



Network Storage 821 Series

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, HDMI High-Definition Multimedia Interface, HDMI Trade dress and the HDMI Logos are trademarks or registered trademarks of HDMI Licensing Administrator, Inc.
- The following trademark is owned by Access Advance LLC and shall not be used without authorization.



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.

Applicable Models

This manual is applicable to the models listed in the following table.

Series	Model
DS-A821XXSI	DS-A82124SI
	DS-A82148SI
	DS-A82172SI

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 overheating 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	1
1.1 Activation	1
Configuration Wizard	4
Chapter 2 Icon on the Menu Bar	9
Chapter 3 Maintenance	10
Overview	10
Running Info	11
1.2 3.2.1 System Info	11
3.2.2 Network Info	11
3.2.3 Recording Status	12
3.1 3.2.4 Exception Center	12
3.2 3.2.5 Device Status Monitoring Info	13
3.2.6 Performance Info	14
3.2.7 Online User	16
System Maintenance	17
3.3.1 Log	17
3.3 3.3.2 Restart	17
3.3.3 Upgrade	18
3.3.4 Backup and Restore	18
3.3.5 HDD Health	19
3.3.6 Snapshot	20
3.3.7 Device Debugging	21
3.3.8 Incoming Bandwidth Configuration	24
3.3.9 Import License	24
Chapter 4 Storage Management	26
4.1 4.2 Recording Schedule	26
4.2 Video Copy-Back	29
4.3 4.2.1 Task List	29
4.2.2 Schedule List	30
4.4 4.2.3 Advanced Configuration	30
Storage Pool	31
4.3.1 Storage Pool Management	31
4.3.2 Storage Space Management	34
4.5 Array Management	35
4.4.1 View Array	35
4.6 4.4.2 Create Array	36
4.7 4.4.3 Rebuild Array	37
4.4.4 Set Rebuilding Speed	37
5.1 HDD Mangement	38
5.2 4.5.1 View/Locate/Upgrade HDD	38
5.3 4.5.2 HDD Detection	39
4.5.3 Clear Dirty Data	39
Hot Spare Disk	39
Advanced Configuration	40
Chapter 5 Channel Management	42
Add and Manage Channels	42
Custom Protocol	43
Batch Time Sync	44

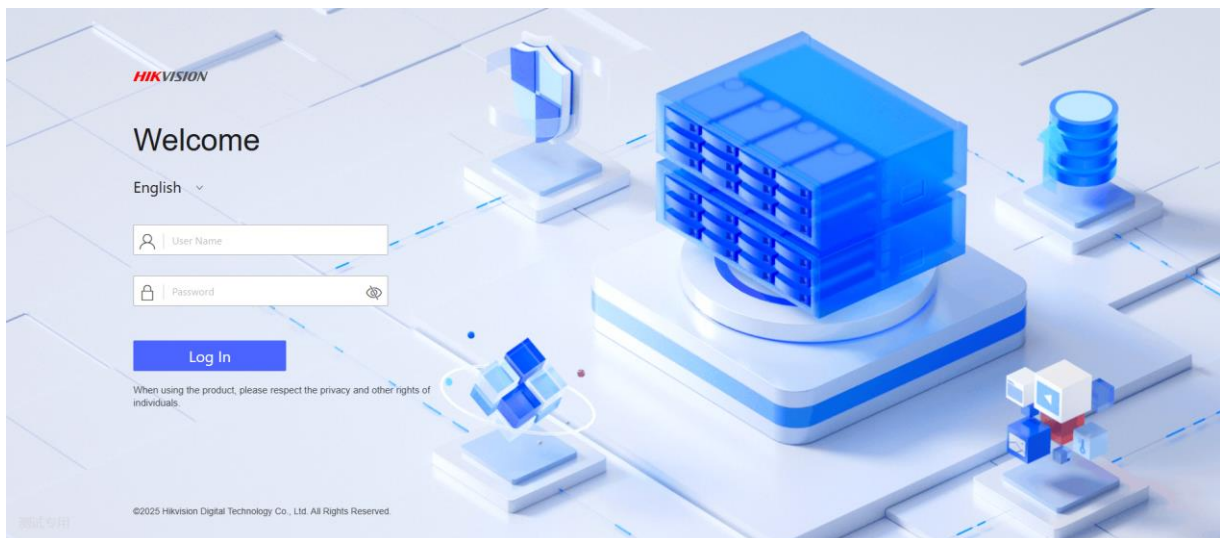
5.3.1	Manual Time Sync.....	44
5.3.2	Schedule Time Sync	45
	Chapter 6 Live View.....	46
	Chapter 7 Playback.....	48
	Playback	48
	Download Video.....	49
	Chapter 8 Event Center	51
	Event Search	51
	Event Configuration	51
	Chapter 9 System Configuration	53
	Local	53
7.1	9.1.1 Live View Parameter	53
7.2	9.1.2 Video Settings	53
8.1	9.1.3 Picture and Clip Settings	54
8.2	System Configuration.....	54
9.1	9.2.1 Region and Time	54
	9.2.2 RS-232	54
	User Management	55
9.2	9.3.1 Add User	55
	9.3.2 Edit/Delete User.....	55
9.3	9.3.3 Account Security Settings	56
	Network Configuration	56
	9.4.1 Network Parameter	56
9.4	9.4.2 Platform Access.....	60
	9.4.3 Network Service	61
9.5	Configure N+1 Hot Spare	62
	Chapter 10 Security	65
10.1	Firewall.....	65
10.2	MAC Address Filtering	65
10.3	Security Service.....	66
10.4	TLS.....	67
10.5	Central Storage Key	67

Chapter 1 Login

You can log in by two methods:

Method 1: Connect LAN interface of computer to the management network interface of the device via the network cable. Enter <http://IP of the management network interface> (10.254.254.254 by default) in the browser, and then enter the user name and password to log in.

Method 2: Connect LAN interface of computer to the LAN interface of the device via the network cable. Enter <http://IP of the LAN interface> (192.168.0.100 by default) in the browser, and then enter the user name and password to log in.

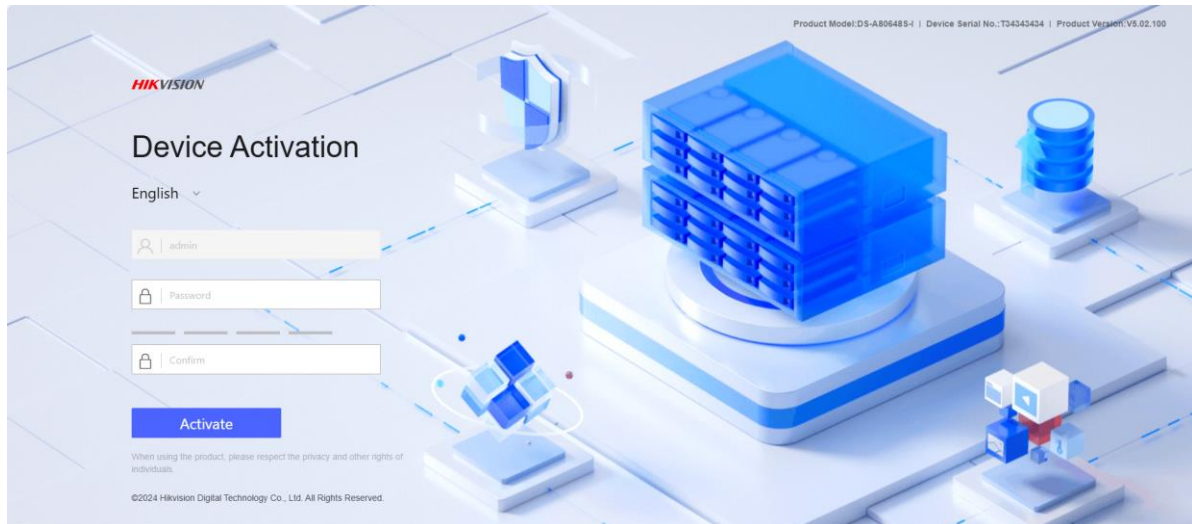


Login Page

1.1 Activation

You should set a password to activate the device for the first time of entering the web page.

Enter the user name (admin), enter the password and confirm it, click **Activate** to activate the device.



Activation



Caution

Figure 1-2

- The password should be 8 to 16 characters long. The password should contain at least 2 character types, such as digits, uppercase letters, lowercase letters, and special characters.
- Do not use risky password:
- The password should not contain user name, “123” and “admin” (case-insensitive), consecutive increasing or decreasing digits of four or more (such as 1234, 12345, 4321), four or more consecutive identical characters (such as 1111, 8888, “aaaa”) and any risky passwords in risky password list.
- After you log in to the system, if there is no operation within five minutes, for security reasons, the system will log out.

After activating the device, you will enter the Account Security Settings page, where you can set password retrieval methods including setting security questions, exporting GUID file, and setting a reserved email.

Account Security Settings

Security Question Configuration

Security Question1

What is your father's name? ▾

Answer

Security Question2

What is your mother's name? ▾

Answer

Security Question3

What is the name of your teacher in charge of class in senior high sc... ▾

Answer

Export GUID File

Note: The GUID file is very important which can help you to retrieve your password. It is highly recommended to export and keep the GUID file properly.

Export

Reserved Email

Set an e-mail address to receive verification code for password recovery.

Reserved Email

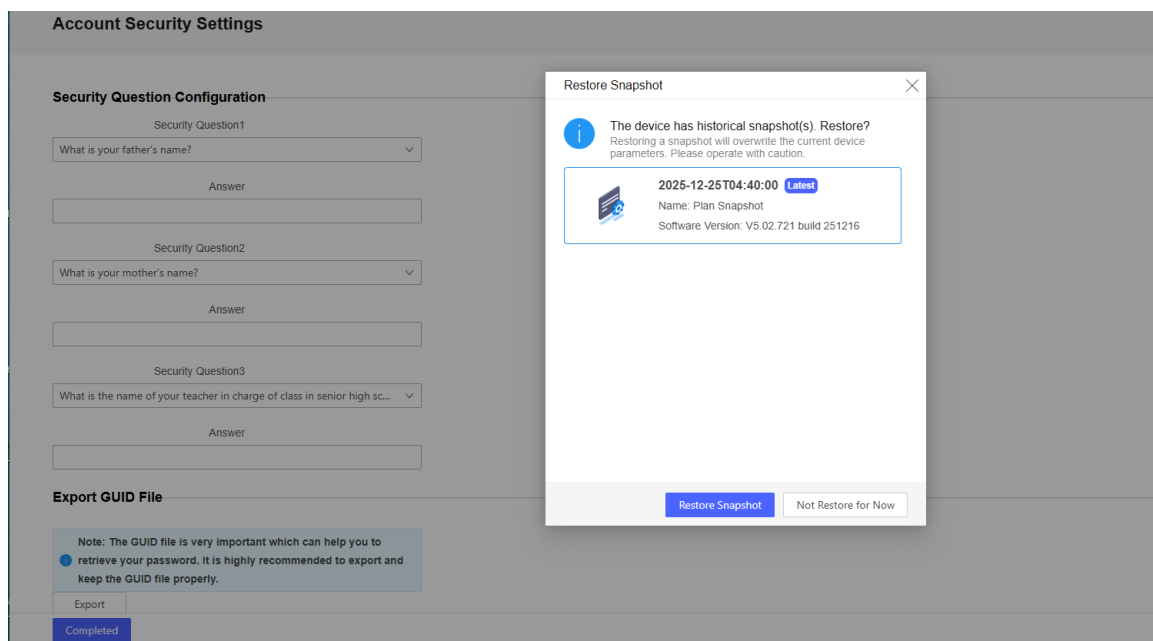
OK

Figure 1-3

Account Security Settings

Note

For the device that has historical snapshot(s) before controller change, you may also need to decide whether to restore the snapshot before entering the Account Security Settings page.



Restore Snapshot

Figure 1-4

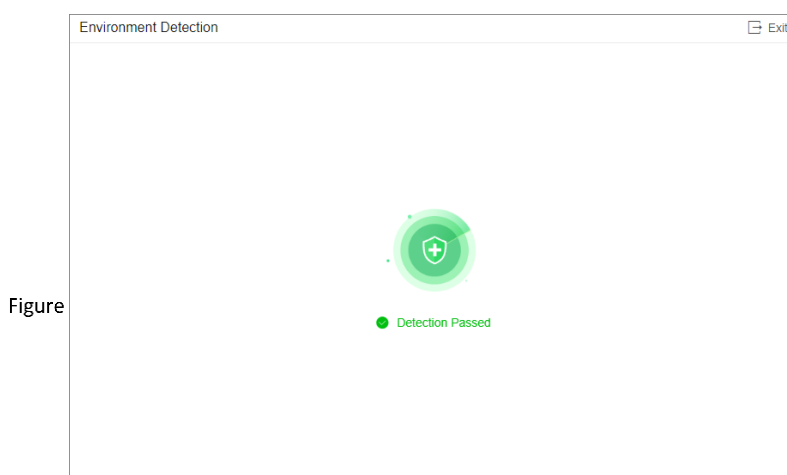
Configuration Wizard

1.2

After login, the system will automatically perform environment detection and then you will enter the Wizard page, where you can configure the NIC bond, configure time and storage. Operations on the Wizard page are all optional, and you can skip them and configure the corresponding parameters later.

Step 1

View the environment detection result.



Figure

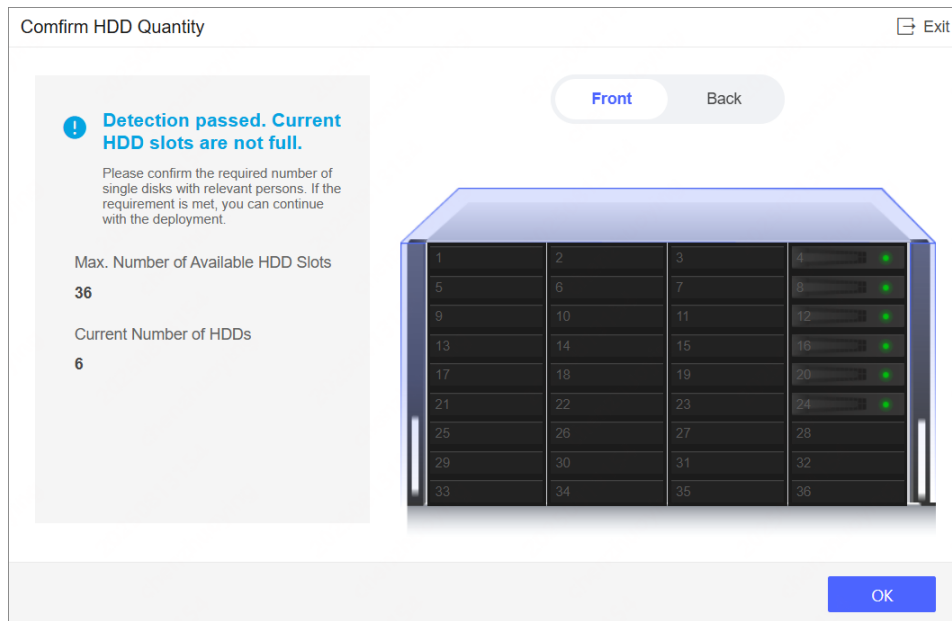
Environment Detection Passed

Note

Some of the reasons that may cause environment detection failure are as follows: the number of HDDs is less than 6, or there is one or more incompatible HDDs, or HDD capacity is insufficient. Click **Details** for the detailed failure information.

If environment detection passed and the current HDD slots are not full, check the maximum and the current number of HDD slots on the device, and click **OK** to enter the wizard configuration page.

Step 2



Check HDD Quantity

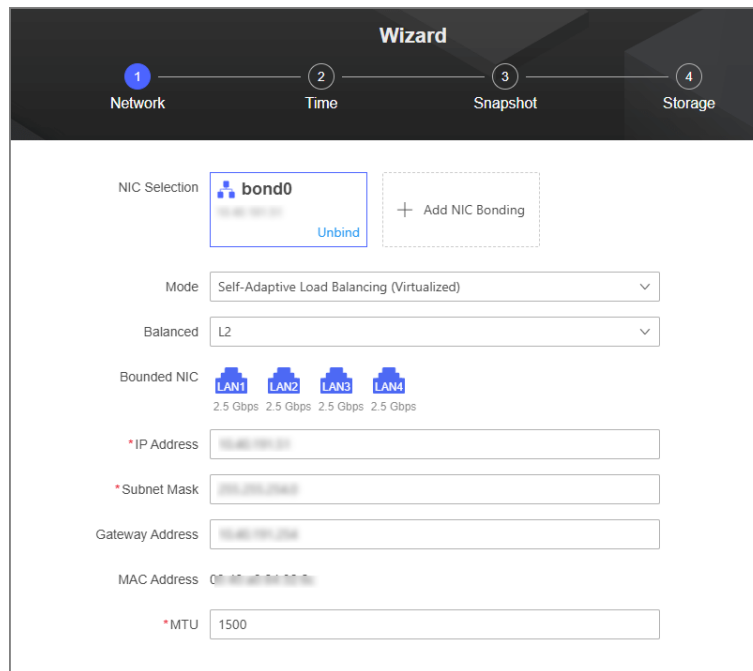
Figure 1-6

Note

Creating a VRAID5/RAID5 array requires at least 10 HDDs, and a VRAID6/RAID6 array requires at least 11 HDDs. It requires one additional HDD designated as a global hot spare compared to manually creating an array. For details about manually creating an array, refer to [Create Array](#).

