



Digital Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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



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

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

Industry Canada ICES-003 Compliance

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

Applicable Model

This manual is applicable to the following models.

Series	Model
DS-E00HGHI-B	DS-E04HGHI-B
	DS-E08HGHI-B
	DS-E16HGHI-B
DS-E00HGHI-D	DS-E04HGHI-D
	DS-E08HGHI-D
DS-E00HGHI-E	DS-E04HGHI-E
DS-E00HGHI-XB	DS-E04HGHI-XB
	DS-E08HGHI-XB
	DS-E16HGHI-XB
DS-E00HGHI-XD	DS-E04HGHI-XD
	DS-E08HGHI-XD
	DS-E16HGHI-XD
DS-E00HGHI-XE	DS-E04HGHI-XE
DS-E00HQHI-B	DS-E04HQHI-B
DS-E00HQHI-XB	DS-E04HQHI-XB
iDS-E00HQHI-B	iDS-E04HQHI-B
	iDS-E08HQHI-B
iDS-E00HQHI-XB	iDS-E04HQHI-XB
	iDS-E08HQHI-XB
iDS-E00HQHI-D	iDS-E04HQHI-D
iDS-E00HQHI-XD	iDS-E04HQHI-XD
iDS-E00HUHI-B	iDS-E04HUHI-B
iDS-E00HUHI-XB	iDS-E04HUHI-XB
iDS-E00HUHI-XD	iDS-E04HUHI-XD
DS-7100HGHI-M1	DS-7104HGHI-M1

Series	Model
	DS-7108HGHI-M1
	DS-7116HGHI-M1
DS-7200HGHI-M1	DS-7204HGHI-M1
	DS-7208HGHI-M1
	DS-7216HGHI-M1
DS-7200HGHI-M2	DS-7232HGHI-M2
DS-7100HQHI-K1	DS-7116HQHI-K1
DS-7200HQHI-K1/E	DS-7216HQHI-K1/E
DS-7100HGHI-K1	DS-7104HGHI-K1
	DS-7108HGHI-K1
	DS-7116HGHI-K1
DS-7200HGHI-K1	DS-7204HGHI-K1
	DS-7208HGHI-K1
	DS-7216HGHI-K1
iDS-7100HQHI-M1/S	iDS-7104HQHI-M1/S
	iDS-7108HQHI-M1/S
iDS-7100HQHI-M1/S	iDS-7116HQHI-M1/S
iDS-7200HQHI-M1/E	iDS-7204HQHI-M1/E
	iDS-7208HQHI-M1/E
iDS-7100HUHI-M1/S	iDS-7104HUHI-M1/S
	iDS-7108HUHI-M1/S
iDS-7200HQHI-M1/FA	iDS-7204HQHI-M1/FA
	iDS-7208HQHI-M1/FA
	iDS-7216HQHI-M1/FA
iDS-7200HQHI-M1/S	iDS-7204HQHI-M1/S
	iDS-7208HQHI-M1/S
	iDS-7216HQHI-M1/S
iDS-7200HQHI-M1/E	iDS-7216HQHI-M1/E

Series	Model
iDS-7200HQHI-M2/FA	iDS-7208HQHI-M2/FA
	iDS-7216HQHI-M2/FA
iDS-7200HQHI-M2/S	iDS-7208HQHI-M2/S
	iDS-7216HQHI-M2/S
	iDS-7232HQHI-M2/S
iDS-7200HQHI-M1/XT	iDS-7204HQHI-M1/XT
	iDS-7208HQHI-M1/XT
	iDS-7216HQHI-M1/XT
iDS-7200HQHI-M2/XT	iDS-7208HQHI-M2/XT
	iDS-7216HQHI-M2/XT
	iDS-7232HQHI-M2/XT
iDS-7200HTHI-M/S	iDS-7204HTHI-M1/S
	iDS-7204HTHI-M2/S
	iDS-7208HTHI-M2/S
iDS-7200HUHI-M1/FA	iDS-7204HUHI-M1/FA
	iDS-7208HUHI-M1/FA
iDS-7200HUHI-M1/E	iDS-7204HUHI-M1/E
	iDS-7208HUHI-M1/E
iDS-7200HUHI-M1/S	iDS-7204HUHI-M1/S
	iDS-7208HUHI-M1/S
iDS-7200HUHI-M1/X	iDS-7204HUHI-M1/X
	iDS-7208HUHI-M1/X
iDS-7200HUHI-M2/X	iDS-7204HUHI-M2/X
	iDS-7208HUHI-M2/X
	iDS-7216HUHI-M2/X
iDS-7200HUHI-M2/FA	iDS-7204HUHI-M2/FA
	iDS-7208HUHI-M2/FA
	iDS-7216HUHI-M2/FA

