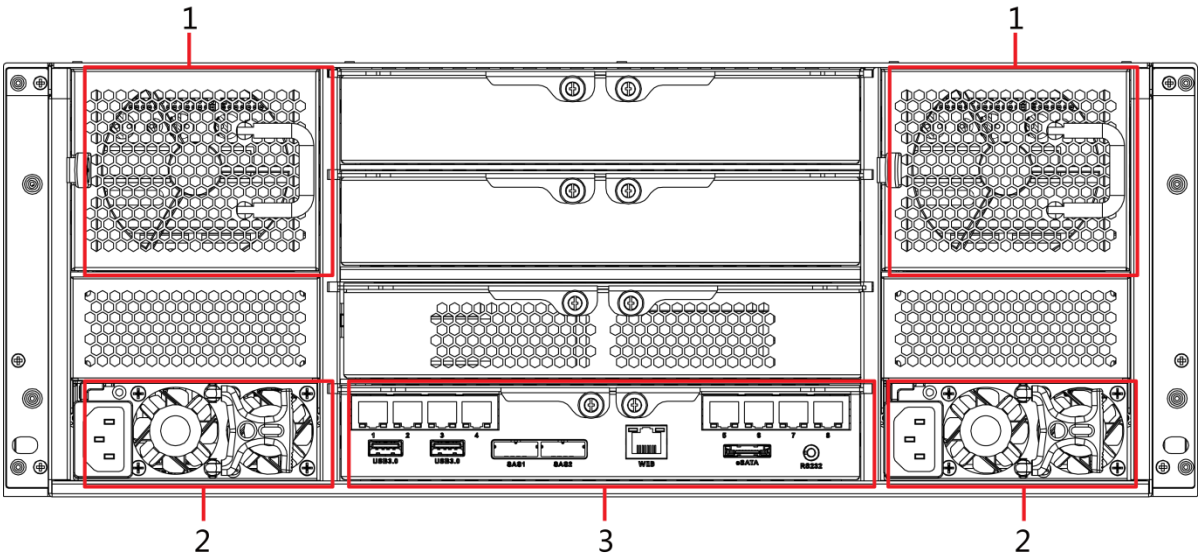


Table 1-2 Description of interfaces on rear panel

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

Table 1-3 Description of interfaces on the master control module

Interface	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. NOTE 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.

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

2 Installing and Powering the Device

2.1 Installing Hard Disk Drive (HDD)

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

WARNING

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

2.1.1 Middle-Class 16-HDD Single-Controller Series

NOTE

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

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

Figure 2-1 Opening the handle

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

Figure 2-2 Hard disk box

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

Figure 2-3 Locking the screws

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

CAUTION

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

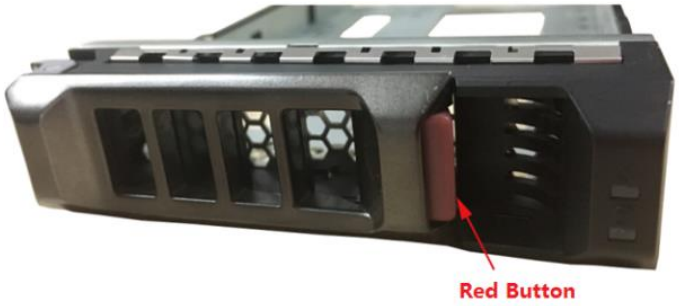
2.1.2 Other Series

NOTE

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

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

Figure 2-4 Opening the handle

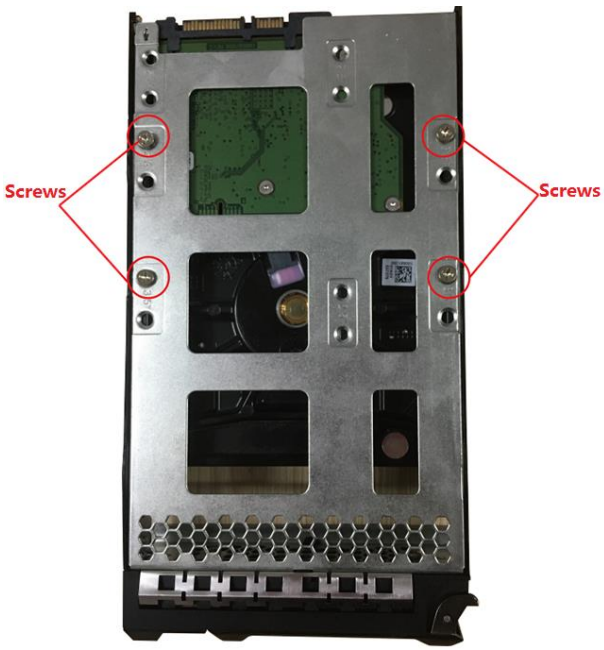


Step 2 Pull out to take the empty hard disk box. See Figure 2-5.

Figure 2-5 Hard disk box

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

Figure 2-6 Locking the screws



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

CAUTION

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

2.2 Powering the Device

2.2.1 Preparation

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

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

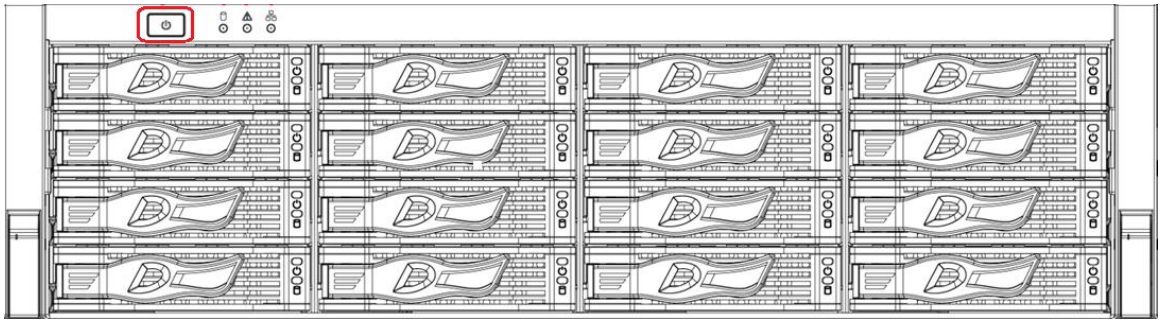
2.2.2 Power on

NOTE

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

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

Figure 2-7 Front panel



See Table 1-1 to check if the indicator lights are normally displayed.

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

3 Web Basic Operations

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

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

NOTE

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

3.1 Connecting the Network

Before logging in Web on PC, you need to connect the device and PC to the same network and confirm 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 routing device in the network, assign IP address of the same network segment for PC and EVS devices.
- If there is routing device in the network, set the corresponding gateway IP and subnet mask for PC and EVS devices respectively.

NOTE

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

- Single control device: Network card 1 to network card n corresponds to default IP 192.168.1.108 to 192.168.n.108.
- Double control device: Different slots have different default IP.
  - ◇ Slot 1: Network card 1 to network card n corresponds to default IP 192.168.1.108 to 192.168.n.108.
  - ◇ Slot 2: Network card 1 to network card n corresponds to default IP 192.168.1.109 to 192.168.n.109.
- The port order is standard card, expansion card and Web management card. You need to confirm the default IP according to the actual device condition.

Step 3 On PC, execute the command of **ping** *192.168.1.108 (192.168.1.108* refers to the device IP address) to check if the network is connected.

3.2 Initializing the Device

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

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

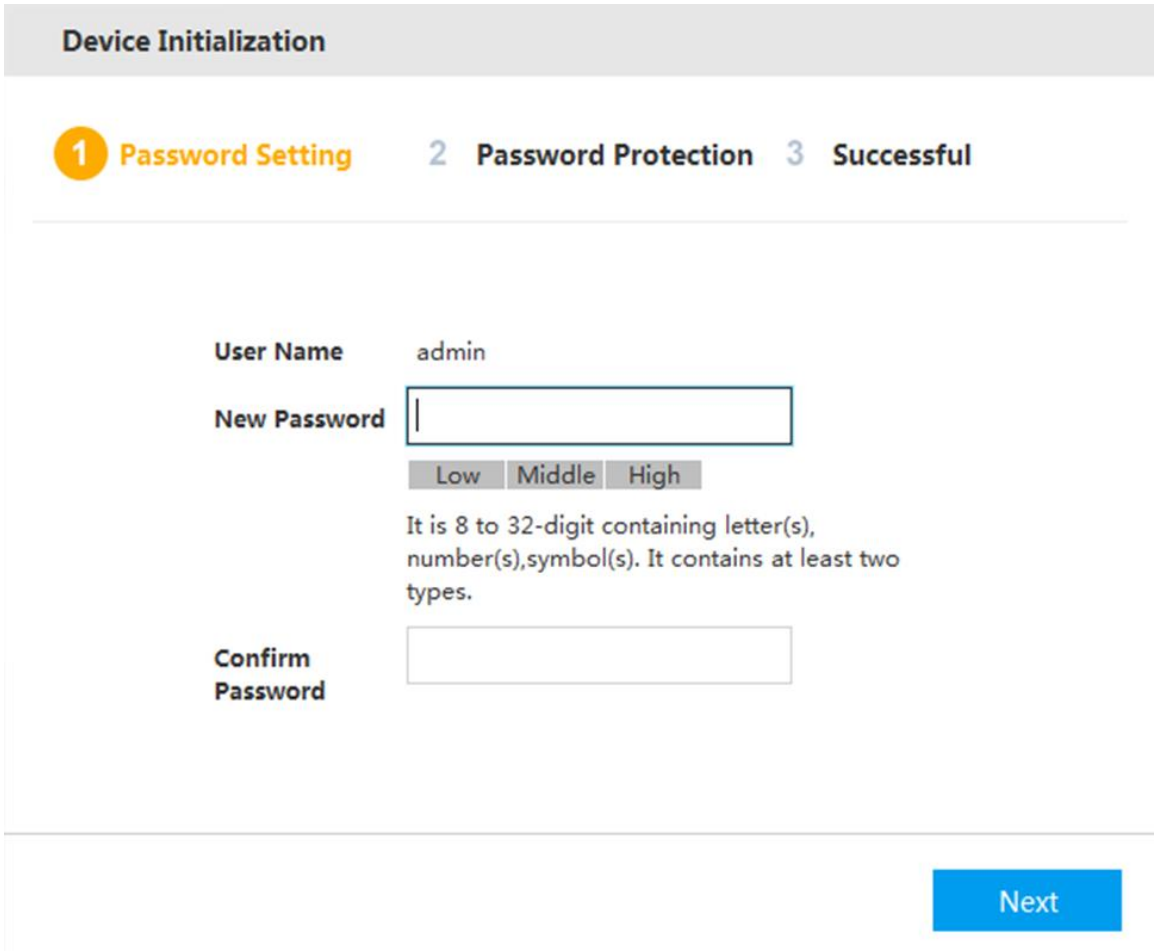
NOTE

- 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



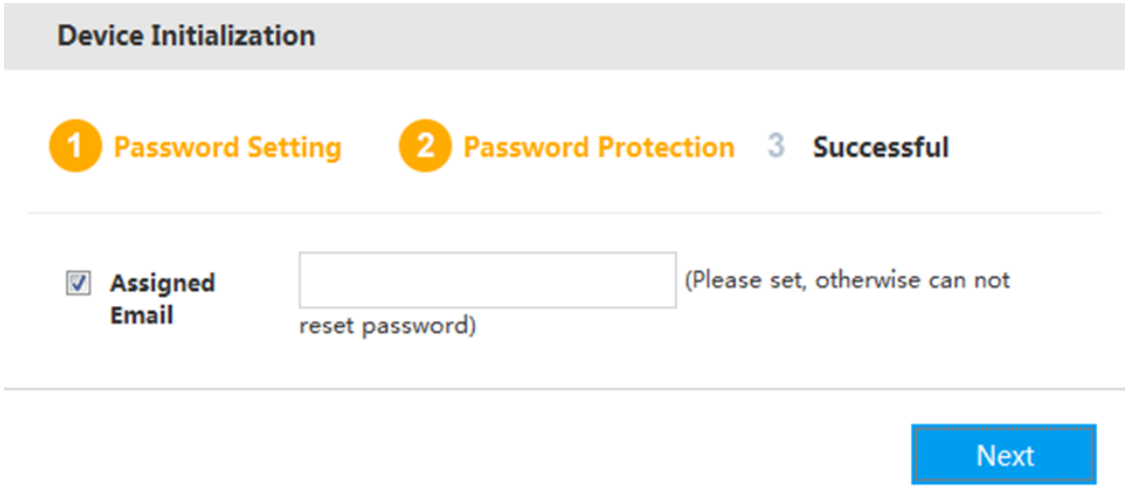
Step 3 In the **New Password** box, enter the new password.

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



Step 5 Enter the **Assigned Email**.

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

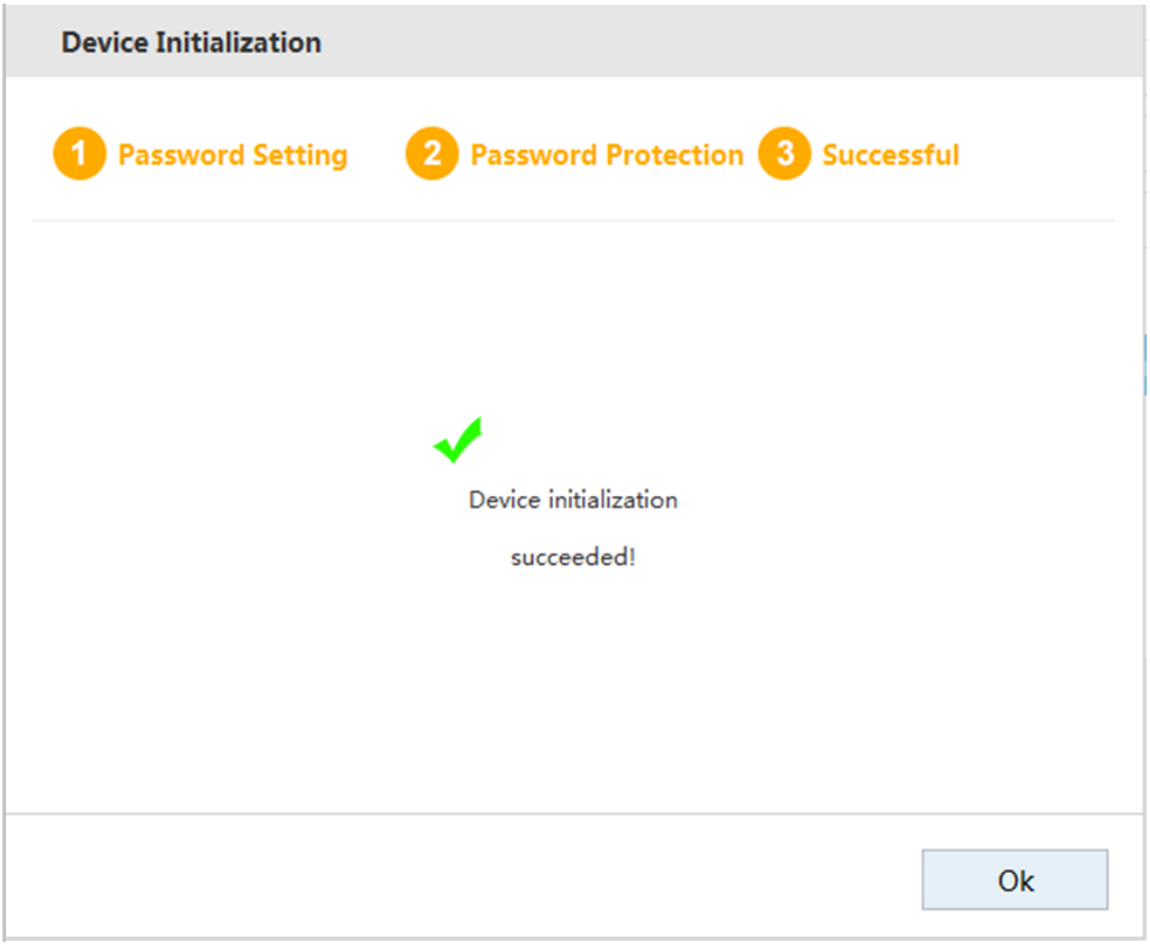
NOTE

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

Step 6 Click **Next**.