Step 3

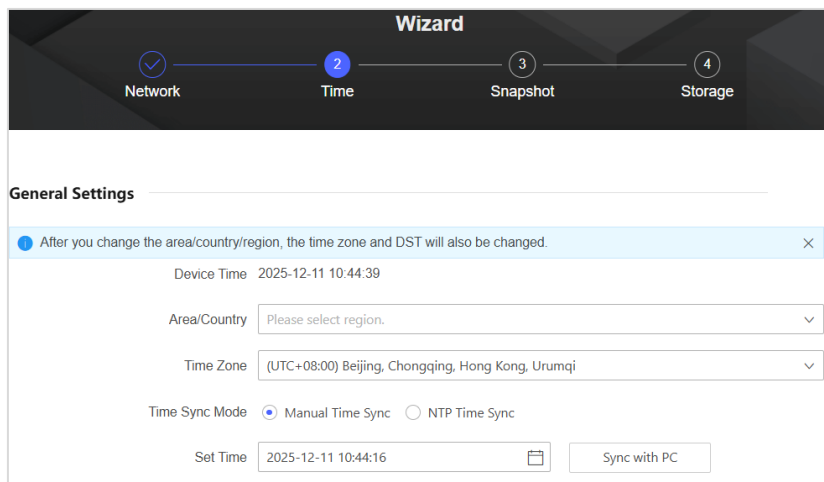
Click **Add NIC bonding** to configure the NIC bonding, and click **Next**.



Add NIC Bonding

Set the device time, and click **Next**. Refer to [Region and Time](#) for more details.

Step 4



System Time

Configure snapshot. Refer to [Snapshot](#) for more details.

Step 5

Wizard

Network Time **Snapshot** Storage

Enable Snapshot Schedule ☒

After enabling this function, the device will periodically back up snapshots according to the schedule.

Backup Location: HDD

Scheduled Cycle: Every Month 10Date 18:59:30

* Snapshot Password: Set Scheduled Snapshot Password

☐ Same as Administrator Password

* Confirm Snapshot Password: Snapshot Password Confirmation

Snapshot

Configure storage.

Figure 1-9

Wizard

Network Time Snapshot **Storage**

Array

Number of HDDs: 6 [View](#)

RAID Level: RAID5 (VRAID)

Hot Spare Disk Quantity: 0

Array Layout

Array Name	Level	Capacity	HDDs
RAID_1	RAID5 (VRAID)	36741 GiB	6

Storage Pool and Bandwidth

Storage Pool: Total Capacity 36740 GiB

Recording Pool: 36740 GiB

Picture Pool: 0 GiB

Input Bandwidth: Total Bandwidth 700Mbps

Record: 700 Mbps

Picture: 0 Mbps

Configure Storage



HDD slots are not full means the number of HDDs is less than the maximum number of available HDD slots but more than 5.

Click **Completed** in the lower-right corner of the page.

Chapter 2 Icon on the Menu Bar

The icons on the menu bar are as follows:



Icons



: Mute the alarm.



: Alarm Center.

Figure 2-1



: Locate the device.



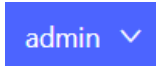
: Enter the Wizard page.



: Download the plug-in. Download or check the installation status.



: View open source software statement and online help, and download general tools.



: View the user name, change password and log out.



: Shut down or restart the device.

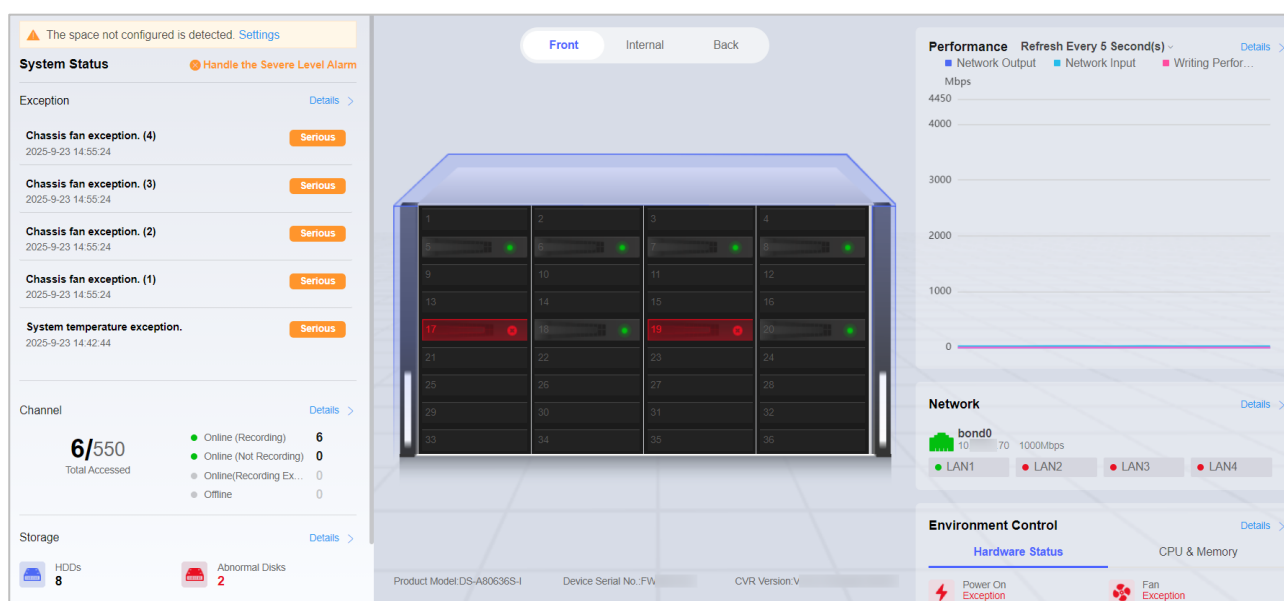
Chapter 3 Maintenance

In the Maintenance module, you can monitor system status, view running information, and perform maintenance operations.

Overview

After logging in the system, you will enter the overview page by default.

3.1



Overview

On the left side, you can have an overview of **System Status**, which includes **Exception**, **Channel** and **Storage**.

- In the **Exception** area, you can view exceptions sorted by levels. Click **Details** to enter the exception center page. Refer to [Exception Center](#) for more details.
- In the **Channel** area, you can view the number of connected channels and status. Click **Details** to enter the recording status page. Refer to [Recording Status](#) for more details.
- In the **Storage** area, you can view the number of total and abnormal HDDs and raids, and used capacity of the storage pool. Click **Details** to enter the array management page. Refer to [Array Management](#) for more details.



Note

For full space usage, when there is unused spaced detected, you will be suggested to set space reasonably. Click **Settings** in the top notification banner to enter storage pool page. Refer to [Storage Pool](#) for more details.

In the Middle side, click **Front Panel** (or **Front**), **Internal** or **Rear Panel** (or **Back**) to view the different parts of the device.

On the right side, you can have an overview of **Performance**, **Network**, and **Environment Control**.

- In the **Performance** area, click **Details** to enter the performance info page. Refer to [Performance Info](#) for more details.
- In the **Network** area, click **Details** to enter the network info page. Refer to [Network Info](#) for more details.
- In the **Environment Control** area, click **Details** to enter device status monitoring info page. Refer to Device Status Monitoring Info for more details.

Running Info

Running information includes system info, network info, recording status, exception center, device status monitoring info, performance info, and online user.

3.2

3.2.1 System Info
You can view system information including device model, serial No., version info, number of channels, HDDs and pools.

Go to **Maintenance** → **Running Info** → **System Info**.

Device Name	CVR
Device Model	
Serial No.	
Firmware Version	Upgrade
Hardware Version	B-R-X100-00
BIOS Version	V1.0.0 build250220 11:11:34
Web Version	V5.1.4_R0120 build 250402
Central Storage Protocol Version	V1.0
SSD Version	TETC1C
Number of Channels	0 / 550
Number of HDDs	7
Number of Storage Pools	0

System Info

3.2.2 Network In

You can view the information of bond network interfaces (NICs) and isolated NICs.

Go to **Maintenance** → **Running Info** → **Network Info**.

Click **Network Configuration** to configure the network interface. For details, refer to [Network Parameter](#).

Refresh Network Configuration >

Bond NIC

Name	Status	Speed	MTU	Mode	Balanced	LAN	IP Address	Subnet Mask	Gateway Address
bond0	Connected	1000 Mbps	1500	Active-Backup	N/A	1, 2, 3, 4 Details	10.40.100.107	255.255.255.0	0.0.0.0

Network Interface List

Name	Status	Speed	MTU	Binding Status	IP Address	Subnet Mask	Gateway Address
LAN1	Connected	1000 Mbps	1500	bond0	-	-	-
LAN2	Connected	1000 Mbps	1500	bond0	-	-	-
LAN3	Connected	1000 Mbps	1500	bond0	-	-	-
LAN4	Connected	1000 Mbps	1500	bond0	-	-	-

Network Info

On the recording status page, you can check recording status, including channel No., camera name, IP address and recording type of all channels.

3.2.3 Recording Status
Go to **Maintenance** → **Running Info** → **Recording Status**.

Supports searching by channel No., camera name or IP address.

Refresh Number of Offline Channels: 0 Channel Management > Total Accessed: 4/550 Copy-Back Task >

No.	Camera Name	Stream ID	Recording Type	Recording Status	Recording Bit Rate	Recording Resolution
1	IPC1	-	Continuous Recording	Online(Recording)	H.265-Constant	1920 * 1080
2	IPC2	-	Continuous Recording	Online(Recording)	H.265-Constant	1920 * 1080
3	IPC3	-	Continuous Recording	Online(Recording)	H.265-Constant	1920 * 1080
4	IPC4	-	-	Online(Not Recording)	H.265-Constant	-

Recording Status

3.2.4 Exception Center

Exception Information

You can view the number of alarms in different levels (Emergency, Serious, and Warning), filter alarms by levels, search for alarms by keywords, etc.

Go to **Maintenance** → **Running Info** → **Exception Center** → **Exception Information**.

Emergency 0

Serious 16

Warning 2

Clear Export Historical Exception

Filter Levels: All Search

☐	Level	Time	Description
☐	Serious	2025-7-28 20:32:29	Chassis fan exception.
☐	Serious	2025-7-28 20:32:29	Chassis fan exception.
☐	Serious	2025-7-28 20:32:29	Chassis fan exception.
☐	Serious	2025-7-28 20:32:29	Chassis fan exception.

Exception Information

You can perform the following as needed.

- Click **Export Historical Exception** to export detailed alarm information to your local PC.

- Click **Clear** to clear alarms in Serious and Warning levels.
- Click an alarm to view alarm details and handling suggestion on the right side.

Exception Linkage

You can configure alarm linkage including notifying surveillance center and sending email.

Go to **Maintenance** → **Running Info** → **Exception Center** → **Exception Linkage**.

Exception Linkage

Figure 3-6

3.2.5 You can check device status including hardware status, CPU, and memory.

Go to **Maintenance** → **Running Info** → **Device Status Monitoring Info**.

On the Hardware Status page, you can view fan status and rotation speed, CPU temperature, and other hardware data.

You can click to switch fan modes. The three fan modes differ primarily in fan rotation speed, with the order from highest to lowest being: High Performance Mode > Balanced Mode > Power Saving Mode. The higher the rotation speed, the better the heat dissipation performance.

Hardware Status

CPU

Memory

Refresh

Fan

Fan Mode: Power Saving Mode

Name	Status	Rotation Speed
Chassis Fan 1	Normal	4320r/min
Chassis Fan 2	Normal	4320r/min
Chassis Fan 3	Normal	4200r/min
Chassis Fan 4	Normal	4200r/min
Chassis Fan 5	Normal	4200r/min

Temperature

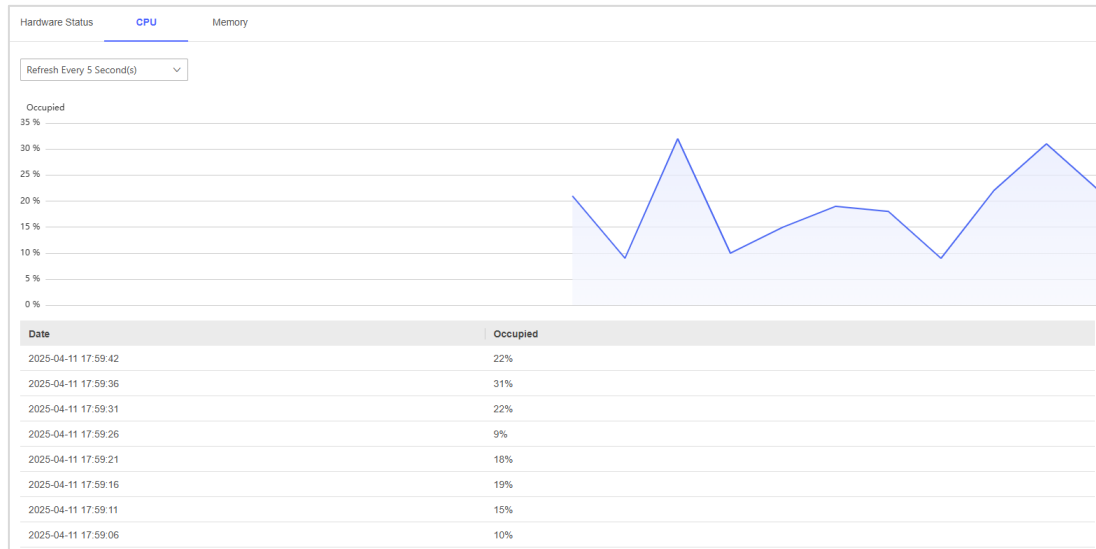
Name	Status	Temperature
CPU Temperature	Normal	86°C
Ambient Temperature	Normal	27°C
System Temperature 1	Normal	43°C

Other

Name	Status	Details
Power On1	Normal	Connected.
Power On2	Normal	Connected.

Hardware Status

On the CPU and Memory pages, you can select refresh rate to filter the data.



CPU Occupied Information

Figure 3-8

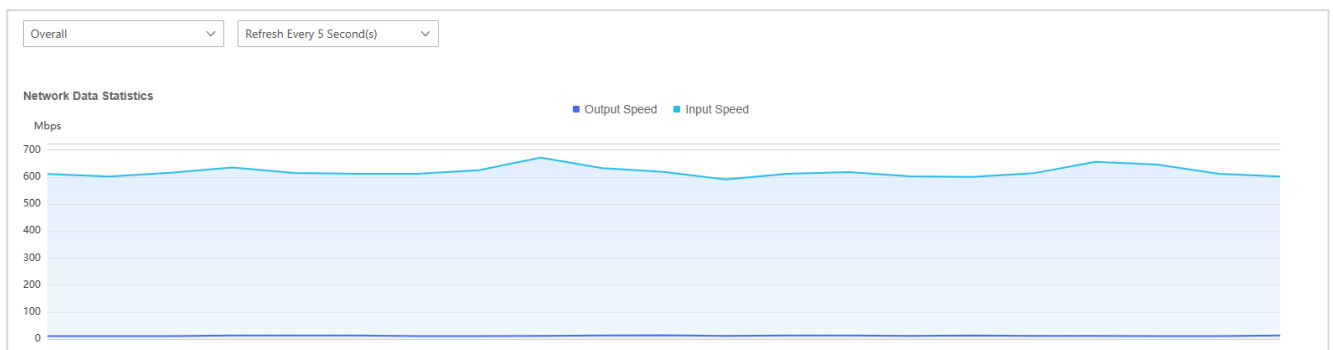
3.2.6 Performance Info. You can check network bandwidth, reading and writing performance, rebuilding speed, IOPS, and UTIL information.

Go to **Maintenance** → **Running Info** → **Performance Info**.

Network Bandwidth

Supports viewing network data statistics and resource statistics.

Network Data Statistics: You can view the statistics of overall/single network interfaces. Supports customizing statistics refreshing rates (refreshing every 1 second, 5 second, 1 minute, or 10 minutes).



Network Data Statistics

Network Resource Statistics: You can view the bandwidth allocated to the video input and picture input, and remaining bandwidth for the network receiving and sending.

Click **Incoming Bandwidth Configuration** to allocate the bandwidth.

