



# **Network Video Recorder**

**User Manual**

## Legal Information

### About this Document

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

### About this Product

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



### Acknowledgment of Intellectual Property Rights

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

### **LEGAL DISCLAIMER**

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

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

## Regulatory Information

### FCC Information

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

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

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

### FCC Conditions

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

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

### EU Conformity Statement



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



2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the



purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: <http://www.recyclethis.info> .

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

## 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
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P

## Network Video Recorder User Manual

---

Series	Model
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S(	DS-7608NXI-I2/8P/S(
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S

## Network Video Recorder User Manual

---

Series	Model
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S
DS-9600NXI-I8/S	DS-9616NXI-I8/S
	DS-9632NXI-I8/S
	DS-9664NXI-I8/S
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X






## 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.
- 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,

## Network Video Recorder User Manual

---

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




## Content Convention

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

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

## Symbol Conventions

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

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

# Contents

<b>Chapter 1 Activate via Local Menu .....</b>	<b>1</b>
<b>Chapter 2 Log In to Your Device .....</b>	<b>3</b>
<b>Chapter 3 User Interface Introduce .....</b>	<b>4</b>
<b>Chapter 4 Network Settings .....</b>	<b>6</b>
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 and Network Camera Occupation Detection .....	8
4.2 Platform Access Settings .....	9
4.2.1 Configure Hik-Connect .....	9
4.2.2 Configure OTAP .....	10
4.2.3 Configure ISUP .....	11
4.2.4 Configure SDK Service .....	12
4.2.5 Enable ISAPI .....	12
4.2.6 Configure ONVIF .....	12
4.2.7 Configure Log Server .....	13
4.3 Network Service Settings .....	13
4.3.1 Configure HTTP(S) .....	13
4.3.2 Configure RTSP .....	13
4.3.3 Configure WebSocket(s) .....	14
4.3.4 Configure Port Mapping (NAT) .....	14
<b>Chapter 5 User Management .....</b>	<b>16</b>
<b>Chapter 6 Device Access .....</b>	<b>17</b>
6.1 Access Video Device .....	17
6.1.1 Add Automatically Searched Online Network Camera .....	17

6.1.2 Add Network Camera Manually .....	17
6.1.3 Add Network Camera via Custom Protocol .....	18
6.1.4 Add Network Camera through Camera Configuration File .....	20
6.2 Add Access Control Device .....	20
6.3 Add Audio Device .....	20
6.4 Add POS Device .....	20
<b>Chapter 7 Camera Settings .....</b>	<b>23</b>
7.1 Enable H.265 Stream Access .....	23
7.2 Batch Configuration .....	23
7.3 Display Settings .....	23
7.4 Configure Video Parameters .....	24
7.5 Configure Privacy Mask .....	25
<b>Chapter 8 Device Grouping .....</b>	<b>26</b>
<b>Chapter 9 Storage Management .....</b>	<b>27</b>
9.1 Manage HDD .....	27
9.2 RAID Configuration .....	27
9.2.1 Create Disk Array .....	28
9.2.2 Rebuild Array .....	30
9.2.3 Delete Array .....	30
9.2.4 View Firmware Info .....	30
9.3 Configure Storage Mode .....	31
9.4 Configure Other Storage Parameters .....	31
<b>Chapter 10 Schedule Configuration .....</b>	<b>33</b>
10.1 Configure Schedule Template .....	33
10.2 Configure Recording Schedule .....	34
10.3 Configure Picture Capture Schedule .....	36
10.4 Configure Audio Recording .....	38
<b>Chapter 11 Live View .....</b>	<b>39</b>

11.1 Configure Live View Layout .....	39
11.2 GUI Introduction .....	39
11.3 PTZ Control .....	40
<b>Chapter 12 Playback .....</b>	<b>42</b>
12.1 GUI Introduction .....	42
12.2 Normal Playback .....	43
12.3 Event Playback .....	44
12.4 Slice Playback .....	44
<b>Chapter 13 Event Center .....</b>	<b>46</b>
13.1 Event Settings .....	46
13.1.1 Basic/Generic Event .....	46
13.1.2 Perimeter Protection .....	48
13.1.3 Abnormal Behavior Event .....	51
13.1.4 Target Event .....	53
13.1.5 Thermal Camera Detection .....	55
13.1.6 Alarm Input Event .....	57
13.1.7 Audio Analysis Event .....	58
13.2 Linkage Configuration .....	60
13.3 Event Search .....	61
13.4 View Alarms .....	62
<b>Chapter 14 Search and Backup .....</b>	<b>63</b>
<b>Chapter 15 Smart Settings .....</b>	<b>65</b>
15.1 Algorithm Management .....	65
15.2 Task Management .....	65
15.3 List library Management .....	65
15.3.1 Add a List Library .....	65
15.3.2 Upload Face Pictures to the Library .....	66
<b>Chapter 16 Application Center .....</b>	<b>67</b>



16.1 Human and Vehicle Detection .....	67
16.2 Person Check-In .....	67
16.2.1 Add Check-In Task .....	67
16.2.2 Search Check-In Records .....	68
16.3 Statistic Report .....	69
<b>Chapter 17 System Parameter Settings .....</b>	<b>70</b>
<b>Chapter 18 Hot Spare Device Backup .....</b>	<b>71</b>
18.1 Set Working Device .....	71
18.2 Set Hot Spare Device .....	71
<b>Chapter 19 Configure Exception Event .....</b>	<b>73</b>
<b>Chapter 20 View System Info .....</b>	<b>75</b>
<b>Chapter 21 System Maintenance .....</b>	<b>76</b>
21.1 Schedule Reboot .....	76
21.2 Upgrade Device .....	76
21.3 Backup and Restore .....	76
21.4 Log Info .....	77
21.5 Configure Log Server .....	77
21.6 Maintenance Tools .....	77
<b>Chapter 22 Security Management .....</b>	<b>79</b>
22.1 Address Filter .....	79
22.2 Stream Encryption .....	79
22.3 Select TLS Version .....	79

## 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.

---

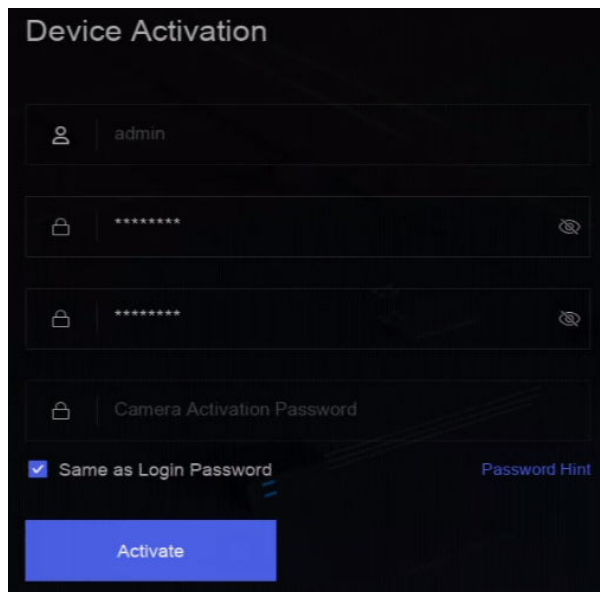


Figure 1-1 Activate via Local Menu

4. Enter a password to activate network cameras that are connected to the device.
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.

