



DS-7608NXI-I2/8P/4S
DS-7616NXI-I2/16P/4S

Network Video Recorder

User Manual

Copyright © 2018-2019 Hikvision USA Inc. and Hikvision Canada Inc.

Hikvision USA Inc., 18639 Railroad St., City of Industry, CA 91748, USA

Hikvision Canada, 4848 rue Levy, Saint Laurent, Quebec, Canada, H4R 2P1

Telephone: +1-909-895-0400 • Toll Free in USA: +1-866-200-6690 • E-Mail: sales.usa@hikvision.com •

www.hikvision.com

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

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 in the company website (<http://overseas.hikvision.com/en/>).

Please use this user manual under the guidance of professionals.

Manual Illustrations and Features

Graphics (screen shots, product pictures, etc.) in this document are for illustrative purposes only. Your actual product may differ in appearance. Your product might not support all features discussed in this document.

Trademarks Acknowledgement

HIKVISION and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS," WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER 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 when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



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, the 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: 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: www.recyclethis.info

Industry Canada ICES-003 Compliance

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

Hikvision North America Privacy Policy

Last Updated: December 2018

Hikvision USA Inc. and Hikvision Canada Inc. and its affiliates (collectively "HIKVISION") provide the following services for use in conjunction with various HIKVISION Internet-connected products ("Products"): a HIKVISION user Website and user accounts that may be accessed at us.hikvision.com, ca.hikvision.com, <https://distributors-us.hikvision.com/>, <https://distributors-us.hikvision.com/guestLogin.htm>, <https://ezviz-rma.hikvision.com/>, <https://order-na.hikvision.com> and all associated sites connected with us.hikvision.com (the "Website"); and any services available on the Website, Web Apps and Mobile Apps ("Available Services"). The term "HIKVISION Services" means the Website and Available Services.

This Privacy Policy explains how HIKVISION handles the collection, storage, and disclosure of information, including personal information, regarding our HIKVISION Services. It also applies to any information we collect from the operation and use of Products we sell while connected to the HIKVISION Services (the "Products"), and any other HIKVISION Service that links to this Privacy Policy.

We may modify this Privacy Policy at any time, provided certain provisions of this Privacy Policy prove to be incomplete or outdated and further provided that these changes are reasonable for you, taking into account your interests. If we make material changes to this Privacy Policy, we will notify you by the e-mail address specified in your account or by means of notice on our Websites.

You can determine when this Privacy Policy was last revised by referring to the date it was "Last Updated" above.

What Information We Collect

In order to provide HIKVISION services to you, we will ask you to provide personal information that is necessary to provide those services to you. If you do not provide your personal information, we may not be able to provide you with our products or services.

"Personal information" shall have the same meaning as "personal data" and shall include any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. Examples of personal information include your name, telephone number, e-mail address, and physical address.

Personal information also includes information that alone cannot directly identify you, but with other information we have access to can identify you such as product serial numbers, log data that automatically records information about your visit such as your browser type, domains, page views, the URL of the page that referred you, the URL of the page you next visit, your IP address, and page navigation, unique device ID collected from Products and your mobile devices, data from cookies, pixel tags, and Web beacons, video content files that do not contain personal visual identity information, the country and time zone of the connected Product, geo-location, mobile phone carrier identification, and device software platform and firmware information.

How We Collect and Use Your Information

Here are some examples of the personal information we may collect and how we may use it:

- When you create your account to use HIKVISION Services ("Account"), we will collect information including your name, phone number, and e-mail and physical address. In addition, when you install and activate Products, we will collect certain basic information via our HIKVISION Services such as your product name, the product's verification code, and serial number, which are unique to the Product connected to the HIKVISION Services and associated with your Account.

- When you respond to our e-mails, contact our customer service, or use other customer support tools, we collect your information to provide you with support, verify your identity with your Account profile information, and confirm your Product.

We may also use the information we collect for the following purpose:

- send you reminders, technical notices, updates, alerts, support and administrative messages, service bulletins, and requested information; and
- pursuant to our legitimate business interests:
 - operate, maintain, improve, and develop our HIKVISION Services and Products;
 - personalize your experience with our HIKVISION Services and Products;
 - increase the safety of our HIKVISION Services and Products – for example, for user authentication, security protection, fraud detection, filing, and backups;
 - perform analytics and conduct customer research;
 - communicate and provide to existing customers additional information that may be of interest to you about our products and services;
 - manage our everyday business needs such as auditing, administration of our HIKVISION Services, forum management, fulfillment, analytics, fraud prevention, and enforcement of our corporate reporting obligations and Terms of Service;
 - enhance other information we have about you to help us better understand you and determine your interests; and
 - in the context of a corporate transaction (e.g., corporate restructuring, sale or assignment of assets, merger) and to protect our rights or property, to enforce our Terms of Service and legal notices and for the establishment, exercise, and defense of legal claims;

with your express consent to

- send you electronic communications in order to inform you about new products and services, unless you choose to unsubscribe;
- use certain non-essential cookies to better understand user behavior, in order to optimize user experience, perfect function design, and offers for products and services from us or to provide better services;
- meet a legal obligation, a court order or other binding decision(s); and accomplish a purpose unrelated to those described in this Privacy Policy by first notifying you and, where required, offering you a choice as to whether or not we may use your Personal Information in this different manner.

Cookies and Other Technologies

We also use cookies, Web beacons, pixel tags, and other technologies to keep records, store your preferences, improve our advertising, and collect information such as log data and device data. This allows us to better understand how you use our HIKVISION Services and Products, diagnose and troubleshoot any problems you have, and otherwise administer and improve our HIKVISION Services and Products. For more information about cookies, please refer to our **Use of Cookies** (<https://order-na.hikvision.com/helpCenter/useOfCookies>).

How We Share Your Information

HIKVISION may disclose personal information to cloud service provider, network service provider, and other service providers on the basis of non-disclosure agreements.

The following are the limited situations where we may share personal information:

- We share your personal information with HIKVISION affiliates, who are required to use that information in accordance with the purposes described in this Privacy Policy.
- We use service providers, vendors, technicians, and other third-parties to help us process, store, and protect some of your data and otherwise help us administer our Products and HIKVISION Services effectively, provide a better user experience, process your purchases, and increase the quality of our Products and HIKVISION Services. These third-parties are forbidden from using your personal information for non-HIKVISION purposes and are required to protect your information in accordance with this Privacy Policy and applicable laws.
- We may provide information to third-parties if we believe in good faith that we are required by mandatory law to do so. For example, to comply with legal orders and government requests; response to a subpoena, or similar legal process, including to law enforcement agencies, regulators, and courts; to protect the interests of our customers and users of the HIKVISION Service; to respond to claims that any content posted or displayed using the HIKVISION Service violates the rights of third parties; in an emergency protect the health and safety of users of the HIKVISION Service or the general public; or to enforce compliance with our Terms of Service.
- If HIKVISION and/or all or part of our assets are ever sold or transferred, your personal information may be among the items sold or transferred. Under such circumstance, we will notify you by the e-mail address specified in your account or by means of notice on us.hikvision.com and associated Websites of (i) the identity and contact information of the purchaser or transferee, (ii) your right to revoke your consent to the provision of personal information, and (iii) the means by which you may revoke such consent.
- We share information to protect our own legitimate business interests when we believe in good faith that we are required or permitted by law to do so. For example, we may share your personal information as needed to support auditing, compliance, and corporate governance functions; to combat fraud or criminal activity; to protect our rights or those of our affiliates and users; or as part of legal proceedings affecting HIKVISION.

We may also disclose non-personal information (for example, aggregated or anonymized data) publicly or with third-parties, provided those data have been rendered anonymous in such a way that the data subject is no longer identifiable. For example, we may share non-personal information:

- for the same reasons we might share Personal information;
- to better understand how our customers interact with our HIKVISION Services and Products, in order to optimize your experience, improve our products, or provide better services;
- for our own research and data analytics; or
- to our vendors for their own analysis and research.

Securing Your Personal Information

HIKVISION has implemented commercially reasonable administrative, technical, and physical security controls that are designed to safeguard personal information. We also conduct periodic reviews and assessments of the effectiveness of our security controls.

Notwithstanding the above, no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, HIKVISION cannot guarantee that your personal information is under absolute security with the existing security technology. If you have any questions about the security of our HIKVISION Services, you can contact us at the contact information below in **Contact Us**.

Accessing, Correcting, and Retention of Your Personal Information

HIKVISION generally stores your personal information on HIKVISION's servers, which is established upon Amazon Servers, until you delete or edit it, or for as long as you remain a HIKVISION customer in order to provide you with the most relevant offers.

Keeping your personal information current helps ensure that we provide you with the most relevant offers. You can access, update, or delete your personal information via your Account profile. We are ready to assist you in managing your subscriptions, deactivating your account, and removing your active profile and data. Your personal information might not be immediately deleted, as we are required to retain records relating to previous purchases through our HIKVISION Services for financial reporting and compliance reasons pursuant to applicable laws. In addition, because of the way we maintain certain services, after you delete certain information, we may temporarily retain backup copies of such information before it is permanently deleted.

We will retain your personal information for the period necessary to fulfill the purpose outlined in this Privacy Policy unless a longer retention period is required or permitted by applicable law.

If you are located in the European Union, subject to limitations in applicable law, you have certain rights in respect to your personal information such as a right of access, rectification, restriction, opposition, and portability. In order to exercise your rights please contact us at the contact information below in **Contact Us**. You also have the right to withdraw your consent at all times, free of charge. You can do this by opting out from direct marketing and by rejecting the use of cookies through your browser settings. If you have concerns about how we handle your personal information, you have the right to lodge a complaint with the data protection authority in your country of residence.

Social Community Features and Social Networks

Social Community Features

Our HIKVISION Services may allow you to publicly post or share information, communicate with others, or otherwise make information accessible to others. Prior to doing so, please read our Terms of Service carefully. All the information you post, share, or communicate may be accessible to anyone with Internet access, and any personal information you include may be read, collected, and used by others.

Social Networks

You have the option to link social networks such as Facebook to your Account. You will be able to post HIKVISION activity to your social network. By proceeding through any of the above steps, you grant HIKVISION permission to access elements of your social network profile information that you have made available to be shared and to use it in accordance with the social network's terms of use and this Privacy Policy.

Links to Other Websites

We may permit others to link to the HIKVISION services or to post a link to their Website. We do not endorse these Websites and are not responsible for other Websites or their privacy practices. Please read their privacy policies before submitting information.

Your Choices

We think that you benefit from a more personalized experience when we know more about you and your preferences. However, you can limit the information you provide to HIKVISION as well as the communications you receive from HIKVISION through your Account preferences.

Commercial E-mails

You will receive commercial e-mails from us only if you have granted prior express consent or if sending those e-mails is otherwise permitted, in accordance with applicable laws.

You may choose not to receive commercial e-mails from us by following the instructions contained in any of the commercial e-mails we send or by logging into your Account and adjusting your e-mail preferences. Please note that even if you unsubscribe from commercial e-mail messages, we may still e-mail you non-commercial e-mails related to your Account on the HIKVISION Services.

Device Data

You may manage how your mobile device and mobile browser share certain device data with HIKVISION by adjusting the privacy and security settings on your mobile device. Please refer to instructions provided by your mobile service provider or the manufacturer of your device to learn how to adjust your settings.

Children's Privacy

HIKVISION does not intend that any portion of its HIKVISION Services will be accessed or used by children under the age of 18, or equivalent minimum age in the relevant jurisdiction and such use is prohibited. Our HIKVISION Services are designed and intended for adults. By using the HIKVISION Services, you represent that you are at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction and understand that you must be at least 18 years old, or above the equivalent minimum age in the relevant jurisdiction in order to create an account and purchase the goods or services advertised through our HIKVISION Services. If we obtain actual knowledge that an account is associated with a registered user who is under the age of 18 years old, or equivalent minimum age in the relevant jurisdiction, we will promptly delete information associated with that account. If you are a parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction and believe he or she has disclosed personal information to us please contact us at the contact information below in **Contact Us**. A parent or guardian of a child under the age of 18, or equivalent minimum age in the relevant jurisdiction may review and request deletion of such child's

personal information as well as prohibit the use thereof.

Global Operations

We transfer and process your information globally both in our own facilities and with service providers, or partners, regardless of where you use our Services. The laws, regulations, and standards of the country in which your information is stored or processed may be different from those of your own country.

California Privacy Rights: Pursuant to Section 1798.83 of the California Civil Code, residents of California can obtain certain information about the types of personal information that companies with whom they have an established business relationship have shared with third parties for direct marketing purposes during the proceeding calendar year. In particular, the law provides that companies must inform consumers about the categories of personal information that have been shared with third parties, the names and addresses of those third parties, and examples of the types of services or products marketed by those third parties. To request a copy of the information disclosure provided by HIKVISION pursuant to Section 1798.83 of the California Civil Code, please contact us at the contact information below in **Contact Us**. Please allow 30 days for a response.

Contact Us

Please contact us if you have any questions or comments about our privacy practices or this Privacy Policy. You can always reach us through the below contact information:

- A&E Program: aepartners.usa@hikvision.com
- Cybersecurity: security.usa@hikvision.com
- Dealer Partner Program: partners.usa@hikvision.com
- Marketing: marketing.usa@hikvision.com
- OEM/ODM: oem.usa@hikvision.com
- Sales: inside.usa@hikvision.com
- Technical Support: techsupport.usa@hikvision.com
- Canadian Technical Support: techsupport.ca@hikvision.com
- Need Help with This Product/Product Detail feature: inside.usa@hikvision.com
- A&E partner inquiries (user registration, new project support, etc.): aepartners.usa@hikvision.com
- HDP partner inquiries (user registration, new partner registration, etc.): partners.usa@hikvision.com
- US Hikcentral Trial Version Request: sales.usa@hikvision.com
- Canada Hikcentral Trial Version Request: sales.canada@hikvision.com
- Hikvision Robotics Division: robotics.USA@hikvision.com
- Hikvision OEM/ODM Division: OEMODM.usa@hikvision.com
- A&E partner registrations: sarkis.timourian@hikvision.com
- RMA: rma.usa@hikvision.com
- Customer Service: csr.usa@hikvision.com
- Careers: hr.usa@hikvision.com
- Hikvision B2B Portal: b2b.usa@hikvision.com

Please provide: (i) your name (or nickname), your country or region of residence and your preferred method of contact; and (ii) the details of your request or comment along with any corresponding Website links.




Mandatory Electrical Requirements

Hikvision requires the following conditions and equipment for all of its electronic equipment:

- **Grounding**
Ensure good conductivity for all ground paths; examine ground path contact surfaces for defects, dirt, corrosion, or non-conductive coatings that may impede conductivity. Repair or clean contact surfaces as necessary to assure good metal-to-metal contact. Ensure fasteners are properly installed and tightened.
- **Electrical Wiring**
Ensure your outlets are properly wired. They can be checked with an electrical outlet tester.
- **Surge Suppressor (Required)**
Hikvision is not responsible for any damage to equipment caused by power spikes in the electrical power grid. Use of a surge suppressor meeting the following specifications is mandatory for all Hikvision electronic equipment:
 - Specifications
 - > Listed by Underwriter's Laboratories, meeting the UL 1449 Voltage Protection Rating (VPR)
 - > Minimum protection of 1,000 joules or higher
 - > Clamping voltage of 400 V or less
 - > Response time of 1 nanosecond or less
 - Usage
 - > Surge suppressors must not be daisy chained with power strips or other surge suppressors
 - Maintenance
 - > Replace after a serious electrical event (e.g., lighting blew out a transformer down the street)
 - > Replace yearly in storm-prone areas
 - > Replace every two years as routine maintenance

Symbol Conventions

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

Symbol	Description
 NOTE	Provides additional information to emphasize or supplement important points of the main text.
 WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100-240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- Please make sure that the plug is firmly connected into the power socket.
- If smoke, odor, or noise rise from the device, turn off the power at once, unplug the power cable, and then contact the service center.

Preventive and Cautionary Tips

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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with a UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION	20
1.1 Front Panel	20
1.2 Rear Panel	21
1.2.1 DS-76xxNXI-I2/xxP/4S	21
1.3 IR Remote Control Operations	22
1.3.1 Pairing (Enabling) the IR Remote to a Specific Device (optional)	22
1.3.2 Unpairing (Disabling) an IR Remote from a Device	22
1.3.3 Troubleshooting	24
1.4 USB Mouse Operation	24
CHAPTER 2 GETTING STARTED	26
2.1 Start up the Device	26
2.2 Activate the Device	26
2.3 Configure Unlock Pattern for Login	27
2.4 Login to the Device	28
2.4.1 Log in via Unlock Pattern	28
2.4.2 Log in via Password	29
2.5 Enter Wizard to Configure Basic Settings	30
2.6 Enter Main Menu	33
2.7 System Operation	34
2.7.1 Log out	34
2.7.2 Shut Down the Device	34
2.7.3 Reboot the Device	35
CHAPTER 3 CAMERA MANAGEMENT	36
3.1 Add the IP Cameras	36
3.1.1 Add the IP Camera Manually	36
3.1.2 Add the Automatically Searched Online IP Cameras	36
3.2 Configure the Customized Protocols	37
CHAPTER 4 CAMERA SETTINGS	38
4.1 Configure OSD Settings	38
4.2 Configure Privacy Mask	38
4.3 Configure the Video Parameters	39
4.4 Configure the Day/Night Switch	40
4.5 Configure Other Camera Parameters	40
CHAPTER 5 LIVE VIEW	41
5.1 Start Live View	41
5.1.1 Digital Zoom	41
5.1.2 3D Positioning	42
5.1.3 Live View Strategy	42
5.2 Configure Live View Settings	42
5.3 Configure Live View Layout	43
5.4 Configure Auto-Switch of Cameras	44
5.5 Configure Channel-Zero Encoding	44
5.6 Use an Auxiliary Monitor	45
CHAPTER 6 PTZ CONTROL	46
6.1 PTZ Control Wizard	46
6.2 Configure PTZ Parameters	46
6.3 Set PTZ Presets, Patrols & Patterns	47
6.3.1 Set a Preset	47
6.3.2 Call a Preset	48
6.3.3 Set a Patrol	48
6.3.4 Call a Patrol	50
6.3.5 Set a Pattern	50
6.3.6 Call a Pattern	51
6.3.7 Set Linear Scan Limits	51
6.3.8 Call Linear Scan	52
6.3.9 One-touch Park	52
6.4 Auxiliary Functions	53

CHAPTER 7 STORAGE	54
7.1 Storage Device Management	54
7.1.1 Install the HDD	54
7.1.2 Add the Network Disk	54
7.1.3 Configure eSATA for Data Storage	56
7.2 Storage Mode	56
7.2.1 Configure HDD Group	56
7.2.2 Configure HDD Quota	58
7.3 Recording Parameters	59
7.3.1 Main Stream	59
7.3.2 Sub-Stream.....	60
7.3.3 Picture.....	60
7.3.4 ANR	60
7.3.5 Configure Advanced Recording Settings	60
7.4 Configure Recording Schedule	61
7.5 Configure Continuous Recording	63
7.6 Configure Motion Detection Triggered Recording	63
7.7 Configure Event Triggered Recording	63
7.8 Configure Alarm Triggered Recording	64
7.9 Configure POS Event Triggered Recording	64
7.10 Configure Picture Capture	64
7.11 Configure Holiday Recording and Capture	65
7.12 Configure Redundant Recording and Capture	66
CHAPTER 8 DISK ARRAY	68
8.1 Create Disk Array	68
8.1.1 Enable RAID	68
8.1.2 One-Touch Creation	69
8.1.3 Manual Creation.....	69
8.2 Rebuild Array	70
8.2.1 Configure Hot Spare Disk.....	71
8.2.2 Automatically Rebuild Array	71
8.2.3 Manually Rebuild Array	72
8.3 Delete Array	72
8.4 Check and Edit Firmware	73
CHAPTER 9 FILE MANAGEMENT	74
9.1 Search and Export Human Files	74
9.1.1 Search Human Files.....	74
9.1.2 Export Human Files.....	74
9.2 Search and Export Vehicle Files	75
9.2.1 Search Vehicle Files	75
9.2.2 Export Vehicle Files	76
9.3 Search History Operation	76
9.3.1 Save Search Condition	76
9.3.2 Call Search History.....	77
CHAPTER 10 PLAYBACK	78
10.1 Playing Video Files	78
10.1.1 Instant Playback	78
10.1.2 Play Video	78
10.1.3 Play Tag Files.....	79
10.1.4 Play by Smart Search.....	80
10.1.5 Play Event Files	82
10.1.6	83
10.1.7 Play by Sub-periods	83
10.1.8 Play Log Files.....	84
10.1.9 Play External File	86
10.2 Playback Operations	86
10.2.1 Normal/Important/Custom Video.....	86
10.2.2 Set Play Strategy in Important/Custom Mode	86
10.2.3 Edit Video Clips	87
10.2.4 Switch between Main Stream and Sub-Stream.....	87

10.2.5	Thumbnails View	87
10.2.6	Fast View	88
10.2.7	Digital Zoom	88
CHAPTER 11 EVENT AND ALARM SETTINGS.....		89
11.1	Configure Arming Schedule	89
11.2	Configure Alarm Linkage Actions.....	89
11.2.1	Configure Auto-Switch Full Screen Monitoring	90
11.2.2	Configure Audio Warning	91
11.2.3	Notify Surveillance Center	91
11.2.4	Configure E-mail Linkage	91
11.2.5	Trigger Alarm Output	91
11.2.6	Configure PTZ Linkage	92
11.3	Configure Motion Detection Alarm	92
11.4	Configure Video Loss Alarm	93
11.5	Configure Video Tampering Alarm.....	94
11.6	Configure Sensor Alarms.....	95
11.6.1	Configure Alarm Input	95
11.6.2	Configure One-Key Disarming.....	96
11.6.3	Configure Alarm Output.....	97
11.7	Configure Exceptions Alarm.....	98
11.8	Trigger or Clear Alarm Output Manually.....	99
CHAPTER 12 VCA EVENT ALARM		101
12.1	Human Body Detection	101
12.2	Vehicle Detection	102
12.3	Line Crossing Detection.....	103
12.4	Intrusion Detection.....	104
12.5	Region Entrance Detection.....	105
12.6	Region Exiting Detection	106
12.7	Unattended Baggage Detection.....	108
12.8	Object Removal Detection.....	109
12.9	Audio Exception Detection	110
12.10	Sudden Scene Change Detection	111
12.11	Defocus Detection.....	112
12.12	PIR Alarm	112
12.13	Enable Smart Analysis	113
CHAPTER 13 SMART SEARCH		114
13.1	Vehicle Search.....	114
13.2	People Counting	114
13.3	Heat Map.....	115
CHAPTER 14 HUMAN BODY DETECTION		116
14.1	View Engine Status.....	116
14.2	Human Body Search	116
CHAPTER 15 POS CONFIGURATION.....		117
15.1	Configure POS Settings.....	117
15.1.1	Configure POS Connection	117
15.1.2	Configure POS Text Overlay	120
15.2	Configure POS Alarm	121
CHAPTER 16 NETWORK SETTINGS		123
16.1	Configure TCP/IP Settings	123
16.2	Configuring Hik-Connect	124
16.3	Configure DDNS.....	125
16.4	Configure PPPoE	126
16.5	Configure NTP	126
16.6	Configure SNMP.....	127
16.7	Configure E-mail.....	128
16.8	Configure Ports.....	130
CHAPTER 17 HOT SPARE DEVICE BACKUP.....		131
17.1	Set Hot Spare Device	131
17.2	Set Working Device.....	132

17.3	Manage Hot Spare System	132
CHAPTER 18 SYSTEM MAINTENANCE		134
18.1	Storage Device Maintenance	134
18.1.1	Configure Disk Clone	134
18.1.2	S.M.A.R.T Detection	135
18.1.3	Bad Sector Detection	135
18.1.4	HDD Health Detection	136
18.2	Search & Export Log Files	136
18.2.1	Search the Log Files	137
18.2.2	Export the Log Files	138
18.3	Import/Export IP Camera Configuration Files	139
18.4	Import/Export Device Configuration Files	140
18.5	Upgrade System	140
18.5.1	Upgrade by Local Backup Device	141
18.5.2	Upgrade by FTP	141
18.6	Restore Default Settings	142
18.7	System Service	142
18.7.1	Network Security Settings	142
18.7.2	Manage ONVIF User Accounts	144
18.7.3	Manage IP Camera Activation	144
CHAPTER 19 GENERAL SYSTEM SETTINGS		146
19.1	Configure General Settings	146
19.2	Configure Date and Time	147
19.3	Configure DST Settings	147
19.4	Manage User Accounts	148
19.4.1	Add a User	148
19.4.2	Set the Permission for a User	149
19.4.3	Set Local Live View Permission for Non-Admin Users	151
19.4.4	Edit the Admin User	152
19.4.5	Edit the Operator/Guest User	153
19.4.6	Delete a User	154
CHAPTER 20 APPENDIX		155
20.1	Glossary	155
20.2	Troubleshooting	155

Key Product Features

General

- Connectable to network cameras, network dome and encoders
- Connectable to third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt an ONVIF protocol
- Connectable to smart IP cameras
- H.265+/H.265/ H.264+/H.264/MPEG4 video formats
- PAL/NTSC adaptive video inputs
- Each channel supports dual-stream
- Up to 64 network cameras can be added according to different models
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc
- The quality of the input and output record is configurable

Local Monitoring

- HDMI/VGA output provided
- HDMI Video output at up to 4K resolution and VGA video output at up to 2K resolution
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable
- Live view screen can be switched in group. Manual switch and auto-switch are provided and the auto-switch interval is configurable
- 3D positioning in live view
- Configurable main stream and sub-stream for the live view
- Quick setting menu is provided for live view
- POS information overlay on live view
- Motion detection, video tampering, video exception alert and video loss alert functions
- Privacy mask
- Multiple PTZ protocols supported; PTZ preset, patrol and pattern
- Zooming in by clicking the mouse and PTZ tracing by dragging mouse

HDD Management

- Up to 4 SATA hard disks and 1 eSATA disk can be connected
- Supports 8 network disks (NAS/IP SAN disk)
- Supports S.M.A.R.T. and bad sector detection
- HDD group management
- Supports HDD standby function
- HDD property: redundancy, read-only, read/write (R/W)
- HDD quota management; different capacity can be assigned to different channel
- RAID0, RAID1, RAID5, RAID6 and RAID 10 are supported
- Hot-swappable RAID storage scheme, and can be enabled and disabled on demand, and 16 arrays can

be configured

- Supports disk clone to the eSATA disk

Recording, Capture and Playback

- Holiday recording schedule configuration
- Continuous and event video recording parameters
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm VCA, and POS
- 8 recording time periods with separated recording types
- POS information overlay on image
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording
- Searching record files and captured pictures by events (alarm input/motion detection)
- Tag adding for record files, searching and playing back by tags
- Locking and unlocking record files
- Local redundant recording and capture
- Provide new playback interface with easy and flexible operation
- Searching and playing back record files by channel number, recording type, start time, end time, etc
- Supports the playback by main stream or sub stream
- Smart search for the selected area in the video
- Zooming in when playback
- Reverse playback of multi-channel
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse
- Supports thumbnails view and fast view during playback
- Up to 12-ch synchronous playback at 1080p real time
- Supports playback by transcoded stream
- Manual capture, continuous capture of video images and playback of captured pictures
- Supports enabling H.264+ to ensure high video quality with lowered bitrate

Backup

- Export video data by USB, SATA or eSATA device
- Export video clips when playback
- Management and maintenance of backup devices
- Either Normal or Hot Spare working mode is configurable to constitute an N+1 hot spare system

Human Body Detection

- Human body detection and alarm linkage actions
- More precise human body analytics based on deep learning algorithm
- Re-recognition of the human body target in behavior analytics (line crossing detection, intrusion detection) to effectively raise the alarm accuracy rate

Alarm and Exception

- Configurable arming time of alarm input/output
- Alarm for video loss, motion detection, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, abnormal record/capture, HDD error, and HDD full, etc
- POS triggered alarm supported
- VCA detection alarm is supported
- VCA search for vehicle plate detection, behavior analysis, people counting and heat map
- Connectable to the thermal network camera
- Supports the advanced search for fire/ship/temperature/temperature difference detection triggered alarm and the recorded video files and pictures
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending e-mail and alarm output
- Automatic restore when system is abnormal

Other Local Functions

- Operable by front panel, mouse, remote control, or control keyboard
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel
- Admin password resetting by exporting/importing the GUID file
- Operation, alarm, exceptions and log recording and searching
- Manually triggering and clearing alarms
- Import and export of device configuration information

Network Functions

- Two self-adaptive 10M/100M/1000Mbps network interfaces, and the multi-address and network fault tolerance working modes are configurable
- IPv6 is supported
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported
- TCP, UDP and RTP for unicast
- Auto/Manual port mapping by UPnP/PTM
- Remote web browser access by HTTPS ensures high security
- The ANR (Automatic Network Replenishment) function is supported, it enables the IP camera save the recording files in the local storage when the network is disconnected, and synchronizes the files to the NVR when the network is resumed
- Remote reverse playback via RTSP
- Supports accessing by the platform via ONVIF
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files broken transfer resume
- Remote parameters setup; remote import/export of device parameters
- Remote viewing of the device status, system logs and alarm status

- Remote keyboard operation
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- RS-232, RS-485 transparent channel transmission
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Virtual host function is provided to get access and manage the IP camera directly
- Two-way audio and voice broadcasting
- Embedded WEB server

Development Scalability:

- SDK for Windows system
- Source code of application software for demo
- Development support and training for application system.

Chapter 1 Introduction

1.1 Front Panel

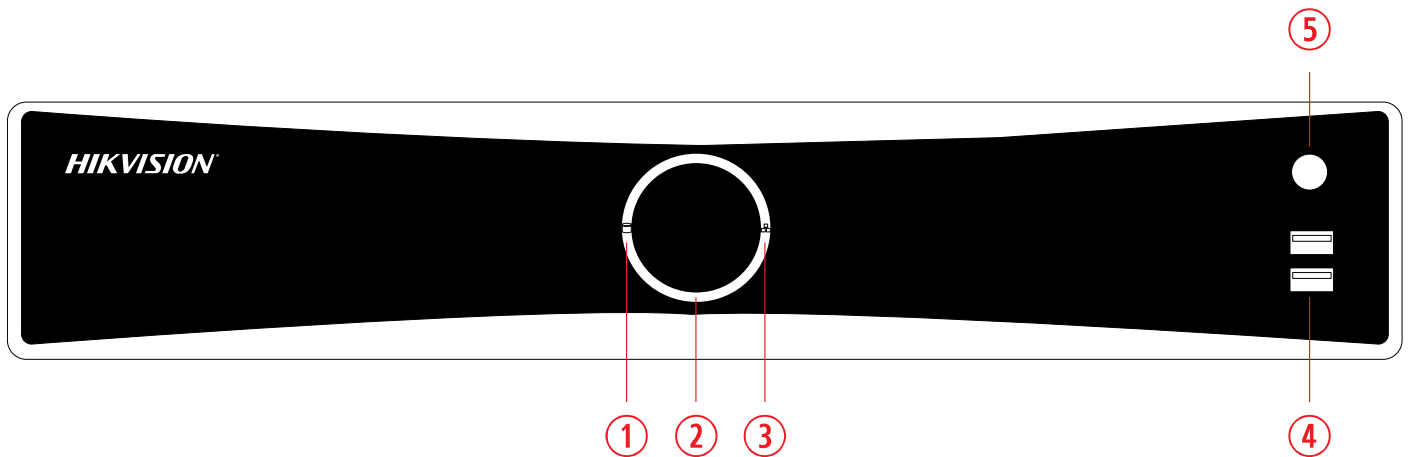


Figure 1-1 Front Panel

Table 1-1 Panel Description

No.	Name	Function Description
1	HDD indicator	<ul style="list-style-type: none"> • Solid white: HDD is abnormal. • Flashing white: HDD is reading/writing. • Unlit: No HDD is detected.
2	Power indicator	<ul style="list-style-type: none"> • Solid white: Device is running normally. • Breathing light: Device is shutdown. • Unlit: No power supply is connected.
3	Network indicator	<ul style="list-style-type: none"> • Solid white: Network connection is normal. • Flashing white: Device is transferring data via network. • Unlit: Network connection failed.
4	USB	Universal Serial Bus (USB) 2.0 port for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
5	IR Receiver	IR receiver for remote control.

1.2 Rear Panel

1.2.1 DS-76xxNXI-I2/xxP/4S

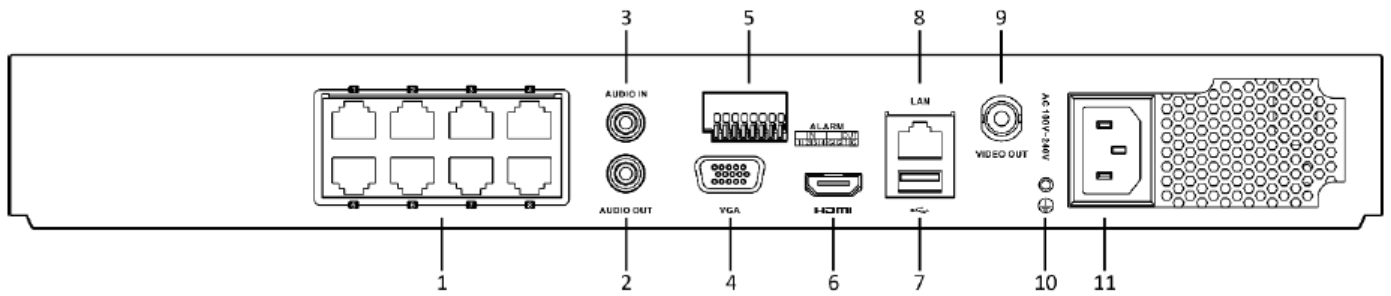


Figure 1-6 Rear Panel

Table 1-5 Panel Description

No.	Name	Description
1	PoE	RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
2	Audio out	RCA connector for audio output
3	Audio in	RCA connector for audio input
4	VGA	DB9 connector for VGA output. Display local video output and menu
5	Alarm in/out	Connector for alarm input/output
6	HDMI	HDMI video output connector
7	USB 3.0	Universal Serial Bus (USB) 3.0 port for additional device such as USB mouse and USB Hard Disk Drive (HDD)
8	LAN	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
9	Video out	CVBS video output
10	GND	Ground
11	Power supply	100 to 240 VAC power supply

1.3 IR Remote Control Operations

The device may also be controlled with the included IR remote control, as shown in Figure 1-2.



Batteries (2 × AAA) must be installed before operation.