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

Figure 3-3 Device initialization succeeded



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

3.3 Logging in Web

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

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

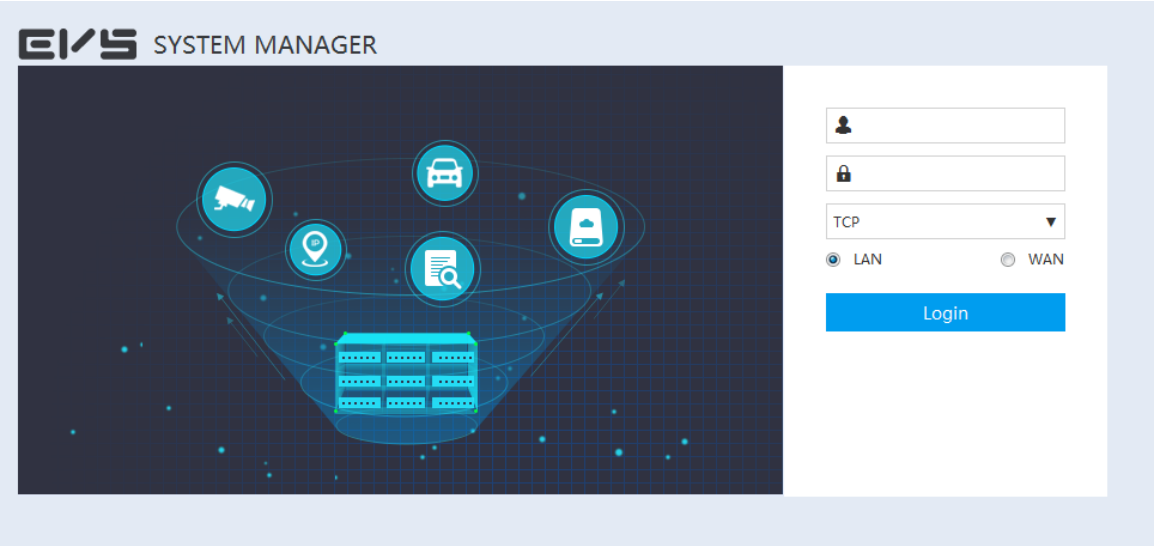
Step 2 Install the control.

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.

NOTE

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

Figure 3-4 WEB login interface



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

NOTE

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

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

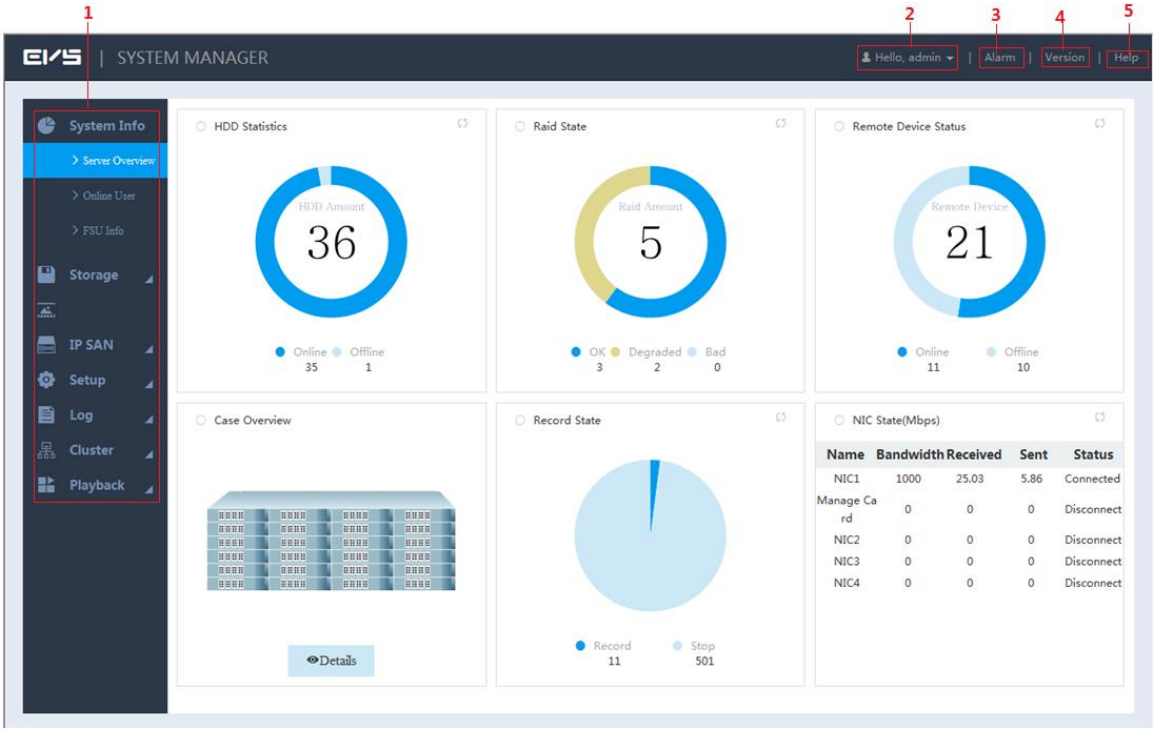


Table 3-1 System manager description

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  on the right side of the user name and you can perform quick guide configuration and user logout. ● Quick guide: You can configure video/image direct storage and IPSAN according to different application scenarios. ● Exit: Log out the current user.
3	Alarm	Click **Alarm** and you can search the alarm logs of the EVS device. For details, see *User's Manual*.
4	Version	Click **Version** and you can view the version information of the EVS device, including video channel, S/N, Web version, system version, Bios version and Onvif Client version.
5	Help	Click **Help** and you can get the Quick Start Guide for the device.

3.4 Initial Configuration

3.4.1 IP Settings

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

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

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

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

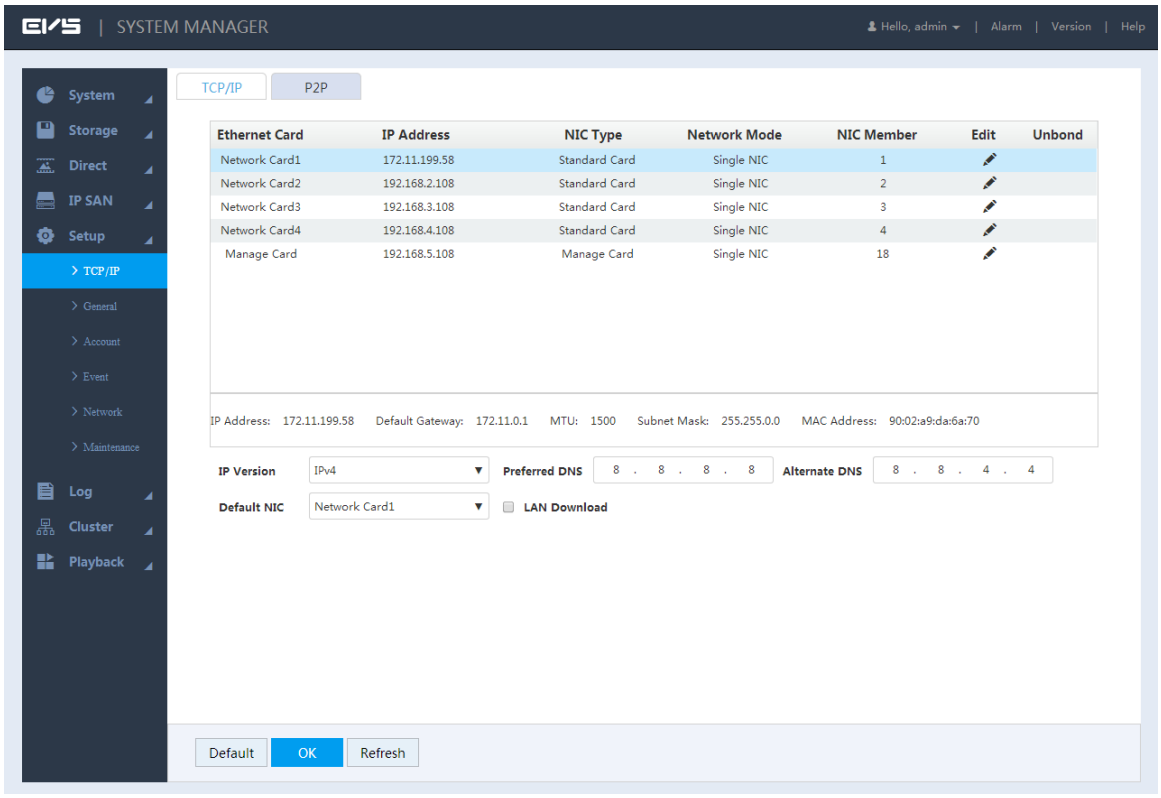


Figure 3-7 TCP/IP settings (dual-control device)

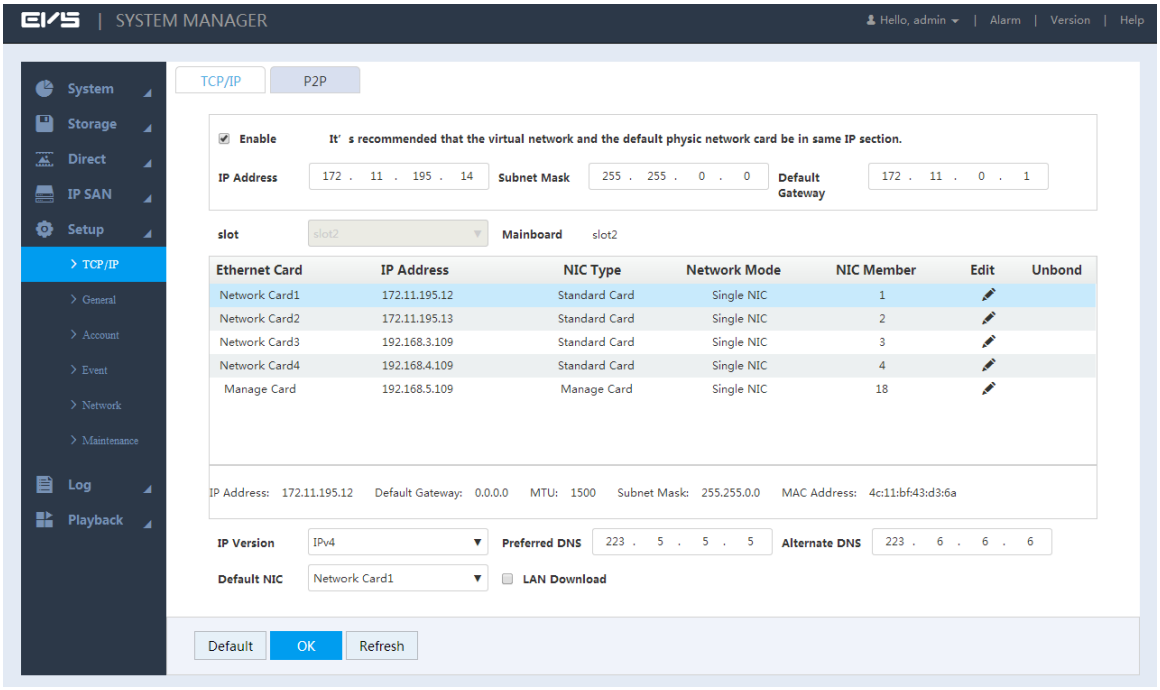


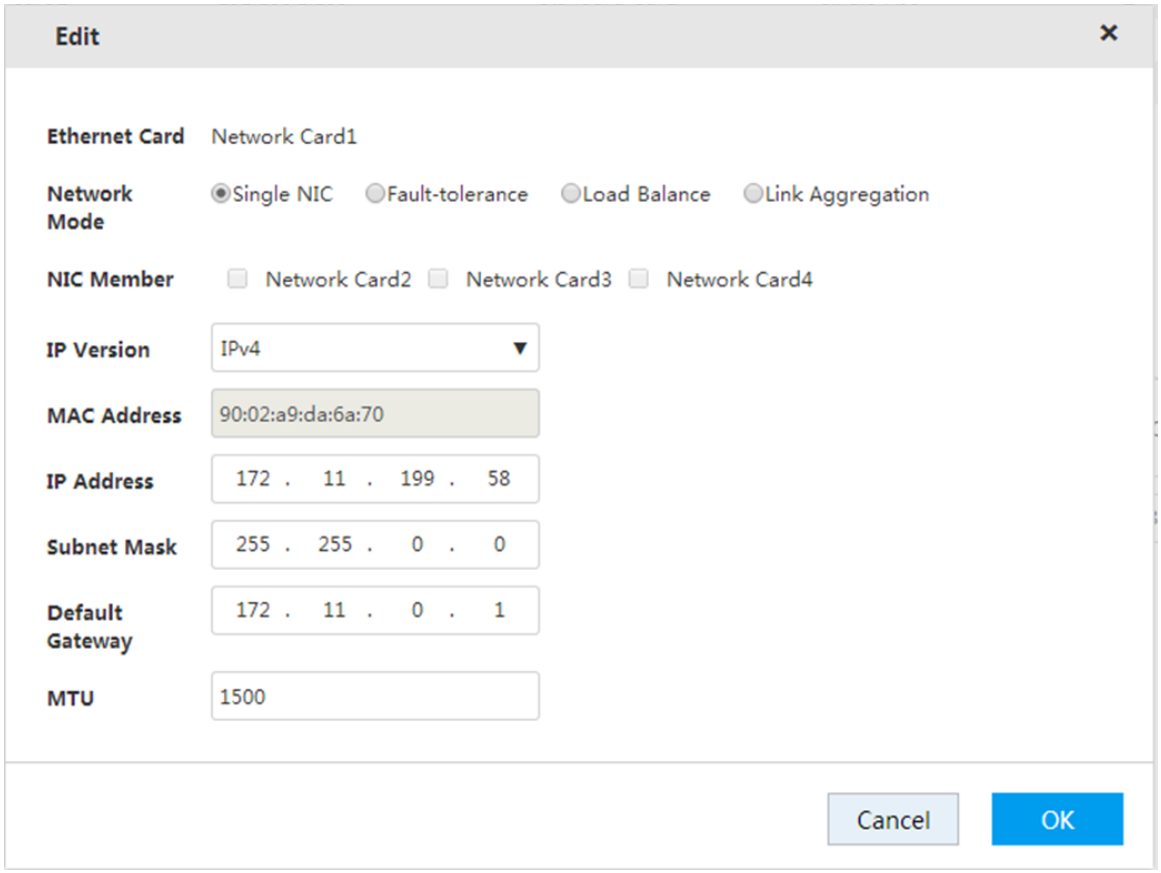
Table 3-2 Description of TCP/IP setting parameters

Parameter	Description
Enable	Enter the virtual IP address of the dual-control device. For details, see *User's Manual*. NOTE 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. NOTE Only dual-control device supports this function.
IP Version	Select the IP version, including IPv4 and IPv6 formats.
Preferred DNS	Enter the IP address of preferred DNS server.
Alternate DNS	Enter the IP address of alternate DNS server.
Default NIC	Select the default NIC of EVS device.
LAN Download	Select the check box. Under the condition of network bandwidth allowed, the LAN download speed is 1.5-2 times of the normal download speed.

Step 2 Click .