Series	Model
iDS-7200HUHI-M2/S	iDS-7204HUHI-M2/S
	iDS-7208HUHI-M2/S
	iDS-7216HUHI-M2/S
RS-7100HGHI-M1	RS-7104HGHI-M1
	RS-7108HGHI-M1
RS-7200HGHI-M1	RS-7204HGHI-M1
	RS-7208HGHI-M1
RS-7200HUHI-M1/S	RS-7204HUHI-M1/S
	RS-7208HUHI-M1/S
RS-7200HQHI-M1/S	RS-7204HQHI-M1/S
	RS-7208HQHI-M1/S
	RS-7216HQHI-M1/S
RS-7200HUHI-M2/S	RS-7204HUHI-M2/S
	RS-7208HUHI-M2/S
	RS-7216HUHI-M2/S
RS-7200HQHI-M2/S	RS-7208HQHI-M2/S
	RS-7216HQHI-M2/S

Symbol Conventions

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

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

Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- For the device with the sign ⚡ indicating hazardous live, the external wiring connected to the terminals requires installation by an instructed person.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Do not ingest battery. Chemical Burn Hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- Use only power supplies same with the original model, or LPS power supplies with the same voltage and electric current.
- In order to prevent data leakage, please use the Secure Erase function to clear data before discarding your SSD device.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current.
- - identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- If the device has been powered off or placed for a long time, its coin/button cell battery may run out power.
- When the coin/button cell battery runs out power, the system time would be incorrect, please contact the after-sales service to replace the battery.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only. The current for the connected device shall be not more than 0.1 A.
- The serial port of the device is used for debugging only.
- If the power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.
- If a power adapter is provided in the device package, use the provided adapter only.

- For the device with sticker  or  , pay attention to the following cautions: CAUTION: Hot parts! Do not touch. Burned fingers when handling the parts. Wait one-half hour after switching off before handling the parts.
- If the device needs to be installed on the wall or ceiling,
 1. Install the device according to the instructions in this manual.
 2. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Under high working temperature (40 °C (104 °F) to 55 °C (131 °F)), the power of some power adapters may decrease.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

HDD Installation

If your device does not support HDD hot swapping, disconnect the power from the device before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

Scan the QR code below to view HDD installation videos.



Figure 1-1 HDD Installation

Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

1. Unfasten screws on the back, and push the cover backwards to remove the cover.

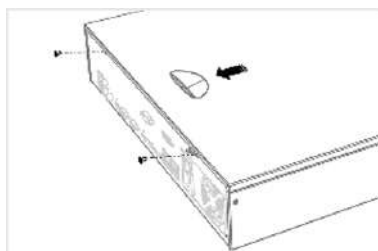


Figure 1-2 Remove Cover

2. Fix the HDD on the bracket with screws.



Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

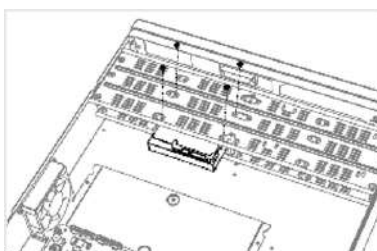


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

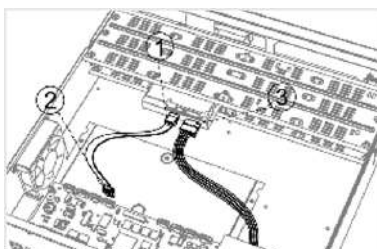


Figure 1-4 Connect Cable



Note

You can repeat the steps above to install other HDDs.

