Storage Management System

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- HDMI The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY,

SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
Note	Provides additional information to emphasize or supplement important points of the main text.
Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100 to 240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

TABLE OF CONTENTS

Chapter 1 Login and Activation 1
1.1 Login 1
1.2 Device Activation 1
Chapter 2 System Configuration 3
2.1 Quick Configuration 3
2.2 Format Storage Space 4
Chapter 3 Hybrid SAN Sub-System Configuration 7
3.1 Network 7
3.1.1 Basic Settings 7
3.1.2 Advanced Settings 8
3.2 System 12
3.2.1 System Settings 12
3.2.2 Maintenance 12
3.2.3 Camera Management 14
3.2.4 User Management 16
3.3 Event 19
3.3.1 Configure Video Tampering Alarms 19
3.3.2 Configure Video Loss Alarms 20
3.3.3 Configure Exceptions Alarms 21
3.3.4 Configure Arming Schedule 21
3.3.5 Configure Alarm Linkage Method 22
3.4 Storage 23
3.4.1 Schedule Settings 23
3.4.2 Storage Management 25
3.4.3 Copy-Back 26
3.4.4 Storage Mode 27
3.4.5 Advanced Settings 29
Chapter 4 Shortcut 30
Chapter 5 Overview 32
5.1 Platform Overview 32
5.2 View Performance 32
5.3 View CPU and Memory Usage 33
Chapter 6 Device 34
6.1 Node Tree 34
6.1.1 View Node Tree 34
6.1.2 Map 34
6.2 Node Status 34
6.3 Refresh Domain 35
6.4 Device Overview 36
6.4.1 Locate Device 36

6.4.2 Mute Device 36
6.4.3 Reboot and Shut down Device 36
6.4.4 More Operations 37
6.5 Device Graph of a Node 37
6.5.1 Device Indicator 37
6.5.2 HDD Slot Graph 38
6.5.3 Health Checkup 39
6.5.4 Information Overview 42
Chapter 7 Resource 50
7.2 Manage RAID Resource Pool 50
7.2.2 Maintain Disks 50
7.2.3 Safely Remove Disks 51
7.3 Manage RAID 51
Chapter 8 Storage 53
8.2 Service 53
8.2.1 Service Management 53
8.2.2 Service Resource 56
8.3 Mirror 57
Chapter 9 Log 58
9.1 Search Log 58
9.2 Download Log 58
9.3 Clear Log 59
Chapter 10 Maintenance 60
10.1 Version Information 60
10.2 System Upgrade 60
10.3 Disk Management 61
10.4 Password Management 61
10.5 Time Management 62
10.5.1 Time Zone Configuration 62
10.5.2 Time Sync Configuration 63
10.5.3 DST Configuration 64
10.6 Default Settings 65
10.7 Snapshot Management 65
10.8 SNMP Management 67
10.9 Security Management 68
10.10 Network Management 69
10.10.1 Modify Network 69
10.10.2 Network Detection 69

Chapter 1 Login and Activation

1.1 Login

Purpose

You can use Microsoft Edge web browser to access your device.

Before you start

- Use a network cable to connect Ethernet port of your computer and the Management LAN of the device.
- Configure your computer IP address. Ensure it is in the same network segment with the Management LAN of the device (the default IP address of Management LAN is 10.254.254.254).

Step 1 Enter the device IP address (https://IP Address:2004) in web browser.

Step 2 Press Enter. Then login interface appears.

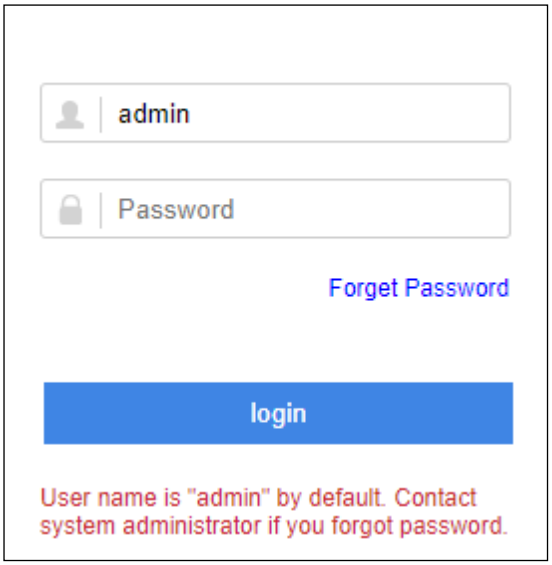


Figure 1-1 Login

Step 3 Enter **User Name** and **Password**.

Step 4 Click **login**.

1.2 Device Activation

Purpose:

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

Step 1 Access device via web browser.

Step 2 Enter the same password in **Create New Password** and **Confirm New Password**.

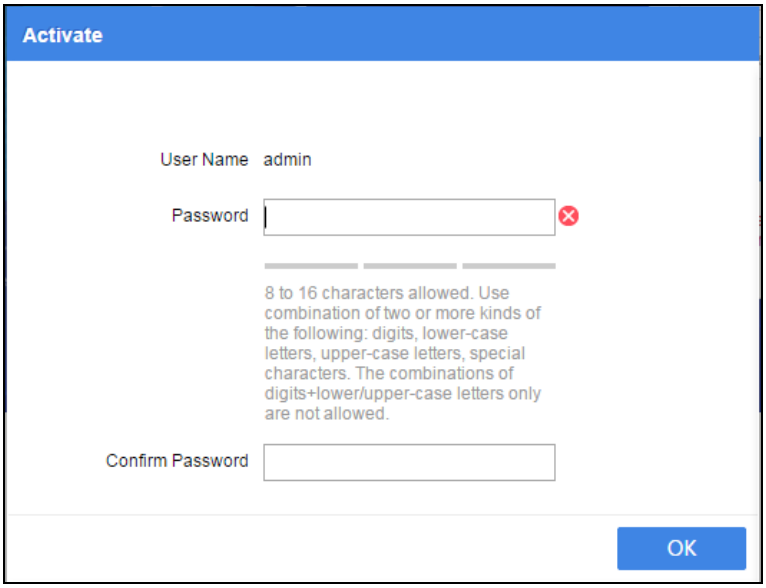


Figure 1-2 Activation

Step 3 Click **OK**.

Caution

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Chapter 2 System Configuration

2.1 Quick Configuration

When you log in to the system for the first time after activation, the Quick Configuration window will pop up.

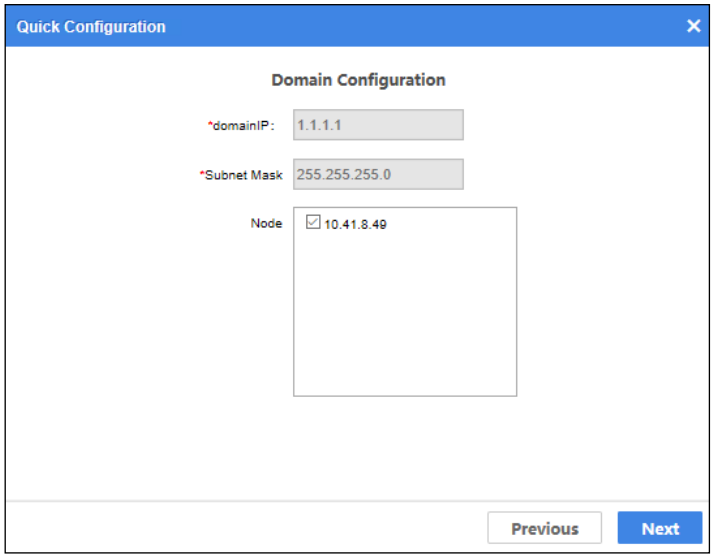


Figure 2-1 Domain Configuration

Step 2 Check the node.

Step 3 Click **Next** to create domain.

The creation process takes some time. The following window will pop up after the creation is completed.

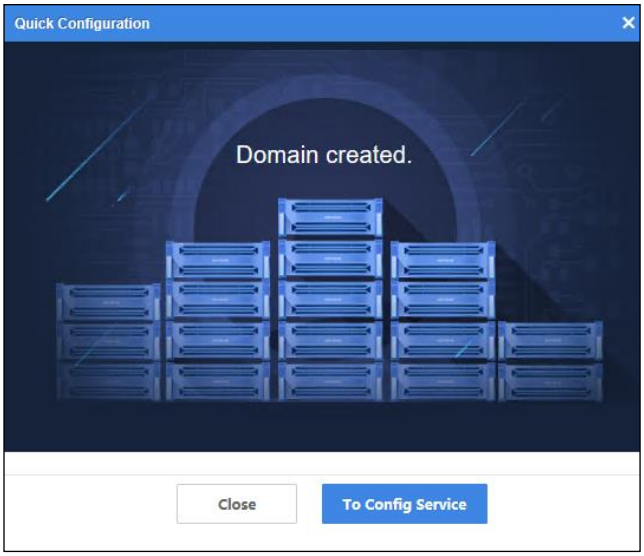


Figure 2-2 Domain Created

Step 4 Click **To Config Service** to follow the wizard to configure service.

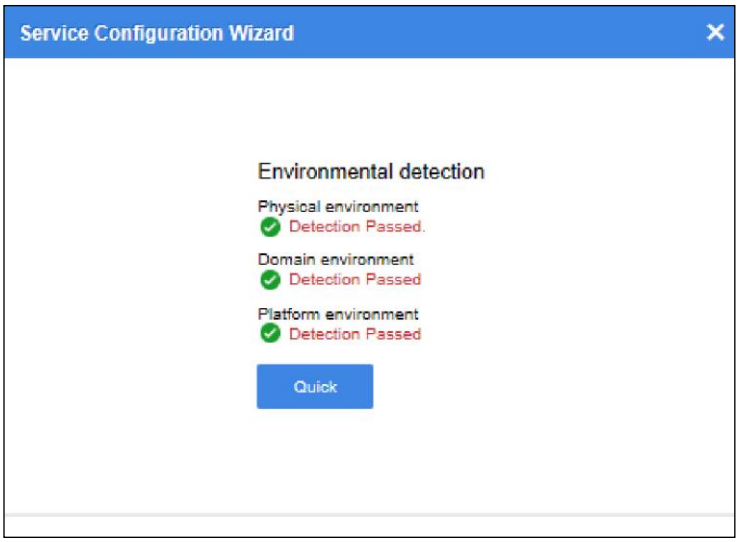


Figure 2-3 Service Configuration Wizard

Note

The service can only be configured after the environment detection is passed.

Step 5 Click **Quick** to select RAID mode.

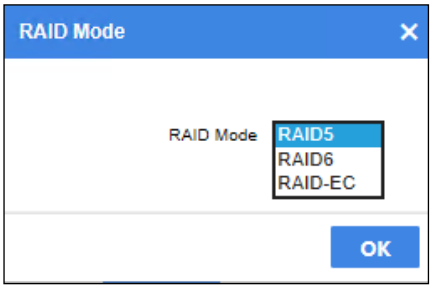


Figure 2-4 RAID Mode

Note

RAID-EC mode is recommended.

Step 6 Click **OK** to start the quick configuration.

2.2 Format Storage Space

Step 1 Go to **Storage**.

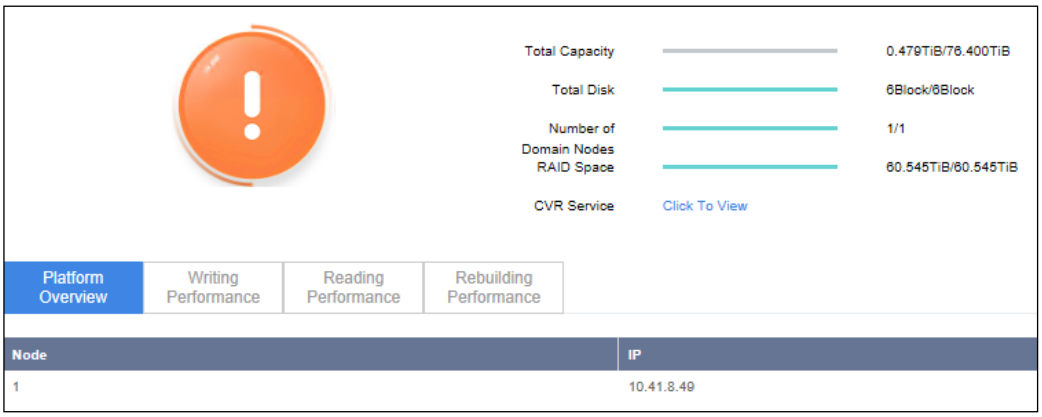


Figure 2-5 Storage

Step 2 Click **Click To View** to redirect to Hybrid SAN sub-system.

Step 3 Enter Hybrid SAN System.

Step 4 Follow the wizard to complete configurations.

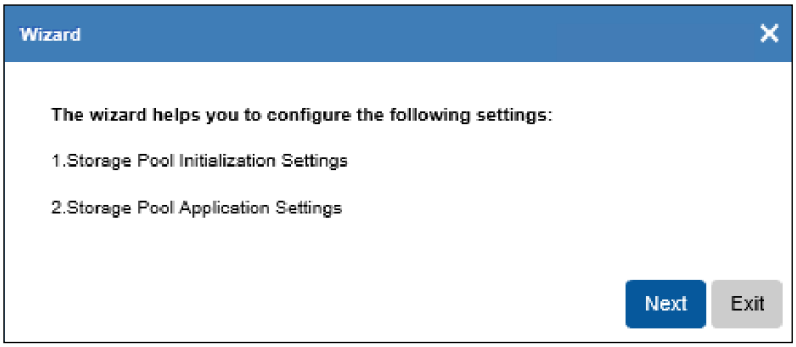


Figure 2-6 Configuration Wizard

Step 5 Click **Next** to configure storage pool initialization.

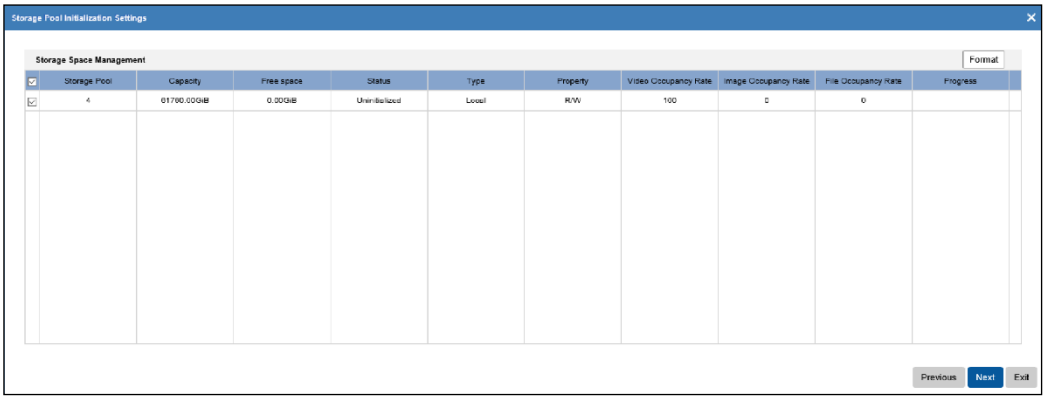


Figure 2-7 Storage Pool Initialization Settings

Step 6 Check the storage pool and click **Format**.

Step 7 Click **OK** to confirm the operation.

The following prompt will pop-up after the storage pool is formatted.

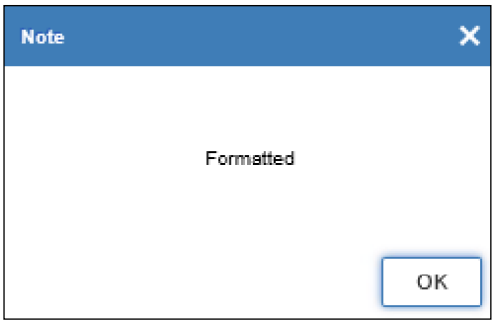


Figure 2-8 Formatting Completion Prompt

Step 8 Click **OK**.

Step 9 Click **Next** to configure storage pool application.

Video Storage Mode is selected by default.

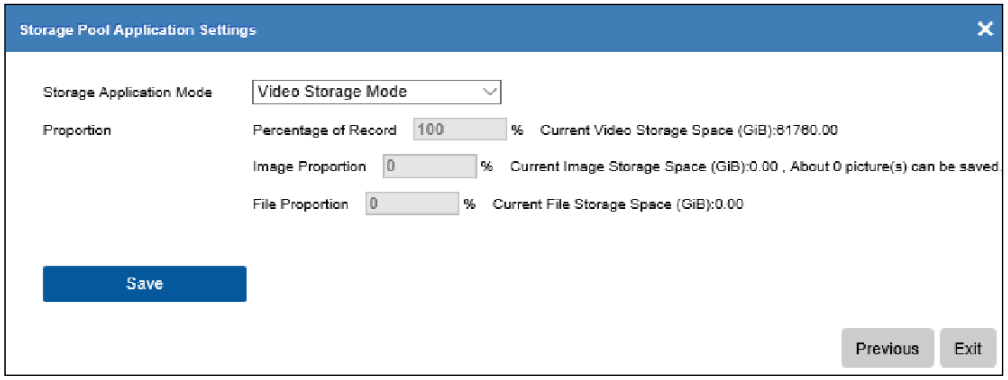


Figure 2-9 Storage Pool Application Settings

Step 10 Click **Save**.

Step 11 Click **OK** to confirm the operation.

Step 12 Click **Exit** to finish the configuration.

Chapter 3 Hybrid SAN Sub-System Configuration

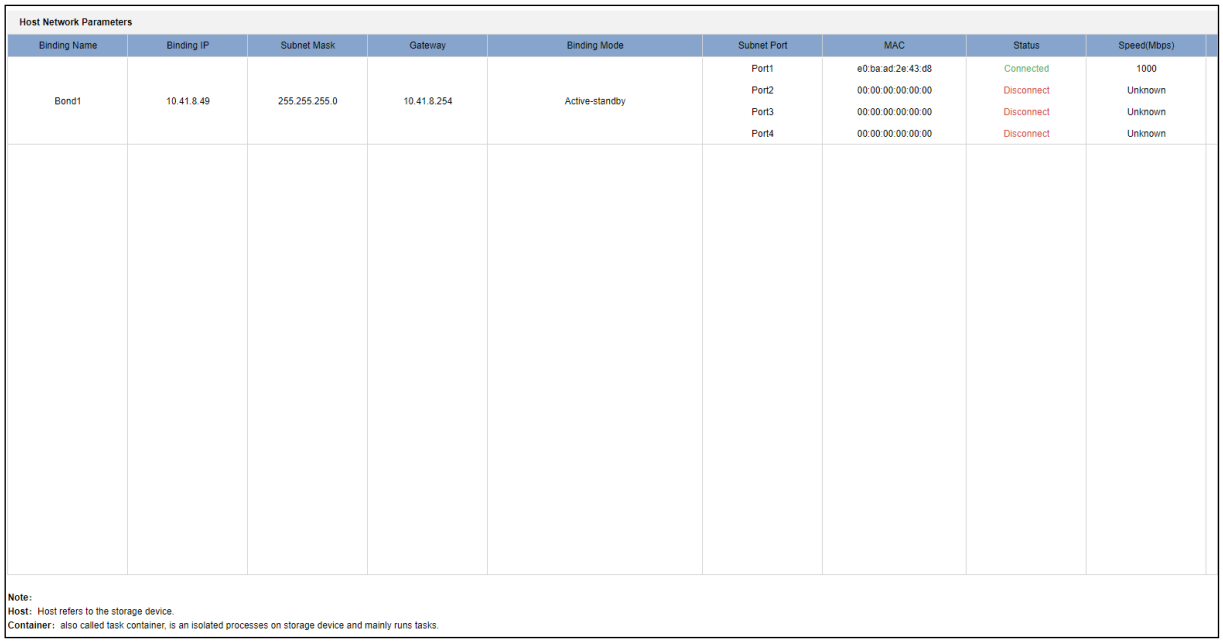
3.1 Network

3.1.1 Basic Settings

TCP/IP

Step 1 Go to **Configuration > Network > Basic Settings > TCP/IP**.

Step 2 View the host network parameters.



Host Network Parameters

Binding Name	Binding IP	Subnet Mask	Gateway	Binding Mode	Subnet Port	MAC	Status	Speed(Mbps)
Bond1	10.41.8.49	255.255.255.0	10.41.8.254	Active-standby	Port1	e0:ba:ad:2e:43:d8	Connected	1000
					Port2	00:00:00:00:00:00	Disconnect	Unknown
					Port3	00:00:00:00:00:00	Disconnect	Unknown
					Port4	00:00:00:00:00:00	Disconnect	Unknown

Note:
Host: Host refers to the storage device.
Container: also called task container, is an isolated processes on storage device and mainly runs tasks.

Figure 3-1 Host Network Parameters

Port

Step 1 Go to **Configuration > Network > Basic Settings > Port**.

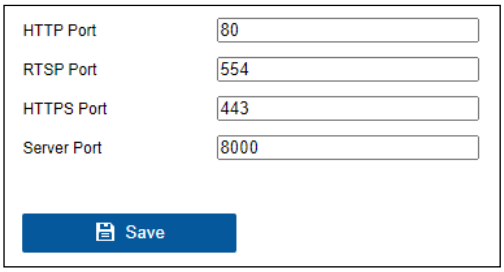


Figure 3-2 Port Settings

Step 2 Set the HTTP port, RTSP port, HTTPS port and server port of the camera.