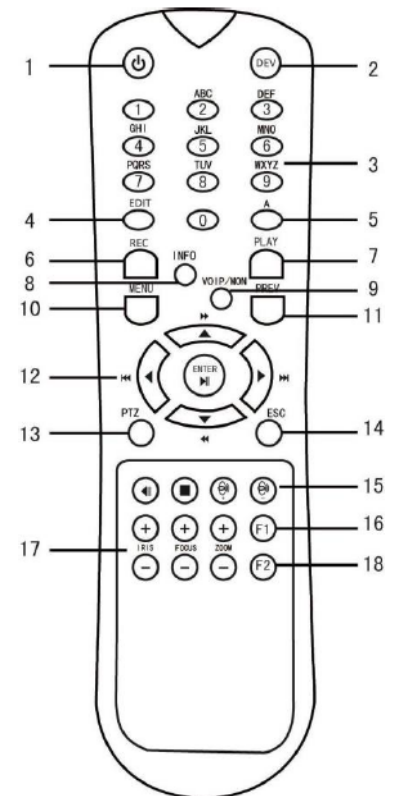
The IR remote is set at the factory to control the device (using default Device ID# 255) without any additional steps. Device ID# 255 is the default universal device identification number shared by the devices. You may also pair an IR Remote to a specific device by changing the Device ID#, as follows:

1.3.1 Pairing (Enabling) the IR Remote to a Specific Device (optional)

You can pair an IR Remote to a specific device by creating a user-defined Device ID#. This feature is useful when using multiple IR Remotes and devices.

On the device:

- 1) Go to **System > General**.
- 2) Type a number (255 digits maximum) into the Device No. field on the IR Remote:
- 3) Press the DEV button.
- 4) Use the Number buttons to enter the Device ID# that was entered into the device.
- 5) Press Enter button to accept the new Device ID#.



1.3.2 Unpairing (Disabling) an IR Remote from a Device

To unpair an IR Remote from a device so that the unit cannot control any device functions, proceed as follows:

Press the DEV key on the IR Remote. Any existing Device ID# will be erased from the unit's memory and it will no longer function with the device.



(Re)-enabling the IR Remote requires pairing to a device. See "Pairing the IR Remote to a Specific device (optional)" section above.

The keys on the remote control closely resemble the ones on the front panel. See Table 1.4.

Figure 1-2 Remote Control

Table 1-2 IR Remote Functions

No.	Name	Function Description
1	POWER ON/OFF	<p>To Turn Power On:</p> <ul style="list-style-type: none"> - If User Has Not Changed the Default device Device ID# (255): <ol style="list-style-type: none"> 1. Press Power On/Off button (1). - If User Has Changed the device Device ID#: <ol style="list-style-type: none"> 1. Press DEV button. 2. Press Number buttons to enter user-defined Device ID#. 3. Press Enter button. 4. Press Power button to start device. <p>To Turn device Off:</p> <ul style="list-style-type: none"> - If User Is Logged On: <ol style="list-style-type: none"> 1. Hold Power On/Off button (1) down for five seconds to display the "Yes/No" verification prompt. 2. Use Up/Down Arrow buttons (12) to highlight desired selection. 3. Press Enter button (12) to accept selection. -If User Is Not Logged On: <ol style="list-style-type: none"> 1. Hold Power On/Off button (1) down for five seconds to display the user name/password prompt. 2. Press the Enter button (12) to display the on-screen keyboard. 3. Input the user name. 4. Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 5. Use the Down Arrow button (12) to move to the "Password" field. 6. Input password (use on-screen keyboard or numeric buttons (3) for numbers). 7. Press the Enter button (12) to accept input and dismiss the on-screen keyboard. 8. Press the OK button on the screen to accept input and display the Yes/No" verification prompt (use Up/Down Arrow buttons (12) to move between fields) 9. Press Enter button (12) to accept selection. <p>User name/password prompt depends on device is configuration. See "System Configuration" section.</p>
2	DEV	<p>Enable IR Remote: Press DEV button, enter device Device ID# with number keys, press Enter to pair unit with the device</p> <p>Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the device</p>
3	Numerals	<p>Switch to the corresponding channel in Live View or PTZ Control mode</p> <p>Input numbers in Edit mode</p>
4	EDIT	<p>Delete characters before cursor.</p> <p>Check the checkbox and select the ON/OFF switch</p>
5	A	<p>Adjust focus in the PTZ Control menu</p> <p>Switch on-screen keyboards (upper and lower case alphabet, symbols, and numerals)</p>
6	REC	<p>Enter Manual Record setting menu</p> <p>Call a PTZ preset by using the numeric buttons in PTZ control settings</p> <p>Turn audio on/off in Playback mode</p>
7	PLAY	<p>Go to Playback mode</p> <p>Auto scan in the PTZ Control menu</p>
8	INFO	Reserved
9	VOIP	Switches between main and spot output Zooms out the image in PTZ control mode
10	MENU	<p>Return to Main menu (after successful login)</p> <p>N/A</p> <p>Show/hide full screen in Playback mode</p>
12	DIRECTION	<p>Navigate between fields and menu items</p> <p>Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode</p> <p>Cycle through channels in Live View mode</p> <p>Control PTZ camera movement in PTZ control mode</p>
	ENTER	<p>Confirm selection in any menu mode</p> <p>Checks checkbox</p> <p>Play or pause video in Playback mode</p> <p>Advance video a single frame in single-frame Playback mode</p> <p>Stop/start auto switch in auto-switch mode</p>
13	PTZ	Enter PTZ Control mode
14	ESC	<p>Go back to previous screen</p> <p>N/A</p>
15	RESERVED	Reserved
16	F1	<p>Select all items on a list</p> <p>N/A</p> <p>Switch between play and reverse play in Playback mode</p>
	PTZ Control	Adjust PTZ camera iris, focus, and zoom
18	F2	<p>Cycle through tab pages</p> <p>Switch between channels in Synchronous Playback mode</p>

1.3.3 Troubleshooting

**NOTE**

Make sure you have installed batteries properly in the remote control. Aim the IR remote control at the IR receiver in the front panel.

If there is no response after you press any button on the remote, follow the troubleshooting procedure below.

- 1) Go to **System** > **General** by operating the front control panel or the mouse.
- 2) Check and remember the device ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.
- 3) Press the DEV button on the remote control.
- 4) Enter the device ID# you set in step 2.
- 5) Press the **ENTER** button on the remote.

If the Status indicator on the front panel turns blue, the remote control is operating properly. If the Status indicator does not turn blue and there is still no response from the remote, please check the following:

- Batteries are installed correctly and the polarities of the batteries are not reversed.
- Batteries are fresh and not discharged.
- IR receiver is not obstructed.
- No fluorescent lamps are being used nearby

If the remote is still functioning properly, please change remote and try again, or contact the device provider.

1.4 USB Mouse Operation

A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this device. To use a USB mouse:

- 1) Plug USB mouse into one of the USB interfaces on the front panel of the device.
- 2) The mouse should automatically be detected. In the rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible. Please refer to the recommended the device list from your provider.

Table 1-3 Description of the Mouse Control

Name	Action	Description
Left-Click	Single-Click	<ul style="list-style-type: none"> • Live view: select channel and show the quick set menu • Menu: select and enter
	Double-Click	Live view: switch between single-screen and multi-screen
	Click and Drag	<ul style="list-style-type: none"> • PTZ control: pan, tilt and zoom • Video tampering, privacy mask and motion detection: select target area • Digital zoom-in: drag and select target area • Live view: drag channel/time bar
Right-Click	Single-Click	<ul style="list-style-type: none"> • Live view: show menu • Menu: exit current menu to upper level menu
Scroll-Wheel	Scrolling up	<ul style="list-style-type: none"> • Live view: previous screen • Menu: Previous item
	Scrolling down	<ul style="list-style-type: none"> • Live view: Next screen • Menu: Next item

Chapter 2 Getting Started

2.1 Start up the Device

Purpose

Proper startup and shutdown procedures are crucial to expanding the life of the device.

Before you start

Check that the voltage of the extra power supply is the same with the device's requirement, and the ground connection is working properly.

- 1) Connect the device power supply interface and electrical socket with delivered power cable. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power button on the front panel should be red, indicating the device is receiving the power.

2.2 Activate the Device

Purpose:

For 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.

- 1) Input the same password in the text field of **Create New Password** and **Confirm New Password**.

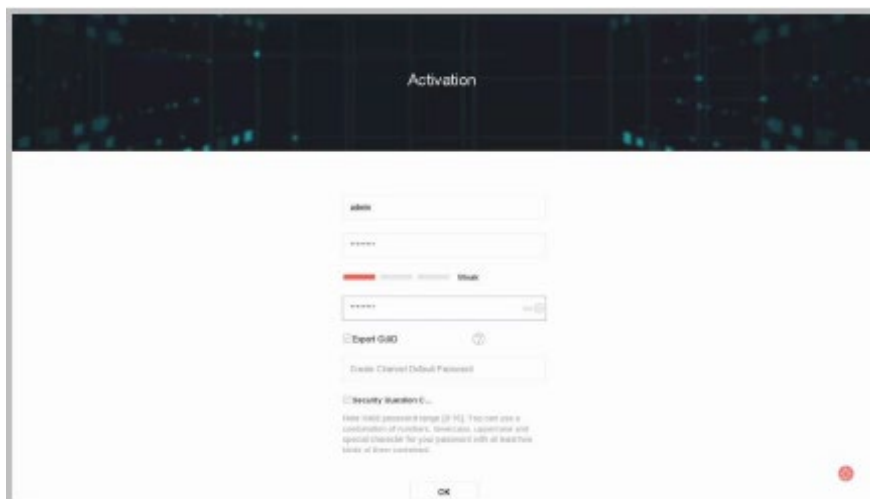


Figure 2-1 Activating the Device

**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. We recommend that you reset your password regularly, especially in high security systems. Resetting the password monthly or weekly can better protect your product.

- 2) In the **Create Channel Default Password** text field, create a login password for IP camera(s) connected to the device.
- 3) (Optional) Check **Export GUID** and **Security Question Configuration**.
 - **Export GUID:** export the GUID for future password resetting.
 - **Security Question Configuration:** configure the security questions which can be used for resetting the password.
- 4) Click **OK**.

What to do next:

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

**NOTE**

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

2.3 Configure Unlock Pattern for Login

For the admin user, you can configure the unlock pattern for device login.

- 1) After the device is activated, you can enter the following interface to configure the device unlock pattern.
- 2) Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

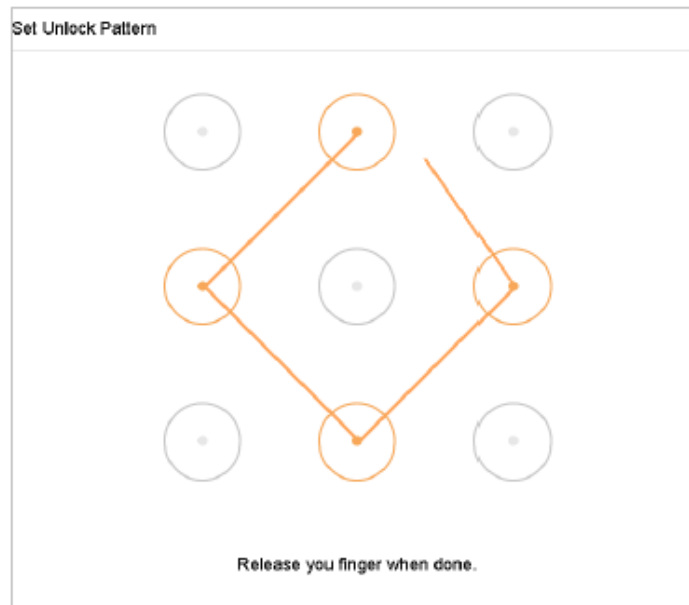


Figure 2-2 Draw the Pattern

i NOTE

Connect at least four dots to draw the pattern. Each dot can be connected once only.

- 3) Draw the same pattern again to confirm it. When the two patterns match, the pattern is configured successfully.

i NOTE

If the two patterns are different, you must set the pattern again.

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

- Only the *admin* user has the permission to unlock the device.
- Please configure the pattern first before unlocking. Please refer to *Chapter 2.3 Configure Unlock Pattern for Login*.

- 1) Right click the mouse on the screen and select the menu to enter the interface.

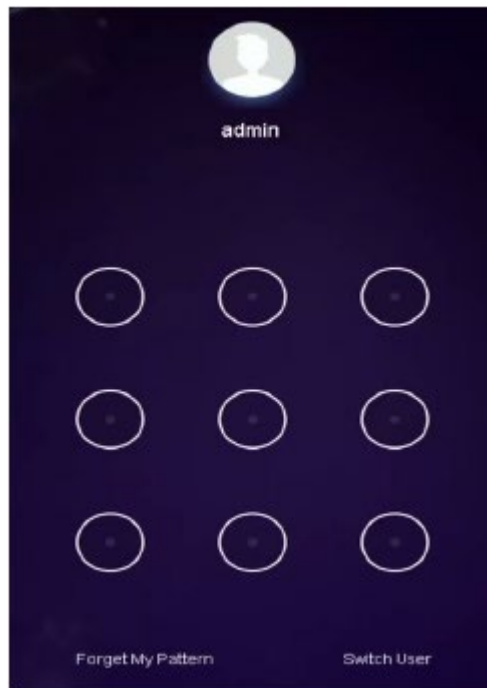


Figure 2-3 Draw the Unlock Pattern

- 2) Draw the pre-defined pattern to unlock to enter the menu operation.

i NOTE

If you have forgotten your pattern, you can select the Forgot My Pattern or Switch User option to enter the normal login dialog box.

When the pattern you draw is different from the pattern you have configured, you should try again.

If you draw the wrong pattern more than 5 times, the system will switch to the normal login mode automatically.

2.4.2 Log in via Password

Purpose:

If device has logged out, you must login the device before operating the menu and other functions.

- 1) Select the **User Name** in the dropdown list.

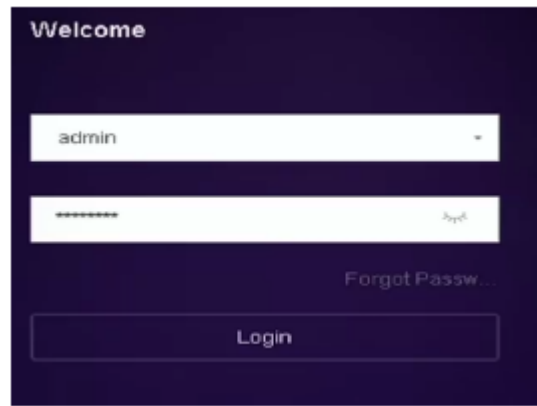


Figure 2-4 Login Interface

- 2) Input password.
- 3) Click **OK** to log in.

**NOTE**

When you forget the admin password, you can click Forgot Password to reset the password.

In the Login dialog box, if you enter the wrong password 7 times, the current user account will be locked for 60 seconds.

2.5 Enter Wizard to Configure Basic Settings

By default, the Setup Wizard starts once the device has loaded.

The Setup Wizard can walk you through some important device settings. If you don't want to use the Setup Wizard at that moment, click the **Exit** button.

- 1) Configure the date and time on the **Date and Time Setup interface**.



Figure 2-5 Date and Time Settings

- 2) After the time settings, click **Next** to enter the Network Setup Wizard window, as shown in the following figure.

Figure 2-6 Network Settings

- 3) Click **Next** after you configured the network parameters, which takes you to the **HDD Management** window.

	Label	Capacity	Status	Property	Type	Free Space
<input type="checkbox"/>	5	931.52GB	Normal	R/W	Local	876.00GB
<input type="checkbox"/>	7	931.52GB	Normal	R/W	Local	831.00GB

Figure 2-7 HDD Management

- 4) To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.
- 5) Click **Next**. You enter the **Camera Setup** interface to add the IP cameras.
- Click **Search** to search the online IP Camera. Before adding the camera, make sure the IP camera to be added is in active status.
 - Click the **Add** to add the camera.

 **NOTE**

If the camera is in inactive status, you can select the camera from the list and click Activate to activate the cameras.

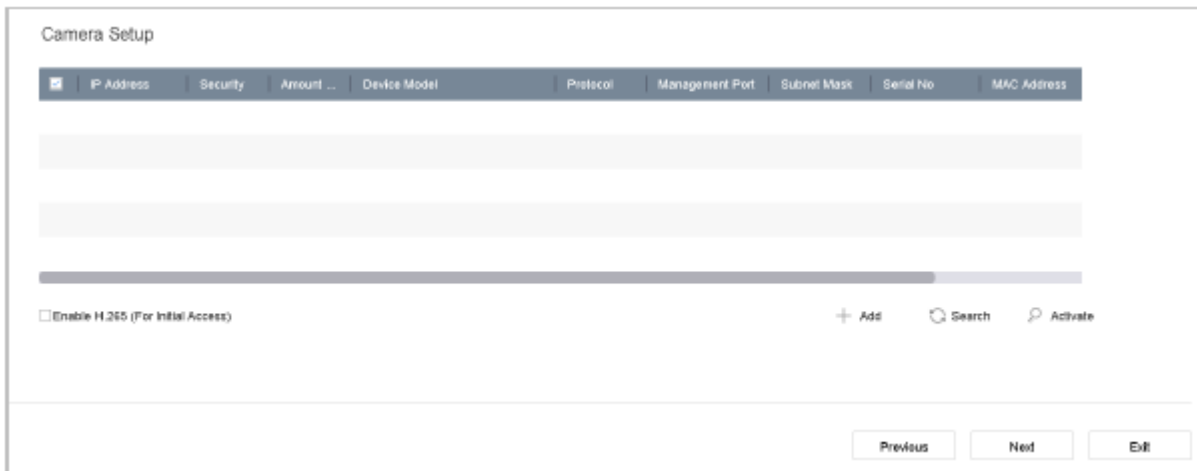


Figure 2-8 Search for IP Cameras

6) Enter Platform Access and configure the Hik-Connect settings.

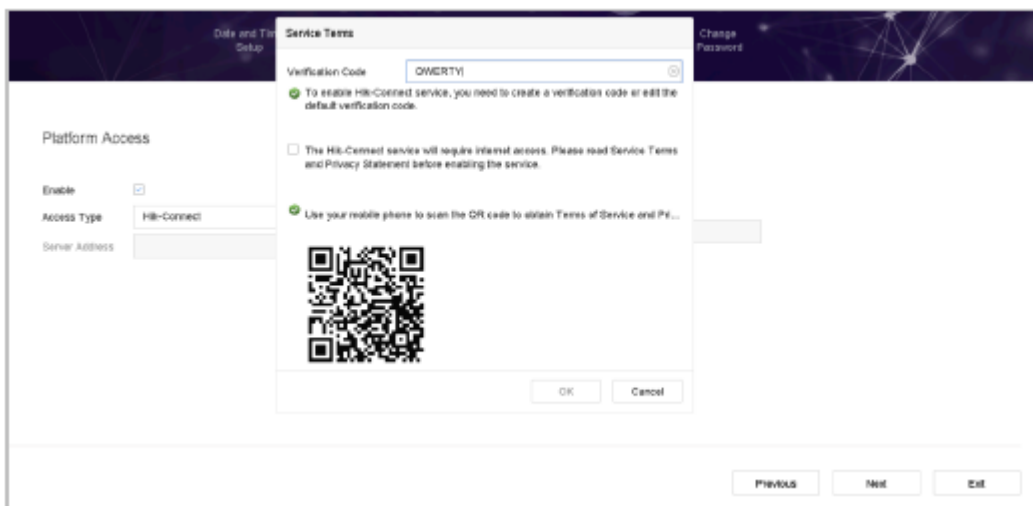


Figure 2-9 Hik-Connect Access

7) Click **Next** to enter the **Change Password** interface to create the new admin password if required.

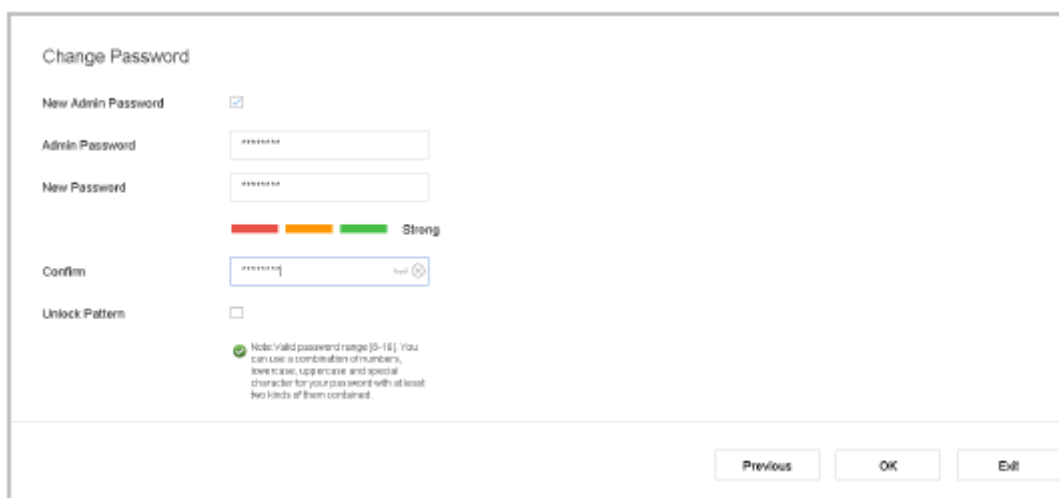


Figure 2-10 Change Password



NOTE You can enter click  to show the inputted characters.

- 1) Check the **New Admin Password** checkbox
- 2) Enter the original password in the **Admin Password** text field
- 3) Input the same password in the **New Password** text field and **Confirm**
- 4) Check the **Unlock Pattern** to enable the unlock pattern login

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. We recommend that you reset your password regularly, especially in high security systems. Resetting the password monthly or weekly can better protect your product.

- 8) Click **OK** to complete the startup Setup Wizard.







2.6 Enter Main Menu



After you have completed the wizard, you can right click on the screen to pop up the main menu bar. Refer to the following figure and table for the description of the main menu and sub-menus.



Figure 2-11 Main Menu Bar

Table 2-1 Description of Icons

Icon	Description
	Live View
	Playback
	File Management
	Smart Analysis
	Camera Management
	Storage Management

	System Mangementet
	System Maintenance

2.7 System Operation

2.7.1 Log out

Purpose:

After logging out, the monitor turns to the live view mode and if you want to perform any operations, you need to enter user name and password to log in again.

- 1) Click on the menu bar.

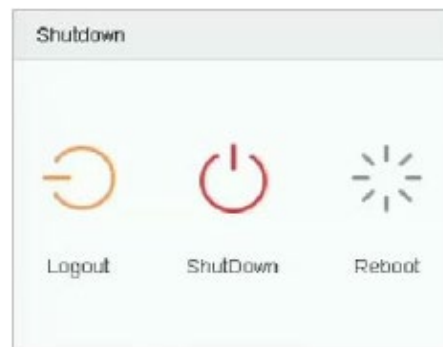



Figure 2-12 Logout

- 2) Click **Logout**.

NOTE

After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.7.2 Shut Down the Device

- 1) Click  on the menu bar.

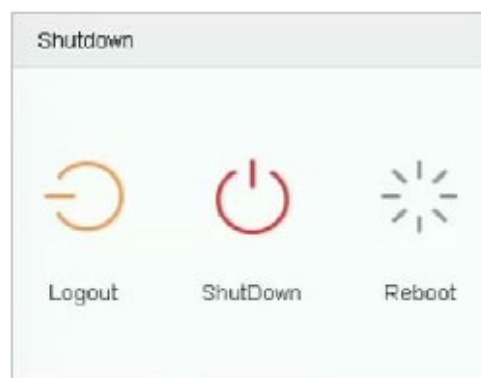


Figure 2-13 Shutdown Menu

- 2) Click the **Shutdown** button.
- 3) Click the **Yes** button.

**NOTE**

Do not press the POWER button again when the system is shutting down.

2.7.3 Reboot the Device

From the Shutdown menu, you can also reboot the device.

- 1) Click on the menu bar.
- 2) Click **Reboot** to reboot the device.

Chapter 3 Camera Management

3.1 Add the IP Cameras


3.1.1 Add the IP Camera Manually

Purpose:

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

Before you start:

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

- 1) Click  on the main menu bar to enter the **Camera Management** section.
- 2) Click the **Custom Add** tab on the title bar to enter the Add IP Camera interface.

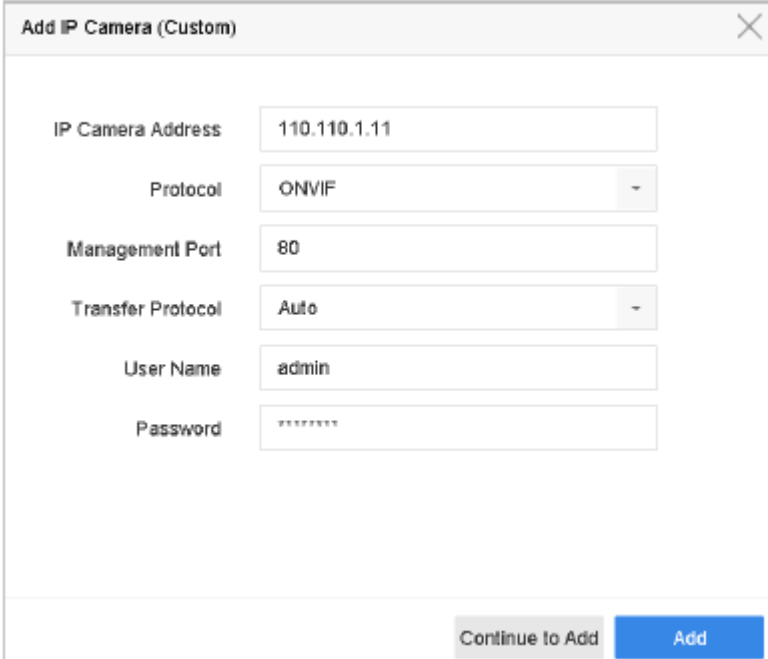


Figure 3-1 Add IP Camera

- 3) Enter the 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 adding the IP camera.
- 6) (Optional) Click **Continue to Add** to continue to add other IP cameras.

3.1.2 Add the Automatically Searched Online IP Cameras

- 1) On the **Camera Management** interface, click the **Online Device** panel to expand the Online Device interface.
- 2) Select the automatically searched online devices.

3) Click **Add**.

NOTE

If the IP camera to add has not been activated, you can activate it from the IP camera list on the camera management interface.

3.2 Configure the Customized Protocols

Purpose:

To connect network cameras that are not configured with the standard protocols, configure their customized protocols. The system provides 16 customized protocols.

1) Click **Protocol** at the top taskbar to enter the protocol management interface.

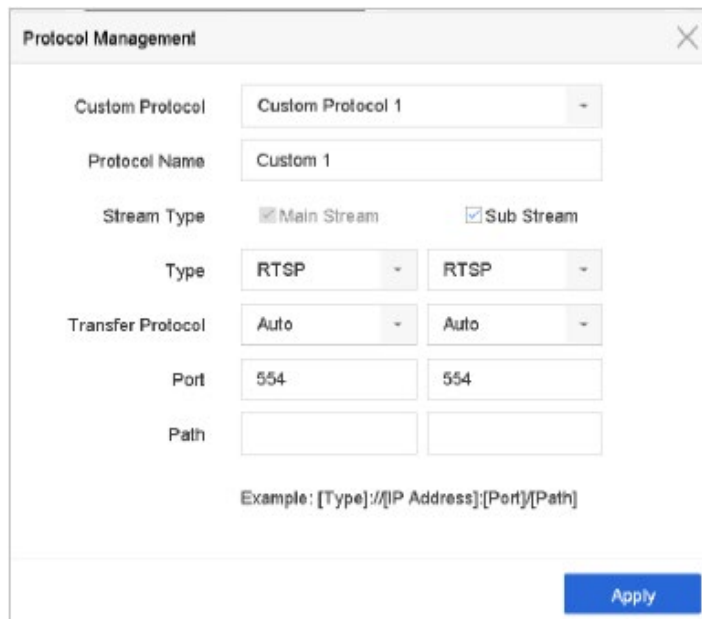


Figure 3-4 Protocol Management

2) Select the transmission protocol type and choose the transfer protocols.

- **Type:** the network camera adopting the custom protocol must support the getting of a stream through standard RTSP
- **Path:** contact the network camera manufacturer to obtain the URL (uniform resource locator) for main stream and sub-streams

The URL format is: [Type]://[IP Address of the network camera]:[Port]/[Path]

Example: rtsp://192.168.1.55:554/ch1/main/av_stream

NOTE

The protocol type and the transfer protocols must be supported by the connected IP camera.

Result:

3) After adding the customized protocols, you can see the protocol name is listed in the drop-down list.

Chapter 4 Camera Settings

4.1 Configure OSD Settings

Purpose:

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

- 1) Go to **Camera > Display**.
- 2) Select the camera from the drop-down list.
- 3) Edit the name in the **Camera Name** text field.
- 4) Check the checkbox of the **Display Name**, **Display Date** and **Display Week** if you want to show the information on the image.
- 5) Set the date format, time format, and display mode.

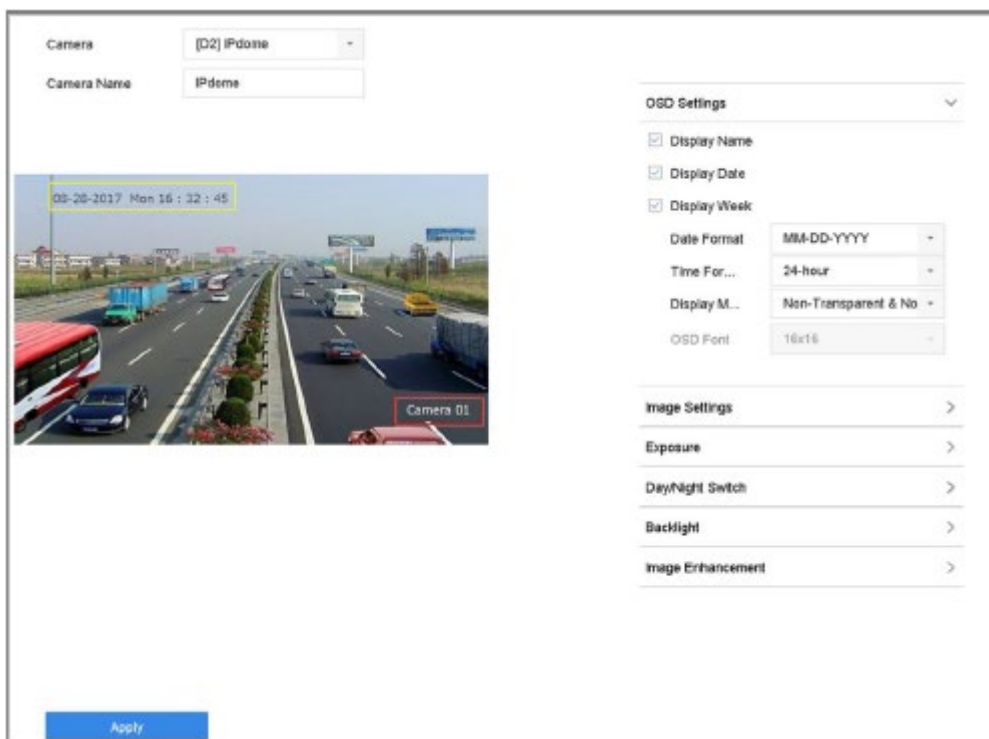


Figure 4-1 OSD Configuration Interface

- 6) You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.
- 7) Click the **Apply** button to apply the settings.

4.2 Configure Privacy Mask

Purpose:

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

- 1) Go to **Camera > Privacy Mask**.

- 2) Select the camera to set the privacy mask to.
- 3) Click the **Enable** checkbox to enable this feature.
- 4) Use the mouse to draw a zone on the window. The zones will be marked with different frame colors.

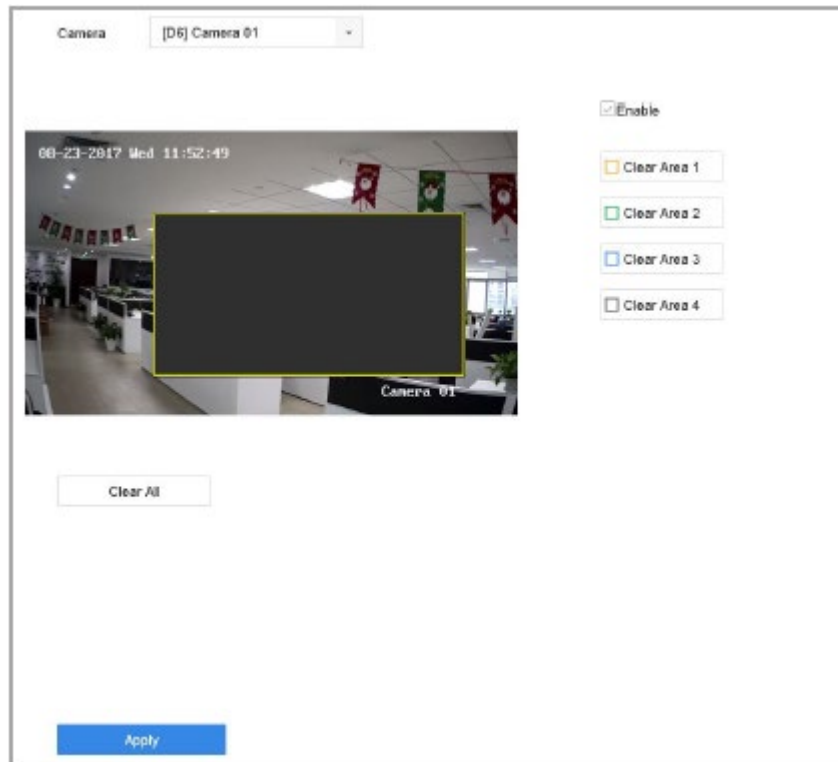


Figure 4-2 Privacy Mask Settings Interface

i NOTE

Up to 4 privacy masks zones can be configured and the size of each area can be adjusted.

Related Operation:

The configured privacy mask zones on the window can be cleared by clicking the corresponding Clear Zone1-4 icons on the right side of the window, or click **Clear All** to clear all zones.

- 5) Click **Apply** to save the settings.

4.3 Configure the Video Parameters

Purpose:

You can customize the image parameters including the brightness, contrast, saturation for the live view and recording effect.

- 1) Go to **Camera > Display**.
- 2) Select the camera from the drop-down list.
- 3) Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast or saturation.
- 4) Click **Apply** to save the settings.

4.4 Configure the Day/Night Switch

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

- 1) Go to **Camera > Display**.
- 2) Select the camera from the drop-down list.
- 3) Select the day/night switch mode to **Day**, **Night**, **Auto** or **Auto-Switch**.
 - **Auto:** The camera switches between day mode and night mode according to the illumination automatically.
 - The sensitivity ranges from 0 to 7, and higher sensitivity results in greater ease in triggering a mode switch.
 - The switch time refers to the interval time between the day/night switch. You can set it from 5 s to 120 s.
 - **Auto-Switch:** The camera switches the day mode and the night mode according to the start time and end time you set.
- 4) Click the **Apply** to save the settings.

4.5 Configure Other Camera Parameters

For the connected camera, you can configure the camera parameters including the exposure mode, backlight and image enhancement.