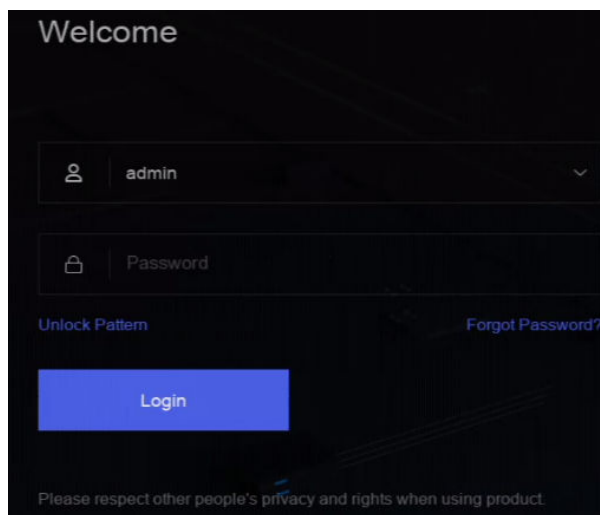


Figure 2-1 Login

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.
-

## 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.

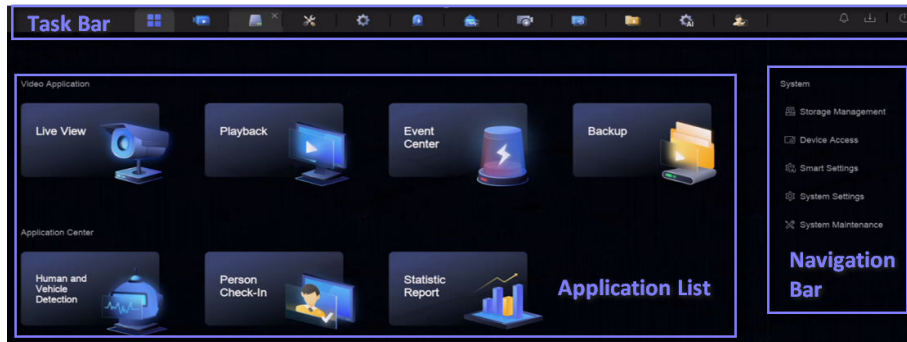


Figure 3-1 Main Function Page

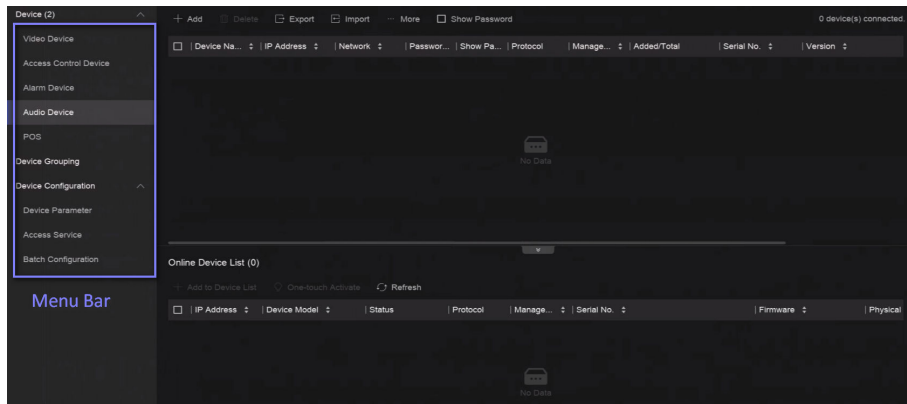


Figure 3-2 Video Application

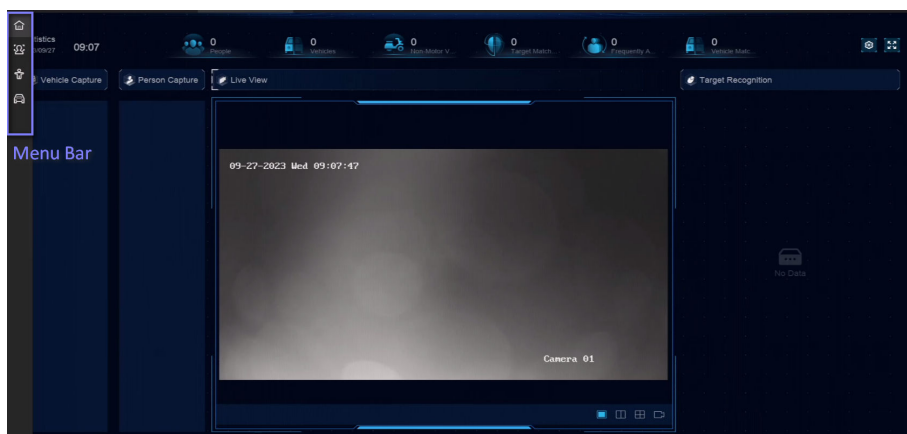








Figure 3-3 Application Center

**Table 3-1 Interface Introduction**

Interface Name	Introduction
Task Bar	<p>The opened applications are listed in the task bar. You can move and close each application tab.</p> <p>Icon introduction :</p> <ul style="list-style-type: none"><li>•  : Main menu.</li><li>•  : Event center. Event alarms can be searched and viewed.</li><li>•  : The download progress of each download task can be viewed here.</li><li>•  : Shut down, log out, or reboot your device.</li></ul>
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	<p>Configurable items of each application are listed here.</p> <p> <b>Note</b></p> <p>For applications in <b>Application Center</b>, you can click  , or right click to display the menu bar.</p>

## Chapter 4 Network Settings

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

### 4.1 Network Parameter Settings

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

#### 4.1.1 Configure TCP/IP

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

##### Steps

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

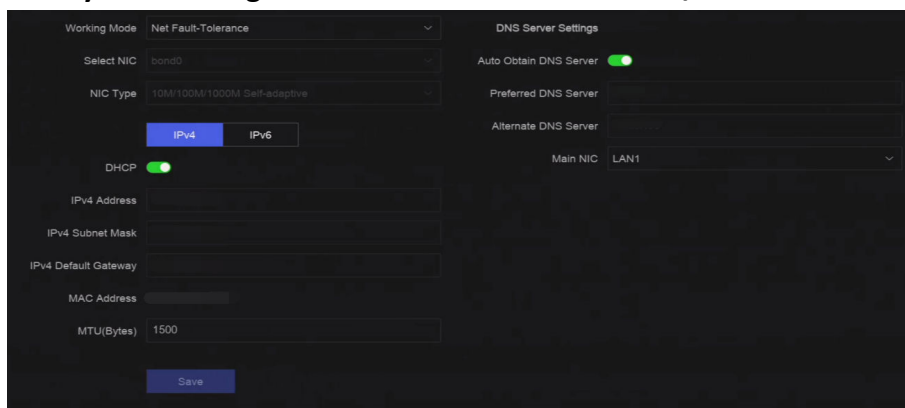


Figure 4-1 TCP/IP Settings

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

##### Multi-address

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

##### Net-fault Tolerance

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



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** .



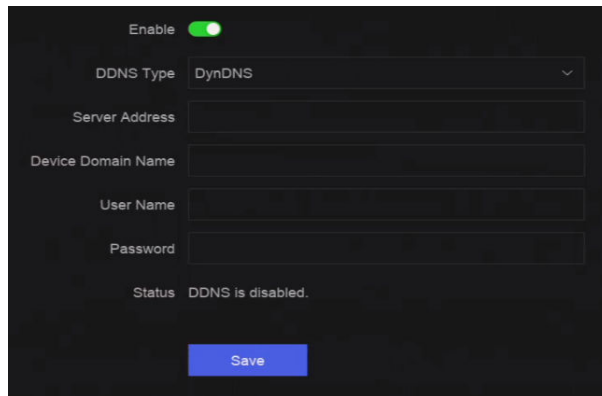


Figure 4-2 DDNS

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** .

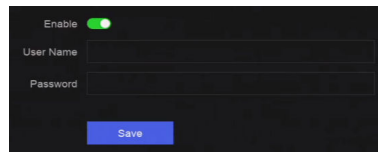


Figure 4-3 PPPoE

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 and Network Camera Occupation Detection

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network. After enabling network camera occupation detection, when searching network cameras, network cameras that have been added by another device will be marked.

## Steps

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

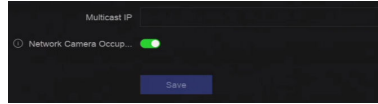


Figure 4-4 Other Settings

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. **Optional:** Turn on **Enable Network Camera Occupation Detection**.

4. 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** → **Platform Access** → **Hik-Connect** .

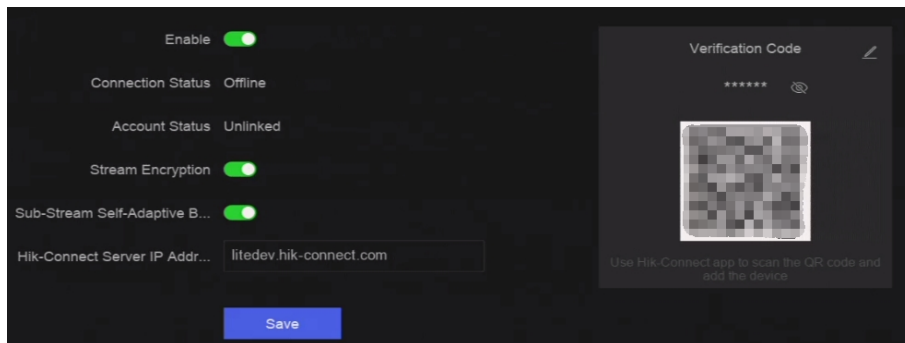



Figure 4-5 Hik-Connect

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**, 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.

