Network Video Recorder

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 pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

- This device may not cause harmful interference.
- 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, 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: ***http://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: ***http://www.recyclethis.info*** .

Safety Instruction

- 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.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- For the device with the sign ϟ indicating hazardous live, the external wiring connected to the terminals requires installation by an instructed person.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- 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.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Do not ingest battery. Chemical Burn Hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- Use only power supplies same with the original model, or LPS power supplies with the same voltage and electric current.

Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- [+] identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- If the device has been powered off or placed for a long time, its coin/button cell battery may run out power.
- When the coin/button cell battery runs out power, the system time would be incorrect, please contact the after-sales service to replace the battery.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only. The current for the connected device shall be not more than 0.1 A.
- The serial port of the device is used for debugging only.
- If the power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.
- If a power adapter is provided in the device package, use the provided adapter only.

- For the device with sticker or

, pay attention to the following cautions: CAUTION: Hot parts! Do not touch. Burned fingers when handling the parts. Wait one-half hour after switching off before handling the parts.
- If the device needs to be installed on the wall or ceiling,
  1. Install the device according to the instructions in this manual.
  2. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Under high working temperature (40 °C (104 °F) to 55 °C (131 °F)), the power of some power adapters may decrease.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

Content Convention

In order to simplify description, please read the following conventions.

- Recorder or device mainly refers to video recorder.
- IP device mainly refers to network camera (IP camera), IP dome (speed dome), DVS (Digital Video Server), or NVS (Network Video Server).
- Channel mainly refers to the video channel in video recorder.

Symbol Conventions

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

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

Indicator and Interface Description

Front Panel Indicator Description

The indicators at the front panel indicates different working status of your device.

Table 1-1 Common Indicator Description

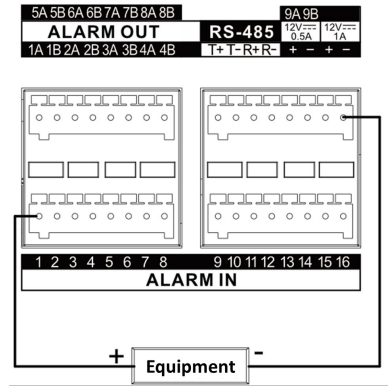
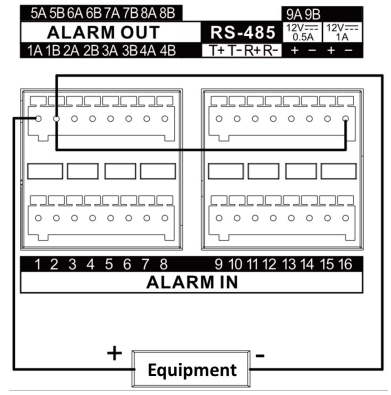
Indicator	Description
⏻	The indicator turns on when device is powered up.
🛢	The indicator flashes when data is being read from or written to HDD.
🖧	The indicator flashes when network connection is functioning properly.

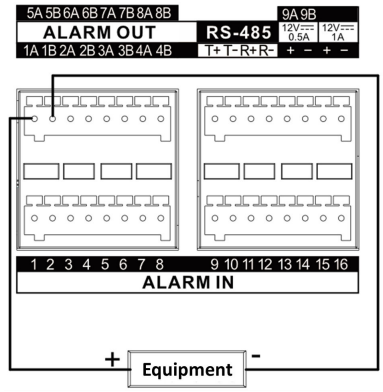
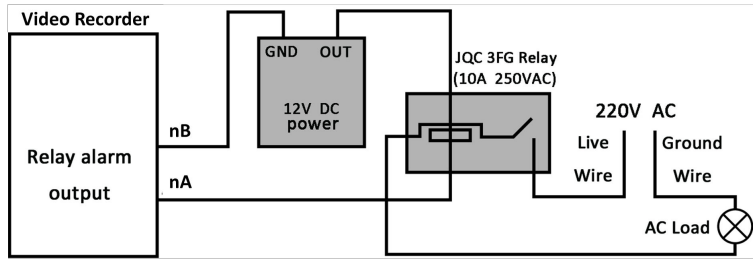
Interface Description

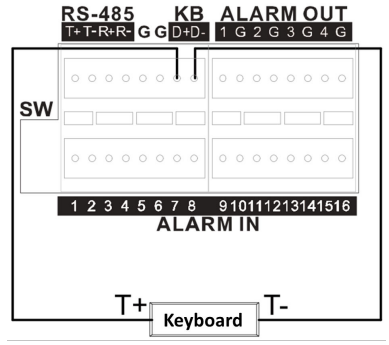
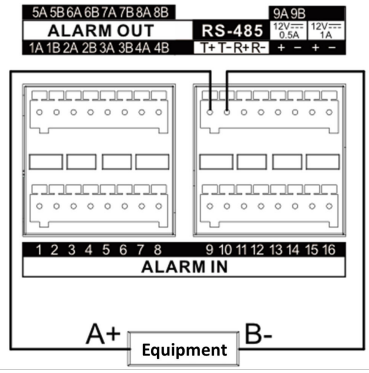
The panel interfaces vary with different models. Refer to the following table for common interface description.

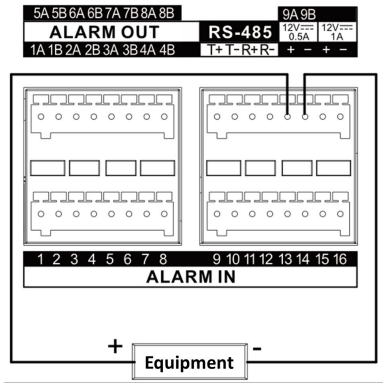
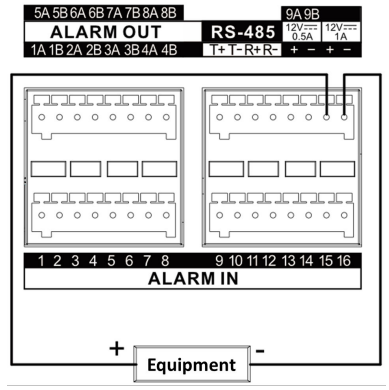
Table 1-2 Common Indicator Description

Item	Description
VIDEO IN	BNC interface for Turbo HD and analog video input.
VIDEO OUT	BNC connector for video output.
AUDIO IN	RCA connector for audio input.
AUDIO OUT	RCA connector for audio output.
LINE IN	RCA connector for two-way audio input.
USB	Universal Serial Bus (USB) interface for additional device.
VGA	DB15 connector for local video output and menu display.
HDMI	HDMI interface for video output.
RS-485	RS-485 serial interface for pan/tilt unit, speed dome, etc.
RS-232	RS-232 interface for parameter configuration, or transparent channel.
LAN	RJ-45 self-adaptive Ethernet interface.
eSATA	Storage and expansion interface for record or backup.
GND	Ground.

Item	Description
Power Switch	Switch for turning on/off the device.
Power Supply	100 to 240 VAC, 48 VDC, or 12 VDC power supply.
USIM Card	UIM/SIM card slot.
Y	SMA antenna interface.
ALARM IN	The alarm input receives alarm input signal. The equipment positive terminal (+) should connect to a number, and the equipment negative terminal (-) should connect to “-“ or “G”. Use the following diagram as a connection example for alarm input. 
ALARM OUT	The alarm output sends out alarm signal. When an equipment uses DC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should both connect to the corresponding number with “B”, and then connect to “-“ or “G”. Use the following diagram as an alarm output connection example for DC equipment. 

Item	Description
	When an equipment uses AC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should connect to the corresponding number with “B”. Use the following diagram as an alarm output connection example for AC equipment.  **Note** For the reason that the AC load voltage could be high, please use an external relay for safety. Use the following diagram for reference.  Note: n represents a number in nA or nB, n can be 1 to 9.
KB	KB represents keyboard. Connect “D+” and “D-” to “T+” and “T-” respectively. Use the following diagram for reference.

Item	Description
	
RS-485	RS-485 is an electrical specification of a two-wire, half-duplex, multipoint serial connection. Connect “T+” and “T-” to “A+” and “B-” respectively. Use the following diagram for reference. 
Ctrl 12V/ 12V 0.5A	Controllable 12 VDC and 0.5/1 A power output for external alarm device. The power will be turned on when the corresponding alarm output is triggered. Use the following diagram for reference.

Item	Description
	
DC 12V/ 12V⎓ 1A	It provides 12 VDC and 1 A power output. Use the following diagram for reference. 

HDD Installation

If your device does not support HDD hot swapping, disconnect the power from the device before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

Scan the QR code below to view HDD installation videos.

Figure 1-1 HDD Installation

Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

1. Unfasten screws on the back, and push the cover backwards to remove the cover.

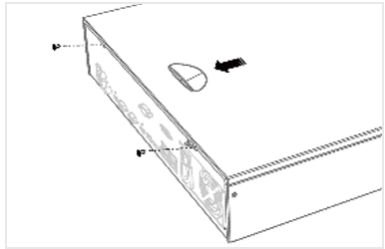


Figure 1-2 Remove Cover

2. Fix the HDD on the bracket with screws.

Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

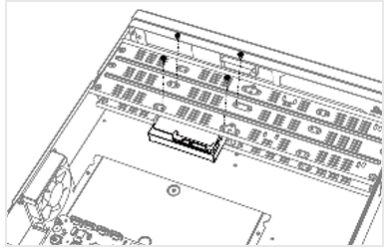


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

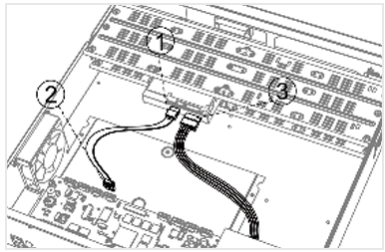


Figure 1-4 Connect Cable

Note

You can repeat the steps above to install other HDDs.

4. Reinstall the device cover and fasten screws.

Front Panel Plug-Pull Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

Steps

1. Fix mounting ears to HDD with screws.

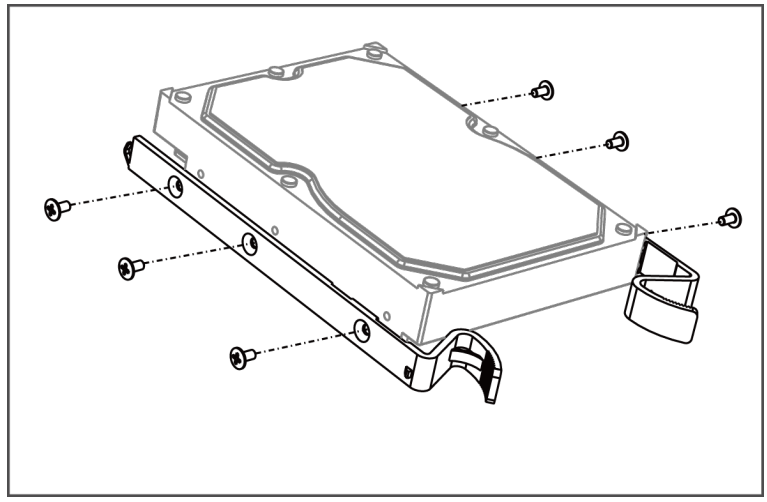


Figure 1-5 Fix Mounting Ears to HDD

2. Unlock the front panel with the attached key, and press the buttons on both sides of the front panel to open it.

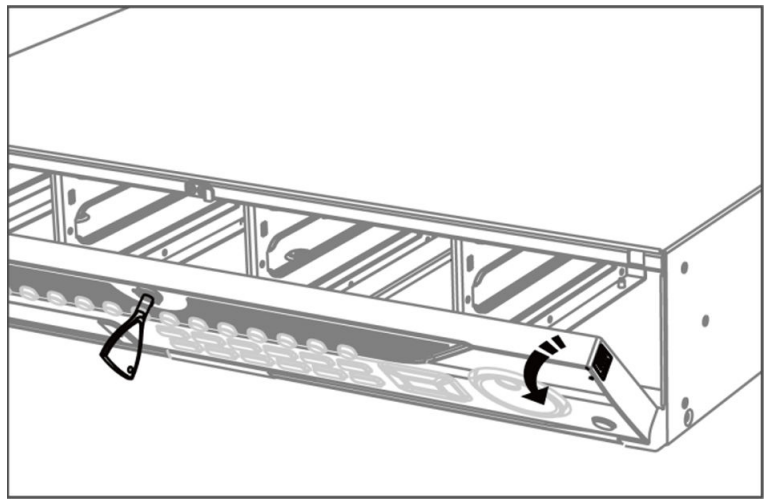


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

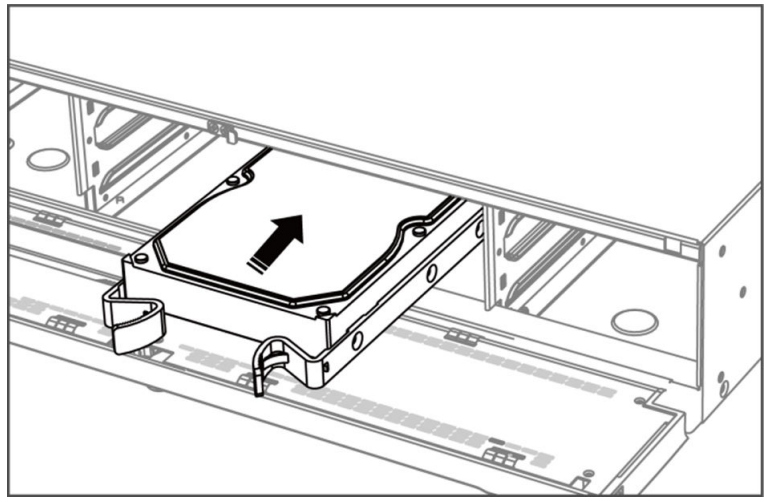


Figure 1-7 Insert HDD

4. **Optional:** Repeat the steps above to install other HDDs.
5. Close the front panel and lock it with key.

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

1. Unlock the front panel with panel key.
2. Pull the front panel out of the device and make it a little above the left handle.

   Note

   The angle between the front panel and the device must be within 10°.
3. Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
4. Fix the hard disk in the HDD case.
   1) Place a HDD in the case. The SATA interface must face the case bottom.
   2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
   3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

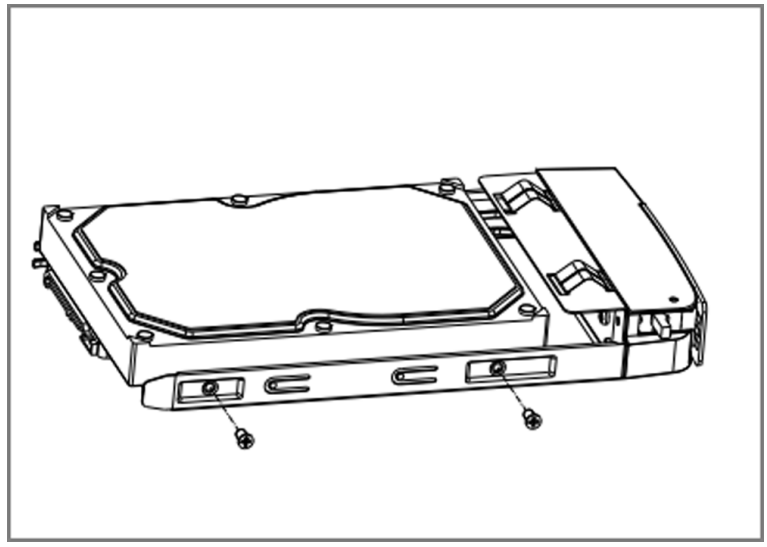


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

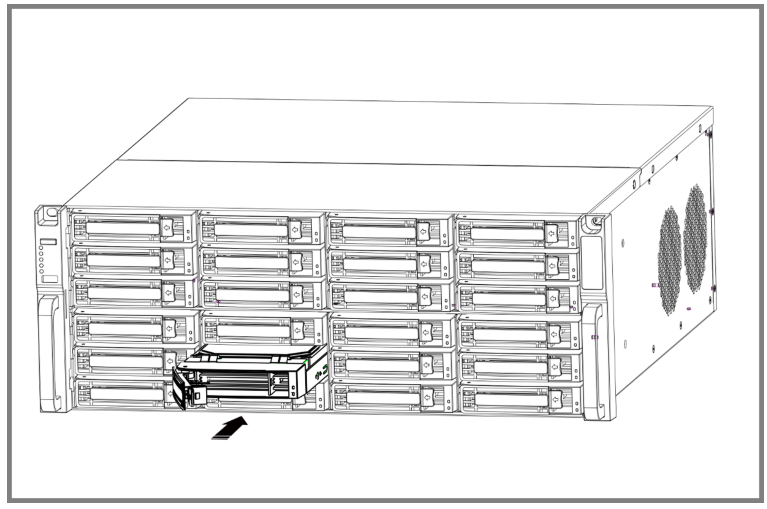


Figure 1-9 Push HDD Case into Slot

6. Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
7. Close the front panel, and lock it with the panel key.

Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

1. Remove the cover from device by unfastening the screws on panels.

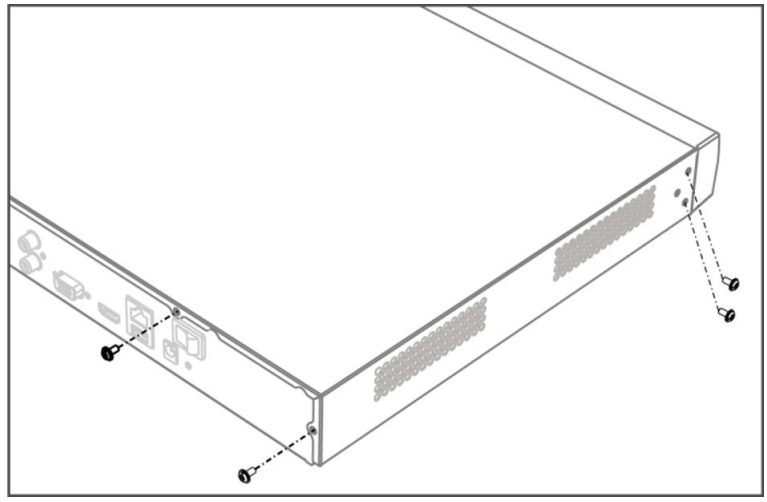


Figure 1-10 Remove Cover

2. Connect the data cable and power cable.

1) Connect one end of data cable to the device motherboard.
2) Connect the other end of data cable to HDD.
3) Connect one end of power cable to HDD.
4) Connect the other end of power cable to the device motherboard.

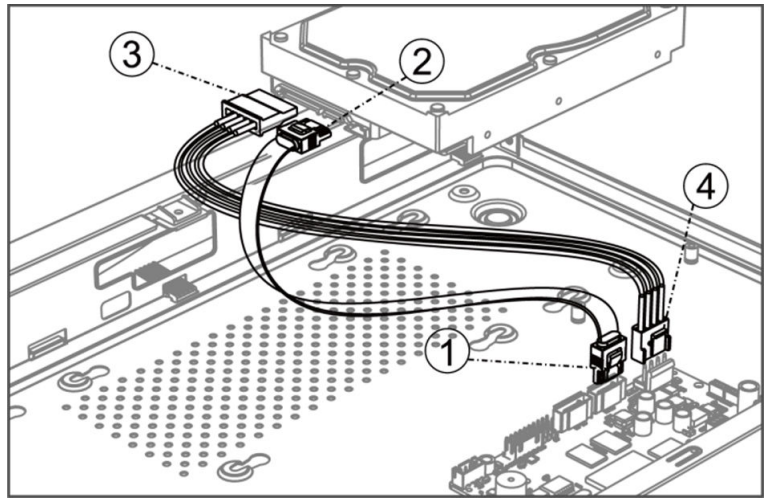


Figure 1-11 Connect Cables

3. Set the device up, match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws.

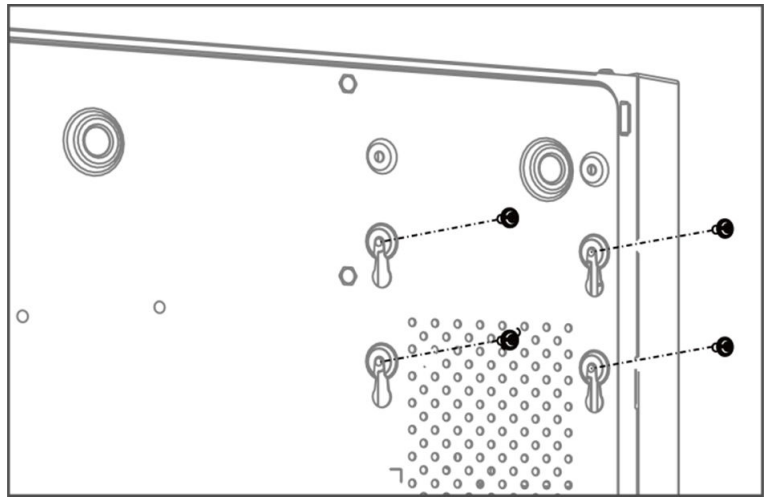


Figure 1-12 Fix HDD to Device Bottom

4. **Optional:** Repeat the steps above to install other HDDs.
5. Reinstall the device cover and fasten screws.

