



Network Video Recorder (AI Series)

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Table 1-1 Applicable Model

Series	Model
iDS-6700NXI-M1/AI(B)	iDS-6716NXI-M1/AI(B)
	iDS-6732NXI-M1/AI(B)
iDS-67000NXI-M1/AI	iDS-67064NXI-M1/AI
	iDS-67096NXI-M1/AI
	iDS-67128NXI-M1/AI
	iDS-67256NXI-M1/AI
iDS-9600NXI-M8/AI(B)	iDS-9632NXI-M8/AI(B)

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 ⚡ 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.

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

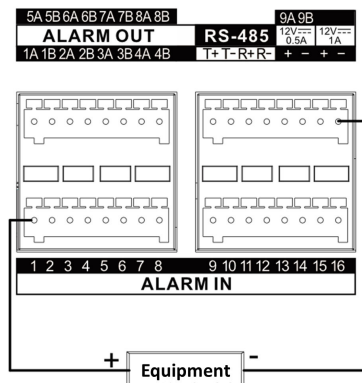
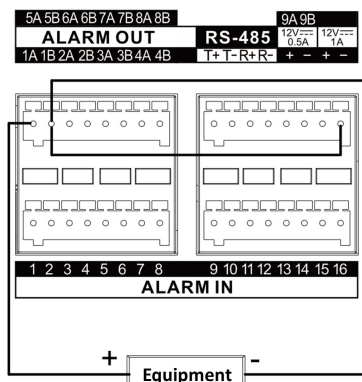
Indicator	Description
	The indicator turns on when device is powered up.
	The indicator flashes when data is being read from or written to HDD.
	The indicator flashes when network connection is functioning properly.

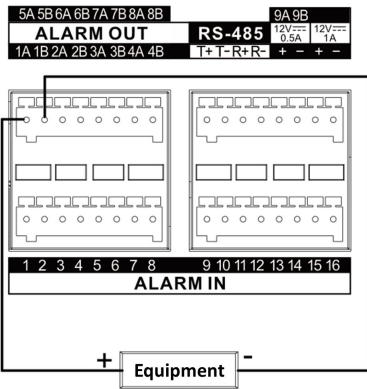
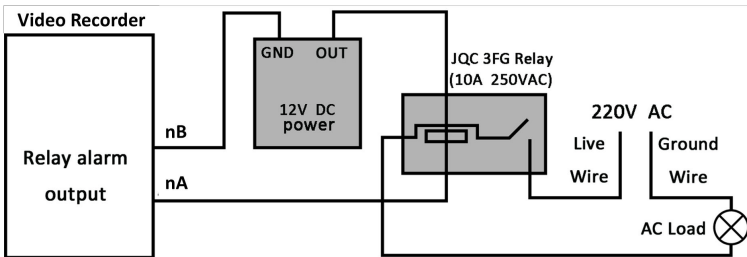
Interface Description

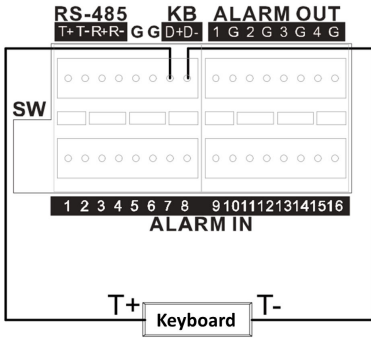
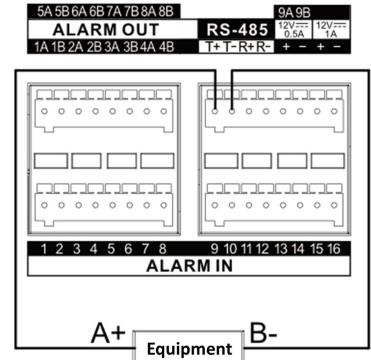
The panel interfaces vary with different models. Refer to the following table for common interface description.

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.
	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/ $\frac{12V}{0.5A}$	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
	5A 5B 6A 6B 7A 7B 8A 8B ALARM OUT 1A 1B 2A 2B 3A 3B 4A 4B 9A 9B RS-485 T+ T- R+ R- 12V 0.5A 12V 1A + - + - 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ALARM IN + Equipment -
DC 12V/ $\frac{12V}{1A}$	It provides 12 VDC and 1 A power output. Use the following diagram for reference. 5A 5B 6A 6B 7A 7B 8A 8B ALARM OUT 1A 1B 2A 2B 3A 3B 4A 4B 9A 9B RS-485 T+ T- R+ R- 12V 0.5A 12V 1A + - + - 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ALARM IN + Equipment -

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.

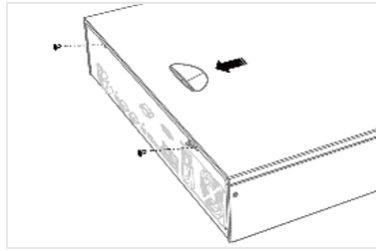


Figure 1-2 Remove Cover

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.

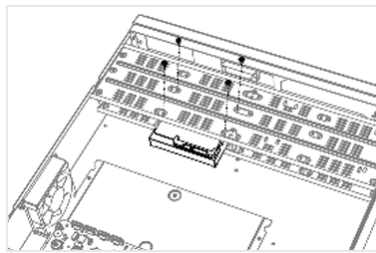


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

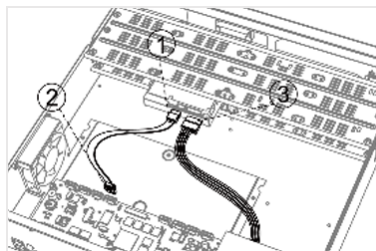


Figure 1-4 Connect Cable



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.

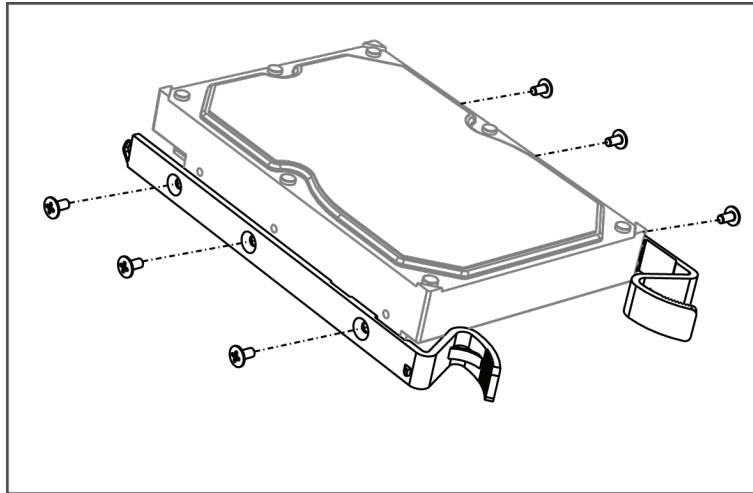


Figure 1-5 Fix Mounting Ears to HDD

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

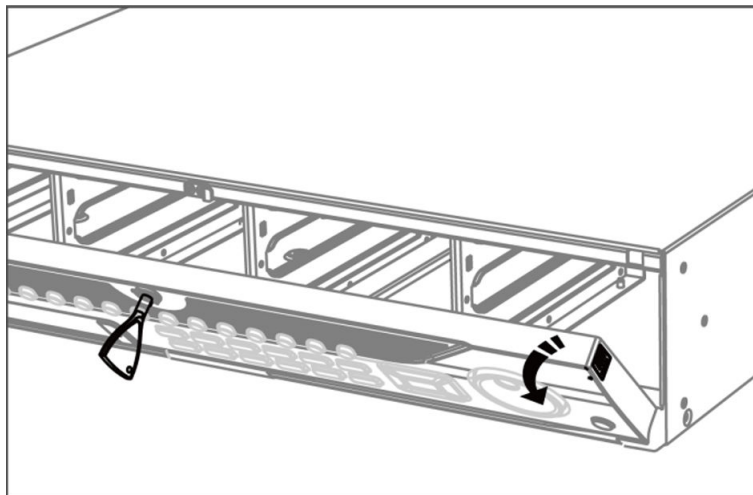


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

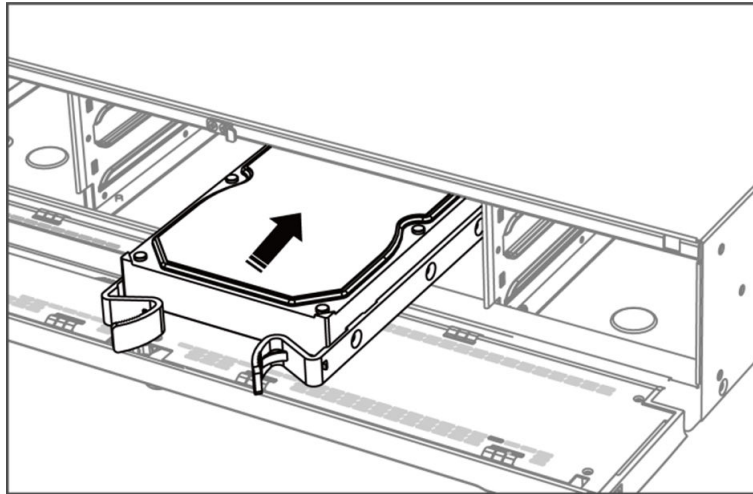


Figure 1-7 Insert HDD

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.

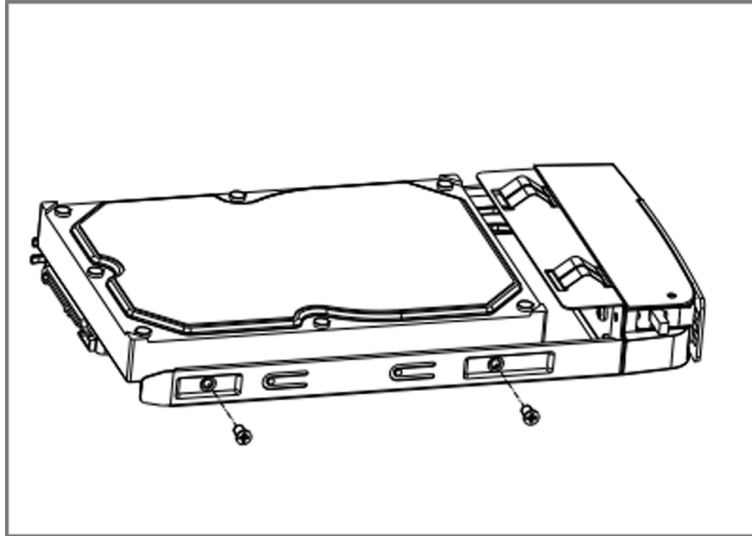


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

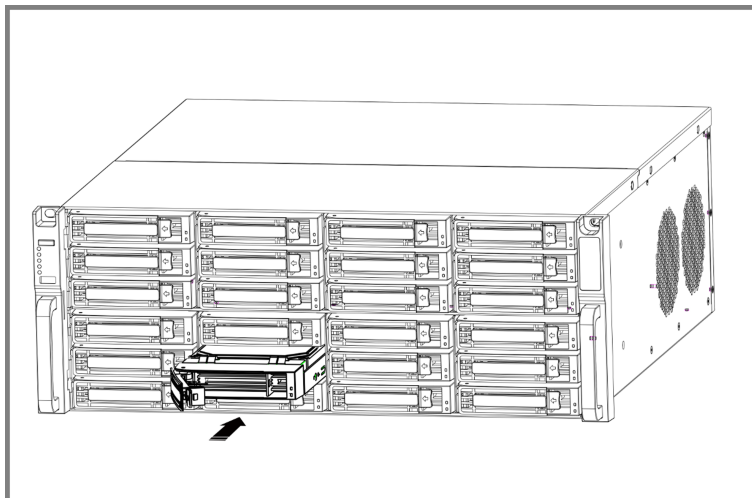


Figure 1-9 Push HDD Case into Slot

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.

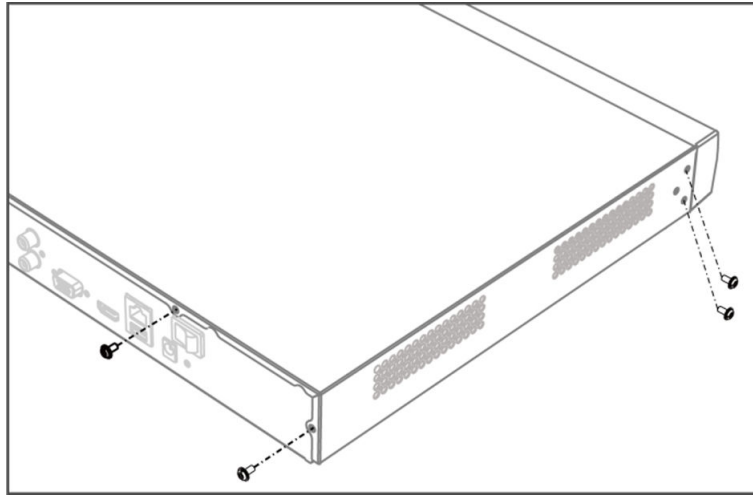


Figure 1-10 Remove Cover

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.

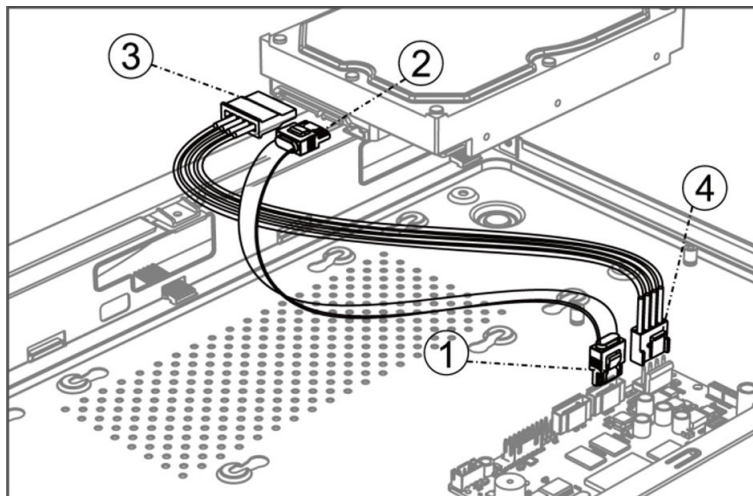


Figure 1-11 Connect Cables

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

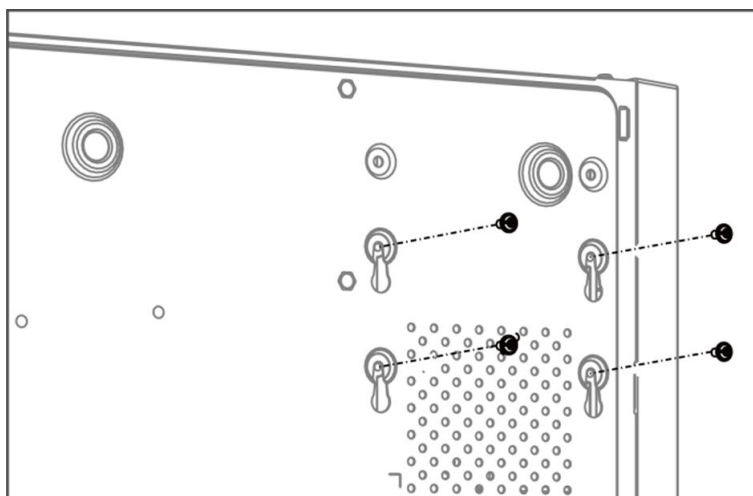


Figure 1-12 Fix HDD to Device Bottom

- 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. Use tweezers to push the metal latch at the middle from its inside, and the battery would automatically pop up.

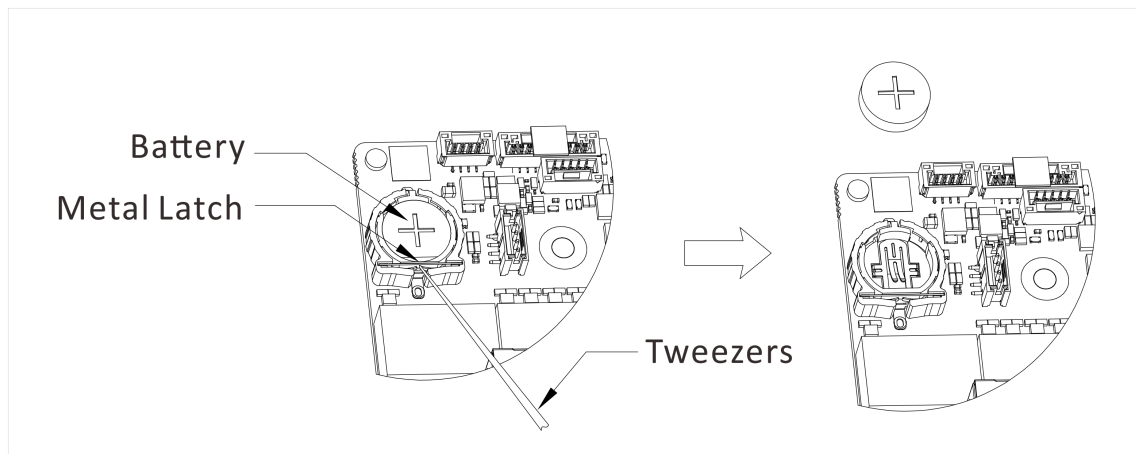


Figure 1-1 Remove Battery

4. Take out the old battery and press a new battery with the same model in to the battery slot.

Note

The battery positive terminal (+ identifies the positive terminal) should be placed upward.

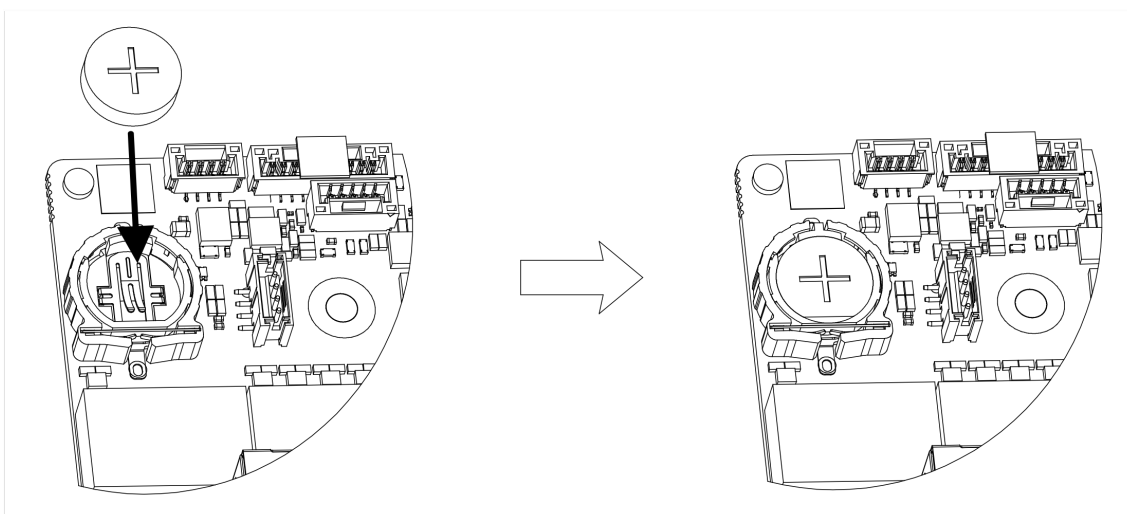


Figure 1-2 Replace Battery

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
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP	11
4.2.3 Configure ISUP	11
4.2.4 Configure SDK Service	13
4.2.5 Enable ISAPI	13
4.2.6 Configure ONVIF	14
4.2.7 Configure Log Server	15
4.3 Network Service Settings	15
4.3.1 Configure HTTP(S)	15
4.3.2 Configure RTSP	16
4.3.3 Configure WebSocket(s)	17
4.3.4 Configure Port Mapping (NAT)	17
Chapter 5 User Management	20
Chapter 6 Device Access	21
6.1 Access Video Device	21
6.1.1 Add Automatically Searched Online Network Camera	21

6.1.2 Add Network Camera Manually	21
6.1.3 Add Network Camera through PoE	23
6.1.4 Add Solar-Powered Camera through OTAP Protocol	23
6.1.5 Add Network Camera via Custom Protocol	24
6.1.6 Add Network Camera through Camera Configuration File	25
6.2 Add Access Control Device	25
6.3 Add Audio Device	25
6.4 Add POS Device	26
6.5 Channel Management	27
Chapter 7 Device Grouping	28
Chapter 8 Video or Audio Device Settings	29
8.1 Enable H.265 Stream Access	29
8.2 Display Settings	29
8.3 Configure Video Parameters	30
8.4 Configure Privacy Mask	30
8.5 Configure Audio Parameter	31
8.6 Configure OTAP Service	31
8.7 Batch Configuration	32
8.8 Configure PoE (Power over Ethernet) Interface	33
Chapter 9 Storage Management	34
9.1 Manage HDD	34
9.2 RAID Configuration	35
9.2.1 Create Disk Array	35
9.2.2 Rebuild Array	37
9.2.3 Delete Array	37
9.2.4 View Firmware Info	38
9.3 Configure Storage Mode	38
9.4 Configure Other Storage Parameters	38

9.5 Mange USB Flash Drive	39
Chapter 10 Schedule Configuration	40
10.1 Configure Schedule Template	40
10.2 Configure Recording Schedule	42
10.3 Configure Picture Capture Schedule	44
10.4 Configure Audio Recording	46
Chapter 11 Live View	47
11.1 Configure Live View Layout	47
11.2 GUI Introduction	47
11.3 PTZ Control	48
Chapter 12 Playback	50
12.1 GUI Introduction	50
12.2 Normal Playback	52
12.3 Event Playback	52
12.4 Slice Playback	53
12.5 Sub-Period Playback	53
Chapter 13 Event Center	55
13.1 Event Settings	55
13.1.1 Basic/Generic Event	55
13.1.2 Perimeter Protection	57
13.1.3 Abnormal Behavior Event	68
13.1.4 Target Event	70
13.1.5 Thermal Camera Detection	73
13.1.6 Alarm Input Event	75
13.1.7 Audio Analysis Event	77
13.2 Linkage Configuration	78
13.3 Disarming Configuration	79
13.4 Batch Configuration	80

13.5 Event Search	81
13.6 View Alarms	82
Chapter 14 Search and Backup	83
Chapter 15 AcuSearch	85
Chapter 16 Intelligent Management (VCA)	87
16.1 Task Management	87
16.1.1 Import Application	87
16.1.2 Advanced Configuration	87
16.1.3 Task Configuration	88
16.2 Large Model (Ultra-High-Precision Algorithm) Configuration	91
16.2.1 Picture Analysis Mode	91
16.2.2 Secondary Analysis Mode	92
16.3 Algorithm Management	93
16.4 Engine Status	95
16.4.1 View Engine Status	95
16.4.2 View Resource Status for Secondary Analysis	96
16.5 Data Archive	97
16.5.1 Comparison Library of Searching	97
16.5.2 Registration and Comparison Library	97
16.5.3 Picture Comparison Library	98
16.5.4 Calibration Library	98
16.5.5 List Library (Face Picture Library)	100
16.5.6 Audio Management	100
16.6 Rule Type Description	100
16.7 Built-In Algorithm Description	102
16.7.1 Safety Helmet and Reflective Clothing Detection	102
16.7.2 Smoking and Making Phone Calls	104
16.7.3 Fire Escape Occupation Detection	105

16.7.4 Non-Motor Vehicle Detection	106
16.7.5 Gun Detection	108
16.7.6 Workwear Regist Compare	109
16.7.7 Motor Vehicle Detection	111
16.7.8 Abnormal Street Event Detection	112
16.7.9 Fire and Smoke Detection	113
16.7.10 People Counting	114
16.7.11 Facial Recognition	115
16.7.12 Perimeter Protection	115
Chapter 17 System Parameter Settings	116
Chapter 18 Hot Spare Device Backup	117
18.1 Set Working Device	117
18.2 Set Hot Spare Device	117
Chapter 19 Configure Exception Event	119
Chapter 20 View System Info	121
Chapter 21 System Maintenance	122
21.1 Schedule Reboot	122
21.2 Upgrade Device	122
21.3 Backup and Restore	122
21.4 Log Info	123
21.5 Configure Log Server	123
21.6 Maintenance Tools	123
Chapter 22 Security Management	125
22.1 Address Filter	125
22.2 Stream Encryption	125
22.3 Select TLS Version	125
Chapter 23 Appendix	126
23.1 List of Applicable Power Adapter	126

23.2 Glossary	127
23.3 Frequently Asked Questions	128
23.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?	128
23.3.2 Why is the video recorder notifying risky password after a network camera is added?	129
23.3.3 Why is the video recorder notifying the stream type is not supported?	129
23.3.4 How to confirm the video recorder is using H.265 to record video?	129
23.3.5 Why is the video recorder notifying IP conflict?	129
23.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?	130
23.3.7 Why is the device not able to control PTZ camera via coaxitron?	130
23.3.8 Why does the PTZ seem unresponsive via RS-485?	130
23.3.9 Why is the video sound quality not good?	130
23.4 Notification for Corrosive Gas	131

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.