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 4-6 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** .
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** .
2. Turn on **Enable**.



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



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



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** → **CX** → **System Settings** → **Network** → **Platform Access** → **Log Server** .
2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. 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** → **TCP/IP** .
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** .
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** .
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

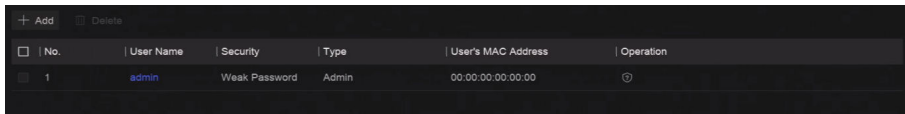
Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.



## 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.
<b>Add</b>	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.

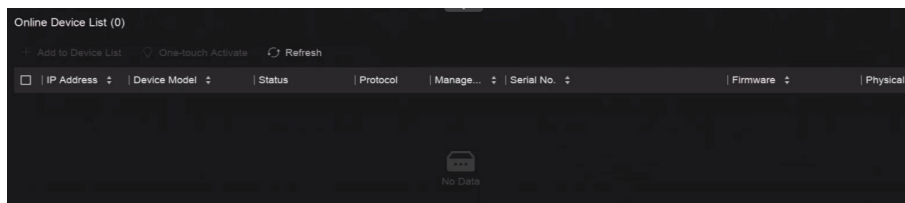


Figure 6-1 Add Automatically Searched Online Network Camera

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

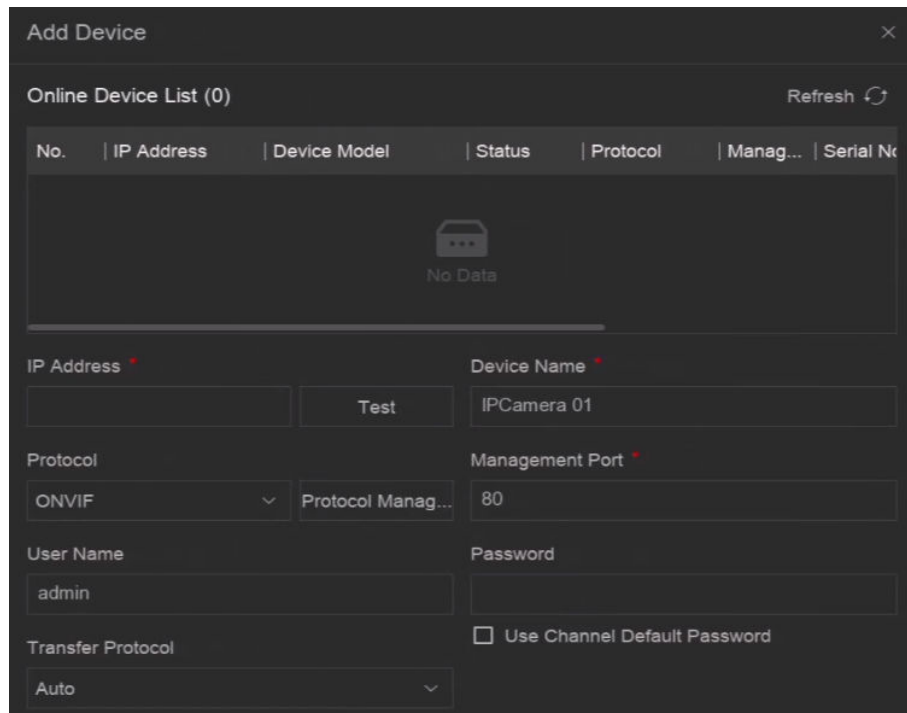
Manually add the network cameras to your video recorder.

## 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 via Custom Protocol

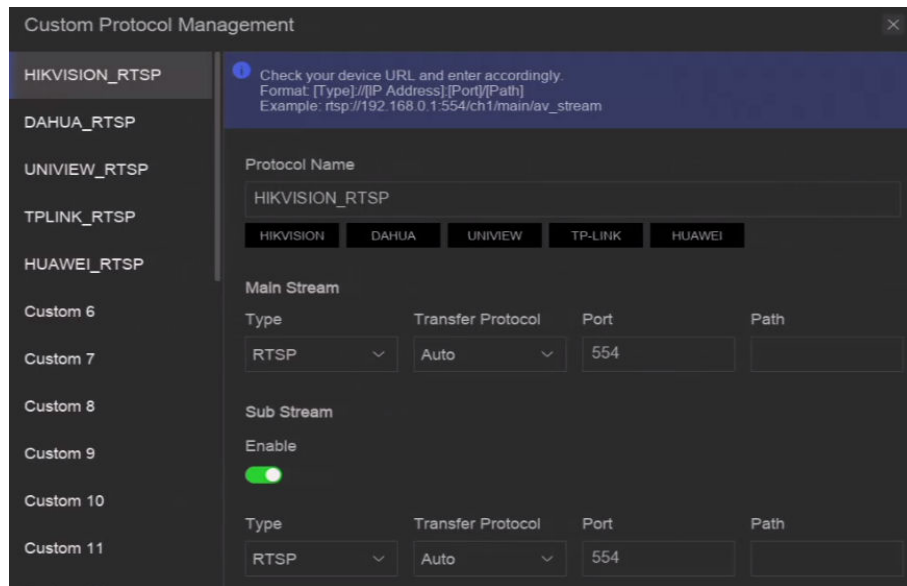
For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

## 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*.



- **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.

### 6.1.4 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.

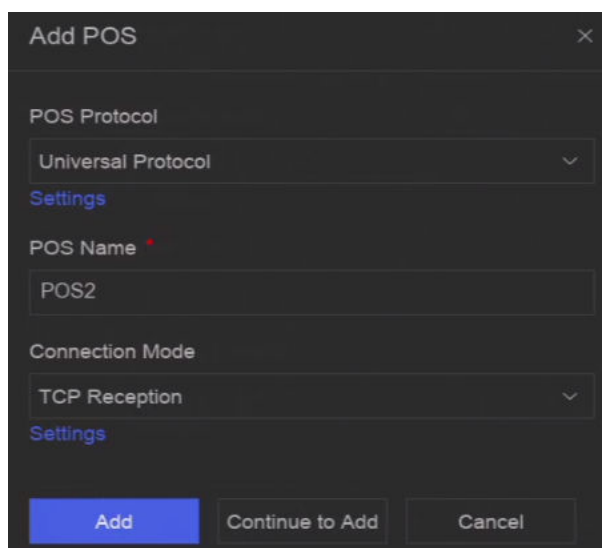
The adding process is similar with [\*\*Access Video Device\*\*](#) .

## 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.

---

## Chapter 7 Camera Settings

You can configure the added camera, such as privacy mask, image parameters, etc.

### 7.1 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**.

### 7.2 Batch Configuration

Cameras can be configured in a batch.

#### Steps

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

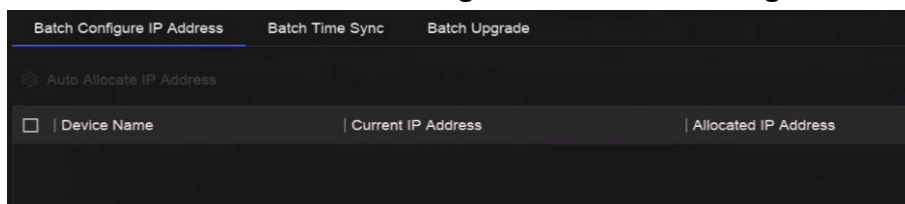


Figure 7-1 Batch Configuration

2. Configure IP address, sync time, or upgrade firmware as your desire.
3. For IP address configuration and time sync, click **Save**.