4. Reinstall the device cover and fasten screws.

Front Panel Plug-Pull Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

Steps

1. Fix mounting ears to HDD with screws.

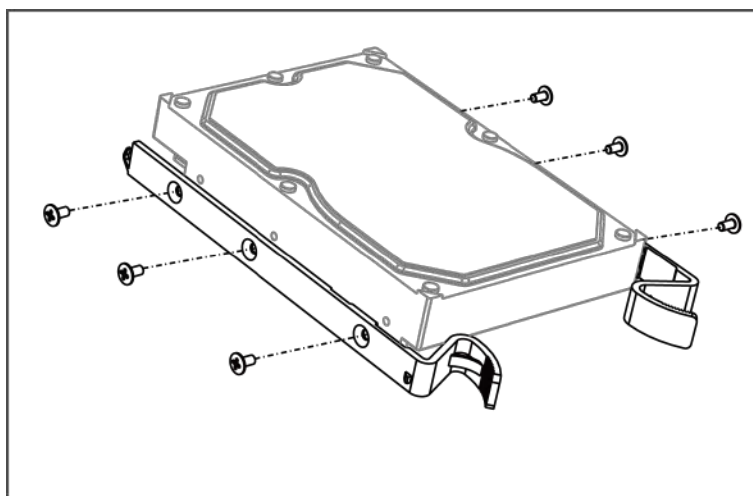


Figure 1-5 Fix Mounting Ears to HDD

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

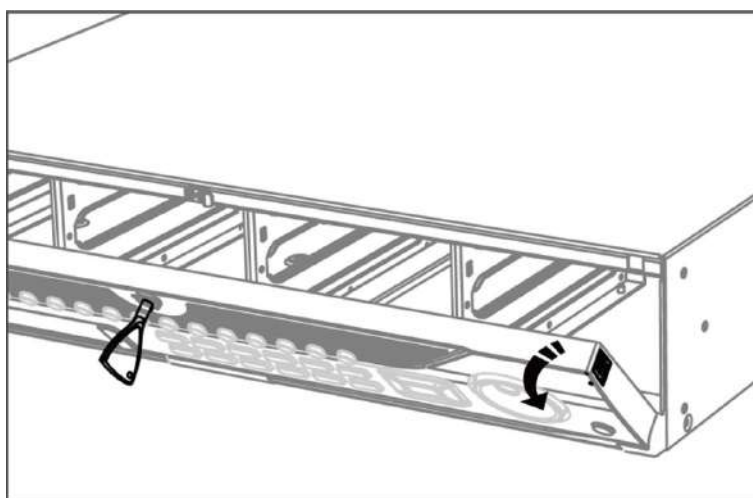


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

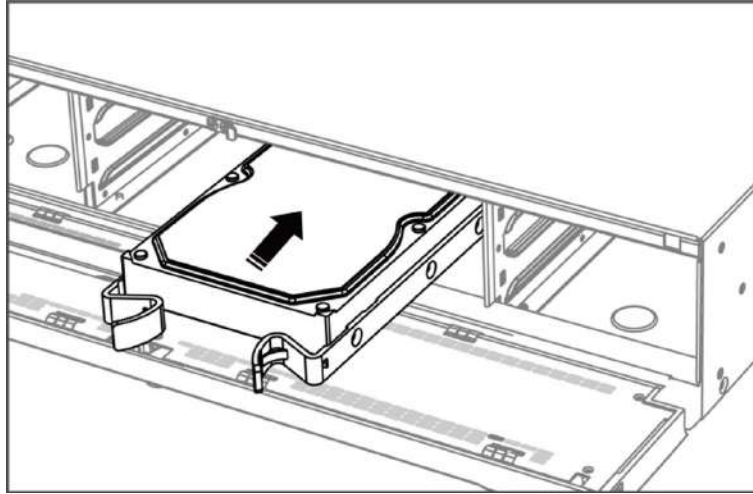


Figure 1-7 Insert HDD

- 4. Optional:** Repeat the steps above to install other HDDs.
- 5.** Close the front panel and lock it with key.

Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

- 1.** Remove the cover from device by unfastening the screws on panels.