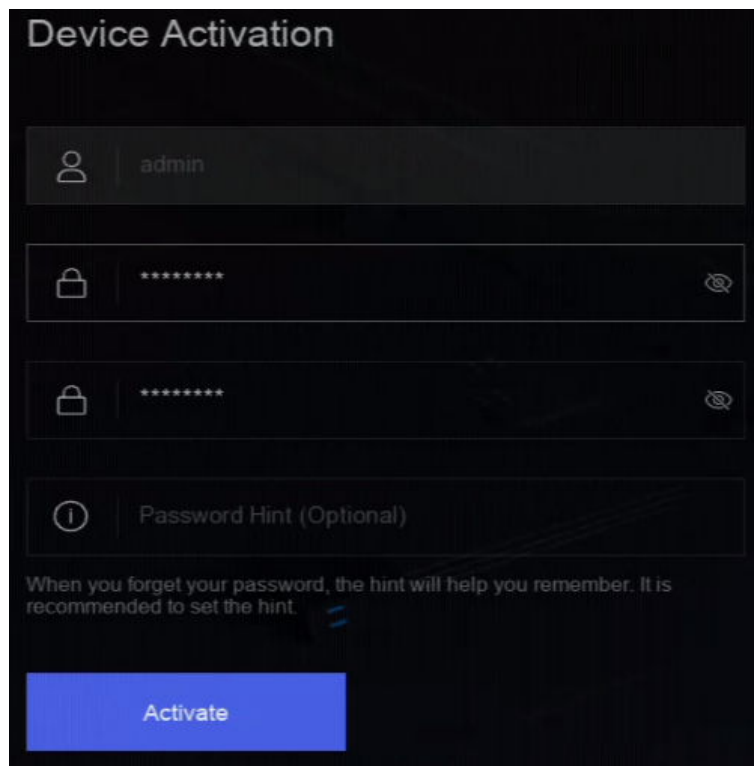
Steps

1. Power on your device.
2. Select a system language.
3. 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.



The image shows a 'Device Activation' screen with a dark background. At the top, the title 'Device Activation' is displayed. Below it, there are three input fields. The first field is for the username, with a person icon and the text 'admin'. The second and third fields are for passwords, each with a lock icon and masked text '*****'. To the right of each password field is an eye icon to toggle visibility. Below the password fields is a field for a 'Password Hint (Optional)' with an information icon. A note below this field states: 'When you forget your password, the hint will help you remember. It is recommended to set the hint.' At the bottom of the screen is a large blue button labeled 'Activate'.

Figure 1-1 Activate via Local Menu

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



Note

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

-
6. **Optional:** Draw an unlock pattern.
 7. 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.

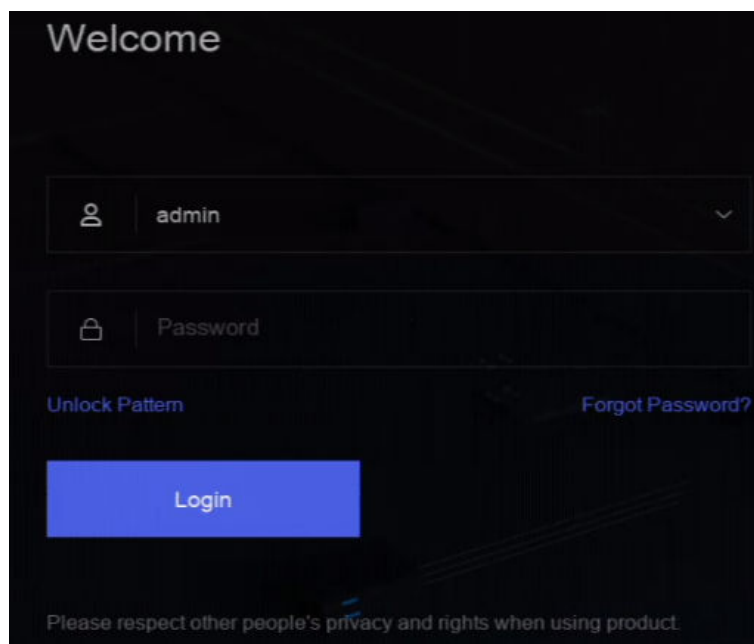


Figure 2-1 Login

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.

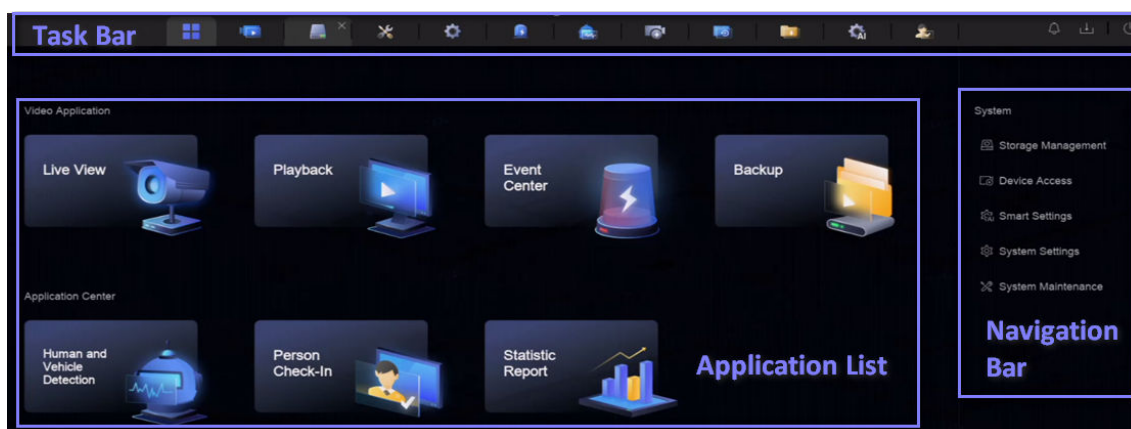


Figure 3-1 Main Function Page

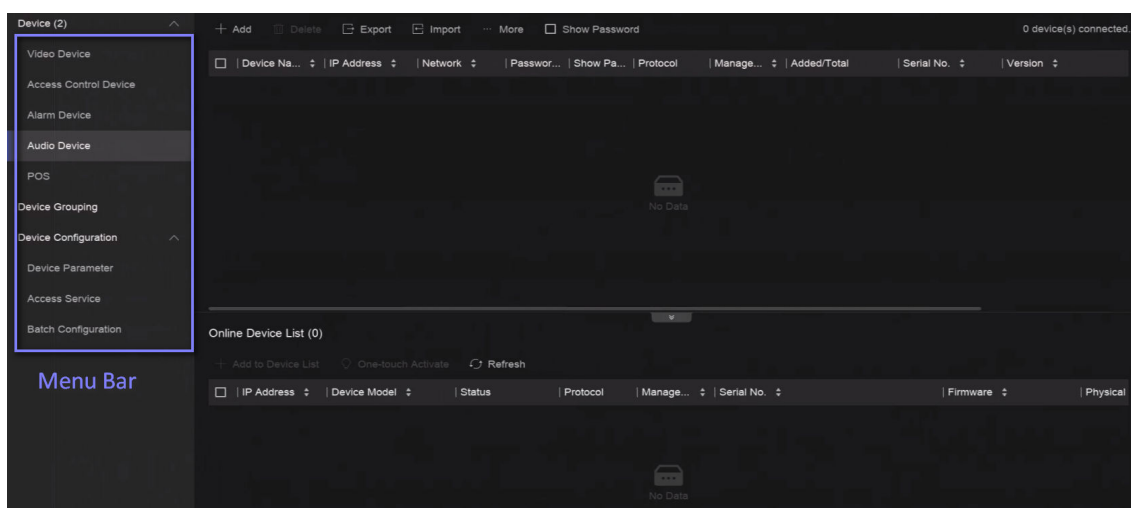


Figure 3-2 Menu Bar Example

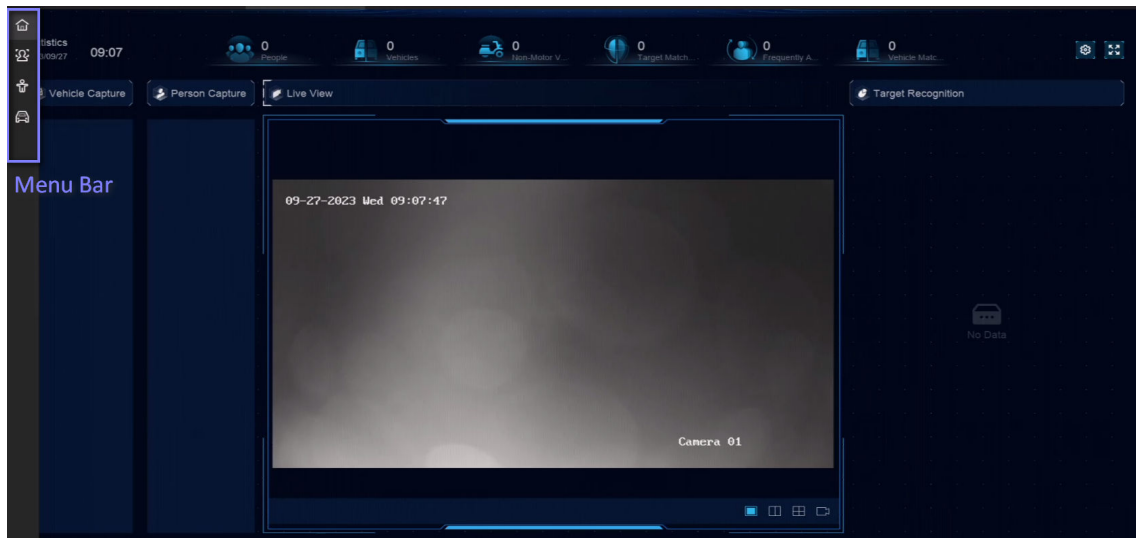


Figure 3-3 Human and Vehicle Detection Example of Application Center

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** .

The screenshot shows the TCP/IP configuration page. On the left, under 'Working Mode', 'Select NIC', and 'NIC Type' are dropdown menus. Below them are 'IPv4' and 'IPv6' buttons, with 'IPv4' being active. Further down are a 'DHCP' toggle switch (turned on), and input fields for 'IPv4 Address', 'IPv4 Subnet Mask', 'IPv4 Default Gateway', 'MAC Address', and 'MTU(Bytes)' (pre-filled with 1500). On the right, the 'DNS Server Settings' section has an 'Auto Obtain DNS Server' toggle (turned on), empty fields for 'Preferred DNS Server' and 'Alternate DNS Server', and a 'Main NIC' dropdown menu set to 'LAN1'. A 'Save' button is at the bottom left.

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** .

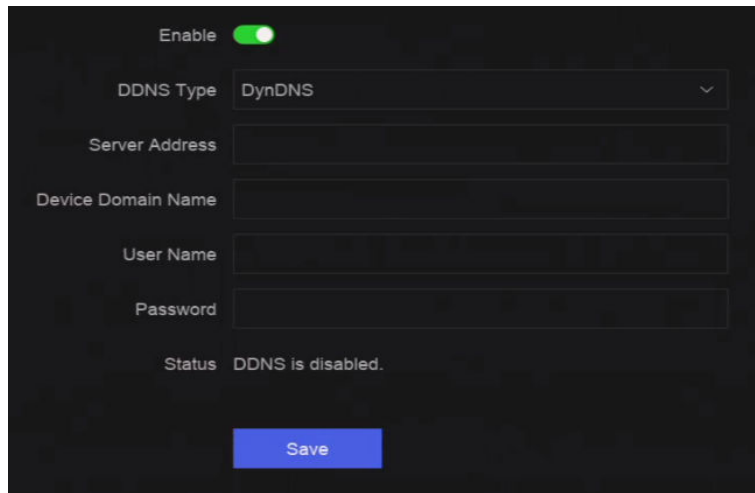


Figure 4-2 DDNS

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**.

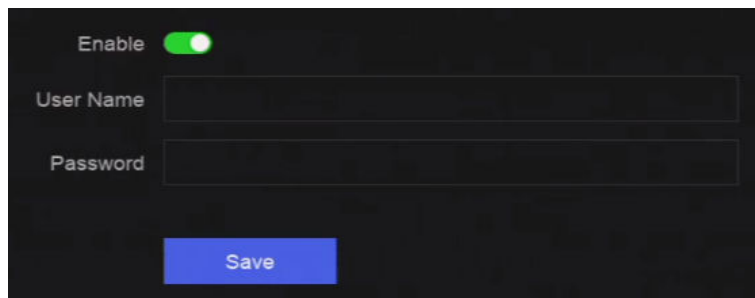


Figure 4-3 PPPoE

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**.

4.2 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**.

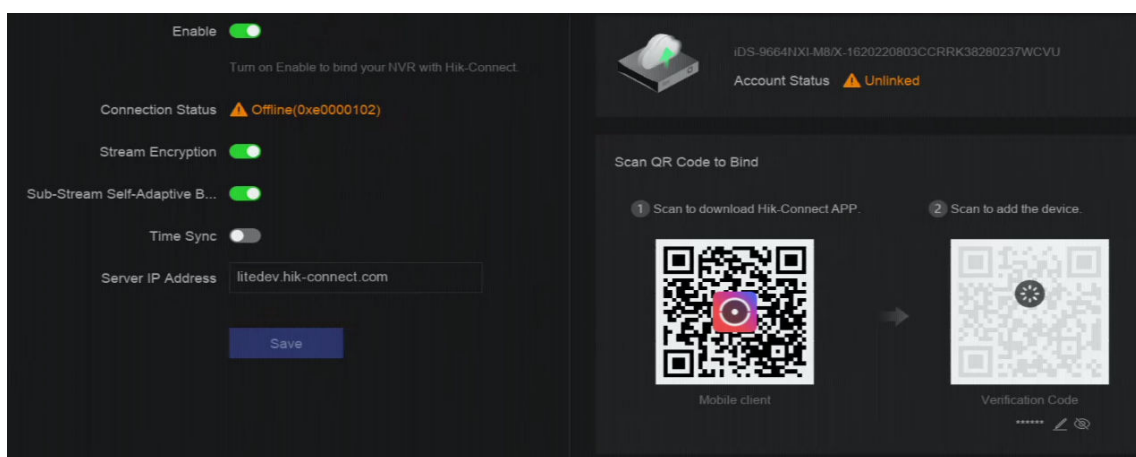


Figure 4-4 Hik-Connect

2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Click  to set verification code.
5. **Optional:** Enable **Stream Encryption**, **Sub-Stream Self-Adaptive Bitrate**, **Time Sync**, or edit server IP address.

Stream Encryption

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

Sub-Stream Self-Adaptive Bitrate

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

Time Sync

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

6. 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

7. 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.

8. Click **Save**.

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

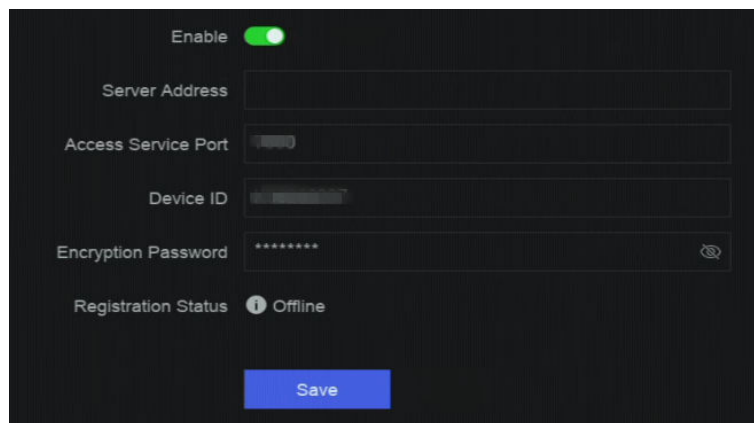
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

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



The screenshot shows the OTAP configuration page. At the top, there is an 'Enable' toggle switch which is turned on (green). Below it are four input fields: 'Server Address', 'Access Service Port', 'Device ID', and 'Encryption Password'. The 'Registration Status' is indicated as 'Offline' with an information icon. At the bottom, there is a blue 'Save' button.

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** .

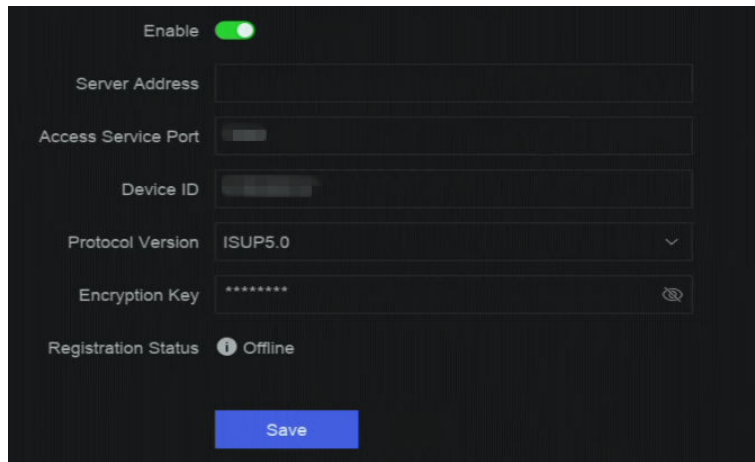


Figure 4-7 ISUP

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**.

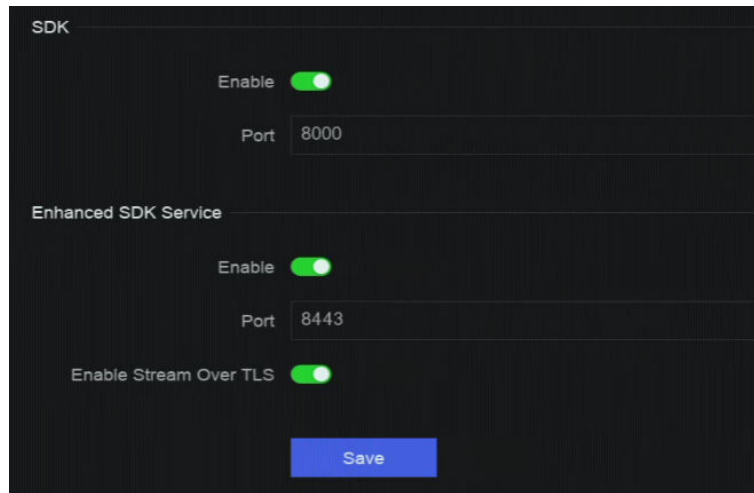


Figure 4-8 SDK Service

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** .

