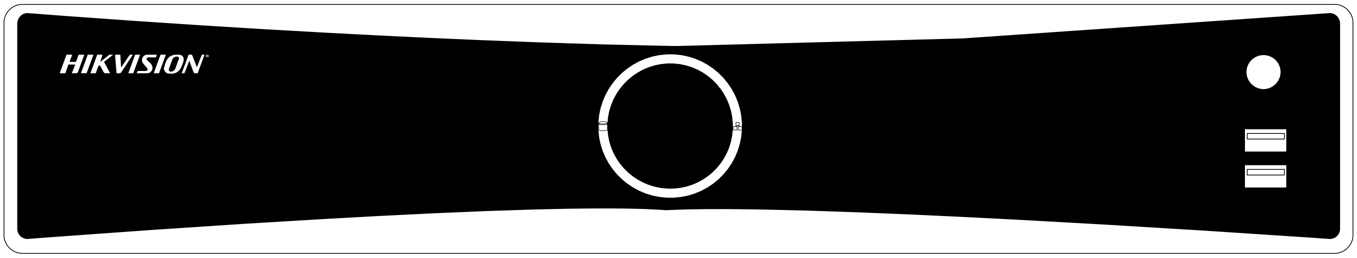


DS-7716NXI-I4/16P/4S
DS-7732NXI-I4/16P/4S

Network Video Recorder

User Manual

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

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 TO THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED FOR 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 verificationcode, 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
ℹ 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.

CONTENTS

Product Key Features

General

- Connectable to network cameras, network dome, and encoders
- Connectable to the third-party network cameras such as ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek, ZAVIO, and cameras that adopt the 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 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
- RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 are supported
- Hot-swappable RAID storage scheme, 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
- Eight 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 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.265+ to ensure high video quality with lowered bitrate

Backup

- Export video data by USB, SATA, or eSATA device
- Export video clips when using 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, HDD full, etc.
- POS triggered alarm supported
- VCA detection alarm is supported
- VCA search for face detection vehicle plate, 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™
- 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 supports 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

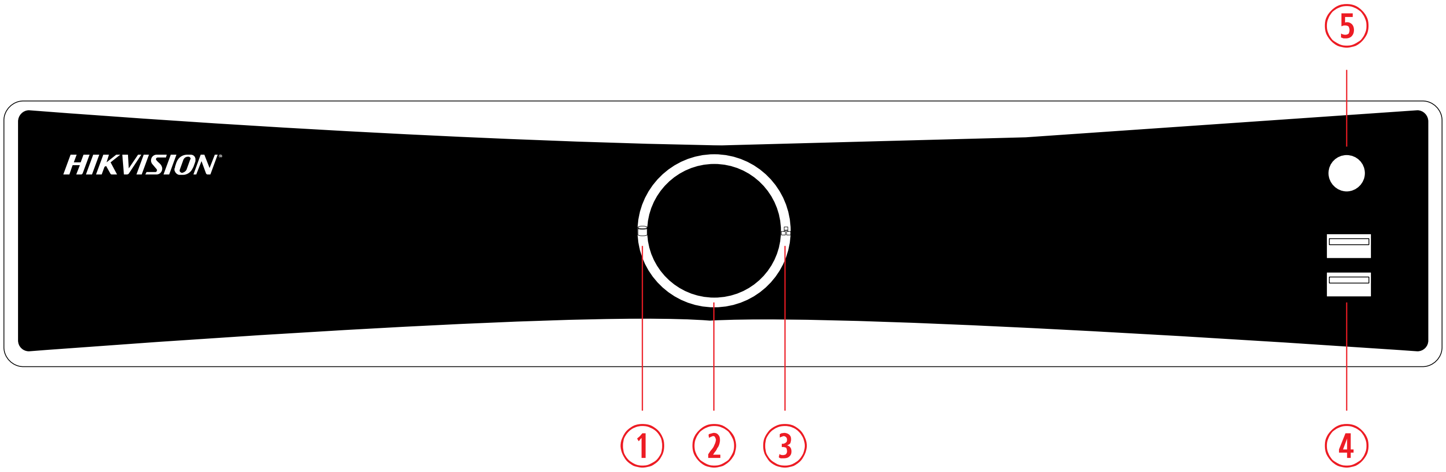


Figure 1-1 Front Panel

Table 1-1 Front Panel Description

No.	Name	Function Description
1	HDD LED Indicator	• **Solid White:** HDD is abnormal • **Flashing White:** HDD is reading/writing • **Unlit:** No HDD is detected
2	Power Ring LED Indicator	• **Solid White:** Device is running normally • **Breathing Light:** Device is shut down • **Unlit:** No power supply is connected
3	Network LED Indicator	• **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-77xxNXI-I4/16P/4S Series

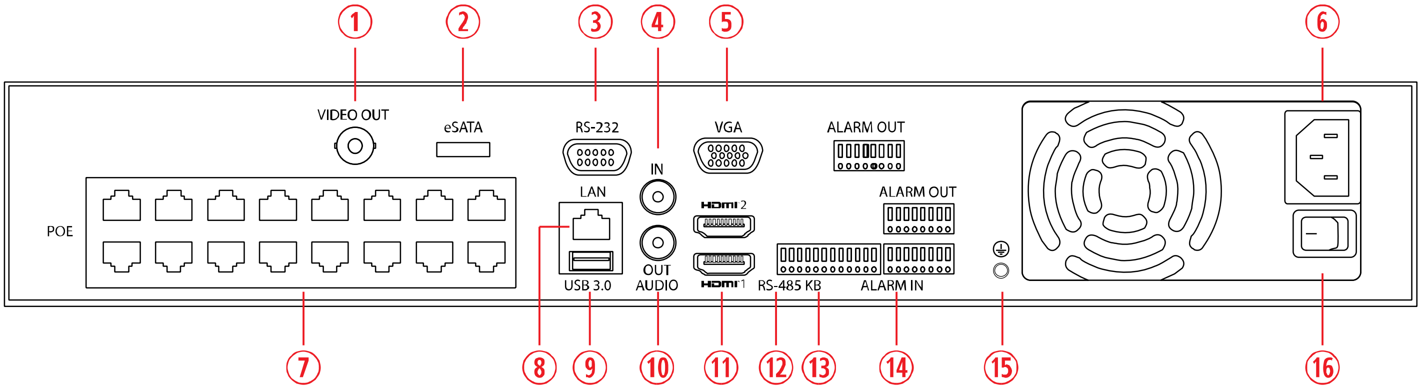


Figure 1-4 Rear Panel

Table 1-5 Rear Panel Description

No.	Name	Description
θ	Video Out	CVBS video output
ω	eSATA	Connects external SATA HDD, CD/DVD-RM
ε	RS-232	Connector for RS-232 device
ρ	Audio In	RCA connector for audio input
τ	VGA	DB9 connector for VGA output. Display local video output and menu
ψ	Power Supply	100 to 240 VAC power supply
υ	PoE	RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
ι	LAN	1 RJ-45 interface. 10/100/1000 Mbps self-adaptive Ethernet
ο	USB 3.0	Universal Serial Bus (USB) 3.0 port for additional device such as USB mouse and USB Hard Disk Drive (HDD)
1)	Audio Out	RCA connector for audio output
1!	HDMI1 and HDMI2	2 x HDMI video output connectors
1≅	RS-485	Connector for RS-485 device
1#	Controller Port/Keyboard	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next NVR.
1∃	Alarm In/Out	Connector for alarm input/output
1%	GND	Ground
1⊥	Power Switch	Switch for turning on/off the device

1.3 IR Remote Control Operations

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

NOTE
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.
3. On the IR Remote: 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#.

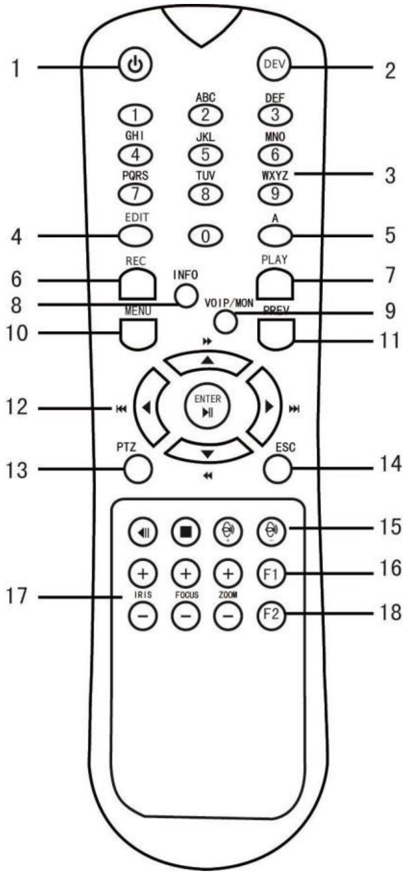


Figure 1-2 Remote Control

1.3.2 Unpairing (Disabling) IR Remote from Device

To unpair an IR Remote from a device so that the unit cannot control any device functions, 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.

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

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

Table 1-2 IR Remote Functions

No.	Name	Function Description
1	**POWER ON/OFF**	To Turn Power On: - If User Has Not Changed the Default device Device ID# (255): 1. Press Power On/Off button (1). - If User Has Changed the device Device ID#: 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. To Turn Device Off: - If User Is Logged On: 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: 1. Hold Power On/Off button (1) down for five seconds to display the user name/password prompt. 2. Press Enter button (12) to display the on-screen keyboard. 3. Input user name. 4. Press Enter button (12) to accept input and dismiss the on-screen keyboard. 5. Use 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 Enter button (12) to accept input and dismiss the on-screen keyboard. 8. Press 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. User name/password prompt depends on device configuration. See "System Configuration" section.
2	**DEV**	Enable IR Remote: Press DEV button, enter device Device ID# with number keys, press Enter to pair unit with the device
		Disable IR Remote: Press DEV button to clear Device ID#; unit will no longer be paired with the device
3	**Numerals**	Switch to the corresponding channel in Live View or PTZ Control mode Input numbers in Edit mode
4	**EDIT**	Delete characters before cursor Check the checkbox and select the ON/OFF switch
5	**A**	Adjust focus in the PTZ Control menu Switch on-screen keyboards (upper and lower case alphabet, symbols, and numerals)
6	**REC**	Enter Manual Record setting menu Call a PTZ preset by using the numeric buttons in PTZ control settings Turn audio on/off in Playback mode
7	**PLAY**	Go to Playback mode Auto scan in the PTZ Control menu
8	**INFO**	Reserved
9	**VOIP**	Switches between main and spot output Zooms out the image in PTZ control mode
10	**MENU**	Return to Main menu (after successful login) N/A Show/hide full screen in Playback mode
12	**DIRECTION**	Navigate between fields and menu items Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 30 secs in Playback mode Cycle through channels in Live View mode Control PTZ camera movement in PTZ control mode
	ENTER	Confirm selection in any menu mode Checks checkbox Play or pause video in Playback mode Advance video a single frame in single-frame Playback mode Stop/start auto switch in auto-switch mode
13	**PTZ**	Enter PTZ Control mode
14	**ESC**	Go back to previous screen N/A
15	**RESERVED**	Reserved
16	**F1**	Select all items on a list N/A Switch between play and reverse play in Playback mode
17	**PTZ Control**	Adjust PTZ camera iris, focus, and zoom
18	**F2**	Cycle through tab pages Switch between channels in Synchronous Playback mode

1.3.3 Troubleshooting the IR Remote

NOTE

Make sure you have installed batteries properly in the remote control. And you have to 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 procedure below to troubleshoot.

1. Go to **System** > **General** by operating the front control panel or the mouse.
2. Check and remember 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 IR remote control is operating properly. If the Status indicator does not turn blue and there is still no response from the IR remote, check the following:

- Batteries are installed correctly and the polarities of the batteries are not reversed
- Batteries are fresh and not out of charge
- IR receiver is not obstructed
- No fluorescent lamp is used nearby

If the remote still can't function properly, change remote and try again, or contact the device provider.

1.4 USB Mouse Operation

A standard 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. If in a 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 Mouse Control Description

Name	Action	Description
Left-Click	Single-Click	• 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	• 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	• Live View: Show menu • Menu: Exit current menu to upper level menu
Scroll-Wheel	Scrolling Up	• Live View: Previous screen • Menu: Previous item
	Scrolling Down	• 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.

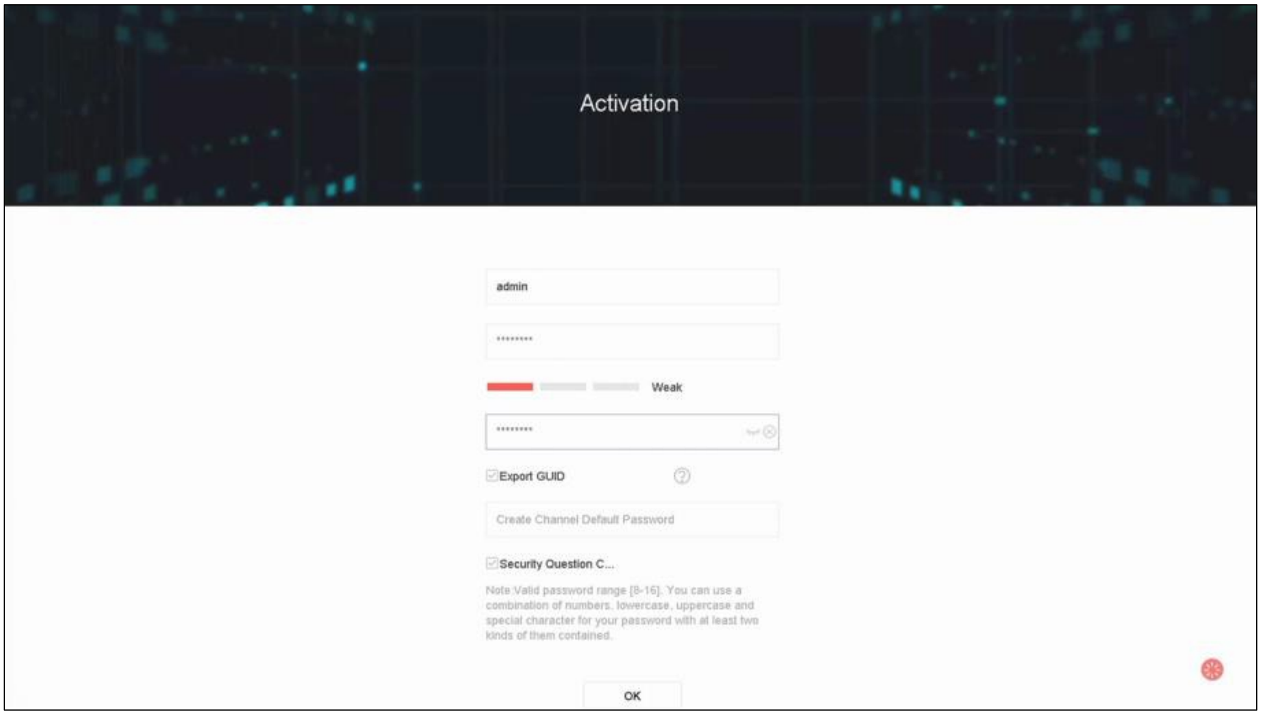
1. Connect the device power supply interface and electrical socket with delivered power cable. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power button on the front panel should be red, indicating the device is receiving power.

2.2 Activate the Device

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

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

NOTE
You can click ⌣ to show the characters input.



Activation

admin

****

Weak

****

☑ Export GUID

Create Channel Default Password

☑ Security Question C...

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

OK

Figure 2-1 Activating the Device

WARNING

We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in 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 used to reset the password.
4. Click **OK**.

What To Do Next:

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

NOTE

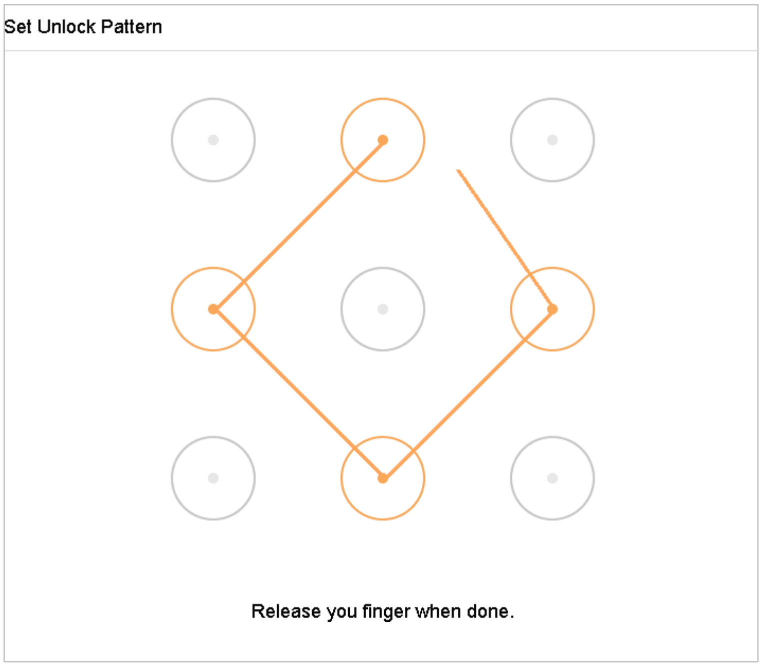
After the device is activated, safely keep the password.

You can duplicate the password to the IP cameras that are connected with default protocol.

2.3 Configure Unlock Pattern for Login

The admin user can configure the unlock pattern for device login.

1. After the device is activated, enter the following interface to configure the device unlock pattern.
2. Hold the left mouse button down and use the mouse to draw a pattern among the nine dots on the screen. Release the mouse button when the pattern is done.



Set Unlock Pattern

Release you finger when done.

Figure 2-2 Draw the Pattern

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.

NOTE

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

2.4 Log in to the Device

2.4.1 Login via Unlock Pattern

NOTE

Only the *admin* user has permission to unlock the device.

Configure the pattern before unlocking. 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.

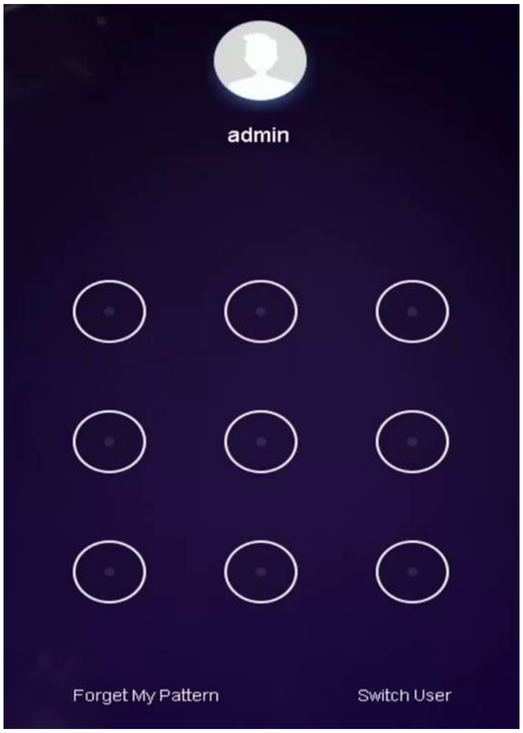


Figure 2-3 Draw the Unlock Pattern

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

NOTE

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

If the pattern you draw is different from the pattern you configured, try again.

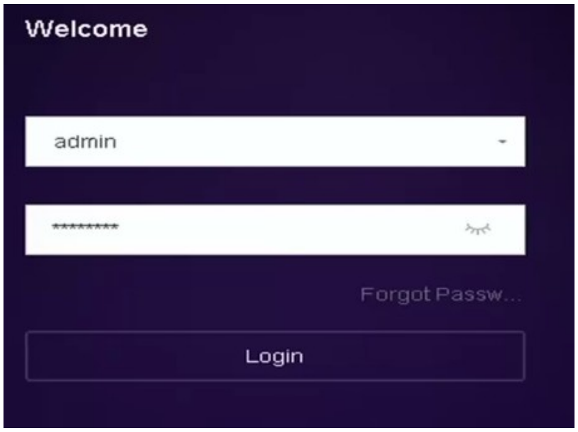
If you draw the wrong pattern more than five times, the system will switch to the normal login mode automatically.

2.4.2 Log in via Password

Purpose

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

1. Select the **User Name** in the drop-down list.


Welcome

admin

****

Figure 2-4 Login Interface

2. Input password.

3. Click **OK** to log in.

NOTE

If you forget the admin password, click **Forgot Password** to reset the password.

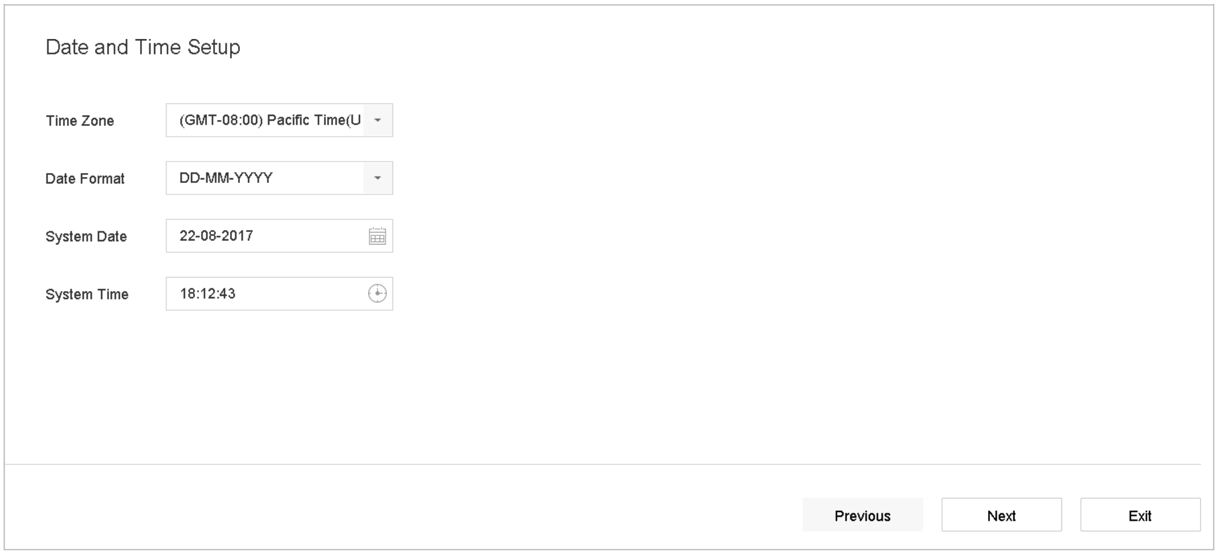
In the Login dialog box, if you enter the wrong password seven times, the current user account will lock for 60 seconds.

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 settings of the device. If you don't want to use the Setup Wizard at that time, click the **Exit** button.

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


Date and Time Setup

Time Zone: (GMT-08:00) Pacific Time(U

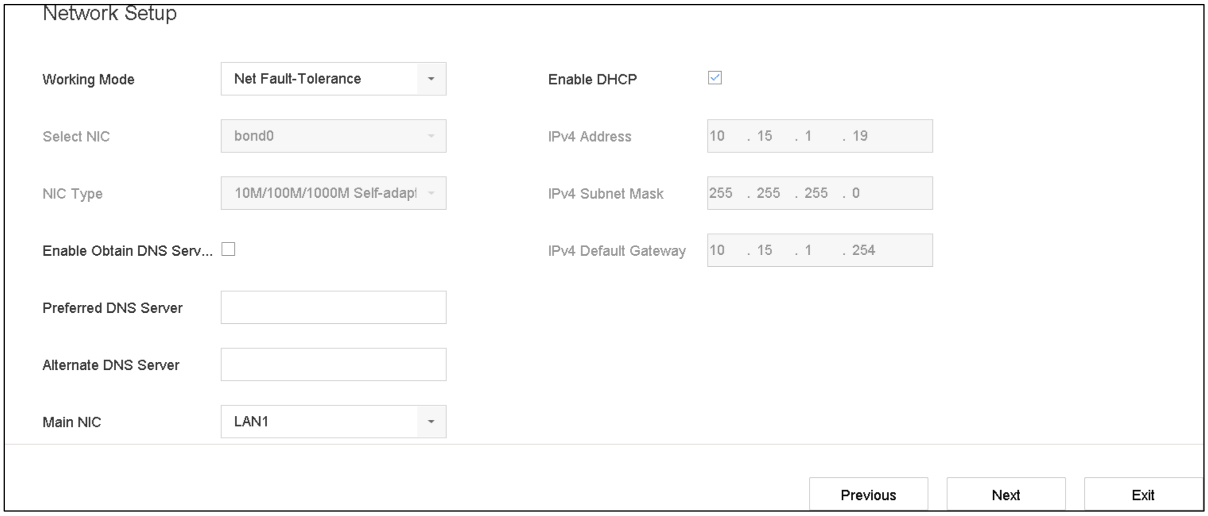
Date Format: DD-MM-YYYY

System Date: 22-08-2017

System Time: 18:12:43

Figure 2-5 Date and Time Settings

2. After the time settings, click **Next** to enter the Network Setup Wizard window.

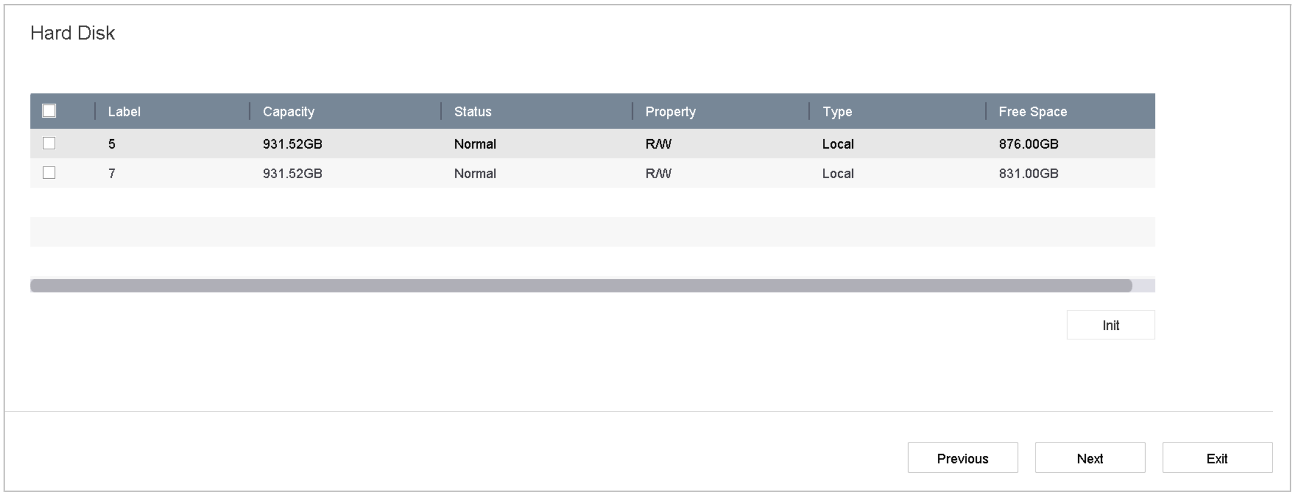


Network Setup

Working Mode	Net Fault-Tolerance	Enable DHCP	☑
Select NIC	bond0	IPv4 Address	10 . 15 . 1 . 19
NIC Type	10M/100M/1000M Self-adapt	IPv4 Subnet Mask	255 . 255 . 255 . 0
Enable Obtain DNS Serv...	☐	IPv4 Default Gateway	10 . 15 . 1 . 254
Preferred DNS Server			
Alternate DNS Server			
Main NIC	LAN1		

Figure 2-6 Network Settings

3. Click **Next** after you configure the network parameters, to take you to the **HDD Management** window.



Hard Disk

☐	Label	Capacity	Status	Property	Type	Free Space
☐	5	931.52GB	Normal	R/W	Local	876.00GB
☐	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.

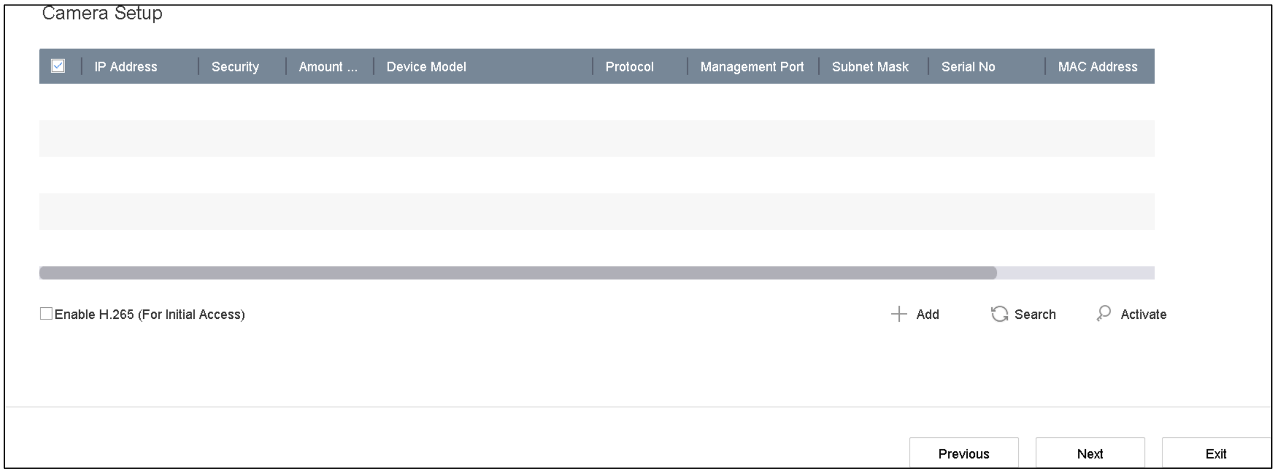
5. Click **Next**. You enter the **Camera Setup** interface to add IP cameras.

   - Click **Search** to search for online IP cameras. Before adding a camera, make sure the IP camera to be added is in active status.

   - Click **Add** to add the camera.

NOTE

If the camera is in inactive status, select the camera from the list and click **Activate** to activate it.



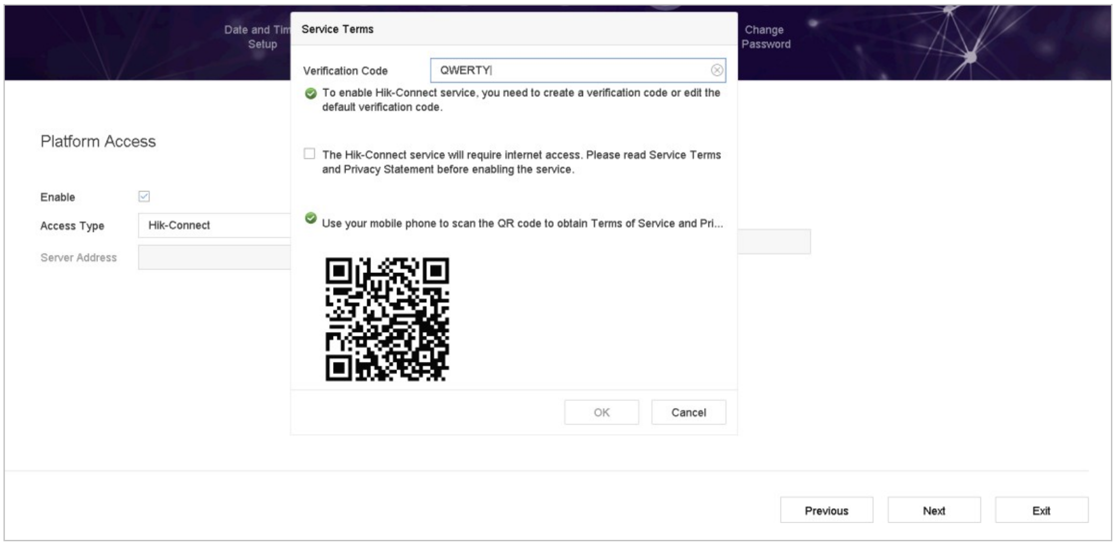
Camera Setup

☑	IP Address	Security	Amount ...	Device Model	Protocol	Management Port	Subnet Mask	Serial No	MAC Address

□Enable H.265 (For Initial Access)

Figure 2-8 Search for IP Cameras

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



Platform Access

Enable ☑

Access Type: Hik-Connect

Server Address

Service Terms

Verification Code: QWERTY

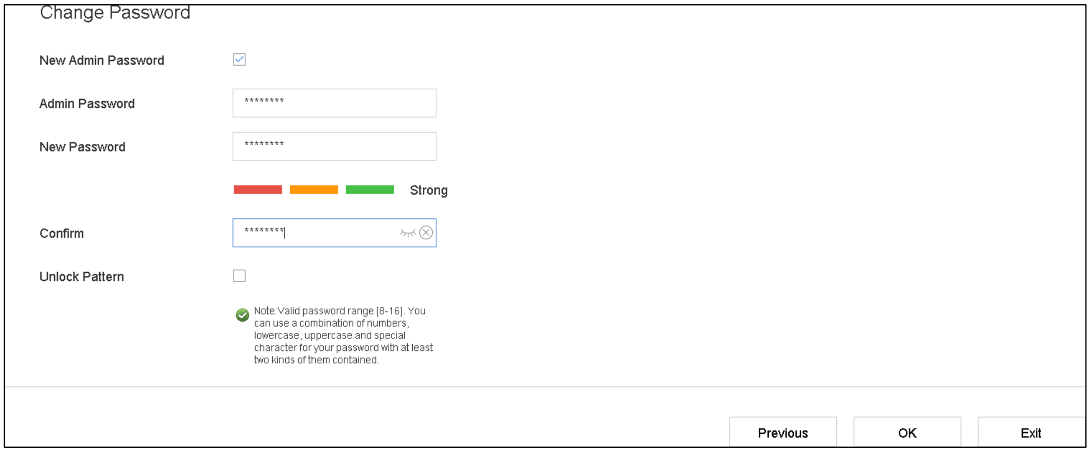
To enable Hik-Connect service, you need to create a verification code or edit the default verification code.

□ The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service.

Use your mobile phone to scan the QR code to obtain Terms of Service and Pri...

Figure 2-9 Hik-Connect Access

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



Change Password

New Admin Password ☑

Admin Password: ********

New Password: ********

Strong

Confirm: ********

Unlock Pattern □

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 2-10 Change Password

NOTE

You can enter click 👁 to show the characters input.

1) Check the **New Admin Password** checkbox.

2) Enter the original password in the **Admin Password** text field.

3) Input a new password in the **New Password** field.

4) Input the same new password in the **Confirm** field.

5) Check the **Unlock Pattern** to enable the unlock pattern login.

WARNING

We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in 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

Once you complete the wizard, right-click on the screen to pop up the main menu bar. Refer to the following figure and table for the main menu and sub-menus descriptions.

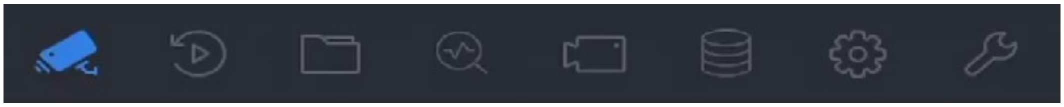


Figure 2-11 Main Menu Bar

Table 2-1 Description of Icons

Icon	Description	Icon	Description
📹	Live View	🎥	Camera Management
↺	Playback	🛢	Storage Management
📁	File Management	⚙	System Management
🔍	Smart Analysis	🔧	System Maintenance

2.7 System Operation

2.7.1 Log Out

Purpose

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

1. Click ⏻ on the menu bar.

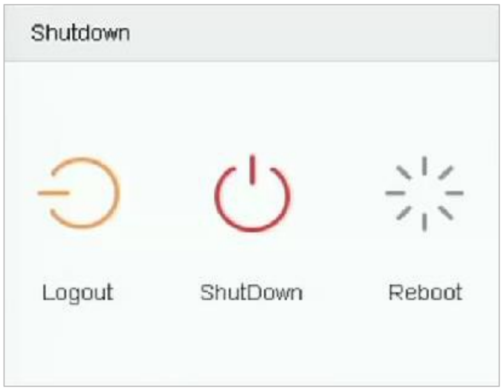


Figure 2-12 Logout

2. Click **Logout**.

NOTE

After you log out of the system, menu operation on the screen is invalid. You must input a user name and password to unlock the system.

2.7.2 Shut Down the Device

1. Click ⏻ on the menu bar.

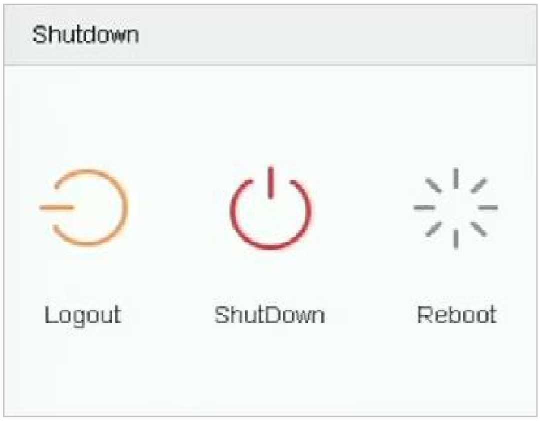


Figure 2-13 Shutdown Menu

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

NOTE

Do not press the POWER button again while 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 an IP Camera Manually

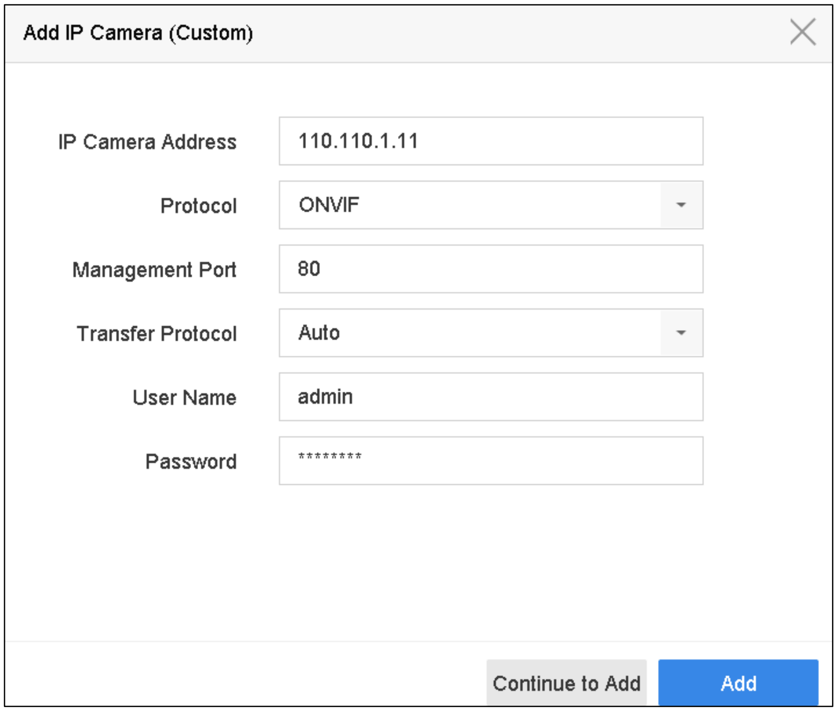
Purpose

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

Before You Start

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

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



Add IP Camera (Custom)

IP Camera Address	110.110.1.11
Protocol	ONVIF
Management Port	80
Transfer Protocol	Auto
User Name	admin
Password	********

Figure 3-1 Add IP Camera

3. Enter IP address, protocol, management port, and other IP camera information to add.
4. Enter the IP camera login user name and password.
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 Manage Cameras for PoE Device

Purpose
The PoE interfaces enable the device system to pass electrical power safely, along with data, on Ethernet cabling to the connected PoE cameras. The number of supported PoE cameras varies by device model.

For each PoE interface you disable, you can connect an online network camera, up to the maximum number of channels the NVR supports. The PoE interface supports Plug-and-Play.

For example, for a DS-7716NXI-I4/16P/4S, which has 16 PoE ports and 16 channels, if you want to connect eight network cameras via PoE interfaces and eight online cameras, you must disable eight PoE interfaces in the Edit IP Camera menu.

Follow the steps to add network cameras for device supporting PoE function.

3.2.1 Add PoE Cameras

1. Connect PoE cameras to the device PoE ports with network cables.

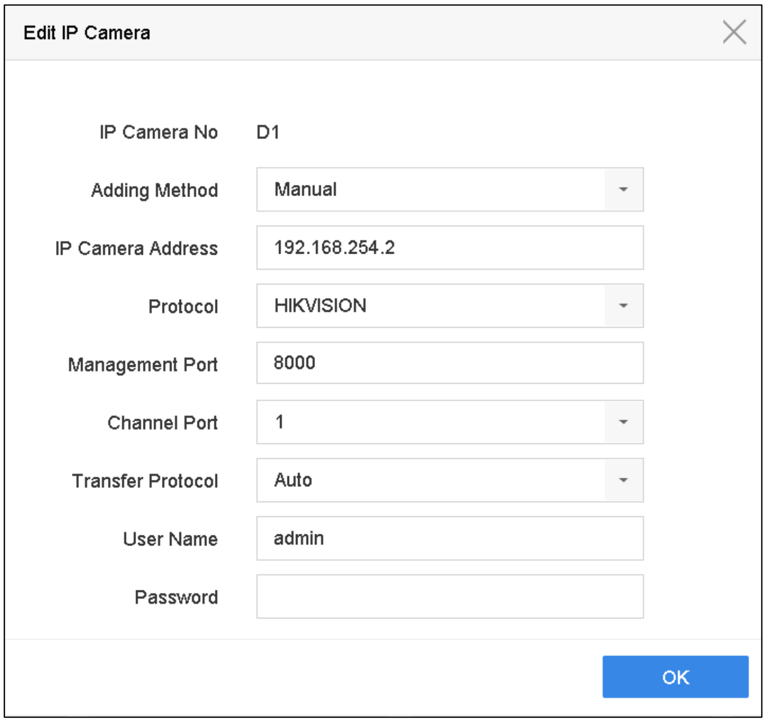
2. Go to **Camera > Camera > IP Camera** to view camera image and information.

3.2.2 Add Non-PoE IP Cameras

You can disable PoE interfaces by selecting manual, while the current channel can be used as a normal channel and the parameters can be edited.

1. Go to Camera > Camera > IP Camera.

2. Position the cursor on a window with no linked IP camera and click the ✎ button.



Edit IP Camera

IP Camera No	D1
Adding Method	Manual
IP Camera Address	192.168.254.2
Protocol	HIKVISION
Management Port	8000
Channel Port	1
Transfer Protocol	Auto
User Name	admin
Password	

Figure 3-2 Edit IP Camera

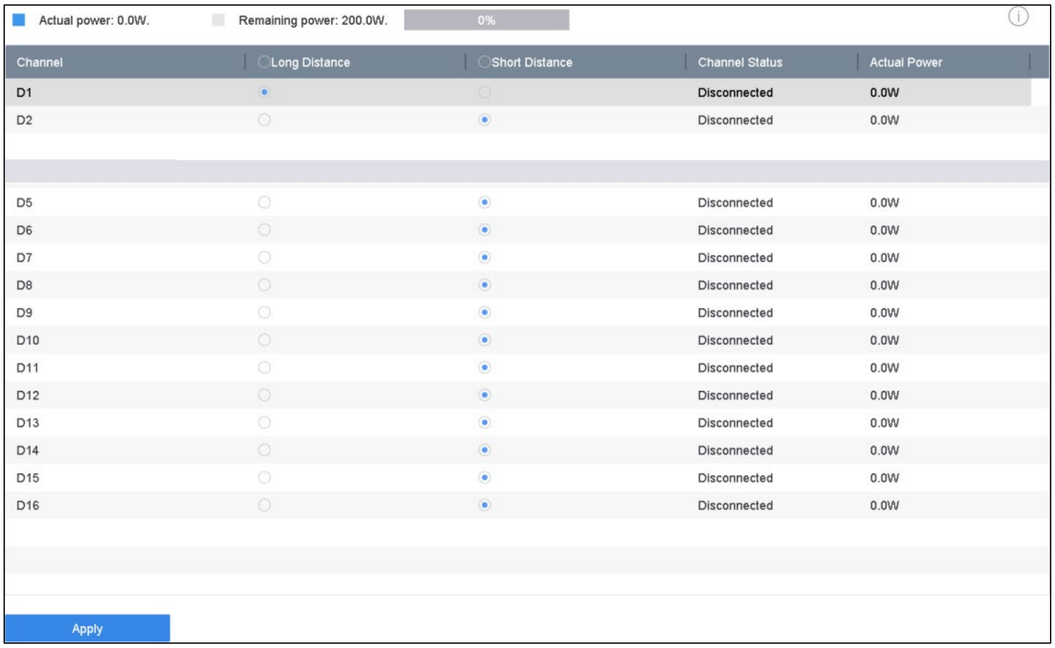
3. Set Adding Method to **Manual**.
   - **Plug-and-Play:** The camera is physically connected to the PoE interface. Its parameters cannot be edited. You can go to **System > Network > TCP/IP** to change IP address of PoE port.
   - **Manual:** Add IP camera without physical connection via the network.
4. Manually enter the IP address, the administrator user name, and administrator password.
5. Click **OK**.