- 1) Go to **Camera > Display**.
- 2) Select the camera from the drop-down list.
- 3) Configure the camera parameters.
 - **Exposure:** Set the exposure time (1/10000 to 1 sec) of the camera. A larger exposure value results in a brighter image.
 - **Backlight:** Set the wide dynamic range (0 to 100) of the camera. When the surrounding illumination and the object have larger difference in brightness, you should set the WDR value.
 - **Image Enhancement:** For optimized image contrast enhancement.
- 4) Click **Apply** to save the settings.

Chapter 5 Live View

Live view shows you the video image obtained from each camera in real time. The device automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy. Pressing the ESC many times (depending on that menu that you are in) brings you to Live View mode.

5.1 Start Live View


- 1) The system automatically enters the live view interface when it starts up, or you can click the  on the main menu bar to enter the live view interface.
- 2) Click to select a window for live view.
- 3) Double-click the IP camera on the left list to start playing the live video.



Figure 5-1 Live View

- 4) You can use the toolbar at the window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.

5.1.1 Digital Zoom

Digital Zoom is for zooming into the live image. You can zoom in the image to different proportions (1 to 16X).


- 1) In the live view mode, click  from the toolbar to enter the digital zoom interface.
- 2) You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to 16x).



Figure 5-2 Digital Zoom

5.1.2 3D Positioning

3D Positioning (for I series device) is for zooming in/out the specific area of live image.

1) In the live view mode, click the  to enter the 3D positioning mode.

2) Operate zoom in/out on the image.

- **Zoom in**

Use the left mouse key to click on the desired position in the video image and drag a rectangle area in the lower right direction to zoom in.

- **Zoom out**

Use the left mouse key to drag a rectangle area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

5.1.3 Live View Strategy

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**.

5.2 Configure Live View Settings

Live View settings can be customized according to different needs. 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.

1) Go to **System > Live View > General**.

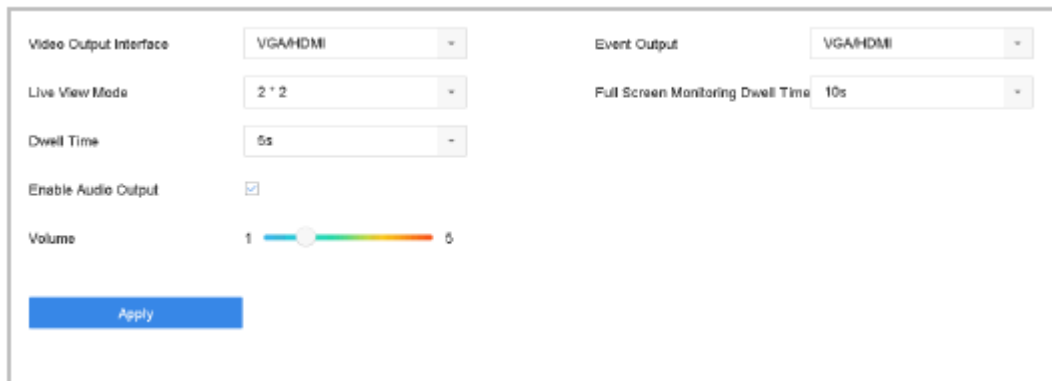


Figure 5-3 Live View-General

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 x 2, 1 x 5, etc.
- **Dwell Time:** the time in seconds to dwell between switching of cameras when enabling auto-switch in Live View.
- **Enable Audio Output:** enable/disable audio output for the selected video output.
- **Volume:** adjust the volume of live view, 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 to save the settings

5.3 Configure Live View Layout

1) Go to **System > Live View > View Settings**.

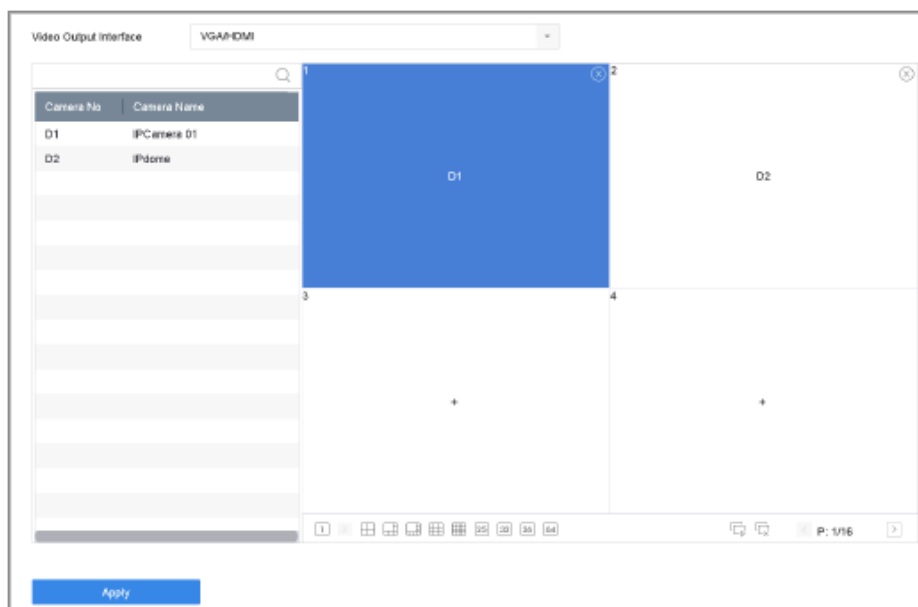


Figure 5-4 Live View

- 2) Select the video output interface, e.g., HDMI/ VGA or channel-zero.
- 3) Select a window division mode from the toolbar.
- 4) Select a division window, and double-click on the camera from the list to set the camera to the window.

**NOTE**

You can enter the number in the text field to quickly search the camera from the list.

- 5) Click **Apply** to save the settings.

5.4 Configure Auto-Switch of Cameras

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

- 1) Go to **System > Live View > General**.
- 2) Set the 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 x 2, 1 x 5, etc.
 - **Dwell Time:** the time in seconds to dwell between switching of cameras when enabling auto-switch. The range is from 5 s to 300 s.
- 3) Go to **View Settings** to set the view layout.
- 4) Click **OK** to save the settings.

5.5 Configure Channel-Zero Encoding

Purpose:

You can enable 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.

- 1) Go to **System > Live View > General**.
- 2) Select the video output interface to Channel-Zero.
- 3) Go to **System > Live View > Channel-Zero**.
- 4) Check the checkbox to enable channel-zero.

The screenshot shows a configuration window for 'Channel-Zero Encoding'. At the top, there is a checkbox labeled 'Enable Channel-Zero Encoding' which is checked. Below this are three dropdown menus: 'Frame Rate' set to 'Full Frame', 'Max. Bitrate Mode' set to 'General', and 'Max. Bitrate(Kbps)' set to '1792'. At the bottom of the window is a blue button labeled 'Apply'.

Figure 5-5 Live View- Channel-Zero Encoding

- 5) Configure the **Frame Rate**, **Max. Bitrate Mode** and **Max. Bitrate**. The higher frame rate and bitrate settings result in the higher requirement of bandwidth.
- 6) Click **Apply**.

Result:

You can view all of the channels in one screen using the CMS or web browser.

5.6 Use an Auxiliary Monitor

Certain Live View features are also available while in an Aux monitor. These features include:

- **Single Screen:** switch to a full screen display of the selected camera. The camera can be selected from a dropdown list.
- **Multi-screen:** switch between different display layout options. Layout options can be selected from a dropdown list.
- **Next Screen:** when displaying less than the maximum number of cameras in Live View, clicking this feature will switch to the next set of displays.
- **Playback:** enter Playback mode.
- **PTZ Control:** enter PTZ Control mode.
- **Main Monitor:** enter Main operation mode.

NOTE

In the live view mode of the main output monitor, the menu operation is not available while Aux output mode is enabled.

Chapter 6 PTZ Control

6.1 PTZ Control Wizard

Before you start

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

Purpose

Follow the PTZ control wizard to guide you through the basic PTZ operation.


- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control wizard pops up as below.




Figure 6-1 PTZ Control Wizard

- 2) Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.
- 3) (Optional) Check ***Do not show this prompt again.***
- 4) Click **OK** to exit.

6.2 Configure PTZ Parameters

Purpose

Follow the procedure to set the parameters for PTZ. The configuration of the PTZ parameters should be done before you control the PTZ camera.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **PTZ Parameters Settings** to set the PTZ parameters.

PTZ Parameter Settings

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 6-2 PTZ Parameters Settings

- 3) Edit the parameters of the PTZ camera.

**NOTE**

All the parameters should be exactly the same as the PTZ camera parameters.

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

6.3 Set PTZ Presets, Patrols & Patterns



Before you start:

Please make sure that the presets, patrols and patterns should be supported by PTZ protocols.

6.3.1 Set a Preset

Purpose:

Follow the steps to set the preset location which you want the PTZ camera to point to when an event takes place.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Use the directional buttons on the PTZ control panel to wheel the camera to the location where you want to set preset, and the zoom and focus operations can be recorded in the preset as well.
- 3) Click  in the lower right corner of live view to set the preset.

1	▼	Preset 1	Call	Apply	Cancel
---	---	----------	------	-------	--------

Figure 6-3 Set Preset


- 4) Select the preset number (1 to 255) from the drop-down list.
- 5) Enter the preset name in the text field.
- 6) Click **Apply** to save the preset.
- 7) Repeat steps 2 to 6 to save more presets.
- 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 6-4 View the Configured Presets

6.3.2 Call a Preset

Purpose:

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




- 1) Click  on the quick settings toolbar of the PTZ camera live view.
- 2) Click  in the lower right corner of live view.
- 3) Select the preset number 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 6-5 Call Preset (1)




Figure 6-6 Call Preset (2)

6.3.3 Set a Patrol

Purpose:

Patrols can be set to move the PTZ to different key points and have it stay there for a set duration before moving on to the next key point. The key points are corresponding to the presets.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **Patrol** to configure patrol.

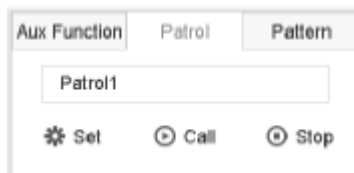


Figure 6-7 Patrol Configuration

- 3) Select the patrol number in the text field.
- 4) Click **Set** to enter the Patrol Settings interface.

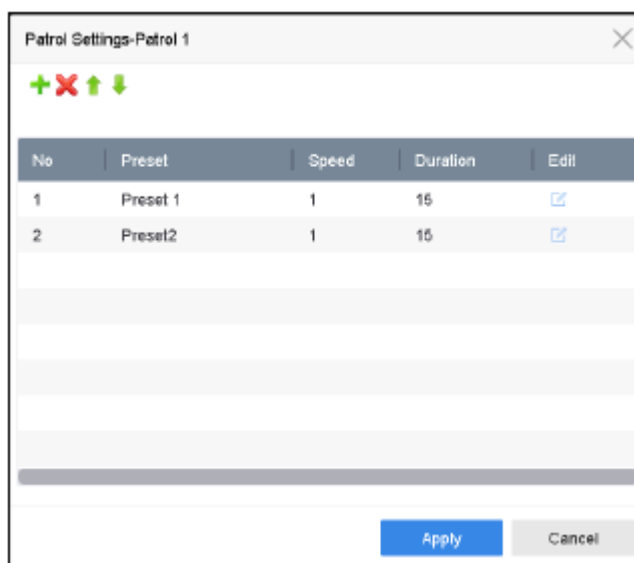



Figure 6-8 Patrol Settings

- 5) Click  to add key point for the patrol.

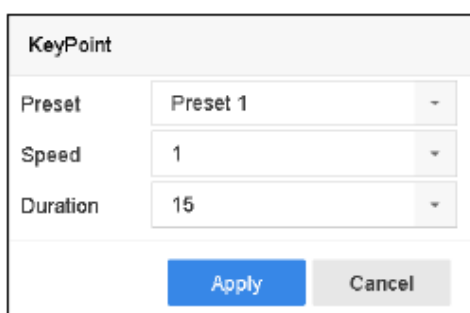



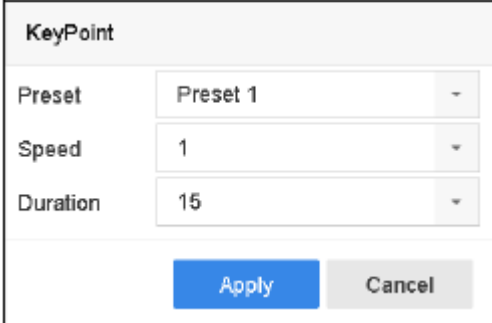
Figure 6-9 Key Point Configuration

1) Configure key point parameters.

- **Preset:** determines the order at which the PTZ will follow while cycling through the patrol.
- **Speed:** defines the speed at which the PTZ will move from one key point to the next.
- **Duration:** refers to the time span to stay at the corresponding key point.

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

6) (Optional) Click  to edit the added key point.



The image shows a dialog box titled "KeyPoint". It contains three dropdown menus: "Preset" with "Preset 1" selected, "Speed" with "1" selected, and "Duration" with "15" selected. At the bottom of the dialog are two buttons: "Apply" (highlighted in blue) and "Cancel".

Figure 6-10 Edit Key Point

7) (Optional) Select a key point and click  to delete it.

8) (Optional) Click  or  to adjust the key point order.


9) Click **Apply** to save the settings of the patrol.

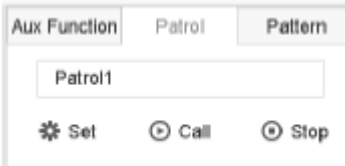
10) Repeat steps 3-9 to set more patrols.

6.3.4 Call a Patrol

Purpose:

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

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **Patrol** on the PTZ control panel.



The image shows a dialog box with three tabs: "Aux Function", "Patrol", and "Pattern". The "Patrol" tab is selected. Inside the dialog, there is a text field containing "Patrol1". Below the text field are three buttons: "Set" (with a gear icon), "Call" (with a play icon), and "Stop" (with a stop icon).


Figure 6-11 Patrol Configuration

- 3) Select a patrol in the text field.
- 4) Click **Call** to call it.
- 5) (Optional) Click **Stop** to stop calling it.

6.3.5 Set a Pattern

Purpose:

Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ movement according to the predefined path.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **Pattern** to configure pattern.

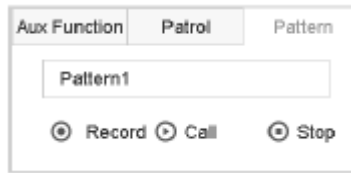


Figure 6-12 Pattern Configuration


- 3) Select the pattern No. in the text field.
- 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 movement of the PTZ is recorded as the pattern.
- 5) Repeat steps 3 to 4 to set more patterns.

6.3.6 Call a Pattern

Purpose:

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

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **Pattern** to configure pattern.

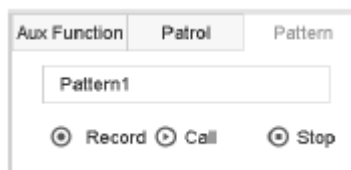


Figure 6-13 Pattern Configuration

- 3) Select a pattern in the text field.
- 4) Click **Call** to call it.
- 5) (Optional) Click **Stop** to stop calling it.

6.3.7 Set Linear Scan Limits

Before you start:


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

Purpose:

The linear scan can be enabled to trigger the scan in the horizontal direction in the predefined range.



This function is supported by some certain models.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click the directional buttons to wheel the camera to the location where you want to set the limit, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.



The dome starts a linear scan from the left limit to the right limit, and you must set the left limit on the left side of the right limit, as well the angle from the left limit to the right limit should be no more than 180°.


6.3.8 Call Linear Scan



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

Purpose:

Follow the procedure to call the linear scan in the predefined scan range.

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.
- 2) Click **Linear Scan** to start the linear scan and click it again to stop it.
- 3) (Optional) Click **Restore** to clear the defined left limit and right limit data.



Reboot the camera to have the settings take effect.


6.3.9 One-touch Park



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

Purpose

For some certain model of the speed dome, it can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

- 1) Click  on the quick settings toolbar of the PTZ camera live view. The PTZ control panel displays on the right of the interface.

- 2) Click **Park (Quick Patrol)**, **Park (Patrol 1)** or **Park (Preset 1)** to activate the park action.
 - **Park (Quick Patrol):** The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset 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.



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

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

6.4 Auxiliary Functions

Before you start

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

Purpose

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






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



Figure 6-14 Aux Function Configuration

- 3) Click the icons to operate the aux functions. See the table for the description of the icons.

Table 6-1 Description of Aux Functions Icons

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

Chapter 7 Storage

7.1 Storage Device Management

7.1.1 Install the HDD

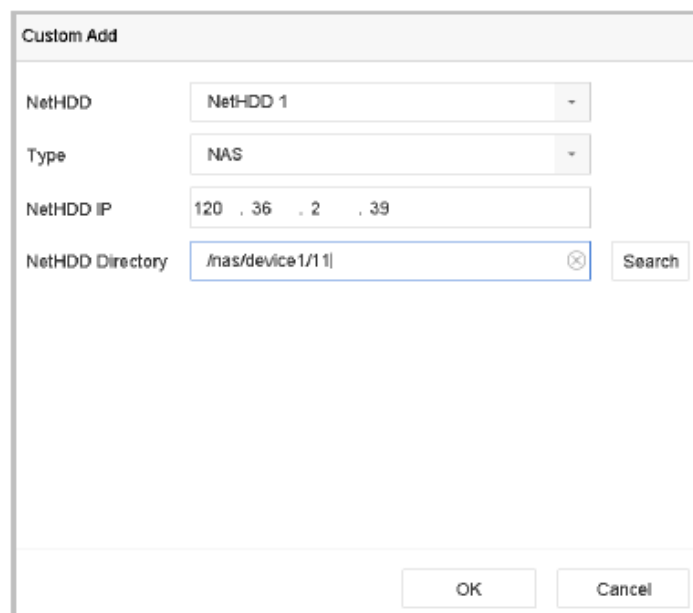
Before startup of the device, install and connect the HDD to the device. Refer to the Quick Start Guide for the installation instructions.

7.1.2 Add the Network Disk

You can add the allocated NAS or disk of IP SAN to device, and use it as network HDD. Up to 8 network disks can be added.

Adding a NAS

- 1) Go to **Storage > Storage Device**.
- 2) Click **Add** to enter the Custom Add interface.
- 3) Select the NetHDD from the drop-down list.
- 4) Select the type to NAS.
- 5) Enter the NetHDD IP address in the text field.
- 6) Click **Search** to search the available NAS disks.



The screenshot shows a dialog box titled "Custom Add" with the following fields and controls:

- NetHDD**: A dropdown menu with "NetHDD 1" selected.
- Type**: A dropdown menu with "NAS" selected.
- NetHDD IP**: A text field containing "120 . 36 . 2 . 39".
- NetHDD Directory**: A text field containing "/nas/device1/1/1|". To the right of this field is a search icon (magnifying glass) and a "Search" button.
- At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 7-1 Add NAS Disk

- 7) Select the NAS disk from the list shown below, or you can manually enter the directory in the text field of NetHDD Directory.
- 8) Click the **OK** to complete the adding of the NAS disk.

Result:

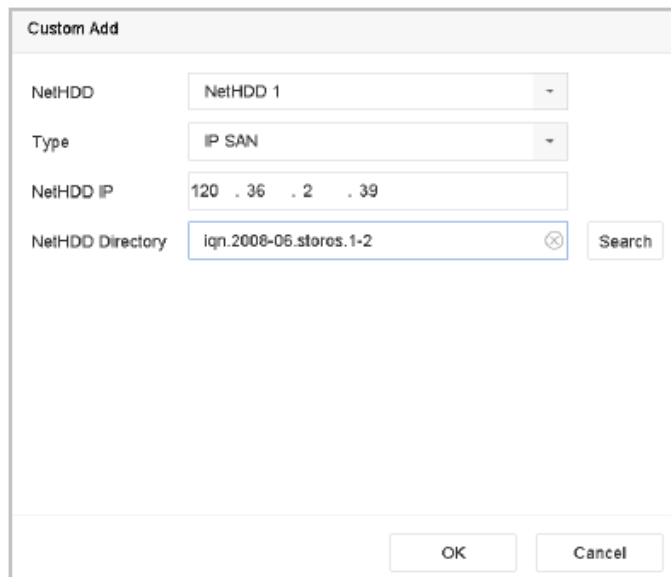
After having successfully added the NAS disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

Adding IP SAN

- 1) Go to **Storage > Storage Device**.
- 2) Click **Add** to enter the Custom Add interface.
- 3) Select the NetHDD from the drop-down list.
- 4) Select the type to IP SAN.
- 5) Enter the NetHDD IP address in the text field.
- 6) Click **Search** to search the available IP SAN disks.
- 7) Select the IP SAN disk from the list shown below.
- 8) Click **OK** to complete the adding of the IP SAN disk.

 **NOTE**

Up to 1 IP SAN disk can be added.



The screenshot shows a 'Custom Add' dialog box with the following fields and values:

- NetHDD:** NetHDD 1
- Type:** IP SAN
- NetHDD IP:** 120 . 36 . 2 . 39
- NetHDD Directory:** iqn.2008-06.stores.1-2

Buttons: Search, OK, Cancel

Figure 7-2 Add IP SAN Disk

Result:

After successfully adding the IP SAN disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

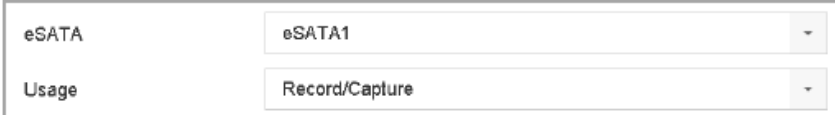
 **NOTE**

If the installed HDD or NetHDD is uninitialized, please select it and click the **Init** button for initialization.

7.1.3 Configure eSATA for Data Storage

When there is an external eSATA device connected to device, you can configure eSATA for the data storage, and you can manage the eSATA in the device.

- 1) Click Storage > Advanced.
- 2) Select the eSATA type to Export or Record/Capture from the dropdown list of **eSATA**.
 - **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 7-3 Set eSATA Mode

- 3) When the eSATA type is selected to Record/Capture, enter the storage device interface.
- 4) Edit the property of the selected eSATA, or initialize it is required.

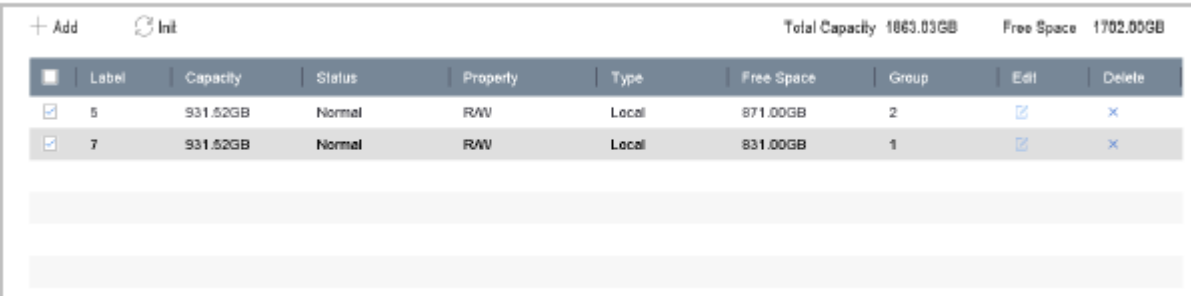
7.2 Storage Mode

7.2.1 Configure HDD Group

Purpose:

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

- 1) Go to **Storage > Storage Device**.
- 2) Check the checkbox to select the HDD to set the group.



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

Figure 7-4 Storage Device

- 3) Click  to enter the Local HDD Settings interface.

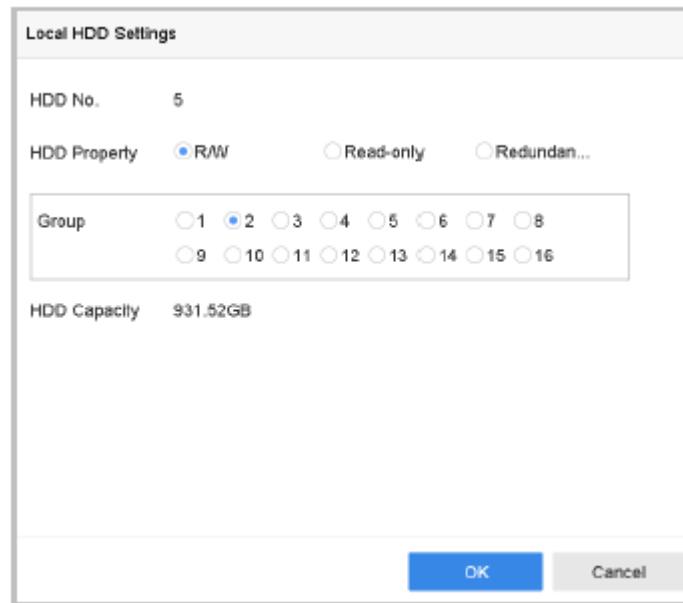


Figure 7-5 Local HDD Settings

- 4) Select the Group number for the current HDD.
- 5) Click **OK**.

 **NOTE**

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

- 6) Go to **Storage > Storage Mode**.
- 7) Check the checkbox of **Group** tab.
- 8) Select the group no. from the list.
- 9) Check the checkbox to select the IP camera to record/capture on the HDD group.

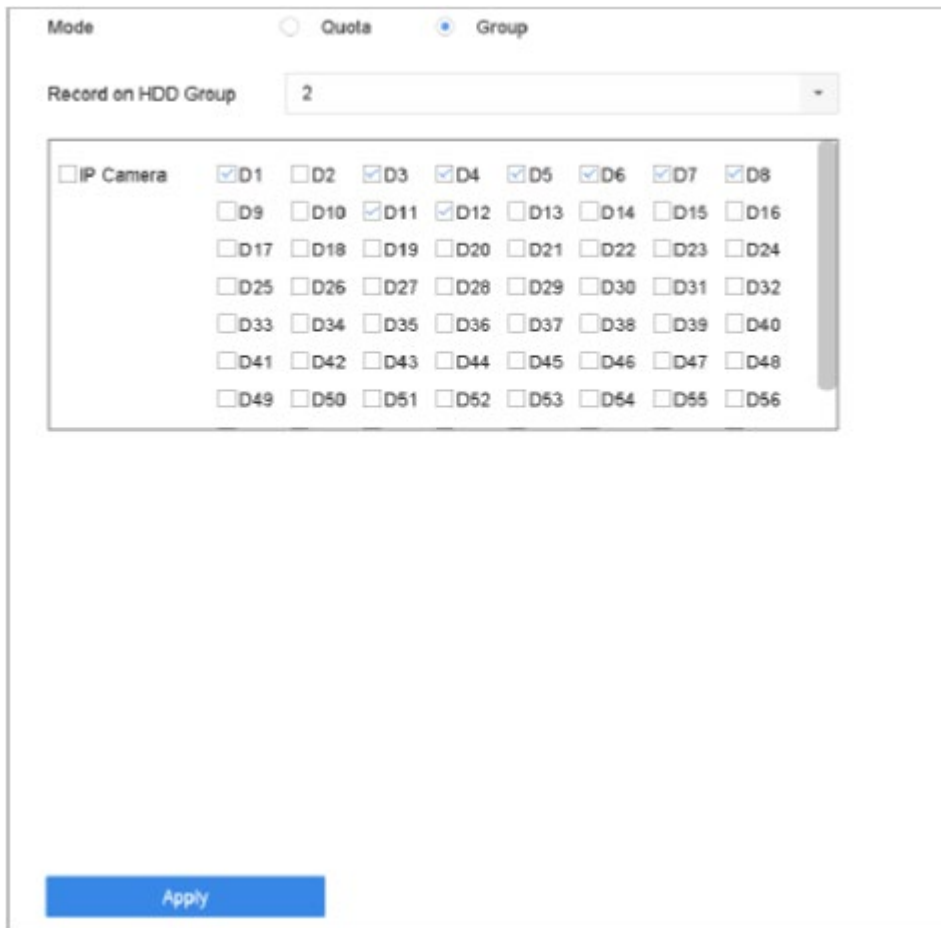


Figure 7-6 Storage Mode-HDD Group

10) Click **Apply**.

i **NOTE**

Reboot the device to activate the new storage mode settings.

7.2.2 Configure HDD Quota

Purpose:

Each camera can be configured with allocated quota for the storage of recorded files or captured pictures.

- 1) Go to **Storage > Storage Mode**.
- 2) Check the checkbox of **Quota** tab.
- 3) Select a camera to set quota.
- 4) Enter the storage capacity in the text fields of **Maximum Record Capacity (GB)** and **Maximum Picture Capacity (GB)**.

Mode Quota Group

Camera [D1] IPCamera 01

Used Record Capacity 18.00GB

Used Picture Capacity 2048.00MB

HDD Capacity (GB) 1863

Max. Record Capacity (GB) 1500

Max. Picture Capacity (GB) 50

⚠ Free Quota Space 313 GB

Copy to Apply

Figure 7-7 Storage Mode-HDD Quota

- 5) (Optional) You can click **Copy to** if you want to copy the quota settings of the current camera to other cameras.
- 6) Click the **Apply** button to apply the settings. Reboot the device to activate the new storage mode settings.

NOTE

When the quota capacity is set to 0, all cameras will use the total capacity of HDD for record and picture capture.

7.3 Recording Parameters

7.3.1 Main Stream

The 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):** 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+ Mode:** The H.264+ mode helps to ensure the high video quality with a lowered bitrate. It can effectively reduce the need of bandwidth and HDD storage space.

A higher resolution, frame rate and bitrate setting will provide you with better video quality, but it will also require more internet bandwidth and use more storage space on the hard drive.

7.3.2 Sub-Stream

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

The sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

7.3.3 Picture

The picture refers to the live picture capture in continuous or event recording type.

- **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.

7.3.4 ANR

ANR (Automatic Network Replenishment) function which enables the IP camera to save the recording files in the local storage when the network is disconnected, and when the network is resumed, it uploads the files to the device.

Enable the ANR (Automatic Network Replenishment) function via the web browser (**Configuration > Storage > Schedule Settings > Advanced**).

7.3.5 Configure Advanced Recording Settings

- 1) Go to **Storage > Schedule Settings > Record Schedule/Capture Schedule**.
- 2) Check the checkbox of **Enable** to enable scheduled recording.
- 3) Click **Advanced** to set the recording parameters.

Figure 7-8 Advanced Record Settings

- **Record Audio:** Check the checkbox to 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.
 - **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. See *Chapter Configure Redundant Recording and Capture*.
 - **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.
- 4) Click **OK** to save the settings.

7.4 Configure Recording Schedule

Set the record schedule, and then the camera automatically starts/stops recording according to the configured schedule.

Before you start

Make sure you have installed the HDDs to the device or added the network disks before you want to store the video files, pictures and log files.



NOTE

Refer to the *Quick Start Guide* for the HDD installation.

Refer to *Chapter 7.1.2 Add the Network Disk* for network HDD connections.

- 1) Go to **Storage > Recording Schedule**.
- 2) Select a camera.

- 3) Check **Enable Schedule**.
- 4) Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion and Alarm, and Event.

Different recording types are configurable.

- **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 Event**: recording triggered by POS and alarm.
- 5) Select a day and click-and-drag the mouse on the time bar to set the record schedule.

Camera No. [D1] Camera 01

Enable Schedule

Advanced

Continuous
 Event
 Motion
 Alarm
 M | A
 M & A
 POS Event
 None

	0	2	4	6	8	10	12	14	16	18	20	22	24
Mon	Event												1
Tue	Continuous												2
Wed	Continuous												3
Thu	Continuous												4
Fri	Continuous												5
Sat	Continuous												6
Sun	Continuous												7

Copy to

Figure 7-9 Record Schedule

- 6) Repeat the above steps to schedule recording or capture for other days in the week.
- 7) Click **Apply** to save the settings.

 **NOTE**

To enable 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. Please refer to *Chapter 11 Event and Alarm Settings* and *Chapter 12 VCA Event Alarm for details*.

7.5 Configure Continuous Recording

- 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) Select **Continuous** recording type.
- 5) Set the schedule for the continuous recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.6 Configure Motion Detection Triggered Recording

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

- 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 *Chapter 11.3 Configure Motion Detection Alarm* 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 **Motion** recording type.
- 7) Set the schedule for the motion detection triggered recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.7 Configure Event Triggered Recording

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

- 1) Go to **System** > **Event**.
- 2) Configure the event detection and select the channel to trigger the recording when event occurs. Refer to *Chapter 11 Event and Alarm Settings* and *Chapter 12 VCA Event Alarm* 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 **Event** recording type.
- 7) Set the schedule for the event triggered recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.8 Configure Alarm Triggered Recording

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

- 1) Go to **System > Event > Normal Event > Alarm Input**.
- 2) Configure the alarm input and select the channels to trigger the recording when alarm occurs. Refer to *Chapter 11 Event and Alarm Settings* and *Chapter 12 VCA Event Alarm* 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 **Alarm** recording type.
- 7) Set the schedule for the alarm triggered recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.9 Configure POS Event Triggered Recording

You can configure the recording triggered by the connected POS event, such as the transaction, etc.

- 1) Go to **System > POS Settings**.
- 2) Configure the POS and select the channel(s) in the **Event Linkage** to trigger the recording when POS event occurs. Refer to *Chapter 13* 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 **POS Event** recording type.
- 7) Set the schedule for the POS event triggered recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.10 Configure Picture Capture

The picture refers to the live picture capture in continuous or event recording type.

- 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.
 - **Interval:** the interval of capturing live picture.
- 3) Go to **Storage > Capture Schedule**.
- 4) Select the camera to configure the picture capture.



Figure 7-10 Set Picture Capture Schedule

5) Set the picture capture schedule. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

7.11 Configure Holiday Recording and Capture

Purpose:

Follow the steps to configure the record or capture schedule on holiday for that year. You may want to have different plan for recording and capture on holiday.

- 1) Go to **System > Holiday Settings**.
- 2) Select a holiday item from the list and click.
- 3) Check the **Enable** to configure the holiday.

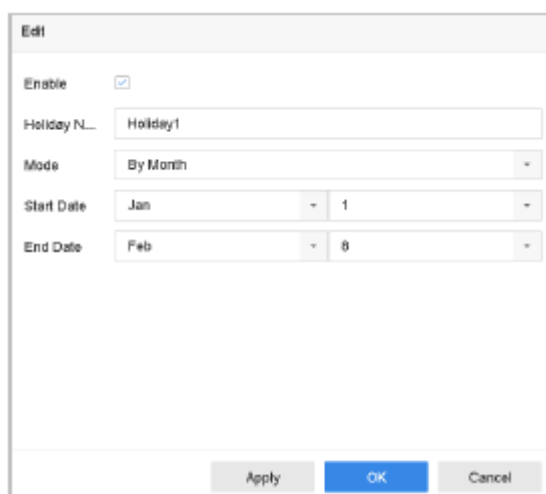


Figure 7-11 Edit Holiday Settings

- 1) Edit the holiday name.