Network Resource Statistics

Refresh

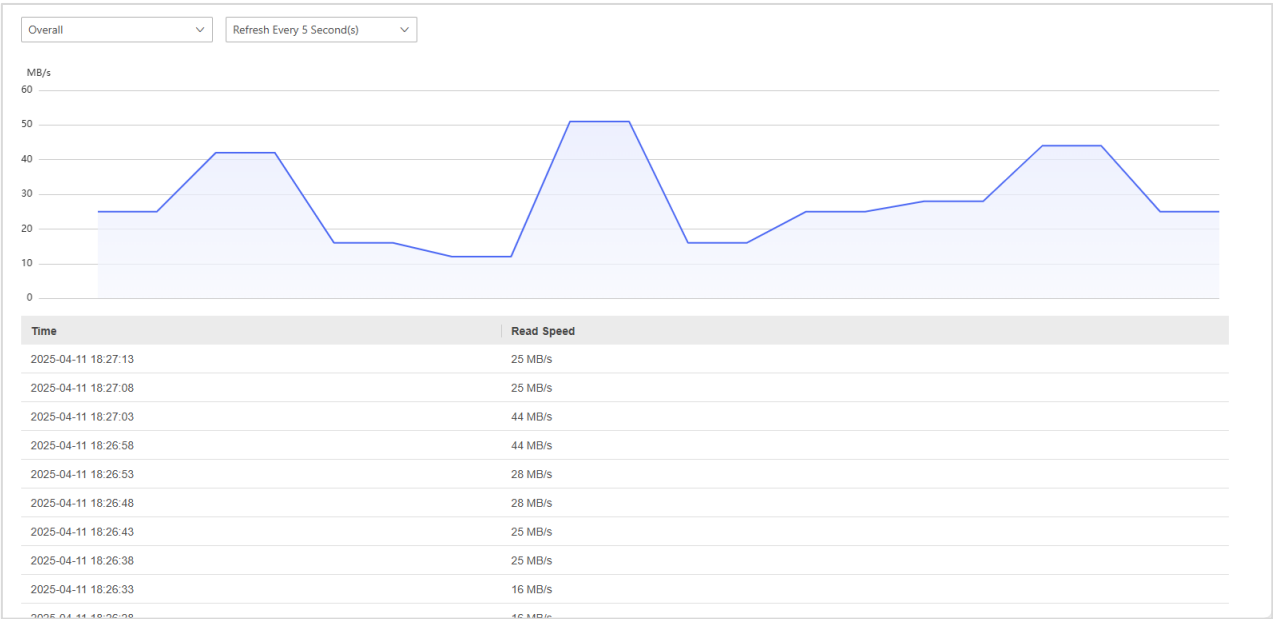
Incoming Bandwidth Configuration

Type	Bandwidth(Mbps)
Allocated to Video Input	1100
Allocated to Picture Input	0
Remaining for Network Receiving	1100
Remaining for Network Sending	1100

Network Resource Statistics

Reading/Writing Performance

Supports checking reading/writing speed of over/single raid.



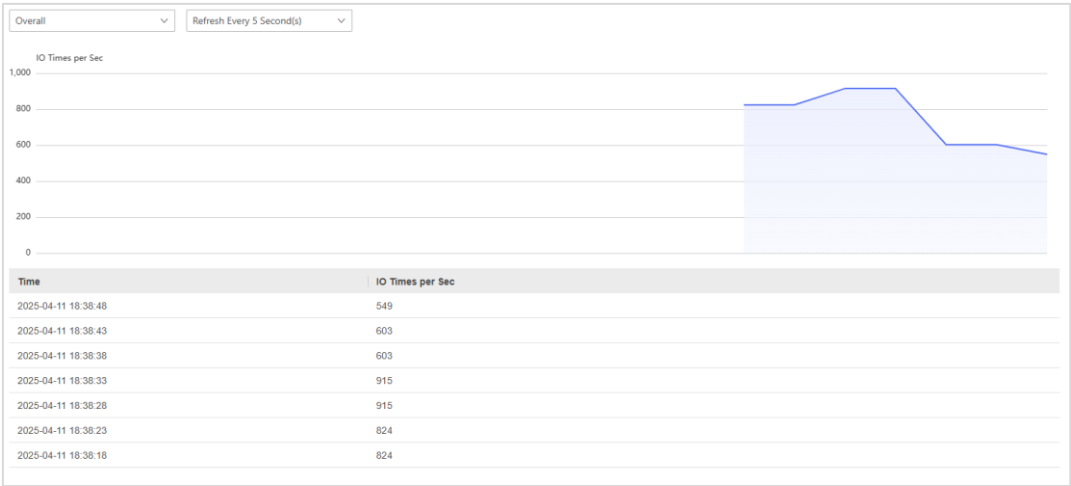
Reading Performance

Rebuilding

Supports viewing the rebuilding speed of RAID(s).

IOPS

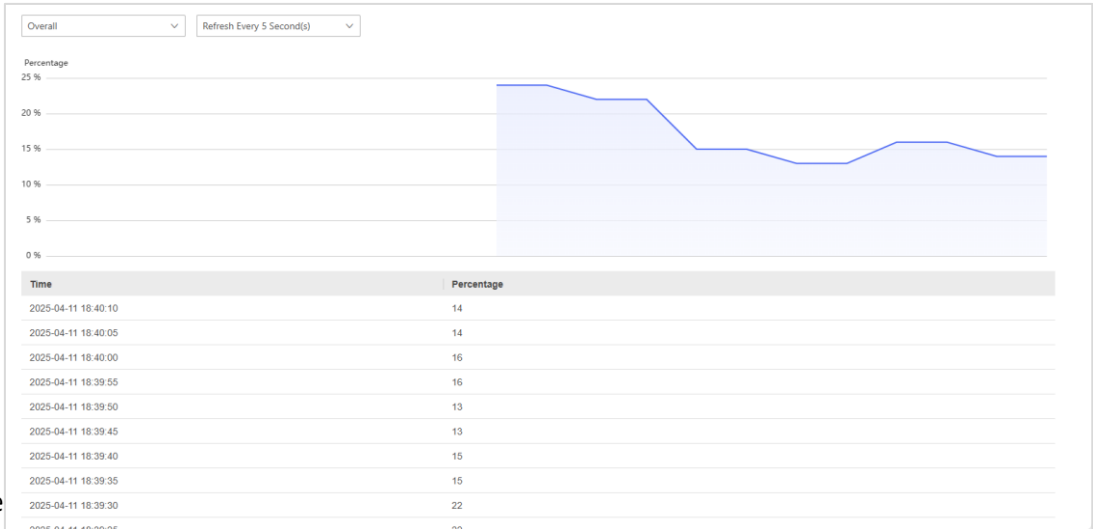
Supports viewing IO times per second of overall/single raid.



IOPS

UTIL

Supports viewing HDD using percentage of overall/single raid.



UTIL

3.2.7 Online

You can view the online user(s) of the device, including user name, user type, IP address and user operation time.

Click **User Management** to enter the User Management page. For details, refer to [User Management](#).

Figure 3-14

Refresh		User Management >		
No.	User Name	User Type	IP Address	User Operation Time
1	admin	Administrator	192.168.1.101	2025-07-14 14:01:47
2	admin	Administrator	192.168.1.102	2025-07-14 14:01:58
3	admin	Administrator	192.168.1.103	2025-07-14 14:02:05
4	admin	Administrator	192.168.1.104	2025-07-14 14:04:03

Online User

System Maintenance

System maintenance includes searching/exporting logs, manually restarting the device, upgrading device, backup and restoring, etc.

Go to **Maintenance** → **System Maintenance**.

3.3

Go to **Maintenance** → **System Maintenance** → **Log**.

You can set searching conditions to search for logs and export logs.

3.3.1 Log

Major Type		Subtype		Select Time			
All Types		All Types		2025-08-01 00:00:00 - 2025-08-13 23:59:59			
Export		Export All					
Search							
No.	Time	Major Type	Subtype	Channel No.	Local/Remote User	Remote Host IP Address	Additional Information
1	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Task: 1 chanCount: 1 Len: 304087040 R: 917792 W: 917792 Time: 2025-08-01 00:03:47 chanInfo: 301
2	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Channel No.: D1 HDD No.: 1 Channel No.: D2 HDD No.: 1 Channel No.: D3 HDD No.: 1 Channel No.: D4 HDD No.: 1 Channel No.: D5 HDD No.: 1 Channel
3	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Channel No.: D65 HDD No.: 1 Channel No.: D66 HDD No.: 1 Channel No.: D67 HDD No.: 1 Channel No.: D68 HDD No.: 1 Channel No.: D69 HDD No.: 1 Channel
4	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Channel No.: D129 HDD No.: 1 Channel No.: D130 HDD No.: 1 Channel No.: D131 HDD No.: 1 Channel No.: D132 HDD No.: 1 Channel No.: D133 HDD
5	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Channel No.: D193 HDD No.: 1 Channel No.: D194 HDD No.: 1 Channel No.: D195 HDD No.: 1 Channel No.: D196 HDD No.: 1 Channel No.: D197 HDD
6	2025-08-01 00:03:54	Information	System Running Status Information	--	--	--	Channel No.: D257 HDD No.: 1 Channel No.: D258 HDD No.: 1 Channel No.: D259 HDD No.: 1 Channel No.: D260 HDD No.: 1 Channel No.: D261 HDD

Log

- Search for Logs: set conditions including major type, subtype, and time, and click **Search** to search for logs.

- Export Logs: click **Export** to export logs selected (no more than 2,000 logs altogether) or click **Export All** to export all logs in txt or csv format.

Go to **Maintenance** → **System Maintenance** → **Restart**.

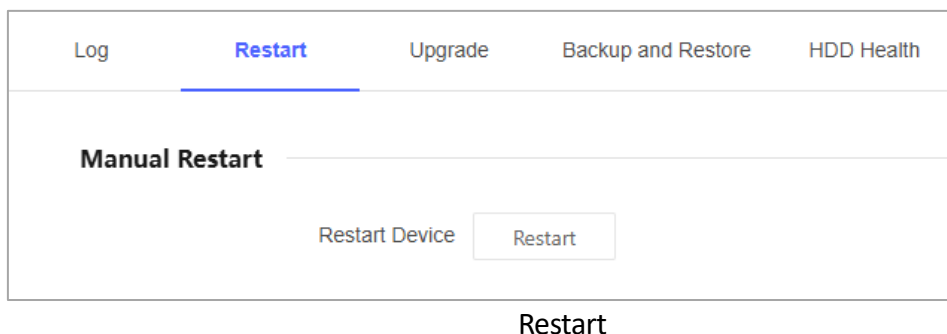
You can manually restart the device if needed.

Click **Restart** to restart the device.



Caution

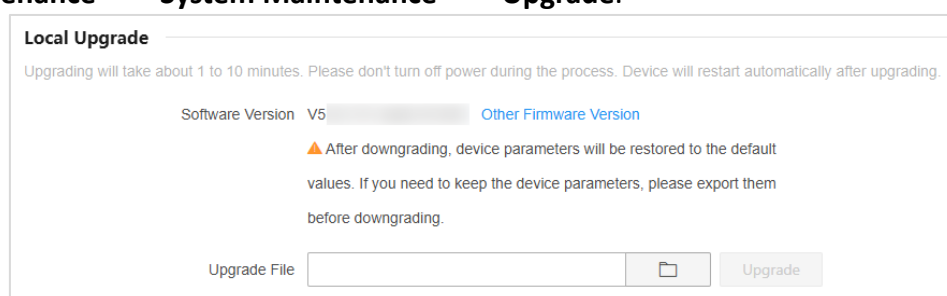
- A system interruption will occur during restarting. Please operate with caution.
- Do not cut off power when restarting.



Restart

Go to **Maintenance** → **System Maintenance** → **Upgrade**.

3.3.3 Upgrade



Upgrade

Figure 3-17

You can view the current software version and click **Other Firmware Version** to view detailed firmware versions.

In addition, you can upload the upgrade package for device software, MCU, CPLD, or SSD to upgrade the device.

Click  to select the upgrade file from your local PC, and click **Upgrade**.

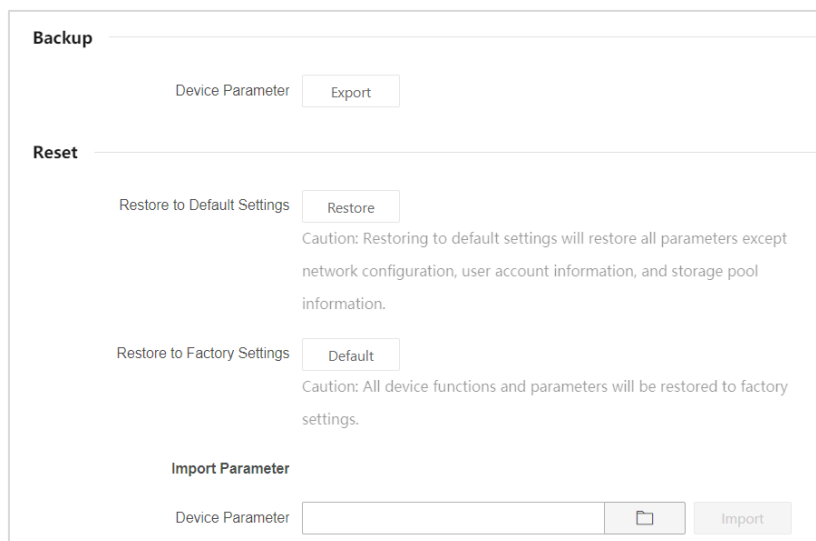


Caution

3.3.4 Backup and Restore

Upgrading normally will take about 1 to 10 minutes. Please do not turn off the power during the process. Device will restart automatically after upgrading.

Go to **Maintenance** → **System Maintenance** → **Backup and Restore**.



Backup and Restore

Backup: Click **Export** and set a password for the device parameter file before exporting the device parameter file for backup.

Reset: Supports restoring to default settings and restoring to factory settings. After resetting, you can import the backup file to restore the device parameters.

- **Restore to Default Settings:** Restore all parameters except network configuration, user account information, and storage pool information.
- **Restore to Factory Settings:** All device functions and parameters will be restored to factory settings.



Caution

3.3.5 HDD Health

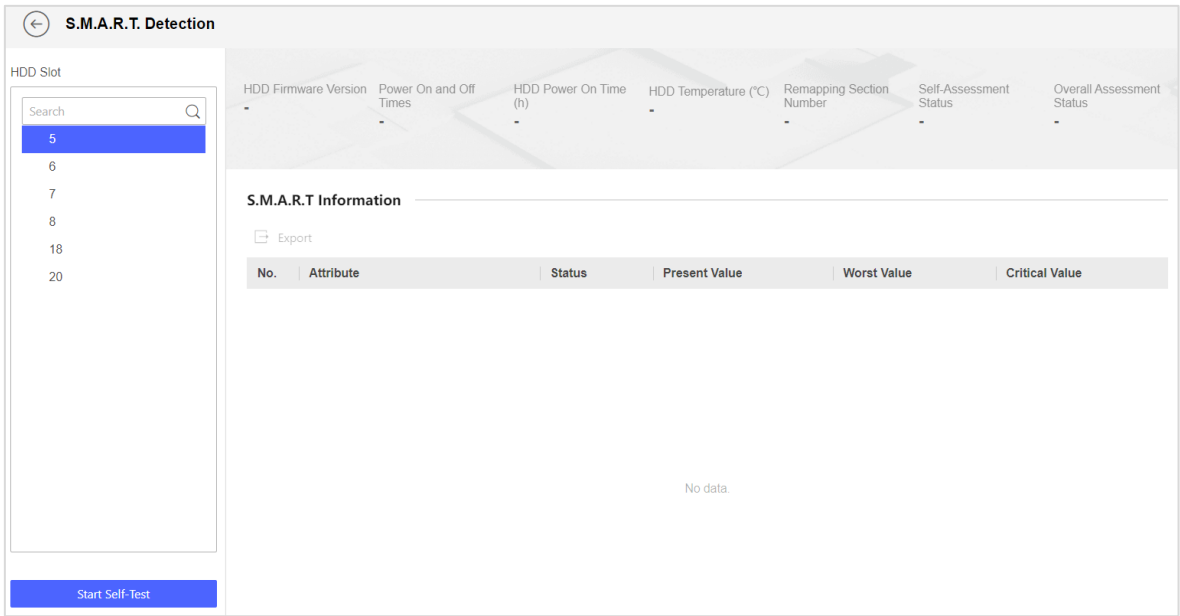
All cleared data and configurations will be permanently lost and cannot be recovered by any means.

Step 1

Go to **Maintenance** → **System Maintenance** → **HDD Health**.

Supports S.M.A.R.T. detection to check HDD health.

Click **HDD Health** → **S.M.A.R.T. Detection**.



S.M.A.R.T. Detection

Select an HDD slot, and then click **Start Self-Test**.