Coin/Button Cell Battery Replacement

The coin/button cell battery should be replaced when the device has been powered off or placed for a long time, and the system time is incorrect.

Before You Start
Power off your device.

Steps
1. Remove the device chassis cover.
2. Find the coin/button cell battery on motherboard.
3. Put the thumb outside the battery slot, and use the index finger to push the positive contact spring outward gently. The battery will pop up automatically.

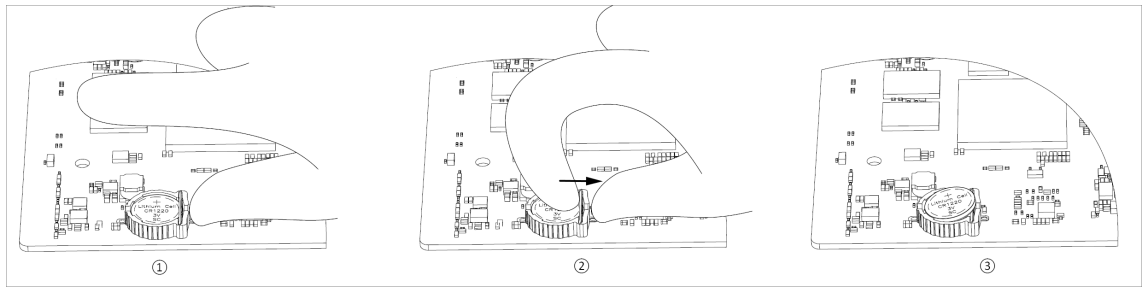


Figure 1-1 Remove Battery

Note
- You should wear anti-static gloves when removing the battery.
- If the spring is deformed due to excessive force when pushing outward, it needs to be adjusted back into its original position before inserting the battery.

4. Insert the battery diagonally towards the side with the plastic snap point in the battery slot, and then press the battery near the positive contact spring to snap it beneath the spring.

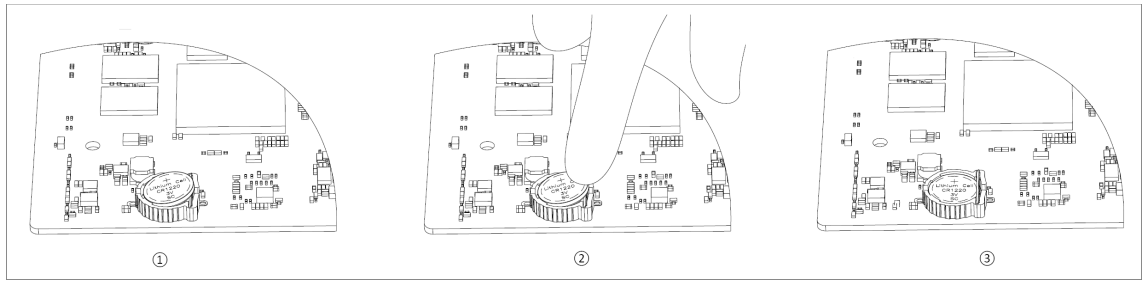


Figure 1-2 Replace Battery

Note

You should wear anti-static gloves when replacing the battery.

5. Reinstall the device chassis cover.

What to do next

If the system time is incorrect, please go to configure the time.

Contents

Chapter 1 Activate via Local Menu 1

Chapter 2 Log In to Your Device 3

Chapter 3 User Interface Introduce 4

Chapter 4 Network Settings 6

4.1 Network Parameter Settings 6

4.1.1 Configure TCP/IP 6

4.1.2 Configure DDNS 7

4.1.3 Configure PPPoE 8

4.1.4 Configure Multicast 9

4.1.5 Enable SVC Network Transmission Frame Extraction 9

4.2 Platform Access Settings 9

4.2.1 Configure Hik-Connect 9

4.2.2 Configure OTAP 11

4.2.3 Configure ISUP 12

4.2.4 Configure SDK Service 13

4.2.5 Enable ISAPI 14

4.2.6 Configure ONVIF 14

4.2.7 Configure Log Server 15

4.3 Network Service Settings 16

4.3.1 Configure HTTP(S) 16

4.3.2 Configure RTSP 17

4.3.3 Configure WebSocket(s) 18

4.3.4 Configure Port Mapping (NAT) 18

4.3.5 Configure IoT 20

Chapter 5 User Management 21

Chapter 6 Device Access 22

6.1 Access Video Device 22
6.1.1 Add Automatically Searched Online Network Camera 22
6.1.2 Add Network Camera Manually 23
6.1.3 Add Network Camera through PoE 24
6.1.4 Add Solar-Powered Camera through OTAP Protocol 24
6.1.5 Add Network Camera via Custom Protocol 25
6.1.6 Add Network Camera through Camera Configuration File 26
6.2 Add Access Control Device 26
6.3 Add Security Control Panel 27
6.4 Add Audio Device 27
6.5 Add POS Device 27
6.6 Channel Management 29
Chapter 7 Device Grouping 30
Chapter 8 Video or Audio Device Settings 31
8.1 Enable H.265 Stream Access 31
8.2 Configure Display Settings 31
8.3 Configure Video Parameters 32
8.4 Configure Privacy Mask 32
8.5 Configure Privacy Protection 33
8.6 Configure Audio Parameter 35
8.7 Configure OTAP Service 35
8.8 Batch Configuration 36
8.9 Configure PoE (Power over Ethernet) Interface 37
Chapter 9 Storage Management 38
9.1 Manage HDD 38
9.2 RAID Configuration 38
9.2.1 Create Disk Array 39
9.2.2 Rebuild Array 41

9.2.3 Delete Array 41
9.2.4 View Firmware Info 41
9.3 Configure Storage Mode 42
9.4 Configure Auto Backup 42
9.5 Configure Other Storage Parameters 43
9.6 Mange USB Flash Drive 43
Chapter 10 Schedule Configuration 45
10.1 Configure Schedule Template 45
10.2 Configure Recording Schedule 47
10.3 Configure Picture Capture Schedule 49
10.4 Configure Audio Recording 51
Chapter 11 Live View 52
11.1 Configure Live View Layout 52
11.2 GUI Introduction 52
11.3 PTZ Control 54
Chapter 12 Playback 55
12.1 GUI Introduction 55
12.2 Normal Playback 56
12.3 Event Playback 57
12.4 Slice Playback 58
12.5 Sub-Period Playback 58
Chapter 13 Event Center 60
13.1 Event Settings 60
13.1.1 Basic/Generic Event 60
13.1.2 Perimeter Protection 62
13.1.3 Abnormal Behavior Event 73
13.1.4 Target Event 76
13.1.5 Thermal Camera Detection 78

13.1.6 Alarm Input Event 79
13.1.7 Audio Analysis Event 81
13.2 Linkage Configuration 83
13.3 Disarming Configuration 85
13.4 Batch Configuration 86
13.5 Event Search 87
13.6 View Alarms 88
Chapter 14 Search and Backup 89
Chapter 15 AcuSearch 91
Chapter 16 Smart Settings 93
16.1 Algorithm Management 93
16.2 Engine Status 93
16.3 Task Plan Management 93
16.4 List library Management 94
16.4.1 Add a List Library 94
16.4.2 Upload Face Pictures to the Library 94
16.5 Self-Learning Settings 95
16.5.1 Self-Learning Task Management 95
16.5.2 Model Management 96
16.5.3 Smart Status 96
Chapter 17 Application Center 97
17.1 Human and Vehicle Detection 97
17.2 Person Check-In 97
17.2.1 Add Check-In Task 98
17.2.2 Search Check-In Records 99
17.3 Statistic Report 99
Chapter 18 System Parameter Settings 101
Chapter 19 Hot Spare Device Backup 103

19.1 Set Working Device 103
19.2 Set Hot Spare Device 103
Chapter 20 Configure Exception Event 105
Chapter 21 View System Info 107
Chapter 22 System Maintenance 108
22.1 Schedule Reboot 108
22.2 Upgrade Device 108
22.3 Backup and Restore 108
22.4 Log Info 109
22.5 Configure Log Server 109
22.6 Maintenance Tools 109
22.7 Soft Power Off Configuration 110
Chapter 23 Security Management 112
23.1 Address Filter 112
23.2 Stream Encryption 112
23.3 Select TLS Version 112
Chapter 24 Appendix 113
24.1 List of Applicable Power Adapter 113
24.2 Glossary 114
24.3 Frequently Asked Questions 115
24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view? 115
24.3.2 Why is the video recorder notifying risky password after a network camera is added? 116
24.3.3 Why is the video recorder notifying the stream type is not supported? 116
24.3.4 How to confirm the video recorder is using H.265 to record video? 116
24.3.5 Why is the video recorder notifying IP conflict? 116
24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras? 117

24.3.7 Why is the device not able to control PTZ camera via coaxitron? 117
24.3.8 Why does the PTZ seem unresponsive via RS-485? 117
24.3.9 Why is the video sound quality not good? 117
24.4 Notification for Corrosive Gas 118

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

1. Power on your device.
2. Set the region or DST (Daylight Saving Time) parameters.
3. Select a system language.
4. Enter the admin password twice.

Caution

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of 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 change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

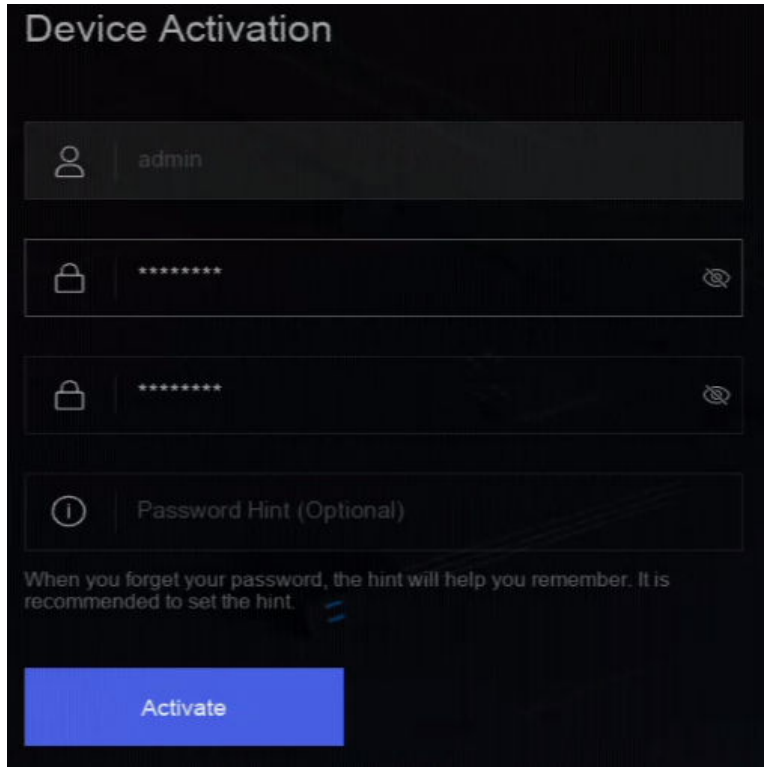


Figure 1-1 Activate via Local Menu

5. **Optional:** Enter a password hint. It will help you remember your password when you forget.
6. Click **Activate**.

Note

After the device is activated, you should properly keep the password.

7. **Optional:** Draw an unlock pattern.
8. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start
Ensure your device is activated.

Steps
1. Power on your device.
2. Right click to display the shortcut menu.
3. Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

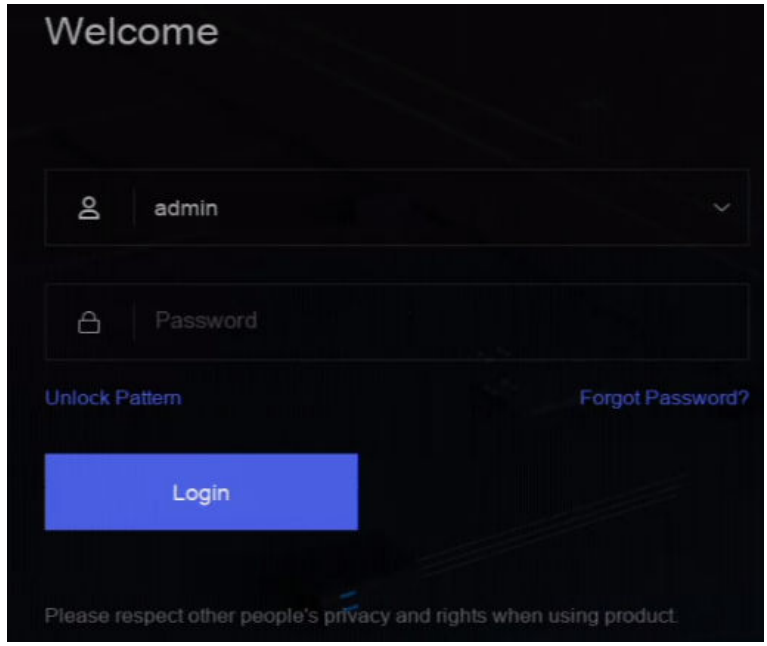


Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

Note
- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.

Figure 3-1 Main Function Page

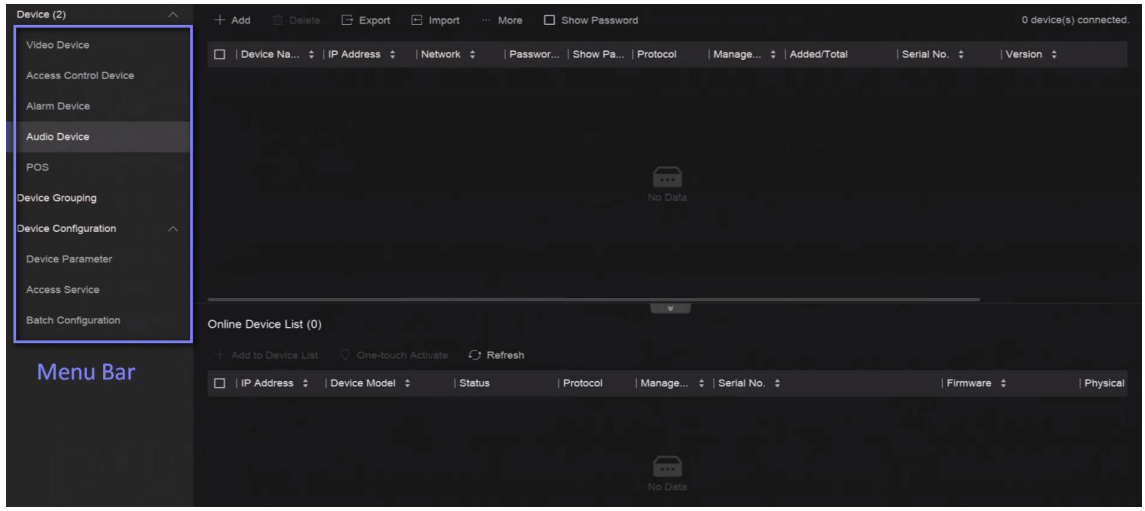


Figure 3-2 Menu Bar Example

Figure 3-3 Human and Vehicle Detection Example of Application Center

Table 3-1 Interface Introduction

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab. Icon introduction ： • : Main menu. • : Event center. Event alarms can be searched and viewed. • : The download progress of each download task can be viewed here. • : Shut down, log out, or reboot your device.
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here. **Note** For applications in **Application Center**, you can click , or right click to display the menu bar.

Chapter 4 Network Settings

Network parameters, platform access settings, and network services are configurable.

4.1 Network Parameter Settings

You shall configure network parameters before using functions that require network access.

4.1.1 Configure TCP/IP

TCP/IP must be properly configured before you operate video recorder over network or access network devices.

Steps

1. Go to **System → System Settings → Network → Network → TCP/IP** .

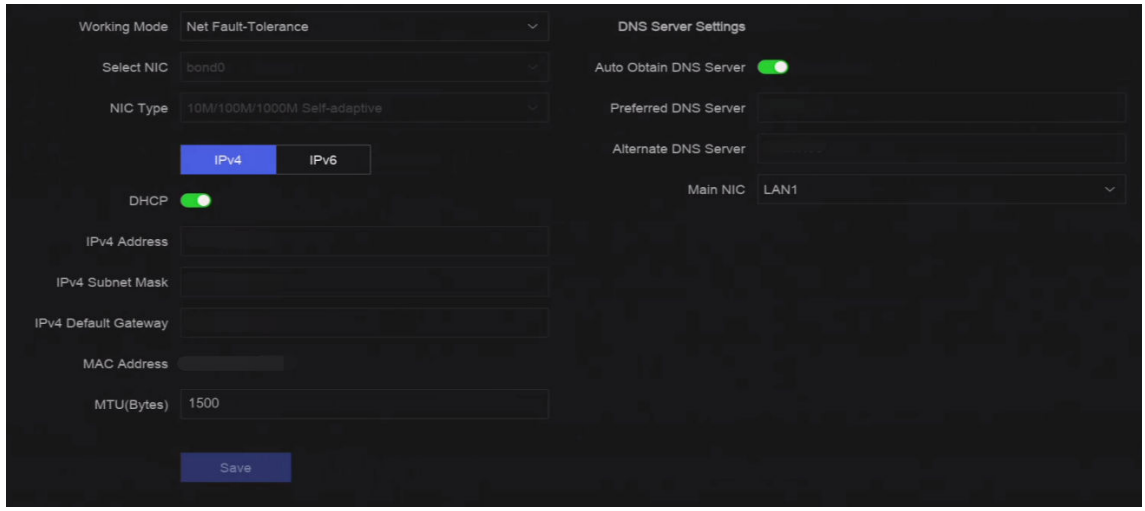


Figure 4-1 TCP/IP Settings

2. Set **Working Mode** and **Select NIC**.

   Multi-address

   The parameters of the two NIC cards can be configured independently. You can select **LAN1** or **LAN2** in the NIC type field for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet and the data will be forwarded through the default route.

   Net-fault Tolerance

The two NIC cards use the same IP address, and you can set **Main NIC** to **LAN1** or **LAN2**. By this way, in case of one NIC card failure, the video recorder will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.

Note

Working mode is only available for certain models.

3. Configure network parameters.
   - **IPv4**

     DHCP

     If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

     MTU

     The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

     Auto Obtain DNS Server

     If **DHCP** is enabled. You can check **Auto Obtain DNS Server** to obtain **Preferred DNS Server** and **Alternate DNS Server**.
   - **IPv6**

     Router Advertisement

     If the router in the network supports IPv6, it is recommended to use this mode as default.

     Auto

     If there is a DHCPv6 device in the network, it is recommended to use this mode

     Manual Configuration

     You shall use this mode if you are going to manually enter IPv6 parameters.
4. Click **Save**.

4.1.2 Configure DDNS

Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to **System → System Settings → Network → Network → DDNS** .

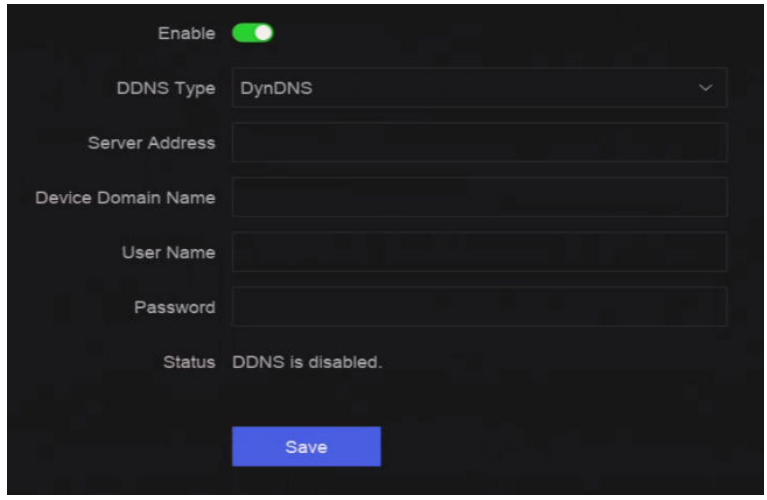


Figure 4-2 DDNS

2. Turn on **Enable**.
3. Select a DDNS type.
4. Set parameters, including service address, domain name, etc.
5. Click **Save**.

4.1.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPoE service.

Steps

1. Go to **System → System Settings → Network → Network → PPPoE** .

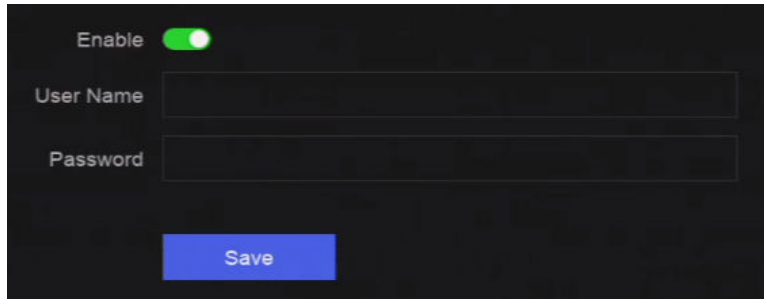


Figure 4-3 PPPoE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

Go to **System → System Maintenance → Running Info → Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

1. Go to **System → System Settings → Network → Network → Other** .
2. Set **Multicast** parameters.

Note

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.