- HTTP Port: The default port number is 80, and it can be changed to any port No. which is not occupied.
- RTSP Port:The default port number is 554 and it can be changed to any port No. ranges from 1024 to 65535.
- HTTPS Port: The default port number is 443, and it can be changed to any port No. which is not occupied.
- Server Port: The default server port number is 8000, and it can be changed to any port No. ranges from 2000 to 65535.

Step 3 Click **Save** to save the settings.

3.1.2 Advanced Settings

Email

Purpose

The system can be configured to send an e-mail notification to all designated users when a specified event occurs such as when an alarm or event is detected, or the administrator password is changed, etc.

Before you start

The device must be connected to a local area network (LAN) that contains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the email accounts to which you want to send notifications.

Step 1 Go to **Configuration > Network > Basic Settings > Email**.

Step 2 Configure the email settings.

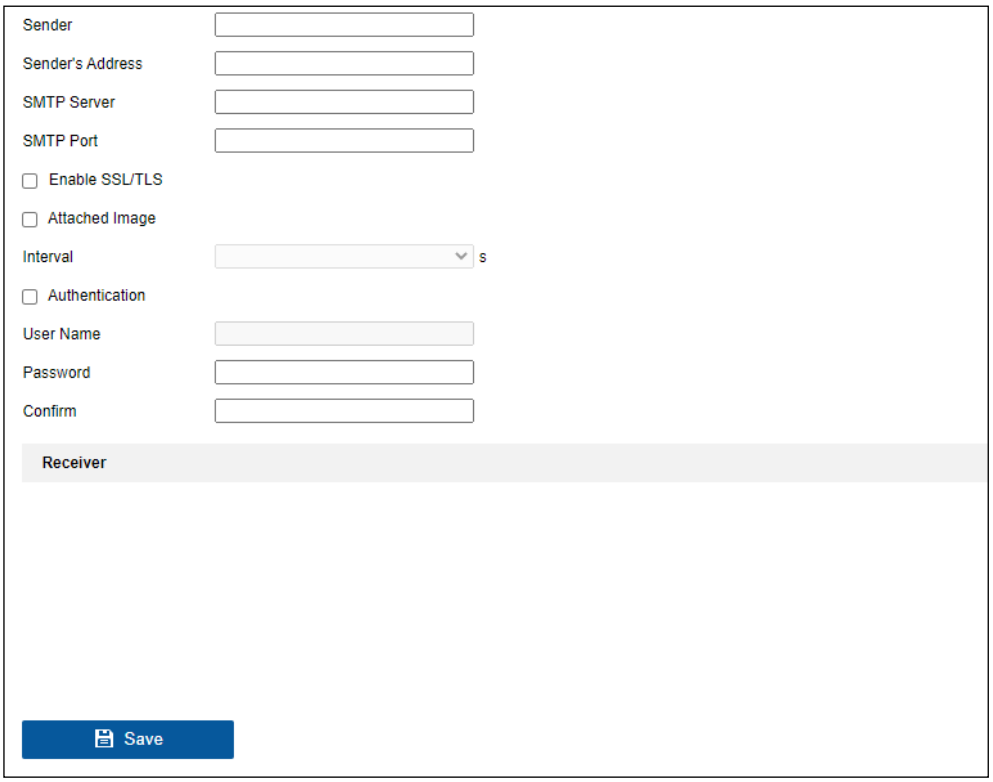


Figure 3-3 Email Settings

Sender

The sender's name.

Sender's Address

The sender's address.

SMTP Server

The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).

SMTP Port

The SMTP port. The default TCP/IP port used for SMTP is 25.

Enable SSL/TLS

Check to enable SSL/TLS if required by the SMTP server.

Attached Image

Check to send email with attached alarm images. The interval is the time between sending two subsequent alarm images.

Interval

The time interval for capturing the attached images.

Authentication

Check to enable the function if the SMTP server requires user authentication and enter the user name and password accordingly.

Select Receivers

Select the receiver. Up to 3 receivers can be configured.

Receiver

The receiver's name.

Receiver's Address

The email address of the user to be notified.

Step 3 Click **Save** to save the settings.

Picture Storage

Step 1 Go to **Configuration > Network > Basic Settings > Picture Storage**.

Step 2 Click **Browse** and select certificate file.

Note

Only CRT and PEM files are supported.

Step 3 Click **Import**.

The certificate status will change to **Imported**.

N+1

Purpose

N+1 working mode refers to N working device(s) and 1 back device.

Step 1 Go to **Configuration > Network > Basic Settings > N+1**.

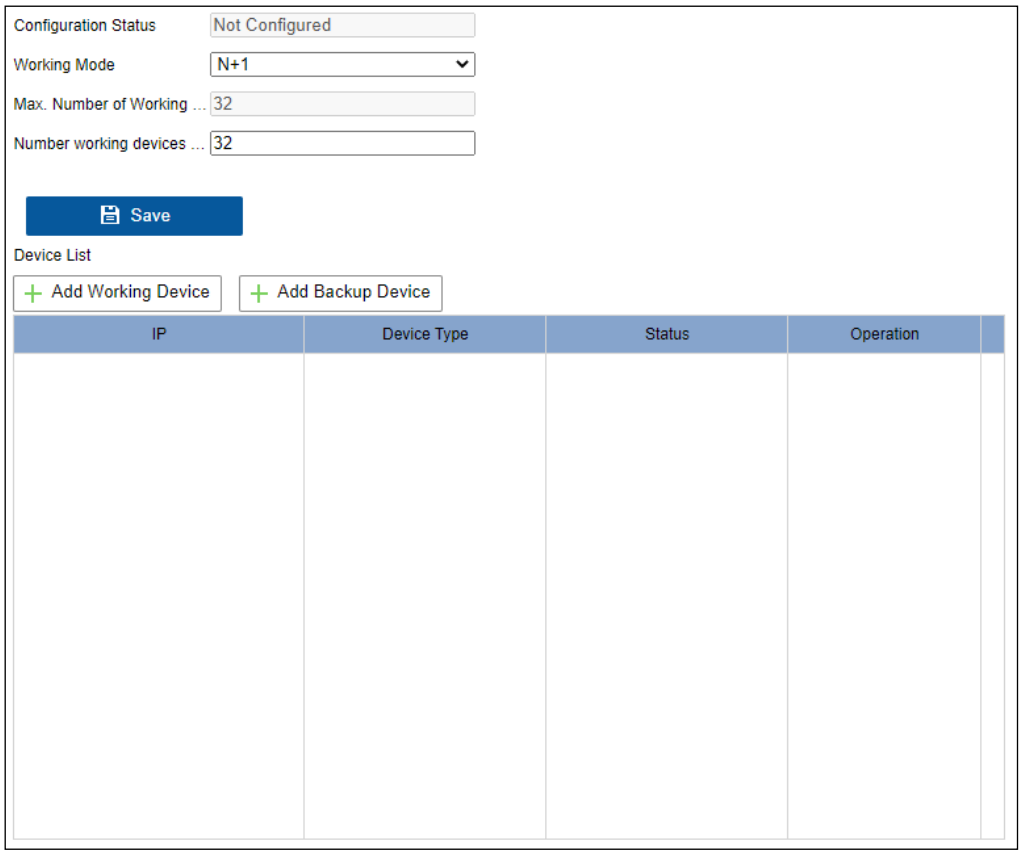


Figure 3-4 N+1 Settings

Step 2 Enter the number of working device(s) to be taken over by the backup device.

Step 3 Click **Save**.

Step 4 Add working device.

1) Click **Add Working Device**.
2) Enter the working device IP address and password.
3) Click **OK**.

Step 5 Add working device.

1) Click **Add Backup Device**.
2) Enter the backup device IP address and password.
3) Click **OK**.

Other

Purpose

Alarm host: If the alarm center is set, the information will be sent to the remote alarm host when an alarm or exception occurs on the device.

Multicast: When remotely accessing a device, use multicast to avoid the problem of the device's access limit.

Step 1 Go to **Configuration > Network > Basic Settings > Other**.

Figure 3-5 Other Settings

Step 2 Enter the IP address and port of the alarm host.

Step 3 Enter the multicast address.

Step 4 Click **Save**.

3.2 System

3.2.1 System Settings

Basic Information

The device information interface allows you to check the basic information of the device. It is the reference for maintenance or modification in future. Only device name and Hybrid SAN No. is editable in this interface.

Basic Settings

Step 1 Go to **Configuration > System > System Settings > Basic Settings**.

Step 2 Check **IP Camera Time Sync** to synchronize the time of connected network camera.

Step 3 Click **Save**.

3.2.2 Maintenance

Reboot Device

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Reboot** to reboot the device.

Restore Default Settings

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Click **Restore to Factory Settings**.

Note

All parameters will be restored to factory settings except IP address, subnet mask, gateway, user information, and storage mode.

Export/Import Configuration Files

Step 1 Go to **Configuration > System > Maintenance > Upgrade & Maintenance**.

Step 2 Export configuration files.

1) Click **Hybrid SAN Parameters**.
2) Enter the encrption password and confirm it.

Step 3 Import configuration files.

1) Click **Browse** to select the saved configuration file.
2) Click **Import**.

Note

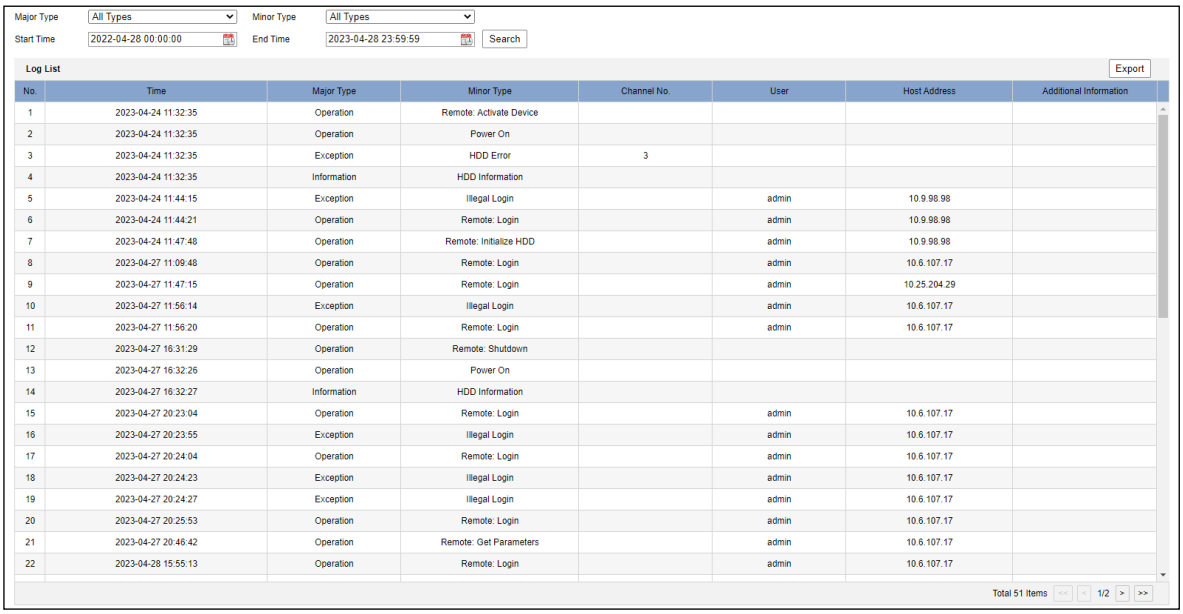
Device will reboot automatically after importing configuration parameters.

Search and Export Log

Purpose

Search and export the log files of operation, alarm, exception, and information.

Step 1 Go to **Configuration > System > Maintenance > Log**.



No.	Time	Major Type	Minor Type	Channel No.	User	Host Address	Additional Information
1	2023-04-24 11:32:35	Operation	Remote: Activate Device				
2	2023-04-24 11:32:35	Operation	Power On				
3	2023-04-24 11:32:35	Exception	HDD Error	3			
4	2023-04-24 11:32:35	Information	HDD Information				
5	2023-04-24 11:44:15	Exception	Illegal Login		admin	10.9.98.98	
6	2023-04-24 11:44:21	Operation	Remote: Login		admin	10.9.98.98	
7	2023-04-24 11:47:48	Operation	Remote: Initialize HDD		admin	10.9.98.98	
8	2023-04-27 11:09:48	Operation	Remote: Login		admin	10.6.107.17	
9	2023-04-27 11:47:15	Operation	Remote: Login		admin	10.25.204.29	
10	2023-04-27 11:56:14	Exception	Illegal Login		admin	10.6.107.17	
11	2023-04-27 11:56:20	Operation	Remote: Login		admin	10.6.107.17	
12	2023-04-27 16:31:29	Operation	Remote: Shutdown				
13	2023-04-27 16:32:26	Operation	Power On				
14	2023-04-27 16:32:27	Information	HDD Information				
15	2023-04-27 20:23:04	Operation	Remote: Login		admin	10.6.107.17	
16	2023-04-27 20:23:55	Exception	Illegal Login		admin	10.6.107.17	
17	2023-04-27 20:24:04	Operation	Remote: Login		admin	10.6.107.17	
18	2023-04-27 20:24:23	Exception	Illegal Login		admin	10.6.107.17	
19	2023-04-27 20:24:27	Exception	Illegal Login		admin	10.6.107.17	
20	2023-04-27 20:25:53	Operation	Remote: Login		admin	10.6.107.17	
21	2023-04-27 20:46:42	Operation	Remote: Get Parameters		admin	10.6.107.17	
22	2023-04-28 15:55:13	Operation	Remote: Login		admin	10.6.107.17	

Figure 3-6 Log

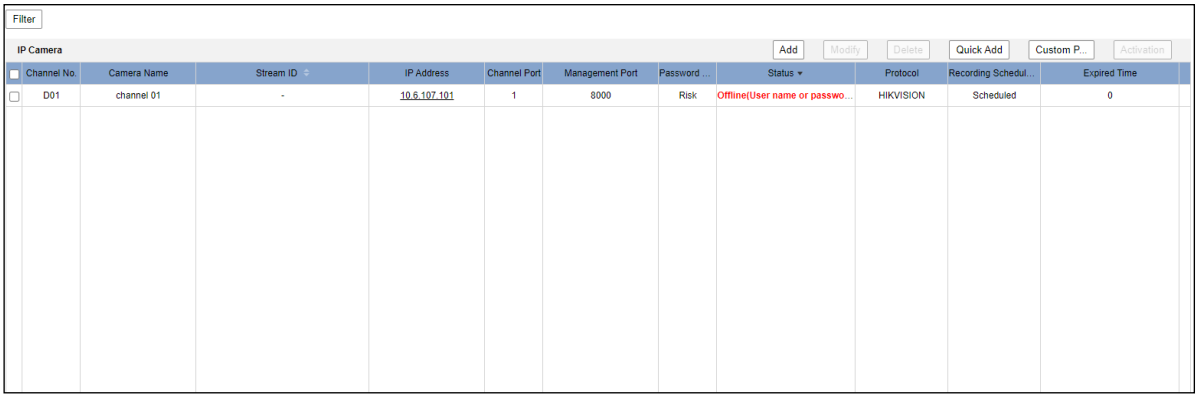
Step 2 Select the **Major Type** and **Minor Type** of log files.

Step 3 Set **Start Time** and **End Time**.

Step 4 Click **Search**.

Step 5 Click **Export** to export the log file of total items.

3.2.3 Camera Management



Channel No.	Camera Name	Stream ID	IP Address	Channel Port	Management Port	Password ...	Status	Protocol	Recording Schedul...	Expired Time
D01	channel 01	-	10.6.107.101	1	8000	Risk	Offline(User name or passwo...	HIKVISION	Scheduled	0

Figure 3-7 Camera Management

Add Camera Manually

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Click **Add**.

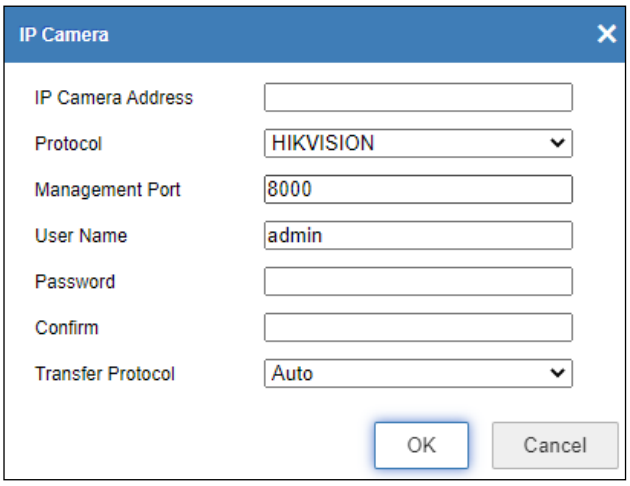


Figure 3-8 Add Camera

Step 3 Enter the IP address, management port, user name, an password of the camera, and select the protocol and transfer protocol.

Step 4 Click **OK**.

Note

If the status changes to **Online**, it indicates that the camera has been added. Otherwise, please check the network or check whether the user name, password, protocol, and other information are correct.

Quick Add Camera

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Click **Quick Add** to search the camera(s) on the same network segment as the device.

Step 3 Check the camera(s) to add.

Step 4 Click **OK**.

Note

Only cameras that support the SADP protocol can be quickly added.

Modify/Delete/Activate Camera

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Check the IP camera in the IP camera list.

Step 3 Modify camera.

1) Click **Modify** to modify the parameters.

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

Step 4 Delete camera.

1) Click **Delete** to delete the selected camera.

2) Click **OK** to confirm the operation.

Step 5 Activate camera.

1) Click **Activation**.

2) Check **Use Admin Password**.

3) Enter the admin password and confirm it

4) Click **OK**.

Filter Camera

Step 1 Go to **Configuration > System > Camera Management > IP Camera**.

Step 2 Click **Filter** to expand the filtering conditions.

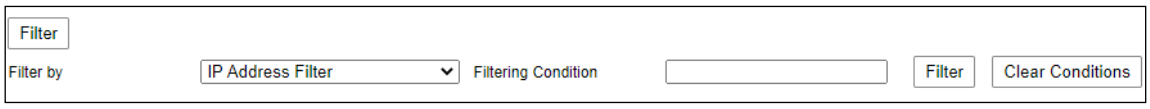


Figure 3-9 Filter Camera

Step 3 Select the types in the **Filter by** drop-down box. You can select **IP Address Filter** or **ID Stream Filter**.

Step 4 Enter the specified IP address or ID stream in the **Filtering Condition**.

Step 5 Click **Filter** to the right of the input box.

3.2.4 User Management

Purpose

Manage users, view online users, and manage encryption key.

Add User

Step 1 Go to **Configuration > System > User Management > User Management**.

Step 2 Click **Add**.

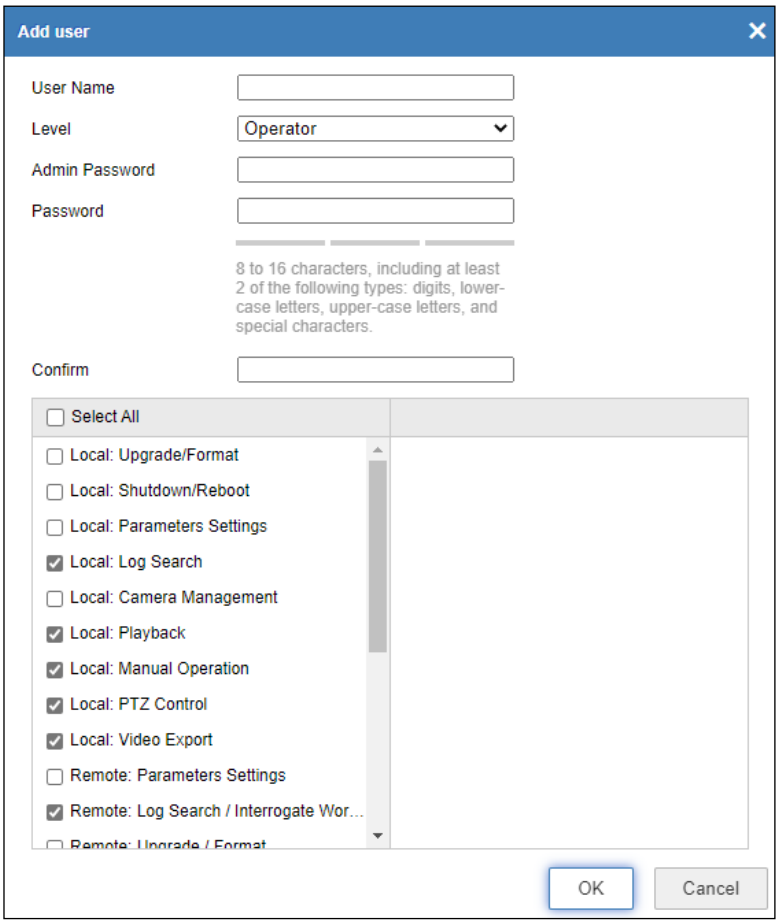


Figure 3-10 Add User

Step 3 Enter the **User Name** and select the **Level** as **Operator** or **User**.

Step 4 Enter admin password.

Step 5 Enter user password and confirm it.

Step 6 Check the user permissionson the right.

Step 7 Click **OK**.

Modify/Delete User

Step 1 Go to **Configuration > System > User Management > User Management**.

Step 2 Select a user in the user list.

Step 3 Modify user.

1) Click **Modify**.
2) Modify the user information.
3) Click **OK** to save the modifications.

Note

For admin user, the user name, password, and permissions cannot be modified. You can select whether to use the admin password to quick add IP cameras and whether to duplicate the admin password to IP cameras that are connected with default protocol.