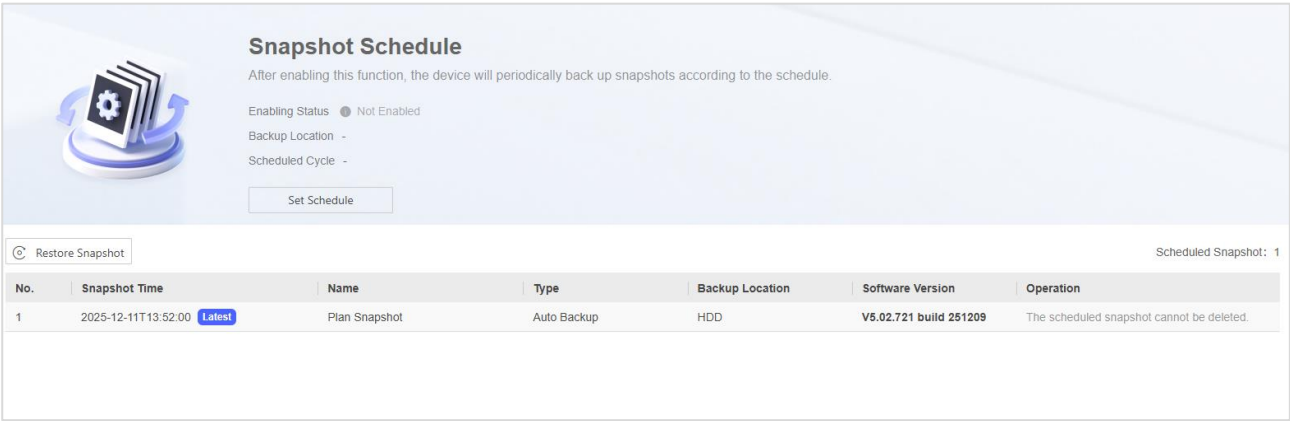
Figure 2-19

- Step 2
- Check the result in the right side of the page.
- Step 3
- (Optional) Click **Export** to export the result to your local PC.
- Step 4

3.3.6 Snapshot

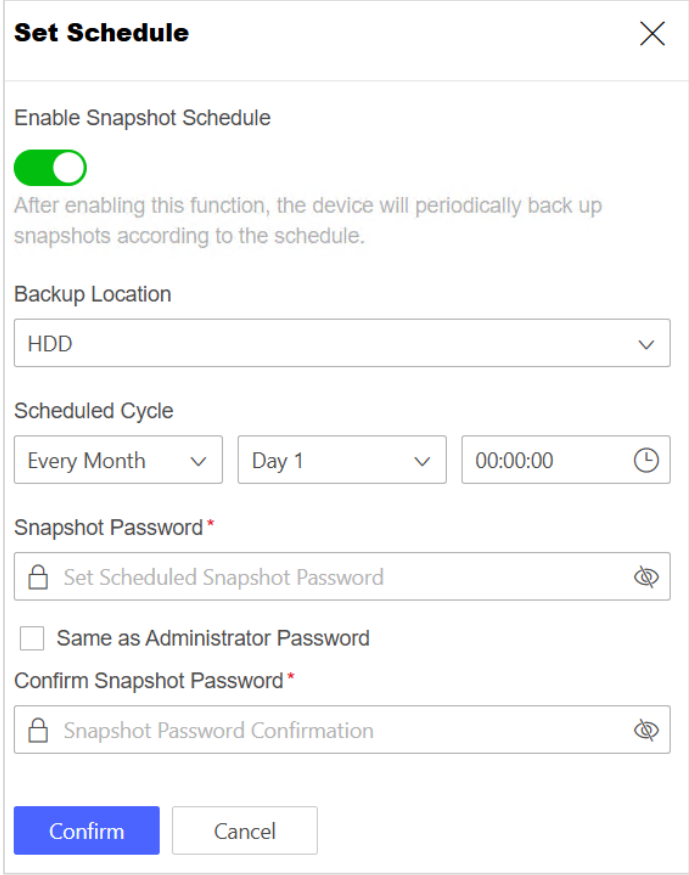
- Step 1
- You can enable and set a snapshot schedule to back up snapshots periodically.

Go to **Maintenance** → **System Maintenance** → **Snapshot**.



Snapshot

Click **Set Schedule** to enable the function and set related parameters.



Set Schedule [X]

Enable Snapshot Schedule

☒

After enabling this function, the device will periodically back up snapshots according to the schedule.

Backup Location

HDD [v]

Scheduled Cycle

Every Month [v] Day 1 [v] 00:00:00 [clock icon]

Snapshot Password *

Set Scheduled Snapshot Password [eye icon]

☐ Same as Administrator Password

Confirm Snapshot Password *

Snapshot Password Confirmation [eye icon]

Confirm Cancel

Figure 3-21

Set Schedule

Note

- The scheduled snapshot quantity is one and the latest snapshot overwrites the previous one according to the schedule.

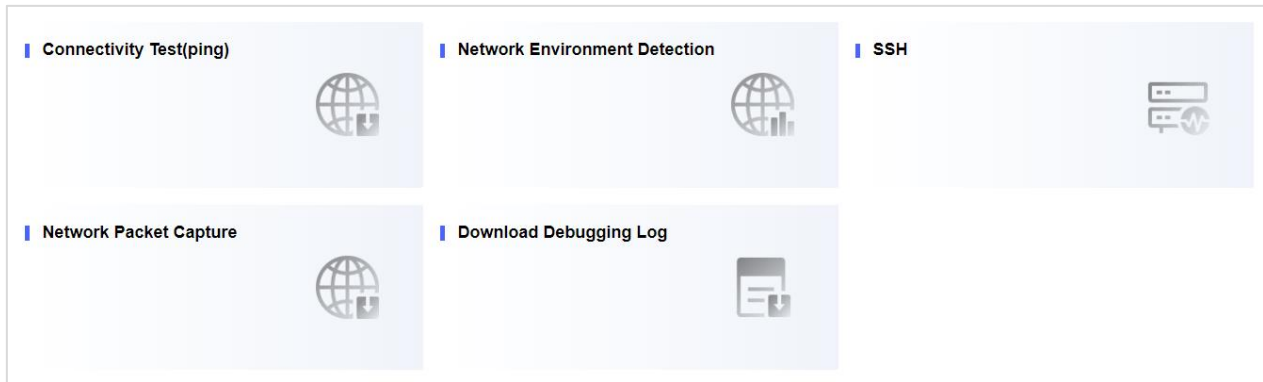
Step 3 ● When **Same as Administrator Password** is checked, the system will create the snapshot using the current Administrator password as the snapshot password.

Step 5 Click **Confirm**.

3.3.7 Device Debugging (Optional) Click **Set Schedule** to edit the schedule after enabling and configuring the snapshot schedule.

(Optional) Click **Restore Snapshot** and enter the statement to restore the snapshot.

Go to **Maintenance** → **System Maintenance** → **Device Debugging**.



Device Debugging

Connectivity Test

You can use ping command to test the connectivity of destination IP address.

Figure 3-22

Go to **Device Debugging** → **Connectivity Test (ping)**.

Enter the destination address, data package size, and then click **Test**. Check the result at the **Ping Result**.

Figure 3-23

Connectivity Test

Network Environment Detection

You can check network-environment-detection result, including IP address detection in the same network segment, multi-gateway detection, MAC address collision detection, and IP address collision detection.

Go to **Device Debugging** → **Network Environment Detection**.

Network Environment Detection

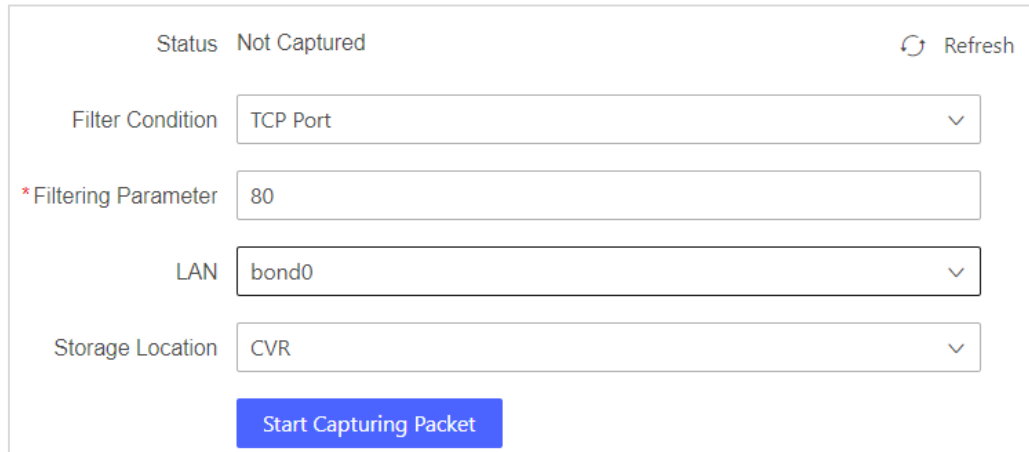
Click **Retry** to go through the detection again.

Network Packet Capture

By using the packet capture tool, you can troubleshoot the network issues.

Click **Device Debugging** → **Network Packet Capture**.

Step 1



The screenshot shows the 'Network Packet Capture' configuration window. At the top, the status is 'Not Captured' with a 'Refresh' button. Below, there are four input fields: 'Filter Condition' (set to 'TCP Port'), '*Filtering Parameter' (set to '80'), 'LAN' (set to 'bond0'), and 'Storage Location' (set to 'CVR'). A blue 'Start Capturing Packet' button is at the bottom.

Network Packet Capture

Configure the parameters.

Step 2

- **Filter Condition:** Filter the data packets. Supports IP address, TCP port etc.
- **Filtering Parameter:** Fill in this box according to the filter condition.
- **LAN:** Select the LAN interface that will be used to capture data packets.
- **Storage Location:** Select **USB** or **CVR**. When selecting **USB**, you should plug in an USB flash drive to the device.

Step 3

Step 4

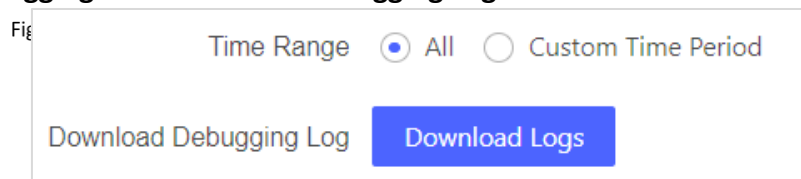
Click **Start Capturing Packet**, and then click **Refresh** to update the status.

Click **Stop Capturing Packet** when finished.

Download Debugging Log

You can download debugging logs to your local PC of all time or custom time period.

Go to **Device Debugging** → **Download Debugging Log**.



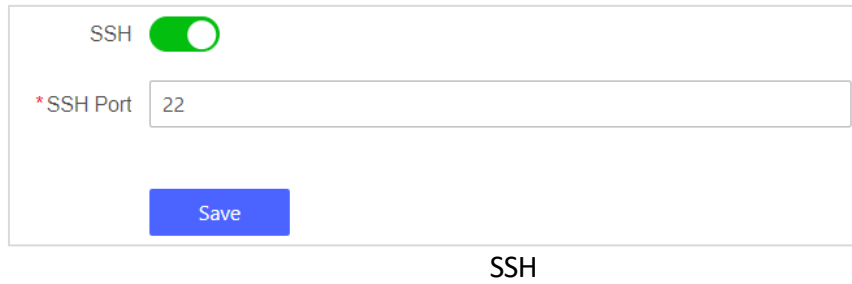
The screenshot shows the 'Download Debugging Log' interface. It has a 'Time Range' section with two radio buttons: 'All' (selected) and 'Custom Time Period'. Below this is a 'Download Debugging Log' label and a blue 'Download Logs' button.

Download Debugging Log

SSH

You can enable or configure the SSH port.

Go to **Device Debugging** → **SSH**.



SSH ☒

* SSH Port

[Save](#)

SSH

After enabling SSH, you can use SSH tunnel for debugging remotely. When there is no need to debug, disable SSH to increase safety.

Figure 3-27

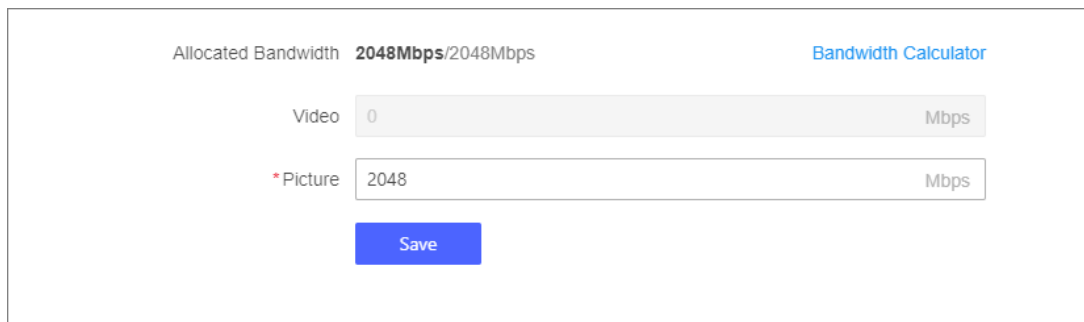
Go to **Maintenance** → **System Maintenance** → **Incoming Bandwidth Configuration**.

You can configure video and picture bandwidth and use the bandwidth calculator for estimation.



Note

Refer to the actual web page for allocated bandwidth.



Allocated Bandwidth **2048Mbps/2048Mbps** [Bandwidth Calculator](#)

Video Mbps

* Picture Mbps

[Save](#)

Incoming Bandwidth Configuration



Note

3.3.9 To modify the configured bandwidth for video or picture, you should allocate a greater bandwidth than the existing one.

Step 1

Step 2

Step 3

Click **Maintenance** → **System Maintenance** → **Import License** to enter the page.

Click  to choose the license.

Click **Import**.

License			Import
---------	----------------------	---	--------

Import License

Figure 3-29

Chapter 4 Storage Management

Recording Schedule

You can configure recording schedule and advanced parameters for the channels.

Click **Storage Management** → **Recording Schedule**.

4.1

Step 1

The screenshot displays the 'Recording Schedule' configuration page. The main table contains 15 rows, each representing an IP camera (D1 to D15). Each row has four columns: 'Camera Name', 'Enable' (with a green toggle switch), 'Recording Schedule' (a dropdown menu showing 'All-Day Continuous Schedule'), and 'Advanced Configuration' (a gear icon). Above the table is a search bar. To the right of the table is a 'Schedule Details' panel. This panel has three tabs: 'Continuous' (selected), 'Event', and 'Motion D...'. Below the tabs is a calendar grid for the week of Monday to Sunday. Each day's grid shows a 24-hour timeline from 00 to 24, with the entire area filled with a solid blue color, indicating that recording is scheduled for all days and times. At the bottom of the 'Schedule Details' panel are two buttons: 'Save' and 'Copy to...'. Below the main table, there is a pagination bar showing 'Total: 550', a dropdown for '20' items per page, and a page number '1' out of '28' pages, with a 'Go' button.

Step 2

Recording Schedule

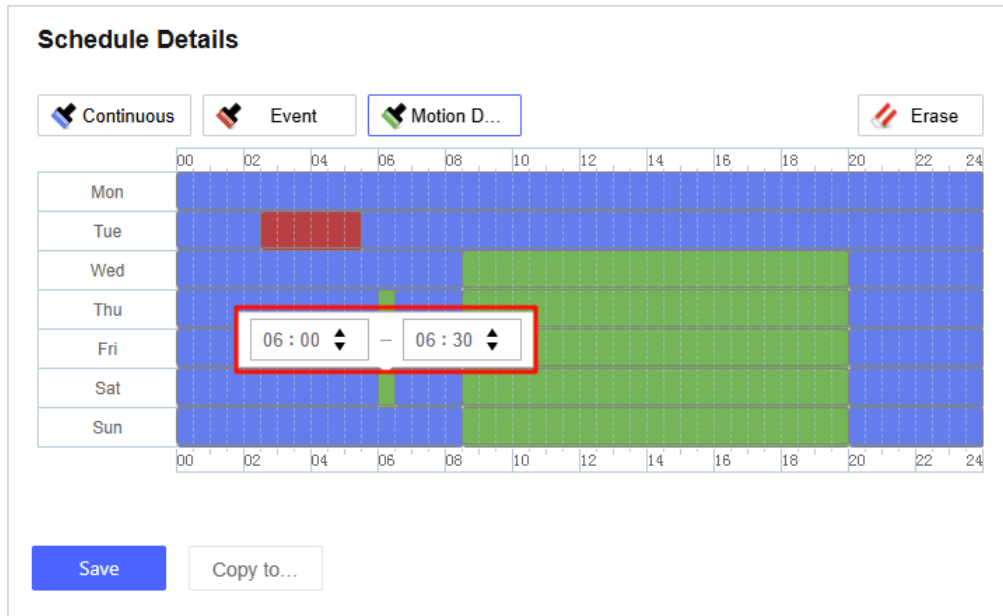
Turn on the switch in the **Enable** column.

Step 3  **Note**

Step 4 For channels added to the device, the switch is disabled by default.

Set the recording schedule as **All-Day Continuous Schedule**, **All-Day Event Schedule**, or **Custom**.

(Optional) When selecting **Custom**, set the schedule details on the right side.