- 2) Select the mode to by date, by week or by month.
 - 3) Set the start and end date of the holiday.
 - 4) Click **OK**.
- 4) Set the schedule for the holiday recording. Refer to *Chapter 7.4 Configure Recording Schedule* for details.

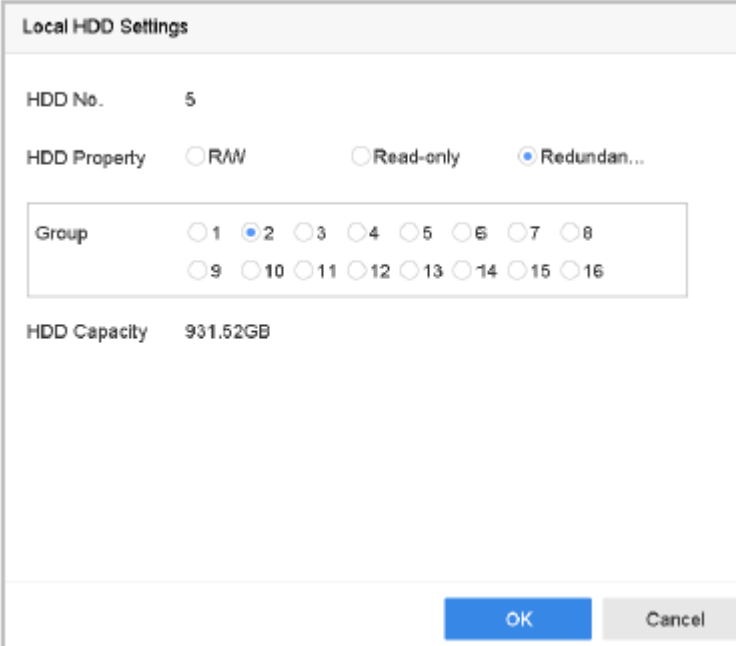
7.12 Configure Redundant Recording and Capture

Purpose:

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.

You must set the storage mode to **Group** before you set the HDD property to Redundancy. For detailed information, please refer to *Chapter 7.2.1 Configure HDD Group*. There should be at least another HDD which is in Read/Write status.

- 1) Go to **Storage > Storage Device**.
- 2) Select an **HDD** from the list and click  to enter the Local HDD Settings interface.
- 3) Set the HDD property to **Redundancy**.



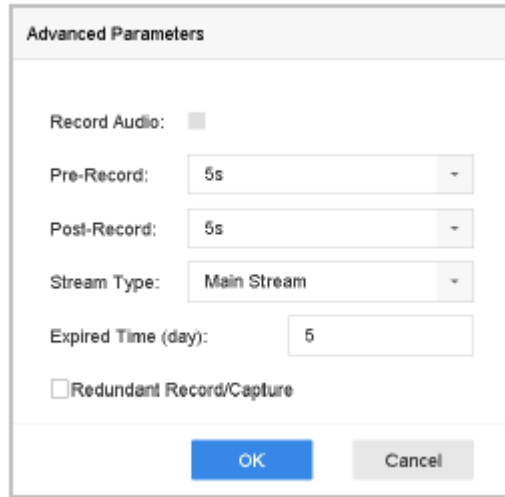
The screenshot shows a dialog box titled "Local HDD Settings". It contains the following information:

- 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

At the bottom right, there are two buttons: "OK" (highlighted in blue) and "Cancel".

Figure 7-12 HDD Property-Redundancy

- 4) Go to **Storage > Schedule Settings > Record Schedule/Capture Schedule**.
- 5) Click **Advanced** to set the camera recording parameters.



The image shows a dialog box titled "Advanced Parameters" with the following settings:

- Record Audio:
- Pre-Record: 5s (dropdown menu)
- Post-Record: 5s (dropdown menu)
- Stream Type: Main Stream (dropdown menu)
- Expired Time (day): 5 (text input)
- Redundant Record/Capture

At the bottom, there are two buttons: "OK" (blue) and "Cancel" (grey).

Figure 7-13 Record Parameters

- 6) Check the checkbox of **Redundant Record/Capture**.
- 7) Click **OK** to save settings.

Chapter 8 Disk Array

Purpose

Disk array is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit. 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", depending on what level of redundancy and performance is required.

8.1 Create Disk Array

Purpose

The device supports the disk array that is realized by software. You can enable the RAID function as required. Two ways are available for creating array: one-touch configuration and manual configuration. The following flow chart shows the process of creating array.

8.1.1 Enable RAID

Purpose

Perform the following steps to enable the disk array function.

- 1) Go to **Storage > Advanced**.

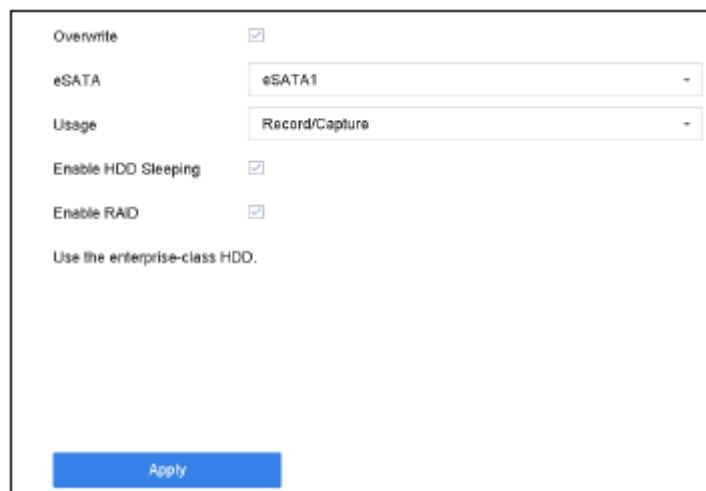


Figure 8-1 Advanced

- 2) Check **Enable RAID**.
- 3) Click **Apply**.
- 4) Reboot device to have settings take effect.

8.1.2 One-Touch Creation

Purpose

One-touch configuration helps you to quickly create the disk array. By default, the array type created by one-touch configuration is a RAID 5.

Before you start

Enable RAID function. For details, refer to *Chapter 8.1.1 Enable RAID*.

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

- 1) Go to **Storage > RAID Setup > Physical Disk**.



No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB		Normal	Functional	ST2000VX000-1CU164	<input checked="" type="checkbox"/>	None
2	2794.52GB		Normal	Functional	ST3000VX000-8YW166	<input checked="" type="checkbox"/>	None
5	1863.02GB		Normal	Functional	ST2000VX000-1CU164	<input checked="" type="checkbox"/>	None
9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	<input checked="" type="checkbox"/>	None
10	1863.02GB		Normal	Functional	ST2000VX000-1CU164	<input checked="" type="checkbox"/>	None

Figure 8-2 Physical Disk

- 2) Click **One-touch Config**.
- 3) Edit the array name in the **Array Name** text field and click **OK** to start configuring.
- 4) A message box will pop up when the array creation is completed. Click **OK**.
- 5) Optionally, the device will automatically initialize the created array. Go to **Storage > RAIDSetup > Array** view the information of the created array.

8.1.3 Manual Creation

Purpose

Manually create the array of RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10.

- 1) Go to **Storage > RAID Setup > Physical Disk**.
- 2) Click **Create**.

Table 8-1 Create Array

- 3) Enter the array name.
- 4) Select **RAID Level** as **RAID 0**, **RAID 1**, **RAID 5**, **RAID 6**, or **RAID 10**, as required.
- 5) Select the physical disks that will constitute the array.

Table 8-2 Required Number of HDD

RAID Level	Required Number of HDD
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.

- 6) Click **OK**.
- 7) Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** view the information of created array.

No	Name	Free Space	Physical Disk	Hot S...	Status	Level	Rebuild	Delete	Task
1	Array01	37253725G	1 5 10		Functional	RAID 5			Initialize (Fast)(Running) 43%

Figure 8-3 Array List

8.2 Rebuild Array

Purpose

The status of array includes Functional, Degraded and Offline. To ensure the high security and reliability

of the data stored in array, you should take immediate and proper maintenance at arrays according their status.

- **Functional:** No disk loss in the array.
- **Offline:** The number of lost disks has exceeded the limit.
- **Degraded:** If amount of HDD fail in array, the array degrades. Recovery consists of array rebuilding and involves returning the disk to the **Functional** stage.

8.2.1 Configure Hot Spare Disk

Purpose

Hot spare disks are required for disk array automatic rebuilding.

- 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	2734.52GB		Normal	Functional	ST3000VX000-9YW166	<input checked="" type="checkbox"/>	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
<input type="checkbox"/> 9	2734.52GB		Normal	Functional	ST3000VX000-1CU166	<input checked="" type="checkbox"/>	None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None

Figure 8-4 Physical Disk

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

8.2.2 Automatically Rebuild Array

Purpose

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

Before you start

Create hot spare disks. For details, refer to *Chapter 8.2.1 Configure Hot Spare Disk*.

- 1) The device will automatically rebuild the degraded arrays with the hot spare disks. Go to **Storage > RAID Setup > Array** to view rebuilding progress.

No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3726G	2 5 10		Degraded	RAID 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Rebuild(Running) 0%

Figure 8-5 Array List

8.2.3 Manually Rebuild Array

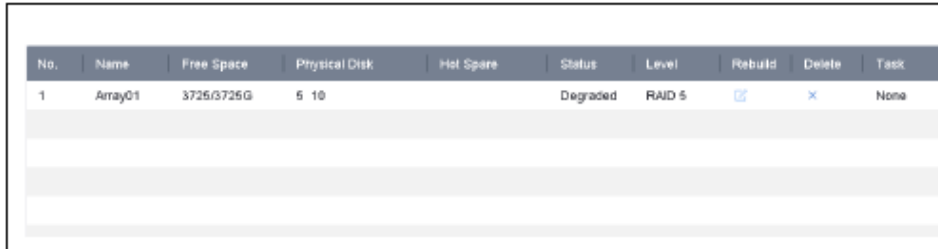
Purpose

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

Before you start

At least one available physical disk should exist for rebuilding the array.

- 1) Go to **Storage > RAID Setup > Array**.





No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3726/3726G	5 10		Degraded	RAID 5			None

Figure 8-6 Array List

- 2) Click  of the degraded array.



Rebuild Array

Array Name:

RAID Level:

Array Disk:

Physical Disk: 2 9

Figure 8-7 Rebuild Array

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

8.3 Delete Array

Deleting array will delete all the data saved in it.

- 1) Go to **Storage > RAID Setup > Array**.

No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	5 10		Degraded	RAID 5			None

Figure 8-8 Array List

2) Click of the array to delete.



Figure 8-9 Attention

3) Click **Yes** on the popup message box.

8.4 Check and Edit Firmware

Purpose

You can view the information of the firmware and set the background task speed in the Firmware interface.

1) Go to **Storage > RAID Setup > Firmware**.

Version	1.1.0.0003
Physical Disk Count	16
Array Count	16
Virtual Disk Count	0
RAID Level	0 1 5 6 10
Hot Spare Type	Global Hot Spare
Support Rebuild	Yes
Background Task Speed	Medium Speed

Figure 8-10 Firmware

2) Optionally, set the **Background Task Speed**.

3) Click **Apply**.

Chapter 9 File Management

9.1 Search and Export Human Files

9.1.1 Search Human Files

Purpose

Specify detailed conditions to search human files.

Before you start

Configure human body detection function for the cameras you want to search and export human files for.

- 1) Go to **File Management > Human File**.
- 2) Click **Show More** and specify detailed conditions, including time, camera, people appearance, etc.

Time	Custom -	2018-03-16 00:00:00	2018-03-16 23:59:59
Camera	[All] Camera -		
Age	None -	Glasses	None -
Bicycle	None -	Backpack	None -

Figure 9-1 Search Conditions

- 3) Click **Search** to display results. The matched files are displayed in thumbnail or list.
- 4) Select **Target Picture** or **Source Picture** in menu bar to display related pictures only.
- 5) Select **Video** or **Picture** to specify the file type.
 - **Target Picture:** Display the search results of people close-up.
 - **Source Picture:** Display the search results of original picture captured by camera.
 - **Group:** Sort the search results by selected item.

9.1.2 Export Human Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

- 1) Search for the human files to export. For details, see *9.1.1 Search Human Files*.
- 2) Click files and click **Export**.

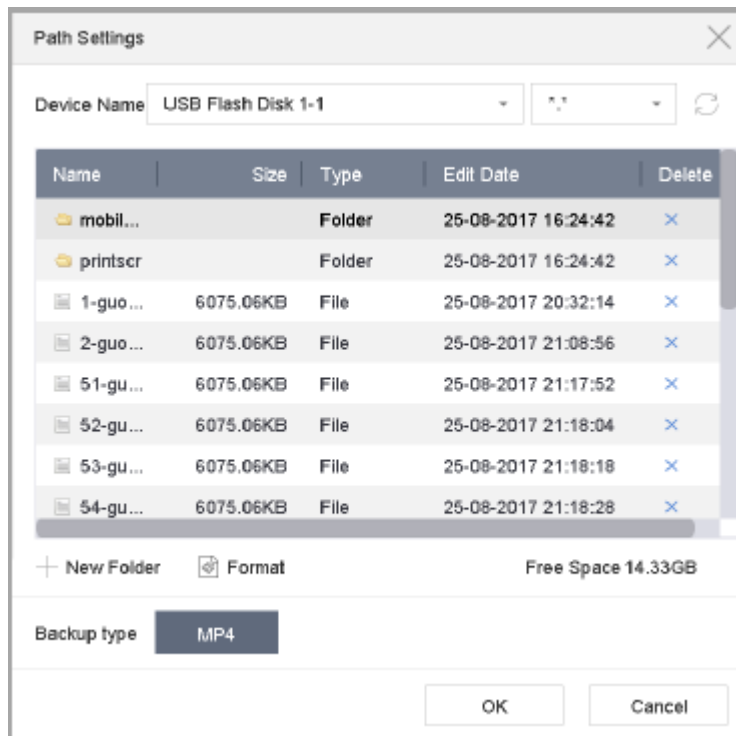


Figure 9-2 Export Files

- 3) Click **OK** to export pictures to backup device.

9.2 Search and Export Vehicle Files

9.2.1 Search Vehicle Files

Purpose

Specify detailed conditions to search vehicle files.

Before you start

Configure vehicle detection function for the cameras you want to search and export vehicle files.

- 1) Go to **File Management > Vehicle Files**.
- 2) Click **Show More** and specify detailed conditions, including time, camera, vehicle appearance, etc.

Figure 9-3 Advanced Search

- 3) Click **Search** to display results. The matched files are displayed in thumbnail or list.
- 4) Select **Target Picture** or **Source Picture** in menu bar to display related pictures only. Select **Video**

or **Picture** to specify the file type.

- **Target Picture:** Display the search results of a vehicle close-up.
- **Source Picture:** Display the search results of an original picture captured by camera.
- **Group:** Sort the search results by selected item.

9.2.2 Export Vehicle Files

Purpose

Export files for backup purposes using USB device (USB flash drive, USB HDD, USB optical disc drive), SATA optical disc drive or eSATA HDD.

- 1) Search for the vehicle files to export. For details, see *9.2.1 Search Vehicle Files*.
- 2) Click files and click **Export**.

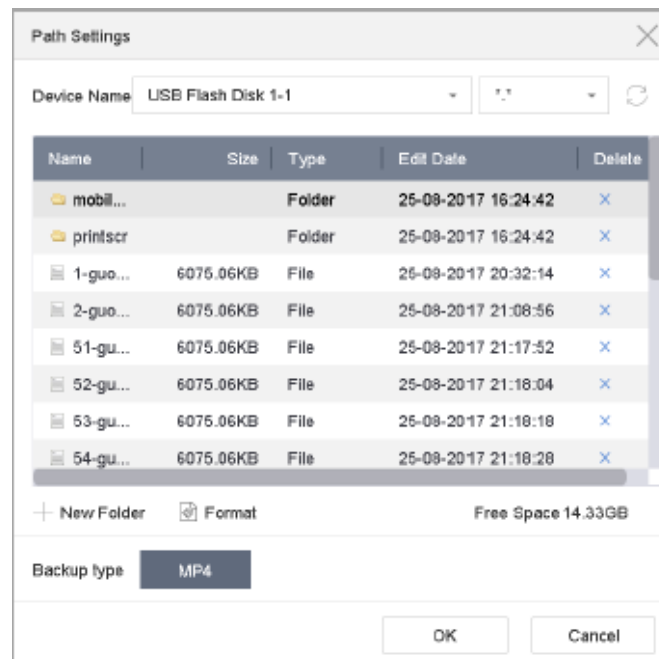


Figure 9-4 Export Files

- 3) Click **OK** to export pictures to backup device.

9.3 Search History Operation

9.3.1 Save Search Condition

Purpose:

You can save the search conditions for future reference and quick search.

- 1) Go to **File Management > All Files/Human File/Vehicle File**.
- 2) Click **Show More** and set the search conditions.

- 3) Click **Save**.
- 4) Enter a name in text field and click **Finished**. The saved search conditions will be displayed in search history list.

9.3.2 Call Search History

Purpose:

You can quickly search files by calling search history.

- 1) Go to **File Management > All Files/Human File/Vehicle File**.
- 2) Click a created search conditon to quickly search files.

Chapter 10 Playback

10.1 Playing Video Files

10.1.1 Instant Playback

Instant Playback enables the device to play the recorded video files in last five minutes. If no video is found, it means there has been no video recorded in the last five minutes.


- 1) On the live view window of the selected camera, move the cursor to the window bottom to access the toolbar.
- 2) Click  to start instant playback.



Figure 10-1 Playback Interface

10.1.2 Play Video

- 1) Go to **Playback**.
- 2) Select one or more cameras in the camera list.
- 3) Select a date in the calendar.
- 4) You can use the toolbar in the bottom part of playback interface to control the playing and realize a series of operations. Refer to *Chapter 10.2 Playback Operations*.



Figure 10-2 Playback Interface

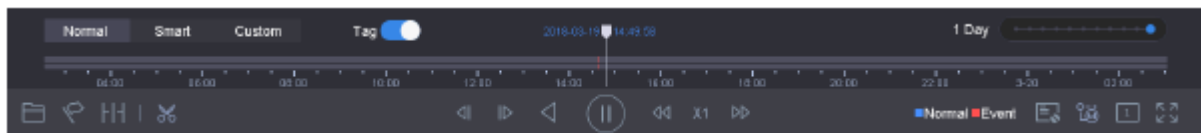


Figure 10-3 Toolbar of Playback

- 5) You can click the channel(s) to execute simultaneous playback of multiple channels. A playing speed of 256x is supported.


10.1.3 Play Tag Files

Purpose:

Video tag allows you to record related information like people and location of a certain time point during playback. You can use video tag(s) to search for video files and position time point.

Before playing back by tag:

Manage Tag Files

- 1) Go to **Playback**.
- 2) Search and play back the video files.
- 3) Click  to add the tag.
- 4) Edit the tag information.

NOTE

A maximum of 64 tags can be added to a single video file.

Play Tag Files

- 1) Go to **File Management > All Files**.

- 2) Enter the search conditions for the tag files, including the time and the tag keyword.

Figure 10-4 Tag Search

- 3) Click **Search**.

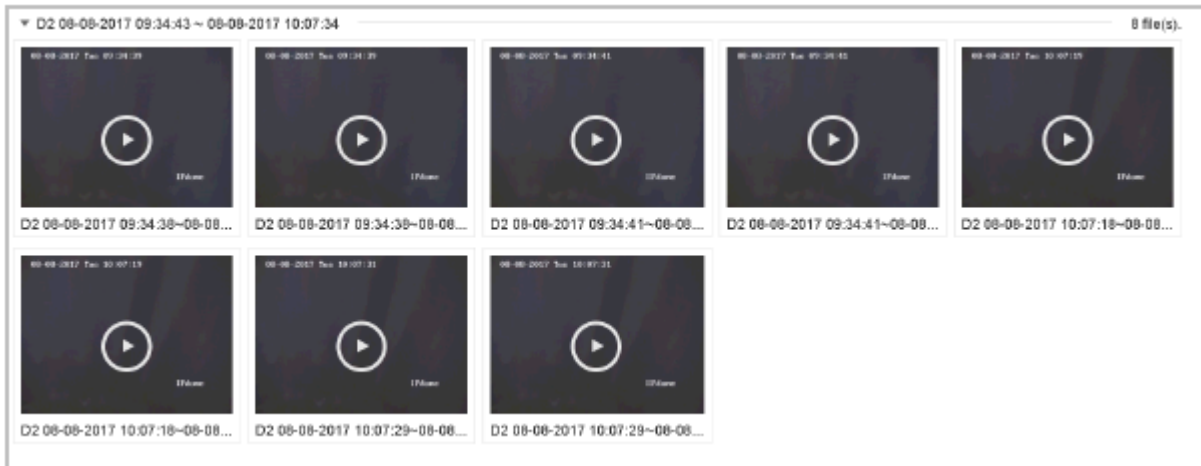


Figure 10-5 Searched Tag Files

- 4) In the search results interface, select a tag file and click to start playing the video.

10.1.4 Play by Smart Search

Purpose





In the smart playback mode, the device will analyze the video containing the motion, line or intrusion detection information, mark it with green, and play it at normal speed. A video without motion will be played at 16x speed.

The smart playback rules and areas are configurable.

- 1) Go to **Playback**.
- 2) Start playing the video files by channel or by time.
- 3) From the toolbar at the bottom of the playing window, click the **motion/line crossing/ intrusion** icon for search.



Figure 10-6 Playback by Smart Search

- 4) Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.
- Line Crossing Detection
 - 1) Click the  icon.
 - 2) Click on the image to specify the start point and end point of the line.
 - Intrusion Detection
 - 1) Click the  icon.
 - 2) Specify four points to set a quadrilateral region for intrusion detection. Only one region can be set.
 - Motion Detection
 - 1) Click the  icon.
 - 2) Hold the mouse on the image to draw the detection area manually.
 - 3) Click Search  to search for the matched video and start playing it.

10.1.5 Play Event Files

Purpose

Play back video files on one or several channels searched by event type (e.g., alarm input, motion detection, line crossing detection, vehicle detection, etc.).

- 1) Go to **Playback**.
- 2) Click **Custom Search** on the left bottom to enter the Search Condition interface.
- 3) Enter the search conditions for the event files, e.g., time, event type, file status, people appearance (for human detection), vehicle information (for vehicle detection event).

The screenshot displays a search condition interface with the following fields and options:

Time	Custom	2018-03-19 00:00:00	2018-03-19 23:59:59
Tag		File Status	All
Event Type	None		
Tops Color	None	Glasses	None
Bicycle	None	Backpack	None
Parent Brand	None	Plate No.	
Vehicle Color	None	Vehicle Mode	None
Area/Country	None		

At the bottom right of the interface, there is a button labeled "Hide" with an upward-pointing arrow.

Figure 10-7 Search Conditions

- 4) Click **Search**.
- 5) On the search results interface, select an event video file/picture file and click to start playing the video or double click to play the picture.

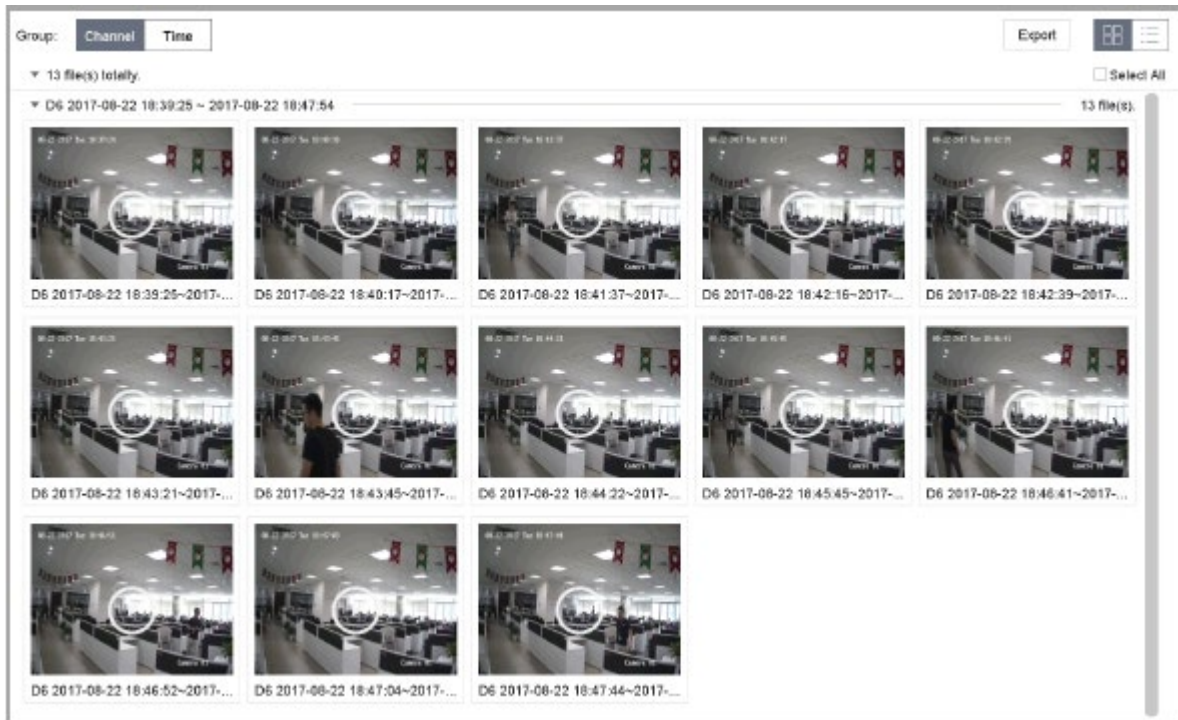




Figure 10-8 Event Files

6) Click  or  to select the previous or next event.

**NOTE**

Refer to *Chapter 11 Event and Alarm Settings* and *Chapter 12 VCA Event Alarm* for details for event and alarm settings.

Refer to *Chapter 7.7 Configure Event Triggered Recording* for the event triggered recording/capture settings.

10.1.7 Play by Sub-periods

Purpose:

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

- 1) Go to **Playback**.
- 2) Select **Sub-periods** from the drop-down list in the upper-left corner of the page to enter the Sub-periods Playback interface.
- 3) Select a date and start playing the video file. Select the Split-screen Number from the dropdown list. Up to 16 screens are configurable.

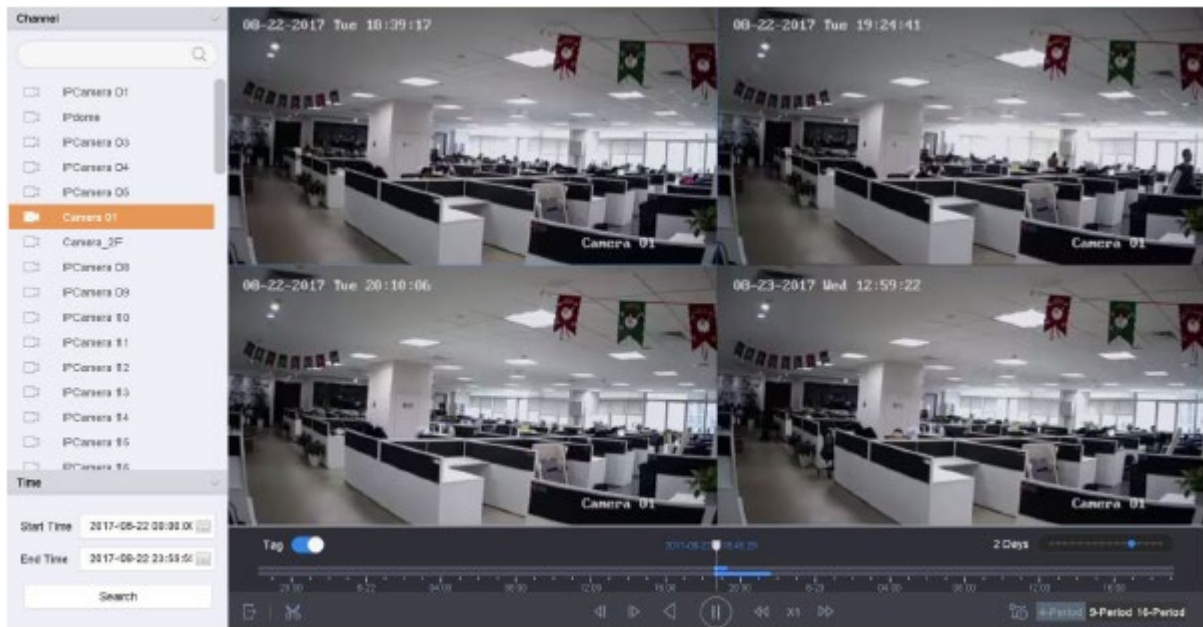


Figure 10-9 Interface of Sub-periods Playback

**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.

10.1.8 Play Log Files

Purpose:

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

- 1) Go to **Maintenance > Log Information**.
- 2) Click **Log Search** tab to enter Playback by System Logs.
- 3) Set search time and type and click **Search**.

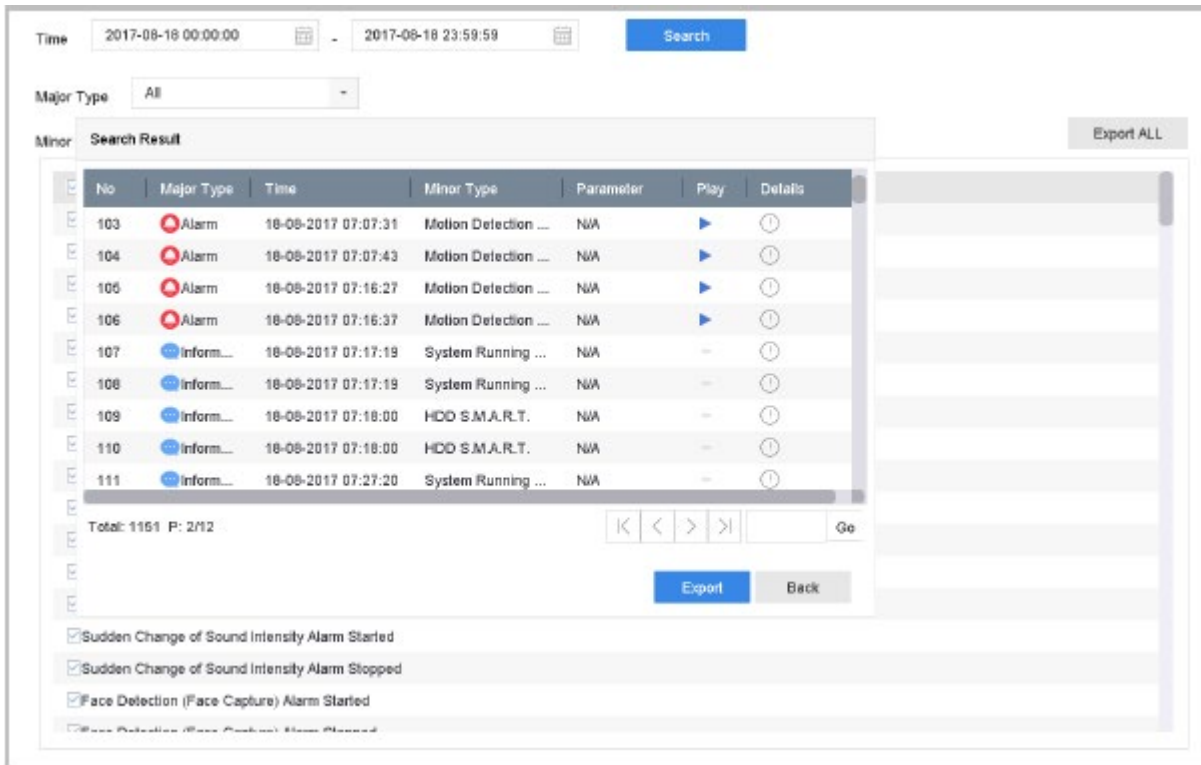



Figure 10-10 System Log Search Interface

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

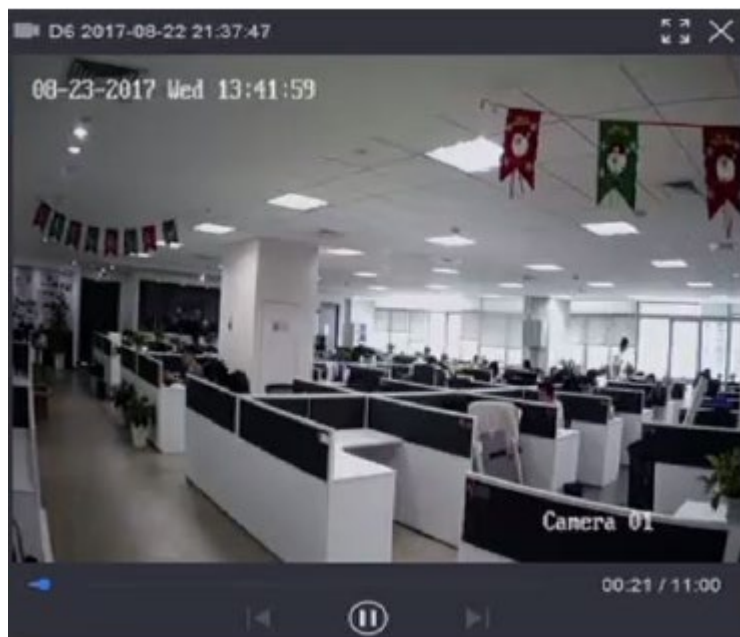


Figure 10-11 Interface of Playback by Log



10.1.9 Play External File

Purpose:

You can play files from the external storage devices.

Before You Start:

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

- 1) Go to **Playback**.
- 2) Click the  icon at the left bottom corner.
- 3) Select and click the  button or double click to play the file.

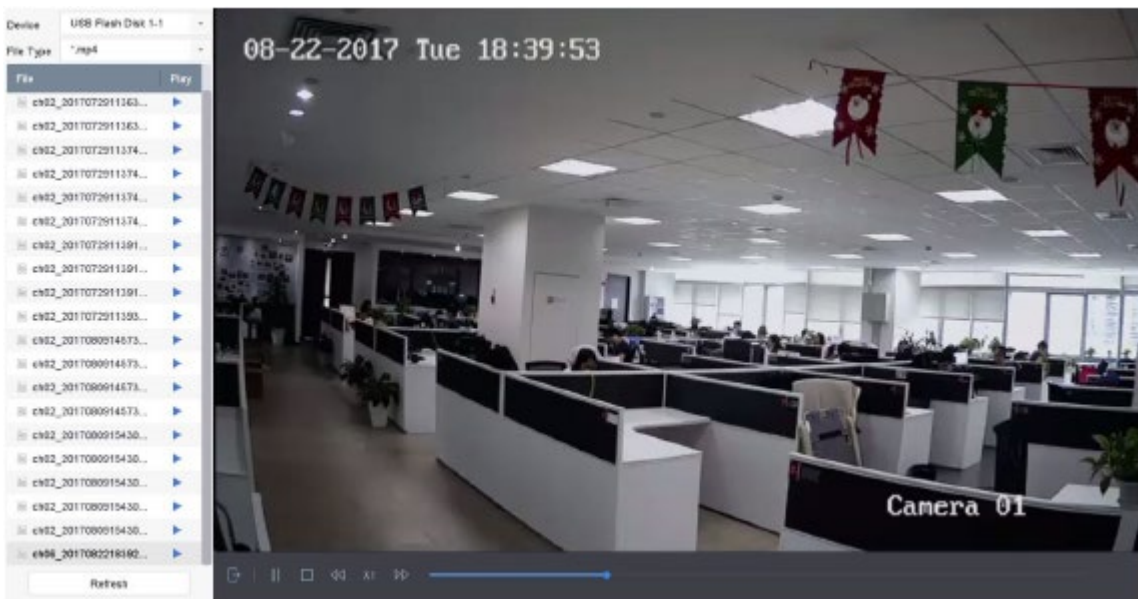


Figure 10-12 External File Playback

10.2 Playback Operations

10.2.1 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.