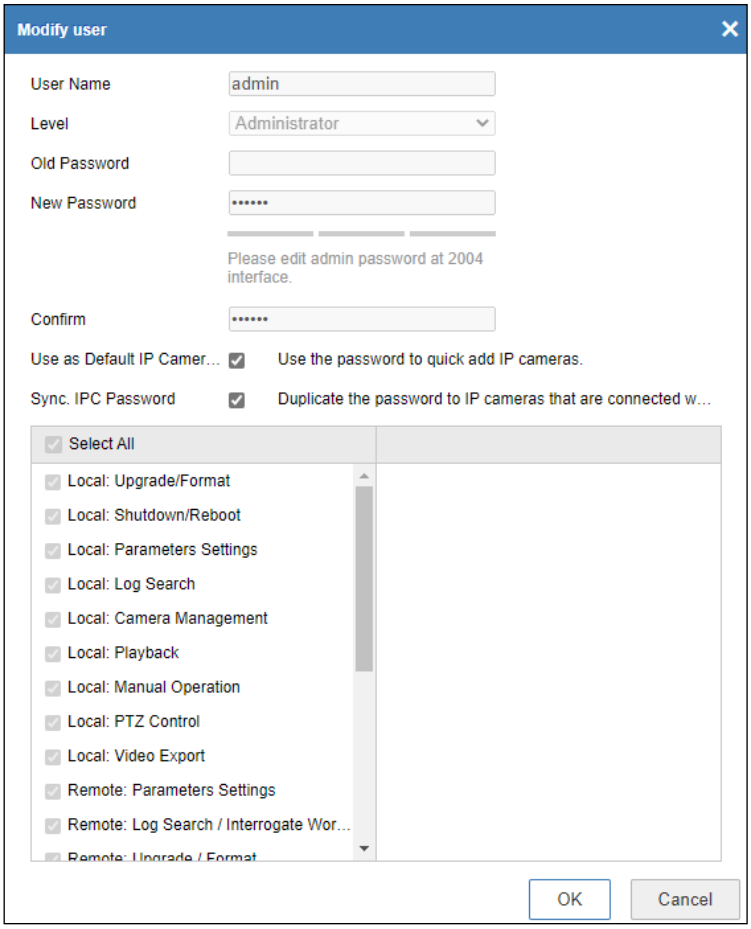


Figure 3-11 Modify Admin User

View Online Users

Step 1 Go to **Configuration > System > User Management > Online User**.

Step 2 View the online user list.

Step 3 (Optional) Click **Refresh** to refresh it.

Manage Key

Step 1 Go to **Configuration > System > User Management > Key Management**.

Step 2 Import key file.

1. Click **Browse** and select the key file.

2. Click **Import** to import the key file.

Note

Key file contains AK and SK, which is used for restful protocol access.

Step 3 Click **Export Encryption Key** to export key file.

Step 4 Click **Reset Password** to use the new password to access the platform.

3.3 Event

Purpose

Basic event settings refer to the configuration of supported basic events type, including video tampering, video loss, exception, etc.

3.3.1 Configure Video Tampering Alarms

Purpose

Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).

Step 1 Go to **Configuration > Event > Basic Event > Video Tampering**.

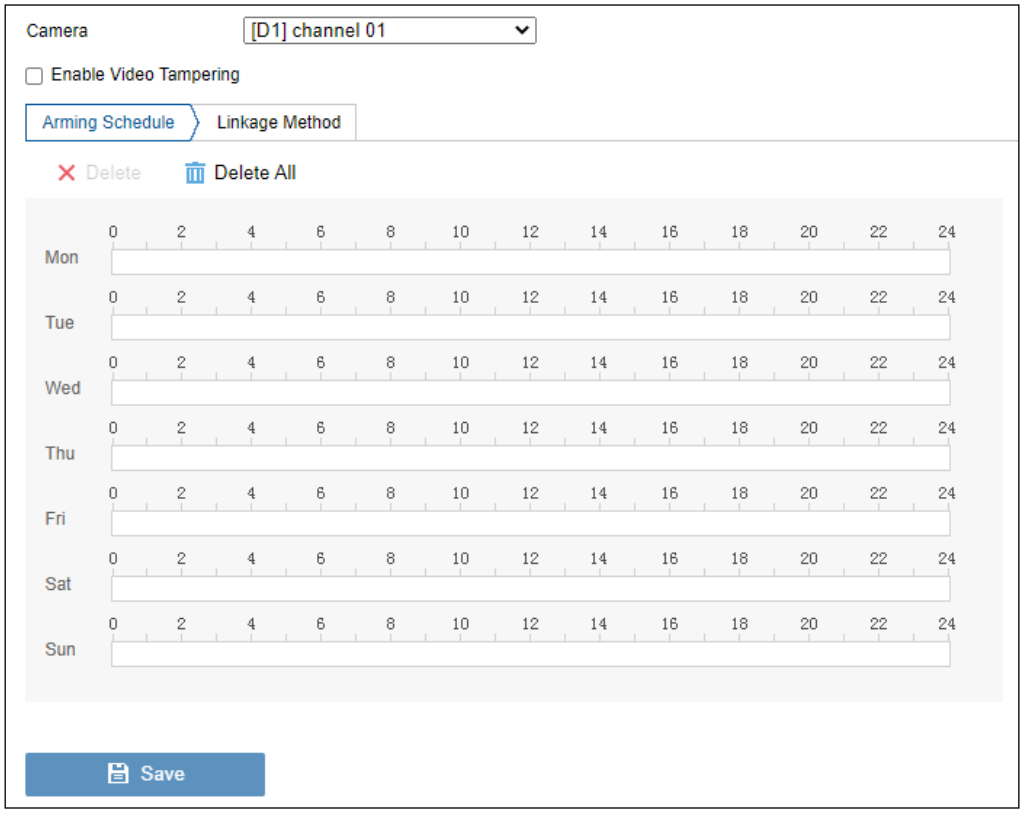


Figure 3-12 Configure Video Tampering Alarms

Step 2 Select the camera in the drop-down box.

Step 3 Check the checkbox of **Enable Video Tampering**.

Step 4 Set the arming schedule. Refer to Configure Arming Schedule for details.

Step 5 Set the linkage methods. Refer to Configure Alarm Linkage Method for details.

Step 6 Click **Save**.

3.3.2 Configure Video Loss Alarms

Purpose

Video loss detection detects video loss of a channel and takes alarm response action(s).

Step 1 Go to **Configuration > Event > Basic Event > Video Loss**.

Figure 3-13 Configure Video Loss Alarms

Step 2 Select the camera in the drop-down box.

Step 3 Check the checkbox of **Enable Video Loss Detection**.

Step 4 Set the arming schedule. Refer to Configure Arming Schedule for details.

Step 5 Set the linkage methods. Refer to Configure Alarm Linkage Method for details.

Step 6 Click **Save**.

3.3.3 Configure Exceptions Alarms

Purpose

Exception events can be configured to take the event hint in the Live View window and trigger alarm output and linkage actions.

Step 1 Go to **Configuration > Event > Basic Event > Exception**.

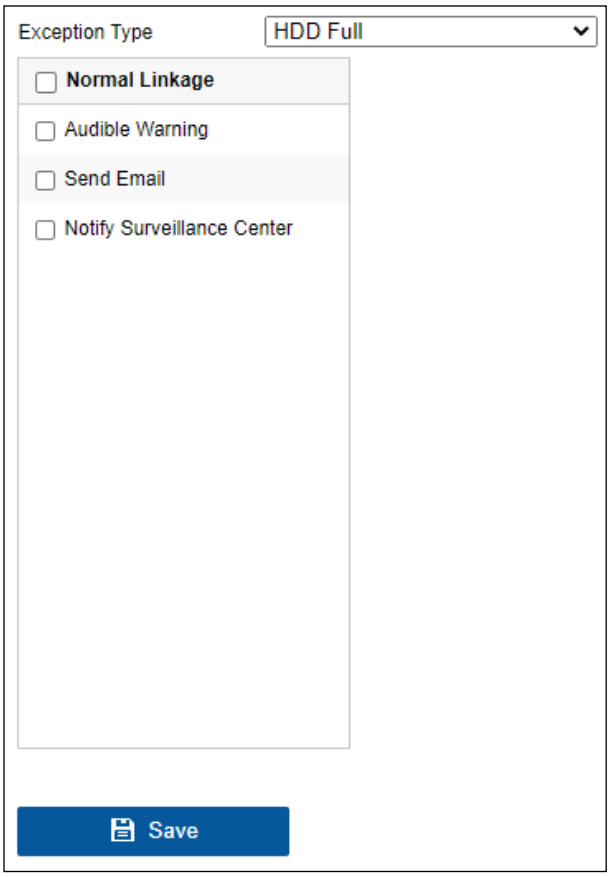


Figure 3-14 Configure Exceptions Alarms

Step 2 Select the **Exception Type** in the drop-down box.

Step 3 Set the linkage methods. Refer to Configure Alarm Linkage Method for details.

Step 4 Click **Save**.

3.3.4 Configure Arming Schedule

Step 1 Select **Arming Schedule**.

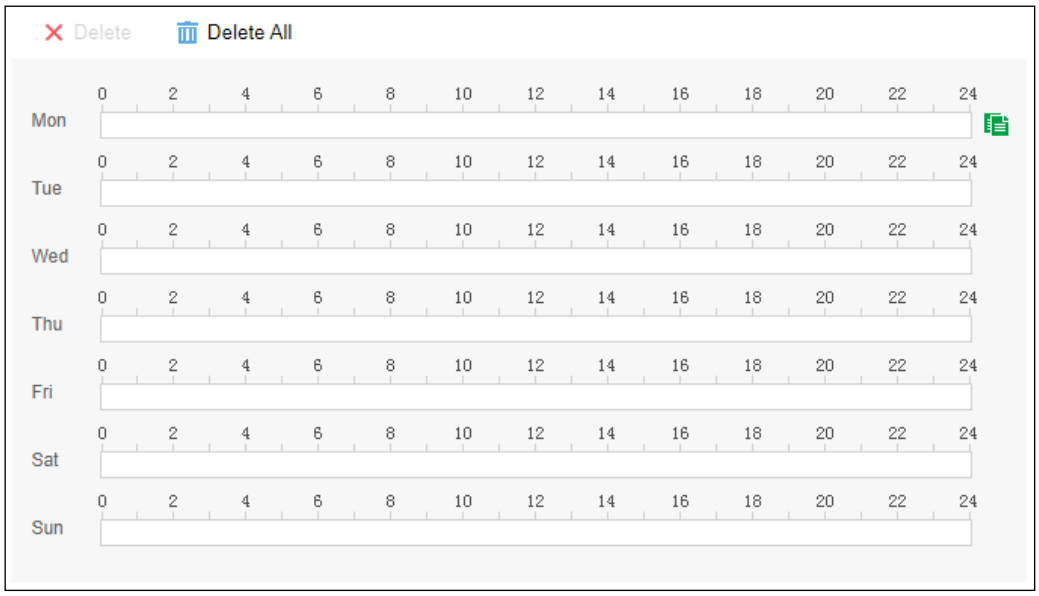


Figure 3-15 Set Arming Schedule

Step 2 Choose the day you want to set the arming schedule.

Step 3 Left-click and drag to draw the time period.

Note

- Up to eight time periods can be set within each day.
- Time periods shall not be repeated or overlapped.

Step 4 Manually adjust the time period.

1) Select a drawn period.
2) Enter the start time and end time of the period in the text box.
3) Click **Save**.

Step 5 (Optional) After you set the arming schedule, you can copy the arming schedule for the day to other days.

1) Click to the right of the time bar.
2) Check the day you want to copy the arming schedule to.
3) Click **OK**.

Step 6 Click **Save**.

3.3.5 Configure Alarm Linkage Method

Purpose

Alarm linkage actions will be activated when an alarm or exception occurs.

Step 1 Select **Linkage Method**.

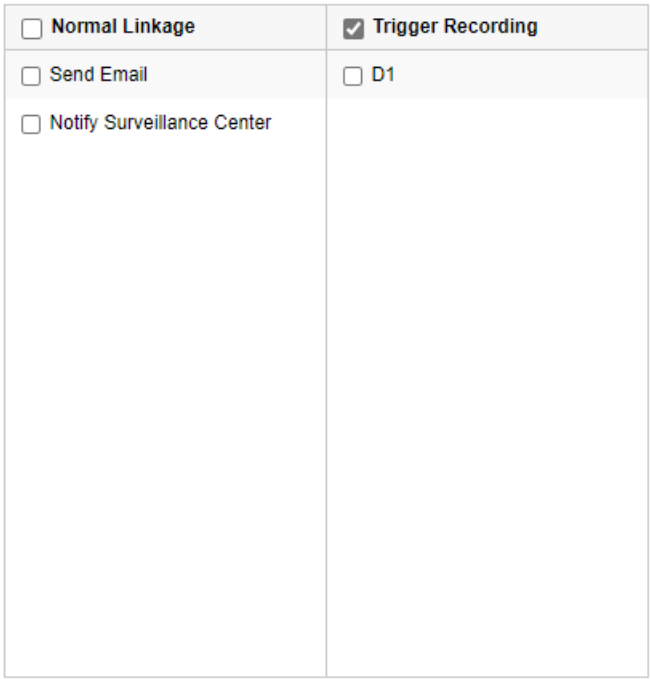


Figure 3-16 Linkage Method

Step 2 Check to set normal linkage actions, trigger recording, etc.

Send Email

It will send an email with alarm information when an alarm is triggered.

Notify Surveillance Center

The device will send an exception or alarm signal to the remote client software when an alarm is triggered.

Audible Warning

It will trigger an audile warning locally when an alarm is triggered. It is only supported by the device with the audio output.

Trigger Recording

The checked channel will start recording when an alarm is triggered. You have to set the recording schedule first.

Step 3 Click **Save**.

3.4 Storage

3.4.1 Schedule Settings

Purpose

When the device is equipped with a local HDD or a network HDD, and the HDD can work normally, the recording schedule of each channel can be configured. After configuring the recording schedule, the device will automatically perform different recording tasks for the configured time and save the recordings.

Step 1 Go to **Configuration > Storage > Schedule Settings > Record Schedule**.

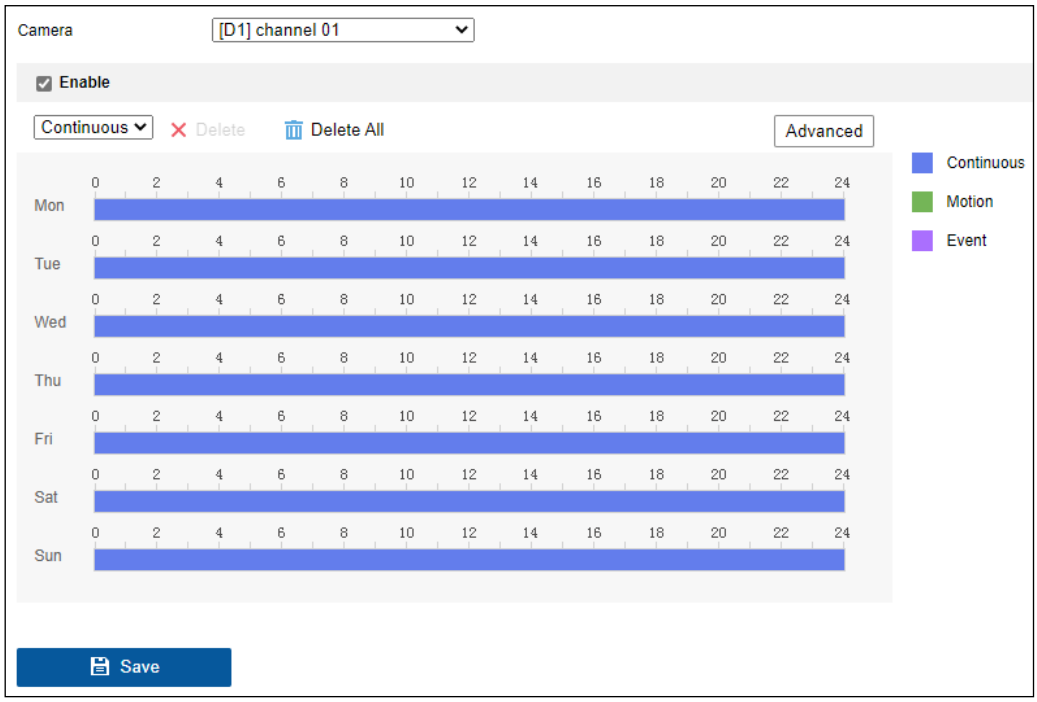


Figure 3-17 Record Schedule

Step 2 Select the camera in the drop-down box.

Step 3 Check **Enable** to enable the record schedule settings.

Step 4 Select recording type in the drop-down box. You can select **Continuous**, **Motion**, and **Event**.

Step 5 Choose the day you want to set the arming schedule.

Step 6 Left-click and drag to draw the time period.

Note

- Up to eight time periods can be set within each day.
- Time periods shall not be repeated or overlapped.

Step 7 Manually adjust the time period.

1) Select a drawn period.

2) Enter the start time and end time of the period in the text box.

3) Click **Save**.

Step 8 (Optional) After you set the arming schedule, you can copy the arming schedule for the day to other days.

1) Click to the right of the time bar.

2) Check the day you want to copy the arming schedule to.

3) Click **OK**.

Step 9 (Optional) Click **Advanced** to make advanced configurations.

Record Audio

After checked, the audio and video will be saved in the HDD together. If unchecked, only the video will be saved.

Pre-record

The pre-recording time before the recording starts.

Note

- **No Pre-record** means no pre-recording.
- **Not Limited** means that pre-recording is carried out according to the maximum pre-recording time. The maximum pre-recording time is calculated at a 2Mbps bitrate, which will become shorter as a higher bitrate is selected.

Post-record

The post-recording time after the recording ends.

Stream Type

Select the stream type of the recording.

Keep Video/Pictures for

The time length the recording was saved on the HDD. If you select **1**, the recording will remain on the HDD for one day and will be automatically overwritten the next day. If you select **0**, the recording will remain on the HDD until the HDD is full.

Step 10 Click **Save**.

3.4.2 Storage Management

Step 1 Go to **Configuration > Storage > Storage Management > Storage Space Management**.

Step 2 View the HDD status.

Step 3 (Optional) Check the HDD and click **Format** to format the HDD.

Note

All data will be lost after formatting. Please be cautious.

3.4.3 Copy-Back

Many Copy-Back

Step 1 Go to **Configuration > Storage > Copy-back > Many Copy-back**.

Step 2 Click **Add Copy-back Task**.

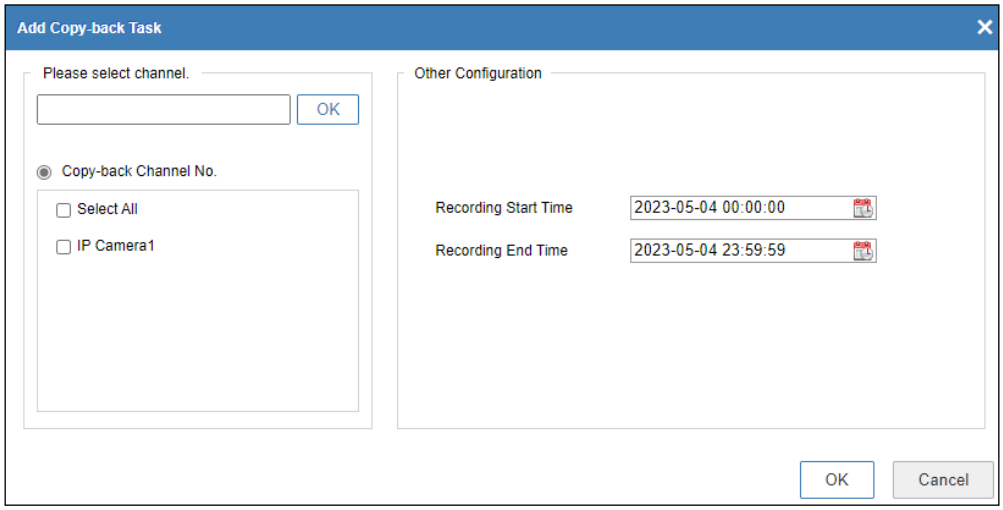


Figure 3-18 Add Copy-Back Task

Step 3 Select channel on the left.

Step 4 Set the **Recording Start Time** and **Recording End Time** on the right.

Step 5 Click **OK**.

Scheduled Copy-Back

Step 1 Go to **Configuration > Storage > Copy-back > Scheduled Copy-back**.

Step 2 Set video upload schedule.

1) Select **Video Upload Schedule Settings** in the drop-down box.
2) Click **Video Upload Schedule Settings**.
3) Select channel on the left.
4) Select date, copy-back mode, and time periods on the right.
5) Click **OK**.

Step 3 Set video upload execution.

1) Select **Video Upload Execution Settings** in the drop-down box.
2) Click **Video Upload Execution Settings**.
3) Select channel on the left.
4) Select date, copy-back mode, and time periods on the right.
5) Click **OK**.

Scheduled Upload Task List

Step 1 Go to **Configuration > Storage > Copy-back > Schedule Upload Task List**.

Step 2 View the scheduled upload task list.

Basic Configuration

Step 1 Go to **Configuration > Storage > Copy-back**.

Step 2 Click **Basic Configuration**.

