



# **Network Video Recorder**

**User Manual**

## Legal Information

©2021 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

### About this Manual

The Manual 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 Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website ( <https://www.hikvision.com/> ).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

### Trademarks

**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.



: 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.

### Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL 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

## Network Video Recorder User Manual

---

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 MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

## Regulatory Information

### FCC Information

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

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference 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>.

### Industry Canada ICES-003 Compliance

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

## Applicable Model




This manual is applicable to the following models.

**Table 1-1 Applicable Model**

Series	Model
iDS-6700NXI-I/BA	iDS-6704NXI-I/BA
iDS-9600NXI-I8/BA	iDS-9632NXI-I8/BA

## 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.


## 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 equipment and shall be easily accessible.
- ⚡ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Never place the equipment in an unstable location. The equipment 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 product contains a coin/button cell battery. If the battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- 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.
- 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.



## 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 equipment shall not be exposed to dripping or splashing and that no objects filled with liquids shall be placed on the equipment, such as vases.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment 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 equipment which is used with, or generates direct current.
- - identifies the negative terminal(s) of equipment 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.
- Use only power supplies listed in the user manual or user instruction.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Use only power supplies listed in the user manual or user instruction.
- 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.

# Contents

<b>Chapter 1 Basic Operation .....</b>	<b>1</b>
1.1 Activate Your Device .....	1
1.1.1 Default User and IP Address .....	1
1.1.2 Activate via Local Menu .....	1
1.1.3 Activate via SADP .....	3
1.1.4 Activate via Client Software .....	4
1.1.5 Activate via Web Browser .....	6
1.2 Configure TCP/IP Settings .....	7
1.3 HDD Settings .....	8
1.4 Add Network Camera .....	8
1.4.1 Add Automatically Searched Online Network Camera .....	9
1.4.2 Add Network Camera Manually .....	9
1.4.3 Add Network Camera via Customized Protocol .....	10
1.5 Platform Access .....	11
1.5.1 Configure Hik-Connect .....	11
1.5.2 Configure ISUP .....	13
<b>Chapter 2 Camera Settings .....</b>	<b>15</b>
2.1 Configure Image Parameters .....	15
2.2 Configure OSD Settings .....	15
2.3 Configure Privacy Mask .....	16
2.4 IP Camera Time Sync .....	17
2.5 Import/Export IP Camera Configuration Files .....	18
2.6 Upgrade IP Cameras .....	18
<b>Chapter 3 Live View .....</b>	<b>19</b>
3.1 Start Live View .....	19
3.1.1 Configure Live View Settings .....	19

3.1.2 Configure Live View Layout .....	20
3.2 Configure Auto-Switch of Cameras .....	21
3.3 Digital Zoom .....	22
3.4 Fisheye View .....	22
3.5 POS Information Overlay .....	23
3.6 3D Positioning .....	23
3.7 Live View Strategy .....	24
3.8 Configure Channel-Zero Encoding .....	24
3.9 Main and Auxiliary Ports Strategy .....	24
3.10 Not Wearing Hard Hat Detection .....	25
3.11 PTZ Control .....	27
3.11.1 Configure PTZ Parameters .....	27
3.11.2 Set a Preset .....	28
3.11.3 Call a Preset .....	28
3.11.4 Set a Patrol .....	29
3.11.5 Call a Patrol .....	30
3.11.6 Set a Pattern .....	31
3.11.7 Call a Pattern .....	31
3.11.8 Set Linear Scan Limit .....	32
3.11.9 One-Touch Park .....	32
3.11.10 Auxiliary Functions .....	33
<b>Chapter 4 Recording and Playback .....</b>	<b>35</b>
4.1 Recording .....	35
4.1.1 Configure Recording Parameters .....	35
4.1.2 Enable H.265 Stream Access .....	37
4.1.3 ANR .....	37
4.1.4 Manual Recording .....	38
4.1.5 Configure Plan Recording .....	38

4.1.6 Configure Continuous Recording .....	39
4.1.7 Configure Motion Detection Triggered Recording .....	40
4.1.8 Configure Event Triggered Recording .....	40
4.1.9 Configure Alarm Triggered Recording .....	40
4.1.10 Configure Picture Capture .....	41
4.1.11 Configure Holiday Recording .....	41
4.1.12 Configure Redundant Recording and Capture .....	42
4.2 Playback .....	43
4.2.1 Instant Playback .....	43
4.2.2 Play Normal Video .....	44
4.2.3 Play Smart Searched Video .....	45
4.2.4 Play Custom Searched Files .....	45
4.2.5 Play Tag Files .....	46
4.2.6 Play by Sub-periods .....	47
4.2.7 Play Log Files .....	48
4.2.8 Play External Files .....	48
4.3 Playback Operations .....	49
4.3.1 Normal/Important/Custom Video .....	49
4.3.2 Set Play Strategy in Important/Custom Mode .....	49
4.3.3 Edit Video Clips .....	49
4.3.4 Switch between Main Stream and Sub-Stream .....	50
4.3.5 Thumbnails View .....	50
4.3.6 Fisheye View .....	50
4.3.7 POS Information Overlay .....	51
4.3.8 Fast View .....	51
4.3.9 Digital Zoom .....	52
<b>Chapter 5 Event .....</b>	<b>53</b>
5.1 Normal Event Alarm .....	53

5.1.1 Configure Motion Detection Alarms .....	53
5.1.2 Configure Video Loss Alarms .....	53
5.1.3 Configure Video Tampering Alarms .....	53
5.1.4 Configure Sensor Alarms .....	54
5.1.5 Configure Exceptions Alarms .....	54
5.2 VCA Event Alarm .....	55
5.2.1 Facial Detection .....	55
5.2.2 Configure Vehicle Detection .....	56
5.2.3 Loitering Detection .....	57
5.2.4 People Gathering Detection .....	58
5.2.5 Fast Moving Detection .....	59
5.2.6 Parking Detection .....	60
5.2.7 Unattended Baggage Detection .....	61
5.2.8 Object Removal Detection .....	63
5.2.9 Audio Exception Detection .....	64
5.2.10 Defocus Detection .....	65
5.2.11 Sudden Scene Change Detection .....	66
5.2.12 PIR Alarm .....	67
5.2.13 Thermal Camera Detection .....	67
5.2.14 Queue Management .....	68
5.3 Configure Arming Schedule .....	68
5.4 Configure Linkage Actions .....	69
5.4.1 Configure Auto-Switch Full Screen Monitoring .....	69
5.4.2 Configure Audio Warning .....	70
5.4.3 Notify Surveillance Center .....	70
5.4.4 Configure Email Linkage .....	70
5.4.5 Trigger Alarm Output .....	71
5.4.6 Configure PTZ Linkage .....	71

<b>Chapter 6 Smart Analysis .....</b>	<b>72</b>
6.1 Engine Configuration .....	72
6.2 Work Behavior Analysis .....	72
6.2.1 Absence/Sleep on Duty Detection .....	72
6.2.2 Staying Overtime Detection .....	74
6.2.3 Number of People Exception Detection .....	75
6.2.4 Playing Mobile Phone Detection .....	77
6.3 Street Behavior Analysis .....	78
6.3.1 People Gathering Detection .....	78
6.3.2 People Running Detection .....	80
6.3.3 Physical Conflict Detection .....	82
6.3.4 People Falling Down Detection .....	83
6.4 Hard Hat Detection .....	85
6.5 Face Picture Library Management .....	86
6.5.1 Add a Face Picture Library .....	86
6.5.2 Upload Face Pictures to the Library .....	87
6.6 People Counting .....	87
6.6.1 People Counting Statistics .....	87
6.6.2 Regional People Counting .....	88
6.7 Smart Search .....	90
6.7.1 Face Picture Search .....	90
6.7.2 Behavior Analysis Search .....	93
6.7.3 Not Wearing Hard Hat Search .....	94
6.7.4 Regional People Counting Search .....	95
6.7.5 Human Body Detection Search .....	95
6.7.6 Vehicle Search .....	96
6.8 Smart Report .....	97
6.8.1 View People Counting Statistics .....	97

6.8.2 Heat Map .....	98
6.9 Target Detection .....	98
<b>Chapter 7 File Management .....</b>	<b>100</b>
7.1 Search Files .....	100
7.2 Export Files .....	100
7.3 Smart Search .....	101
<b>Chapter 8 POS Configuration .....</b>	<b>102</b>
8.1 Configure POS Connection .....	102
8.2 Configure POS Text Overlay .....	105
8.3 Configure POS Alarm .....	106
<b>Chapter 9 Storage .....</b>	<b>108</b>
9.1 Storage Device Management .....	108
9.1.1 Manage Local HDD .....	108
9.1.2 Add a Network Disk .....	110
9.1.3 Manage eSATA .....	111
9.2 Disk Array .....	113
9.2.1 Create a Disk Array .....	113
9.2.2 Rebuild an Array .....	115
<b>Chapter 10 Hot Spare Recorder Backup .....</b>	<b>118</b>
10.1 Set Hot Spare Device .....	118
10.2 Set Working Recorder .....	119
10.3 Manage Hot Spare System .....	119
<b>Chapter 11 Network Settings .....</b>	<b>121</b>
11.1 Configure DDNS .....	121
11.2 Configure PPPoE .....	121
11.3 Configure Port Mapping (NAT) .....	122
11.4 Configure SNMP .....	123
11.5 Configure Email .....	125

11.6 Configure Port .....	126
11.7 Configure ONVIF .....	128
<b>Chapter 12 User Management and Security .....</b>	<b>129</b>
12.1 Manage User Accounts .....	129
12.1.1 Add a User .....	129
12.1.2 Edit the Admin User .....	130
12.1.3 Edit an Operator/Guest User .....	131
12.2 Manage User Permissions .....	131
12.2.1 Set User Permissions .....	131
12.2.2 Set Live View Permission on Lock Screen .....	134
12.3 Configure Password Security .....	135
12.3.1 Export GUID File .....	135
12.3.2 Configure Security Questions .....	135
12.4 Reset Password .....	136
12.4.1 Reset Password by GUID .....	136
12.4.2 Reset Password by Security Questions .....	137
<b>Chapter 13 System Management .....</b>	<b>138</b>
13.1 Configure Device .....	138
13.2 Configure Time .....	138
13.2.1 Manual Time Synchronization .....	139
13.2.2 NTP Synchronization .....	139
13.2.3 DST Synchronization .....	139
13.3 Network Detection .....	140
13.3.1 Network Traffic Monitoring .....	140
13.3.2 Test Network Delay and Packet Loss .....	140
13.3.3 Export Network Packet .....	141
13.3.4 Network Resource Statistics .....	141
13.4 Storage Device Maintenance .....	142



13.4.1 Bad Sector Detection .....	142
13.4.2 S.M.A.R.T. Detection .....	143
13.4.3 HDD Health Detection .....	144
13.4.4 Configure Disk Clone .....	144
13.4.5 Repair Database .....	145
13.5 Upgrade Device .....	146
13.5.1 Upgrade by Local Backup Device .....	146
13.5.2 Upgrade by FTP .....	146
13.5.3 Upgrade by Web Browser .....	147
13.6 Import/Export Device Configuration Files .....	147
13.7 Search & Export Log Files .....	148
13.8 Restore Default Settings .....	149
13.9 Security Management .....	149
13.9.1 RTSP Authentication .....	149
13.9.2 ISAPI Service .....	150
13.9.3 HTTP Authentication .....	150
<b>Chapter 14 Appendix .....</b>	<b>151</b>
14.1 Glossary .....	151
14.2 Communication Matrix .....	152
14.3 Device Command .....	152
14.4 Frequently Asked Questions .....	153
14.4.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view? .....	153
14.4.2 Why is the video recorder notifying the stream type is not supported? .....	153
14.4.3 Why is the video recorder notifying risky password after a network camera is added? .....	154
14.4.4 How to improve the playback image quality? .....	154
14.4.5 How to confirm the video recorder is using H.265 to record video? .....	154
14.4.6 Why is the timeline at playback not constant? .....	154

14.4.7 Why is the video recorder notifying the network is unreachable when a network camera is being added? .....	155
14.4.8 Why is the IP address of network camera being changed automatically? .....	155
14.4.9 Why is the video recorder notifying IP conflict? .....	155
14.4.10 Why is image getting stuck when playing back by single or multi-channel cameras? .....	156
14.4.11 Why does my video recorder make a beeping sound after booting? .....	156
14.4.12 Why is there no recorded video after the motion detection is set? .....	156
14.4.13 Why is the video sound quality not good? .....	157

# Chapter 1 Basic Operation

## 1.1 Activate Your Device

### 1.1.1 Default User and IP Address

- Default administrator account: admin.
- Default IPv4 address: 192.168.1.64.

### 1.1.2 Activate via Local Menu

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. You can also activate the device via Web Browser, SADP or Client Software.

#### Steps

1. Enter the admin password twice.

admin

\*\*\*\*\*

Strong

\*\*\*\*\*

Export GUID ?

Create Channel Default Password

Security Question C...

Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.

OK

Figure 1-1 Activate via Local Menu

---

 **Warning**

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.

---

2. Enter the password to activate the IP cameras.
  3. **Optional:** Check **Export GUID**, or **Security Question Configuration**.
  4. Click **OK**.
- 

 **Note**

- After the device is activated, you should properly keep the password.
  - You can duplicate the password to the IP cameras that are connected with default protocol.
-

## What to do next

- When you have enabled **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- When you have enabled **Security Question Configuration**, continue to set the security questions for the future password resetting.

### 1.1.3 Activate via SADP

SADP software is used for detecting the online device, activating the device, and resetting its password.

#### Before You Start

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts.

#### Steps

1. Connect your video recorder power supply to an electrical outlet and turn on it.
2. Run the SADP software to search the online recorders.
3. Check the recorder status from the device list, and select the inactive recorder.

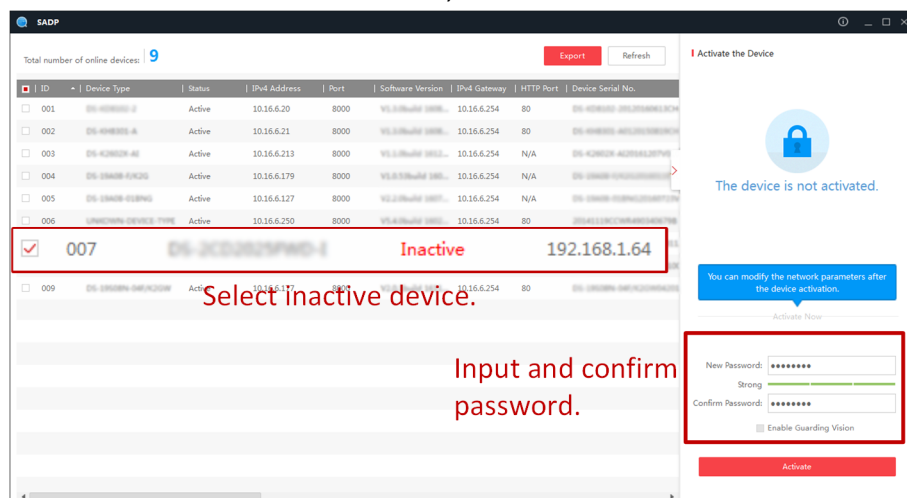


Figure 1-2 Activate via SADP

4. Create and input the new password in the password field, and confirm the password.

#### Note

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.

5. Click **Activate**.

## 1.1.4 Activate via Client Software

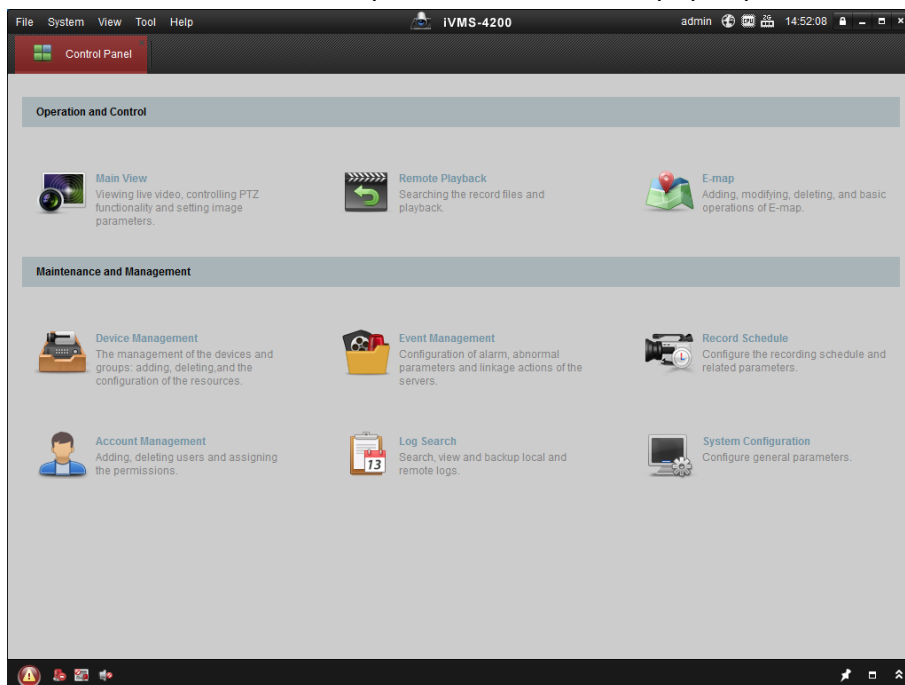
The client software is versatile video management software for multiple kinds of devices.

### Before You Start

Get the client software from the supplied disk or the official website, and install the software according to the prompts.

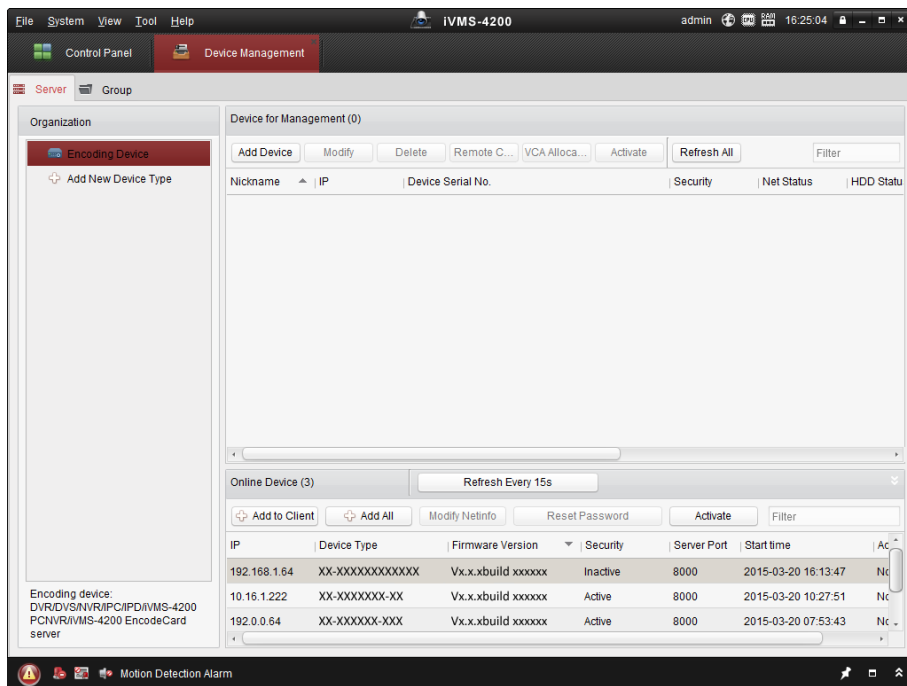
### Steps

1. Run the client software and the control panel of the software pops up, as shown below.



**Figure 1-3 Control Panel**

2. Click **Device Management** to enter the Device Management interface, as shown below.

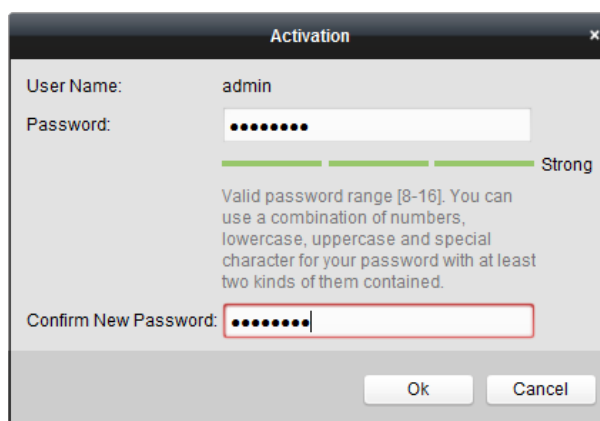


**Figure 1-4 Device Management Interface**

3. Check the recorder status from the device list, and select an inactive recorder.
4. Click **Activate** to pop up the Activation interface.
5. Create a password and input the password in the password field, and confirm the password.

**Note**

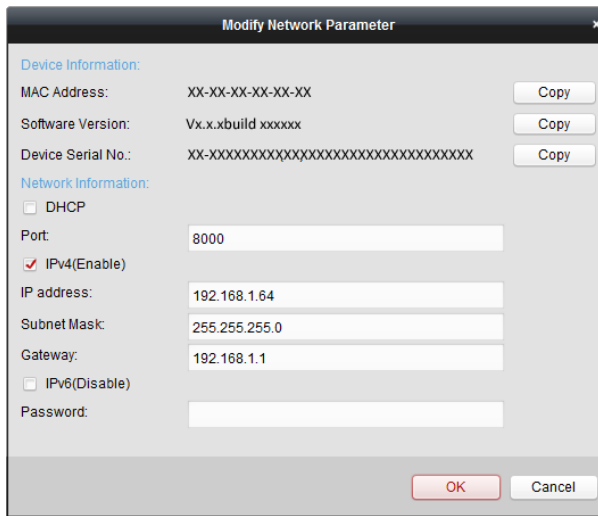
We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend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



**Figure 1-5 Activation**

6. Click **OK** to start activation.

7. Click **Modify Netinfo** to pop up the Network Parameter Modification interface, as shown below.



**Figure 1-6 Modify Network Parameters**

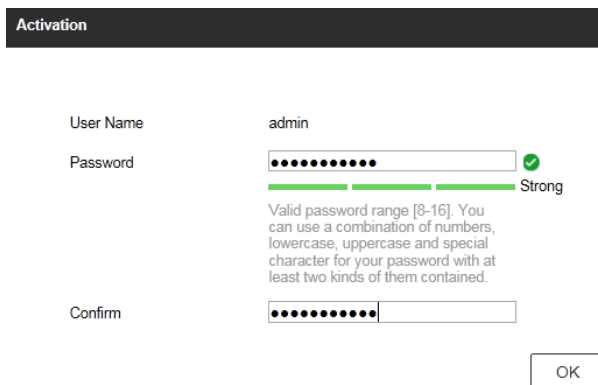
8. Change the recorder IP address to the same subnet with your computer.
  - Modify the IP address manually.
  - Check **Enable DHCP**.
9. Input the password to activate your IP address modification.

## 1.1.5 Activate via Web Browser

You can get access to the recorder via web browser. You may use one of the following listed web browsers: Internet Explorer 6.0 and above, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolutions include 1024\*768 and above.

### Steps

1. Enter the IP address in web browser, and then press **Enter**.



**Figure 1-7 Web Browser Activation**

2. Set the password for the admin user account.



## Note

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.

3. Click **OK**.

## 1.2 Configure TCP/IP Settings

TCP/IP settings must be properly configured before you can operate the device will operate over a network.

### Steps

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

The screenshot shows the TCP/IP configuration page with the following settings:

- Working Mode: Net Fault-Tolerance
- Select NIC: bond0
- NIC Type: 10M/100M/1000M Self-adap
- Enable DHCP:
- Enable Obtain DNS...:
- IPv4 Address: 10 . 15 . 2 . 107
- Preferred DNS Server: [Empty]
- IPv4 Subnet Mask: 255 . 255 . 255 . 0
- Alternate DNS Server: [Empty]
- IPv4 Default Gateway: 10 . 15 . 2 . 254
- MAC Address: e4:14:37:aa:09:a3
- MTU(Bytes): 1500
- Main NIC: LAN1

An **Apply** button is located at the bottom of the form.

Figure 1-8 TCP/IP Settings

2. Select **Working Mode** as **Net-Fault Tolerance** or **Multi-Address Mode**.

### Net-Fault Tolerance

The two NIC cards use the same IP address, and you can select the main NIC to LAN1 or LAN2. In this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure the normal running of the system.

### Multi-Address Mode

The parameters of the two NIC cards can be configured independently. You can select LAN1 or LAN2 under Select NIC for parameter settings. Select one NIC card as the default route. When the system connects with the extranet, the data will be forwarded through the default route.

3. Configure other IP settings as needed.

4. Click **Apply**.

## Note

- Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available on the network.
  - Valid MTU value range is 500 to 9676.
- 

## 1.3 HDD Settings

Ensure the video recorder storage media is well. You can install at least one HDD and initialize it, or create a RAID and initialize it.


## 1.4 Add Network Camera

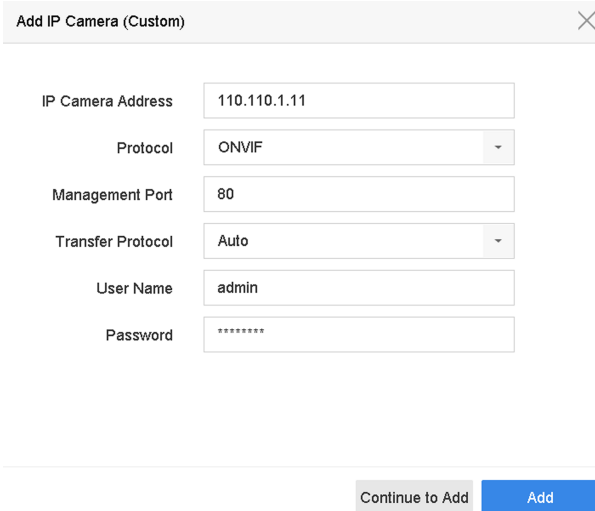
Before you can get live video or record the video files, you must add the network cameras to the connection list of the device.

### Before You Start

Ensure the network connection is valid and correct and the IP camera to add has been activated.

### Steps

1. Click  on the main menu bar.
2. Click **Custom Add** tab on the title bar.




IP Camera Address	<input type="text" value="110.110.1.11"/>
Protocol	<input type="text" value="ONVIF"/>
Management Port	<input type="text" value="80"/>
Transfer Protocol	<input type="text" value="Auto"/>
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

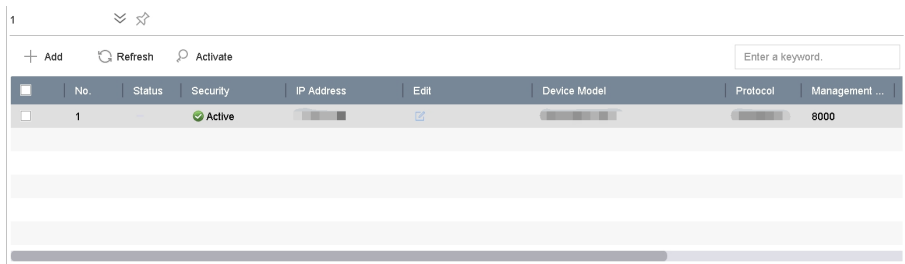
**Figure 1-9 Add IP Camera**

3. Enter IP address, protocol, management port, and other IP camera information to add.
4. Enter the login user name and password of the IP camera.
5. Click **Add** to finish the adding of the IP camera.
6. **Optional:** Click **Continue to Add** to continue to add additional IP cameras.

## 1.4.1 Add Automatically Searched Online Network Camera

### Steps

1. Click  on the main menu.
2. Click **Number of Unadded Online Device** at the bottom.
3. Select the automatically searched online network cameras.
4. Click **Add** to add the camera which has the same login password with the video recorder.



**Figure 1-10 Add Automatically Searched Online Network Camera**



### Note

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

---


## 1.4.2 Add Network Camera Manually

Before you view live video or record video files, you must add network cameras to the device.

### Before You Start

Ensure the network connection is valid and correct, and the network camera is activated.

### Steps

1. Click  on the main menu.
2. Click **Custom Add**.
3. Set **IP Camera Address**, **Protocol**, **Management Port**, **Transfer Protocol**, **User Name**, and **Password**. Management port ranges from 1 to 65535.

The screenshot shows a dialog box titled "Add IP Camera (Custom)". It features a tabbed interface with tabs for "No.", "Stat...", "Security", "IP Address", "Device Model", and "Proto". The "IP Address" tab is selected. The form includes the following fields and options:

- IP Camera Address: Text input field.
- Protocol: Dropdown menu with "HIKVISION" selected.
- Management Port: Text input field with "8000" entered.
- Transfer Protocol: Dropdown menu with "Auto" selected.
- User Name: Text input field with "admin" entered.
- Password: Text input field.
- Use Channel Default...: Checkbox (unchecked).
- Use Default Port: Checkbox (unchecked).
- Verify Certificate: Checkbox (unchecked).

At the bottom of the dialog are three buttons: "Search", "Continue to Add", and "Add".

**Figure 1-11 Add Network Camera**

- Optional:** Check **Use Channel Default Password** to use the default password to add the camera.
- Optional:** Check **Use Default Port** to use the default management port to add the camera. For SDK service, the default port value is 8000. For enhanced SDK service, the default value is 8443.

---

 **Note**

The function is only available when you use HIKVISION protocol.

---

- Optional:** Check **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. For details, refer to .

---

 **Note**

The enhanced SDK service is only available when you use HIKVISION protocol.

---

- Click **Add**.
- Optional:** Check **Continue to Add** to add other network cameras.

### 1.4.3 Add Network Camera via Customized Protocol

For network cameras that are not using standard protocols, you can configure customized protocols to add them. The system provides 16 customized protocols.

#### Steps

- Go to **More Settings** → **Protocol** .

Protocol Management

Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type:  Main Stream  Sub Stream

Type: RTSP RTSP

Transfer Protocol: Auto Auto

Port: 554 554

Path:

Example: [Type]://[IP Address]:[Port]/[Path]  
rtsp://192.168.0.1:554/ch1/main/av\_stream

OK Cancel

**Figure 1-12 Protocol Management**

2. Set protocol parameters.

### Type

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

### Path

Contact the manufacturer of network camera for the URL (Uniform Resource Locator) of getting main stream and sub-stream.



### Note

The protocol type and the transfer protocol must be supported by the network camera to add.