### 7.3 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.

## 7.4 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.

## 7.5 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** .

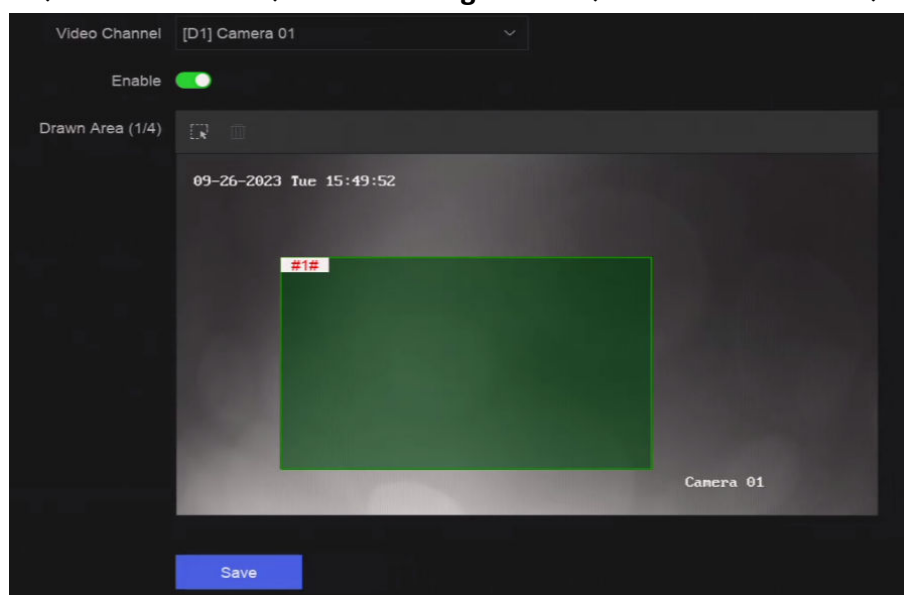


Figure 7-2 Privacy Mask

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**.

## Chapter 8 Device Grouping

The added devices can be classified into different customized groups.

### Steps

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

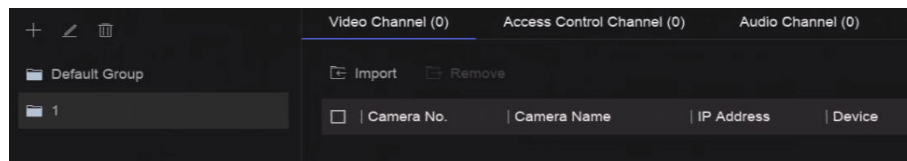




Figure 8-1 Device Grouping

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 9 Storage Management

## 9.1 Manage HDD

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

### Before You Start

Ensure the HDD is properly installed to your device.

### Steps

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

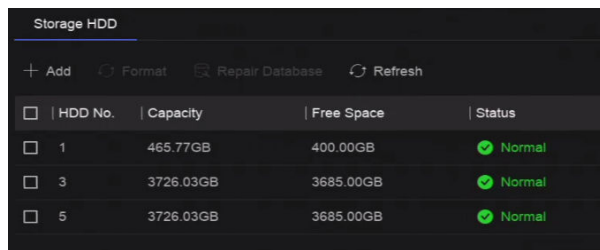


Figure 9-1 Manage HDD

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

- Add** 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

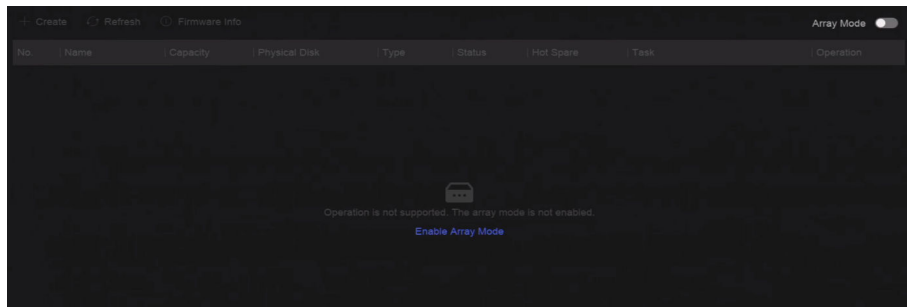
A disk array can be created after enabling array mode.

### 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

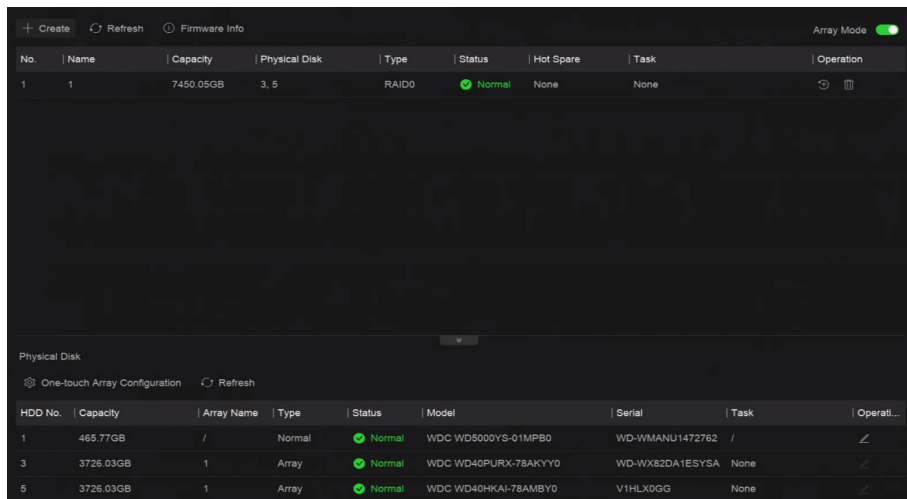
1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Enable Array Mode**, or enable **Array Mode**.



**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**

Description

**One-touch Array Configuration**

Click **One-touch Array Configuration**.

**Note**

By default, the array type created by one-touch configuration is RAID 5.

**Manual Creation**

Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.



### 9.2.2 Rebuild Array

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

#### Steps

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

**Table 9-2 Rebuilding Method**

Rebuilding Method	Description
Auto Rebuild	<p>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 <b>Operation</b> column under <b>Physical Disk</b> to set a hot spare disk.</p> <p>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.</p> <p> <b>Note</b> After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.</p>
Manual Rebuild	<p>If there is no hot spare disks in the array, you have to manually rebuild the array.</p> <p>Go to <b>System → Storage Management → Storage HDD → Array Management</b> , and select the hot spare disk in the list to rebuild.</p>

### 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.

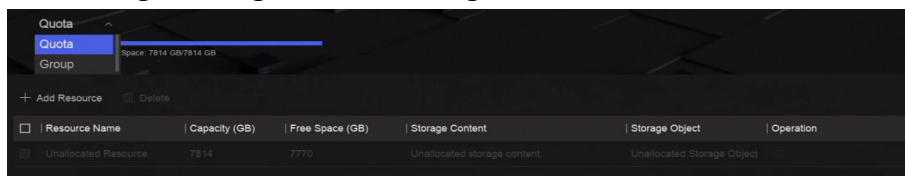
**Steps**

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 <b>Event Center</b> .



Parameter Name	Description
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	<p>After adding a tag to a video, it is the time you set to record after the scheduled time.</p> <p> <b>Note</b></p> <ul style="list-style-type: none"><li>• You can click  during live view or playback to add a tag.</li><li>• For searching tag videos, go to  → <b>Backup</b> → <b>By Tag</b> .</li></ul>