The **Edit** interface is displayed. See Figure 3-8.

Figure 3-8 Editing



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

Table 3-3 Description of NIC editing parameters

Parameter	Description
Ethernet Card	Display the current NIC name.

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

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

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

3.4.2 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.

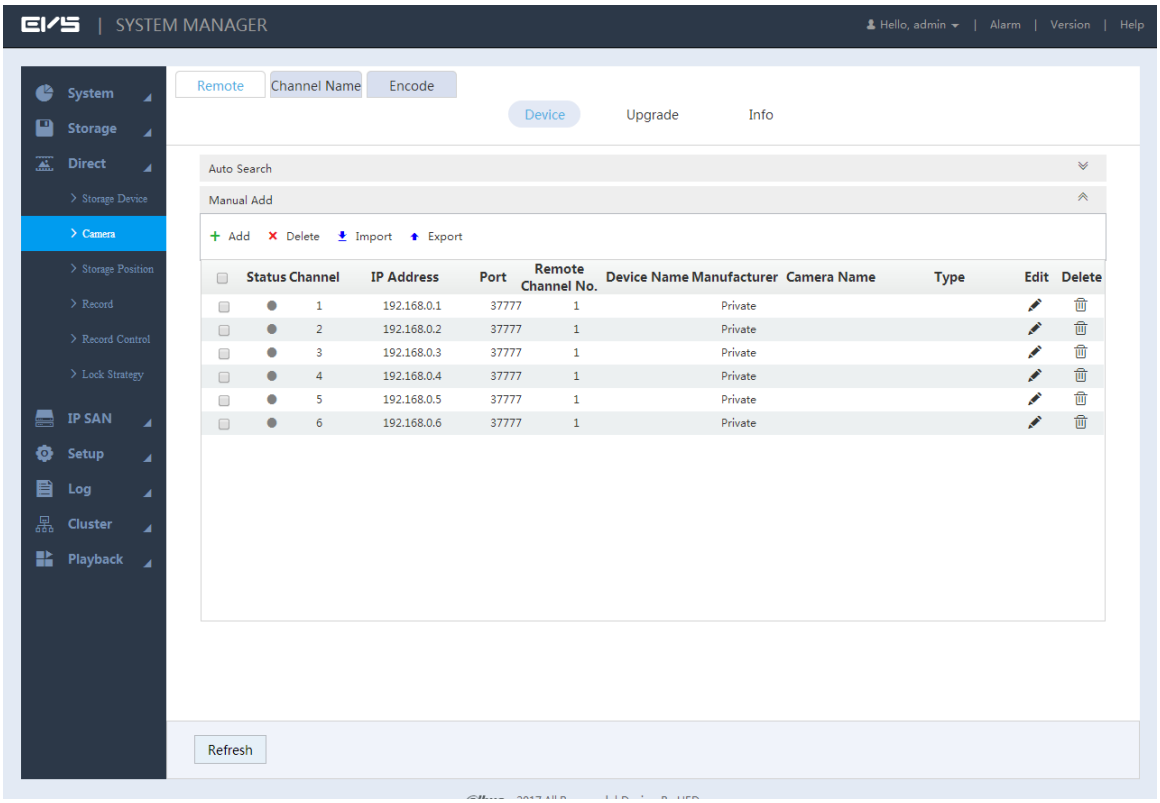
The system supports adding remote devices in three ways: searching add, single add and batch add.

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

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

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

Figure 3-9 Remote device



Step 2 Add remote device.

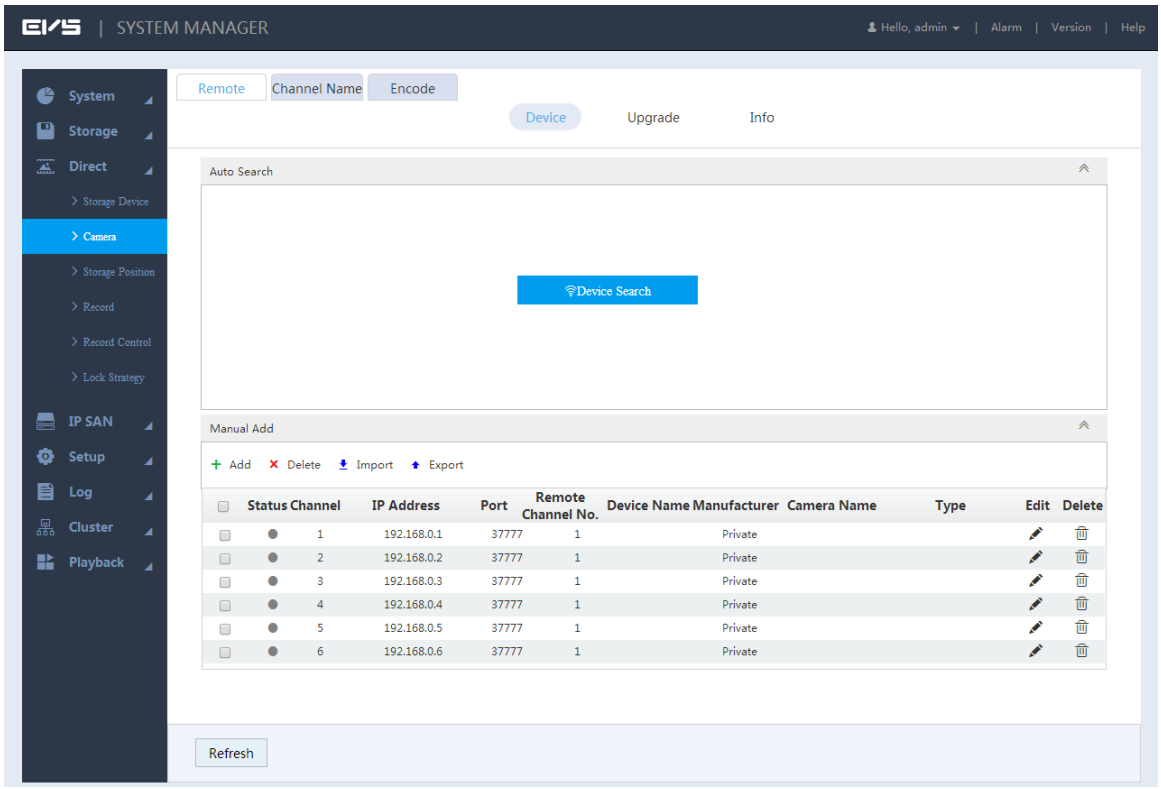
You can use searching add, single add or batch add.

- Searching add

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

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

Figure 3-10 Automatic search



2) Click **Device Search**.

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

NOTE

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

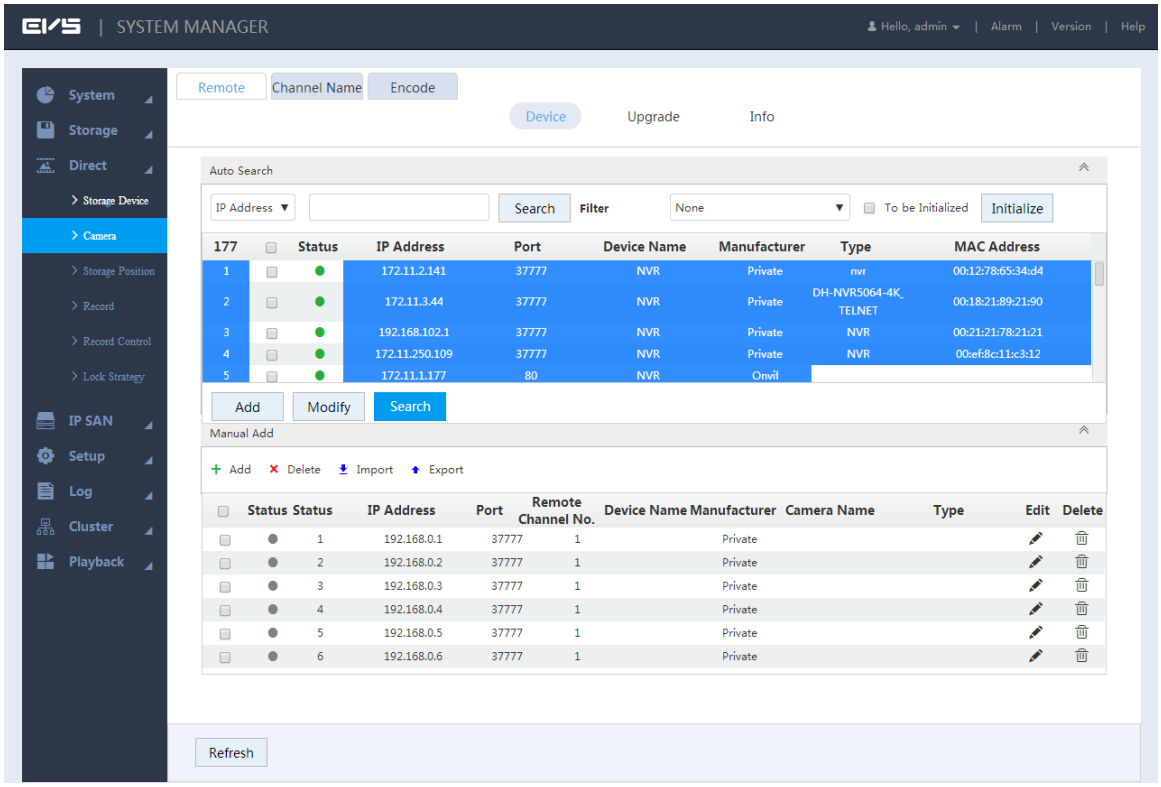


Table 3-4 Description of auto search icons

Icon/Parameter	Description
IP Address ▼	Screen out the remote devices you need to add through IP address or MAC address. Steps see below: 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 on the right 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. NOTE ● The IP address of the remote device can be modified only when the **Manufacturer** is **Private**. ● You can only modify one IP address at a time.
Search	Click this icon to search the remote devices again.

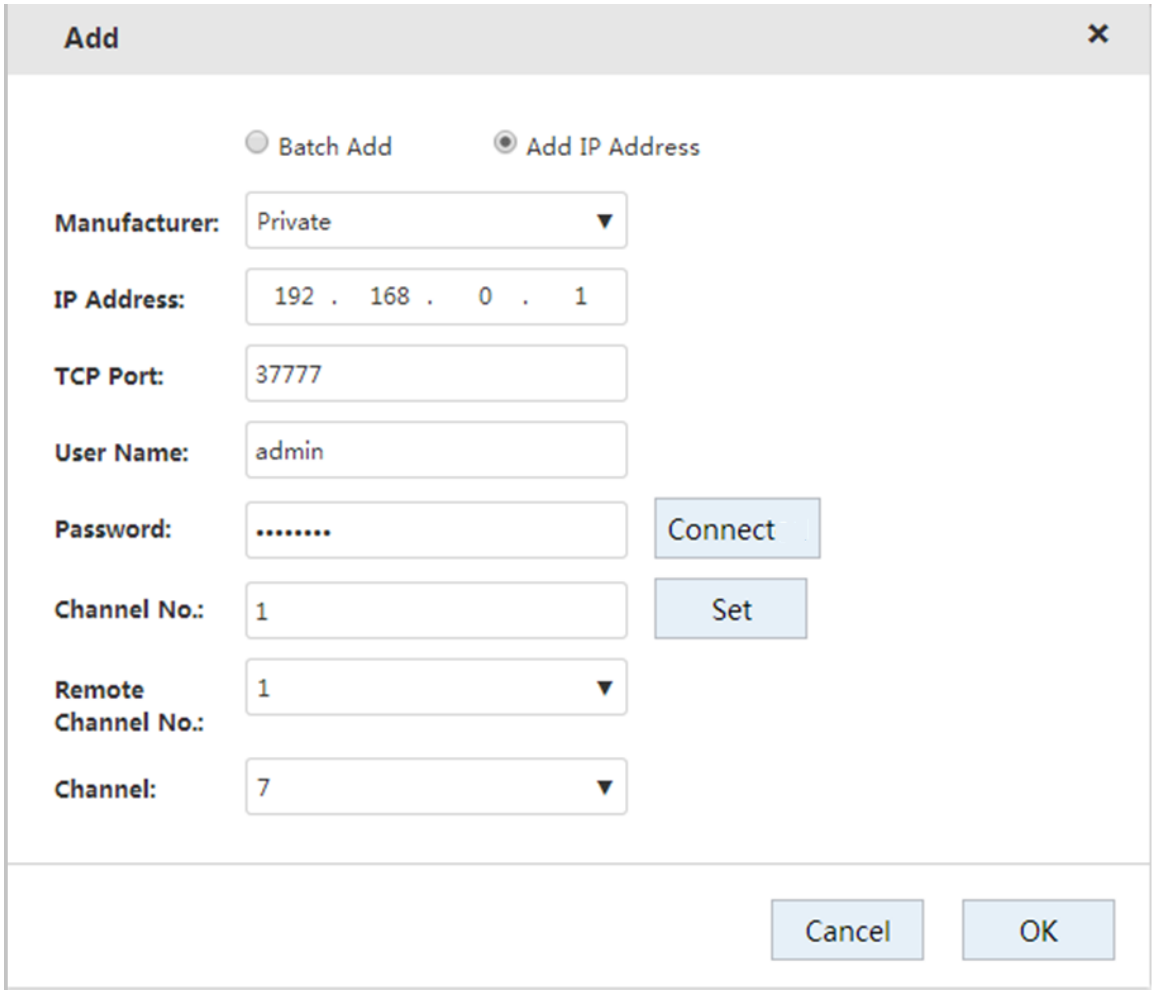
3) Double-click the remote device, or select the check box in front of the device and click **Add**, the system adds this remote device to the added list.

- Single add

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

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

Figure 3-12 Single add



2) Select/Enter the parameters. For details, see Table 3-5.

Table 3-5 Parameter description of adding

Parameter	Description
Manufacturer	Select the manufacturer in the drop-down box according to the actual situation. NOTE Different models support different manufacturer protocols. You need to refer to the actual situation.
IP Address	Set the IP address of the remote device.
TCP Port	Provides services with TCP protocol. You can set according to actual needs. The default is 37777. NOTE You neet to set it when the **Manufacturer** is set to **Private**.
RTSP Port	Set the RTSP port No. of the remote device. The default is 554. NOTE You do not need to configure it when the **Manufacturer** is set to **Private** or **Custom**.
HTTP Port	Set the HTTP port of the remote device. The default is 80. NOTE You do not need to configure it when the **Manufacturer** is set to **Private** or **Custom**.

Parameter	Description
User Name/Password	Enter the user name and password to log in the remote device.
Channel No.	Enter the **Channel No.** or click **Connect** to get the total channel number of the front-end device. NOTE It is recommended to obtain the channel number of the front-end device by clicking **Connect**. If the total number of channels entered does not 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.
Service Type	Set the corresponding service type of the remote device. NOTE ● Different manufacturers support different service types. See the actual interface. ● When the remote device is connected through private protocol, the default connection type is TCP.