---

3. Click **OK**.
4. Click **Custom Add** to add cameras.
5. Set the parameters.
6. Click **OK**.

## 1.5 Platform Access

### 1.5.1 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 surveillance system.

#### Steps

1. Go to **System → Network → Advanced → Platform Access**.
2. Check **Enable** to activate the function. Then the service terms will pop up.

- 1) Enter **Verification Code**.
- 2) Scan the QR code to read the service terms and privacy statement.
- 3) Check **The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service.** if you agree with the service terms and privacy statement.
- 4) Click **OK**.

---

### **Note**

- Hik-Connect is disabled by default.
- The verification code is empty by default. It must contain 6 to 12 letters or numbers, and it is case sensitive.

- 
3. **Optional:** Check **Custom** and enter **Server Address** as your desire.
  4. **Optional:** Check **Enable Stream Encryption**, then verification code is required for remote access and live view.
  5. Bind your device with a Hik-Connect account.
    - 1) Use a smart phone to scan the QR code, and download Hik-Connect app. You can also download it from <https://appstore.hikvision.com> , or the QR code below. Refer to *Hik-Connect Mobile Client User Manual* for details.



Figure 1-13 Download Hik-Connect

- 2) Use Hik-Connect to scan the device QR, and bind the device.

---

### **Note**

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

- 
6. Click **Apply**.

### **What to do next**

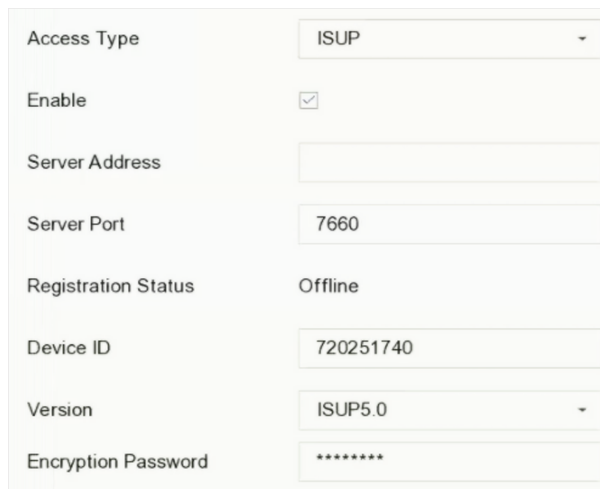
You can access your video recorder via Hik-Connect.

## 1.5.2 Configure ISUP

SDK is based on Intelligent Security Uplink Protocol (ISUP). It 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 → Network → Advanced → Platform Access** .



Access Type	ISUP
Enable	<input checked="" type="checkbox"/>
Server Address	
Server Port	7660
Registration Status	Offline
Device ID	720251740
Version	ISUP5.0
Encryption Password	*****

**Figure 1-14 ISUP Settings**

2. Select **Access Type** as **ISUP**.
3. Check **Enable**.

---

### **Note**

Enabling ISUP will disable other platform access.

---

4. Set the related parameters.

#### **Server Address**

The platform server IP address.

#### **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.

#### **Version**

ISUP protocol version, only V5.0 is available.

#### **Encryption Password**

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".

5. Click **Apply** to save the settings and restart the device.

### **What to do next**

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



## Chapter 2 Camera Settings

### 2.1 Configure Image Parameters

You can customize image parameters, including day/night switch, backlight, contrast, and saturation in **Camera → Display** .

#### Image Settings

Customize the image parameters including brightness, contrast, and saturation.

#### Exposure

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

#### Day/Night Switch

Set the camera to day, night, or auto switch mode according to time or the surrounding illumination condition. When the light diminishes at night, the camera can switch to night mode with high quality black and white image.

#### Backlight

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

#### Image Enhancement

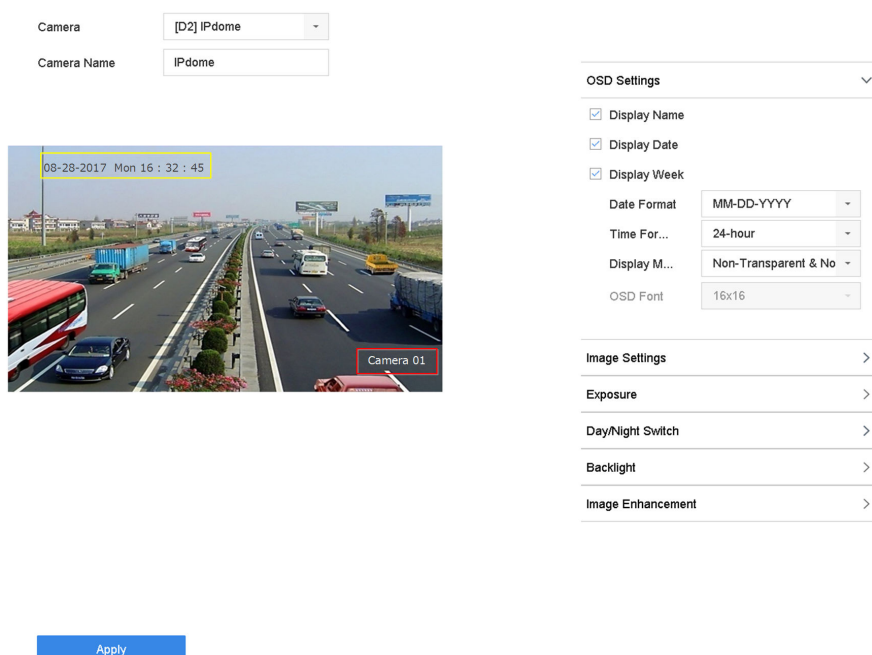
For optimized image contrast enhancement that reduces noise in video stream.

### 2.2 Configure OSD Settings

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

#### Steps

1. Go to **Camera → Display** .
2. Select a camera as your desire.
3. Edit name in **Camera Name**.
4. Check **Display Name**, **Display Date** and **Display Week** to show the information on the image.
5. Set the date format, time format, and display mode.



**Figure 2-1 OSD Configuration**

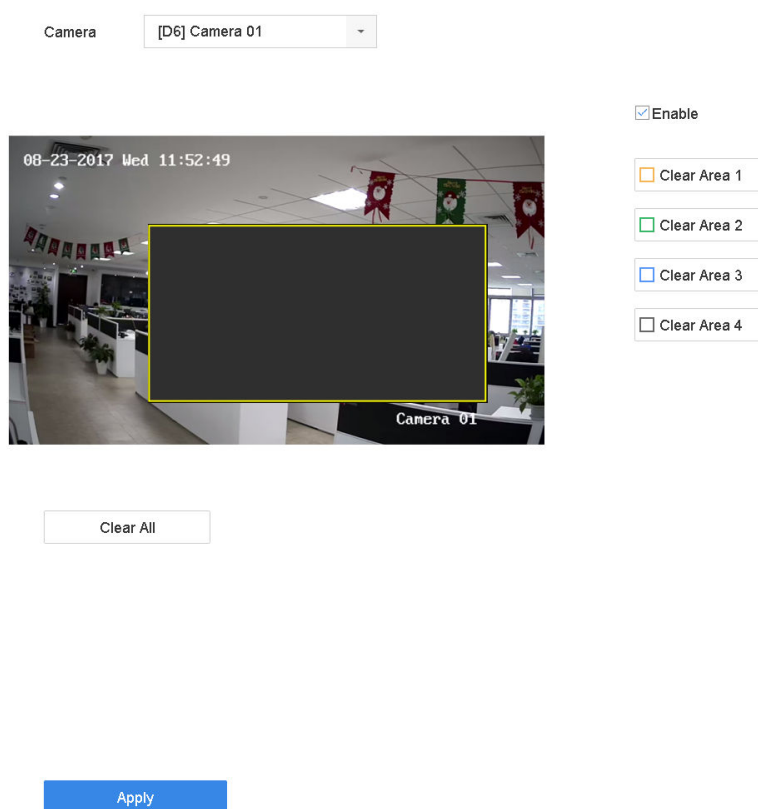
6. Drag the text frame on the preview window to adjust the OSD position.
7. Click **Apply**.

## 2.3 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 **Camera** → **Privacy Mask**.
2. Select a camera to set privacy mask.
3. Check **Enable**.
4. Draw a zone on the window. The zone will be marked by different frame colors.



**Figure 2-2 Privacy Mask Settings**

---

**Note**


- Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.
- You can clear the configured privacy mask zones on the window by clicking the corresponding clear zone 1 to 4 icons on the right of the window, or click **Clear All** to clear all zones.

5. Click **Apply**.

## 2.4 IP Camera Time Sync

The device can automatically synchronize the time of connected IP camera after enabling this function.

### Steps

1. Go to **Camera → Camera → IP Camera** .
2. Position the cursor on the window of the IP camera and click  .
3. Check **Enable IP Camera Time Sync**.
4. Click **OK**.

## 2.5 Import/Export IP Camera Configuration Files

The IP camera information, including the IP address, manage port, password of admin, etc., can be saved in Microsoft Excel format and backed up to the local device. The exported file can be edited on a PC, including adding or deleting the content, and copying the setting to other devices by importing the Excel file to it.

### Before You Start

When importing the configuration file, connect the storage device that contains the configuration file to the device.

### Steps

1. Go to **Camera → IP Camera Import/Export** .
2. Click **IP Camera Import/Export**, and the detected external device contents appear.
3. Export or import the IP camera configuration files.
  - Click **Export** to export the configuration files to the selected local backup device.
  - To import a configuration file, select the file from the selected backup device and click **Import**.



### Note

After the importing process is completed, you must reboot the device to activate the settings.

---

## 2.6 Upgrade IP Cameras

The IP camera can be remotely upgraded through the device.

### Before You Start

Ensure you have inserted the USB flash drive to the device, and it contains the IP camera upgrade firmware.

### Steps


1. On the camera management interface, select a camera.
2. Go to **More Settings → Upgrade** .
3. Select the firmware upgrade file from the USB flash drive.
4. Click **Upgrade**.

The IP camera will reboot automatically after the upgrading completes.

## Chapter 3 Live View

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

### 3.1 Start Live View

Click  on the main menu bar to enter the Live View.

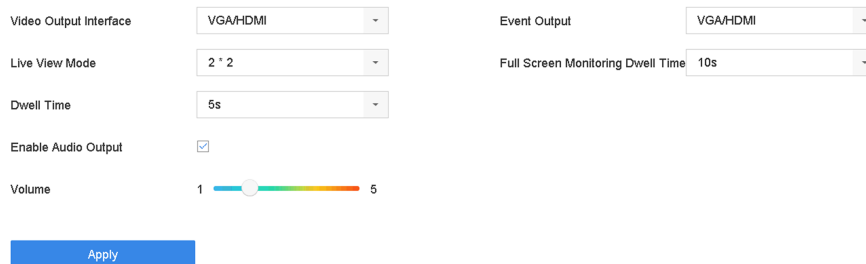
- Select a window and double click a camera from the list to play the video from the camera in the selected window.
- Use the toolbar at the playing window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.


#### 3.1.1 Configure Live View Settings

Live View settings can be customized. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

##### Steps

1. Go to **System → Live View → General**.



Video Output Interface	VGA/HDMI	Event Output	VGA/HDMI
Live View Mode	2 * 2	Full Screen Monitoring Dwell Time	10s
Dwell Time	5s		
Enable Audio Output	<input checked="" type="checkbox"/>		
Volume	1  5		

Apply

**Figure 3-1 Live View-General**

2. Configure the live view parameters.

##### Video Output Interface

Select the video output to configure.

##### Live View Mode

Select the display mode for Live View, e.g., 2\*2, 1\*5, etc.

##### Dwell Time

The time in seconds to wait between switching of cameras when using auto-switch in Live View.

##### Enable Audio Output

Enable/disable audio output for the selected video output.

## Volume

Adjust the Live View volume, playback and two-way audio for the selected output interface.

## Event Output

Select the output to show event video.

## Full Screen Monitoring Dwell Time

Set the time in seconds to show alarm event screen.


3. Click **OK**.

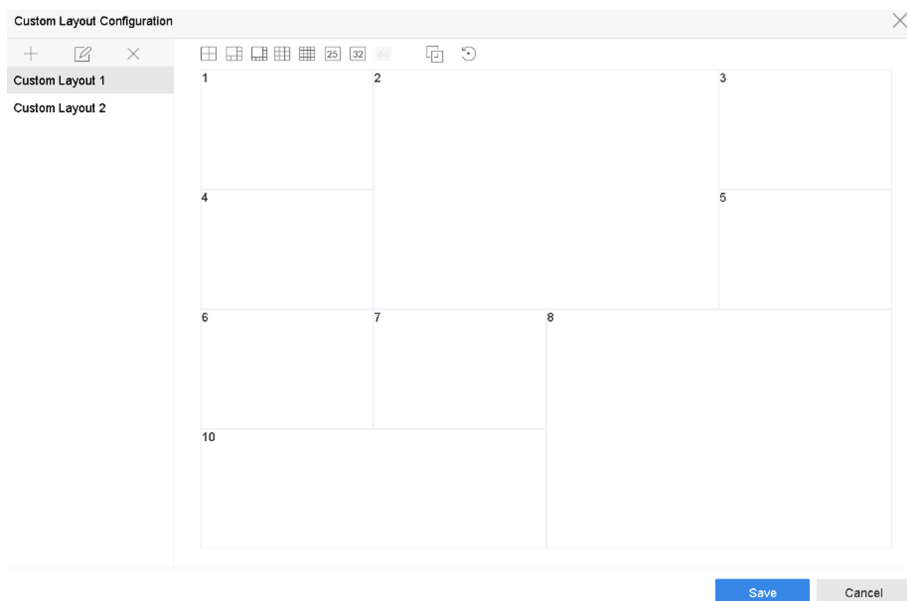
## 3.1.2 Configure Live View Layout

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


### Configure Custom Live View Layout

#### Steps



1. Go to **System → Live View → View**.
2. Click **Set Custom Layout**.
3. Click  on the Custom Layout Configuration interface.
4. Edit the layout name.
5. Select a window division mode from the toolbar.



**Figure 3-2 Configure Live View Layout**

6. Select multiple windows and click  to joint the windows. The selected windows must be in rectangle area.
7. Click **Save**.

The successfully configured layout is displayed in the list.

- 8. Optional:** Select a live view layout from the list and click  to edit the name, or click  to delete the name.

### Configure Live View Mode



#### Steps

1. Go to **System → Live View → View** .
2. Select the video output interface.
3. Select a layout or custom layout from the toolbar.
4. Select a division window, and double-click on a camera in the list to link the camera to the window.



#### Note

- You can also click-and-drag the camera to the desired window on the Live View interface to set the camera order.
- You can enter the number in the text field to quickly search the camera from the list.

- 
5. Click **Apply**.
  6. **Optional:** Click  to start live view for all channels, or click  to stop all live view channels.

### 3.2 Configure Auto-Switch of Cameras

You can set the auto-switch of cameras to play in different display modes.

#### Steps

1. Go to **System → Live View → General** .
2. Set **Video Output Interface**, **Live View Mode**, and **Dwell Time**.

#### Video Output Interface

Select the video output interface.

#### Live View Mode

Select the display mode for live view, e.g., 2\*2, 1\*5, etc.

#### Dwell Time

The time in seconds to dwell between switching of cameras when enabling auto-switch. The range is from 5s to 300s.

3. Go to **View Settings** to set the view layout.
4. Click **OK** to save the settings.

## 3.3 Digital Zoom

Digital Zoom zooms into the live image in different magnifications (1x to 16x).

### Steps


1. Start live view.
2. Click  from the toolbar.
3. Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).



Figure 3-3 Digital Zoom


## 3.4 Fisheye View

The device supports the fisheye camera expansion in Live View or playback mode.

### Before You Start





- The fisheye expansion view feature is supported only by certain models.
- The connected camera must support the fisheye view.

### Steps

1. Start live view, click  to enter the fisheye expansion mode.
2. Select the expansion view mode.



**Table 3-1 Fisheye View Icon Description**

Icon	Description	Icon	Description
180° Panorama (  )	Switch the Live View image to the 180° panorama view.	360° Panorama (  )	Switch the Live View image to the 360° panorama view.
PTZ Expansion (  )	The PTZ Expansion is the close-up view of some defined area in the fisheye view or panorama expansion. It supports the electronic PTZ function, also called e-PTZ.	Radial Expansion (  )	In radial expansion mode, the whole wide-angle view of the fisheye camera is displayed. This view mode is called Fisheye View because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

## 3.5 POS Information Overlay


The device can be connected with the POS machine/server, and receive the transaction message for overlay on the image during playback.

---

### Note

When the playing speed is higher than 2x, the POS information cannot be overlaid on the video.

---

In the video live or playback mode, click  to overlay the POS transaction information on the playback video.

## 3.6 3D Positioning

3D Positioning zooms in/out a specific live image area.

### Steps


1. Start live view, and click .

## 2. Zoom in/out the image.

- Zoom in: Click on the desired position in the video image and drag a rectangle area in the lower right direction to zoom in.
- Zoom out: Drag a rectangle area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

## 3.7 Live View Strategy

### Steps

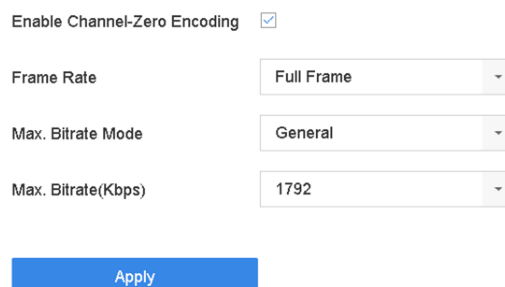
1. In the live view mode, click  to enter the digital zoom operation interface in full screen mode.
2. Select the live view strategy to **Real-time**, **Balanced** or **Fluency**.

## 3.8 Configure Channel-Zero Encoding

Enable the channel-zero encoding when you need to get a remote view of many channels in real time from a web browser or CMS (Client Management System) software, in order to decrease the bandwidth requirement without affecting the image quality.

### Steps

1. Go to **System** → **Live View** → **Channel-Zero** .
2. Check **Enable Channel-Zero Encoding**.



Enable Channel-Zero Encoding

Frame Rate Full Frame

Max. Bitrate Mode General

Max. Bitrate(Kbps) 1792

**Apply**

**Figure 3-4 Channel-Zero Encoding**

3. Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**. The higher frame rate and bitrate require the higher bandwidth.
4. Click **Apply**.

You can view all the channels on one screen via CMS or web browser.

## 3.9 Main and Auxiliary Ports Strategy

There are three video output types: HDMI, VGA, and HDMI2. Priority of video outputs: HDMI > VGA > HDMI2.

You can go to **System → General** to configure HDMI/VGA simultaneous output and menu output mode.

### Main port

All operations are available for main port.

### Aux port

You can switch to aux port to do some basic operations, like playback, switching live view image.

### Third port

You can only preview camera image in third port.

**Table 3-2 Main and Auxiliary Ports Strategy**

HDMI/VGA simultaneous output	Menu output mode	HDMI	HDMI2	VGA
On	Auto	Main port	Aux port	Main port
Off	Auto	Main port	Aux port	Third port
On	HDMI2	Aux port	Main port	Aux port
Off	HDMI2	Aux port	Main port	Third port
On	HDMI/VGA	Main port	Aux port	Main port
Off	VGA	Aux port	Third port	Main port
	HDMI	Main port	Third port	Aux port





## 3.10 Not Wearing Hard Hat Detection

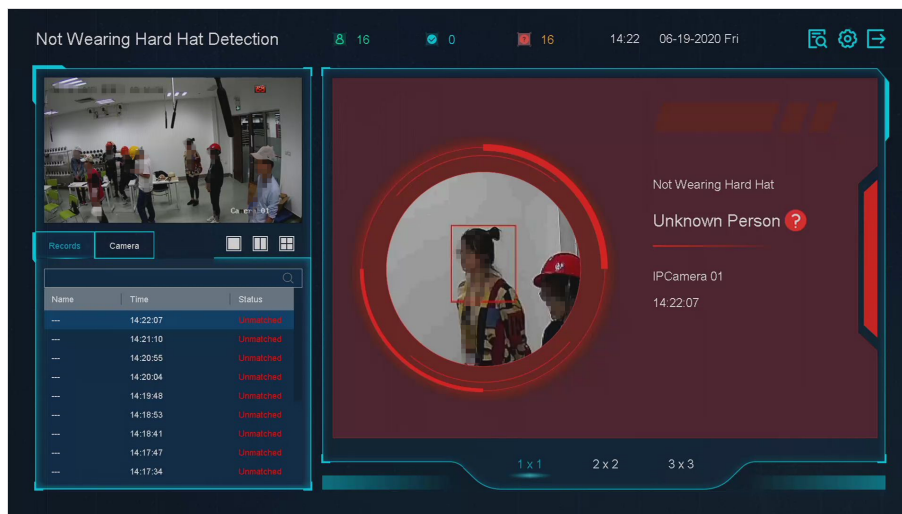
You can view real-time results of not wearing hard hat detection.

### Before You Start

Ensure you have properly configured the detection rules of not wearing hard hat detection. Refer to **Hard Hat Detection** for details.

### Steps

1. Go to live view interface, and click  in the toolbar.
2. Click , , or  to adjust window division.
3. Select a window as you desired.
4. Double click a camera from the camera list on the left bottom.




**Figure 3-5 Not Wearing Hard Hat Detection**

5. Click **Records** to select and view real-time detection records. The records will also be shown in the window on the right. The detection number are displayed at the top, including the not wearing hard hat number, matched person number and unmatched person number.
6. **Optional:** For the unregistered face picture, you can double click it in records list, and add it to face picture library.

### **Note**

For guest and operator user, it requires Local Parameters Settings permission to add unregistered face picture to face picture library.

7. **Optional:** Click  at the upper right corner to configure the display and audio linkage settings as you desired.

#### **Configure Display Settings**

The device will display a prompt when an alarm is triggered. You can edit the prompt theme, prompt information, and prompt picture. If **Alarm Picture** is set as **Capture Pic**, it will display the real-time captured picture. If **Alarm Picture** is set as **FaceLib Pic**, it will display the picture from face picture library.

#### **Configure Audio Linkage Settings**

The device will play an audio file when an alarm is triggered.

- a. Click **On** to turn on audio linkage.
- b. Set **Audio Output**.
- c. Set **Audio Source**. If you set **Audio Source** as **Custom**, it requires to click **View** to import audio files from peripherals.
- d. Click **OK**.

8. **Optional:** Click  at the upper right corner to search and export record.

## Note


- Ensure you have inserted USB flash drive before export.
  - For guest and operator user, it requires "Local Video Export permission" (in "Camera Permission") to search and export record.
- 

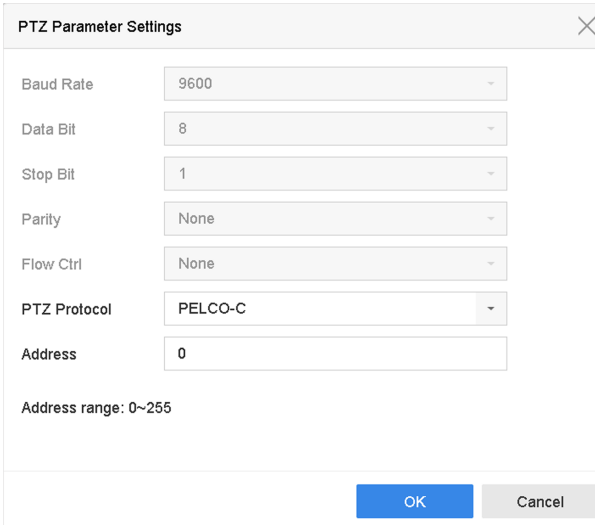
## 3.11 PTZ Control

### 3.11.1 Configure PTZ Parameters

Follow these procedures to set the PTZ parameters. The PTZ parameters configuration must be done before you can control the PTZ camera.

#### Steps

1. Click  on the quick settings toolbar of the PTZ camera.
2. Click **PTZ Parameters Settings** to set the PTZ parameters.



Parameter	Value
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-C
Address	0

Address range: 0~255

OK Cancel

Figure 3-6 PTZ Parameters Settings

3. Edit the PTZ parameters.

## Note

All the parameters should be exactly match the PTZ camera parameters.

---

4. Click **OK** to save the settings.

## 3.11.2 Set a 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.

### Steps



1. Click  on the quick settings toolbar of the PTZ camera's live view.
2. Click directional buttons to wheel the camera to a location.
3. Adjust the zoom, focus and iris status.
4. Click  in the lower right corner of Live View to set the preset.



Figure 3-7 Set Preset


5. Select the preset No. (1 to 255) from the drop-down list.
6. Enter the preset name.
7. Click **Apply** to save the preset.
8. **Optional:** Click **Cancel** to cancel the location information of the preset.
9. **Optional:** Click  in the lower right corner of Live View to view the configured presets.



Figure 3-8 View the Configured Presets

## 3.11.3 Call a Preset

A preset enables the camera to point to a specified position such as a window when an event takes place.

### Steps




1. Click  on the quick settings toolbar of the PTZ camera's Live View.
2. Click  in the lower right corner of Live View to set the preset.
3. Select the preset No. from the drop-down list.
4. Click **Call** to call it, or click  in the lower right corner of Live View, and click the configured preset to call it.



Figure 3-9 Call Preset (1)




Figure 3-10 Call Preset (2)

### 3.11.4 Set a 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.

#### Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.
2. Click **Patrol** to configure patrol.

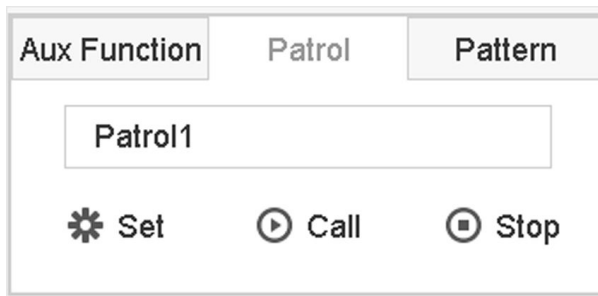


Figure 3-11 Patrol Configuration

3. Select the patrol No.
4. Click **Set**.

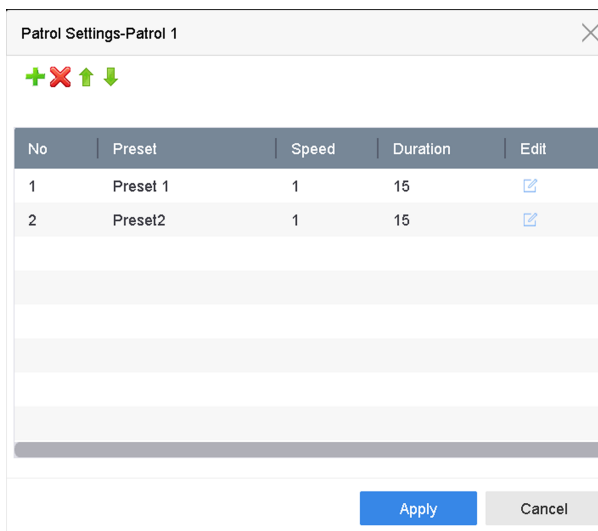


Figure 3-12 Patrol Settings

5. Click  to add a key point to the patrol.

**Figure 3-13 Key Point Configuration**

1) Configure key point parameters.

**Preset**

Determines the order the PTZ will follow while cycling through the patrol.

**Speed**

Defines the speed the PTZ will move from one key point to the next.

**Duration**

Refers to the duration to stay at the corresponding key point.

2) Click **Apply** to save the key points to the patrol.

6. Other operation is as follows.

**Table 3-3 Operation Description**

Operation	Description	Operation	Description
	Select a key point to delete.		Edit the added key point.
	Adjust the key point order		Adjust the key point order

7. Click **Apply** to save the patrol settings.

**3.11.5 Call a Patrol**

Calling a patrol makes the PTZ move according to the predefined patrol path.

**Steps**

1. Click on the quick settings toolbar of the PTZ camera's live view.
2. Click **Patrol** on the PTZ control panel.



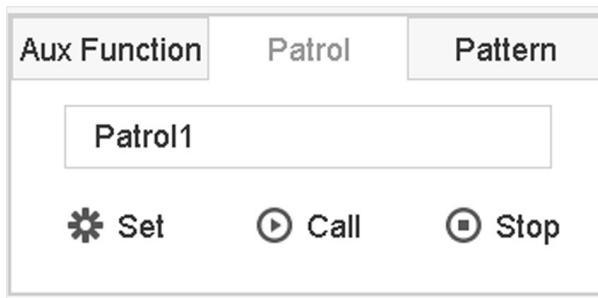



Figure 3-14 Patrol Configuration

3. Select a patrol.
4. Click **Call** to start the patrol.
5. **Optional:** Click **Stop** to stop the patrol.

### 3.11.6 Set a 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.

#### Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.
2. Click **Pattern** to configure a pattern.

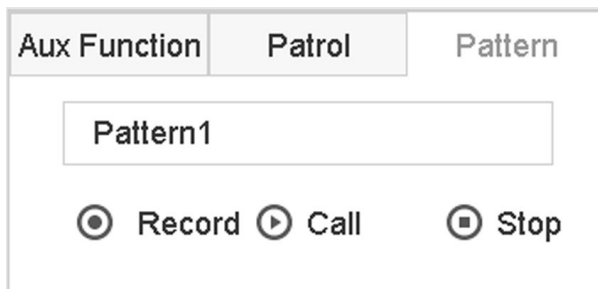



Figure 3-15 Pattern Configuration

3. Select the pattern No.
4. Set the pattern.
  - 1) Click **Record** to start recording.
  - 2) Click corresponding buttons on the control panel to move the PTZ camera.
  - 3) Click **Stop** to stop recording. The PTZ movement is recorded as the pattern.

### 3.11.7 Call a Pattern

Follow the procedure to move the PTZ camera according to the predefined patterns.

#### Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.
2. Click **Pattern** to configure pattern.



**Figure 3-16 Pattern Configuration**

3. Select a pattern.
4. Click **Call** to start the pattern.
5. **Optional:** Click **Stop** to stop the pattern.

### 3.11.8 Set Linear Scan Limit

Linear Scan trigger a scan in the horizontal direction in the predefined range.

#### Before You Start

Make sure the connected IP camera supports the PTZ function and is properly connected.


---

#### Note

This function is supported only by certain models.

---

#### Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.
  2. Click directional buttons to wheel the camera to a location, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.
- 

#### Note

The speed dome linear scans from the left limit to the right limit, and you must set the left limit on the left side of the right limit. Also, the angle from the left limit to the right limit must be not greater than 180°.