## Chapter 10 Schedule Configuration

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

### 10.1 Configure Schedule Template

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

#### Steps

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

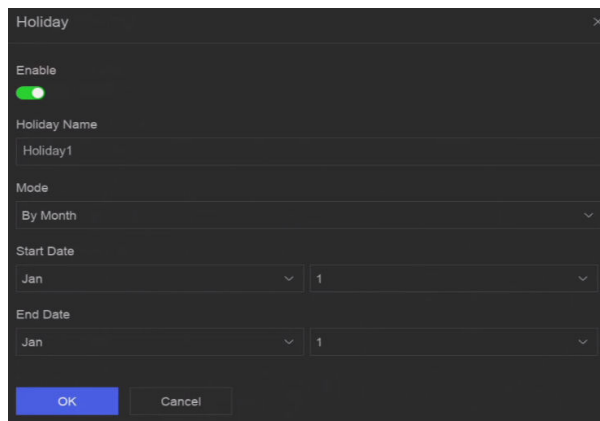


Figure 10-1 Add Holiday

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

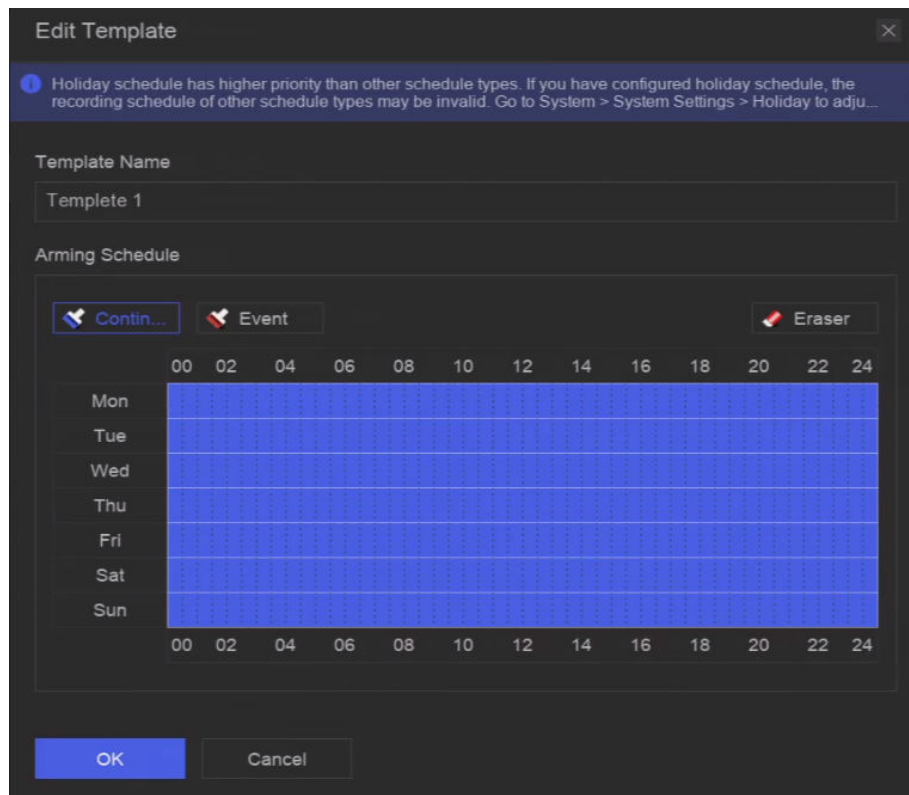
---

#### **Note**

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

---

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




**Figure 10-2 Edit Template**

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

---

**Note**

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

---

**Note**

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

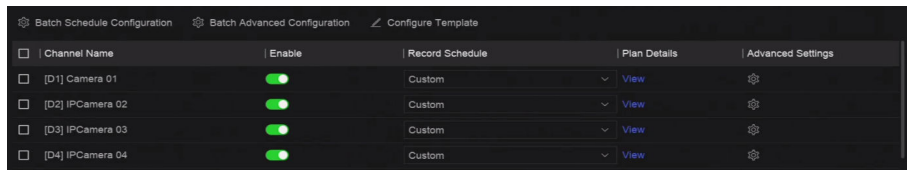
6. Click **OK**.

## 10.2 Configure Recording Schedule

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

### Steps

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



**Figure 10-3 Video Recording Configuration**

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

**Note**

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

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




**Figure 10-4 View Schedule**

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

**Table 10-1 Advanced Parameter Description**

Parameter	Description
Record Audio	Enable or disable audio recording.

Parameter	Description
	 <b>Note</b> 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.
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 <b>Main Stream</b> , its resolution is usually higher. For <b>Sub-Stream</b> , you can record for a longer time with the same storage space, but its resolution would be low. For <b>Dual Stream</b> , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

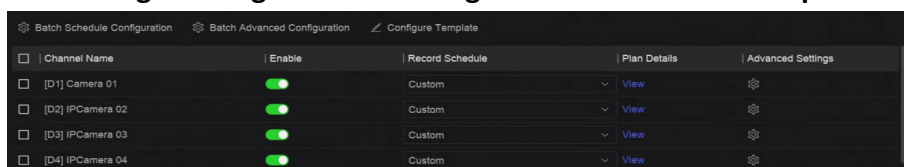
**7.** Click **Save**.

## 10.3 Configure Picture Capture Schedule

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

### Steps

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




**Figure 10-5 Picture Capture Configuration**

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

**3.** Select a schedule type.

 **Note**

If you set **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 10-6 View Schedule**

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

**Table 10-2 Advanced Parameter Description**

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

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

## 10.4 Configure Audio Recording


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

### Steps

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

---

### Note

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

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

**Table 10-3 Advanced Parameter Description**

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




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

## Chapter 11 Live View

### 11.1 Configure Live View Layout

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

#### Steps

1. Go to **Live view** .
2. Click  at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click .
6. Set the live view image output interface.
7. Click .

### 11.2 GUI Introduction

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

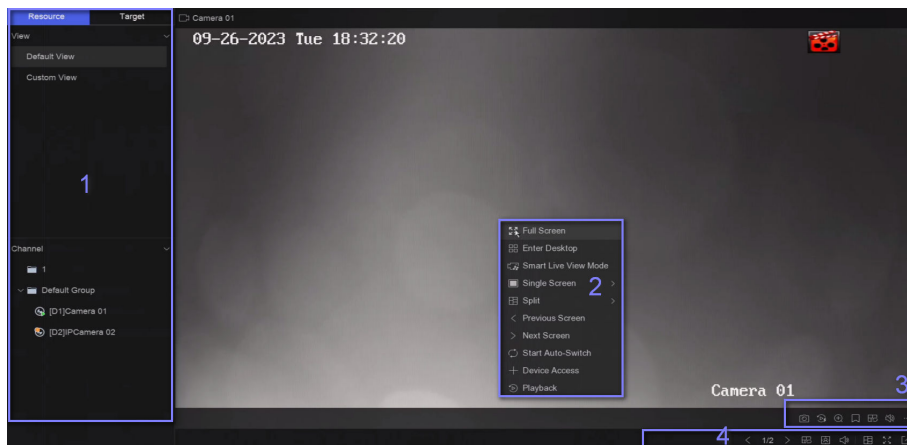





Figure 11-1 Live View

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	Channel tool bar.









No.	Description
	<ul style="list-style-type: none"> <li>Click  to add a tag to the channel. After adding, you can go to  → <b>Backup</b> → <b>By Tag</b> to search videos by tag.</li> <li>You can select  → <b>Show VCA Info</b> to display rule frames.</li> </ul>
4	Live view tool bar.

### 11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is added 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 expand 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: <ol style="list-style-type: none"> <li>1. Select a preset.</li> <li>2. Use to direction buttons to adjust the image.</li> <li>3. Click .</li> </ol>
		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 correspond to the presets.	Set a patrol: <ol style="list-style-type: none"> <li>1. Select a patrol.</li> <li>2. Click .</li> <li>3. Add presets for the patrol.</li> <li>4. Click <b>OK</b>.</li> </ol>
		Call a patrol: Click  .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: <ol style="list-style-type: none"> <li>1. Click .</li> <li>2. Use to direction buttons to adjust the image, the device will record the movement.</li> <li>3. Stop recording.</li> </ol>
		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.

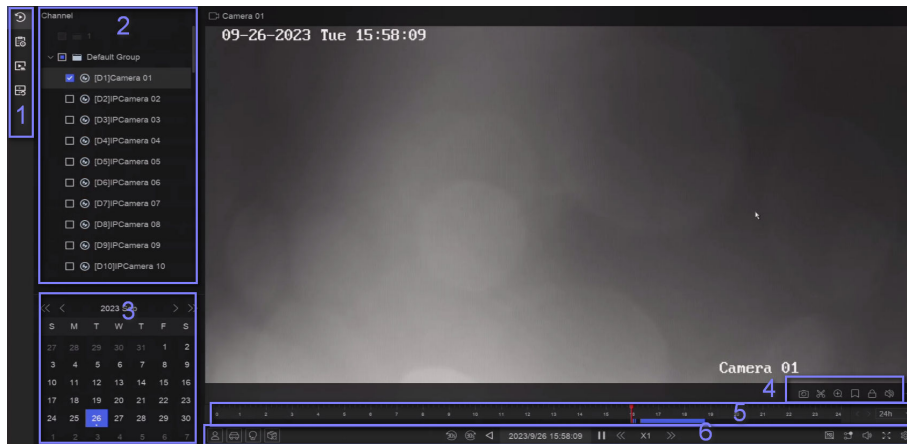













Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	<p>Channel tool bar.</p> <ul style="list-style-type: none"> <li>Click  to add a tag go the channel. After adding, you can go to  → <b>Backup</b> → <b>By Tag</b> to search videos by tag.</li> <li>Click  to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to  → <b>Backup</b> → <b>By Tag</b> to search videos by lock.</li> <li>Select  → <b>Dual-VCA</b> to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type.</li> </ul>