3.2.3 Configure PoE Interface

Purpose

When requiring long-distance PoE transmission (100 to 300 m), enable long distance mode for the PoE channel.

1. Go to **Camera > Camera > PoE Settings**.
2. Enable or disable long network cable mode by selecting the relevant **Long Distance** or **Short Distance** radio button.
   - **Long Distance**: Long-distance (100 to 300 meters) network transmissions via PoE interface.
   - **Short Distance**: Short-distance (<100 meters) network transmission via PoE interface.



■ Actual power: 0.0W. □ Remaining power: 200.0W. 0%

Channel	○Long Distance	○Short Distance	Channel Status	Actual Power
D1	●	○	Disconnected	0.0W
D2	○	●	Disconnected	0.0W
D5	○	●	Disconnected	0.0W
D6	○	●	Disconnected	0.0W
D7	○	●	Disconnected	0.0W
D8	○	●	Disconnected	0.0W
D9	○	●	Disconnected	0.0W
D10	○	●	Disconnected	0.0W
D11	○	●	Disconnected	0.0W
D12	○	●	Disconnected	0.0W
D13	○	●	Disconnected	0.0W
D14	○	●	Disconnected	0.0W
D15	○	●	Disconnected	0.0W
D16	○	●	Disconnected	0.0W

Figure 3-3 PoE Settings

NOTE

The PoE ports are enabled with short distance mode by default.

The bandwidth connected to the IP camera PoE via a long network cable (100 to 300 meters) cannot exceed 6 MP.

The allowed maximum long network cable may be less than 300 meters depending on IP camera model and cable materials.

When the transmission distance reaches 100 to 250 meters, you must use Cat 5e or Cat 6 network cable to connect to the PoE interface.

When the transmission distance reaches 250 to 300 meters, you must use Cat 6 network cable to connect to the PoE interface.

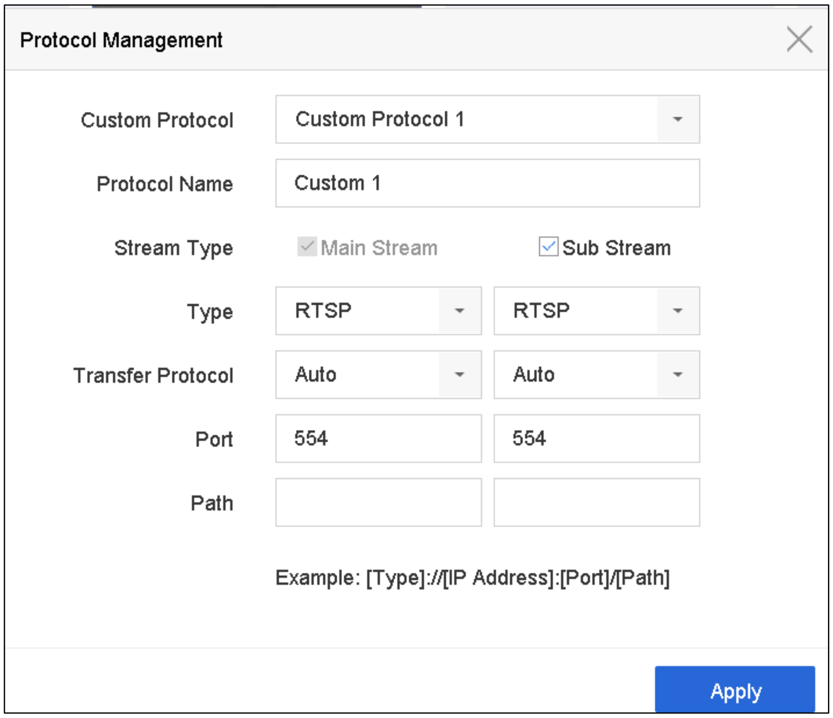
3. Click **Apply**.

3.3 Configure the Customized Protocols

Purpose

To connect network cameras that are not configured with standard protocols, you can configure customized protocols for them. The system provides 16 customized protocols.

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



Protocol Management

Custom Protocol: Custom Protocol 1

Protocol Name: Custom 1

Stream Type: ☑ Main Stream ☑ Sub Stream

Type: RTSP RTSP

Transfer Protocol: Auto Auto

Port: 554 554

Path:

Example: [Type]://[IP Address]:[Port]/[Path]

Figure 3-4 Protocol Management

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

   - **Type:** A network camera adopting a custom protocol must support getting a stream through standard RTSP.
   - **Path:** Contact the network camera manufacturer for the URL (uniform resource locator) needed to get the main stream and the sub-stream.

     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:

After adding the customized protocols, the protocol name will be listed in the drop-down list.

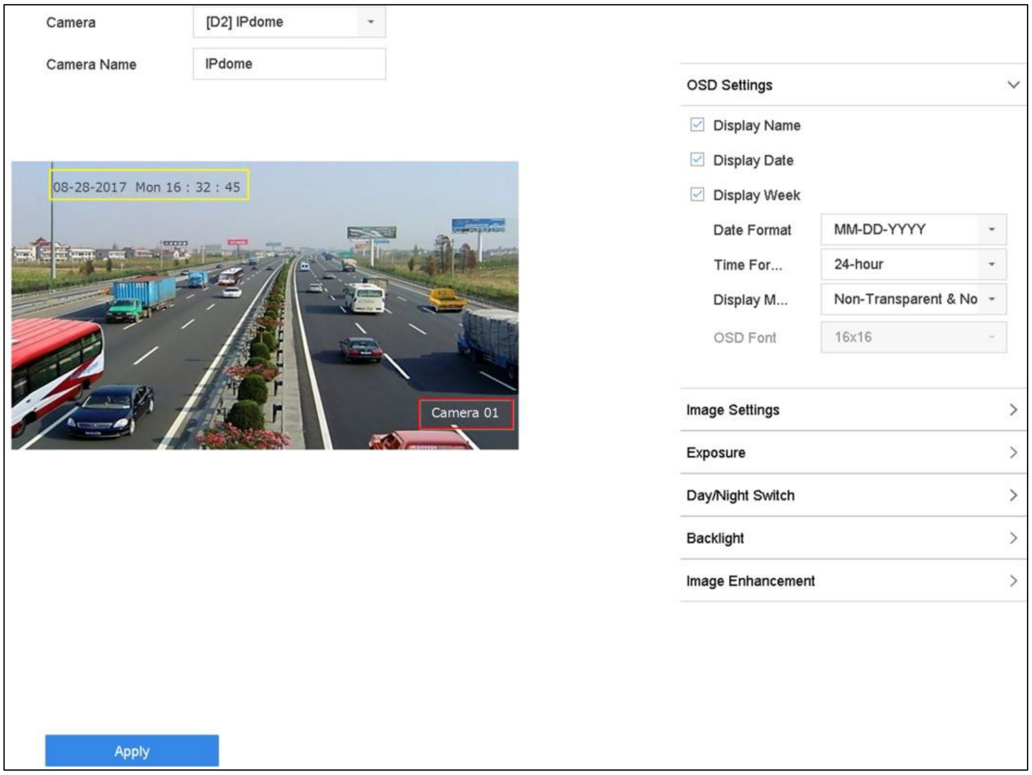
Chapter 4 Camera Settings

4.1 Configure OSD Settings

Purpose

You can configure the camera's OSD (On-screen Display) settings, 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 **Display Name**, **Display Date**, and **Display Week** checkbox(es) to show the information on the image.
5. Set the date format, time format, and display mode.



Camera: [D2] IPdome

Camera Name: IPdome

OSD Settings

☑ Display Name

☑ Display Date

☑ Display Week

Date Format: MM-DD-YYYY

Time For...: 24-hour

Display M...: Non-Transparent & No

OSD Font: 16x16

Figure 4-1 OSD Configuration Interface

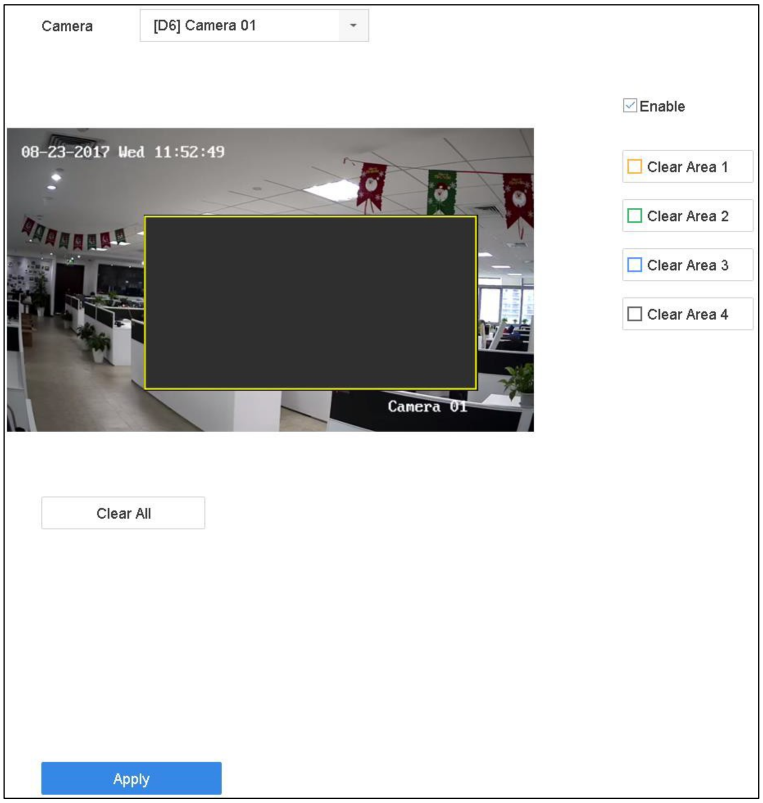
6. Use the mouse to click and drag the text frame on the preview window to adjust the OSD position.
7. Click the **Apply** button to apply the settings.

4.2 Configure Privacy Mask

Purpose

The privacy mask can 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 privacy mask.
3. Check 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.



Camera: [D6] Camera 01

☑ Enable

Figure 4-2 Privacy Mask Settings Interface

NOTE

Up to four privacy mask 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 brightness, contrast, live view saturation, 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. Set the day/night switch mode to **Day**, **Night**, **Auto**, or **Auto-Switch**.

    - **Auto**: The camera automatically switches between day mode and night mode according to the illumination.

      The sensitivity ranges from 0 to 7; higher sensitivity more easily triggers the mode switch.

      Switch time refers to the interval between the day/night switch. You can set it from 5 sec to 120 sec.

    - **Auto-Switch**: The camera switches day mode and night mode according to the start time and end time set.

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

4.5 Configure Other Camera Parameters

For a connected camera, you can configure camera parameters including 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 camera's exposure time (1/10000 to 1 sec). A longer exposure value results in a brighter image.
- **Backlight:** Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have a large 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 the video image 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, thus pressing ESC multiple times (depending on which menu you're on) takes you back to Live View mode.

5.1 Start Live View

1. The system automatically enters the live view interface when 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.

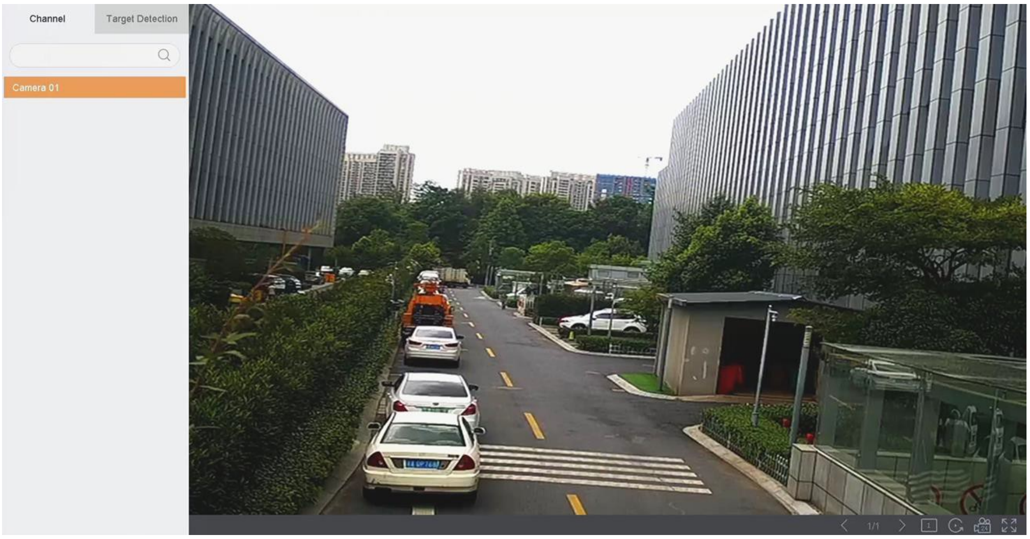


Figure 5-1 Live View

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

5.1.1 Digital Zoom

Digital Zoom zooms into the live image. You can zoom into the image at different magnifications (1x to 16x).

1. In 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 of the image to different magnifications (1 to 16x).

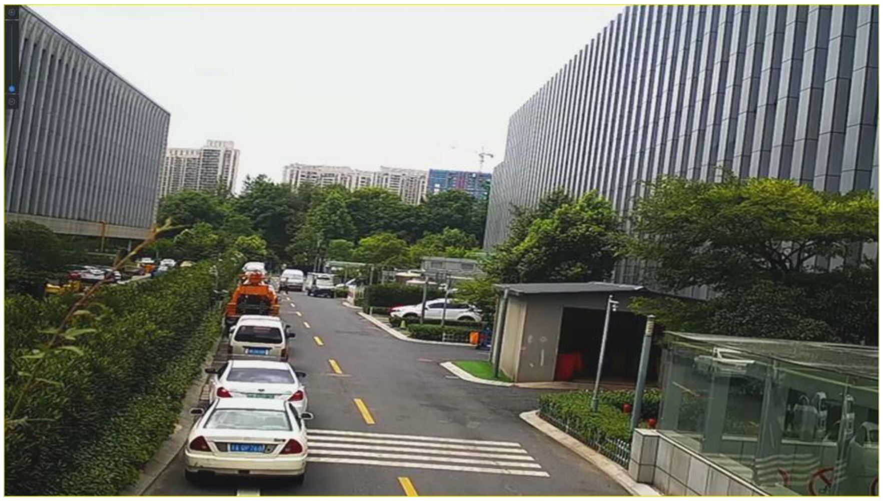


Figure 5-2 Digital Zoom

5.1.2 3D Positioning

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

1. In live view mode, click 3D to enter the 3D positioning mode.
2. Operate the zoom in/out in the image.
   - **Zoom In** – Use the left mouse key to click on the desired position in the video image, and drag a rectangular area in the lower right direction to zoom in.
   - **Zoom Out** – Use the left mouse key to drag a rectangular area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

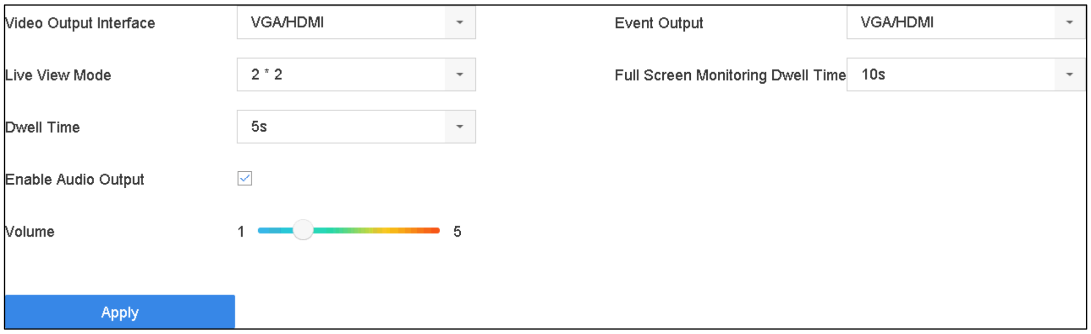
5.1.3 Live View Strategy

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

5.2 Configure Live View Settings

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

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



Video Output Interface	VGA/HDMI	Event Output	VGA/HDMI
Live View Mode	2 * 2	Full Screen Monitoring Dwell Time	10s
Dwell Time	5s		
Enable Audio Output	☑		
Volume	1 5		

Figure 5-3 Live View-General

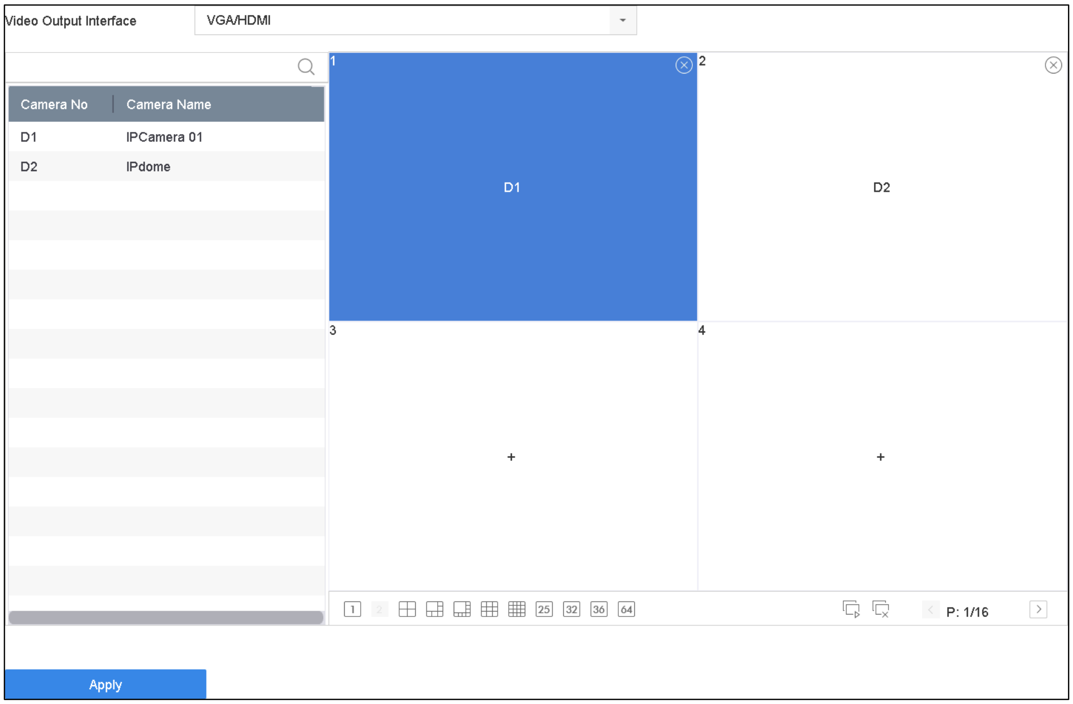
2. Configure the live view parameters.

- **Video Output Interface:** Select the video output to configure.
- **Live View Mode:** Select the display mode for live view, e.g., 2*2, 1*5, etc.
- **Dwell Time:** The time in seconds to wait between switching 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**.



Video Output Interface: VGA/HDMI

Camera No	Camera Name
D1	IPCamera 01
D2	IPdome

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 on the list to set the camera to the window.

NOTE

Enter the number in the text field to quickly search for the camera from the list.

You can also click-and-drag the camera to the desired window on the live view interface to set the camera order.

Related Operation:

- Click to start live view for all the channels.
- Click to stop all live views.

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

5.4 Configure Cameras' Auto-Switch

You can set the cameras' auto-switch 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*2, 1*5, etc.
- **Dwell Time:** The time in seconds to dwell between switching cameras when enabling auto-switch. The range is from 5s to 300s.

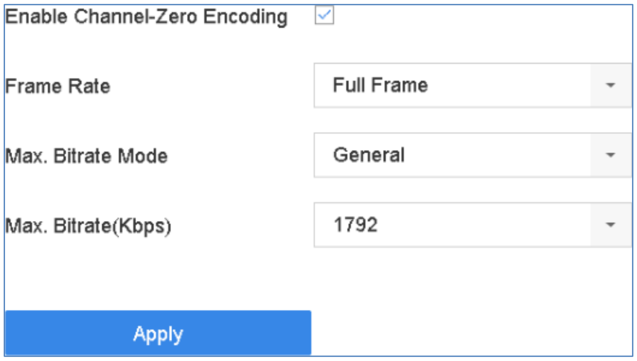
3. Go to **View Settings** to set the view layout.
4. Click **OK** to save the settings.

5.5 Configure Channel-Zero Encoding

Purpose

You can enable channel-zero encoding when you need to view many channels remotely in real time from a Web browser or CMS (Client Management System) software, by decreasing 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 **Enable Channel-Zero Encoding** checkbox.



Enable Channel-Zero Encoding	☑
Frame Rate	Full Frame
Max. Bitrate Mode	General
Max. Bitrate(Kbps)	1792

Figure 5-5 Live View – Channel-Zero Encoding

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

Result:

You can view all the channels in one screen using the CMS or a Web browser.

5.6 Use an Auxiliary Monitor

Certain features of Live View are also available while using an auxiliary monitor. These features include:

- **Single Screen:** Switch to a full screen display of the selected camera. Select camera from a drop-down list.
- **Multi-Screen:** Switch between different display layout options. Select layout options from a drop-down 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 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

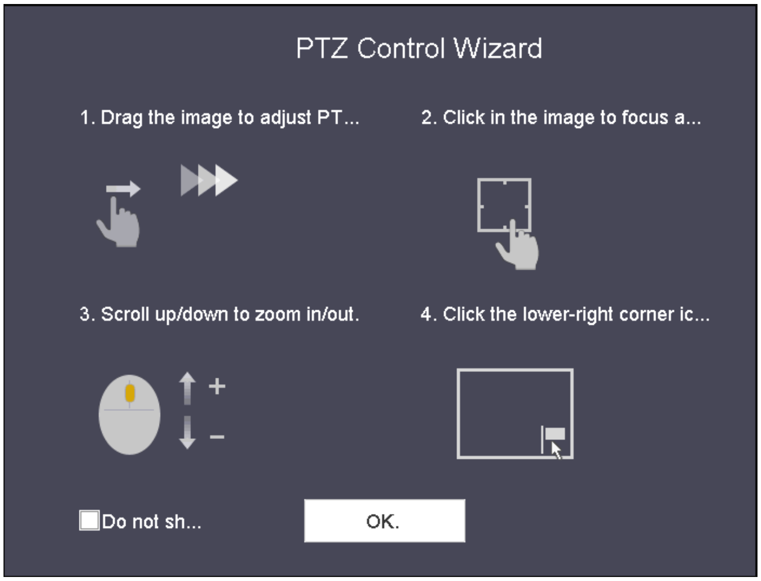
Before You Start

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.



PTZ Control Wizard

1. Drag the image to adjust PT...

2. Click in the image to focus a...

3. Scroll up/down to zoom in/out.

4. Click the lower-right corner ic...

Figure 6-1 PTZ Control Wizard

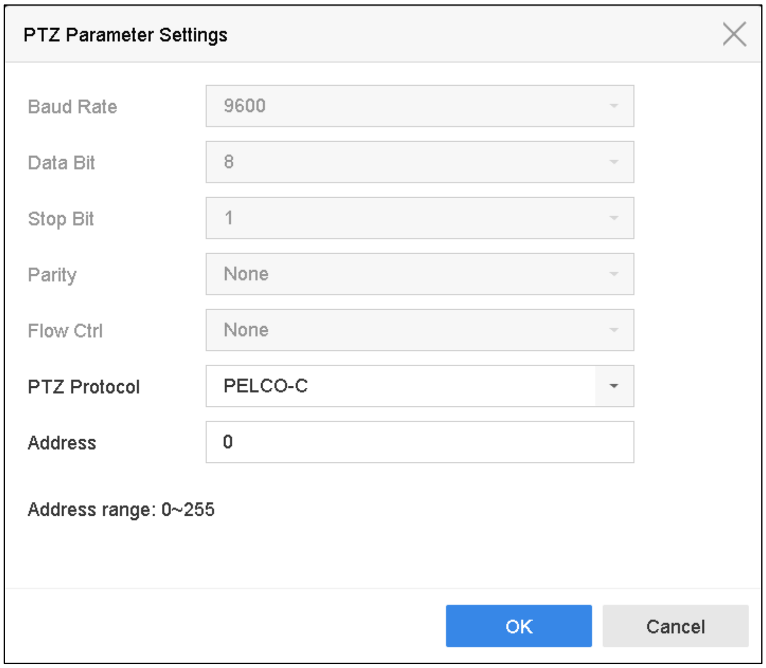
2. Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.
3. (Optional) Check the ***Do not show this prompt again*** checkbox.
4. Click **OK** to exit.

6.2 Configure PTZ Parameters

Purpose

Follow this procedure to set the PTZ parameters. Configure the PTZ parameters 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

Figure 6-2 PTZ Parameters Settings

3. Edit the PTZ camera parameters.

NOTE

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

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

6.3 Set PTZ Presets, Patrols, and Patterns

Before You Start

Make sure that the presets, patrols, and patterns are supported by PTZ protocols.

6.3.1 Set a Preset

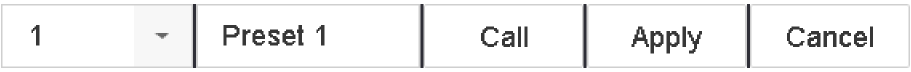
Purpose

Follow these steps to set the preset location you want the PTZ camera to point to when an event occurs.

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 the preset. 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

Figure 6-3 Set Preset

4. Select the preset no. (1~255) from the drop-down list.
5. Enter the preset name in the text field.
6. Click **Apply** to save the preset.
7. Repeat steps 2-6 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.

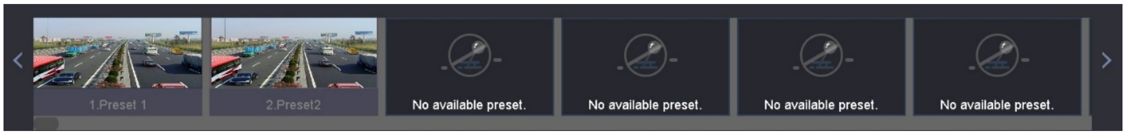


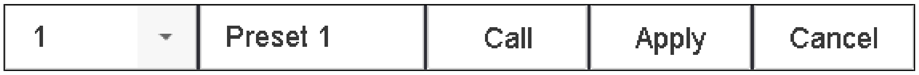
Figure 6-4 View the Configured Presets

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 occurs.

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 no. from the drop-down list.
4. Click **Call** to call it, or click ︽ in the lower right corner of live view, and click the configured preset to call it.



1

Preset 1

Figure 6-5 Call Preset (1)

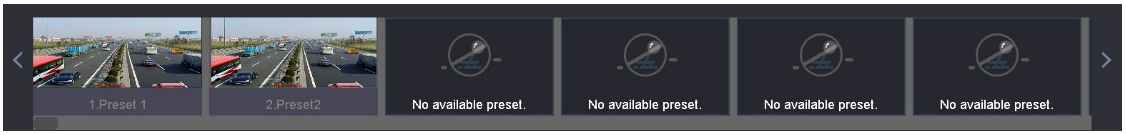


Figure 6-6 Call Preset (2)

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 correspond to 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 a patrol.

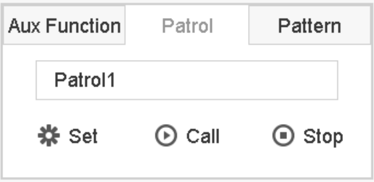
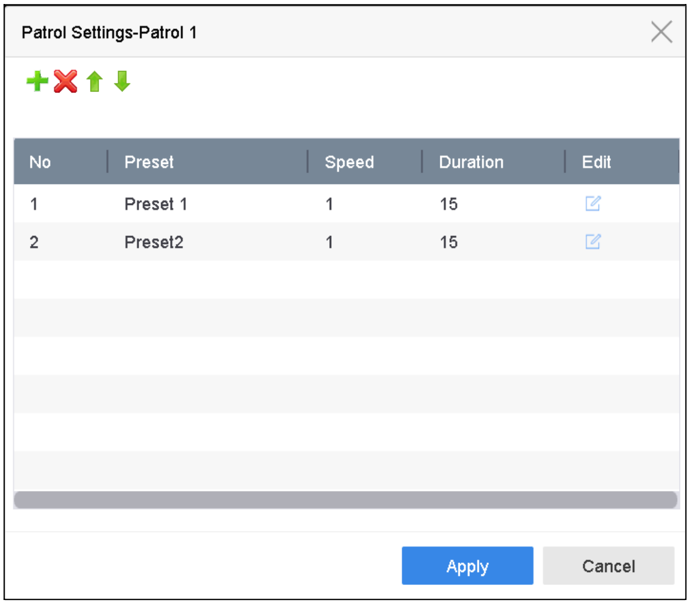


Figure 6-7 Patrol Configuration

3. Select the patrol no. in the text field.

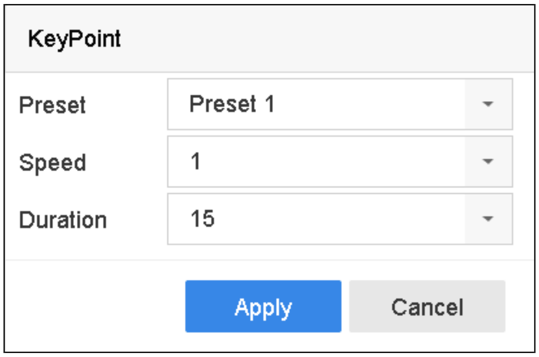
4. Click **Set** to enter the Patrol Settings interface.



No	Preset	Speed	Duration	Edit
1	Preset 1	1	15	
2	Preset2	1	15	

Figure 6-8 Patrol Settings

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



KeyPoint

Preset: Preset 1

Speed: 1

Duration: 15

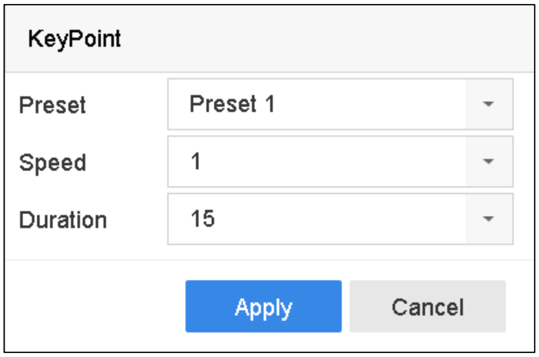
Figure 6-9 Key Point Configuration

1) Configure key point parameters.

   - **Preset:** The order the PTZ will follow while cycling through the patrol.
   - **Speed:** The speed the PTZ will move from one key point to the next.
   - **Duration:** 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.



KeyPoint

Preset: Preset 1

Speed: 1

Duration: 15

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.

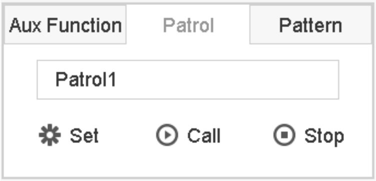
6.3.4 Call a Patrol

Purpose

Calling a patrol makes the PTZ 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.



Patrol1

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.

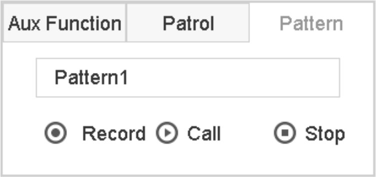
6.3.5 Set a Pattern

Purpose

Patterns can be set by recording the PTZ movement. You can call the pattern to make the PTZ move 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 the pattern.



Pattern1

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 PTZ movement is recorded as the pattern.

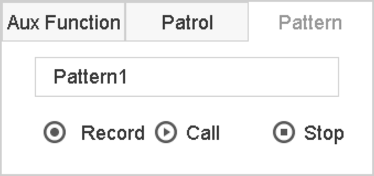
5. Repeat steps 3-4 to set more patterns.

6.3.6 Call a Pattern

Purpose
Follow this 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.



Pattern1

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

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

NOTE
This function is supported by 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.

NOTE
The dome starts the linear scan from the left limit to the right limit, and you must set the left limit to the

left of the right limit, and the angle from the left limit to the right limit should be no more than 180º.

6.3.8 Call Linear Scan

NOTE

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

Purpose

Follow this 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.

NOTE

Reboot the camera to have the settings take effect.

6.3.9 One-Touch Park

NOTE

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

Purpose

Certain dome models can be configured to start a predefined park action (scan, preset, patrol, 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 the patrol from predefined preset 1 to preset 32 in order after the park time. Undefined presets will be skipped.

   - **Park (Patrol 1):** The dome starts moving according to the predefined patrol 1 path after the park time.

   - **Park (Preset 1):** The dome moves to the predefined preset 1 location after the park time.

NOTE

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

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

6.3.10 Auxiliary Functions

Before You Start

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**.

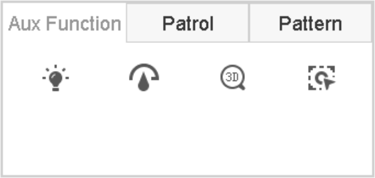


Figure 6-14 Aux Function Configuration

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

Table 6-1 Description of Aux Functions Icons

Icon	Description
💡	Light on/off
💧	Wiper on/off
3D	3D positioning
⌖	Center

Chapter 7 Storage

7.1 Storage Device Management

7.1.1 Install the HDD

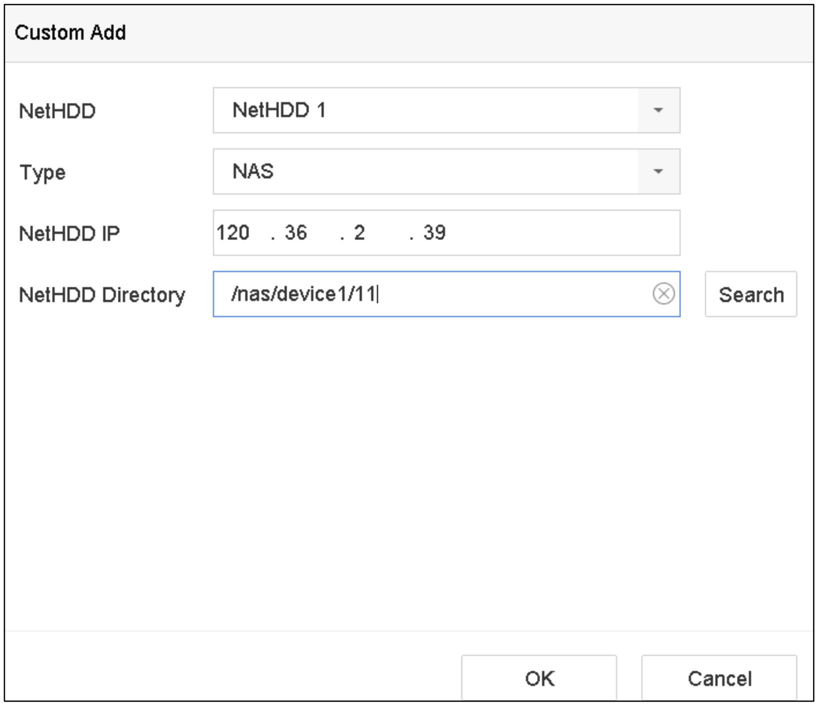
Before starting the device, install and connect the HDD to the device. Refer to the Quick Start Guide for installation instructions.

7.1.2 Add the Network Disk

You can add the allocated NAS or IP SAN disk to the device and use it as a network HDD. Up to eight 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. Set the type to NAS.
5. Enter the NetHDD IP address in the text field.
6. Click **Search** to search the available NAS disks.



Custom Add

NetHDD	NetHDD 1
Type	NAS
NetHDD IP	120 . 36 . 2 . 39
NetHDD Directory	/nas/device1/11

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 NetHDD Directory text field.

8. Click **OK** to complete adding the NAS disk.

Result

Return to the HDD Information menu after adding the NAS disk. The added NetHDD will display on the list.

Adding an IP SAN

1. Go to **Storage > Storage Device**.

2. Click **Add** to enter the Custom Add interface.

3. Select NetHDD from the drop-down list.

4. Set the type to IP SAN.

5. Enter the NetHDD IP address in the text field.

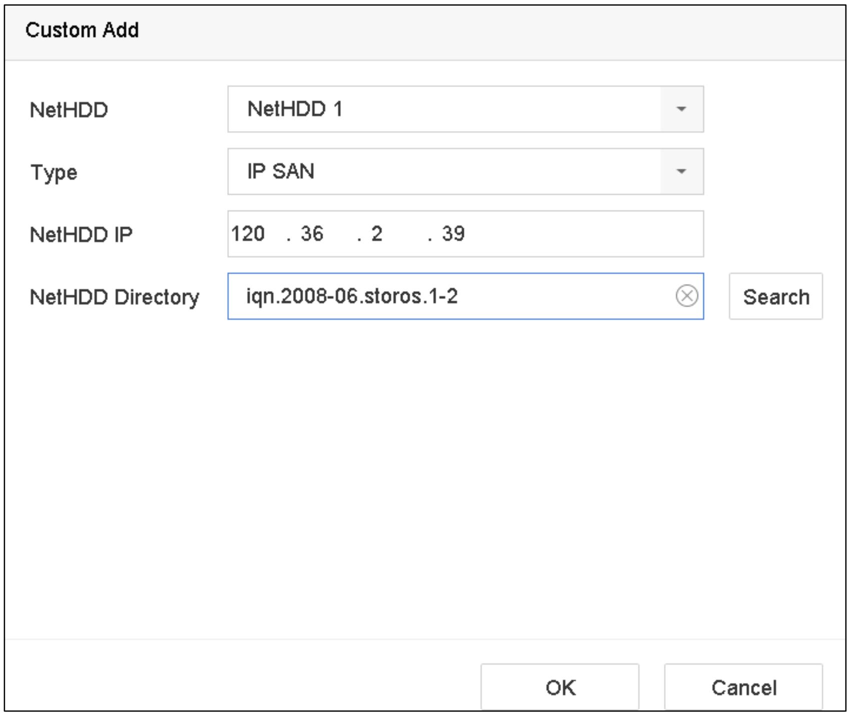
6. Click **Search** to search the available IP SAN disks.

7. Select the IP SAN disk from the list shown.

8. Click **OK** to complete adding the IP SAN disk.

NOTE

Up to one IP SAN disk can be added.



Custom Add

NetHDD: NetHDD 1

Type: IP SAN

NetHDD IP: 120 . 36 . 2 . 39

NetHDD Directory: iqn.2008-06.storos.1-2

Figure 7-2 Add IP SAN Disk

Result

Return to the HDD Information menu after adding the IP SAN disk. The added NetHDD will display in the list.

NOTE

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

7.1.3 Configure eSATA for Data Storage

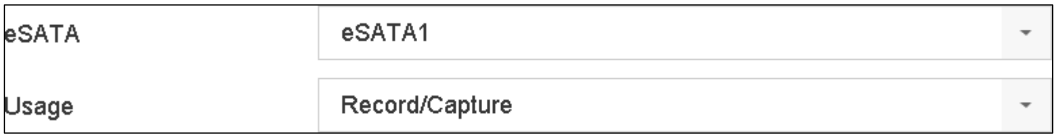
When there is an external eSATA device connected to the device, you can configure the eSATA for data storage and manage the eSATA in the device.

1. Click **Storage** > **Advanced**.

2. Set the eSATA type to Export or Record/Capture from the drop-down **eSATA** list.

   - **Export**: Use the eSATA for backup.

   - **Record/Capture:** Use the eSATA for record/capture. Refer to the following steps for 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 as required.

7.2 Storage Mode

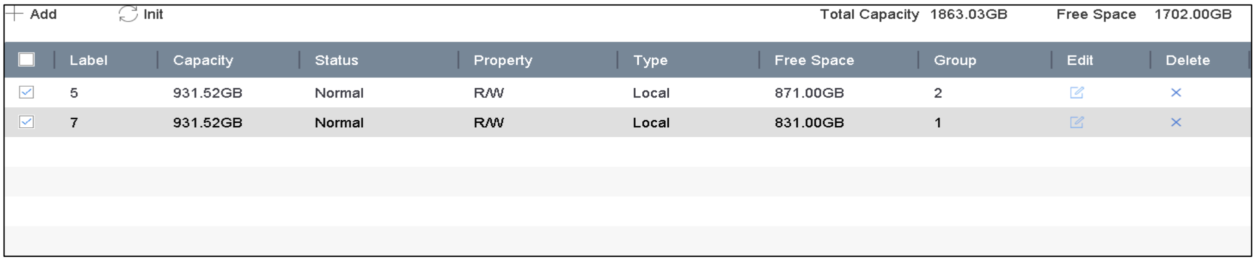
7.2.1 Configure HDD Group

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.

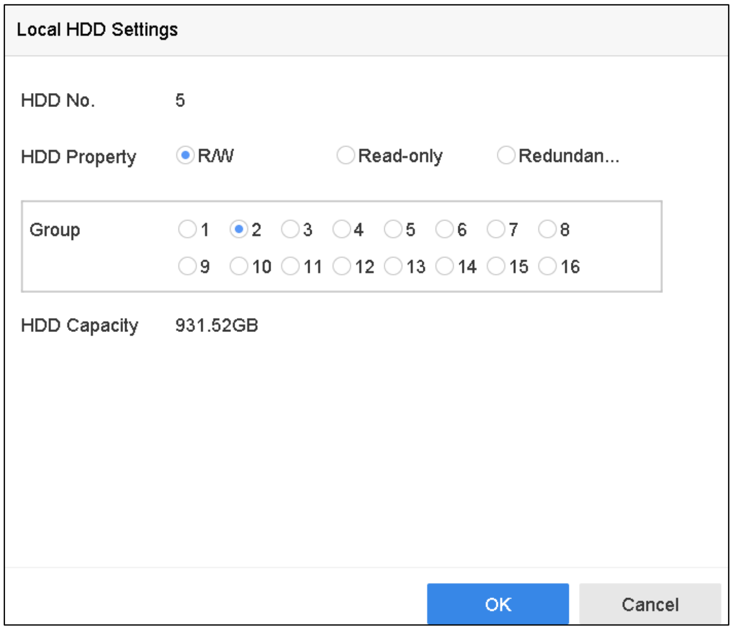


Total Capacity 1863.03GB Free Space 1702.00GB

□	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete
☑	5	931.52GB	Normal	R/W	Local	871.00GB	2	✎	×
☑	7	931.52GB	Normal	R/W	Local	831.00GB	1	✎	×

Figure 7-4 Storage Device

3. Click ✎ to enter the Local HDD Settings interface.



Local HDD Settings

HDD No. 5

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

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

HDD Capacity 931.52GB

Figure 7-5 Local HDD Settings

4. Select the Group number for the current HDD.

5. Click **OK**.

NOTE

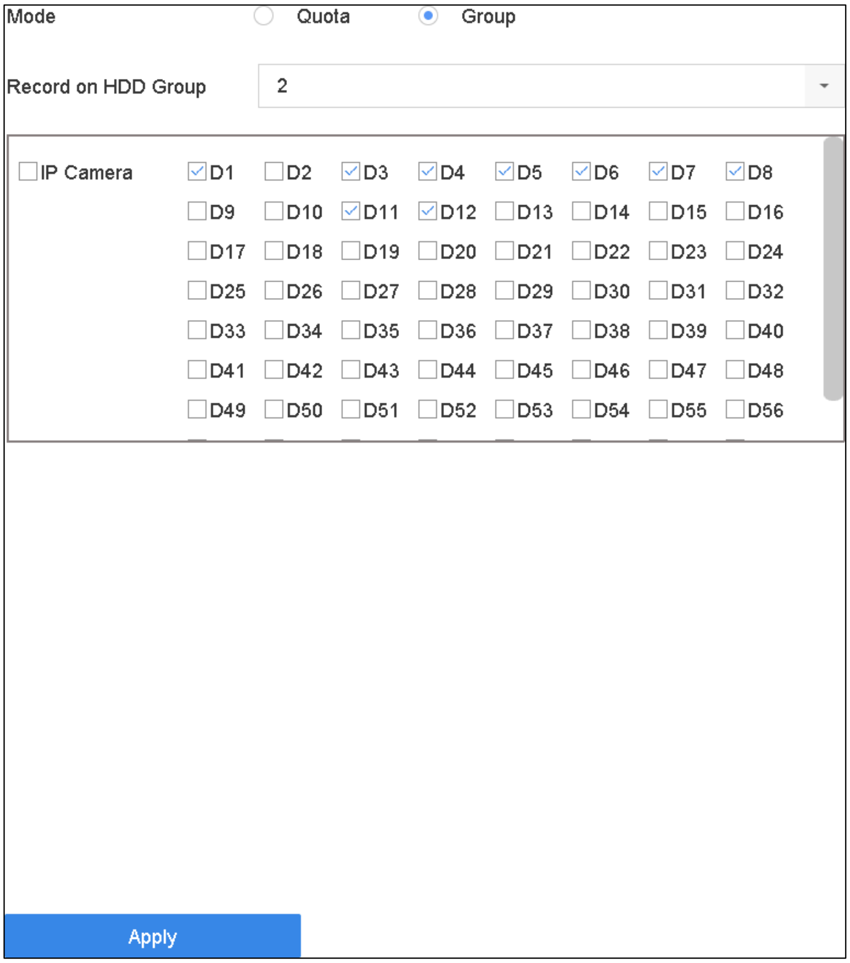
Regroup the cameras for HDD if the HDD group number is changed.