---


### 3.11.9 One-Touch Park

Certain speed dome models can be configured to start a predefined park action (scan, preset, patrol, etc.) automatically after a period of inactivity (park time).

#### Before You Start

Before operating this function, make sure the connected camera supports linear scan and is in HIKVISION protocol.

## Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.
2. Click **Park (Quick Patrol)**, **Park (Patrol 1)**, or **Park (Preset 1)** to activate the park action.

### **Park (Quick Patrol)**

The dome starts patrolling from the predefined preset 1 to preset 32 in order after the park time. Undefined presets will be skipped.

### **Park (Patrol 1)**

The dome starts moving according to the predefined patrol 1 path after the park time.

### **Park (Preset 1)**

The dome moves to the predefined preset 1 location after the park time.



## **Note**

The park time can be set only via the speed dome configuration interface. The default value is 5s by default.

---

3. **Optional:** Click **Stop Park (Quick Patrol)**, **Stop Park (Patrol 1)**, or **Stop Park (Preset 1)** to inactivate it.


## 3.11.10 Auxiliary Functions

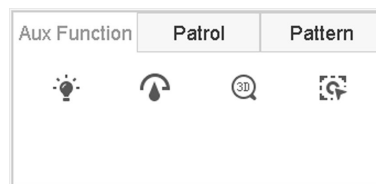
You can operate the auxiliary functions including light, wiper, 3D positioning, and center on the PTZ control panel.

### **Before You Start**

Make sure the connected IP camera supports the PTZ function, and is properly connected.

## Steps





1. Click  on the quick settings toolbar of the PTZ camera's live view. The PTZ control panel displays on the right of the interface.
2. Click **Aux Function**.



**Figure 3-17 Aux Function Configuration**

3. Click the icons to operate the aux functions. See the table for the icon descriptions.

**Table 3-4 Description of Aux Functions Icons**

Icon	Description
	Light on/off
	Wiper on/off
	3D positioning
	Center

## Chapter 4 Recording and Playback

### 4.1 Recording

#### 4.1.1 Configure Recording Parameters

Go to **Camera** → **Video Parameters** .

##### **Main Stream**

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your recording quality and image size.

Comparing with the sub-stream, the main stream can provide a higher quality video with higher resolution and frame rate.

##### **Frame Rate (FPS - Frames Per Second)**

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

##### **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**

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

##### **Enable H.264+**

H.264+ combines intelligent analysis technology with predictive encoding, noise suppression, and long-term bit rate control to realize a lower bit rate, which plays a significant role in cutting storage costs and provides a higher return value for the investment.

##### **Enable H.265+**

H.265+ is an optimized encoding technology based on the standard H.265/HEVC compression. With H.265+, the video quality is almost the same as that of H.265/HEVC but with less transmission bandwidth and storage capacity required.



##### **Note**

- A higher resolution, frame rate and bit rate setting will provide you the better video quality, but it will also require more internet bandwidth and use more storage space on the hard disk drive.
  - H.264+ or H.265+ encoding technology is only available for certain models.
-

## Sub-Stream

Sub-stream is a second codec that runs alongside the main stream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality.

Sub-stream is often exclusively used by apps to view live video. Users with limited internet speeds may benefit most from this setting.

## Picture

The picture refers to the live picture capture in continuous or event recording type. ( **Storage → Capture Schedule → Advanced**

### Picture Quality

Set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

### Interval

The interval of capturing live picture.

### Capture Delay Time

The duration of capturing pictures.

## Configure Advanced Recording Parameters

### Steps

1. Go to **Storage → Schedule → Record** .
2. Check **Enable Schedule** to enable scheduled recording.
3. Click **Advanced** to set the advanced parameters.

Advanced Parameters

Record Audio:

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

Redundant Record/Capture

OK Cancel

**Figure 4-1 Advanced Record Settings**

### Record Audio

Enable or disable audio recording.

### 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**

Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

### **Expired Time**

The expired time is period for a recorded 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.

### **Redundant Record/Capture**

By enabling redundant record or capture you save the record and captured picture in the redundant HDD.

## **4.1.2 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.

Go to **Camera** → **More Settings** → **H.265 Auto Switch Configuration** to enable the function.

## **4.1.3 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.

### **Before You Start**

- Ensure the network connection between your device and network cameras is valid and correct.
- Ensure the network camera has been installed with an SD card.

### **Steps**

1. Log in your device via web browser and go to **Configuration** → **Storage** → **Schedule Settings** → **Advanced** .
2. Check **Enable ANR**.
3. Click **OK**.

### 4.1.4 Manual Recording

You can click  to manually start/stop recording videos at live view.

### 4.1.5 Configure Plan Recording

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

#### Before You Start

- Ensure you have installed the HDDs to the device or added the network disks before storing the video files, pictures and log files.
- Before enabling **Motion, Alarm, M | A** (motion or alarm), **M & A** (motion and alarm) and **Event** triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Refer to for details.

#### Steps

1. Go to **Storage → Schedule → Record** .
2. Select a camera.
3. Check **Enable Schedule**.
4. Select a recording type.

##### Continuous

Scheduled recording.

##### Event

Recording triggered by all event triggered alarm.

##### Motion

Recording triggered by motion detection.

##### Alarm

Recording triggered by alarm.

##### M/A

Recording triggered by either motion detection or alarm.

##### M&A

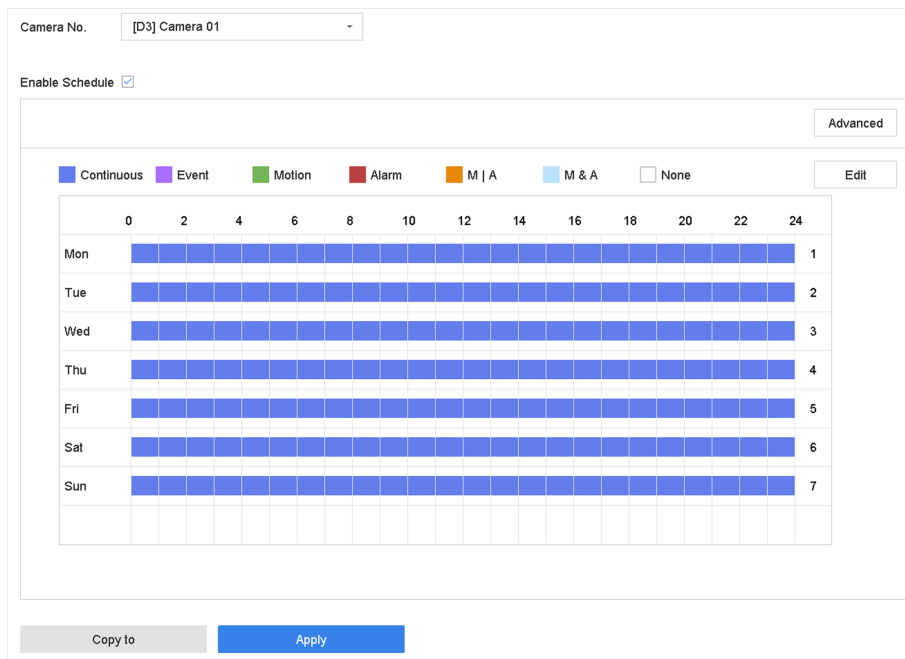
Recording triggered by motion detection and alarm.

##### POS

Recording triggered by POS and alarm.

5. Drag the cursor on time bar to set the record schedule.





**Figure 4-2 Record Schedule**



## Note

- You can repeat the above steps to set schedule recording or capture for each day in the week.
- Continuous recording is applied to each day by default.

### 6. **Optional:** Copy the recording schedule to other camera(s).

- 1) Click **Copy to**.
- 2) Select camera(s) to duplicate with the same schedule settings.
- 3) Click **OK**.

### 7. Click **Apply**.

## 4.1.6 Configure Continuous Recording

The device can continuously record the video within the configured time schedule.

### Steps

1. Go to **Camera** → **Encoding Parameters** → **Recording Parameters** .
2. Set the continuous main stream/sub-stream recording parameters for the camera.
3. Go to **Storage** → **Recording Schedule** .
4. Drag the mouse on the time bar to set the continuous recording schedule. Refer to **Configure Plan Recording** for details.

### 4.1.7 Configure Motion Detection Triggered Recording

You can configure the recording triggered by the motion detection event.

#### Steps

1. Go to **System → Event → Normal Event → Motion Detection** .
2. Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to **Configure Linkage Actions** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Motion**.
7. Drag the mouse on the time bar to set motion detection recording schedule. Refer to **Configure Plan Recording** for details.

### 4.1.8 Configure Event Triggered Recording

You can configure the recording triggered by the motion detection, motion detection and alarm, face detection, vehicle detection, line crossing detection, etc.

#### Steps

1. Go to **System → Event** .
2. Configure the event detection and select the channel(s) to trigger the recording when event occurs. Refer to **Event** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Event**.
7. Drag the mouse on the time bar to set the event detection recording schedule. Refer to **Configure Plan Recording** for details.

### 4.1.9 Configure Alarm Triggered Recording

You can configure the recording triggered by the motion detection, face detection, vehicle detection, line crossing detection, etc.

#### Steps

1. Go to **System → Event → Normal Event → Alarm Input** .
2. Configure the alarm input and select the channel(s) to trigger the recording when alarm occurs. Refer to **Event** for details.
3. Go to **Camera → Encoding Parameters → Recording Parameters** .
4. Set the event main stream/sub-stream recording parameters for the camera.
5. Go to **Storage → Recording Schedule** .
6. Select the recording type to **Alarm**.

7. Drag the mouse on the time bar to set the alarm recording schedule. Refer to ***Configure Plan Recording*** for details.

### 4.1.10 Configure Picture Capture

The picture refers to the live picture capture in continuous or event recording type. Only certain models support this function.

#### Steps

1. Go to **Camera → Encoding Parameters → Capture** .
2. Set the picture parameters.

#### Resolution

Set the resolution of the picture to capture.

#### Picture Quality

Set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

#### Interval

The interval of capturing live picture.

3. Go to **Storage → Capture Schedule** .
4. Select the camera to configure the picture capture.
5. Set the picture capture schedule. Refer to ***Configure Plan Recording*** for details.

### 4.1.11 Configure Holiday Recording

You may want to have different plan for recording on holiday, this function allows you to set the recording schedule on holiday for the year.

#### Steps

1. Go to **System → Holiday** .
2. Select a holiday item from the list.
3. Click  to edit the selected holiday.
4. Check **Enable**.

**Edit**

Enable

Holiday N...

Mode

Start Date

End Date

**Figure 4-3 Edit Holiday Settings**

5. Set **Holiday Name**, **Mode**, **Start Date**, and **End Date**.
6. Click **OK**.
7. Set the schedule for holiday recording. Refer to ***Configure Plan Recording*** for details.


## 4.1.12 Configure Redundant Recording and Capture

Enabling redundant recording and capture, which means saving the record files and captured pictures not only in the R/W HDD but also in the redundant HDD, will effectively enhance the data safety and reliability.

### Before You Start

You must set the storage mode to **Group** before you set the HDD property to **Redundancy**. For detailed information, refer to ***Configure HDD Group***. There should be at least another HDD which is in Read/Write status.

### Steps

1. Go to **Storage** → **Storage Device**.
2. Select a HDD from the list and click  to enter the **Local HDD Settings** interface.
3. Set the HDD property to **Redundancy**.
4. Go to **Storage** → **Schedule Settings** → **Record Schedule/Capture Schedule**.
5. Click **Advanced** to set the camera recording parameters.

**Advanced Parameters**

Record Audio:

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

Redundant Record/Capture

OK Cancel

Figure 4-4 Record Parameters

6. Check **Redundant Record/Capture**.
7. Click **OK** to save settings.

## 4.2 Playback

### 4.2.1 Instant Playback

Instant playback enables the device to play the recorded video files recorded in the last five minutes. If no video is found, it means there is no recording during the last five minutes.


After selecting the camera on **Live View**, you can move the cursor to the window bottom to access the toolbar, and click  to start instant playback.



Figure 4-5 Playback

## 4.2.2 Play Normal Video

Go to **Playback**, select date and camera(s), and use the toolbar at the bottom to perform playback operations. Refer to **Playback Operations**. You can click camera(s) to execute simultaneous playback of multiple camera(s).



**Note**

256x playing speed is supported.

---



Figure 4-6 Play Normal Video Interface

## 4.2.3 Play Smart Searched Video

In smart playback mode, the device can analyze videos that containing motion, line, or intrusion detection information, and mark them in red.




Go to **Playback**, click **Smart**, and then click motion detection (  ), line crossing detection (  ), or intrusion detection (  ) in the toolbar at the bottom to play the video as your desire.



Figure 4-7 Playback by Smart Search

## 4.2.4 Play Custom Searched Files

You can play video by customized search conditions.

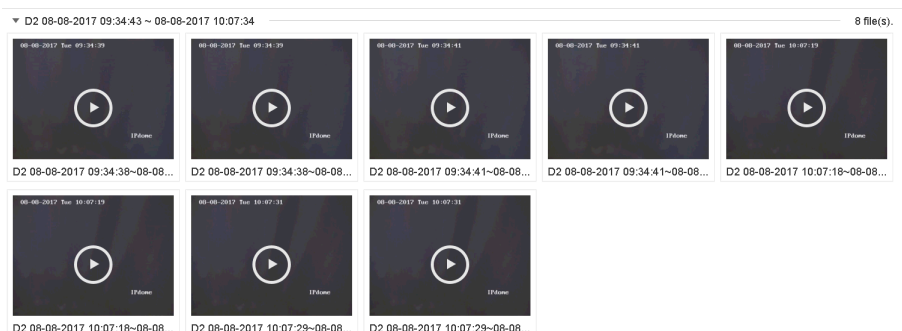
### Steps

1. Go to **Playback**.
2. Select camera(s) from the list.
3. Click **Custom Search** on the left bottom.
4. Enter search conditions, including **Time**, **File Status**, **Event Type**, etc.

Time	Custom	2017-10-01 00:00:00	2017-10-23 23:59:59
Tag	A	File Status	All
Event Type	None		
Plate No.			
Area/Country	None		
<input type="button" value="Empty Conditions"/> <input type="button" value="Search"/> <input type="button" value="Save"/>			

Figure 4-8 Custom Search

## 5. Click **Search**.



**Figure 4-9 Custom Searched Video Files**


## 6. Select a file and start playing the video on search results interface.

### 4.2.5 Play Tag Files

Video tag allows you to record information, such as people and locations of a certain time point, during playback. You can use video tag(s) to search video files and position time point.

### Add Tag Files

#### Steps

1. Go to **Playback**.
2. Search and play back the video file(s).
3. Click  to add the tag.
4. Edit the tag information.
5. Click **OK**.

---

#### **Note**

Max. 64 tags can be added to a single video file.

---

### Play Tag Files

#### Steps

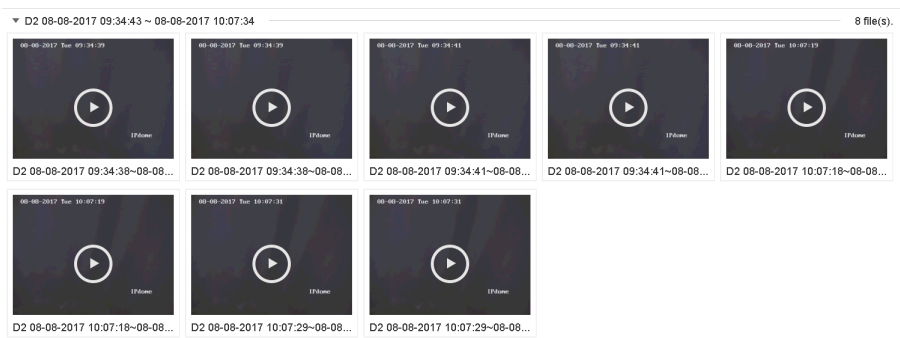
1. Go to **Playback**.
2. Click **Custom Search** at the left bottom.
3. Enter search conditions, including time and tag keyword.



Time: Custom, 2017-10-01 00:00:00, 2017-10-23 23:59:59  
Tag: A, File Status: All  
Event Type: None  
Plate No.:  
Area/Country: None  
Empty Conditions Search Save

**Figure 4-10 Tag Search**

#### 4. Click Search.



**Figure 4-11 Searched Tag Files**

#### 5. Select a tag file, and play the video on the search results interface.

### 4.2.6 Play by Sub-periods

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

#### Steps

1. Go to **Playback**.
2. Click **HH** at the lower-left corner.
3. Select a camera.
4. Set the start time and end time for searching video.
5. Select the different multi-period at the lower-right corner, e.g., 4-Period.

#### **Note**

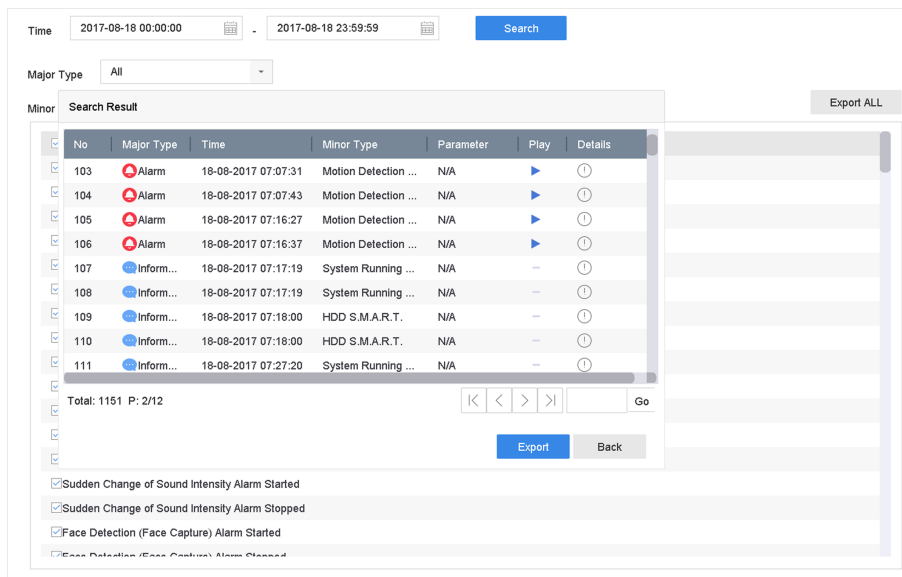
According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen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

## 4.2.7 Play Log Files

Play back record file(s) associated with channels after searching system logs.

### Steps

1. Go to **Maintenance** → **Log Information** .
2. Click **Log Search** .
3. Set search time and type and click **Search**.



**Figure 4-12 System Log Search Interface**

4. Choose a log with a video file and click to start playing the log file.



## 4.2.8 Play External Files

You can play files from external storage devices.

### Before You Start

Connect the storage device with the video files to your device.

### Steps

1. Go to **Playback**.
2. Click  at the lower-left corner.
3. Click , or double-click the file to play it.

## 4.3 Playback Operations

### 4.3.1 Normal/Important/Custom Video

During the playback, you can select the following three modes to play the video.

#### Normal

Video files from the continuous recording.

#### Important


Video files from the event and alarm recording triggered recording.

#### Custom

Video files searched by custom conditions.

### 4.3.2 Set Play Strategy in Important/Custom Mode

When you are in the smart or custom video playback mode, you can set the playing speed separately for the normal video and the smart/custom video, or you can select to skip the normal video.

In the Smart/Custom video playback mode, click  to set the play strategy.

- When **Do not Play Normal Videos** is checked, the device will skip the normal video and play the smart (motion/line crossing/intrusion) video and the custom (searched video) only in the normal speed (X1).
- When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video the smart/custom video separately. The speed range is from X1 to XMAX.



#### Note




You can set the speed in the single-channel play mode only.

---

### 4.3.3 Edit Video Clips



You can cut and export video clips during playback.

#### Steps

1. Go to **Playback**.
2. Click  at the bottom toolbar.
3. Set the start time and end time. You can click  to set the time period, or set a time segment on time bar.
4. Click  to save the video clip to a storage device.

## 4.3.4 Switch between Main Stream and Sub-Stream

You can switch between the main stream and the sub-stream during the playback.

Icon	Description
	Play the video in main stream.
	Play the video in sub-stream.

### Note

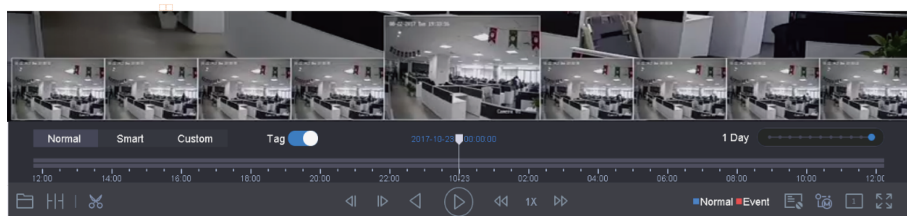
The encoding parameters for the main stream and sub-stream can be configured in **Storage → Encoding Parameters** .

---

## 4.3.5 Thumbnails View

With the thumbnails view on the playback interface, you can conveniently locate the required video files on the time bar.

In the playback mode, position the cursor on time bar to get preview thumbnails.



**Figure 4-13 Thumbnails View**

You can click a thumbnail to enter the full-screen playback.


## 4.3.6 Fisheye View

The device supports the fisheye camera expansion in Live View or playback mode.





### Before You Start

- The fisheye expansion view feature is supported only by certain models.
- The connected camera must support the fisheye view.

### Steps

1. Start live view, click  to enter the fisheye expansion mode.
2. Select the expansion view mode.

**Table 4-1 Fisheye View Icon Description**


Icon	Description	Icon	Description
180° Panorama (  )	Switch the Live View image to the 180° panorama view.	360° Panorama (  )	Switch the Live View image to the 360° panorama view.
PTZ Expansion (  )	The PTZ Expansion is the close-up view of some defined area in the fisheye view or panorama expansion. It supports the electronic PTZ function, also called e-PTZ.	Radial Expansion (  )	In radial expansion mode, the whole wide-angle view of the fisheye camera is displayed. This view mode is called Fisheye View because it approximates the vision of a fish's convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

### 4.3.7 POS Information Overlay

The device can be connected with the POS machine/server, and receive the transaction message for overlay on the image during playback.

 **Note**

When the playing speed is higher than 2x, the POS information cannot be overlaid on the video.

In the video live or playback mode, click  to overlay the POS transaction information on the playback video.

### 4.3.8 Fast View

Hold the mouse to drag on the time bar to get a fast view of the video files.

In the Video Playback mode, hold and drag the mouse through the playing time bar to fast view the video files.

Release the mouse at the required time point to enter the full-screen playback.

## 4.3.9 Digital Zoom

Digital Zoom zooms into the live image in different magnifications (1x to 16x).

### Steps


1. Start live view.
2. Click  from the toolbar.
3. Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).



Figure 4-14 Digital Zoom

## Chapter 5 Event

### 5.1 Normal Event Alarm

#### 5.1.1 Configure Motion Detection Alarms

Motion detection enables the device to detect the moving objects in the monitored area and trigger alarms.

##### Steps

1. Go to **System → Event → Normal Event → Motion Detection** .
2. Select a camera.
3. Check **Enable**.
4. Set the motion detection area.

**Full screen** Click to set the full-screen motion detection for the image.

**Customized area** Drag on the preview screen to draw the customized motion detection area(s).

5. Set **Sensitivity** (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.
6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set linkage actions. Refer to **Configure Linkage Actions** .

#### 5.1.2 Configure Video Loss Alarms

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

##### Steps

1. Go to **System → Event → Normal Event → Video Loss** .
2. Select a camera.
3. Check **Enable**.
4. Set the arming schedule. Refer to **Configure Arming Schedule** .
5. Set linkage actions. Refer to **Configure Linkage Actions** .

#### 5.1.3 Configure Video Tampering Alarms

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

##### Steps


1. Go to **System → Event → Normal Event → Video Tampering** .

2. Select a camera.
3. Check **Enable**.
4. Set the video tampering area. Drag on the preview screen to draw the customized video tampering area.
5. Set **Sensitivity** (0-2). 3 levels are available. The sensitivity calibrates how readily movement triggers the alarm. A higher value more readily triggers the video tampering detection.
6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set linkage actions. Refer to **Configure Linkage Actions** .

### 5.1.4 Configure Sensor Alarms

Set the handling action of an external sensor alarm.


#### Steps

1. Go to **System → Event → Normal Event → Alarm Input** .
2. Select an alarm input item from the list and click  .
3. Select the alarm input type.
4. Edit the alarm name.
5. Check **Input**.
6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set linkage actions. Refer to **Configure Linkage Actions** .

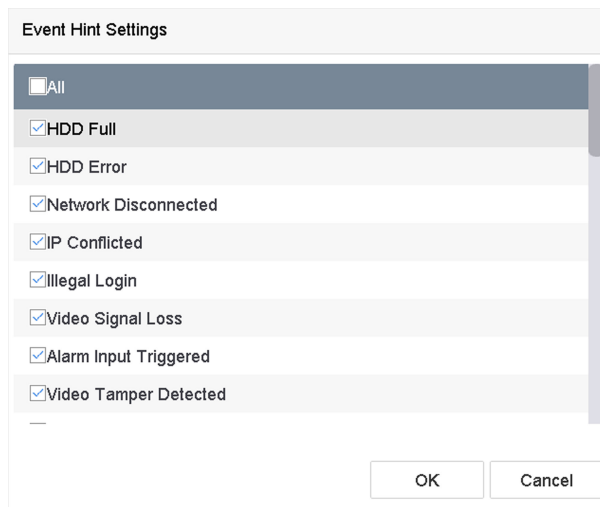
### 5.1.5 Configure Exceptions Alarms

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

#### Steps

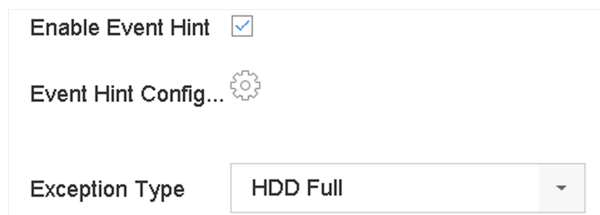
1. Go to **System → Event → Normal Event → Exception** .
2. **Optional:** Enable the event hint to display it in the live view window.
  - 1) Check **Enable Event Hint**.
  - 2) Click  to select the exception type(s) to take the event hint.





**Figure 5-1 Event Hint Settings**

3. Select an exception type.



**Figure 5-2 Exceptions Handling**

4. Set the linkage actions. Refer to **Configure Linkage Actions** .

## 5.2 VCA Event Alarm

The device supports receiving VCA detections sent by connected IP cameras. Enable and configure VCA detection on the IP camera settings interface first.

---

### Note

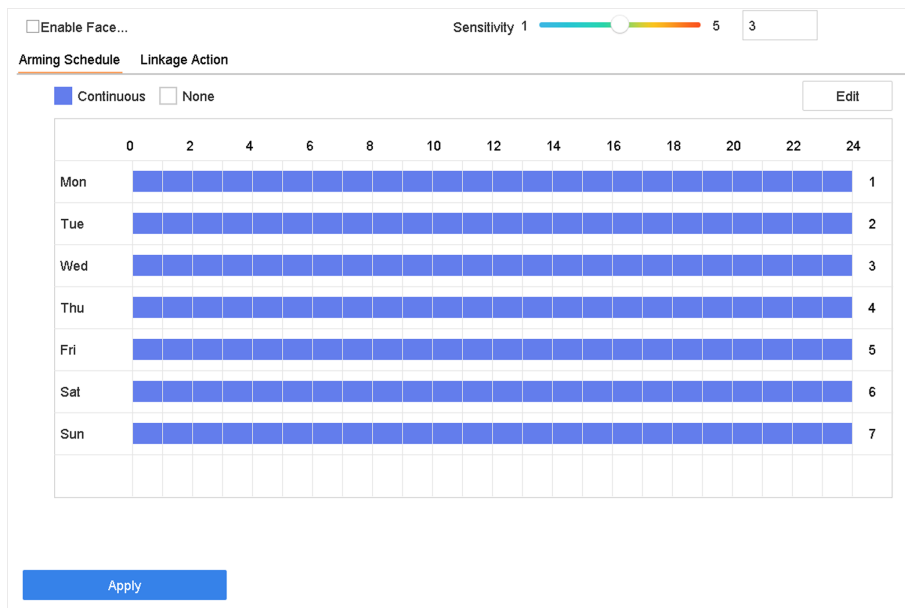
- VCA detections must be supported by the connected IP camera.
  - Refer to the network camera user manual for detailed VCA detection instructions.
- 

### 5.2.1 Facial Detection

The facial detection detects the face appearing in the surveillance scene. Linkage actions can be triggered when a human face is detected.

#### Steps

1. Go to **System** → **Event** → **Smart Event** .
2. Click **Face Detection**.



**Figure 5-3 Facial Detection**

3. Select a camera to configure.
4. Check **Enable Face Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured pictures of face detection.
6. Set the detection sensitivity. Sensitivity range: [1-5]. The higher the value is, the more easily the face will be detected.
7. Set the arming schedule. Refer to *Configure Arming Schedule*.
8. Set linkage actions. Refer to *Configure Linkage Actions*.
9. Click **Apply**.

## 5.2.2 Configure Vehicle Detection

Vehicle detection is available for road traffic monitoring. In vehicle detection, a passed vehicle can be detected, and the picture of its license plate can be captured.