3. Click **Save**.

4.1.5 Enable SVC Network Transmission Frame Extraction

Enabling SVC network transmission frame extraction allows for efficient transmission of video streams over networks with varying bandwidth conditions. It can save network bandwidth by reducing frame rates during live view and playback.

Note

Make sure you have enabled SVC Network Transmission Frame Extraction on the Web page of the related camera.

Go to **System → System Settings → Network → Network → Other** to enable the function.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **System → System Settings → Network → Hik-Connect**.

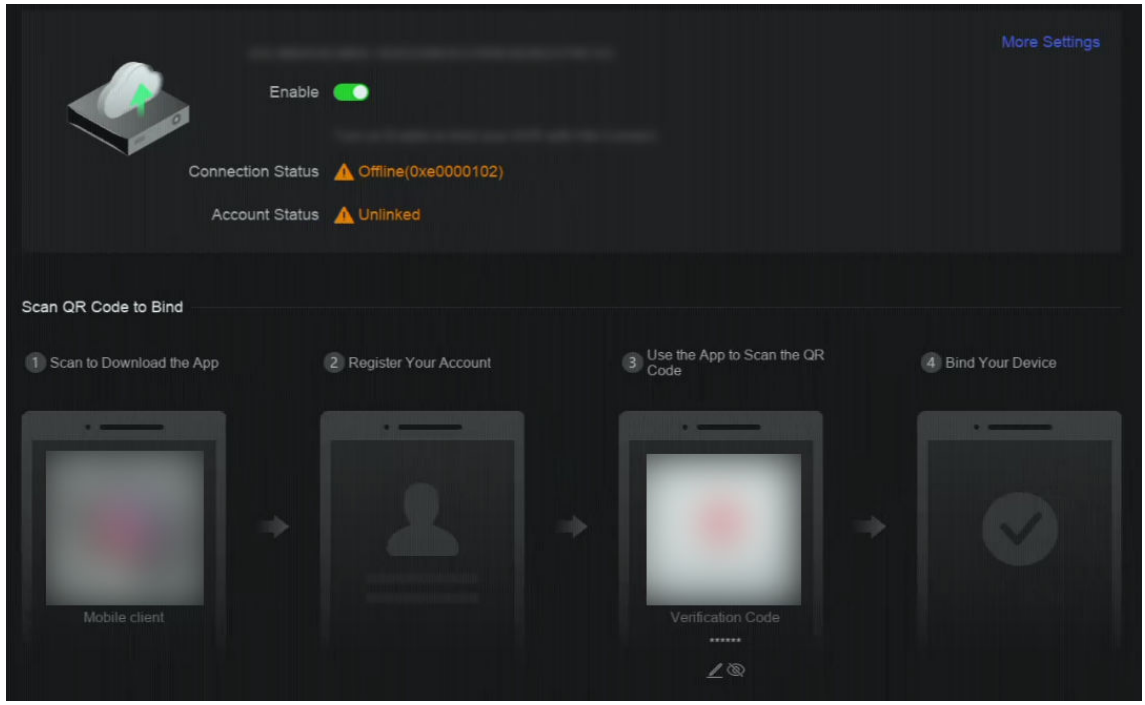


Figure 4-4 Hik-Connect

2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Download Hik-Connect app.
   - Use a smart phone to scan the QR code, and download Hik-Connect app.
   - Download the app from ***https://appstore.hikvision.com*** .

Figure 4-5 Download Hik-Connect

5. Register an account at the app.
6. **Optional:** Click **More Settings** to enable **Stream Encryption**, **Platform Time Sync**, and **Adaptive Bitrate Streaming**, or edit **Server IP Address**.

   Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

7. Click to set verification code.
8. Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

Result

- If your device is connected with Hik-Connect, **Connection Status** will be **Online**.
- If your device is bound with a Hik-Connect account, **Account Status** will be **Linked**.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

1. Go to **System → System Settings → Network → Platform Access → OTAP** .

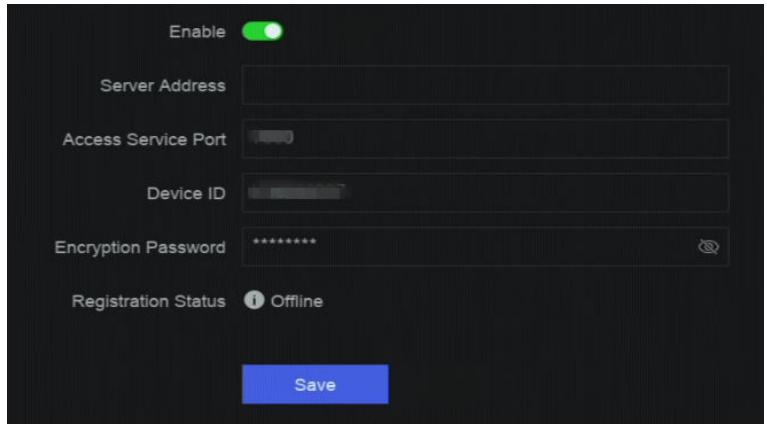


Figure 4-6 OTAP

2. Turn on **OTAP**.
3. Set the parameters.
4. Click **Save**.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ISUP** .

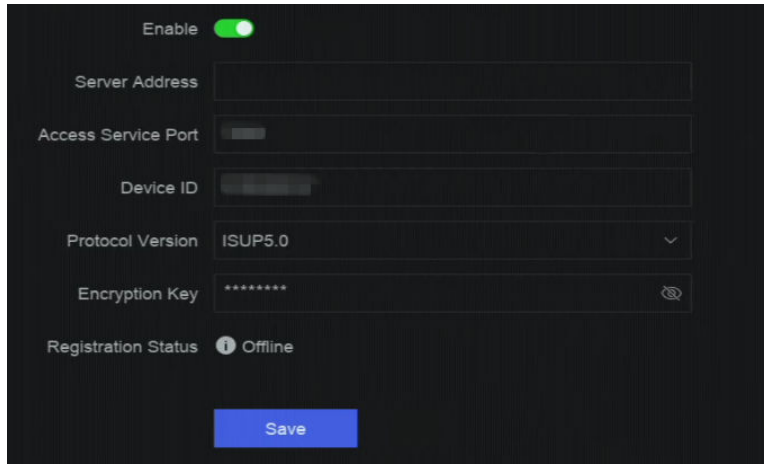


Figure 4-7 ISUP

2. Turn on **Enable**.

Note

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click **Save**.

You can see the registration status (online or offline) after the device is restarted.

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to **System → System Settings → Network → Platform Access → SDK**.

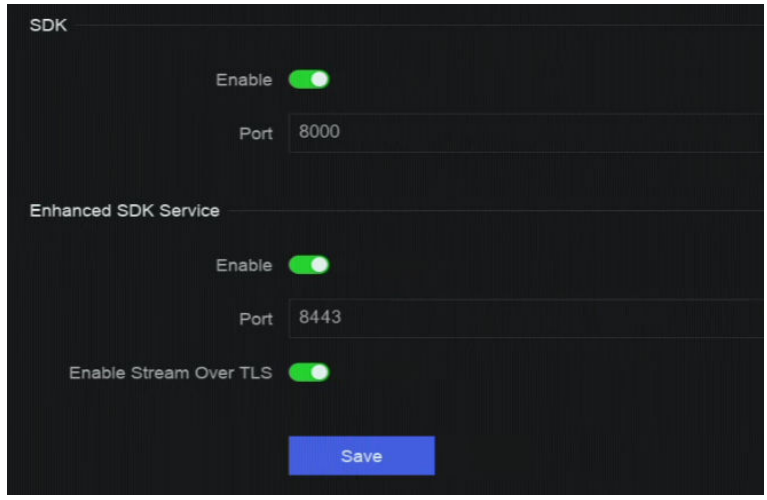


Figure 4-8 SDK Service

2. Configure **SDK** and **Enhanced SDK Service** according to your requirement.

Note

The port for **Enhanced SDK Service** is 8443 by default.

3. **Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
4. Click **Save**.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to **System → System Settings → Network → Platform Access → ISAPI** to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ONVIF** .

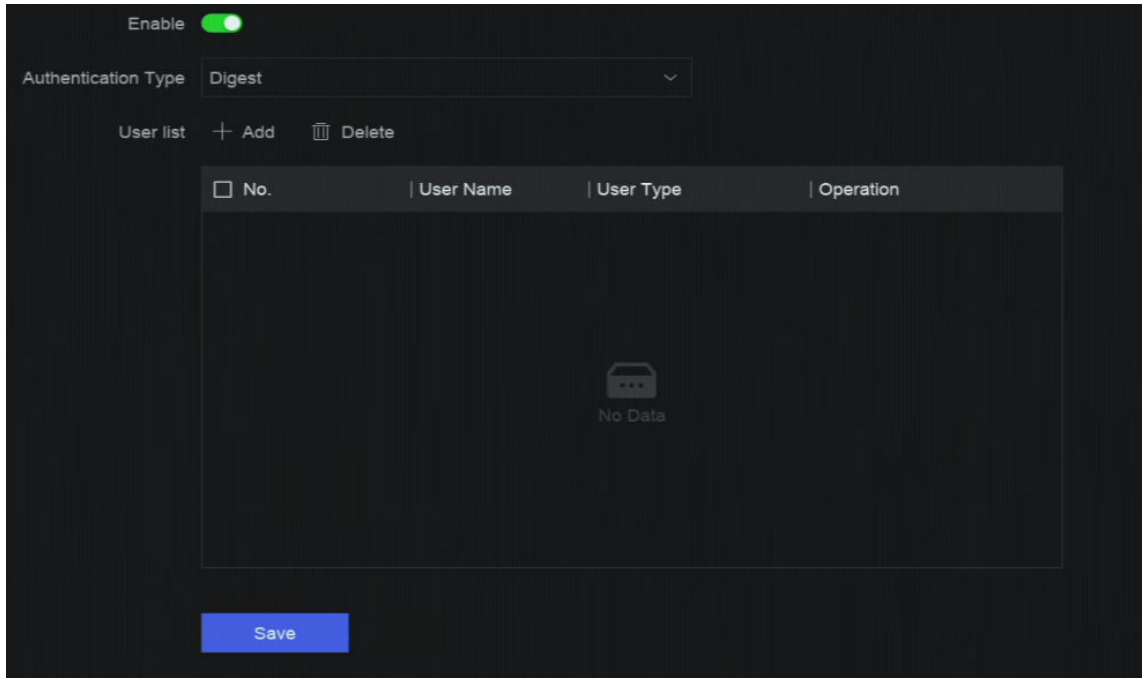


Figure 4-9 ONVIF

2. Turn on **Enable**.
3. Select an authentication type.
4. Click **Add** to add a user.
5. Set the user name and password.

Caution

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

6. Click **Save**.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to **System → System Settings → Network → Platform Access → Log Server**.

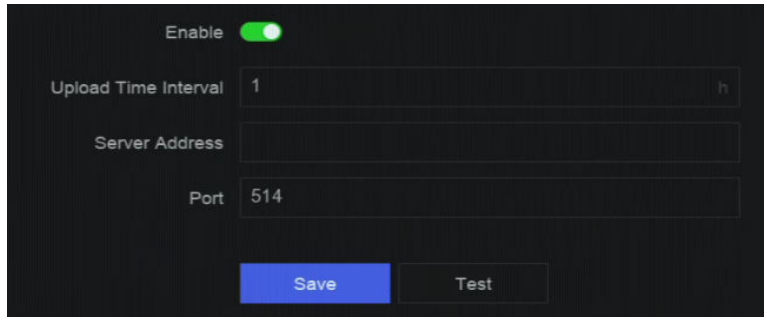


Figure 4-10 Log Server

2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. **Optional:** Click **Test** to check if parameters are valid.
5. Click **Save**.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

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

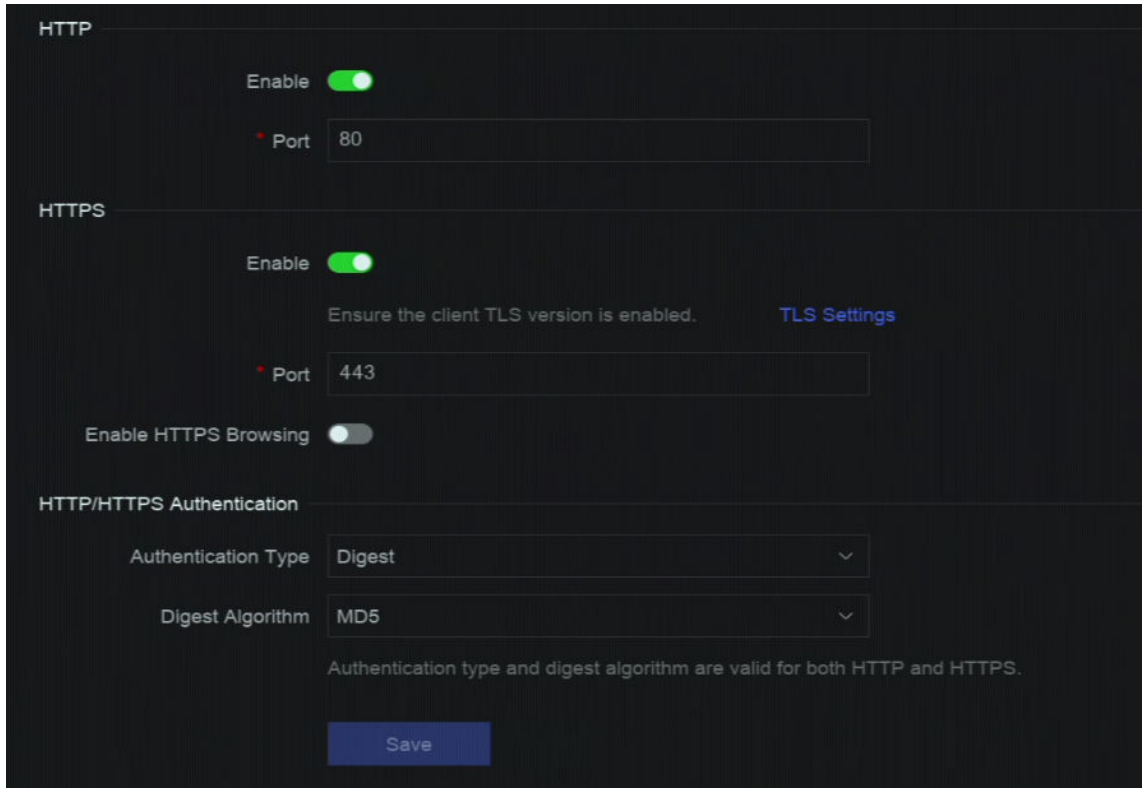


Figure 4-11 HTTP(S)

2. **Optional:** Turn on HTTP or HTTPS.
3. View or edit **Port** of HTTP or HTTPS.
4. Set **HTTP/HTTPS Authentication**.

   Authentication Type

   Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

   Digest Algorithm

   Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.
5. Click **Save**.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to **System → System Settings → Network → Network Service → RTSP** .

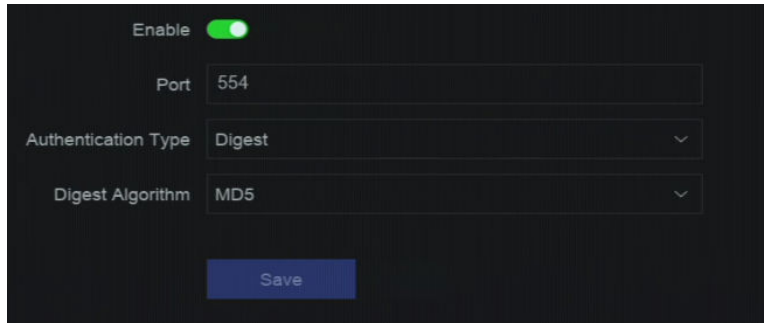


Figure 4-12 RTSP

2. Set parameters.

   Port

   The port is 554 by default.

   Authentication Type

   Two authentication types are selectable, if you select **Digest**, only the request with digest authentication can access the video stream by RTSP via the IP address. For security reasons, it is recommended to select **Digest** as the authentication type.

   RTSP Digest Algorithm

   RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click **Save**.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to **System → System Settings → Network → Network Service → WebSocket(s)** .
2. Turn on **Enable**.
3. Set **Port**.
4. Click **Save**.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ (Universal Plug and Play), and manual mapping. UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

1. Go to **System → System Settings → Network → Network Service → NAT** .

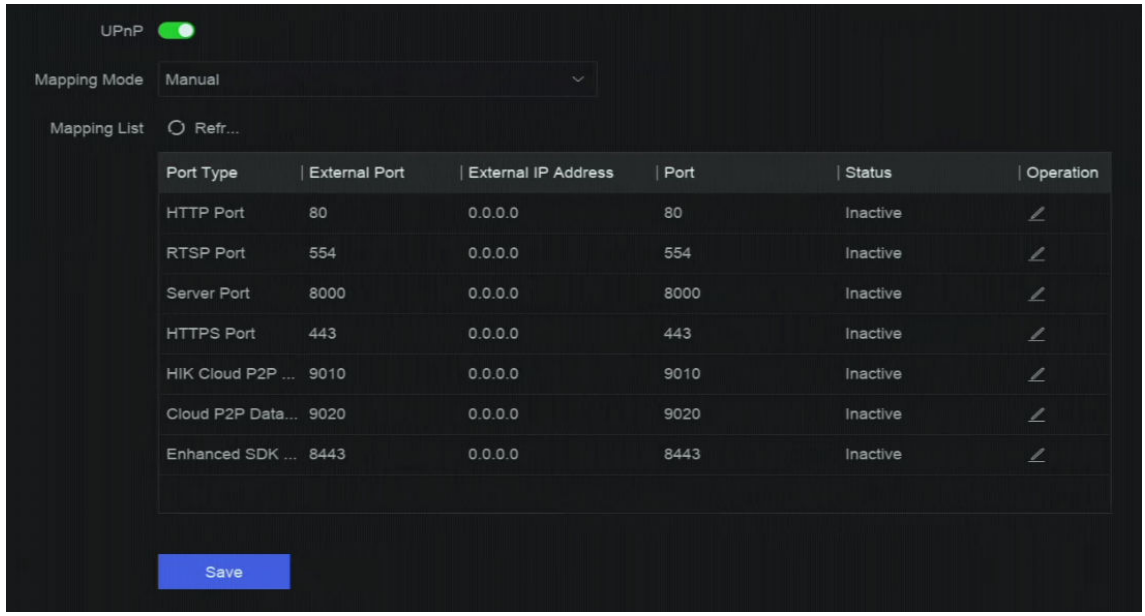


Figure 4-13 Port Mapping (NAT)

2. Turn on **Enable**.
3. Set **Mapping Mode**.

   Auto

   The port mapping items are read-only, and the external ports are set by the router automatically.

   Manual

   You can manually edit the external port.
4. If **Mapping Mode** is selected as **Manual**, click to edit corresponding ports.

Note

- The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.
- **External Port** indicates the internal port number for port mapping in the router.

5. Click **Save**.

What to do next

Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.

4.3.5 Configure IoT

You can configure the network port through which the NVR will receive alarms from a security control panel.

Go to **System → System Settings → Network → Network Service → IoT** to enable the function and configure the port number.

Note

The port number you configured here should be the same as the alarm sending port on the security control panel.

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to **System → System Settings → User Management** .

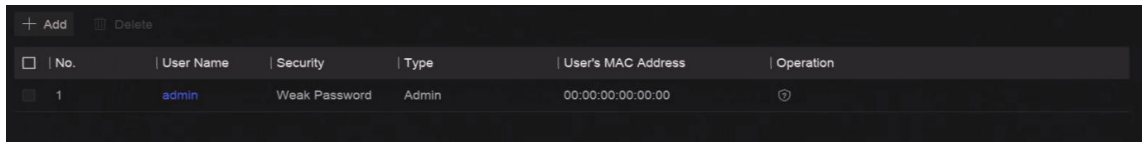


Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
	Set account security.
Add	Add a new guest or operator user.
	Delete the selected user.

Note

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to **System → Device Access → Device → Video Device → Online Device List** .
2. Select the device(s) from the list.

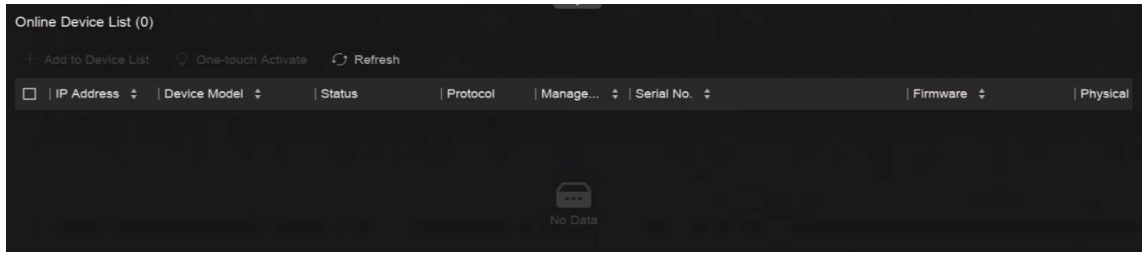


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click **Add to Device List**.