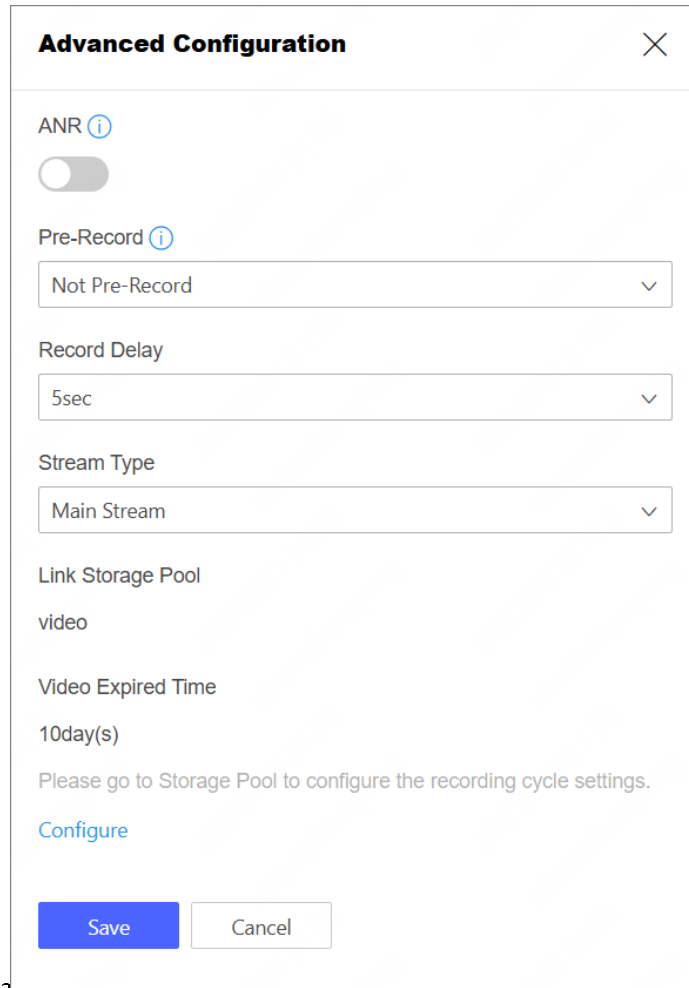


Custom Schedule Details

- 1) Select a schedule type, including **Continuous**, **Event** and **Motion Detection**. Drag the mouse to set the schedule period.
- 2) (Optional) Select **Erase** and then drag the mouse to cancel the schedule you have drawn.
- 3) (Optional) Hover around the time table to adjust the schedule at minute level.
- 4) Click **Save** to apply the schedule.
- 5) (Optional) Click **Copy To...**, you can copy the schedule to other channels.

Step 5

Click  in the **Advanced Configuration** column to set the corresponding parameters.

The image shows a web-based configuration window titled "Advanced Configuration" with a close button (X) in the top right corner. The window contains several settings: "ANR" with an information icon and a disabled toggle switch; "Pre-Record" with an information icon and a dropdown menu set to "Not Pre-Record"; "Record Delay" with a dropdown menu set to "5sec"; "Stream Type" with a dropdown menu set to "Main Stream"; "Link Storage Pool" with the text "video"; and "Video Expired Time" with the text "10day(s)". Below these settings is a greyed-out instruction: "Please go to Storage Pool to configure the recording cycle settings." followed by a blue "Configure" link. At the bottom are two buttons: a blue "Save" button and a white "Cancel" button with a grey border.

Advanced Configuration ✕

ANR ⓘ
☐

Pre-Record ⓘ
Not Pre-Record ▾

Record Delay
5sec ▾

Stream Type
Main Stream ▾

Link Storage Pool
video

Video Expired Time
10day(s)

Please go to Storage Pool to configure the recording cycle settings.
[Configure](#)

Save Cancel

Figure 4-3

Advanced Configuration

- **ANR:** Asynchronous Node Recovery (ANR) is a fault tolerance mechanism. When it is enabled, if there is a network anomaly between the device and the camera, the camera will be used for recording storage temporarily (provided that the camera is equipped with storage media). Once the network is restored, the stored data will automatically synchronize to the device, ensuring the integrity of the recordings.
- **Pre-Record:** Record before the alarm.
- **Record Delay:** Record after the alarm.
- **Stream Type:** Supports main stream and sub stream.

**Note**

- Actual pre-record time may be shorter than the setting.
- After reaching the recording cycle, the outdated recordings will be deleted.
- For detailed recording cycle settings, click **Configure** to go to storage pool page.

Video Copy-Back

Video copy-back refers to the process of automatic or manual duplication of recorded video footage from one storage location to another.

4.2

You can view and manage scheduled and manual tasks of video copy-back in the task list. Manual tasks take priority over scheduled tasks.

4.2.1 Task List

Go to **Storage Management** → **Video Copy-Back** → **Task List**.

- View Scheduled Task

Figure 4-4

Scheduled Task

Scheduled tasks currently can only be configured on the platform. After configuring on the platform, you can view tasks on the web page of the device.

On the Scheduled Task page, you can view task details, search for tasks, filter tasks by camera name and status, and view failed tasks in last 7 days, etc.

- Add Manual Task

On the Manual Task page, click **Add**, select channel(s), and then set the recording start and end time to create a manual task.

Figure 4-5

Add Task

After creating tasks, you can view task details, search for tasks, filter tasks by camera name and status, and delete tasks, etc.

4.2.2 Schedule List

4.2.3 Advanced Configuration You can view, enable/disable copy-back schedules that are configured on the platform.

Go to **Storage Management** → **Video Copy-Back** → **Schedule List**.

You can configure advanced parameters for video copy-back, including scheduled copy-back start/end time, interval for scheduling data copy-back, and so on.

Go to **Storage Management** → **Video Copy-Back** → **Advanced Configuration**.

Scheduled Copy-Back Start Time
From

14

day(s)

0

h

0

min

Scheduled Copy-Back End Time
From

0

day(s)

2

h

0

min

Interval for Scheduling Data Copy-Back

0

h

10

min

Range: [from 10 minutes to 24 hours].

*Upper Limit of Single CVR/NVR Copy-Back

32

The maximum number of channels that can be simultaneously copied back by the front-end devices with the same IP address.

Maximum Copy-Back Speed of Single Channel

32Mbps

*Maximum Uploading Channels

200

Save

Advanced Configuration

Storage Pool

Figure 4-6

- 4.3 The storage pool combines multiple physical storage devices into a single logical storage unit to provide greater storage capacity and improved management capabilities.

4.3.1 Storage Pool Management

Supports adding, editing, deleting, and adjusting storage pool space. After adding a storage pool, you need to link channel(s) to the storage pool.

Step 1 Add Storage Pool

- Step 2 Click **Storage Management** → **Storage Pool** → **Storage Pool**.
Click **Add**.

Add Storage Pool

Vehicle Type*

☒ Recording Pool
☐ Picture Pool

Name*

Storage Space*

Tool for Estimating Recording Duration

GiB

Minimum Quota 1400 GiB, Remaining Quota Space 36740 GiB

Select Channel

Search

☒ Select All

☐ IPC

☒ Channel is not connected.

☒ [D1] Channel 1
☒ [D2] Channel 2
☒ [D3] Channel 3
☒ [D4] Channel 4
☒ [D5] Channel 5

Overwrite

☒

Video Expired Time ⓘ

Never Expire

Confirm

Cancel

Add Storage Pool

Configure storage pool parameters.

- **Type:** Select **Recording Pool** or **Picture Pool**.
- **Storage Space:** Enter the storage space. You can click **Tool for Estimating Recording Duration** to calculate the estimated storage space or recording period.
- **Overwrite:** Enable this function to allow overwriting of the oldest recording when storage space is insufficient. Disable this function to stop recording when storage space is insufficient.
- **Video Expired Time:** When **Custom** is selected, recordings will be stored according to the configured recording cycle. Expired recordings will be cleared and cannot be recovered.

**Note**

You can add up to 8 storage pools.

Click **Confirm**.

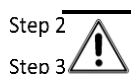
Edit/Delete Storage Pool

Click **Storage Management** → **Storage Pool** → **Storage Pool**.

Hover around the card of the storage pool, and then click **Edit** or **Delete**.

Step 4 Edit or delete the storage pool.

Step 1 Click **Confirm** to complete the operation.

**Caution**

Step 4 After you delete the recording pool, the linked channel(s) of this recording pool will become unable to record. Link to another storage pool promptly.

Adjust Storage Pool Space

Click **Storage Management** → **Storage Pool** → **Storage Pool**.

Step 1 Click **Adjust Storage Pool Space**.

Step 2 Click **Adjust Storage Pool Space**.

Step 3 Adjust storage pool space as needed.

- **Enter Remaining Quantity:** Allocate all the remaining capacity to the storage pool.
- **Tool for Estimating Recording Duration:** Calculate the estimated storage space or recording period.

Adjust Storage Pool Space

Allocate enough space in the recording pool to ensure the channel can record normally. Note: reducing the space in the recording pool will shorten the recording cycle.

Total Capacity **551730GiB** Not Configured **0GiB** [Tool for Estimating Recording Duration](#)

+ Add Storage Pool

Legend	Name	Capacity	Operation
	Recording Pool	551730 GiB 100.00%	Enter R... Delete

Confirm

Cancel

Adjust Storage Pool Space

Link Channel(s)

You can configure the linked channel(s) for the storage pool.

Click **Storage Management** → **Storage Pool** → **Storage Pool**.

Click a storage pool in the list.

Configure linked channel(s) for the storage pool as needed.

- Step 1 ●  **Linked Channel** : Add linked channel.
- Step 2 ●  **Move To** : Move the checked channel(s) to another storage pool.
- Step 3 ●  **Unlink Channel** : Batch unlink the checked channel(s) from the current storage pool.
-  : Search the linked channel(s) by channel name.

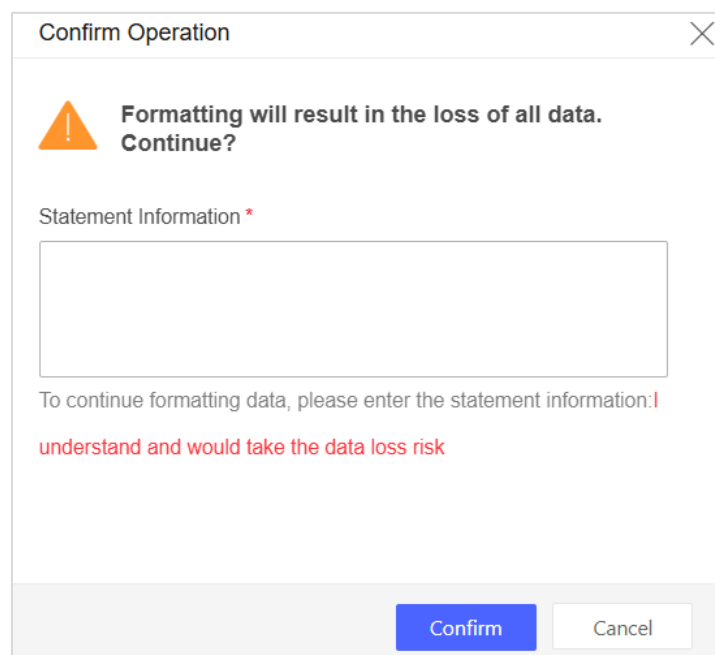
4.3.2 Storage Space Management



Caution

Formatting will delete all data of the array. Operate with caution.

- Step 1 Click **Storage Management** → **Storage Pool** → **Storage Space / Storage System**.
- Step 2 Check the array(s) that need to be formatted, and then click **Format / Initialize**.
- Step 3 Enter the statement information, and then click **Confirm** to start formatting.



Formatting

Metadata Repair

Figure 4-9

You can use metadata repair when the array cannot work normally.

- Step 1 Click **Storage Management** → **Storage Pool** → **Storage Space / Storage System**.
- Step 2 Check the array(s) that need to be repaired, and then click **Metadata Repair**.
- Step 3 Click **Confirm** to start metadata repairing. You can check the progress in the status column.



Caution

- Metadata repair will not affect recordings, but searching and playback will be temporarily unavailable.
- Do not turn off the device during repairing.

4.4.1 View Array

Array Management

You can manage arrays, configure array synchronization rates, and rebuild arrays. Through RAID technology, data reliability and fault tolerance capabilities are enhanced.

You can check the basic information and HDDs status of the array.

Go to **Storage Management** → **Array Management** → **Array**.

Array

HDD

Create Array

Quick Rebuild

Set Rebuilding Speed

☒	No.	Name	Type	Capacity (GiB)	HDD Slot	Status	Operation
☒	1	RAID_1	VRAID	36740	4, 8, 12, 16, 20, 24	Normal	

HDD List (RAID_1)

Refresh

☐	Slot	Capacity (GiB)	Status	Belonged Array	Usage	Serial No.	Model
☐	4	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102
☐	8	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102
☐	12	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102
☐	16	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102
☐	20	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102
☐	24	7452.04	Normal	RAID_1	Array	WSD13453	ST8000NM002A-2KE102

View Arrays

- Click the array, there will be HDD information in the HDD List. You can click **Refresh** to refresh the list.
- Click  to show more arrays.

4.4.2 Create Array

Before creating an array, make sure the number of installed HDDs meets the need of a new array.

Step 1

Click **Storage Management** → **Array Management** → **Array**.

Step 2

Click **Create Array**, and then set the parameters.

- RAID Position:** The position assigned for the newly created array.
- Array Name:** There is a default name, which can be customized.
- Select HDD:** Select the HDDs according to the RAID level.
- Level:** Indicates the RAID level.
- Available Capacity:** When the number of selected HDDs matches the requirement, it will display the number.

Step 3

Step 4



Note

Creating a VRAID5/RAID5 array requires at least 9 HDDs, and a VRAID6/RAID6 array requires at least 10 HDDs.

Click **Confirm**.

(Optional) Perform the following after creating arrays.

- Rebuild Array:** Click  in the **Operation** column to manually rebuild the array that is in degraded status.

- Quick Rebuild: Click **Quick Rebuild** to automatically rebuild all arrays that are in degraded status. This function is only available when the array type is **VRAID**.
- Delete Array: Click  in the **Operation** column to delete the array.



Caution

Deleting array will cause irreversible loss of all data contained within the array, with no data recovery capability under any circumstances. Please operate with caution.

When one or more HDDs fail, you can rebuild an array manually or batch rebuild arrays.

Click **Storage Management** → **Array Management** → **Array**.

4.4.3 Rebuild Array

Rebuild arrays.

- Step 1
- Step 2
- Rebuild Array: Click  in the Operation column to manually rebuild the array that is in degraded status.
 - Quick Rebuild: Click **Quick Rebuild** to automatically rebuild all arrays that are in degraded status. This function is only available when the array type is **VRAID**.

4.4.4 Set Rebuilding Speed

You can set rebuilding speed for all arrays in the device.

Step 1

Step 2 Click **Storage Management** → **Array Management** → **Array**.

Click **Set Rebuilding Speed**.

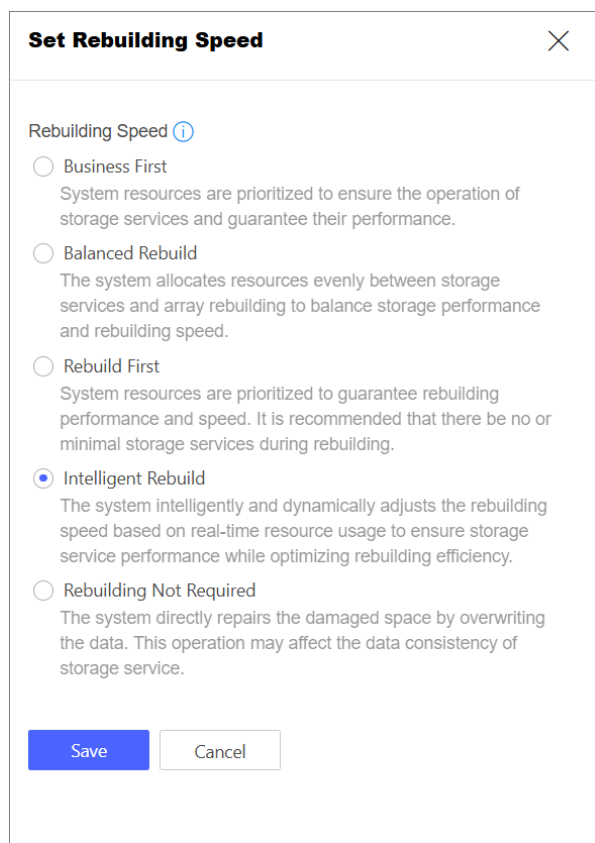


Figure 4-11

Set Rebuilding Speed

- Step 3 Select the rebuilding speed. Refer to the explanation of each rebuilding mode.
- Step 4 Click **Save** to save the above setting.