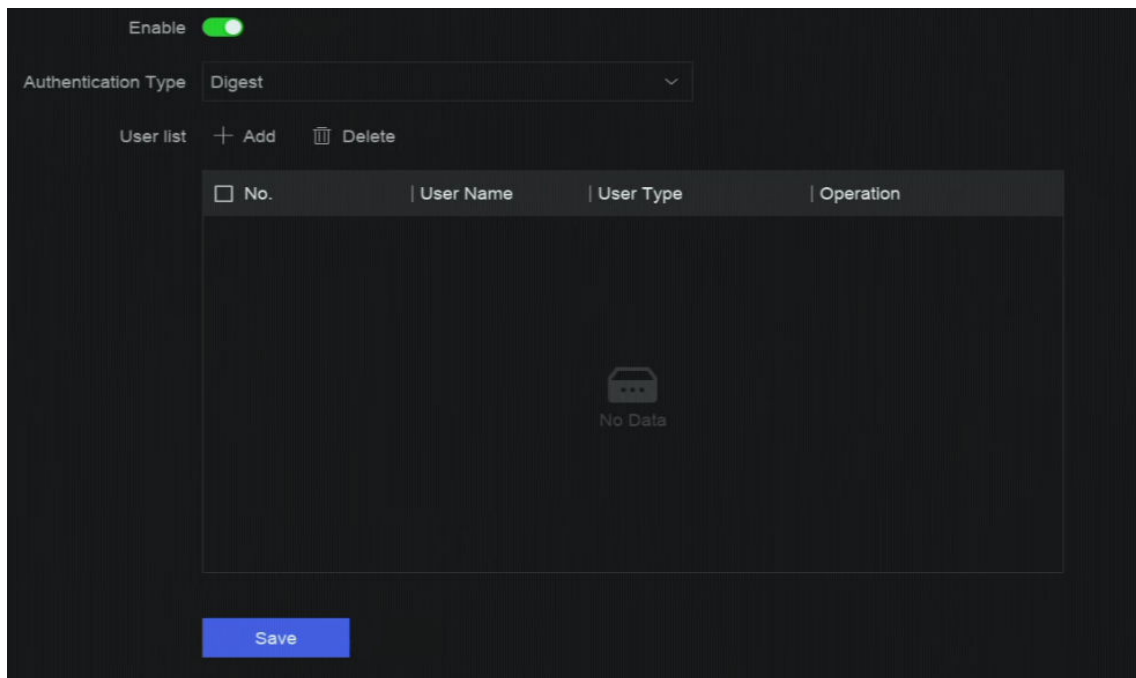


Figure 4-9 ONVIF

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

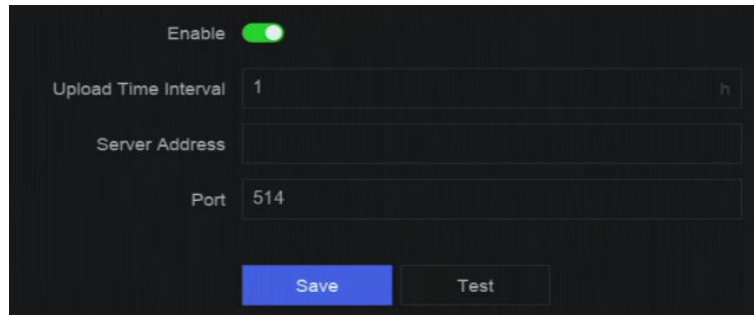
6. Click **Save**.

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**.



The screenshot shows a dark-themed configuration window for the Log Server. At the top, there is a toggle switch labeled 'Enable' which is currently turned on (green). Below this, there are three input fields: 'Upload Time Interval' with a value of '1' and a unit 'h', 'Server Address' which is empty, and 'Port' with a value of '514'. At the bottom of the window, there are two buttons: 'Save' (highlighted in blue) and 'Test'.

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)**.

The screenshot shows the configuration interface for HTTP and HTTPS services. It is divided into three main sections: HTTP, HTTPS, and HTTP/HTTPS Authentication. In the HTTP section, the 'Enable' toggle is turned on (green), and the 'Port' is set to 80. In the HTTPS section, the 'Enable' toggle is also turned on (green), with a note 'Ensure the client TLS version is enabled.' and a link to 'TLS Settings'. The 'Port' for HTTPS is set to 443. Below this, the 'Enable HTTPS Browsing' toggle is turned off (grey). The 'HTTP/HTTPS Authentication' section shows 'Authentication Type' set to 'Digest' and 'Digest Algorithm' set to 'MD5'. A note states 'Authentication type and digest algorithm are valid for both HTTP and HTTPS.' At the bottom, there is a blue 'Save' button.

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**.

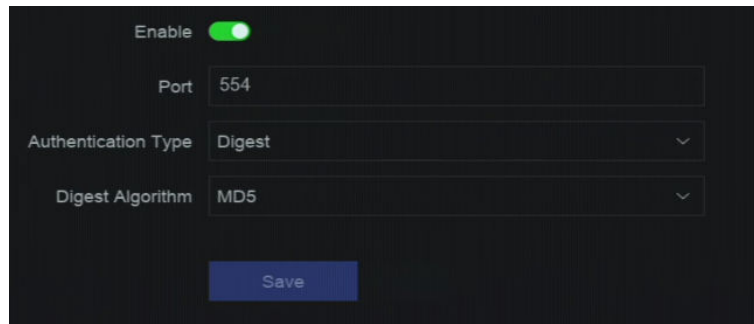


Figure 4-12 RTSP

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**.

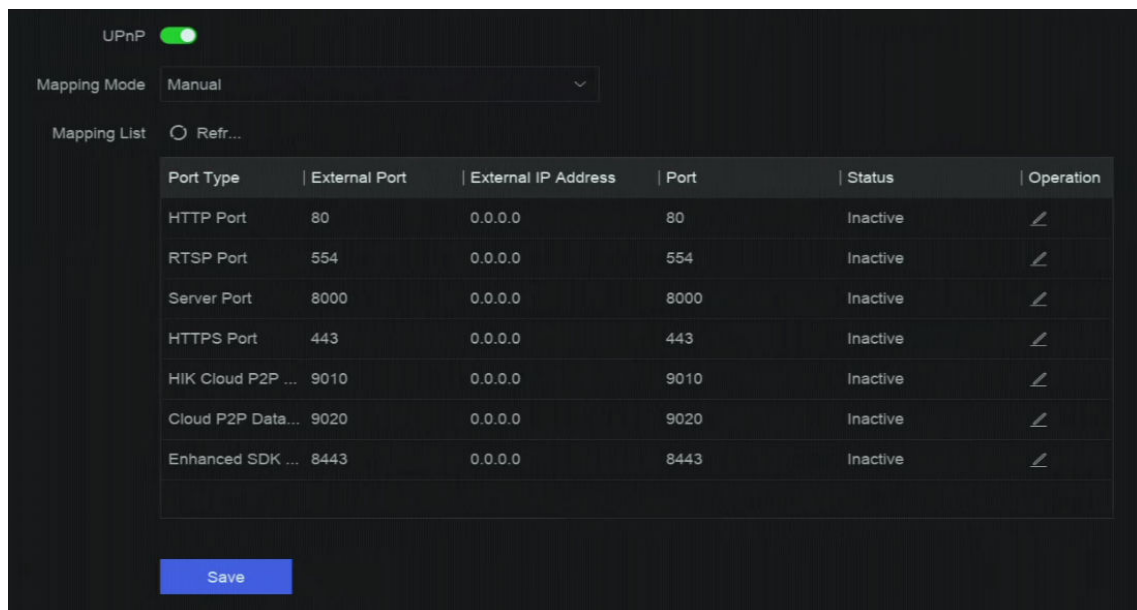


Figure 4-13 Port Mapping (NAT)

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.

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** .

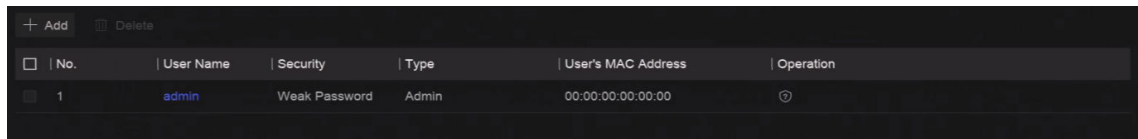


Figure 5-1 User Management

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.

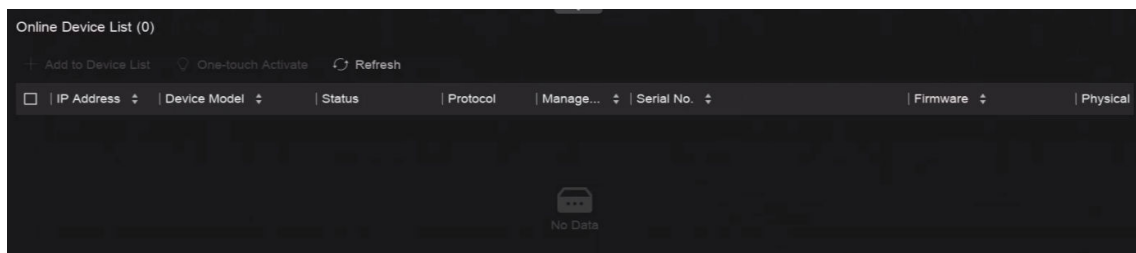


Figure 6-1 Add Automatically Searched Online Network Camera

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.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- 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**.

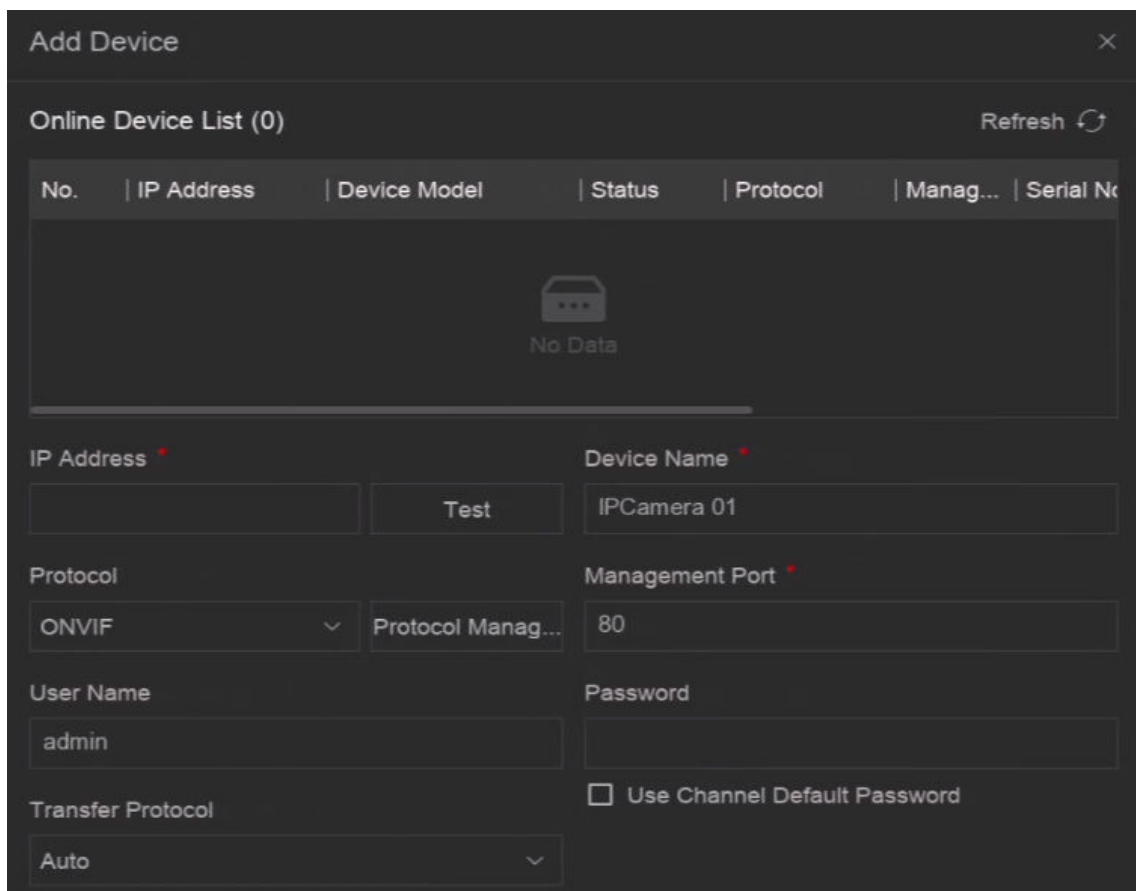


Figure 6-2 Add Network Camera Manually

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**.

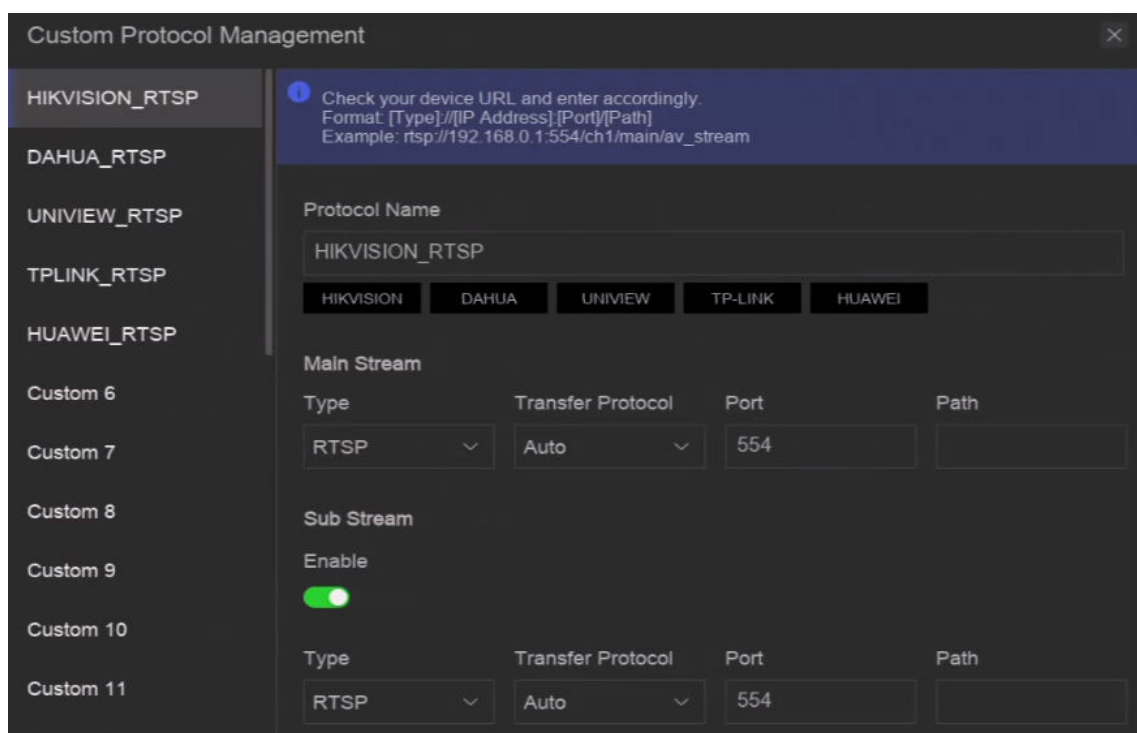


Figure 6-3 Add Network Camera via Customized Protocol

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 Audio Device

Audio devices can be added to your video recorder.

The adding process is similar with [Access Video Device](#).

6.4 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.

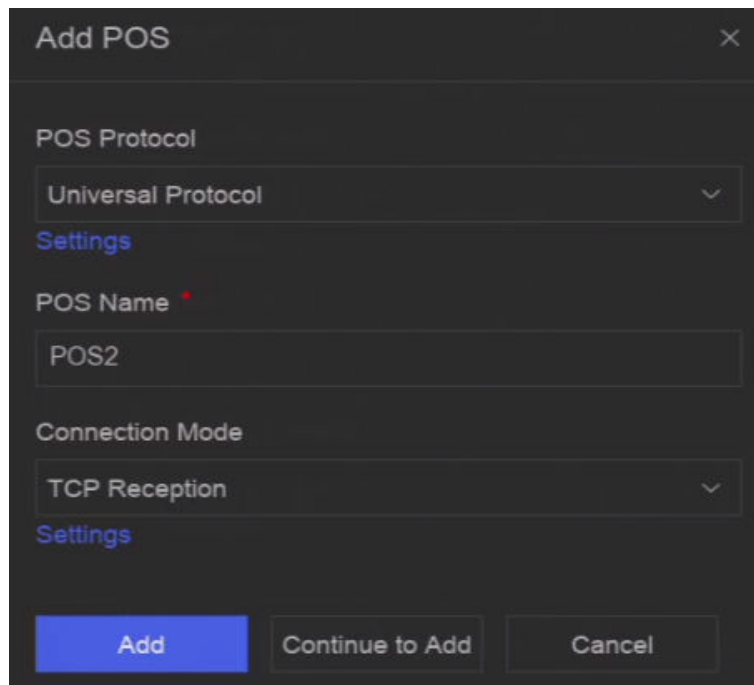


Figure 6-4 Add POS Device

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.

6.5 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** .

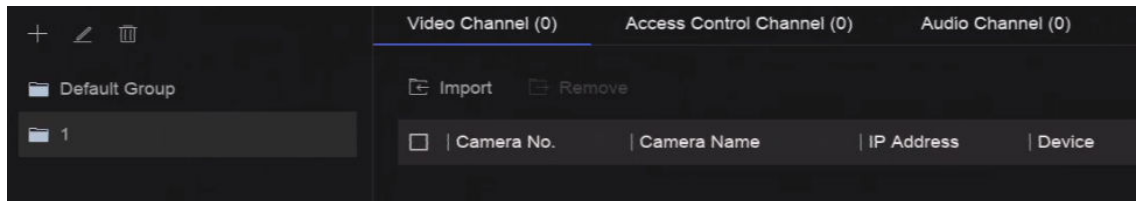


Figure 7-1 Device Grouping

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 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 → 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

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 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 → Privacy Mask** .

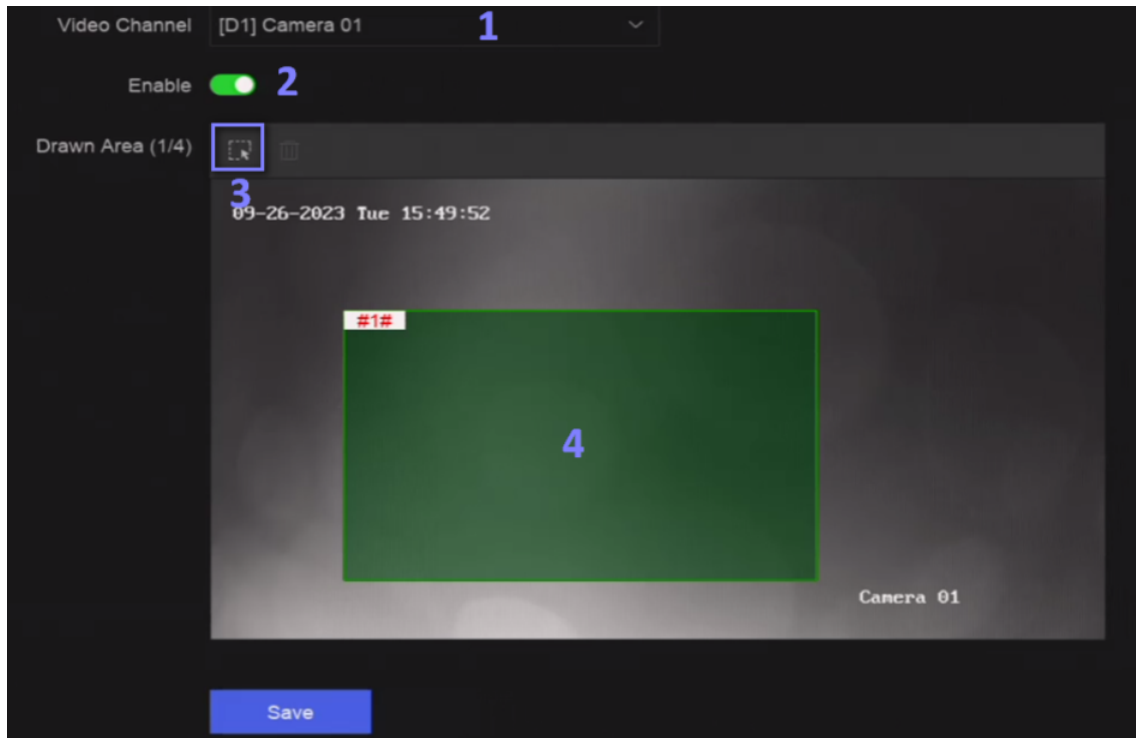


Figure 8-1 Privacy Mask

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 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.

8.6 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**.

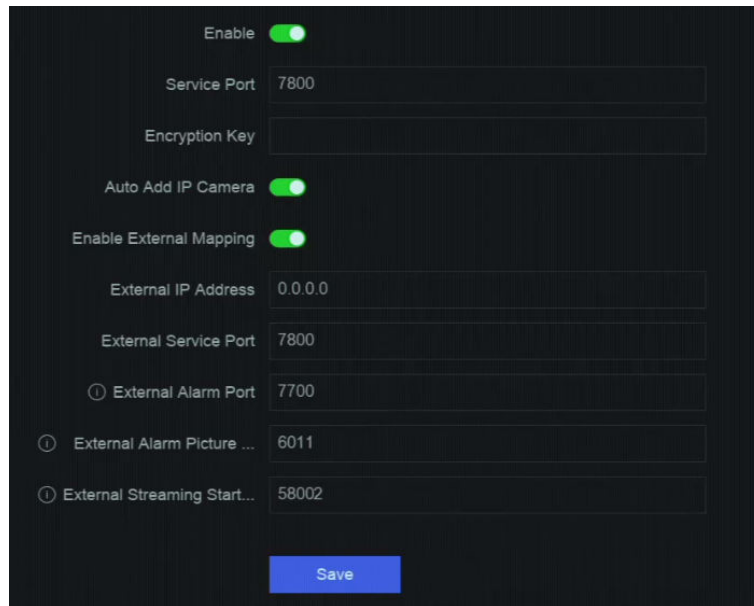


Figure 8-2 Configure OTAP Service

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

8.7 Batch Configuration

Cameras can be configured in a batch.