### Steps

1. Go to **System** → **Event** → **Smart Event**.
2. Select a camera to configure.
3. Click **Vehicle**.

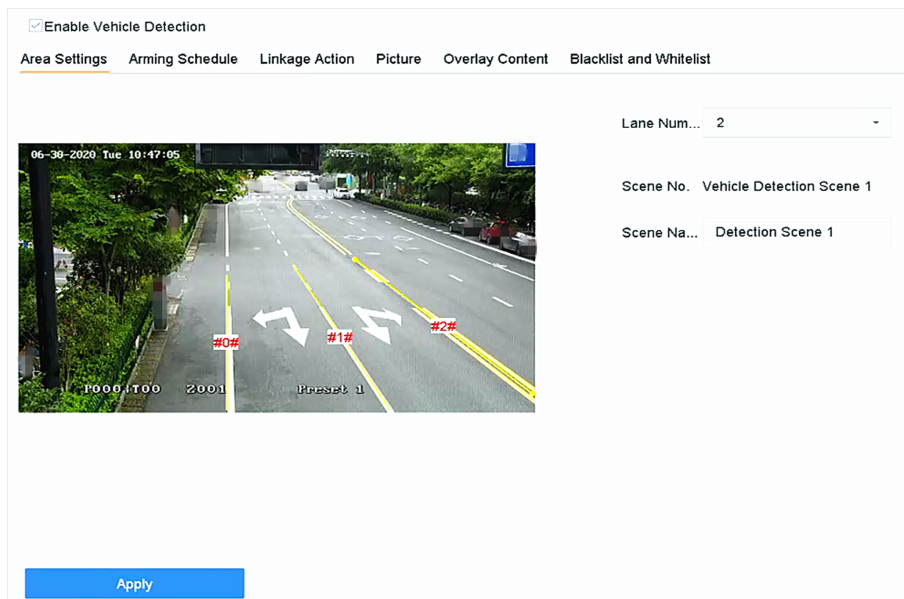


Figure 5-4 Vehicle Detection

4. Check **Enable Vehicle Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured vehicle detection pictures.
6. Set the arming schedule. Refer to **Configure Arming Schedule**.
7. Set the linkage actions. Refer to **Configure Linkage Actions**.
8. Configure rules, including **Area Settings**, **Picture**, **Overlay Content**, and **Blacklist and Whitelist**.

### Area Settings

Up to 4 lanes are selectable.

### Blacklist and Whitelist

You should firstly export the list file, and then use its format to edit it. Thereafter, import it back to your device.

9. Click **Apply**.



### Note

Refer to the Network Camera User Manual for detailed instructions for the vehicle detection.

---

## 5.2.3 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.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events**.
2. Select a camera.
3. Click **Loitering Detection**.

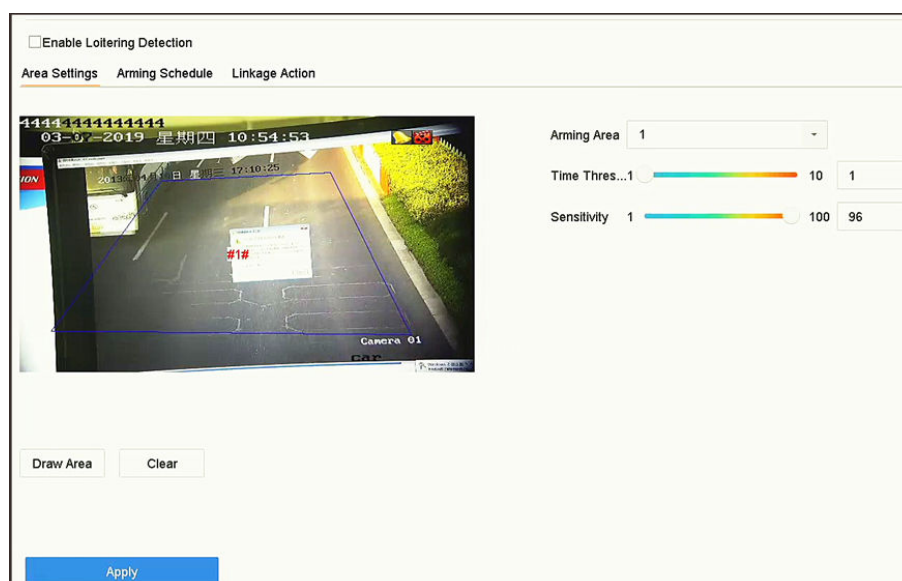


Figure 5-5 Loitering Detection

4. Check **Enable Loitering Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured loitering detection pictures.
6. Set loitering detection parameters.
  - 1) Select **Arming Area**.

---

 **Note**

Up to 4 areas are selectable.

---

- 2) Set **Time Threshold**.

**Time Threshold**

The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].

- 3) Set **Sensitivity**.

**Sensitivity**

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

7. Set the arming schedule. Refer to **Configure Arming Schedule**.
8. Set the linkage actions. Refer to **Configure Linkage Actions**.
9. Click **Apply**.

## 5.2.4 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.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events**.

2. Select a camera.
3. Click **People Gathering**.

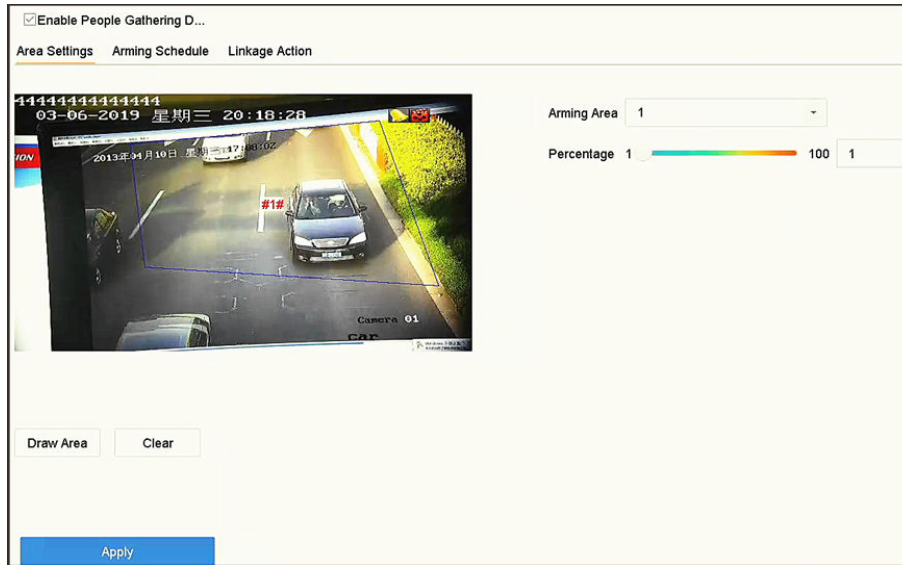


Figure 5-6 People Gathering Detection

4. Check **Enable People Gathering Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured people gathering detection pictures.
6. Set people gathering detection parameters.
  - 1) Select **Arming Area**.

---

 **Note**

Up to 4 areas are selectable.

- 2) Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.
- 3) Set **Percentage**.

**Percentage**

The density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm.

7. Set the arming schedule. Refer to **Configure Arming Schedule**.
8. Set the linkage actions. Refer to **Configure Linkage Actions**.
9. Click **Apply**.

## 5.2.5 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.

## Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Fast Moving**.

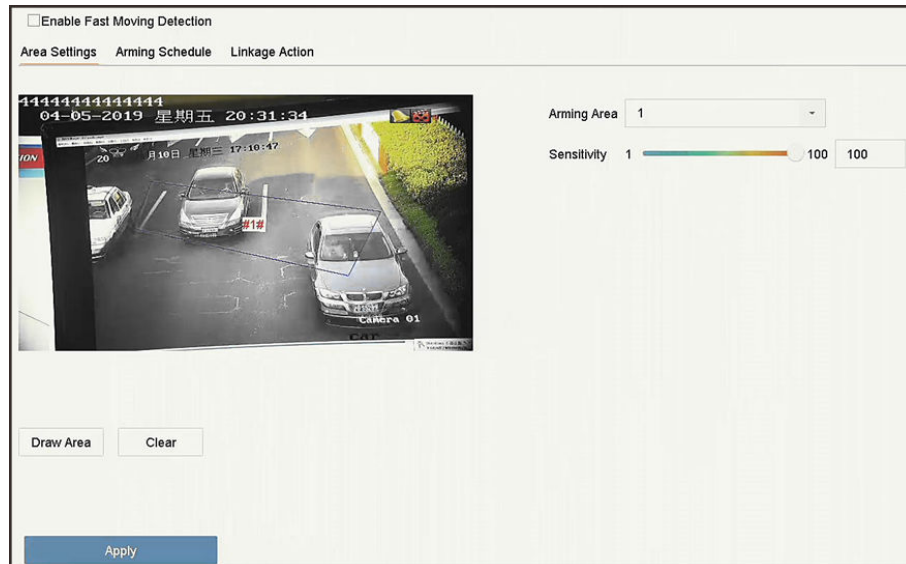


Figure 5-7 Fast Moving Detection

4. Check **Enable Fast Moving**.
5. **Optional:** Check **Save VCA Picture** to save the captured fast moving detection pictures.
6. Set fast moving detection parameters.
  - 1) Select **Arming Region**. Up to 4 regions are selectable.
  - 2) Click **Draw Area** to draw a quadrilateral in the preview window by specifying four vertices of the area.
  - 3) Set **Sensitivity**.

**Sensitivity**

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.
7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set the linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Apply**.

## 5.2.6 Parking Detection

Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.

### 3. Click **Parking**.

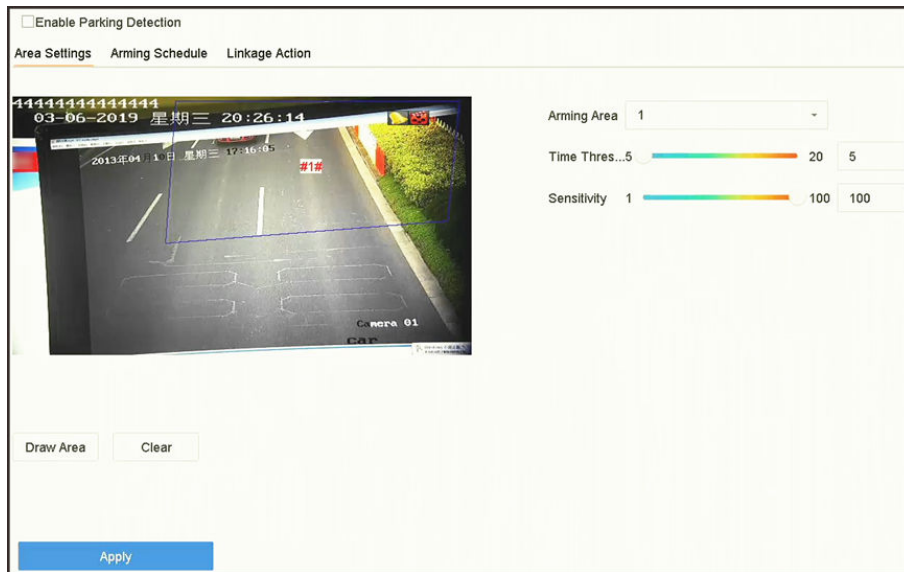


Figure 5-8 Parking Detection

### 4. Check **Enable Parking Detection**.

5. **Optional:** Check **Save VCA Picture** to save the captured parking detection pictures.

### 6. Set parking detection parameters.

#### 1) Select **Arming Area**.



Up to 4 areas are selectable.

#### 2) Set **Time Threshold**.

##### **Time Threshold**

The time of a vehicle staying in the region. If the value is 10, an alarm will be triggered after the vehicle has stayed in the region for 10 s. Range: [5-20].

#### 3) Set **Sensitivity**.

##### **Sensitivity**

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

7. Set the arming schedule. Refer to **Configure Arming Schedule**.

8. Set the linkage actions. Refer to **Configure Linkage Actions**.

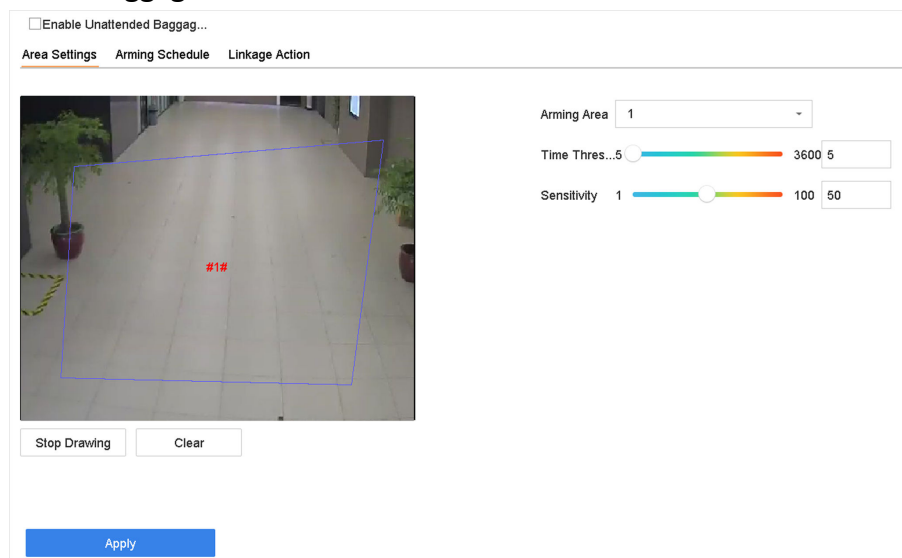
9. Click **Apply**.

## 5.2.7 Unattended Baggage Detection

Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.

## Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Unattended Baggage**.



**Figure 5-9 Unattended Baggage Detection**

4. Check **Enable Unattended Baggage Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured unattended baggage detection pictures.
6. Set the detection rules and detection areas.
  - 1) Select **Arming Area**.

---

### Note

Up to 4 areas are selectable.

- 2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

#### **Time Threshold**

The time of the objects left in the region. If the value is 10, an alarm will be triggered after the object is left and stayed in the region for 10 s. Range: [5-20].

#### **Sensitivity**

Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered.

- 3) Click **Draw Region** and draw a quadrilateral in the preview window.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Apply**.



## 5.2.8 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.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Object Removable**.

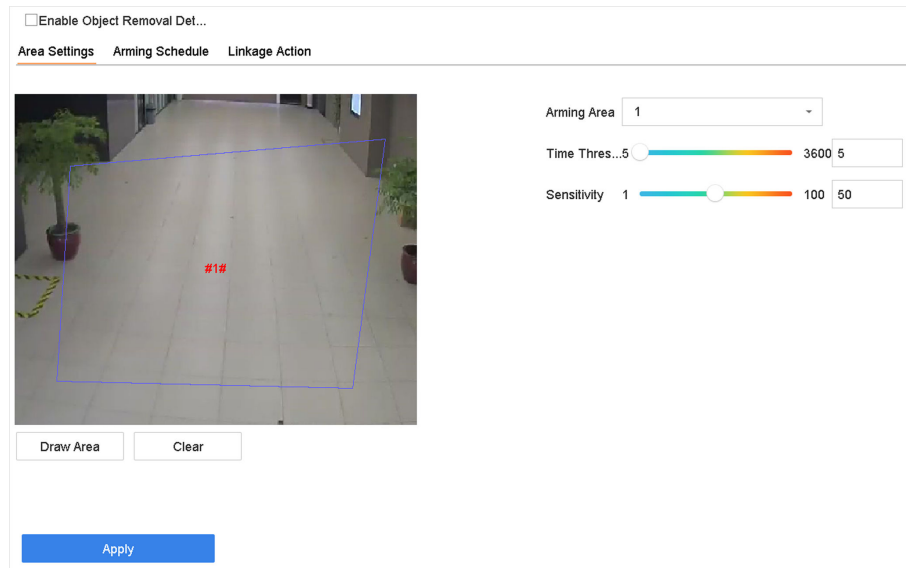


Figure 5-10 Object Removal Detection

4. Check **Enable Object Removable Detection**.
5. **Optional:** Check **Save VCA Picture** to save the captured object removable detection pictures.
6. Follow these steps to set the detection rules and detection areas.
  - 1) Select **Arming Area**.

### Note

Up to 4 areas are selectable.

- 2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

#### Time Threshold

The time of the objects removed from the region. If the value is 10, alarm will be triggered after the object disappears from the region for 10 s. Range [5-20].

#### Sensitivity

The similarity degree of the background image. If the sensitivity is high, a very small object taken from the region will trigger the alarm.

- 3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection region.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .

8. Set the linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Apply**.

## 5.2.9 Audio Exception Detection

Audio exception detection detects abnormal sounds in the surveillance scene, such as a sudden increase/decrease in sound intensity.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Audio Exception**.

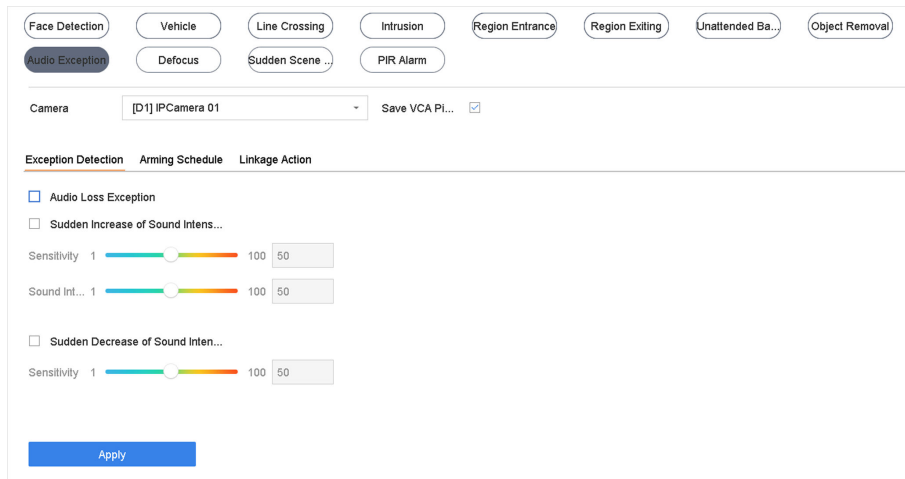


Figure 5-11 Audio Exception Detection

4. **Optional:** Check **Save VCA Picture** to save the captured audio exception detection pictures.
5. Set the detection rules.
  - 1) Select **Exception Detection**.
  - 2) Check **Audio Loss Exception**, **Sudden Increase of Sound Intensity Detection**, and/or **Sudden Decrease of Sound Intensity Detection**.

### Audio Loss Exception

Detects a steep sound rise in the surveillance scene. Set **Sensitivity** and **Sound Intensity Threshold** for the steep sound rise.

### Sensitivity

The smaller the value is, the more severely the change would trigger the detection. Range [1-100].

### Sound Intensity Threshold

It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment. Range [1-100].

### Sudden Decrease of Sound Intensity Detection

Detects a steep sound drop in the surveillance scene. Detection sensitivity [1-100].

6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set the linkage actions. Refer to **Configure Linkage Actions** .
8. Click **Apply**.

## 5.2.10 Defocus Detection

Image blur caused by lens defocus can be detected.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Defocus**.

The screenshot shows the configuration interface for Defocus Detection. At the top, there is an 'Enable' checkbox and a 'Sensitivity 1' slider set to 100. Below this, there are two tabs: 'Arming Schedule' and 'Linkage Action'. Under 'Arming Schedule', there are radio buttons for 'Continuous' (selected) and 'None', and an 'Edit' button. The main area is a 24-hour grid for each day of the week (Mon-Sun). The grid shows that the 'Continuous' action is applied for all 24 hours of every day. At the bottom, there is an 'Apply' button.

Figure 5-12 Defocus Detection

4. Check **Enable**.
5. **Optional:** Check **Save VCA Picture** to save the captured defocus detection pictures.
6. Set the detection sensitivity.

### Sensitivity

Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image will be detected.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set the linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Apply**.

## 5.2.11 Sudden Scene Change Detection

Scene change detection detects the change of the surveillance environment affected by external factors, such as the intentional rotation of the camera.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **Sudden Scene Change**.

The screenshot shows the configuration interface for Sudden Scene Change detection. At the top, there is an 'Enable' checkbox and a 'Sensitivity 1' slider set to 50. Below this, there are tabs for 'Arming Schedule' and 'Linkage Action'. Under 'Linkage Action', 'Continuous' is selected. The 'Arming Schedule' section features a grid with days of the week (Mon-Sun) and time slots (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24). All cells in the grid are filled with blue, indicating that detection is enabled for all days and times. An 'Apply' button is at the bottom left, and an 'Edit' button is at the top right of the grid area.

Figure 5-13 Sudden Scene Change

4. Check **Enable**.
5. **Optional:** Check **Save VCA Picture** to save the captured sudden scene change detection pictures.
6. Set the detection sensitivity.

### Sensitivity

Ranges from 1 to 100, the higher the value, the more easily the change of scene can trigger the alarm.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set the linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Apply**.

## 5.2.12 PIR Alarm

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector vision field. The heat energy dissipated by a person or any other warm blooded creature such as dogs, cats, etc., can be detected.

### Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Other Events** .
2. Select a camera.
3. Click **PIR Alarm**.

The screenshot shows the configuration interface for a PIR Alarm. At the top, there is a checkbox labeled "Enable PIR Alarm" which is currently unchecked. Below this, there are two tabs: "Arming Schedule" (selected) and "Linkage Action". Under the "Arming Schedule" tab, there are two radio buttons: "Continuous" (selected) and "None". To the right of these buttons is an "Edit" button. The main part of the interface is a grid for setting the arming schedule. The columns represent time in 2-hour increments from 0 to 24. The rows represent the days of the week from Monday to Sunday. Each cell in the grid contains a blue bar, indicating that the alarm is armed continuously for all days and times. At the bottom of the form is an "Apply" button.

Figure 5-14 PIR Alarm

4. Check **PIR Alarm**.
5. **Optional:** Check **Save VCA Picture** to save the captured of PIR alarm pictures.
6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set the linkage actions. Refer to **Configure Linkage Actions** .
8. Click **Apply**.

## 5.2.13 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 **Smart Analysis** → **Smart Event Settings** → **Other Events** .

2. Select a thermal camera.
3. **Optional:** Check **Save VCA Picture** to save the captured pictures of detection.
4. Select an event detection (Temperature Measurement Alarm, etc.).
5. Set the arming schedule. Refer to **Configure Arming Schedule** .
6. Set the linkage actions. Refer to **Configure Linkage Actions** .
7. Click **Apply**.

### 5.2.14 Queue Management

After connecting with queue management camera, you can set the arming schedule and linkage action of queue management.

#### Before You Start

Ensure the recorder have connected with queue management camera.

#### Steps

1. Go to **Smart Analysis → Smart Event Settings → Other Events** .
2. Select a queue management camera.
3. **Optional:** Check **Save VCA Picture** to save the captured pictures of detection.
4. Set the arming schedule. Refer to Chapter **Configure Arming Schedule** for details.
5. Set the linkage actions. Refer to Chapter **Configure Linkage Actions** for details.
6. Click **Apply**.

## 5.3 Configure Arming Schedule

#### Steps

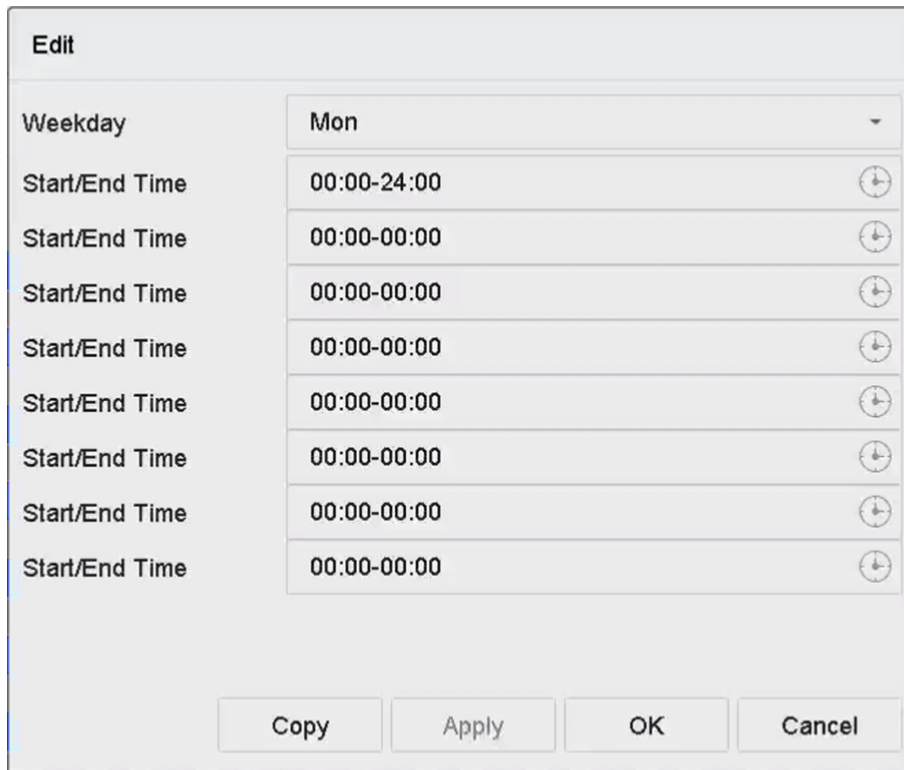
1. Click **Arming Schedule**.
2. Click **Edit**.
3. Select a day of the week and set the time period. Up to eight time periods can be set each day.



#### Note

Time periods cannot repeat or overlapped.

---



**Figure 5-15 Set Arming Schedule**

- 4. You can click **Copy** to copy the current day arming schedule settings to other day(s).
- 5. Click **Apply** to save the settings.

## 5.4 Configure Linkage Actions

Alarm linkage actions will be activated when an alarm or exception occurs, including Event Hint Display, Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Trigger Alarm Output, and Send Email.

### 5.4.1 Configure Auto-Switch Full Screen Monitoring

When an alarm is triggered, the local monitor displays in full screen the video image from the alarming channel configured for full screen monitoring. And when the alarm is triggered simultaneously in several channels, you must configure the auto-switch dwell time.

---

 **Note**

Auto-switch will terminate once the alarm stops and back to the live view interface.

---

#### Steps

- 1. Go to **System → Live View → General** .
- 2. Set the event output and dwell time.

### Event Output

Select the output to show the event video.

### Full Screen Monitoring Dwell Time

Set the time in seconds to show the alarm event screen. If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time).

3. Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select the **Full Screen Monitoring** alarm linkage action.
5. Select the channel(s) in **Trigger Channel** for full screen monitoring.

### 5.4.2 Configure Audio Warning

The audio warning has the system to trigger an audible beep when an alarm is detected.

#### Steps

1. Go to **System → View → General** .
2. Enable the audio output and set the volume.
3. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select the **Audio Warning** alarm linkage action.

### 5.4.3 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).

#### Steps

1. Go to **System → Network → Advanced → More Settings** .
2. Set the alarm host IP and alarm host port.
3. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
4. Select **Notify Surveillance Center**.

### 5.4.4 Configure Email Linkage

The system can send an email with alarm information to a user or users when an alarm is detected.

#### Steps

1. Go to **System → Network → Advanced → Email** .
2. Set the email parameters.
3. Click **Apply**.



4. Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
5. Select **Send Email** alarm linkage action.

### 5.4.5 Trigger 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.

#### Steps

1. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, face detection, line crossing detection, intrusion detection, etc.).
2. In **Trigger Alarm Outputs** Area, Select the alarm output (s) to trigger.
3. Go to **System → Event → Normal Event → Alarm Output** .
4. Select an alarm output item from the list.

### 5.4.6 Configure PTZ Linkage

The system can trigger the PTZ actions (e.g., call preset/patrol/pattern) when the alarm event, or VCA detection events occurs.

#### Before You Start

Make sure the connected PTZ or speed dome connected supports PTZ linkage.

#### Steps

1. Go to **Linkage Action** interface of the alarm input or VCA detection (e.g., face detection, line crossing detection, intrusion detection, etc.).
2. Select the **PTZ Linkage**.
3. Select the camera to perform the PTZ actions.
4. Select the preset/patrol/pattern No. to call when the alarm events occur.



#### Note

You can set only one PTZ type for the linkage action each time.

---

## Chapter 6 Smart Analysis

### 6.1 Engine Configuration

Each engine processes a specified VCA type as its working mode. You can configure the engine working mode as your desire.

#### Steps

1. Go to **Smart Analysis → Engine Settings → Engine Configuration** .
2. Configure each engine usage. You can view the engine temperature and linked channel status of each function.

---

#### Note

If the engine has been bound with channel(s), switching engine working mode will unbind the engine and channel(s), and cancel the related smart event of the channel.

---

3. Select an analysis mode.

#### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).

#### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Click **Save** to save the settings.

### 6.2 Work Behavior Analysis

Work behavior analysis includes absence/sleep on duty detection, people overstay detection, number of people exception detection, and using mobile phone detection. You can configure behavior analysis via web browser.

#### 6.2.1 Absence/Sleep on Duty Detection

Absence detection detects people who leave duty area over the set time in detection area. Sleep on duty detection detects whether people stay motionless on duty. If the person has not moved during the set time, the device will predicate the person is sleeping.

#### Before You Start

Ensure the engine mode is set as **Work Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

## Steps

1. Go to **Configuration → VCA → Behavior Analysis** .
2. Select a camera.
3. Select an analysis mode.

### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).

### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.

- 1) Click **+** to add a rule.
- 2) Select **Rule Type** as **Absence Detection**.
- 3) Select **Mode** as **Absence Detection** or **Sleep On Duty Detection** according to your requirement.
- 4) Enter the rule name.
- 5) Enable the rule.
- 6) Set **Person Mode**.

### Single Person Mode

Only one person is on duty. It will trigger an alarm when the person is absence or sleeping (motionless).

### Two-Person Mode

Two people are on duty. It will trigger an alarm when both of them are absence or sleeping (motionless).

- 7) Set **Asleep Period/Absence Duration**.

### Asleep Period/Absence Duration

The device will trigger an alarm when the time exceeds the limit.


- 8) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

### Overlay Rule Frame


The rule frame will be displayed on the captured picture.

### Overlay Target Frame

The target frame will be displayed on the captured picture.

- 9) Click  to draw the detection area in the preview window.
  - 10) Click **Save**.
6. Set the arming schedule. Refer to **Configure Arming Schedule** .
  7. Set linkage actions. Refer to **Configure Linkage Actions** .
  8. Click **Save**.

## What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

## 6.2.2 Staying Overtime Detection

Staying overtime detection can trigger alarm when overstay time of the target is beyond the set value in the detection area.

### Before You Start

Ensure the engine mode is set as **Work Behavior Analysis**. You can go to **Configuration** → **System** → **VCA Configuration** to configure the engine mode.

### Steps

1. Go to **Configuration** → **VCA** → **Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

#### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


#### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

#### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **Staying Overtime Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Mode**.

#### Arbitrary Mode

When there are people staying in the detection area among the leaving crowd, the device will trigger an alarm.

#### Single Person Mode

When there is only one person staying in the detection area among the leaving crowd, the device will trigger an alarm.

- 6) Set **Duration**.

#### Duration

The device will trigger an alarm when the time exceeds the limit.


- 7) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

### Overlay Rule Frame


The rule frame will be displayed on the captured picture.

### Overlay Target Frame

The target frame will be displayed on the captured picture.