Note

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password. The default password can be configured in **More → Default Password Settings**.
- If the searched network cameras are not activated, the device will use a default password to activate and add inactive network cameras. The default password can be configured in **More → Default Password Settings**.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **System → Device Access → Device → Video Device** .

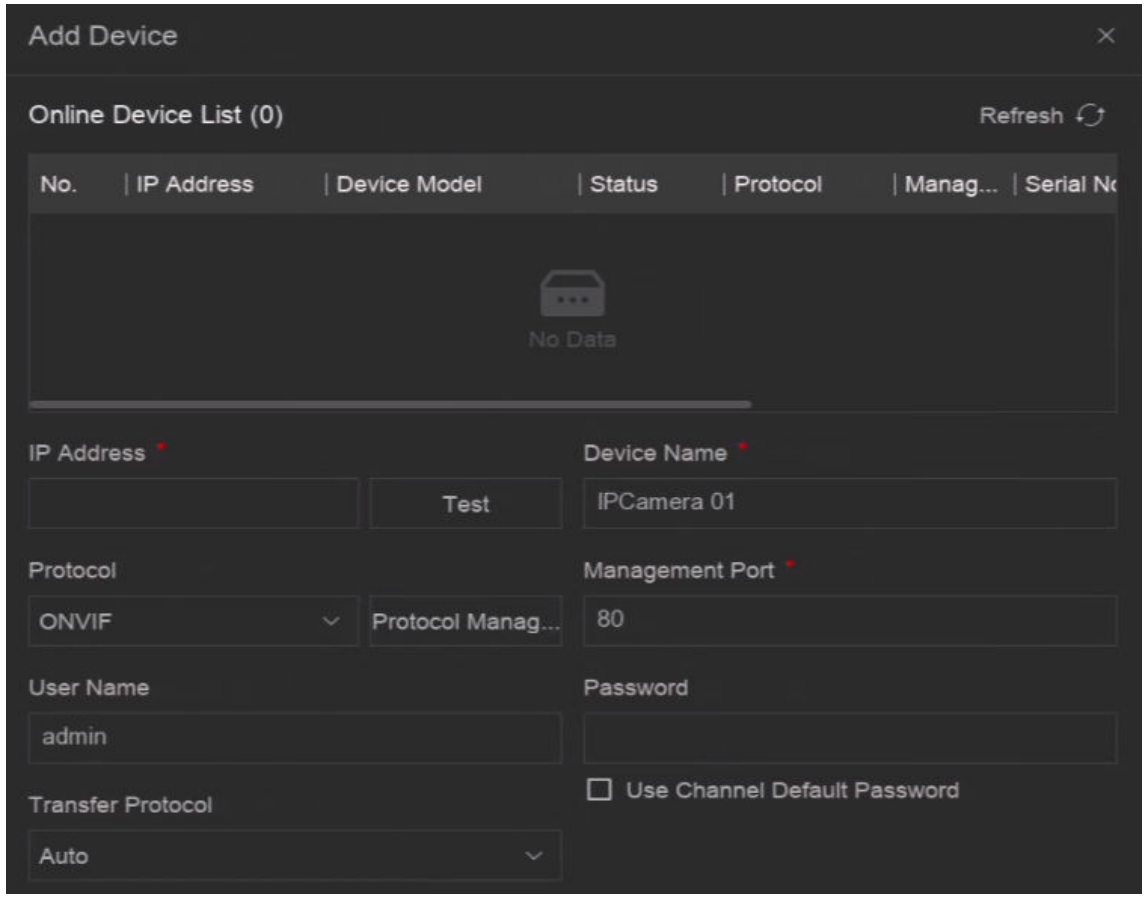


Figure 6-2 Add Network Camera Manually

2. Click **Add**.
3. Enter network camera parameters.

   Use Channel Default Password

   If it is enabled, the video recorder will add the camera by the set channel default password.

   More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

4. **Optional:** Click **Continue to Add** to add other network cameras.
5. Click **Add**.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to ***Configure PoE (Power over Ethernet) Interface*** for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start
Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.
Enter the context of your task here (optional).

Steps
1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.
2. Turn on **Enable**.
3. Set OTAP **Server Port** and **Encryption Key**.
4. **Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
5. Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.

   Note
   The solar-powered camera OTAP protocol parameters shall be the same as the device.
6. Add solar-powered camera(s) to your device.
   - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
   - Select solar-powered camera(s) from **Online Device List**, and click **Quick Add**.
7. Click **Add** in **System → Device Access → Device → Video Device**, select **Protocol** as **OTAP**, and click **Add**.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to ***Configure Recording Schedule*** .

6.1.5 Add Network Camera via Custom Protocol

For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

1. Go to **System → Device Access → Device → Video Device** .
2. Click **More → Custom Protocol Management** , or **Add → Protocol Management** .

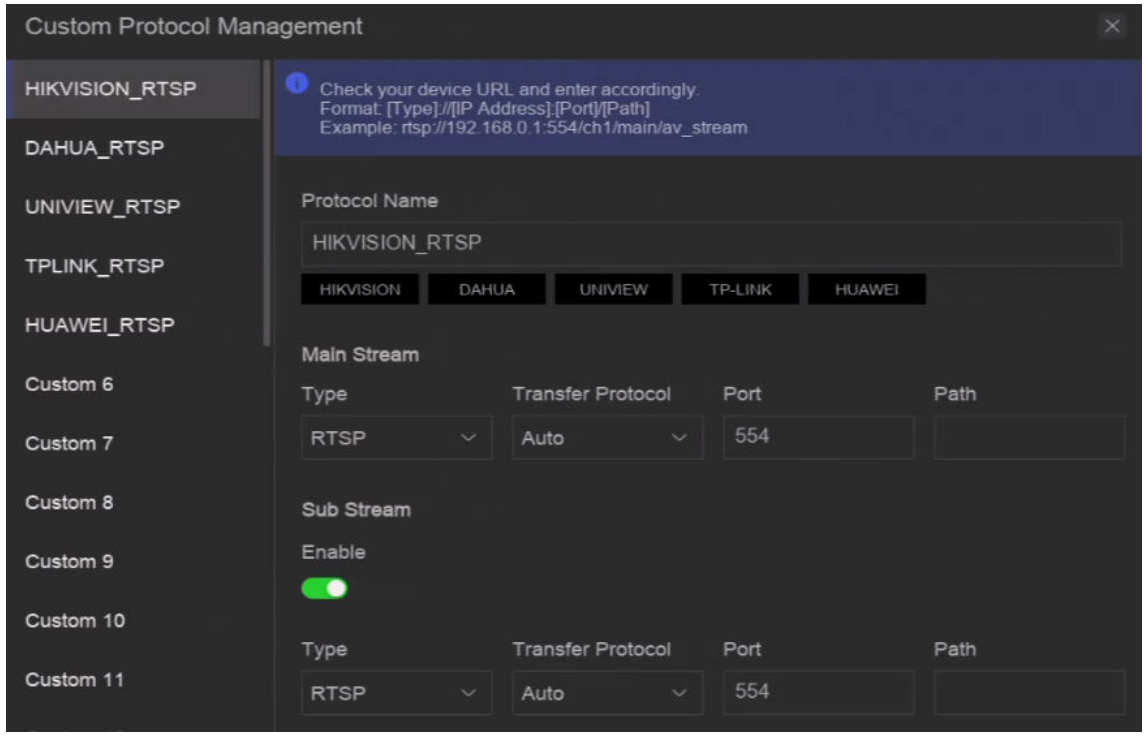


Figure 6-3 Add Network Camera via Customized Protocol

3. Select a protocol type at the left side.
4. Set protocol parameters.

Type

The network camera adopting custom protocol must support getting stream through standard RTSP.

Transfer Protocol

3 types are selectable, including **Auto**, **UDP**, and **RTP Over RTSP**.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and sub-stream. The general format is *[Type]://[IP Address]:[Port]/[Resource Path]*, for example, *rtsp://192.168.0.1:554/ch1/main/av_stream*.

Note

- **Protocol Name** and **Path** can be automatically generated if you click a brand name below **Protocol Name**.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.

5. Click **OK**.
6. Click **Add** in **System → Device Access → Device → Video Device** to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

1. Go to **System → Device Access → Device → Video Device** .
2. Click **Import** to import the configuration file in USB flash drive.
3. Set the folder path.
4. Click **Confirm**.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with ***Access Video Device*** .

6.3 Add Security Control Panel

Steps

1. Go to **System → Device Access → Device → Security Control Panel** .
2. Click **Add**.
3. **Optional:** Select a protocol.
4. Enter device IP address, name, and IoT service port.
5. **Optional:** Select a transfer protocol if you select **OPTEX** as the protocol type.
6. **Optional:** Click in the Operation column to set OSD parameters including character encoding, overlay mode, font size, etc.

Note

The Linked Channel cannot be edited. Go to **Event Center → Event Configuration → Event Configuration → Security Control Panel Event** to edit the linked channel.

OSD information you have set will be displayed on the video image.

6.4 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with ***Access Video Device*** . If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.5 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

1. Go to **System → Device Access → Device → POS** .
2. Click **Add** to add a POS device.

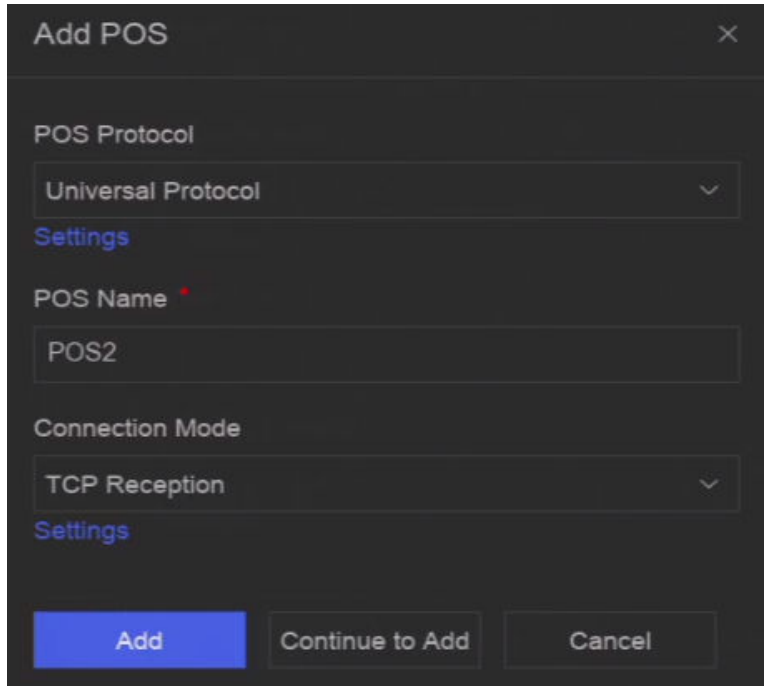


Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click **Add**.

Note

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.6 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System → Device Access → Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to **System → Device Access → Device Grouping** .

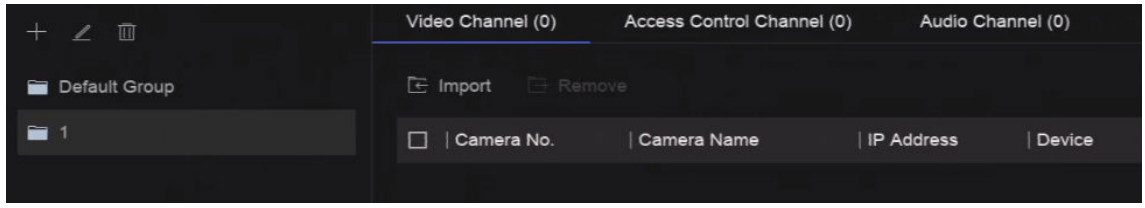


Figure 7-1 Device Grouping

2. Click + to add a group.

Note

After a group is added, you can click / to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

1. Go to **System → Device Access → Device → Video Device** .
2. Click **More → Auto Switch to H.265** .
3. Enable this function.
4. Click **Save**.

8.2 Configure Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Display Settings**. Select a camera, and configure parameters as your desire.

OSD Settings

Configure the OSD (On-screen Display) settings for the camera, including date/time, camera name, etc.

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure Time

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Video Parameters**. Select a camera, and configure parameters as your desire.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

It refers to the number of frames captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask**.

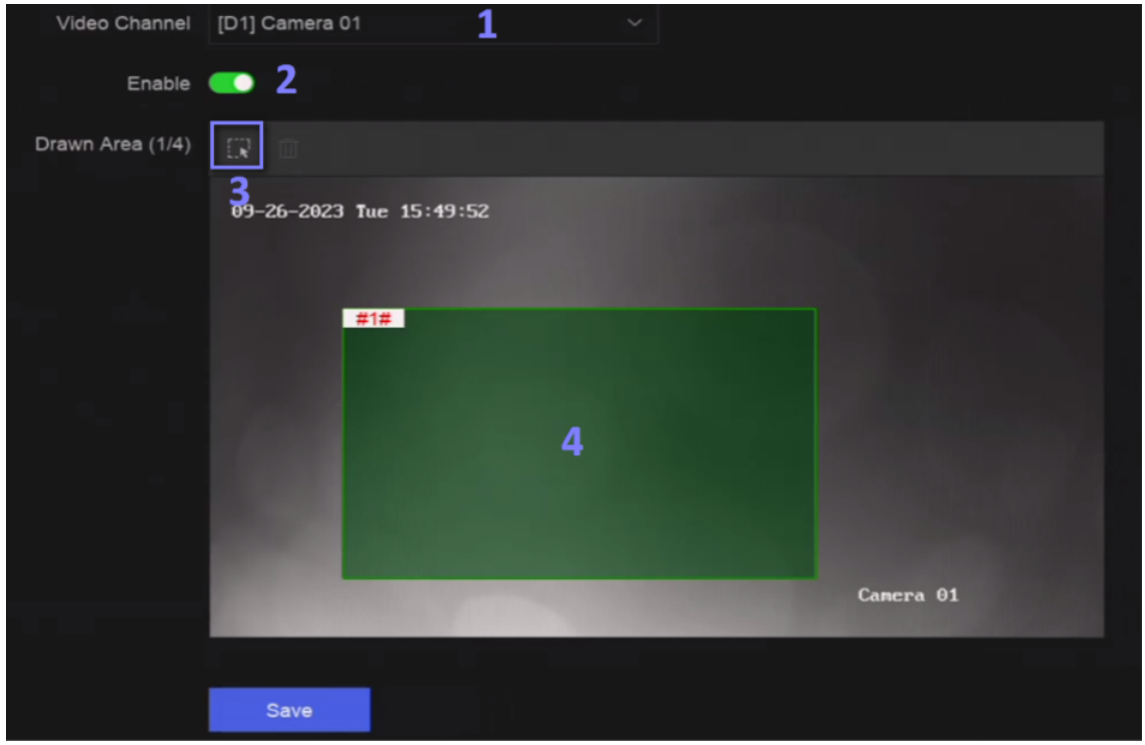


Figure 8-1 Privacy Mask

2. Select a camera.
3. Turn on **Enable**.
4. Draw mask areas on the preview window. The areas will be marked with different frame colors.

Note

Up to 4 privacy mask areas can be configured and the size of each area can be adjusted.

5. Click **Save**.

8.5 Configure Privacy Protection

This function allows for the automatic obscuring or blurring of specific areas (including human faces, human bodies, and vehicles) on the video footage to protect personal privacy or sensitive information.

Before You Start

This function should be supported by the camera.

Steps

1. Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Protection** .

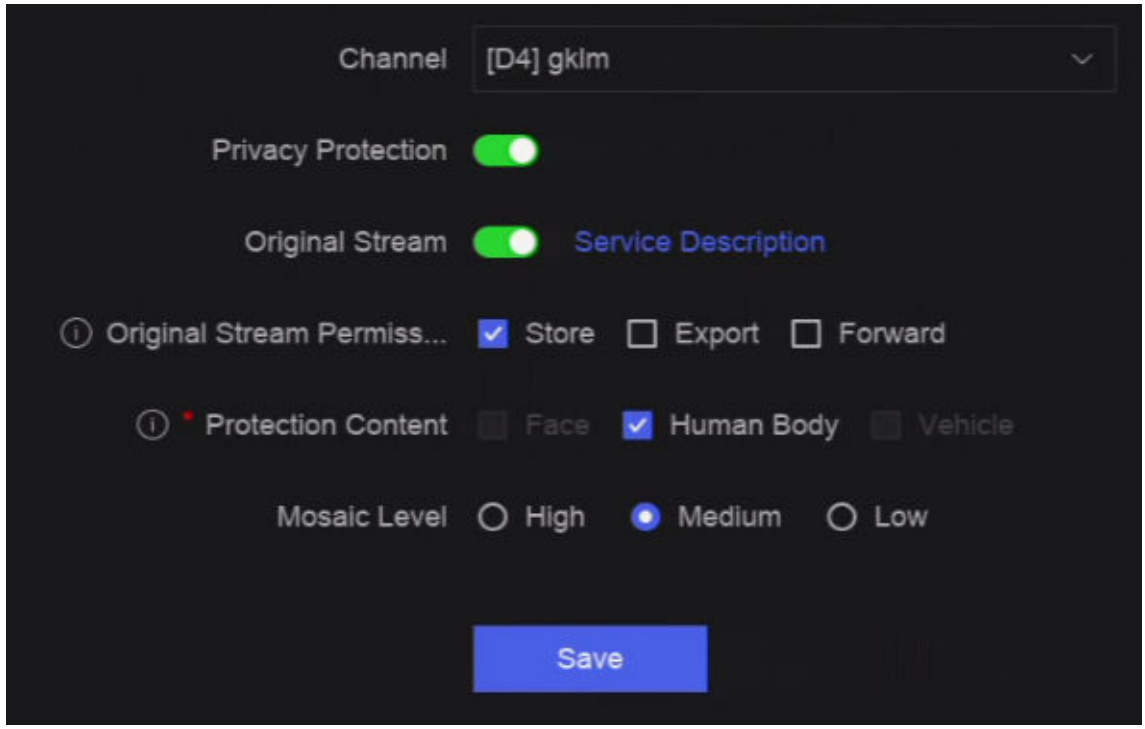


Figure 8-2 Privacy Protection

2. Select a camera.
3. Enable **Privacy Protection**.
4. **Optional:** Enable **Original Stream** and set the stream permission.

Note

Original stream means the video stream without mosaic.

Store

The original stream can be stored. Storing original stream will cost more storage space or decrease the recording storage period of the channel. The original stream bitrate is the same as the camera, which is not configurable.

Export

The channel original stream can be exported.

Forward

The original stream can be forwarded.

Note

You should check Store permission before checking Export and/or Forward permissions.

5. Set **Protection Content**. The selected protection content will be blurred during live view and playback.
6. Set **Mosaic Level**. Higher the level, more blurred the target image.
7. Click **Save**.

8.6 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System → Device Access → Device Configuration → Device Parameter → Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.7 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.

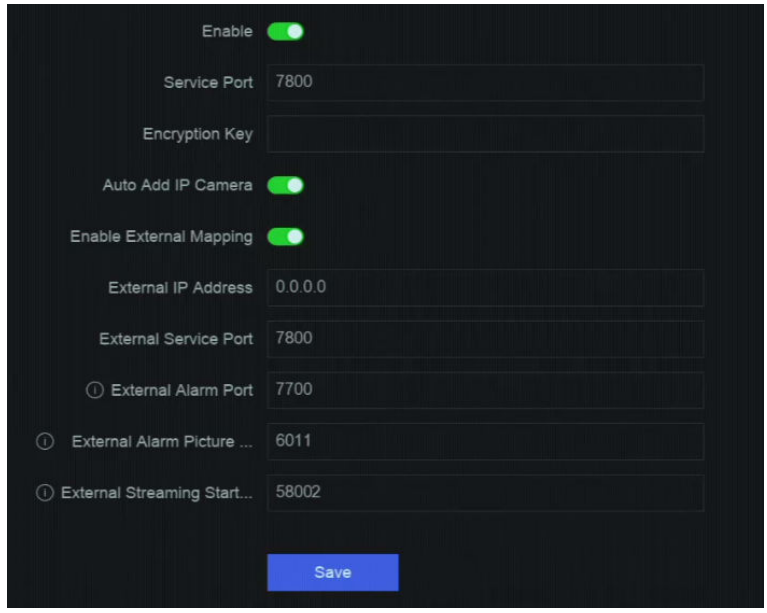


Figure 8-3 Configure OTAP Service

2. Turn on **Enable**.
3. Set the parameters.
4. Click **Save**.

8.8 Batch Configuration

Connected devices can be configured in a batch.