10.2.2 Set Play Strategy in Important/Custom Mode

Purpose:

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

In the Important/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 important (event) video and the custom (searched video) only at normal speed (x1).
- When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video and the important/custom video separately. The speed range is from x1 to xMAX.

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

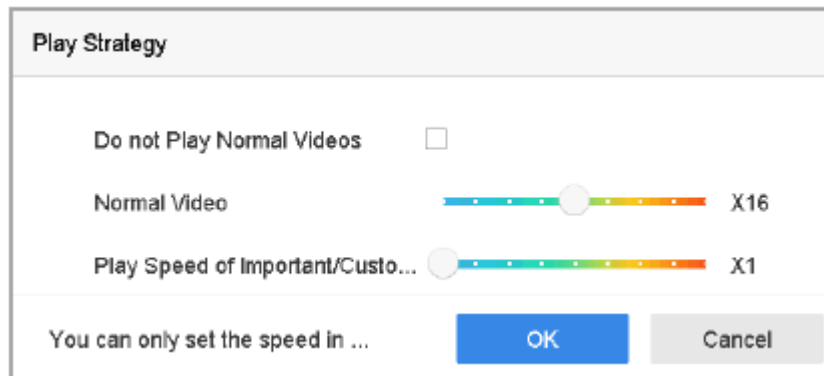




Figure 10-13 Play Strategy

10.2.3 Edit Video Clips



You can take video clips during the playback and export the clips.

In the video playback mode, click  to start video clipping operation.

- : set the start time and end time of the video clip.
- : export the video clips to the local storage device.

10.2.4 Switch between Main Stream and Sub-Stream

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

- : 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**.

10.2.5 Thumbnails View

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

In the video playback mode, move the mouse to the time bar to get the preview thumbnails of the video files.



Figure 10-14 Thumbnails View

You can select and double click on a required thumbnail to enter full-screen playback.

The thumbnail view is supported only in the 1x single-camera playback mode.

10.2.6 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

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

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



NOTE

The fast view is supported only in 1x single-camera playback mode.

10.2.7 Digital Zoom

In the video playback mode, click from the toolbar to enter the digital zoom interface.

You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to 16x).



Figure 10-15 Digital Zoom

Chapter 11 Event and Alarm Settings

11.1 Configure Arming Schedule

- 1) Select the **Arming Schedule** tab.
- 2) Choose one day of a week and set the time segment. Up to eight time periods can be set within each day.

Time periods cannot be repeated or overlapped.

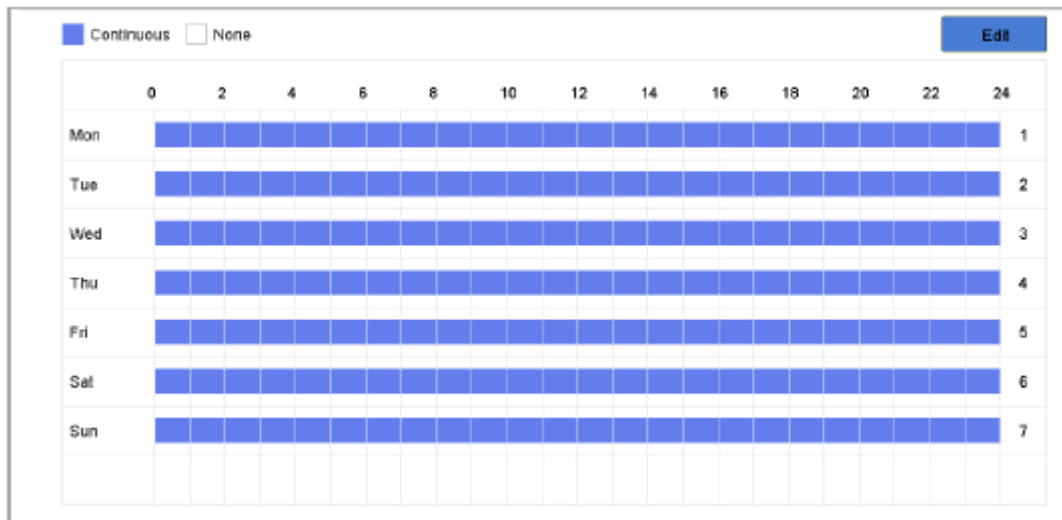



Figure 11-1 Set Arming Schedule

- 3) (Optional) If you want to copy the same arming schedule of the current day to the other day(s) of the week or holiday, you can click the  icon to copy arming schedule settings.
- 4) Click **Apply** to save the settings.

11.2 Configure Alarm Linkage Actions

Purpose:

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 E-mail.

- 1) Click **Linkage Action** to set the alarm linkage actions.

Area Arming Schedule <u>Linkage Action</u>		
<input checked="" type="checkbox"/> Normal Linkage	<input checked="" type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Channel
<input checked="" type="checkbox"/> Full Screen Monitoring	<input checked="" type="checkbox"/> Local->1	<input type="checkbox"/> D1
<input checked="" type="checkbox"/> Audible Warning	<input checked="" type="checkbox"/> Local->2	<input checked="" type="checkbox"/> D2
<input checked="" type="checkbox"/> Notify Surveillance Center	<input checked="" type="checkbox"/> Local->3	
<input checked="" type="checkbox"/> Send Email	<input checked="" type="checkbox"/> Local->4	
	<input checked="" 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.

Apply

Figure 11-2 Set Linkage Actions

- 2) Select the normal linkage actions, trigger alarm output or trigger recording channel. For details, refer to Chapter 11.2.1 to 11.2.6 .
- 3) Click **Apply** to save the settings.

11.2.1 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.

- 1) Go to **System > Live View > General**.
- 2) Set the event output and dwell time.
 - **Event Output:** Select the output to show event video.
 - **Full Screen Monitoring Dwell Time:** Set the time in seconds to show 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, etc.)
- 4) Select the **Full Screen Monitoring** alarm linkage action.
- 5) Select the channel(s) in **Trigger Channel** settings you want to make full screen monitoring.



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

11.2.2 Configure Audio Warning

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

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

11.2.3 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).

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

11.2.4 Configure E-mail Linkage

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

Please refer to *Chapter 16.7 Configure E-mail* for details of E-mail configuration.

- 1) Go to **System > Network > Advanced**.
- 2) Configure the E-mail settings.
- 3) Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, etc.)
- 4) Select the **Send E-mail** alarm linkage action.

11.2.5 Trigger Alarm Output

The alarm output can be triggered by the alarm input, motion detection, video tampering detection, line crossing detection, and all other events.

- 1) Go to the **Linkage Action** interface of the alarm input or event detection (e.g., motion detection,

line crossing detection, intrusion detection, etc.)

- 2) Click the **Trigger Alarm Output** tab.
- 3) Select the alarm output(s) to trigger.
- 4) Go to **System > Event > Normal Event > Alarm Output**.
- 5) Select an alarm output item from the list.



Refer to *Chapter 11.6.3 Configure Alarm Output* for the alarm output settings.

11.2.6 Configure PTZ Linkage

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

- 1) Go to the **Linkage Action** interface of the alarm input or VCA detection (e.g., 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 number to call when the alarm events occur. Only one PTZ type can be set per linkage action at a time.

Figure 11-3 PTZ Linkage

11.3 Configure Motion Detection Alarm

The motion detection enables the device to detect the moving objects in the monitoring area and trigger the alarm.

- 1) Go to **System > Event > Normal Event > Motion Detection**.

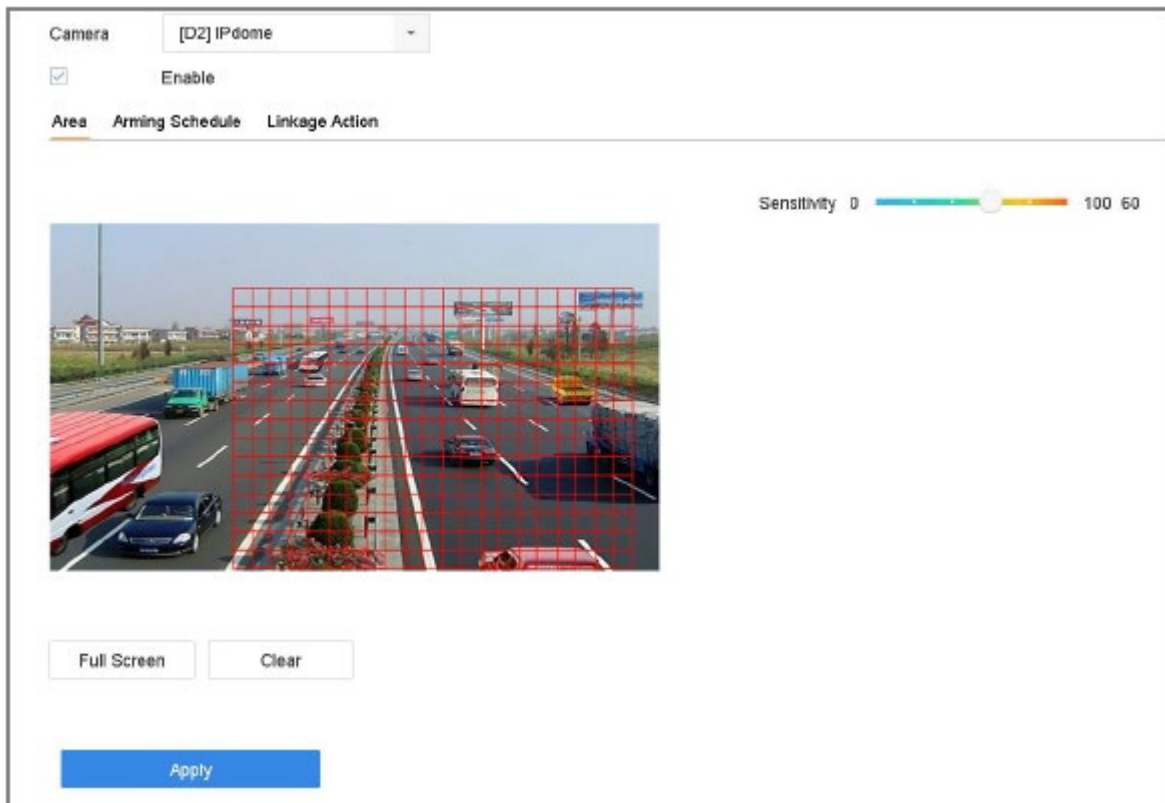


Figure 11-4 Set Motion Detection

- 2) Select the camera to configure the motion detection.
- 3) Check **Enable**.
- 4) Set the motion detection area.
 - **Full screen:** click to set the full-screen motion detection for the image.
 - **Customized area:** use the mouse to click and drag on the preview screen to draw the customized motion detection area(s).

NOTE

You can click **Clear** to clear the current motion detection area settings and draw again.

- 5) Set sensitivity (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the motion detection.
- 6) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 7) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

11.4 Configure Video Loss Alarm

Purpose

Video loss detection detects video loss on a channel and allows for appropriate alarm response action(s) to be taken.

- 1) Go to **System > Event > Normal Event > Video Loss**

Camera: [D1] IPCamera 01

Enable

Arming Schedule Linkage Action

Continuous None Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon	█	█	█	█	█	█	█	█	█	█	█	█	█	1
Tue	█	█	█	█	█	█	█	█	█	█	█	█	█	2
Wed	█	█	█	█	█	█	█	█	█	█	█	█	█	3
Thu	█	█	█	█	█	█	█	█	█	█	█	█	█	4
Fri	█	█	█	█	█	█	█	█	█	█	█	█	█	5
Sat	█	█	█	█	█	█	█	█	█	█	█	█	█	6
Sun	█	█	█	█	█	█	█	█	█	█	█	█	█	7

Apply

Figure 11-5 Set Video Loss Detection

- 2) Select the camera to configure the video loss detection.
- 3) Check **Enable**.
- 4) Set the arming schedule. *Refer to Chapter 11.1 Configure Arming Schedule.*
- 5) Set the linkage actions. *Refer to Chapter 11.2 Configure Alarm Linkage Actions.*

11.5 Configure Video Tampering Alarm

Purpose:

The video tampering detection enables to trigger alarm when the camera lens is covered and take alarm response action(s).

- 1) Go to **System > Event > Normal Event > Video Tampering**.
- 2) Select the camera to configure video tampering detection.

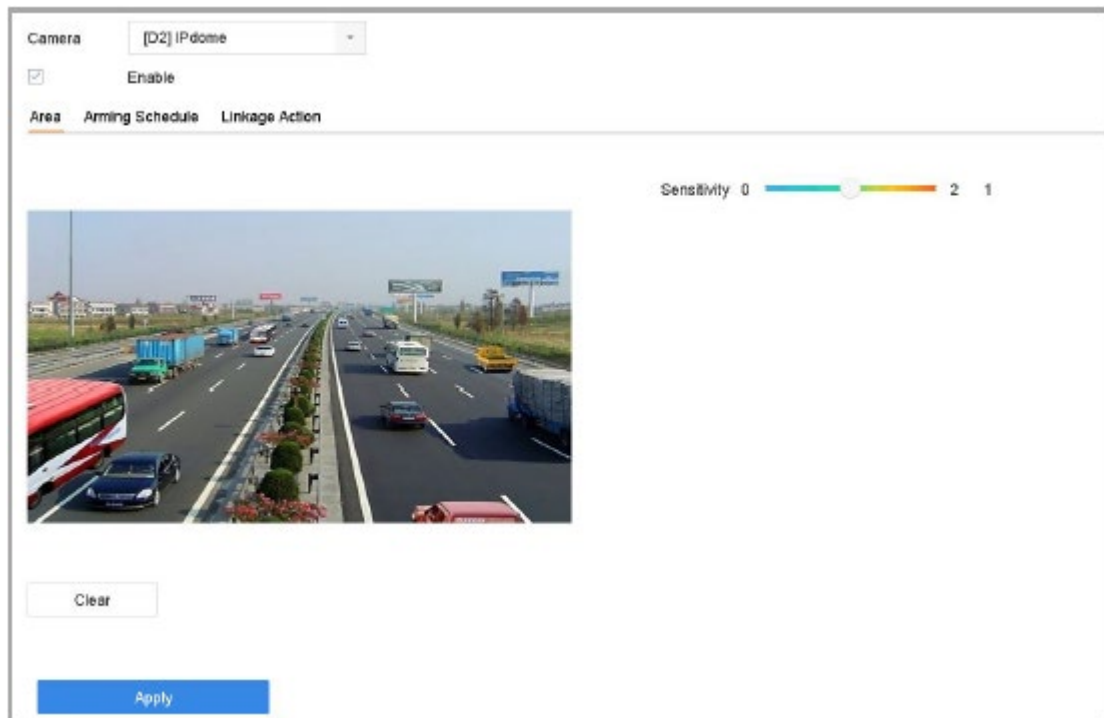


Figure 11-6 Set Video Tampering Setting


- 3) Check **Enable**.
- 4) Set the video tampering area. Use the mouse to click and drag on the preview screen to draw the customized video tampering area.
You can click **Clear** to clear the current area settings and draw again.
- 5) Set sensitivity level (0-2). 3 levels are available. The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the video tampering detection.
- 6) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 7) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

11.6 Configure Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

11.6.1 Configure Alarm Input

- 1) Go to **System > Event > Normal Event > Alarm Input**
- 2) Select an alarm input item from the list and click .

The screenshot shows the 'Edit' window for an alarm input. At the top, there are two dropdown menus: 'Alarm Input No.' set to 'Local-1' and 'Type' set to 'N.O.'. Below these is a text field for 'Alarm Name' containing the letter 'A'. Under the 'Settings' section, three radio buttons are visible: 'Nonuse', 'Input', and 'One-Key Disarming', with the latter being selected. A large rectangular area below contains a 'Normal Linkage' section with a header and several checked checkboxes: 'Full Screen Monitor...', 'Audible Warning', 'Notify Surveillance ...', 'Trigger Alarm Output', and 'Send Email'. At the bottom right of the window, there are two buttons: 'Copy to' and 'Apply'.

Figure 11-7 Alarm Input

- 3) Select the alarm input type to **N.C** or **N.O**.
- 4) Edit the alarm name.
- 5) Check the radio button of **Input**.
- 6) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 7) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 8) Click **Apply** and follow the message box to reboot device to take effect the settings.

11.6.2 Configure One-Key Disarming

One-key disarming enables the device to disarm an alarm input by one-key operation.

- 1) Go to **System > Event > Normal Event > Alarm Input**
- 2) Select the alarm input1 item from the list and click.
- 3) Change the alarm input type to **N.C** or **N.O**.
- 4) Edit the alarm name.
- 5) Check the **Enable One-Key Disarming** radio button.

The screenshot shows a software window titled "Edit" with a close button in the top right corner. Inside the window, there are several fields and a settings section. At the top, "Alarm Input No." is set to "Local-1" and "Type" is set to "N.O.". Below that, "Alarm Name" is set to "A". Under the "Settings" section, there are three radio buttons: "Nonuse", "Input", and "One-Key Dis...", with "One-Key Dis..." being selected. A large rectangular area contains a "Normal Linkage" section with five checked checkboxes: "Full Screen Monitori...", "Audible Warning", "Notify Surveillance ...", "Trigger Alarm Output", and "Send Email". At the bottom right of the window, there are two buttons: "Copy to" and "Apply".

Figure 11-8 One-Key Alarm Disarming

- 6) Select the alarm linkage action(s) you want to disarm for local alarm input 1.


NOTE

When the alarm input 1 (Local-1) is enabled with one-key disarming, the other alarm input settings are not configurable.

- 7) Click **Apply** to save the settings.

11.6.3 Configure Alarm Output

Trigger an alarm output when an alarm is triggered.

- 1) Go to **System > Event > Normal Event > Alarm Output**.
- 2) Select an alarm output item from the list and click .
- 3) Edit the alarm name.
- 4) Select the dwell time (the alarm duration) from 5s to 600s, or **Manually Clear**.
- 4) **Manually Clear**: you should manually clear the alarm when the alarm occurs. Refer to *Chapter 11.8 Trigger or Clear Alarm Output Manually* for detailed instructions.
- 5) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.

Edit

Alarm Output No. Local->1 Dwell Time 5s

Alarm Name B01 Alarm Status Enable

Arming Schedule

Continuous None Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon	█	█	█	█	█	█	█	█	█	█	█	█	█	1
Tue	█	█	█	█	█	█	█	█	█	█	█	█	█	2
Wed	█	█	█	█	█	█	█	█	█	█	█	█	█	3
Thu	█	█	█	█	█	█	█	█	█	█	█	█	█	4
Fri	█	█	█	█	█	█	█	█	█	█	█	█	█	5
Sat	█	█	█	█	█	█	█	█	█	█	█	█	█	6
Sun	█	█	█	█	█	█	█	█	█	█	█	█	█	7


Clear Copy Apply

Figure 11-9 Alarm Output

6) (Optional) You can click **Copy** to copy the same settings to other alarm output (s).

11.7 Configure Exceptions Alarm

The exception events can be configured to take the event hint in the live view window, trigger alarm output and linkage actions.

- 1) Go to **System > Event > Normal Event > Exception**.
- 2) (Optional) Enable the event hint if you want to display the event hint in the live view window.
 - 1) Check the checkbox of **Enable Event Hint**.
 - 2) Click  to select the exception type(s) and take an event hint.

Event Hint Settings

All

HDD Full

HDD Error

Network Disconnected

IP Conflicted

Illegal Login

Video Signal Loss

Alarm Input Triggered

Video Tamper Detected

OK Cancel

Figure 11-10 Event Hint Settings

3) Select the exception type from the drop-down list to set the linkage actions.

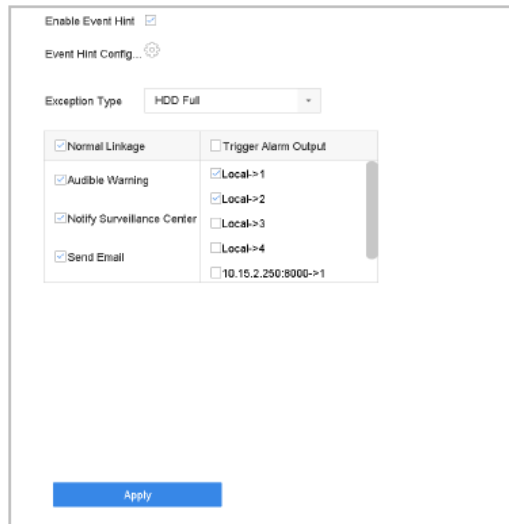


Figure 11-11 Exceptions Handling

4) Set the normal linkage and alarm output triggering. Refer to Chapter 10.2 Setting Alarm Linkage Actions.

11.8 Trigger or Clear Alarm Output Manually

Purpose:

Sensor alarm can be triggered or cleared manually. When the **Manually Clear** is selected for the dwell time of an alarm output, the alarm can be cleared only by clicking the **Clear** button.

- 1) Go to **System > Event > Normal Event > Alarm Output**.
- 2) Select the alarm output you want to trigger or clear.
- 3) Click **Trigger/Clear** to trigger or clear an alarm output.

Edit
✕

Alarm Output No.

Alarm Name

Dwell Time

Alarm Status

Arming Schedule

Continuous
 None
 Edit

	0	2	4	6	8	10	12	14	16	18	20	22	24	
Mon														1
Tue														2
Wed														3
Thu														4
Fri														5
Sat														6
Sun														7

Clear
Copy
Apply

Figure 11-12 Alarm Output

Chapter 12 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.



VCA detections must be supported by the connected IP camera.

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

12.1 Human Body Detection

Human body detection is used to detect human bodies that appear in the monitoring scene, and capture human body pictures.

This feature is available only when the connected camera supports human body detection.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Human Body**.
- 3) Select the camera to configure the human body detection.
- 4) Check **Save VCA Picture** to save the captured pictures of human body detection.
- 5) Check **Target of Interest (Human Body)** to discard non-human body pictures and videos which are not triggered by human body detection.
- 6) Set detection area.
 - 1) Select the detection area to configure from the **Area** drop-down list. Up to 8 detection areas are selectable.
 - 2) Check the checkbox of **Enable Area** to enable the selected detection area.
 - 3) Edit the area name in the **Scene Name**. The scene name can contain up to 32 characters.

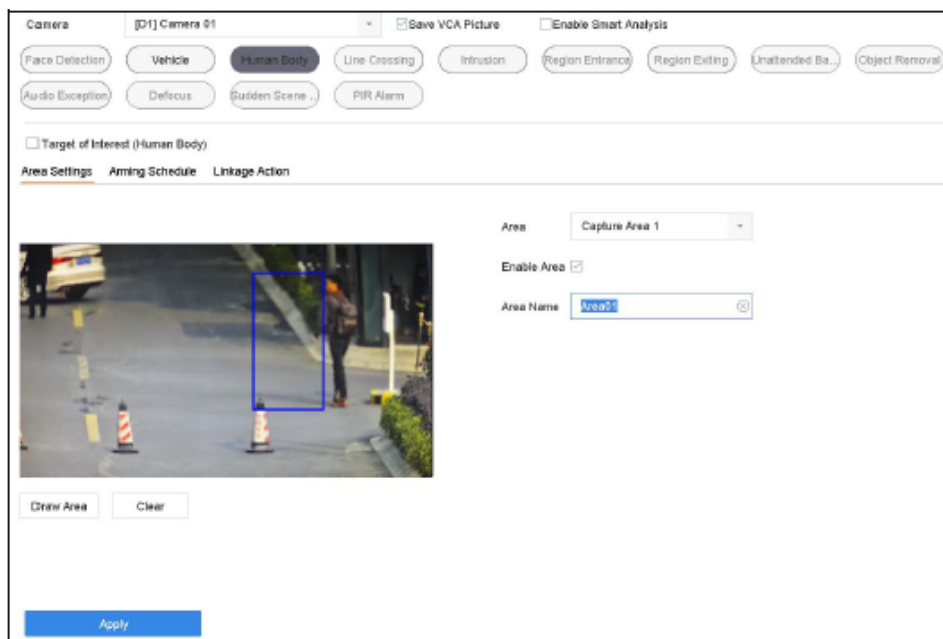


Figure 12-1 Human Body Detection

- 4) Click **Draw Area** to draw a quadrilateral in the preview window and then click **Stop Drawing**.



You can click Clear to clear the existing virtual line and re-draw it.

- 7) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 8) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 9) Click **Apply** to activate the settings.

12.2 Vehicle Detection

Purpose

Vehicle Detection is available for road traffic monitoring. In Vehicle Detection, the passed vehicle can be detected and the picture of its license plate can be captured. You can send alarm signal to notify the surveillance center and upload the captured picture to a FTP server.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Vehicle**.

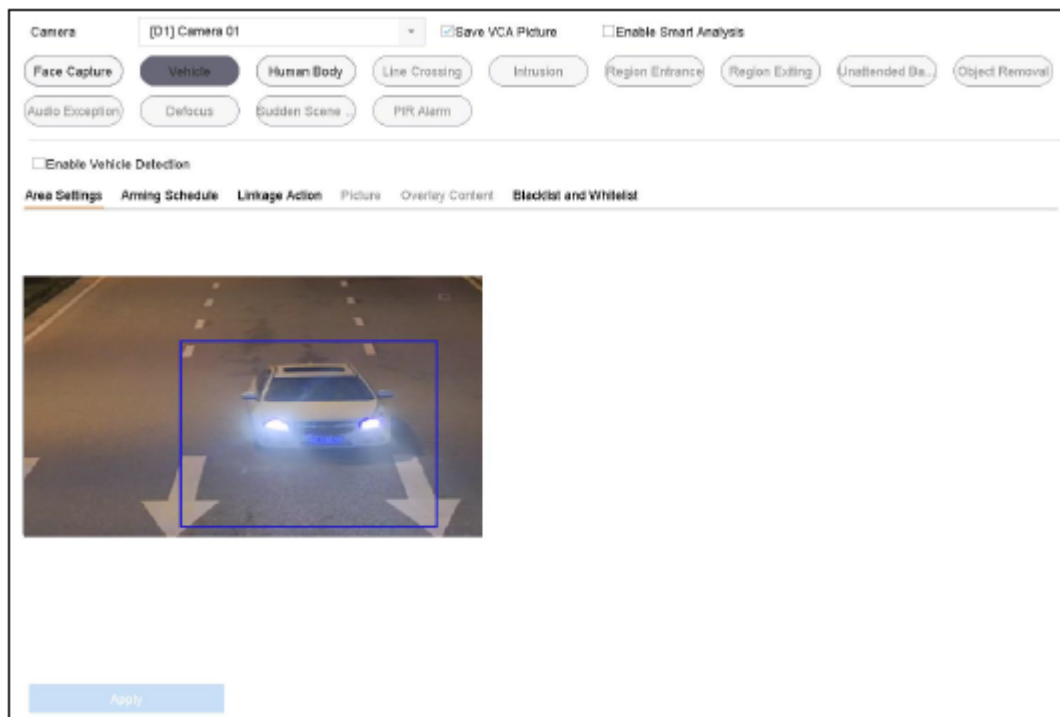


Figure 12-3 Vehicle Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Vehicle Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of vehicle detection.
- 6) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 7) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 8) Configure rules, including **Area Settings**, **Picture**, **Overlay Content**, and **Blacklist and Whitelist**.
Area Settings: Up to 4 lanes are selectable.

9) Click **Save**.

12.3 Line Crossing Detection

Purpose

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

- 1) Go to **System > Event > Smart Event**.
- 2) Click *Line Crossing*.

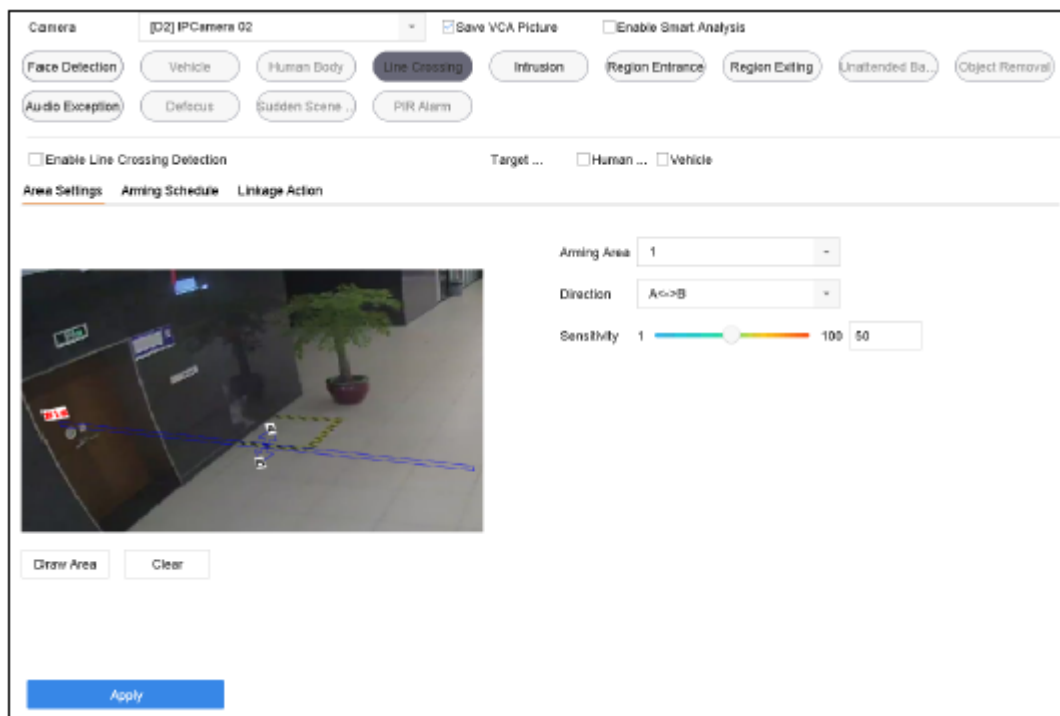


Figure 12-4 Line Crossing Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Line Crossing Detection** checkbox.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of line crossing detection.
- 6) Select Target Detection as Human Body or Vehicle.
 - **Human Body:** Discard non-human body pictures and videos which are not triggered by line crossing detection.
 - **Vehicle:** Discard non-vehicle pictures and videos which are not triggered by line crossing detection.
- 7) Follow the steps to set the line crossing detection rules and detection areas.
 - 1) Select an Arming Region to configure. Up to 4 arming regions are selectable.
 - 2) Select the Direction as A<->B, A->B, or A<-B.
 - **A<->B:** Only the arrow on the B side shows. When an object goes across the configured line with both direction can be detected and alarms are triggered.

- **A->B:** Only the object crossing the configured line from the A side to the B side can be detected.
 - **B->A:** Only the object crossing the configured line from the B side to the A side can be detected.
- 3) Drag the Sensitivity slider to set the detection sensitivity. Sensitivity range: sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
 - 4) Click **Draw Region** and set two points in the preview window to draw a virtual line.
- 8) Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger line crossing detection.
- 1) Click **Max. Size/Min. Size**.
 - 2) Draw an area in the preview window.
 - 3) Click **Stop Drawing**.
- 9) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 10) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 11) Click **Apply**.

12.4 Intrusion Detection

Purpose

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Intrusion**.

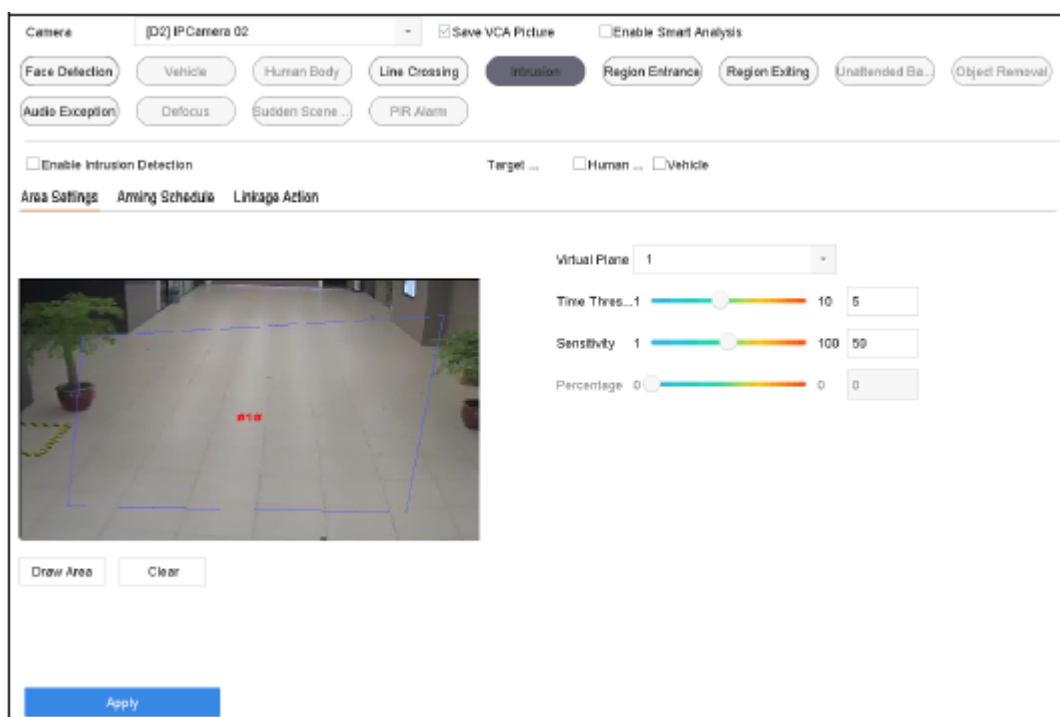


Figure 12-5 Intrusion Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Intrusion Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured intrusion detection pictures.
- 6) Select **Target Detection** as **Human Body** or **Vehicle**.
 - **Human Body:** Discard non-human body pictures and videos which are not triggered by intrusion detection.
 - **Vehicle:** Discard non-vehicle pictures and videos which are not triggered by intrusion detection.
- 7) Follow the steps to set the detection rules and detection areas.
 - 1) Select a Virtual Panel to configure. Up to 4 virtual panels are selectable.
 - 2) Drag the sliders to set **Time Threshold**, **Sensitivity**, and **Percentage**.
 - **Time Threshold:** The threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the threshold, device will trigger an alarm. Its range is [1s-10s].
 - **Sensitivity:** The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered. Its range is [1-100].
 - **Percentage:** The ratio of the in-region part of the object that can trigger the alarm. For example, if the percentage is 50%, when the object enters the region and occupies half of the whole region, device will trigger an alarm. Its range is [1-100].
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
- 8) Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger intrusion detection.
 - 1) Click **Max. Size/Min. Size**.
 - 2) Draw an area in the preview window.
 - 3) Click **Stop Drawing**.
- 9) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 10) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 11) Click **Apply**.