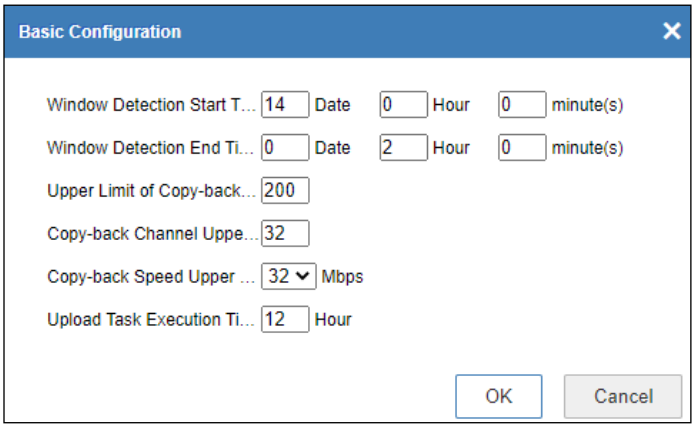


Figure 3-19 Basic Configuration

Step 3 Set the parameters.

Step 4 Click **OK**.

3.4.4 Storage Mode

Storage Application Mode

Step 1 Go to **Configuration > Storage > Storage Mode > Storage Application Mode**.

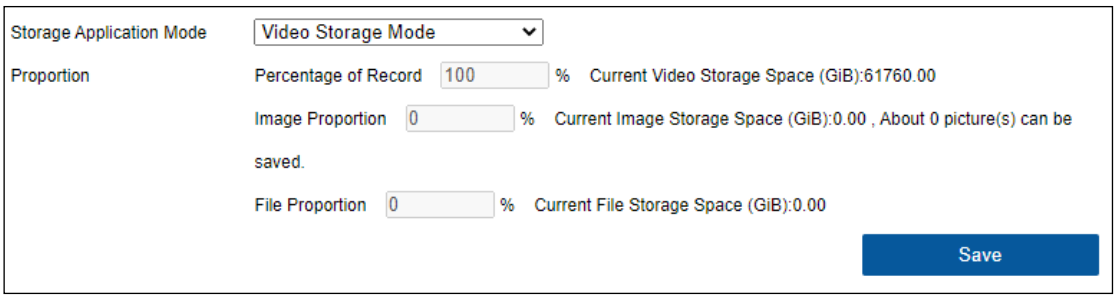


Figure 3-20 Storage Application Mode

Step 2 View the storage space of video, image, and file.

Advanced Storage Mode

Step 1 Go to **Configuration > Storage > Storage Mode > Advanced Storage Mode**.

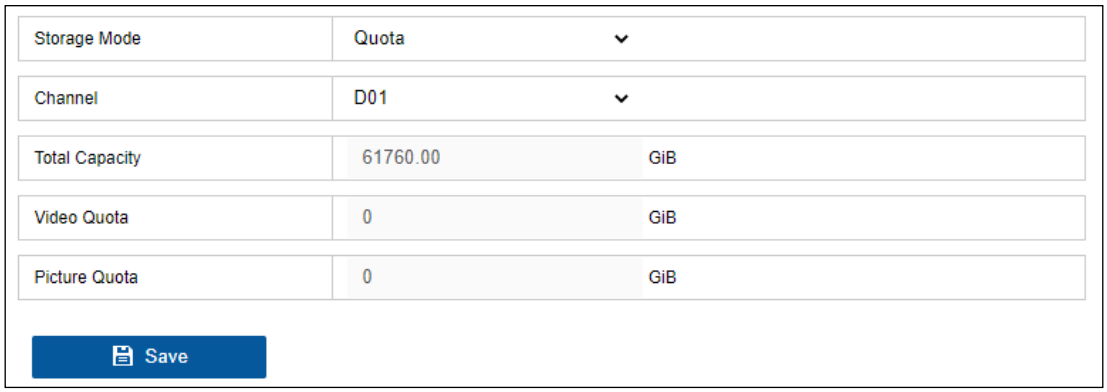


Figure 3-21 Advance Storage Mode

Step 2 Select the **Storage Mode** as **Quota**.

Note

Under quota mode, the CVR will use all storage spaces.

Step 3 Selece the **Channel** in the drop-down box.

Step 4 Set the quota for video and picture.

Note

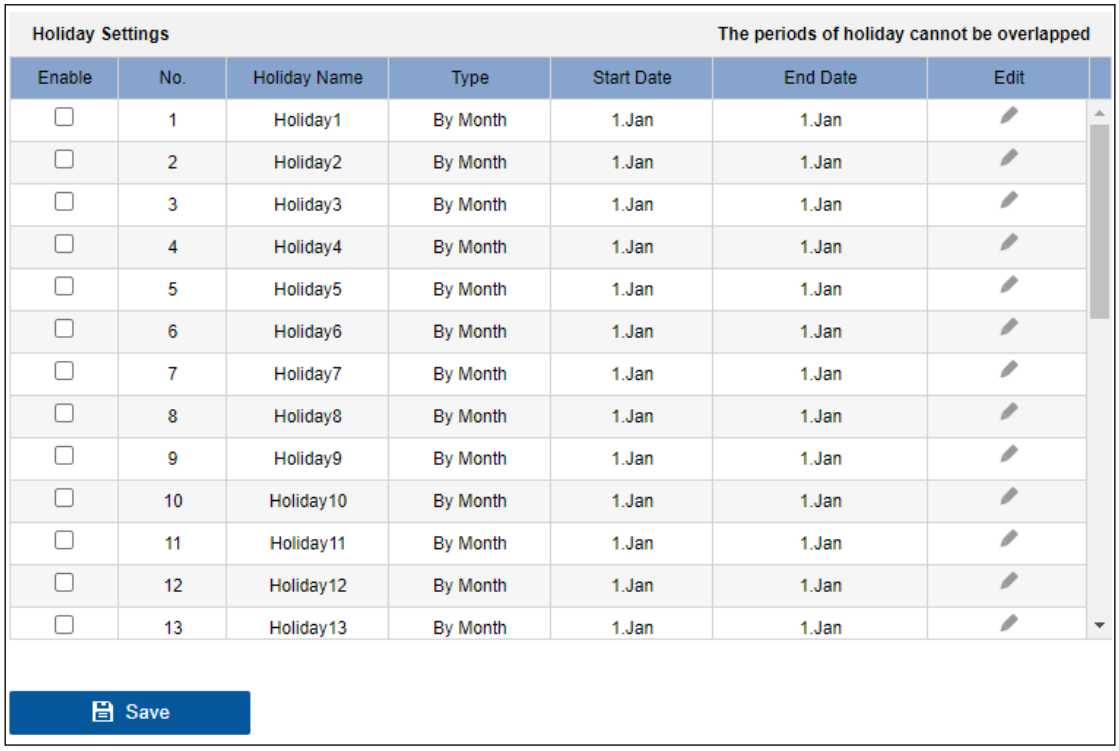
- When video quota and picture quota are set as 0, the videos of all channels would be recorded and overwritten as the same time.
- When video quota and picture quota are not set as 0, videos of the channel would be recorded as the preset space.
- The picture quota of quota mode refers to the pictures that are generated by network camera, differs from the pictures of direct storage.

Step 5 Click **Save**.

3.4.5 Advanced Settings

Holiday

Step 1 Go to **Configuration > Storage > Advanced Settings > Holiday**.



Holiday Settings — The periods of holiday cannot be overlapped

Enable	No.	Holiday Name	Type	Start Date	End Date	Edit
☐	1	Holiday1	By Month	1.Jan	1.Jan	
☐	2	Holiday2	By Month	1.Jan	1.Jan	
☐	3	Holiday3	By Month	1.Jan	1.Jan	
☐	4	Holiday4	By Month	1.Jan	1.Jan	
☐	5	Holiday5	By Month	1.Jan	1.Jan	
☐	6	Holiday6	By Month	1.Jan	1.Jan	
☐	7	Holiday7	By Month	1.Jan	1.Jan	
☐	8	Holiday8	By Month	1.Jan	1.Jan	
☐	9	Holiday9	By Month	1.Jan	1.Jan	
☐	10	Holiday10	By Month	1.Jan	1.Jan	
☐	11	Holiday11	By Month	1.Jan	1.Jan	
☐	12	Holiday12	By Month	1.Jan	1.Jan	
☐	13	Holiday13	By Month	1.Jan	1.Jan	

Save

Figure 3-22 Holiday Settings

Step 2 Click to edit holiday name, select holiday type, and set the start date and end date.

Step 3 Check the holiday.

Step 4 Click **Save** to make the holiday settings take effect.

Other

Step 1 Go to **Configuration > Storage > Advanced Settings > Other**.

Step 2 Check **Enable Overwriting**.

Note

After checked, after the HDD is full, the latest video files will overwrite the first video files one by one. If unchecked, recording will stop after the HDD is full.

Step 3 Click **Save**.

Chapter 4 Shortcut

The bar on top right corner of device webpage shows the shortcut buttons for quick configuration.

Figure 4-1 Shortcut

- : Mute alarm sound for alarm events. Only valid for current alarm events.
- : Show the exception alarm information. You can search alarm information by specifying alarm level and keyword.

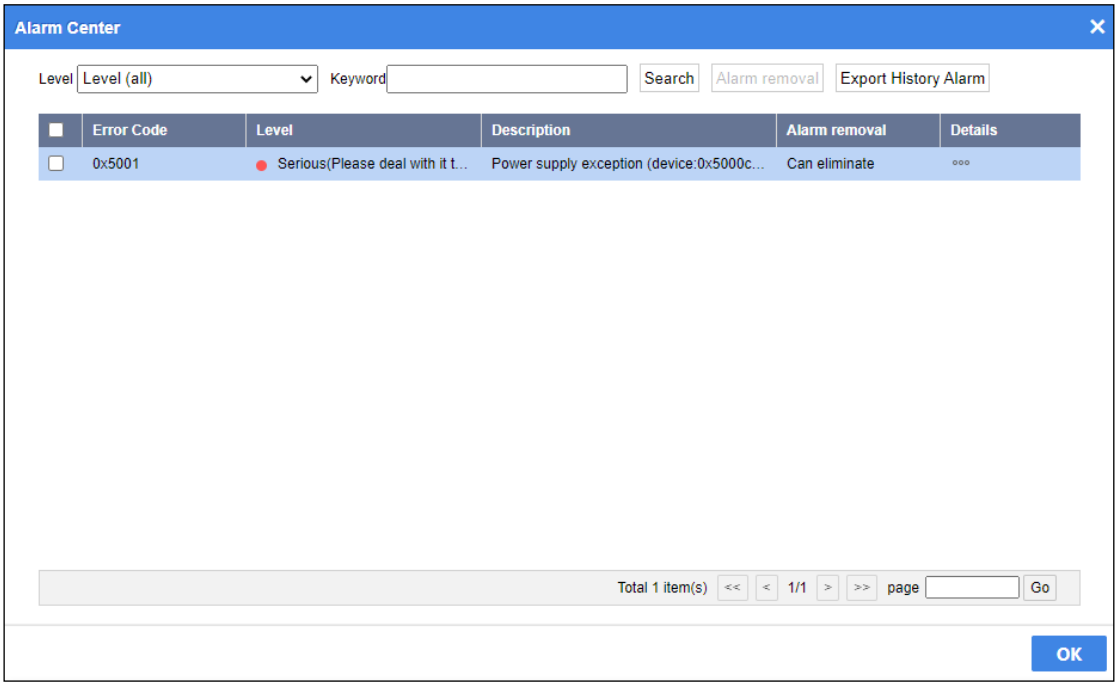


Figure 4-2 Alarm Center

- Search alarm information: Select the **Level** of the alarm, enter the **Keyword**, and click **Search** to search the alarm information
- Remove alarm: Select the alarm item(s) you want to eliminate, click **Alarm removal**, and enter the administrator password and verification code in the pop-up window to confirm the operation.
- Export history alarm: Click **Export History Alarm** to download the historical alarm information file to the local computer.

- : View quick start guide, user manual, and download Command Line Tool.

- : After following the wizard to complete quick configuration, click the icon and the following prompt will pop up to show that the system is configured.

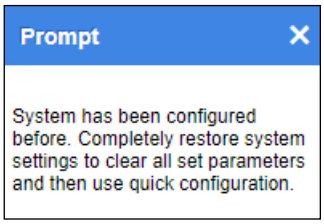


Figure 4-3 System Configuration Completion Prompt

- admin: Change admin password.

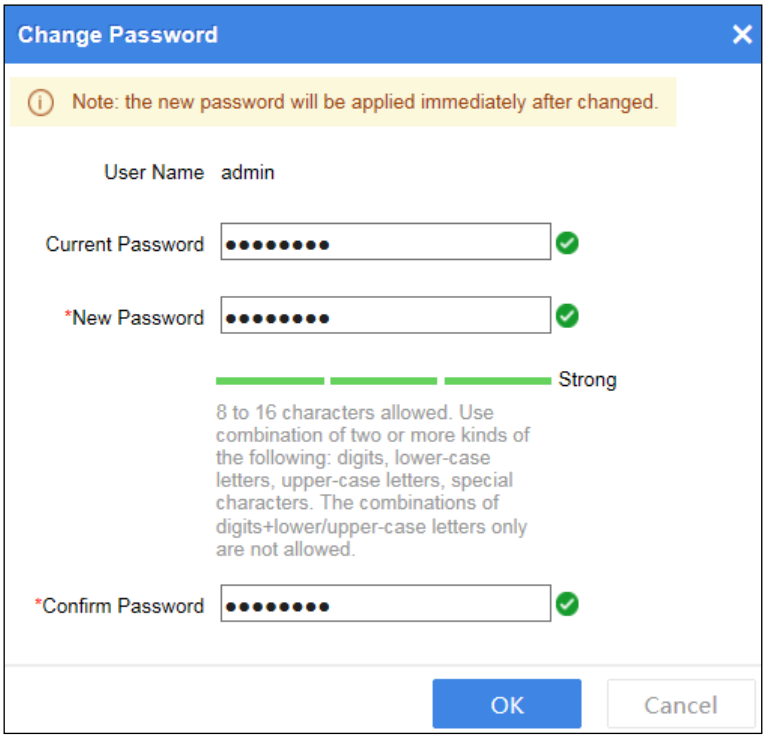


Figure 4-4 Change Password

- Logout: Log out system. At the next login, you will automatically enter the page of last login.

Chapter 5 Overview

5.1 Platform Overview

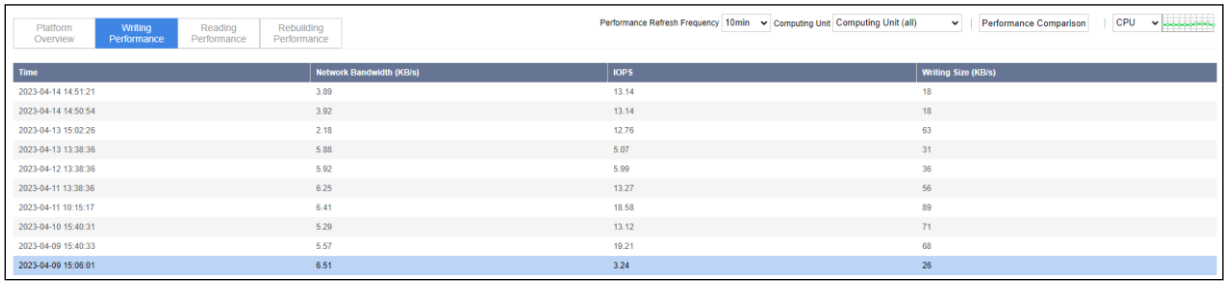
Step 1 Go to **Storage**.

Step 2 Select **Platform Overview** to view the IP address, running state, and number of mirrors.

5.2 View Performance

Step 1 Go to **Storage**.

Step 2 Click **Writing Performance**, **Reading Performance**, or **Rebuilding Performance** to view system performance.



Time	Network Bandwidth (KB/s)	IOPS	Writing Size (KB/s)
2023-04-14 14:51:21	3.89	13.14	18
2023-04-14 14:50:54	3.92	13.14	18
2023-04-13 15:02:26	2.18	12.76	63
2023-04-13 13:38:36	5.88	5.07	31
2023-04-12 13:38:36	5.92	5.99	36
2023-04-11 13:38:36	6.25	13.27	56
2023-04-11 10:15:17	6.41	18.58	89
2023-04-10 15:40:31	5.29	13.12	71
2023-04-09 15:40:33	5.57	19.21	68
2023-04-09 15:06:01	6.51	3.24	26

Figure 5-1 System Performance

Table 5-1 Performance Description

Status	Description
Writing performance	Shows the time, network bandwidth, IOPS, and writing size.
Reading performance	Shows the time, network bandwidth, IOPS, and reading size.
Rebuilding performance	Shows the time and speed.

Step 3 Set the **Performance Refresh Frequency**.

Step 4 Compare the writing, reading, and rebuilding performances of different devices.

1) Click **Performance Comparison**.
2) Click **Select Device**.
3) Check the device you want to compare and click **OK**.

Note

Up to 5 devices can be selected for performance comparison.

Step 5 (Optional) Select the **Computing Unit** to filter performance to show.

Note

Selecting computing unit is only available for dual-controller devices.

5.3 View CPU and Memory Usage

Purpose:

You can view the CPU and memory usage, number of cores, and total memory.

Step 1 Go to **Storage**.

Step 2 Select **CPU** or **Memory** to view.

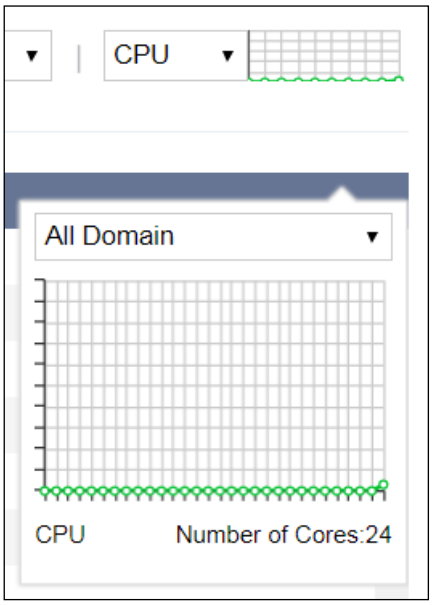


Figure 5-2 View CPU and Memory Performance

Chapter 6 Device

6.1 Node Tree

6.1.1 View Node Tree

Step 1 Go to **Device**.

Step 2 Click of node tree dropdown list.

Step 3 Click to show device name.

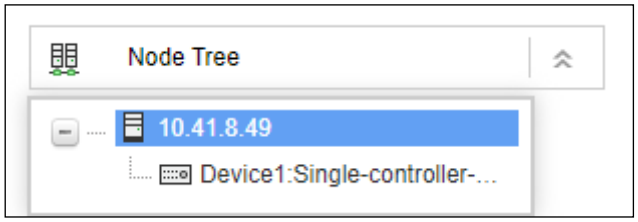


Figure 6-1 Node Tree

6.1.2 Map

Step 1 Go to **Device**.

Step 2 Click a node in node tree to refresh the topological graph of network switch node and the topological graph of specified device.

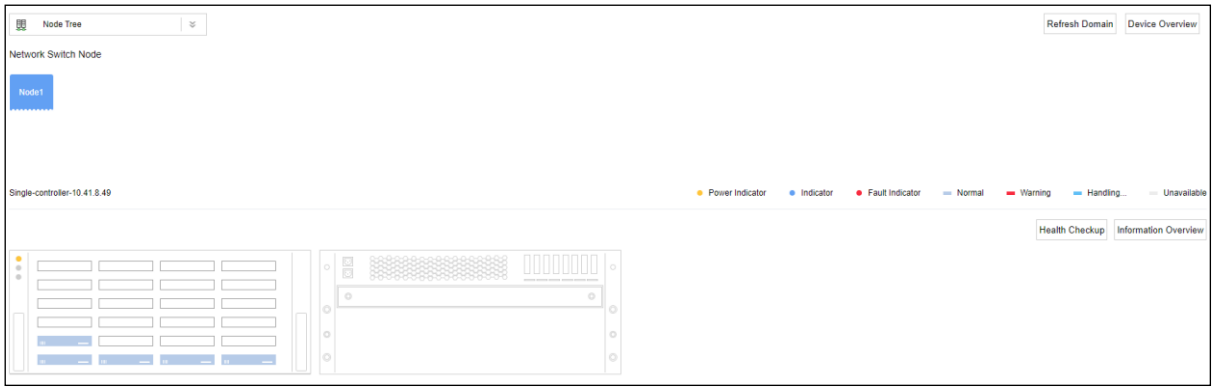


Figure 6-2 Node Mapping

6.2 Node Status

Step 1 Go to **Device**.

Step 2 Position the mouse on a node to show node status, including **Device Name, Device Status, Serial No.**, and **Product Model**.

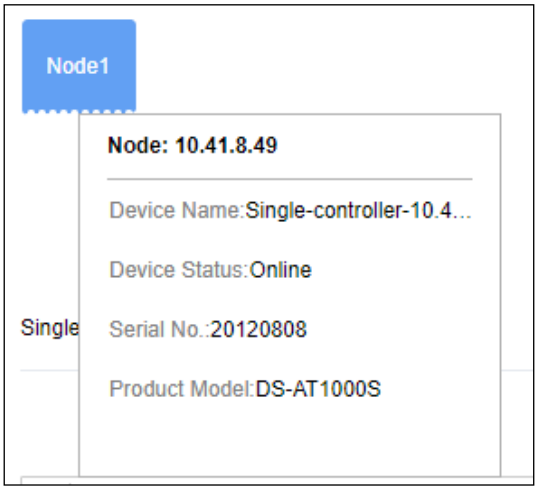


Figure 6-3 Node Status

6.3 Refresh Domain

Step 1 Go to **Device**.