6. Go to **Storage**> **Storage Mode**.

7. Check the **Group** tab checkbox.

8. Select the group no. from the list.

9. Check the checkbox to select the IP camera(s) to record/capture on the HDD group.



Mode ○ Quota ● Group

Record on HDD Group 2

□ IP Camera

☑D1 □D2 ☑D3 ☑D4 ☑D5 ☑D6 ☑D7 ☑D8
□D9 □D10 ☑D11 ☑D12 □D13 □D14 □D15 □D16
□D17 □D18 □D19 □D20 □D21 □D22 □D23 □D24
□D25 □D26 □D27 □D28 □D29 □D30 □D31 □D32
□D33 □D34 □D35 □D36 □D37 □D38 □D39 □D40
□D41 □D42 □D43 □D44 □D45 □D46 □D47 □D48
□D49 □D50 □D51 □D52 □D53 □D54 □D55 □D56

Figure 7-6 Storage Mode-HDD Group

10. Click **Apply**.

NOTE

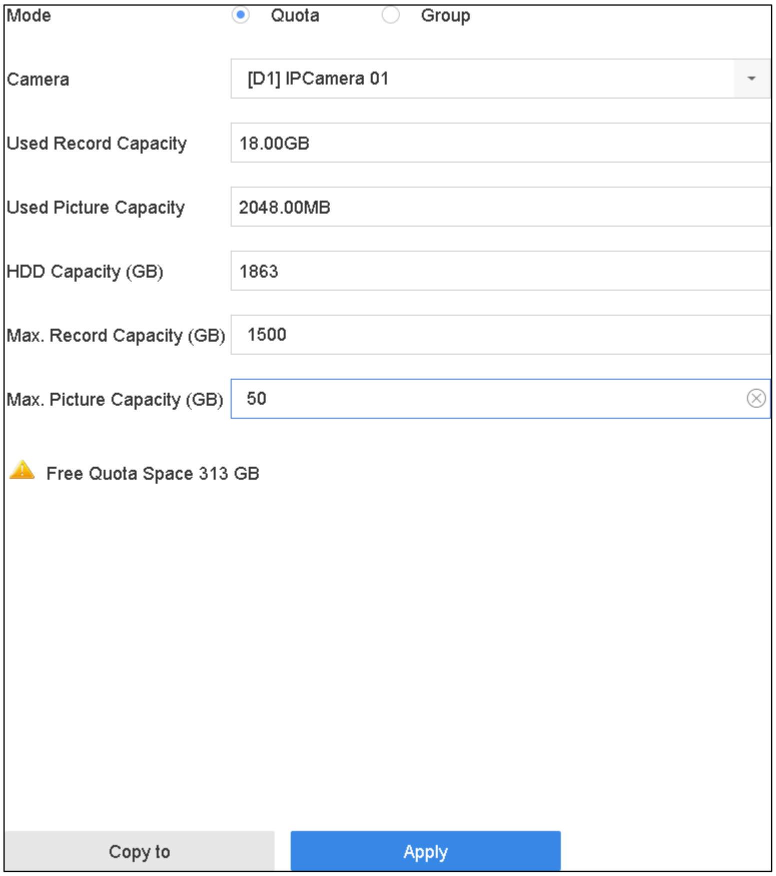
Reboot the device to activate the new storage mode settings.

7.2.2 Configure HDD Quota

Purpose

Each camera can be configured with an allocated quota for storing recorded files or captured pictures.

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



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

Figure 7-7 Storage Mode – HDD Quota

5. (Optional) 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 the 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.

Compared to 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**: H.264+ mode helps to ensure high video quality with a lowered bitrate. It can effectively reduce the need for bandwith and HDD storage space.

NOTE

A higher resolution, frame rate, and bitrate setting will provide better video quality, but will also require more internet bandwidth and use more storage space on the hard disk 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 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. Higher picture quality results in more storage space requirement.
- **Interval**: The interval of capturing live picture.

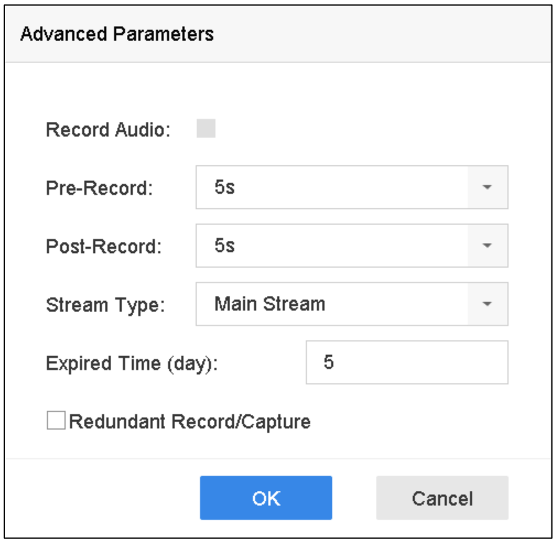
7.3.4 ANR

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

Enable ANR (Automatic Network Replenishment) via a 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 **Enable** checkbox to enable scheduled recording.
3. Click **Advanced** to set the recording parameters.



Advanced Parameters

Record Audio: □

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

□ Redundant Record/Capture

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, if an alarm triggers 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 scheduled time. For example, if an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records until 11:00:05.
- **Expired Time**: The 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. If you select sub-stream, you can record for a longer time in the same storage space.

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

7.4 Configure Recording Schedule

Set the record schedule, and the camera will automatically start/stop recording according to the configured schedule.

Before You Start

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

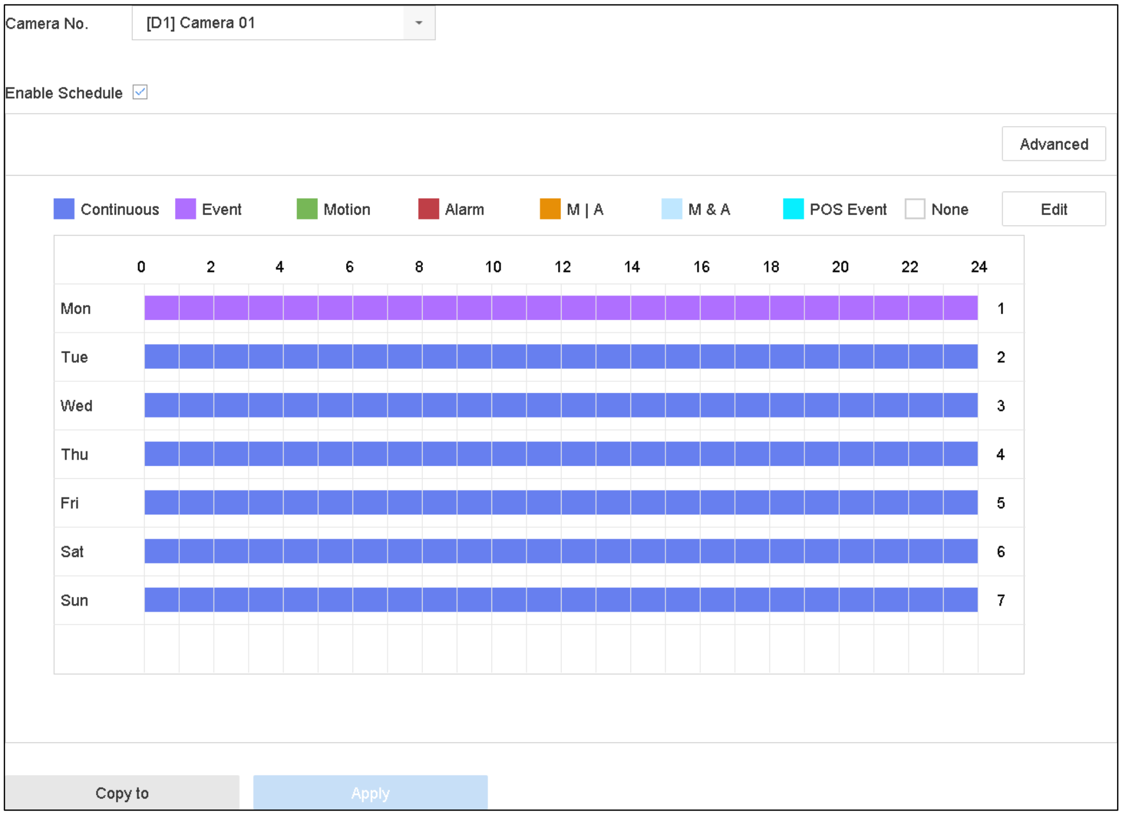
2. Select a camera.

3. Check **Enable Schedule**.

4. Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, or Event. The recording types are configurable.

   - **Continuous:** Scheduled recording
   - **Event**: Recording triggered by all event triggered alarms
   - **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 ☑

	0 – 24	
Mon	🟪 Event	1
Tue	🟦 Continuous	2
Wed	🟦 Continuous	3
Thu	🟦 Continuous	4
Fri	🟦 Continuous	5
Sat	🟦 Continuous	6
Sun	🟦 Continuous	7

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. 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** for 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 a 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 a 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 recordings triggered by motion detection, vehicle detection, line crossing detection, etc.

1. Go to **System** > **Event**.

2. Configure the event detection and select the channel(s) to trigger the recording when an 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 recordings triggered by 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 channel(s) to trigger recording when an 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 recordings 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 a 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 POS event triggered recording schedule. Refer to *Chapter 7.4 Configure Recording Schedule* .

7.10 Configure Picture Capture

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

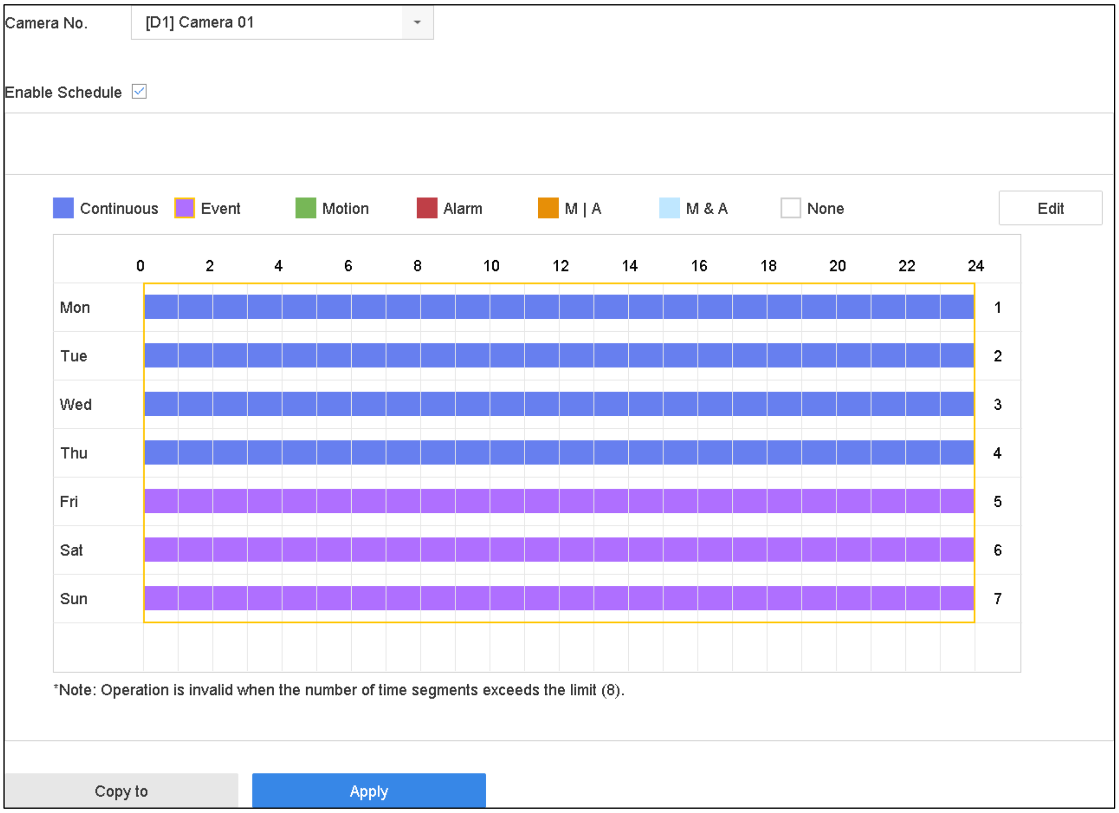
1. Go to **Camera** > **Encoding Parameters** > **Capture**.

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.



Camera No. [D1] Camera 01

Enable Schedule ☑

*Note: Operation is invalid when the number of time segments exceeds the limit (8).

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

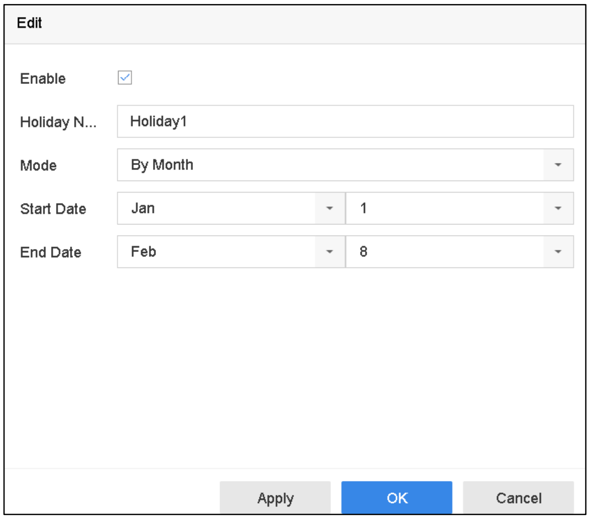
Purpose

Follow these steps to configure the record or capture schedule on holidays for the year. You may want to have different plans for recording and capture on holidays.

1. Go to **System > Holiday Settings**.

2. Select a holiday item from the list and click ✎ .

3. Check the **Enable** to configure the holiday.



Edit

Enable ☑

Holiday N... Holiday1

Mode By Month

Start Date Jan 1

End Date Feb 8

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

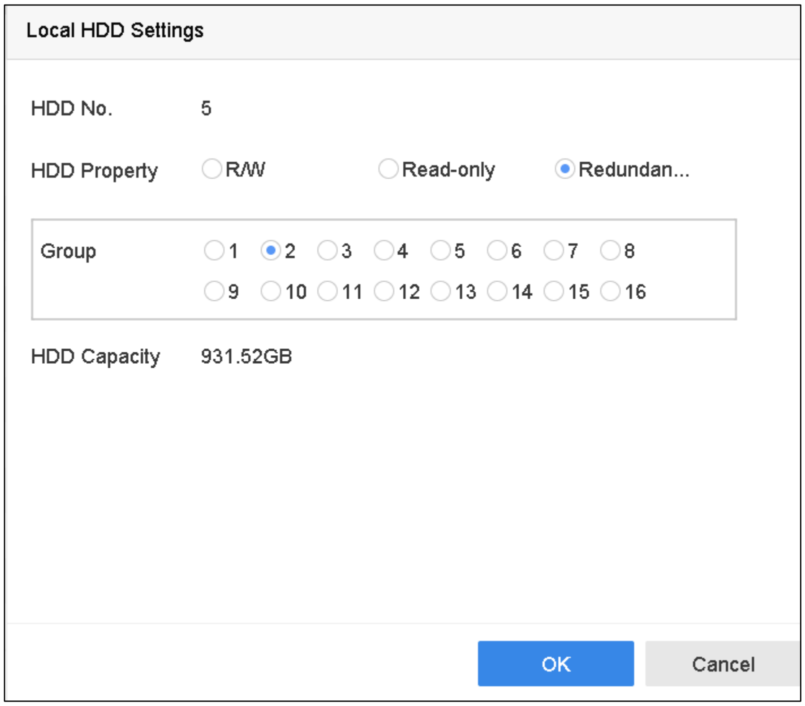
Purpose

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

NOTE

You must set the storage mode to **Group** before you set the HDD property to **Redundancy**. For detailed information, refer to *Configure HDD Group*. There should be at least another HDD 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**.



Local HDD Settings

HDD No. 5

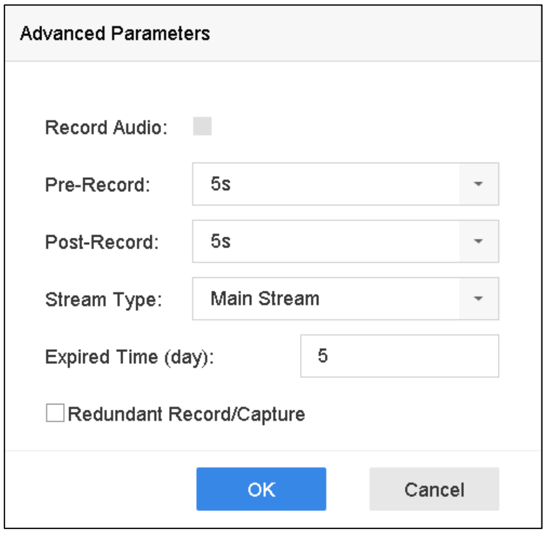
HDD Property ○ R/W ○ Read-only ● Redundan...

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

HDD Capacity 931.52GB

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.



Advanced Parameters

Record Audio: □

Pre-Record: 5s

Post-Record: 5s

Stream Type: Main Stream

Expired Time (day): 5

□ Redundant Record/Capture

Figure 7-13 Record Parameters

6. Check the **Redundant Record/Capture** checkbox.
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

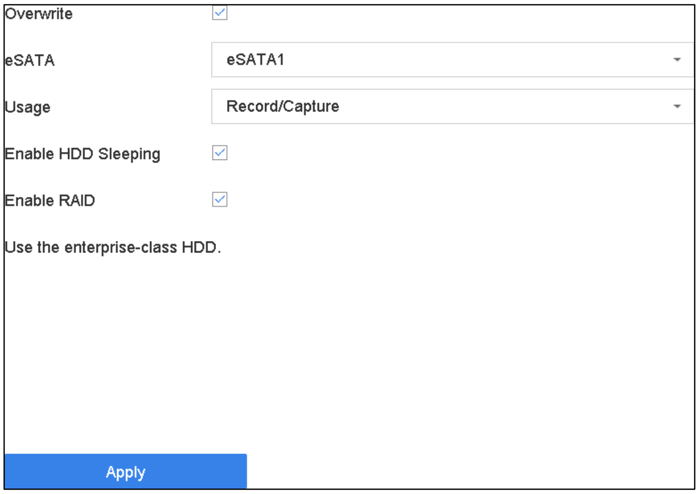
The device supports a software-based disk array. You can enable the RAID function as required. Two ways are available for creating an array: one-touch configuration and manual configuration. The following flow chart shows the process to create an array.

8.1.1 Enable RAID

Purpose

Perform the following steps to enable the disk array function.

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



Overwrite ☑

eSATA: eSATA1

Usage: Record/Capture

Enable HDD Sleeping ☑

Enable RAID ☑

Use the enterprise-class HDD.

Figure 8-1 Advanced

2. Check **Enable RAID**.

3. Click **Apply**.

4. Reboot device to have the settings take effect.

8.1.2 One-Touch Creation

Purpose

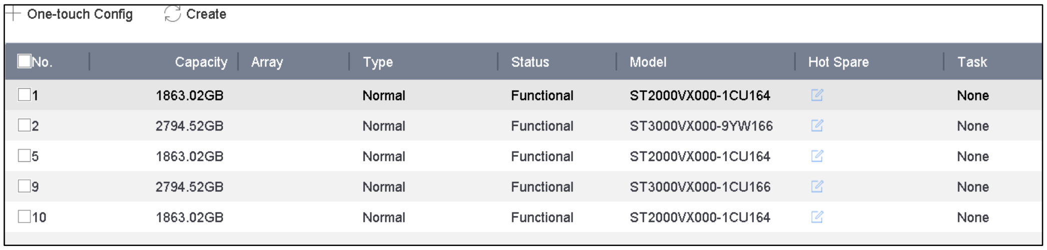
One-touch configuration helps you quickly create a disk array. By default, the array type created by one-touch configuration is RAID 5.

Before You Start

Enable the RAID function.

Install at least three HDDs. If more than 10 HDDs are installed, two arrays will be created. To maintain reliable and stable 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	✎	None
□2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	✎	None
□5	1863.02GB		Normal	Functional	ST2000VX000-1CU164	✎	None
□9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	✎	None
□10	1863.02GB		Normal	Functional	ST2000VX000-1CU164	✎	None

Figure 8-2 Physical Disk

2. Click **One-touch Config**.

3. Edit the array name in the **Array Name** text field.

4. Click **OK** to start configuring.

NOTE

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

5. A message box will pop up when the array creation is completed, click **OK** on it.

6. Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** to view the created arrray's information.

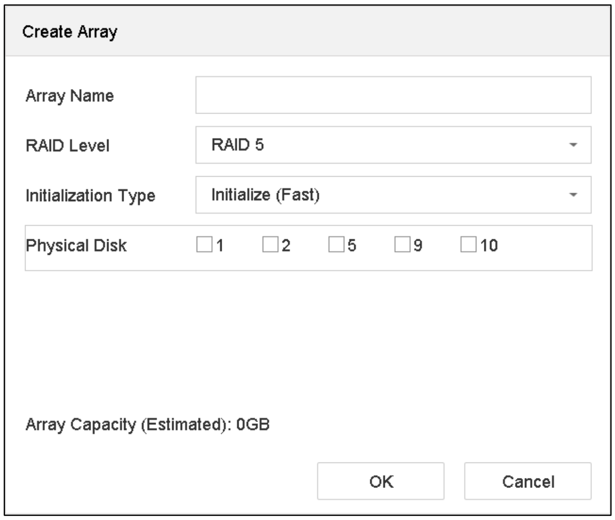
8.1.3 Manual Creation

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**.



Create Array

Array Name	
RAID Level	RAID 5
Initialization Type	Initialize (Fast)
Physical Disk	□1 □2 □5 □9 □10

Array Capacity (Estimated): 0GB

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.

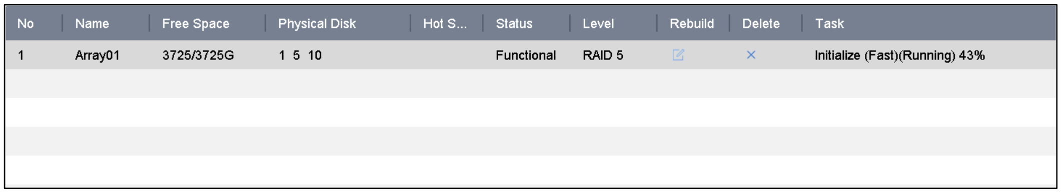
5. Select the physical disks to constitute the array.

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 HDDs must be an even range from 4 to 16

6. Click **OK**.

7. Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** to view the created arrray's information.



No	Name	Free Space	Physical Disk	Hot S...	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	1 5 10		Functional	RAID 5	✎	×	Initialize (Fast)(Running) 43%

Figure 8-3 Array List

8.2 Rebuild Array

Purpose

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

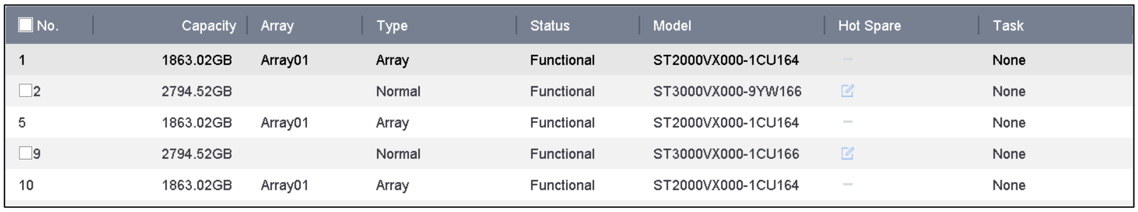
- **Functional:** No disk loss in the array.
- **Offline:** The number of lost disks has exceeded the limit.
- **Degraded:** If HDDs fail in the array, the array degrades. You should recover it to **Functional** by array rebuilding.

8.2.1 Configure Hot Spare Disk

Purpose

Hot spare disks are required for automatic disk array 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
□2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	✎	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	–	None
□9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	✎	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

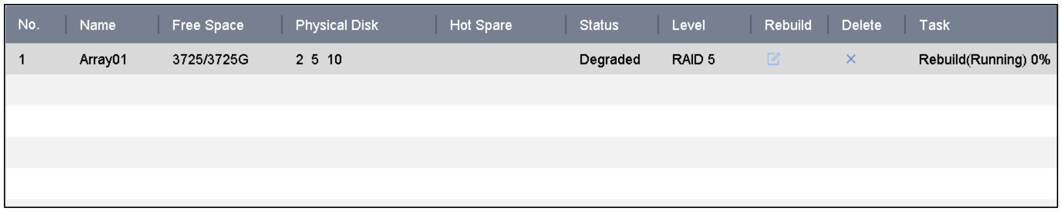
Purpose

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

Before You Start

Create hot spare disks. For details, refer to *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 the rebuilding progress.



No.	Name	Free Space	Physical Disk	Hot Spare	Status	Level	Rebuild	Delete	Task
1	Array01	3725/3725G	2 5 10		Degraded	RAID 5	✎	×	Rebuild(Running) 0%

Figure 8-5 Array List

8.2.3 Manually Rebuild Array

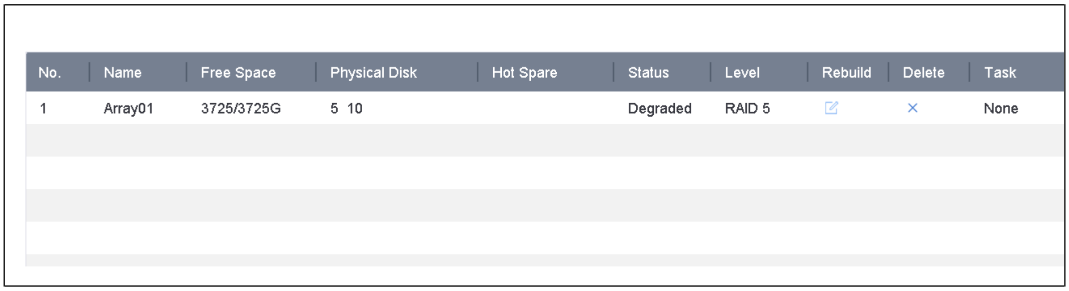
Purpose

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.

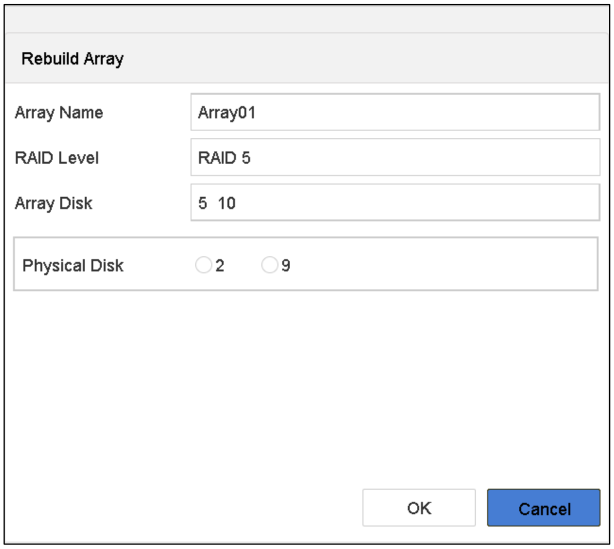
1. Go to **Storage > RAID Setup > Array**.



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

Figure 8-6 Array List

2. Click ✎ of degraded array.



Rebuild Array

Array Name	Array01
RAID Level	RAID 5
Array Disk	5 10

Physical Disk ○2 ○9

Figure 8-7 Rebuild Array

3. Select the available physical disk.

4. Click **OK**.

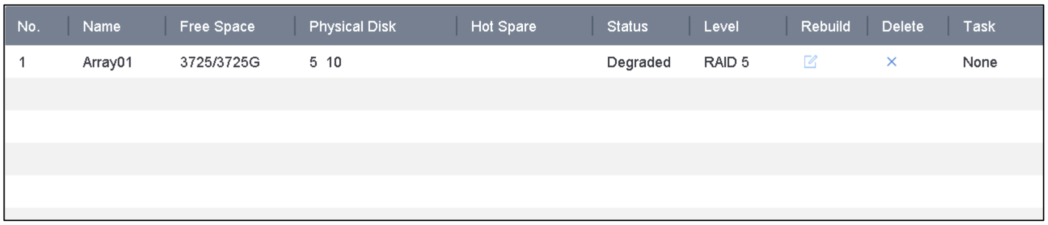
5. Click **OK** on the pop-up message box "Do not unplug the physical disk when it is under rebuilding."

8.3 Delete Array

NOTE

Deleting an array will delete all the data saved in it.

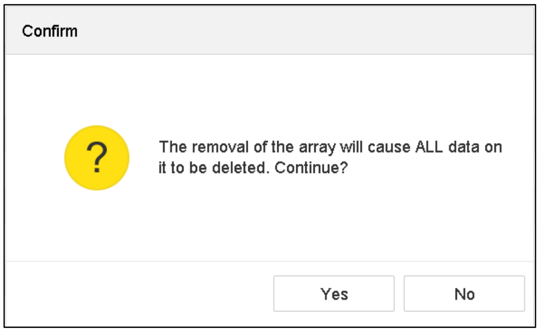
1. Go to **Storage > RAID Setup > Array**.



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 array to delete.



Confirm

The removal of the array will cause ALL data on it to be deleted. Continue?

Figure 8-9 Attention

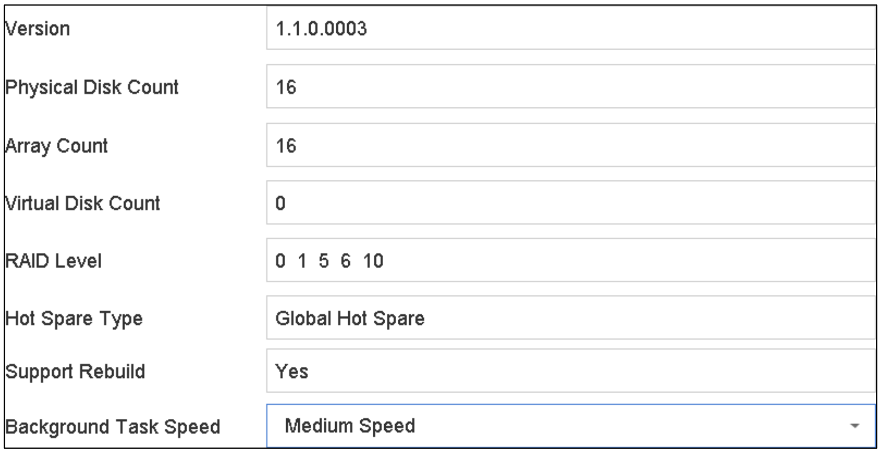
3. Click **Yes** on the pop-up message box.

8.4 Check and Edit Firmware

Purpose

You can view the firmware information and set the background task speed on 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

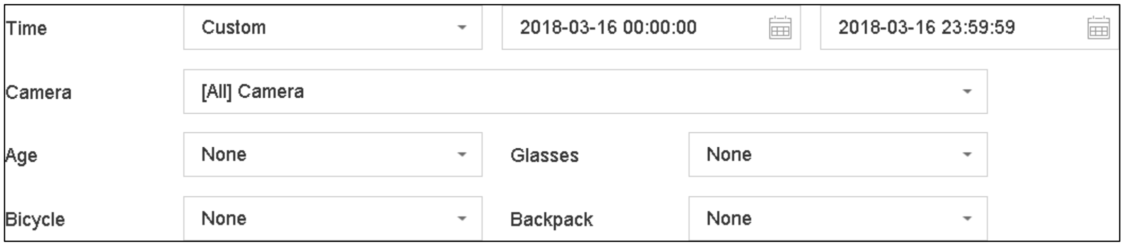
Purpose

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.

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 thumbnails or a 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.

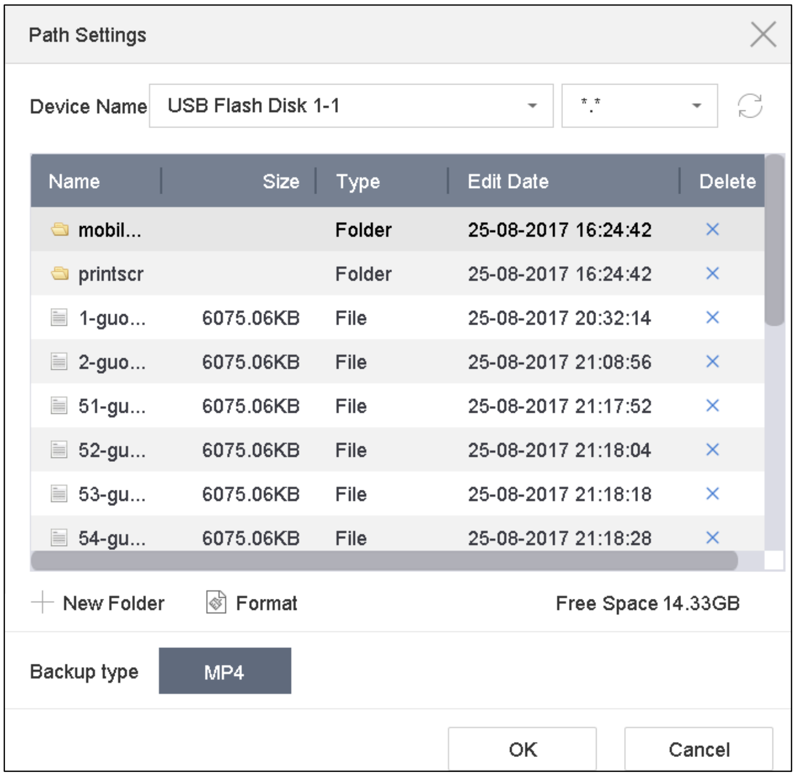
   - **Target Picture**: Display the search results of people close up.
   - **Source Picture**: Display the search results of original picture captured by camera.
   - **Group**: Sort the search results by selected item.

9.1.2 Export Human Files

Purpose

Export files for backup purposes using a 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 *Search Human Files*.
2. Click files and click **Export**.



Path Settings

Device Name: USB Flash Disk 1-1 | *.*

Name	Size	Type	Edit Date	Delete
mobil...		Folder	25-08-2017 16:24:42	×
printscr		Folder	25-08-2017 16:24:42	×
1-guo...	6075.06KB	File	25-08-2017 20:32:14	×
2-guo...	6075.06KB	File	25-08-2017 21:08:56	×
51-gu...	6075.06KB	File	25-08-2017 21:17:52	×
52-gu...	6075.06KB	File	25-08-2017 21:18:04	×
53-gu...	6075.06KB	File	25-08-2017 21:18:18	×
54-gu...	6075.06KB	File	25-08-2017 21:18:28	×

Free Space 14.33GB

Backup type: MP4

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

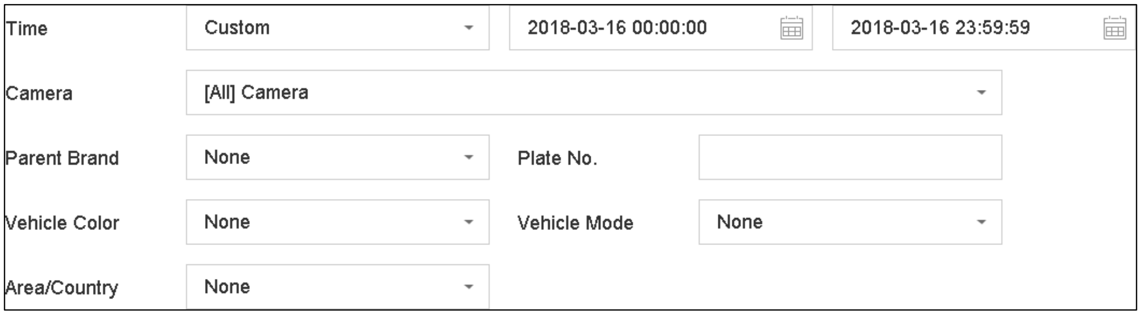
Specify detailed conditions to search vehicle files.

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.



Time	Custom	2018-03-16 00:00:00	2018-03-16 23:59:59
Camera	[All] Camera		
Parent Brand	None	Plate No.	
Vehicle Color	None	Vehicle Mode	None
Area/Country	None		

Figure 9-3 Advanced Search

3. Click **Search** to display results. The matched files are displayed in thumbnails or a 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 vehicle close up.
   - **Source Picture**: Display the search results of original picture captured by camera.
   - **Group**: Sort the search results by selected item.

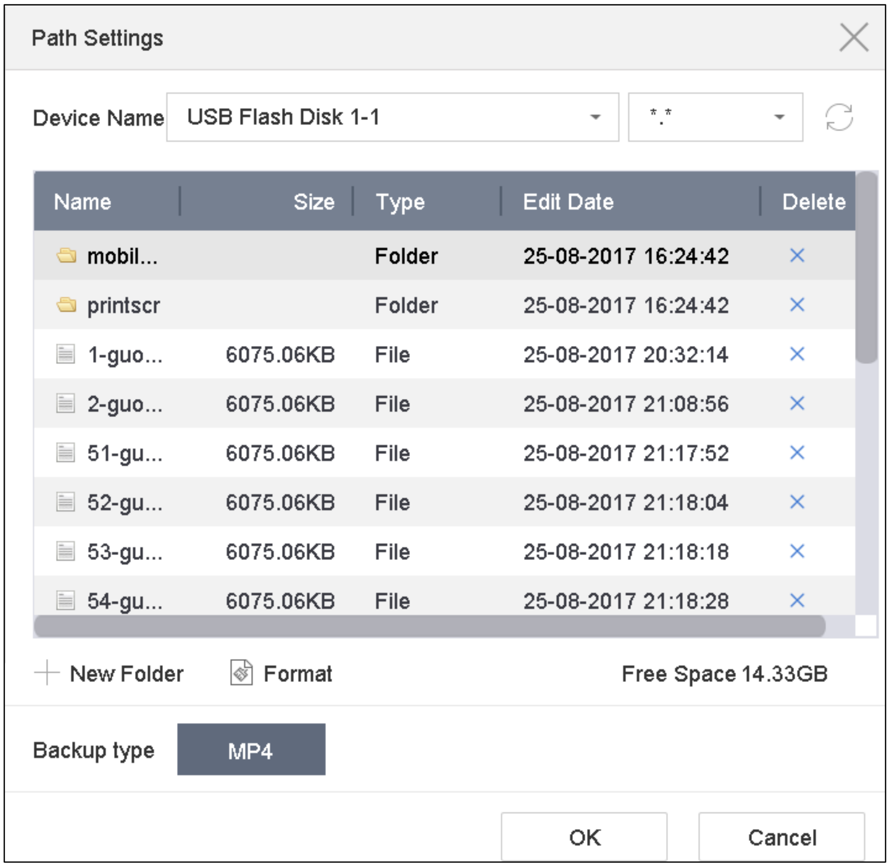
9.2.2 Export Vehicle Files

Purpose

Export files for backup purposes using a 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 *Search Vehicle Files*.

2. Click files and click **Export**.



Path Settings

Device Name: USB Flash Disk 1-1 | *.*

Name	Size	Type	Edit Date	Delete
mobil...		Folder	25-08-2017 16:24:42	×
printscr		Folder	25-08-2017 16:24:42	×
1-guo...	6075.06KB	File	25-08-2017 20:32:14	×
2-guo...	6075.06KB	File	25-08-2017 21:08:56	×
51-gu...	6075.06KB	File	25-08-2017 21:17:52	×
52-gu...	6075.06KB	File	25-08-2017 21:18:04	×
53-gu...	6075.06KB	File	25-08-2017 21:18:18	×
54-gu...	6075.06KB	File	25-08-2017 21:18:28	×

Free Space 14.33GB

Backup type: MP4

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 video files recorded in the last five minutes. If no video is found, it means there was no video recorded during 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.

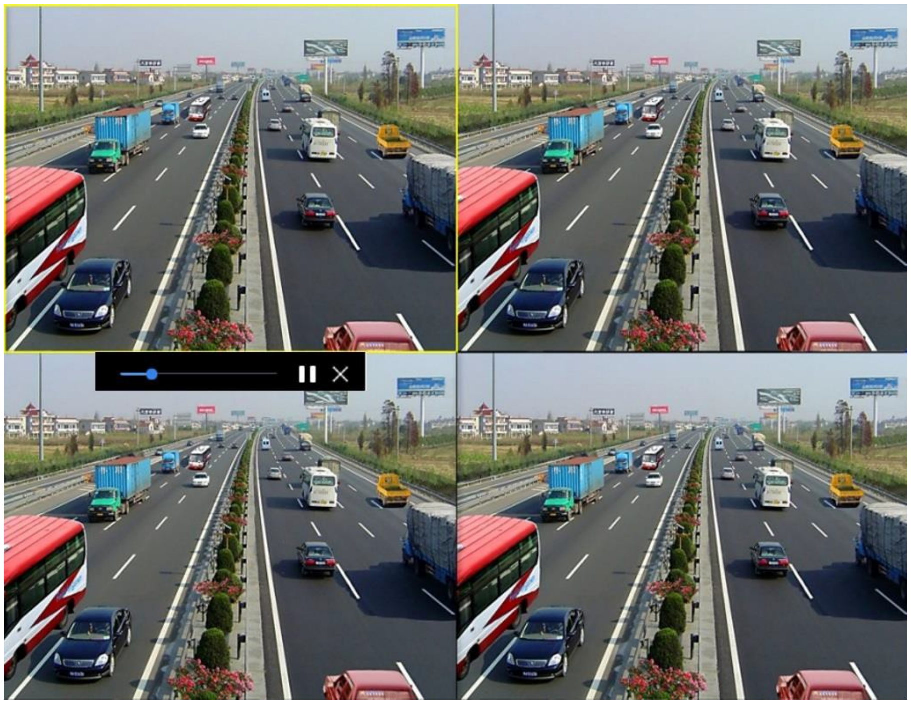


Figure 10-1 Playback Interface

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 at the bottom of the playback interface to control the playing and realize a series of operations. Refer to *Chapter 10.2 Playback Operations*.

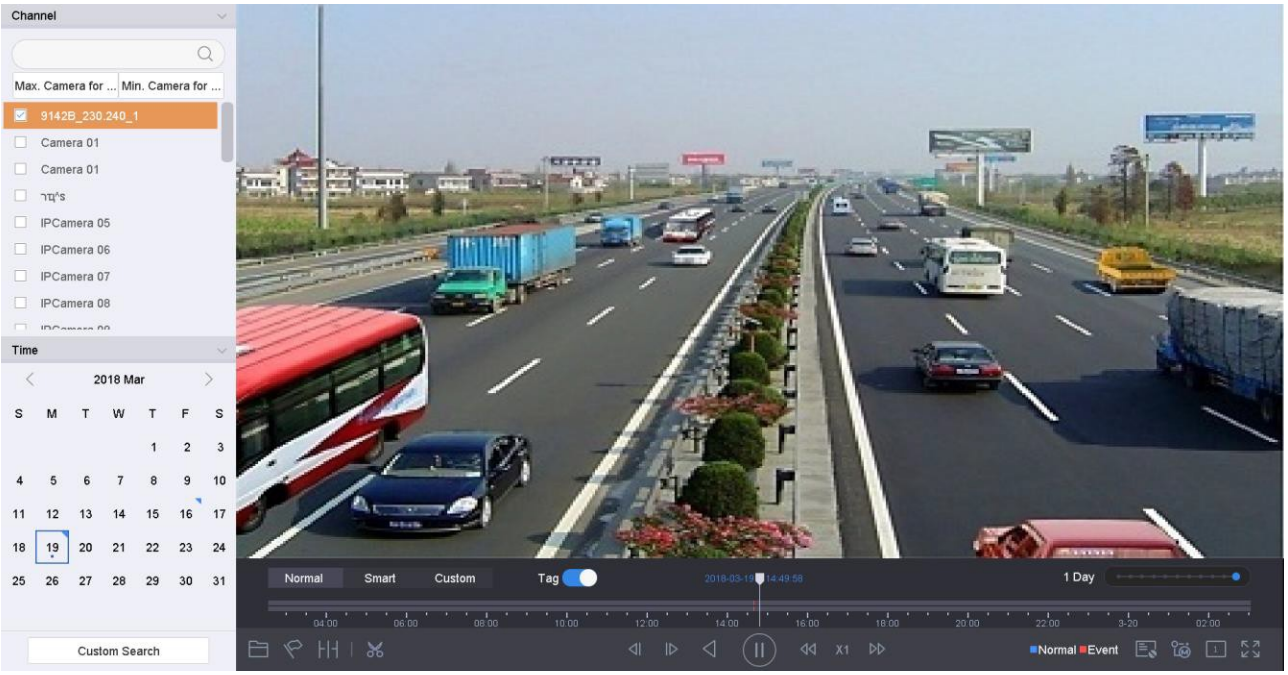


Figure 10-2 Playback Interface

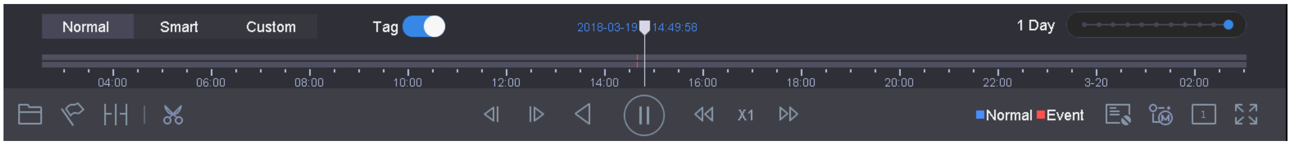


Figure 10-3 Toolbar of Playback

5. You can click the channel(s) to execute simultaneous playback of multiple channels.

NOTE

256x playing speed is supported.