12.5 Region Entrance Detection

Purpose

Region entrance detection function detects objects that enter a pre-defined virtual region from the outside.

- 1) Go to **System Management > Event Settings > Smart Event**.

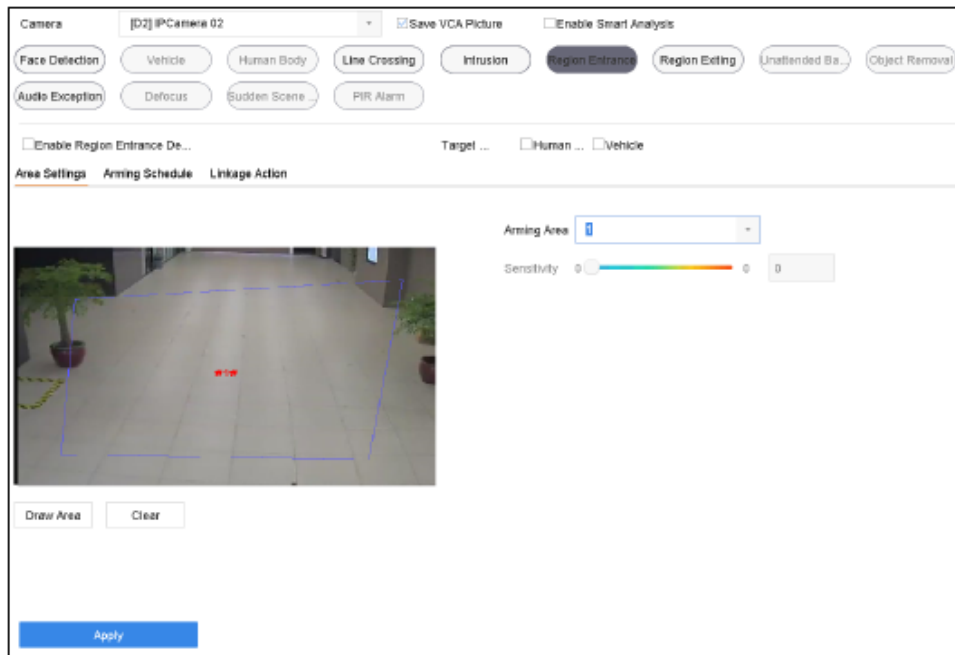
2) Click **Region Entrance Detection**.

Figure 12-6 Region Entrance Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Region Entrance Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of region entrance detection.
- 6) Select Target Detection as Human Body or Vehicle.
 - **Human Body:** Discard non-human body pictures and videos which are not triggered by region entrance detection.
 - **Vehicle:** Discard non-vehicle pictures and videos which are not triggered by region entrance detection.
- 7) Follow the steps to set the detection rules and detection areas.
 - 1) Select an Arming Region to configure. Up to 4 regions are selectable.
 - 2) Drag the sliders to set Sensitivity.
 - **Sensitivity:** The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
- 8) Configure Arming Schedule and Linkage Action.
- 9) Click **Apply**.

12.6 Region Exiting Detection

Purpose

Region exiting detection function detects objects that exit from a pre-defined virtual region.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Region Exiting**.

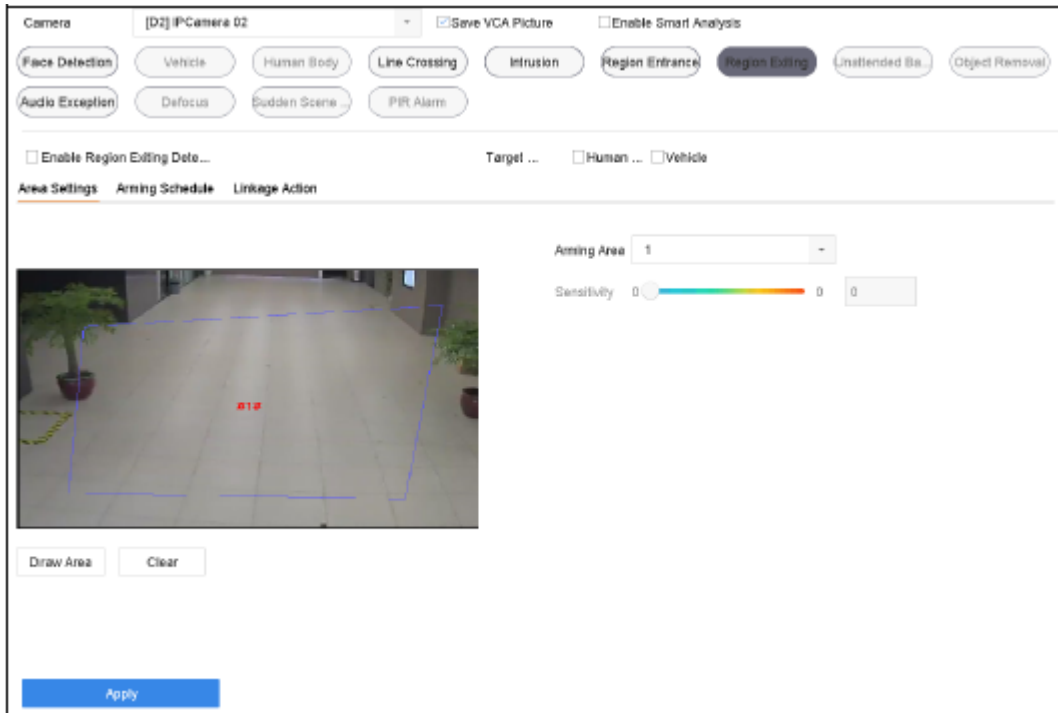


Figure 12-7 Region Exiting Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Region Exiting Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of region exiting detection.
- 6) Select **Target Detection** as **Human Body** or **Vehicle**.
 - **Human Body:** Discard non-human body pictures and videos which are not triggered by region exiting detection.
 - **Vehicle:** Discard non-vehicle pictures and videos which are not triggered by region exiting detection.
- 7) Follow the steps to set the detection rules and detection areas.
 - 1) Select an Arming Region to configure. Up to 4 regions are selectable.
 - 2) Drag the sliders to set Sensitivity.
 - **Sensitivity:** The higher the value is, the more easily the detection alarm can be triggered. Its range is [0-100].
 - 3) Click Draw Region and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
- 8) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 9) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 10) Click **Apply**.

12.7 Unattended Baggage Detection

Purpose

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

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Unattended Baggage**.

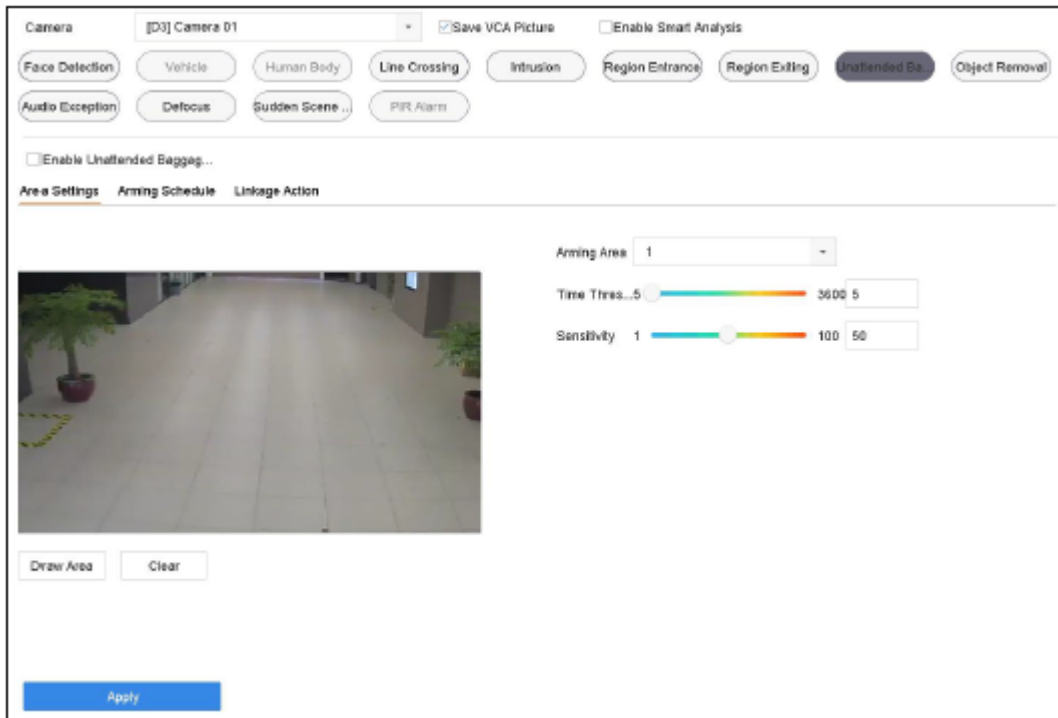


Figure 12-8 Unattended Baggage Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Unattended Baggage Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of unattended baggage detection.
- 6) Follow the steps to set the detection rules and detection areas.
 - 1) Select an **Arming Region** to configure. Up to 4 regions are selectable.
 - 2) Drag the sliders to set **Time Threshold** and **Sensitivity**.
 - **Time Threshold:** The time of the objects left over in the region. If the value is 10, alarm is triggered after the object is left and stayed in the region for 10s. Its range is [5s-20s].
 - **Sensitivity:** Similarity degree of the background image. The higher the value is, the more easily the detection alarm can be triggered.
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
- 7) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 8) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

9) Click **Apply**.

12.8 Object Removal Detection

Purpose

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Object Removable**.

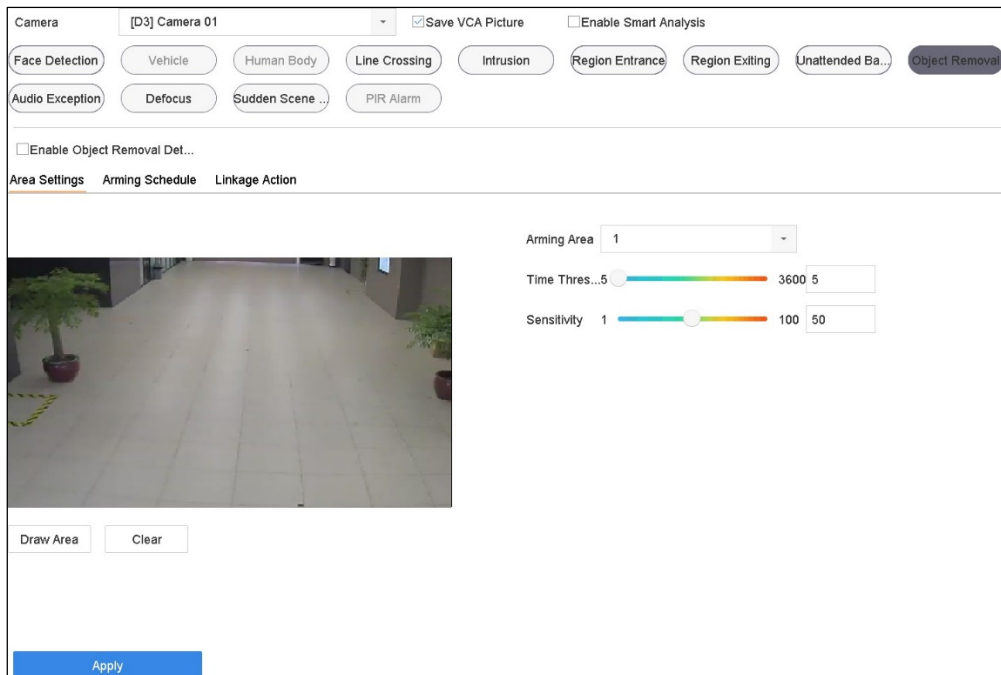


Figure 12-9 Object Removal Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Object Removable Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of object removable detection.
- 6) Follow the steps to set the detection rules and detection areas.
 - 1) Select an **Arming Region** to configure. Up to 4 regions 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 is triggered after the object disappeared from the region for 10s. Its range is [5s-20s].
 - **Sensitivity:** The similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
- 7) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 8) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

9) Click **Apply**.

12.9 Audio Exception Detection

Purpose

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

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Audio Exception**.

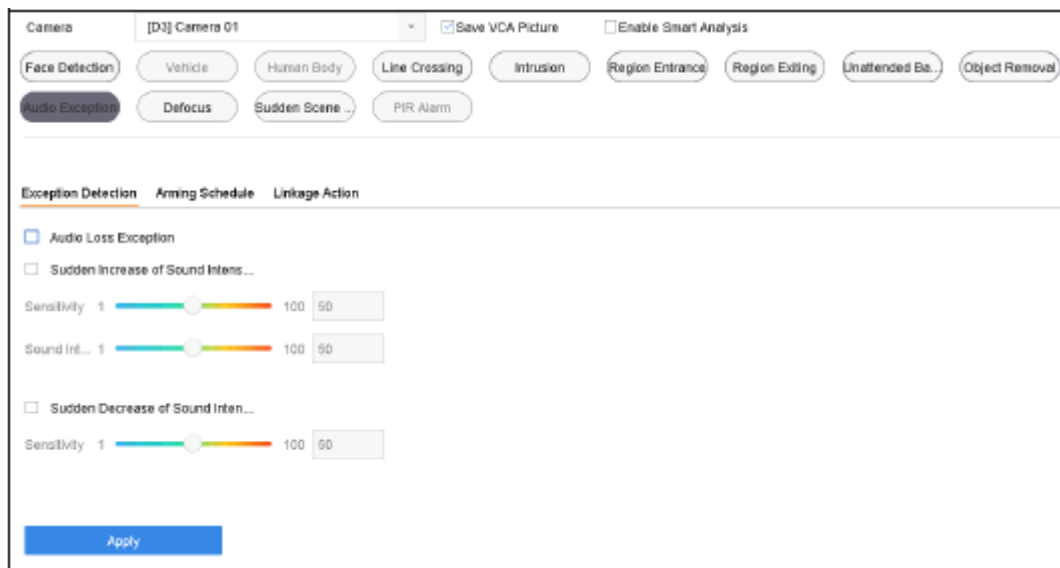


Figure 12-10 Audio Exception Detection

- 3) Select a **Camera** to configure.
- 4) Optionally, check **Save VCA Picture** to save the captured pictures of audio exception detection.
- 5) Follow the steps to set the detection rules.
 - 1) Select the **Exception Detection** tab.
 - 2) Check the **Audio Loss Exception**, **Sudden Increase of Sound Intensity Detection**, or **Sudden Decrease of Sound Intensity Detection** checkboxes.
 - **Audio Loss Exception:** Detects the sound step rise in the surveillance scene. You can set the detection sensitivity and threshold for sound step rise. You need to configure its **Sensitivity** and **Sound Intensity Threshold**.
 - **Sensitivity:** The smaller the value is, the more severe the change should be to trigger the detection. Range [1-100].
 - **Sound Intensity Threshold:** It can filter the sound in the environment. The louder the environment sound, the higher the value should be. Adjust it according to the environment. Range [1-100].
 - **Sudden Decrease of Sound Intensity Detection:** Detects the sound step drop in the surveillance scene. You need set the detection sensitivity [1-100].
- 6) Set the arming schedule. *Refer to Chapter 11.1 Configure Arming Schedule.*

- 7) Set the linkage actions. *Refer to Chapter 11.2 Configure Alarm Linkage Actions.*
- 8) Click **Apply**.

12.10 Sudden Scene Change Detection

Purpose

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

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Sudden Scene Change**.

The screenshot shows the configuration page for Sudden Scene Change Detection. At the top, there is an 'Enable' checkbox and a 'Sensitivity' slider ranging from 1 to 100, currently set at 50. Below this are two tabs: 'Arming Schedule' and 'Linkage Action'. Under 'Arming Schedule', there are radio buttons for 'Continuous' (which is selected) and 'None', along with an 'Edit' button. The main area is a grid for setting the arming schedule. The grid has 7 rows for days of the week (Mon to Sun) and 24 columns for hours (0 to 24). Each cell in the grid contains a blue bar, indicating that detection is enabled continuously for all days and hours. At the bottom of the grid, there is an 'Apply' button.

Figure 12-11 Sudden Scene Change

- 3) Select a **Camera** to configure.
- 4) Check **Enable Sudden Scene Change Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of sudden scene change detection.
- 6) Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the change of scene can trigger the alarm.
- 7) Set the arming schedule. *Refer to Chapter 11.1 Configure Arming Schedule.*
- 8) Set the linkage actions. *Refer to Chapter 11.2 Configure Alarm Linkage Actions.*
- 9) Click **Apply**.

12.11 Defocus Detection

Purpose

The image blur caused by defocus of the lens can be detected.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **Defocus**.

The screenshot shows the configuration page for Defocus Detection. At the top, there is an 'Enable' checkbox and a 'Sensitivity 1' slider set to 100. Below this are two tabs: 'Arming Schedule' and 'Linkage Action'. Under 'Arming Schedule', there are radio buttons for 'Continuous' (which is selected) and 'None', and an 'Edit' button. The main part of the interface is a 7x24 grid representing the days of the week (Mon-Sun) and hours (0-24). All cells in the grid are filled with blue, indicating that defocus detection is armed continuously. At the bottom left, there is an 'Apply' button.

Figure 12-12 Defocus Detection

- 3) Select a **Camera** to configure.
- 4) Check **Enable Defocus Detection**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of defocus detection.
- 6) Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image can be detected.
- 7) Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.
- 8) Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.
- 9) Click **Apply**.

12.12 PIR Alarm

Purpose

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 creatures, such as a dog, cat, etc., can be detected.

- 1) Go to **System > Event > Smart Event**.
- 2) Click **PIR Alarm**.

- 3) Select a **Camera** to configure.
- 4) Check **PIR Alarm**.
- 5) Optionally, check **Save VCA Picture** to save the captured pictures of PIR alarm.
- 6) Set the arming schedule. *Refer to Chapter 11.1 Configure Arming Schedule.*
- 7) Set the linkage actions. *Refer to Chapter 11.2 Configure Alarm Linkage Actions.*
- 8) Click **Apply**.

12.13 Enable Smart Analysis

Purpose

Smart search can be enabled for IP cameras that do not support line crossing and intrusion detection, and allow for line crossing and intrusion events to be analyzed. Smart events will be changed after enabling Smart Analysis.

- 1) Go to **System > Event > Smart Event**.
- 2) Check **Enable Smart Analysis**.
- 3) Click **Yes** on popup message box.

Chapter 13 Smart Search

With VCA detection configured, the NVR can search for pictures, video files and resources related to human body detection, behavior analysis, people counting and heat map results.

13.1 Vehicle Search

Purpose:

You can search and view the matched captured vehicle pictures.

- 1) Go to **Smart Analysis > Smart Search > Vehicle Search**.
- 2) Select the IP camera for vehicle search.
- 3) Set search conditions.
- 4) Click **Start Search**.

The screenshot shows a web interface titled "Search by Appearance". It contains several search filters:

- IP Channel:** A dropdown menu with "[All] Camera" selected.
- Time Segment:** A dropdown menu with "Today" selected, followed by a date range from "2017-09-19 00:00:00" to "2017-09-19 23:59:59".
- Vehicle Brand:** A dropdown menu with "All" selected.
- Vehicle Color:** A dropdown menu with "All" selected.
- Vehicle Model:** A dropdown menu with "All" selected.
- License Plate N...:** An empty text input field.

Figure 13-2 Plate Search

13.2 People Counting

Purpose:

People Counting is used to calculate the number of people entering or leaving a certain configured area, and to create daily/weekly/monthly/annual analysis reports.

- 1) Go to **Smart Analysis > Counting**.
- 2) Select the camera.
- 3) Select the report type to **Daily Report, Weekly Report, Monthly Report, or Annual Report**.
- 4) Set the **Date** to analyze. The people counting graphic will be shown.

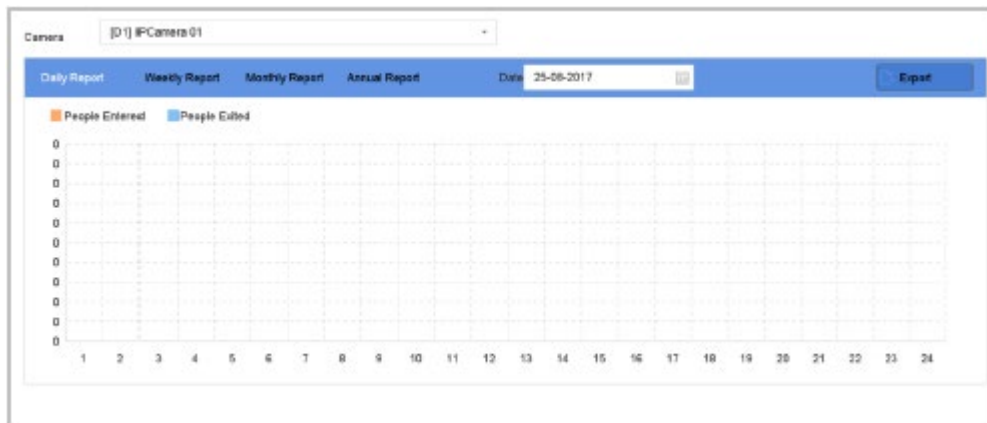


Figure 13-3 People Counting Interface

- 5) (Optional) Click **Export** to export the report in excel format.

13.3 Heat Map

Purpose:

Heat map is a graphical representation of data. The heat map function is usually used to analyze how many people visited and stayed in a specified area.

The heat map function must be supported by the connected IP camera and the corresponding configuration must be set.

- 1) Go to **Smart Analysis > Heat Map**.
- 2) Select a camera.
- 3) Select the report type as **Daily Report, Weekly Report, Monthly Report, or Annual Report**.
- 4) Set the **Data** to analyze.

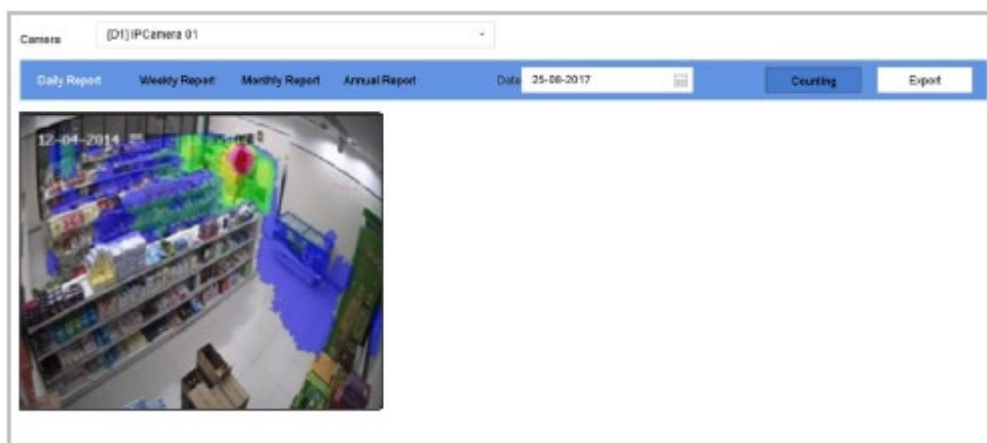


Figure 13-4 Heat Map Interface

- 5) Click **Counting**. The results will be displayed in graphics that are marked in different colors.
- 6) (Optional) Click **Export** to export the statistics report in excel format.

Chapter 14 Human Body Detection

14.1 View Engine Status

Purpose

Smart analysis engine is applied to analyze false alarm and smart analysis tasks. Go to **Smart Analysis > Smart Analysis > Engine Configuration** to view the working status, usage rate, and applied channel of smart analysis engine.

14.2 Human Body Search

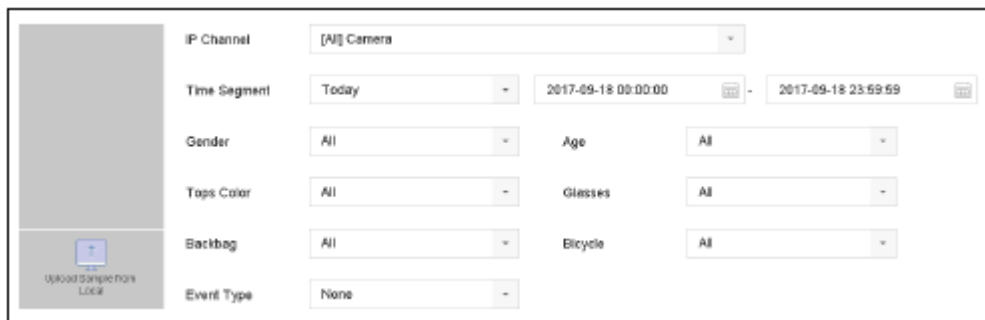
Purpose

Search human body pictures according to manually specified search conditions.

Before you start

Import human body pictures you want to search.

- 1) Go to **Smart Analysis > Smart Search > Human Body Detection > Search by Appearance**.



The screenshot shows a web interface for searching human body pictures. On the left, there is a vertical sidebar with a button labeled 'Upload Inspection Logs'. The main area contains several search filters:

- IP Channel:** [All] Camera
- Time Segment:** Today, 2017-09-18 09:00:00, 2017-09-18 23:59:59
- Gender:** All
- Age:** All
- Top Color:** All
- Glasses:** All
- Backbag:** All
- Bicycle:** All
- Event Type:** None

Figure 14-1 Search by Appearance

- 2) Specify search conditions.
- 3) Click **Start Search**.

Chapter 15 POS Configuration

The device can be connected to the POS machine/server, receive an overlay transaction message on the image during live view or playback, and trigger a POS event alarm.

15.1 Configure POS Settings

15.1.1 Configure POS Connection

- 1) Go to **System > POS Settings**.
- 2) Click **Add** to enter the POS adding interface.
- 3) Select a POS from the drop-down list.
- 4) Check **Enable**.

NOTE

The number of POS devices supported for each device is half of its channel number.



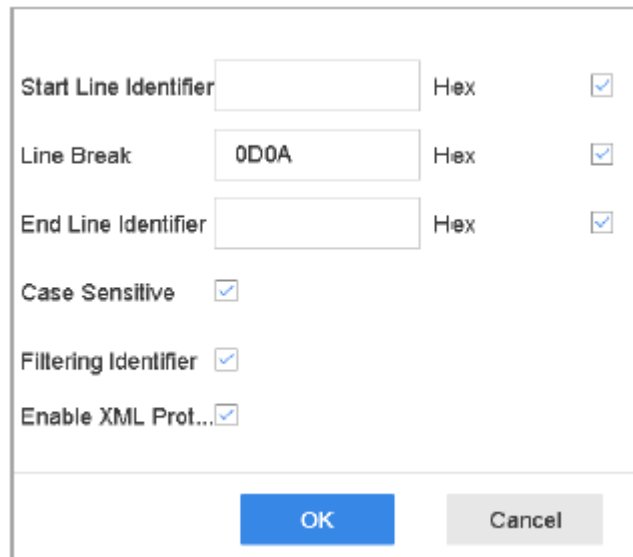
Figure 15-1 POS Settings

- 5) Select the POS protocol to **Universal Protocol, EPSON, AVE** or **NUCLEUS**.

NOTE

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

- **Universal Protocol:** Click the **Advanced** button 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.



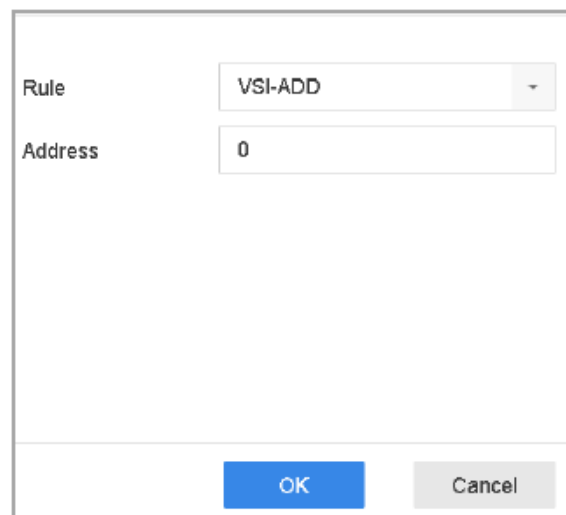
The dialog box contains the following settings:

- Start Line Identifier: [Empty text box] Hex
- Line Break: 0D0A Hex
- End Line Identifier: [Empty text box] Hex
- Case Sensitive:
- Filtering Identifier:
- Enable XML Prot...:

Buttons: OK (blue), Cancel (grey)

Figure 15-2 Universal Protocol Settings

- **EPSON:** The fixed start and end-line tag are used for the EPSON protocol.
- **AVE:** The fixed start and end line tag are used for the AVE protocol. Serial and virtual serial port connection types are supported.
 - 1) Click **Custom** to configure AVE settings.
 - 2) Set the rule to **VSI-ADD** or **VNET**.
 - 3) Set the address bit of the POS message to send.
 - 4) Click **OK** to save settings.



The dialog box contains the following settings:

- Rule: VSI-ADD (dropdown menu)
- Address: 0 (text box)

Buttons: OK (blue), Cancel (grey)

Figure 15-3 AVE Settings

- **NUCLEUS**

- 1) Click **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. The NUCLEUS protocol must be used in the RS-232 connection communication.

- 6) Select the connection mode to TCP Reception, UDP Reception, Multicast, RS-232, USB-to-RS-232 or Sniff, and click **Parameters** to configure the parameters for each connection mode.

- **TCP Connection**

- 1) When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.
- 2) Set the **Allowed Remote IP Address** of the device sending the POS message.

The image shows a dialog box titled "TCP Connection Settings". It has two input fields. The first is labeled "Port" and contains the text "10010". The second is labeled "Allowed Remote IP A..." and contains the text "192 . 0 . 0 . 64". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

Figure 15-4 TCP Connection Settings

- **UDP Connection**

- 1) When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.
- 2) Set the **Allowed Remote IP Address** of the device sending the POS message.

- **USB-to-RS-232 Connection:** Configure the port parameters of the USB-to-RS-232 convertor, including the serial number of port, 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 15-5 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.

Sniff Settings	
Enable Source Port F...	<input checked="" type="checkbox"/>
Source Address	18 . 16 . 1 . 1
Source Port	10020
Enable Destination A...	<input checked="" type="checkbox"/>
Enable Destination P...	<input checked="" type="checkbox"/>
Destination Address	20 . 18 . 1 . 24
Destination Port	10030
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 15-6 Sniff Settings

15.1.2 Configure POS Text Overlay

- 1) Go to **System > POS Settings**.
- 2) Click **Channel Linkage and Display** tab.
- 3) Select the linked channel to overlay the POS characters.
- 4) Set character 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 mode.
 - Font size and font color.
 - Display time (sec) of the characters. The value ranges from 5 to 3600 s.
 - Timeout of POS event. The value ranges from 5 to 3600 s. When the device has not received the POS message over the defined time, the transaction is finished.
- 5) In the **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, or the user name, etc. The defined privacy information will be displayed in * * * on the image instead.
 - 6) (Optional) Check the checkbox to enable the **Overlay POS in Live View**. When this feature is enabled, the POS information can be overlain on the live view image.

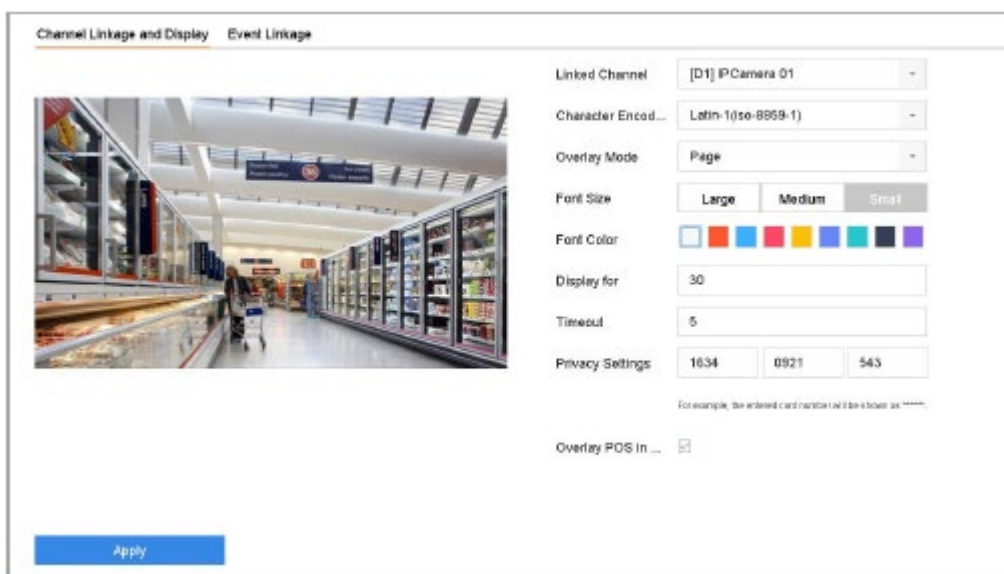


Figure 15-7 Overlay Character Settings

NOTE

You can adjust the size and position of textbox on the preview screen of POS settings interface by dragging the frame.

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

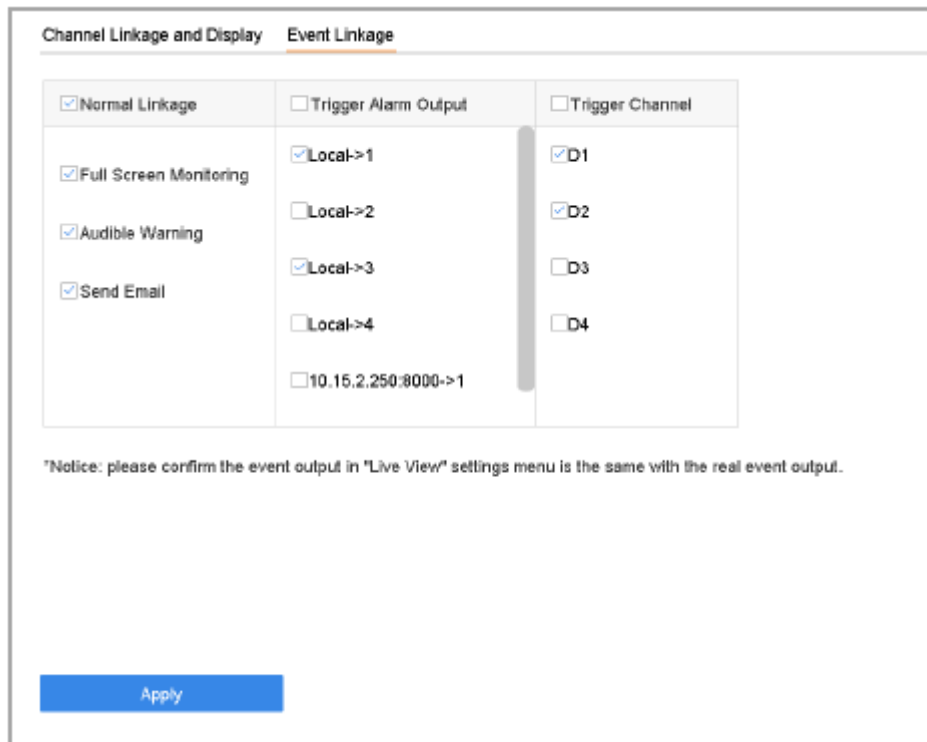
15.2 Configure POS Alarm

Purpose:

The POS event can trigger channels to start recording, or trigger full screen monitoring, audio warning, notifying the surveillance center, sending e-mail and so on.