4.5

HDD Mangement

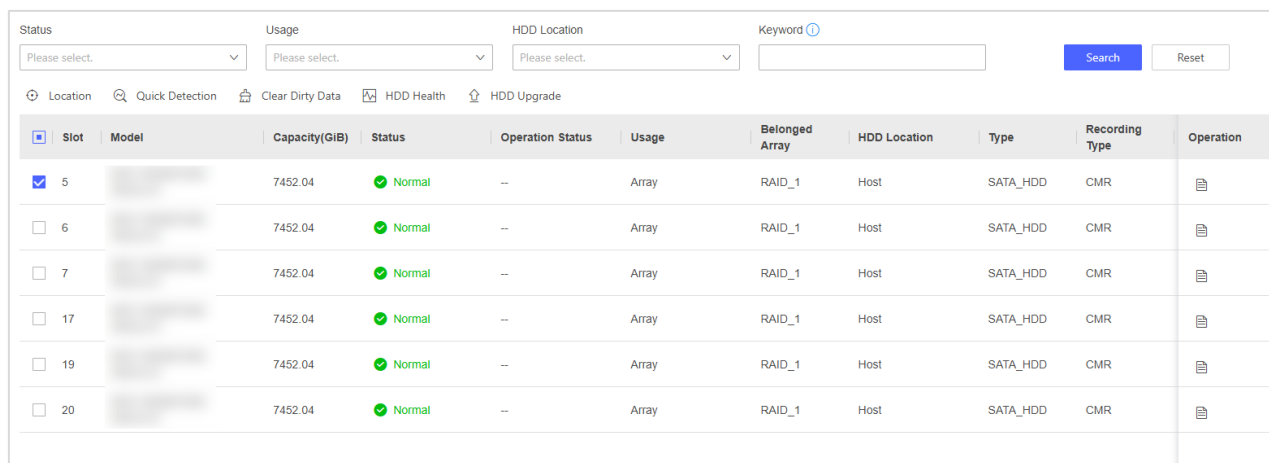
- 4.5.1 View/locate/Upgrade HDD Supports searching and checking the HDD information. You can run an S.M.A.R.T. detection or initialize the HDD(s).

Go to **Storage Management** → **Array Management** → **HDD**.

- View HDD: Select status, usage, and HDD location, and then click **Search**.
- Locate HDD: Check the HDD, and then click **Location**. Follow the instructions to find the HDD on device.
- Upgrade HDD: Check the HDD(s) to be upgraded, and then click **HDD Upgrade**. Click  to import upgrade file and click **Upgrade**.

Note

Supported keywords: Slot, model, status, array, type, recording method, and serial number.



Slot	Model	Capacity(GiB)	Status	Operation Status	Usage	Belonged Array	HDD Location	Type	Recording Type	Operation
☒ 5		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	
☐ 6		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	
☐ 7		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	
☐ 17		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	
☐ 19		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	
☐ 20		7452.04	Normal	--	Array	RAID_1	Host	SATA_HDD	CMR	

View HDD

Figure 4-12

HDD detection includes quick detection and S.M.A.R.T. detection.

4.5.2 HDD Detection

Click **Storage Management** → **Array Management** → **HDD** to enter the page.

Step 1 Check the HDD(s) that need to be detected, and then click **Quick Detection** or **HDD Health**.

- Step 2
- Quick Detection: The detection result will be displayed in the **Status** column.
 - HDD Health: Refer to [HDD Health](#) for more details.

4.5.3 Clear Dirty Data

The HDD needs to be cleared when there is non-local metadata.



Caution

Step 1

Step 2 Clearing dirty data will erase all data in the HDD. Operate with caution.

Step 3

Click **Storage Management** → **Array Management** → **HDD** to enter the page.

Step 4

Find and check the HDD(s) that need to be initialized.

Step 5

4.6 Click **Clear Dirty Data**.

Follow the instructions to initialize HDD(s).

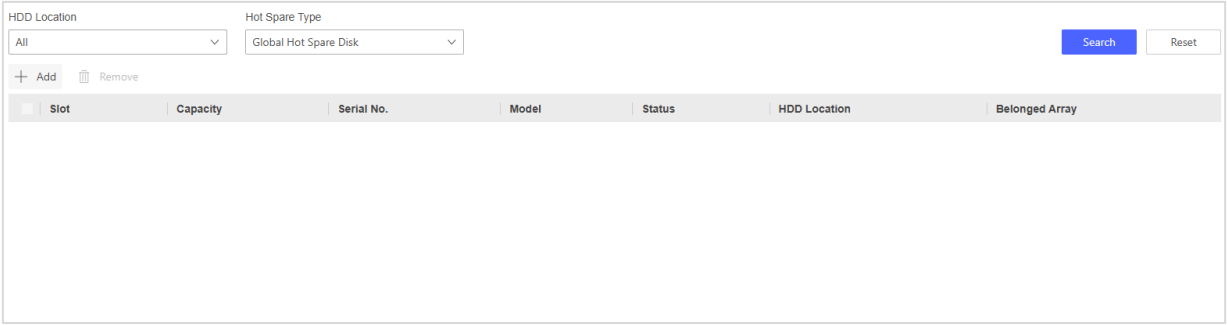
Step 1

After clearing dirty data, you need to add the HDD(s) to the array manually.

Hot Spare Disk

Supports adding hot spare disks in the storage system to ensure automatic fault tolerance and data reconstruction.

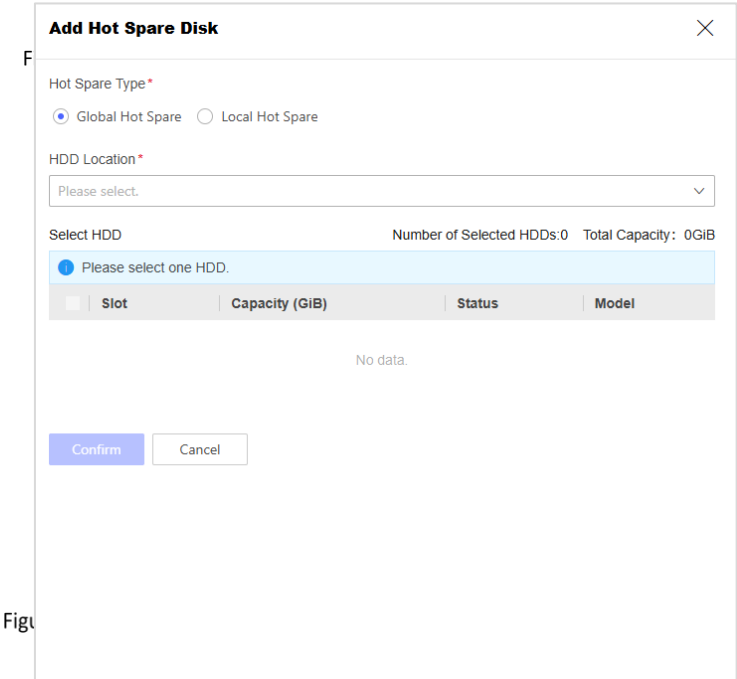
Go to **Storage Management** → **Array Management** → **Hot Spare Disk**.



Hot Spare Disk

Click **Add** to add a hot spare disk.

Step 2



Add Hot Spare Disk

Step 3
Step 4
Step 5

Select type, location, and HDD.

4.7 Click **Confirm**.

(Optional) Check the created hot spare disk(s) and click **Remove** to delete the added hot spare disk(s).

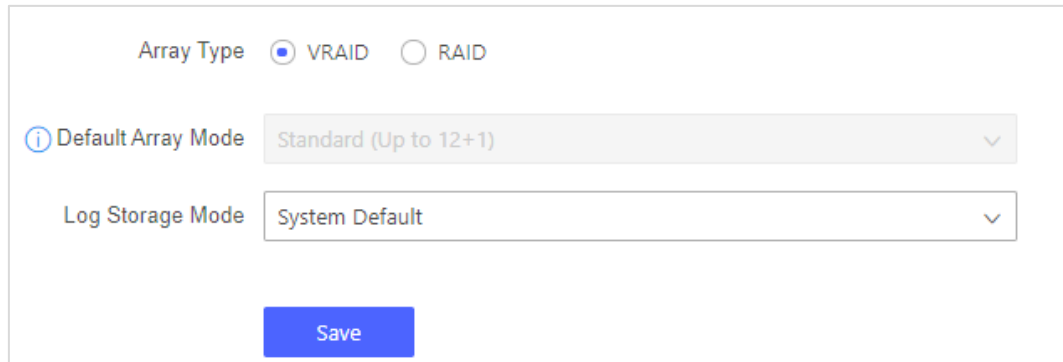
Advanced Configuration

You can configure the advanced parameters for storage.

 Note

Configurations vary by device models and versions. The actual interface prevails.

Go to **Storage Management** → **Advanced Configuration** → **Advanced Configuration**.



Array Type ☒ VRAID ☐ RAID

i Default Array Mode Standard (Up to 12+1) ▼

Log Storage Mode System Default ▼

Save

Advanced Configuration (Version 1)



Log Storage Mode System Default ▼

Save

Advanced Configuration (Version 2)

- **Array Type:** Select **VRAID** (default) or **RAID**.
- **Default Array Mode:** Select **Standard** or **High Utilization Rate**. The two modes suggest different preconfigured storage redundancy and performance setting automatically applied when initializing a storage system.
- **Log Storage Mode:** Select **System Default** or **Custom**. When you select **System Default**, the previous logs will be overwritten when the storage space is full. When selecting **Custom**, you should set the log storage cycle.

Note

- Before switching array type, you should delete the added arrays.
- Only the latest device version supports **Default Array Mode**. The actual interface prevails.

Chapter 5 Channel Management

Add and Manage Channels

You can add channels using IP addresses and manage them by performing actions like exporting and editing.

Click **Channel Management**.

5.1

Step 1

+ Add - Delete Export Import Refresh ... More												
☐	Channel No.	Camera Name	IP Address	Stream ID	Status	Storage Pool	Password S...	Protocol Type	Port	Serial No.	Version	Operation
☐	D1	10.17.196.25	10.17.196.25	-	Online	video	Weak	HIKVISION	20000	10.17.196.25	V5.5.95 build 210104	
☐	D2	10.17.196.25	10.17.196.25	-	Online	video	Weak	HIKVISION	20000	10.17.196.25	V5.5.95 build 210104	
☐	D3	10.17.196.25	10.17.196.25	-	Online	video	Weak	HIKVISION	20001	10.17.196.25	V5.5.95 build 210104	
☐	D5	10.17.196.25	10.17.196.25	-	Online	video	Weak	HIKVISION	8000	10.17.196.25	V5.4.50 build 250124	

Channel List

Click **Add**.

Figure 5-1

Step 2

Add Channel

[Add Single IP](#)

IP Address *

Protocol HIKVISION Port *

User Name Password

Transfer Protocol Auto

Add Channel

Enter the IP address of the channel.

Click **Test** to check connectivity.

Set the following parameters.

- **Protocol:** Select from the drop-down list or set a custom protocol. For details about customizing protocols, refer to [Custom Protocol](#) for more details.
- **User Name & Password:** Set for later channel management.
- **Port:** Port of the channel. It is 8,000 by default and you can edit the port number. After editing, you can click to set the port number to the default value.

- **Transfer Protocol:** Data transmission protocol. Select **Auto**, **TCP** or **UDP**.

Click **Confirm** to finish adding the channel, or click **Continue to Add** to add the channel and continue to add the next channel.

(Optional) Perform the following after adding channels.

- **Edit Channel:** Click the camera name to enter the **Edit Channel** page and edit parameters.
- **Export Channels:** Click **Export** to export information of all channels to your local PC. Select channel(s) and click **Export** to export information of the selected channel(s) to your local PC.
- **Import Channels:** After exporting channels, enter channel information in the exported file. Click **Import**, and click  to batch import channels.

Step 6

Step 7

Custom Protocol

You can customize the protocol for a channel.

5.2

Click **Channel Management** to enter the page.

Step 1

Click **More** → **Custom Protocol**.

Step 2

Select a custom slot from the left panel.

Step 3

Step 4

Configure the parameters.

- **Protocol Name:** Customize or choose from the tag below.
- **Main Stream / Sub-Stream**
 - **Transfer Protocol:** Supports Auto, UDP and RTP over RTSP.
 - **Port:** The port will be used by the protocol. 554 by default.
 - **Stream Path:** Format: [Type]://[IP Address]:[Port]/[Resource Path].
Example: RTSP://192.168.0.1:554/ch1/main/av_stream.



Note

- If the IP camera does not support sub-stream or has no need to use the sub-stream, please set the sub-stream to disable.
- IP channels added via the custom protocol must support standard RTSP streaming, and you need to obtain the main/sub-stream URLs from the camera manufacturer beforehand.

Custom Protocol

HIKVISION_RTSP

HIKVISION_HTTP

HIKVISION_HTTPS

DAHUA_RTSP

UNIVIEW_RTSP

TPLINK_RTSP

HUAWEI_RTSP

Custom 8

Custom 9

Custom 10

Custom 11

Custom 12

Custom 13

Custom 14

Custom 15

Custom 16

Custom 17

Custom 18

Custom 19

Custom 20

Check your device URL address, and enter accordingly.

Format: [Type]://[IP Address]:[Port]/[Resource Path]

Example: RTSP://192.168.0.1:554/ch1/main/av_stream

Protocol Name *

HIKVISION_RTSP

HIKVISION

DAHUA

UNIVIEW

TPLINK

HUAWEI

Main Stream

Protocol Type

Transfer Protocol

RTSP

Auto

Port *

Stream Path

554

ch1/main/av_stream

Sub-Stream

Stream

Protocol Type

Transfer Protocol

Confirm

Cancel

Custom Protocol

5.3

5.3.1 Manual Time Sync

Step 1 Batch Time Sync

Step 2 You can batch sync device time manually or in a scheduled way.

Step 3

Click **Channel Management**.

Click **More** → **Batch Time Sync**.

Click **Sync Time Now** to synchronize the time for all devices.

Manual Time Sync

Manual Time Sync

Sync Time Now

Sync

The time of all devices would be synced after clicking.

Manual Time Sync

Click **Channel Management** to enter the page.

Click **More** → **Batch Time Sync**.

Figure 5-4

Enable **Schedule Time Sync**, and then select device(s).

5.3.2 Schedule Time Sync

- Step 1
- Step 2
- Step 3
- Step 4
- Set the **Time Sync Interval**, and then click **Save** to apply the configuration.

Schedule Time Sync

Enable

After enabling, the time of following devices would be synced according to the schedule.

Select Device

Refresh

Device Name	Time Sync	Status
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled
IPCamera 011	☒	Disabled

Total: 550

60

<123456...10>1 / 10PageGo

*Time Sync Interval

60

min

Scheduled Time Sync

Chapter 6 Live View

Click **Live View** on the left menu.

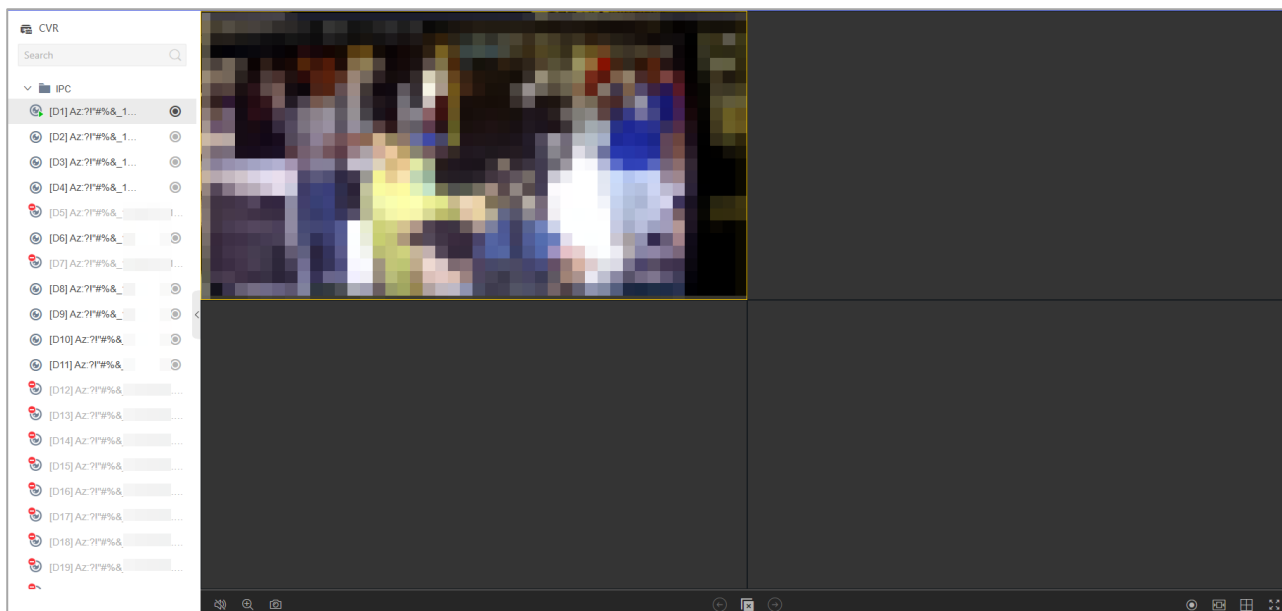


Figure 6-1
Live View

Refer to the table below for detailed explanation of icons on the live view control bar.

Table 6-1

Controls in the Live View

Button	Description
 / 	Start/Stop live view.
 / 	Previous/next page. Button available only when live view started.
  	Audio control.
	Digital zoom. Using mouse wheel to zoom in or zoom out.
	Capture. Refer to Picture and Clip Settings for configuring saving path.
	Split screen. Supported 1, 4, 9, 16.
	Start recording. Refer to Video Settings for configuring saving path.
	Live view image ratio.