Steps

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

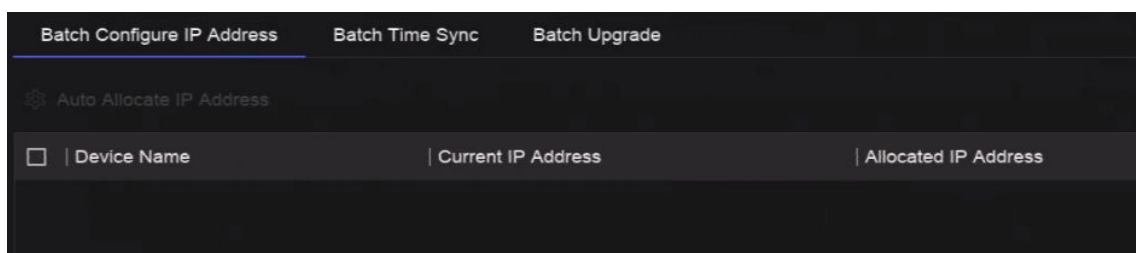


Figure 8-3 Batch Configuration

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

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

8.8 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

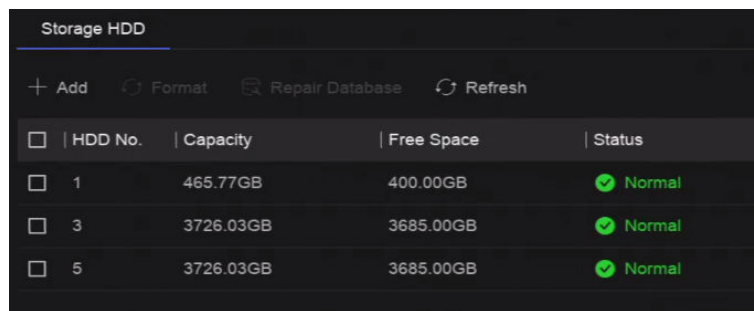
A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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



Storage HDD				
+ Add Format Repair Database Refresh				
☐	HDD No.	Capacity	Free Space	Status
☐	1	465.77GB	400.00GB	✓ Normal
☐	3	3726.03GB	3685.00GB	✓ Normal
☐	5	3726.03GB	3685.00GB	✓ Normal

Figure 9-1 Manage HDD

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

Add Add a network HDD.

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**.

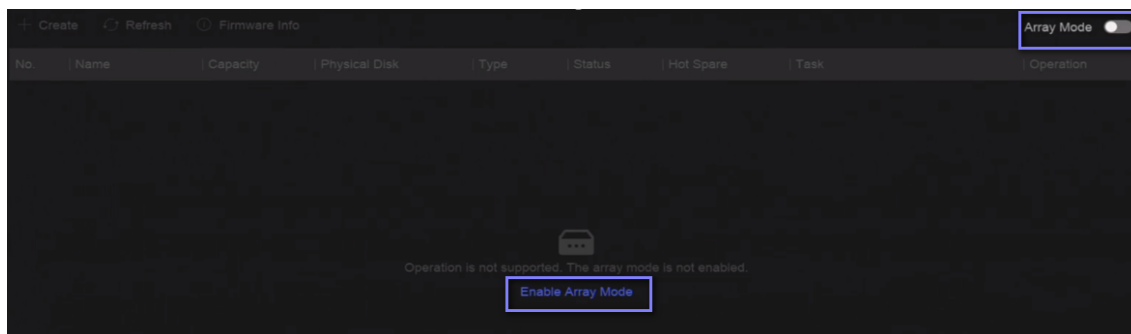


Figure 9-2 Enable RAID

3. Wait for the device to restart.

4. Go to **System → Storage Management → Storage HDD → Array Management** again.

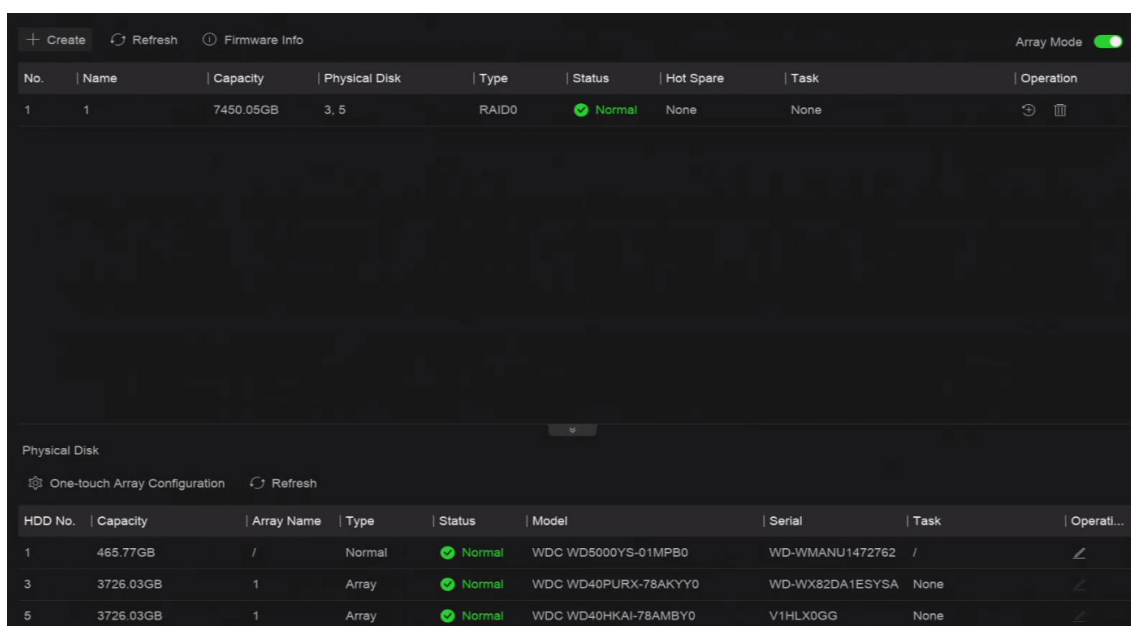


Figure 9-3 Array Management

5. Create an array.

Creation Method

One-touch Array Configuration

Description

Click **One-touch Array Configuration**.



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** .

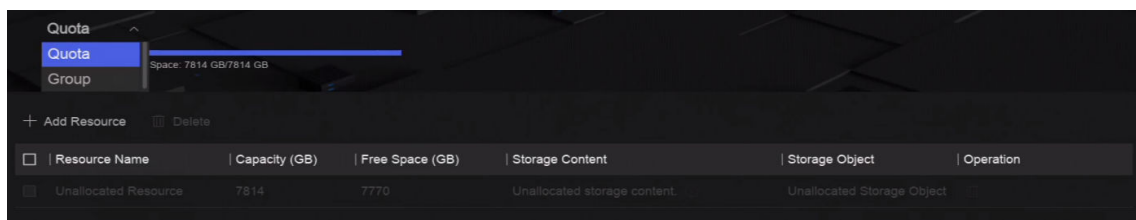


Figure 9-4 Storage Mode

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 Other Storage Parameters

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

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	When the HDD is not used for a period, it will turn to sleep.
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. Time for Clip Export	When videos are exported from the device, package time means the video duration of each video package file.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.
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.

9.5 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**.

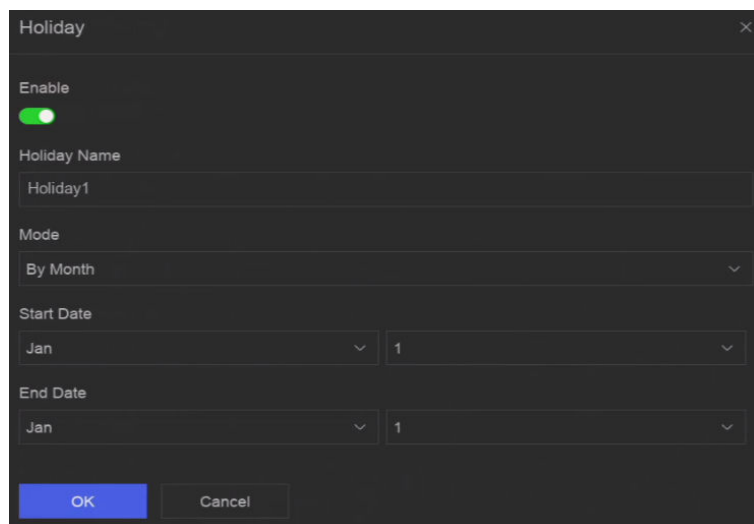


Figure 10-1 Add Holiday

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.

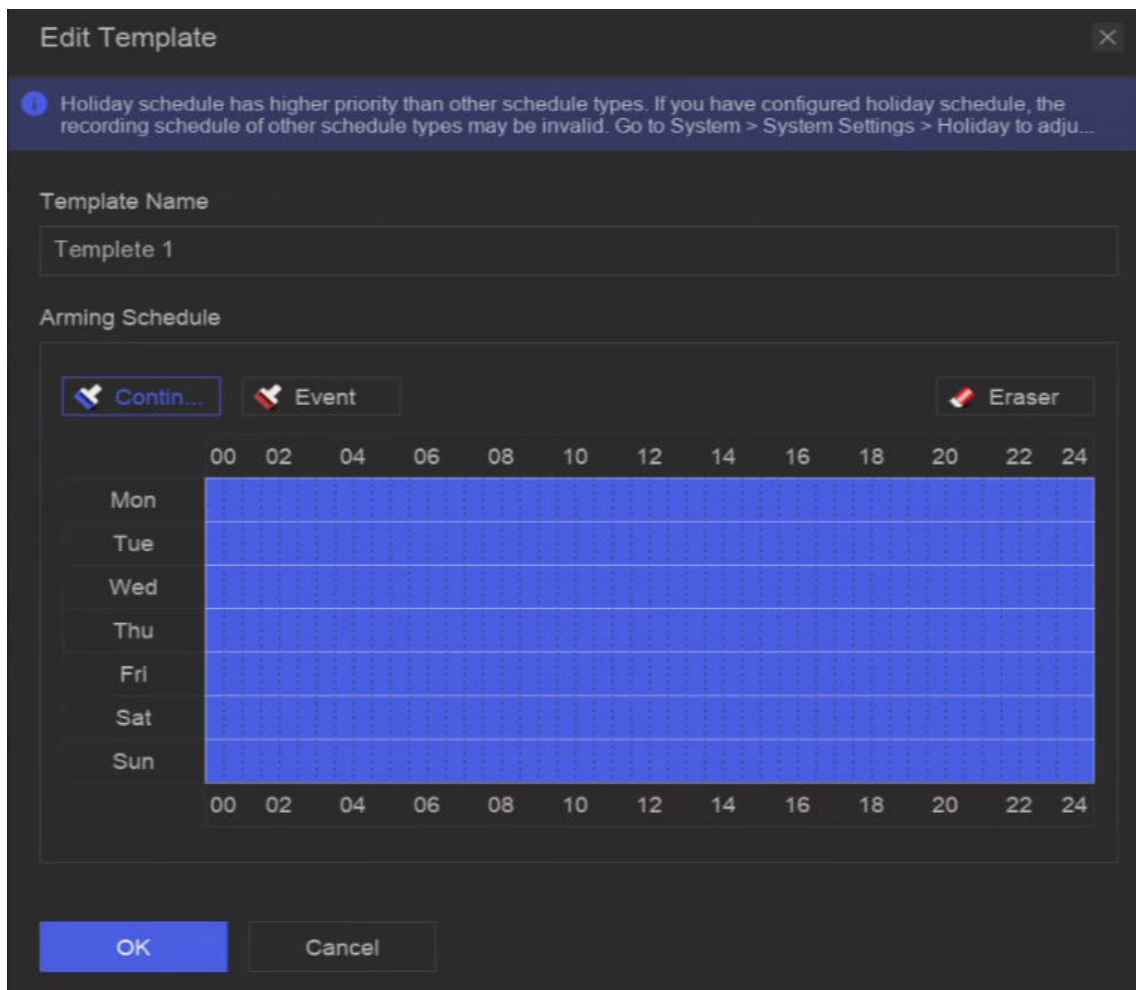


Figure 10-2 Edit Template

- 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** .

 Batch Schedule Configuration

 Batch Advanced Configuration

 Configure Template

☐	Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
☐	[D1] Camera 01		Custom	View	
☐	[D2] IPCamera 02		Custom	View	
☐	[D3] IPCamera 03		Custom	View	
☐	[D4] IPCamera 04		Custom	View	

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.

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

10.3 Configure Picture Capture Schedule

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

Steps

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

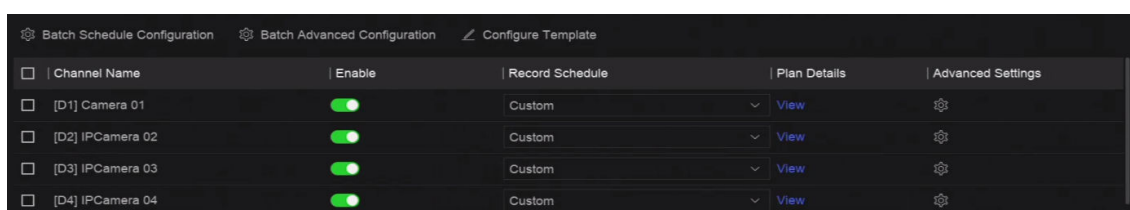


Figure 10-5 Picture Capture Configuration

- Turn on **Enable** for a camera.
- 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.

- 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  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 .
6. Set the live view image output interface. You can drag a channel from the channel list to a window, or 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

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.
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.

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  .

Task	Description	Operation
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.

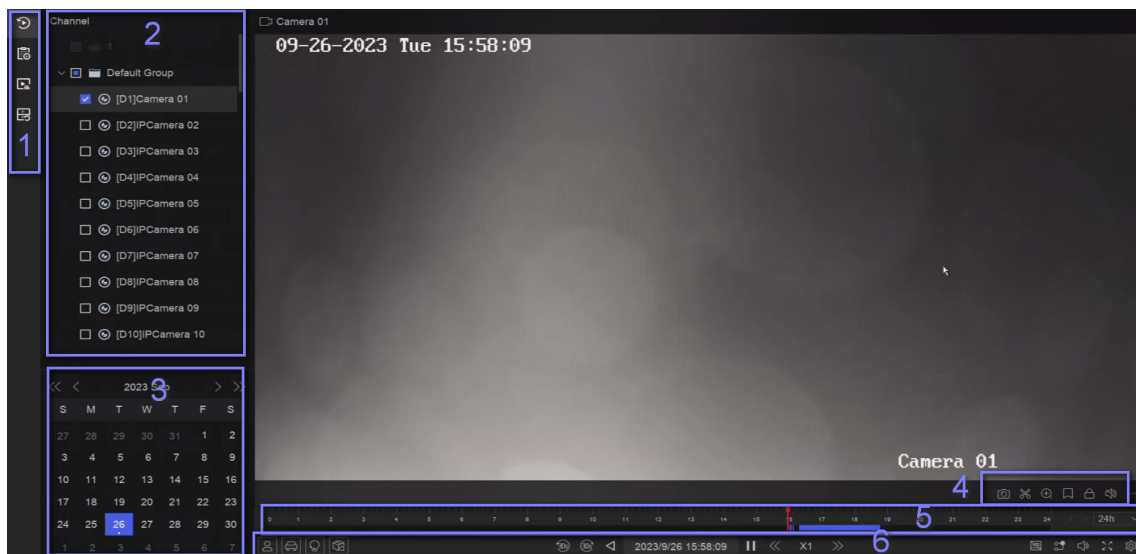


Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	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. - 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.

No.	Description
	- 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 In order 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. - You can select  → Show VCA Info to display rule frames.
5	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.
6	Playback tool bar. - 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  to set normal video and smart video (the video that contains smart data) playback strategy. - Click  to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. - Click  to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

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.



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

3. Select a date in the calendar.



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

4. **Optional:** Play back videos that contain human or vehicle targets.
 -  : Videos that contain human would be marked in red.
 -  : Videos that contain vehicle would be marked in red.

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.



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**.

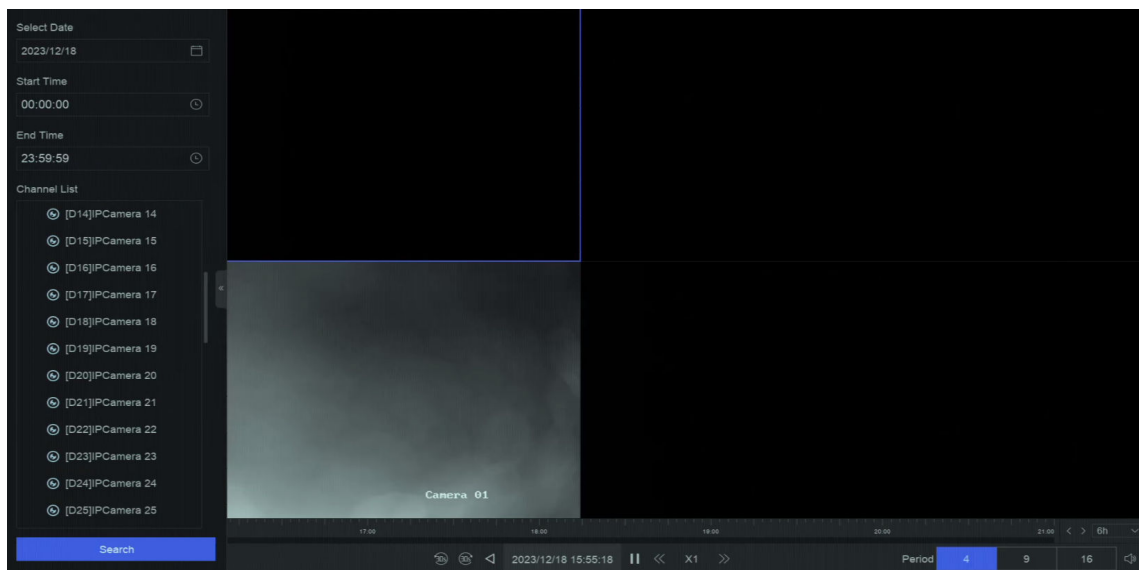


Figure 12-2 Sub-Period Playback

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	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	
		Human and Vehicle are selectable, apart from false alarms, only the 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.

Before You Start

If your device supports **AI by NVR** function, and its corresponding functions are required, please go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

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 **Enable AI by NVR**.

The device will analyze the video, and cameras only transmit video stream.

4. Select **Line Crossing**.

5. Turn on **Enable**.

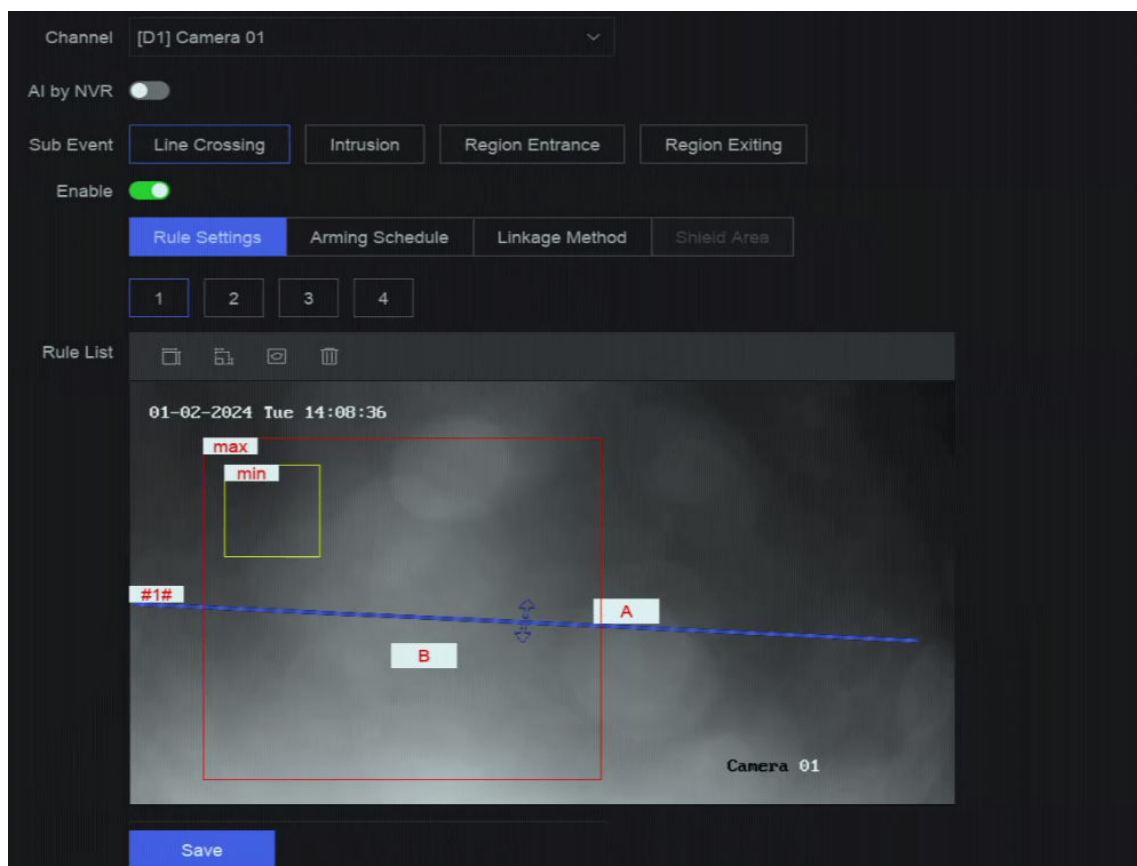


Figure 13-1 Line Crossing Detection

6. 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**, and **Detection Target**.

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.

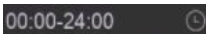
4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.

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

7. 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  to set specified time schedule.

8. 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.
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.

9. 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.

10. 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.

Before You Start

If your device supports **AI by NVR** function, and its corresponding functions are required, please go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

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 **Enable AI by NVR**.

The device will analyze the video, and cameras only transmit video stream.