No.	Description
	<p> <b>Note</b></p> <p>In order to use this function, go to <b>Configuration</b> → <b>Device Access</b> → <b>Device Configuration</b> → <b>Device Parameter</b> → <b>Display Info. on Screen</b> to turn on <b>Enable Dual-VCA</b> via web browser, and go to <b>System</b> → <b>Storage Management</b> → <b>Advanced Settings</b> to turn on <b>Save Camera VCA Data</b> via local GUI interface.</p> <ul style="list-style-type: none"> <li>You can select  → <b>Show VCA Info</b> to display rule frames.</li> </ul>
5	<p>Playback timeline.</p> <ul style="list-style-type: none"> <li>Position the cursor on the timeline, drag the timeline to position to a certain time.</li> <li>Period marked with blue bar contains video. Red bar indicates the video in the period is event video.</li> <li>Scroll up/down to zoom out/in timeline.</li> </ul>
6	<p>Playback tool bar.</p> <ul style="list-style-type: none"> <li>Click  /  to show videos that contain human/vehicle.</li> </ul> <p> <b>Note</b></p> <p>In order to use this function, ensure you have configured <b>Detection Target</b> as <b>Human</b> or <b>Vehicle</b> for certain event types.</p> <ul style="list-style-type: none"> <li>Click  to set normal video and smart video (the video that contains smart data) playback strategy.</li> </ul>

## 12.2 Normal Playback

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

### Steps

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

---

 **Note**

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

---

3. Select a date in the calendar.



---

## Note

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

---

### 4. **Optional:** 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.
- 

## Note

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

---

3. Click  → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
  4. Click **Search**.  
Videos meet the detection rule requirement will be marked in red.
  5. Click  to set normal video and smart video (the video that contains smart data) playback strategy.
- 

## Note


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

---

## 12.4 Slice Playback

Divide the video into slices and play them back.

### Steps

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

**4. Click Search.**

The retrieved video will be divided into one-hour slices for playback.


**5. Optional:** Select an one-hour slice and click  to divide it into one-minute slices for playback.

## 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.	<p>Use the tool bar at the top of image to draw the detection area.</p> <p><b>AI by NVR</b></p> <p>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.</p> <p><b>AI by Camera</b></p> <p>The motion detection event will be analyzed by camera.</p> <p><b>Detection Target</b></p> <p><b>Human and Vehicle</b> are selectable, apart</p>	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	
		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	<p>When an alarm is detected, the selected channel would record videos.</p> <p> <b>Note</b></p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to <b>System → Storage Management → Storage Schedule → Video Recording</b> to configure video recording schedule.</p>


8. Click **Save**.

### 13.1.2 Perimeter Protection

#### Before You Start

If human or vehicle target requires to be detected, ensure your camera supports this function or the engine is running **Perimeter Protection** algorithm.

#### Steps

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 an event type.
5. Turn on **Enable**.
6. Click **Rule Settings** to set the rule.

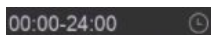
**Table 13-3 Perimeter Protection Events**

Event Name	Event Description	Rule Configuration
Line Crossing 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.	<p>a. Select a rule number.</p> <p>b. Use the tool bar at the top of image to draw the detection line. If <b>Max. Size</b> or <b>Min. Size</b> is configured, only targets that meet the size requirement can trigger alarms.</p> <p>c. Set <b>Direction</b> and <b>Sensitivity</b>.</p> <p><b>Direction</b></p> <p>For <b>A&lt;-&gt;B</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.</p> <p>For <b>A-&gt;B</b>, only the object crossing the configured line from the A side to the B side can be detected. For <b>B-&gt;A</b>, only the object crossing the configured line from the B side to the A side can be detected.</p> <p><b>Sensitivity</b></p> <p>The higher the value is, the easier the detection alarm can be triggered.</p> <p>d. Optional: Select <b>Detection Target</b> as <b>Human</b> or <b>Vehicle</b> to discard alarms which are not triggered by human or vehicle.</p> <p>e. Optional: Repeat the above steps to set another one.</p>
Intrusion 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.	<p>a. Select a rule number.</p> <p>b. Use the tool bar at the top of image to draw the detection area. If <b>Max. Size</b> or <b>Min. Size</b> is configured, only targets that meet the size requirement can trigger alarms.</p> <p>c. Set <b>Time Threshold</b> and <b>Sensitivity</b>.</p> <p><b>Time Threshold</b></p> <p>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.</p> <p><b>Sensitivity</b></p>

Event Name	Event Description	Rule Configuration
		<p>The higher the value is, the easier the detection alarm can be triggered.</p> <p>d. Optional: Select <b>Detection Target</b> as <b>Human</b> or <b>Vehicle</b> to discard alarms which are not triggered by human or vehicle.</p> <p>e. Optional: Repeat the above steps to set another one.</p>
Region Entrance Detection	Region entrance detection detects objects that enter a predefined virtual region.	<p>a. Select a rule number.</p> <p>b. Use the tool bar at the top of image to draw the detection area. If <b>Max. Size</b> or <b>Min. Size</b> is configured, only targets that meet the size requirement can trigger alarms.</p> <p>c. Set <b>Sensitivity</b>. The higher the value is, the easier the detection alarm can be triggered.</p> <p>d. Optional: Select <b>Detection Target</b> as <b>Human</b> or <b>Vehicle</b> to discard alarms which are not triggered by human or vehicle.</p> <p>e. Optional: Repeat the above steps to set another one.</p>
Region Exiting Detection	Region exiting detection detects objects that exit from a predefined virtual region.	

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 13-4 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.

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


9. Click **Save**.

### 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 13-5 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.	<ol style="list-style-type: none"> <li>a. Select a rule number.</li> <li>b. Use the tool bar at the top of image to draw the detection line.</li> <li>c. Set <b>Time Threshold</b> and <b>Sensitivity</b>.</li> </ol> <p><b>Time Threshold</b></p> <p>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].</p> <p><b>Sensitivity</b></p> <p>Similarity of the background image to the object. The higher the value is, more</p>
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	

Event Name	Event Description	Rule Configuration
	region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so 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 <b>Percentage</b> . 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 13-6 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	<p>When an alarm is detected, the selected channel would record videos.</p> <p> <b>Note</b></p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to <b>System → Storage Management → Storage Schedule → Video Recording</b> to configure video recording schedule.</p>

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.	<p><b>Target Grading</b></p> <p>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.</p> <p><b>Non-Real-Time Mode</b></p> <p>For places with a high flow of people, the device processing speed may not be fast enough, <b>Non-Real-Time Mode</b> 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. <b>Non-Real-Time Mode</b> will not trigger real-time alarm, so <b>Arming Schedule</b> is unavailable.</p> <p><b>Linkage Succeeded / Linkage Failed</b></p> <p>When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in <b>Target of Live View</b>.</p>
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  to set specified time schedule.

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

**Table 13-7 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	<p>When an alarm is detected, the selected channel would record videos.</p> <p> <b>Note</b></p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to <b>System</b> → <b>Storage Management</b> → <b>Storage Schedule</b> → <b>Video Recording</b> to configure video recording schedule.</p>

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 13-8 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.