Button	Description
	Full-screen.

Chapter 7 Playback

Playback



Note

Playback capability is limited by the computer's memory usage and may not support 16-screen playback.

7.1 Click **Playback** on the left menu.

Select a playback channel and date on the left.

View and adjust playback panel as needed.

Descriptions of icons on the playback control bar are in Table 7-1.



Playback

Description of Playback Page Buttons

Button	Description
	Playback control buttons: Play, Pause, Stop.
	Reverse playback.
	Play frame-by-frame. Click to play one frame at a time.
	Playback speed.
	Volume adjustment.

Button	Description
	Capture. Refer to Picture and Clip Settings for capturing file path.
	Digital zoom. After enabling, you can use mouse wheel to zoom in or out.
	Clip. Refer to Picture and Clip Settings for file saving path.
	Lock recordings.
	Download recording. Refer to Video Settings for more details.
	Stop all playback.
	Screen size.
	Screen split. Supports 1,4,9,16.
	Full-screen.
	Timeline rage.

7.2

Download Video

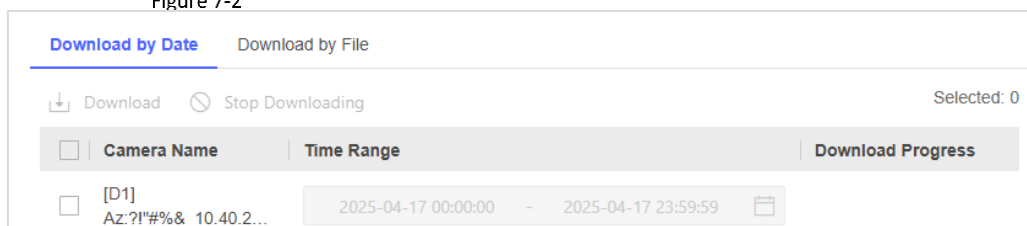
On the Playback page, click  in the lower right corner.

Select a download type.

Download by Date

1. Check the channel(s).
2. Select stream type and time range.
3. Click **Download** to start.

Figure 7-2



Download by Date

Download by File

1. Select channel(s), file type, time range, lock type, and stream type.
2. Click **Search** to search recording files.
3. Check the file(s) as needed.
4. (Optional) Change lock status. After being locked, the recording will not be overwritten.
5. Click **Download** to start. You can check the process in **Download Progress** column.

Download by Date
Download by File

Channel
File Type
Time Range

[D1] Az:?!*#%&_10.40.2...
All Types
2025-04-17 00:00:00 - 2025-04-17 23:59:59

Lock Type

All
Search

Download
Stop Downloading
Selected: 0

	File Name	File Size	Time Range	Locking Status	Opera...	Download Progress
☐	0268013...	116 MB	2025-04-17 16:55:04 - 2025-04-17 17:03:22	Unlocked		
☐	0268013...	64 MB	2025-04-17 17:47:44 - 2025-04-17 17:52:55	Unlocked		
☐	0268014...	20 MB	2025-04-17 17:55:57 - 2025-04-17 17:57:35	Unlocked		

Figure 7-3

Download by Files

Chapter 8 Event Center

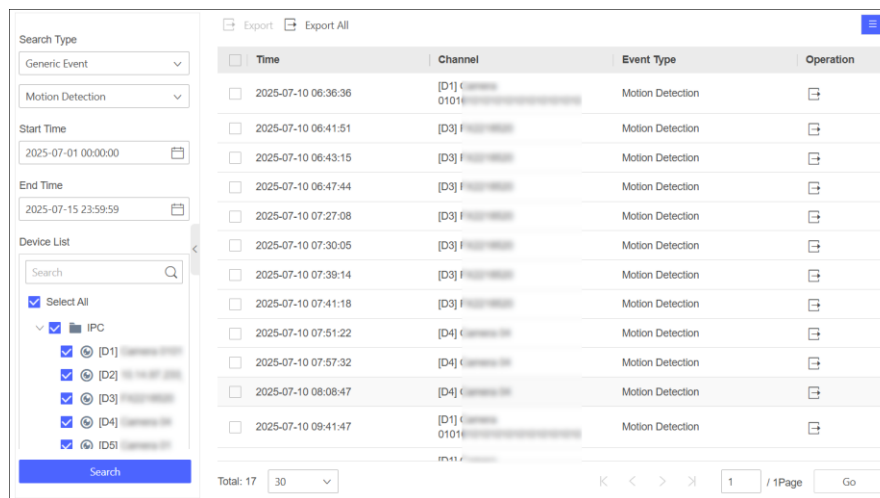
Event configuration includes motion detection, video tampering and video loss.

Event Search

You can set conditions to search for events. After searching, you can view event details, start playback linked with the event, export event(s), etc.

Go to **Event Center** → **Event Search**.

8.1



Search for Events

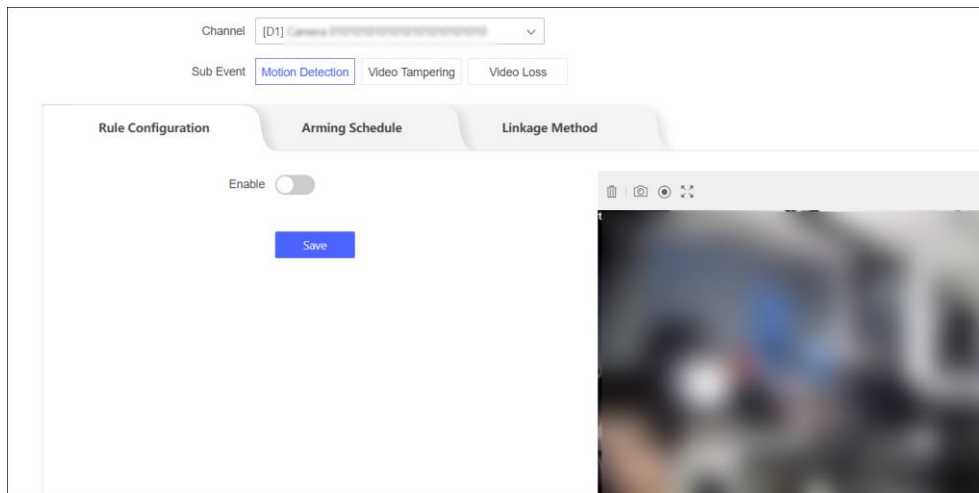
8.2

Event Configuration

Go to **Event Center** → **Event Configuration** → **Event Configuration**.

Select a channel, select the sub event, and then configure parameters.

Click **Save** to apply the configuration.



Event Configuration

Figure 8-2

Chapter 9 System Configuration

Local

You can configure live view parameters, video settings, picture and clip settings.

9.1 Go to **System Configuration** → **Local** → **Live View Parameter**.

- **Playing Performance:**

9.1.1 Live View Parameter

- **Shortest Delay:** Minimizes delay for real-time video.

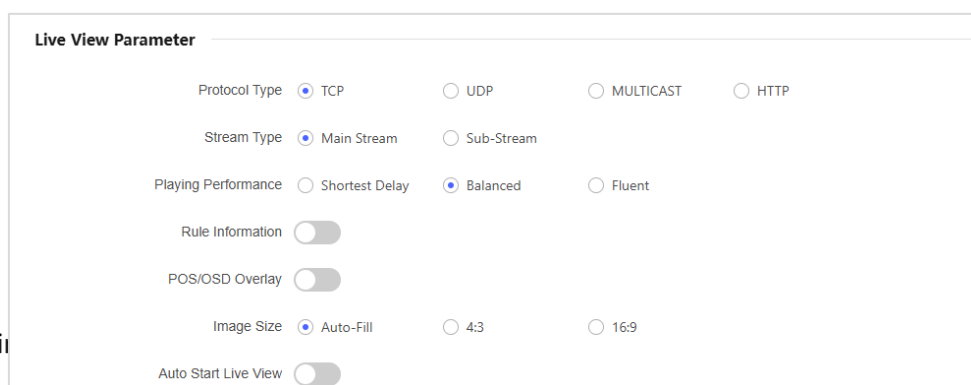
- **Balanced:** Optimizes both delay and smoothness.

- **Fluent:** Prioritizes smooth playback.

- **Rule Information:** If the function is enabled, rule information will overlay the live view image.

- **POS/OSD Overlay:** If the function is enabled, POS and OSD information will overlay the live view image.

- **Auto Start Live View:** If the function is enabled, all channels will automatically start live view when the user enters this page.



9.1.2 Video Settings

Live View Parameter

You can configure video size, video saving path, and downloaded file saving path.

Go to **System Configuration** → **Local** → **Video Settings**.

Video Settings

You can configure image format, capture file saving path, and clip saving path.

Go to **System Configuration** → **Local** → **Picture and Clip Settings**.

9.1.3 Picture and Clip Settings

Figure 9-3

Picture and Clip Settings

9.2 System Configuration

System time synchronization and serial port management.

9.2.1 Region and Time

Step 1

Step 2

Step 3 Click **System Configuration** → **System Configuration** → **Region & Time**.

Step 4

Select an area/country/region.

Select a time zone.

Step 5

Select time sync mode and set the corresponding parameters.

Step 6

- **NTP Time Sync:** Enter the IP address and port number of the NTP server, and

9.2.2 RS-232 synchronization interval.

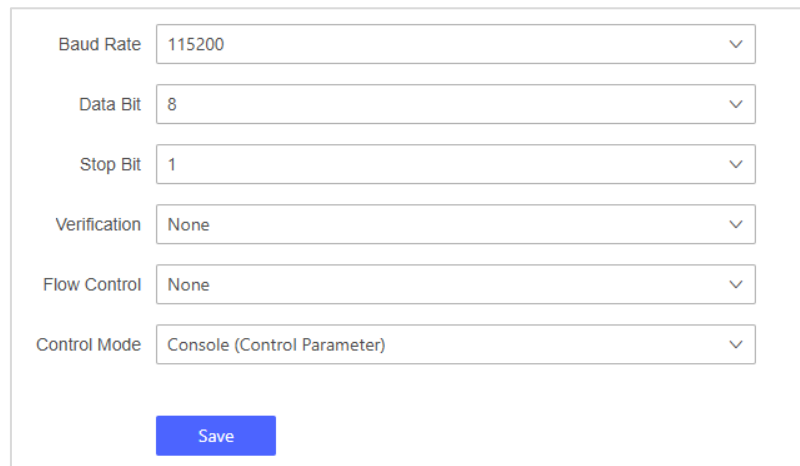
- **Manual Time Sync:** Set the time manually or synchronize with computer time.

Enable **DST** and sync time if the selected area/country/region observes DST.

Click **Save** to apply the configuration.

Go to **System Configuration** → **System Configuration** → **RS-232**.

- **Baud Rate:** Data transmission speed (bps). Default: 115200.
- **Data Bit:** Number of valid data bits per character. Default: 8.
- **Stop Bit:** Bits signaling end of character transmission. Default: 1.
- **Verification:** Data verification method. Default: None.
- **Flow Control:** Data rate regulation. Default: None.
- **Control Mode:** Serial port operation method.



The image shows a configuration form for RS-232 Serial Port. It contains six dropdown menus, each with a label on the left and a value in the box with a downward arrow on the right. The values are: Baud Rate (115200), Data Bit (8), Stop Bit (1), Verification (None), Flow Control (None), and Control Mode (Console (Control Parameter)). Below these fields is a blue button labeled 'Save'.

RS-232 Serial Port Configuration

Figure 9-4

9.3 User Management

You can add and manage users. Up to 32 users (admin included) can be created.

9.3.1 Add User

Step 1

Step 2

Click **System Configuration** → **User Management**.

Step 3

Step 4

Click **Add**.

9.3.2 Edit/Delete User

Configure user information and permissions.

Step 1

Click **Confirm** to create user.

Step 2

Click **System Configuration** → **User Management**.

Edit or delete a user as needed.

- Edit: Click  to edit user information.
- Delete:
 - Delete Single User: Click  at the **Operation** column.
 - Batch Delete Users: Check the users and then click **Delete**.

Go to **System Configuration** → **User Management** → **Account Security Settings**.

- **Security Question Configuration:** The answers to the security questions can help you to retrieve your password.
- **Export GUID File:** The GUID file can help you to retrieve your password.

9.3.3 Account Security Settings



It is highly recommended to export and keep the GUID file properly.

- **Reserved Email:** Set an e-mail address to receive verification code for password recovery.

Account Security Settings

Security Question Configuration

Security Question1
What is your father's name? ▾

Answer*
[Text Input]

Security Question2
What is your mother's name? ▾

Answer*
[Text Input]

Security Question3
What is the name of your teacher in charge of class in senior ... ▾

Answer*
[Text Input]

Export GUID File ⓘ

[Export]

Reserved Email

Set an e-mail address to receive verification code for password recovery. [X]

[OK] [Cancel]

Figure 9-5

Account Security Settings

9.4

9.4.1 Network Parameter

Network Configuration

Step 1

You can add NIC bonding, enable SNMP, configure email, etc.

Add NIC Bonding

Click **System Configuration** → **Network Configuration** → **Network Parameter** → **NIC Configuration**.

Click **Add NIC Bonding**.

Step 2

Add NIC Bonding

Name

bond1

Mode

☒ Active-Backup

No need to configure switch. Automatically fails over to backup port if active port fails.

☐ XOR Mode

Need to enable static link aggregation on both switch and device; otherwise, network disconnection will occur.

☐ 802.3ad

Need to enable LACP on switch; otherwise, network disconnection will occur.

☐ Self-Adaptive Load Balancing (Virtualized)

No need to configure switch. Not suitable for cross-subnet environments.

Balanced

N/A

Select Network Port

☐ All

☐ LAN5

2.5 Gbps

☐ LAN6

2.5 Gbps

☐ LAN7

2.5 Gbps

☐ LAN8

2.5 Gbps

Save

Cancel

Add NIC Bonding

Step 3

Select a bonding mode.

- **Active-Backup:** A basic fault-tolerant solution that provides redundancy for data ports/data transmission. Only one data port remains active at all times, while the others serve as backups, automatically taking over if the active port fails. The entire link appears as a single MAC address externally, ensuring normal switch operation.

- **XOR Mode:** A solution that achieves load balancing and fault tolerance based on a specified packet distribution strategy. The system dynamically allocates network traffic according to the configured HASH algorithm. Note: This mode requires configuring and enabling static link aggregation on both the switch and the device. Otherwise, the network will be disconnected.
- **802.3ad:** A solution that achieves load balancing and fault tolerance based on LACP (Link Aggregation Control Protocol). Data ports within the same dynamic link aggregation group operate at the same speed and duplex settings. Note: This mode requires configuring and enabling LACP on the switch. Otherwise, the network will be disconnected.
- **Self-Adaptive Load Balancing (Virtualized):** No need to configure switch in this mode. However, this mode is not applicable to any cross-subnet environments that require gateway routing, where inbound load balancing will completely fail. It has higher network stability requirements and slightly lower fault tolerance capability compared with the XOR mode (recommended).



Note

If the active-backup mode does not meet the bandwidth requirements, you can choose XOR (preferred) or self-adaptive load balancing mode. For choosing XOR mode, you should ensure your switch supports static link aggregation and the function is enabled.

- Step 4 Check the NICs to be added to the bond.
- Step 5 Click **Save** to save the above settings.
- Step 6 (Optional) Edit the default parameters such as IP address and subnet mask for the NIC bonding.

Configure DNS

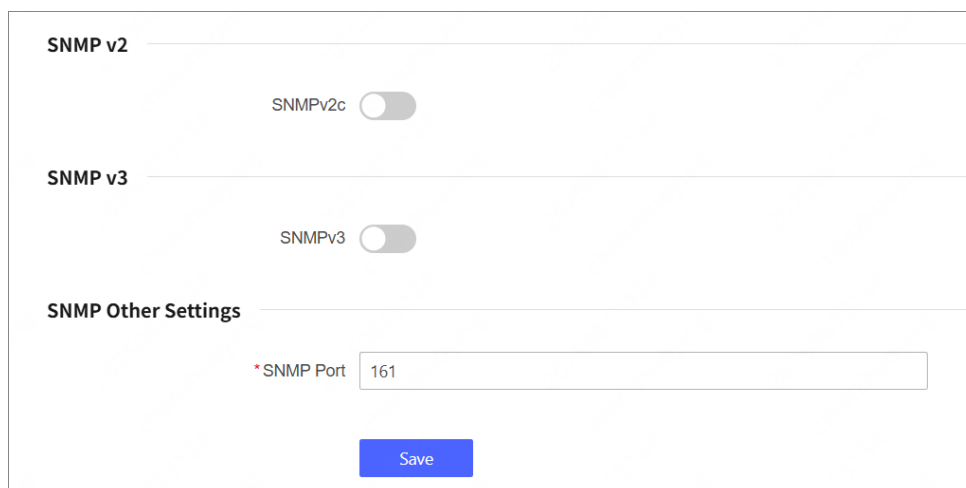
Go to **System Configuration** → **Network Configuration** → **Network Parameters** → **NIC Configuration**.