4. Select **Intrusion**.

5. Turn on **Enable**.

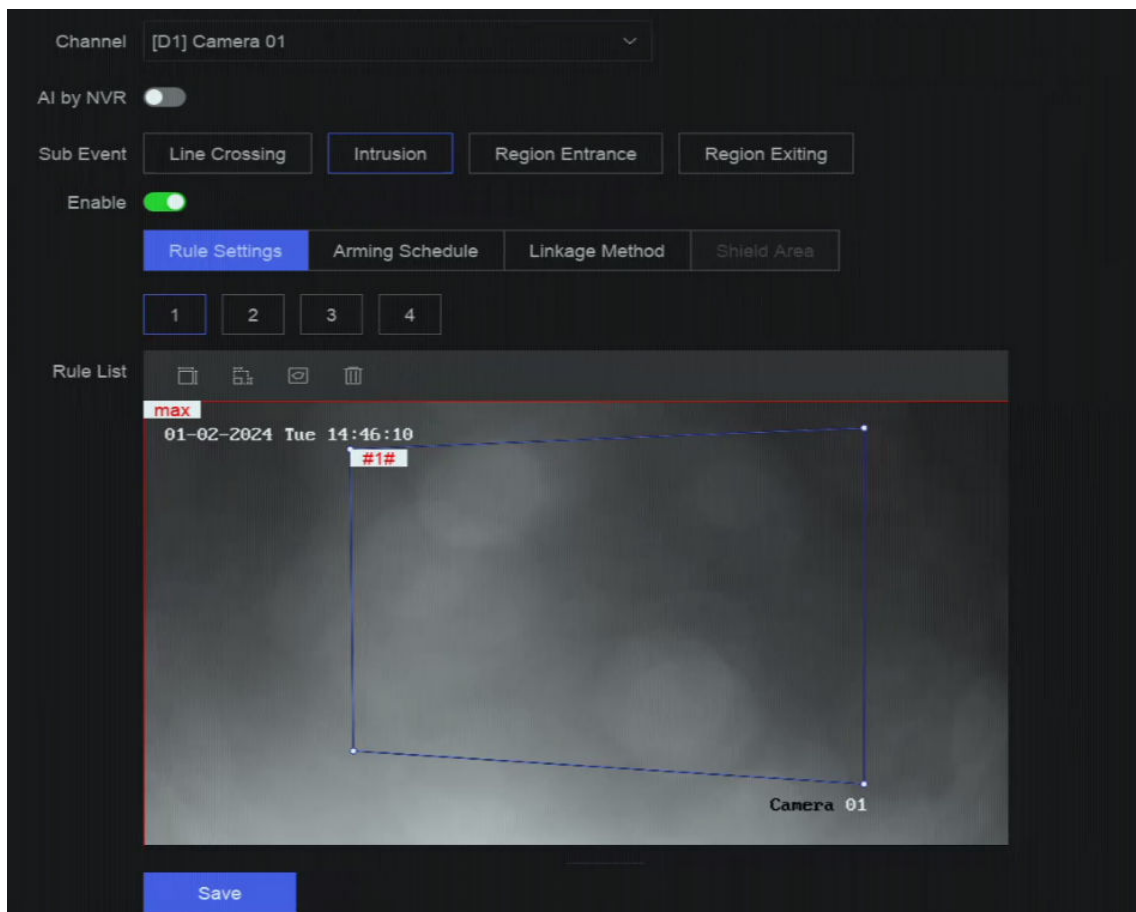


Figure 13-2 Intrusion Detection

6. 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 area.
- 3) Set **Time Threshold**, **Sensitivity**, and **Detection Target**.

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.

- 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.

- 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.

- 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.

- 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.
- 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.

Before You Start

If your device supports **AI by NVR** function, and its corresponding functions are required, please go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

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 **Enable AI by NVR**.

The device will analyze the video, and cameras only transmit video stream.

4. Select **Region Entrance**.
5. Turn on **Enable**.

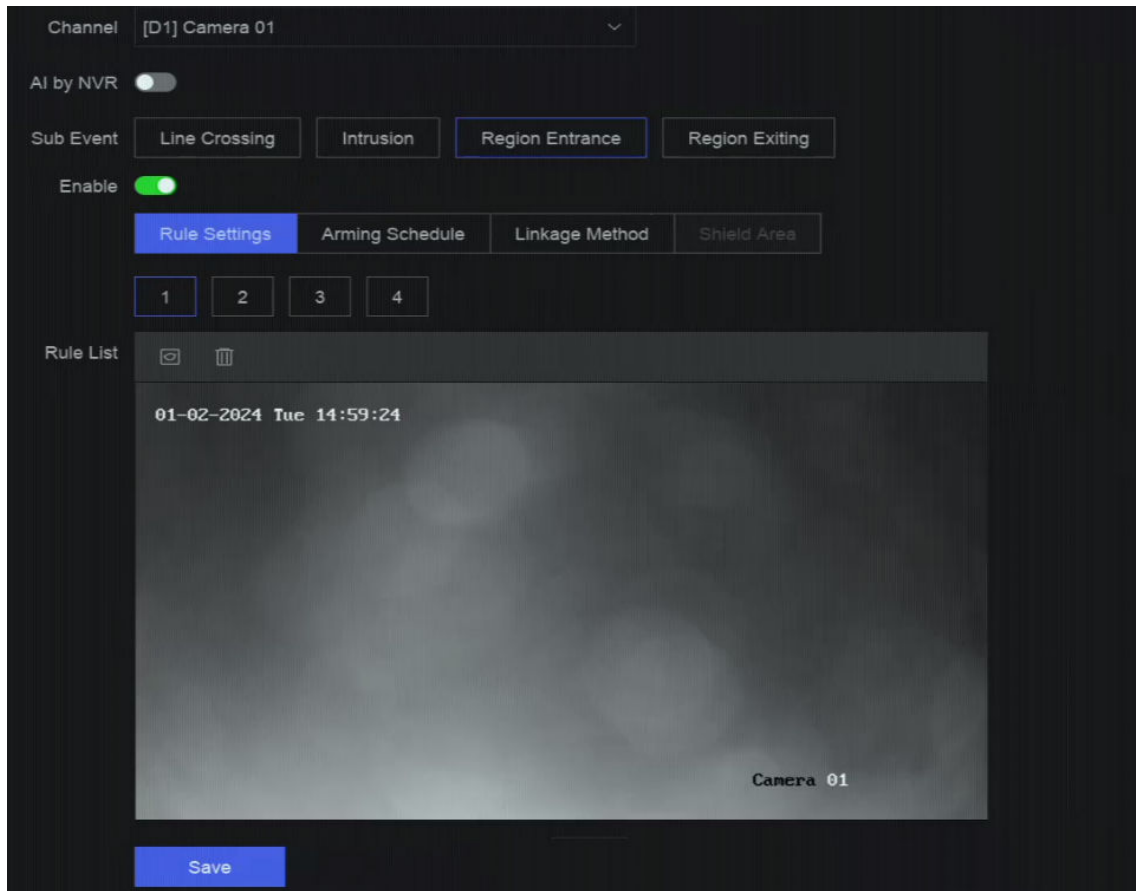


Figure 13-3 Region Entrance Detection

6. 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 area.
 - 3) Set **Sensitivity** and **Detection Target**.

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.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
7. 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.

8. 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.

9. **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.

10. 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.

Before You Start

If your device supports **AI by NVR** function, and its corresponding functions are required, please go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

Steps



Note

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

1. Go to **Event Center → [AI icon] → Event Configuration → Perimeter Protection**.

2. Select a camera.

3. **Optional:** Turn on **Enable AI by NVR**.

The device will analyze the video, and cameras only transmit video stream.

4. Select **Region Exiting**.

5. Turn on **Enable**.

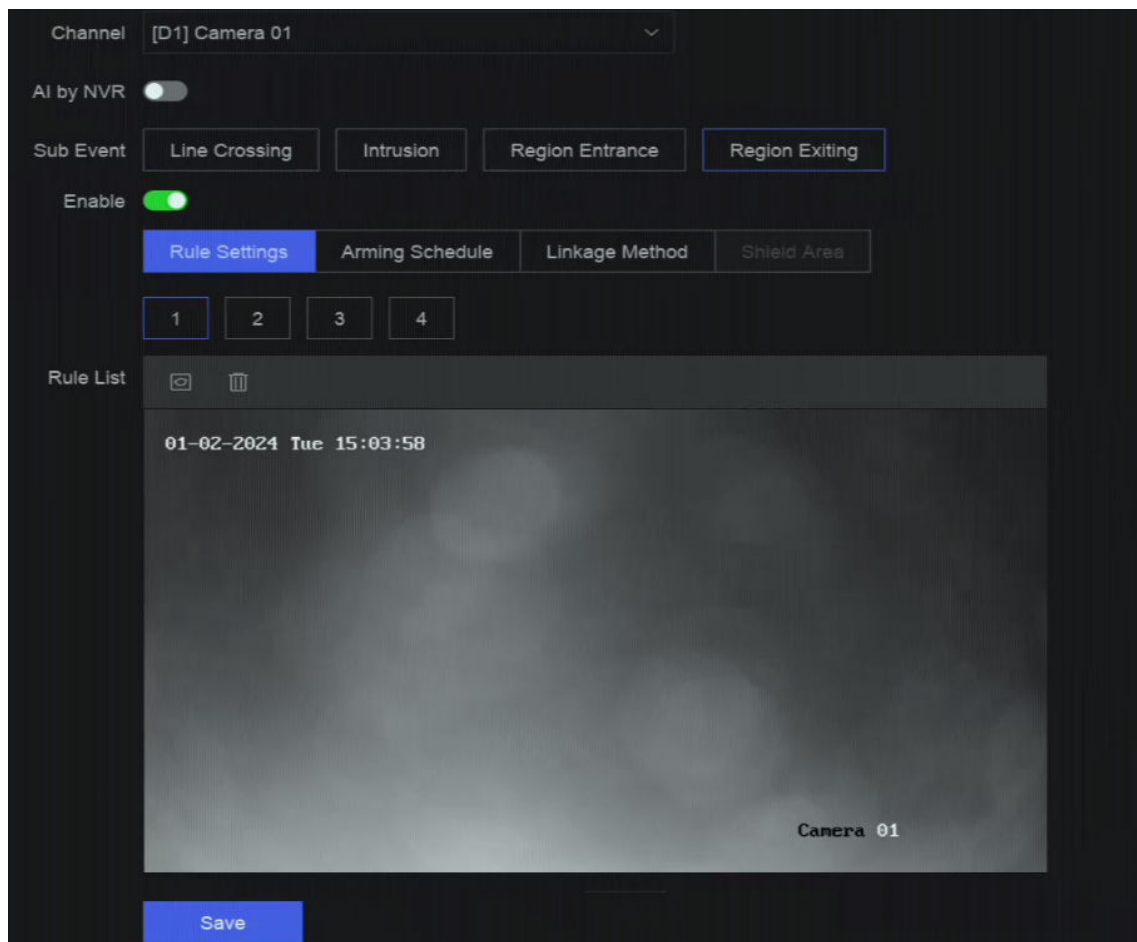


Figure 13-4 Region Exiting Detection

6. 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 area.
- 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

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

Detection Target

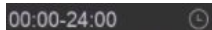
Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

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

7. 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  to set specified time schedule.

8. 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 →

Linkage Method	Description
	Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

9. 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.

10. 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
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	

Event Name	Event Description	Rule Configuration
	can be taken when the alarm is triggered.	easily the detection alarm will be 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.	d. Optional: Repeat the above steps to set another one.
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 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.  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**.

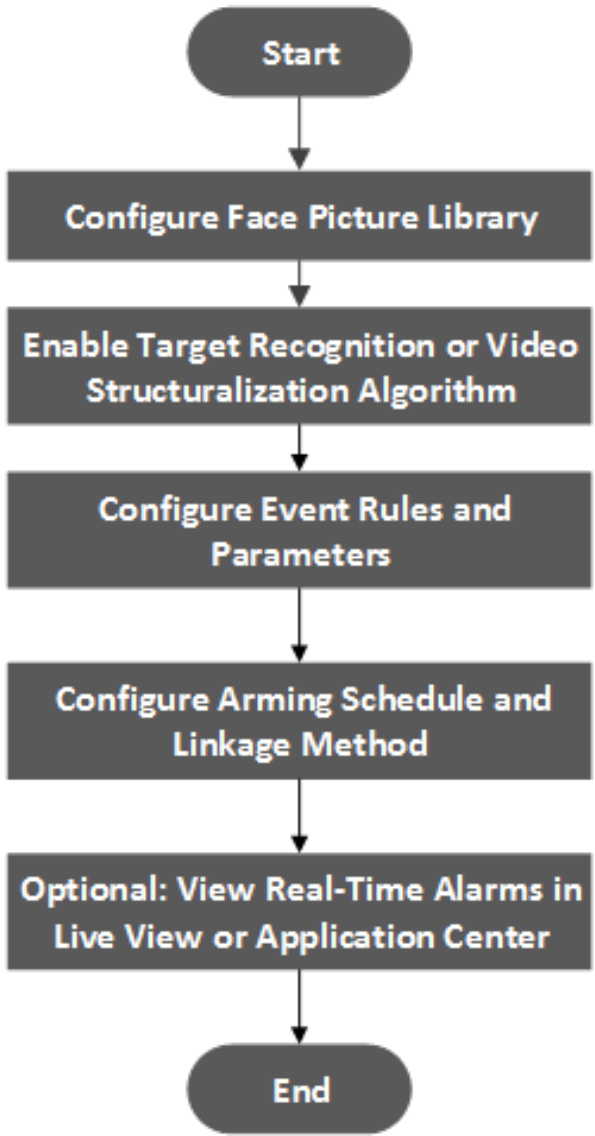
13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System → 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.	 <pre> graph TD Start([Start]) --> Step1[Configure Face Picture Library] Step1 --> Step2[Enable Target Recognition or Video Structuralization Algorithm] Step2 --> Step3[Configure Event Rules and Parameters] Step3 --> Step4[Configure Arming Schedule and Linkage Method] Step4 --> Step5[Optional: View Real-Time Alarms in Live View or Application Center] Step5 --> End([End]) </pre> Figure 13-5 Flow Diagram of Face Picture Comparison Target Grading

Event Name	Event Description	Rule Configuration
		Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis. Non-Real-Time Mode For places with a high flow of people, the device processing speed may not be fast enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View.
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.  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.

- 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.

- 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.

- 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.

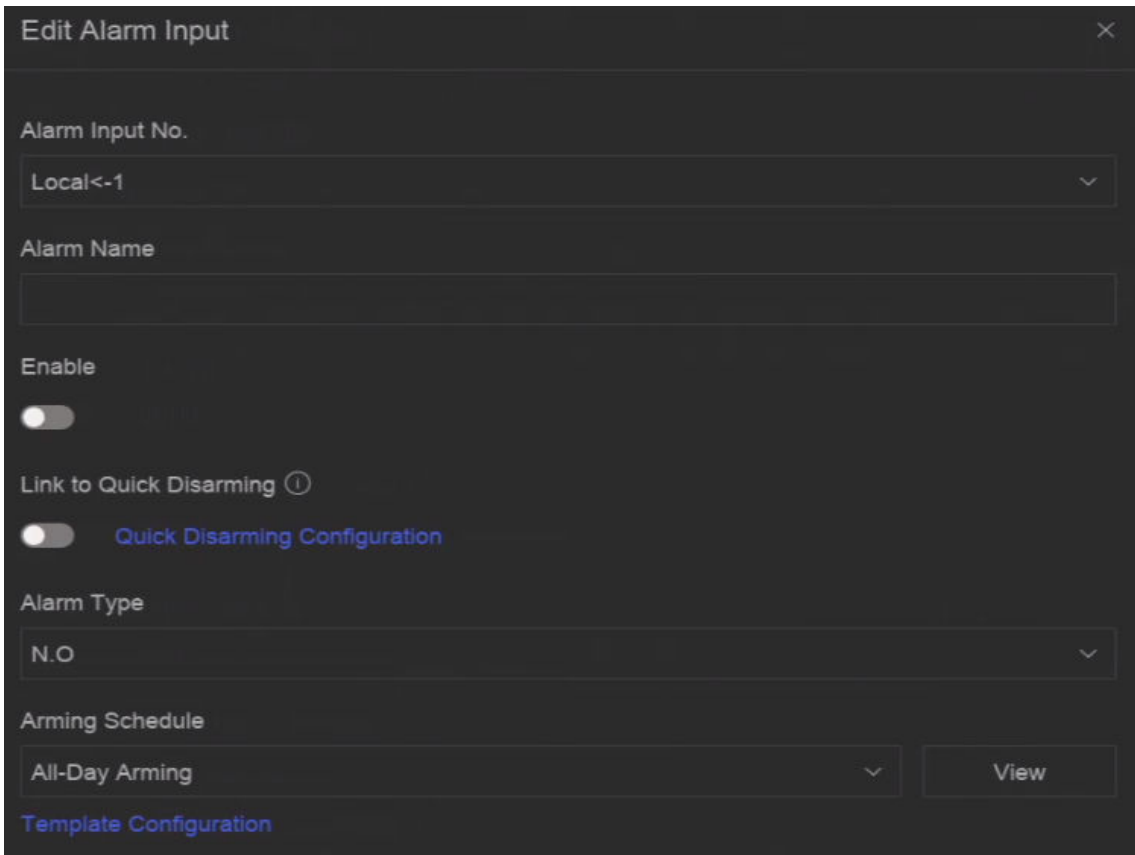


Figure 13-6 Configure Alarm Input



Note

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

3. Edit **Alarm Name**.
4. Turn on **Enable**.
5. Set **Quick Disarming**. Quick disarming can disable the selected alarm linkage methods in a batch.
6. Set **Alarm Type**.



Note

Refer to the alarm source to correctly configure the 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.

- 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.

- 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.

- 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.

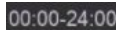
Table 13-13 Audio Analysis Event

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  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.

Linkage Method	Description
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**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

1. Go to **Event Center** →  → **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.

Item	Description
Attached Image	Send email with attached alarm images.
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.

3. Click **Audio Management** to manage audio files for alert 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. 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.

5. Click **Alarm Host** to set security control panel parameters.
6. Click **Flashing Light Alarm Output** to set the camera flashing light.
7. Click **Audio Alarm Output** to set the camera speaker.

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**.

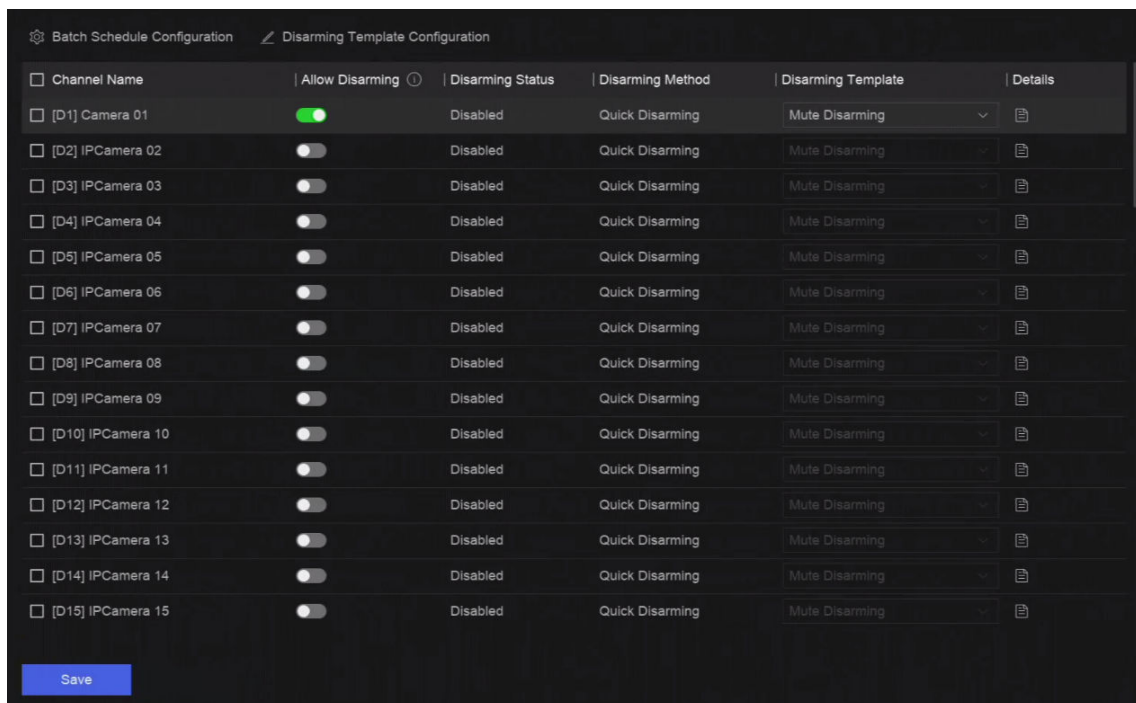


Figure 13-7 Disarming Configuration

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.