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

- Batch add

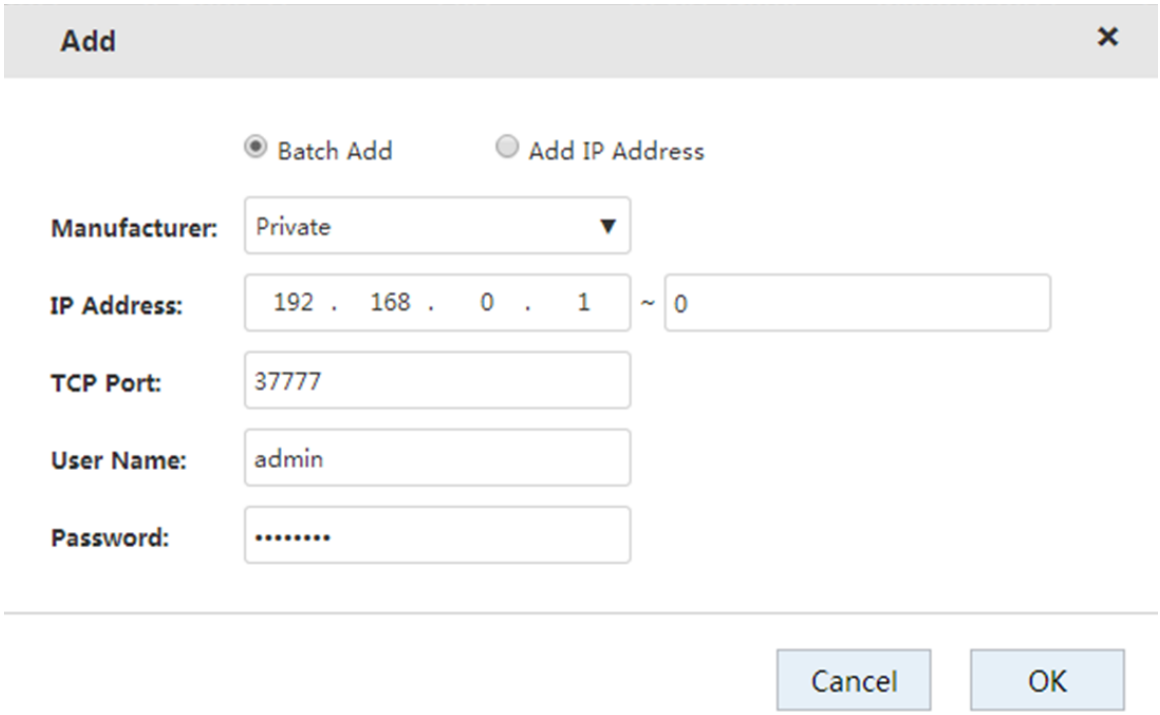
NOTE

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

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

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

Figure 3-13 Batch add



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

NOTE

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

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

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

- Template Import

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

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

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

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

CAUTION

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

3) Click to select template file.

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

NOTE

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

3.4.3 Record Plan Settings

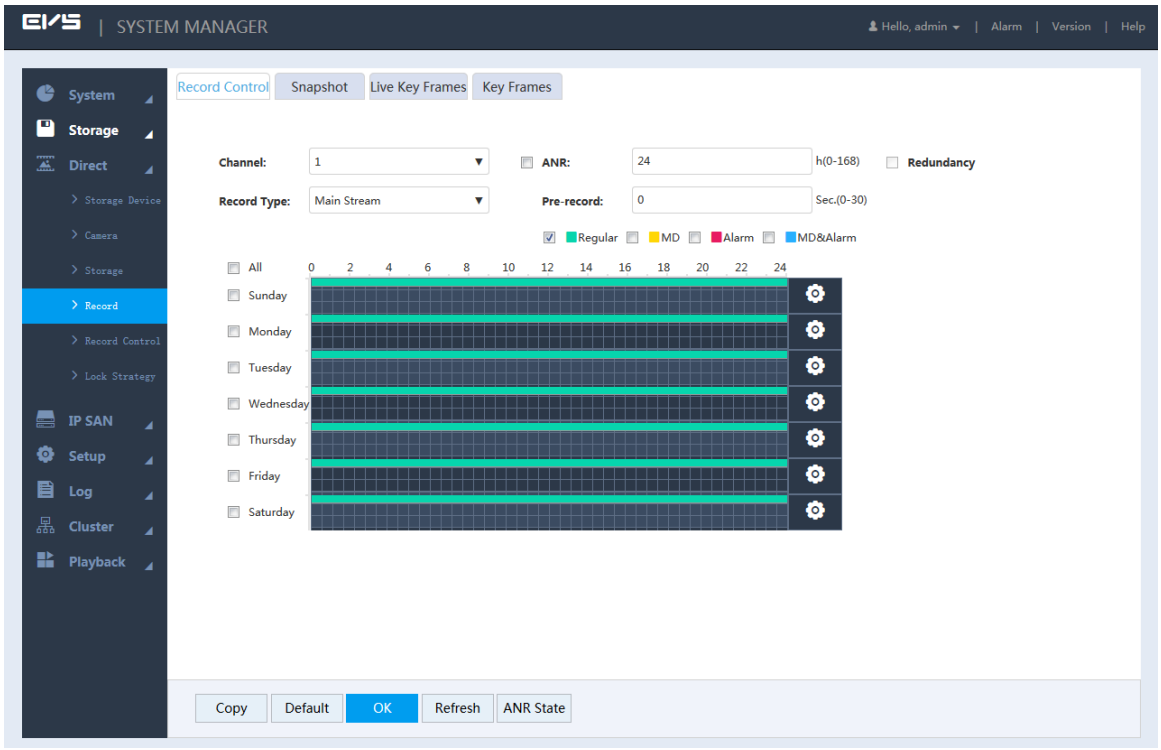
The system performs the corresponding video recording according to the set record plan. For example, when you set the time period of alarm videos to 6:00-18:00, the system automatically takes records if any alarm occurs during this period.

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

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

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

Figure 3-14 Record plan



Step 2 Select/Enter the parameters. For details, see Table 3-6.

Table 3-6 Description of record parameters

Parameter	Description
Channel	Select the channel number. You can set different plans for different channels. Select the **All** check box if you want to perform the same settings for all the channels.
ANR	Select the check box to enable the function. ● When the network connection between the EVS device and IPC is broken, IPC keeps on recording. After the network recovery, the EVS device downloads the records during the disconnection period from IPC, so as to keep the record integrity. ● Enter the max record upload time period in the text box. If the time of network outage is longer than the set period, the system only uploads the records during the set time period. NOTE This function is available for IPC that has installed the SD card.

Parameter	Description
Redundancy	When multiple disks are available in the EVS device, select one disk to be the redundancy to realize the double backup of records. The records are stored in different disks at the same time to guarantee the data security. 1. 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. NOTE The recording in the redundant disk corresponds to a backup of recording in the read-write disk. Images are not backed up.
Record Type	Select the record type, including main stream and sub stream.
Pre-record	Start to record 0-30 seconds (according to the stream size and status) before the preset action.

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

Figure 3-15 Alarm type

NOTE

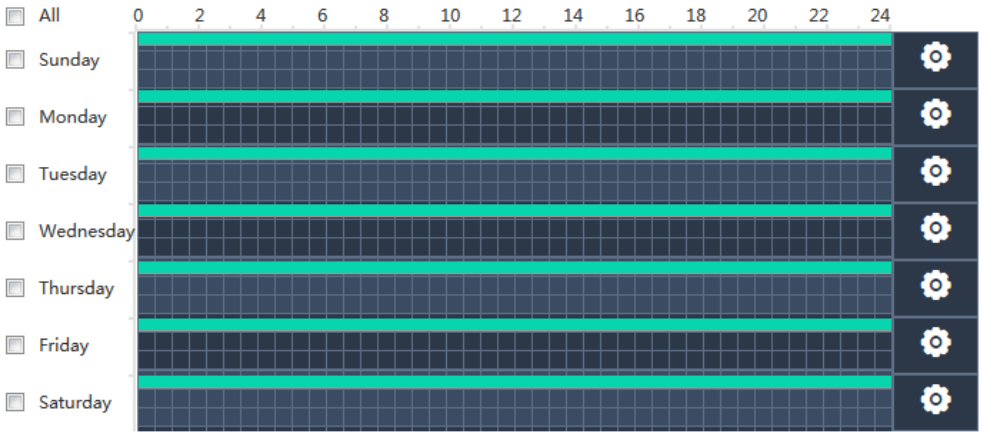
- When you select the **MD**, **Alarm** or **MD & Alarm**, you need to enable the alarm record linkage for the corresponding channel. For details, see *User's Manual*.
- The color bar in Figure 3-16 indicates the record type of the corresponding time period.

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

NOTE

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. EVS device performs recording in the corresponding period.

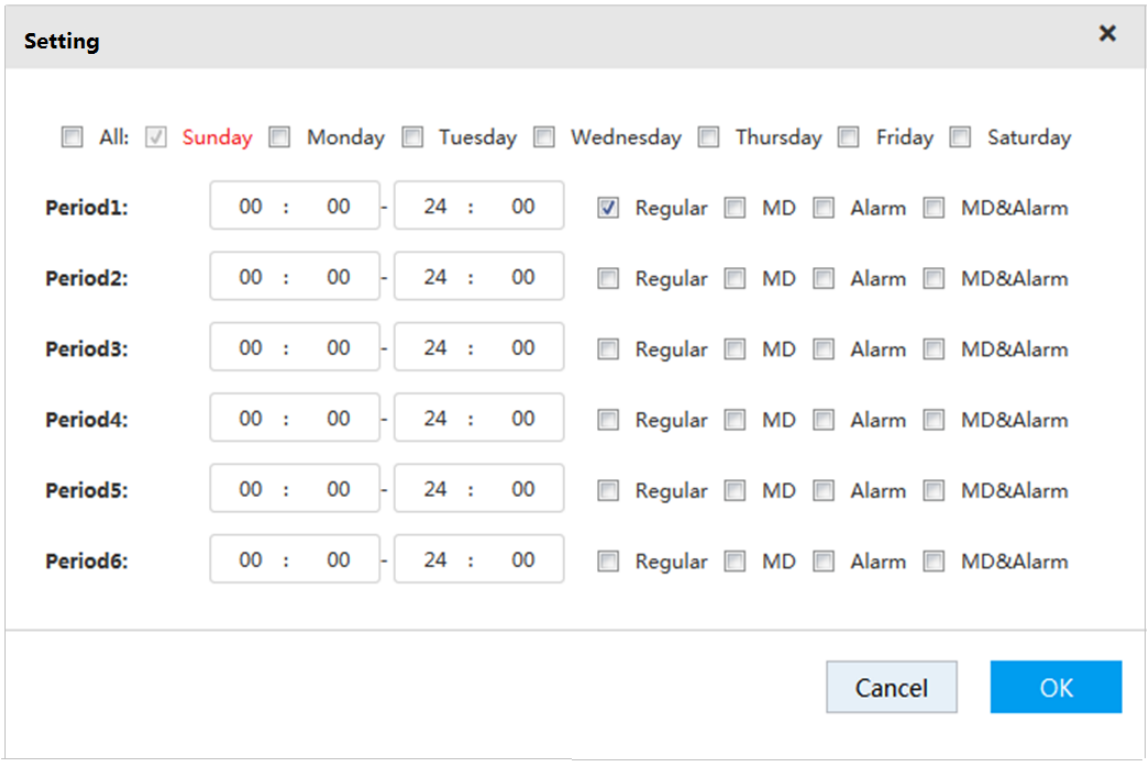
◇ When the record time is overlapped, see following for the record priority: MD & alarm > alarm > MD > regular.

- Editing:

1) Select the corresponding weekday and click .

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

Figure 3-17 Period setting



2) Select the weekday, record type and period.

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

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

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

NOTE

The record plan comes into effect after enabling the auto record function. For details to 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 streams.

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

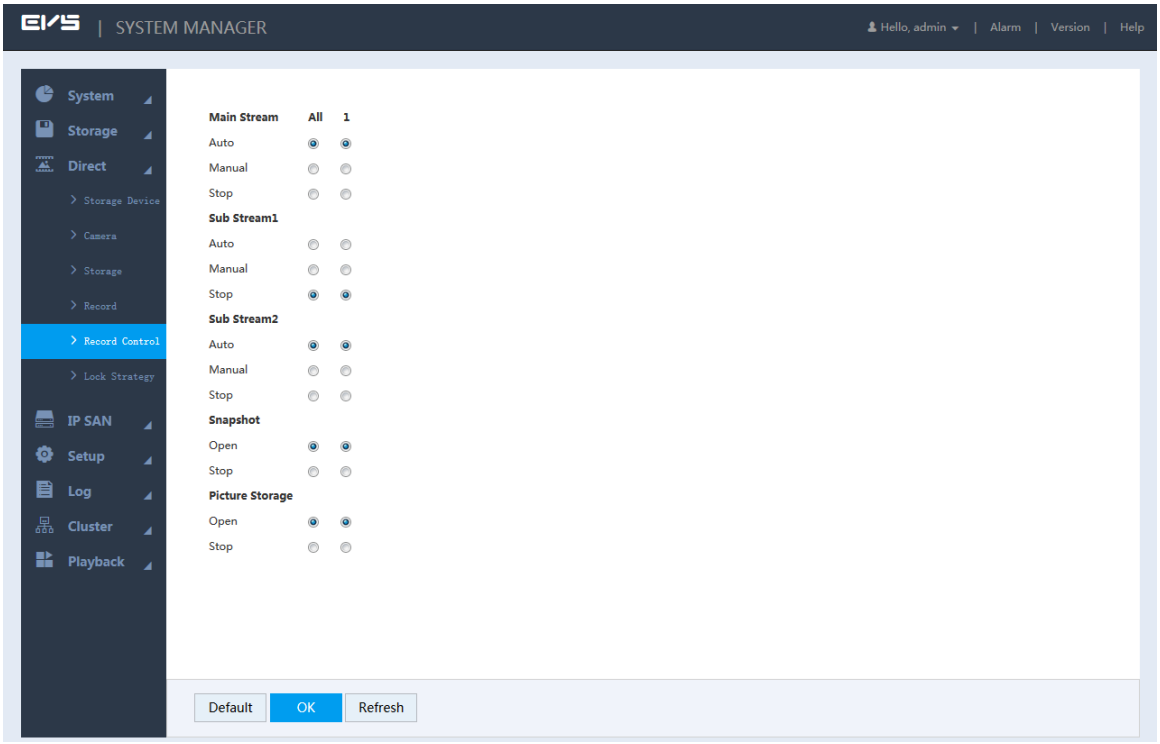
CAUTION

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

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

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

Figure 3-18 Record control



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

Table 3-7 Description of record control parameters

Parameter	Description
Channel	Display all the channels with remote devices added. You can select a single channel or multiple channels or select **All** for all the channels.
Status	Display the current status of the corresponding channel. ● : Not selected. ● : Selected.
Main Stream	Select the record mode of the main stream and sub streams, including manual, auto and stop. ● Manual: Highest priority. In spite of the current channel status, all the

Parameter	Description
Sub Stream	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 Record Plan Settings." ● Stop: All the channels stop recording.
Snapshot	Select single or multiple channels and open/close the snapshot of the corresponding channel.
Picture Storage	Select single or multiple channels and open/close the image direct storage in the corresponding channel.

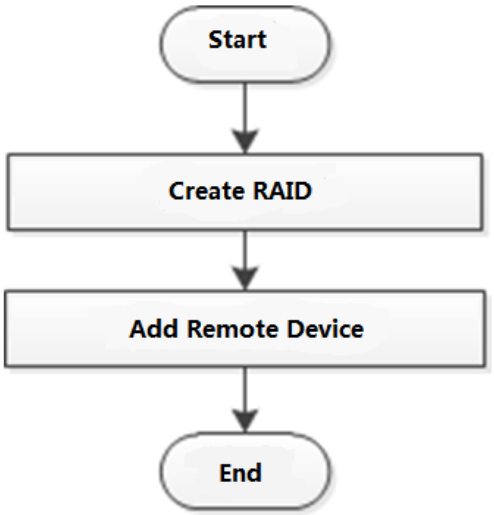
Step 3 Click **OK** to save the configuration.