- 8) Click  to draw the detection area in the preview window.
- 9) Click **Save**.
6. Set the arming schedule. Refer to **Configure Arming Schedule**.
7. Set linkage actions. Refer to **Configure Linkage Actions**.
8. Click **Save**.

### What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

## 6.2.3 Number of People Exception Detection

Number of people exception detection counts the amount of people in the detection area, when the number reaches the threshold, it will trigger an alarm.

### Before You Start

Ensure the engine mode is set as **Work Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

### Steps

1. Go to **Configuration → VCA → Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

#### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


#### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

#### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **Number of People Exception Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Duration**.

#### Duration

The device will trigger an alarm when the time exceeds the limit.

6) **Optional:** Check **Overlay Rule Frame**.

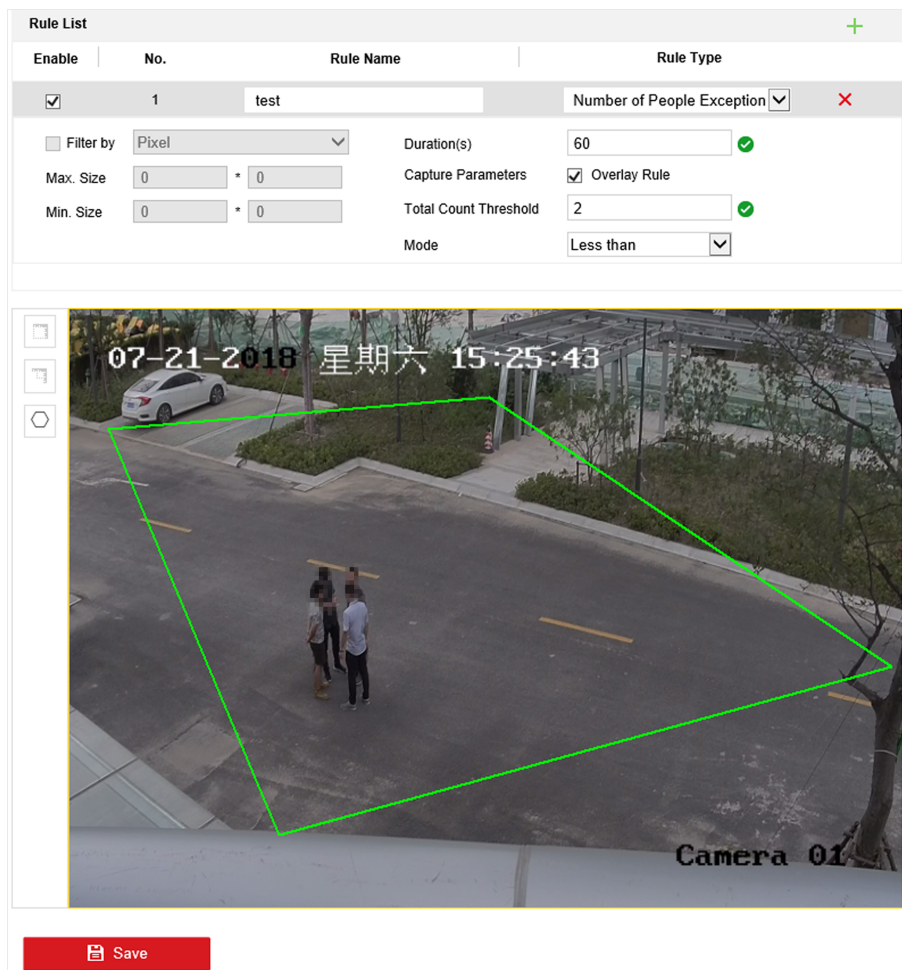
### Overlay Rule Frame

The rule frame will be displayed on the captured picture.

7) Set **Mode**.

8) Click  to draw the detection area in the preview window.

9) Click **Save**.




**Figure 6-1 Number of People Exception Detection**

6. Set the arming schedule. Refer to **Configure Arming Schedule** .

7. Set linkage actions. Refer to **Configure Linkage Actions** .

8. Click **Save**.

### What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

### 6.2.4 Playing Mobile Phone Detection

Playing mobile phone detection detects whether the person in the detection is using mobile phone.

#### Before You Start

Ensure the engine mode is set as **Work Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

#### Steps

1. Go to **Configuration → VCA → Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

##### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


##### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

##### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **Playing Mobile Phone Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Duration**.

##### Duration

The device will trigger an alarm when the time exceeds the limit.


- 6) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

##### Overlay Rule Frame


The rule frame will be displayed on the captured picture.

##### Overlay Target Frame

The target frame will be displayed on the captured picture.

- 7) Click  to draw the detection area in the preview window.
  - 8) Click **Save**.
6. Set the arming schedule. Refer to **Configure Arming Schedule**.
  7. Set linkage actions. Refer to **Configure Linkage Actions**.
  8. Click **Save**.

## What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

## 6.3 Street Behavior Analysis

Street behavior analysis includes people gathering detection, people running detection, violent motion detection, and people falling down detection. You can configure behavior analysis via web browser.

### 6.3.1 People Gathering Detection

People gathering detection is used to detect whether the density of people within a specified area exceeds the set value.

#### Before You Start

Ensure the engine mode is set as **Street Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

#### Steps

1. Go to **Configuration → VCA → Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

##### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).

##### Auto-Switch


Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

##### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.

- 1) Click  to add a rule.
- 2) Select **Rule Type** as **People Gathering**.
- 3) Enter the rule name.
- 4) Enable the rule.
- 5) Set **Duration**.

##### Duration

The device will trigger an alarm when the time exceeds the limit.

- 6) Set **Sensitivity**.

##### Sensitivity

The higher the sensitivity is, the easier the alarm will be triggered.



7) Set **Alarm Interval**.

**Alarm Interval**

Alarm interval is the shortest time interval between two alarms.

8) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

**Overlay Rule Frame**

The rule frame will be displayed on the captured picture.

**Overlay Target Frame**

The target frame will be displayed on the captured picture.

9) Set **Number of People Threshold**.

**Number of People Threshold**

When the number of people in the detection area exceeds the threshold, it will trigger an alarm.

10) Click  to draw the detection area in the preview window.


11) Click **Save**.



Figure 6-2 People Gathering Detection

6. Set the arming schedule. Refer to **Configure Arming Schedule** .
7. Set linkage actions. Refer to **Configure Linkage Actions** .
8. Click **Save**.

### What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

## 6.3.2 People Running Detection

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

### Before You Start

Ensure the engine mode is set as **Street Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

### Steps

1. Go to **Configuration → VCA → Behavior Analysis** .
2. Select a camera.
3. Select an analysis mode.

#### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


#### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

#### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **People Running Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Duration**.

#### Duration

The device will trigger an alarm when the time exceeds the limit.

- 6) Set **Mode**.

#### Multiple Persons Mode

When multiple persons are running in the detection area, the device will trigger an alarm.

#### Single Person Mode

When a single person is running in the detection area, the device will trigger an alarm.

7) Set **Sensitivity**.

**Sensitivity**

The higher the sensitivity is, the easier the alarm will be triggered.

8) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

**Overlay Rule Frame**

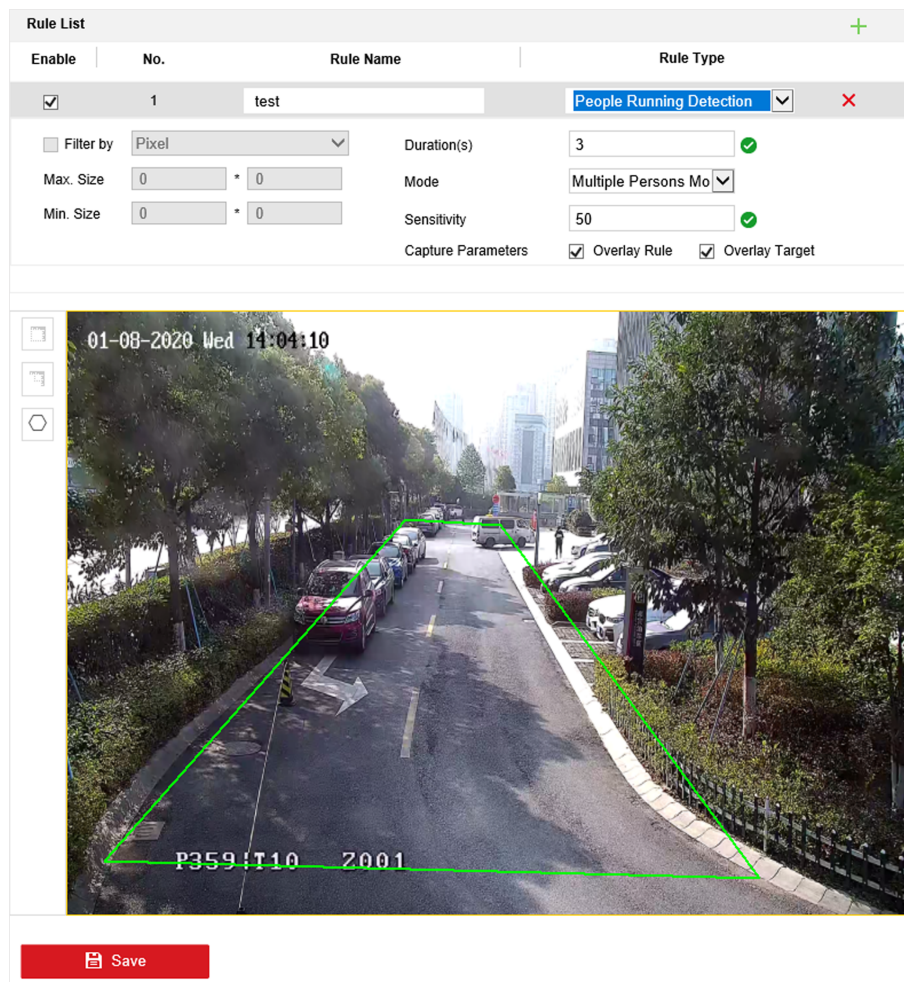
The rule frame will be displayed on the captured picture.

**Overlay Target Frame**

The target frame will be displayed on the captured picture.

9) Click  to draw the detection area in the preview window.

10) Click **Save**.




**Figure 6-3 People Running Detection**

6. Set the arming schedule. Refer to **Configure Arming Schedule** .

7. Set linkage actions. Refer to **Configure Linkage Actions** .

8. Click **Save**.

### What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

### 6.3.3 Physical Conflict Detection

Physical conflict detection alarm will be triggered when the movement degree exceeds the set value in the detection area.

#### Before You Start

Ensure the engine mode is set as **Work Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

#### Steps

1. Go to **Configuration → VCA → Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

##### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


##### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

##### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **Physical Conflict Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Duration**.

##### Duration

The device will trigger an alarm when the time exceeds the limit.

- 6) Set **Sensitivity**.

##### Sensitivity

The higher the sensitivity is, the easier the alarm will be triggered.

- 7) Set **Alarm Interval**.

##### Alarm Interval

Alarm interval is the shortest time interval between two alarms.


- 8) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

##### Overlay Rule Frame


The rule frame will be displayed on the captured picture.

### Overlay Target Frame

The target frame will be displayed on the captured picture.

- 9) Click  to draw the detection area in the preview window.
- 10) Click **Save**.
6. Set the arming schedule. Refer to **Configure Arming Schedule**.
7. Set linkage actions. Refer to **Configure Linkage Actions**.
8. Click **Save**.

### What to do next

You can check  to view the live detection result via GUI. Refer to **Target Detection** for details.

## 6.3.4 People Falling Down Detection

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

### Before You Start

Ensure the engine mode is set as **Street Behavior Analysis**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

### Steps

1. Go to **Configuration → VCA → Behavior Analysis**.
2. Select a camera.
3. Select an analysis mode.

#### Real Time

Provide real-time intelligent analysis for the video stream of the IP camera(s).


#### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Local VCA Behavior Analysis**.

#### Enable Local VCA Behavior Analysis

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

5. Set rules and detection areas.
  - 1) Click  to add a rule.
  - 2) Select **Rule Type** as **People Falling Down Detection**.
  - 3) Enter the rule name.
  - 4) Enable the rule.
  - 5) Set **Sensitivity**.

#### Sensitivity

The higher the sensitivity is, the easier the alarm will be triggered.


- 6) **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

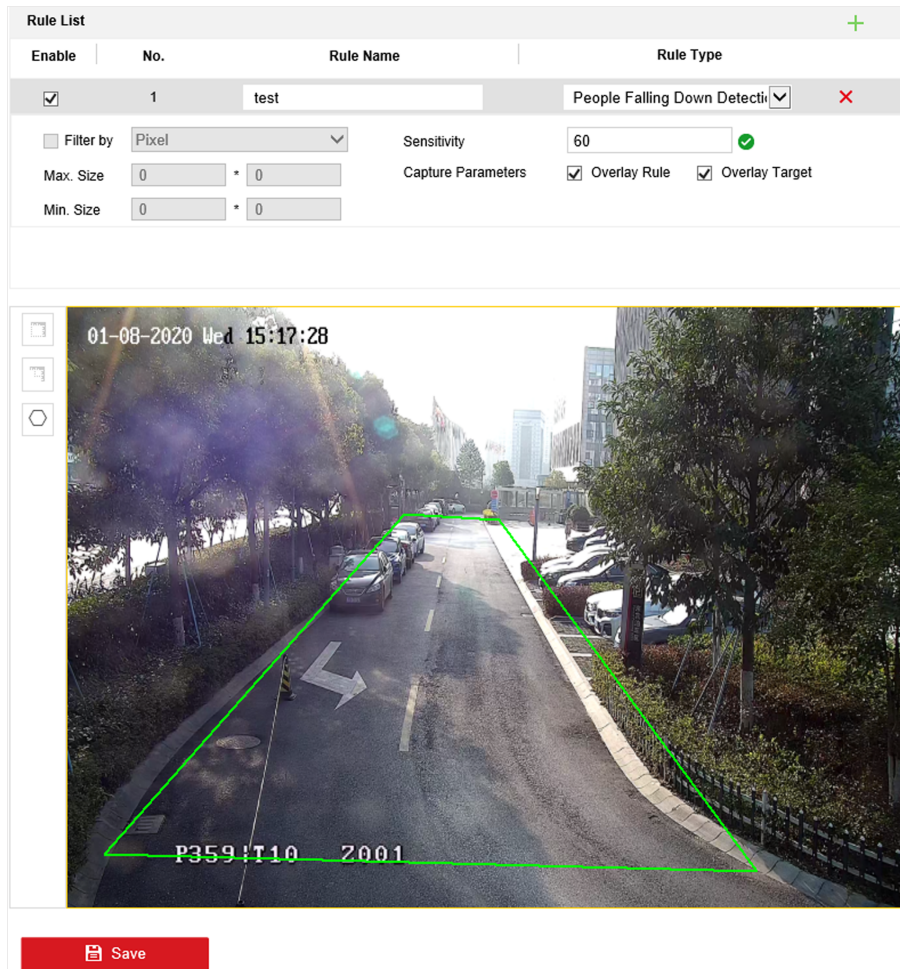
## Overlay Rule Frame

The rule frame will be displayed on the captured picture.

## Overlay Target Frame

The target frame will be displayed on the captured picture.


- 7) Click  to draw the detection area in the preview window.
- 8) Click **Save**.



**Figure 6-4 People Falling Down Detection**

6. Set the arming schedule. Refer to *Configure Arming Schedule* .
7. Set linkage actions. Refer to *Configure Linkage Actions* .
8. Click **Save**.

## What to do next

You can check  to view the live detection result via GUI. Refer to *Target Detection* for details.

## 6.4 Hard Hat Detection

Hard hat detection detects people who are wearing hard hats or not. For the people who are not wearing hard hats, you can link face picture library to the detection to recognize these people and know their names. You can configure hard hat detection via web browser.

### Before You Start

Ensure the engine mode is set as **Hard Hat Detection**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

### Steps

---

#### Note

- The camera installation tilt angle is recommended to be 20° to 60°.
  - When people are standing straightly in the image, the length of people should be larger than 25% of the total image length.
  - There should not be too many people in the detection area.
- 

1. Go to **Configuration → VCA → Hard Hat Detection** .
2. Select a camera.
3. Select an analysis mode.

#### **Real Time**

Provide real-time intelligent analysis for the video stream of the IP camera(s).

#### **Auto-Switch**

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable Without Hard Hat Detection** or **Hard Hat Detection** as your desire.
- 

#### Note

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

---

5. **Optional:** Check **Overlay Rule Frame** or **Overlay Target Frame**.

#### **Overlay Rule Frame**

The rule frame will be displayed on the captured picture.

#### **Overlay Target Frame**

The target frame will be displayed on the captured picture.

6. Set the detection area.
    - 1) Set **Region**. You can select a region number for the detection area.
    - 2) Click **Draw Area** to draw the detection area in the preview window.
    - 3) Click **Stop Drawing**.
    - 4) Click **Save**.
  7. Set the arming schedule. Refer to **Configure Arming Schedule** .
-

8. Set linkage actions. Refer to **Configure Linkage Actions** . If you requires to recognize the people who are not wearing hard hat, check **Face Recognition**.
9. If you have enabled **Face Recognition** in **Linkage Method**, you shall set the face picture library and face grading parameters.
  - 1) Select the face picture libraries and set the similarity for each face picture library. If the similarity of face picture exceeds the value, it will trigger an alarm.
  - 2) Check **Enable** to set face grading parameters. Face grading is used for face picture selection. It only uses face pictures which satisfy grading requirement for analysis. The larger the pupil distance is, and the smaller the tilt and pan angles are, the better the analysis effect will be.

### Confidence Interval of Facial Feature

The face grading score of each face picture quality level. You can set the score of high, medium, and low rating pictures.

### Pupil Distance

Pupil distance is the distance between two pupils.

### Elevation Angle



Tilt angle is the angle between your view and horizontal plane.

### Pan Angle

Pan angle is the angle between your view and vertical plane.

10. Click **Save**.

### What to do next

- a. You can check  to view the live detection results via GUI. Refer to **Target Detection** for details.
- b. You can click  in to detailed results via GUI. Refer to **Not Wearing Hard Hat Detection** for details.

## 6.5 Face Picture Library Management

Face picture library is mainly used for face picture storage and face picture comparison.

### 6.5.1 Add a Face Picture Library

#### Steps

1. Go to **Smart Analysis** → **Face Picture Database** .
2. Click **+** .
3. Enter the face picture library name.
4. Click **OK**.



#### Note

You can click  or  to edit the library name or delete the library.

---





### 6.5.2 Upload Face Pictures to the Library

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

#### Before You Start

- Ensure the picture format is JPEG or JPG.
- For each picture, ensure it only has one face.
- Import all pictures to a backup device in advance.

#### Steps

1. Select a face picture library in the list.
2. Click **Add** or **Import Face Picture Library**.
3. Import picture(s).
  - **Add**: Select a picture to import and click **Import**.
  - **Import Face Picture Library**: Select multiple pictures to import and click **Import**.
4. **Optional**: Select pictures and click **Copy to** to copy the uploaded pictures of the current library to other library.
5. **Optional**: Select a picture and click **Edit** to modify the picture information.
6. **Optional**: Select a picture from the list and click **Delete** to delete the picture.
7. **Optional**: Select a library and click **Export Face Picture Library** to export library to backup device.
8. **Optional**: Click  or  to view by figure or list.

## 6.6 People Counting

People counting statistics and regional people counting of the IP camera video stream are available, and you can configure them via web browser.

### 6.6.1 People Counting Statistics

The device can analyze the people counting statistics of the rule area, generate people counting statistics report, and upload the alarm information to the platform or the client server center.

#### Before You Start

Ensure the engine mode is set as **People Counting**. You can go to **Configuration** → **System** → **VCA Configuration** to configure the engine mode.

#### Steps

1. Go to **Configuration** → **VCA** → **People Counting** → **People Counting Statistics** via web browser.
2. Select an IP camera.
3. Select an analysis mode.

#### Real Time





Provide real-time intelligent analysis for the video stream of the IP camera(s).

**Auto-Switch**

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable People Counting**.
5. Click **Rule**.

**Table 6-1 Rule Drawing Instruction**

Icon	Description
	Draw a detection line.
	Draw the rule area: <ul style="list-style-type: none"> <li>Left click the screen to draw a polygon. A point will be fixed and a line can be drawn accordingly. Right click to stop drawing. You can adjust the shape of polygon after drawing.</li> <li>One rule area is supported.</li> <li>Polygon area supports 3 to 10 lines.</li> <li>Please draw convex polygon. Concave polygon is not available.</li> </ul>
	Change the direction that should be detected. This direction indicates the direction of crowds crossing detection line.
	Delete the detection line and area.

 **Note**

The people counting statistics provided by the device is the statistics of people who cross the detection line and within the rule area in the recording or video stream.

---

6. Set **Alarm Upload Interval**.

**Alarm Upload Interval**

Alarm interval is the shortest time interval between two alarms.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Save**.

**What to do next**

You can view people counting statistics report via local device GUI. Refer to **View People Counting Statistics** .

## 6.6.2 Regional People Counting

You can analyze the number of people threshold within the rule area and trigger the alarm.

## Before You Start

Ensure the engine mode is set as **People Counting**. You can go to **Configuration → System → VCA Configuration** to configure the engine mode.

## Steps


1. Go to **Configuration → VCA → People Counting → Regional People Counting** .
2. Select a camera.
3. Select an analysis mode.

### Real Time



Provide real-time intelligent analysis for the video stream of the IP camera(s).

### Auto-Switch

Provide sequential intelligent analysis for the video stream of the IP camera. (Once one IP camera only).

4. Check **Enable**.
5. Click **Rule**.
6. Set rules and detection areas.
  - 1) Click  to add rule.
  - 2) Configure **Number of People Threshold** and **Mode**.
  - 3) Draw detection areas.

**Table 6-2 Area Drawing Instruction**

Icon	Description
	Draw the rule area: <ul style="list-style-type: none"> <li>Left click the screen to draw a polygon. A point will be fixed and a line can be drawn accordingly. Right click to stop drawing. You can adjust the shape of polygon after drawing.</li> <li>One rule area is supported.</li> <li>Polygon area supports 3 to 10 lines.</li> <li>Please draw convex polygon. Concave polygon is not available.</li> </ul>
	Delete the detection line and area.



### Note

When the device detects that the number of people in the recording or video stream within the rule area exceeds **Number of People Threshold** and **Mode**, the alarm will be triggered.

7. Set the arming schedule. Refer to **Configure Arming Schedule** .
8. Set linkage actions. Refer to **Configure Linkage Actions** .
9. Click **Save**.

## 6.7 Smart Search

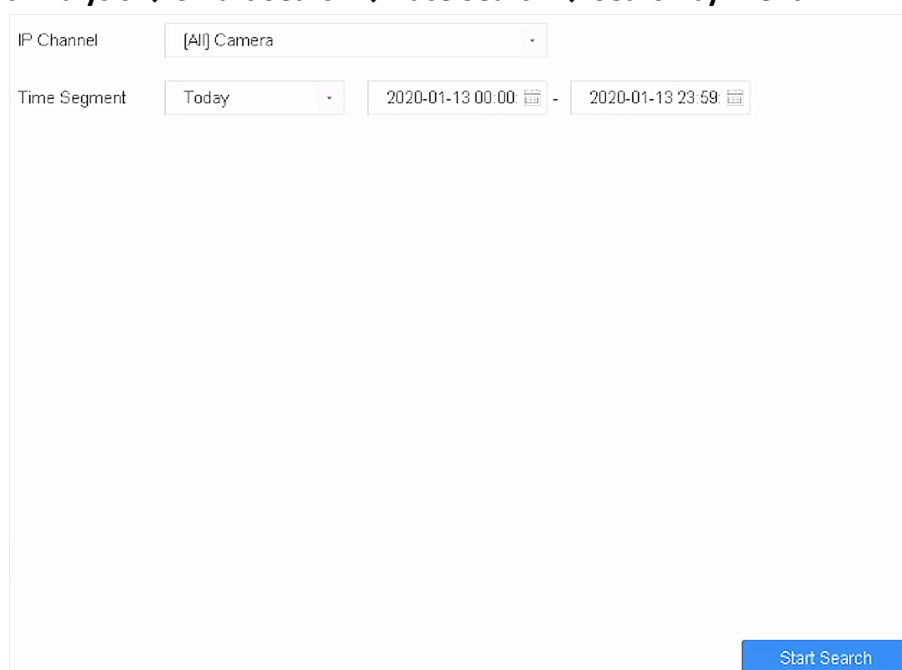
### 6.7.1 Face Picture Search

#### Search by Event

Search face picture by face picture comparison results.

#### Steps

1. Go to **Smart Analysis** → **Smart Search** → **Face Search** → **Search by Event** .



The screenshot displays a search interface with the following elements:

- IP Channel:** A dropdown menu currently showing "[All] Camera".
- Time Segment:** A dropdown menu currently showing "Today".
- Date Range:** Two date-time input fields showing "2020-01-13 00:00" and "2020-01-13 23:59", separated by a hyphen. Each field has a calendar icon to its right.
- Start Search:** A blue button located at the bottom right of the form.

**Figure 6-5 Search by Event**

2. Set the start time and end time.
3. Select a channel.
4. Click **Start Search**. The search result list displays 1 channel.
5. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

#### What to do next

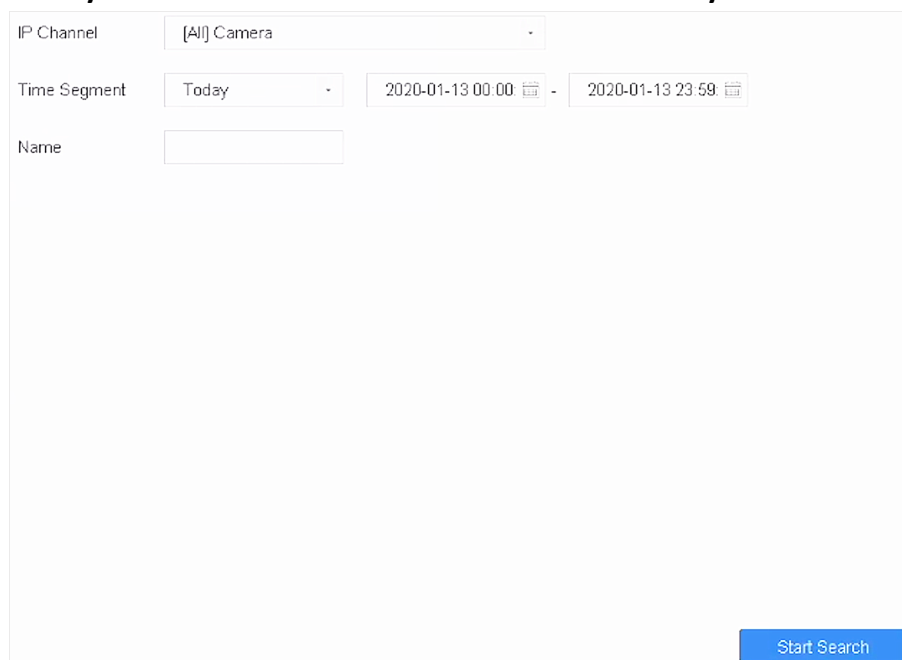
Refer to **View Searching Result** .

#### Search by Personal Name

Search face picture by personal name.

## Steps

1. Go to **Smart Analysis** → **Smart Search** → **Face Search** → **Search by Name** .



The screenshot shows a search interface with the following elements:

- IP Channel:** A dropdown menu currently showing "[All] Camera".
- Time Segment:** A dropdown menu showing "Today", followed by two date-time pickers. The first is set to "2020-01-13 00:00" and the second to "2020-01-13 23:59".
- Name:** An empty text input field.
- Start Search:** A blue button located at the bottom right of the form.

**Figure 6-6 Search by Personal Name**

2. Set the start time and end time of the face pictures to search.
3. Select a channel.
4. Enter a name.
5. Click **Start Search**. The search result list displays 1 channel.
6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

## What to do next

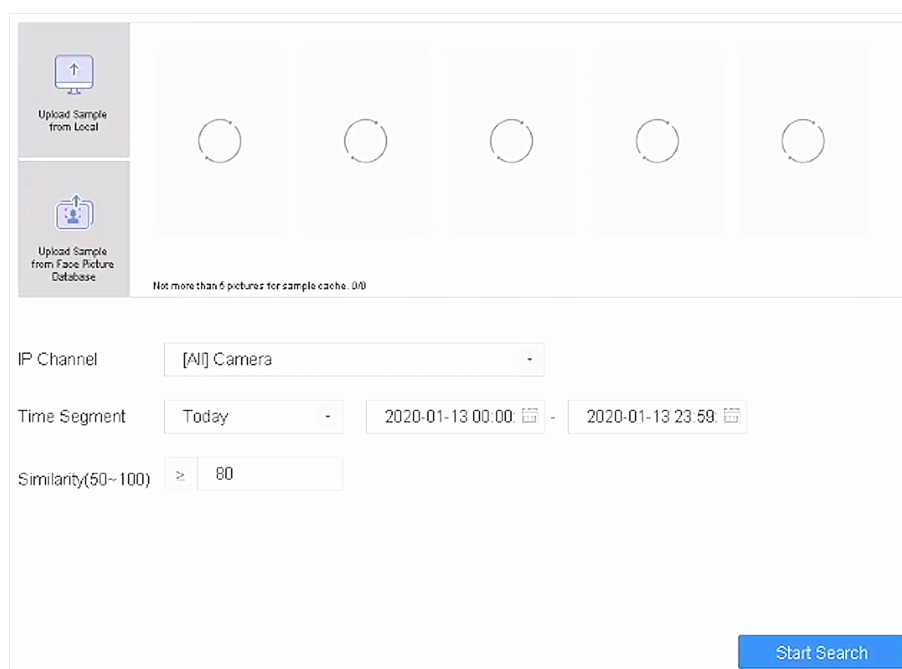
Refer to **View Searching Result** .

## Search by Uploaded Picture

You can search the face pictures by uploaded picture.

## Steps

1. Go to **Smart Analysis** → **Smart Search** → **Face Search** → **Search by Picture** .



**Figure 6-7 Search by Uploaded Picture**

2. Select a channel.
3. Select face pictures for search.
  - Click **Upload Sample from Local** and select face pictures from your local directory.
  - Click **Upload Sample from Face Picture Database** and select face pictures from created face picture libraries.
4. Set the start time and end time.
5. Set the **Similarity** value (range: 0 to 100). Device will analyze the similarity between samples and face pictures in library and show pictures the similarity of which are higher than the set one.
6. Click **Start Search**. The search result list displays 1 channel.
7. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

### **What to do next**

Refer to ***View Searching Result*** .