- 1) Go to **Storage > Recording Schedule**.
- 2) Set the arming schedule of the POS event.
- 3) Go to **System > POS Settings**.
- 4) On the POS adding or editing interface, click the **Event Linkage** tab.
- 5) Select the normal linkage actions: full screen monitoring, audio warning or send E-mail.

- 6) Select one or more alarm output(s) to trigger.
- 7) Select one or more channels to record or become full-screen monitoring when the POS alarm is triggered.



<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.

Apply

Figure 15-8 Set Trigger Cameras of POS

- 8) Click **Apply** to save the settings.

Chapter 16 Network Settings

16.1 Configure TCP/IP Settings

Purpose

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

- 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: a4:14:37:aa:09:a3
- MTU(Bytes): 1500
- Main NIC: LAN1

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

Figure 16-1 TCP/IP Settings

- 2) Select **Net-Fault Tolerance** or **Multi-Address Mode** under Working Mode.
 - **Net-Fault Tolerance:** The two NIC cards use the same IP address, and you can set the main NIC to LAN1 or LAN2. When one NIC card fails, the device will automatically enable the other standby NIC card to ensure normal running of the system.
 - **Load Balance:** The two NIC cards share the same IP address and the total bandwidth load, which enables the system to provide a two Gigabit network capacity.
 - **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. You can select one NIC card as the default route. When the system is connected to the extranet, the data will be forwarded through the default route.
- 3) Configure other IP settings as needed.



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

- 4) Click **Apply**.

16.2 Configuring Hik-Connect

Hik-Connect is a mobile phone application and service platform page (www.hik-connect.com) that provides access and management for connected encoders, which provides convenient remote access to the surveillance system.



Hik-Connect can be enabled via the SADP software, GUI and Web browser. GUI operation steps are provided in this section.

- 1) Go to **Configuration > Network > Advanced Settings > Platform Access** to enter the Hik-Connect Settings page.

Figure 16-2 Hik-Connect Settings

- 2) Check the **Enable** to activate the function. Then the Service Terms page pops up as below.

Figure 16-3 Service Terms

- 1) Create the verification code in the **Verification Code** text field.
- 2) Confirm the verification code.
- 3) Read **Terms of Service** and **Privacy Policy** before enabling the service.
- 4) Click **OK** to save the settings and return to the Hik-Connect page.

Figure 16-4 Hik-Connect Settings



Hik-Connect is disabled by default. The verification code is empty when the device leaves the factory. The verification code must contain 6 to 12 letters or numbers and is case sensitive. Every time you enable Hik-Connect, the Service Terms page pops up and you should read Terms of Service and Privacy Policy before enabling it.

- 3) If you want to customize the server, enable **Custom** and enter the **Server Address** in the text field.
 - 4) Click **Save**.
 - 5) After configuration, you can access and manage the DVR by your mobile phone or by the website (www.hik-connect.com).
- **iOS Users:** scan the QR code below to download the Hik-Connect application for the subsequent operations.



Figure 16-5 QR Code for iOS Users

- **Android Users:** scan the QR code below to download the Hik-Connect application for the subsequent operations. You must install *googleplay* on your Android mobile phone to skip to the address successfully.



Figure 16-6 QR Code for Android Users

16.3 Configure DDNS

Purpose

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 DynDNS, PeanutHull and NO-IP services with your ISP before configuring DDNS settings.

- 1) Go to **System > Network > TCP/IP > DDNS**.
- 2) Check **Enable**.

3) Select **DynDNS** under **DDNS Type**.

NOTE

PeanutHull and NO-IP are also available under DDNS Type, and required information should be entered accordingly.

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 the **User Name** and **Password** registered in the DynDNS website.

The screenshot shows the DDNS Settings configuration page. At the top, there are tabs for TCP/IP, DNS, PPPoE, NTP, and NAT. The DNS tab is selected. Below the tabs, there is an 'Enable' checkbox which is checked. The 'DDNS Type' is set to 'DynDNS'. The 'Server Address' is 'member.dyndns.org'. The 'Device Domain Name' is '1233dyndns.com'. The 'User Name' is 'test' and the 'Password' is masked with asterisks. The status message says 'DDNS is disabled.' and there is an 'Apply' button at the bottom.

Figure 16-7 DDNS Settings

7) Click **Apply**.

16.4 Configure PPPoE

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

NOTE

Contact your Internet service provider for details about the PPPoE service.

16.5 Configure NTP

Purpose

Connection to a network time protocol (NTP) server can be configured on your device to ensure the accuracy of the system date and time.

1) Go to **System** > **Network** > **TCP/IP** > **NTP**.

TCP/IP	DDNS	PPPoE	NTP	NAT
Enable			<input checked="" type="checkbox"/>	
Interval (min)			<input type="text" value="180"/>	
NTP Server			<input type="text" value="au.pool.ntp.org"/>	
NTP Port			<input type="text" value="123"/>	
<input type="button" value="Apply"/>				

Figure 16-8 NTP Settings

- 2) Check **Enable**.
- 3) Configure NTP settings as needed.
 - **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**.

16.6 Configure SNMP

Purpose

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

Before You Start

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

- 1) Go to **System > Network > Advanced > SNMP**.

Figure 16-9 SNMP Settings

- 2) Check **Enable**. A message will pop up to prompt possible security risk and click **Yes** to continue.
- 3) Configure the SNMP settings as needed.
 - **Trap Address:** IP address of the SNMP host.
 - **Trap Port:** Port of the SNMP host.
- 4) Click **Apply**.

16.7 Configure E-mail

Purpose

The system can be configured to send an E-mail notification to all designated users when a specified event occur, such as 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 notification.

- 1) Go to **System > Network > Advanced > E-mail**.

Figure 16-10 E-mail Settings

2) Configure the following E-mail settings.

- **Enable Server Authentication:** Check to enable the function if the SMTP server requires user authentication and enter 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 name of the sender.
- **Sender's Address:** Sender's Address.
- **Select Receivers:** Select the receiver. Up to 3 receivers can be configured.
- **Receiver:** The name of the receiver.
- **Receiver's Address:** The E-mail address of user to be notified.
- **Enable Attached Picture:** Check to enable the function if you want to send e-mail with attached alarm images. The interval is the time between two adjacent alarm images.

3) Click **Apply**.

4) (Optional) Click **Test** to send a test e-mail.

16.8 Configure Ports

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

- 1) Go to **System > Network > Advanced > More Settings** and 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.
 - **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 the 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 for use in entertainment and communications systems to control streaming media servers. The port is 554 by default.

SNMP	Email	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"/>
<input type="button" value="Apply"/>		

Figure 16-11 Port Settings

Chapter 17 Hot Spare Device Backup

Purpose:

The device can form an N+1 hot spare system. The system consists of several working devices and a hot spare device; when the working device fails, the hot spare device switches into operation, thus increasing the reliability of the system. Please contact your dealer for details regarding the models that support the hot spare function.

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

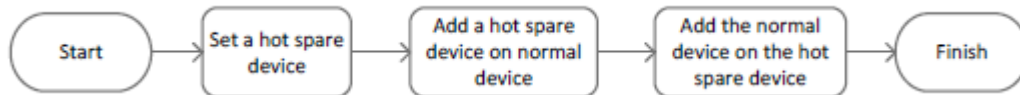


Figure 17-1 Building Hot Spare System

Before you start:

Ensure that at least two devices are online.

17.1 Set Hot Spare Device

Purpose:

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

- 1) Go to **System > Hot Spare**.
- 2) Set the **Work Mode** as **Hot Spare Mode**.



Figure 17-2 Hot Spare

- 3) Click **Apply**.
- 4) Click **Yes** in popup attention box to reboot the device.
 - The camera connection will be disabled when the device is in hot spare mode.
 - It is highly recommended to restore device defaults after switching the working mode of the hot spare device to normal mode, in order to ensure normal operation afterwards.

17.2 Set Working Device

- 1) Go to **System > Hot Spare**.
- 2) Set the **Work Mode** as **Normal Mode**.
- 3) Check **Enable**.
- 4) Enter the IP address and admin password of the hot spare device.

Work Mode: Normal Mode

Enable:

IPv4 address of the hot spare: 10 . 15 . 1 . 19

Password of the hot spare: [masked]

Working Status: [empty]

*Notice: After the hot spare is enabled, you must link the working device to the hot spare device...

Figure 17-3 Hot Spare

- 5) Click **Apply**.

17.3 Manage Hot Spare System

- 1) Go to **System > Hot Spare** in hot spare device.
- 2) Check working devices from the device list and click **Add** to link the working device to the hot spare device.



A hot spare device can connect up to 32 working devices.

Work Mode: Hot Spare Mode

Device List

No.	IP Address
1	10.15.2.107

Add

Working Dev...

No.	IP Address	Connection Status	Working Status	Delete
-----	------------	-------------------	----------------	--------

Apply

Figure 17-4 Add Working Device

Table 17-1 Working Status Description

Working Status	Description
No record	The working device works properly.
Backing up	When the working device is offline, the hot spare device will record the video of the IP camera that is connected to the working device for backup. The recording backup can function for one working device at a time.
Synchronizing	When the working device comes online, the lost video files will be restored via the record synchronization function. The record synchronization function can be enabled for one working device at a time.

Chapter 18 System Maintenance

18.1 Storage Device Maintenance

18.1.1 Configure Disk Clone

Purpose:

Select the HDDs to clone to eSATA HDD.

Before you start:

Connect an eSATA disk to the device.

- 1) Go to **Maintenance > HDD Operation > HDD Clone**.

Label	Capacity	Status	Property	Type	Free Space	Group
<input type="checkbox"/> 1	1863.02GB	Normal	RAW	Local	1858.05GB	1
<input type="checkbox"/> 2	2794.52GB	Normal	RAW	Local	2794.05GB	1
<input type="checkbox"/> 5	1863.02GB	Normal	RAW	Local	1862.05GB	1
<input type="checkbox"/> 9	2794.52GB	Normal	RAW	Local	2794.05GB	1
<input type="checkbox"/> 10	1863.02GB	Normal	RAW	Local	1862.05GB	1

Clone Destination

eSATA:

Capacity:

Figure 18-1 HDD Clone

- 2) Check the HDD to clone. The capacity of selected HDD must match the capacity of clone destination.
- 3) Click **Clone**.
- 4) Click **Yes** on popup message box to continue clone.

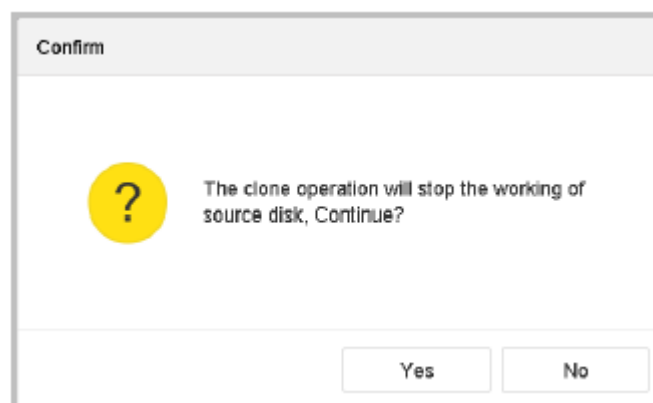


Figure 18-2 Message Box

18.1.2 S.M.A.R.T Detection

Purpose:

The device provides HDD detection functions, such as S.M.A.R.T. and Bad Sector Detection. S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is an HDD monitoring system that detects and reports on various indicators of reliability in the hopes of anticipating failures.

- 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) Select the self-test types as **Short Test**, **Expanded Test** or the **Conveyance Test**.
- 4) Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.
- 5) The related S.M.A.R.T. information is shown in the interface. You can check the HDD status.

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	2*	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 18-3 S.M.A.R.T Settings Interface

NOTE

To use the HDD even when S.M.A.R.T. checking has failed, you can check **Continue to use the disk when self-evaluation is failed** checkbox.

18.1.3 Bad Sector Detection

- 1) Go to **Maintenance > HDD Operation > Bad Sector Detection**.
- 2) Select the HDD no. to be configured in the dropdown list.
- 3) Select **All Detection** or **Key Area Detection** as the detection type.
- 4) Click the **Self-Test** button to start the detection.

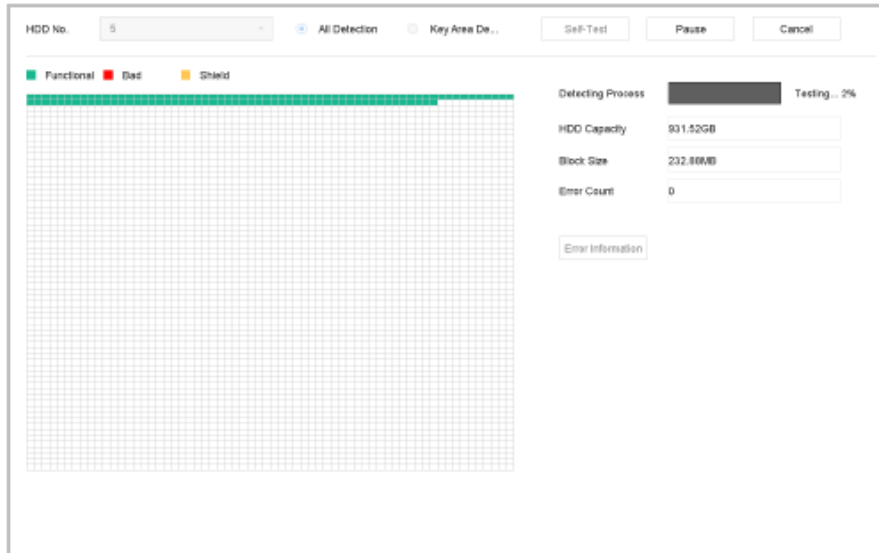


Figure 18-4 Bad Sector Detection

- You can also pause/resume or cancel the detection.
- After testing completed, you can click the **Error information** button to see the detailed damage information.

18.1.4 HDD Health Detection

Purpose:

You can view the health status of Seagate HDDs manufactured after October 1th, 2017, with capacity ranges between 4 TB and 8 TB. The function allows for HDD problems to be troubleshooted. Compared to S.M.A.R.T function, health detection shows HDD status with more details.

- 1) Go to **Maintenance > HDD Operation > Health Detection**.



Figure 18-5 Health Detection

- 2) Click an HDD to view details.

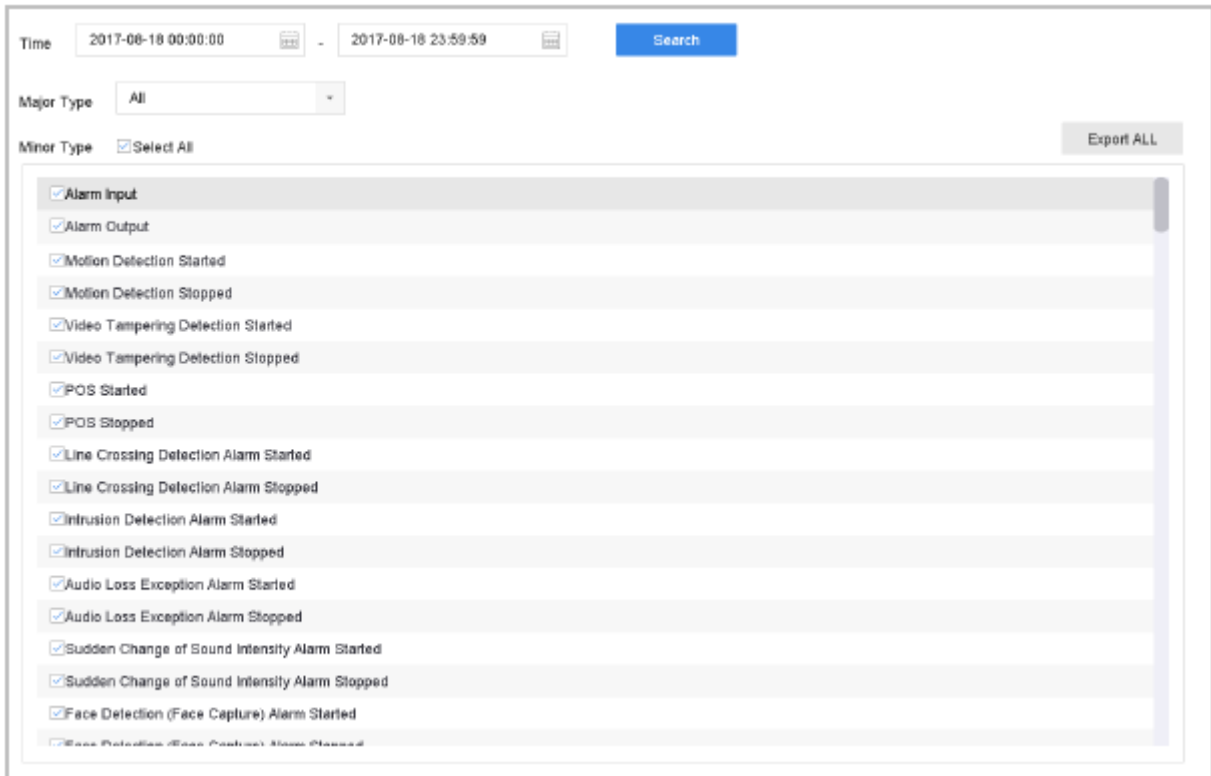
18.2 Search & Export Log Files

Purpose:

The operation, alarm, exception and information of the device can be stored in log files, which can be viewed and exported at any time.

18.2.1 Search the Log Files

- 1) Go to **Maintenance > Log Information**.



The screenshot displays the Log Search Interface. At the top, there is a 'Time' field with two date-time pickers: '2017-08-18 00:00:00' and '2017-08-18 23:59:59', separated by a minus sign. To the right of the second picker is a blue 'Search' button. Below the time field is a 'Major Type' dropdown menu currently set to 'All'. Underneath that is a 'Minor Type' section with a checked checkbox for 'Select All' and an 'Export ALL' button to the right. The main area contains a scrollable list of alarm types, each with a checked checkbox:

- Alarm Input
- Alarm Output
- Motion Detection Started
- Motion Detection Stopped
- Video Tampering Detection Started
- Video Tampering Detection Stopped
- POS Started
- POS Stopped
- Line Crossing Detection Alarm Started
- Line Crossing Detection Alarm Stopped
- Intrusion Detection Alarm Started
- Intrusion Detection Alarm Stopped
- Audio Loss Exception Alarm Started
- Audio Loss Exception Alarm Stopped
- Sudden Change of Sound Intensity Alarm Started
- Sudden Change of Sound Intensity Alarm Stopped
- Face Detection (Face Capture) Alarm Started
- Face Detection (Face Capture) Alarm Stopped

Figure 18-6 Log Search Interface

- 2) Set the log search conditions, including the Time, Major Type and Minor Type.
- 3) Click **Search** to start search log files.
 - The matched log files will be displayed on the list shown below.

Time: 2017-08-18 00:00:00 - 2017-08-18 23:59:59 Search

Major Type: All

Minor: Search Result

No.	Major Type	Time	Minor Type	Parameter	Play	Details
103	Alarm	18-08-2017 07:07:31	Motion Detection ...	N/A	▶	ⓘ
104	Alarm	18-08-2017 07:07:43	Motion Detection ...	N/A	▶	ⓘ
105	Alarm	18-08-2017 07:16:27	Motion Detection ...	N/A	▶	ⓘ
106	Alarm	18-08-2017 07:16:37	Motion Detection ...	N/A	▶	ⓘ
107	Inform...	18-08-2017 07:17:19	System Running ...	N/A	—	ⓘ
108	Inform...	18-08-2017 07:17:19	System Running ...	N/A	—	ⓘ
109	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	—	ⓘ
110	Inform...	18-08-2017 07:18:00	HDD S.M.A.R.T.	N/A	—	ⓘ
111	Inform...	18-08-2017 07:27:20	System Running ...	N/A	—	ⓘ

Total: 1151 P: 2/12

Export ALL

Export Back

Sudden Change of Sound Intensity Alarm Started
 Sudden Change of Sound Intensity Alarm Stopped
 Face Detection (Face Capture) Alarm Started
 Face Detection (Face Capture) Alarm Stopped

Figure 18-7 Log Search Results

**NOTE**

Up to 2000 log files can be displayed each time.

Related Operation:

- Click the ⓘ button or double click it to view its detailed information.
- Click the ▶ button to view the related video file.

18.2.2 Export the Log Files

Before You Start:

Connect a storage device to your device.

- 1) Search the log files. Refer to *Chapter 18.2.1 Search the Log Files*.
- 2) Select the log files you want to export, and click **Export**.

Or you can click **Export ALL** on the Log Search interface to export all the system logs to the storage device.

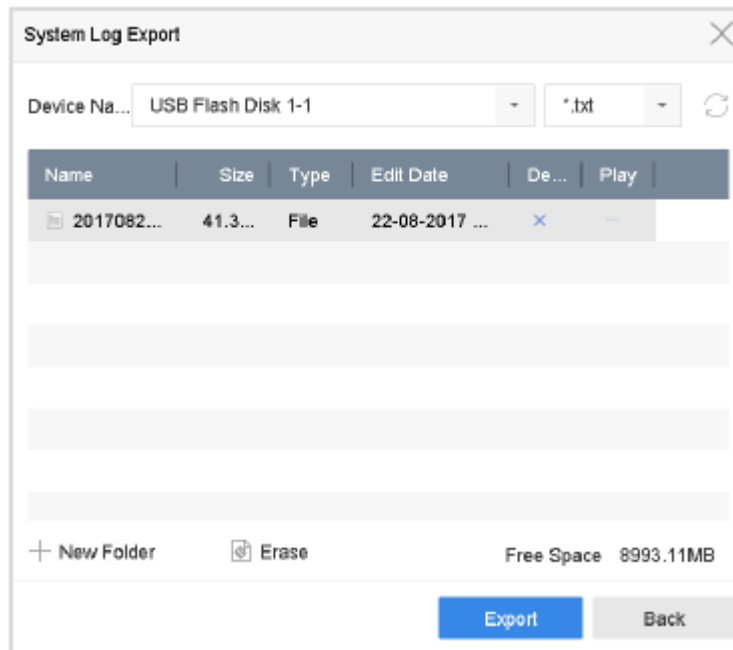


Figure 18-8 Export Log Files

- 3) On the Export interface, select the storage device from the dropdown list of **Device Name**.
- 4) Select the format of the log files to be exported. Up to 15 formats are selectable.
- 5) Click the **Export** to export the log files to the selected storage device.

Related Operation:

- Click the New Folder button to create a new folder in the storage device.
- Click the Format button to format the storage device before log export.

18.3 Import/Export IP Camera Configuration Files

Purpose:

Added IP camera information, such as IP addresses, managed ports, admin passwords, etc., can be generated into an Excel file and exported to a local device for backup. The exported file can be edited on a PC. Content can be added or deleted, and settings can be exported to other devices by copying the Excel file.

Before You Start:

Connect a storage device to your device. In order to import the configuration file, the storage device must contain the file.

- 1) Go to **Camera > IP Camera Import/Export**.
- 2) Click the **IP Camera Import/Export** tab, and the content of detected plugged external device appears.
- 3) Export or import the IP camera 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 the **Import** button.



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

18.4 Import/Export Device Configuration Files

Purpose:

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.

Connect a storage device to your device. To import a configuration file, the storage device must contain the file.

Before You Start:

Connect a storage device to your device. To import a configuration file, the storage device must contain the file.

- Go to **Maintenance > Import/Export**

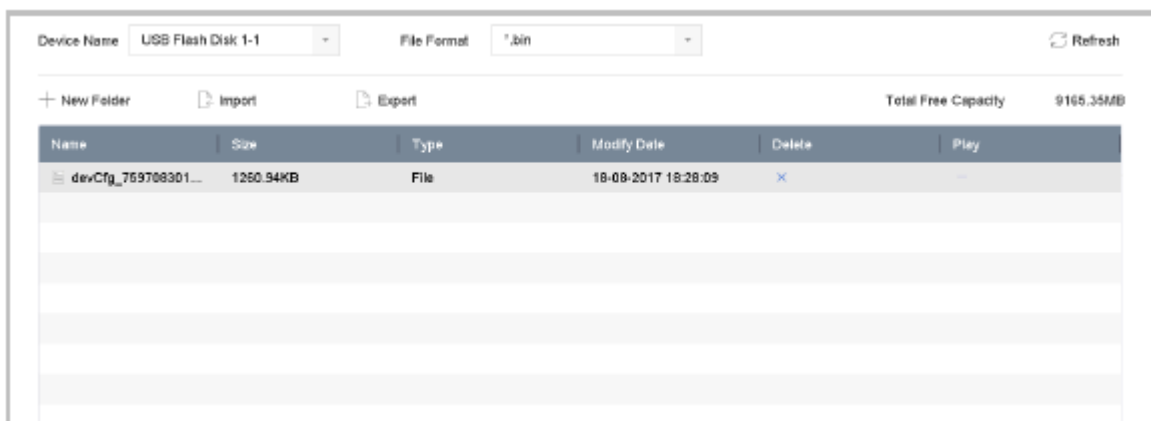


Figure 18-9 Import/Export Config File

- 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 the **Import** button.



After having finished the import of configuration files, the device will reboot automatically.

18.5 Upgrade System

Purpose:

The firmware on your device can be upgraded by local backup device or remote FTP server.

18.5.1 Upgrade by Local Backup Device

Before You Start:

Connect your device with a local storage device with update firmware file.

- 1) Go to **Maintenance > Upgrade**.
- 2) Click the **Local Upgrade** tab to enter the local upgrade interface.

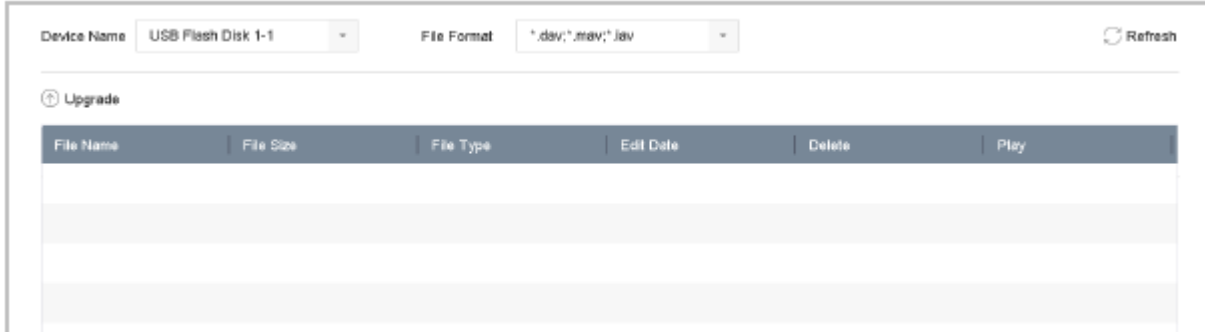


Figure 18-10 Local Upgrade Interface

- 3) Select the update file from the storage device.
- 4) Click **Upgrade** to start upgrading.
- 5) After the upgrading is complete, the device will reboot automatically to activate the new firmware.

18.5.2 Upgrade by FTP

Before you start:

Ensure the network connection of the PC (running FTP server) and device are valid. Run the FTP server on the PC and copy the firmware into the corresponding directory on your PC.

- 1) Go to **Maintenance > Upgrade**.
- 2) Click the **FTP** tab to enter the local upgrade interface.

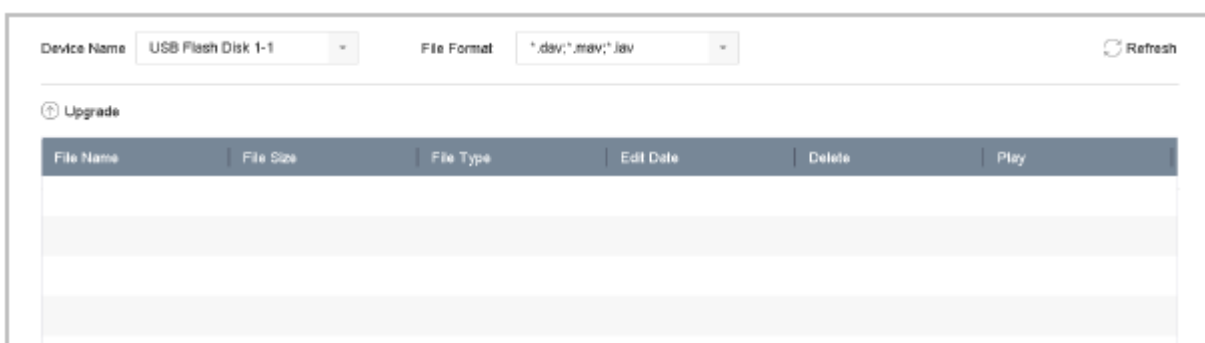


Figure 18-11 FTP Upgrade Interface

- 3) Enter the **FTP Server Address** in the text field.
- 4) Click the **Upgrade** button to start upgrading.
- 5) After the upgrading is complete, reboot the device to activate the new firmware.

18.6 Restore Default Settings

1) Go to **Maintenance > Default**.

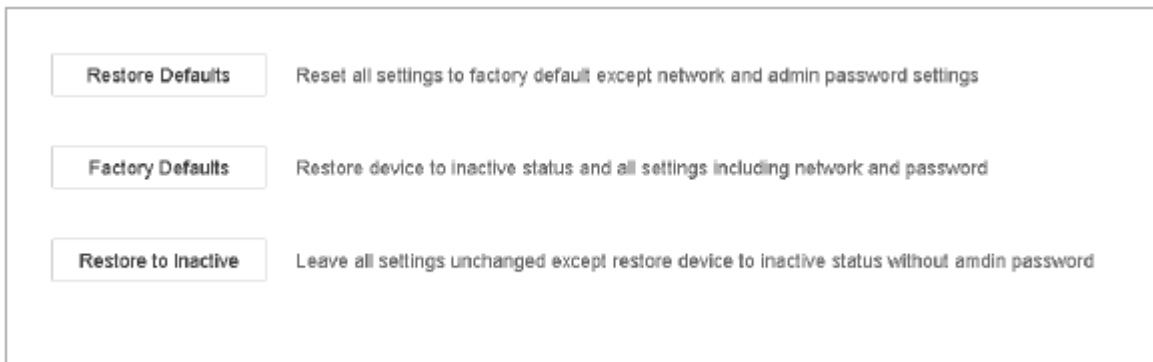


Figure 18-12 Restore Defaults

2) Select the restoring 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 device to the inactive status.



NOTE

The device will reboot automatically after restoring to the default settings.

18.7 System Service

18.7.1 Network Security Settings

Disable SADP Services

Purpose

You can disable SADP service to enhance the access security, e.g., when you are in an untrusted network environment.

- 1) Go to **System > System Service > System Service**.
- 2) Uncheck **Enable SADP** to disable the service.

HTTP

You can choose to disable the HTTP, or set the HTTP authentication when it is enabled to enhance access security.



NOTE

HTTP is enabled by default.

Set HTTP Authentication

Purpose

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security.

- 1) Go to **System > System Service > System Service**.



The screenshot shows a configuration panel for HTTP authentication. At the top, there is a checkbox labeled 'Enable HTTP' which is checked. Below it, there is a dropdown menu labeled 'HTTP Authentication Type' with 'digest' selected.

Figure 18-13 HTTP Authentication

- 2) Check the **Enable HTTP** to enable the HTTP service.
- 3) Select the **digest** as the **HTTP Authentication** in the drop-down list.
- 4) Click **Save** to save the settings.

NOTE

Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select **digest** as the authentication type.

Disable HTTP

Purpose

The admin user account can disable the HTTP service from the GUI or the web browser. After the HTTP is disabled, all its related services, including the ISAPI, Onvif and Genetec, will terminate as well.

- 1) Go to **System > System Service > System Service**.
- 2) Uncheck the **Enable HTTP** to disable the HTTP service.

RTSP Authentication

Purpose

You can specifically secure the stream data of live view by setting the RTSP authentication.

- 1) Go to **System > System Service > System Service**.



The screenshot shows a configuration panel for RTSP authentication. At the top, there is a checkbox labeled 'Enable RTSP' which is checked. Below it, there is a dropdown menu labeled 'RTSP Authentication Type' with 'digest' selected.

Figure 18-14 RTSP Authentication

- 2) Select the authentication type.

NOTE

Two authentication types are available: **digest** and **digest/basic**. If you select **digest**, as the RTSP authentication, 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 **Save** to save the settings.

18.7.2 Manage ONVIF User Accounts

Purpose

For third-party camera connections to the device via ONVIF, you can enable ONVIF and manage user accounts.

- 1) Go to **System > System Service > ONVIF**.
- 2) Check **Enable ONVIF** to enable ONVIF access management.
- 3) Click **Add** to enter the Add User interface.

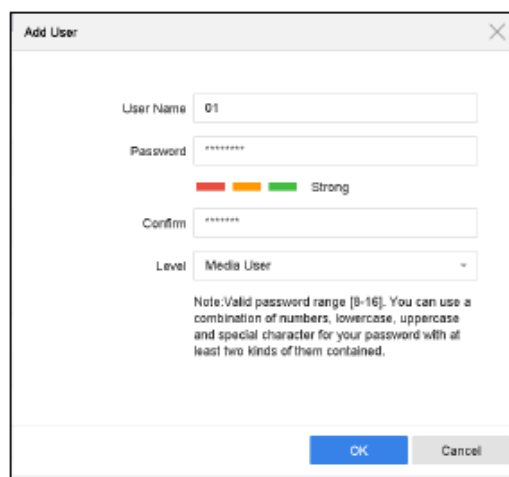


Figure 18-15 Add User

- 4) Edit the user name, and enter the strong password.
- 5) Select the user level to **Media User**, **Operator** and **Admin**.
- 6) Click **OK** to save the settings.

Result:

The added user accounts have the permission to connect other devices to the device via ONVIF protocol.