10.1.3 Play Tag Files

Purpose

Video tag allows you to record related information such as 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 file(s).
3. Click to add the tag.
4. Edit the tag information.

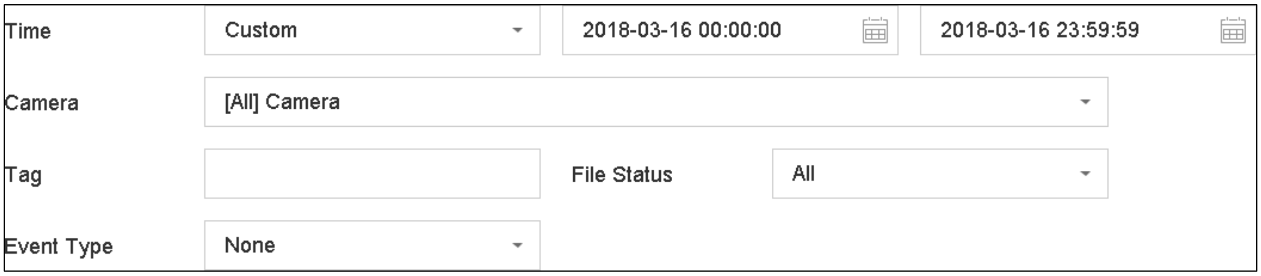
NOTE

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

Play Tag Files

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

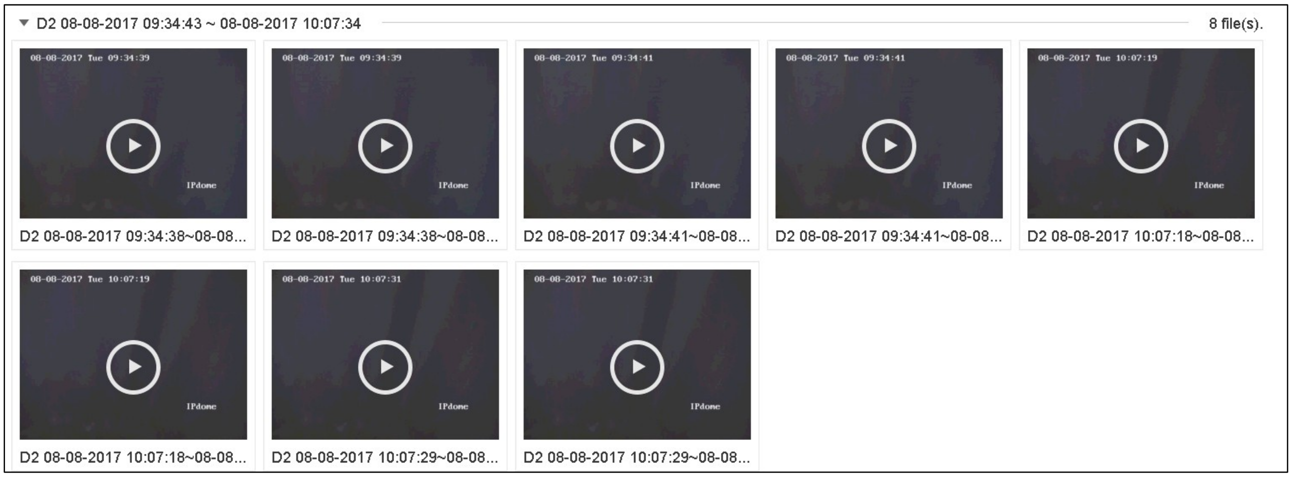
2. Enter the search conditions for the tag files, including the time and the tag keyword.



Time	Custom	2018-03-16 00:00:00	2018-03-16 23:59:59
Camera	[All] Camera		
Tag		File Status	All
Event Type	None		

Figure 10-4 Tag Search

3. Click **Search.**



D2 08-08-2017 09:34:43 ~ 08-08-2017 10:07:34 8 file(s).

D2 08-08-2017 09:34:38~08-08...
D2 08-08-2017 09:34:38~08-08...
D2 08-08-2017 09:34:41~08-08...
D2 08-08-2017 09:34:41~08-08...
D2 08-08-2017 10:07:18~08-08...
D2 08-08-2017 10:07:18~08-08...
D2 08-08-2017 10:07:29~08-08...
D2 08-08-2017 10:07:29~08-08...

Figure 10-5 Searched Tag Files

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

10.1.4 Play by Smart Search

Purpose

In smart playback mode, the device will analyze the video containing the motion, line, or intrusion detection information, mark it in green, and play it at normal speed. 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.

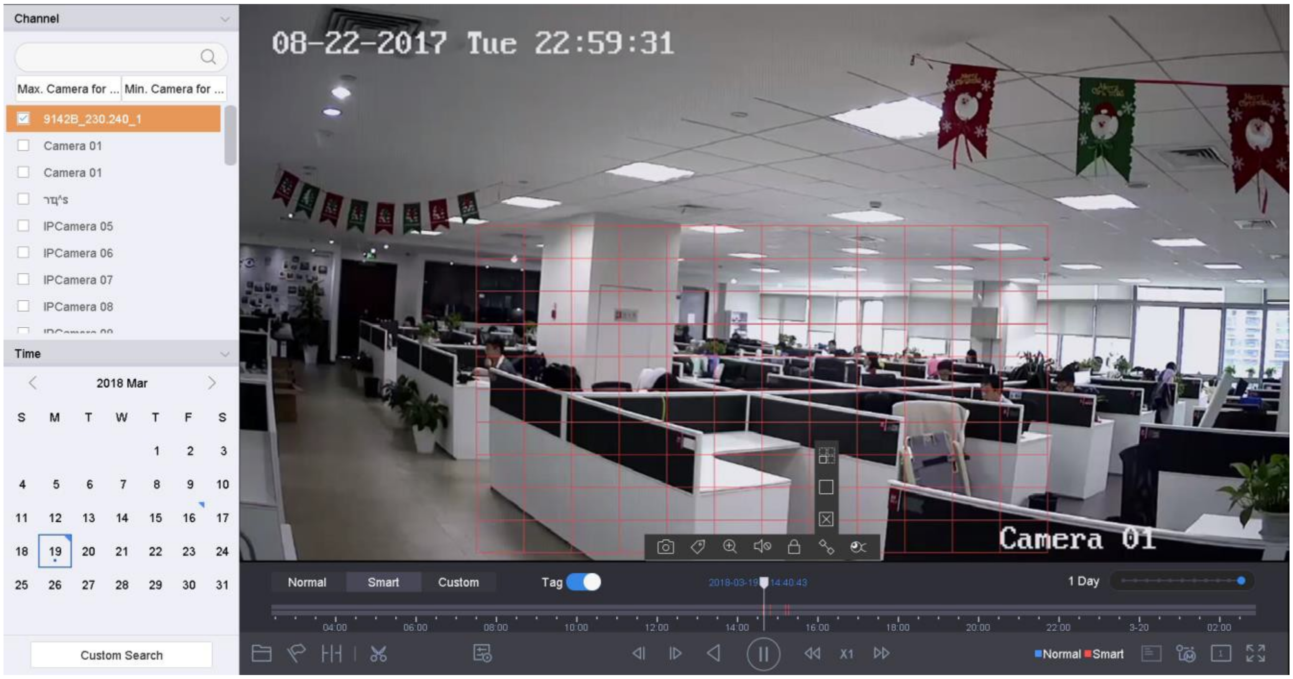


Figure 10-6 Playback by Smart Search

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 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.

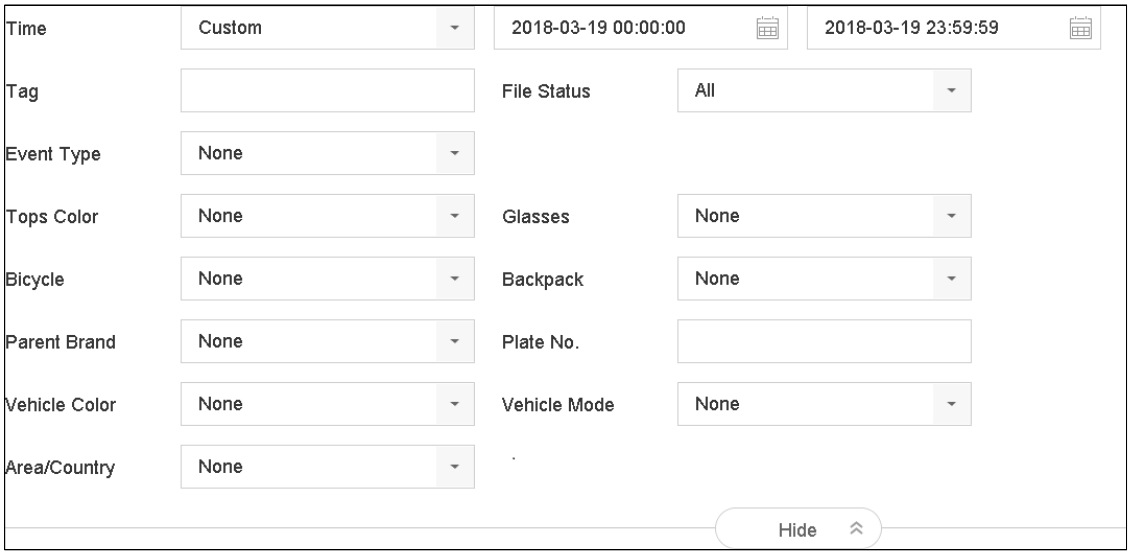
   3) Click Search 🔍 to search the matched video and start to play it.

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, face detection, vehicle detection, etc.).

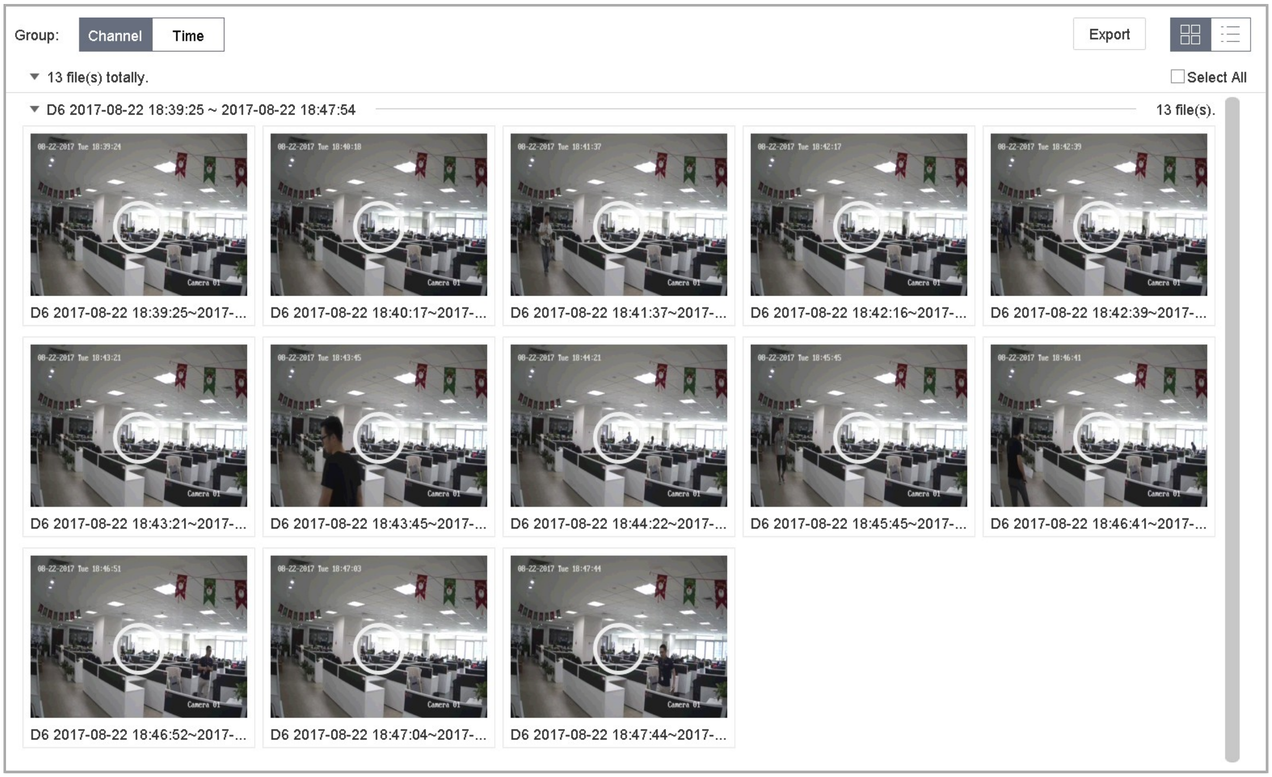
1. Go to **Playback**.
2. Click **Custom Search** on the left bottom to enter the Search Condition interface.
3. Enter the search conditions for the event files, e.g., time, event type, file status, people appearance (for face detection, human detection, etc.), vehicle information (for vehicle detection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



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		

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.



Group: Channel Time

Export

▾ 13 file(s) totally.

□ Select All

▾ D6 2017-08-22 18:39:25 ~ 2017-08-22 18:47:54

13 file(s).

D6 2017-08-22 18:39:25~2017-...
D6 2017-08-22 18:40:17~2017-...
D6 2017-08-22 18:41:37~2017-...
D6 2017-08-22 18:42:16~2017-...
D6 2017-08-22 18:42:39~2017-...
D6 2017-08-22 18:43:21~2017-...
D6 2017-08-22 18:43:45~2017-...
D6 2017-08-22 18:44:22~2017-...
D6 2017-08-22 18:45:45~2017-...
D6 2017-08-22 18:46:41~2017-...
D6 2017-08-22 18:46:52~2017-...
D6 2017-08-22 18:47:04~2017-...
D6 2017-08-22 18:47:44~2017-...

Figure 10-8 Event Files

6. You can 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.

10.1.6 Play by Sub-Periods

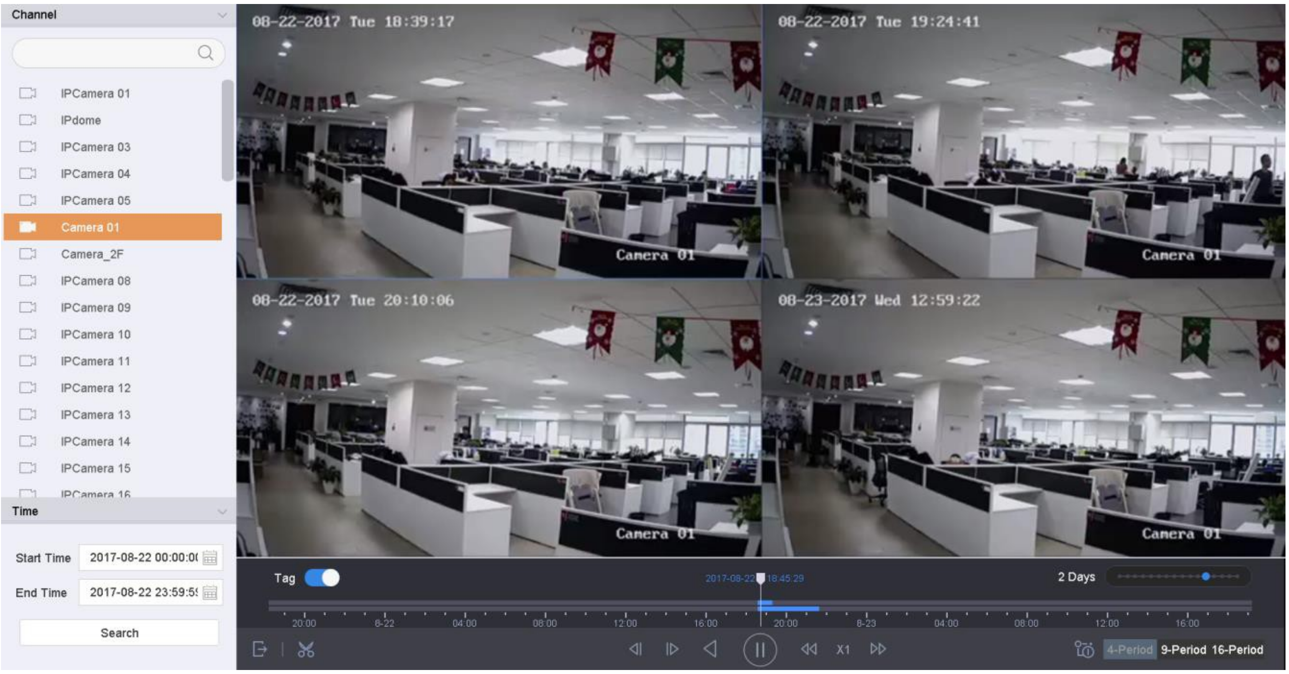
Purpose

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 drop-down list. Up to 16 screens are configurable.



Start Time 2017-08-22 00:00:0(

End Time 2017-08-22 23:59:5(

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 video files exist between 16:00 and 22:00, and 6-screen display mode is selected, it can play the video files for one hour on each screen simultaneously.

10.1.7 Play Log Files

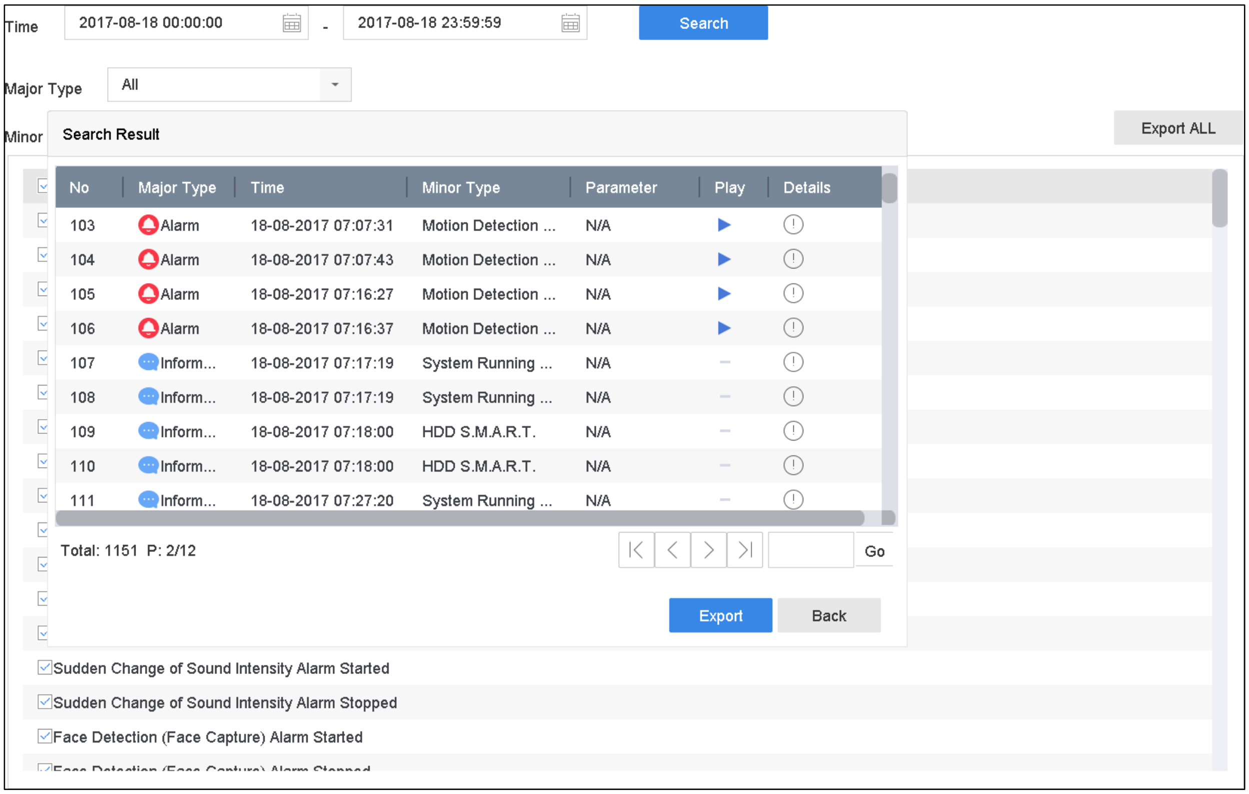
Purpose

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**.



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

Major Type All

Minor

Search Result

Export ALL

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

Go

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 10-10 System Log Search Interface

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

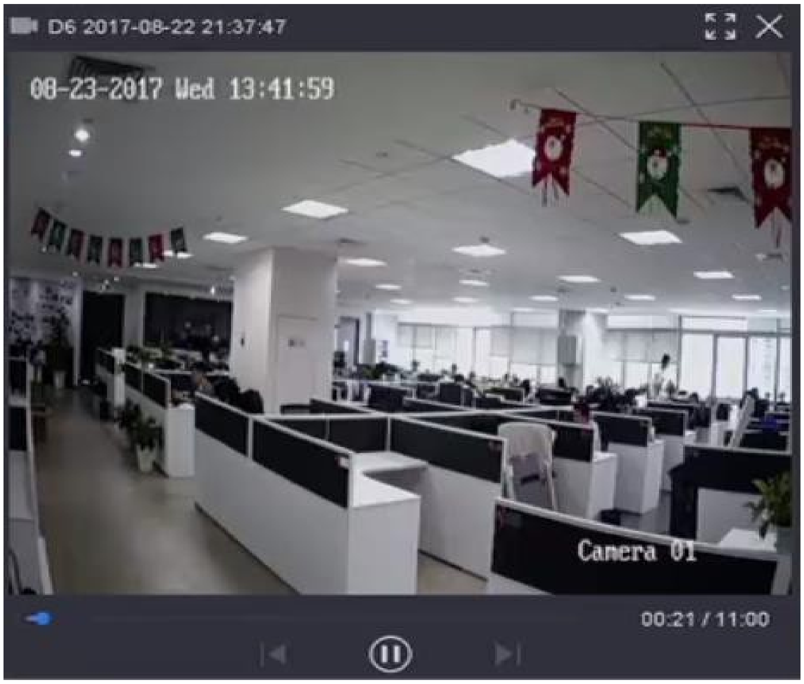


Figure 10-11 Interface of Playback by Log

10.1.8 Play External File

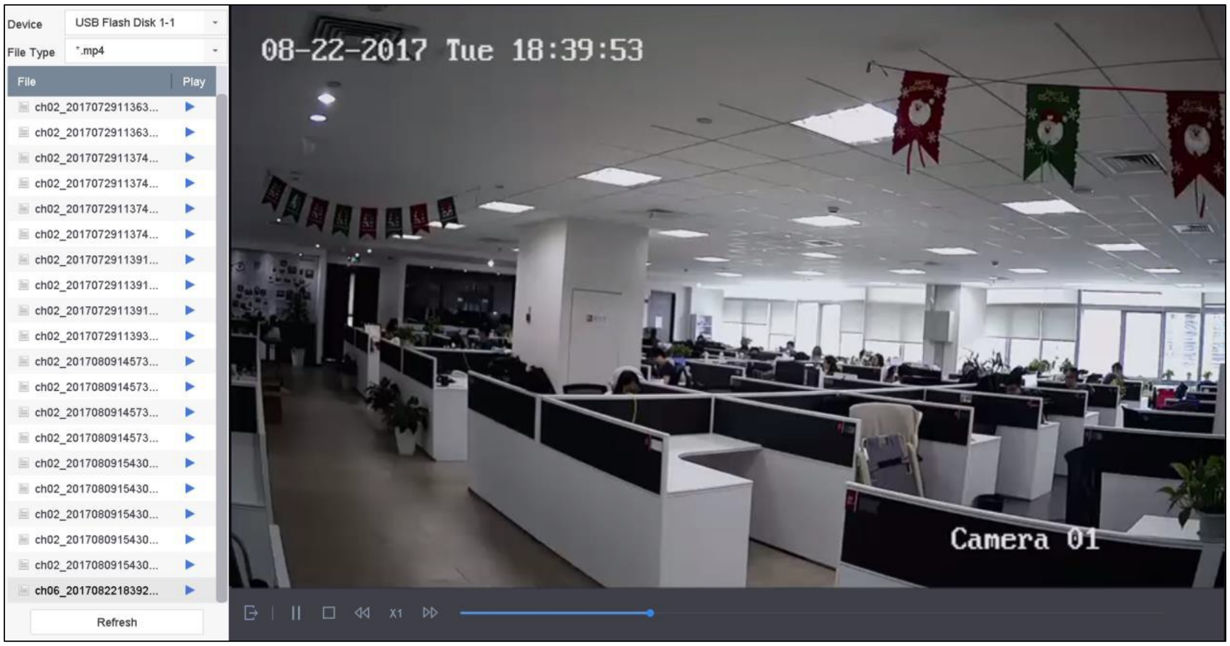
Purpose

You can play files from 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.



Device: USB Flash Disk 1-1

File Type: *.mp4

File	Play
ch02_2017072911363...	▶
ch02_2017072911363...	▶
ch02_2017072911374...	▶
ch02_2017072911374...	▶
ch02_2017072911374...	▶
ch02_2017072911374...	▶
ch02_2017072911391...	▶
ch02_2017072911391...	▶
ch02_2017072911391...	▶
ch02_2017072911393...	▶
ch02_2017080914573...	▶
ch02_2017080914573...	▶
ch02_2017080914573...	▶
ch02_2017080914573...	▶
ch02_2017080915430...	▶
ch02_2017080915430...	▶
ch02_2017080915430...	▶
ch02_2017080915430...	▶
ch02_2017080915430...	▶
ch06_2017082218392...	▶

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

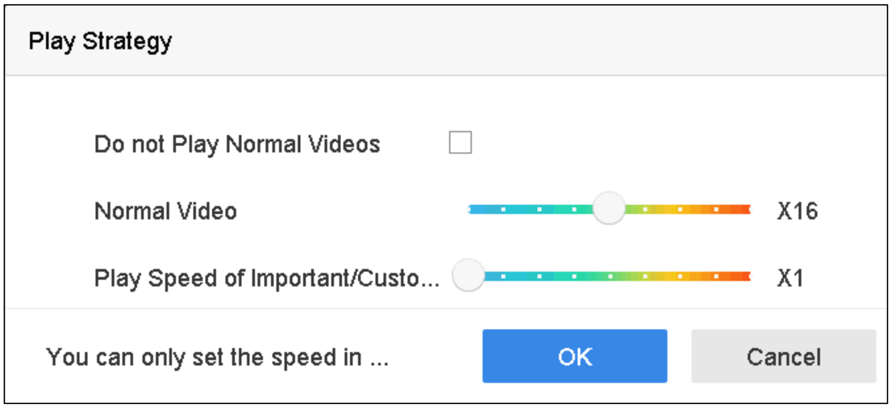
When you are in the important or custom video playback mode, you can set the playing speed separately for the normal video and the important/custom video, or you can select to skip the normal video.

In 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 in the 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.

NOTE

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



Play Strategy

Do not Play Normal Videos □

Normal Video X16

Play Speed of Important/Custo... X1

You can only set the speed in ...

Figure 10-13 Play Strategy

10.2.3 Edit Video Clips

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

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

- [✂]: Set the start time and end time of the video clipping.
- 💾 : 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.

- ①: Play the video in main stream.
- ②: 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.

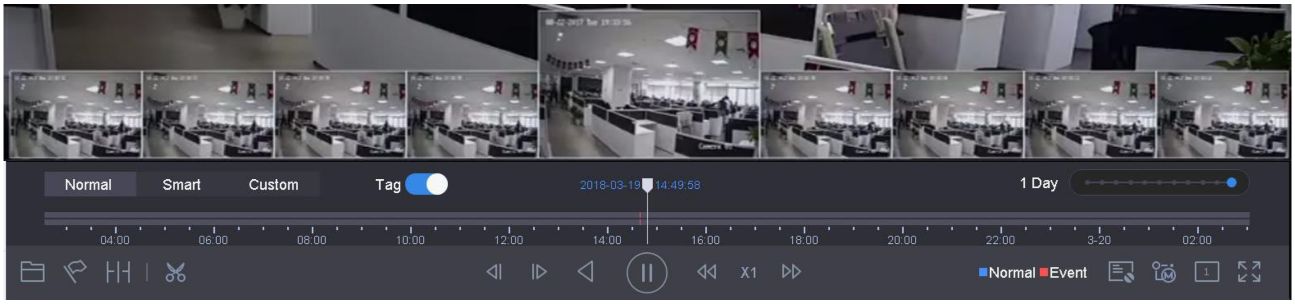


Figure 10-14 Thumbnails View

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

NOTE

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 for a fast view of the video files.

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

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

NOTE

Fast view is supported only in the 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 magnifications (1x to16x).

Figure 10-15 Digital Zoom

Chapter 11 Event and Alarm Settings

11.1 Configure Arming Schedule

1. Select the **Arming Schedule** tab.

2. Choose day of the week and set the time segment. Up to eight time periods can be set for each day.

NOTE

Time periods cannot repeat or overlap.

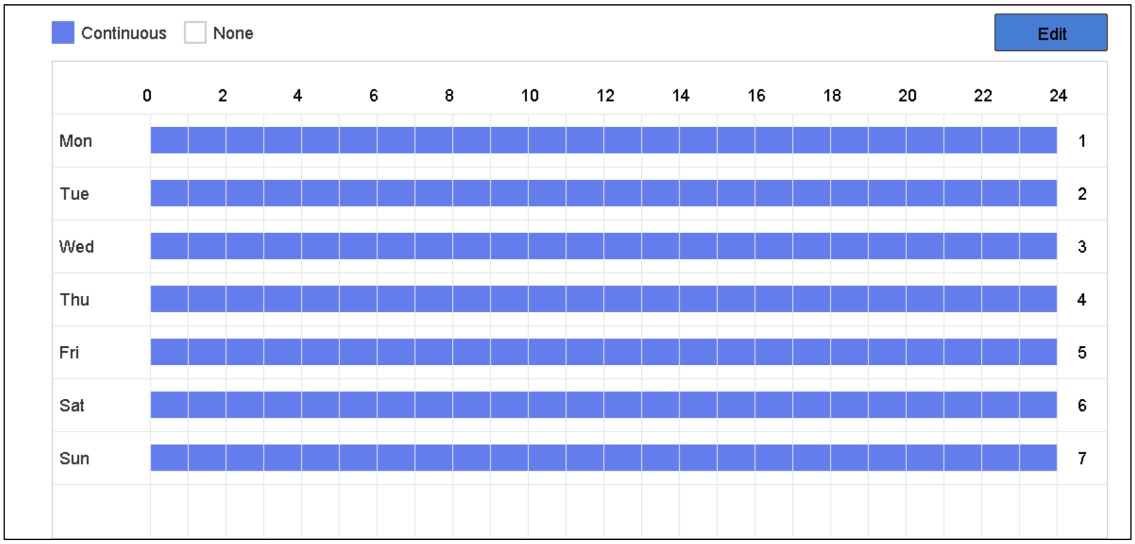


Figure 11-1 Set Arming Schedule

3. (Optional) To copy the arming schedule of the current day to the other day(s) of the week or holiday, click the 📋 icon to copy arming schedule settings.

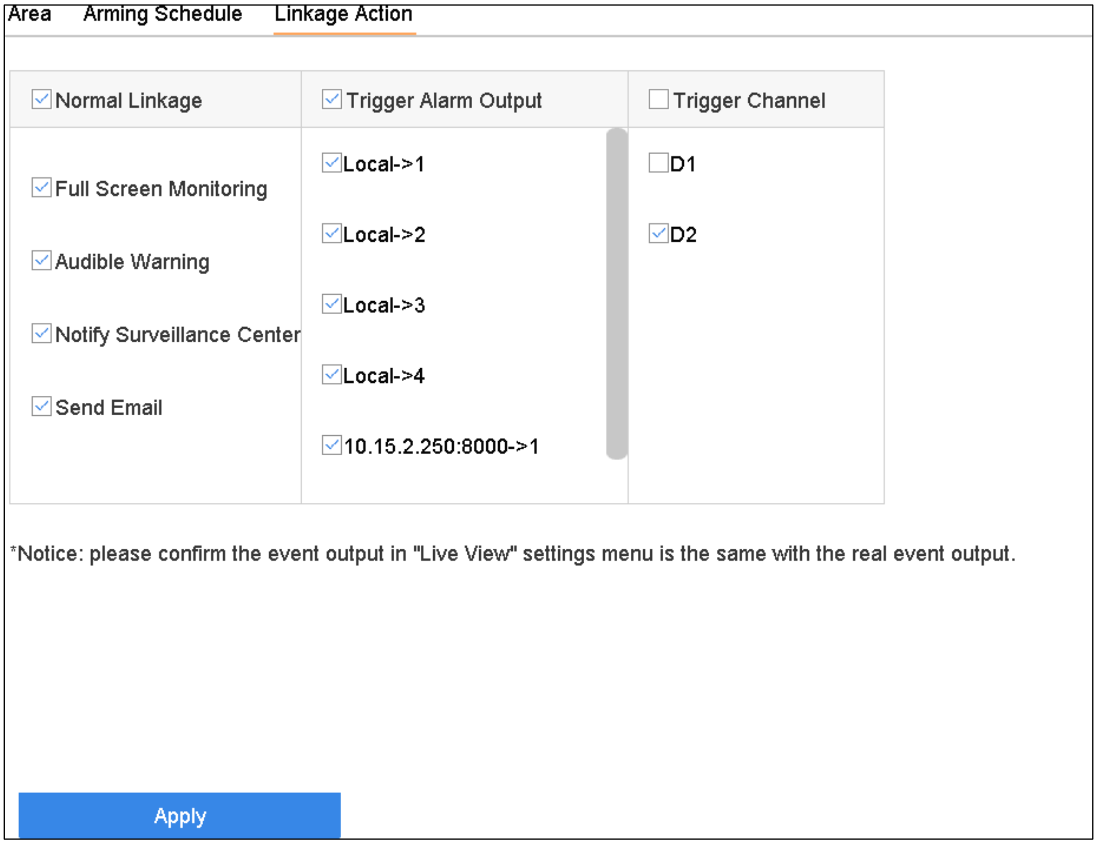
4. Click **Apply** to save the settings.

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 Email.

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



☑ Normal Linkage

☑ Full Screen Monitoring

☑ Audible Warning

☑ Notify Surveillance Center

☑ Send Email

☑ Trigger Alarm Output

☑ Local->1

☑ Local->2

☑ Local->3

☑ Local->4

☑ 10.15.2.250:8000->1

□ Trigger Channel

□ D1

☑ D2

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

Figure 11-2 Set Linkage Actions

2. Select the normal linkage actions, trigger alarm output, or trigger recording channel.

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.

NOTE

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 triggers 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 alarm detection (e.g., motion detection, video tampering, etc.) **Linkage Action** interface.
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).

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. Refer to *Chapter 16.7 Configure Email* for details.

1. Go to **System** > **Network** > **Advanced**.
2. Configure the Email settings.
3. Go to the alarm detection (e.g., motion detection, video tampering, etc.) **Linkage Action** interface.
4. Select the **Send Email** 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 alarm input or event detection (e.g., motion detection, line crossing detection, intrusion detection, etc.) **Linkage Action** interface.

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.

NOTE

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.

NOTE

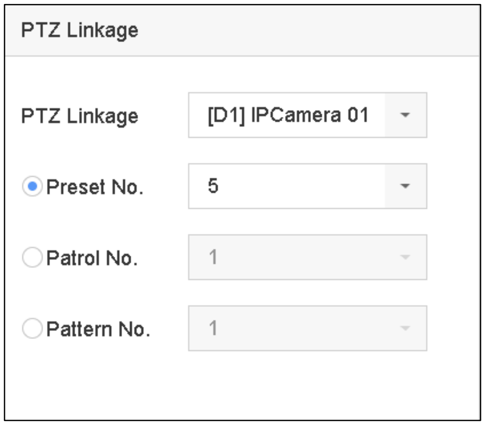
Make sure the PTZ or speed dome connected supports PTZ linkage.

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 no. to call when the alarm events occur.



PTZ Linkage

PTZ Linkage: [D1] IPCamera 01

● Preset No.: 5

○ Patrol No.: 1

○ Pattern No.: 1

Figure 11-3 PTZ Linkage

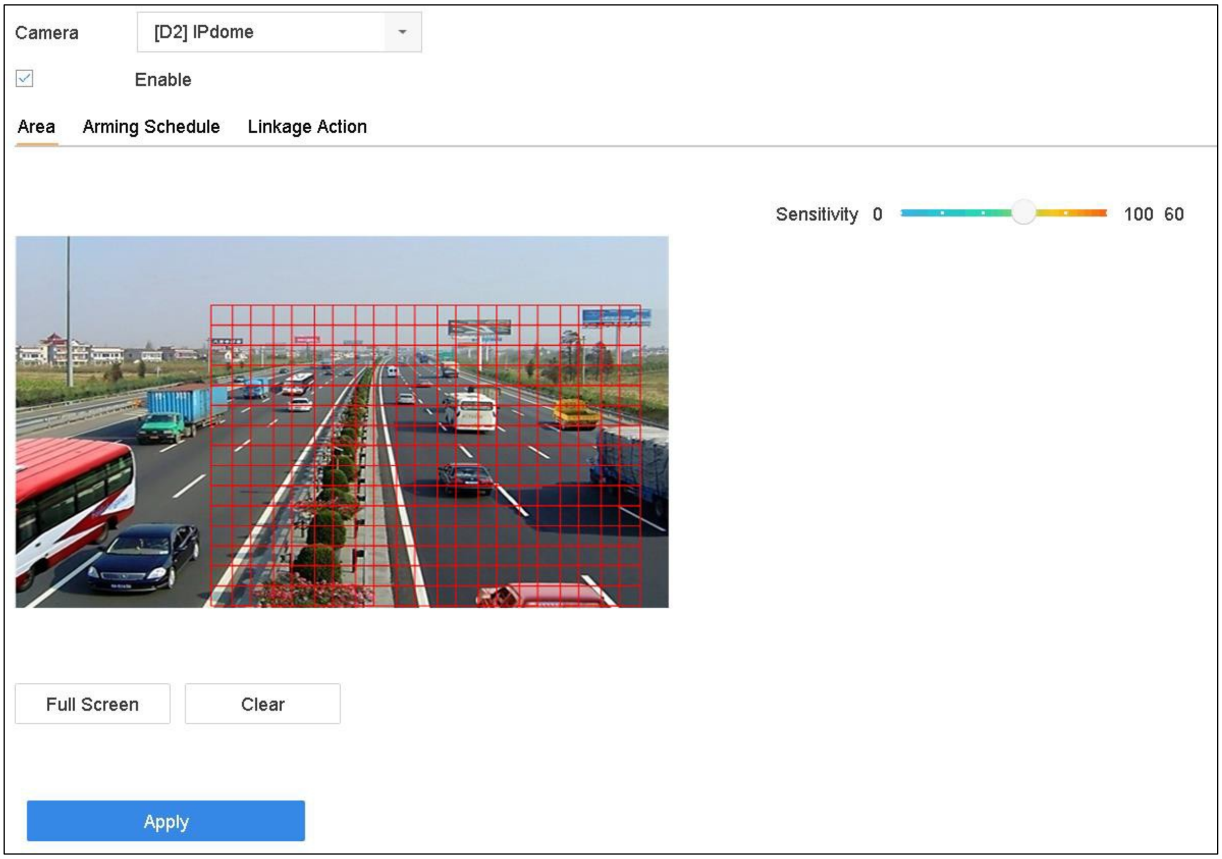
NOTE

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

11.3 Configure Motion Detection Alarm

Motion detection detects moving objects in the monitoring area and triggers an alarm.

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



Camera: [D2] IPdome

☑ Enable

Sensitivity: 60

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.

A higher value more readily triggers motion detection.

6. Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.

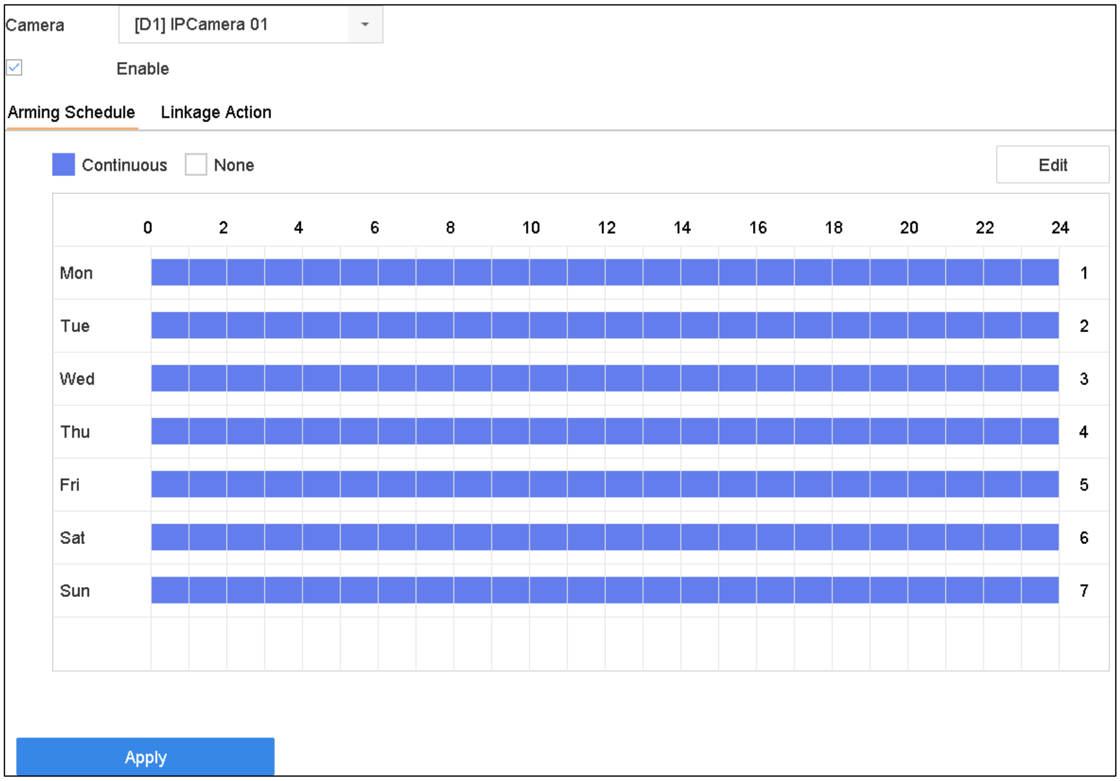
7. Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

11.4 Configure Video Loss Alarm

Purpose

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

1. Go to **System > Event > Normal Event > Video Loss**.



Camera [D1] IPCamera 01

☑ Enable

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*.

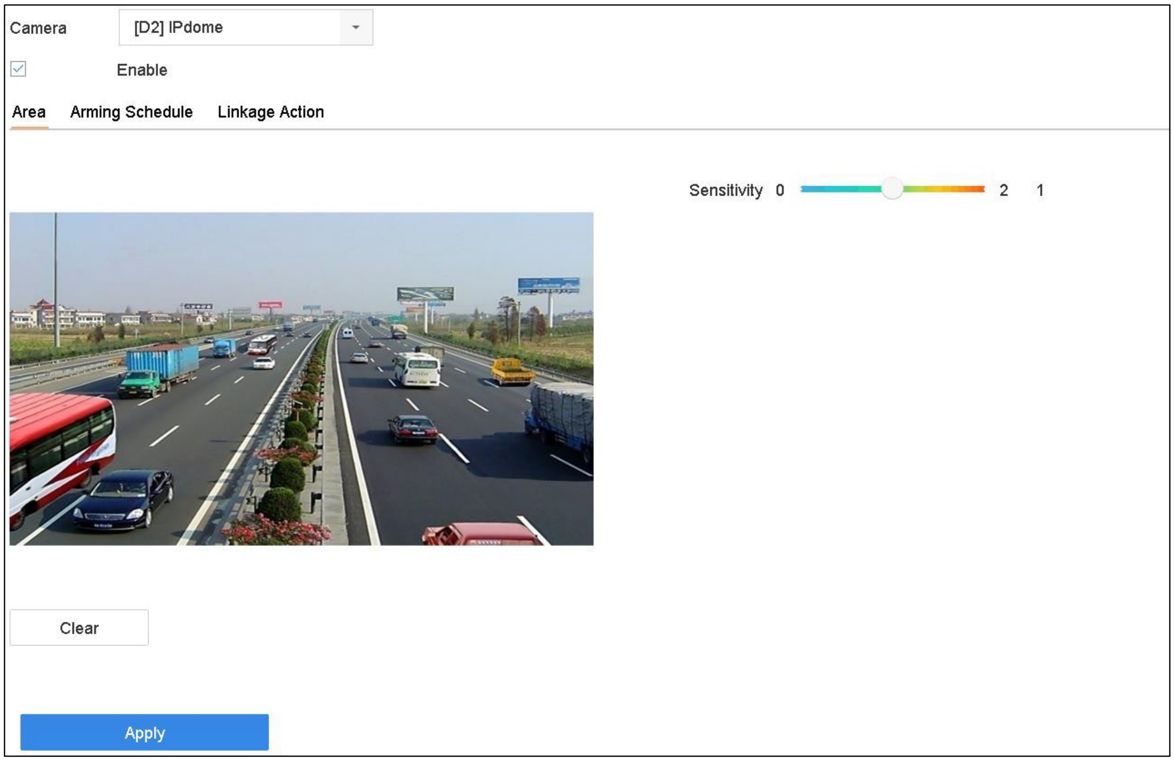
11.5 Configure Video Tampering Alarm

Purpose

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

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

2. Select the camera for which to configure video tampering detection.



Camera [D2] IPdome

☑ Enable

Sensitivity 0 2 1

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 a customized video tampering area.