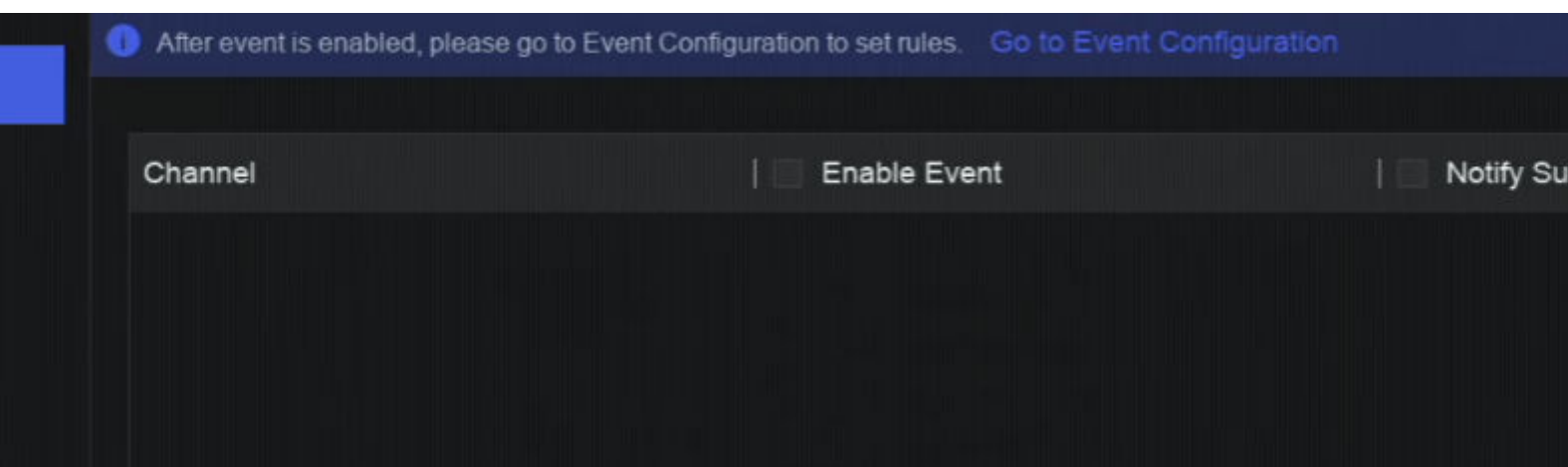


Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

1. Go to **Event Center** → .

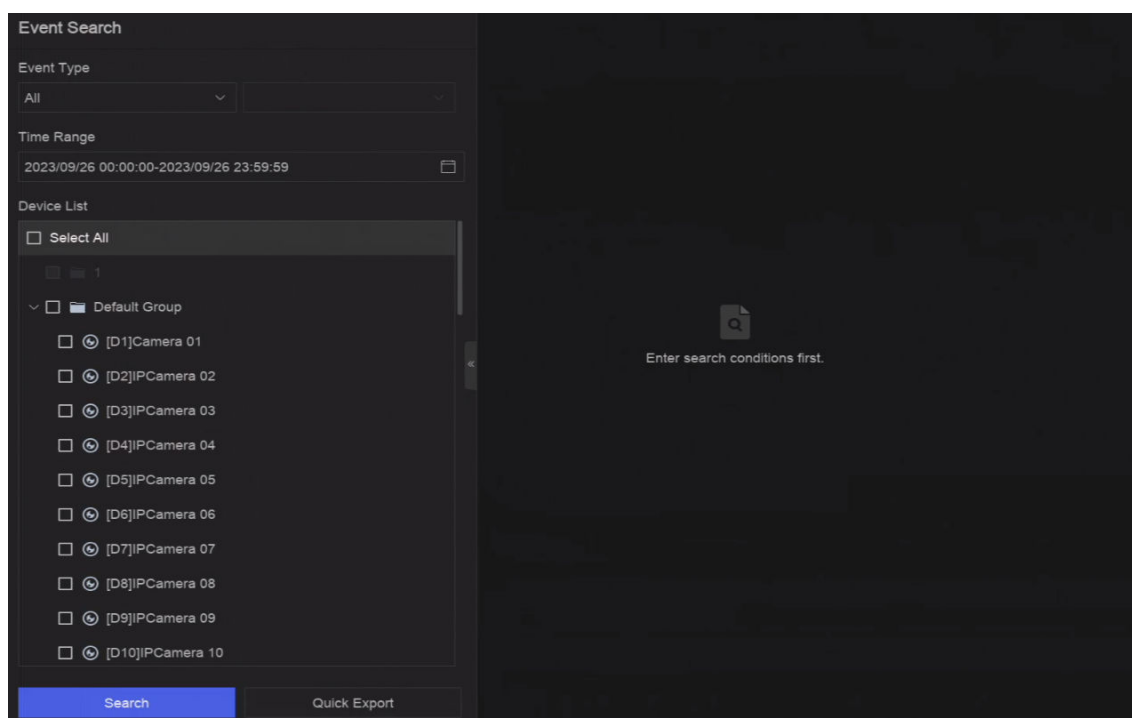


Figure 13-9 Event Search

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**.

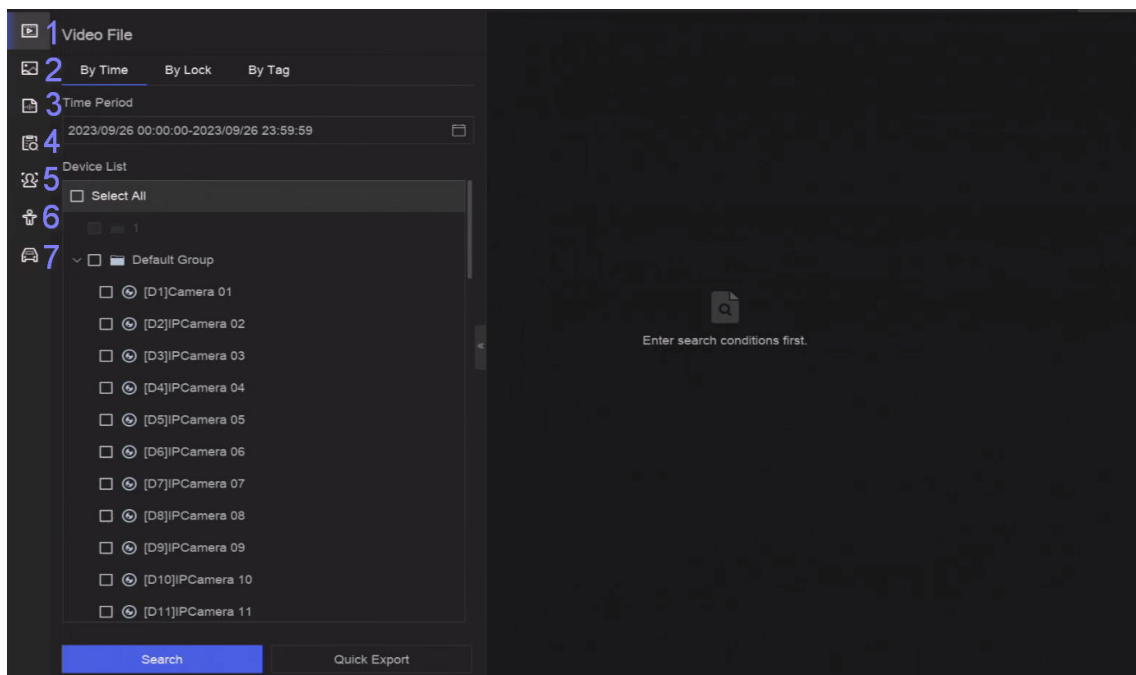


Figure 14-1 Search and Backup

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**.

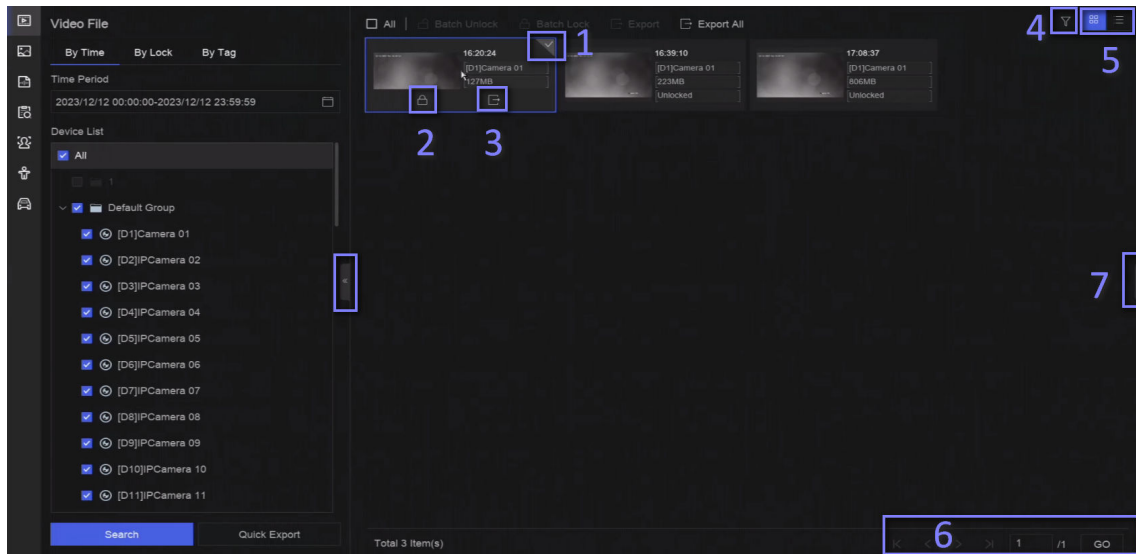


Figure 14-2 Searching Result

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 file(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.

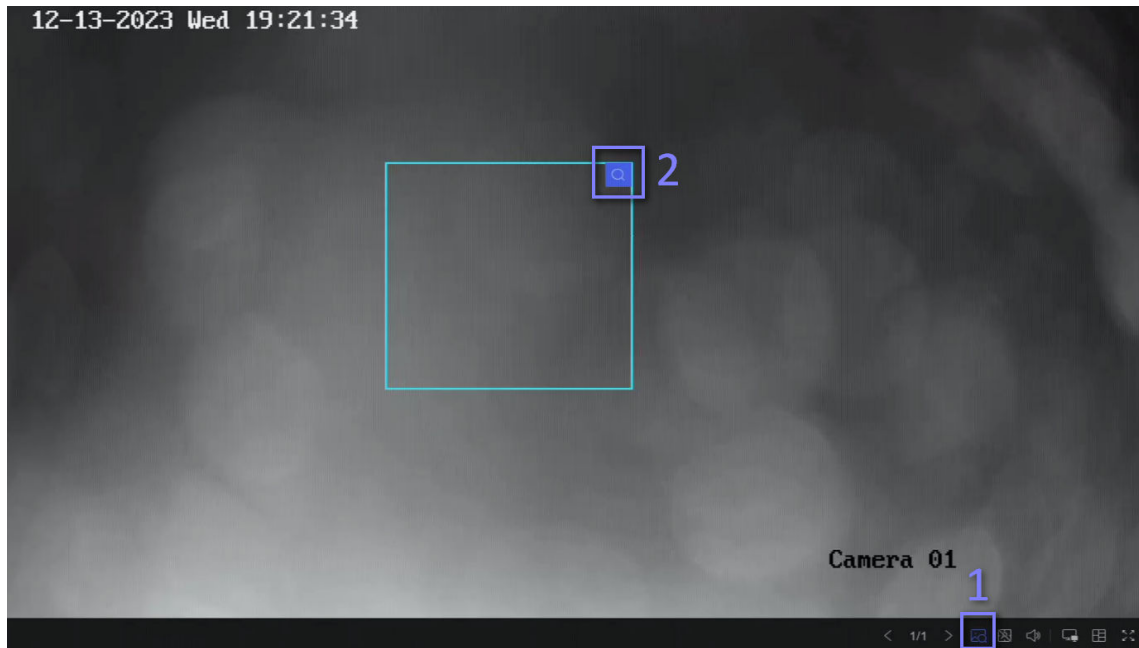


Figure 15-1 AcuSearch

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

4. View searching results.

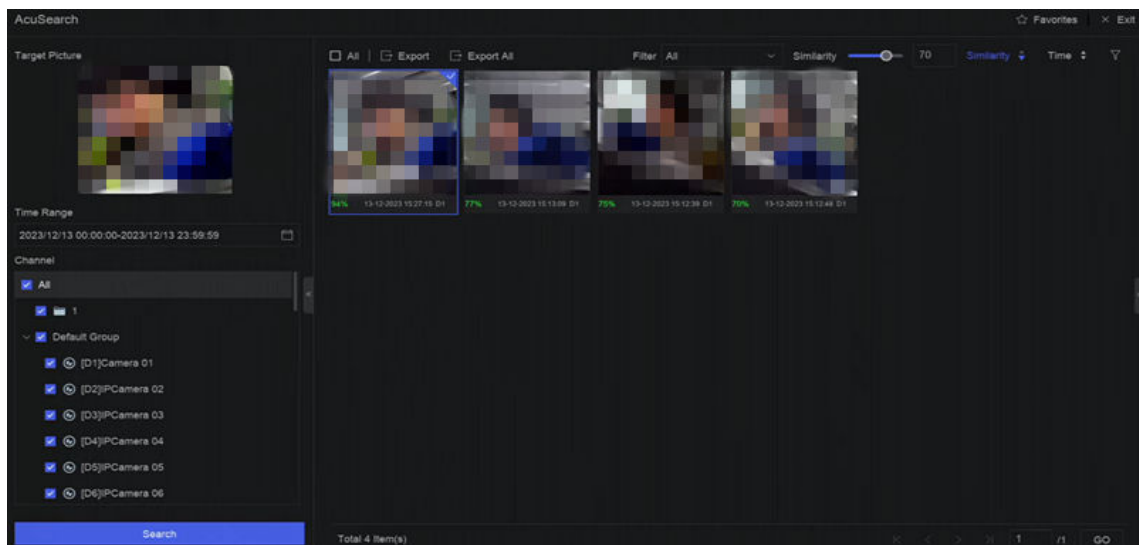


Figure 15-2 AcuSearch Result

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 Intelligent Management (VCA)

The operations for this chapter are recommended to be performed through web browser.

Configuration path: **VCA → Intelligent Management**.

16.1 Task Management

16.1.1 Import Application

Third-party applications can be imported in to your device.

Go to **VCA → Intelligent Management → Routine Analysis**, and click **Import Application** to import third-party applications.

16.1.2 Advanced Configuration

Go to **VCA → Intelligent Management → Routine Analysis**, and click **Advanced Configuration** to configure **AI Alarm Automatic Network Replenishment** and **Overlay Info Settings**.

AI Alarm Automatic Network Replenishment

When network is disconnected, this function can automatically store AI alarms, and then upload AI alarms after network is recovered.

The number of alarms that are not uploaded would be displayed, and you can click **View** or **Clear** to upload or clear these alarms.

Overlay Info Settings

The target frame, dot matrix chart, and target information can be overlaid on the image, and you can set corresponding parameters.

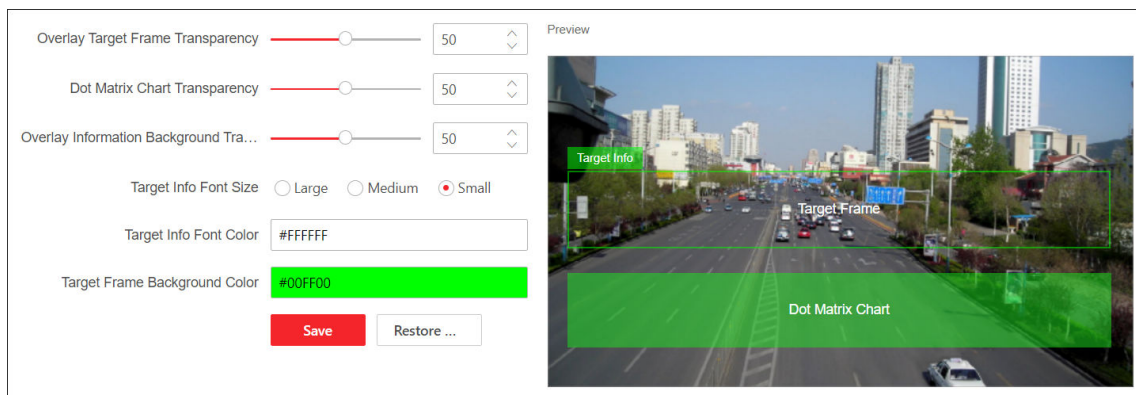


Figure 16-1 Overlay Info Settings

16.1.3 Task Configuration

After an application card is selected, you can configure its analysis mode and rules.

Steps

1. Go to **VCA → Intelligent Management → Routine Analysis**.
2. Select an application card.

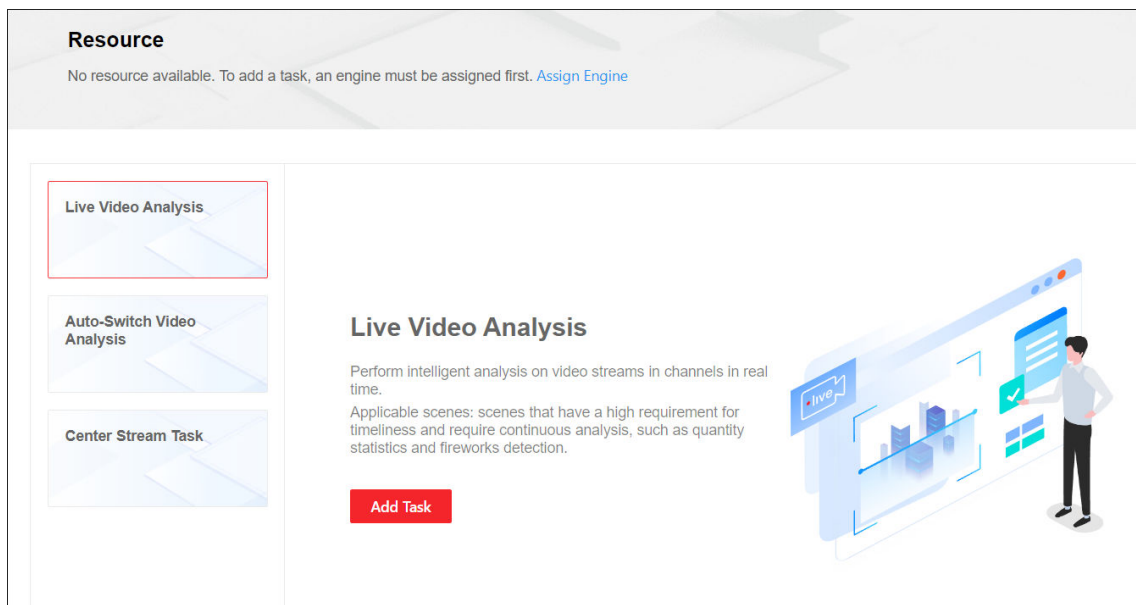


Figure 16-2 Task Configuration

3. Click **Assign Engine** at the top side, and assign an engine for the application.



Note

If the device engine does not have enough analysis resource, please move the cursor on the engine and click  to disable the applications which are not required.

4. Select analysis mode.

Live Video Analysis

Perform intelligent analysis on video streams in channels in real time.

Auto-Switch Video Analysis

The device analyzes auto-switch videos of linked channels. Auto-switch will switch videos from one channel to another automatically according to the auto-switch time.

Scheduled Capture Analysis

The device will capture pictures according to the capture schedule (capture interval), and analyze captured pictures of all linked channels.

Offline Picture Analysis

Perform intelligent analysis on pictures uploaded from devices or offline pictures or picture URLs distributed from the platform.

Alarm Picture Analysis

Perform secondary intelligent analysis on pictures captured by the network camera.

Center Stream Task

The device would add RTSP video stream address as custom channel, and cooperate with platform. The platform controls the analysis process.

5. Click **Add Task**.

6. Set the task information.

① Task Info... ② Channel ...

Task Name

① Alarm Mode

Arming Schedule

Advanced Configuration

Select Channel

▼ ☐ Default Group

☐ [D8] IPCamera 08

4 channels available for the currently assigned engine. [Assign Engine](#)

Figure 16-3 Set Task Info

Note

- After enabling **Alarm Target Frame Overlay** in **Advanced Configuration**, the target frame will be shown in alarm data.
- If **Alarm Mode** is set as **Traditional Alarm Mode**, you can only select the regional target status detection as the rule type. The way to search for alarm pictures differs, depending on the alarm mode. For **AI Alarm** mode, alarm pictures are searched in AIOP event types. For **Traditional Alarm Mode**, alarm pictures are searched in traditional event types.

7. Click **Next**.

8. Select a channel and configure rules. Refer to [Rule Type Description](#) and [Bulit-In Algorithm Description](#) for details.

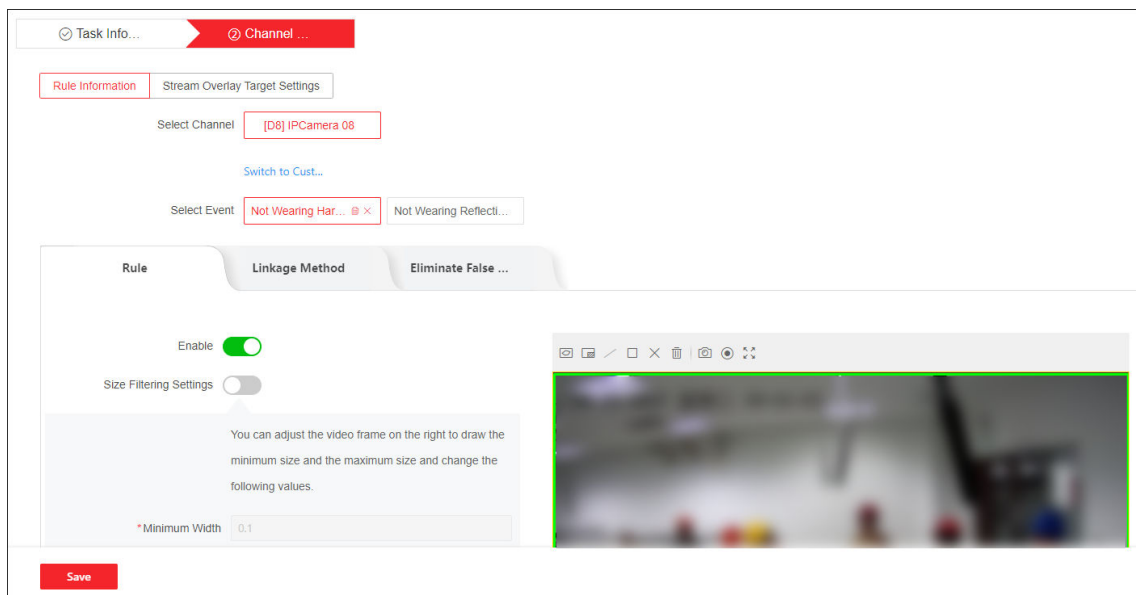


Figure 16-4 Configure Rules

9. Set Linkage Method.

10. For a few models, you can configure **Eliminate False Alarms During Secondary Analysis** to reduce false alarms. Refer to **Secondary Analysis Mode** for details.

11. Click **Save**.

16.2 Large Model (Ultra-High-Precision Algorithm) Configuration

With strong and intelligent analysis capability, large model (ultra-high-precision algorithm) is expected to gain the insight into all objects and know their status, features and patterns. The large model has a three-level architecture, which is basic large model, industry large model, and task model.

In compare with normal model, the large model requires less dependence on the amount of samples during the initial training period, which saves the manpower of marking samples. Meanwhile, the large model is more adaptable to different scenes, and can provide more effective detection results.

16.2.1 Picture Analysis Mode

This analysis mode can only analyze pictures. Hence only **Scheduled Capture Analysis** or **Offline Picture Analysis** would be available. Scenes with low real-time requirements are suitable for this mode, such as OCR (Optical Character Recognition), non-motor vehicle parking detection, etc.

The configuration method for this analysis mode is the same as normal models. Refer to **Task Management** for details.

16.2.2 Secondary Analysis Mode

For real-time event alarms, the device engine can analyze them for a second time to reduce false alarms and improve alarm accuracy. The procedure may take more time, so there would be a long delay for an alarm.

Steps

1. Go to **VCA → Intelligent Management → Algorithm Management** to select an application card with **Ultra-High-Precision Algorithm** tag.
2. Click **Secondary Analysis Settings**.