3.5 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



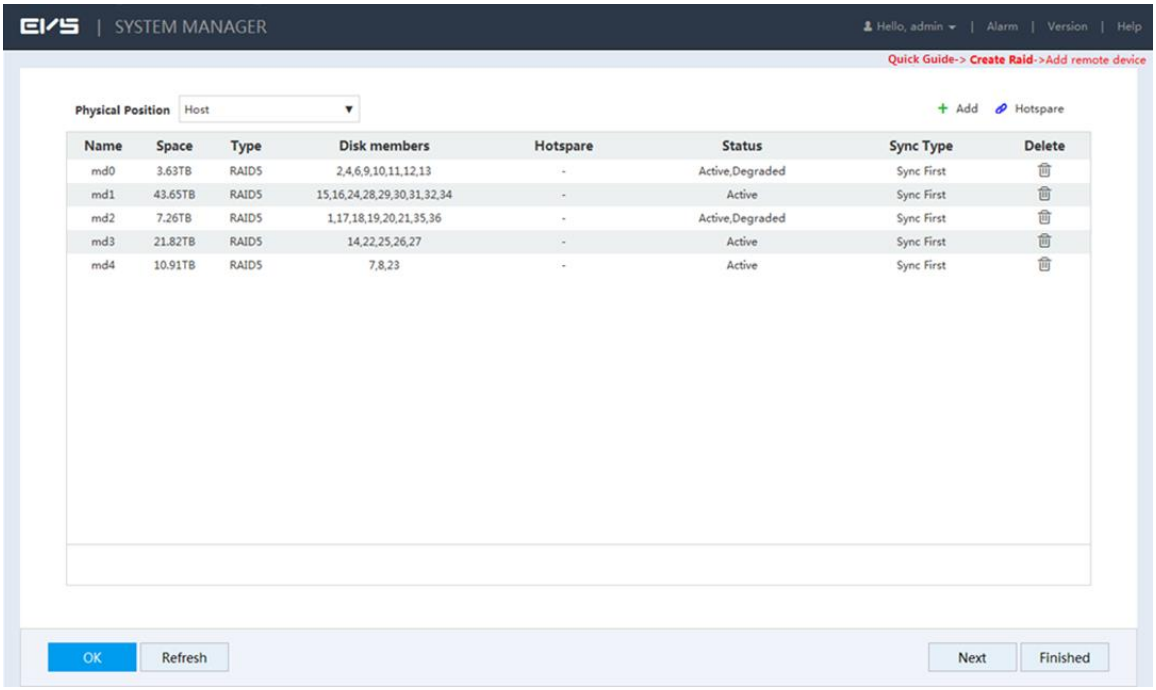
Step 1 Click on the right side of the user name. Select **Quick Guide** > **Video Direct Storage**.

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

NOTE

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

Figure 3-20 RAID management

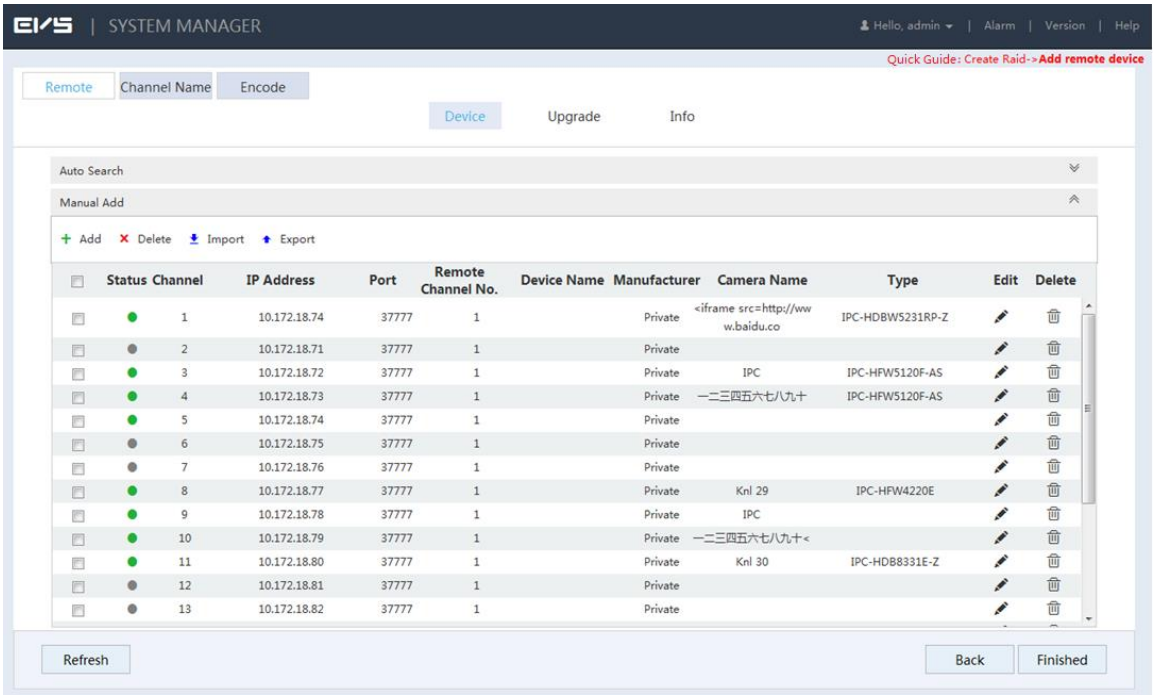


Step 2 Create RAID. For details, see "3.8.1 Creating RAID"

Step 3 Click **Next**.

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

Figure 3-21 Registering remote device



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

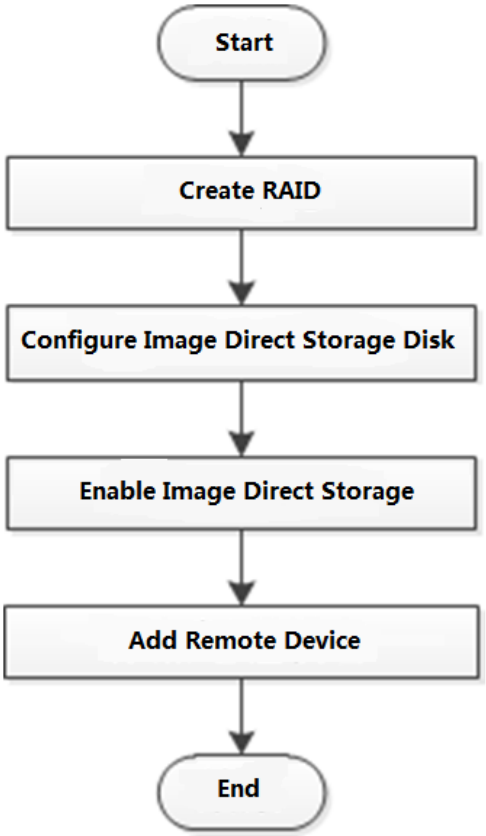
Step 5 Click **Finished** to save the configuration.

3.6 Image Direct Storage

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

For the procedure to configure image direct storage, see Figure 3-22.

Figure 3-22 Image direct storage



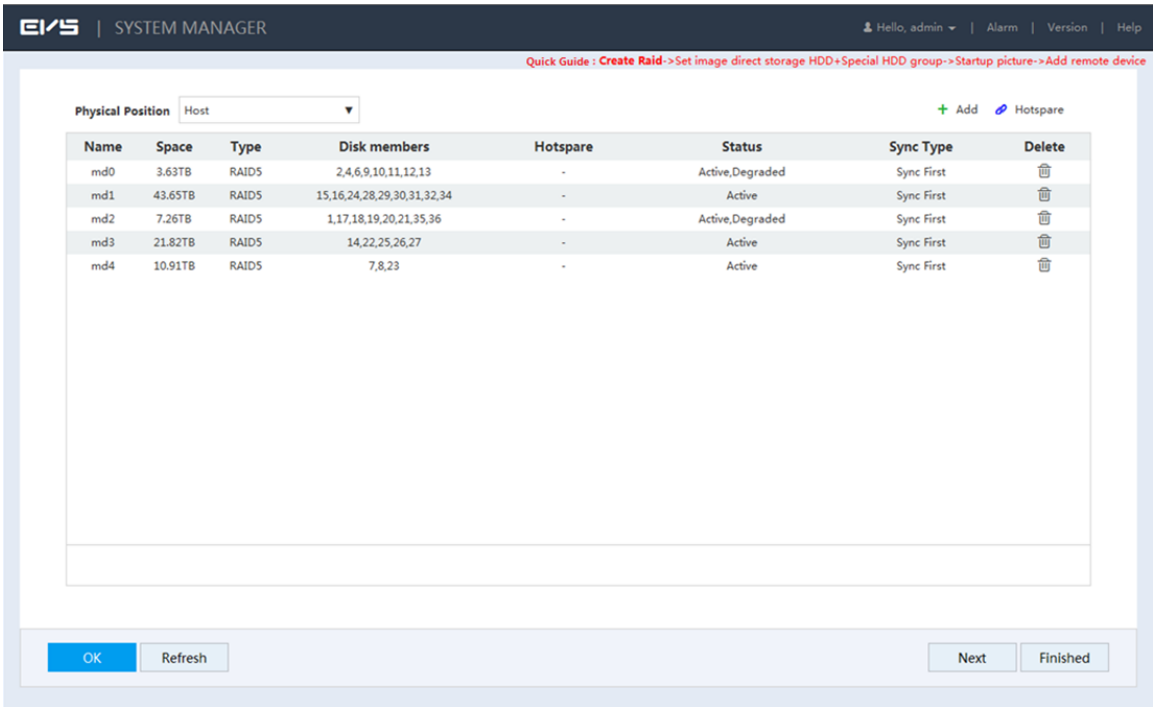
Step 1 Click on the right side of the user name. Select **Quick Guide** > **Image Direct Storage**.

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

NOTE

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

Figure 3-23 RAID management

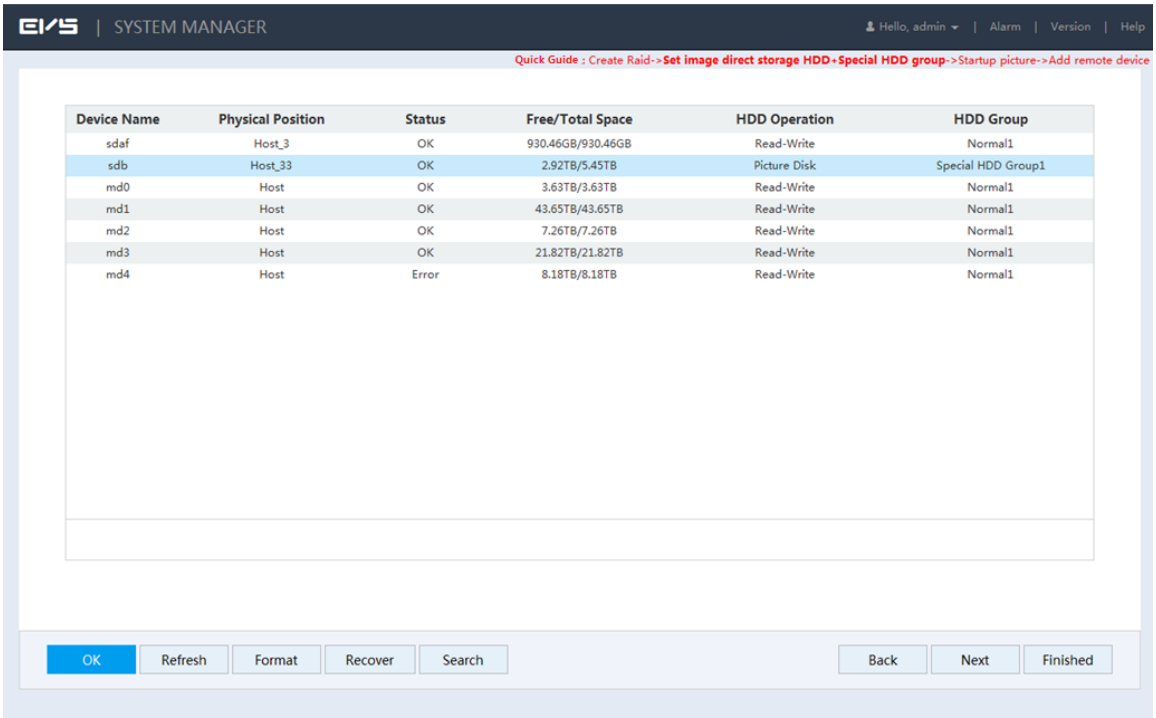


Step 2 Create RAID. For details, see "3.8.1 Creating RAID"

Step 3 Click **Next**.

The **Set image direct storage HDD + Special HDD group** interface is displayed. See Figure 3-24.

Figure 3-24 Setting image direct storage HDD and special HDD group



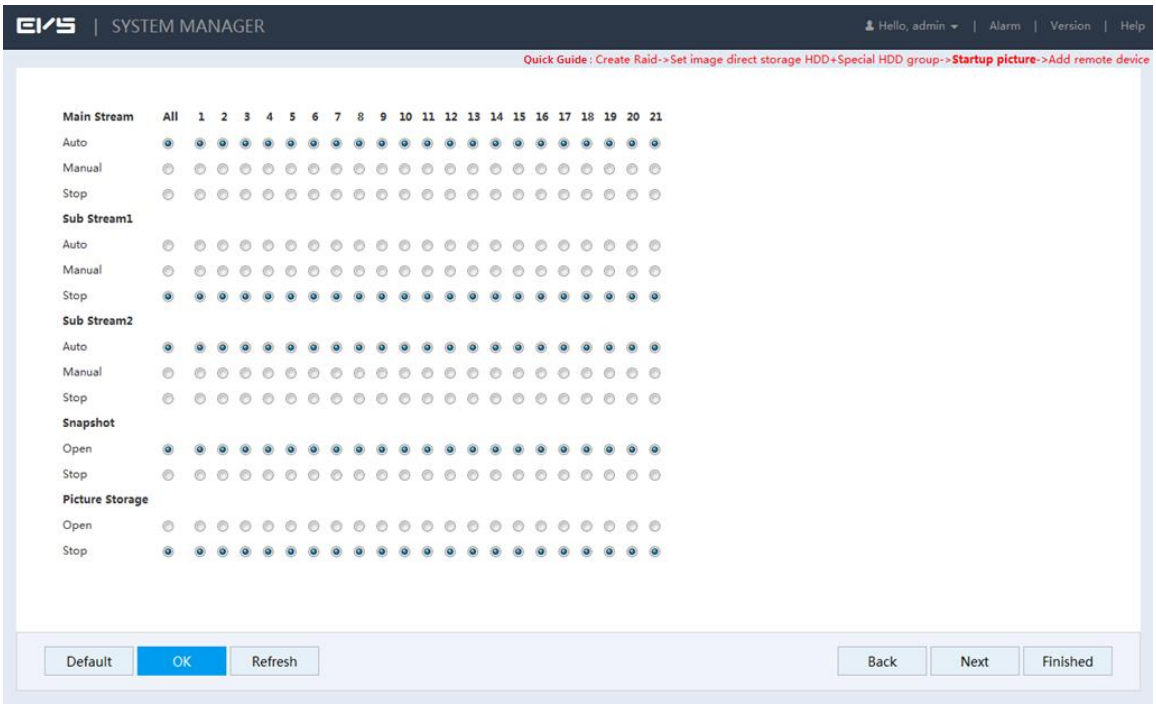
Step 4 Set the image direct storage HDD and HDD group.

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

Step 5 Click **Next**.