Step 2 Click **Refresh Domain**.

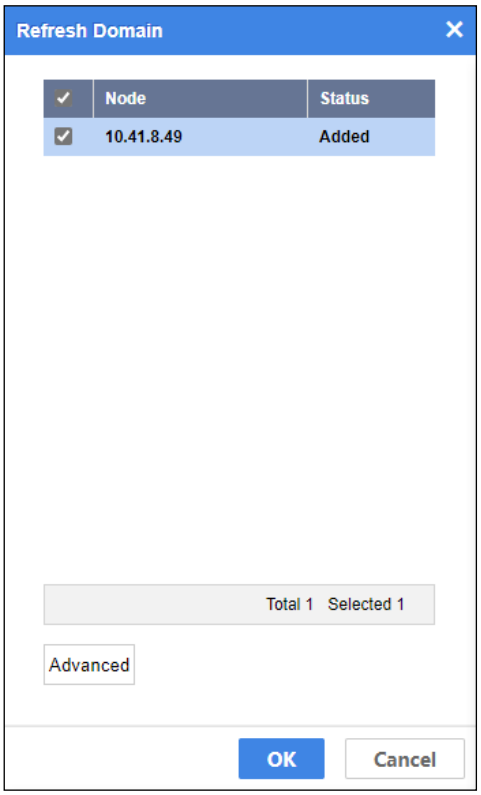


Figure 6-4 Refresh Domain

Step 3 Check the node(s) you want to refresh.

Step 4 (Optional) Click **Advanced** to set **domainIP** and **Subnet Mask**.

Step 5 Click **OK** to refresh domain.

6.4 Device Overview

Go to **Device** and click **Device Overview** to view device name, IP address, port, status, etc.

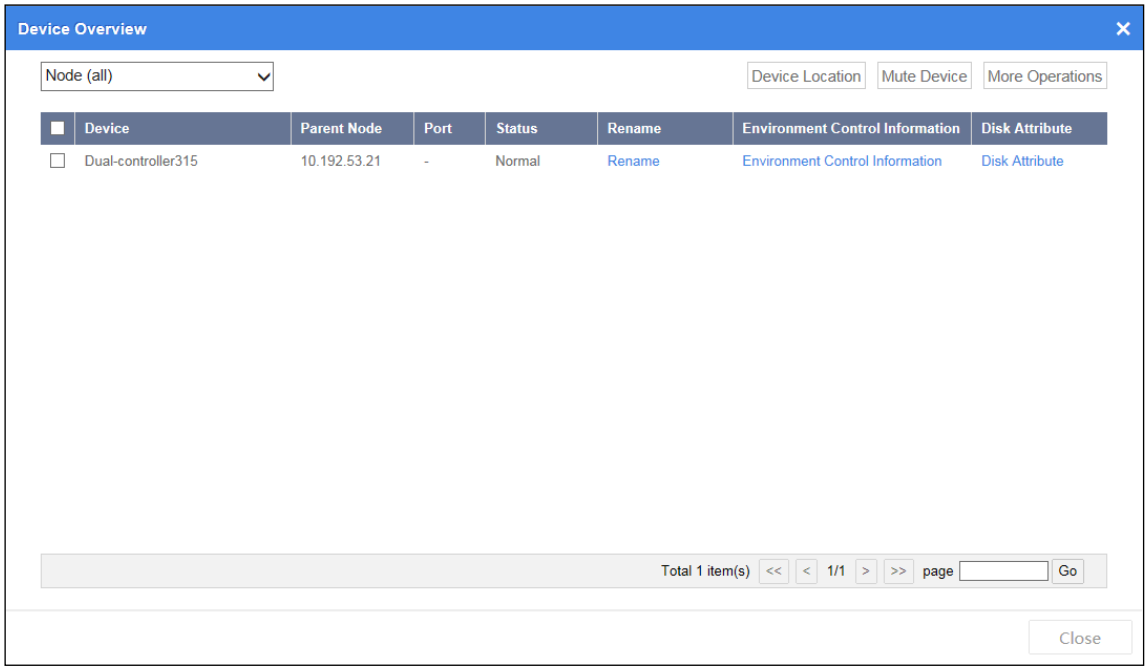


Figure 6-5 Device Overview

6.4.1 Locate Device

Purpose:

To find a device, turn on FN indicator on its front panel.

Step 1 Check the device.

Step 2 Click **Device Location**. FN indicator of the selected device will keep flashing for 10 minutes.

6.4.2 Mute Device

Purpose:

Turn off alarm sound of a device.

Step 1 Check the device.

Step 2 Click **Mute Device**. Device alarm sound will be turned off.

6.4.3 Reboot and Shut down Device

Purpose:

Restart or shut down a device.

Step 1 Check the device.

Step 2 Click **More Operations**.

Step 3 Select **Device Restart** or **Device Shutdown**.

Step 4 Enter the administrator password and verification code to confirm the operation.

6.4.4 More Operations

- Rename a device. For details, refer to *Rename Device*.
- Modify device network parameters. For details, refer to *View Environment and Control Information*.
- Modify HDD property. For details, refer to *Manage Disk*.

6.5 Device Graph of a Node

The bottom half of the **Device** page shows the device graph, device name, and device indicators.

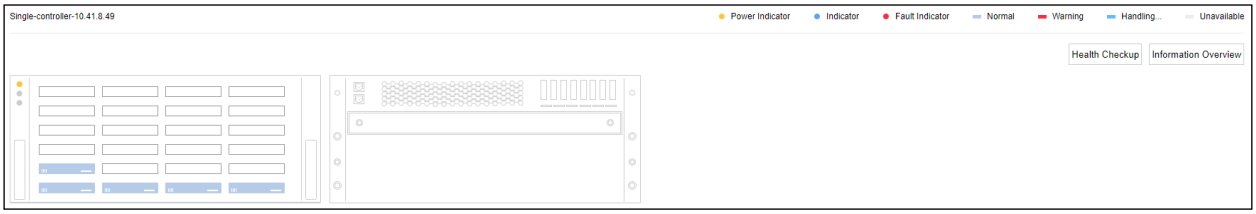


Figure 6-6 Device Graph

6.5.1 Device Indicator

Status Indicator

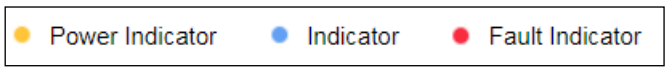


Figure 6-7 Status Indicator

Table 6-1 Indicator Description

No.	Description
Power indicator	● Yellow: Default. ● Grey: Device is powered off or shut down.
FN indicator	Blue.
Fault indicator	Red: Device is abnormal.

HDD Indicator

Figure 6-8 HDD Indicator

Table 6-2 Indicator Description

No.	Description
Normal	Blue: HDD detection is normal.
Warning	Red: HDD is not available instantly after HDD detection. Only after repair can you decide if the HDD is normal or not.
Handling	Light blue: HDD is being detected or located.
Unavailable	Grey: HDD detection fails and HDD cannot be repaired.

6.5.2 HDD Slot Graph

Purpose:

HDD slot graph shows the HDD working status.

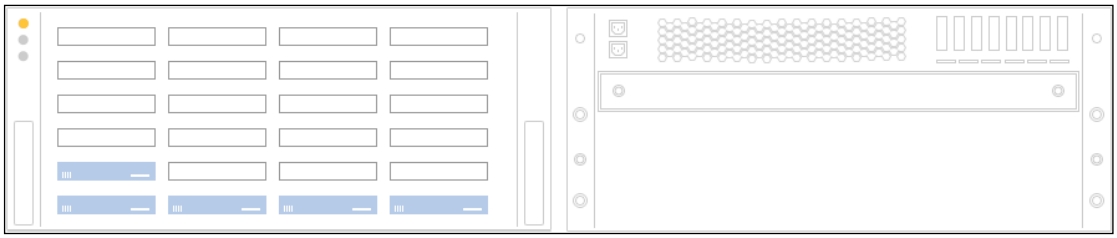


Figure 6-9 HDD Slot Graph

Step 1 Go to **Device**.

Step 2 Click an HDD slot. Then the disk information window will pop up.

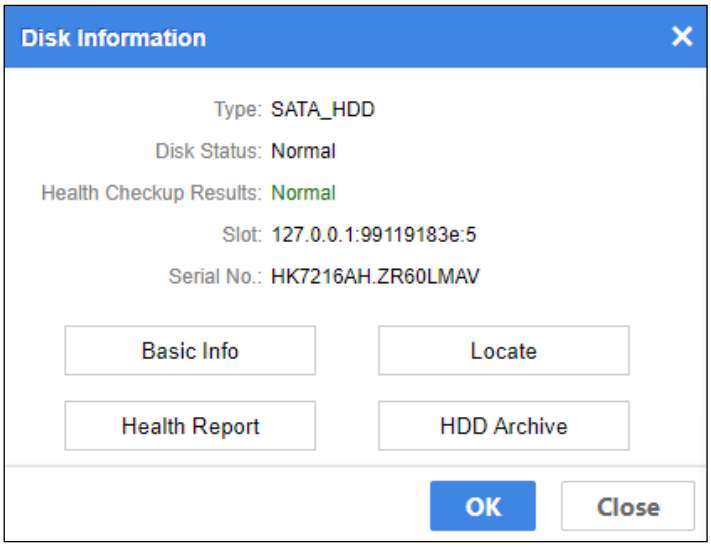


Figure 6-10 Disk Information

- **Basic Info**: Click to show the status, statistics data, and S.M.A.R.T. information of HDD.
- **Locate**: Click to turn on FN indicator of the selected HDD. The indicator will keep flashing (default flashing time is 600 seconds).
- **Health Report**: Click to show the health checkup results. For details, please refer to View Health Checkup Report.
- **HDD Archive**: For details, please refer to View HDD Archive.

6.5.3 Health Checkup

View Health Checkup Report

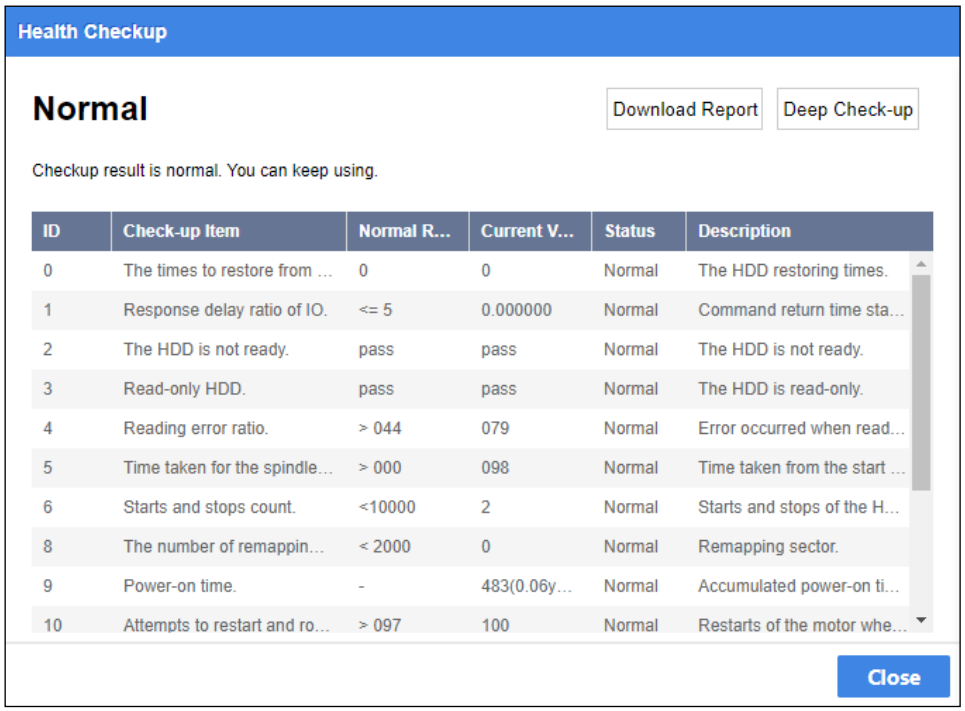
Step 1 Go to **Device**.

Step 2 Click **Health Checkup**.

Step 3 Check the **Health Checkup Results** of HDD.

Step 4 Click to view the health report.

You can view all health check-up items and the normal value, current value, health status, and description of each check-up item.



ID	Check-up Item	Normal R...	Current V...	Status	Description
0	The times to restore from ...	0	0	Normal	The HDD restoring times.
1	Response delay ratio of IO.	<= 5	0.000000	Normal	Command return time sta...
2	The HDD is not ready.	pass	pass	Normal	The HDD is not ready.
3	Read-only HDD.	pass	pass	Normal	The HDD is read-only.
4	Reading error ratio.	> 044	079	Normal	Error occurred when read...
5	Time taken for the spindle...	> 000	098	Normal	Time taken from the start ...
6	Starts and stops count.	<10000	2	Normal	Starts and stops of the H...
8	The number of remappin...	< 2000	0	Normal	Remapping sector.
9	Power-on time.	-	483(0.06y...	Normal	Accumulated power-on ti...
10	Attempts to restart and ro...	> 097	100	Normal	Restarts of the motor whe...

Figure 6-11 Health Report

Step 5 Download the health checkup report.

- Click and click **Download Report** to download the health checkup report.
- Check HDDs and click to download multiple HDD health check reports.

Step 6 Click **Deep Check-up** to start a deep check-up.

Note

The deep check-up may cost HDD resource and affect the performance.

Start an Isolated Deep Checkup

Step 1 Go to **Device**.

Step 2 Click **Health Checkup**.

Step 3 Click to start an isolated deep checkup.

View HDD Archive

Step 1 Go to **Device**.

Step 2 Click **Health Checkup**.

Step 3 Click to view HDD archive.

Step 4 Check the growth trend of bad sector(s), temperature, and vibration.

1) Click **Trend**.

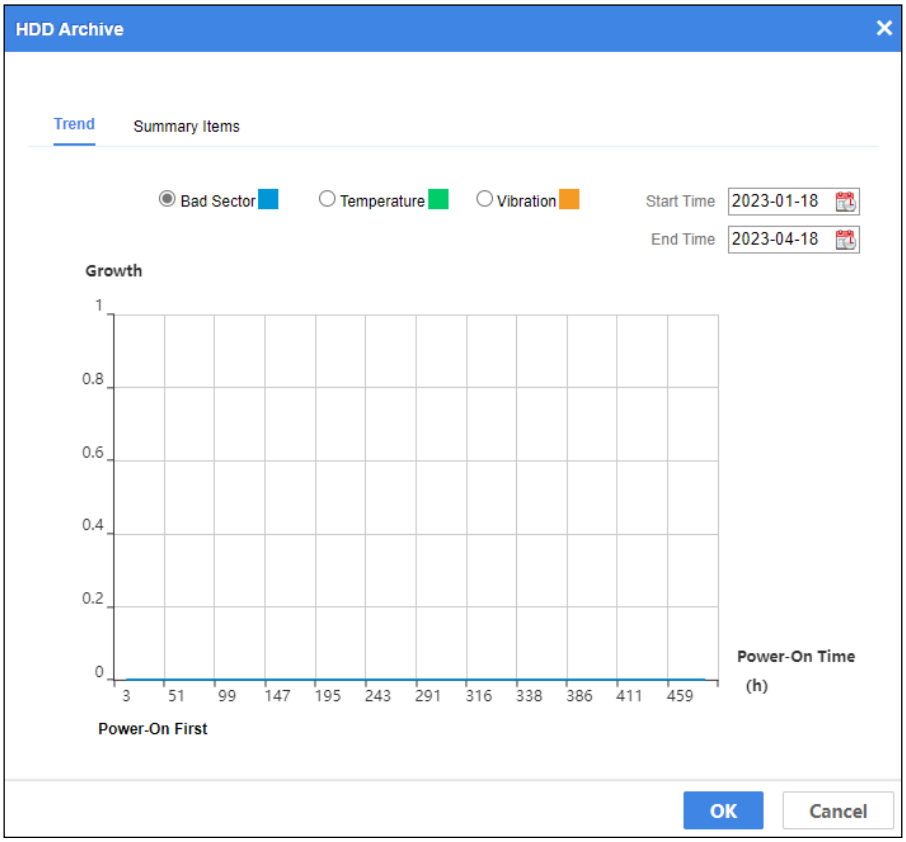


Figure 6-12 Growth Trend

2) Set the start time and end time.
3) Check **Bad Sector**, **Temperature**, or **Vibration**.
4) View the growth trend in the line chart below.

Step 5 Check the summary items.

1) Click **Summary Items**.

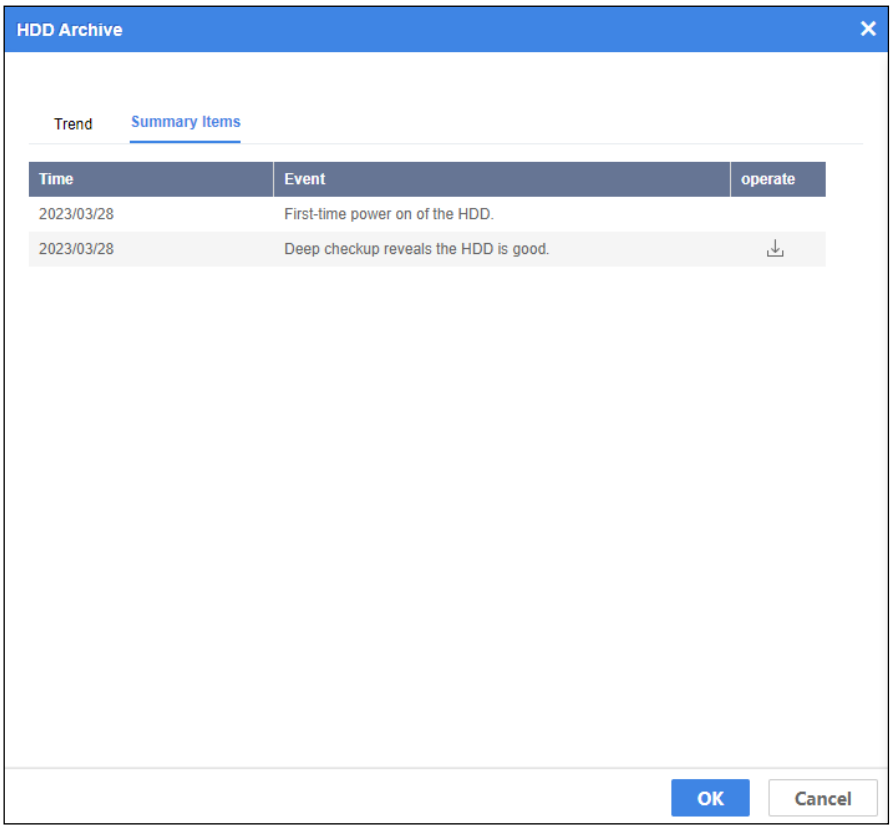


Figure 6-13 Summary Items

2) View the time and events.
3) Click to download logs.

6.5.4 Information Overview

Purpose:

View environment and control information, manage disks, mute device, etc.

View Environment and Control Information

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 View environment and control information.

- **Temperature**: Temperature of CPU, IC, system, etc.
- **Fan**: Working status of chassis fan.
- **Power**: Power module working status.

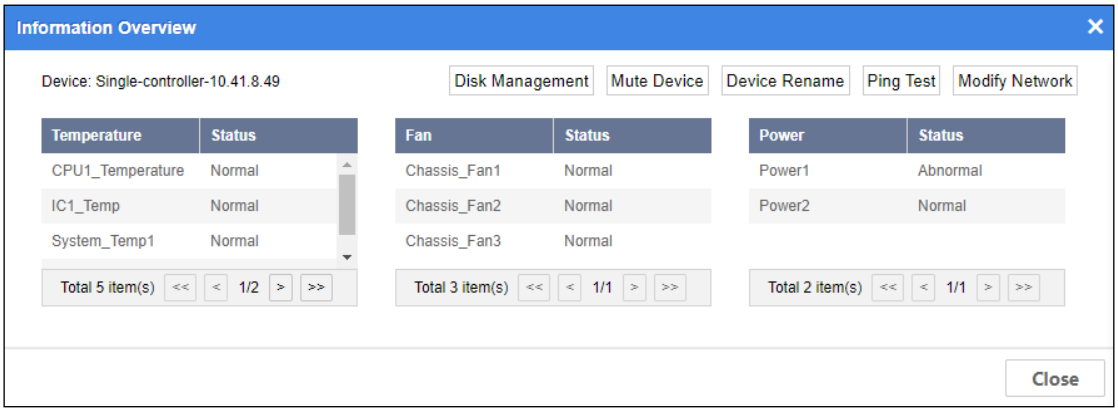


Figure 6-14 Information Overview

Manage Disk

Purpose:

You can search the information of all the HDDs in storage device.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Disk Management**.