### **View Searching Result**

- Double click a file to view the related video.
- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to ***Search by Uploaded Picture*** .
- Click **Export** to export the selected file(s) to a backup device. You can click **Select All** to select all files.

## Note

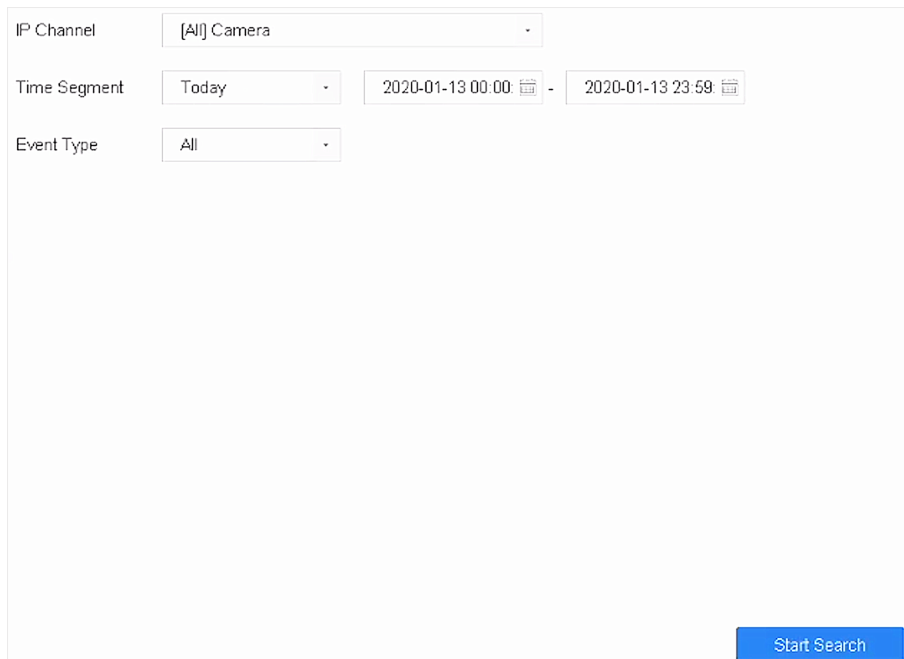
- You can click  to view export progress.
  - You can click  to return to search interface.
- 

## 6.7.2 Behavior Analysis Search

You can search work behavior analysis events and street behavior analysis event, including absence/sleep on duty detection, people overstay detection, number of people exception detection, using mobile phone detection, people gathering detection, people running detection, violent motion detection, and people falling down detection.

### Steps

1. Go to **Smart Analysis → Smart Search → Behavior Analysis → Search by Event** .



The screenshot displays a search interface with the following fields:

- IP Channel:** [All] Camera
- Time Segment:** Today (with a date range from 2020-01-13 00:00 to 2020-01-13 23:59)
- Event Type:** All



A blue **Start Search** button is positioned at the bottom right of the search area.

**Figure 6-8 Behavior Analysis Search**

2. Specify search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
5. **Optional:** Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.

---

## Note

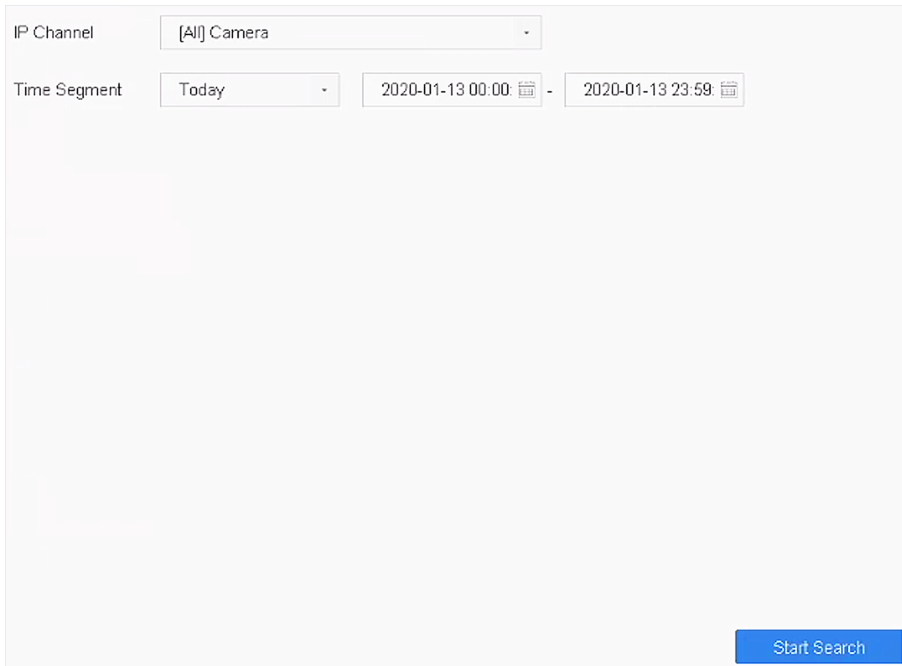
- You can click  to view export progress.
  - You can click  to return to search interface.
- 

## 6.7.3 Not Wearing Hard Hat Search

You can search not wearing hard hat event according to manually specified search conditions.

### Steps

1. Go to **Smart Analysis** → **Smart Search** → **Not Wearing Hard Hat** → **Search by Event** .




**Figure 6-9 Not Wearing Hard Hat Search**

2. Specify search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
5. **Optional:** Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.

---

## Note

- You can click  to view export progress.
  - You can click  to return to search interface.
-



### 6.7.4 Regional People Counting Search



Based on picture search of regional people counting, this function provides recording file 5 seconds before or after the picture searched.

#### Steps

1. Go to **Smart Analysis** → **Smart Search** → **Regional People Counting** .
2. Set regional people counting searching parameters.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
5. **Optional:** Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.



#### Note

- You can click  to view export progress.
  - You can click  to return to search interface.
- 

### 6.7.5 Human Body Detection Search

Search human body pictures according to manually specified search conditions.

#### Steps

1. Go to **Smart Analysis** → **Smart Search** → **Human Body Detection** → **Search by Appearance** .

The screenshot displays a search configuration interface. It includes three main sections: 'IP Channel' with a dropdown menu currently showing '[All] Camera'; 'Time Segment' with a dropdown menu showing 'Today' and a date range from '2020-01-13 00:00' to '2020-01-13 23:59'; and 'Event Type' with a dropdown menu showing 'Human Body Alarm'. A blue button labeled 'Start Search' is positioned at the bottom right of the form.

**Figure 6-10 Human Body Detection Search**

2. Specify search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
5. **Optional:** Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.

---

 **Note**

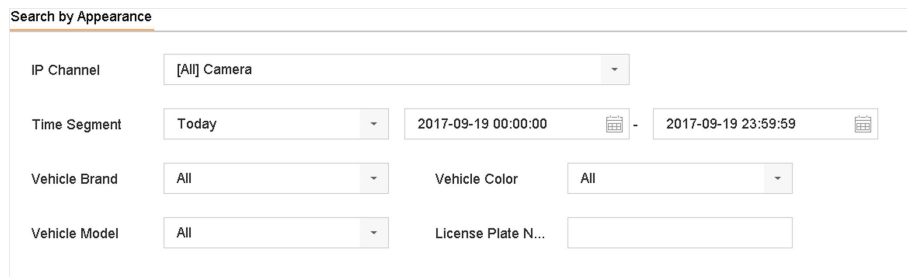
- You can click  to view export progress.
  - You can click  to return to search interface.
- 

## 6.7.6 Vehicle Search

You can search and view the matched vehicle pictures.

### Steps

1. Go to **Smart Analysis** → **Smart Search** → **Vehicle Search** .
2. Select the IP camera for the vehicle search.
3. Set search conditions.



**Figure 6-11 Vehicle Search**

4. Click **Start Search**. The search result list displays 1 channel.
5. Click Channel to select a channel as your desire. It will display search results for the selected channel.
6. Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.

## Note

You can click  to view export progress.

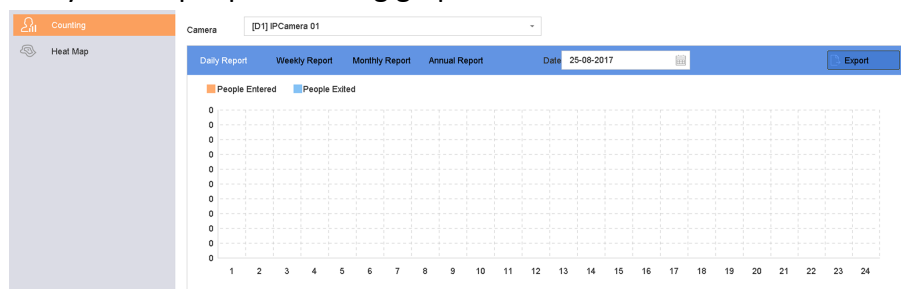
## 6.8 Smart Report

### 6.8.1 View People Counting Statistics

People counting statistics calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

#### Steps

1. Go to **Smart Analysis** → **Smart Report** → **Counting** via local device GUI.
2. Select a camera.
3. Select the report type.
4. Set **Date** to analyze. The people counting graphic will show.



**Figure 6-12 People Counting Interface**

5. **Optional:** Click **Export** to export the report in Microsoft Excel format.

## 6.8.2 Heat Map

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.

### Before You Start

The function must be supported by the connected IP camera and the corresponding parameters must be set.

### Steps

1. Go to **Smart Analysis** → **Smart Report** → **Heat Map**.
2. Select a camera.
3. Select the report type.
4. Set **Date** to analyze.

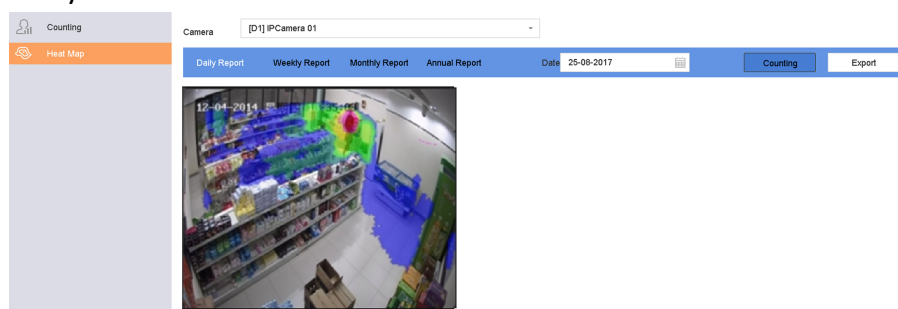


Figure 6-13 Heat Map

5. Click **Counting**.

---

### Note

As shown in the figure above, red color block (255, 0, 0) indicates the most trafficked area, and blue color block (0, 0, 255) indicates the less-popular area.

---







The results will be displayed in graphics marked in different colors.

6. **Optional:** Click **Export** to export the statistics report in Microsoft Excel format.

## 6.9 Target Detection


In live view mode, the target detection function can achieve smart detection, facial detection, vehicle detection, and human body detection during the last 5 seconds and the following 10 seconds.

### Steps

1. In Live View mode, click Target Detection to enter the target detection interface.
2. Select different detection types: smart detection (  ), vehicle detection (  ), face detection (  ), and human body detection (  ).
3. Select the historical analysis (  ) or real-time analysis (  ) to obtain the results.

---

 **Note**





- The smart analysis results of the detection are displayed in the list. Click a result in list to play the related video.
  - Smart detection (  ) includes work behavior analysis, street behavior analysis, not wearing hart hat detection, perimeter protection, etc.
-

## Chapter 7 File Management

### 7.1 Search Files



Specify detailed conditions to search videos and pictures.

#### Steps

1. Go to **File Management** → **Video** , or **File Management** → **Picture** .
2. Select a search method. For example, **Search by Appearance**, or **Search by Event**.
3. Specify detailed conditions, including time, camera, etc.
4. Click **Start Search**.
5. Click **Channel** to select a channel as your desire. It will display the searching results of the selected channel.
6. **Optional:** Click  or  to switch view mode.
7. **Optional:** For videos, click  or  in different view mode to lock a video. The locked video will not be overwritten.
8. **Optional:** Export search results.
  - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
  - 2) Click **Export** to export the selected file(s) to a backup device.



#### Note

- You can click  to view export progress.
  - You can click  to return to search interface.
- 

### 7.2 Export Files

Export files for backup purposes to a USB device, or eSATA HDD.

#### Steps

1. Search files. Refer to **Search Files** for details.
2. Select files.
3. Click **Export**.
4. **Optional:** For vehicle files, check **Backup License Plate Statistics Info** to export license plate statistics information later.
5. Select the file to export as **Video and log** and click **OK**.
6. Select the backup device and folder path.
7. Click **OK**.

### 7.3 Smart Search

You can search face files, behavior analysis files, not wearing hard hat files, human body files and vehicles in **File Management** → **Smart Search** . Refer to ***Smart Search*** for details.

## Chapter 8 POS Configuration

The device can be connected to a POS machine/server, and receive a transaction message to overlay on the image during Live View or playback, as well as trigger a POS event alarm.

### 8.1 Configure POS Connection

#### Steps

1. Go to **System** → **POS** .
2. Click **Add**.



The screenshot shows a web interface for adding a POS device. It features the following elements: an 'Add POS' title, an 'Enable' checkbox, a 'POS Name' dropdown menu with 'POS 3' selected, a 'POS Protocol' dropdown menu with 'AVE' selected and a 'Custom' button, a 'Connection Mode' dropdown menu with 'Sniff' selected, and a 'Parameters' button.

**Figure 8-1 POS Settings**

3. Select a POS device from the drop-down list.
4. Check **Enable**.

---

#### **Note**

The number of POS devices supported by each device is the half of its number of channel, e.g., 8 POS devices are supported for the DS-9616NI-I8 model.

---

5. Select **POS Protocol**.

---

#### **Note**

When a new protocol is selected, reboot the device to activate the new settings.

---

#### **Universal Protocol**

Click **Advanced** to expand more settings when selecting the 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.



Start Line Identifier	<input type="text"/>	Hex	<input checked="" type="checkbox"/>
Line Break	0D0A	Hex	<input checked="" type="checkbox"/>
End Line Identifier	<input type="text"/>	Hex	<input checked="" type="checkbox"/>
Case Sensitive	<input checked="" type="checkbox"/>		
Filtering Identifier	<input checked="" type="checkbox"/>		
Enable XML Prot...	<input checked="" type="checkbox"/>		

OK Cancel

**Figure 8-2 Universal Protocol Settings**

## 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.

Click **Custom** to configure the AVE settings. Select **Rule** as **VSI-ADD** or **VNET**. Set the address bit of the POS message to send. Click **OK** to save the settings.

## NUCLEUS

Click the **Custom** to configure the NUCLEUS settings.

Enter the employee No., shift No., and the terminal No. in the field. The matching message sent from the POS device will be used as the valid POS data.



### Note

The NUCLEUS protocol must be used in the RS-232 connection communication.

---

6. Select **Connection Mode** and click **Parameters** to configure the parameters for each 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.

Set the **Allowed Remote IP Address** of the device sending the POS message.

### 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.

Set the **Allowed Remote IP Address** of the device sending the POS message.

## 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, parity, and flow ctrl.

USB-to-RS-232 Settings	
Serial Port Number	1
Baud Rate	4800
Data Bit	5
Stop Bit	1
Parity	None
Flow Ctrl	None
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**Figure 8-3 USB-to-RS-232 Settings**

## RS-232 Connection

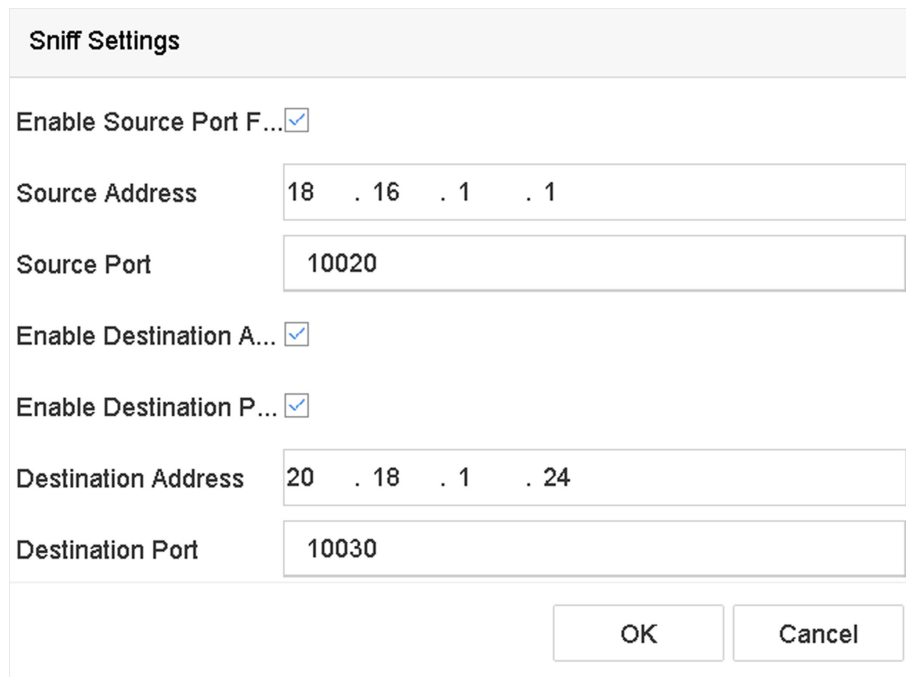
Connect the device and the POS machine via RS-232. The RS-232 settings can be configured in **Menu → Configuration → RS-232**. The Usage must be set to Transparent Channel.

## 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.



The Sniff Settings dialog box contains the following fields and options:

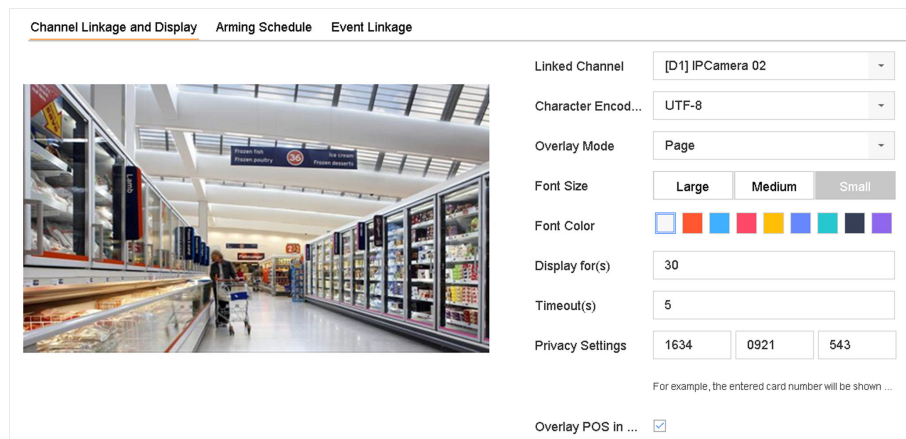
- Enable Source Port Filtering:**
- Source Address:** 18 . 16 . 1 . 1
- Source Port:** 10020
- Enable Destination Address Filtering:**
- Enable Destination Port Filtering:**
- Destination Address:** 20 . 18 . 1 . 24
- Destination Port:** 10030
- Buttons:** OK, Cancel

Figure 8-4 Sniff Settings

## 8.2 Configure POS Text Overlay

### Steps

1. Go to **System** → **POS** .
2. Click **Channel Linkage and Display**.



The Overlay Character Settings dialog box includes the following configuration options:

- Channel Linkage and Display:** (Active tab)
- Arming Schedule:**
- Event Linkage:**
- Linked Channel:** [D1] IPCamera 02
- Character Encod...:** UTF-8
- Overlay Mode:** Page
- Font Size:** Large (selected), Medium, Small
- Font Color:** [Color selection palette]
- Display for(s):** 30
- Timeout(s):** 5
- Privacy Settings:** 1634, 0921, 543
- For example, the entered card number will be shown ...**
- Overlay POS in ...:**

Figure 8-5 Overlay Character Settings

3. Select **linked channel** to overlay the POS characters.
4. Set the characters overlay for the enabled POS.
  - Character encoding format: currently the Latin-1 format is available
  - Overlay mode of the characters to display in scrolling or page mod

- Font size and font color
  - Display time (sec) of the characters. The value ranges 5 -3600 sec.
  - Timeout of POS event. The value ranges 5 -3600 sec. When the device has not received the POS message within the defined time, the transaction ends.
5. In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc.
- The defined privacy information will be displayed using \*\*\*on the image instead.
6. Check **Overlay POS in Live View**. When this feature is enabled, the POS information is overlaid on the Live View image.



Drag the frame to adjust the textbox size and position on POS settings interface preview screen.

---

7. Click **Apply** to activate the settings.

### 8.3 Configure POS Alarm

A POS event can trigger channels to start recording, or trigger full screen monitoring or an audio warning, notifying the surveillance center, send e-mail, etc.

#### Steps

1. Go to **Storage → Recording Schedule** .
2. Set the POS event's arming schedule.
3. Go to **System → POS** .
4. Click **Event Linkage** on the POS adding or editing interface.

Channel Linkage and Display Event Linkage

<input checked="" type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Channel
<input checked="" type="checkbox"/> Full Screen Monitoring	<input checked="" type="checkbox"/> Local->1	<input checked="" type="checkbox"/> D1
<input checked="" type="checkbox"/> Audible Warning	<input type="checkbox"/> Local->2	<input checked="" type="checkbox"/> D2
<input checked="" type="checkbox"/> Send Email	<input checked="" type="checkbox"/> Local->3	<input type="checkbox"/> D3
	<input type="checkbox"/> Local->4	<input type="checkbox"/> D4
	<input type="checkbox"/> 10.15.2.250:8000->1	

\*Notice: please confirm the event output in "Live View" settings menu is the same with the real event output.

**Figure 8-6 Set Trigger Cameras of POS**

5. Select the normal linkage actions.
6. Select one or more alarm output(s) to trigger.
7. Select one or more channels to record or become full-screen monitoring when a POS alarm is triggered.
8. Click **Apply** to save the settings.

# Chapter 9 Storage

 **Note**

The available functions in this chapter may vary according to different models.

## 9.1 Storage Device Management

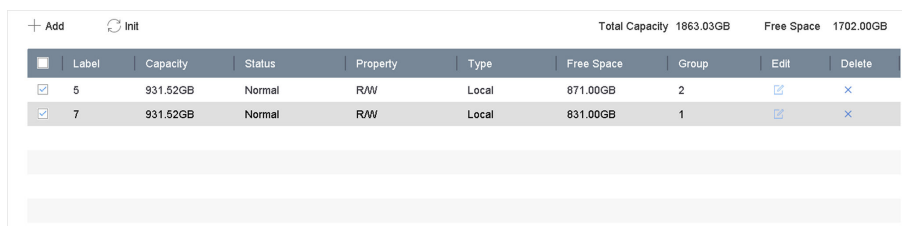
### 9.1.1 Manage Local HDD





#### Configure HDD Group

Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular HDD group through HDD settings.

#### Steps

1. Go to **Storage** → **Storage Mode** .
2. Select **Mode** as **Group**.
3. Click **Apply**.
4. Go to **Storage** → **Storage Device** .
5. Select a HDD.



+ Add		Init		Total Capacity 1863.03GB		Free Space 1702.00GB			
<input type="checkbox"/>	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
<input checked="" type="checkbox"/>	5	931.52GB	Normal	R/W	Local	871.00GB	2		
<input checked="" type="checkbox"/>	7	931.52GB	Normal	R/W	Local	831.00GB	1		

**Figure 9-1 Storage Device**

6. Click  to enter Local HDD Settings interface.

Local HDD Settings

HDD No. 5

HDD Property  R/W  Read-only  Redundan...

Group  1  2  3  4  5  6  7  8  
 9  10  11  12  13  14  15  16

HDD Capacity 931.52GB

OK Cancel

**Figure 9-2 Local HDD Settings**

7. Select a group number for the HDD.
8. Click **OK**.



**Note**

Regroup the cameras for HDD if the HDD group number is changed.

---

9. Go to **Storage → Storage Mode** .
10. Select group number from the list.
11. Select related camera(s) to save videos and pictures on the HDD group.
12. Click **Apply**.


## Configure the HDD Property

HDD property can be set as R/W, Read-only, or Redundant.

### Before You Start

Set the storage mode to Group. For detailed steps, refer to *Configure HDD Group*

### Steps

1. Go to **Storage → Storage Device** .
2. Click  of desired HDD.
3. Select **HDD Property**.

### R/W

HDD supports both read and write.

### Read-only

Files in read-only HDD will not be overwritten.

### Redundant

Save the videos and pictures not only in the R/W HDD but also in the redundant HDD. It effectively enhances the data safety and reliability. Ensure at least another HDD which is in Read/Write status exists.

4. Click **OK**.

## Configure the HDD Quota

Each camera can be configured with an allocated quota for storing videos or pictures.

### Steps

1. Go to **Storage** → **Storage Mode** .
2. Select **Mode** as **Quota**.
3. Select a camera to set quota.
4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)**.
5. Click **Copy to** to copy the quota settings of the current camera to other cameras.
6. Click **Apply**.



### Note

- When the quota capacity is set to 0, all cameras will use the total capacity of HDD for videos and pictures.
  - Reboot the video recorder to activate the new settings.
- 

### 9.1.2 Add a Network Disk

You can add the allocated NAS or IP SAN disk to the device, and use it as a network HDD.

### Steps

1. Go to **Storage** → **Storage Device** .
2. Click **Add**.



Custom Add

NetHDD: NetHDD 1

Type: NAS

NetHDD IP: 120 . 36 . 2 . 39

NetHDD Directory: /nas/device1/11|

Search

OK Cancel

**Figure 9-3 Add NetHDD**

3. Select **NetHDD** type.
4. Enter **NetHDD IP** address and click **Search** to search the available NetHDD.
5. Select the desired NetHDD.
6. Click **OK**.
7. The added NetHDD will be displayed in the HDD list. Select the newly added NetHDD and click **Init**.

### 9.1.3 Manage eSATA

#### Configure eSATA for Data Storage

When there is an external eSATA device connected to your video recorder, you can configure the eSATA usage as data storage and manage the eSATA.

##### Steps

1. Go to **Storage** → **Advanced** .
2. Select eSATA Usage as **Export** or **Record/Capture**.

##### Export

Use the eSATA for backup.

## Record/Capture

Use the eSATA for record/capture. Refer to the following steps for operating instructions.

eSATA	eSATA1
Usage	Record/Capture

**Figure 9-4 eSATA Mode**

### What to do next

If eSATA usage is set as **Record/Capture**, enter the storage device interface to edit its property or initialize it.

## Configure eSATA for Auto Backup

If you made an automatic backup plan, the video recorder will back up the local videos of 24 hours ahead of the backup start time to eSATA.

### Before You Start

Ensure the device has correctly connected with an external eSATA hard drive, and its usage type is set as **Export**. Refer to *Manage eSATA* for details.

### Steps

1. Go to **Storage → Auto Backup** .
2. Check **Auto Backup**.
3. Set the backup start time in **Start Backup at**.

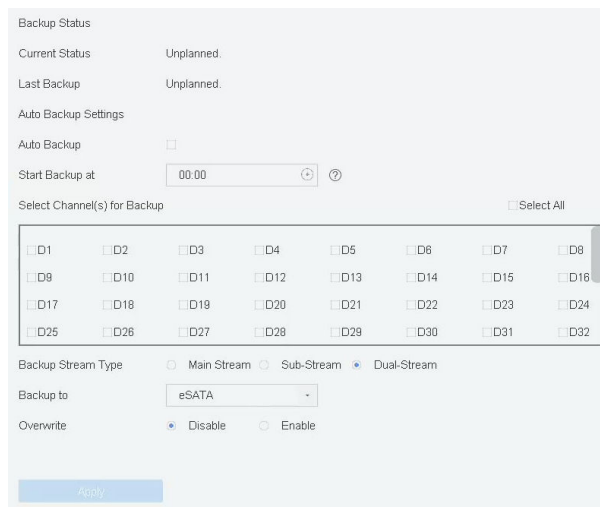
---

#### Note

If the day experiences a failed backup, the video recorder will back up the videos 48 hours ahead of the backup start time in the next day.

---

4. Select channels for backup.
5. Select **Backup Stream Type** as your desire.
6. Select **Overwrite** type.
  - **Disable**: When HDD is full, it will stop writing.
  - **Enable**: When HDD is full, it will continue to write new files by deleting the oldest files.
7. Click **Apply**.



**Figure 9-5 Configure eSATA for Auto Backup**

## 9.2 Disk Array

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.

### 9.2.1 Create a Disk Array

The video recorder supports software-based disk arrays. Enable the RAID function as required, and ensure each HDD capacity is not less than 4 TB. Two ways are available for creating an array: one-touch configuration and manual configuration.

#### One-Touch Creation

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

#### Before You Start

Install at least 3 HDDs. If more than 10 HDDs are installed, 2 arrays will be created. To maintain reliability and stability running of the HDDs, it is recommended to use of enterprise-level HDDs of the same model and capacity.

#### Steps

1. Go to **Storage** → **Advanced** .
2. Check **Enable RAID**.

3. Click **Apply** and reboot the device to have settings take effect.
4. After reboot, go to **Storage → RAID Setup → Physical Disk**.
5. Click **One-touch Config**.
6. Edit **Array Name** and click **OK** to start configuring.

---

 **Note**

If you install 4 or more HDDs, a hot spare disk for array rebuilding will be created.

---

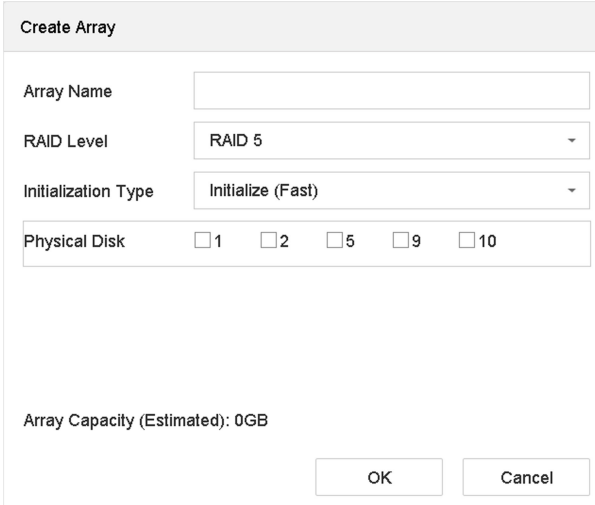
7. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage → RAID Setup → Array** to view the information of the created array.