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	<p>When an alarm is detected, the selected channel would record videos.</p> <p> <b>Note</b></p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to <b>System</b> → <b>Storage Management</b> → <b>Storage Schedule</b> → <b>Video Recording</b> to configure video recording schedule.</p>

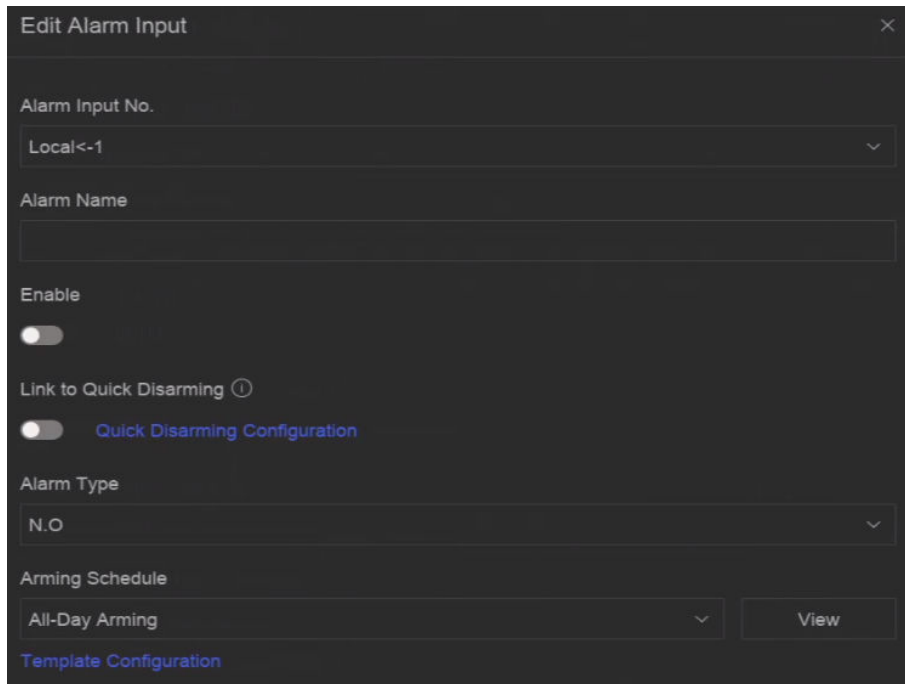
8. Click **Save**.

## 13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

### Steps

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



**Figure 13-1 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.


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 13-10 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	<p>When an alarm is detected, the selected channel would record videos.</p> <p> <b>Note</b></p> <p>Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to <b>System</b> → <b>Storage Management</b> → <b>Storage Schedule</b> → <b>Video Recording</b> to configure video recording schedule.</p>

9. 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 13-11 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.	<p><b>Sudden Increase of Sound Intensity Detection</b> Detects a steep sound increase in the scene.</p> <p><b>Sudden Decrease of Sound Intensity Detection</b> Detects a steep sound drop in the scene.</p> <p><b>Sensitivity</b> The higher the value is, the easier the detection alarm can be triggered.</p> <p><b>Sound Intensity Threshold</b> 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.</p>

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 13-12 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.


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

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 13-13 Email Linkage**

Item	Description
Server Authentication	<b>Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.</b>
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
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.

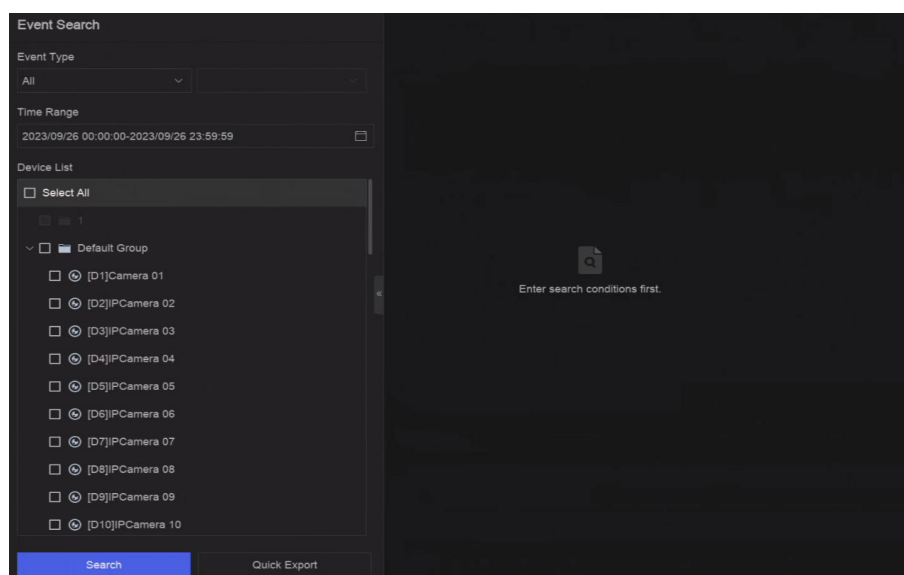
7. Click **Audio Alarm Output** to set the camera speaker.

### 13.3 Event Search

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

**Steps**

1. Go to **Event Center** →  .



**Figure 13-2 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.

## 13.4 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 **Back** .

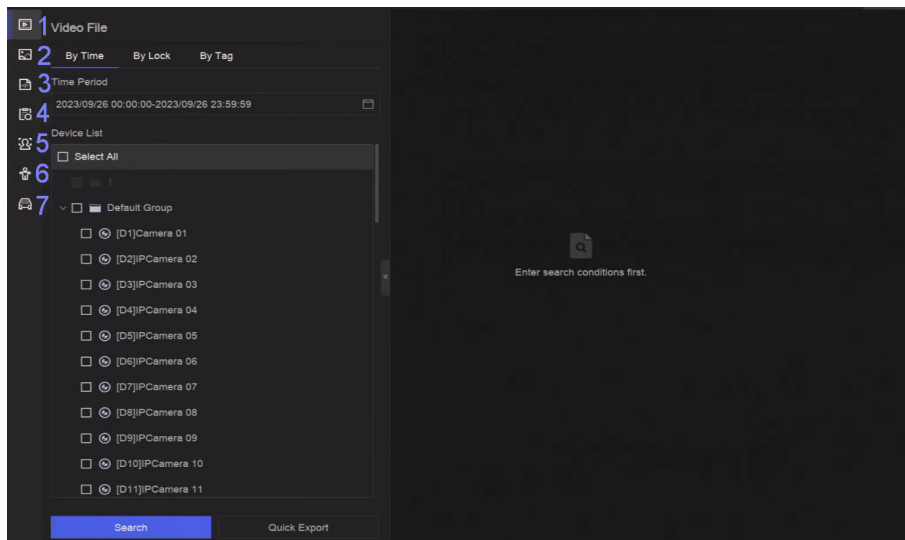


Figure 14-1 Search and Backup

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

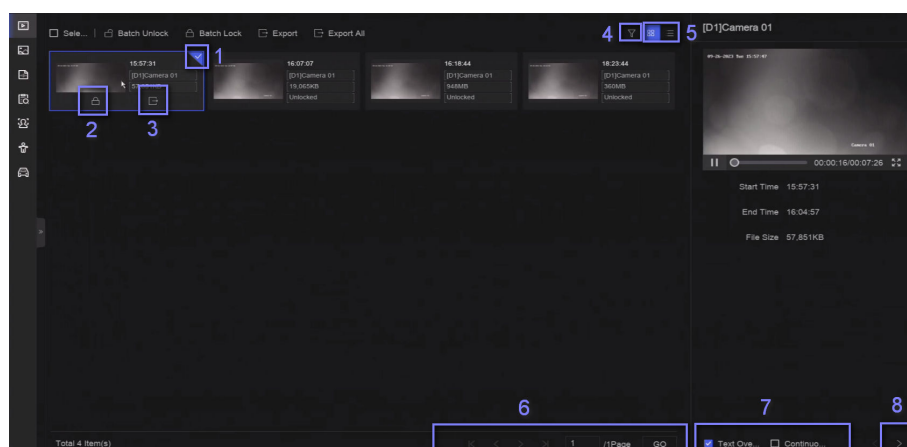
---

### 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 Select file(s) and click **Text Overlay** or **Continuous Play** at the lower-right corner. The select file will overlay text or be played in order.
  - 8 Use the shortcuts at the upper-right corner to play the next/previous file.
- 6.** Insert a USB flash drive to the device for backup.
- 7.** Export files to the USB flash drive.
- Select files(s) in the result list and click **Export**.
  - Click **Export All** to export all the files.

## Chapter 15 Smart Settings

### 15.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** . The available algorithms would be listed, and you can click the required algorithm to link engine(s).

### 15.2 Task Management

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

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

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

#### Disabled

No analysis task is enabled on the camera.

#### Waiting

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

#### Enabled

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

### 15.3 List library Management

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

#### 15.3.1 Add a List Library

##### Steps

1. Go to **System → Smart Settings → Data Archive → List Library** .
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.



## Note

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


### 15.3.2 Upload Face Pictures to the Library

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

#### Before You Start

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


#### Steps

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

#### Delete Pictures from the Library

- Select a picture and delete it.
- Select pictures and click **Delete in Batch** to delete the select ones.

#### Search Pictures in the Library

Click  at the tool bar to search pictures.