NOTE

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

5. Set sensitivity level (0-2). Three levels are available. The sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value more readily triggers 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

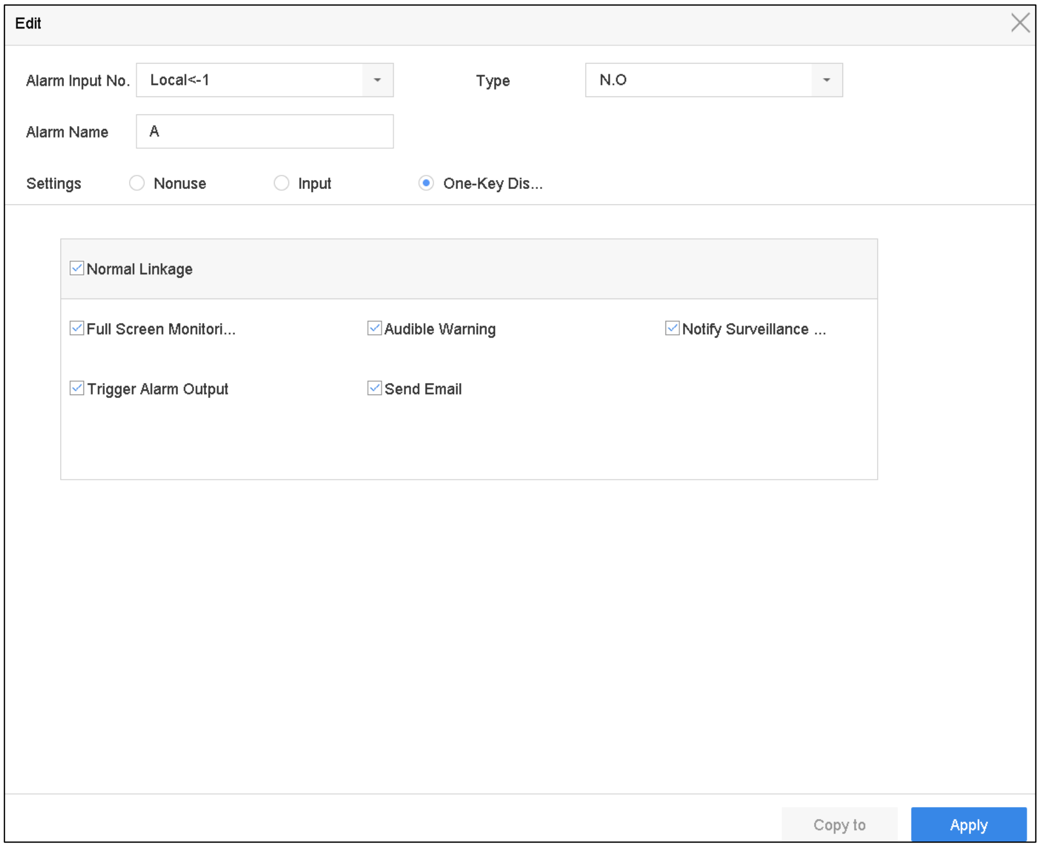
Purpose

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 ✎ .



Alarm Input No. Local<-1

Type N.O

Alarm Name A

Settings ○ Nonuse ○ Input ● One-Key Dis...

☑ Normal Linkage

☑ Full Screen Monitori... ☑ Audible Warning ☑ Notify Surveillance ...

☑ Trigger Alarm Output ☑ Send Email

Figure 11-7 Alarm Input

3. Set the alarm input type to **N.C** or **N.O**.

4. Edit the alarm name.

5. Check the **Input** radio button.

6. Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.

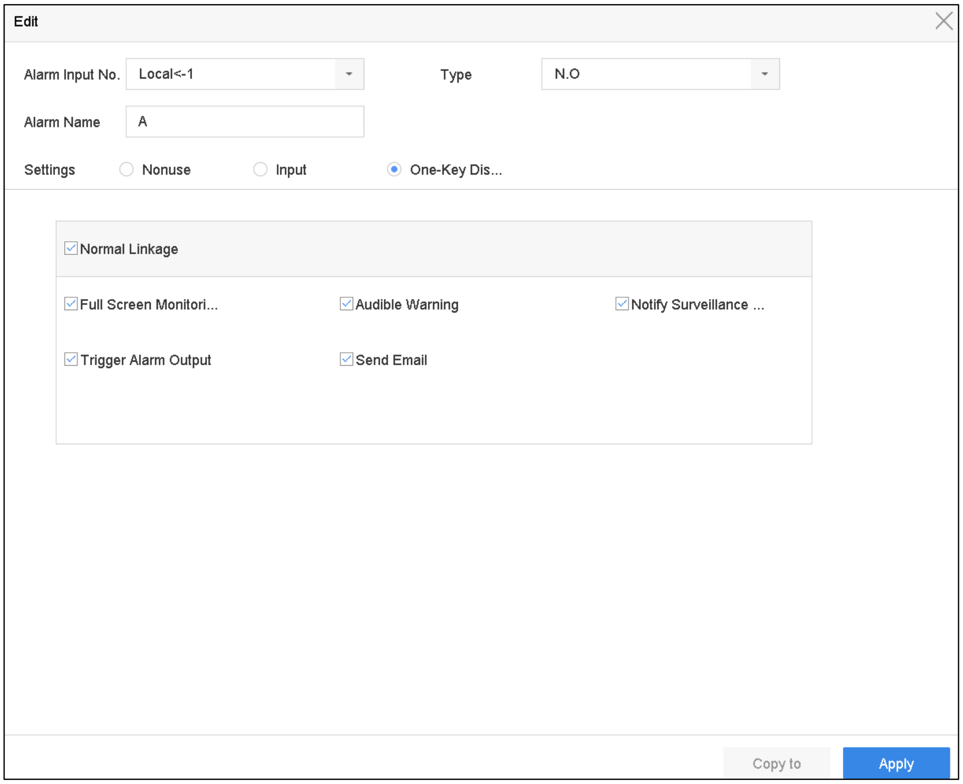
7. Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

8. Click **Apply** and follow the message box to reboot the device to have the settings take effect.

11.6.2 Configure One-Key Disarming

One-key disarming disarms alarm input 1 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. Set the alarm input type to **N.C.** or **N.O**.
4. Edit the alarm name.
5. Check the **Enable One-Key Disarming** radio button.



Edit

Alarm Input No. Local<-1

Type N.O

Alarm Name A

Settings ○ Nonuse ○ Input ● One-Key Dis...

☑ Normal Linkage

☑ Full Screen Monitori... ☑ Audible Warning ☑ Notify Surveillance ...

☑ Trigger Alarm Output ☑ Send Email

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 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**.

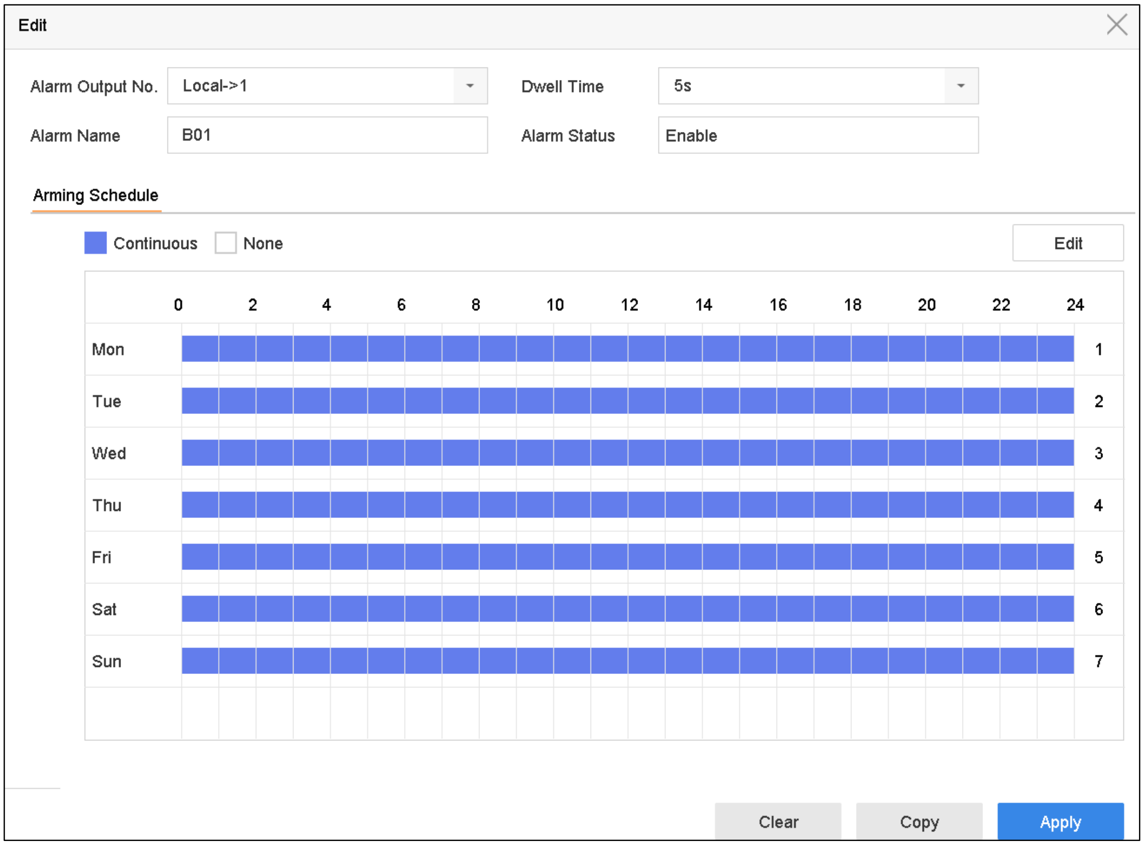
2. Select an alarm output item from the list and click ✎ .

3. Edit the alarm name.

4. Select the dwell time (the alarm duration) from 5s to 600s, or **Manually Clear**.

    - **Manually Clear**: Manually clear an alarm when one 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*.



Alarm Output No. Local->1

Dwell Time 5s

Alarm Name B01

Alarm Status Enable

Figure 11-9 Alarm Output

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

11.7 Configure Exceptions Alarm

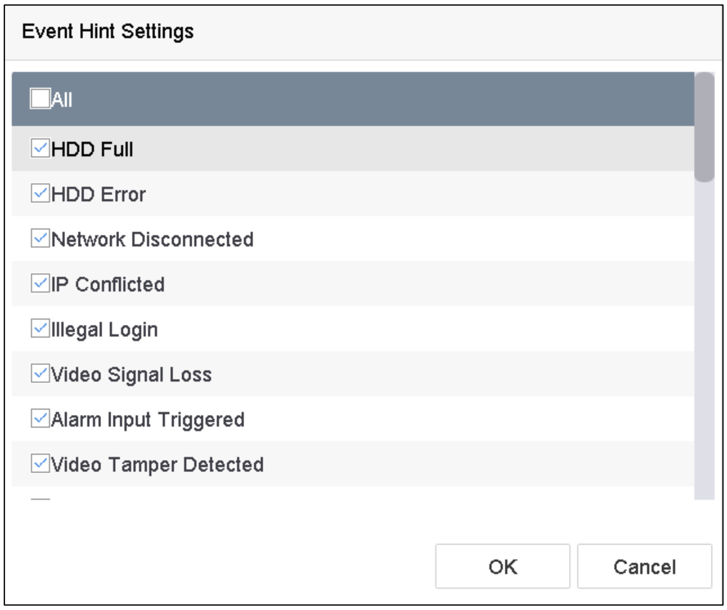
Exception events can be configured to show an event hint in the live view window and trigger alarm output and linkage actions.

1. Go to **System > Event > Normal Event > Exception**.

2. (Optional) Enable the event hint if you want to display it in the live view window.

   1) Check the **Enable Event Hint** checkbox.

   2) Click ⚙ to select the exception type(s) to take the event hint.



Event Hint Settings

□ All

☑ HDD Full

☑ HDD Error

☑ Network Disconnected

☑ IP Conflicted

☑ Illegal Login

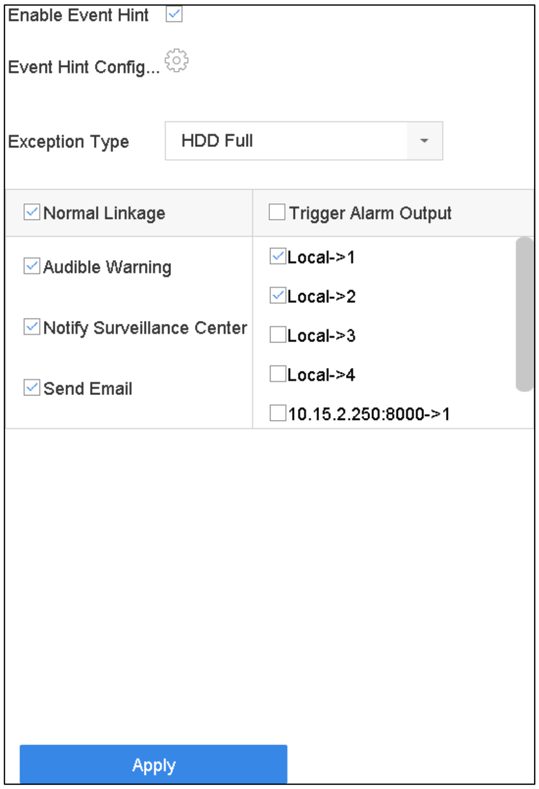
☑ Video Signal Loss

☑ Alarm Input Triggered

☑ Video Tamper Detected

Figure 11-10 Event Hint Settings

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



Enable Event Hint ☑

Event Hint Config...

Exception Type: HDD Full

☑ Normal Linkage	□ Trigger Alarm Output
☑ Audible Warning	☑ Local->1
	☑ Local->2
☑ Notify Surveillance Center	□ Local->3
	□ Local->4
☑ Send Email	□ 10.15.2.250:8000->1

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

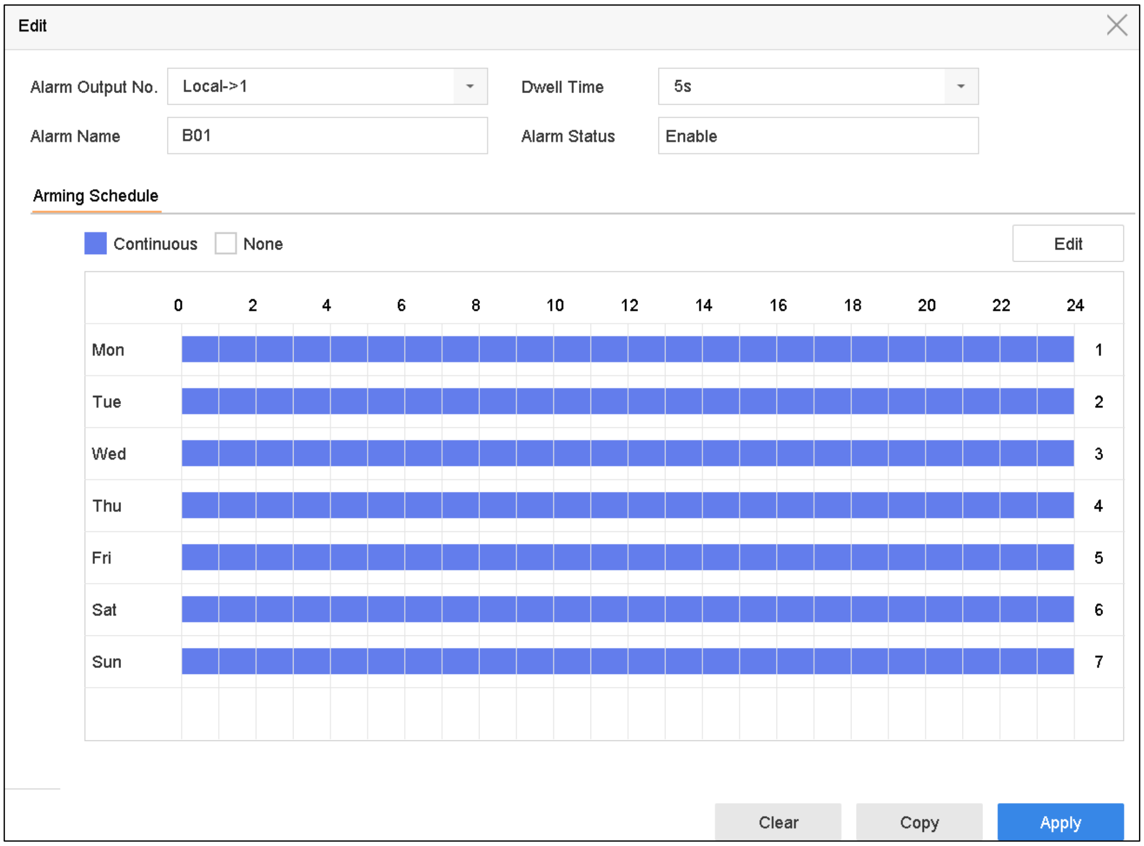
Purpose

A sensor alarm can be triggered or cleared manually. When **Manually Clear** is selected for an alarm output dwell time, 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. Local->1

Dwell Time 5s

Alarm Name B01

Alarm Status Enable

Arming Schedule

Figure 11-12 Alarm Output

Chapter 12 VCA Event Alarm

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

NOTE

VCA detections must be supported by the connected IP camera.

Refer to the network camera user manual for detailed VCA detection instructions.

12.1 Human Body Detection

Human body detection detects human bodies appearing in the monitoring scene, and captures the human body pictures.

NOTE

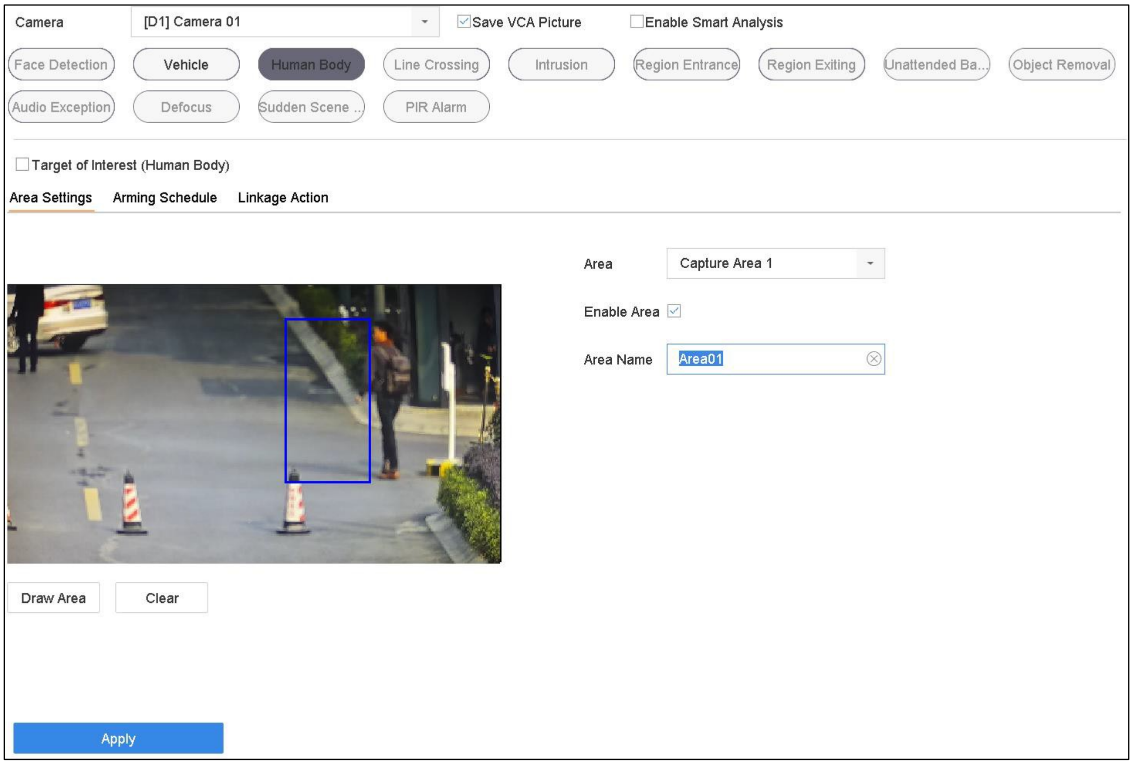
This feature is available only when the connected camera supports human body detection.

1. Go to **System > Event > Smart Event**.
2. Click **Human Body**.
3. Select the camera for which to configure human body detection.
4. Check **Save VCA Picture** to save the captured human body detection pictures.
5. Check **Target of Interest (Human Body)** to discard non-human body pictures and videos that 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 eight detection areas are selectable.

    2) Check the **Enable Area** checkbox to enable the selected detection area.

    3) Edit the area name in the **Scene Name** field. The scene name can contain up to 32 characters.



Camera: [D1] Camera 01

☑ Save VCA Picture

□ Enable Smart Analysis

□ Target of Interest (Human Body)

Area: Capture Area 1

Enable Area ☑

Area Name: Area01

Figure 12-1 Human Body Detection

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

NOTE

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.

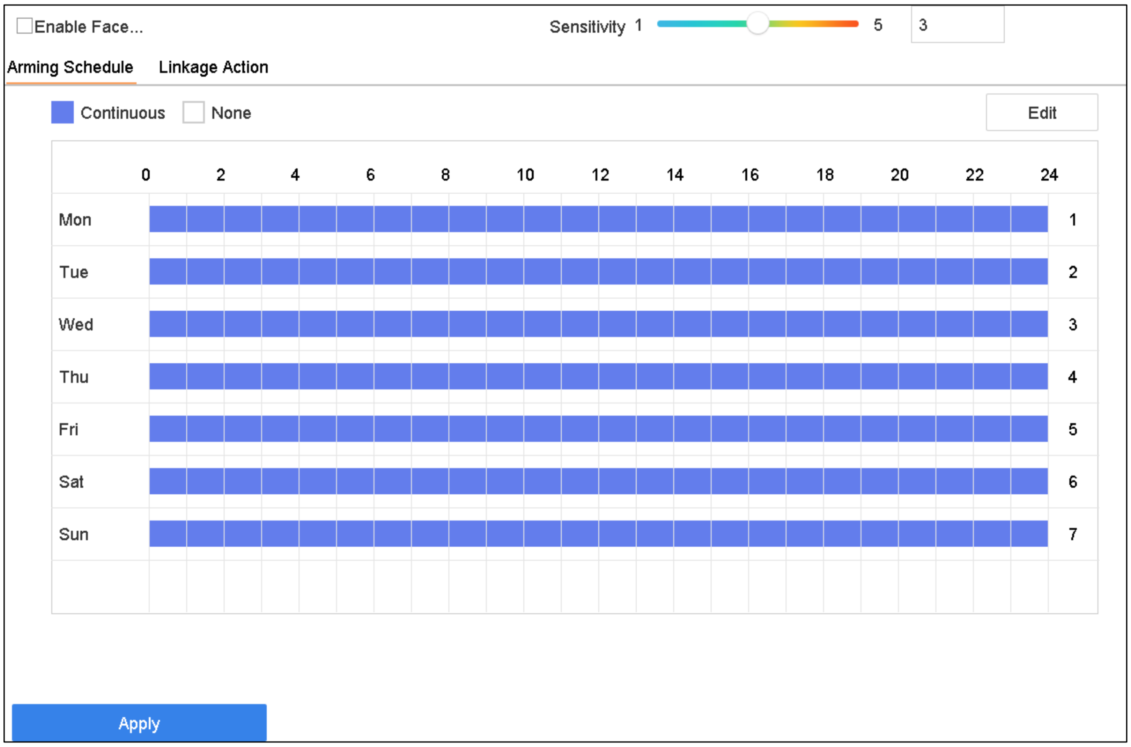
12.2 Face Detection

Purpose

Face detection detects faces appearing in the surveillance scene. Linkage actions will be triggered when a human face is detected.

1. Go to **System > Event > Smart Event**.

2. Click **Face Capture**.



☐Enable Face...

Sensitivity 1 — 5 3

Figure 12-2 Face Detection

3. Select a **Camera** to configure.

4. Check **Enable Face Detection**.

NOTE

For some IP cameras, the checkbox is grey and cannot be checked. In this situation, the function is enabled by default.

5. (Optional) Check **Save VCA Picture** to save the captured face detection pictures.

6. Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-5]. The higher the value, the more easily the face 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**.

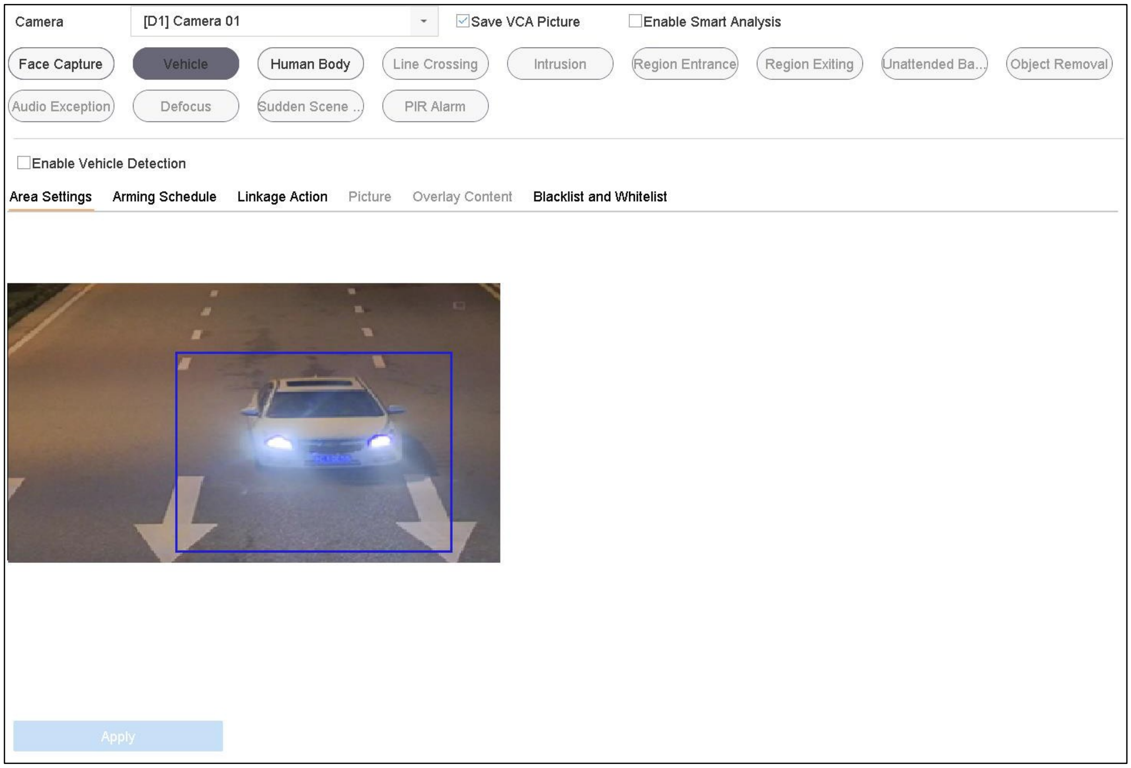
12.3 Vehicle Detection

Purpose

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

1. Go to **System > Event > Smart Event**.

2. Click **Vehicle**.



Camera [D1] Camera 01

☑ Save VCA Picture

□ Enable Smart Analysis

□ Enable Vehicle Detection

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 four lanes are selectable.

9. Click **Save**.

NOTE

Refer to the network camera user manual for detailed vehicle detection instructions.

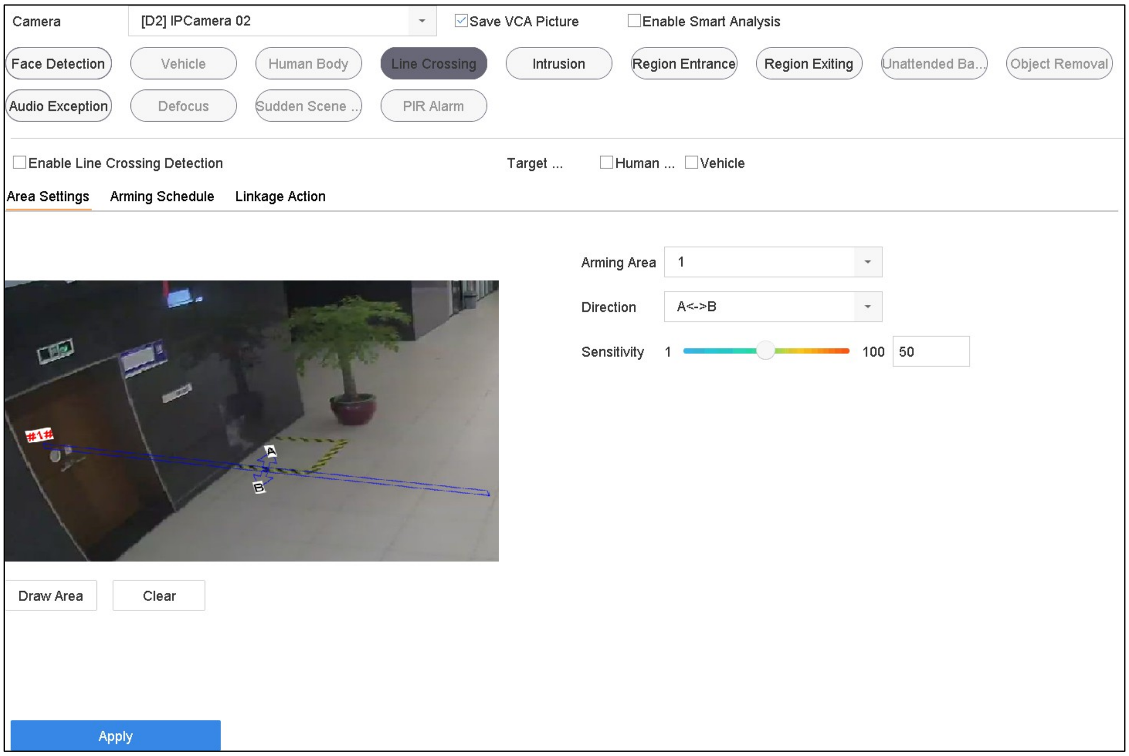
12.4 Line Crossing Detection

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.



Camera [D2] IPCamera 02 ☑Save VCA Picture □Enable Smart Analysis

□Enable Line Crossing Detection Target ... □Human ... □Vehicle

Arming Area 1

Direction A<->B

Sensitivity 1 100 50

Figure 12-4 Line Crossing Detection

3. Select a **Camera** to configure.

4. Check the **Enable Line Crossing Detection** checkbox.

5. (Optional) Check **Save VCA Picture** to save the captured pictures of line crossing detection.

6. Set **Target Detection** as **Human Body** or **Vehicle**.

   - **Human Body**: Discard non-human body pictures and videos that are not triggered by line crossing detection.

   - **Vehicle**: Discard non-vehicle pictures and videos that 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 four arming regions are selectable.

   2) Set 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, both direction can be detected and alarms are triggered.

      - **A->B**: Only an object crossing the configured line from the A side to the B side can be detected.

- **B->A**: Only an 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. The higher the value, 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 targets the size of which ranges from maximum to minimum will 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**.

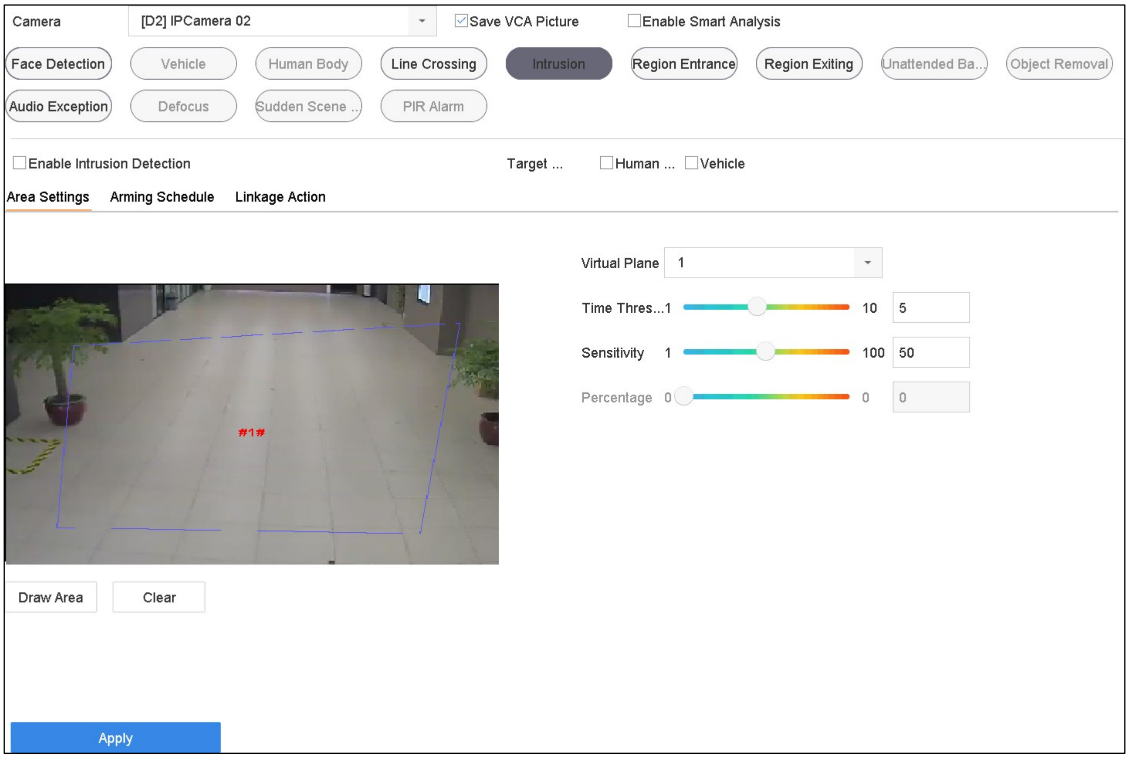
12.5 Intrusion Detection

Purpose

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

1. Go to **System > Event > Smart Event**.

2. Click Intrusion.



Camera [D2] IPCamera 02 ☑Save VCA Picture □Enable Smart Analysis

□Enable Intrusion Detection Target ... □Human ... □Vehicle

Virtual Plane 1

Time Thres... 1 10 5

Sensitivity 1 100 50

Percentage 0 0 0

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 pictures of intrusion detection.

6. Set **Target Detection** as **Human Body** or **Vehicle**.

   - **Human Body**: Discard non-human body pictures and videos that are not triggered by intrusion detection.

   - **Vehicle:** Discard non-vehicle pictures and videos that 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 four virtual panels are selectable.

   2) Drag the sliders to set Time Threshold, Sensitivity, and Percentage.

      - **Time Threshold:** The threshold for the time object loiters in the region. When the object is in the defined detection area longer than the threshold, the device will trigger an alarm. Its range is [1s-10s].

      - **Sensitivity:** The size of an object that can trigger the alarm. The higher the value, 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%, if an object enters the region and occupies half of the whole region, the 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 targets the size of which range from maximum to minimum will 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*.

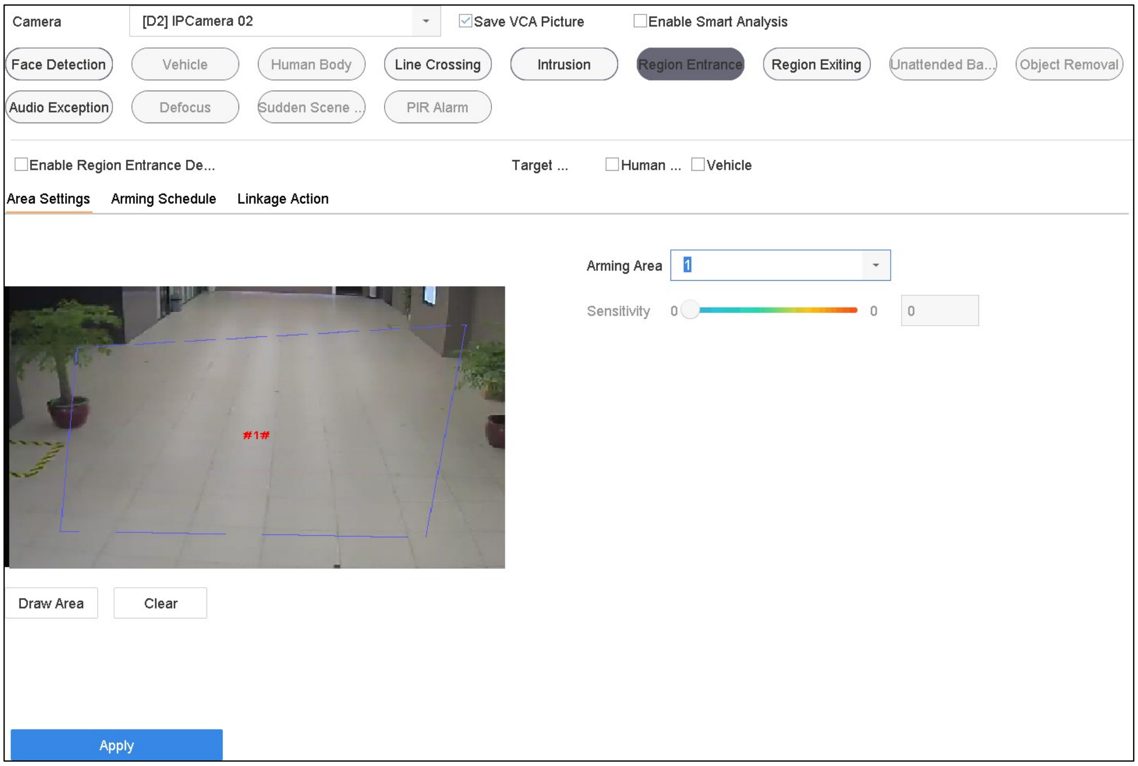
11. Click **Apply**.

12.6 Region Entrance Detection

Purpose
Region entrance detection detects objects that enter a pre-defined virtual region.

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

2. Click **Region Entrance Detection**.



Camera [D2] IPCamera 02

☑ Save VCA Picture

□ Enable Smart Analysis

□ Enable Region Entrance De...

Target ... □ Human ... □ Vehicle

Arming Area 1

Sensitivity 0 0

Figure 12-6 Region Entrance Detection

3. Select a **Camera** to configure.

4. Check **Enable Region Entrance Detection**.

5. (Optional) Check **Save VCA Picture** to save the captured pictures of region entrance detection.

6. Set **Target Detection** as **Human Body** or **Vehicle**.

    - **Human Body**: Discard non-human body pictures and videos not triggered by region entrance detection.

    - **Vehicle:** Discard non-vehicle pictures and videos 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 four regions are selectable.

    2) Drag the sliders to set Sensitivity.

        - **Sensitivity:** The higher the value, 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**.

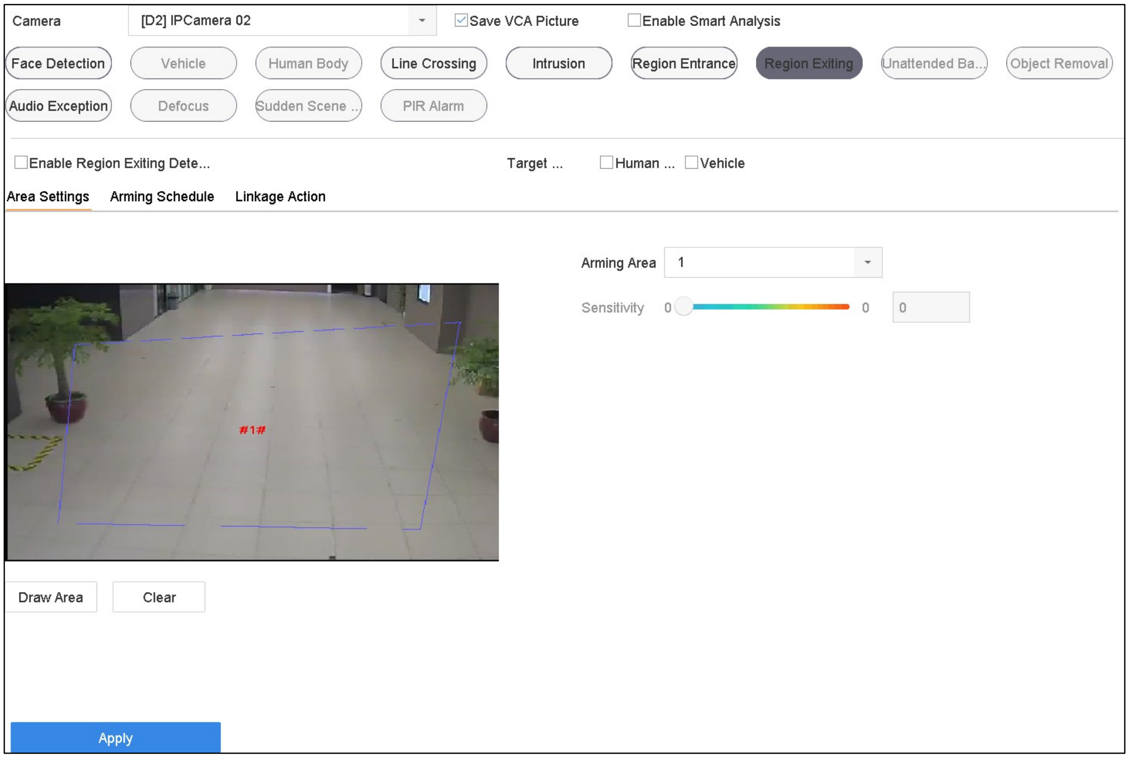
12.7 Region Exiting Detection

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**.



Camera [D2] IPCamera 02

☑ Save VCA Picture

□ Enable Smart Analysis

□ Enable Region Exiting Dete...

Target ... □ Human ... □ Vehicle

Arming Area 1

Sensitivity 0 0 0

Figure 12-7 Region Exiting Detection

3. Select a **Camera** to configure.

4. Check **Enable Region Exiting Detection**.

5. (Optional) Check **Save VCA Picture** to save the captured pictures of region exiting detection.

6. Set **Target Detection** as **Human Body** or **Vehicle**.

   - **Human Body**: Discard non-human body pictures and videos not triggered by region exiting detection.

   - **Vehicle:** Discard non-vehicle pictures and videos 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 four regions are selectable.

   2) Drag the sliders to set Sensitivity.

  - **Sensitivity:** The higher the value, the more easily detection alarm is triggered. 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**.