## Manual Creation

Manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

### Steps

1. Go to **Storage → Advanced**.
2. Check **Enable RAID**.
3. Click **Apply** and reboot the device to have settings take effect.
4. After reboot, go to **Storage → RAID Setup → Physical Disk**.
5. Click **Create**.



The screenshot shows a 'Create Array' dialog box with the following fields and options:

- Array Name:** A text input field.
- RAID Level:** A dropdown menu set to 'RAID 5'.
- Initialization Type:** A dropdown menu set to 'Initialize (Fast)'.
- Physical Disk:** A row of checkboxes for disks 1, 2, 5, 9, and 10.
- Array Capacity (Estimated):** 0GB.
- Buttons:** 'OK' and 'Cancel'.

**Figure 9-6 Create Array**

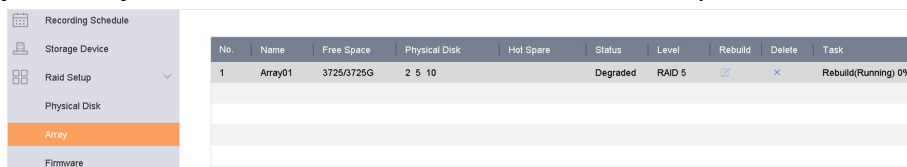
6. Enter **Array Name**.
7. Select **RAID Level** as required.
8. Select the physical disks to constitute the array.

**Table 9-1 The Required Number of HDDs**

RAID Level	The Required Number of HDDs
RAID 0	At least 2 HDDs.
RAID 1	At least 2 HDDs.
RAID 5	At least 3 HDDs.
RAID 6	At least 4 HDDs.
RAID 10	The number of HDD must be an even ranges from 4 to 16.

9. Click **OK**.

10. **Optional:** The video recorder will automatically initialize the created array. Go to **Storage** → **RAID Setup** → **Array** to view the information of the created array.



**Figure 9-7 Array List**

### 9.2.2 Rebuild an 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.

#### Functional

No disk loss in the array.

#### Offline

The number of lost disks has exceeded the limit.

#### Degraded

If any HDD fails in the array, the array degrades. Restore it to Functional status by rebuilding the array.

### Configure a Hot Spare Disk

The hot spare disk is required for the disk array automatic rebuilding.

#### Steps

1. Go to **Storage** → **RAID Setup** → **Physical Disk** .

No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	--	None
<input type="checkbox"/> 2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	<input type="checkbox"/>	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	--	None
<input type="checkbox"/> 9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	<input type="checkbox"/>	None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	--	None

**Figure 9-8 Physical Disk**

- Click  of an available HDD to set it as the hot spare disk.

## Automatically Rebuild an Array

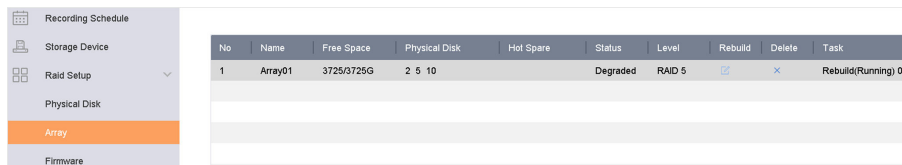
The video recorder can automatically rebuild degraded arrays with the hot spare disks.

### Before You Start

Create hot spare disks. For details, refer to *Configure a Hot Spare Disk* .

### Steps

- Go to **Storage** → **RAID Setup** → **Array** .



No	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5	<input type="checkbox"/>	<input type="checkbox"/>	Rebuild(Running) 0%

**Figure 9-9 Array List**

## Manually Rebuild an Array

If no hot spare disks are configured, rebuild a degraded array manually.

### Before You Start

At least one available physical disk must exist to rebuild an array.

### Steps

- Go to **Storage** → **RAID Setup** → **Array** .
- Click  of the degraded array.

**Rebuild Array**

Array Name: Array01

RAID Level: RAID 5

Array Disk: 5 10

Physical Disk:  2  9

OK Cancel

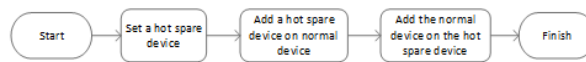
**Figure 9-10 Rebuild Array**

3. Select the available physical disk.
4. Click **OK**.
5. Click **OK** on the pop up message box "Do not unplug the physical disk when it is under rebuilding."

## Chapter 10 Hot Spare Recorder Backup

Video recorders can form an N+1 hot spare system. The system consists of several working video recorders and a hot spare video recorder; when the working video recorder fails, the hot spare video recorder switches into operation, thus increasing the reliability of the system. Contact your dealer for details of models that support the hot spare function.

A bidirectional connection shown in the figure below is required to be built between the hot spare video recorder and each working video recorder.



**Figure 10-1 Building a Hot Spare System**

---

### Note

The available functions in this chapter may vary according to different models.

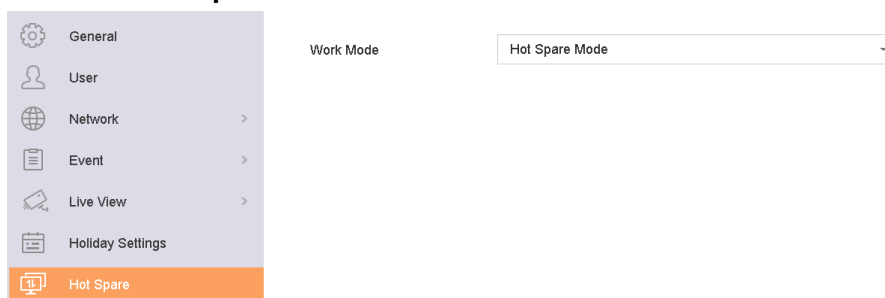
---

## 10.1 Set Hot Spare Device

Hot spare devices takes over working device tasks when working device fails.

### Steps

1. Go to **System → Hot Spare**.
2. Select **Work Mode** as **Hot Spare Mode**.



**Figure 10-2 Hot Spare**

3. Click **Apply**.
4. Click **Yes** in the pop-up attention box to reboot the device.

---

### 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 working mode of the hot spare device to normal mode to ensure the normal operation afterward.
-



## 10.2 Set Working Recorder

### Steps

1. Go to **System → Hot Spare**.
2. Select **Work Mode** as **Normal Mode**.
3. Check **Enable**.
4. Enter IP address, user name, and admin password of the hot spare recorder.

Work Mode	<input type="text" value="Normal Mode"/>
Enable	<input checked="" type="checkbox"/>
IPv4 address of the hot spare device	<input type="text" value="10 . 15 . 1 . 106"/>
User Name of Hot Spare Device	<input type="text" value="admin"/>
Password of the hot spare device	<input type="password" value="*****"/>
Working Status	<input type="text" value="Connected"/>

\*Notice: After the hot spare is enabled, you must link the working device to the hot spare device, otherwise, this function is not available.

**Figure 10-3 Hot Spare**

5. Click **Apply**.

## 10.3 Manage Hot Spare System

### Steps

1. Go to **System → Hot Spare** in the hot spare recorder.
2. Check working recorders on the device list and click **Add** to link the working recorder to the hot spare recorder. The working recorder working status descriptions are as follows:

#### No record

The working recorder works properly.

#### Backing up

If the working recorder goes offline, the hot spare recorder will record the videos of the network camera connected to the working device. The video back up functions for one working recorder at a time.

#### Synchronizing

When the working recorder comes back online, the lost videos will be restored by the video synchronization function. The video synchronization function can be enabled for one working recorder at a time.



#### Note

A hot spare recorder can connect up to 32 working recorders.

---

Work Mode

Device List

<input type="checkbox"/>	No.	IP Address
<input type="checkbox"/>	1	10.15.2.107

Working Dev...

No.	IP Address	Connection Status	Working Status	Delete

**Figure 10-4 Add Working Recorder**

## Chapter 11 Network Settings

### 11.1 Configure DDNS

You can set Dynamic DNS service for network access. Different DDNS modes are available: DynDNS, PeanutHull, and NO-IP.

#### Before You Start

You must register the DynDNS, PeanutHull, or NO-IP services with your ISP before configuring DDNS settings.

#### Steps

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

The screenshot shows the DDNS configuration interface. At the top, there are navigation tabs: TCP/IP, DDNS (highlighted), PPPoE, NTP, and NAT. Below the tabs, there is a section for enabling DDNS. The 'Enable' checkbox is checked. The 'DDNS Type' is set to 'DynDNS'. The 'Server Address' is 'member.dyndns.org', 'Device Domain Name' is '1233dyndns.com', 'User Name' is 'test', and 'Password' is masked with asterisks. The status shows 'DDNS is disabled.' and an 'Apply' button is at the bottom.

Figure 11-1 DDNS Settings

2. Check **Enable**.
3. Select **DDNS Type** as DynDNS.
4. Enter Server Address for DynDNS (i.e., members.dyndns.org).
5. Under Device Domain Name, enter the domain name obtained from the DynDNS Website.
6. Enter **User Name** and **Password** registered in the DynDNS Website.
7. Click **Apply**.

### 11.2 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly under **System** → **Network** → **TCP/IP** → **PPPoE** .

Contact your Internet service provider for details about PPPoE service.

### 11.3 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ and manual 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.

Universal Plug and Play (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.

#### Steps

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

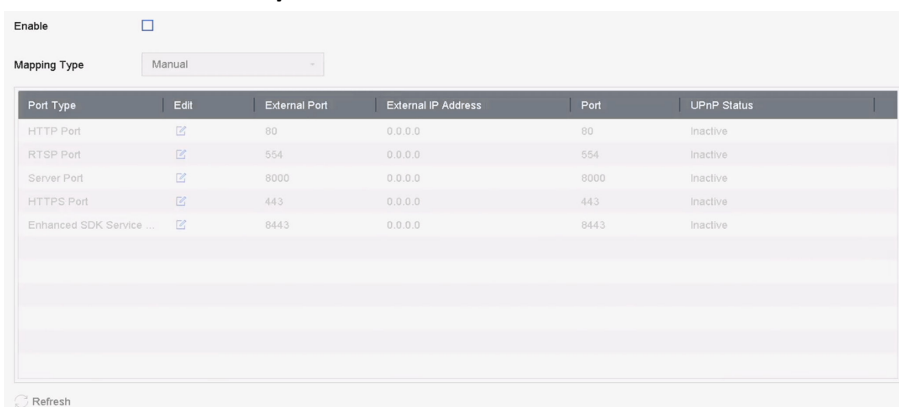


Figure 11-2 Port Mapping Setting

2. Check **Enable**.
3. Select **Mapping Type** as **Manual** or **Auto**.
  - Auto: If you select **Auto**, the port mapping items are read-only, and the external ports are set by the router automatically.
  - Manual: If you select **Manual**, you can edit the external port on your demand by clicking to activate **External Port Settings**.

#### Note

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. 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.

---

4. Enter the virtual server setting page of router; fill in the blank of **Internal Source Port** with the internal port value, the blank of **External Source Port** with the external port value, and other required contents.
- 

 **Note**

- Each item should be corresponding with the device port, including server port, http port, RTSP port and https port.
  - The virtual server setting interface below is for reference only, it may be different due to different router manufactures. Please contact the manufacture of router if you have any problems with setting virtual server.
- 

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
<input type="checkbox"/>	81	TCP	192.168.251.101	80	HTTP

Figure 11-3 Set Virtual Server Item

## 11.4 Configure SNMP

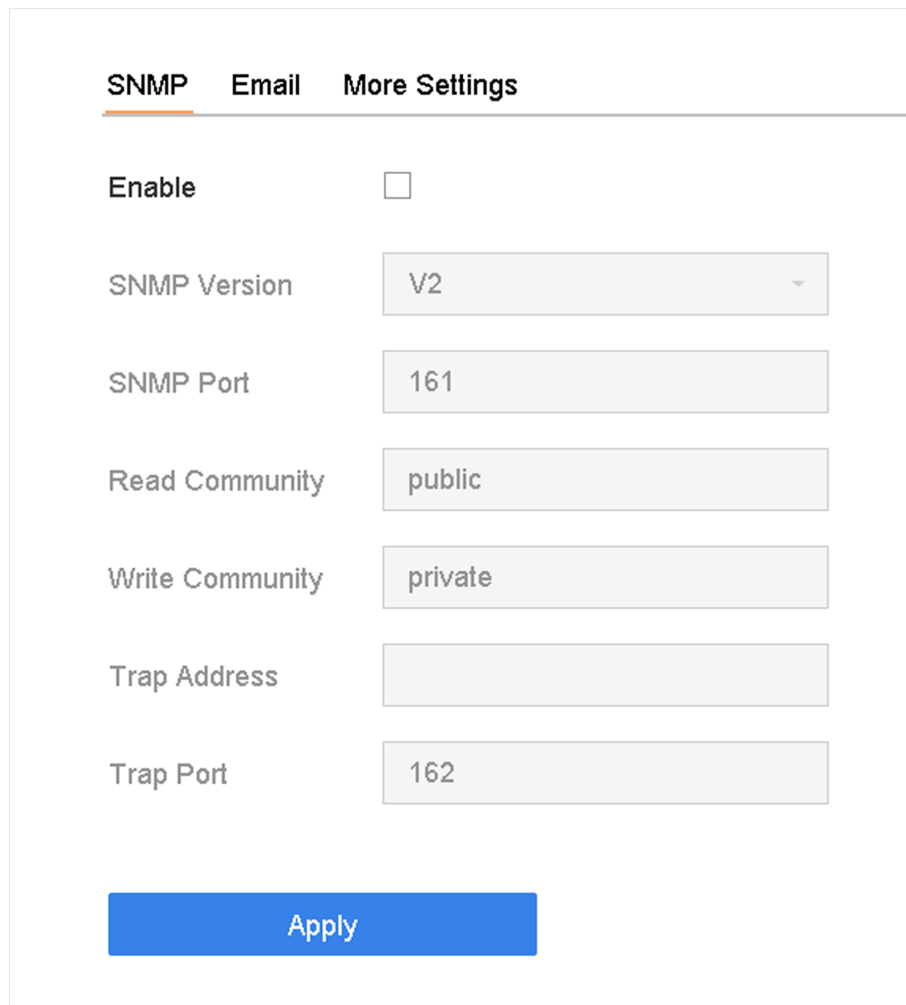
You can configure SNMP settings to get device status and parameter information.

### Before You Start

Download the SNMP software to receive device information via the SNMP port. By setting the trap address and port, the device is allowed to send alarm events and exception messages to the surveillance center.

### Steps

1. Go to **System** → **Network** → **Advanced** → **SNMP** .



The image shows a web interface for configuring SNMP settings. At the top, there are three tabs: 'SNMP' (which is selected and underlined), 'Email', and 'More Settings'. Below the tabs, there are several configuration options:

- Enable:** A checkbox that is currently unchecked.
- SNMP Version:** A dropdown menu set to 'V2'.
- SNMP Port:** A text input field containing '161'.
- Read Community:** A text input field containing 'public'.
- Write Community:** A text input field containing 'private'.
- Trap Address:** An empty text input field.
- Trap Port:** A text input field containing '162'.

At the bottom of the form is a blue button labeled 'Apply'.

**Figure 11-4 SNMP Settings**

2. Check **Enable**. A message will pop up to notify about a possible security risk. Click **Yes** to continue.
3. Configure the SNMP settings as needed.

**Trap Address**

SNMP host IP address.

**Trap Port**

Port of the SNMP host.

4. Click **Apply**.

## 11.5 Configure Email

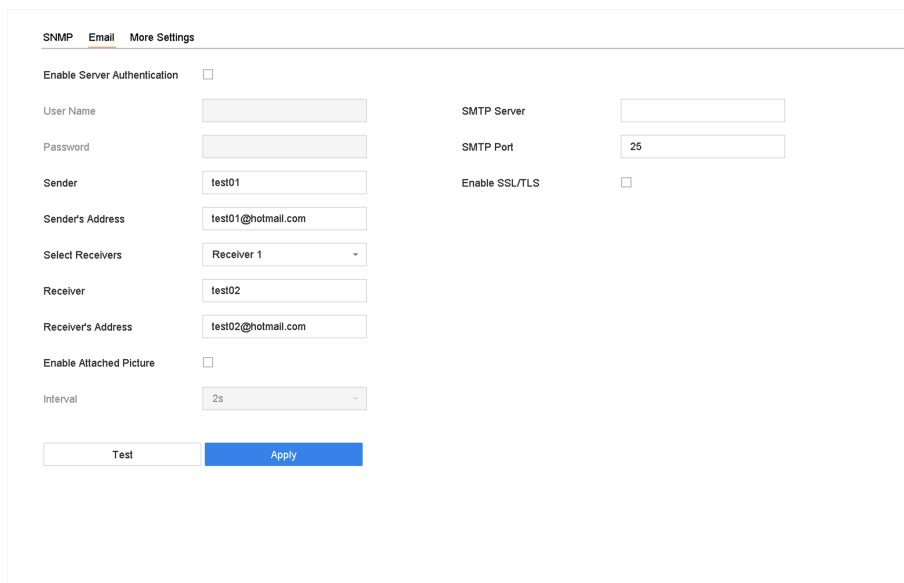
The system can be configured to send an e-mail notification to all designated users when a specified event occurs such as when an alarm or motion event is detected, or the administrator password is changed, etc.

### Before You Start

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

### Steps

1. Go to **System** → **Network** → **Advanced** → **Email** .



The screenshot shows the 'Email' configuration page with the following fields and options:

- Enable Server Authentication:**
- User Name:**
- Password:**
- SMTP Server:**
- SMTP Port:**
- Sender:**
- Enable SSL/TLS:**
- Sender's Address:**
- Select Receivers:**
- Receiver:**
- Receiver's Address:**
- Enable Attached Picture:**
- Interval:**

At the bottom, there are two buttons: 'Test' and 'Apply'.

Figure 11-5 Email Settings

2. Configure the email settings.

### Enable Server Authentication

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

### SMTP Server

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

### SMTP Port

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

### Enable SSL/TLS

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

### Sender

The sender's name.

### **Sender's Address**

The sender's address.

### **Select Receivers**

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

### **Receiver**

The receiver's name.

### **Receiver's Address**

The e-mail address of the user to be notified.

### **Enable Attached Picture**

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

**3.** Click **Apply**.

**4. Optional:** Click **Test** to send a test email.

## **11.6 Configure Port**

You can configure different types of ports to enable relevant functions.

### **Steps**

**1.** Go to **System → Network → Advanced → More Settings** .



Alarm Host IP	<input type="text"/>
Alarm Host Port	<input type="text" value="0"/>
Server Port	<input type="text" value="8000"/>
HTTP Port	<input type="text" value="80"/>
Multicast IP	<input type="text"/>
RTSP Port	<input type="text" value="554"/>
Enhanced SDK Ser...	<input type="text" value="8443"/>

**Figure 11-6 Port Settings**

2. configure port settings as needed.

### **Alarm Host IP/Port**

With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the client management system (CMS) software installed. The alarm host IP refers to the IP address of the remote PC on which the CMS software (e.g., iVMS-4200) is installed, and the alarm host port (7200 by default) must be the same as the alarm monitoring port configured in the software.

### **Server Port**

Server port (8000 by default) should be configured for remote client software access and its valid range is 2000 to 65535.

### **HTTP Port**

HTTP port (80 by default) should be configured for remote Web browser access.

### **Multicast IP**

Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through network. A multicast IP address 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.

### **RTSP Port**

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. The port is 554 by default.

### Enhanced SDK Service Port

The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission. The port is 8443 by default.

3. Click **Apply**.

## 11.7 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 **Maintenance** → **System Service** → **ONVIF**.
2. Check **Enable ONVIF** to enable the ONVIF access management.



### Note

ONVIF protocol is disabled by default.

---

3. Click **Add**.
4. Enter **User Name**, and **Password**



### Caution

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

---

5. Select **Level** as **Media User**, **Operator** or **Admin**.
6. Click **OK**.

## Chapter 12 User Management and Security

### 12.1 Manage User Accounts

The Administrator user name is admin and the password is set when you start the device for the first time. The Administrator has the permission to add and delete users and configure user parameters.

#### 12.1.1 Add a User

##### Steps

1. Go to **System → User** .
2. Click **Add** to enter the operation permission interface.
3. Input the admin password and click **OK**.
4. In the Add User interface, enter the information for a new user.



##### Caution

**Strong Password Recommended**—We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in the high security systems, resetting the password monthly or weekly can better protect your product.

---

##### User Level

Set the user level to Operator or Guest. Different user levels have different operating permission.

- **Operator:** An Operator user level has Two-way Audio permission in Remote Configuration and all operating permissions in Camera Configuration by default.
- **Guest:** The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

##### User's MAC Address

The MAC address of the remote PC that logs onto the device. If it is configured and enabled, it allows only the remote user with this MAC address to access the device.

5. Click **OK**.  
In the User Management interface, the added new user is displayed on the list.

## 12.1.2 Edit the Admin User

For the admin user account, you can modify your password and unlock pattern.

### Steps

1. Go to **System** → **User** .
2. Select the admin user from the list.
3. Click **Modify**.

The screenshot shows a dialog box titled "Edit User" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- User Name: admin
- Password: [masked with asterisks] Discard C...
- Confirm: [masked with asterisks]
- Note: Valid password range [8-16]. You can use...
- Password S...: [Progress indicator with three bars]
- User's MAC Ad...: 00 : 00 : 00 : 00 : 00 : 00
- Unlock Patt...:  Enable Unlock Pattern [gear icon]
- GUID File:  Export [question mark icon]
- Security Qu...: [gear icon]
- Reserved E...: [empty field] [question mark icon] Modify

At the bottom of the dialog are two buttons: "OK" (blue) and "Cancel" (grey).

**Figure 12-1 Edit User (Admin)**

4. Edit the admin user information as desired, including a new admin password (strong password is required) and MAC address.
5. Edit the unlock pattern for the admin user account.
  - 1) Check **Enable Unlock Pattern** to enable the use of an unlock pattern when logging in to the device.
  - 2) Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.
6. Check **Export** of **GUID File** to export the GUID file for the admin user account.

---

### **Note**

When the admin password is changed, export the new GUID to the connected USB flash drive in the Import/Export interface for the future password resetting.

---

7. Configure security question for password resetting.
8. Configure reserved email for password resetting.

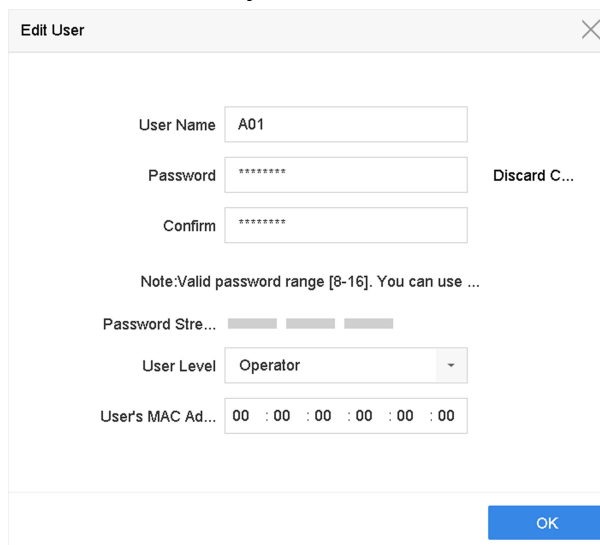
9. Click **OK** to save the settings.

## 12.1.3 Edit an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address.

### Steps

1. Go to **System → User**.
2. Select a user from the list and click **Modify**.



**Figure 12-2 Edit User (Operator/Guest)**

3. Edit the user information as desired, including the new password (strong password is required) and MAC address.
4. Click **OK**.

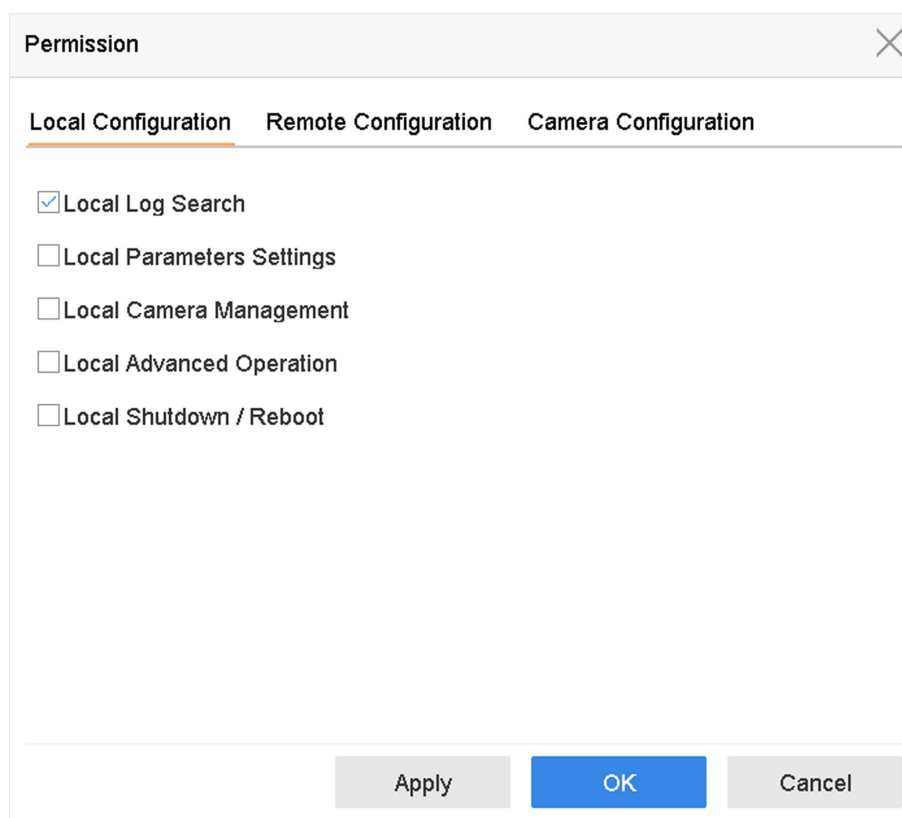
## 12.2 Manage User Permissions

### 12.2.1 Set User Permissions

For an added user, you can assign the different permissions, including local and remote operation of the device.

### Steps

1. Go to **System → User**.
2. Select a user from the list, and then click  to enter the permission settings interface.



**Figure 12-3 User Permission Settings Interface**

**3. Set the user's operating permissions for **Local Configuration**, **Remote Configuration**, and **Camera Configuration** for the user.**

1) Set Local Configuration

**Local Log Search**

Searching and viewing logs and system information of device.

**Local Parameters Settings**

Configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

**Local Camera Management**

Adding, deleting, and editing of IP cameras.

**Local Advanced Operation**

Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

**Local Shutdown Reboot**

Shutting down or rebooting the device.

2) Set Remote Configuration

**Remote Log Search**

Remotely viewing logs that are saved on the device.

### **Remote Parameters Settings**

Remotely configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

### **Remote Camera Management**

Remote adding, deleting, and editing of the IP cameras.

### **Remote Serial Port Control**

Configuring settings for RS-232 and RS-485 port settings.

### **Remote Video Output Control**

Sending remote button control signals.

### **Two-Way Audio**

Operating the two-way radio between the remote client and the device.

### **Remote Alarm Control**

Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.

### **Remote Advanced Operation**

Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

### **Remote Shutdown/Reboot**

Remotely shutting down or rebooting the device.

## 3) Set Camera Configuration

### **Remote Live View**

Remotely viewing live video of the selected camera(s).

### **Local Manual Operation**

Locally starting/stopping manual recording and alarm output of the selected camera(s).

### **Remote Manual Operation**

Remotely starting/stopping manual recording and alarm output of the selected camera(s).

### **Local Playback**

Locally playing back recorded files of the selected camera(s).

### **Remote Playback**

Remotely playing back recorded files of the selected camera(s).

### **Local PTZ Control**

Locally controlling PTZ movement of the selected camera(s).

### **Remote PTZ Control**

Remotely controlling PTZ movement of the selected camera(s).

## Local Video Export

Locally exporting recorded files of the selected camera(s).

## Local Live View

View live video of the selected camera(s) in local.

4. Click **OK** to save the settings.

## 12.2.2 Set Live View Permission on Lock Screen

The admin user can set live view permission for specific cameras in the screen lock status of device.

- The admin user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

### Steps

1. Go to **System → User**.
2. Click **Live View Permission on Lock Screen**.
3. Input admin password and click **Next**.

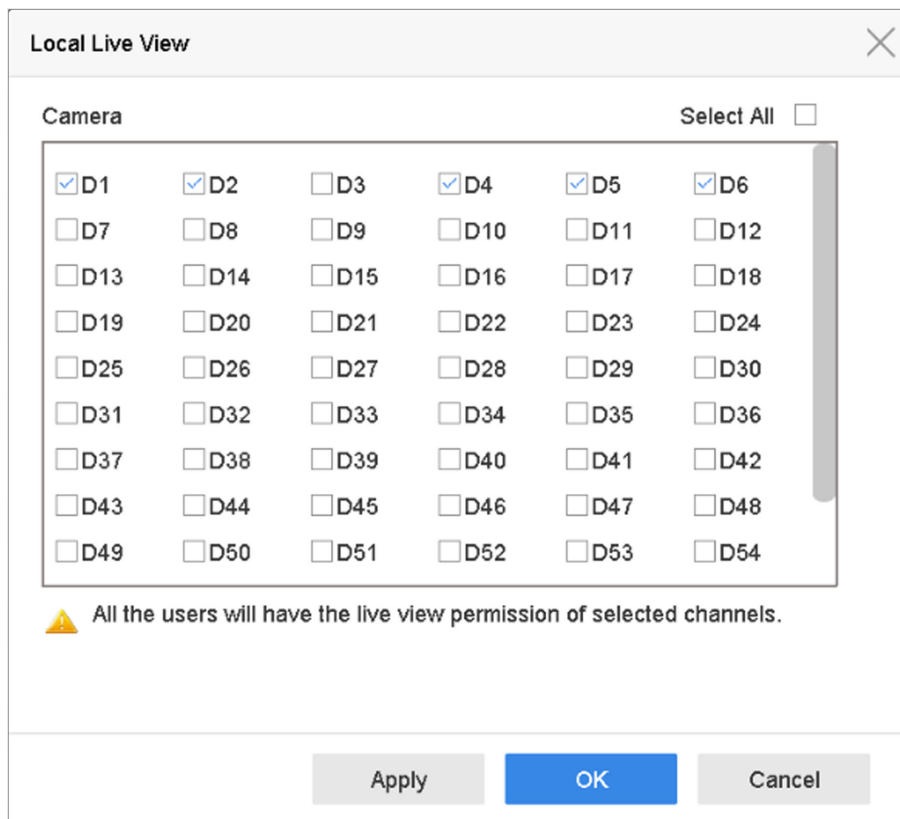


Figure 12-4 Set Live View Permissions on Lock Screen



4. Set the permissions. Select the camera (s) to allow live view when the current user account is in logout status.
5. Click **OK**.