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

Figure 3-25 Picture startup

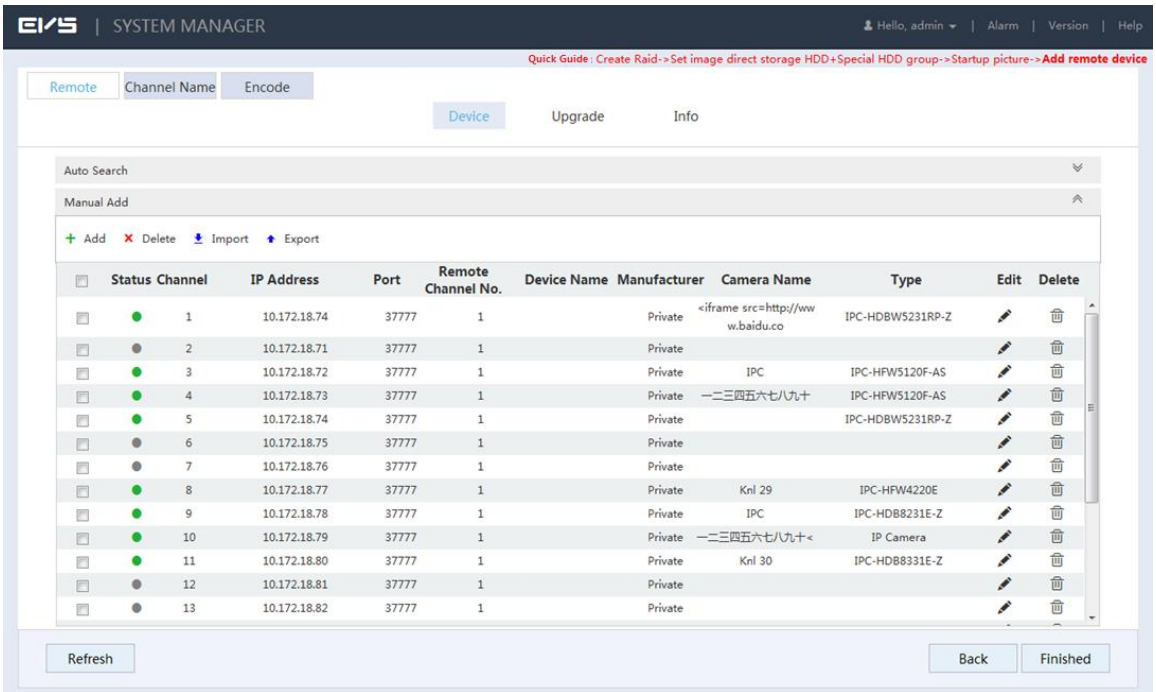


Step 6 Enable the **Picture Storage** of the channels and click **OK** to save the configuration.

Step 7 Click **Next**.

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

Figure 3-26 Registering remote device



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

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

NOTE

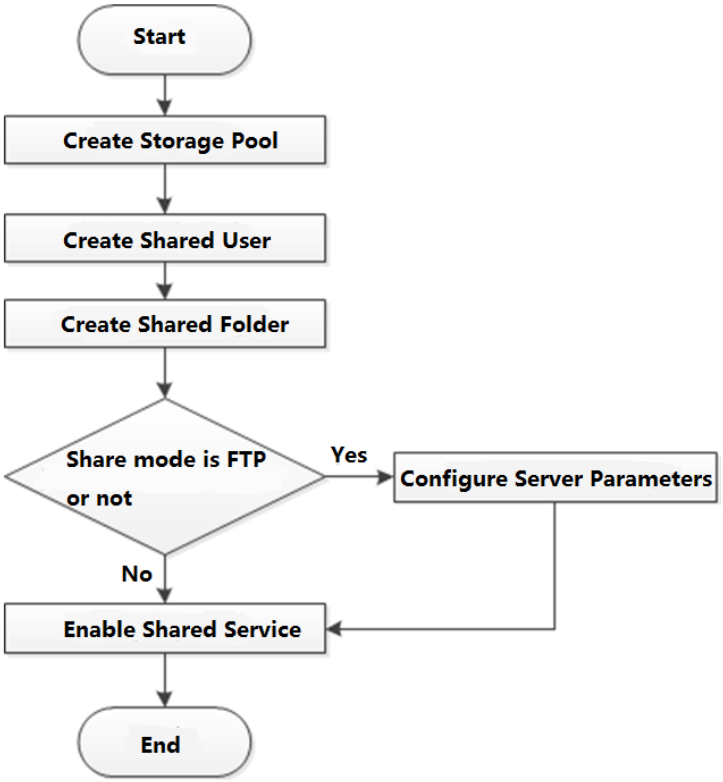
After the configuration, you can search the direct stored images. For details, see *User's Manual*.

3.7 IPSAN

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

For the procedure to configure IPSAN, see Figure 3-27.

Figure 3-27 Configuring IPSAN



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.

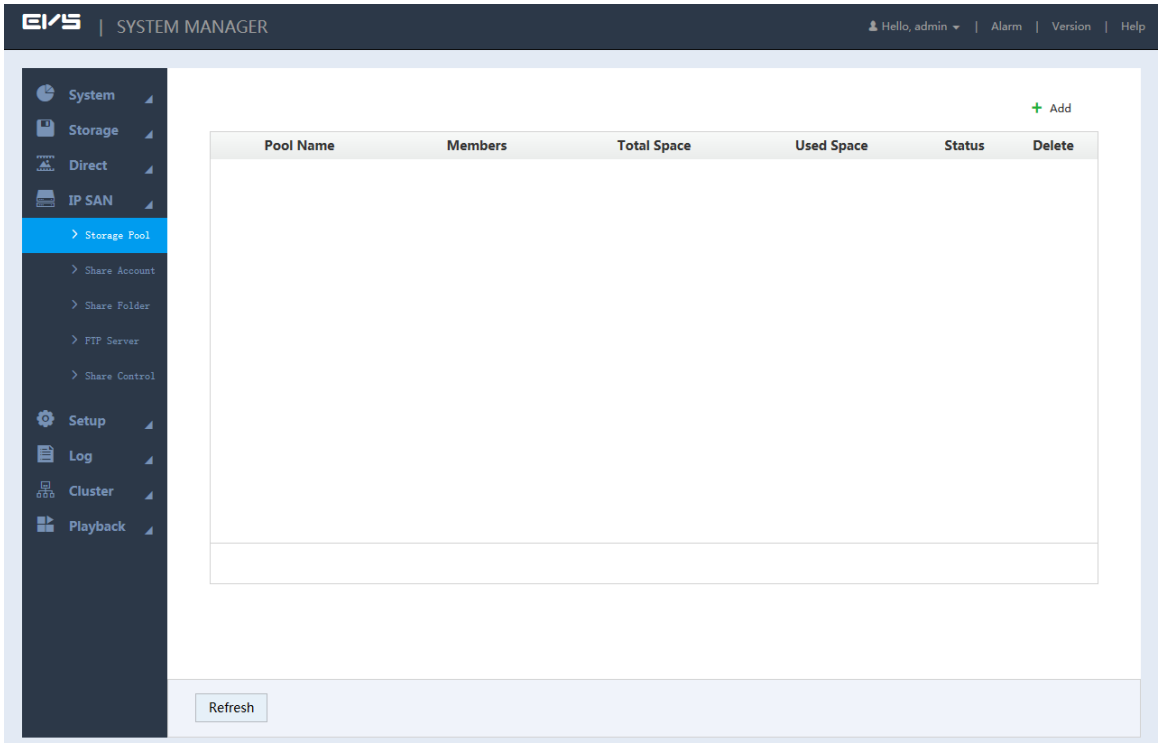
CAUTION

When creating the storage pool, the system will format the selected disk. Be careful to perform it.

Step 1 Select **IPSAN** > **Storage Pool**.

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

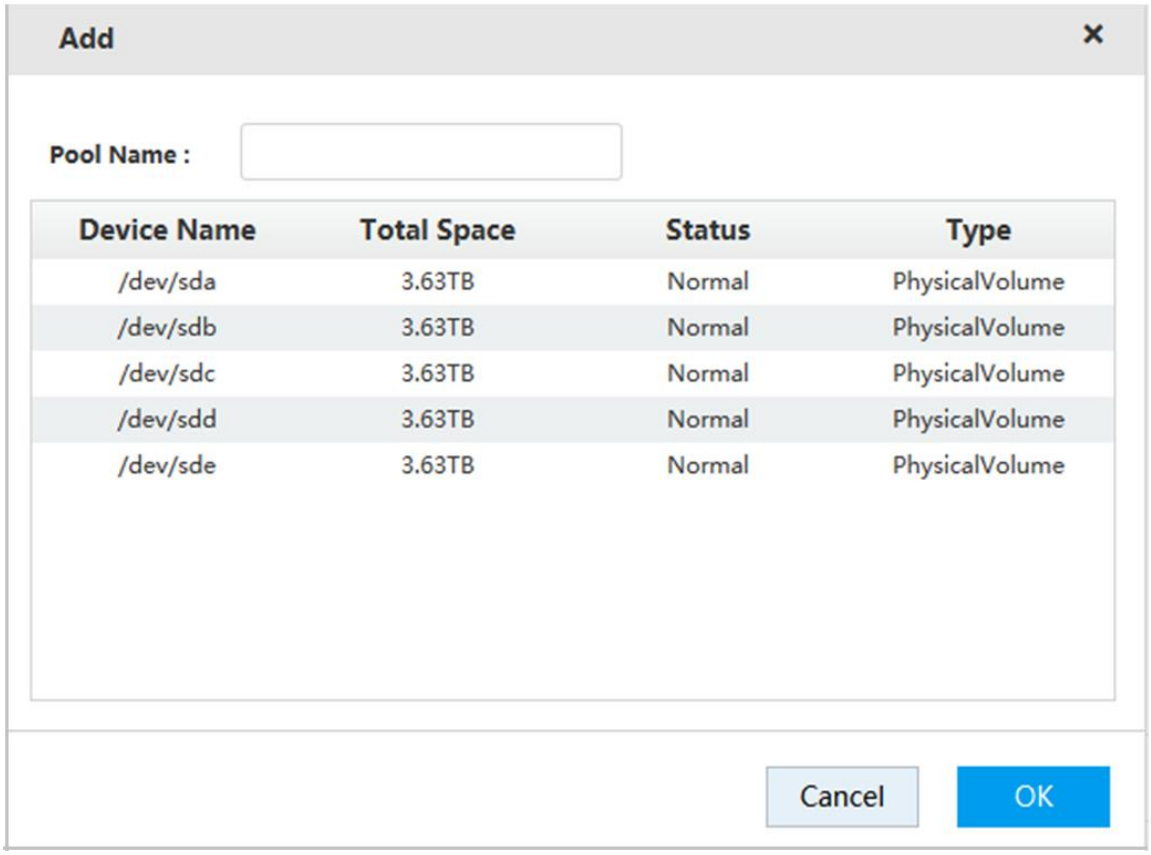
Figure 3-28 Storage pool



Step 2 Click + .

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

Figure 3-29 Adding storage pool



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

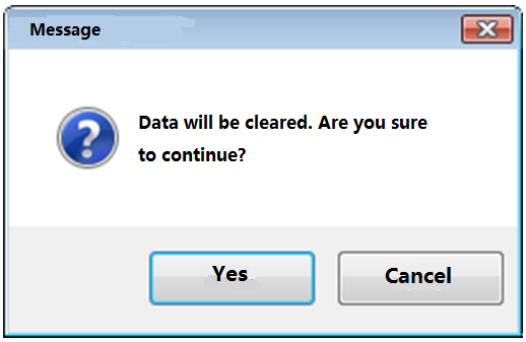
NOTE

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. See Figure 3-30.

Figure 3-30 Prompt



Step 5 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.

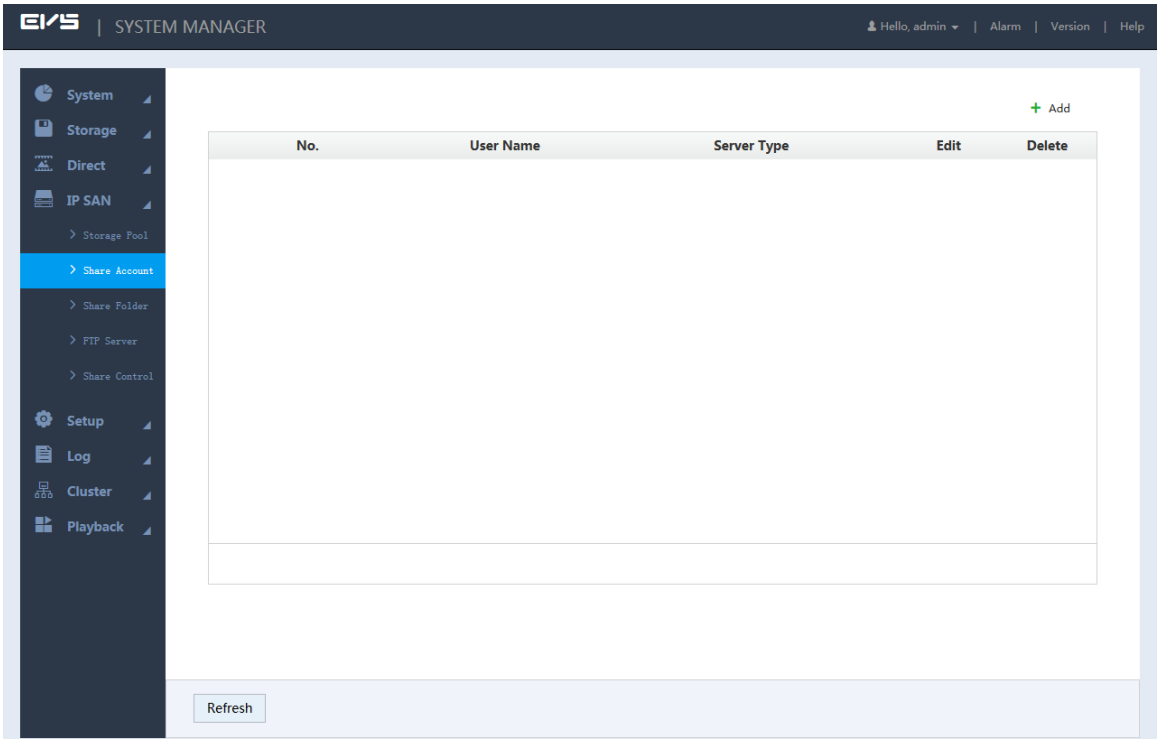
3.7.2 Shared Account Management

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

Step 1 Select **IPSAN** > **Shared Account**.

The **Shared Account** interface is displayed. See Figure 3-31.

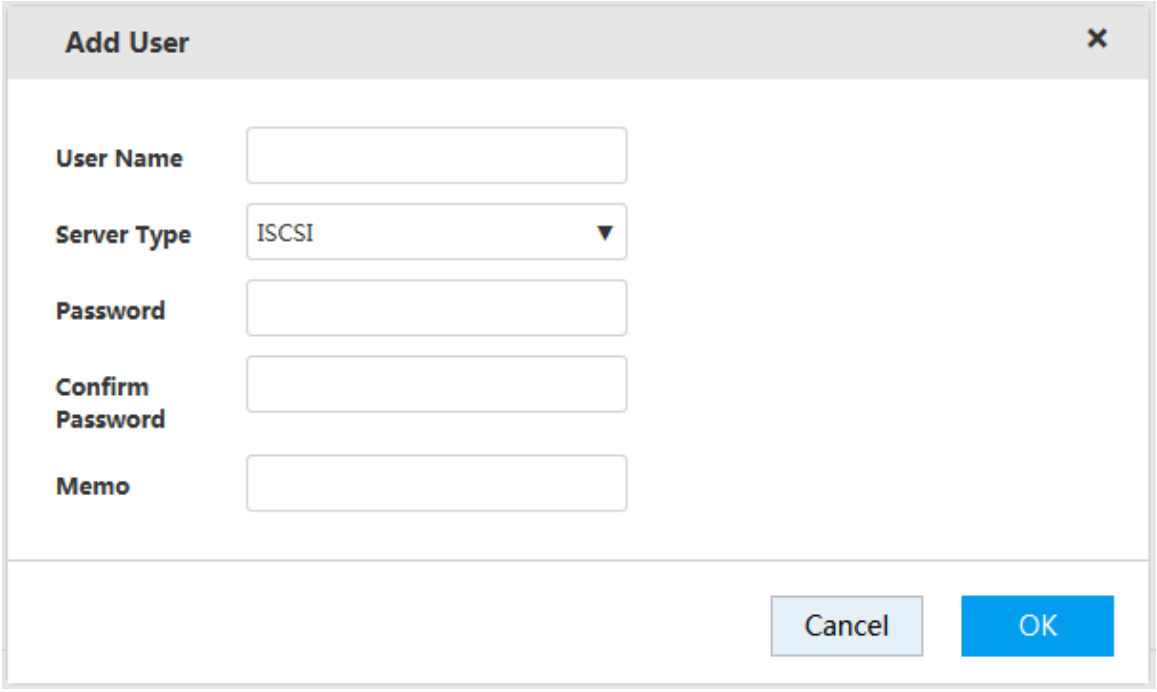
Figure 3-31 Shared account management



Step 2 Click + .