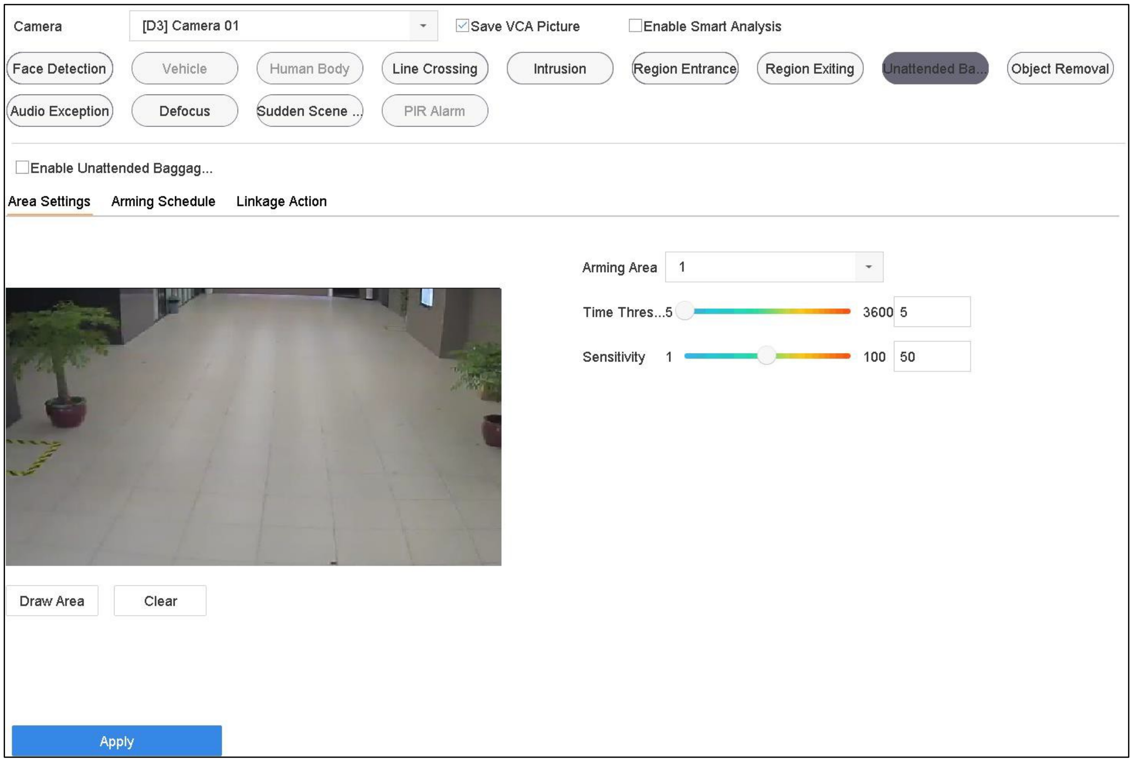
12.8 Unattended Baggage Detection

Purpose

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

1. Go to **System > Event > Smart Event**.

2. Click **Unattended Baggage**.



Camera [D3] Camera 01

☑Save VCA Picture

□Enable Smart Analysis

□Enable Unattended Baggag...

Arming Area 1

Time Thres...5 3600 5

Sensitivity 1 100 50

Figure 12-8 Unattended Baggage Detection

- Select a **Camera** to configure.
- Check **Enable Unattended Baggage Detection**.
- Optionally, check **Save VCA Picture** to save the captured pictures of unattended baggage detection.

- Follow the steps to set the detection rules and detection areas.

  1) Select an **Arming Region** to configure. Up to four 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, the more easily the detection alarm can be triggered.

  3) Click **Draw Region** and draw a quadrilateral in the preview window by specifying four detection region vertexes.

- Set the arming schedule. Refer to *Chapter 11.1 Configure Arming Schedule*.

- Set the linkage actions. Refer to *Chapter 11.2 Configure Alarm Linkage Actions*.

- Click **Apply**.

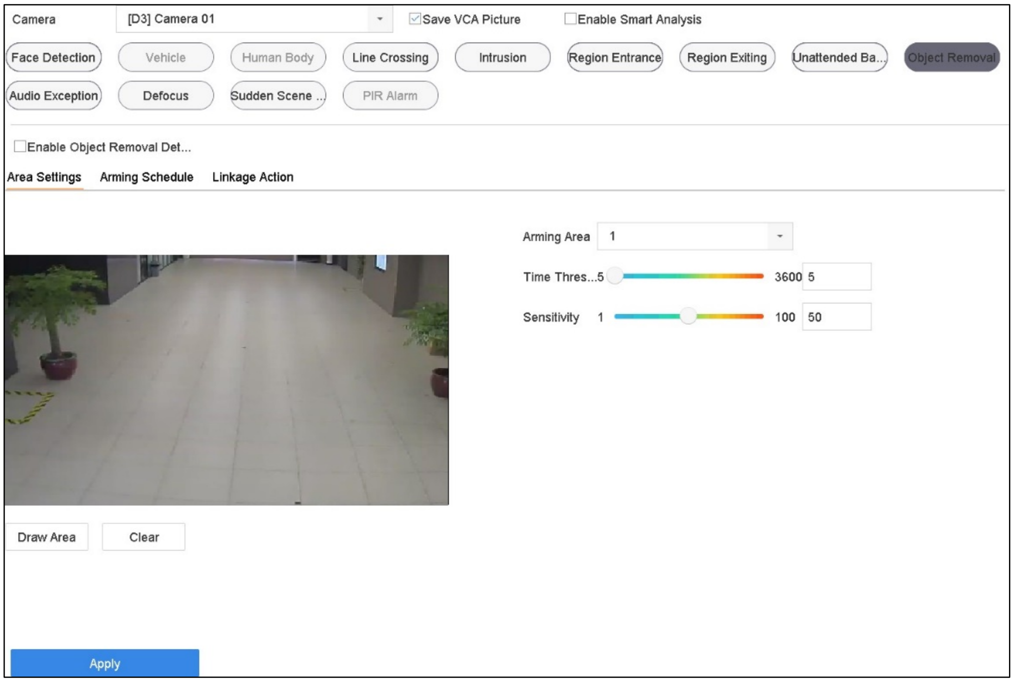
12.9 Object Removal Detection

Purpose

Object removal detection detects objects removed from a pre-defined region such as 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 Removal**.



Camera [D3] Camera 01

☑ Save VCA Picture

☐ Enable Smart Analysis

☐ Enable Object Removal Det...

Arming Area 1

Time Thres...5 3600 5

Sensitivity 1 100 50

Figure 12-9 Object Removal Detection

3. Select a **Camera** to configure.

4. Check **Enable Object Removable Detection**.

5. (Optional) Check **Save VCA Picture** to save the captured object removable detection pictures.

6. Follow the steps to set the detection rules and detection areas.

   1) Select an Arming Region to configure. Up to four regions are selectable.

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

      - **Time Threshold:** The time the objects were 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. If the sensitivity is high, a very small object taken from the region will trigger an 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*.

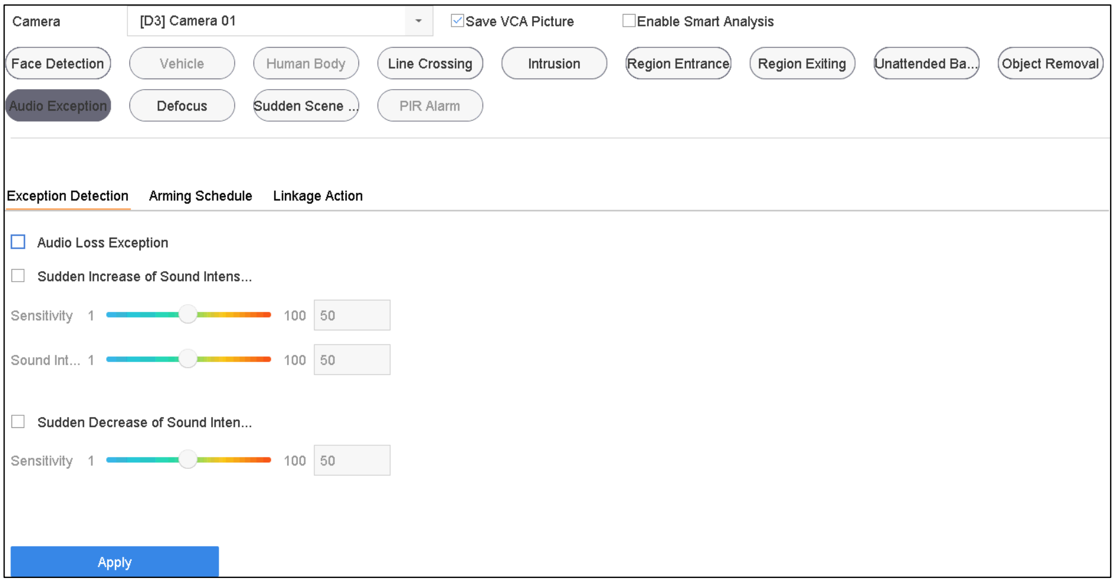
9. Click **Apply**.

12.10 Audio Exception Detection

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

1. Go to **System > Event > Smart Event**.

2. Click **Audio Exception**.



Camera [D3] Camera 01 ☑ Save VCA Picture □ Enable Smart Analysis

□ Audio Loss Exception

□ Sudden Increase of Sound Intens...

Sensitivity 1 100 50

Sound Int... 1 100 50

□ Sudden Decrease of Sound Inten...

Sensitivity 1 100 50

Figure 12-10 Audio Exception Detection

3. Select a **Camera** to configure.

4. Optionally, check **Save VCA Picture** to save the captured audio exception detection pictures.

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 steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise. You need to configure its **Sensitivity** and **Sound Intensity Threshold**.

        - **Sensitivity**: The smaller the value, the more severe the change must be to trigger detection. Range [1-100].

        - **Sound Intensity Threshold**: Filters the environment sound. 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 a steep drop in the surveillance scene sound. 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**.

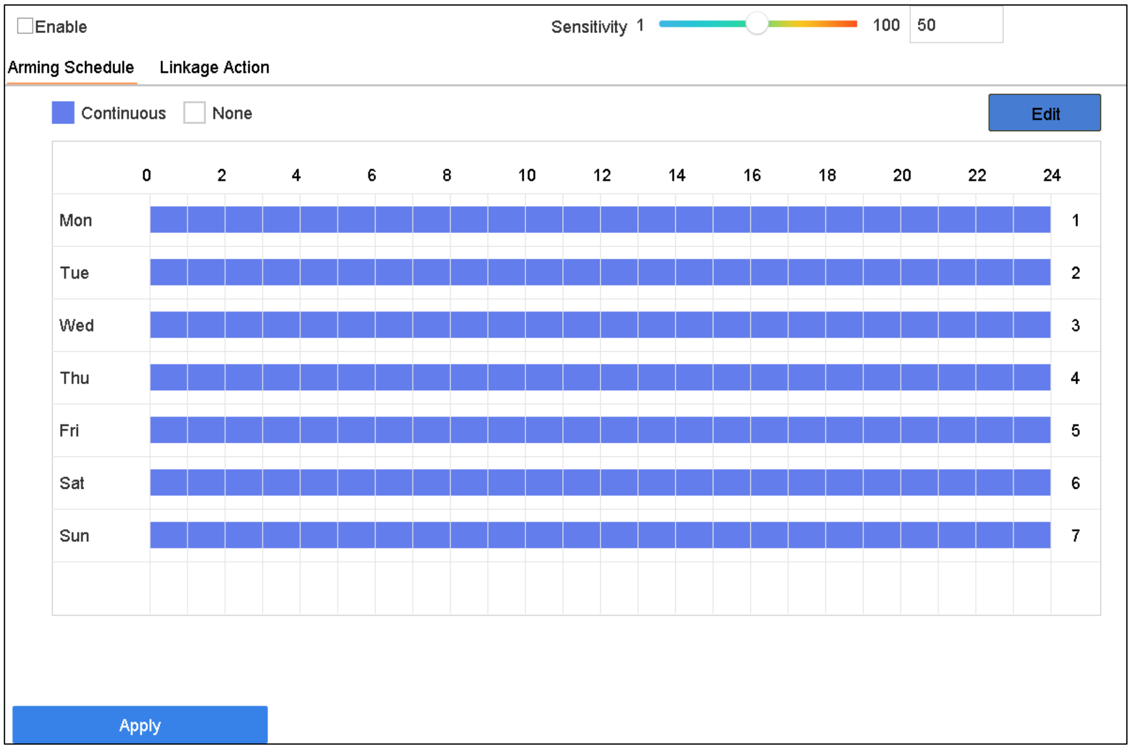
12.11 Sudden Scene Change Detection

Purpose

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

1. Go to **System > Event > Smart Event**.

2. Click **Sudden Scene Change**.



□ Enable

Sensitivity 1 100 50

Figure 12-11 Sudden Scene Change

3. Select a **Camera** to configure.

4. Check **Enable Sudden Scene Change Detection**.

5. (Optional) Check **Save VCA Picture** to save the captured sudden scene change detection pictures.

6. Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value, the more easily the change of scene will 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**.

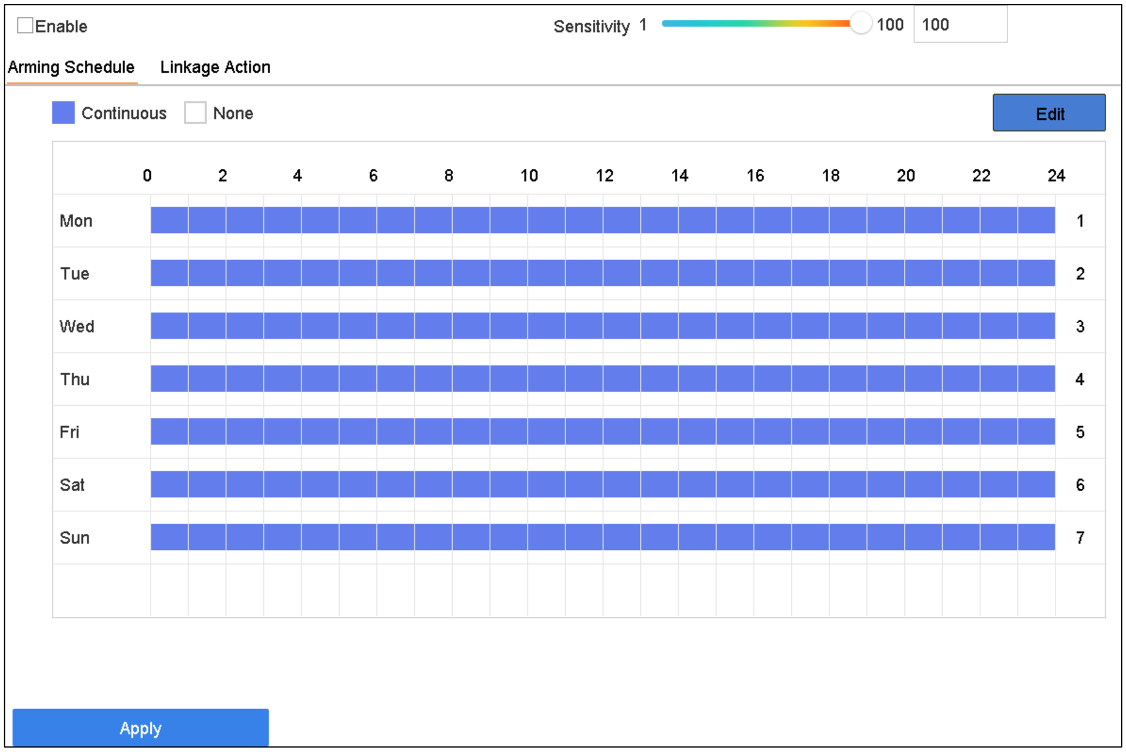
12.12 Defocus Detection

Purpose

Image blur caused by lens defocus can be detected.

1. Go to **System > Event > Smart Event**.

2. Click **Defocus**.



□ Enable

Sensitivity 1 —— 100 100

🟦 Continuous □ None

	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

Figure 12-12 Defocus Detection

3. Select a **Camera** to configure.

4. Check **Enable Defocus Detection**.

5. (Optional) Check **Save VCA Picture** to save the captured defocus detection pictures.

6. Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value, the more easily the defocus image will 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**.

12.13 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 creature such as dogs, cats, etc., can be detected.

1. System > Event > Smart Event.
2. Click **PIR Alarm**.
3. Select a **Camera** to configure.
4. Check **PIR Alarm**.
5. (Optional) Check **Save VCA Picture** to save the captured PIR alarm pictures.
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**.

12.14 Enable Smart Analysis

Purpose
You can enable smart search for IP cameras that do not support line crossing or intrusion detection, and the NVR will analyze line crossing and intrusion events. Supported 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 the pop-up message box.

Chapter 13 Smart Search

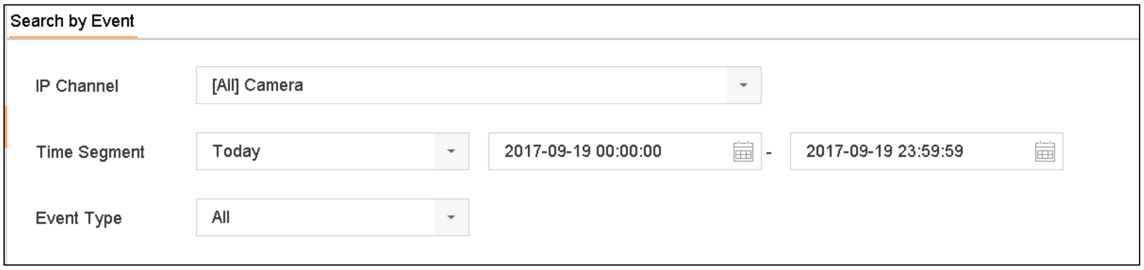
With the configured VCA detection, the NVR can search for pictures, video files and resources of the human body detection, behavior analysis, face detection, people counting, and heat map results.

13.1 Face Search

Purpose
When face pictures are captured and saved in the HDD, you can search the face pictures and play the picture-related video file according to the specified conditions.

1. Go to **Smart Analysis** > **Smart Search** > **Face Search**.

2. Select the IP camera for the face search.



Search by Event

IP Channel: [All] Camera

Time Segment: Today 2017-09-19 00:00:00 - 2017-09-19 23:59:59

Event Type: All

Figure 13-1 Face Search

3. Specify the start time and end time to search for captured face pictures or video files.

4. Click **Start Search** to start searching.

5. Double-click a face picture to play its related video file in the view window on the top right.

6. To export the captured face pictures to a local storage device, connect the storage device to the NVR and click **Export**.

13.2 Vehicle Search

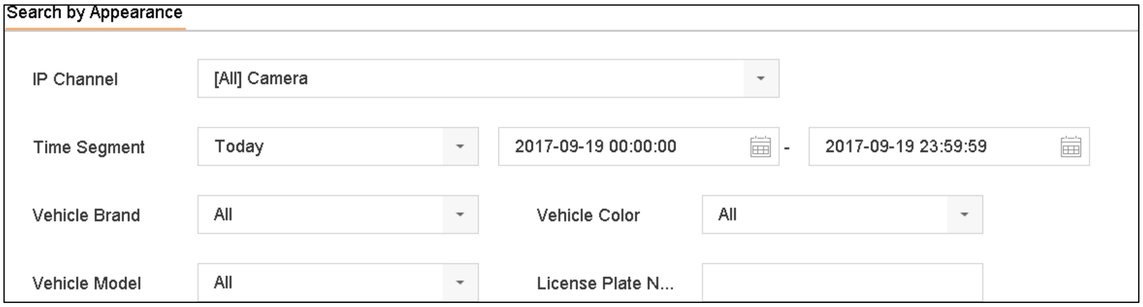
Purpose
You can search and view the matched captured vehicle pictures.

1. Go to **Smart Analysis > Smart Search > Vehicle Search**.

2. Select the IP camera for the vehicle search.

3. Set search conditions.

4. Click **Start Search**.



Search by Appearance

IP Channel: [All] Camera

Time Segment: Today 2017-09-19 00:00:00 - 2017-09-19 23:59:59

Vehicle Brand: All Vehicle Color: All

Vehicle Model: All License Plate N...

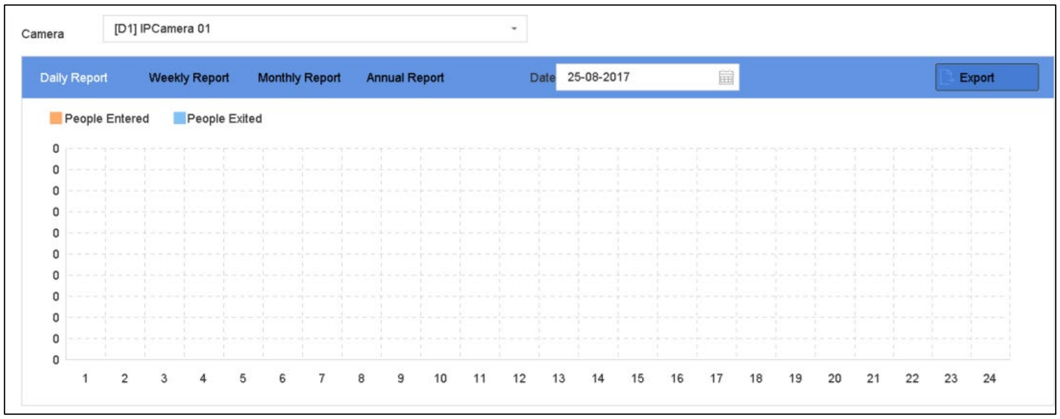
Figure 13-2 Plate Search

13.3 People Counting

Purpose

People Counting calculates the number of people who entered or left a configured area and creates daily/weekly/monthly/annual reports for analysis.

1. Go to **Smart Analysis** > **Counting**.
2. Select a camera.
3. Set the report type to **Daily Report, Weekly Report, Monthly Report**, or **Annual Report**.
4. Set the **Date** to analyze, then the people counting graphic will show.



Camera: [D1] IPCamera 01

Date: 25-08-2017

Figure 13-3 People Counting Interface

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

13.4 Heat Map

Purpose

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

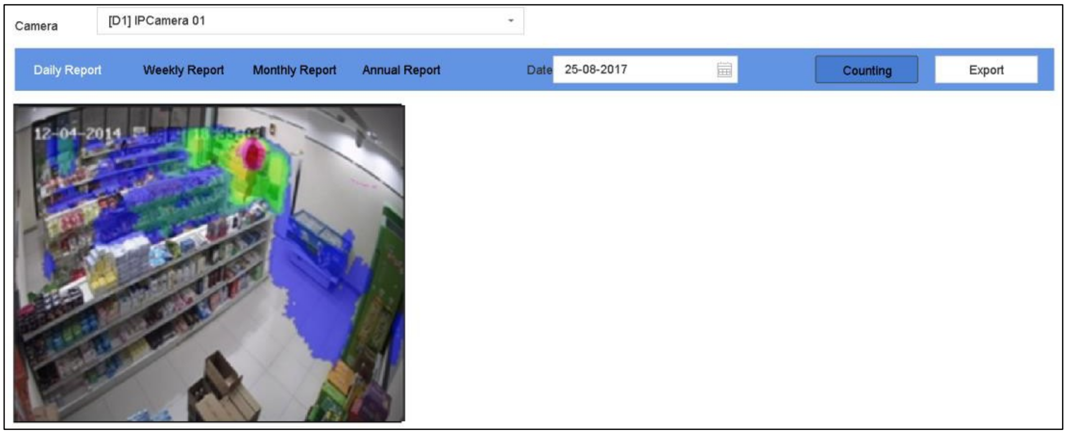
The heat map function must be supported by the connected IP camera and the corresponding configuration must be set.

1. Go to **Smart Analysis > Heat Map**.

2. Select a camera.

3. Set the report type as **Daily Report, Weekly Report, Monthly Report**, or **Annual Report.**

4. Set the **Data** to analyze.



Camera [D1] IPCamera 01

Date 25-08-2017

Figure 13-4 Heat Map Interface

5. Click **Counting**. The results displayed in graphics marked in different colors will show.

NOTE

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

6. (Optional) Click **Export** to export the statistics report in Excel format.

Chapter 14 Human Body Detection

14.1 View Engine Status

Purpose

A smart analysis engine is applied to analyze false alarms and smart analysis tasks.

1. Go to **Smart Analysis > Smart Analysis > Engine Configuration** to view the working status, usage rate, and applied channel of the smart analysis engine.

14.2 Human Body Search

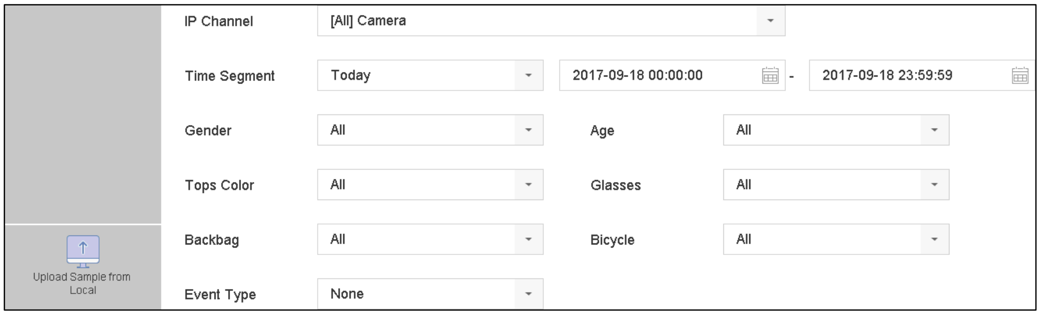
Purpose

Search human body pictures according to manually specified search conditions.

Before You Start

Import the human body pictures you want to search.

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



IP Channel: [All] Camera

Time Segment: Today 2017-09-18 00:00:00 - 2017-09-18 23:59:59

Gender: All

Age: All

Tops 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 with to a POS machine/server and receive transaction messages for overlay on the image during live view or playback, as well as trigger the POS event alarm.

15.1 Configure POS Settings

15.1.1 Configure POS Connection

1. Go to **System > POS Settings**.

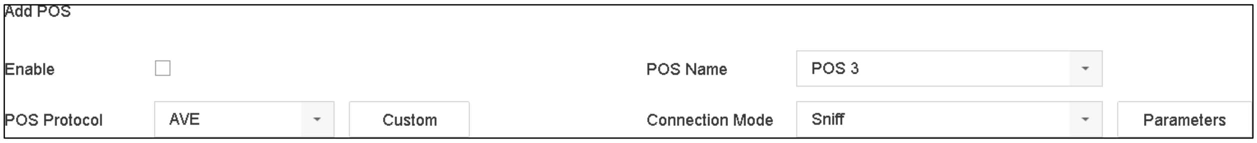
2. Click **Add** to enter the POS adding interface.

3. Select a POS from the drop-down list.

4. Check **Enable**.

NOTE

The number of POS devices supported by each NVR is half its number of channels.



Add POS

Enable □

POS Name: POS 3

POS Protocol: AVE

Connection Mode: Sniff

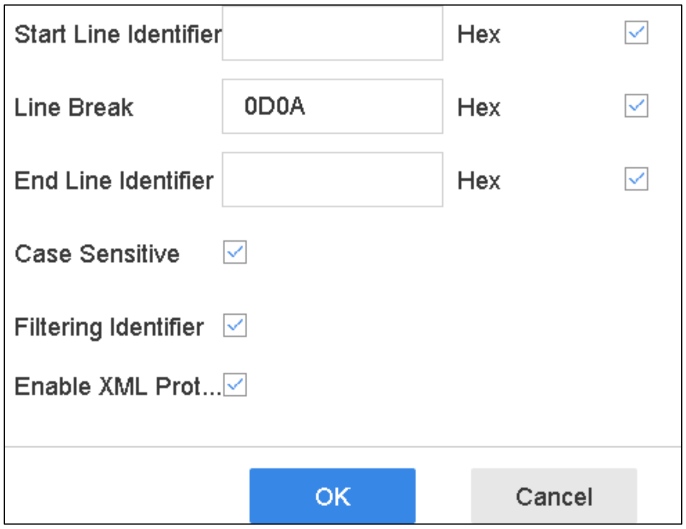
Figure 15-1 POS Settings

5. Set the POS protocol to **Universal Protocol**, **EPSON**, **AVE**, or **NUCLEUS**, as appropriate.

NOTE

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

- **Universal Protocol** – Click the **Advanced** button to expand more settings when selecting universal protocol. You can set the start line identifier, line break tag, end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.



Start Line Identifier		Hex	☑
Line Break	0D0A	Hex	☑
End Line Identifier		Hex	☑
Case Sensitive	☑		
Filtering Identifier	☑		
Enable XML Prot...	☑		

Figure 15-2 Universal Protocol Settings

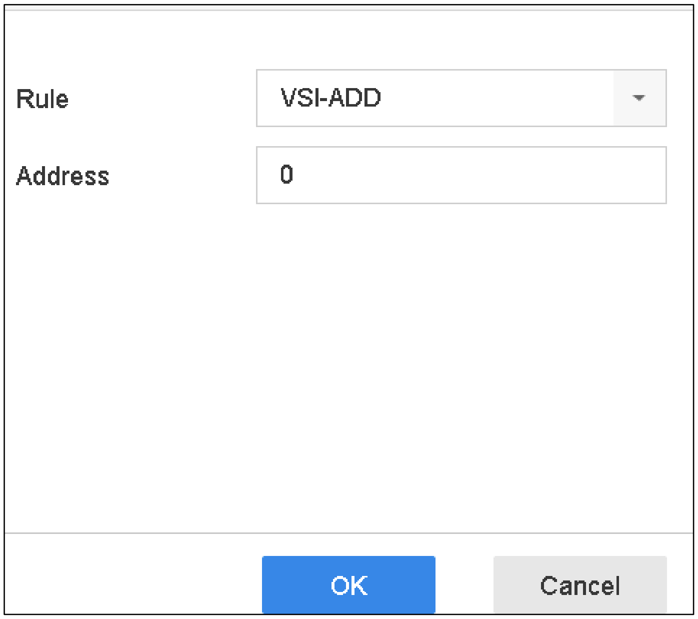
- **EPSON** – The fixed start and end line tag are used for EPSON protocol.
- **AVE** – The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

1) Click **Custom** to configure the 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 the settings.



Rule: VSI-ADD

Address: 0

Figure 15-3 AVE Settings

- **NUCLEUS** – 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.

NOTE

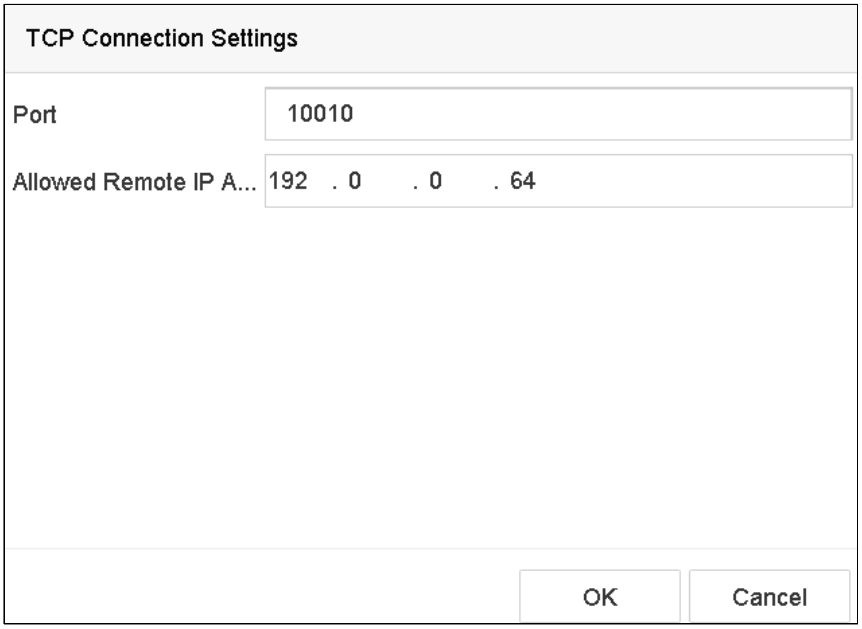
NUCLEUS protocol must be used for RS-232 connection communication.

6. Set the connection mode to **TCP Connection**, **UDP Connection**, **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.



TCP Connection Settings

Port: 10010

Allowed Remote IP A...: 192 . 0 . 0 . 64

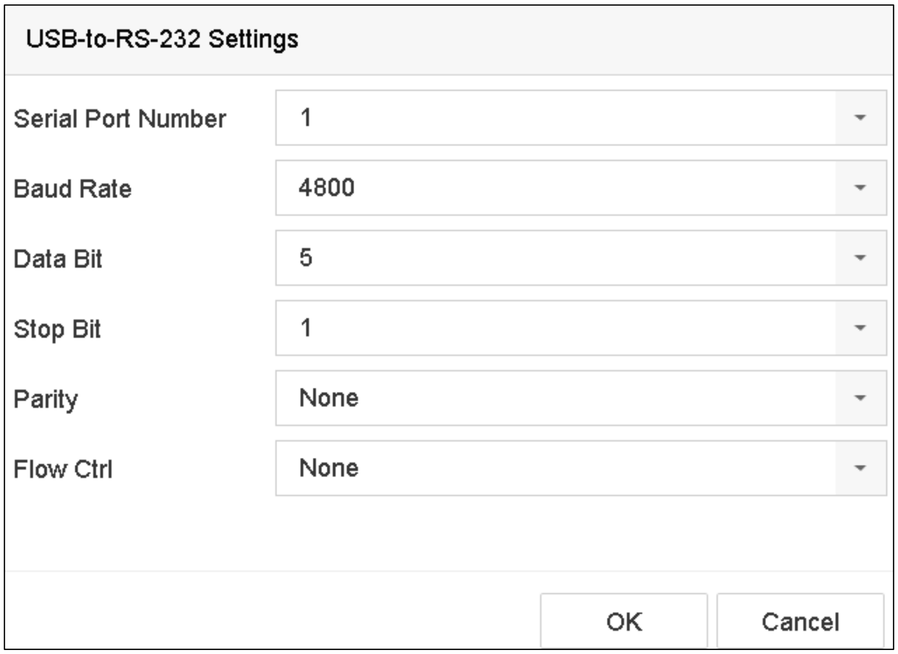
Figure 15-4 TCP Connection Settings

- UDP Connection

  1) When using a 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 USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, parity, and flow ctrl.

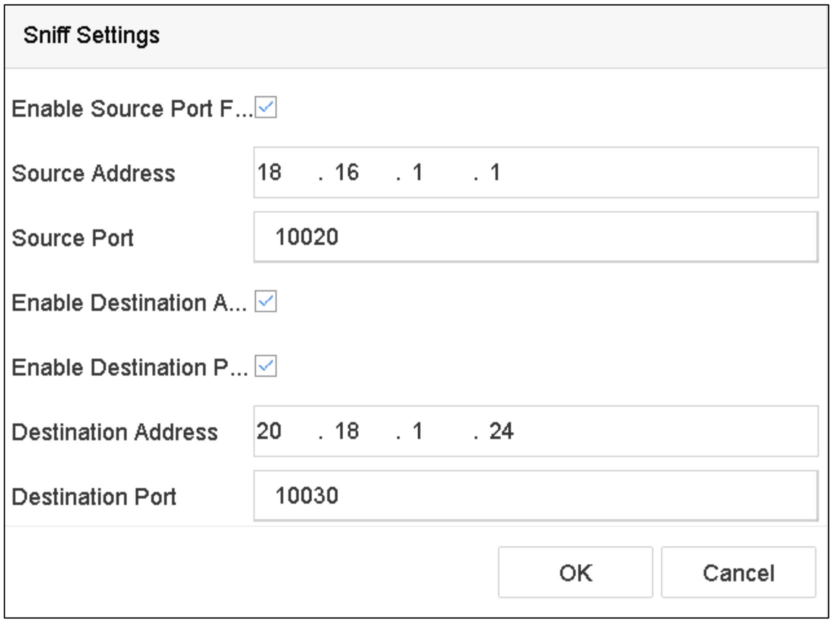


USB-to-RS-232 Settings

Serial Port Number	1
Baud Rate	4800
Data Bit	5
Stop Bit	1
Parity	None
Flow Ctrl	None

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.



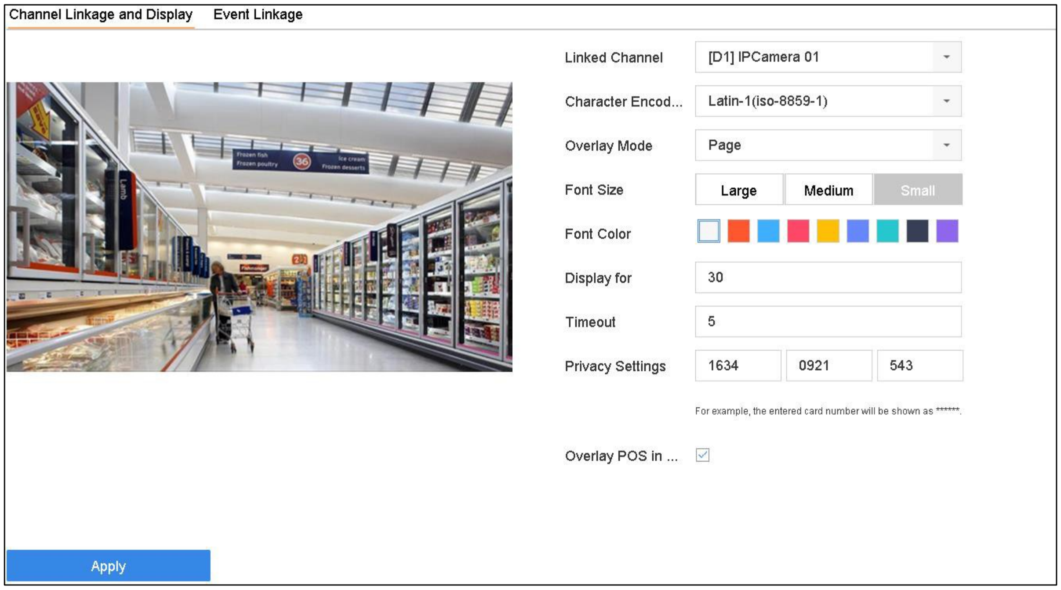
Sniff Settings

Enable Source Port F...	☑
Source Address	18 . 16 . 1 . 1
Source Port	10020
Enable Destination A...	☑
Enable Destination P...	☑
Destination Address	20 . 18 . 1 . 24
Destination Port	10030

Figure 15-6 Sniff Settings

15.1.2 Configure POS Text Overlay

1. Go to **System > POS Settings**.
2. Click the **Channel Linkage and Display** tab.
3. Select the linked channel to overlay the POS characters.
4. Set the characters overlay for the enabled POS.
   - Character encoding format: currently the Latin-1 format is available
   - Overlay mode of the characters to display in scrolling or page mode
   - Font size and font color
   - Display time (sec) of the characters (the value ranges from 5-3600 sec.)
   - Timeout of POS event. The value ranges 5-3600 sec. When the device has not received the POS message by the defined time, the transaction is finished.
5. In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number or user name, etc. The defined privacy information will be displayed as *** 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 overlaid on the live view image.



Linked Channel: [D1] IPCamera 01

Character Encod...: Latin-1(iso-8859-1)

Overlay Mode: Page

Font Size: Large | Medium | Small

Font Color

Display for: 30

Timeout: 5

Privacy Settings: 1634 | 0921 | 543

For example, the entered card number will be shown as ******.

Overlay POS in ... ☑

Figure 15-7 Overlay Character Settings

NOTE

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

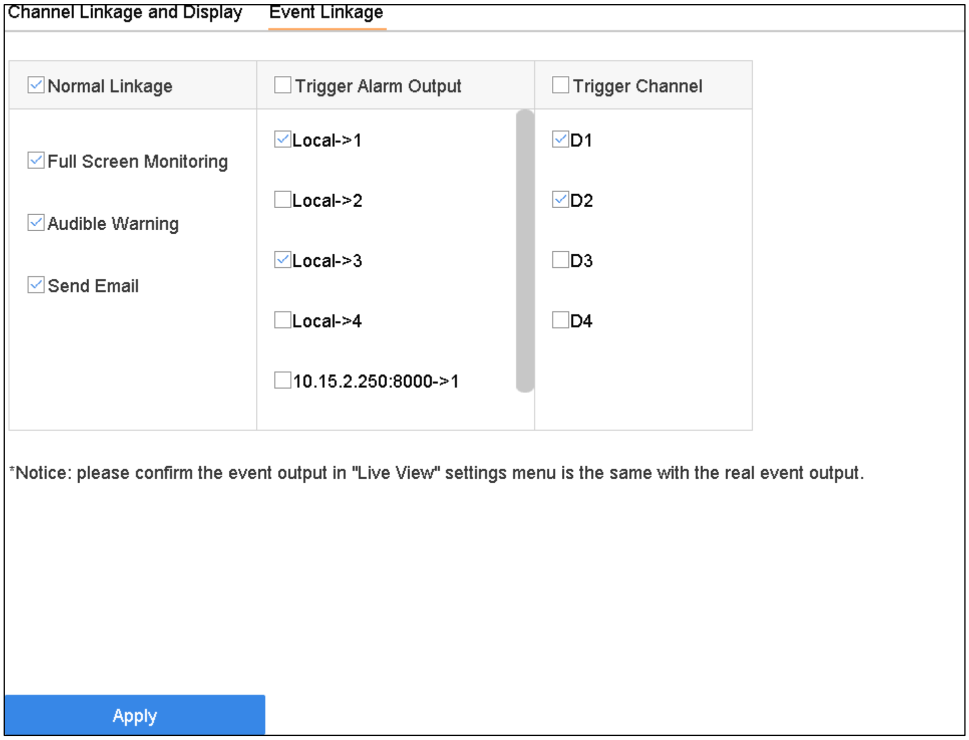
7. Click **Apply** to activate the settings.

15.2 Configure POS Alarm

Purpose

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

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 a POS alarm is triggered.



☑ Normal Linkage	□ Trigger Alarm Output	□ Trigger Channel
☑ Full Screen Monitoring	☑ Local->1	☑ D1
☑ Audible Warning	□ Local->2	☑ D2
☑ Send Email	☑ Local->3	□ D3
	□ Local->4	□ D4
	□ 10.15.2.250:8000->1	

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

Figure 15-8 Set POS Trigger Cameras

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

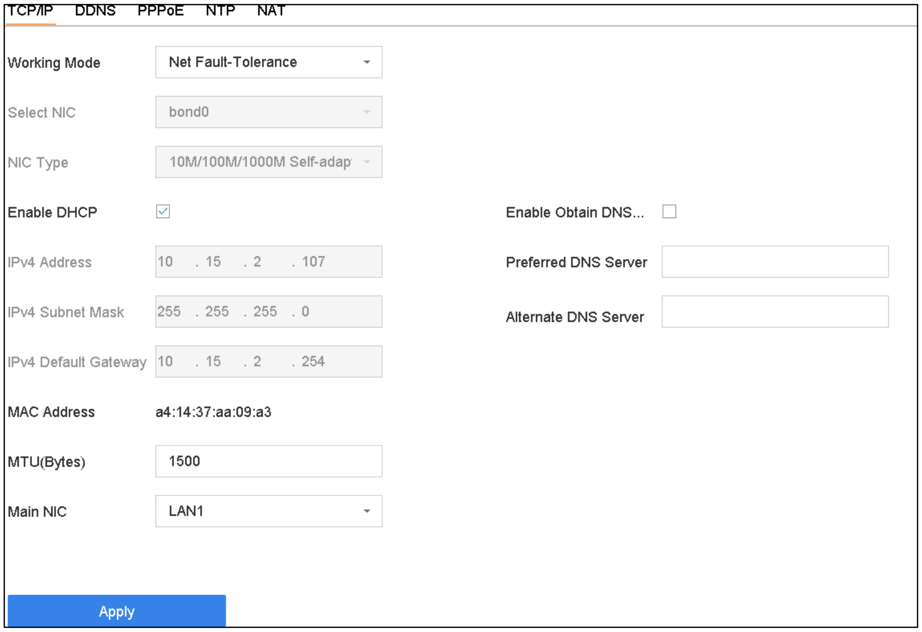
Chapter 16 Network Settings

16.1 Configure TCP/IP Settings

Purpose

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

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



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:

IPv4 Subnet Mask: 255 . 255 . 255 . 0

Alternate DNS Server:

IPv4 Default Gateway: 10 . 15 . 2 . 254

MAC Address: a4:14:37:aa:09:a3

MTU(Bytes): 1500

Main NIC: LAN1

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. In this way, if 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 use the same IP address and share the total bandwidth load, which enables the system to provide two Gigabit network capacity.

- **Multi-Address Mode**: The two NIC card parameters can be configured independently. Select LAN1 or LAN2 under Select NIC for parameter settings. You can select one NIC card as the default route, and then for the system connecting with the extranet, the data will be forwarded through the default route.

3. Configure other IP settings as needed.

NOTE

Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available in the network.

Valid range of MTU value is 500 to 9676.

4. Click **Apply**.

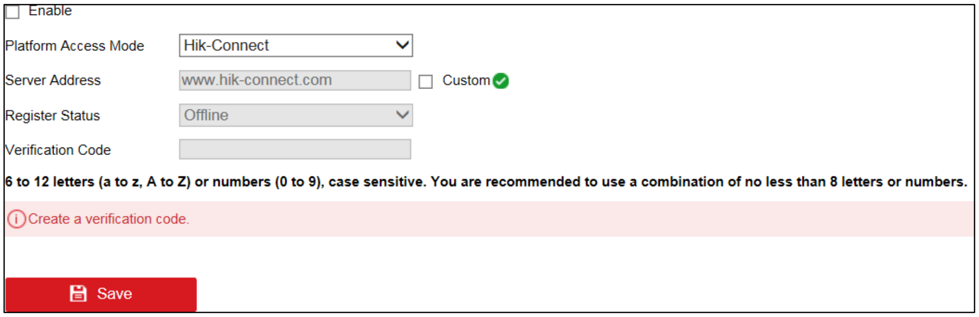
16.2 Configuring Hik-Connect

Hik-Connect provides a mobile phone application and service platform page (www.hik-connect.com) to access and manage your connected encoder, which provides convenient remote access to the surveillance system.

NOTE

Hik-Connect can be enabled via SADP software, GUI, or Web browser. We explain the GUI operation steps in this section.