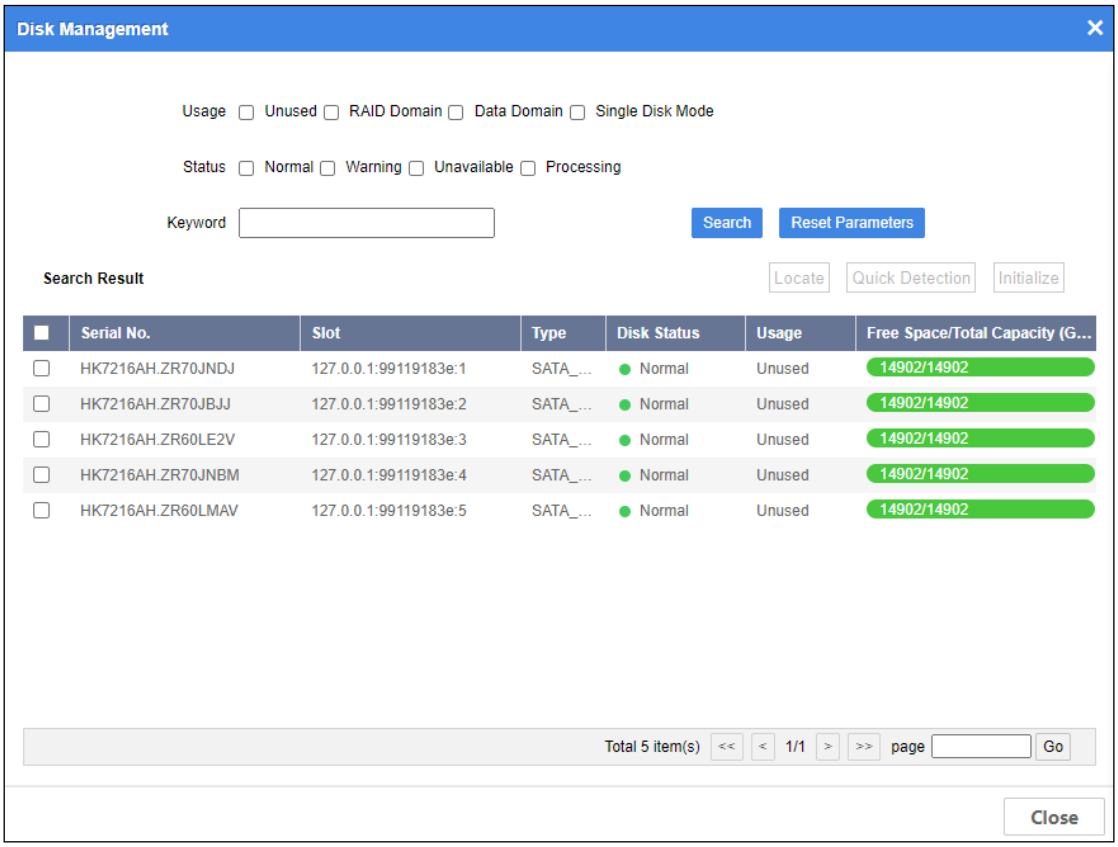


Figure 6-15 Disk Management

Step 4 Specify search conditions.

Usage

- **Unused**: Disk not used by any RAID domain.
- **Single Disk Mode**: Reserved.

Status

- **Normal**: Disk is normal in all online nodes.
- **Warning**: Disk is normal in some online nodes. Or bad sector exists in the disk.
- **Unavailable**: Disk is abnormal in all the online nodes. Disk will be removed from resource pool.
- **Processing**: Disk is being detected, located, repaired, moved, or maintained.

Step 5 (Optional) Enter the keyword.

Step 6 Click **Search**.

Note

When disk status is warning, unavailable, or processing, click the status in status column to show help. You can follow the help to recover disk.

Step 7 (Optional) To locate a disk, check the disk and click **Locate** to turn on FN indicator of the disk. FN indicator will keep flashing (default flashing time is 600 seconds).

Step 8 (Optional) To detect a disk, check the disk and click **Quick Detection**. Detection progress will be shown in **Status** column.

Step 9 (Optional) To initialize a disk, check the disk and click **Initialize**. Enter the admin password and verification code to initialize HDD.

Note

Initialize the HDD will cause its data loss. Please proceed with caution.

Mute Device

Purpose:

When device is abnormal and sending alarm sound, you can mute it.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Mute Device**.

Rename Device

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Device Rename**.

Step 4 Enter **New Name** and click **OK**.

Note

Device name must be unique in the domain. Valid name contains 1 to 16 characters and only digits, lowercase, and uppercase are allowed.

Perform Ping Test

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Ping Test**.

Step 4 Enter the **Test IP Address**, set **Test Time** and **Data Package Size**.

Step 5 Click **Test**.

Step 6 Check the **Connection Status**.

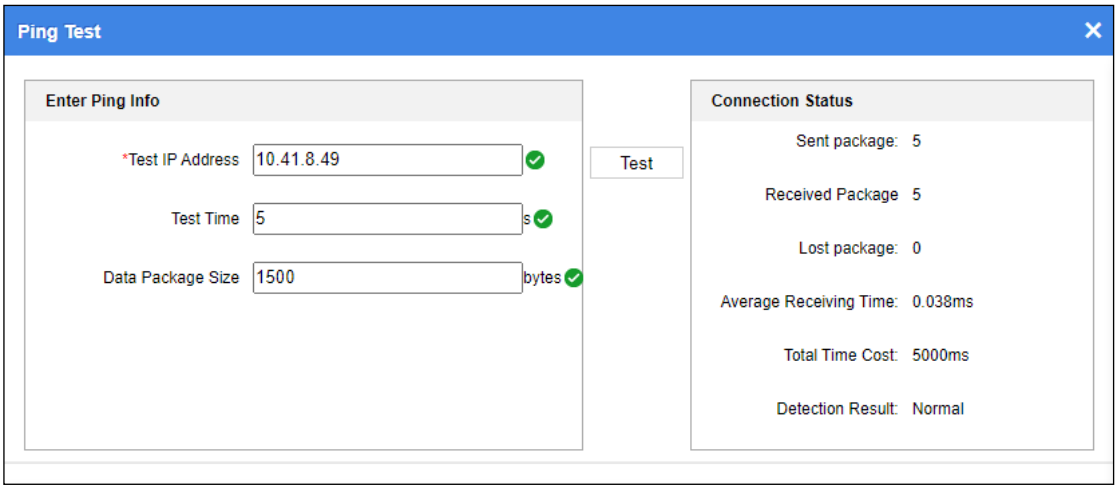


Figure 6-16 Ping Test

Modify Network

You can view port name, status, speed, IP address, subnet mask, gateway IP, and jumbo frame size, bound ports, and modify network parameters.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

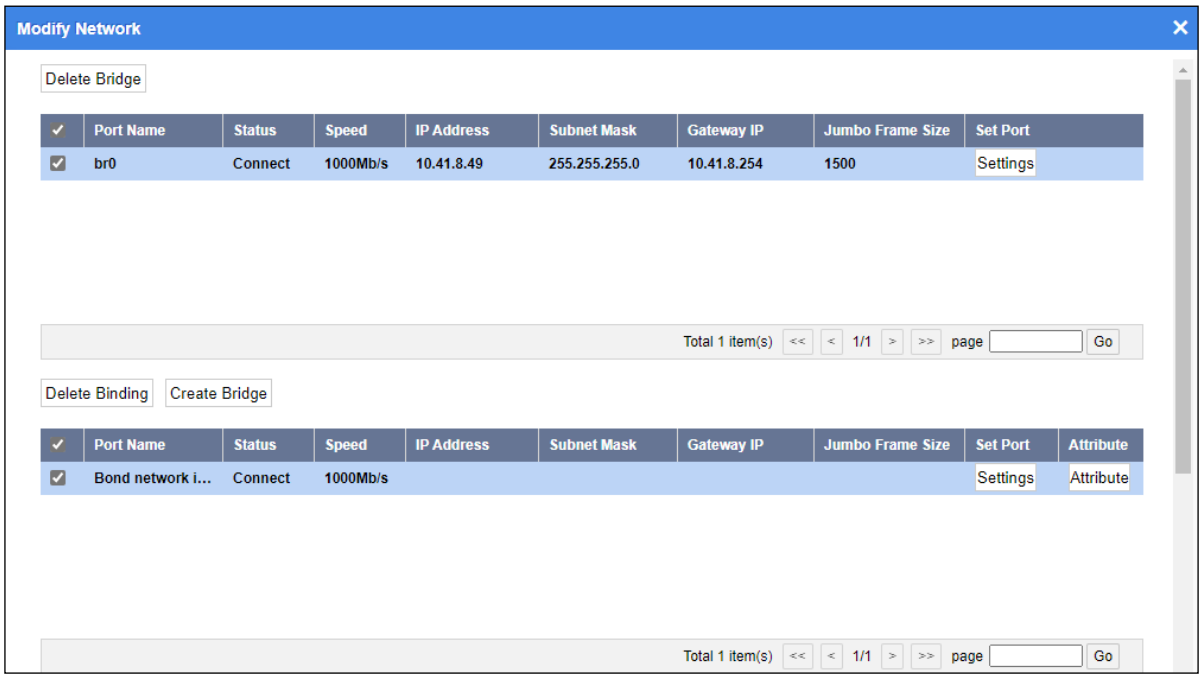


Figure 6-17 Modify Network

Set Bound Port

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Click **Settings** of a bound port.

Port Name

Not editable.

Select Mode

3 bound modes are selectable. Default mode is **active-backup**.

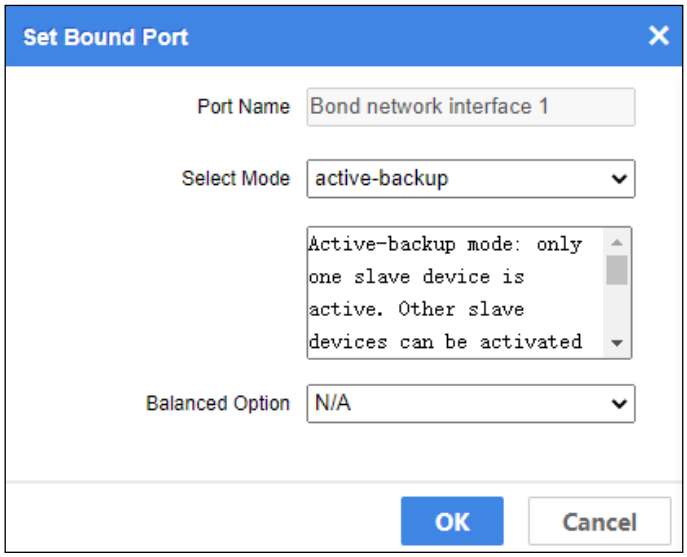


Figure 6-18 Set Bound Port

Note

- Management port does not support port binding.
- Connect all bound ports to network.

View Bound Port Attribute

Purpose:

View bound port attribute, including port name, port attribute, binding mode, etc.

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Click **Attribute** of a bound port.

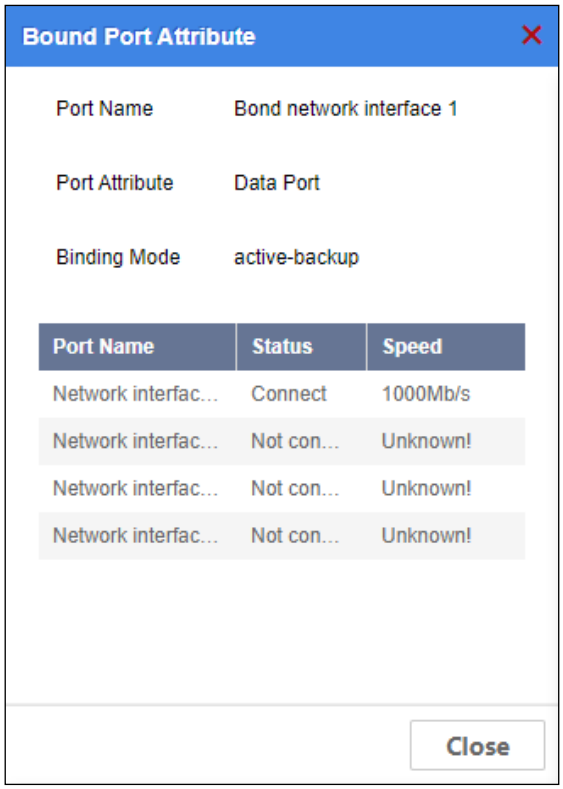


Figure 6-19 Bound Port Attribute

Delete Bound Port

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click **Modify Network**.

Step 4 Check bound port to delete.

Step 5 Click **Delete Binding**.

Step 6 Click **OK** in message box to confirm the operation.

Note

Unbounded ports will be listed in top half of the page.

Set Port Parameters

Step 1 Go to **Device**.

Step 2 Click **Information Overview**.

Step 3 Click Modify Network.

Step 4 Click **Settings** of unbounded port to configure its network parameters.

Port Name

Not editable.

Jumbo Frame Size

Default value is 1500. Default value is recommended.

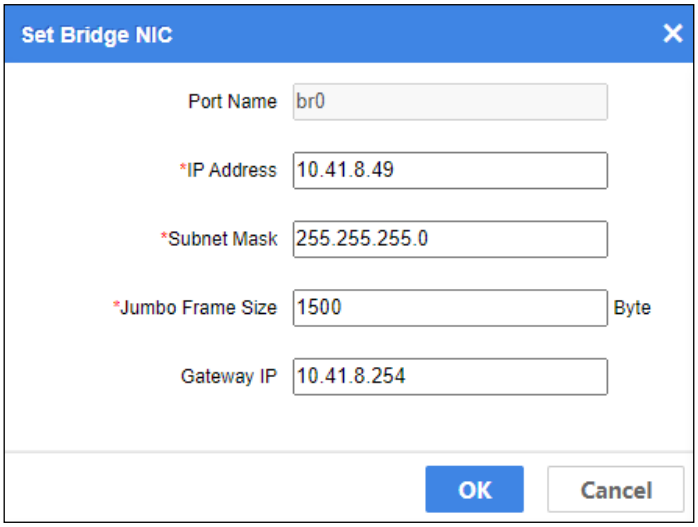


Figure 6-20 Set Port Parameters

Chapter 7 Resource

Purpose:

Manage resource pool and RAID.

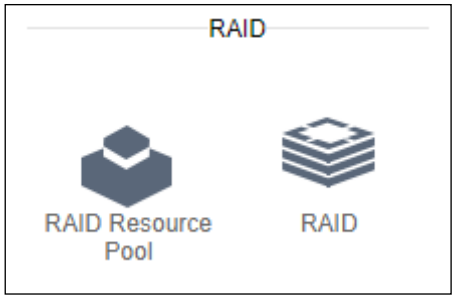


Figure 7-1 Details and Management

7.2 Manage RAID Resource Pool

Step 1 Go to **Resource**.

Step 2 Click **RAID Resource Pool**.

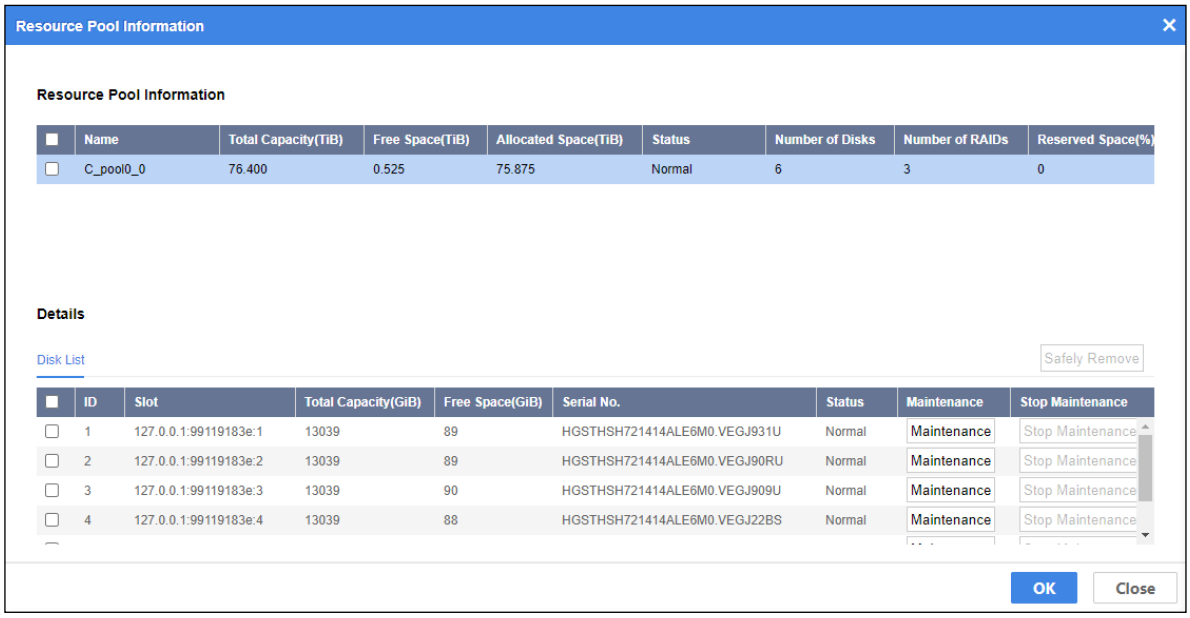


Figure 7-2 Resource Pool Information

Step 3 View the resource pool information and disk information.

7.2.2 Maintain Disks

Step 1 Go to **Resource**.

Step 2 Click **RAID Resource Pool**.

Step 3 In the **Disk List**, click **Maintenance** in the information bar of the disk that need to be maintained.

Step 4 Click **Stop Maintenance** to stop disk maintenance.

7.2.3 Safely Remove Disks

Step 1 Go to **Resource**.

Step 2 Click **RAID Resource Pool**.

Step 3 In the **Disk List**, check disk(s) to be removed.

Step 4 Click **Safely Remove**.

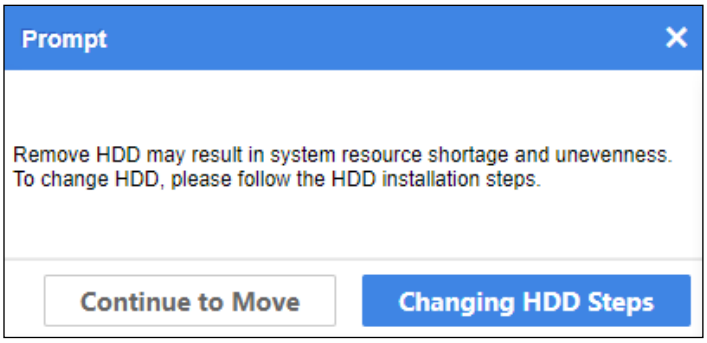


Figure 7-3 Disk Removal Prompt

Step 5 Remove disks or change disks.

- Click **Continue to Move** to remove the selected disk(s) safely.
- Click to view **Changing HDD Steps** and follow the steps.

7.3 Manage RAID

Step 1 Go to **Resource**.

Step 2 Click **RAID** to view RAID information.

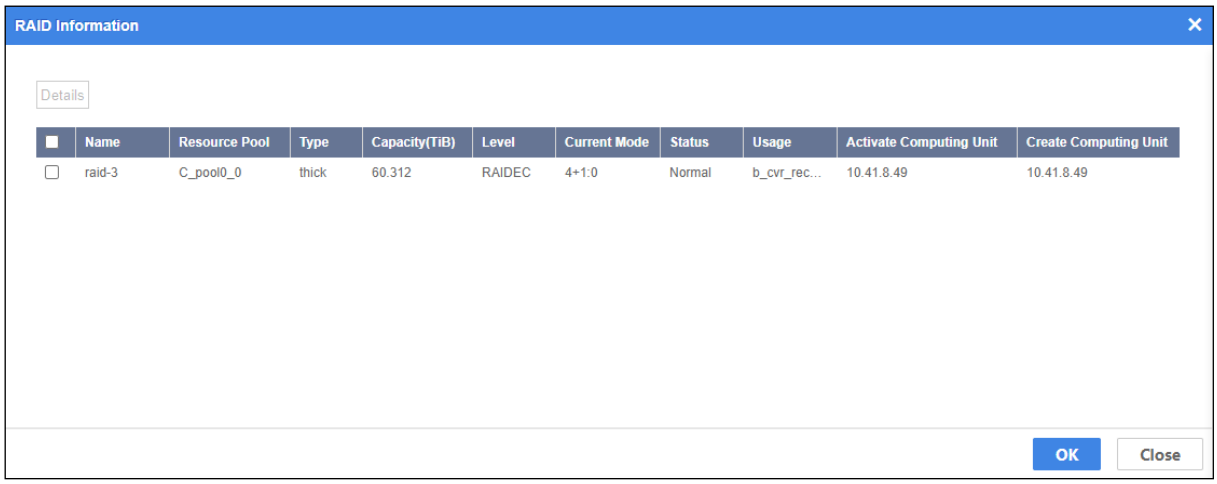


Figure 7-4 RAID Information

Step 3 Check RAID and click **Details** to view RAID details.

Chapter 8 Storage

Purpose:

Manage service and mirror.

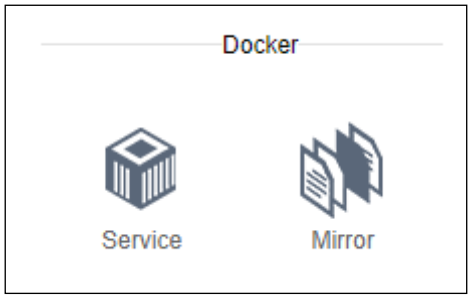


Figure 8-1 Storage

8.2 Service

8.2.1 Service Management

Step 1 Go to **Storage > Service > Service Management**.