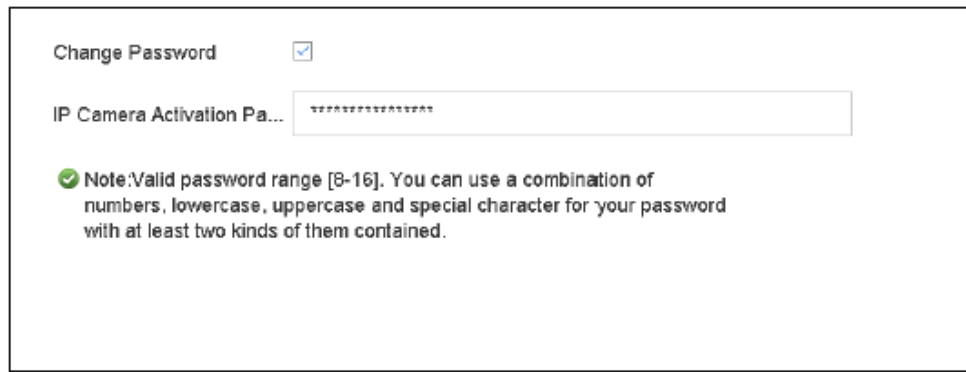


The ONVIF protocol is disabled by default.

18.7.3 Manage IP Camera Activation

When you activate the device for the first-time, you can set the IP camera activation password as well. You can also manage the password to enhance security.

- 1) Go to **System > System Service > IP Camera Activation**.
- 2) Check the **Change Password** to enable the permission.
- 3) Enter the admin password of the device to obtain the permission.



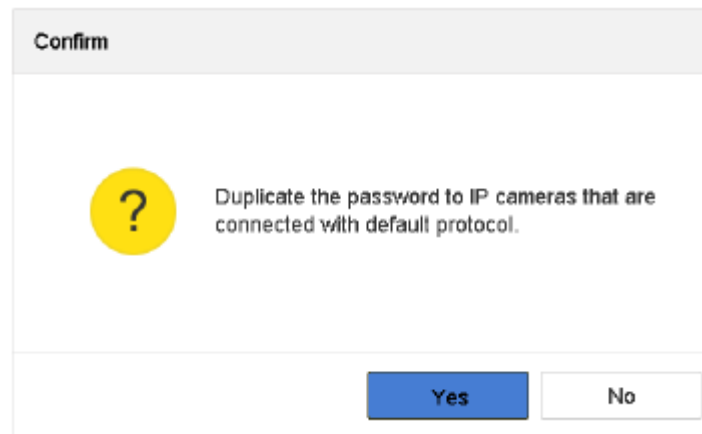
Change Password

IP Camera Activation Pa...

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.

Figure 18-16 Change IP Camera Activation Password

- 4) In the **IP Camera Activation Password** text field, enter a new strong password.
- 5) Click **Apply** to see the following pop-up attention box.



Confirm

? Duplicate the password to IP cameras that are connected with default protocol.

Yes **No**

Figure 18-17 Attention

- 6) Click **Yes** to duplicate the current password for IP cameras that are connected using the default protocol.

Chapter 19 General System Settings

19.1 Configure General Settings

Purpose:

You can configure the BNC output standard, VGA output resolution, and mouse pointer speed via the **System > General** interface.

- 1) Go to **System > General**.

The screenshot displays the 'General Settings' interface with the following configurations:

- Language:** English
- Time Zone:** (GMT+08:00) Beijing, Urumc
- Date Format:** DD-MM-YYYY
- System Date:** 22-08-2017
- System Time:** 11:34:09
- Device Name:** Network Video Recorder
- Device No.:** 255
- Auto Log out:** Never
- Enable Wizard:**
- Enable Password:**
- VGA/HDMI Resolution:** 1920*1080,60HZ,(1080P)
- VGA2/HDMI2 Resolution:** 1920*1080,60HZ,(1080P)
- Mouse Pointer Speed:** Slow (slider set to approximately 25%)
- Enable DST:**
- DST Mode:** Auto (radio button selected)
- Start Time:** Apr 1st Sun 2 : 00
- End Time:** Oct last Sun 2 : 00
- DST Bias:** 60 Minutes

An 'Apply' button is located at the bottom left of the settings panel.

Figure 19-1 General Settings Interface

- 2) Configure the following settings.

- **Language:** The default language used is *English*.
- **Output Standard:** Select the output standard to NTSC or PAL, which must be the same as the video input standard.
- **Resolution:** Configure the resolution of the video output.
- **Device Name:** Edit the name of the device
- **Device No.:** Edit the serial number of the device. The Device No. can be set in the range of 1 to 255, and the default number is 255. The number is used for the remote and keyboard control.
- **Auto Logout:** Set 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 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 the **Apply** button to save the settings.

19.2 Configure Date and Time

- 1) Go to **System > General**.
- 2) Configure the date and time.
 - **Time Zone:** Select the time zone.
 - **Date Format:** Select the date format.
 - **System Date:** Select the system date.
 - **System Time:** Set the system time.

Time Zone	(GMT+08:00) Beijing, Urumc
Date Format	DD-MM-YYYY
System Date	22-08-2017
System Time	11:34:09

Figure 19-2 Date and Time Settings

- 3) Click the **Apply** button to save the settings.

19.3 Configure DST Settings

The 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).

- 1) Go to **System > General**.
- 2) Check the **Enable DST**.

Enable DST	<input checked="" type="checkbox"/>
DST Mode	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Start Time	Apr 1st Sun 2 :00
End Time	Oct 1st Sun 2 :00
DST Bias	60 Minutes

Figure 19-3 DST Settings Interface

- 3) Select the DST mode to **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.
 - **DST Bias:** set the time (30/60/90/120 minutes) offset from the standard time.
- Example:** The DST begins at 2:00 a.m. on the second Sunday of March and ends at 2:00

a.m. on the first Sunday of November, with 60 minutes ahead.

- 4) Click the **Apply** button to save the settings.

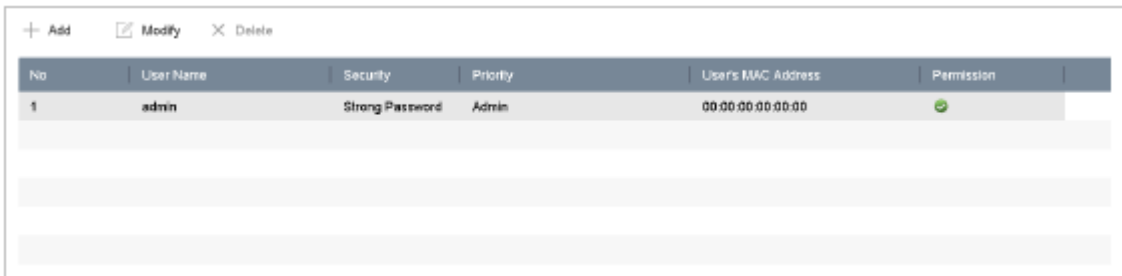
19.4 Manage User Accounts

Purpose:

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

19.4.1 Add a User

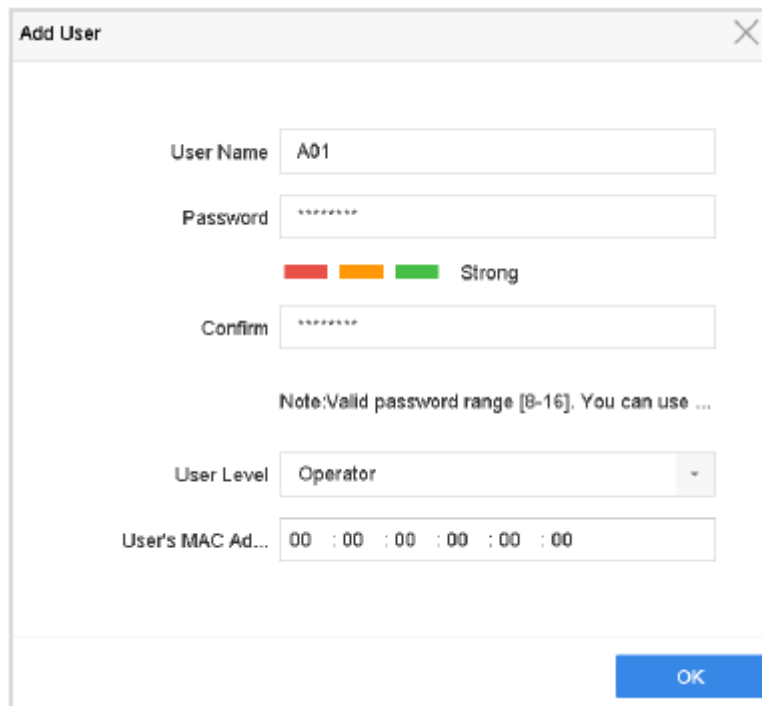
- 1) Go to **System > User**.



No	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Strong Password	Admin	00:00:00:00:00:00	✔

Figure 19-4 User Management Interface

- 2) Click **Add** to enter the operation permission interface.
- 3) Enter the admin password and click **OK**.



Add User

User Name: A01

Password: *****

Strong

Confirm: *****

Note: Valid password range [8-16]. You can use ...

User Level: Operator

User's MAC Ad...: 00 : 00 : 00 : 00 : 00 : 00

OK

Figure 19-5 Add User

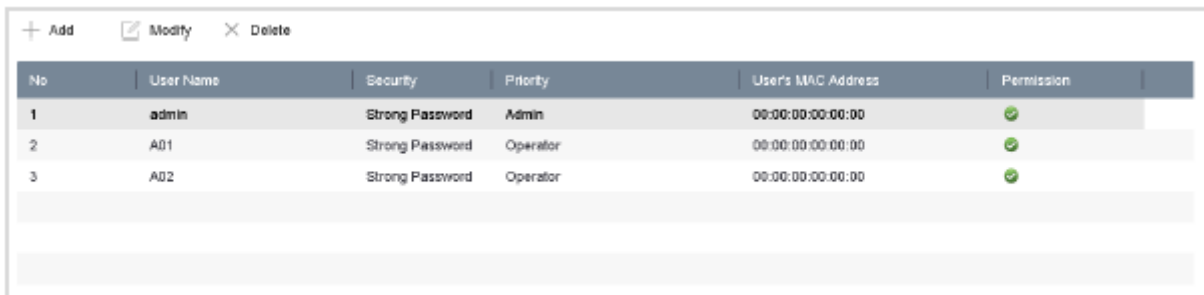
- 4) In the Add User interface, enter the information for new user, including **User Name**, **Password**, **Confirm** (password), **User Level** (Operator/Guest) and **User's MAC Address**.

 **WARNING**

Strong Password recommended—We highly recommend that 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 recommend that you reset your password regularly, especially in 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 permissions.
 - **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission 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 which logs onto the device. If it is configured and enabled, it only allows the remote user with this MAC address to access the device.
- 5) Click **OK** to finish the new user account adding.

Result: In the User Management interface, the added new user is displayed on the list.



No	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Strong Password	Admin	00:00:00:00:00:00	
2	A01	Strong Password	Operator	00:00:00:00:00:00	
3	A02	Strong Password	Operator	00:00:00:00:00:00	

Figure 19-6 User List

19.4.2 Set the Permission for a User

For the added user, you can assign the different permissions, including the local and remote operation for the device.

- 1) Go to **System > User**.
- 2) Select a user from the list and click the  button to enter the permission settings interface.

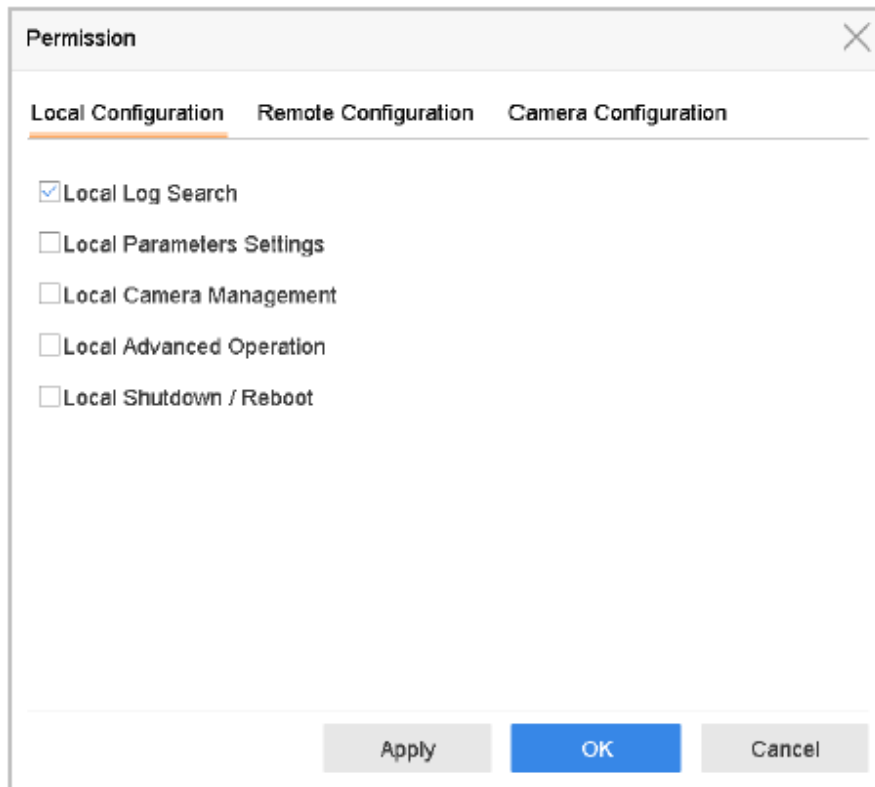


Figure 19-7 User Permission Settings Interface

3) Set the user's **Local Configuration**, **Remote Configuration** and **Camera Configuration** permissions.

- **Local Configuration**

- **Local Log Search:** Search and view device log and system information.
- **Local Parameters Settings:** Configure parameters, restore factory default parameters and import/export configuration files.
- **Local Camera Management:** Add, delete and edit IP cameras.

- **Local Advanced Operation:** Operating HDD management (initialize HDD, set HDD property), upgrade system firmware, clear I/O alarm output.

- **Local Shutdown Reboot:** Shut down or reboot the device.

- **Remote Configuration**


- **Remote Log Search:** Remotely view logs that are saved on the device.
- **Remote Parameters Settings:** Remotely configure parameters, restore factory default parameters and import/export configuration files.
- **Remote Camera Management:** Remotely add, delete and edit IP cameras.
- **Remote Serial Port Control:** Configure settings for RS-232 and RS-485 ports.
- **Remote Video Output Control:** Send remote button control signals.
- **Two-Way Audio:** Perform two-way radio communication between the remote client and device.
- **Remote Alarm Control:** Remotely arm (notify alarm and exception message to the remote client) and control the alarm output.
- **Remote Advanced Operation:** Remotely operate HDD management (initialize HDD, set HDD property), upgrade system firmware, clear I/O alarm output.
- **Remote Shutdown/Reboot:** Remotely shut down or reboot the device.

- Camera Configuration
 - **Remote Live View:** Remotely view selected camera live video.
 - **Local Manual Operation:** Locally start/stop manual recording and alarm output for selected cameras.
 - **Remote Manual Operation:** Remotely start/stop manual recording and alarm output for selected cameras.
 - **Local Playback:** Locally play back recorded files for selected cameras.
 - **Remote Playback:** Remotely play back recorded files for selected cameras.
 - **Local PTZ Control:** Locally control PTZ movement for selected cameras.
 - **Remote PTZ Control:** Remotely control PTZ movement for selected cameras.
 - **Local Video Export:** Locally export recorded files for selected cameras.
- 4) Click **OK** to save the settings.



Only the admin user account has the permission to restore factory default parameters.

19.4.3 Set Local Live View Permission for Non-Admin Users

- 1) Go to **System > User**.
- 2) Click  of admin user.
- 3) Enter admin password and click **OK**.
- 4) Select cameras that a non-admin user can view locally and click **OK**.

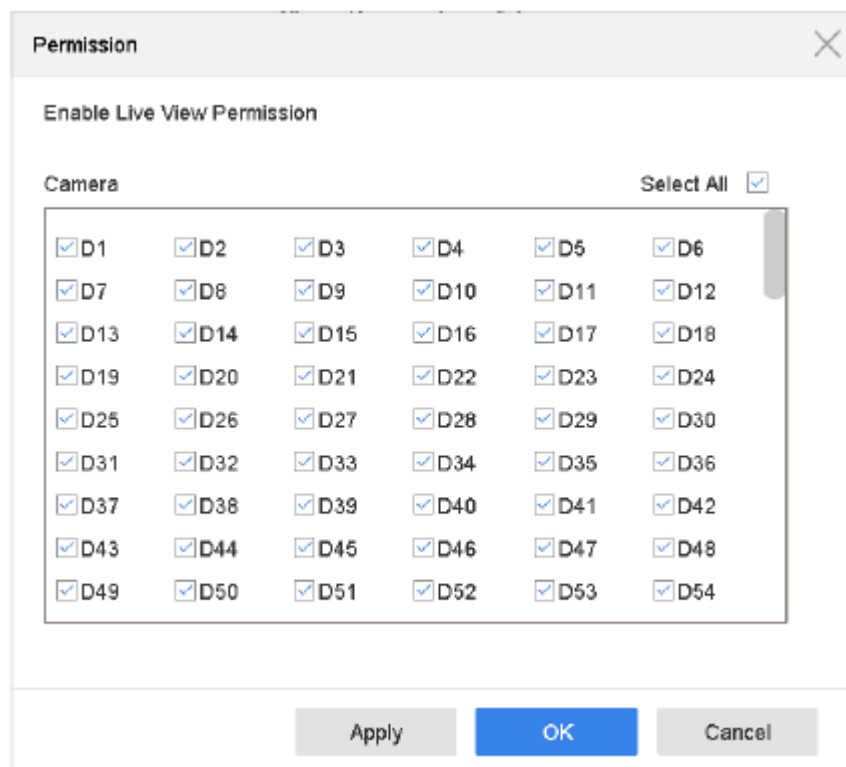



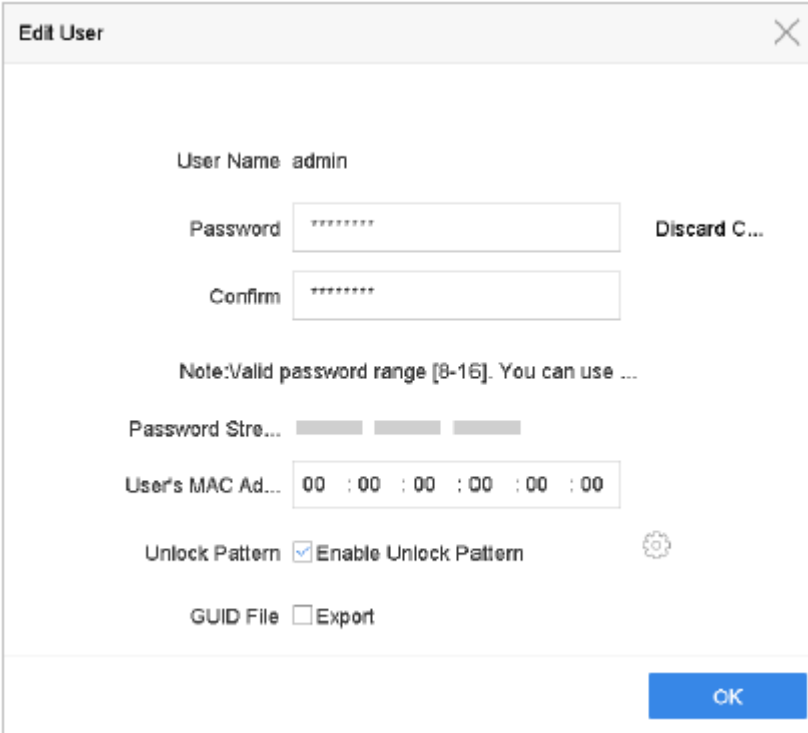
Figure 19-8 Enable Live View Permission

- 5) Click  of non-admin user.
- 6) Enter **Camera Configuration** tab.
- 7) Select Camera Permission as **Local Live View**.
- 8) Select cameras to live view.
- 9) Click **OK**.

19.4.4 Edit the Admin User

The admin user account can modify its password and the unlock pattern.

- 1) Go to **System > User**.
- 2) Select the admin user from the list and 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:** A text box containing seven asterisks (*****). To its right is a "Discard C..." button.
- Confirm:** A text box containing seven asterisks (*****).
- Note:** Valid password range [8-16]. You can use ...
- Password Stre...:** A progress indicator consisting of three horizontal bars.
- User's MAC Ad...:** A text box containing the MAC address 00 : 00 : 00 : 00 : 00 : 00.
- Unlock Pattern:** A checkbox labeled "Enable Unlock Pattern" which is checked. To its right is a gear icon.
- GUID File:** A checkbox labeled "Export" which is unchecked.
- OK:** A blue button at the bottom right of the dialog.

Figure 19-9 Edit User (Admin)

- 3) Edit the admin user information as required, including the new admin password (strong password is required) and MAC address.
- 4) Edit the unlock pattern for the admin user account.
 - 1) Check the checkbox of **Enable Unlock Pattern** to enable the use of unlock pattern when logging in to the device.
 - 2) Use the mouse to draw a pattern from the 9 dots on the screen, and release the mouse when the pattern drawing is complete.

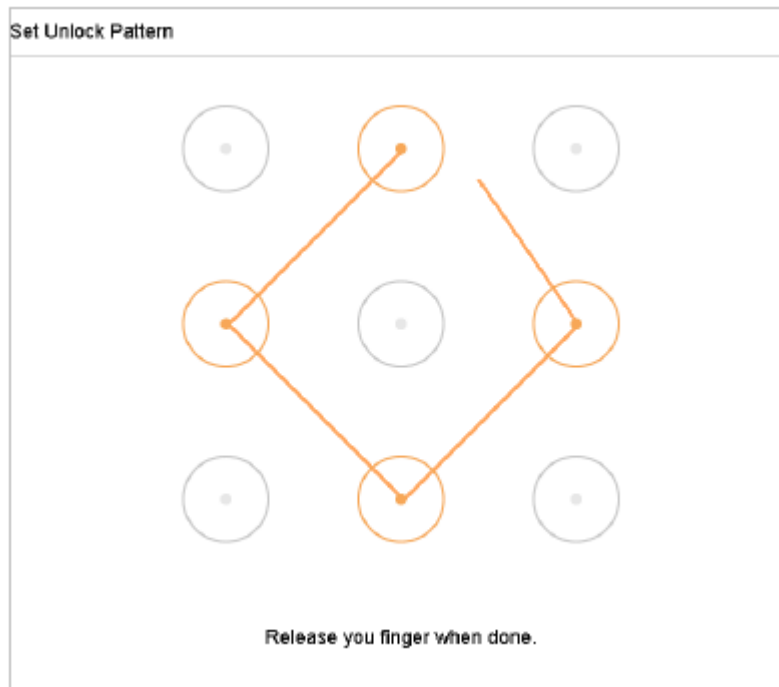




Figure 19-10 Set Unlock Patter for Admin User

- 5) Click  in the **Export GUID** to enter the reset password interface to export the GUID file for the admin user account.

 **NOTE**

When the admin password is changed, you can export the new GUID to the connected USB flash disk in the Import/Export interface for future password resetting.

- 6) Click the **OK** button to save the settings.
- 7) For the **Operator** or **Guest** user account, you can also click the  button on the user management interface to edit permissions.

19.4.5 Edit the Operator/Guest User

You can edit the user information, including user name, password, permission level and MAC address. Check the checkbox of **Change Password** if you want to change the password, and input the new password in the **Password** text field, and **Confirm**. A strong password is recommended.

- 1) Go to **System > User**.
- 2) Select a user from the list and click **Modify**.

Figure 19-11 Edit User (Operator/Guest)

- 3) Edit the user information as required, including the new password (strong password is required) and MAC address.

19.4.6 Delete a User

The admin user account has the permission to delete the operator/guest user account.

- 1) Go to **System > User**.
- 2) Select a user from the list.
- 3) Click **Delete** to delete the selected user account.

Chapter 20 Appendix

20.1 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 device, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **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
- **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.
- **PPPoE:** Stands for "Point-to-Point Protocol over Ethernet." PPPoE is a network configuration used for establishing a PPP connection over an Ethernet protocol.
- **Hybrid device:** A hybrid device is a combination of a DVR and device.
- **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.
- **Device:** Acronym for Network Video Recorder. A device can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other devices.
- **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.

20.2 Troubleshooting

No image displayed on the monitor following normal startup**Possible reasons include:**

- No VGA or HDMI connections.
 - Connection cable is damaged.
 - Input mode of the monitor is incorrect.
- 1) Verify that the device is connected to the monitor via HDMI or VGA cable.
 - 2) If not, please connect the device with the monitor and reboot.
 - 3) Verify the connection cable is good.
 - 4) If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.
 - 5) Verify Input mode of the monitor is correct.
 - 6) Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of device is HDMI output, then the input mode of monitor must be the HDMI input). And if not, please modify the input mode of monitor.
 - 7) Check if the fault is solved in Step 1 to Step 3.
 - 8) If it is solved, finish the process. If not, please contact a Hikvision engineer for further assistance.

A “Di-Di-Di-DiDi” warning sounds after a newly bought device starts up**Possible reasons include:**

- No HDD is installed in the device.
 - The installed HDD has not been initialized.
 - The installed HDD is not compatible with the device, or is broken.
- 1) Verify that at least one HDD is installed in the device.
 - If not, install a compatible HDD.
 - If you do not wish to install an HDD, go to **Menu > System > Event > Normal Event > Exception**, and uncheck the “HDD Error” **Audible Warning** checkbox.
 - 2) Verify that the HDD is initialized.
 - 1) Go to **Menu > Storage > Storage Device**.
 - 2) If the status of the HDD is “Uninitialized”, please check the corresponding HDD checkbox and click the “**Init**” button.
 - 3) Verify that the HDD is detected or is in good condition.
 - 1) Select **Menu > Storage > Storage Device**.
 - 2) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to requirements.
 - 4) Check if the fault is solved by performing steps 1 to 3. If it is solved, finish the process. If not, please contact a Hikvision engineer for further assistance.

The status of the added IP camera displays as “Disconnected” when it is connected through Private Protocol.



Select **Menu > Camera > Camera > IP Camera** to get the camera status.

Possible reasons include:

- Network failure, and the device and IP camera lost connections.
 - The configured parameters are incorrect when adding the IP camera.
 - Insufficient bandwidth.
- 1) Verify that the network is connected.
 - 1) Connect the device and PC using the RS-232 cable.
 - 2) Open the Super Terminal software, and execute the ping command. Input "ping IP" (e.g. ping 172.6.22.131).



Simultaneously press **Ctrl** and **C** to exit the ping command. If there is return information and the time value is small, the network is normal.

- 2) Verify that the configuration parameters are correct.
 - 1) Go to **Menu > Camera**.
 - 2) Verify that the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.
- 3) Verify that the bandwidth is acceptable.
 - 1) Go to **Menu > Maintenance > Net Detect > Network Stat**.
 - 2) Check the access bandwidth usage, and see if the total bandwidth has reached its limit.
- 4) Check if the fault is solved by steps 1 to 3. If resolved, finish the process. If not, please contact a Hikvision engineer for further assistance.

The IP camera frequently goes online and offline and its status is displayed as "Disconnected"

Possible reasons include:

- The IP camera and the device versions are not compatible
 - Unstable IP camera power supply
 - Unstable network between IP camera and device
 - Limited flow through the switch that connects the IP camera and device
- 1) Verify that the IP camera and device versions are compatible.
 - 1) Go to **Menu > Camera**, and view the firmware version of the connected IP camera.
 - 2) Go to **Menu > Maintenance > System Info > Device Info** and view the firmware version of device.
 - 2) Verify that the power supply of the IP camera and device is stable.
 - 1) Verify that the power indicator is normal.

- 2) When the IP camera is offline, try the ping command on the PC to check if the PC connects with the IP camera.
- 3) Verify that the network between IP camera and device is stable.
 - 1) When the IP camera is offline, connect the PC and device with the RS-232 cable.
 - 2) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there are signs of packet loss.

**NOTE**

Simultaneously press **Ctrl** and **C** to exit the ping command.

Example: Input ping 172.6.22.131 -l 1472 -f.

- 4) Verify that the switch is not in flow control. Check the brand and model of the switch that connects the IP camera and the device, and contact the manufacturer of the switch to check if it is equipped with the flow control function. If so, please turn it down.
- 5) Check if the fault can be solved by steps 1 to 4. If solved, finish the process. If not, contact a Hikvision engineer for further assistance.

There is no monitor connected to the local device. When you are managing an IP camera that is remotely connected to the device by web browser, the status shows as "Connected", and you connect the device to the monitor via VGA or HDMI interface and reboot the device, a black screen is displayed.

When a device is connected to a monitor before startup via a VGA or HDMI interface, the IP camera connects to the device locally or remotely, and the status of IP camera displays as "Connected", but when a the device is connected to CVBS, a black screen is also displayed.

Possible reasons include:

After connecting the IP camera to the device, the image outputs via the main spot interface by default.

- 1) Enable the output channel.
- 2) Go to **Menu > System > Live View > General**, and select video output interface in the drop-down list and configure the window that you wish to view.

**NOTE**

View settings can only be configured via local device operation.

Different camera orders and window-division modes can be set for different output interfaces separately. Digits such as "D1" and "D2" represent a channel number, and "X" indicates that the selected window has no image output.

- 3) Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

Live view stuck when video is outputed locally.

Possible reasons include:

- Poor network between the device and IP camera, and there is packet loss during transmission.
 - The frame rate has not reached a real-time frame rate.
- 1) Verify the network connection between the device and IP camera.
 - When the image is stuck, connect the RS-232 ports on the PC and the rear panel of the device using the RS-232 cable.
 - Open the Super Terminal, and execute the "**ping 192.168.0.0 -l 1472 -f**" (the IP address may change according to the real condition) command, and check for the packet loss.

**NOTE**

Simultaneously press **Ctrl** and **C** to exit the ping command.

- 2) Verify that the frame rate is real-time frame rate.
- 3) Go to **Menu > Camera > Encoding Parameters**, and set the **Frame rate** to **Full Frame**.
- 4) Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

Live view is stuck when the video outputs remotely via Internet Explorer or platform software.

Possible reasons include:

- Poor network between the device and IP camera, as well as packet loss during transmission.
 - Poor network between the device and PC, and packet loss during transmission.
 - Hardware performance, including CPU, memory, etc., is not enough
- 1) Verify that the network between the device and IP camera is connected.
 - 1) When the image is stuck, connect the RS-232 ports on the PC and the rear panel of the device with the RS-232 cable.
 - 2) Open the Super Terminal, and execute the "**ping 192.168.0.0 -l 1472 -f**" (the IP address may change according to the real condition) command, and check for packet loss.

**NOTE**

Simultaneously press **Ctrl** and **C** to exit the ping command.

- 2) Verify that the network between the device and PC is connected.
 - 1) Open the cmd window in the **Start** menu, or press the "Windows + R" shortcut key to open it.
 - 2) Use the ping command to send a large packet of data to the device, execute the "**ping 192.168.0.0 -l 1472 -f**" command (the IP address may change according to the real condition), and check if there is packet loss.

**NOTE**

Simultaneously press **Ctrl** and **C** to exit the ping command.

- 3) Verify that the PC hardware is adequate.
 - 1) Simultaneously press **Ctrl, Alt** and **Delete** to enter the windows task management interface, as shown in the following figure.

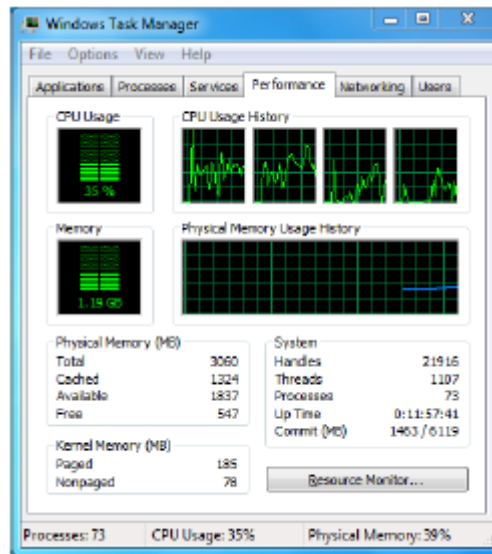


Figure 20-1 Windows task management interface

- 2) Select the "**Performance**" tab; check the status of the CPU and Memory.
- 3) If the resources are not enough, please end unnecessary processes.
- 4) Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further assistance.

When using the device to obtain live view audio, there is no sound, too much noise, or the volume is too low.

Possible reasons include:

- The stream type is not set as "**Video & Audio**".
- The encoding standard is not supported by device.
- Verify that the cable between the pickup and IP camera is connected well; impedance matches and compatible.
- Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.
- Verify the setting parameters are correct.
 - 1) Go to **Menu > Camera > Encoding Parameters**, and set the Stream Type as "**Audio & Video**".
- 1) Verify the audio encoding standard of the IP camera is supported by the device. The device supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.
- 5) Check if the fault is solved by the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further assistance.

The image becomes stuck when the device performs single or multi-channel playback.

Possible reasons include:

- Poor network between device and IP camera, and there exists packet loss during the transmission.
- The frame rate is not the real-time frame rate.
- Frame extracting may occur for devices that support up to 16-channel synchronized playback at a resolution of 4CIF, which leads to the image becoming stuck.

1) Verify the network between device and IP camera is connected.

- 1) When the image is stuck, connect the RS-232 ports on the PC and the rear panel of the device with the RS-232 cable.
- 2) Open the Super Terminal, and execute the "**ping 192.168.0.0 -l 1472 -f**" (the IP address may change according to the real condition) command, and check if there is packet loss.

**NOTE**

Simultaneously press the **Ctrl** and **C** to exit the ping command.

2) Verify that the frame rate is the real-time frame rate.

- Select **Menu > Record > Parameters > Record**, and set the **Frame Rate** to "**Full Frame**".

3) Verify that the hardware can manage playback. Reduce the playback channel number.

- Go to **Menu > Camera > Encoding Parameters**, and set the resolution and bitrate to a lower level.

4) Reduce the local playback channel number.

- Go to **Menu > Playback**, and uncheck unnecessary channel checkboxes.

5) Check if the fault is solved in the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further assistance.

No record file found in the device's local HDD, followed by a "No record file found" prompt.**Possible Reasons:**

- The time setting of the system is incorrect.
- The search condition is incorrect.
- HDD error or HDD not detected.

1) Verify that the system time setting is correct.

- Go to **Menu > System > General**, and verify that the "Device Time" is correct.

2) Verify that the search condition is correct.

- Go to the playback interface, and verify that the channel and time are correct.

3) Verify that the HDD status is normal.

- Go to **Menu > Storage > Storage Device** to view the HDD status, and verify that the HDD is detected and can be read and written normally.

4) Check if the fault is solved in the above steps. If it is solved, finish the process. If not, contact a Hikvision engineer for further assistance.