The **Add User** interface is displayed. See Figure 3-32.

Figure 3-32 Adding shared user



Step 3 Select/Enter the parameters. For details, see Table 3-8.

Table 3-8 Description of adding user parameters

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

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

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

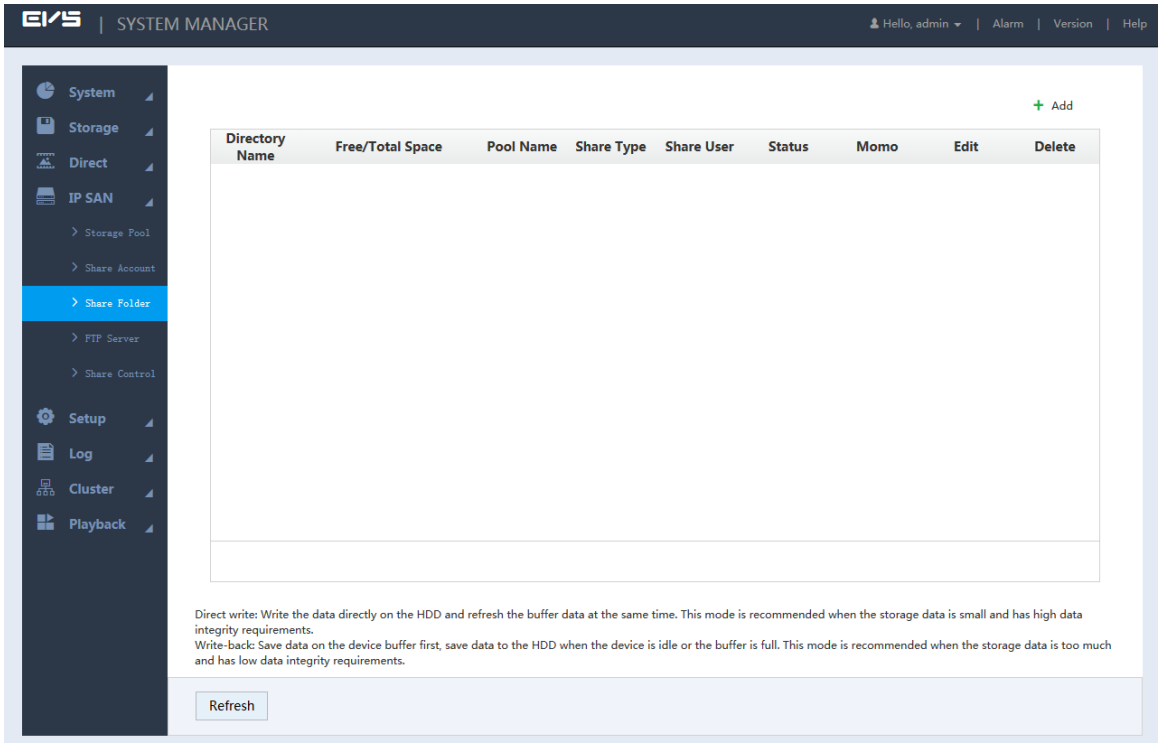
3.7.3 Shared Folder Settings

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

Step 1 Select **IPSAN** > **Shared Folder**.

The **Shared Folder** interface is displayed. See Figure 3-33.

Figure 3-33 Shared folder



Step 2 Click + .

The Add interface is displayed. See Figure 3-34 or Figure 3-35.

Figure 3-34 Adding shared folder (NFS)

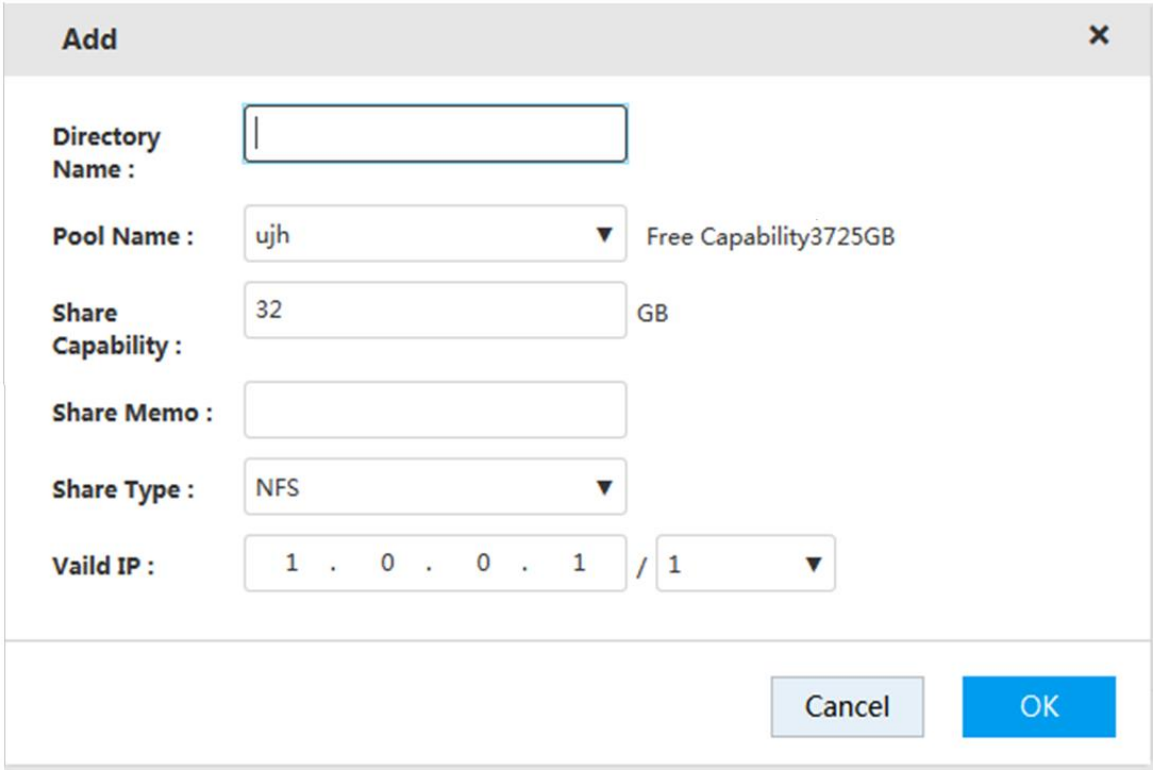
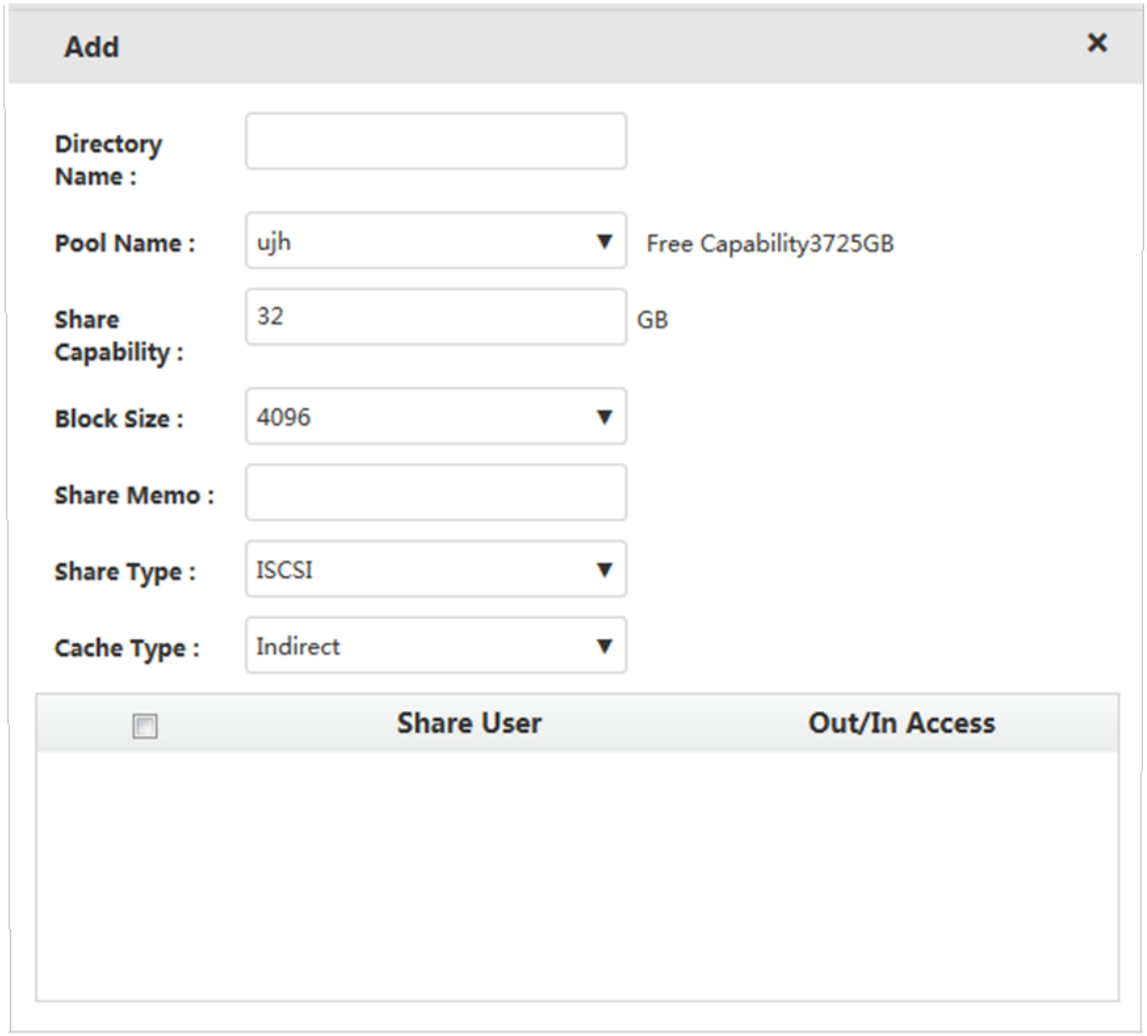


Figure 3-35 Adding shared folder (iSCSI)



Step 3 Select/Enter the parameters. For details, see Table 3-9.

Table 3-9 Description of shared folder parameters

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

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

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

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

NOTE

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

3.7.4 FTP Parameter Settings

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

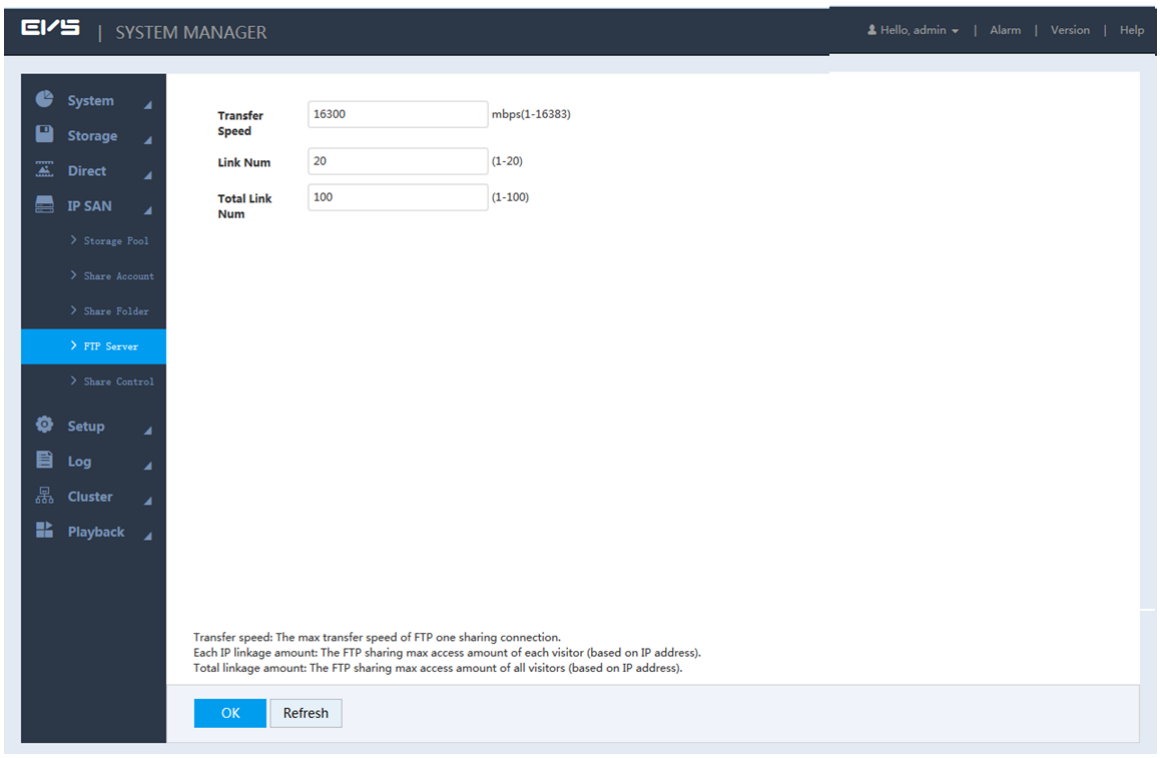
NOTE

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

Step 1 Select **IPSAN** > **FTP Server**.

The **FTP Server** interface is displayed. See Figure 3-36.