Steps

1. Go to **System → Device Access → Device Configuration → Batch Configuration** .

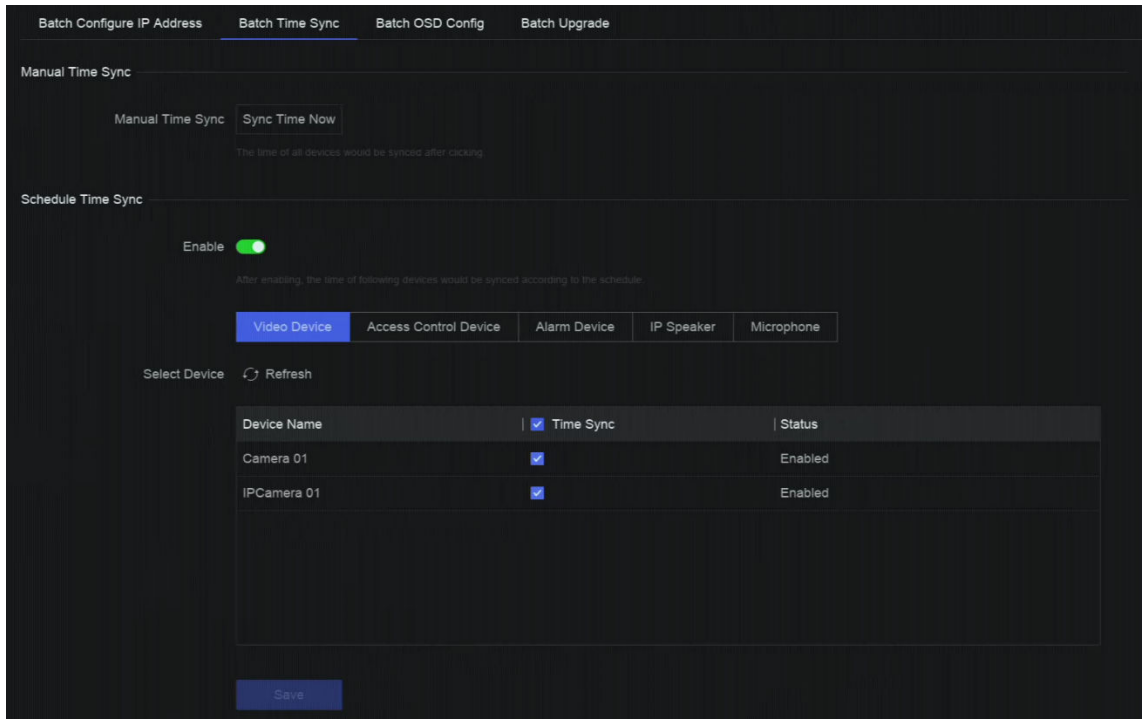


Figure 8-4 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

   Manual Time Sync

   Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

   Schedule Time Sync

   The recorder would sync time of the selected devices according a fixed schedule.

3. For IP address configuration and time sync, click **Save**.

8.9 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start
Ensure your NVR support PoE function.

Steps
1. Go to **System → Device Access → Device Configuration → PoE**.
2. Enable **Plug-and-Play** function of PoE interfaces according to your requirement.
3. Select the device type as **IP Speaker** or **Camera**.
4. If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

   Long Distance

   Long-distance (100 to 300 meters) network transmissions via PoE interface.

   Short Distance

   Short-distance (< 100 meters) network transmission via PoE interface.

   Note
   - The PoE interfaces are enabled with the short distance mode by default.
   - The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
   - The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
   - When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
   - When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.
5. Click **Save**.

What to do next
When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start
Ensure the HDD is properly installed to your device.

Steps
1. Go to **System → Storage Management → Storage HDD → Storage HDD** .

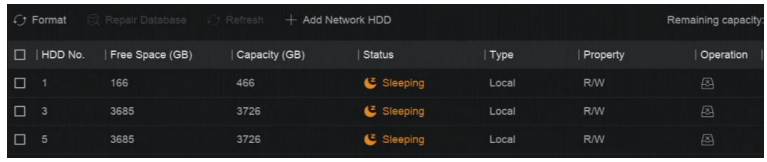


Figure 9-1 Manage HDD

2. **Optional:** Perform the following operations as your desire.

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Note
- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.

/	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed

across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

Table 9-1 HDD Requirement for Each RAID Type

RAID Type	Required Number of HDDs
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Note

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in **System → System Settings → Exception** .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- **Storage Mode** is set to **Quota** in **System → Storage Management → Storage Mode** .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Enable Array Mode**, or enable **Array Mode**.

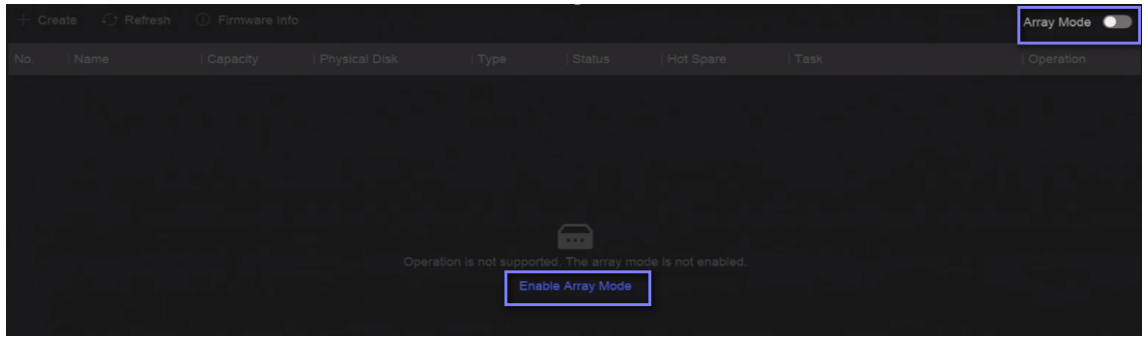


Figure 9-2 Enable RAID

3. Wait for the device to restart.
4. Go to **System → Storage Management → Storage HDD → Array Management** again.

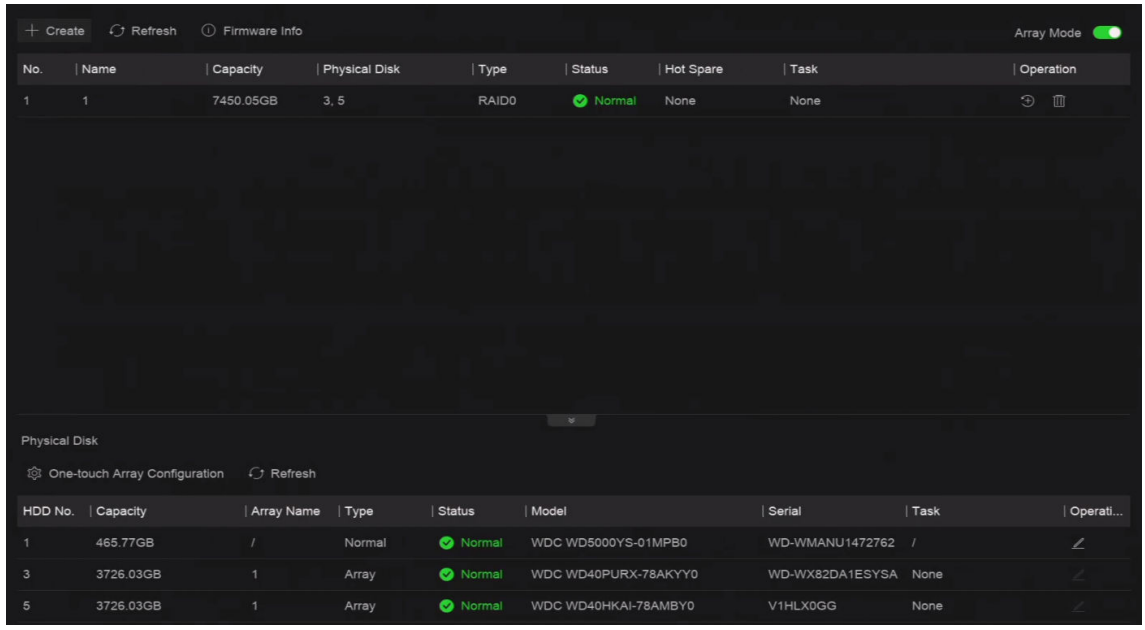


Figure 9-3 Array Management

5. Create an array.

Creation Method	Description
One-touch Array Configuration	Click **One-touch Array Configuration**. **Note** By default, the array type created by one-touch configuration is RAID 5.
Manual Creation	Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

The array status includes **Functional**, **Degraded**, and **Offline**. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Rebuild an array.

Table 9-2 Rebuilding Method

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in **Operation** column under **Physical Disk** to set a hot spare disk. When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt. **Note** After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array. Go to **System → Storage Management → Storage HDD → Array Management** , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to **System → Storage Management → Storage HDD** to click to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Firmware Info**.
3. **Optional:** Set **Back Ground Task Speed**.

9.3 Configure Storage Mode

Steps

1. Go to **System → Storage Management → Storage Mode** .

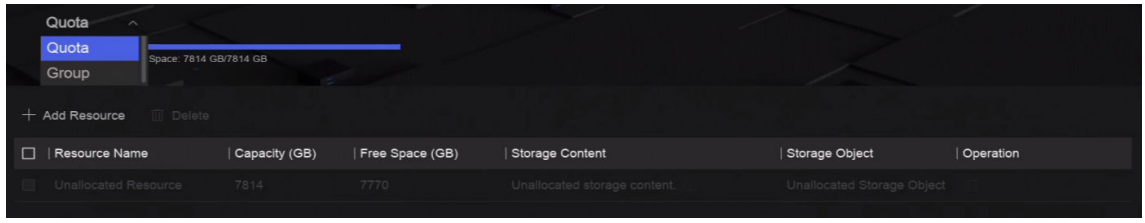


Figure 9-4 Storage Mode

2. Select **Quota** or **Group**.

   Quota

   Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

   Group

   Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.
3. Set corresponding parameters.
   - **Quota**: Allocate space for storage objects.
   - **Group**: Link channels to HDD groups.

9.4 Configure Auto Backup

You can enable auto backup so that specific channels will start backing up recordings at the configured time.

Note

This function should be supported by the device. Before using the function, make sure the eSATA storage device have been connected.

Go to **System → Storage Management → Backup Configuration → Auto Backup Configuration** , and enable **Auto Backup**.

Stop Writing

When the HDD space used for backup is full, new recording data will stop being written to HDD.

Overwrite

When the HDD space used for backup is full, the older recordings will be overwritten so that new recording data can be written to HDD.

9.5 Configure Other Storage Parameters

Go to **System → Storage Management → Advanced Settings** .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. **Performance Mode**, **Balanced Mode**, and **Energy Saving Mode** are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in **Event Center**.
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time. **Note** • You can click during live view or playback to add a tag. • For searching tag videos, go to → **Backup → By Tag**.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.6 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

The device will follow the schedule to store files to the disk.

10.1 Configure Schedule Template

After a schedule template is configured, you can use the template as the recording schedule.

Steps

1. Go to **System → System Settings → Template Configuration → Holiday Schedule** .
2. Click **Add**.

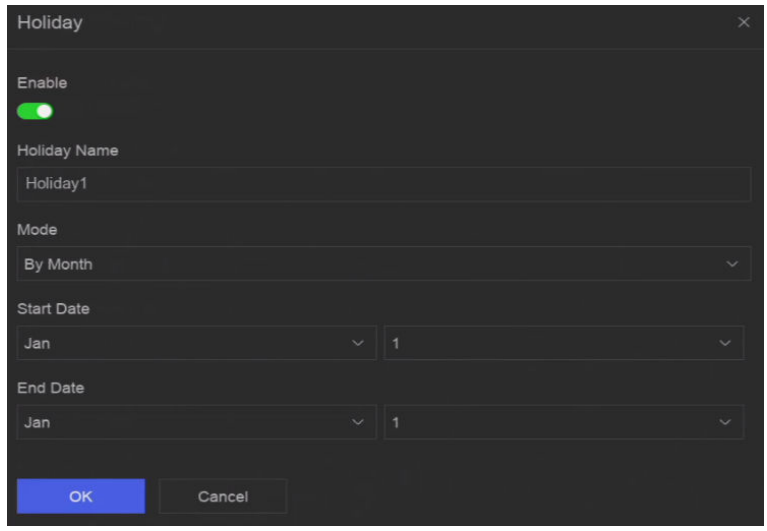


Figure 10-1 Add Holiday

3. Turn on **Enable**.
4. Configure the holiday.

Note

After holidays are configured, you will be able to set the holiday schedule independently. Holiday schedule has higher priority than normal schedule (from Mon to Sun).

5. Set **Storage Schedule**.
   1) Click **Storage Schedule**.
   2) Select a template name.

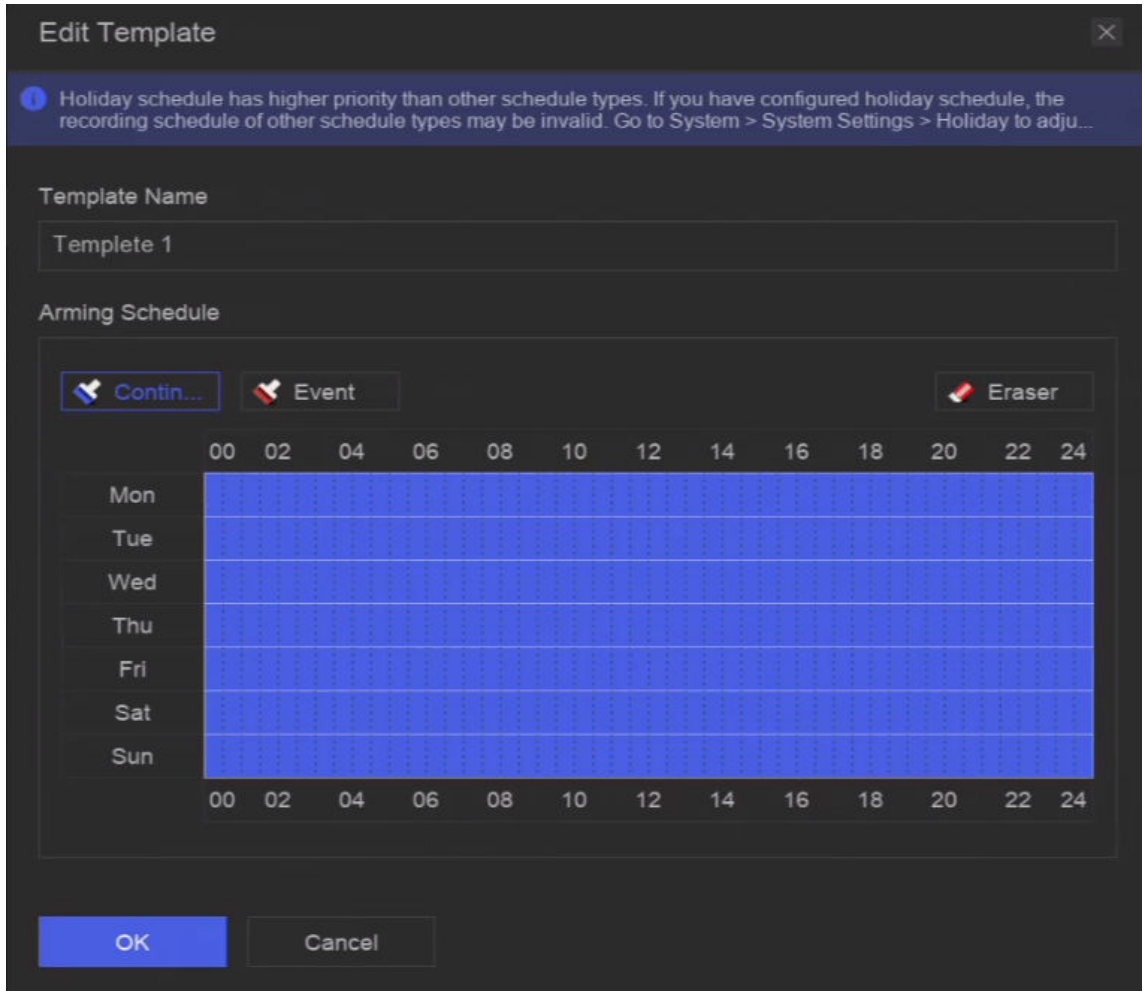


Figure 10-2 Edit Template

3) Select a recording type. For example, **Event**.
4) Drag the cursor on time bar to draw the schedule.

Note

- After moving the cursor on time bar, you can also click 00:00-24:00 to set specified time schedule.
- You can click **Eraser** to clear schedule.

Note

You can also click **Configure Template** to configure template in **System → Storage Management → Storage Schedule → Video Recording / Picture Capture / Audio Recording** .

6. Click **OK**.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Video Recording** .

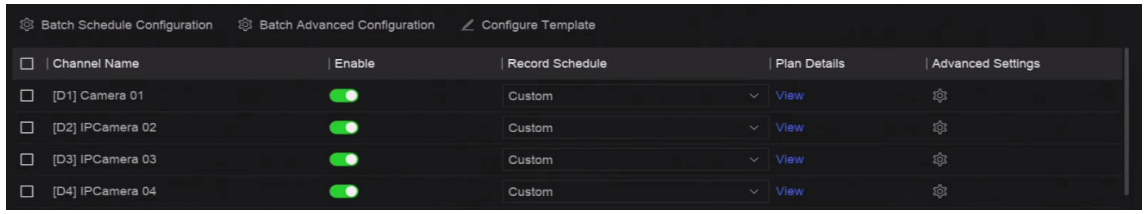


Figure 10-3 Video Recording Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.

Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

4. Click **View** to view the schedule.

Figure 10-4 View Schedule

5. **Optional:** Click ⚙ under **Advanced Settings** to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording. **Note** The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Parameter	Description
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For **Main Stream**, its resolution is usually higher. For **Sub-Stream**, you can record for a longer time with the same storage space, but its resolution would be low. For **Dual Stream**, the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Picture Capture** .

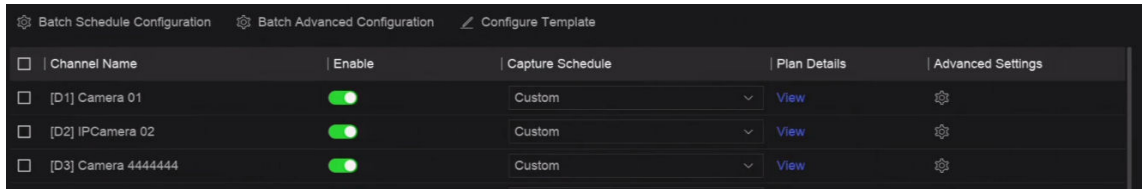


Figure 10-5 Picture Capture Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.

Note

If you set **Capture Schedule** as **Custom**, you can drag the cursor on time bar to set customized picture capture schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

4. Click **View** to view the schedule.

Figure 10-6 View Schedule

5. Click under **Advanced Settings** to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Audio Recording** .
2. Turn on **Enable** for a channel.
3. Select a schedule type.

Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

4. Click **View** to view the schedule.
5. **Optional:** Click under **Advanced Settings** to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

Chapter 11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

1. Go to **Live View**.
2. Click at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click at the right side of **View**.
6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
7. Click .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.

Figure 11-1 Live View (Type 1)

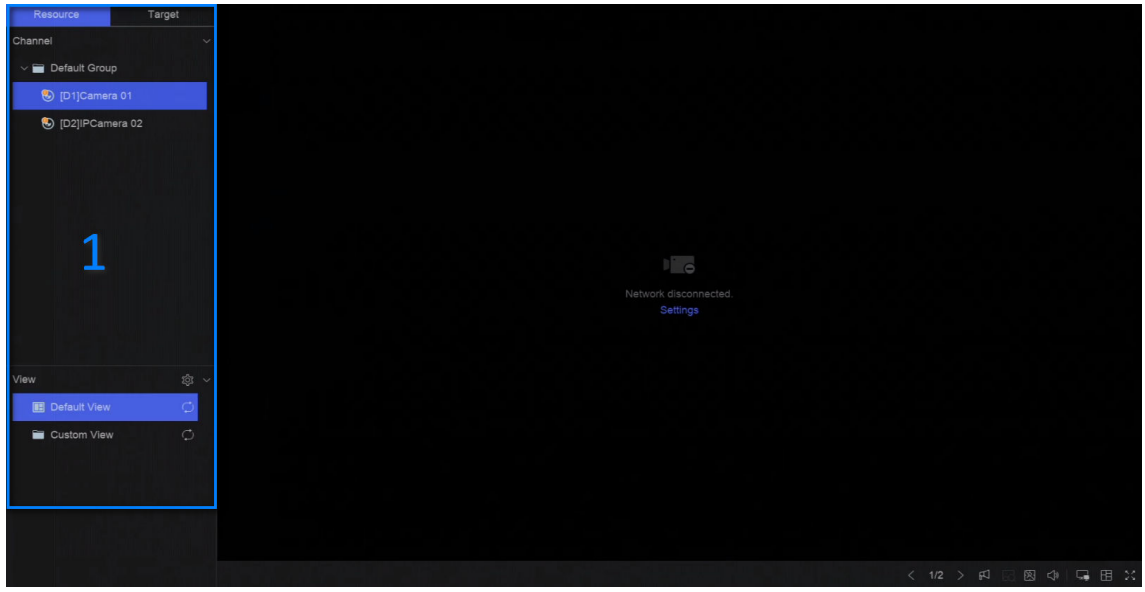


Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window. If you click **Target**, you can view live target detection results in the list, and click to configure the corresponding settings.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	Channel tool bar. • Click to add a tag go the channel. After adding, you can go to → **Backup** → **By Tag** to search videos by tag. • You can select → **Show VCA Info** to display rule frames.
4	Live view tool bar. Functions like **Voice Broadcast**, **Display VCA Info** and **Switch Output** can be performed here.