In the **DNS Server Address** area, enter the preferred DNS server address and the alternate DNS server address, and click **Save** to save the settings.

Step 1 Enable SNMP

You can enable SNMP and configure corresponding parameters for the third party to access the functions of the device.

Go to **System Configuration** → **Network Configuration** → **Network Parameter** → **SNMP**.



The image shows a configuration form for SNMP. It has three sections: 'SNMP v2' with a toggle for 'SNMPv2c', 'SNMP v3' with a toggle for 'SNMPv3', and 'SNMP Other Settings' with a text input for '* SNMP Port' set to '161'. A blue 'Save' button is at the bottom.

Enable SNMP

Enable SNMPv2c and configure parameters.

Enable SNMPv3 and configure parameters.

Step 2

Step 3

Configure SNMP port number.

Step 4

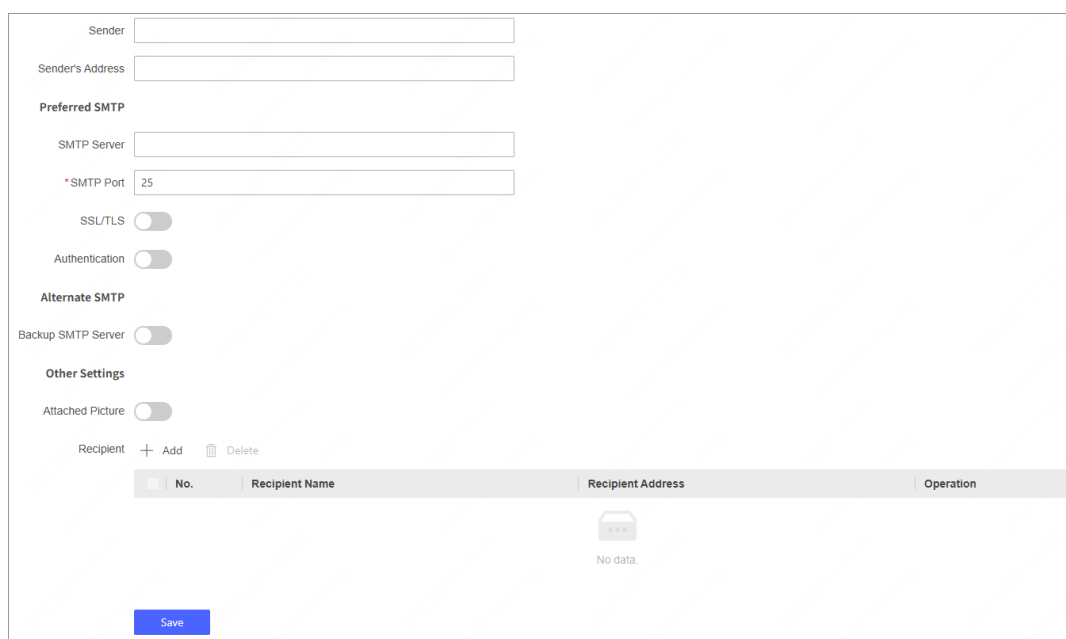
Click **Save**.

Step 5

Configure Email

After configuring the email, you can receive alarm notifications via email.

Step 1 Click **System Configuration** → **Network Configuration** → **Network Parameter** → **Email**.



The image shows an email configuration form. It includes fields for 'Sender', 'Sender's Address', 'Preferred SMTP' (with 'SMTP Server' and '* SMTP Port' set to '25'), 'SSL/TLS', 'Authentication', 'Alternate SMTP' (with 'Backup SMTP Server'), and 'Other Settings' (with 'Attached Picture'). At the bottom, there is a table for recipients with columns 'No.', 'Recipient Name', 'Recipient Address', and 'Operation'. A blue 'Save' button is at the bottom left.

Configure Email

Step 2 Configure sender information: sender name and sender address.

Step 3 Configure the primary SMTP server.

- **SMTP Port:** Default: 25. If SSL/TLS is enabled, enter 587.
- **SSL/TLS:** When this function is enabled, email content will be encrypted during transmission.
- **Authentication:** When this function is enabled, authentication username and password are required.

Step 4 (Optional) Configure a secondary SMTP server.

Step 5 (Optional) Configure image attachments. When this function is enabled, select the snapshot interval.

Step 6 Configure recipients. Click **Add**, and then enter recipient name and recipient address.

Step 7 Click **Test** to verify if the address can successfully receive emails.

Step 8 Click **OK** to add the recipient. Repeat steps 6-8 until all recipients are added.

Step 9 Click **Save** to apply the configuration.

Other Configurations

You can configure multicast address and download bandwidth.

Go to **System Configuration** → **Network Configuration** → **Network Parameter** → **Other**.

After configuration, click **Save** to apply the configuration.

Other Network Configuration

9.4.2 Platform Access

You can enable SDK service and enhanced SDK service, and configure related parameters.

Go to **System Configuration** → **Network Configuration** → **Platform Access** → **SDK**.

After configuration, click **Save** to apply the settings.

- Enable **Enhanced SDK Service**: The enhanced SDK service is a network service constructed with SDK + TLS protocol that enables encrypted transmission and identity authentication. When enabled with stream encryption at the transport layer, TLS provides end-to-end encryption. The

device uses SDK over TLS protocol to forward streams (including previewing, playback, and downloading recorded files), significantly enhancing product security.

- Enable **SDK Service**: The SDK service operates based on the Hikvision Protocol. When the function is enabled, the device becomes accessible to clients and platforms.

SDK Service Configuration

Figure 9-10

9.4.3 Network Service

During remote network live view, the RTSP port is required for real-time video streaming. When accessing web services remotely, HTTP (unsecured) or HTTPS (secured) ports are used for browser-based access. The service port enables direct client connections, while the Enhanced Service Port supports both clients and third-party platform integrations.

HTTP(S)

Go to **System Configuration** → **Network Configuration** → **Network Service** → **HTTP(S)**.

- Enable **HTTP**: If HTTP is enabled, you can use HTTP to access the device.
- Enable **HTTPS**: If HTTPS is enabled, you can use HTTPS to access the device.



Note

Before enabling HTTPS, please make sure the TLS for client is enabled. Refer to [TLS](#) for more details.

- **Port**: The default HTTP port is 80, and the HTTPS port defaults to 443.
- **Enable HTTPs Browsing / Automatic Redirection to HTTPS**: After this is enabled, device access requests will be automatically redirected to the HTTPS protocol.
- **Authentication Mode**:
 - **digest**: Only digest-authenticated requests are permitted.
 - **digest/basic**: Both digest and basic authentication schemes are accepted.

RTSP

Go to **System Configuration** → **Network Configuration** → **Network Service** → **RTSP**.

- **Enable:** Check to enable RTSP access to the device.
- **Port:** The port used for the RTSP protocol. Default: 554.
- **Authentication Mode:**
 - **digest:** Only digest-authenticated requests are permitted.
 - **digest/basic:** Both digest and basic authentication schemes are accepted.



Note

For security reasons, it is recommended to select digest as the RTSP authentication mode.

WAN Mapping

WAN mapping directs external requests to internal devices by binding a specific port on the router's public IP to the private IP and port of the target device.

Go to **System Configuration** → **Network Configuration** → **Network Service** → **WAN Mapping**.

Configure WAN IP address and port, and then click **Save** to apply the configuration.

9.5

WAN Mapping

Configure N+1 Hot Spare

Step 1 You can configure N+1 hot spare, which consists of several working devices and a hot spare device. Under normal operation, the working devices handle all operational workloads while the hot spare device remains in standby mode, continuously synchronizing data and monitoring the status of the working devices. In the event of a failure in any working device, the hot spare device automatically detects the fault and takes over the operations, ensuring uninterrupted service.

Click **System Configuration** → **N+1 Hot Spare**.

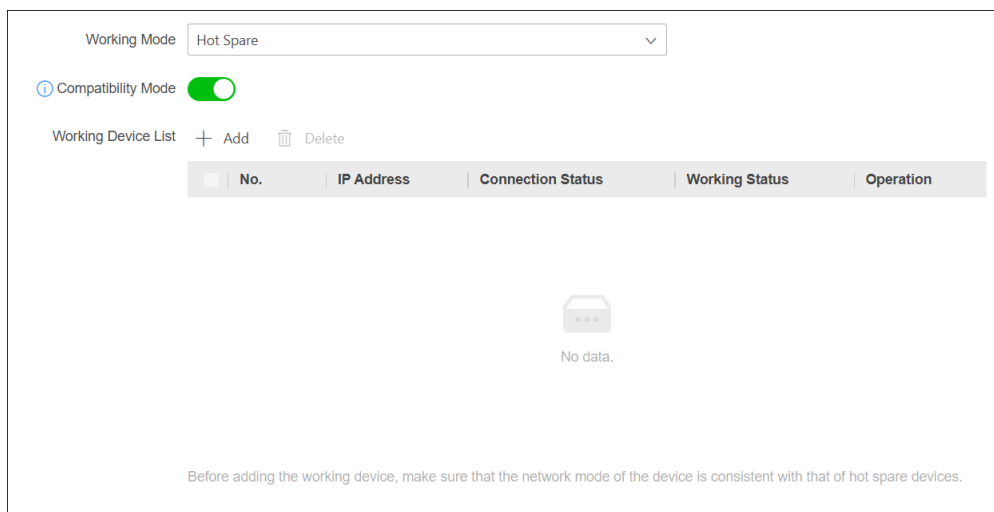


Note

The working mode is **Working Device** by default.

Set the working mode as **Hot Spare**.

Step 2



Set Working Mode As Hot Spare

(Optional) Enable/disable **Compatibility Mode**.

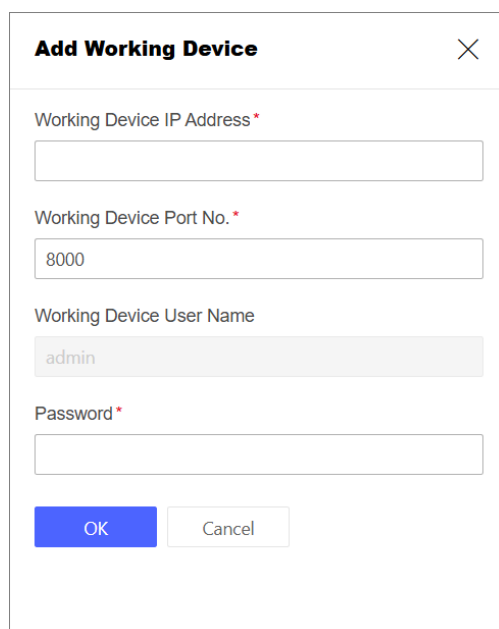
Figure 9-12

Step 3  **Note**

The switch is enabled by default. Disable it if the device is accessed to HikCentral Professional V3.0.0 or lower.

Step 4 Click **Add** to enter the adding working device panel.

Figure 9-13



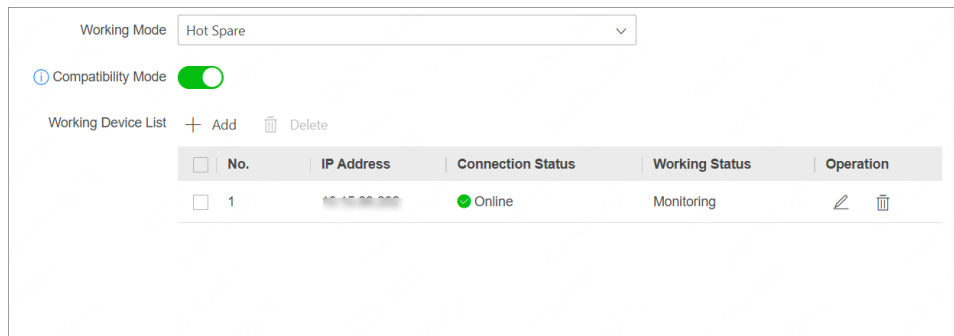
Add Working Device

Enter the working device's parameters such as IP address and port No.

Click **OK** to add the device.

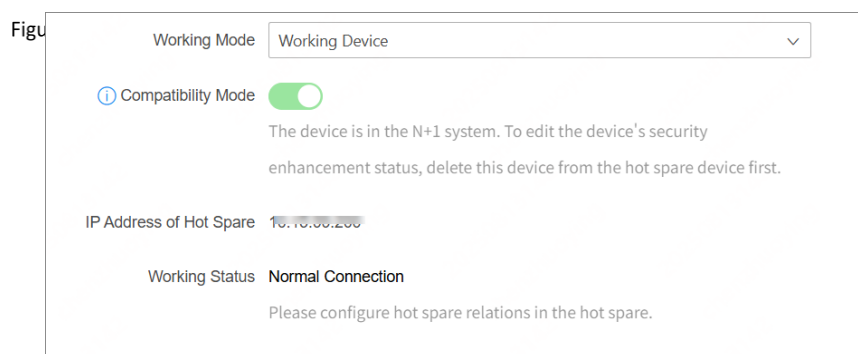
Step 5

Step 6



Page After Adding Working Device

What to do next: You can switch the working mode to **Working Device** and check its linked hot spare device.



Figure

Figure 9-15

Working Device Page



Note

A device restart will be triggered in conditions of working mode switch.

Chapter 10 Security

You can configure security parameters, including firewall, MAC address filtering, TLS, etc.

Firewall

You can configure firewall rules based on IP address and protocol type.

Click **Security** → **Security** → **Firewall**.

10.1 Enable firewall.

Click **Add**.

Step 1

Configure firewall rules.

Step 2

Step 3

Click **Confirm** to finish adding.

Step 4

Step 5

Add

IP *

Port No. *

Protocol

☒ TCP

☐ UDP

Strategy

DROP

Confirm Cancel

10.2

Add Firewall Rules

MAC Address Filtering

You can implement MAC address filtering to allow/deny access requests.

Click **Security** → **Security** → **MAC Address Filtering**.

Step 1

Enable ☐

MAC Address Filtering Type ☒ Blocklist ☐ Allowlist

List Table

No.	MAC Address	Operation
No data.		

MAC Address Filtering

Toggle **Enable**, and then select MAC address filtering type.

Step 2

- **Blocklist:** All the MAC addresses in this list will be blocked.
- **Allowlist:** Only the MAC addresses that are in this list will be allowed to access to the system.

Step 3

Click **Add**, and then enter the MAC address.

Step 4

After adding, click **Save** to save the settings.

10.3

Security Service

Go to **Security** → **Security** → **Security Service**.

- **Picture Download Security Authentication:** This involves token-based validation to ensure only authorized users can access and download recorded pictures.
- **Picture URL Digest Authentication:** When this function is enabled, each request to access a picture via a URL must include a unique digest.
- **Serial Port Authentication Service:** When this function is enabled, users must first enter an authentication command via the serial port to access serial port printing. Re-authentication is required every 2 hours after successful verification.
- **Service Close Time:** Sets a time limit for deactivating the Serial Port Authentication Service. Upon reaching the set deadline, the service will automatically reactivate.
- **Notification for Secure Login:** When this function is enabled, successful logins following failed attempts (due to incorrect credentials) will display a notification about the previous login failure.
- **SDK Protocol Authentication Mode:** This defines the authentication method used by third-party applications or systems interacting with the device via its Software Development Kit (SDK).

TLS

TLS can be configured for authentication of HTTP(s).

Go to **Security** → **Security** → **TLS**.

Before configuring, you need to disable HTTP(s) function.

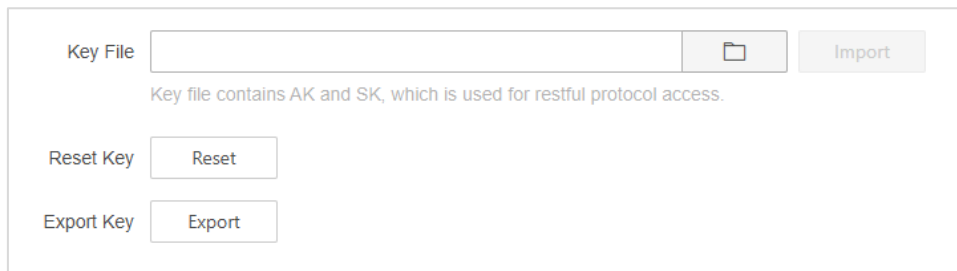
10.4 Note

Full-link TLS encryption significantly impacts device performance for video streams; therefore, total bandwidth for encrypted streams via TLS must be restricted. When device transport-layer encryption is enabled without array activation, the encrypted stream bandwidth via TLS is limited to 128 Mbps; when enabled with array activation, it is limited to 64 Mbps.

Central Storage Key

You can configure the key for restful protocol.

10.5 Go to **Security** → **Security** → **Central Storage Key**.



The image shows a web-based configuration interface for the Central Storage Key. It features a 'Key File' section with a text input field, a folder icon button, and an 'Import' button. Below this is a descriptive text: 'Key file contains AK and SK, which is used for restful protocol access.' There are also two rows of buttons: 'Reset Key' with a 'Reset' button, and 'Export Key' with an 'Export' button.

Central Storage Key



See Far, Go Further