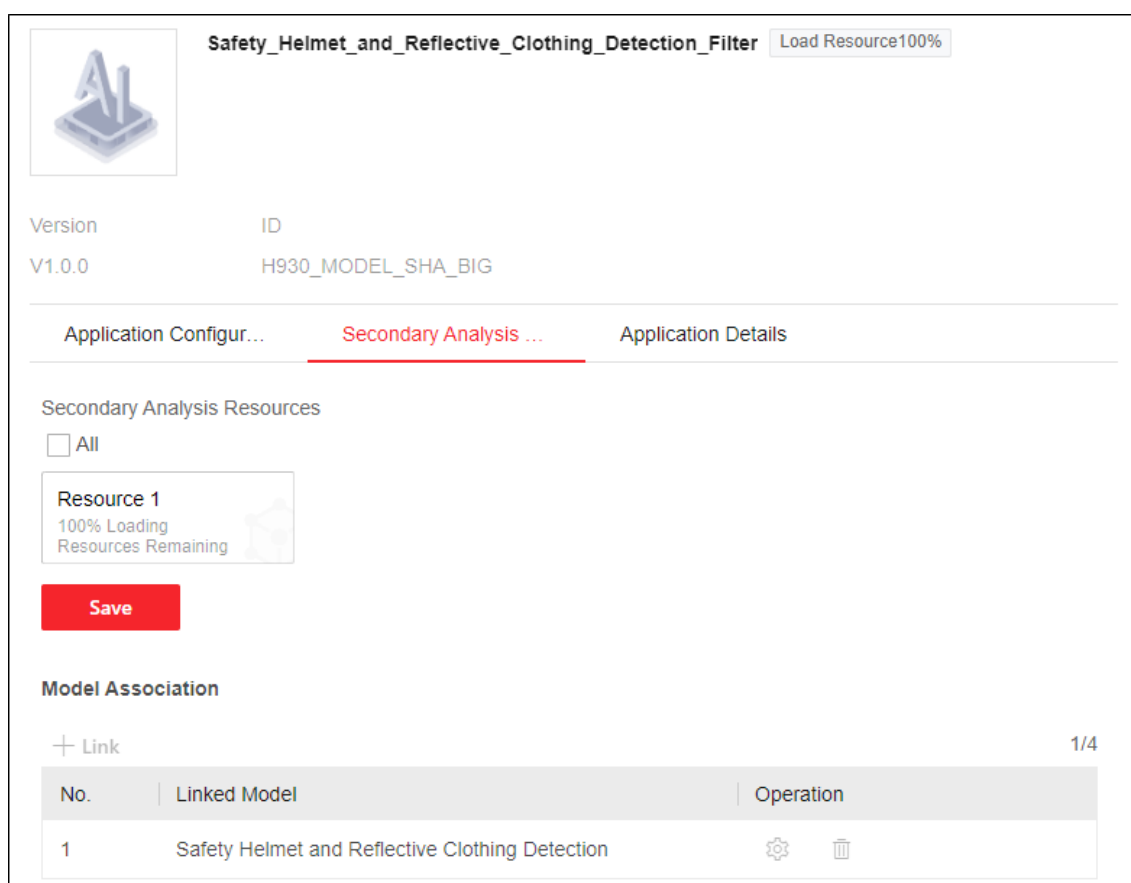


Figure 16-5 Secondary Analysis Settings

3. Allocate engine resource.
4. **Optional:** For a few models, click **Link** to link a normal model for secondary analysis.
5. **Optional:** For a few models, you can click to set its target parameters.

Note

The target type and target attribute of large model should be the same as the normal model.

6. Complete the task configuration of normal model. Refer to ***Task Configuration*** for details.

7. Click **Eliminate False Alarms During Secondary Analysis** after the task configuration of normal model.

The screenshot shows a web interface for configuring secondary analysis. At the top, there are two tabs: 'Task Info...' and 'Channel ...'. Below these, there are two sub-tabs: 'Rule Information' and 'Stream Overlay Target Settings'. Under 'Rule Information', there is a 'Select Channel' dropdown menu with '[D8] IPCamera 08' selected. Below this is a 'Switch to Cust...' link. Then, there is a 'Select Event' section with two buttons: 'Not Wearing Har...' (highlighted with a red box) and 'Not Wearing Reflecti...'. Below the 'Select Event' section, there are three tabs: 'Rule', 'Linkage Method', and 'Eliminate False ...' (highlighted with a blue box). Under the 'Eliminate False ...' tab, there is an 'Enable' toggle switch (turned on), an 'Adding Target' toggle switch (turned off), and a 'Linked Model' dropdown menu with 'Safety_Helmet_and_Reflective_Clothing_Detection_Filter' selected. At the bottom, there is a '* Confidence Filter (≥)' input field with the value '50'. A red 'Save' button is located at the bottom left of the configuration area.

Figure 16-6 Configure Secondary Analysis

8. Turn on **Enable**, and configure other parameters.

Adding Target

To add alarm targets that are missed during the first time.

Confidence Filter

Only targets satisfy the value of **Confidence Filter** can trigger alarms.

9. Click **Save**.

16.3 Algorithm Management

Go to **VCA → Intelligent Management → Algorithm Management** manage algorithms.

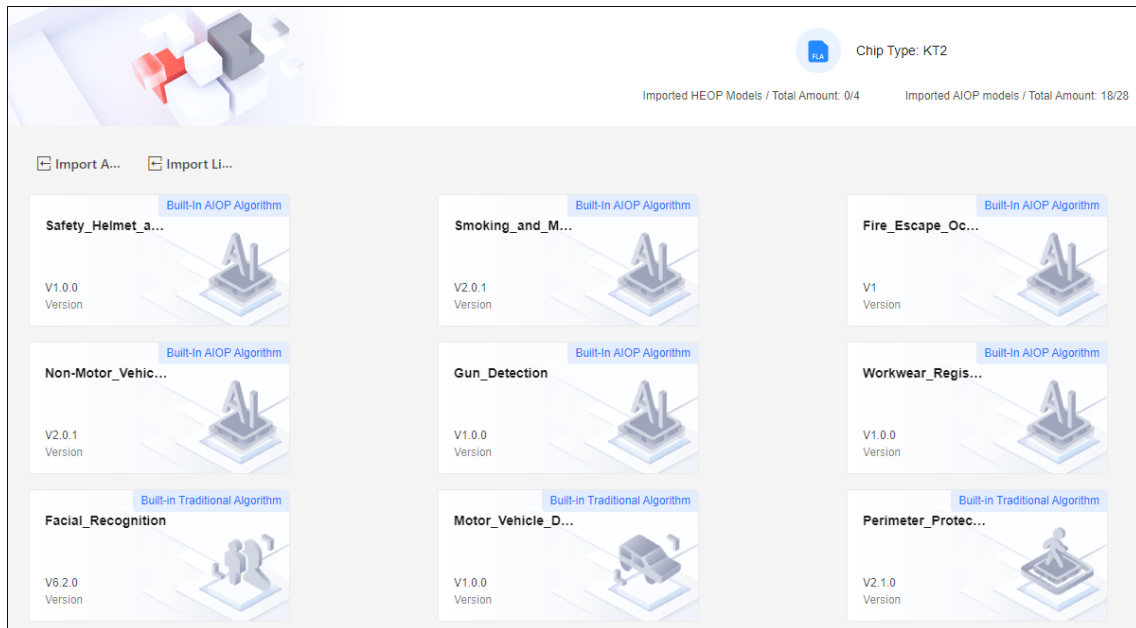


Figure 16-7 Algorithm Management

- Import model: Click **Import Application** to import AIOP or third-party models. For third-party models, please click **Import License** to import the authorization file.
- Edit model name: Move the cursor on the model, and click . Only a few models support this function.
- Update model: Move the cursor on the model, and click .
- Reverse model version: Move the cursor on the model, and click . The model would be reversed to the initial version.
- Delete model: Move the cursor on the model, and click . Only third-party models support this function.
- Link engine: Click an algorithm card, and select an engine for it.

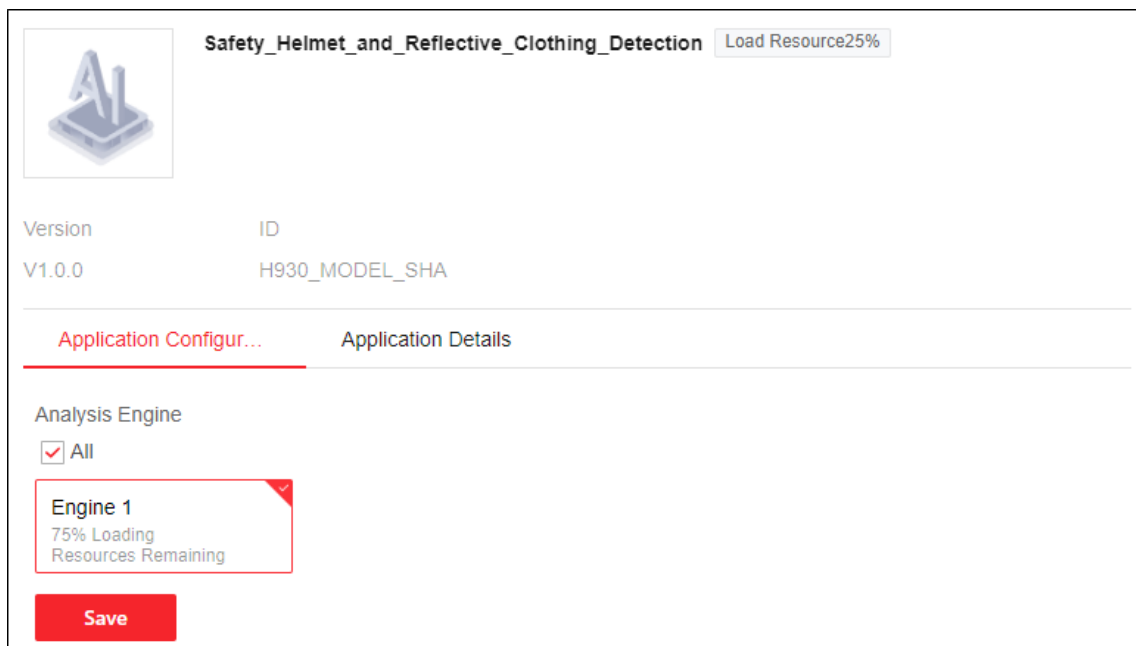


Figure 16-8 Link Engine

16.4 Engine Status

You can view the engine status and resource status for secondary analysis.

16.4.1 View Engine Status

Go to **VCA → Intelligent Management → Engine Status → Engine Status** to view engine status, including engine usage, temperature, etc.

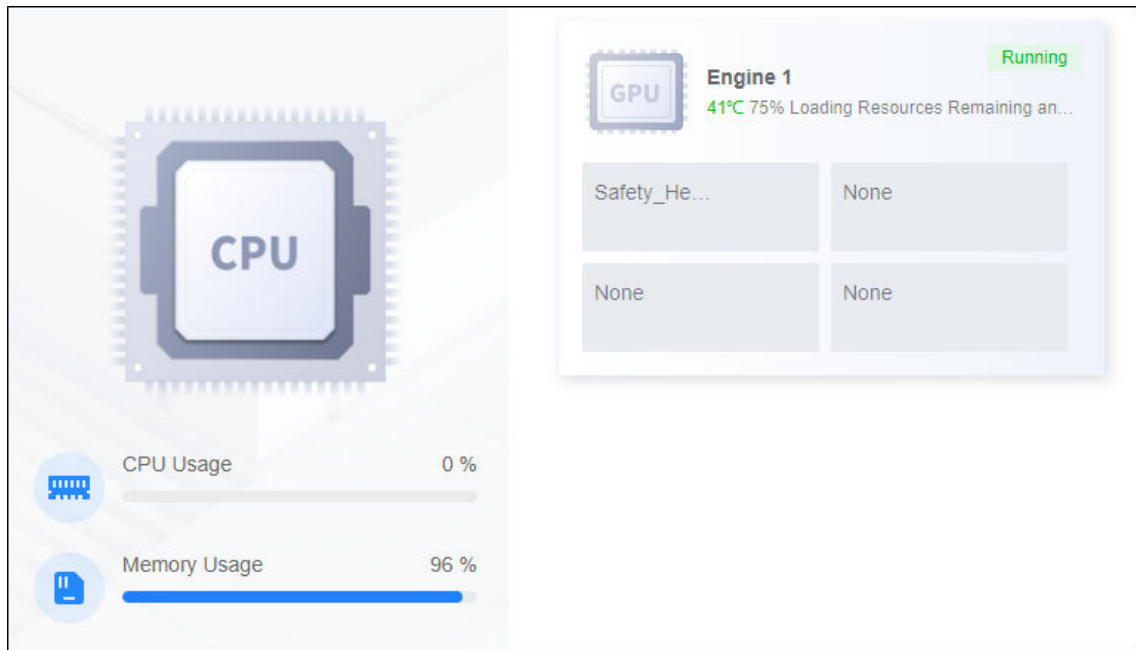


Figure 16-9 View Engine Status

16.4.2 View Resource Status for Secondary Analysis

Go to **VCA → Intelligent Management → Engine Status → Resource Status for Secondary Analysis** to view the working status of secondary analysis.

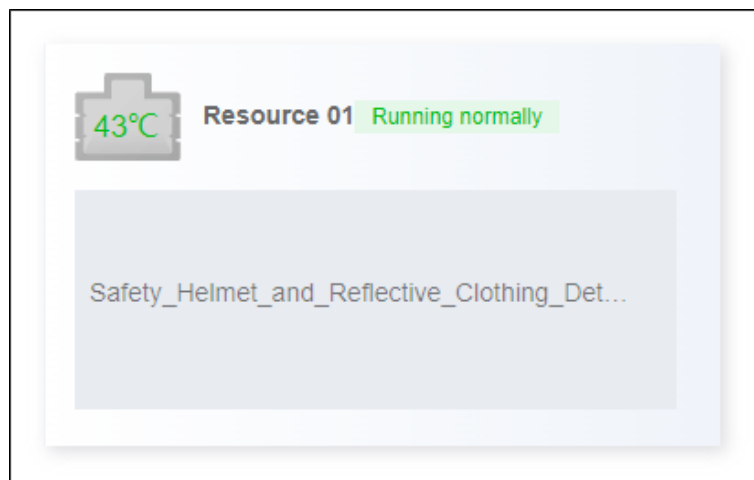


Figure 16-10 Resource Status for Secondary Analysis

16.5 Data Archive

Enter a short description of your concept here (optional).

This is the start of your concept.

16.5.1 Comparison Library of Searching

This library is used to compare the captured target picture and recognize what the target is.

Steps

1. Go to **VCA → Intelligent Management → Data Archive → Comparison Library of Searching**.
2. Click **Add** to add a library.
3. Set the library parameters.
4. Click the library card.
5. Click **Add** or **Batch Add** to add pictures.



Note

You can import pictures in GIF, JPEG, TIFF, PNG, and BMP format with a maximum size of 2 MB.

6. Click **Save**.
7. **Optional:** After a library or picture is added, you can move the cursor on the library or picture card to edit or delete it.

16.5.2 Registration and Comparison Library

This library is used for algorithms like **Workwear_Regist_Compare**. It can detect whether uniform or working cap is worn correctly, and report alarms according to event rules.

Steps

1. Go to **VCA → Intelligent Management → Data Archive → Registration and Comparison Library**.
2. Click **Add** to add a library.
3. Click the library card.
4. Click **Add** or **Batch Add** to add pictures.



Note

- You can import pictures in GIF, JPEG, TIFF, PNG, and BMP format with a maximum size of 2 MB.
 - Each uniform and working cap should contain samples in 4 direction, including front side, back side, left side, and right side. The registration image should be clean and without masking. The width of resolution should be larger than 128. Usually, high resolution is recommended.
-
5. **Optional:** After a picture is added, you can click **Draw Area** to draw the required area on the picture.

6. Click **Save**.

7. **Optional:** After a library or picture is added, you can move the cursor on the library or picture card to edit or delete it.

16.5.3 Picture Comparison Library

Picture comparison library is used for picture comparison models. The pictures in the library are used as reference pictures. Alarms can be triggered when the channel images are similar with reference pictures.

Steps

1. Go to **VCA → Intelligent Management → Data Archive → Picture Comparison Library**.
2. Select a channel in the list at left side for picture comparison.
3. Click **Add** to add a reference picture for the channel.
 - **Add Captured Picture:** Click **Capture** to capture a real-time picture through the channel live image, and then click **Save**.
 - **Add From Local:** Click **Select** to import a picture through your local PC, and then click **Save**.
4. Click **Imported-Picture Analysis** in the list at left side.
5. Click **Add** to add a reference picture.
6. Click **Save**.

16.5.4 Calibration Library

The calibration library is used to approximately calculate the size of an actual object in the image.

Steps



Note

This function is only available for a few models.

1. Go to **VCA → Intelligent Management → Data Archive → Calibration Library**.

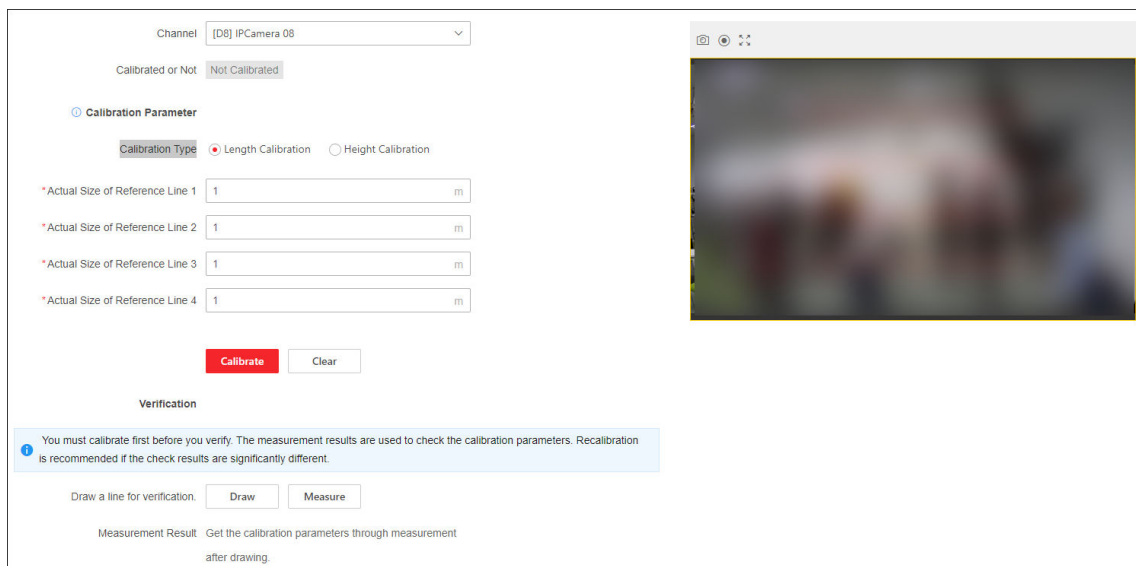


Figure 16-11 Calibration Library

2. Select a camera.
3. Select **Calibration Type**. **Length Calibration** or **Height Calibration** is selectable.
4. Move and adjust 4 red calibration lines to the target on the image.

Note

- For **Height Calibration**, the calibration target should be a complete perpendicular to the ground, the position of four calibration lines should be scattered, and the endpoints of any two calibration lines cannot be on the same horizontal line.
- For **Length Calibration**, the calibration target should be a target parallel to the horizontal plane, and the four calibration lines should be scattered and are recommended not to be intersect.

5. Enter the actual length or height of each calibration line.
6. Click **Calibration**.
7. Verify the calibration result.
 - 1) Click **Draw**.
 - 2) Move and adjust the blue verification line to the target on the image.
 - 3) Click **Measure**.

The verification value would be displayed at the right side of **Measurement Result**.

- 4) Compare the calculated size to the actual size to verify the calibration result.

Note

- You cannot start verification without finishing calibration
- If the measured result deviates greatly from the actual size, it is recommended to recalibrate.

What to do next

If you select **Target Length/Area on Stream** under **Display Configuration** during task configuration, the target length or area value would be overlaid on stream.

16.5.5 List Library (Face Picture Library)

The list library is used for face picture storage and face picture comparison. Click Add to create a library, and then upload face pictures in to it.

Steps

1. Go to **VCA → Intelligent Management → Data Archive → List Library**.
2. Click **Add** to add a library.
3. Set the library name and other parameters.
4. Click the library card.
5. Click **Add** or **Import** to import face pictures.
6. **Optional:** If you click **Search by Picture**, the device can compare the uploaded picture with the ones in the library.

16.5.6 Audio Management

Audio files can be imported in to your device for alarm linkage action. For certain event types, when alarms are triggered, the audio files can be played.

Go to **VCA → Intelligent Management → Data Archive → Audio Management** to import or delete audio files.

16.6 Rule Type Description

After clicking **Switch to Custom Mode**, you can edit **Rule Name** and **Rule Type**.

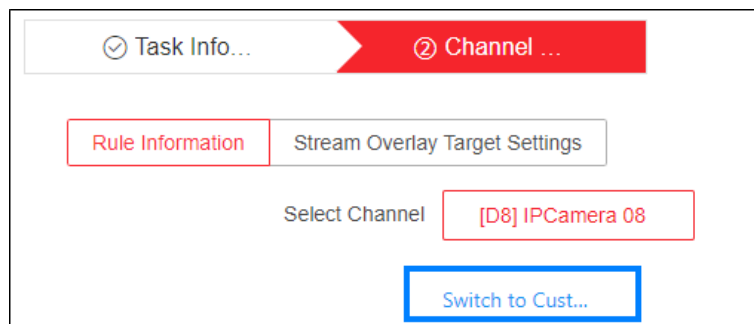


Figure 16-12 Configure Rule Type

Detection of Abnormal Status of Regional Targets

Detect the target quantity, target attribute, etc.

Line Crossing Target Detection

When targets have crossed the line, the device will detect the target type, quantity, and attribute.

Region Overlap Ratio Exception Detection

The device will calculate the ratio between the specified object area (occupied in the image) and the rule area. When the ratio satisfies the condition value, the device will trigger an alarm. For example, it can be used for detecting the floating objects in rivers. If the ratio satisfies the given value, an alarm will be triggered to notify that the waterway requires to be cleaned up.