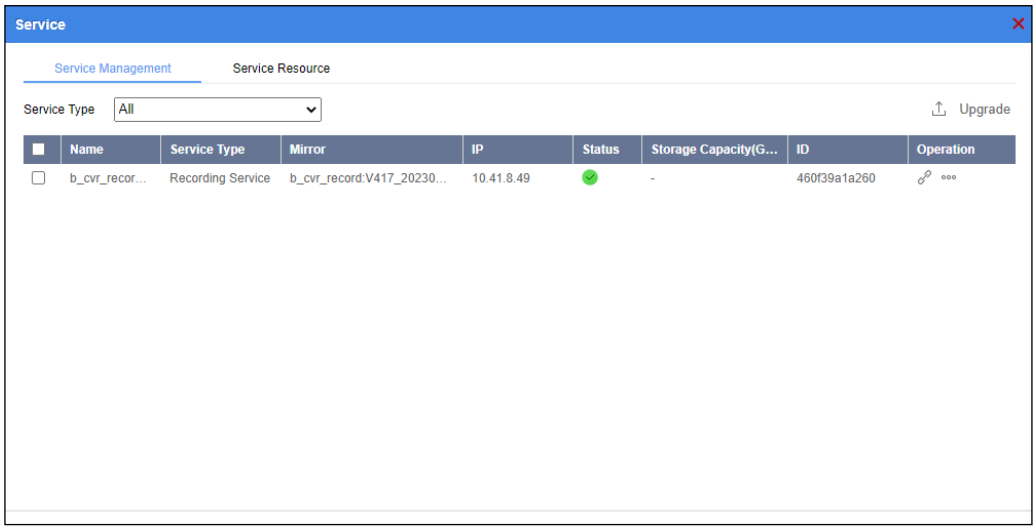


Figure 8-2 Service Management

Step 2 Select **Service Type**.

View the service information.

Redirect to Hybrid SAN System

Step 1 Click to redirect to the Hybrid SAN system.

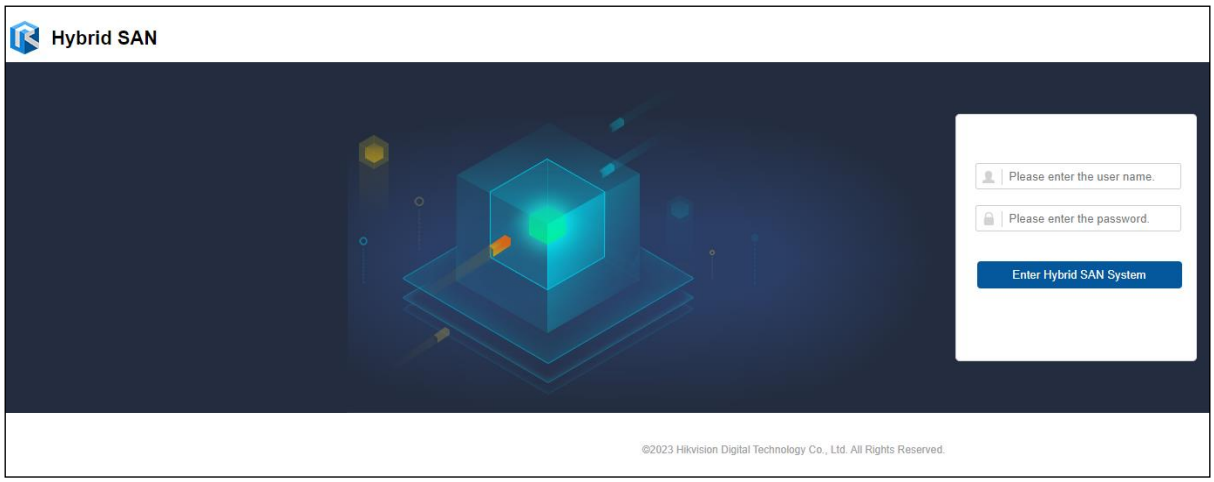


Figure 8-3 Hybrid SAN System

Step 2 Enter the user name and password.

Step 3 Click **Enter Hybrid SAN System**.

Step 4 Configure the Hybrid SAN system. Refer to Hybrid SAN Sub-System Configuration.

Switch Service

Step 1 Click ⋯.

Step 2 Click **Switch Service**.

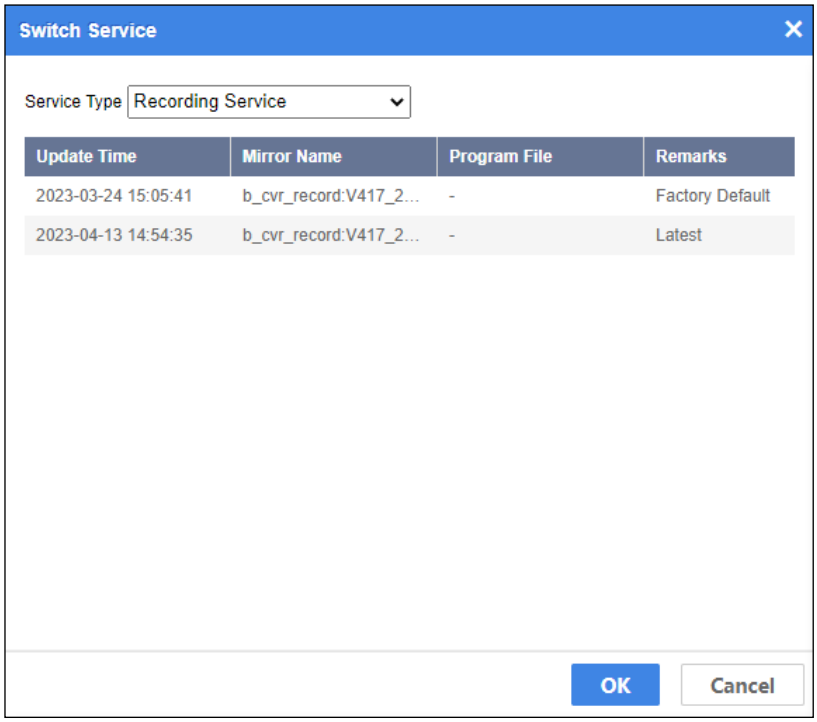


Figure 8-4 Switch Service

Step 3 Select the **Service Type** in the drop-down box.

Step 4 Select the service version to switch to.

Step 5 Click **OK**.

Modify Service

Step 1 Click ⋯.

Step 2 Click **Modify Service**.

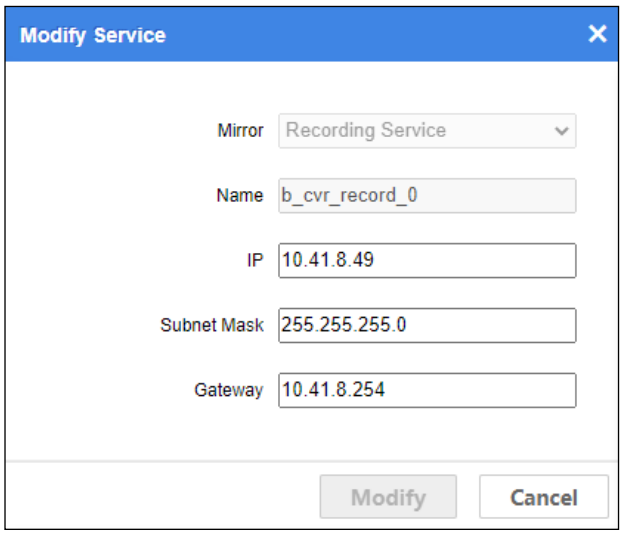


Figure 8-5 Modify Service

Step 3 Edit the **IP**, **Subnet Mask**, and **Gateway** of the service.

Step 4 Click **Modify**.

Pause Service

Step 1 Click ⋯.

Step 2 Click **Pause Service**.

The Status icon switches to ⏸.

Step 3 Click **Start Service** to recover.

Upgrade Service

Step 1 Check the service.

Step 2 Click **Upgrade**.

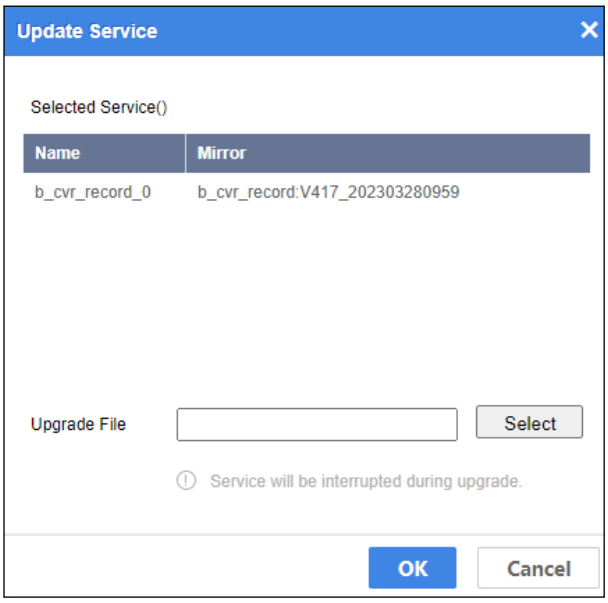


Figure 8-6 Upgrade Service

Step 3 Click **Select** to select and open an upgrade file.

Step 4 Click **OK**.

8.2.2 Service Resource

Step 1 Go to **Storage > Service > Service Resource**.

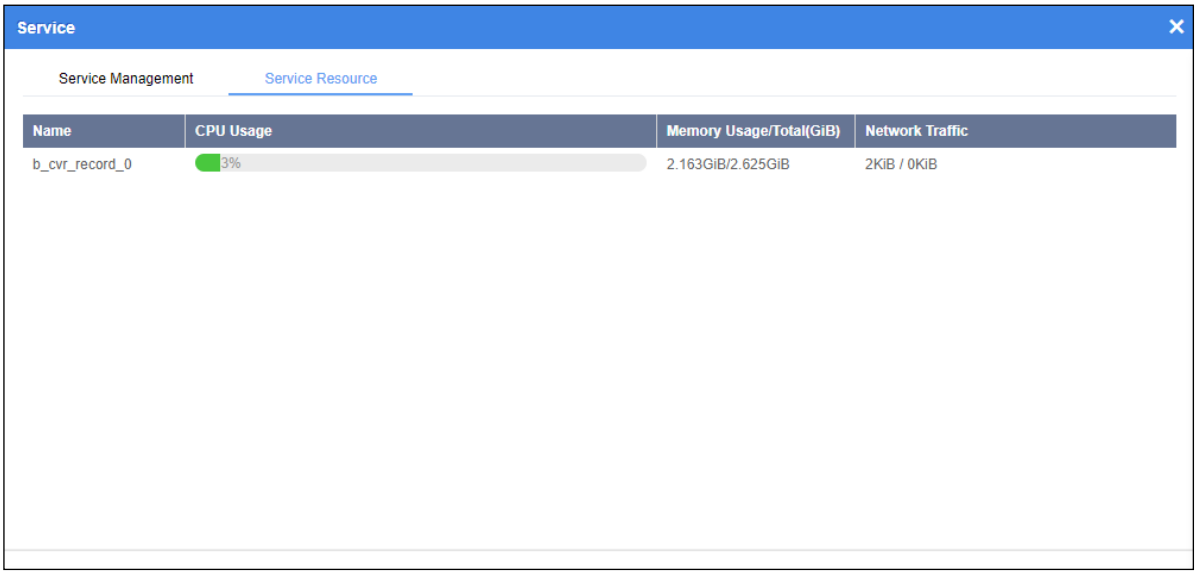


Figure 8-7 Service Resource

Step 2 View the service resource information.

8.3 Mirror

Step 1 Go to **Storage**.

Step 2 Click **Mirror**.

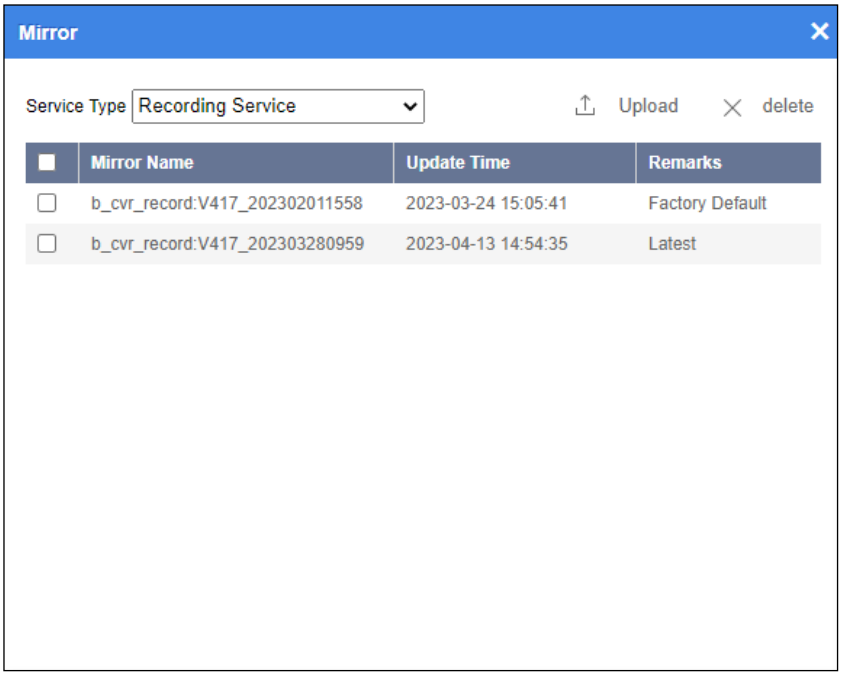


Figure 8-8 Mirror

Step 3 Select the **Service Type** in the drop-down box.

View the **Name**, **Update Time** and **Remarks** of the mirrors.

Step 4 Click **Upload** and select a mirror to upload.

Step 5 Check the mirror(s) to delete and click **delete**.

Chapter 9 Log

9.1 Search Log

Step 1 Go to **Log**.

Step 2 Specify search conditions.

Step 3 Click **Search**.

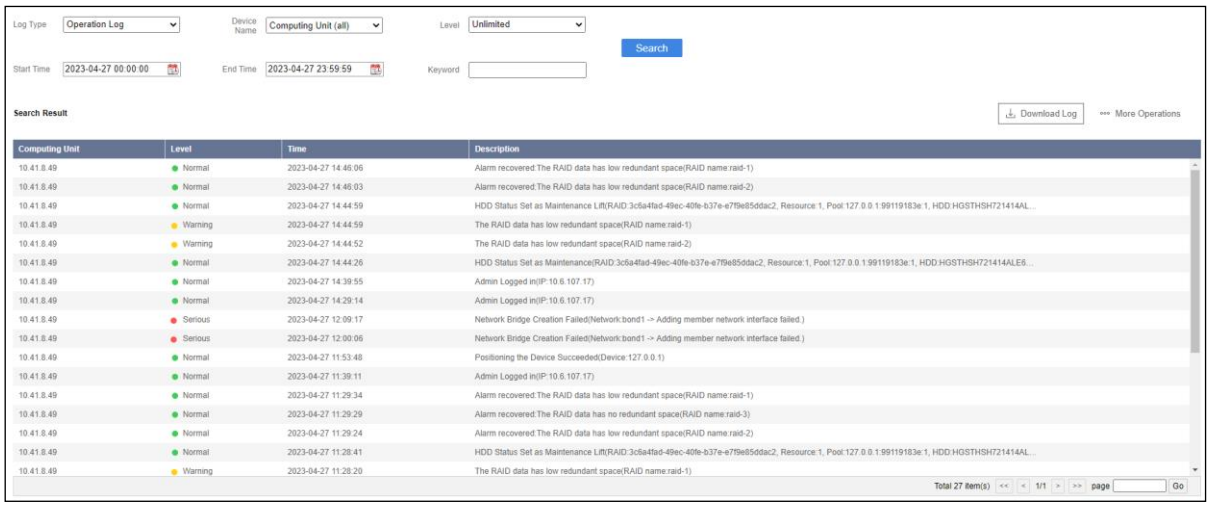


Figure 9-1 Log

9.2 Download Log

Before you start:

Enable web browser file download permission by going to **Options > Security > Internet > Custom Level Download**.

Step 1 Go to **Log**.

Step 2 Click **Download Log**.

Step 3 Check **Maintenance Log** or **Module Log**.

Step 4 Specify download conditions.

- Maintenance log: Select log type in **Downloads** drop-down box, and select **Download Mode**.
- Module log: Select the module in **Downloads** drop-down box..

Step 5 Check the computing unit to download.

Step 6 Click **Download**.

View the download progress in **Progress**.

9.3 Clear Log

Step 1 Go to **Log**.

Step 2 Click **More Operations** and select **Clear Log**.

Step 3 Enter **Admin Password** and **Verification Code.**

Step 4 Click **OK** to confirm the operation.

Note

The operation will clear all logs in device. You are recommended to back up logs before clearing.

Chapter 10 Maintenance

10.1 Version Information

Step 1 Go to **Maintenance**.

Step 2 Click **Version Information**.

Step 3 Select a node in **Node List**.

View the version information.

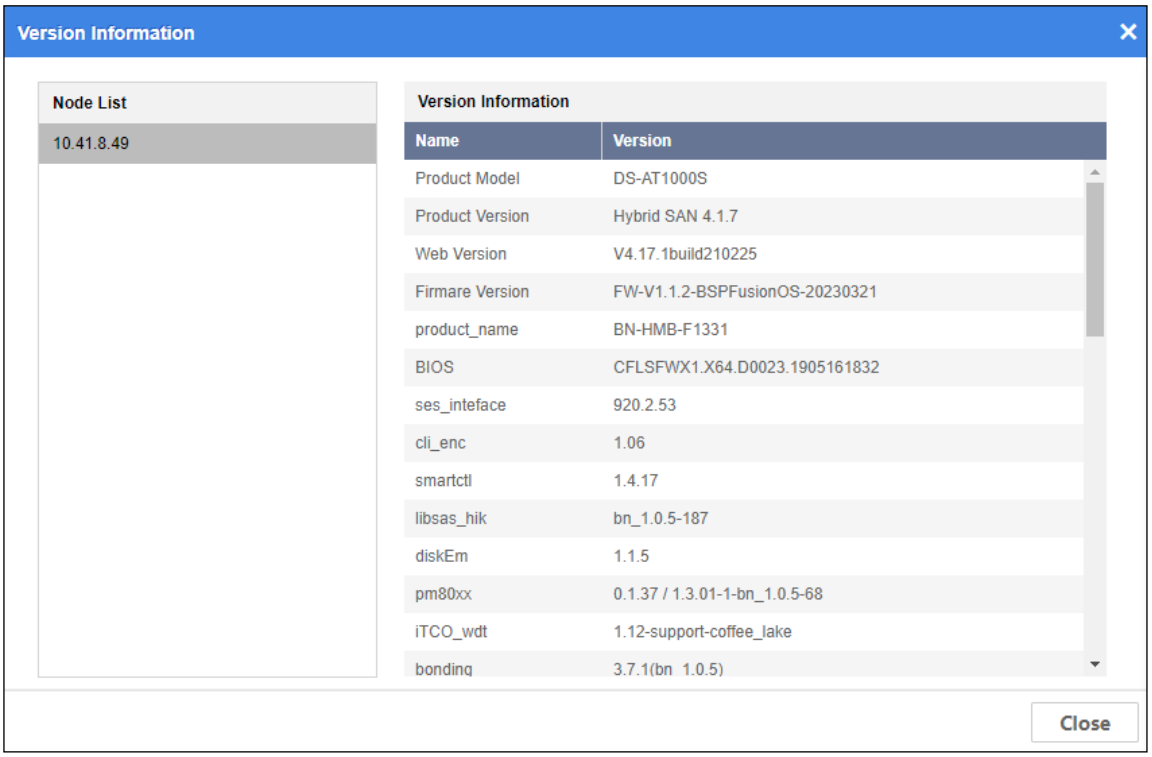


Figure 10-1 Version Information

10.2 System Upgrade

Step 1 Go to **Maintenance**.

Step 2 Click **Upgrade**.

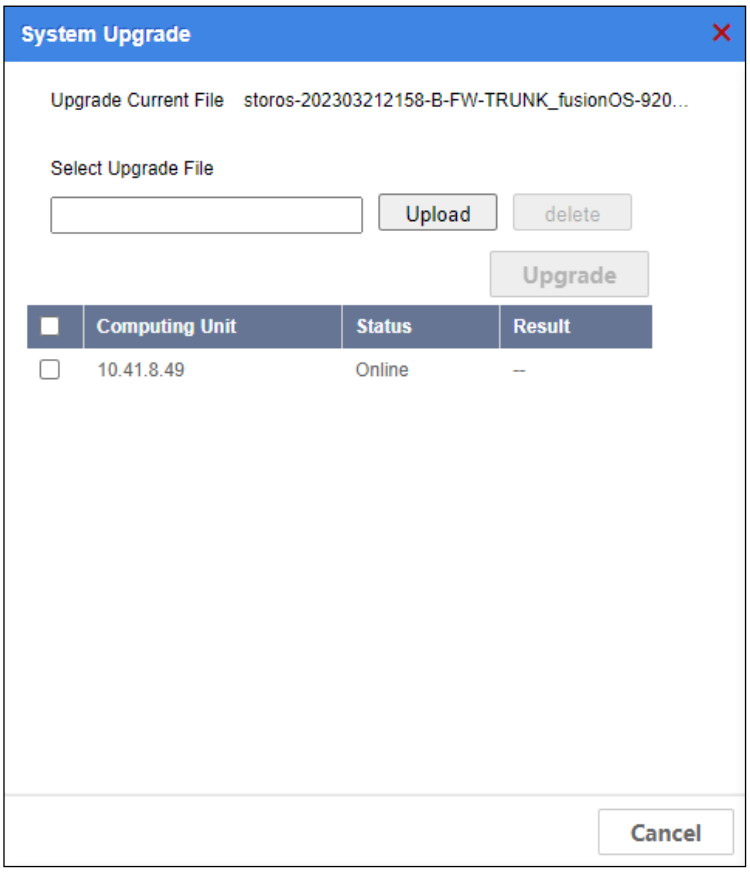


Figure 10-2 System Upgrade

Step 3 Click **Upload** to select upgrade file.