Note

- You can scroll up/down your mouse to turn to previous/next screen.
- If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Table 11-2 PTZ Operation

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click .
		Call a preset: Click .
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click . 3. Add presets for the patrol. 4. Click **OK**.
		Call a patrol: Click .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording.
		Call a pattern: Click .

Note

If the PTZ panel cannot be used, please click to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.

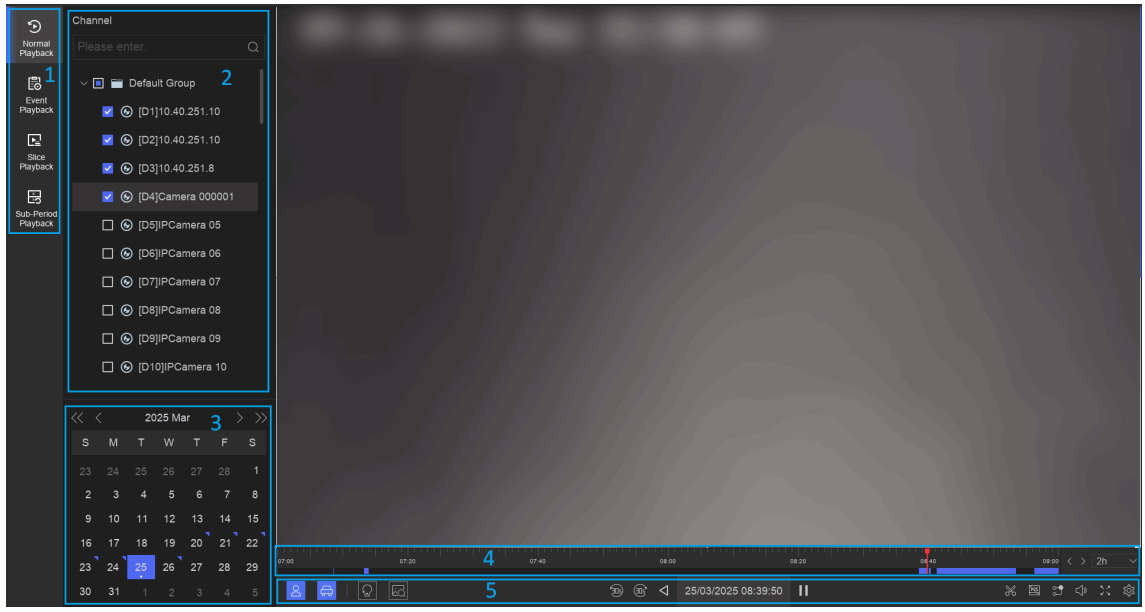


Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	Playback timeline. • Position the cursor on the timeline, drag the timeline to position to a certain time. • Period marked with blue bar contains video. Red bar indicates the video in the period is event video. • Scroll up/down to zoom out/in timeline.
5	Playback tool bar.

No.	Description
	• Click (Smart Search), then follow the pop-up tips to draw event rule and search videos that can trigger the corresponding event rule. The operations are similar with Dual-VCA function. • Click to perform AcuSearch function. Refer to ***AcuSearch*** for details. • Click / to show videos that contain human/ vehicle. **Note** In order to use this function, ensure you have configured **Detection Target** as **Human** or **Vehicle** for certain event types. • Click , select channels, and set the start and end time to clip the video in the selected channels within specific time period. • Click to set normal video and smart video (the video that contains smart data) playback strategy.

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

1. Go to **Playback** → .
2. Select channel(s) in the list at the left side.

   Note

   Group playback: Select a group in the list, and channels in the group can be played back.
3. Select a date in the calendar.

   Note

   The blue triangle at the calendar date corner indicates there are available videos.
4. **Optional:** Perform more operations.

Capture	Click to capture pictures during playback.
Digital Zoom	Click to zoom in a certain part of the video image.

	Click to add a tag to the channel. After adding, you can go to → **Backup → By Tag** to search videos by tag.
	Click to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → **Backup → By Tag** to search videos by lock.
Dual-VCA	Select → **Dual-VCA** to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type. **Note** To use this function, go to **Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream** to turn on **Enable Dual-VCA** via web browser, and go to **System → Storage Management → Advanced Settings** to turn on **Save Camera VCA Data** via local GUI interface.
Show VCA Info	You can select → **Show VCA Info** to display rule frames.
Disable Privacy Protection	If privacy protection is enabled, the image may contain mosaics. You can select → **Display Privacy Protection** to display the original video (without mosaics) if the storage permission of privacy protection is enabled as well. Refer to ***Configure Privacy Protection*** for details about privacy protection function.

12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start

- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration → Video/Audio → Display Info. on Stream** .
- Ensure your video recorder has enabled **Save Camera VCA Data** in **Storage management → Advanced Settings** .

Steps

1. Select **Playback →** .
2. Select a date in the calendar.

Note

The blue triangle at the calendar date corner indicates there are available videos.

3. Click ··· → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
4. Click **Search**.

   Videos meet the detection rule requirement will be marked in red.
5. Click ⚙ to set normal video and smart video (the video that contains smart data) playback strategy.

Note

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

1. Go to **Playback** → .
2. Select a camera from the camera list.
3. Select a date on the calendar.
4. Click **Search**.

   The retrieved video will be divided into one-hour slices for playback.
5. **Optional:** Select an one-hour slice and click to divide it into one-minute slices for playback.

12.5 Sub-Period Playback

The video files can be played in multiple sub-periods simultaneously on the screen.

Steps

1. Go to **Playback** → .
2. Select a camera.
3. Set the start time and end time.
4. Click **Search**.

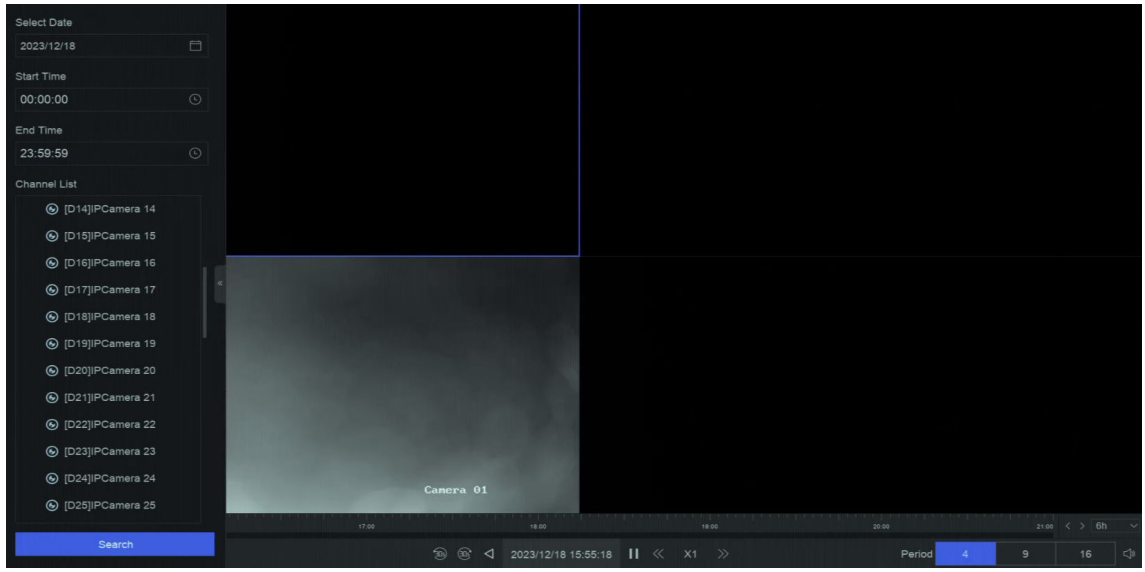


Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

Note

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to **Event Center** → ⚙ → **Event Configuration** → **Basic Event / Generic Event** .
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Configuration	
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. • **AI by NVR**: The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects. • **AI by Camera**: The motion detection event will be analyzed by camera. • **Detection Target**: **Human** and **Vehicle** are selectable, apart from false alarms, only the	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.

Event Name	Event Description	Rule Configuration	
		selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-2 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

8. Click **Save**.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center → ⚙ → Event Configuration → Perimeter Protection**.

2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Line Crossing**.
6. Turn on **Enable**.

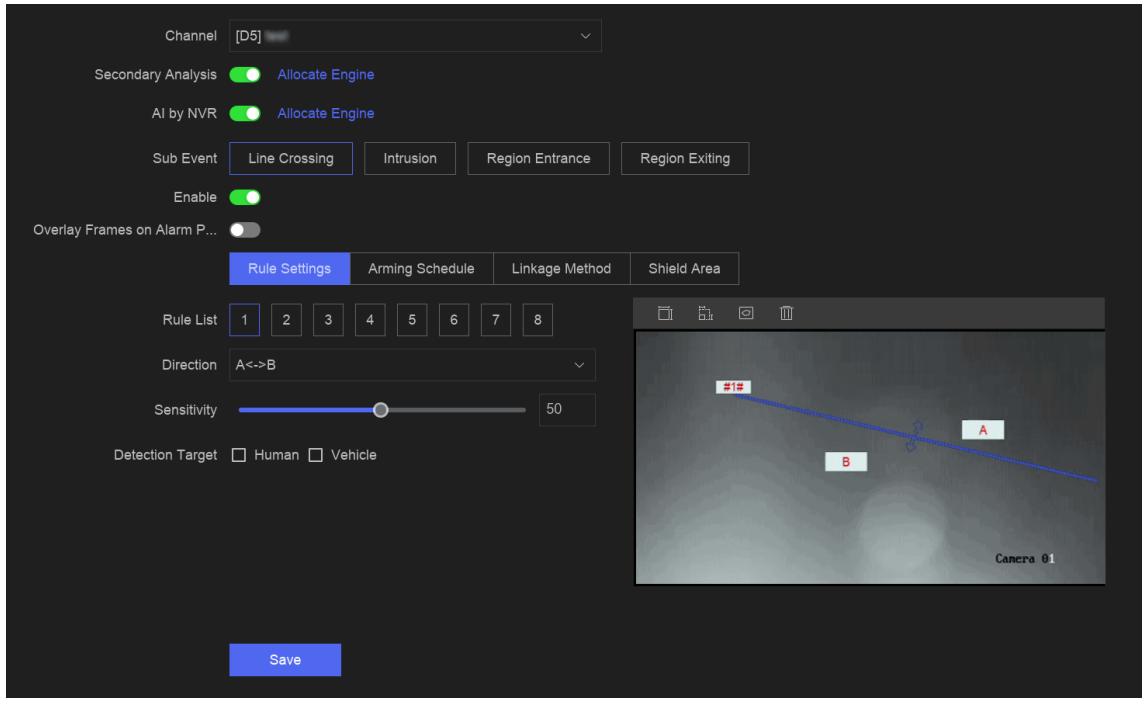


Figure 13-1 Line Crossing Detection

7. Click **Rule Settings** to detection rules.
   1) Select a rule number. For example, select **1**.
   2) Click , and click on the image twice respectively to draw the start point and end point of the detection line.

3) Set **Direction**, **Sensitivity**, **Detection Target**, and **Target Confidence**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting line crossing events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.

5) **Optional:** Repeat above steps to draw more rules. Up to 8 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-3 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.
11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a pre-defined virtual region. Specific actions can be taken when an alarm is triggered.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center → ⚙ → Event Configuration → Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

   Note

   At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.
4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Intrusion**.
6. Turn on **Enable**.

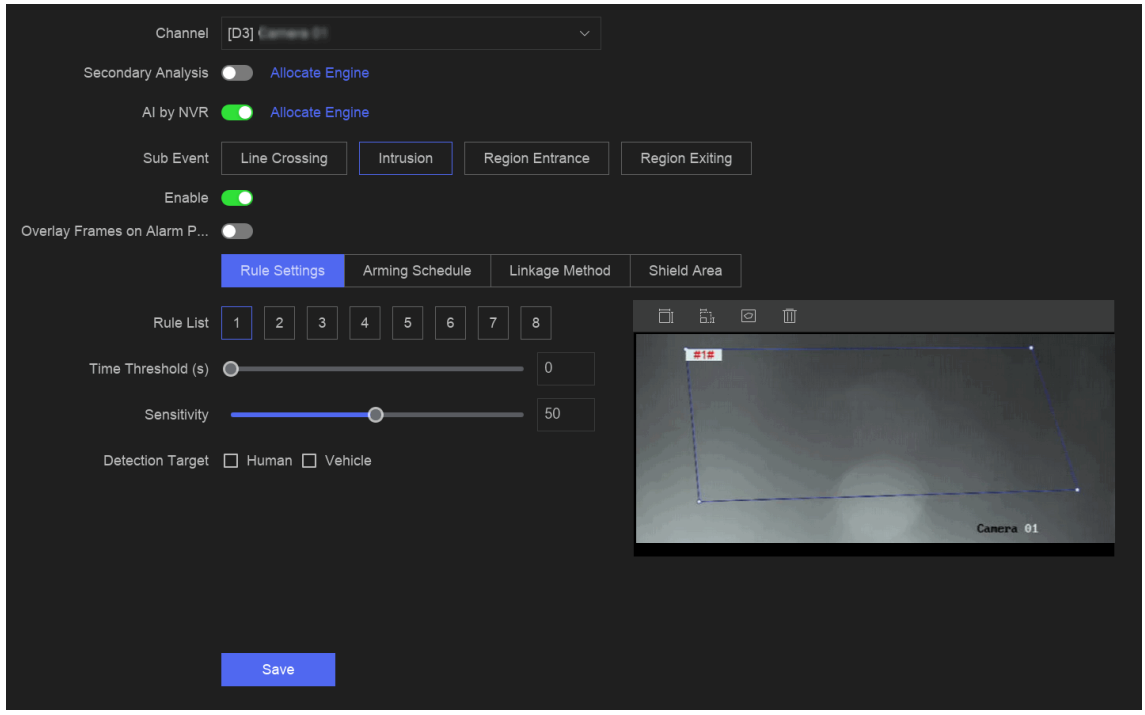


Figure 13-2 Intrusion Detection

7. Click **Rule Settings** to detection rules.
   1) Select a rule number. For example, select **1**.
   2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
   3) Set **Time Threshold**, **Sensitivity**, **Detection Target**, and **Target Confidence**.

   Time Threshold

   The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

   Sensitivity

   The higher the value is, the more easily the detection alarm can be triggered.

   Detection Target

   Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting intrusion events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-4 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next
You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps

Note
A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** → ⚙ → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

   Note
   At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.
4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

   Note
   At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Perimeter Protection** algorithm.
5. Select **Region Entrance**.
6. Turn on **Enable**.

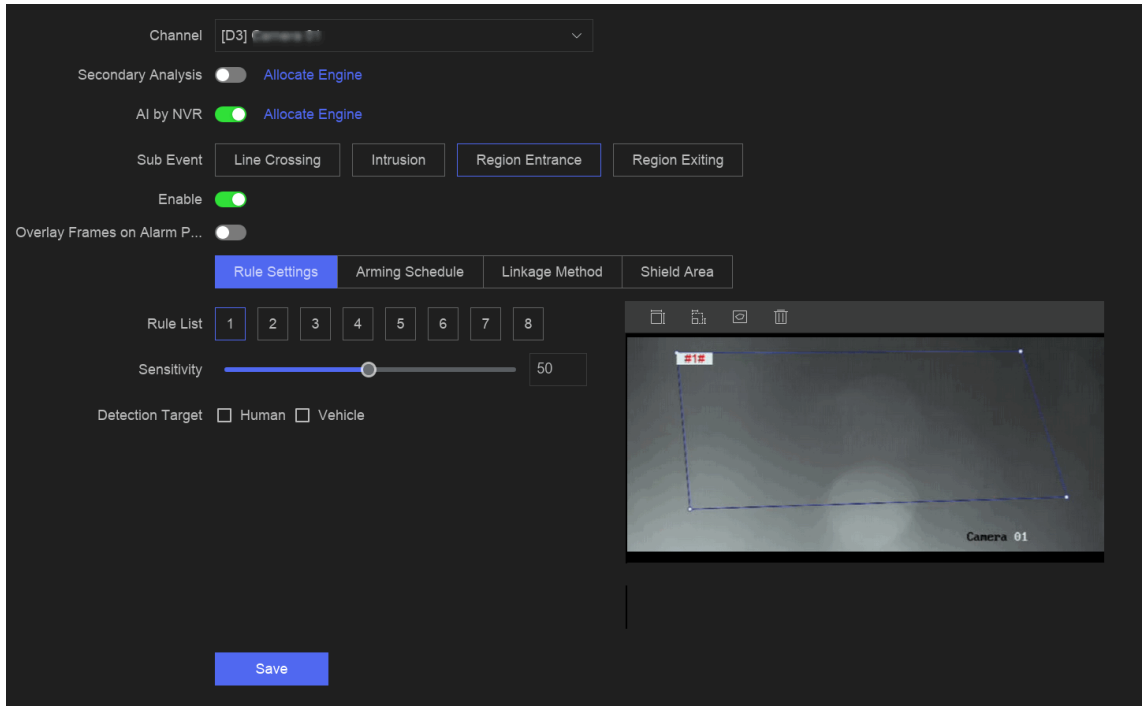


Figure 13-3 Region Entrance Detection

7. Click **Rule Settings** to detection rules.

1) Select a rule number. For example, select **1**.
2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
3) Set **Sensitivity**, **Detection Target**, and **Target Confidence**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting region entrance events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-5 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.
11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** → ⚙ → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

   Note

   At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.
4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

   Note

   At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Perimeter Protection** algorithm.
5. Select **Region Exiting**.
6. Turn on **Enable**.

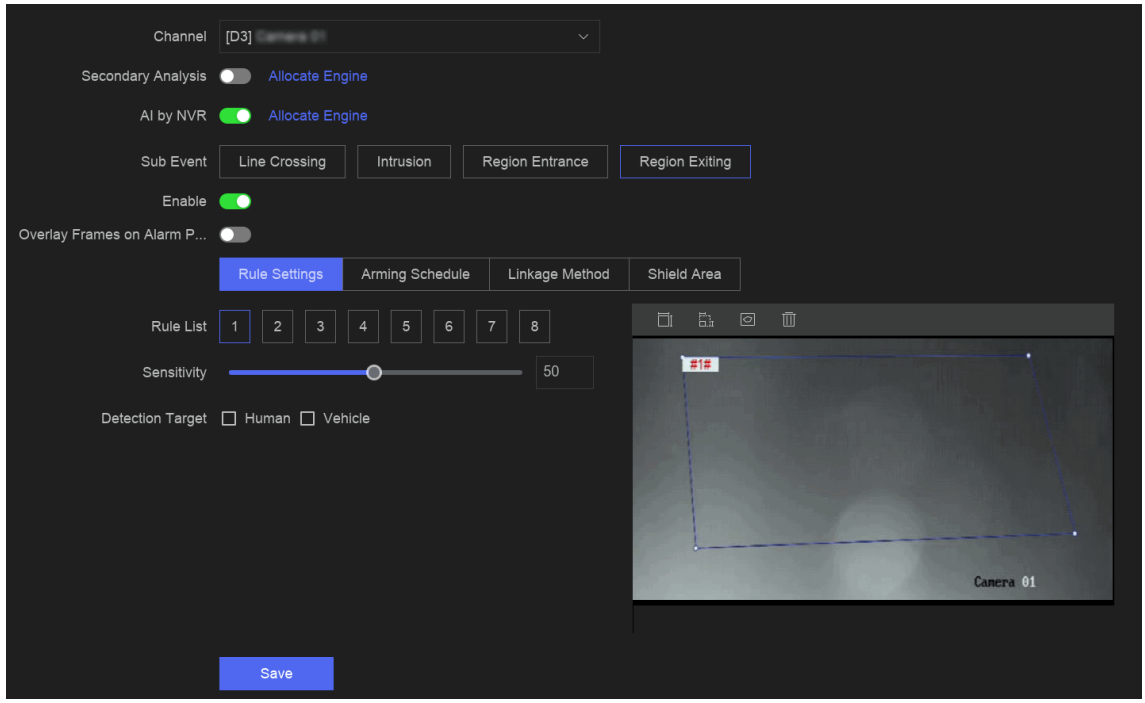


Figure 13-4 Region Exiting Detection

7. Click **Rule Settings** to detection rules.

1) Select a rule number. For example, select **1**.
2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
3) Set **Sensitivity**, **Detection Target**, and **Target Confidence**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting region exiting events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

4) **Optional:** Repeat above steps to draw more rules. Up to 8 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-6 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.
11. Click **Save**.