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



□ Enable

Platform Access Mode: Hik-Connect

Server Address: www.hik-connect.com □ Custom ✓

Register Status: Offline

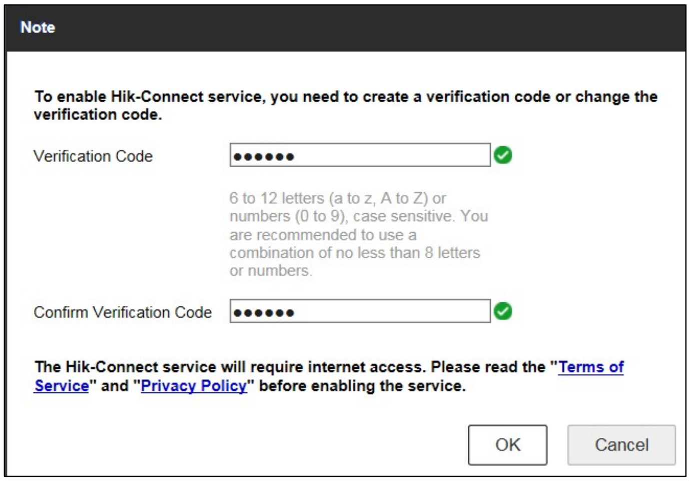
Verification Code:

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

ⓘ Create a verification code.

Figure 16-2 Hik-Connect Settings

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



Note

To enable Hik-Connect service, you need to create a verification code or change the verification code.

Verification Code: •••••• ✓

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

Confirm Verification Code: •••••• ✓

The Hik-Connect service will require internet access. Please read the "Terms of Service" and "Privacy Policy" before enabling the service.

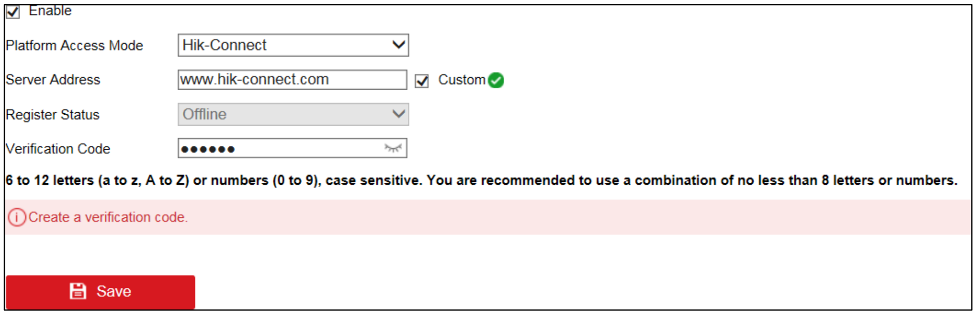
Figure 16-3 Service Terms

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.



☑ Enable

Platform Access Mode: Hik-Connect

Server Address: www.hik-connect.com ☑ Custom ✓

Register Status: Offline

Verification Code: ●●●●●●

6 to 12 letters (a to z, A to Z) or numbers (0 to 9), case sensitive. You are recommended to use a combination of no less than 8 letters or numbers.

ⓘ Create a verification code.

Figure 16-4 Hik-Connect Settings

NOTE

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 the 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 with your mobile phone or the Website (www.hik-connect.com).

   - **iOS Users:** Scan the QR code below to download the Hik-Connect application for subsequent operations.

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

Figure 16-5 QR Code for iOS Users

Figure 16-6 QR Code for Android Users

NOTE

Refer to the help file on the official Website (www.hik-connect.com) and the *Hik-Connect Mobile Client User Manual* for adding the device to Hik-Connect and more operating instructions.

16.3 Configure DDNS

Purpose

You can set Dynamic DNS service for network access. Modes available: **DynDNS**, **PeanutHull,** and **NO-IP**.

Before You Start

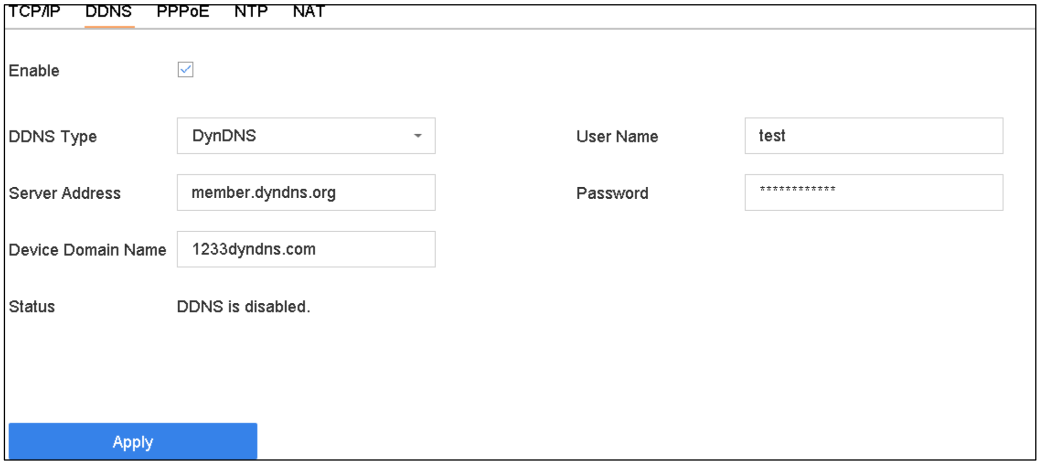
You must register DynDNS, PeanutHull, and NO-IP services with your ISP before configuring DDNS settings.

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. Enter required information 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.



Enable ☑

DDNS Type: DynDNS

Server Address: member.dyndns.org

Device Domain Name: 1233dyndns.com

Status: DDNS is disabled.

User Name: test

Password: ************

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 a user name and password accordingly under **System** > **Network** > **TCP/IP** > **PPPoE**.

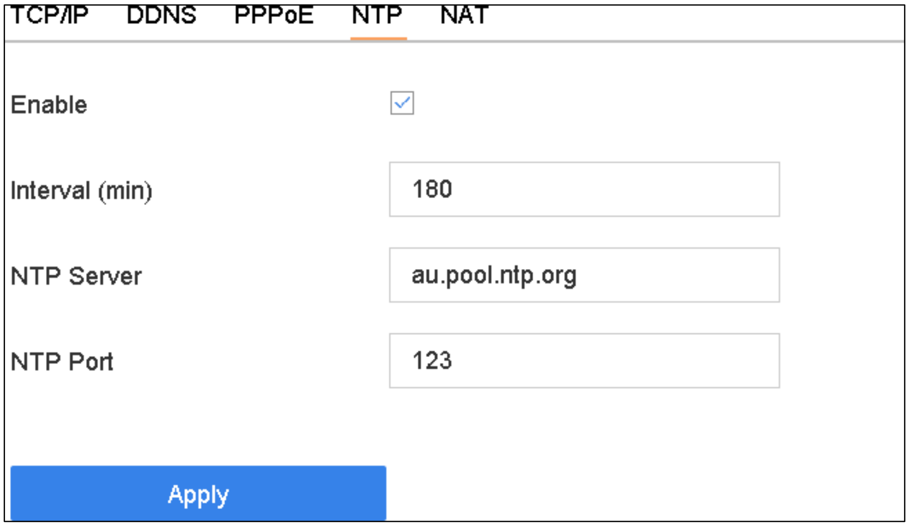
NOTE

Contact your Internet service provider (ISP) for details about 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 system date and time.

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



Enable ☑

Interval (min): 180

NTP Server: au.pool.ntp.org

NTP Port: 123

Figure 16-8 NTP Settings

2. Check **Enable**.

3. Configure NTP settings as need.

   - **Interval (min)**: Time interval between two time synchronization with NTP server.
   - **NTP Server**: IP address of the NTP server.
   - **NTP Port**: Port of the NTP server.

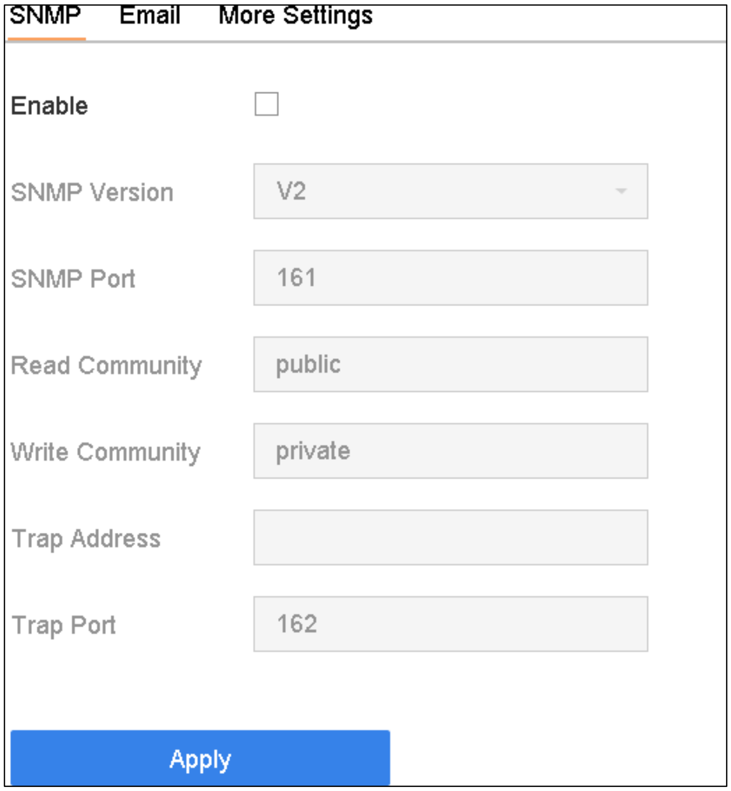
4. Click **Apply**.

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

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



Enable □

SNMP Version: V2

SNMP Port: 161

Read Community: public

Write Community: private

Trap Address:

Trap Port: 162

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

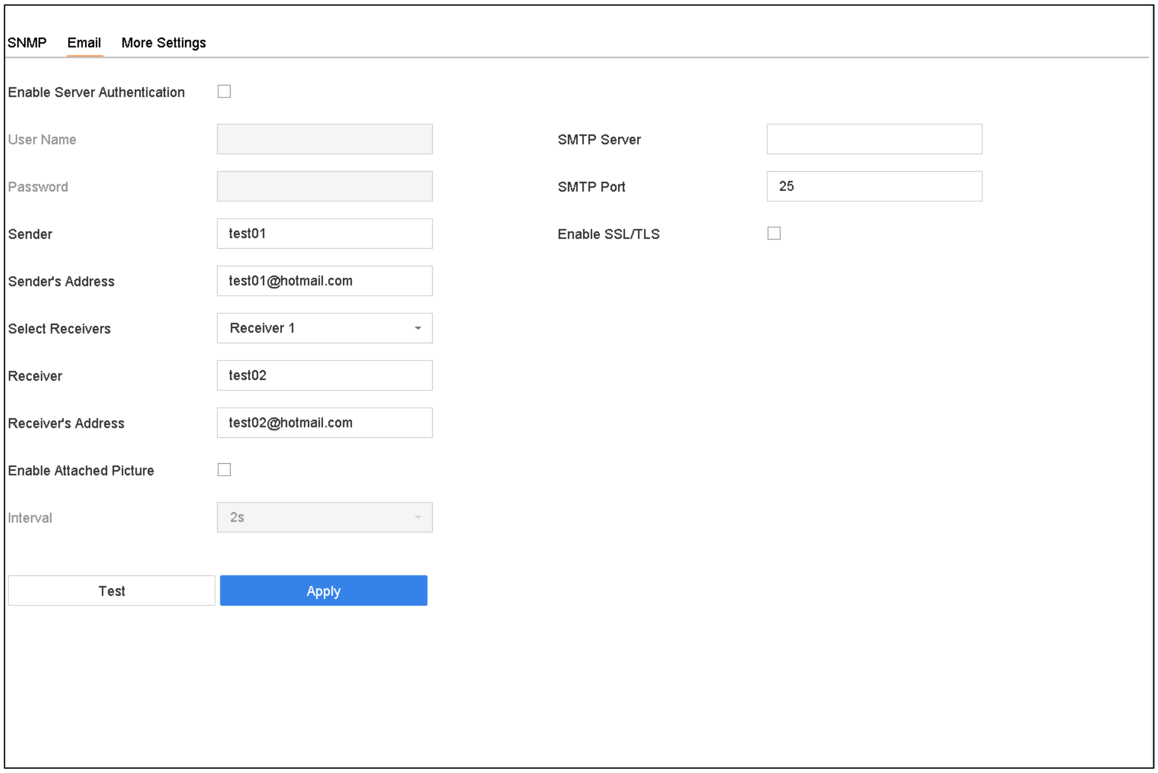
Purpose

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

Before You Start

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

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



Enable Server Authentication □

User Name

Password

Sender: test01

Sender's Address: test01@hotmail.com

Select Receivers: Receiver 1

Receiver: test02

Receiver's Address: test02@hotmail.com

Enable Attached Picture □

Interval: 2s

SMTP Server

SMTP Port: 25

Enable SSL/TLS □

Figure 16-10 Email 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 is25.
   - **Enable SSL/TLS**: Check to enable SSL/TLS if required by the SMTPserver.
   - **Sender**: The name of the sender.
   - **Sender's Address**: Sender's address.
   - **Select Receivers**: Select the receiver. Up to three 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**.

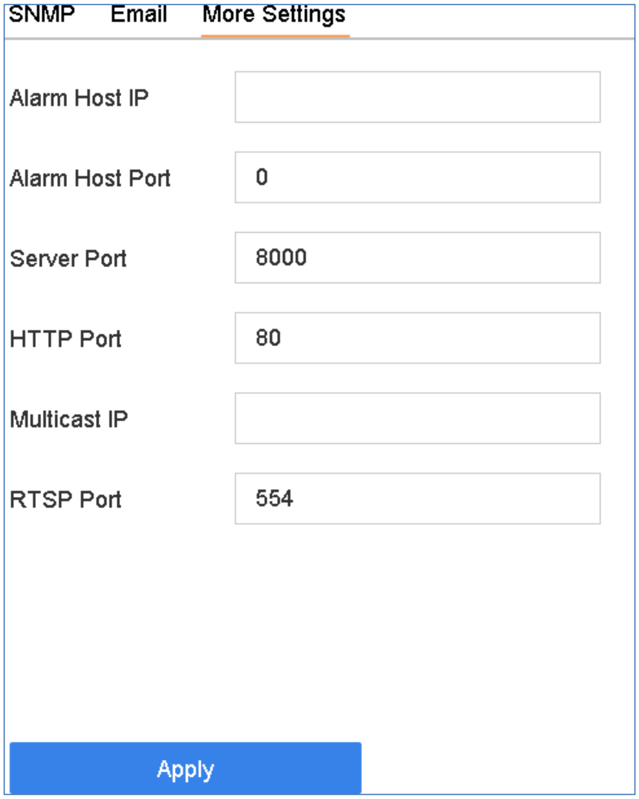
4. (Optional) Click **Test** to send a test e-mail.

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 a 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.



Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554

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 system reliability. Contact your dealer for 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.

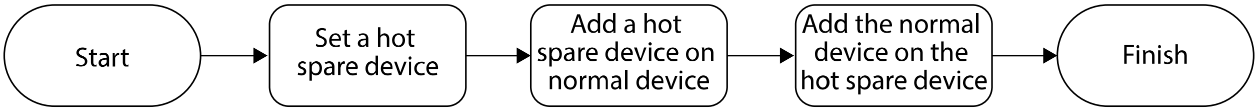

Start
Set a hot spare device
Add a hot spare device on normal device
Add the normal device on the hot spare device
Finish

Figure 17-1 Building Hot Spare System

Before You Start

Ensure that at least two devices are online.

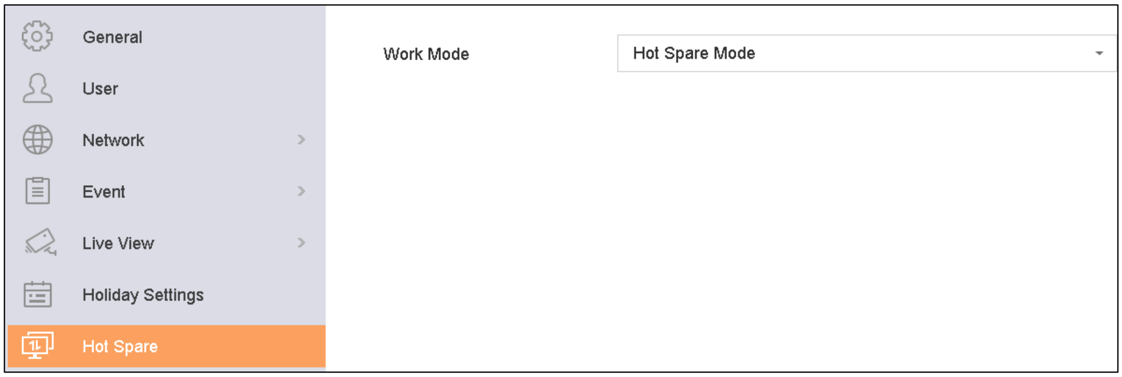
17.1 Set Hot Spare Device

Purpose

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

1. Go to **System > Hot Spare**.

- Set the Work Mode to Hot Spare Mode.



Work Mode: Hot Spare Mode

Figure 17-2 Hot Spare

- Click **Apply**.

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

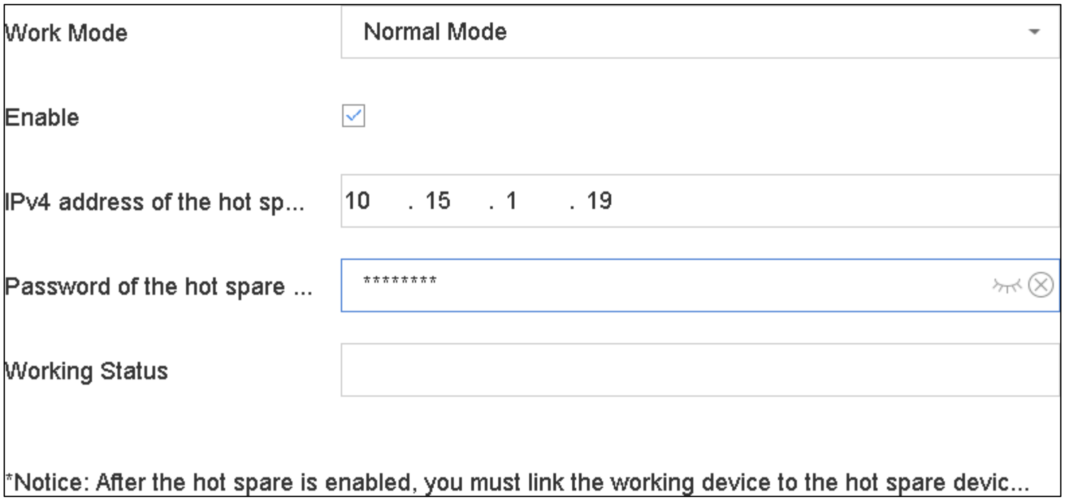
NOTE

The camera connection will be disabled when the device is in hot spare mode.

It is highly recommended to restore the device defaults after switching the working mode of the hot spare device back to normal mode to ensure the 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 hot spare device IP address and admin password.



Work Mode: Normal Mode

Enable: ☑

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

Password of the hot spare ...: ********

Working Status:

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

Figure 17-3 Hot Spare

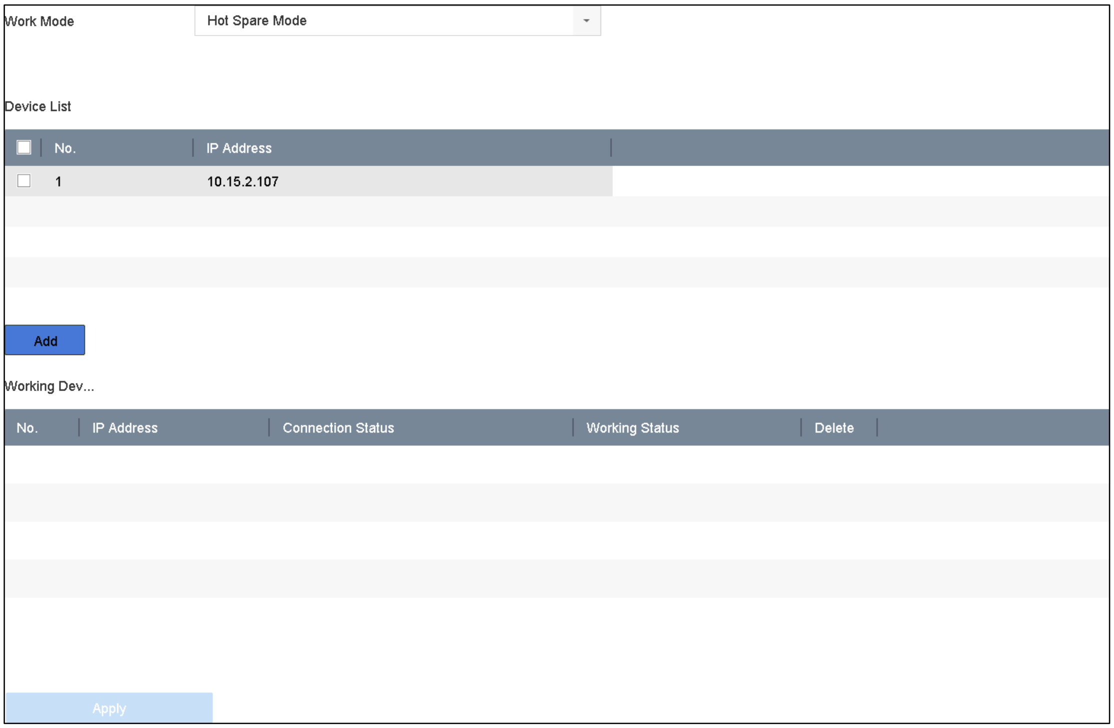
5. Click **Apply**.

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.

NOTE

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

Working Dev...

No.	IP Address	Connection Status	Working Status	Delete

Figure 17-4 Add Working Device

Table 17-1 Working Status Description

Working Status	Description
No Record	The working device is working properly.
Backing Up	The working device is offline, and the hot spare device will record the video of the IP camera connected to the working device for backup. The record backing up can function for one working device at a time.
Synchronizing	The working device has come online, and the lost video files are being restored by 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

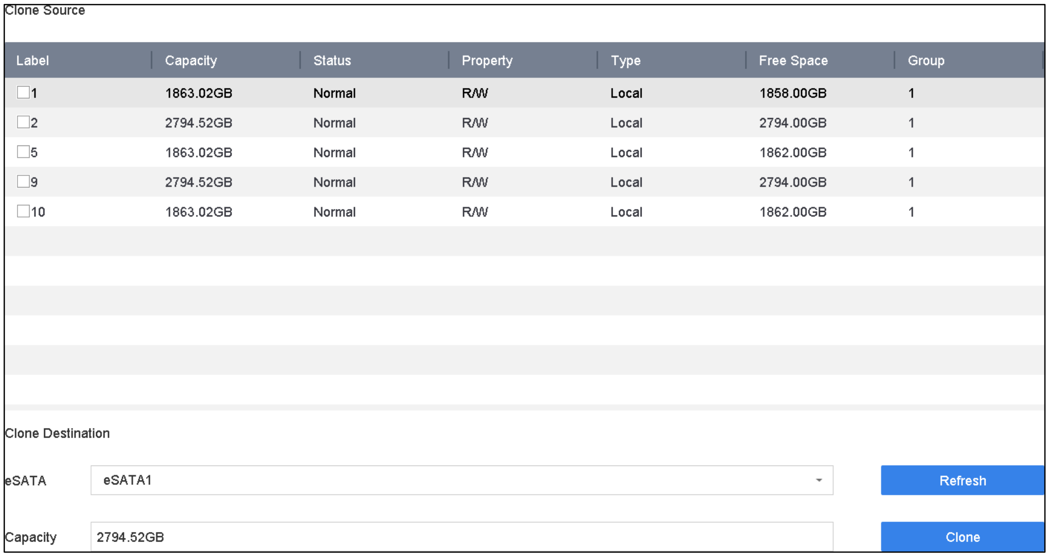
Purpose

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**.



Clone Source

Label	Capacity	Status	Property	Type	Free Space	Group
□1	1863.02GB	Normal	R/W	Local	1858.00GB	1
□2	2794.52GB	Normal	R/W	Local	2794.00GB	1
□5	1863.02GB	Normal	R/W	Local	1862.00GB	1
□9	2794.52GB	Normal	R/W	Local	2794.00GB	1
□10	1863.02GB	Normal	R/W	Local	1862.00GB	1

Clone Destination

eSATA: eSATA1

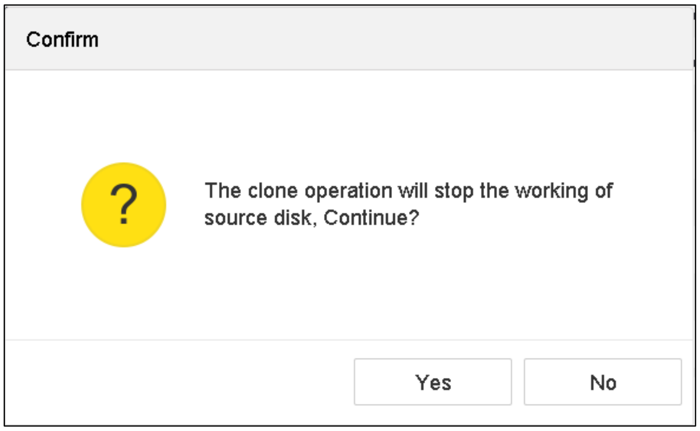
Capacity: 2794.52GB

Figure 18-1 HDD Clone

2. Check the HDD to clone. The selected HDD's capacity must match the clone destination capacity.

3. Click **Clone**.

4. Click **Yes** on the pop-up message box to continue cloning.



Confirm

The clone operation will stop the working of source disk, Continue?

Figure 18-2 Message Box

18.1.2 S.M.A.R.T. Detection

Purpose

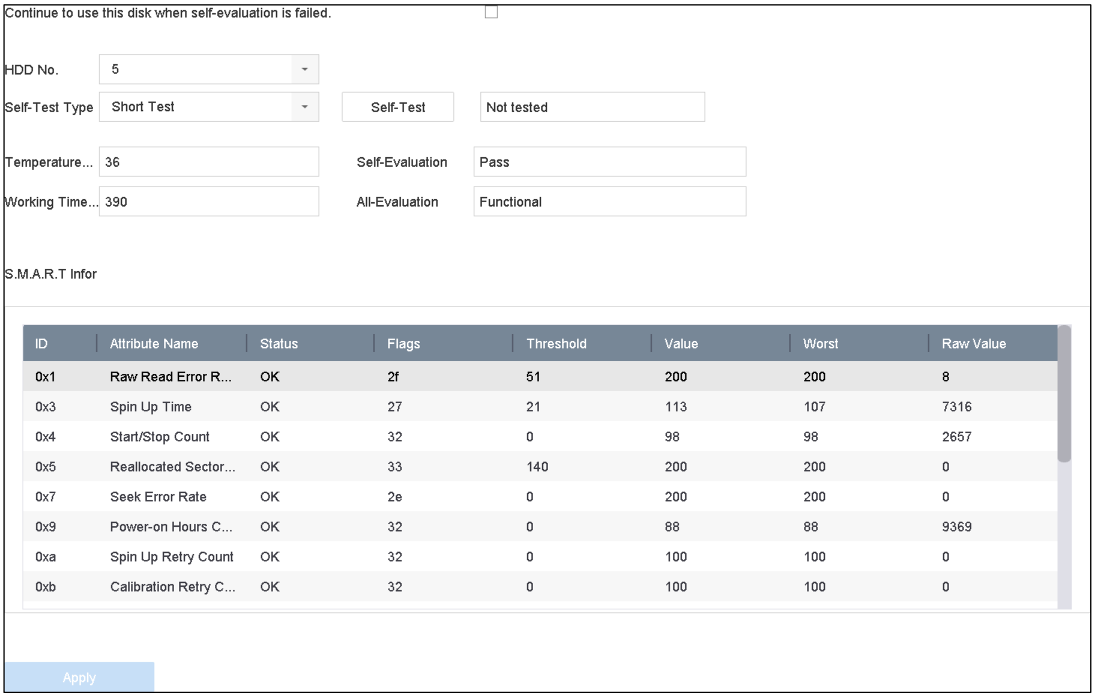
Bad Sector Detection detection and S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) monitor the HDD to detect and report on various reliability indicators in the hopes of anticipating failures.

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. Set the self-test types as **Short Test**, **Expanded Test,** or **Conveyance Test**.

4. Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation. The related S.M.A.R.T. information is shown on the interface. You can check the HDD status.



Continue to use this disk when self-evaluation is failed. □

HDD No. 5

Self-Test Type Short Test

Not tested

Temperature... 36

Self-Evaluation Pass

Working Time... 390

All-Evaluation Functional

S.M.A.R.T Infor

ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
0x1	Raw Read Error R...	OK	2f	51	200	200	8
0x3	Spin Up Time	OK	27	21	113	107	7316
0x4	Start/Stop Count	OK	32	0	98	98	2657
0x5	Reallocated Sector...	OK	33	140	200	200	0
0x7	Seek Error Rate	OK	2e	0	200	200	0
0x9	Power-on Hours C...	OK	32	0	88	88	9369
0xa	Spin Up Retry Count	OK	32	0	100	100	0
0xb	Calibration Retry C...	OK	32	0	100	100	0

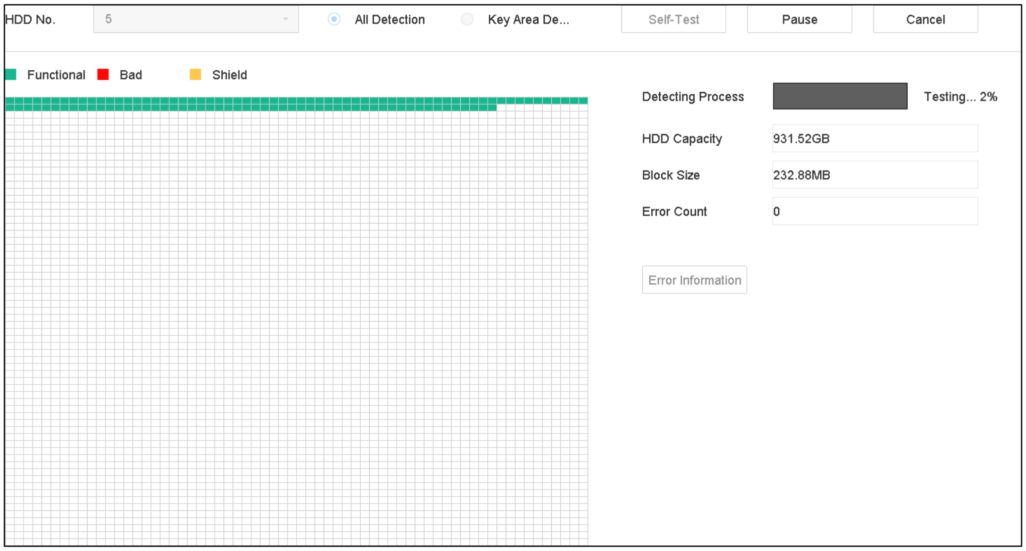
Figure 18-3 S.M.A.R.T Settings Interface

NOTE

To use the HDD even if S.M.A.R.T. checking has failed, check the **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. in the drop-down list you want to configure.
3. Select **All Detection** or **Key Area Detection** as the detection type.
4. Click the **Self-Test** button to start the detection.



HDD No.: 5

● All Detection ○ Key Area De...

🟩 Functional 🟥 Bad 🟨 Shield

Detecting Process: Testing... 2%

HDD Capacity: 931.52GB

Block Size: 232.88MB

Error Count: 0

Figure 18-4 Bad Sector Detection

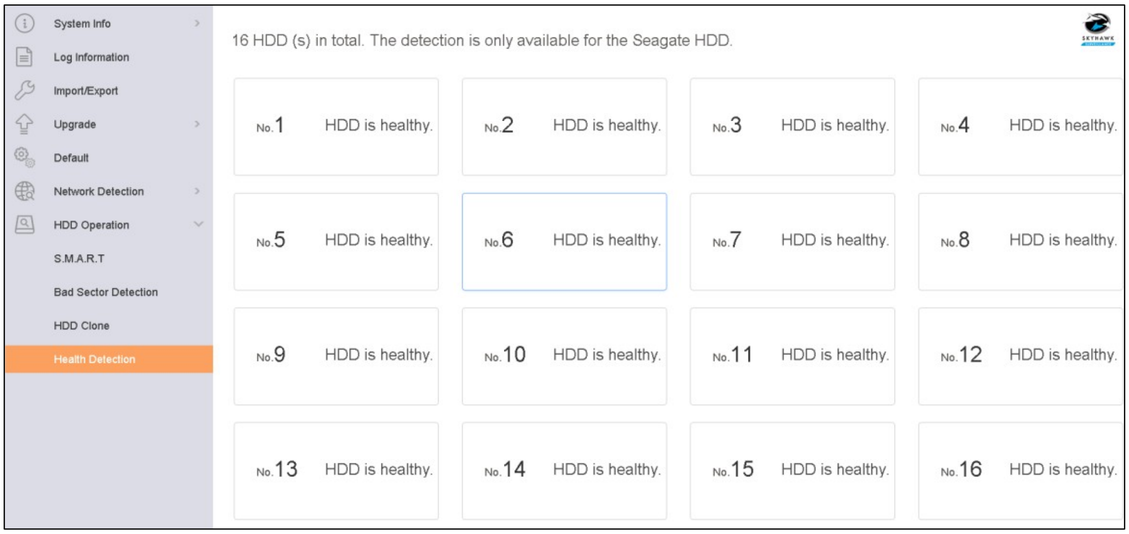
- You can also pause/resume or cancel the detection.
- After testing has completed, you can click **Error information** button to see the detailed damage information.

18.1.4 HDD Health Detection

Purpose

You can view the health status of a Seagate HDD that was built after October 1, 2017, with a capacity from 4 TB to 8 TB. The function helps you to troubleshoot HDD problems. Compared to the S.M.A.R.T function, HDD Health Detection shows the HDD status with more details.

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



16 HDD (s) in total. The detection is only available for the Seagate HDD.

No.1 HDD is healthy.	No.2 HDD is healthy.	No.3 HDD is healthy.	No.4 HDD is healthy.
No.5 HDD is healthy.	No.6 HDD is healthy.	No.7 HDD is healthy.	No.8 HDD is healthy.
No.9 HDD is healthy.	No.10 HDD is healthy.	No.11 HDD is healthy.	No.12 HDD is healthy.
No.13 HDD is healthy.	No.14 HDD is healthy.	No.15 HDD is healthy.	No.16 HDD is healthy.

Figure 18-5 Health Detection

2. Click an HDD to view details.

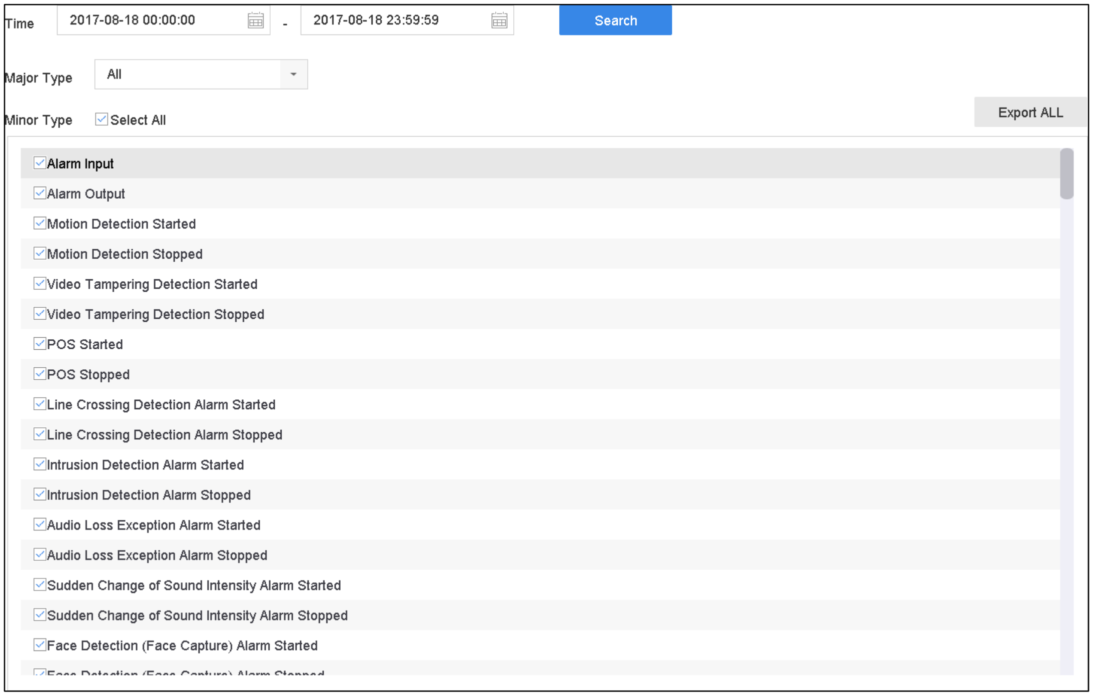
18.2 Search and Export Log Files

Purpose

The device operation, alarm, exception, and information 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**.



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

Major Type All

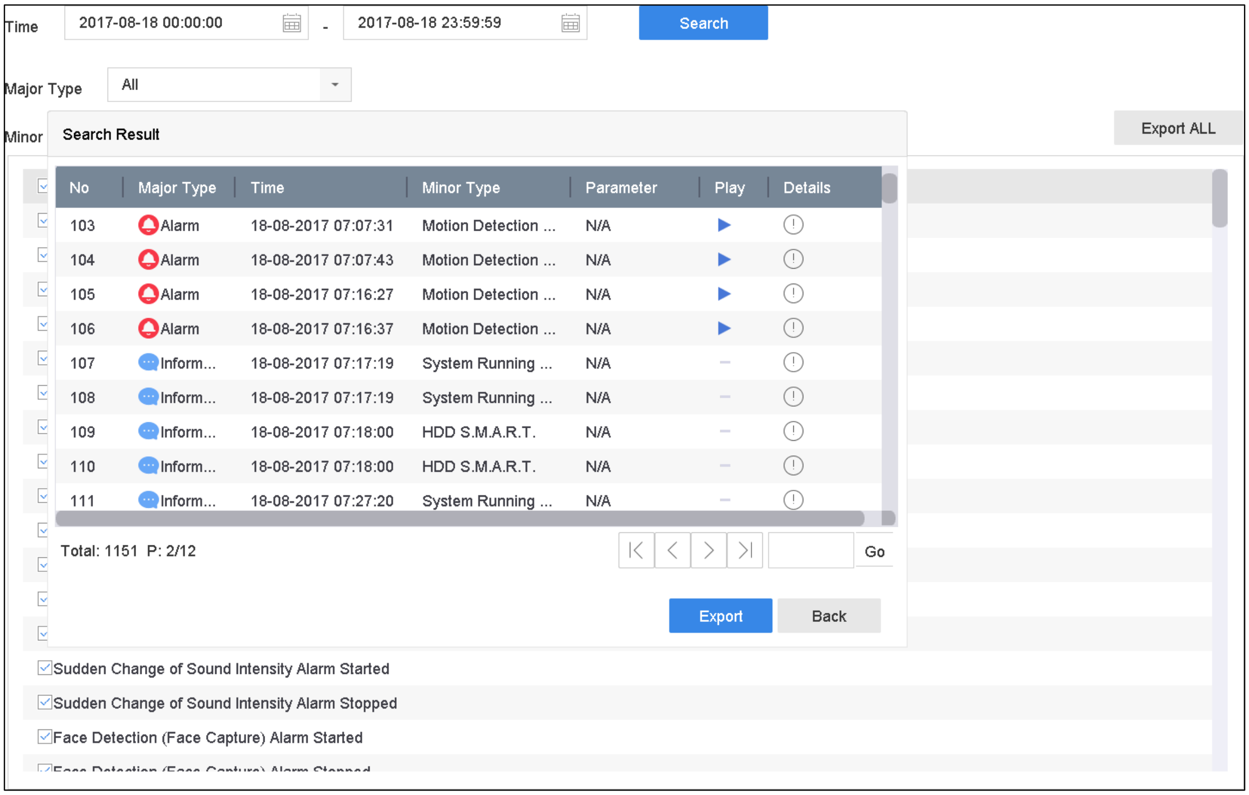
Minor Type ☑Select All

☑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

☑ 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 Operations:

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

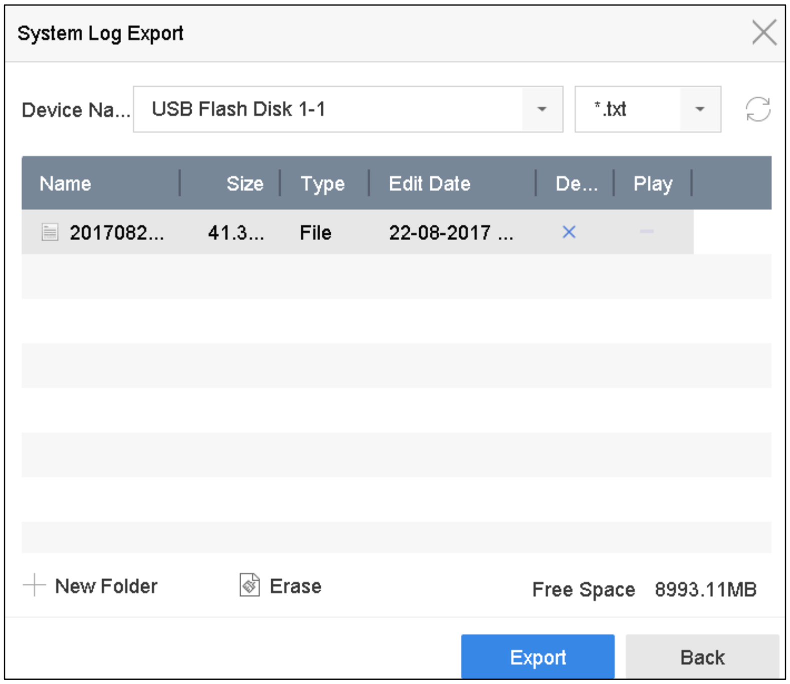
18.2.2 Export the Log Files

Before You Start

Connect a storage device to the NVR.

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.



Device Na... USB Flash Disk 1-1 | *.txt

Name	Size	Type	Edit Date	De...	Play
2017082...	41.3...	File	22-08-2017 ...	×	—

Free Space 8993.11MB

Figure 18-8 Export Log Files

3. On the Export interface, select the storage device from the **Device Name** drop-down list.

4. Select the format of the log files to be exported. Up to 15 formats are selectable.

5. Click **Export** to export the log files to the selected storage device.

Related Operation:

- Click the **New Folder** button to create 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

The added IP camera information can be generated into an Excel file and exported to the local device for backup, including the IP address, manage port, password of admin, etc. The exported file can be edited on a PC (e.g., add or delete content, or copy the settings to other devices by importing the Excel file to it).

Before You Start

Connect a storage device to your NVR. 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 the 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.

NOTE

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

18.4 Import/Export Device Configuration Files

Purpose

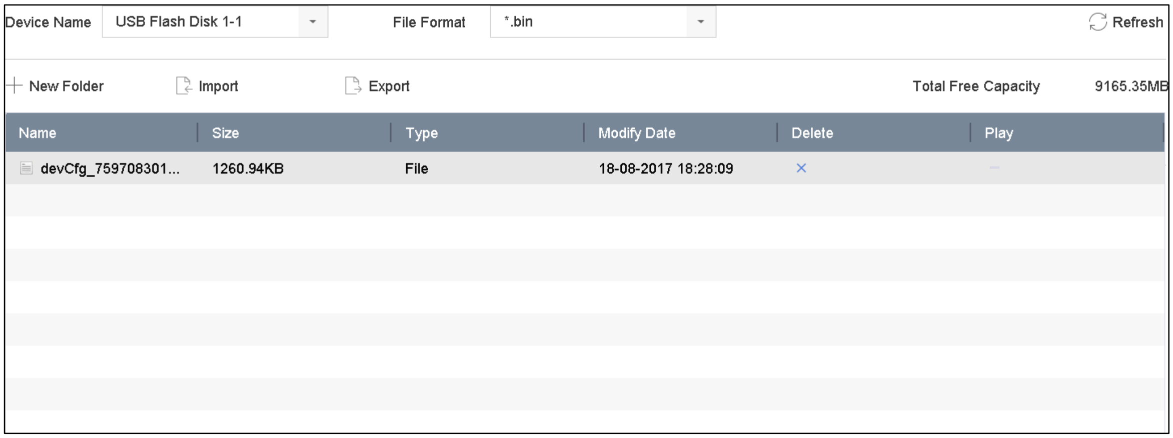
The device configuration files can be exported to a local device for backup, and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Connect a storage device to your device. For importing the configuration file, the storage device must contain the file.

Before You Start

Connect a storage device to your device. For importing the configuration file, the storage device must contain the file.