#### Copy Pictures to Another Library

Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.

#### Edit Pictures

Click the picture name, and edit its attributes.


#### Export Pictures

Select pictures, and click **Export** to export them to a USB flash drive.

## Chapter 16 Application Center

### 16.1 Human and Vehicle Detection

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

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

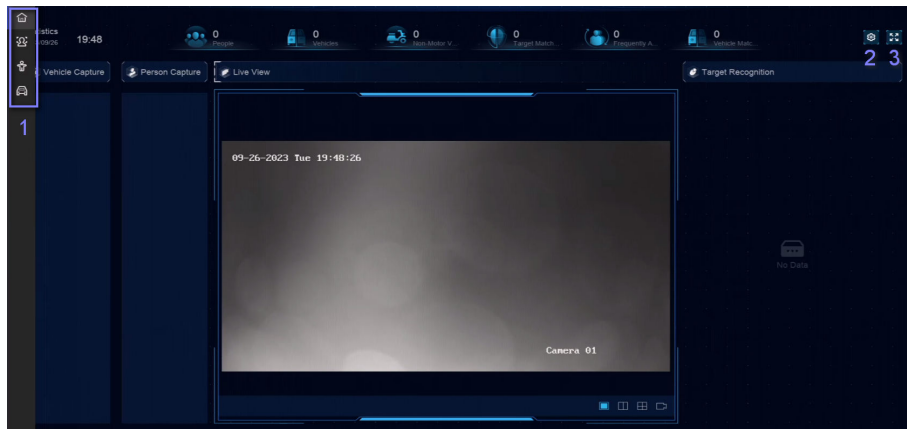


Figure 16-1 Human and Vehicle Detection

Table 16-1 Human and Vehicle Detection Description

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

### 16.2 Person Check-In

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


#### 16.2.1 Add Check-In Task

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

## Before You Start

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

## Steps

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

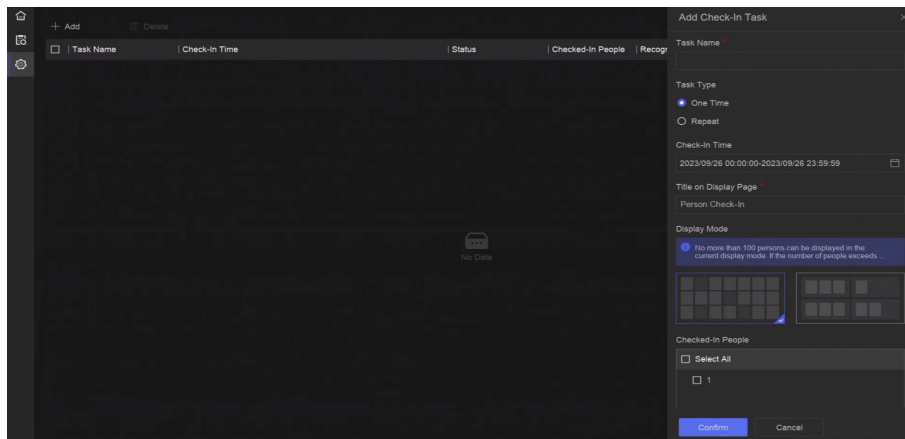


Figure 16-2 Add Check-In Task

## 5. Set Task.

### One-Time

The task will be used for one time.

### Repeat

The task will be used and repeated for several times.

## 6. Configure other parameters, including **Task Name**, **Check-In Time**, **Recognition Channel**, etc.

## 7. Click **Confirm**.

## 16.2.2 Search Check-In Records

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

## Before You Start

Ensure check-in tasks are configured.

## Steps

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

3. Click .

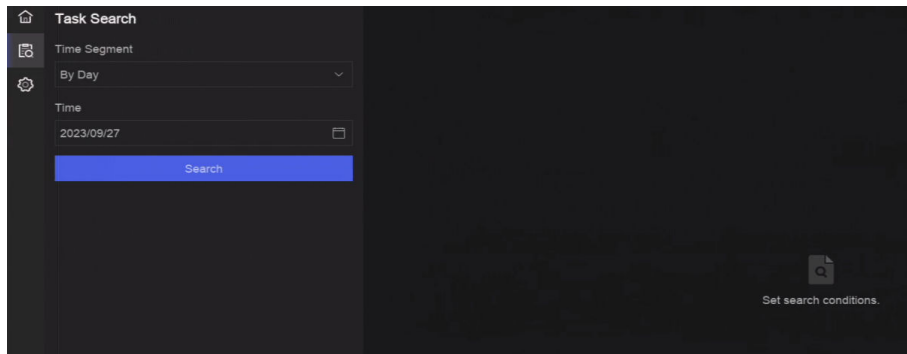




Figure 16-3 Search Check-In Records

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

## 16.3 Statistic Report

You can view reports of people counting and heat map.

Table 16-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		<ul style="list-style-type: none"> <li>• The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device.</li> <li>• Camera statistic data can be stored to the device HDD.</li> </ul>	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.
Heat Map		<ul style="list-style-type: none"> <li>• The function must be supported by the connected IP camera.</li> <li>• Camera statistic data can be stored to the device HDD.</li> </ul>	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

## Chapter 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	<p><b>NTP Time Sync</b></p> <p>Your device can connect to a network time protocol (NTP) server to ensure that the system time is accurate.</p> <p><b>Manual Time Sync</b></p> <p>Manually set the system time.</p>
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	<p><b>Console</b></p> <p>After connecting it to PC with a convertor, PC can set the device parameters.</p> <p><b>Transparent Channel</b></p> <p>It is directly connected to a serial device. PC can remotely access the serial device through network.</p>

## 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.
-



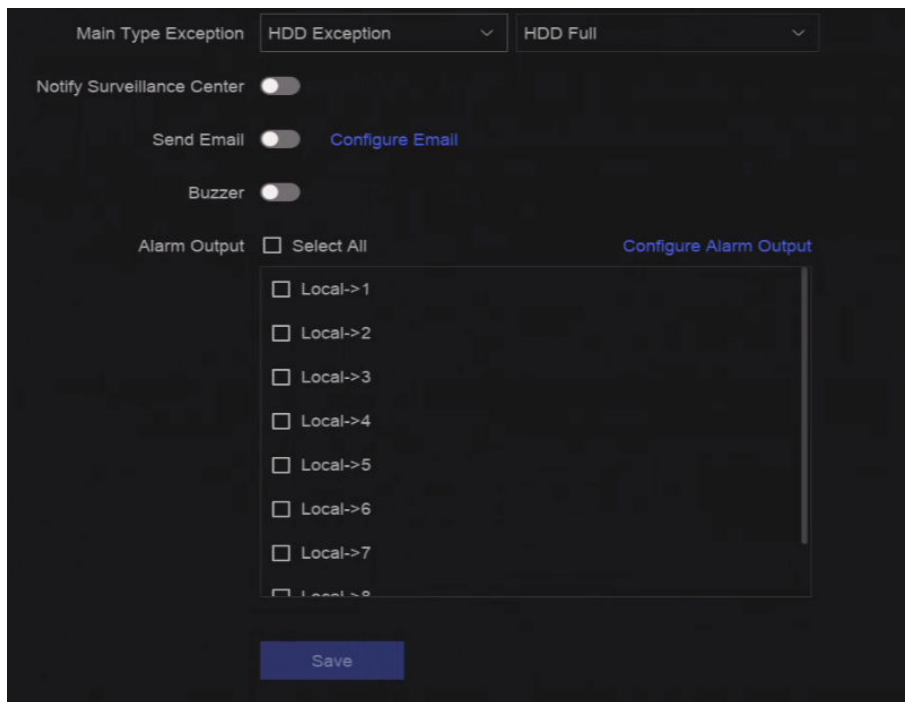
4. Go to **System** → **System Management** → **N+M Hot Spare** again.
5. Add working devices to the hot spare system.
6. Add hot spare devices to the hot spare system.
7. Click **Save**.

## 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** .



**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.

Linkage Method	Description
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**

<b>Tool Name</b>	<b>Description</b>
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	<b>Ping</b> The ping test is used to detect whether the destination IP address is reachable. <b>NIC Packet Capture</b>

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 <a href="#">??</a>	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

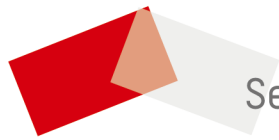
The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.

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.





See Far, Go Further