What to do next
You can go to **Live View** and click **Target** to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start
Ensure the camera supports this function.

Steps
1. Go to **Event Center → ⚙ → Event Configuration → Abnormal Behavior Event** .
2. Select a camera
3. Select an event type.

4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set **Time Threshold** and **Sensitivity**. **Time Threshold** The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10]. **Sensitivity** Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	
Object Removal Detection	The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so	

Event Name	Event Description	Rule Configuration
	that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set **Percentage**. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.

Linkage Method	Description
	Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

8. Click **Save**.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **Event Center → Event Configuration → Smart Settings → Algorithm Configuration → Algorithm Management** .

Steps

1. Go to **Event Center →** ⚙ **→ Event Configuration → Target Event** .
2. Select a camera.
3. Select an event.
4. Turn on **Enable**.
5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can be triggered when a human face is detected.	-
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	• Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). • Supports configuring prompts for failed and succeeded comparisons.

Event Name	Event Description	Rule Configuration
Stranger Detection	Faces not in the list library appearing in the video will be identified as strangers.	• Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). • Supports configuring the prompt for detecting strangers.
Multi-Target-Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.

Linkage Method	Description
	Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

8. Click **Save**.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start
Add the thermal network camera to your device and make sure the camera is activated.

Steps
1. Go to **Event Center → ⚙ → Event Configuration → Thermal Event** .
2. Select a camera.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.
Perimeter Protection	Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

6. Click **Arming Schedule** to select an arming schedule type.

Note
If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-11 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

8. Click **Save**.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to **Event Center → ⚙ → Event Configuration → Alarm Input Event** .
2. Select an alarm input name.

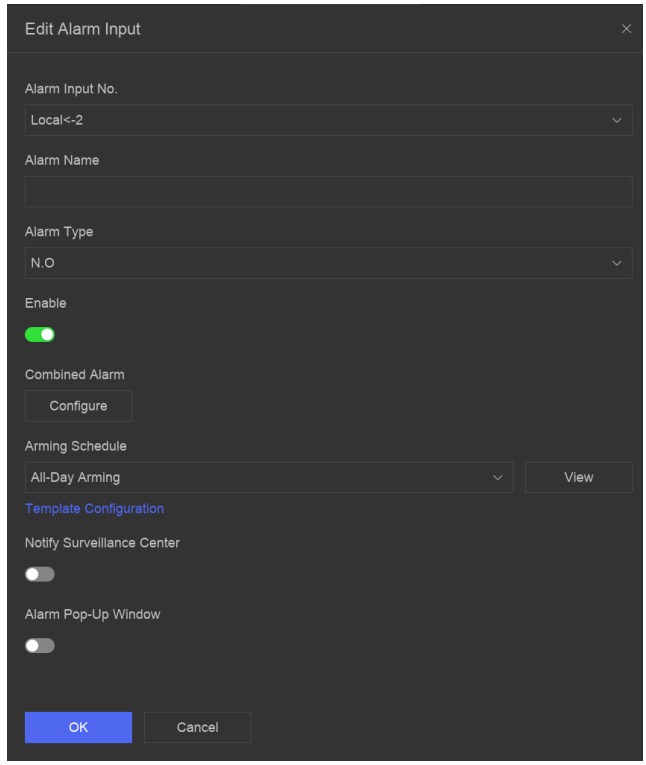


Figure 13-5 Configure Alarm Input

Note

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

3. Edit **Alarm Name**.
4. Set **Alarm Type**.

   N.O

   When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

   N.C

   When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.
5. Turn on **Enable**.
6. **Optional:** If you select **Local<-1** in Step 2, select the processing method.
   - Select **Process Alarm Input**, and then you can set the corresponding arming schedule, linkage methods, etc.

     Note

     The operations below are all available when you select this processing method.
   - Select **Quick Disarming**, and then linkage methods of all events will be disabled.
7. Click **Configure** to configure combined alarm.

1) Select a channel.
2) Select combined alarm events such as motion detection and video tampering detection.
3) Click **OK**.

The combined alarm will be triggered when it receives alarms from both alarm input and events.

8. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-12 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

10. Click **Save**.

13.1.7 Audio Analysis Event

Steps

1. Go to **Event Center → ⚙ → Event Configuration → Audio Analysis** .

2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-13 Audio Analysis Event

Event Name	Event Description	Rule Configuration
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/ decrease in sound intensity.	**Sudden Increase of Sound Intensity Detection** Detects a steep sound increase in the scene. **Sudden Decrease of Sound Intensity Detection** Detects a steep sound drop in the scene. **Sensitivity** The higher the value is, the easier the detection alarm can be triggered. **Sound Intensity Threshold** It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-14 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. **Note** Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to **System → Storage Management → Storage Schedule → Video Recording** to configure video recording schedule.

8. Click **Save**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

1. Go to **Event Center → ⚙ → Event Configuration → Linkage Configuration** or **System → Event Configuration → ⚙ → Event Configuration → Linkage Configuration**.
2. Click **Email** to configure email parameters.

Table 13-15 Email Linkage

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
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	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.

Item	Description
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

Note

If you are using an Outlook email account, please set **Email Type** as **Outlook**, and click **Help** at the right side to read the configuration instructions, then follow the steps on the interface to complete the configuration.

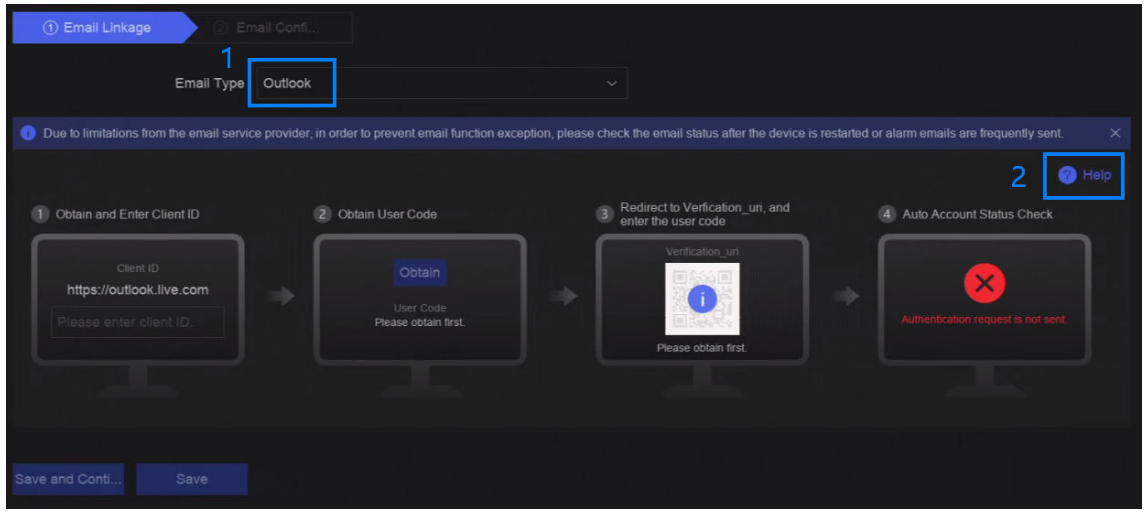


Figure 13-6 Outlook Email Configuration

3. Click **Audio Management** to manage audio files for alarm linkage.

Note

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

Note

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.

5. Click **Alarm Output** to set alarm output parameters.

Note

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, **Local->1** means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

Note

This linkage action is only available for few event types.

7. If you have connected security control panels, click **Security Control Panel** to configure parameters including IP address and port number.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

1. Go to **Event Center** → ⚙ → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** → ⚙ → **Event Configuration** → **Linkage Configuration**.

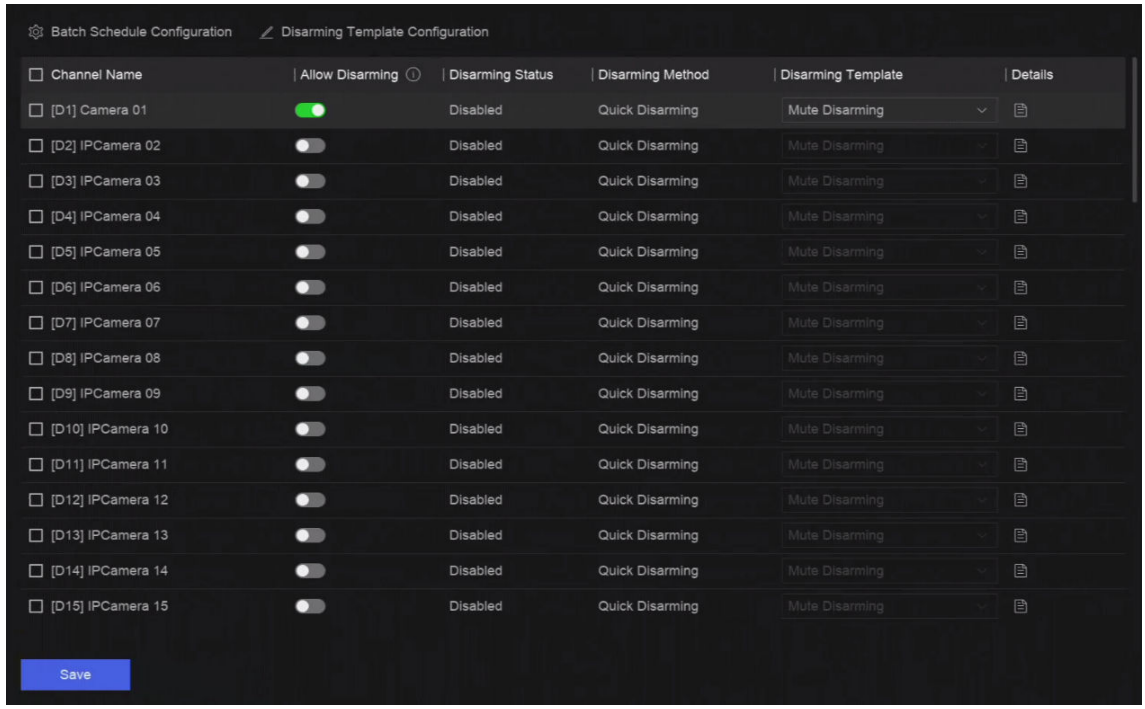


Figure 13-7 Disarming Configuration

2. Select channel(s) that are allowed for disarming.
3. Click **Batch Schedule Configuration**.
4. Turn on**Enable**.
5. Select **Disarming Template**. Only two types are available

Note

Currently, only two template types are available and each template parameters cannot configured.

6. Click **OK**.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center → ⚙ → Event Configuration → Batch Configuration** or **System → Event Configuration → ⚙ → Event Configuration → Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

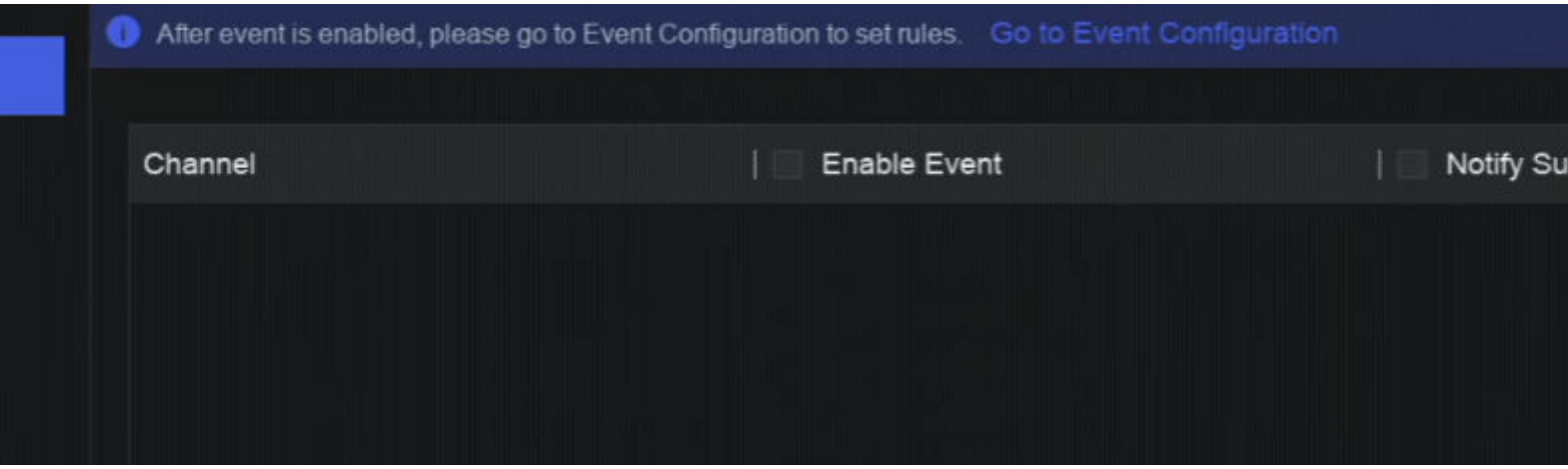


Figure 13-8 Batch Configuration

13.5 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

1. Go to **Event Center** → .

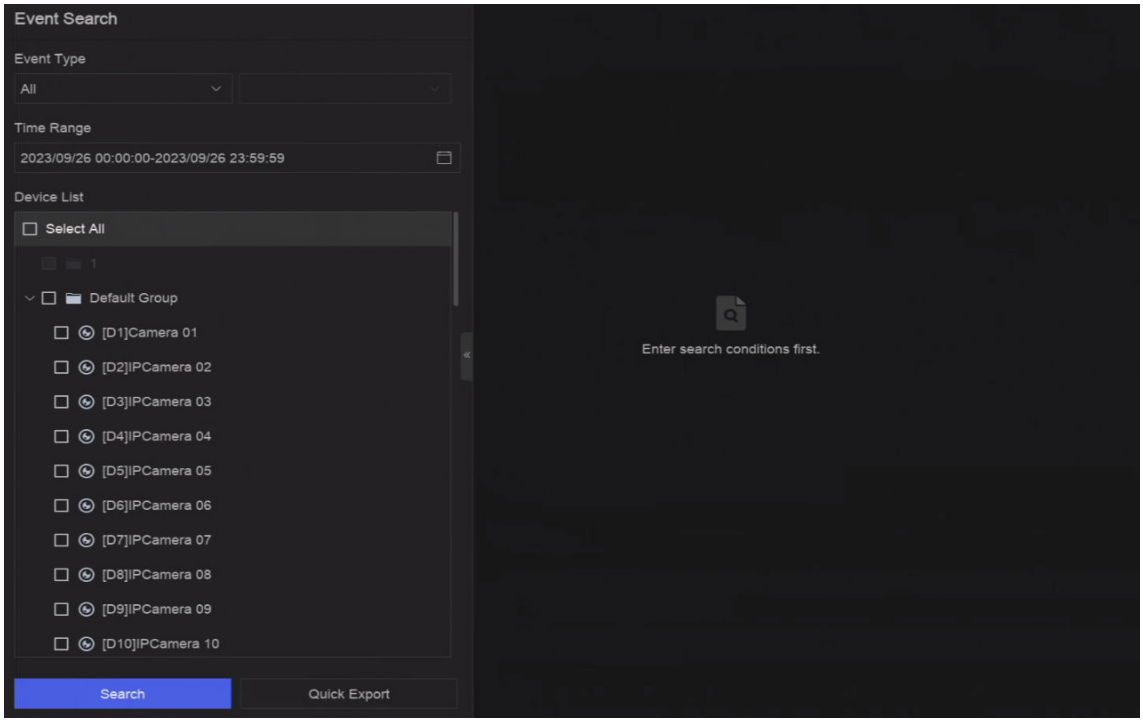


Figure 13-9 Event Search

2. Specify detailed conditions, including event type, time, channel, etc.
3. Click **Search**.

   The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

1. Go to **Event Center** → .
2. Click **Real-Time Alarm**.
3. Select the alarm from the list.

   If there are too many alarms, click **Filter** to search and find the alarm.
4. Click **Playback**, and the alarm recording video would be played back.
5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to **Backup**.

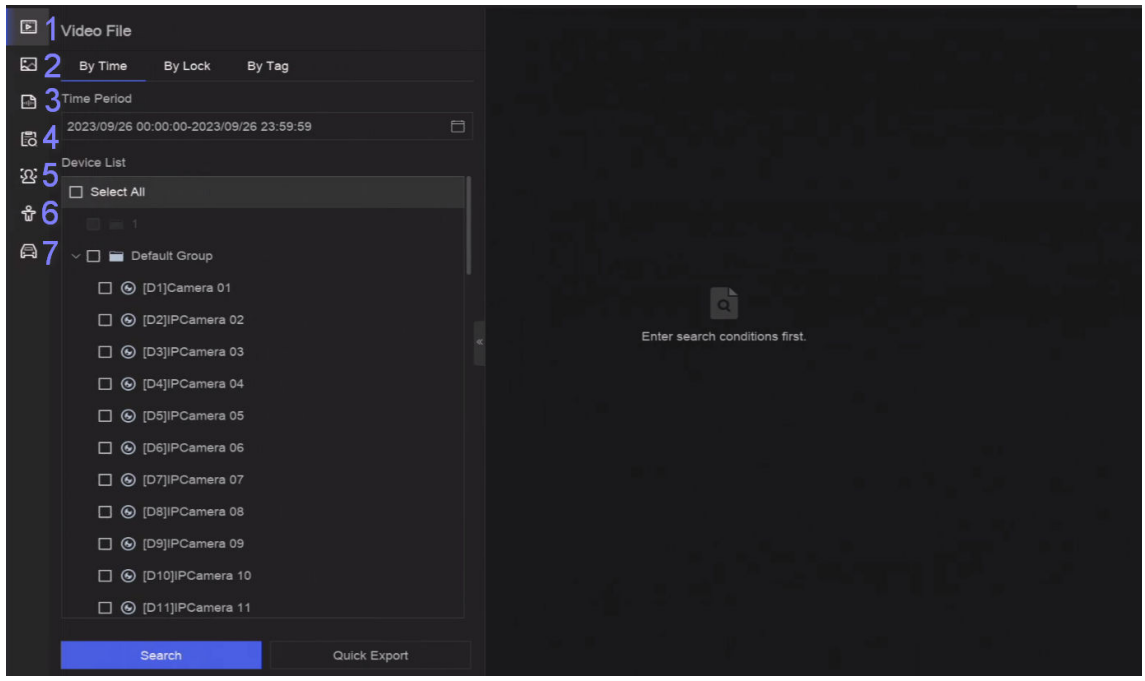


Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, 7 types are supported.

Note

The searching conditions would vary according to the selected searching method.

3. Set the searching conditions.
4. Click **Search**.

Figure 14-2 Searching Result

5. **Optional:** Perform the following operations.

    1 Click to select a file.

    2 Click to lock a file. After a file is locked, it will not be overwritten.

    3 Click to export a file.

    4 Use the tool bar at the top to filter results by channel.

    5 Use the tool bar at the top to switch display effect.

    6 Go to different result pages.

    7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.

6. Insert a USB flash drive to the device for backup.
7. Export files to the USB flash drive.
    - Select files(s) in the result list and click **Export**.
    - Click **Export All** to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

1. Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable AcuSearch algorithm.
   - **AI by Camera**: The camera will perform the AcuSearch analysis.
   - **AI by NVR**: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
2. Go to Live View or Playback, and click at the lower-left corner during video playing.

   Note

   - If targets are hard to find during playback, it is recommended to use **Smart Search** ( ) to find scenes that contain targets.
   - Human face and body would be framed with different colors.
   - After clicking , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
3. Click of the selected target.