Combined Rule

Combined Rule have are two modes: **All Satisfy** and **Satisfy In Order**. **All Satisfy** means that the device will trigger alarms when all sub rule conditions are satisfied. **Satisfy In Order** means that the device will trigger alarms when sub rule conditions are satisfied in order. For example, if you have set sub rule 1 and sub rule 2, **All Satisfy** means that both rule 1 and rule 2 satisfy the conditions. For **Satisfy In Order**, it means that rule 1 shall firstly satisfy the condition, and thereafter rule 2 satisfies the condition, then will the device trigger an alarm.

Area Status Change Detection

Compare the video image with the reference picture. If the image is different with the reference picture, and all rule conditions are satisfied, the device will trigger an alarm. You can click **Reference Picture** at the top to add pictures.



Note

The picture file format should be JPEG, resolution should be between 32 × 32 and 3840 × 2160, file size cannot exceed 2 MB, and file name cannot exceed 32 characters.

Region Exception Status Detection

Detect the target attribute in the rule area.

Full Analysis Rule

Report all structured information in the region according to the alarm interval.

Line Crossing Target Counting

When specified targets have crossed the line, the device will count the number of specified targets.

Region Target Number Counting

Report specified target quantity in the region according to the report interval.

OCR Trigger

Optical Character Recognition (OCR) means to recognize texts in image. The device can output the recognition results. When the text triggers the configured line crossing detection rule, an alarm will be triggered.

Region Overlap Ratio Statistics

The device will calculate the ratio between the specified object area (occupied in the image) and the rule area.

Search Comparison

Search comparison is used to compare targets with the comparison library of searching.

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.

People Running Detection

People running detection detects the moving speed of people. When people are moving at a high speed, the device will consider people are running, and trigger an alarm.

Physical Conflict Detection

Physical conflict detection detects whether there is physical conflict, such as people pulling.

People Falling Down Detection

People falling down detection detects whether people are falling down. When height of people is lower than the threshold , it will trigger an alarm.



Note

The available rule types will vary according to the model type.

16.7 Built-In Algorithm Description

Enter a short description of your concept here (optional).

This is the start of your concept.

16.7.1 Safety Helmet and Reflective Clothing Detection

This algorithm is used to detect whether a target is wearing safety helmet or reflective clothing.



Note

Only **Detection of Abnormal Status of Regional** is allowed for **Rule Type**.

Object

For the detection of wearing safety helmet, please select head and shoulder. For the detection of wearing reflective clothing, please select upper body.

Target Attribute

Alarms would be triggered according to the target attributes.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Target Quantity

Alarms would be triggered when the number of targets meet the condition of **Symbol** and **Value**.



Note

Only when the device has detected targets, then would the device perform this function.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Continuous Sensitivity

This parameter is based on **Duration**, the lower the sensitivity value, the stricter for the requirement of targets continuously triggering alarm rule.

Alarm Reporting Interval

It is the duration between two alarm reports.

Sensitivity

The higher the sensitivity value, the easier an alarm can be triggered.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Displacement Filter

For **Static Filter**, targets that are static can be filtered. For **Motion Target Filtering** targets that are moving can be filtered.

Linkage With Sub Targets

Main Target Alarm

Alarm will be triggered when the main target is detected. If the sub target is linked, the alarm content will contain the sub target information.

Main Target Link Sub Target Alarm

Alarm will be triggered when the main target is detected and the sub target is linked. The alarm content contains the sub target information.

Main Target Unlink Sub Target Alarm

Alarm will be triggered when the main target is detected, but no sub target is set or linking the sub target to the main target. The alarm content does not contain the sub target information.

16.7.2 Smoking and Making Phone Calls

This algorithm is used to detect whether a target is smoking or making phone calls.

Object

For smoking detection, please select smoking. For the detection of making phone calls, please select talking on phone.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Target Quantity

Alarms would be triggered when the number of targets meet the condition of **Symbol** and **Value**.



Note

Only when the device has detected targets, then would the device perform this function.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Continuous Sensitivity

This parameter is based on **Duration**, the lower the sensitivity value, the stricter for the requirement of targets continuously triggering alarm rule.

Alarm Reporting Interval

It is the duration between two alarm reports.

Sensitivity

The higher the sensitivity value, the easier an alarm can be triggered.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Displacement Filter

For **Static Filter**, targets that are static can be filtered. For **Motion Target Filtering** targets that are moving can be filtered.

Linkage With Sub Targets

Main Target Alarm

Alarm will be triggered when the main target is detected. If the sub target is linked, the alarm content will contain the sub target information.

Main Target Link Sub Target Alarm

Alarm will be triggered when the main target is detected and the sub target is linked. The alarm content contains the sub target information.

Main Target Unlink Sub Target Alarm

Alarm will be triggered when the main target is detected, but no sub target is set or linking the sub target to the main target. The alarm content does not contain the sub target information.

16.7.3 Fire Escape Occupation Detection

This algorithm is used to detect whether the fire escape route is occupied by other objects.



Note

Only **Detection of Abnormal Status of Regional** is allowed for **Rule Type**.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Alarm Reporting Interval

It is the duration between two alarm reports.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Specific Target Filtering

The selected target type would not trigger alarms.

16.7.4 Non-Motor Vehicle Detection

Electric Moped Detection, **Head and Shoulder Counting**, and **Gas Cylinder Detection** are selectable according to your requirement.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Target Quantity

Alarms would be triggered when the number of targets meet the condition of **Symbol** and **Value**.



Note

Only when the device has detected targets, then would the device perform this function.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Continuous Sensitivity

This parameter is based on **Duration**, the lower the sensitivity value, the stricter for the requirement of targets continuously triggering alarm rule.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Displacement Filter

For **Static Filter**, targets that are static can be filtered. For **Motion Target Filtering** targets that are moving can be filtered.

Linkage With Sub Targets

Main Target Alarm

Alarm will be triggered when the main target is detected. If the sub target is linked, the alarm content will contain the sub target information.

Main Target Link Sub Target Alarm

Alarm will be triggered when the main target is detected and the sub target is linked. The alarm content contains the sub target information.

Main Target Unlink Sub Target Alarm

Alarm will be triggered when the main target is detected, but no sub target is set or linking the sub target to the main target. The alarm content does not contain the sub target information.

16.7.5 Gun Detection

This algorithm is used to detect guns.

Object

Select **Gun** as the detection target.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Target Quantity

Alarms would be triggered when the number of targets meet the condition of **Symbol** and **Value**.



Note

Only when the device has detected targets, then would the device perform this function.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Continuous Sensitivity

This parameter is based on **Duration**, the lower the sensitivity value, the stricter for the requirement of targets continuously triggering alarm rule.

Alarm Reporting Interval

It is the duration between two alarm reports.

Sensitivity

The higher the sensitivity value, the easier an alarm can be triggered.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Displacement Filter

For **Static Filter**, targets that are static can be filtered. For **Motion Target Filtering** targets that are moving can be filtered.

Linkage With Sub Targets

Main Target Alarm

Alarm will be triggered when the main target is detected. If the sub target is linked, the alarm content will contain the sub target information.

Main Target Link Sub Target Alarm

Alarm will be triggered when the main target is detected and the sub target is linked. The alarm content contains the sub target information.

Main Target Unlink Sub Target Alarm

Alarm will be triggered when the main target is detected, but no sub target is set or linking the sub target to the main target. The alarm content does not contain the sub target information.

16.7.6 Workwear Regist Compare

This algorithm is used to detect whether targets are correctly wearing uniforms or working caps. For uniform detection, please select **Upper Body Detection**. For working cap detection, please select **Head and Shoulder Detection**.

Registration and Comparison Library

Select the library as you needed. Refer to **Registration and Comparison Library** for details about how to configure the library.

When **Type** is set as **Allowable Library**, the pictures in the library are allowable. Hence when the captured picture matches with the ones in the library, no alarms would be triggered. If the captured picture mismatches with the ones in the library, alarms would be triggered.

When **Type** is set as **Unallowable Library**, the pictures in the library are not allowable. Hence when the captured picture matches with the ones in the library, alarms would be triggered.

Target Attribute

Alarms would be triggered according to the target attributes.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Target Quantity

Alarms would be triggered when the number of targets meet the condition of **Symbol** and **Value**.



Note

Only when the device has detected targets, then would the device perform this function.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Continuous Sensitivity

This parameter is based on **Duration**, the lower the sensitivity value, the stricter for the requirement of targets continuously triggering alarm rule.

Alarm Reporting Interval

It is the duration between two alarm reports.

Sensitivity

The higher the sensitivity value, the easier an alarm can be triggered.

Max. Number of Alarm Triggered Times

When a target has triggered a lot of alarms, this is the maximum alarm times of that target.

Custom Info Stream on Stream

When an alarm is triggered for a target in the live view screen, this custom information will be displayed in the upper-left corner of the target for about 1 second.

Confidence Filter

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Overlay Rule Frame on Stream

The device would display rule frame during live view and playback. The rule frame data would be stored together with the video stream on the hard disk.

Overlay Rule Name on Stream

The device would display rule name during live view and playback. The rule name data would be stored together with the video stream on the hard disk.

Displacement Filter

For **Static Filter**, targets that are static can be filtered. For **Motion Target Filtering** targets that are moving can be filtered.

Linkage With Sub Targets

Main Target Alarm

Alarm will be triggered when the main target is detected. If the sub target is linked, the alarm content will contain the sub target information.

Main Target Link Sub Target Alarm

Alarm will be triggered when the main target is detected and the sub target is linked. The alarm content contains the sub target information.

Main Target Unlink Sub Target Alarm

Alarm will be triggered when the main target is detected, but no sub target is set or linking the sub target to the main target. The alarm content does not contain the sub target information.

16.7.7 Motor Vehicle Detection

There are two modes for this algorithm, which are **Normal Mode** and **Gas Station Mode**. Please switch the mode as you required first, and then configure rules.

Go to **VCA → Intelligent Management → Algorithm Management**, and select the motor vehicle detection algorithm card. Thereafter, move the cursor on the engine, and click ⚙️ to switch mode.

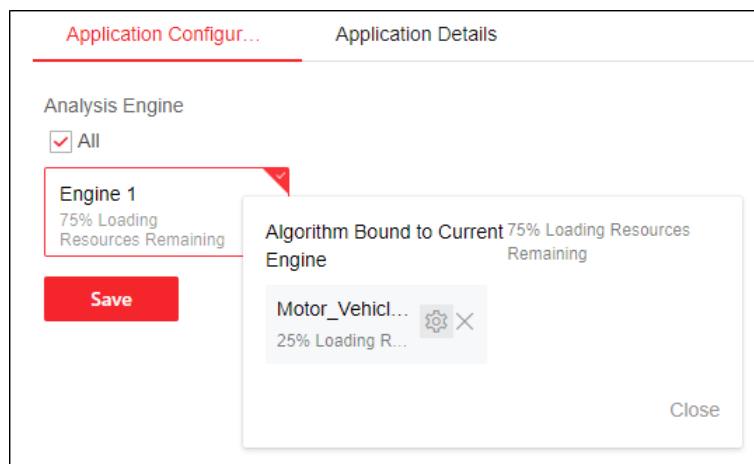


Figure 16-13 Switch Mode

Type

Click **Download Template** to download and edit the template file, then import the file back to your device. Click  to draw a detection area, and the device would detect vehicle license plate number in the detection area. If the detected license plate number matches with the ones in

the template, corresponding **Blocklist/Allowlist** alarms would be triggered. If the detected license plate number mismatches, then it would trigger **Other** alarms.

Area Type

The detection area type.

Refueling Area Entry/Exit Detection Time

When a vehicle is entering or exiting the refueling area, the device would count the time of the action. If the time meet the set value, an alarm would be triggered.



Note

- The detection area should contain the refueling area.
 - The time unit is second.
-

Parking Detection Time

When a vehicle is parking, the device would count the time of the action. If the time meet the set value, an alarm would be triggered.



Note

- The detection area should contain the parking area.
 - The time unit is second.
-

16.7.8 Abnormal Street Event Detection

Abnormal street events include **People Gathering**, **People Running**, **Violent Motion**, and **People Falling Down**. Select an event type as you required.

Size Filtering Settings

Only the targets within the size range (from maximum size to minimum size) will trigger alarms. You can enter maximum and minimum size values below **Size Filtering Settings**, or click  /  on the top of the channel image to draw the maximum size and minimum size.

Duration

Alarms would be triggered when a target continuously triggers alarm rule and the duration has reached the threshold value.

Sensitivity

The higher the sensitivity value, the easier an alarm can be triggered.

Alarm Reporting Interval

It is the duration between two alarm reports.

Confidence

The confidence level of an event refers to the probability that the event meets the alarm condition. When the confidence level of current event is greater than or equal to the set value, an alarm will be triggered.

Alarm Rule Frame Overlay

The device would display and overlay rule frame on the alarm image.

Alarm Target Frame Overlay

The device would display and overlay target frame on the alarm image.

16.7.9 Fire and Smoke Detection

There are three event type, including **Smoke Alarm**, **Fire Detection Alarm**, and **Fire and Smoke Detection Alarm**. Select an event type as you required.

Analysis Mode

Filtering Mode refers to the secondary filtering of algorithm results on the basis of **Normal Mode**. Therefore, **Filtering Mode** is more accurate than **Normal Mode**. **Filtering Mode** applies to scenes with higher algorithm accuracy requirements.

Smoke Detection Sensitivity

The sensitivity of smoke detection. The higher the value is, the more easily the smoke could be detected, and the false alarm rate would be higher.

Fire Detection Sensitivity

The sensitivity of fire detection. The higher the value is, the more easily the smoke could be detected, and the false alarm rate would be higher.

Sky Filtering Sensitivity

It is used to filter false alarms triggered by clouds in the sky. The higher the sensitivity, the poorer the filtering performance.

Secondary Smoke Detection Sensitivity / Secondary Fire Detection Sensitivity

This parameter would be available when **Analysis Mode** is set as **Filtering Mode**. It is similar to the filtering mode, the smoke sensitivity for secondary confirmation is configured based on the normal mode. In a video screen, false alarms are firstly filtered in the normal mode (smoke sensitivity is the sensitivity used for the initial filtering). Then the filtering result will go through another filtering process (smoke sensitivity for secondary confirmation is the sensitivity used for secondary filtering).

Alarm Sensitivity for Night Scene

It is used to reduce false alarms which are caused by night scene. The higher the sensitivity value, the less false alarms would be triggered, however, this would increase false negatives.

Alarm Sensitivity for Raindrop Scene

It is used to reduce false alarms which are caused by raindrop scene. The higher the sensitivity value, the less false alarms would be triggered, however, this would increase false negatives.

Alarm Sensitivity for Mist Scene

It is used to reduce false alarms which are caused by mist scene. The higher the sensitivity value, the less false alarms would be triggered, however, this would increase false negatives.

Sensitivity for Confirming Alarm

The higher the sensitivity value, the quicker an alarm would be confirmed and triggered, this would reduce the alarm accuracy. When the sensitivity value is low, targets have to constantly trigger alarm rules for a long time, then would alarms being triggered.

Alarm Rule Frame Overlay

The device would display and overlay rule frame on the alarm image.

Alarm Target Frame Overlay

The device would display and overlay target frame on the alarm image.

16.7.10 People Counting

People Counting Statistics is used to count the people entering, exiting and passing by a specific scene, such as the supermarket, museum that features a large flow of people. **Regional People Counting** is used to count the people in a fixed area, alarms would be triggered when the detected number of people meet the condition value.

People Counting Statistics

Alarm Upload Interval

It is the duration between two alarm reports.

Flow Overlay

None

Do not overlay.

Enter

Overlay the number of people who enter this region in real time in the live-view video streams.

Leave

Overlay the number of people who leave this region in real time in the live-view video streams.

Enter/Leave

Overlay the number of people who enter and leave this region in real time in the live-view video streams.

Daily Reset Time

The daily counting number would be reset according to the time.

OSD Clearing

If OSD overlay is enabled, you can click **Manual Reset** the reset the OSD value.

Regional People Counting

People / Mode

Alarms would be triggered when the detected number of people meet the condition value.

Flow Overlay

The number of people would be overlaid on live view image.

Alarm Rule Frame Overlay

The device would display and overlay rule frame on the alarm image.

16.7.11 Facial Recognition

The configuration steps are similar with the ones in **Target Event** . Refer to the previous section for reference.

16.7.12 Perimeter Protection

The configuration steps are similar with the ones in **Perimeter Protection** . Refer to the previous section for reference.

Chapter 17 System Parameter Settings

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

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

Table 17-1 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.
Time Configuration	Time Sync Mode	NTP Time Sync Your device can connect to a network time protocol (NTP) server to ensure that the system time is accurate. Manual Time Sync Manually set the system time.
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 18 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.

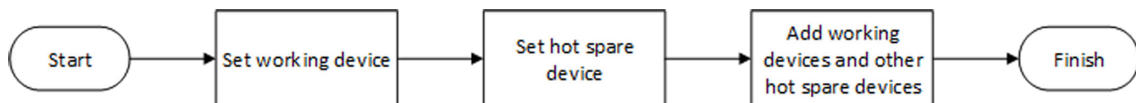


Figure 18-1 Build a Hot Spare System

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.
-

18.1 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**.

18.2 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.

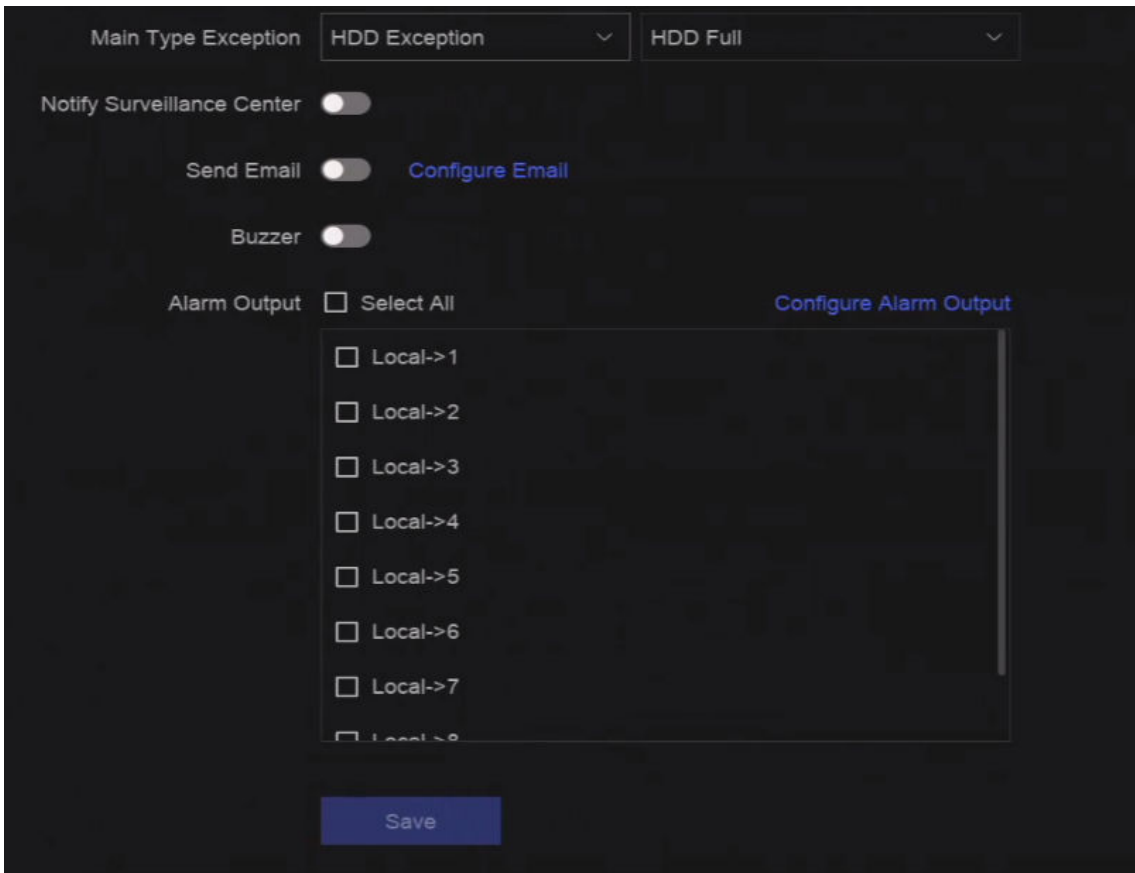
-
4. Go to **System → System Management → N+M Hot Spare** again.
 5. Add working devices to the hot spare system.
 6. Add hot spare devices to the hot spare system.
 7. Click **Save**.

Chapter 19 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** .



The screenshot shows the 'Exception' configuration page. At the top, there are two dropdown menus: 'Main Type Exception' set to 'HDD Exception' and 'HDD Full'. Below these are three toggle switches: 'Notify Surveillance Center' (off), 'Send Email' (off), and 'Buzzer' (on). To the right of the 'Send Email' toggle is a blue link 'Configure Email'. Below the 'Buzzer' toggle is another blue link 'Configure Alarm Output'. Under 'Alarm Output', there is a checkbox 'Select All' and a list of checkboxes labeled 'Local->1' through 'Local->8'. At the bottom is a blue 'Save' button.

Figure 19-1 Exception Event Configuration

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

Table 19-1 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 20 View System Info

Go to **System** → **System Maintenance** → **System Info** → **System Info** to view the system information.

Chapter 21 System Maintenance

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

21.1 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.

21.2 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.

21.3 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.

21.4 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.

21.5 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**.

21.6 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 21-1 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.

Chapter 22 Security Management

22.1 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**.

22.2 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**.

22.3 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 23 Appendix

23.1 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, $\Phi 5.5 \times 2.1 \times 10$	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, $\Phi 5.5 \times 2.1 \times 10$	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, $\Phi 2.1$	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.

23.2 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.

23.3 Frequently Asked Questions

23.3.1 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.

23.3.2 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.

23.3.3 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.

23.3.4 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.

23.3.5 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.

23.3.6 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.

23.3.7 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.

23.3.8 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.

23.3.9 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.

23.4 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 23-1 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 ₂ S (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 23-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H ₂ S (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 _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.



See Far, Go Further