Step 4 Check the computing unit to upgrade.

Step 5 Click **Upgrade**.

Step 6 Reboot the computing unit after upgrade finishes.

10.3 Disk Management

For details, please refer to *Manage Disk*.

10.4 Password Management

Step 1 Go to **Maintenance**.

Step 2 Click **Password Management**.

Step 3 Enter the **Current Password**.

Step 4 Enter the same password in **New Password** and **Confirm Password**.

Caution

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 5 Click **OK**.

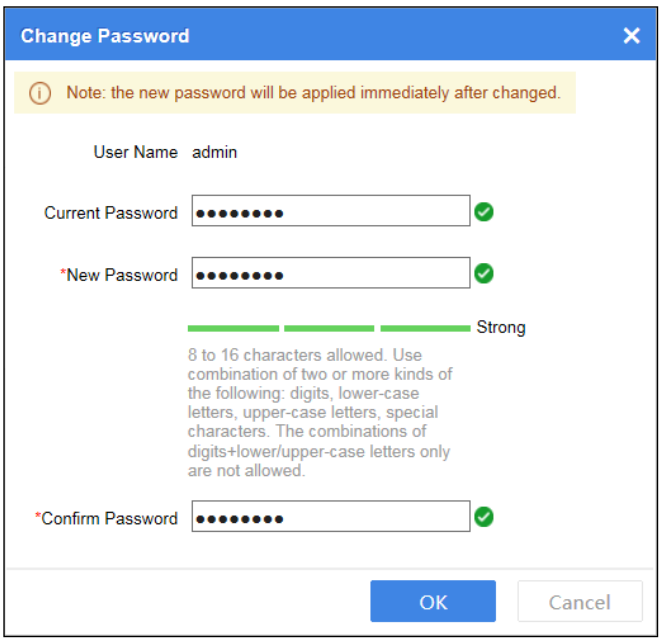


Figure 10-3 Change Password

10.5 Time Management

10.5.1 Time Zone Configuration

Step 1 Go to **Maintenance.**

Step 2 Click **Time Management**.

Step 3 Select **Time Zone** in the drop-down box.

Figure 10-4 Time Zone Configuration

Step 4 Click **OK**.

10.5.2 Time Sync Configuration

Synchronize Time Manually

Step 1 Go to **Maintenance**.

Step 2 Click **Time Management**.

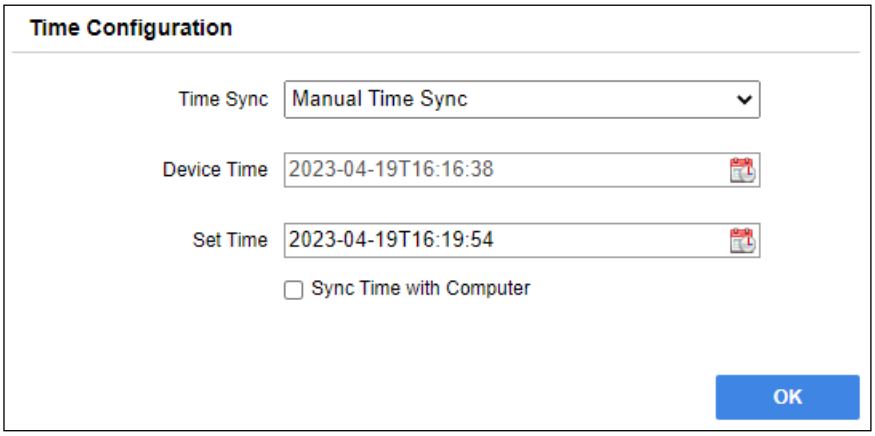


Figure 10-5 Manual Time Sync

Step 3 Select **Time Sync** as **Manual Time Sync**.

Step 4 Set time.

- Click to set time manually.
- Check **Sync Time with Computer**.

Step 5 Click **OK**.

Synchronize Time by NTP

Step 1 Go to **Maintenance**.

Step 2 Click **Time Management**.

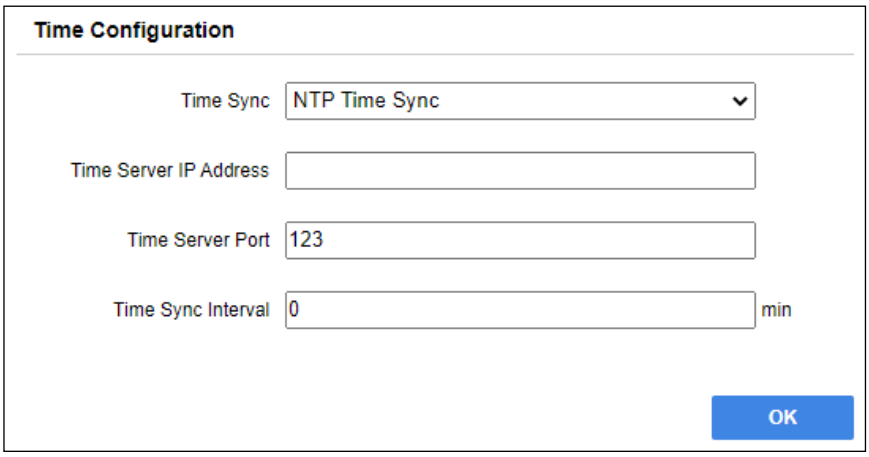


Figure 10-6 NTP Time Sync

Step 3 Select **Time Sync** as **NTP Time Sync**.

Step 4 Enter **Time Server IP Address**, **Time Server Port**, and **Time Sync Interval**.

Step 5 Click **OK**.

10.5.3 DST Configuration

Daylight Saving Time (DST) is the practice of setting the clocks forward a time period from standard time during the set months

Step 1 Go to **Maintenance**.

Step 2 Click **Time Management**.

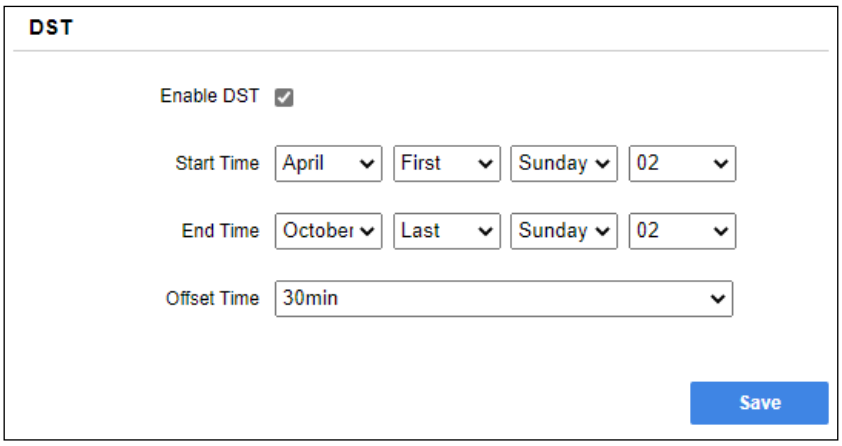


Figure 10-7 DST Configuration

Step 3 Check **Enable DST**.

Step 4 Set the **Start Time** and **End Time** of the DST.

Step 5 Set the **Offset Time** from standard time.

Step 6 Click **Save**.

10.6 Default Settings

Purpose:

Restore all parameters to default settings.

Step 1 Go to **Maintenance**.

Step 2 Click **All system settings reset**.

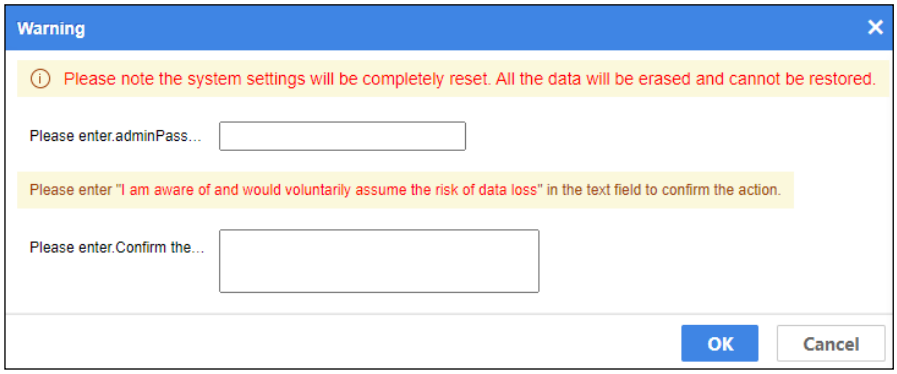


Figure 10-8 System Reset

Step 3 Enter admin **Password**.

Step 4 Enter the confirmed text in the pop-up window to confirm the action.

Step 5 Click **OK.**

10.7 Snapshot Management

Purpose:

Create, restore, or delete snapshots.

Step 1 Go to **Maintenance** > **Snapshot Management**.

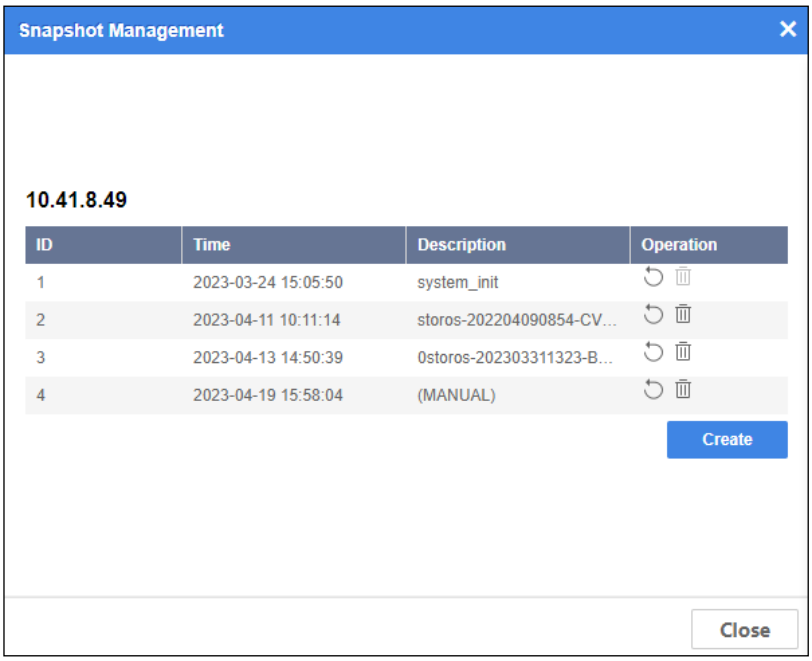


Figure 10-9 Snapshot Management

Step 2 Click **Create**.

Step 3 Enter the snapshot description.

Step 4 Click **OK**.

Note

Up to 4 snapshots can be created. The earliest snapshots will be automatically overwritten when the number of snapshot exceeds 4.

Step 5 (Optional) Restore snapshot.

1) Click .
2) Enter the **Root Password** and **Verification Code** to confirm the operation.
3) Click **OK**.

Note

The current data will be lost after restoring snapshots. Restart your device after snapshots are restored.

Step 6 (Optional) Delete snapshot.

1) Click .
2) Enter the **Admin Password** and **Verification Code** to confirm the operation.
3) Click **OK**.

Note

The deleted snapshots cannot be restored.

10.8 SNMP Management

Step 1 Go to **Maintenance** > **SNMP Management**.

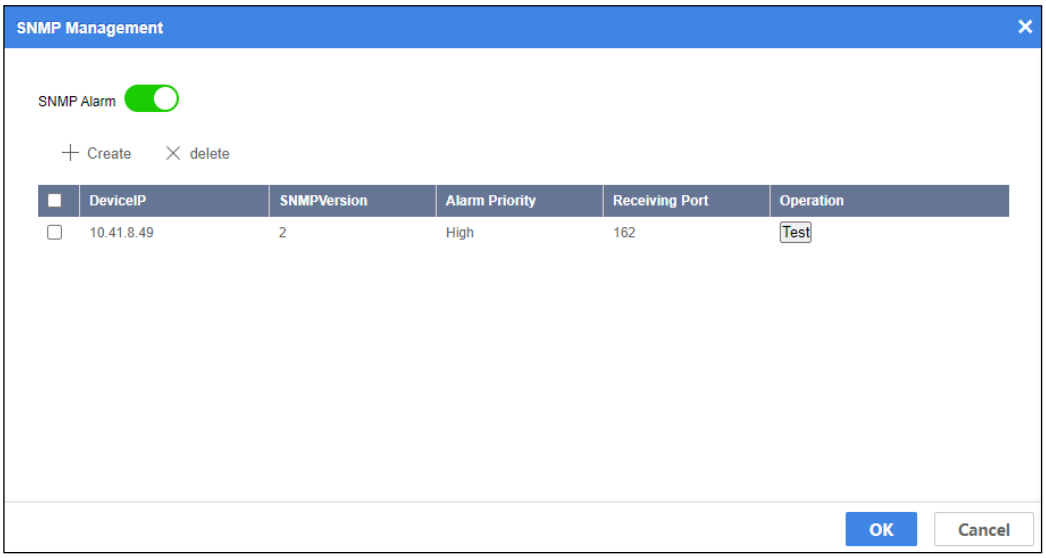


Figure 10-10 SNMP Management

Step 2 Enable **SNMP Alarm**.

Step 3 Click **Create**.

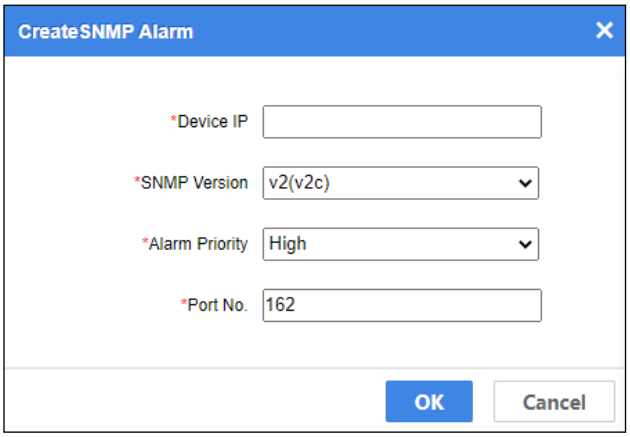


Figure 10-11 Create SNMP Alarm

Step 4 Enter the **Device IP**, select the **SNMP Version** and **Alarm Priority**, and enter the **Port No.**

Step 5 (Optional) Click **Test**.

Step 6 (Optional) Delete SNMP alarm.

1) Check the SNMP alarm(s) to delete.
2) Click **delete**.
3) Click **OK**.

Step 7 Click **OK**.

10.9 Security Management

Step 1 Go to **Maintenance** > **Security Management**.

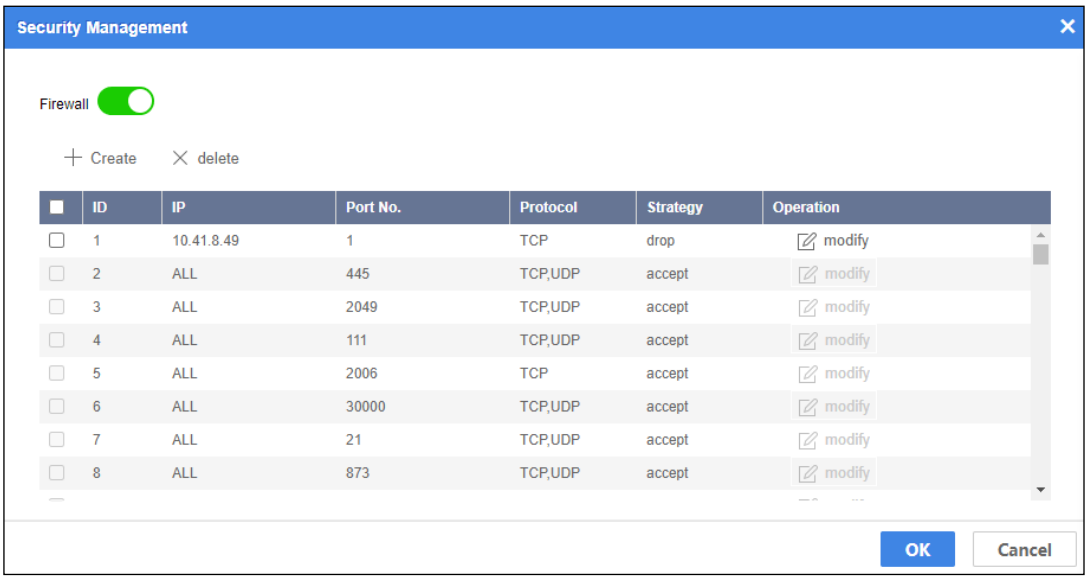


Figure 10-12 Network Detection

Step 2 Enable **Firewall**.

Step 3 Click **Create** to create a firewall.

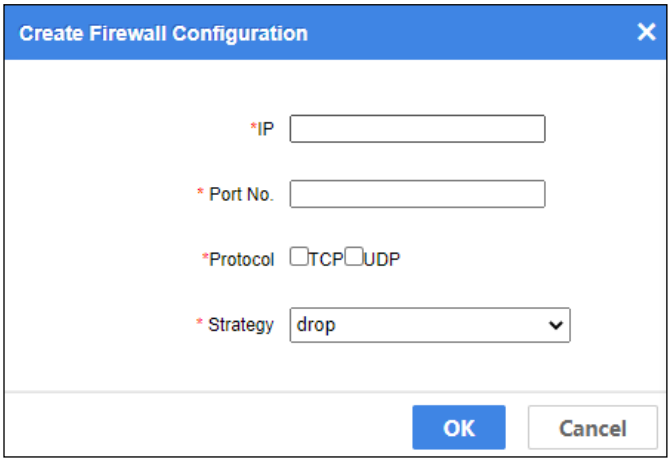


Figure 10-13 Create Firewall

Step 4 Enter **IP** and **Port No.** of the firewall.

Step 5 Check the **Protocol**.

Step 6 Select the **Strategy**.

Step 7 Click **OK**.

Step 8 (Optional) Modify or delete the direwall.

- Click **modify** to modify the firewall.
- Check the firewall(s) and click delete to delete the selected firewall(s).

Step 9 Click **OK**.

10.10 Network Management

10.10.1 Modify Network

For details, please refer to *Modify Network*.

10.10.2 Network Detection

Purpose:

Perform ping test and network environment detection.

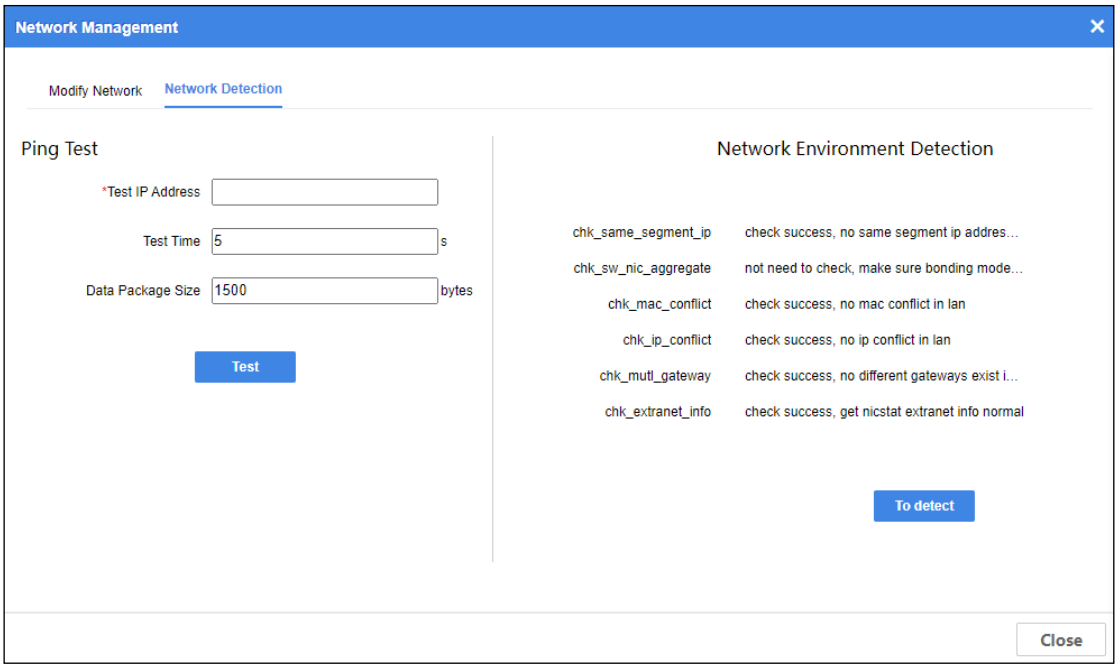


Figure 10-14 Network Detection

Ping Test

Step 1 Enter the **Test IP Address**, **Test Time**, and **Data Package Size**.

Step 2 Click **Test**.

View the test results displayed on the interface.

Step 3 Click **Back**.

Network Environment Detection

Step 1 Go to **Maintenance** > **Network Management > Network Detection**.

Step 2 Click **To detect**.

See Far, Go Further

UD33222B