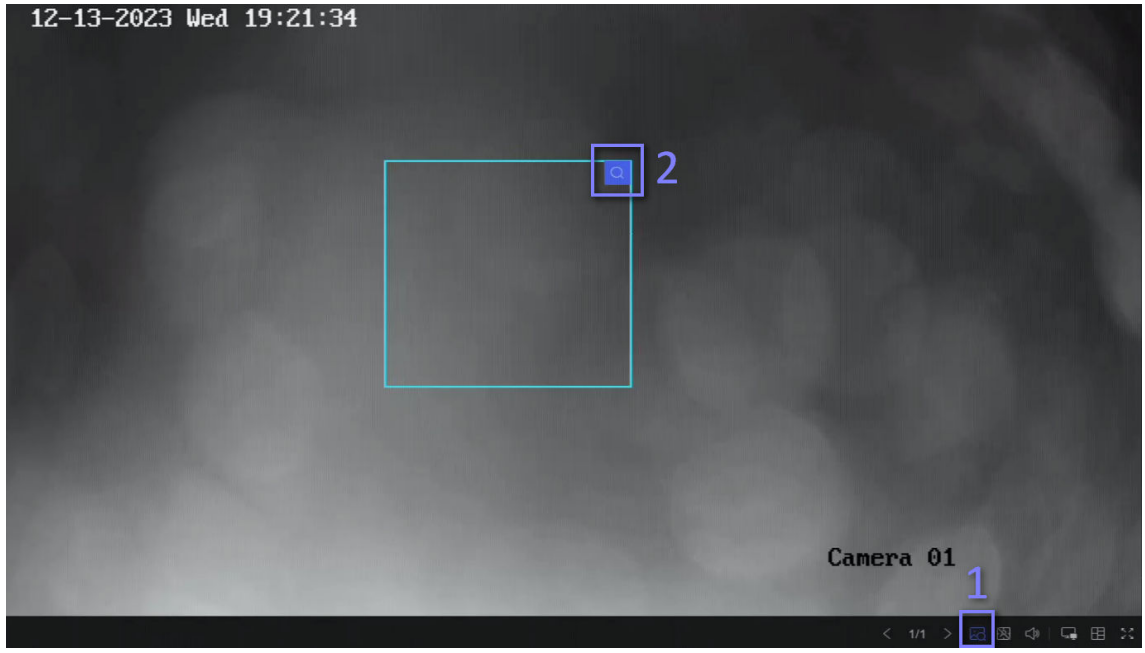


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

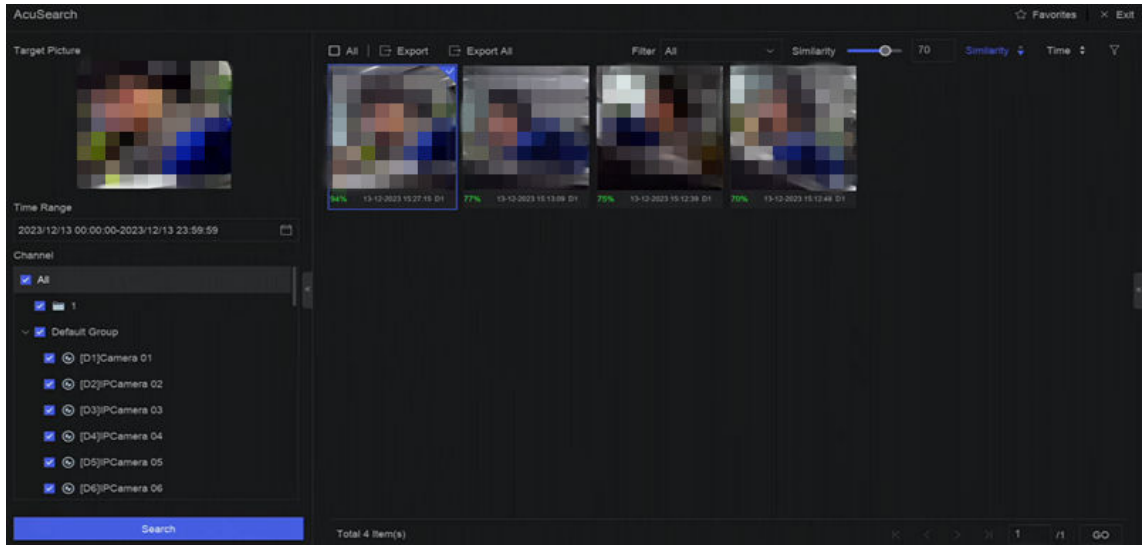


Figure 15-2 AcuSearch Result

5. **Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
6. **Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. You can use the smart function after allocating the corresponding algorithm to an engine.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management** . You can will the supported algorithms and click the required algorithm to link it with engine(s).

Note

Please go to the web page of device for the application of secondary analysis for perimeter alarm from thermal camera. Currently only engine configuration is available on the GUI interface.

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Engine Status** or **Event Center → Event Configuration → Smart Settings → Engine Status**. If you need to switch the algorithm, refer to ***Algorithm Management*** .

16.3 Task Plan Management

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Task Plan Management** or **Event Center → Event Configuration → Smart Settings → Task Plan Management**. For **Non-Real-Time Target Comparison**, you can view the progress of each day.

Task status mainly includes 3 conditions: **Disabled**, **Waiting**, and **Enabled**.

Disabled

No analysis task is enabled on the camera.

Waiting

The analysis task of the camera is enabled. Device is waiting to analyze data.

Enabled

The analysis task of the camera is enabled and device is analyzing data of the camera.

16.4 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers** library is used to store pictures for strangers, and it cannot be deleted.

16.4.1 Add a List Library

Steps

1. Go to **System → Event Configuration → Event Configuration → Data Archive → List Library** or **Event Center → Event Configuration → Data Archive → List Library**.
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.

Note

- After a list library, you can move the cursor on the library to edit or delete it.
- You can click **Delete in Batch** to delete selected libraries, or clear all pictures in the selected libraries.

16.4.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

1. Double click a list library.
2. **Optional:** Click **Custom Tag** to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.
3. Click **Add** or **Import**.
4. Import picture(s).
   - **Add**: Click to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
   - **Import**: Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.
5. **Optional:** Perform the following operations.

Delete Pictures from the Library	• Select a picture and delete it. • Select pictures and click **Delete in Batch** to delete the select ones.
Search Pictures in the Library	Click at the tool bar to search pictures.
Copy Pictures to Another Library	Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click **Export** to export them to a USB flash drive.

16.5 Self-Learning Settings

Self-learning technology optimizes algorithm accuracy and requires minimum manual intervention from users. When self-learning function is enabled, the device would automatically collect false alarm materials, and use the collected materials to constantly train and optimize the corresponding algorithm.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management** to enable **Self-Learning** algorithm.

Note

- Only certain models support this function.
- Currently, self-learning function can only be adopted for perimeter protection events.
- If your device only has one engine, **AI by NVR** has to be disabled and the camera should perform the analysis of detection targets. If your device only has two or more engines, you can enable **AI by NVR** and use one engine for the analysis of detection targets, then use another engine to run the self-learning algorithm.

16.5.1 Self-Learning Task Management

After self-learning algorithm is running, the self-learning task should be enabled as well.

Go to **System → Event Configuration → Event Configuration → Self-Learning → Task Management** or **Event Center → Event Configuration → Self-Learning → Task Management** to enable the task.

The available task would be listed, and you can view task status and progress bar. It would take a long time for the material collection.

When the task is completed, self-learning algorithm would be updated automatically. You can click **Auto Update Config** to set **Update Time**.

Note

- When the self-learning algorithm would be unavailable for perimeter protection events when the algorithm is updating.
- **Force Training** is only used for the technical support.

16.5.2 Model Management

You can set the self-learning algorithm model version according to your requirement.

Go to **System → Event Configuration → Event Configuration → Self-Learning → Model Management** or **Event Center → Event Configuration → Self-Learning → Model Management** to set the model version.

Restore to Previous Version

Restore the model to the version before this one.

Restore to Default Version

Restore the model to the factory default version.

16.5.3 Smart Status

You can view the self-learning algorithm performance status of each channel in **System → Event Configuration → Event Configuration → Self-Learning → Smart Status** or **Event Center → Event Configuration → Self-Learning → Smart Status**.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time.

Human and vehicle detection should be configured in advance. Go to **Event Center** → ⚙ to configure.

Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

No.	Description
1	Right-click shortcut menu.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

17.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

17.2.1 Add Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** . Allocate **Target Recognition** to at least one engine.
- The list library for check-in comparison is properly configured. Refer to ***Add a List Library*** for details.

Steps

1. Click **Person Check-In** .
2. Right click to display the menu at left side.
3. Click .
4. Click **Add**.

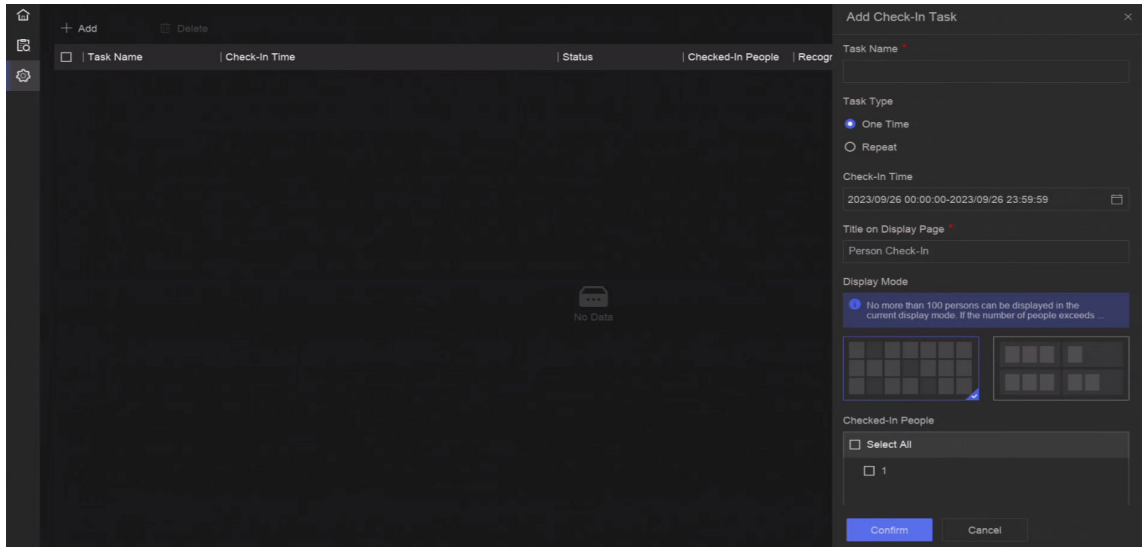


Figure 17-2 Add Check-In Task

5. Set **Task**.

   One-Time

   The task will be used for one time.

   Repeat

   The task will be used and repeated for several times.
6. Configure other parameters, including **Task Name**, **Check-In Time**, **Recognition Channel**, etc.
7. Click **Confirm**.

17.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start
Ensure check-in tasks are configured.

Steps
1. Go to **Person Check-In** .
2. Right click to display the menu at the left side.
3. Click .

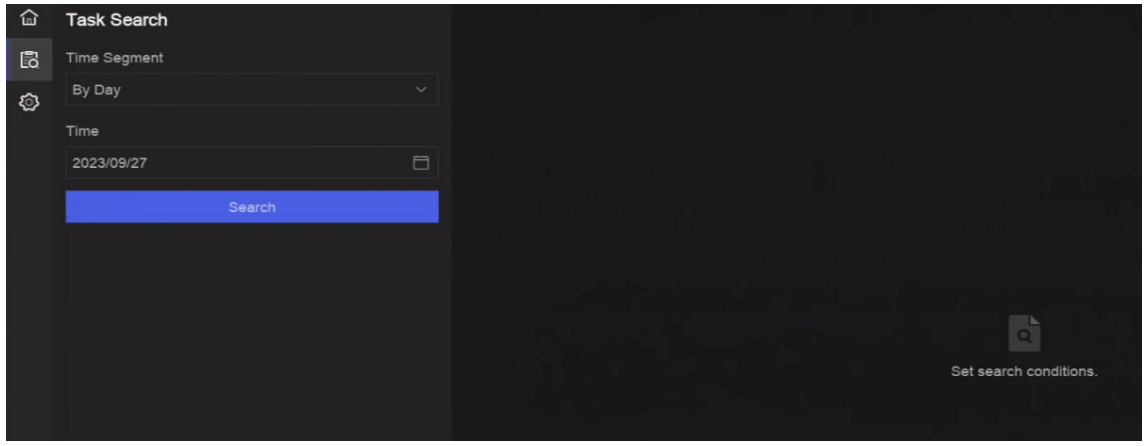


Figure 17-3 Search Check-In Records

4. Set time.
5. Click **Search**.

17.3 Statistic Report

You can view reports of people counting and heat map.

Table 17-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		• The function must be supported by the connected IP camera. For example, a people counting	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Function Name	Icon	Condition	Description
		camera is connected to your device. • Camera statistic data can be stored to the device HDD.	
Heat Map		• The function must be supported by the connected IP camera. • Camera statistic data can be stored to the device HDD.	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Chapter 18 System Parameter Settings

System parameters include device name, region, time, lock screen time, language, etc.

Go to **System → System Settings → System Configuration** to configure parameter.

Table 18-1 Parameter Description

Type	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Region & Time Configuration	Time Zone Lock	The admin password is required for this operation. After **Time Zone** is locked, the device time zone information cannot be remotely changed from other platforms or interfaces, such as the web interface via web browser. You can only lock or unlock **Time Zone** through local GUI interface.
	Time Sync Mode	• **NTP Time Sync**: You can select **NTP Time Sync** and configure **NTP Server**, **NTP Server Port**, **NTP Client Port,** and **Interval**. Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization. • **Manual Time Sync**: Manually set the system time. • **Hik-Connect Server Time Sync**: The device will sync time with Hik-Connect instead of NTP server. • **Guarding Vision Server Time Sync**:The device will sync time with Guarding Vision instead of NTP server.
	DST	DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

Type	Parameter Name	Description
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	**Console** After connecting it to PC with a convertor, PC can set the device parameters. **Transparent Channel** It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.

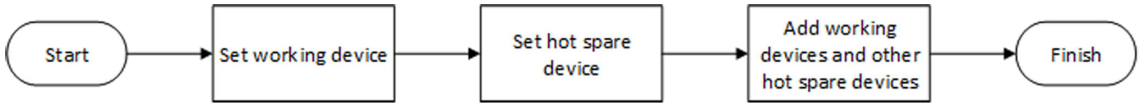


Figure 19-1 Build a Hot Spare System

Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

1. Go to **System → System Management → N+M Hot Spare** .
2. Set **Working Mode** as **Normal Mode**.
3. Turn on **Enable**.
4. Click **Save**.
5. **Optional:** View **Hot Spare Device IP Address** and **Hot Spare Device Working Status**.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

1. Go to **System → System Management → N+M Hot Spare** .
2. Set **Working Mode** as **Hot Spare Mode**.
3. Click **Save**. Your device will restart automatically.

Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to **System → System Management → N+M Hot Spare** again.
5. Add working devices to the hot spare system.
6. Add hot spare devices to the hot spare system.
7. Click **Save**.

Chapter 20 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System → System Settings → Exception** .

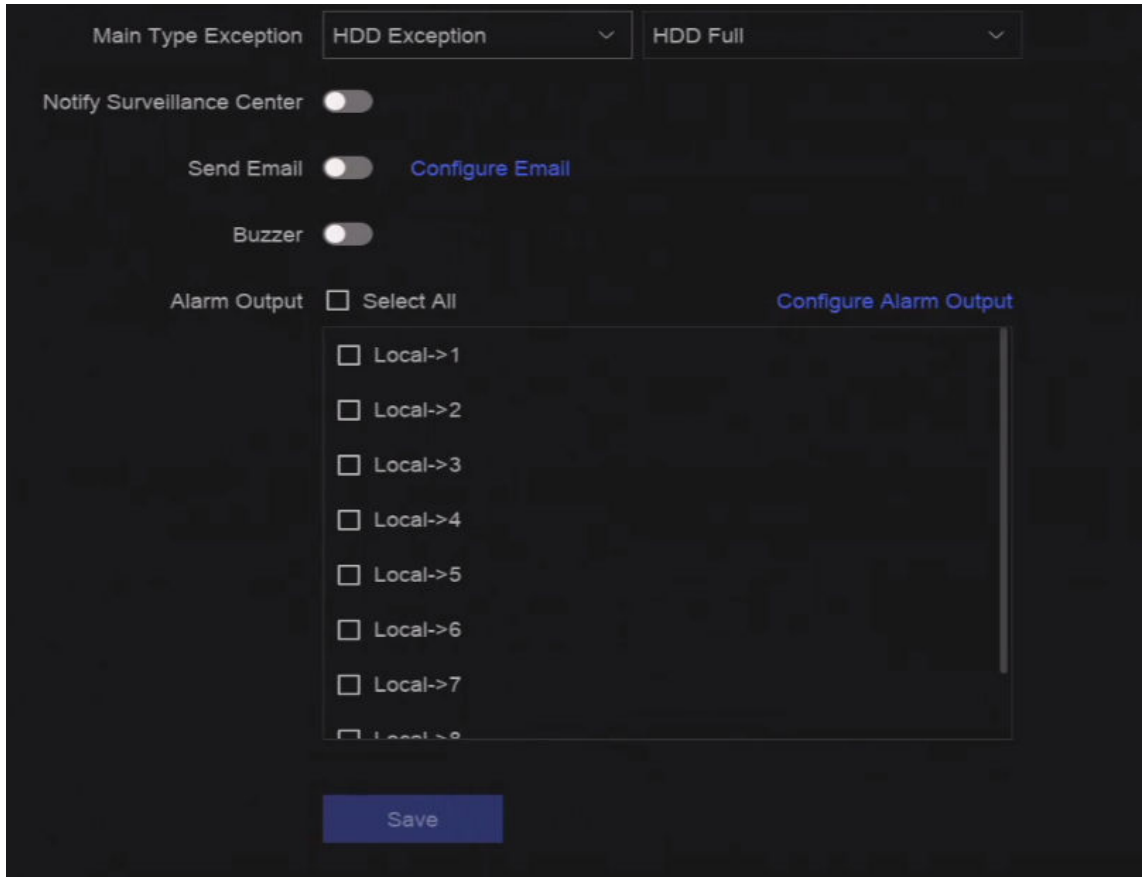


Figure 20-1 Exception Event Configuration

2. Select exception type.
3. Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

Note

When exception events occur, at the upper-right corner would notify, and you can click to view.

4. Click **Save**.

Chapter 21 View System Info

Go to **System → System Maintenance → Running Info → System Info** to view the system information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to **System → System Maintenance → Maintenance → Schedule Reboot** to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System → System Maintenance → Maintenance → Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System → System Maintenance → Maintenance → Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

The device configuration files can be exported to a local device for backup, and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Simple Restore

Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the device to the inactive status, and leave all settings unchanged except restoring user accounts.

22.4 Log Info

Go to **System → System Maintenance → Maintenance → Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

1. Go to **System → CX → System Settings → Network → Network → Log Server** .
2. Turn on **Enable**.
3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. **Optional:** Click **Test** to test if parameters are valid.
5. Click **Save**.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

1. Go to **System → System Maintenance → Maintenance → Maintenance Tools** .
2. Select tools according to your requirement.

Table 22-1 Tool Description

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	**Ping** The ping test is used to detect whether the destination IP address is reachable. **NIC Packet Capture**

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.

Note

It is recommended to use maintenance tools with the help of technical support.

22.7 Soft Power Off Configuration

Soft power off function is only available for devices with POWER-AC (AC power exception), POWER-UPS (UPS exceptioin), and POWER-UPSL (UPS low power) alarm outputs (at the real panel). The device can receive and record these alarms. When both POWER-AC and POWER-UPSL alarms are triggered, the device will automatically be powered off according to the preset time. When either POWER-AC or POWER-UPSL alarm is not triggered, the device will automatically be powered on.

Steps

1. Go to **System → System Maintenance → Maintenance → Soft Power Off Configuration**.

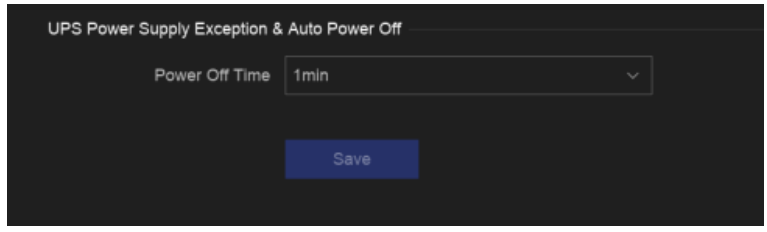


Figure 22-1 Soft Power Off Configuration

2. Set **Power Off Time**. The device would automatically power off after the preset time when corresponding alarms are triggered.
3. Click **Save**.

Example

For example, if **Power Off Time** is set as **1min**, when both POWER-AC (AC power exception) and POWER-UPSL (UPS low power) alarms are triggered, the device would automatically power off after 1 minute.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start
Log in with the admin account.

Steps
1. Go to **System → System Maintenance → Security Management → Address Filter** .
2. Turn on **Enable**.
3. Set **Filtering Type**. Choose to filter by IP address or MAC Address.
4. Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
5. **Optional:** Set **Restriction List**. You can add, edit or delete address.
6. Click **Save**.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps
1. Go to **System → System Maintenance → Security Management → Stream Encryption** .
2. Turn on **Enable**.
3. Set **Encryption Key**.

   Note
   The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.
4. Click **Save**.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to **System → System Maintenance → Security Management → TLS** to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 Glossary

Dual-Stream

Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

DDNS

Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

NVR

Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

   Note

   If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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.

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Table 24-1 Corrosive Gas Concentration Limit

Corrosive Gas Category	Average Value (mg/m^3)	Max. Value (mg/m^3)
SO_2 (Sulfur Dioxide)	0.3	1.0
H_2S (Hydrogen Sulfide)	0.1	0.5
Cl_2 (Chlorine)	0.1	0.3
HCl (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH_3 (Ammonia)	1.0	3.0
O_3 (Ozone)	0.05	0.1
NO_X (Nitrogen Oxides)	0.5	1.0

Note

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Table 24-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H_2S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO_2 (Sulfur Dioxide), SO_3 (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO_X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH_3 (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl_2 (Chlorine), ClO_2 (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O_3 (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C_nH_n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.

See Far, Go Further

UD43871B