1. Go to **Maintenance > Import/Export**.



Device Name: USB Flash Disk 1-1

File Format: *.bin

Total Free Capacity: 9165.35MB

Name	Size	Type	Modify Date	Delete	Play
devCfg_759708301...	1260.94KB	File	18-08-2017 18:28:09	×	—

Figure 18-9 Import/Export Config File

2. Export or import the device configuration files.
   - Click **Export** to export configuration files to the selected local backup device.
   - To import a configuration file, select the file from the selected backup device and click the **Import** button.

NOTE

After finishing importing configuration files, the device will reboot automatically.

18.5 Upgrade System

Purpose

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

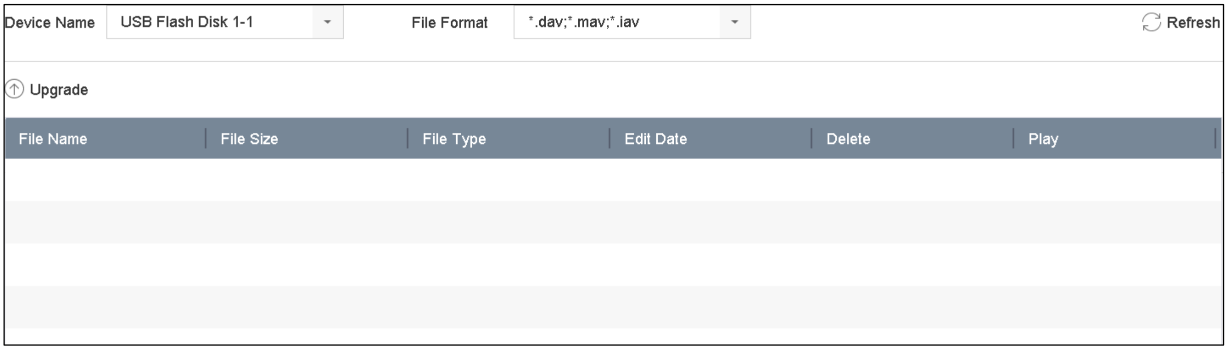
18.5.1 Upgrade by Local Backup Device

Before You Start

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

1. Go to **Maintenance > Upgrade**.

2. Click the **Local Upgrade** tab to enter the local upgrade interface.



Device Name: USB Flash Disk 1-1

File Format: *.dav;*.mav;*.iav

File Name	File Size	File Type	Edit Date	Delete	Play

Figure 18-10 Local Upgrade Interface

3. Select the update file from the storage device.

4. Click **Upgrade** to start upgrading.

5. After upgrading is complete, the device will reboot automatically to activate the new firmware.

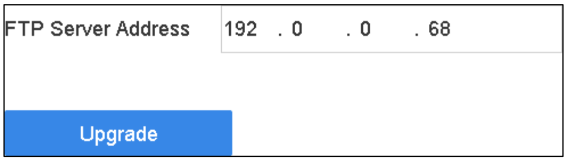
18.5.2 Upgrade by FTP

Before You Start

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

1. Go to **Maintenance > Upgrade**.

2. Click the **FTP** tab to enter the local upgrade interface.



FTP Server Address: 192 . 0 . 0 . 68

Figure 18-11 FTP Upgrade Interface

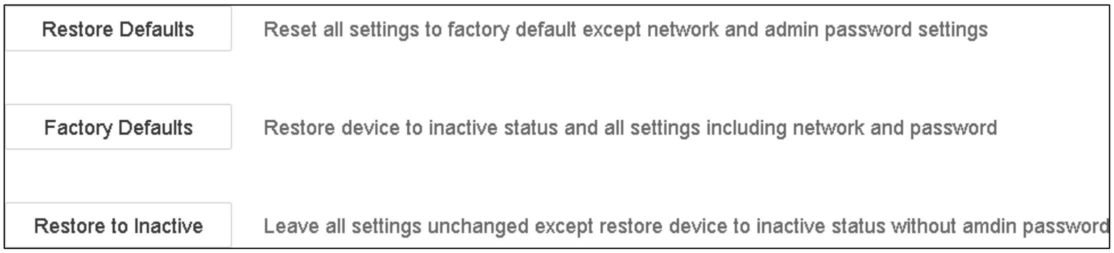
3. Enter the FTP Server Address in the text field.

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**.



Restore Defaults	Reset all settings to factory default except network and admin password settings
Factory Defaults	Restore device to inactive status and all settings including network and password
Restore to Inactive	Leave all settings unchanged except restore device to inactive status without amdin password

Figure 18-12 Restore Defaults

2. Select the restore type from the following three options.

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

   - **Factory Defaults**: Restore all parameters to the factory default settings.

   - **Restore to Inactive**: Restore the device to 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 HTTP, or set HTTP authentication when it is enabled on demand to enhance the access security.

NOTE

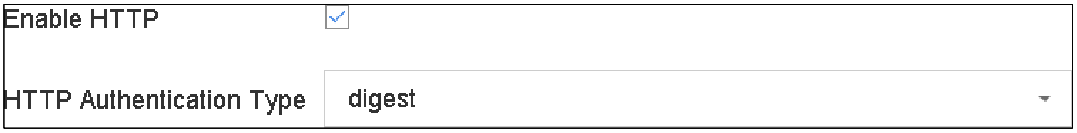
By default, HTTP service is enabled.

Set HTTP Authentication

Purpose

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

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



Enable HTTP ☑

HTTP Authentication Type: digest

Figure 18-13 HTTP Authentication

2. Check the **Enable HTTP** checkbox to enable the HTTP service.

3. Select **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**.

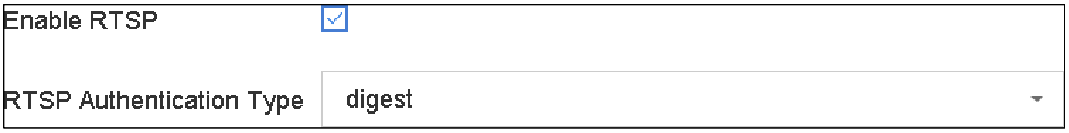
2. Uncheck the **Enable HTTP** to disable the HTTP service.

RTSP Authentication

Purpose

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

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



Enable RTSP ☑

RTSP Authentication Type: digest

Figure 18-14 RTSP Authentication

2. Select the authentication type.

NOTE

Two authentication types are selectable: **digest** and **digest/basic**. If you select **digest** as the RTSP authentication, only requests with digest authentication can access the video stream by 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

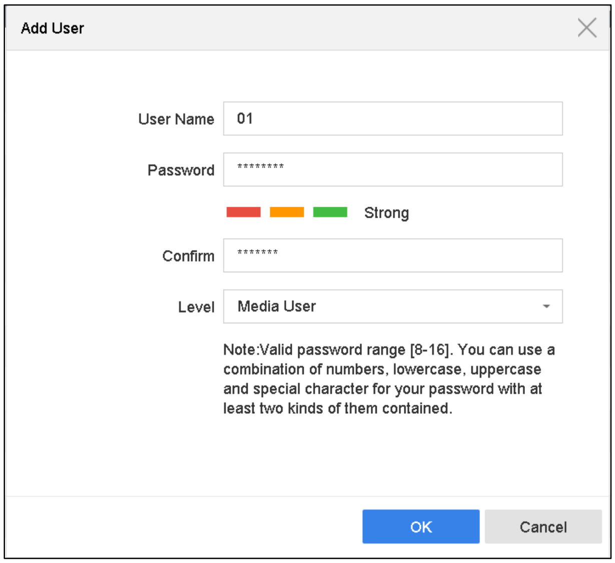
Purpose

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

1. Go to **System > System Service > ONVIF**.

2. Check the **Enable ONVIF** checkbox to enable ONVIF access management.

3. Click **Add** to enter the Add User interface.



Add User

User Name: 01

Password: ********

🟥 🟧 🟩 Strong

Confirm: *******

Level: Media User

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 18-15 Add User

4. Edit the user name and enter a strong password.

5. Set the user level to **Media User**, **Operator,** or **Admin**.

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

Result:
The added user accounts will have permission to connect other devices to the NVR via ONVIF protocol.

NOTE
ONVIF protocol is disabled by default.

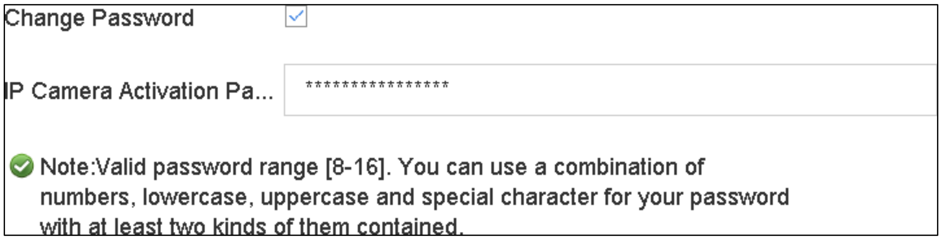
18.7.3 Manage IP Camera Activation

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

1. Go to **System** > **System Service** > **IP Camera Activation**.

2. Check the **Change Password** checkbox to enable the permission.

3. Enter the device admin password to obtain the permission.



Change Password ☑

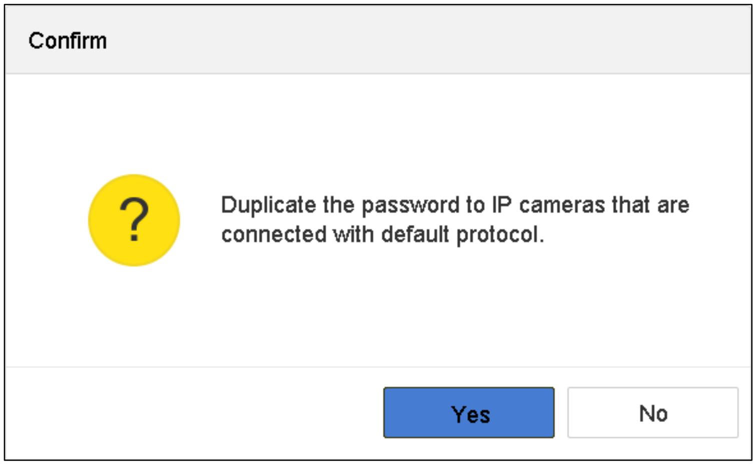
IP Camera Activation Pa... *****************

✓ 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. Enter a new strong password for the cameras in the **IP Camera Activation Password** text field.

5. Click **Apply** to show the following pop-up attention box.



Confirm

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

Figure 18-17 Attention

6. Click **Yes** to duplicate the current password to the IP cameras that are connected with the default protocol.

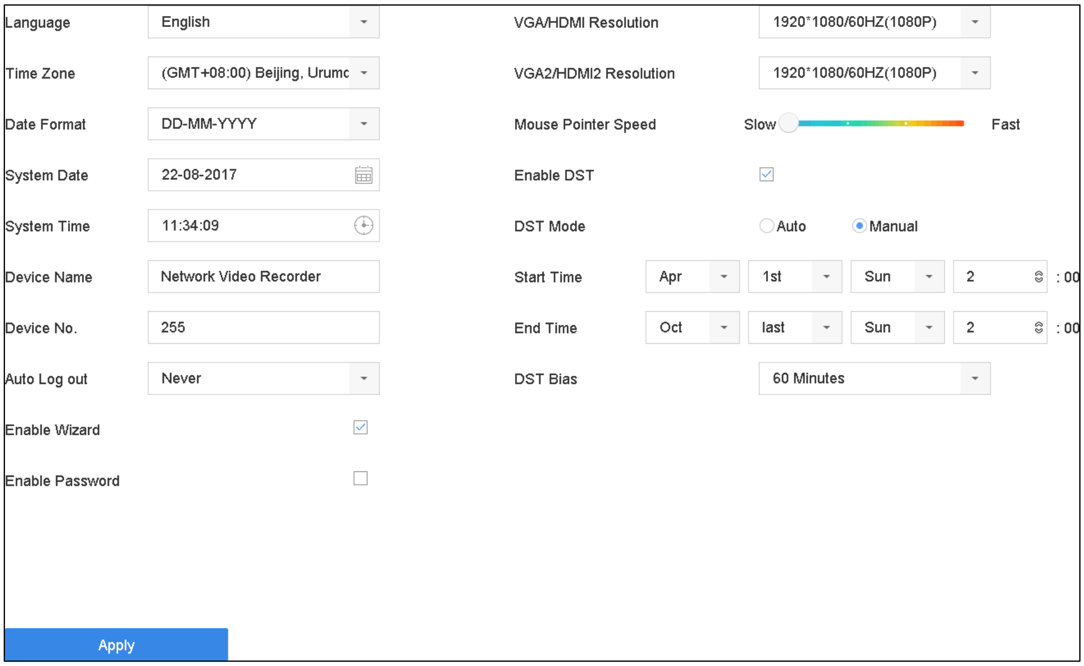
Chapter 19 General System Settings

19.1 Configure General Settings

Purpose

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

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



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

Figure 19-1 General Settings Interface

2. Configure the following settings.

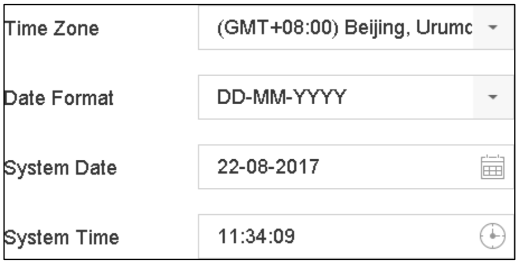
- **Language:** The default language used is *English*.
- **Output Standard:** Set the output standard to NTSC or PAL, which must match the video input standard.
- **Resolution:** Configure the video output resolution.
- **Device Name:** Edit the name of the device.
- **Device No.:** Edit the device serial number. The Device No. can be set in the range of 1~255, and the default no. 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*, the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.
- **Mouse Pointer Speed:** Set the speed of the mouse pointer. Four levels are configurable.

- **Enable Wizard:** Enable/disable the device startup Wizard.
- **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

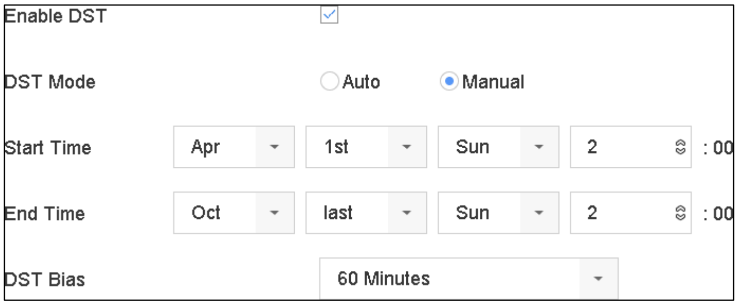
3. Click the **Apply** button to save the settings.

19.3 Configure DST Settings

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.

Advance clocks ahead a certain period of time (depends on the DST bias you set) at the beginning of DST, and move them back the same period when returning to standard time (ST).

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



Enable DST ☑

DST Mode ○ Auto ● Manual

Start Time Apr 1st Sun 2 : 00

End Time Oct last Sun 2 : 00

DST Bias 60 Minutes

Figure 19-3 DST Settings Interface

3. Set the DST mode to **Auto** or **Manual**.
   - **Auto:** Automatically enable the default DST period according to 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: 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.

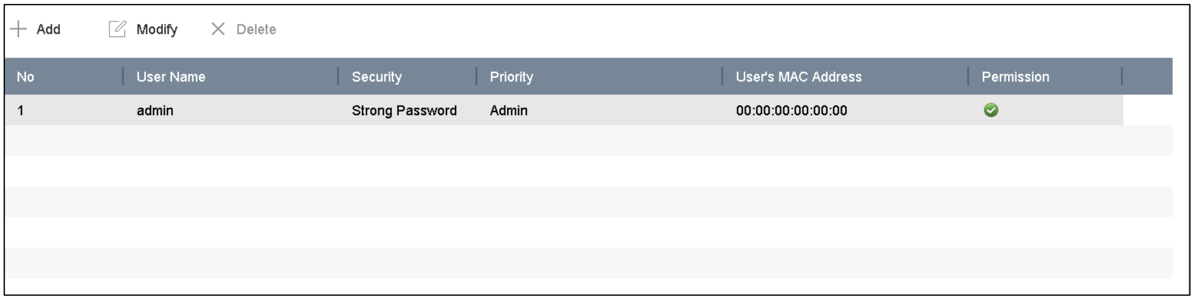
19.4 Manage User Accounts

Purpose

The *Administrator* user name is *admin* and the password is set when you start 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**.

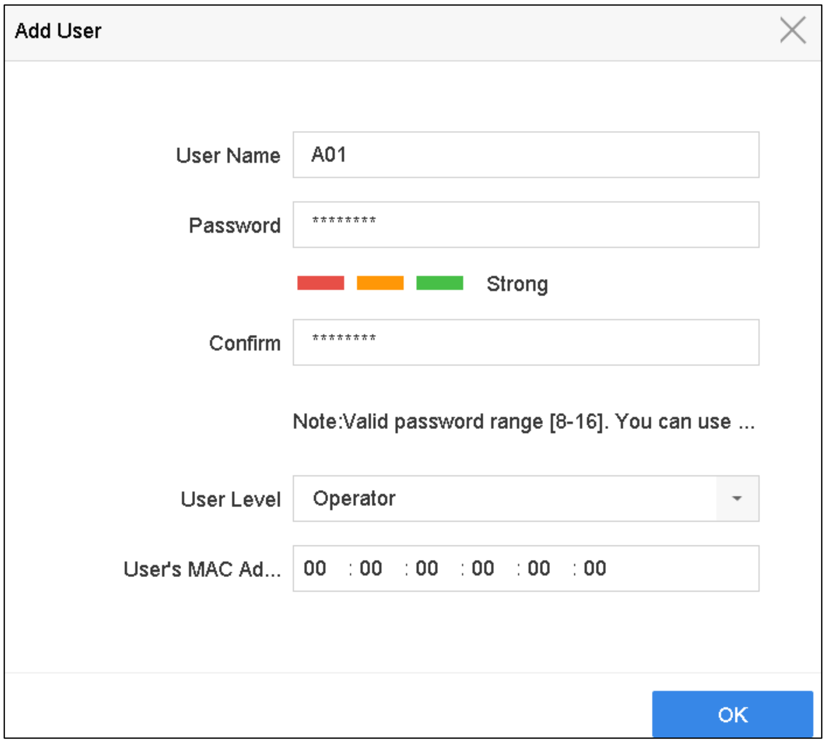


No	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Strong Password	Admin	00:00:00:00:00:00	✓

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

Figure 19-5 Add User

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

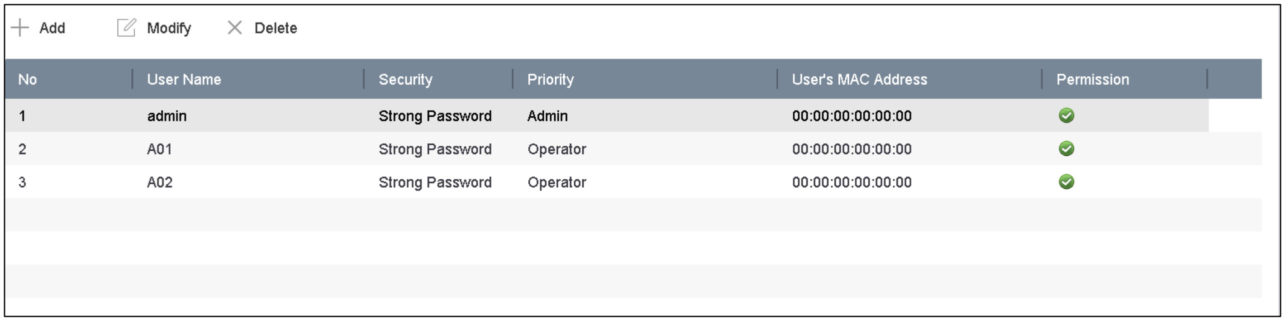
WARNING

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

- **User Level:** Set the user level to Operator or Guest. Different user levels have different operating permission.
  - **Operator:** The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permissions in Camera Configuration by default.
  - **Guest:** A Guest user has no permission of Two-way Audio in Remote Configuration and has only local/remote playback in the Camera Configuration by default.
- **User's MAC Address:** The MAC address of the remote PC that logs onto the device. If it is configured and enabled, it allows only a remote user with this MAC address to access the device.

5. Click **OK** to finish adding the new user account.

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



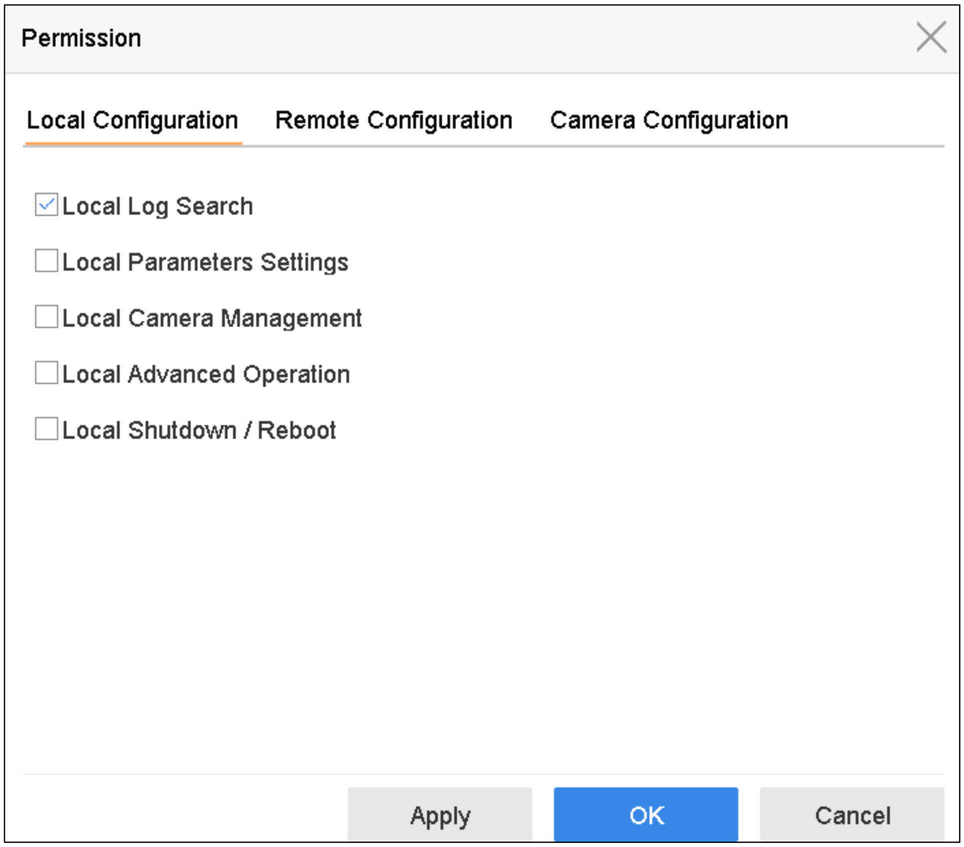
No	User Name	Security	Priority	User's MAC Address	Permission
1	admin	Strong Password	Admin	00:00:00:00:00:00	✓
2	A01	Strong Password	Operator	00:00:00:00:00:00	✓
3	A02	Strong Password	Operator	00:00:00:00:00:00	✓

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 local and remote operation of the device.

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



☑ Local Log Search

□ Local Parameters Settings

□ Local Camera Management

□ Local Advanced Operation

□ Local Shutdown / Reboot

Figure 19-7 User Permission Settings Interface

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

   - Local Configuration
     - **Local Log Search**: Search and view device logs 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
     - Operate HDD management (initialize HDD, set HDD property)
     - Upgrade system firmware
     - Clear I/O alarm output
   - Local Shutdown Reboot
     - Shut down the device
     - Reboot the device
   - Remote Configuration
     - **Remote Log Search**: Remotely view logs 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 the IP cameras.
     - **Remote Serial Port Control**: Configure settings for RS-232 and RS-485 ports.
     - **Remote Video Output Control**: Send remote button control signal.
     - **Two-Way Audio**: Realize two-way radio between the remote client and the 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 live video of the selected camera (s).
  - **Local Manual Operation**: Locally start/stop manual recording and alarm output of the selected camera(s).
  - **Remote Manual Operation**: Remotely start/stop manual recording and alarm output of the selected camera(s).
  - **Local Playback**: Locally play back recorded files of the selected camera(s).
  - **Remote Playback**: Remotely play back recorded files of the selected camera(s).
  - **Local PTZ Control**: Locally control PTZ movement of the selected camera(s).
  - **Remote PTZ Control**: Remotely control PTZ movement of the selected camera(s).
  - **Local Video Export**: Locally export recorded files of the selected camera(s).

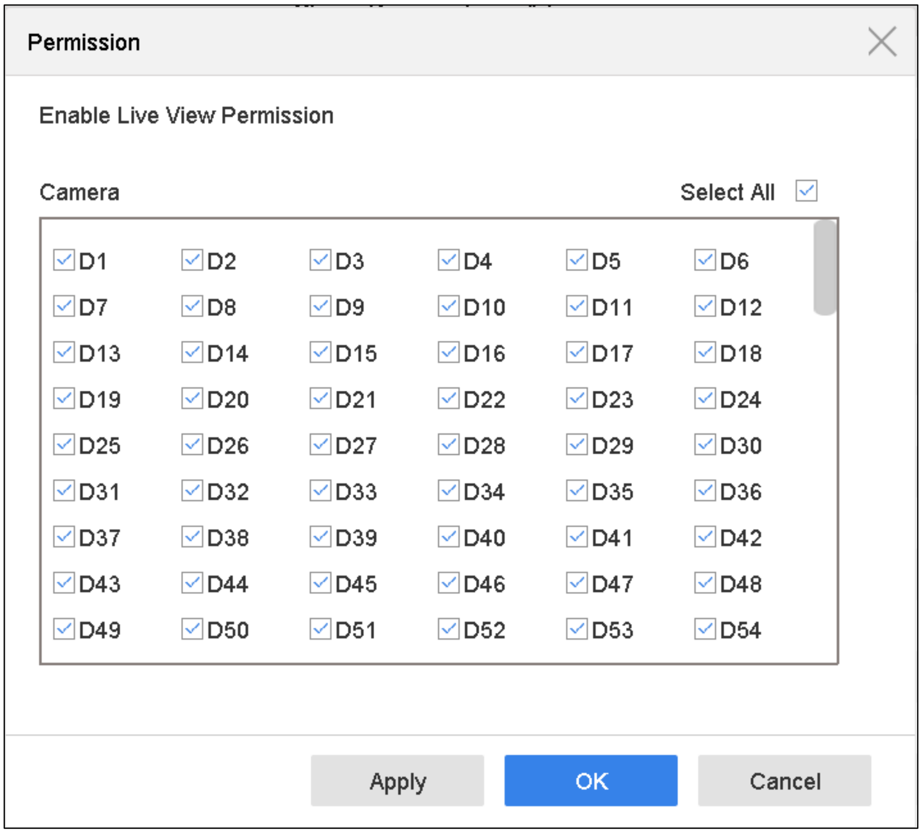
4. Click **OK** to save the settings.

NOTE

Only the admin user account has 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.**



Permission

Enable Live View Permission

Camera Select All ☑

☑D1	☑D2	☑D3	☑D4	☑D5	☑D6
☑D7	☑D8	☑D9	☑D10	☑D11	☑D12
☑D13	☑D14	☑D15	☑D16	☑D17	☑D18
☑D19	☑D20	☑D21	☑D22	☑D23	☑D24
☑D25	☑D26	☑D27	☑D28	☑D29	☑D30
☑D31	☑D32	☑D33	☑D34	☑D35	☑D36
☑D37	☑D38	☑D39	☑D40	☑D41	☑D42
☑D43	☑D44	☑D45	☑D46	☑D47	☑D48
☑D49	☑D50	☑D51	☑D52	☑D53	☑D54

Figure 19-8 Enable Live View Permission

5. Click ✓ of non-admin user.

6. Enter **Camera Configuration** tab.

7. Set Camera Permission to **Local Live View**.

8. Select cameras to live view.

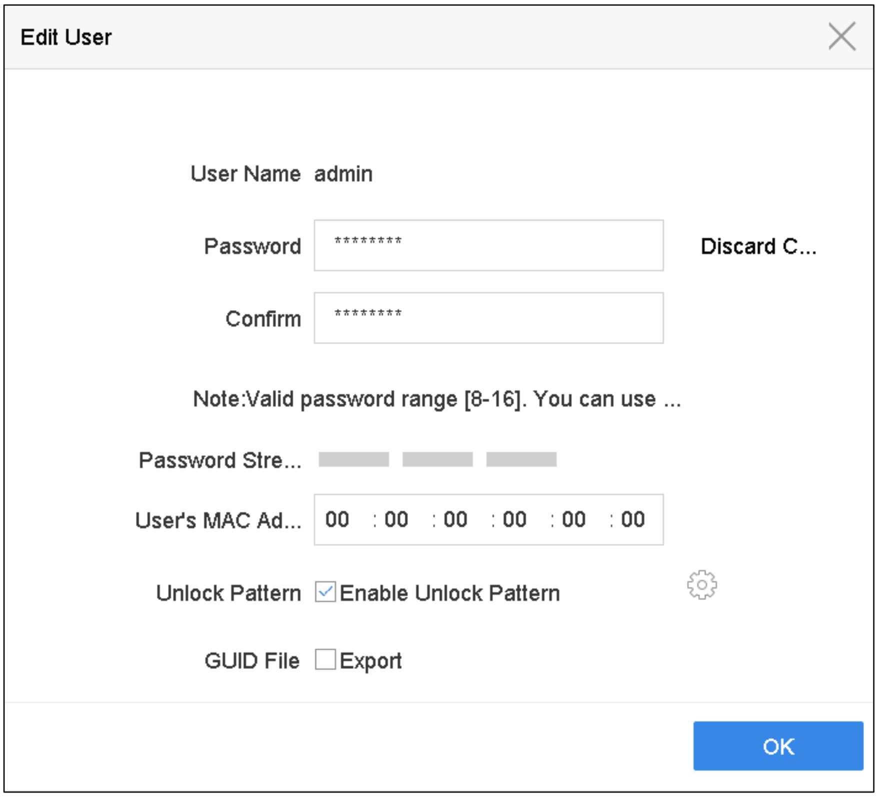
9. Click **OK**.

19.4.4 Edit the Admin User

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

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

2. Select the admin user from the list and click **Modify**.



Edit User

User Name admin

Password ******** Discard C...

Confirm ********

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

Password Stre...

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

Unlock Pattern ☑ Enable Unlock Pattern

GUID File □ Export

Figure 19-9 Edit User (Admin)

3. Edit the admin user information as desired, including adding a new admin password (strong password is required), and MAC address.

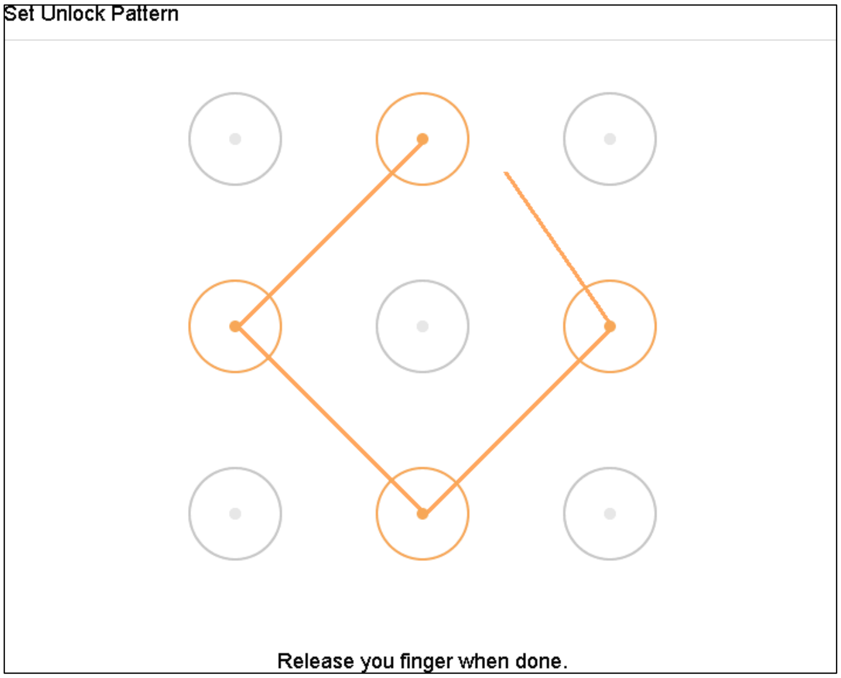
4. Edit the admin user account unlock pattern.

   1) Check the **Enable Unlock Pattern** checkbox to enable the use of an unlock pattern when logging in to the device.

   2) Use the mouse to draw a pattern among the nine dots on the screen, and release the mouse when the pattern is done.

NOTE

Refer to *Configure Unlock Pattern for Login* for detailed instructions.



Release you finger when done.

Figure 19-10 Set Unlock Patter for Admin User

5. Click **Export GUID** ⚙ to enter the reset password interface and export the GUID file for the admin user account.

NOTE

If the admin password is changed, export a 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.

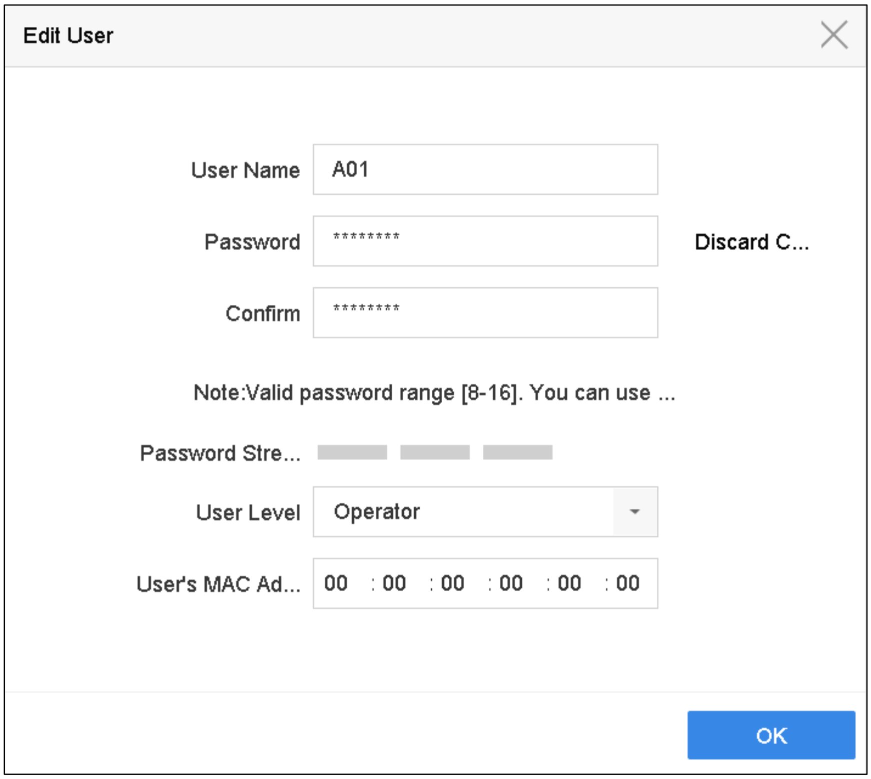
7. For the **Operator** or **Guest** user account, you can also click the ✓ button on the user management interface to edit the permission.

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 **Change Password** checkbox if you want to change the password, and input the new password in the **Password** and **Confirm** text field. A strong password is recommended.

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

2. Select a user from the list and click **Modify**.



User Name A01

Password ********

Confirm ********

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

User Level Operator

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

Figure 19-11 Edit User (Operator/Guest)

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

19.4.6 Delete a User

The admin user account has permission to delete an 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 that 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 requests 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 to establish a PPP connection over 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 countries such as the United States and Japan. Each NTSC signal frame contains 525 scan lines at 60 Hz.
- **NVR:** Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP domes, and other devices.
- **PAL:** Acronym for Phase Alternating Line. PAL is another video standard used in broadcast television systems in large parts of the world. The PAL signal contains 625 scan lines at 50 Hz.
- **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 Monitor After Starting Normally

Possible Reasons:

- No VGA or HDMI connection
- Connection cable is damaged
- Monitor input mode is incorrect

1. Verify the device is connected with the monitor via HDMI or VGA cable. If not, connect the device to the monitor and reboot.
2. Verify the connection cable is good.
3. If there is still no image displayed on the monitor after rebooting, check if the connection cable is good, and change cable to connect again.
4. Verify that the monitor Input mode is correct.
5. Check that the monitor input mode matches the device output mode (e.g., if the device output mode is HDMI, the monitor input must be the HDMI input). If not, change the monitor input mode.
6. Check if the fault is solved by the step 1 to step 3. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

- A "Di-Di-Di-DiDi" Audible Warning Sounds After a New Device Starts

Possible Reasons:

- No HDD is installed in the device
- The installed HDD has not been initialized

1. The installed HDD is not compatible with the device or is broken.
2. Verify at least one HDD is installed in the device.
    - If not, install a compatible HDD.

NOTE

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

- If you don't want to install an HDD, go to Menu > System > Event > Normal Event > Exception, and uncheck the "HDD Error" **Audible Warning** checkbox.

3. Verify the HDD is initialized.

1) Go to **Menu > Storage > Storage Device**.

2) If the status of the HDD is “Uninitialized,” check the checkbox of the corresponding HDD, and click the “Init” button.

4. Verify the HDD is detected and is in good condition.

1) Select Menu > Storage > Storage Device.

2) If the HDD is not detected or the status is “Abnormal,” replace the dedicated HDD according to the requirement.

5. Check if the fault is solved by step 1 to step 3. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

IP Camera Connected through Private Protocol Displays “Disconnected” Status

NOTE

Select “Menu > Camera > Camera > IP Camera” to get the camera status.

Possible Reasons:

- Network failure, and the device and IP camera lost connections
- The configured parameters are incorrect when adding the IP camera
- Insufficient bandwidth

1. Verify the network is connected.

1) Connect the device and PC with the RS-232 cable.

2) Open Super Terminal software, and execute the ping command. Input “ping IP” (e.g., ping 172.6.22.131).

NOTE

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 the configuration parameters are correct.

1) Go to **Menu > Camera**.

2) Verify the following parameters match those of the connected IP devices: IP address, protocol, management port, user name, and password.

3. Verify that the bandwidth is adequate.

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 step 1 to step 3. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

IP Camera Frequently Goes Online/Offline and Status Is "Disconnected"

Possible Reasons:

- The IP camera and the device versions are not compatible
- Unstable IP camera power supply
- Unstable network between IP camera and device
- Limited flow by the switch connected with IP camera and device.
- Verify the IP camera and the device versions are compatible
    1) Go to **Menu > Camera** and view the connected IP camera's firmware version.
    2) Go to **Menu > Maintenance > System Info > Device Info** and view the device firmware version.

1. Verify the IP camera power supply is stable.
    1) Verify 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.
2. Verify the network between IP camera and device is stable.
    1) When the IP camera is offline, connect 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 is packet loss.

NOTE

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

Example: Input ping 172.6.22.131 –l 1472 –f.

3. Verify the switch is not using flow control. Check the switch brand and model, and contact the switch manufacturer to check if it has flow control function. If so, turn it down.
4. Check if the fault is solved by the step 1 to step 4. If it is solved, finish the process. If not, contact a Hikvision engineer for further processing.

With No Local Monitor Connected to Device, When IP Camera Connects to Device Remotely by Web Browser, Status Displays "Connected." If Then Connect Device to Monitor via VGA or HDMI and Reboot Device, there Is Black Screen with Mouse Cursor.

Connect device to monitor before startup via VGA or HDMI, and connect IP camera to device locally or remotely, IP camera status displays "Connect," then connect device via CVBS, there is also a black screen.

Possible Reasons:
After connecting the IP camera to the device, the image is output 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 you want to view.

NOTE
The view settings can be configured only by the local device operation.

Different camera orders and window division modes can be set for different output interfaces separately. Digits like "D1"and "D2" stand for channel number, and "X" means 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 Freezes when Video Is Output Locally

Possible Reasons:

- Poor network connection between device and IP camera, and there is packet loss during transmission.

- The frame rate has not reached the real-time frame rate.

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

2. If image is stuck, connect the RS-232 ports on the PC and the device rear panel with the RS-232 cable.

3. Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (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.

4. Verify the frame rate is real-time frame rate.

5. Go to **Menu > Camera > Encoding Parameters**, and set the Frame Rate to Full Frame.

6. 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 Frozen when Video Is Output Remotely via Internet Explorer or Platform Software

Possible Reasons:

- Poor network connection between the device and the IP camera, and there is packet loss during transmission.
- Poor network connection between the device and the PC, and there is packet loss during transmission.
- The hardware performance is not good enough, including CPU, memory, etc.

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

   1) When image is frozen, connect the RS-232 port on the PC and the rear panel of the device with the RS-232 cable.

   2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (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.

2. Verify the network between the device and the PC is connected.

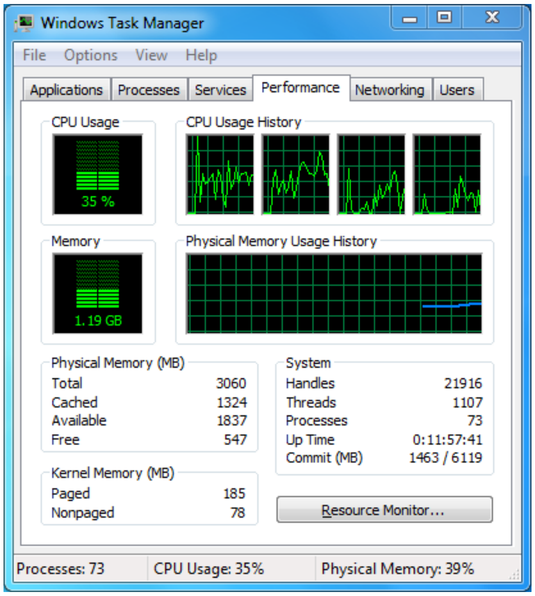
   1) Open the cmd window in the Start menu or you can press the "windows + R" shortcut key.

   2) Use the ping command to send large packets to the device, execute the command of "ping 192.168.0.0 –l 1472 –f" (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 the PC hardware is good enough.

   1) Simultaneously press **Ctrl**, **Alt**, and **Delete** to enter the windows task management interface, as shown in the following figure.



CPU Usage: 35 %

Memory: 1.19 GB

Physical Memory (MB)	
Total	3060
Cached	1324
Available	1837
Free	547

Kernel Memory (MB)	
Paged	185
Nonpaged	78

System	
Handles	21916
Threads	1107
Processes	73
Up Time	0:11:57:41
Commit (MB)	1463 / 6119

Processes: 73　CPU Usage: 35%　Physical Memory: 39%

Figure 20-1 Windows Task Management Interface

- Select the “Performance” tab; check the CPU and Memory status.
- If the resources are not adequate, end some 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 processing.

When Using Live View Audio, There Is No Sound, Too Much Noise, or Volume Is Too Low

Possible Reasons:

- Cable between the pickup and IP camera is not connected well; impedance mismatches or is incompatible.
- The stream type is not set to “Video & Audio.”
- The encoding standard is not supported by device.

1. Verify the cable between the pickup and IP camera is connected well, impedance matches, and compatible.
2. Log in to the IP camera directly, turn the audio on, and check if the sound is normal. If not, contact the IP camera manufacturer.
3. Verify the setting parameters are correct.

    1) Go to **Menu > Camera > Encoding Parameters**, and set the Stream Type to “Audio & Video.”

4. Verify the IP camera audio encoding standard 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 these two standards, log in to the IP camera to configure it to a 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 processing.

Image Freezes when Device Plays Single or Multi-Channel

Possible Reasons:

- Poor network connection between device and IP camera, and there is packet loss during transmission.
- The frame rate is not the real-time frame rate.
- The device supports up to 16-channel synchronized playback at 4CIF resolution. For 16-channel synchronized playback at 720p resolution, frame extracting may occur, which leads to slight stuttering.

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

   1) When image freezes, connect the RS-232 ports on the PC to the rear panel of the device with an RS-232 cable.

   2) Open the Super Terminal, and execute the command of "**ping** *192.168.0.0* **–l 1472 –f**" (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.

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

   1) Select Menu > Record > Parameters > Record, and set the Frame Rate to "Full Frame."

3. Verify the hardware can afford the playback. Reduce the playback channel's settings.

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

4. Reduce the number of local playback channels.

   - Go to **Menu > Playback**, and uncheck the checkbox(es) of unnecessary channels.

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 processing.

No Record File in Local HDD, and "No Record File Found" Prompt

Possible Reasons:

- The system time setting is incorrect
- The search condition is incorrect
- The HDD is in error or not detected

1. Verify the system time setting is correct.

    1) Go to **Menu > System > General**, and verify the “Device Time” is correct.

2. Verify the search condition is correct.

    1) Go to playback interface, and verify the channel and time are correct.

3. Verify the HDD status is normal.

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

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.

See Far, Go Further