Figure 3-36 FTP Parameters



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

Table 3-10 Description of FTP server parameters

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

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

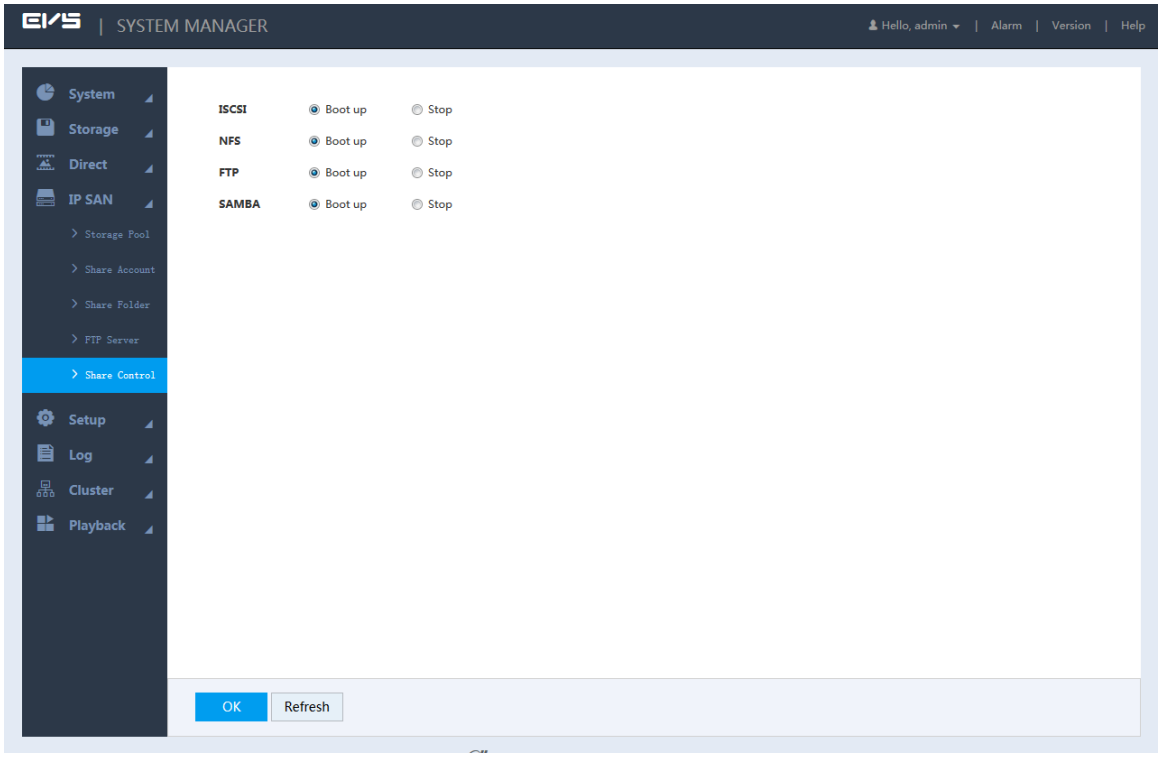
3.7.5 Opening Shared Services

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

Step 1 Select **IPSAN** > **Share Control**.

The **Share Control** interface is displayed. See Figure 3-37.

Figure 3-37 Share control



Step 2 Boot up or stop the shared 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.

NOTE

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

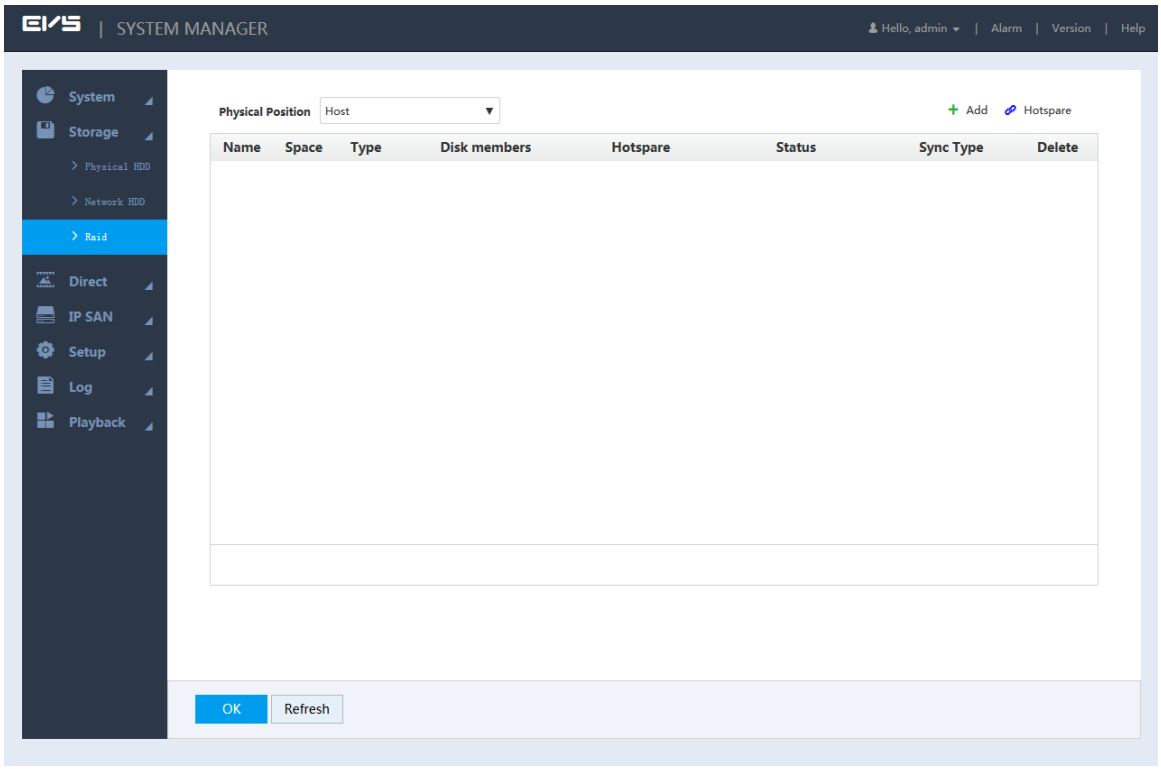
CAUTION

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

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

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

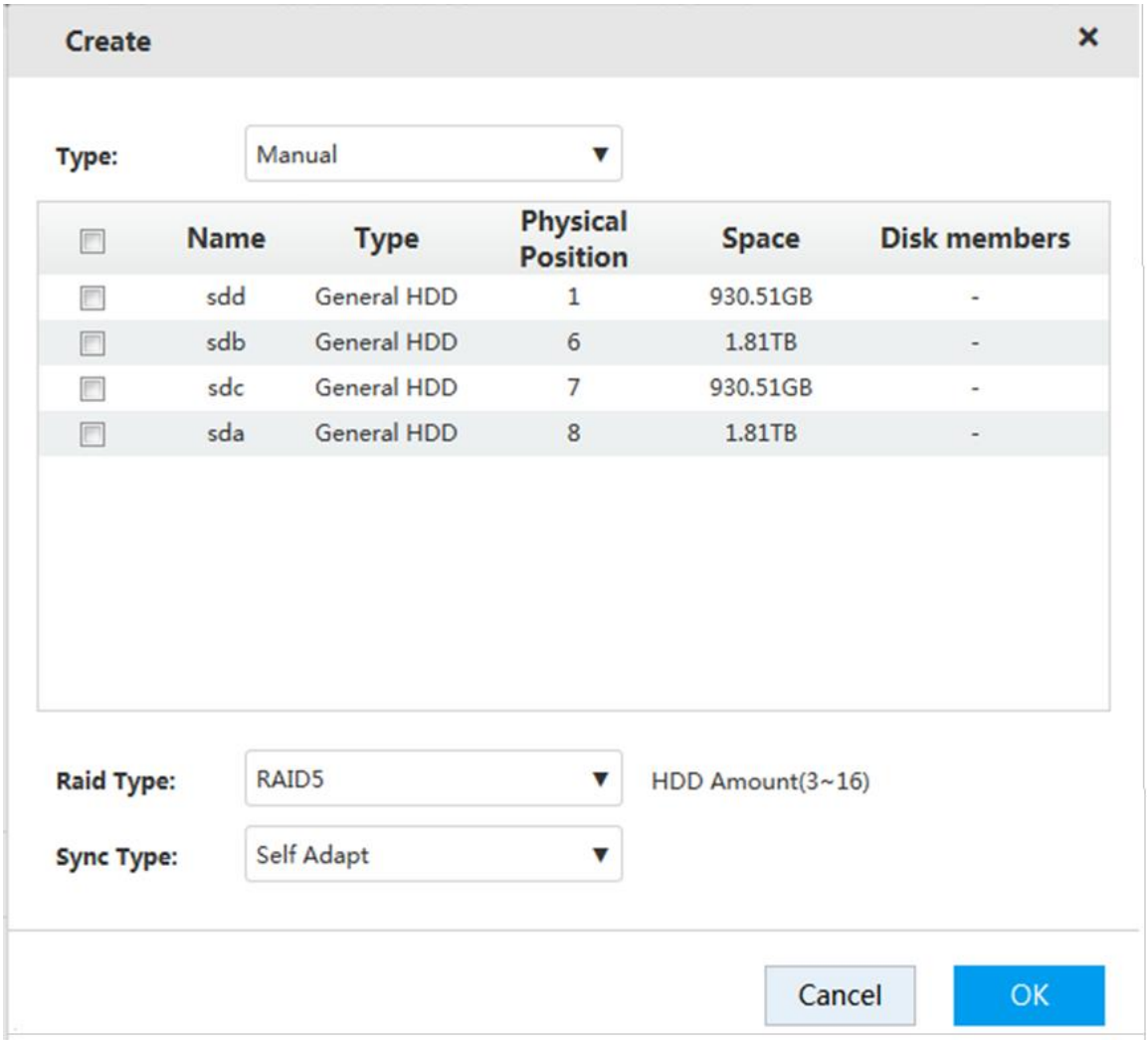
Figure 3-38 Raid management



Step 2 Click + .

The **Create** interface is displayed. See Figure 3-39.

Figure 3-39 Creating RAID



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

Table 3-11 Description of RAID creation parameters

Parameter	Description
Type	Select the RAID creation type, including manual and one-click. NOTE When you choose the one-click RAID creation, the system automatically creates RAID 5 according to the one-click RAID creation strategy. For details, see Table 3-12.
HDD	Select the HDD you want to use to create RAID. NOTE Different RADI type needs different number of disks. See the actual situation.
Raid Type	Select the RAID type you want to create.

Parameter	Description
Sync Type	Select the sync mode of the business resources allocation. ● Self-adaption: Automatically adjust the RAID sync speed according to the current business loads. NOTE When there is no external business, sync is performed at a high speed. When there is external business, sync is performed at a low speed. ● Sync priority: Resource priority is assigned to RAID sync. ● Business priority: Resource priority is assigned to business operations. ● Balance: Resource is evenly distributed to RAID sync and business operations.

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

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

NOTE

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

One-Click RAID Creation Strategy

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

NOTE

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

Table 3-12 One-click RAID creation strategy

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

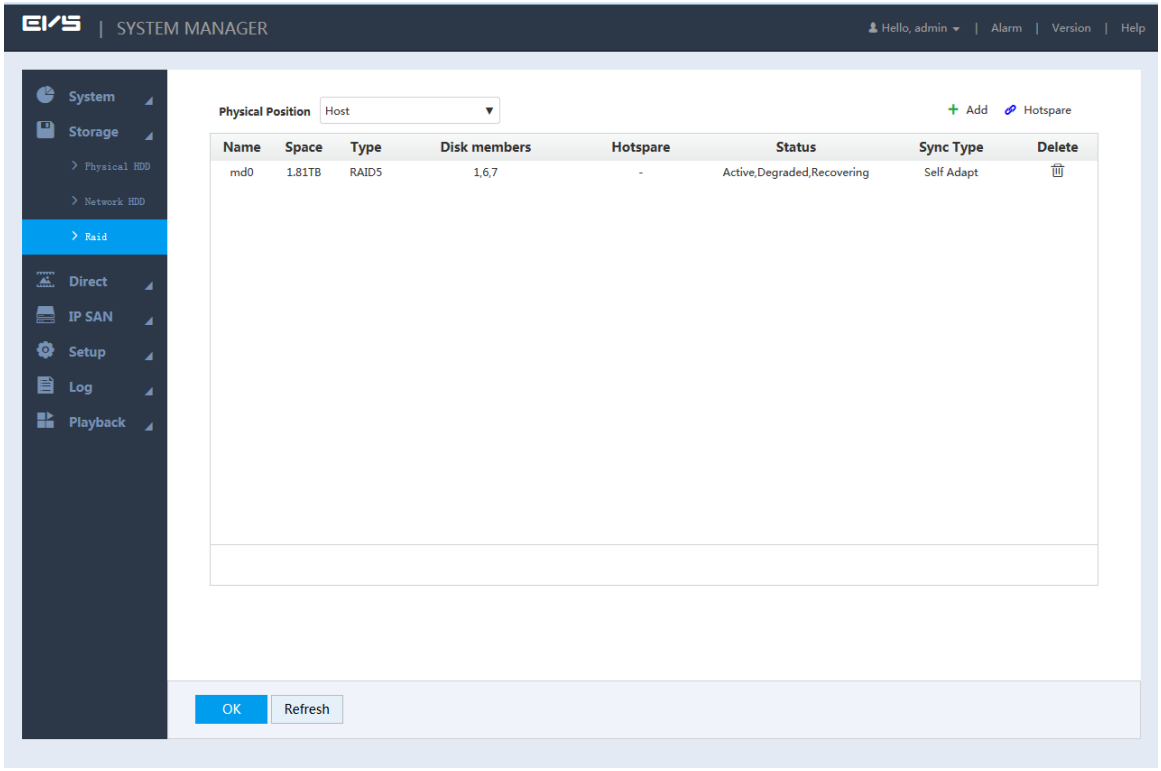
3.8.2 Hotspare Management

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

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

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

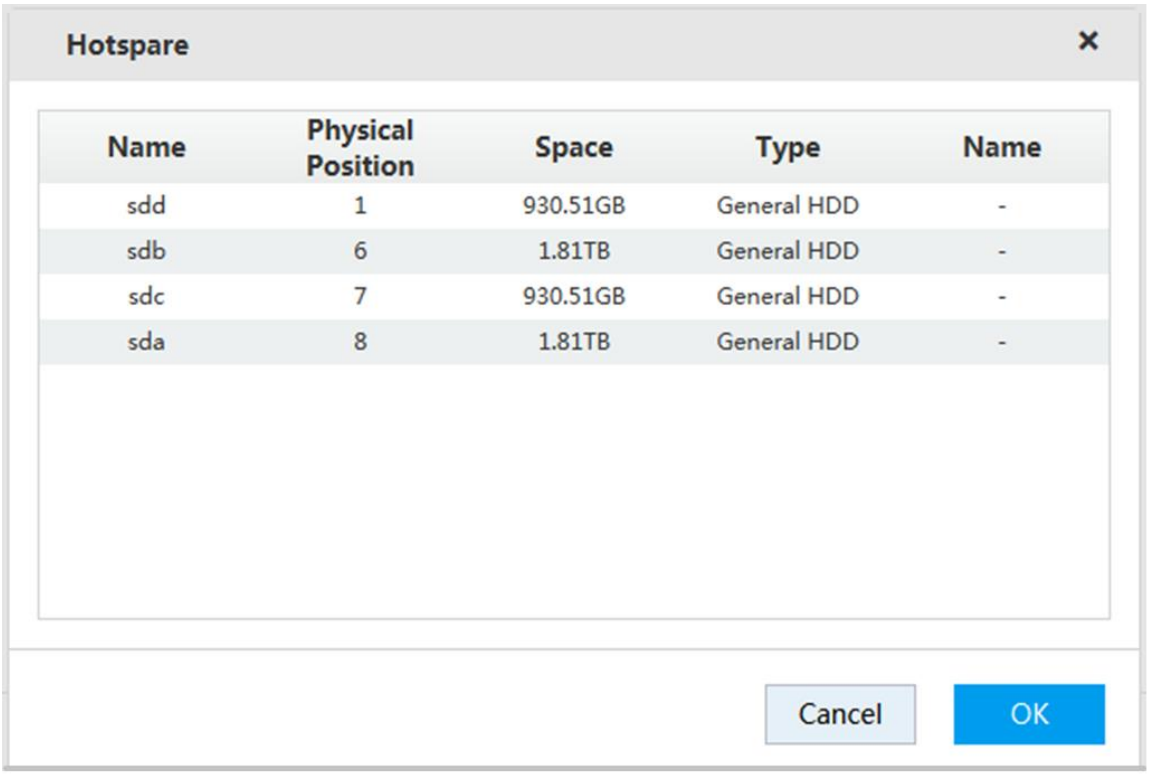
Figure 3-40 Raid management



Step 2 Click .

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

Figure 3-41 Hotspare management



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

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

- Private hotspare: Double-click the corresponding **Name**, select the RAID group, and then this HDD is used as a hotspare only for the corresponding group.
- General hotspare: It is used as a hotspare for all the RAID groups.

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