## 12.3 Configure Password Security

### 12.3.1 Export GUID File

The GUID file can help you to reset password when you forget password. Please keep it properly.

#### Steps

1. Check **Export** and click **OK** to export GUID file when you are activating the device, or editing the admin user account.
2. Insert a USB flash drive to your device, and export the GUID file to the USB flash drive.

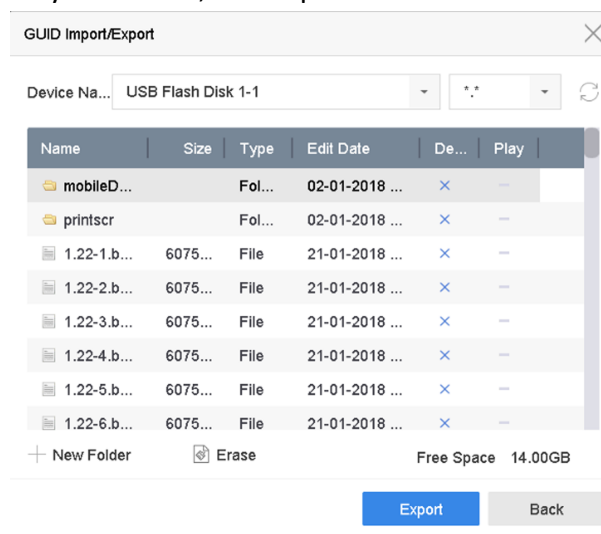


Figure 12-5 Export GUID File

3. Select a Device.
4. Select a directory on the device.
5. Click **Export**.

### 12.3.2 Configure Security Questions

The security questions can help you to reset password when you forget your password, or encounter security issues.

#### Steps

1. Click **Security Question Configuration** when you are activating the device, or editing the admin user account.
2. Select three security questions from the drop-down list and input the answers.

Security Question Configuration

Question 1 10. Your favorite book. ▾

Answer 1 A

Question 2 11. Your favorite color. ▾

Answer 2 Blue

Question 3 13. Your favorite flower. ▾

Answer 3 Rose

OK Cancel

**Figure 12-6 Configure Security Questions**

3. Click **OK**.

## 12.4 Reset Password

When you forget the admin password, you can reset the password by importing the GUID file, answering security questions, or entering verification code from your reserved email.

### 12.4.1 Reset Password by GUID

#### Before You Start

The GUID file must be exported and saved in a USB flash drive after you have activated the device or edited the admin user account.

#### Steps

1. On the user login interface, click **Forgot Password**.
2. On **Password Reset Type**, Select **Verify by GUID**.

---

#### **Note**

Please insert the USB flash drive stored with the GUID file to the device before resetting password.

---

3. Select the GUID file from the USB flash drive and click **Import** to import the file to the device.

---

 **Note**

If you have imported the wrong GUID file for 7 times, you will be not allowed to reset the password for 30 minutes.

---

4. After the GUID file is successfully imported, enter the reset password interface to set the new admin password.
  5. Click **OK** to set the new password. You can export the new GUID file to the USB flash drive for future password resetting.
- 

 **Note**

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter **User** → **User Management** to edit the admin user and export the GUID file.

---

### 12.4.2 Reset Password by Security Questions

#### Before You Start

You have configured the security questions when you activate the device or edit the admin user account. (Refer to Chapter 17.3.2 Configure Security Questions).

#### Steps

1. On the user login interface, click **Forgot Password**.
2. Select the **password resetting type** as **Verify by Security Question**.
3. Input the correct answers of the three security questions.
4. Click **OK**.
5. Create the new admin password on the Reset Password interface.

## Chapter 13 System Management

### 13.1 Configure Device

#### Steps

1. Go to **System** → **General** .
2. Configure the following settings.

#### Language

The default language used is English.

#### Output Standard

Set the output standard to NTSC or PAL, which must be the same as the video input standard.

#### Resolution

Configure video output resolution.

#### Device Name

Edit device name.

#### Device No.

Edit the device serial number. The Device No. can be set in the range of 1 to 255, and the default No. is 255. The number is used for the remote and keyboard control.

#### Auto Logout

Set the timeout time for menu inactivity. E.g., when the timeout time is set to 5 minutes, then the system will exit from the current operation menu to Live View screen after 5 minutes of menu inactivity.

#### Mouse Pointer Speed

Set the speed of the mouse pointer; 4 levels are configurable.

#### Enable Wizard

Enable/disable the Wizard when the device starts up.

#### Enable Password

Enable/disable the use of the login password.

3. Click **Apply** to save the settings.

### 13.2 Configure Time

## 13.2.1 Manual Time Synchronization

### Steps

1. Go to **System → General** .
2. Configure the date and time.
3. Click **Apply** to save the settings.

## 13.2.2 NTP Synchronization

Connection to a network time protocol (NTP) server can be configured on your device to ensure the system's date and time accuracy.

### Steps

1. Go to **System → Network → TCP/IP → NTP** .
2. Check **Enable**.
3. Configure NTP settings as need.

#### Interval (min)

Time interval between two time synchronization with NTP server

#### NTP Server

IP address of the NTP server

#### NTP Port

Port of the NTP server

4. Click **Apply**

## 13.2.3 DST Synchronization

DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

### Steps

1. Go to **System → General** .
2. Check **Enable DST**.
3. Set **DST mode** as **Auto** or **Manual**.

#### Auto

Automatically enable the default DST period according to the local DST rules.

#### Manual

Manually set the start time and end time of the DST period, and the DST bias.

4. Set the DST Bias. Set the time (30/60/90/120 minutes) offset from the standard time.
5. Click **Apply** to save the settings.

## 13.3 Network Detection

### 13.3.1 Network Traffic Monitoring

Network traffic monitoring is the process of reviewing, analyzing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security.

#### Steps

1. Go to **Maintenance → Network → Traffic**.
2. You can view the real-time network traffic status, including MTU (Maximum Transmission Unit), and network throughput.

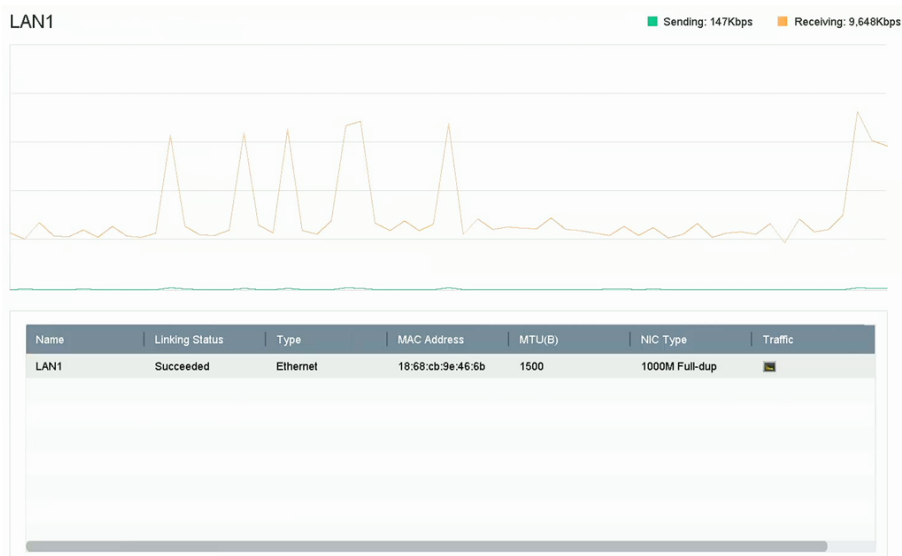


Figure 13-1 Network Traffic

### 13.3.2 Test Network Delay and Packet Loss

Network delay is caused by slow response of the device when oversized data information is not limited during transmission under certain network protocol, e.g. TCP/IP. Packet loss test is for testing network packet loss rate that is the ratio of lost data packet and total number of transmitted data packet.

#### Steps

1. Go to **Maintenance → Network → Network Detection**.
2. Select a network card in **Select NIC**.

3. Enter the destination IP address in **Destination Address**.
4. Click **Test**.



Network Delay, Packet Loss Test

Select NIC: LAN1

Destination Address: 10.6.114.33

Test

**Figure 13-2 Test Network Delay and Packet Loss**

### 13.3.3 Export Network Packet

After the recorder accessing network, you can use USB flash drive to export network packet.

#### Before You Start

Prepare a USB flash drive to export network packet.

#### Steps

1. Insert the USB flash drive.
2. Go to **Maintenance** → **Network** → **Network Detection** .
3. Select network card in **Select NIC**.
4. Select the USB flash drive in **Device Name**. You can click **Refresh** if the connected local backup device cannot be displayed.



Network Packet Export

Device Name: USB Flash Disk 1-1

Refresh

Status

LAN1	10.6.114.17	3.132Kbps	Export
------	-------------	-----------	--------

**Figure 13-3 Export Network Packet**

5. **Optional:** Click **Status** to view the network status.
6. Click **Export**.



#### Note

It will export 1 MB data each time as default.

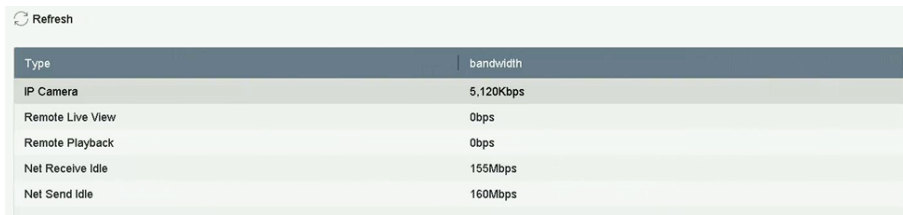
---

### 13.3.4 Network Resource Statistics

The remote access, including web browser and client software, will consume output bandwidth. You can view the real-time bandwidth statistics.

#### Steps

1. Go to **Maintenance** → **Network** → **Network Stat** .



The screenshot shows a table with a 'Refresh' button at the top left. The table has two columns: 'Type' and 'bandwidth'. The data rows are as follows:

Type	bandwidth
IP Camera	5,120Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Receive Idle	155Mbps
Net Send Idle	160Mbps

**Figure 13-4 Network Resource Statistics**

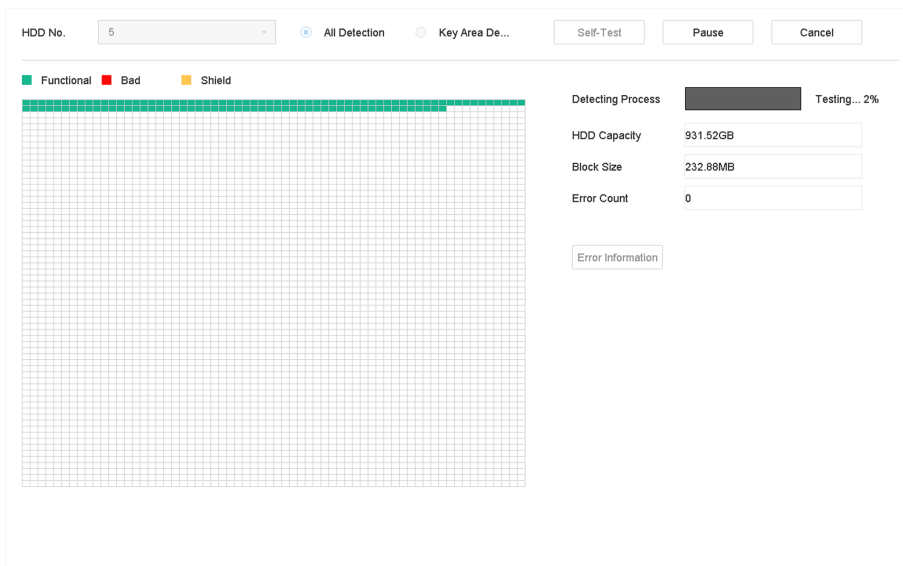
2. View the bandwidth statistics, including **IP Camera**, **Remote Live View**, **Remote Play**, **Net Total Idle**, etc.
3. **Optional:** Click **Refresh** to obtain the latest data.

## 13.4 Storage Device Maintenance

### 13.4.1 Bad Sector Detection

#### Steps

1. Go to **Maintenance** → **HDD Operation** → **Bad Sector Detection** .
2. Select the HDD No. you want to configure in the dropdown list.
3. Select **All Detection** or **Key Area Detection** as the detection type.
4. Click **Self-Test** to start the detection.



**Figure 13-5 Bad Sector Detection**



 **Note**

- You can pause/resume or cancel the detection.
  - After testing has been completed, you can click **Error information** to see the detailed damage information.
- 

## 13.4.2 S.M.A.R.T. Detection

HDD detection functions such as the adopting of the S.M.A.R.T. and the Bad Sector Detection techniques. 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.

### Steps

1. Go to **Maintenance → HDD Operation → S.M.A.R.T.**
2. Select the HDD to view its S.M.A.R.T. information list.
3. Set **Self-Test Type**.
4. Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

Continue to use this disk when self-evaluation is failed.

HDD No.

Self-Test Type

Temperature...  Self-Evaluation

Working Time...  All-Evaluation

S.M.A.R.T Infor

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error R...	OK	2f	51	200	200	8
0x3	Spin Up Time	OK	27	21	113	107	7316
0x4	Start/Stop Count	OK	32	0	98	98	2657
0x5	Reallocated Sector...	OK	33	140	200	200	0
0x7	Seek Error Rate	OK	2e	0	200	200	0
0x9	Power-on Hours C...	OK	32	0	88	88	9369
0xa	Spin Up Retry Count	OK	32	0	100	100	0
0xb	Calibration Retry C...	OK	32	0	100	100	0

**Figure 13-6 S.M.A.R.T. Settings Interface**

 **Note**

To use the HDD even when the S.M.A.R.T. checking has failed, check **Continue to use the disk when self-evaluation is failed**.

---

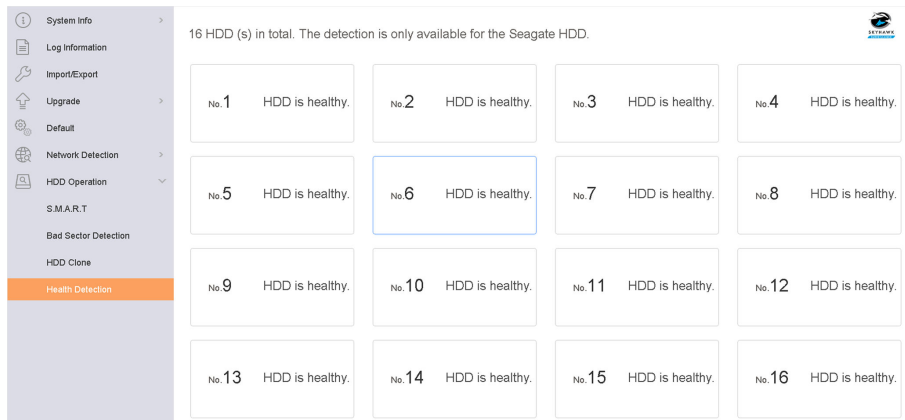
The related information of the S.M.A.R.T. is shown, and you can check the HDD status.

## 13.4.3 HDD Health 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.

### Steps

1. Go to **Maintenance → HDD Operation → Health Detection** .



**Figure 13-7 Health Detection**

2. Click a HDD to view details.

## 13.4.4 Configure Disk Clone

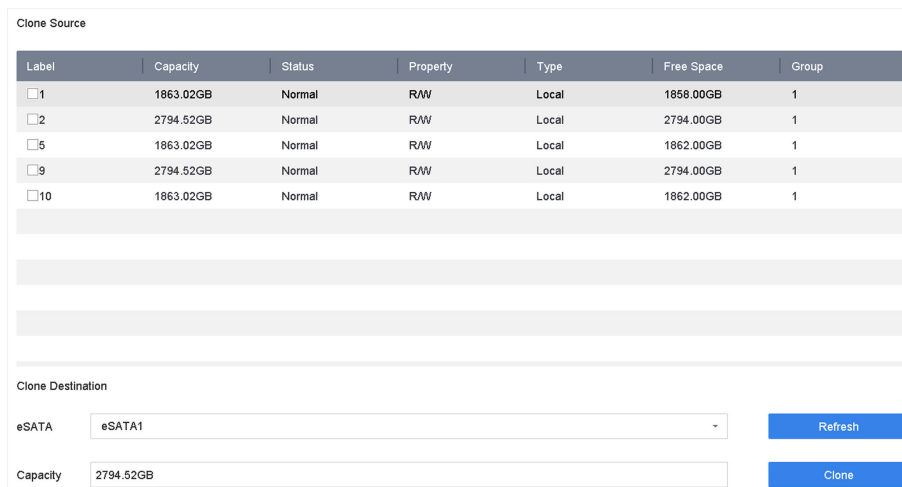
Select the HDDs to clone to the eSATA HDD.

### Before You Start

Connect an eSATA disk to the device.

### Steps

1. Go to **Maintenance → HDD Operation → HDD Clone** .



**Figure 13-8 HDD Clone**

2. Check the HDD to clone. The capacity of the selected HDD must match the capacity of the clone destination.
3. Click **Clone**.
4. Click **Yes** on the pop up message box to create the clone.

## 13.4.5 Repair Database

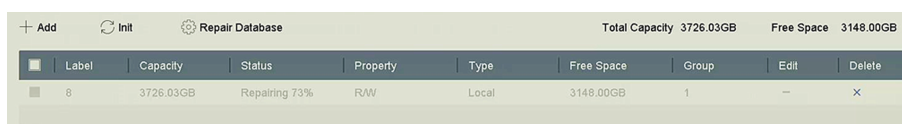
Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

### Steps

1. Go to **Storage → Storage Device**.
2. Select the drive.
3. Click **Repair Database**.
4. Click **Yes**.

### 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.
- You can see the repairing progress at **Status**.



**Figure 13-9 Repair Database**

## 13.5 Upgrade Device

Your device firmware can be upgraded with a local backup device or remote FTP server.

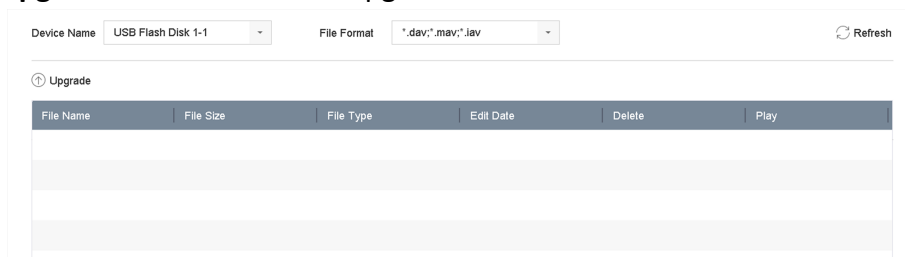
### 13.5.1 Upgrade by Local Backup Device

#### Before You Start

Connect your device to a local storage device that contains the firmware update file.

#### Steps

1. Go to **Maintenance** → **Upgrade** .
2. Click **Local Upgrade** to enter the local upgrade interface.



**Figure 13-10 Local Upgrade**

3. Select the firmware update file from the storage device.
4. Click **Upgrade** to start upgrading.

After the upgrade is completed, the device will reboot automatically to activate the new firmware.

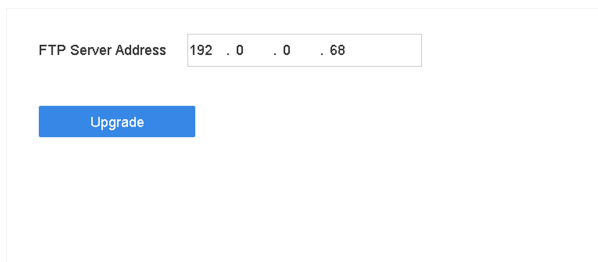
### 13.5.2 Upgrade by FTP

#### Before You Start

Ensure the network connection of the PC (running FTP server) and the device are valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

#### Steps

1. Go to **Maintenance** → **Upgrade** .
2. Click **FTP** to enter the local upgrade interface.



**Figure 13-11 FTP Upgrade**

3. Enter **FTP Server Address**.
4. Click **Upgrade** to start upgrading.
5. After the upgrading is complete, reboot the device to activate the new firmware.

### 13.5.3 Upgrade by Web Browser

You can upgrade the device by web browser

After logging in to the device via web browser, go to **Configuration → System → Maintenance → Upgrade** . Click **Browse** to upload the firmware, and upgrade the device.

### 13.6 Import/Export Device Configuration Files

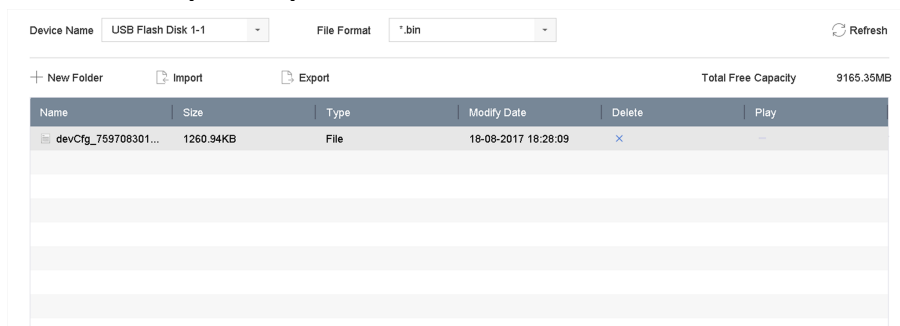
The device configuration files can be exported to a local device for backup; and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

#### Before You Start

Connect a storage device to your device. To import the configuration file, the storage device must contain the file.

#### Steps

1. Go to **Maintenance → Import/Export** .



**Figure 13-12 Import/Export Configuration File**

2. Export or import the device configuration files.
  - Click **Export** to export configuration files to the selected local backup device.

- To import a configuration file, select the file from the selected backup device and click **Import**.



## Note

After having finished importing configuration files, the device will reboot automatically.

## 13.7 Search & Export Log Files

The device operation, alarm, exception, and information can be stored in log files, which can be viewed and exported at any time.

### Steps

1. Go to **Maintenance → Log Information**.

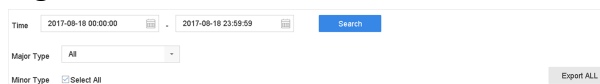


Figure 13-13 Log Search Interface

2. Set the log search conditions, including the time, major type and minor type.
3. Click **Search** to start searching the log files.
4. The matched log files will be displayed on the list, as shown below.

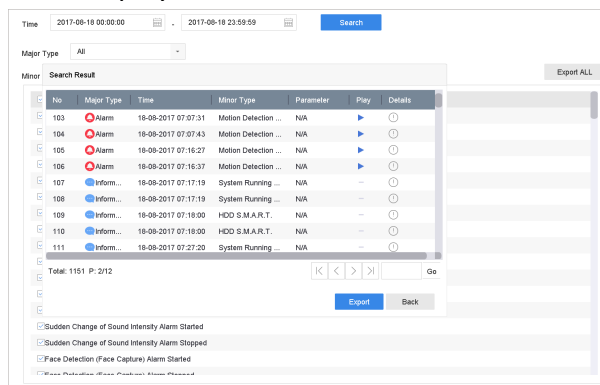


Figure 13-14 Log Search Results



## Note

Up to 2,000 log files can be displayed each time.

### 5. Related Operation:



Click or double-click it to view detailed information.



Click it to view the related video file.

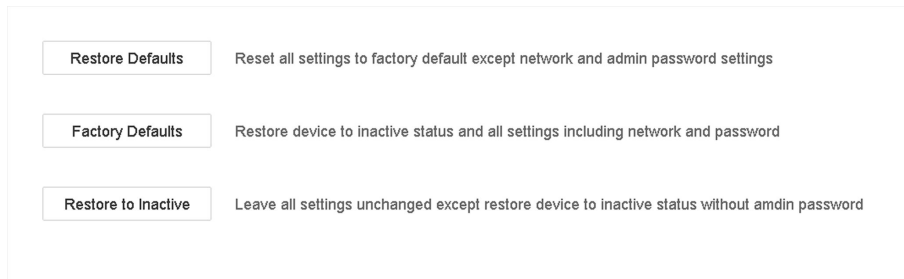
### Export/Export ALL

Click it to export all the system logs to the storage device.

## 13.8 Restore Default Settings

### Steps

1. Go to **Maintenance → Default** .



**Figure 13-15 Restore Default Settings**

2. Select the restore type from the following three options.

#### Restore Defaults

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 recorder to inactive status.



#### Note

The recorder will reboot automatically after restoring to the default settings.

---

## 13.9 Security Management

### 13.9.1 RTSP Authentication

You can specifically secure the stream data of live view by setting the RTSP authentication.

#### Steps

1. Go to **System → System Service → System Service** .



**Figure 13-16 RTSP Authentication**

2. Select **RTSP Authentication Type**.

---

## Note

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

---

3. Click **Apply**.
4. Restart the device to take effect the settings.

## 13.9.2 ISAPI Service

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.). The device is as a server, the system can find and connect the device.

### Steps

1. Go to **System → System Service → System Service** .
2. Check **Enable ISAPI**.
3. Click **Apply**.
4. Restart the device to take effect the settings.

## 13.9.3 HTTP Authentication

If you need to enable the HTTP service, you can set HTTP authentication to enhance access security.

### Steps

1. Go to **Maintenance → System Service → System Service** .



The screenshot shows two settings: 'Enable HTTP' with a checked checkbox, and 'HTTP Authentication Type' with a dropdown menu set to 'digest'.

**Figure 13-17 HTTP Authentication**

2. Check **Enable HTTP**.
3. Select **HTTP Authentication Type**.

---

## Note

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

---

4. Click **Apply** to save the settings.
5. Restart the device to take effect the settings.



## Chapter 14 Appendix

### 14.1 Glossary

#### Dual-Stream

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

#### DVR

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

#### HDD

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

#### DHCP

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

#### HTTP

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

#### PPPoE

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

#### DDNS

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

#### Hybrid DVR

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

#### NTP

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

### **NTSC**

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

### **NVR**

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

### **PAL**

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

### **PTZ**

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

### **USB**

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

## **14.2 Communication Matrix**

Please scan the QR code below to view the communication matrix document.



**Figure 14-1 Communication Matrix**

## **14.3 Device Command**

Please scan the QR code below to view the device command document.



Figure 14-2 Device Command

## 14.4 Frequently Asked Questions

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

#### Reason

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

#### Solution

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

---

#### Note

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

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

### 14.4.2 Why is the video recorder notifying the stream type is not supported?

#### Reason

The camera encoding format mismatches with the video recorder.

### **Solution**

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

### **14.4.3 Why is the video recorder notifying risky password after a network camera is added?**

#### **Reason**

The camera password is too weak.

#### **Solution**

Change the camera password.



#### **Warning**

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

---

### **14.4.4 How to improve the playback image quality?**

#### **Reason**

Recording parameter settings are inappropriate.

#### **Solution**

Go to **Camera → Video Parameters** . Increase resolution and max. bitrate, and try again.

### **14.4.5 How to confirm the video recorder is using H.265 to record video?**

#### **Solution**

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

### **14.4.6 Why is the timeline at playback not constant?**

### Reason

1. When the video recorder is using event recording, it only records video when event occurs. Hence the video may not be continuous.
2. Exception occurs, such as the device offline, HDD error, record exception, network camera offline, etc.

### Solution


1. Ensure the recording type is continuous recording.
2. Go to **Maintenance** → **Log Information** . Search the log file during the video time period. See if there are unexpected events, such as HDD error, record exception, etc.

### 14.4.7 Why is the video recorder notifying the network is unreachable when a network camera is being added?

#### Reason

1. The IP address or port of network camera is incorrect.
2. The network between video recorder and camera is disconnected.

#### Solution

1. Go to **Camera** → **Camera** → **IP Camera** . Click  of the selected camera, and edit its IP address and port. Ensure the video recorder and camera is using the same port.
2. Go to **Maintenance** → **Network** → **Detection** . Enter the IP address of network camera in **Destination Address**, and click **Test** to see if the network is reachable.

### 14.4.8 Why is the IP address of network camera being changed automatically?

#### Reason

When network camera and video recorder are using the same switch but in different subnets, the video recorder will change the IP address of network camera to the same subnet as itself.

#### Solution

When adding camera, click **Custom Add** to add camera.

### 14.4.9 Why is the video recorder notifying IP conflict?

#### Reason

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

### **Solution**

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

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

#### **Reason**

HDD read/write exception.

#### **Solution**

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

### **14.4.11 Why does my video recorder make a beeping sound after booting?**

#### **Reason**

1. The front panel is not fastened (for the device which its front panel is removable).
2. HDD error, or do not have HDD.

#### **Solution**

1. If it makes continuous beeps, and your device's front panel is removable, ensure the front panel is fastened.
2. If it makes non-continuous beeps (3 long, 2 short), take HDD error as an example, check if the device has installed HDD. If not, you can go to **System → Event → Normal Event → Exception**, and uncheck **Event Hint Configuration** to disable HDD error event hint.  
Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.  
Check if the HDD is broken. You can change it, and try again.

### **14.4.12 Why is there no recorded video after the motion detection is set?**

#### **Reason**

1. The recording schedule is incorrect.
2. The motion detection event setting is incorrect.
3. HDD exception.

### **Solution**

1. The recording schedule is setup correctly by following the steps listed in Configuring Record/Capture Schedule.
2. The motion detection area is configured correctly. The channels are being triggered for motion detection (See Configuring Motion Detection).
3. Check if the device has installed HDD.  
Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.  
Check if the HDD is broken. You can change it, and try again.

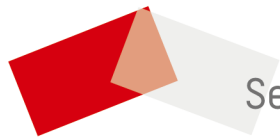
### **14.4.13 Why is the video sound quality not good?**

#### **Reason**

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

#### **Solution**

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



See Far, Go Further