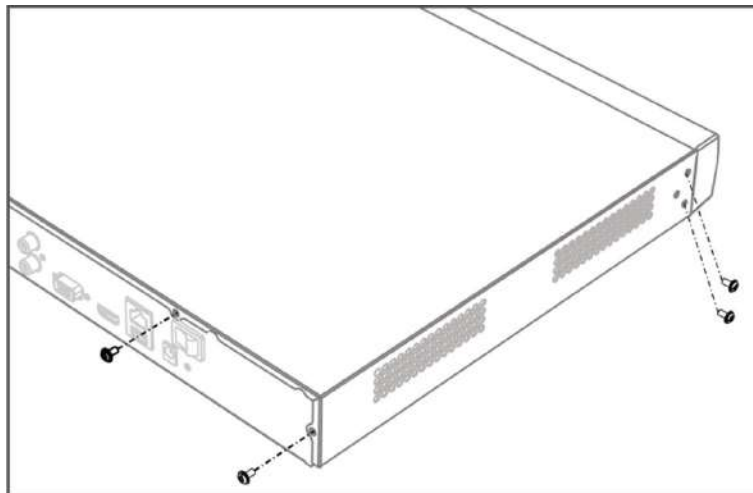


Figure 1-8 Remove Cover

- 2.** Connect the data cable and power cable.
 - 1) Connect one end of data cable to the device motherboard.

- 2) Connect the other end of data cable to HDD.
- 3) Connect one end of power cable to HDD.
- 4) Connect the other end of power cable to the device motherboard.

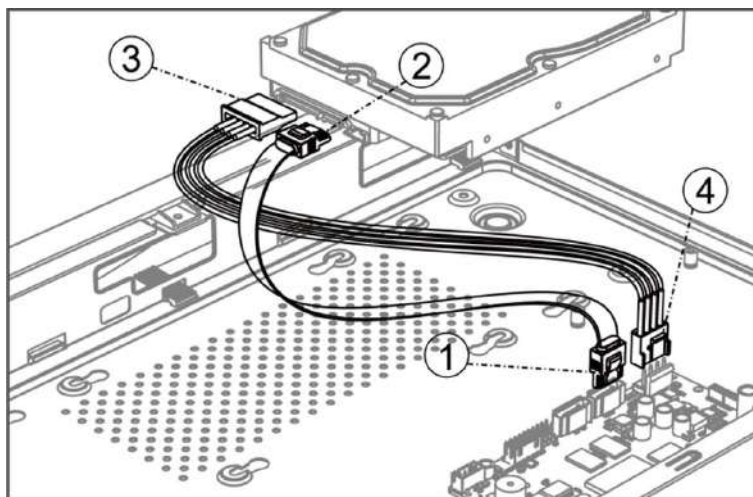


Figure 1-9 Connect Cables

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

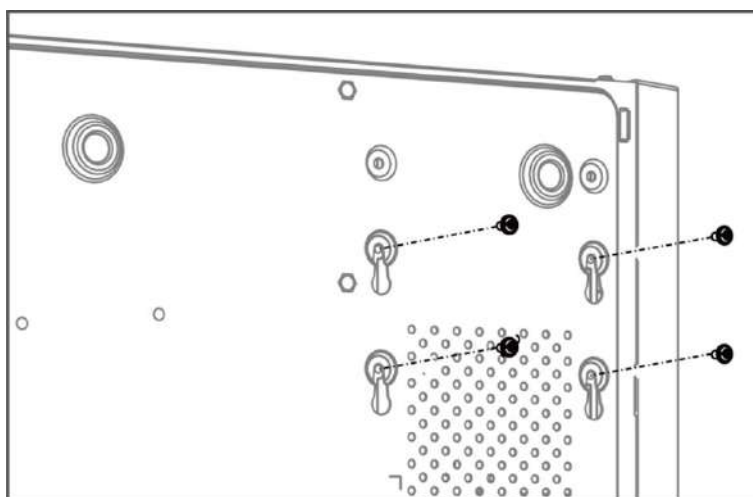


Figure 1-10 Fix HDD to Device Bottom

4. **Optional:** Repeat the steps above to install other HDDs.
5. Reinstall the device cover and fasten screws.

Coin/Button Cell Battery Replacement

The coin/button cell battery should be replaced when the device has been powered off or placed for a long time, and the system time is incorrect.

Before You Start

Power off your device.

Steps

1. Remove the device chassis cover.
2. Find the coin/button cell battery on motherboard.
3. Use tweezers to push the metal latch at the middle from its inside, and the battery would automatically pop up.

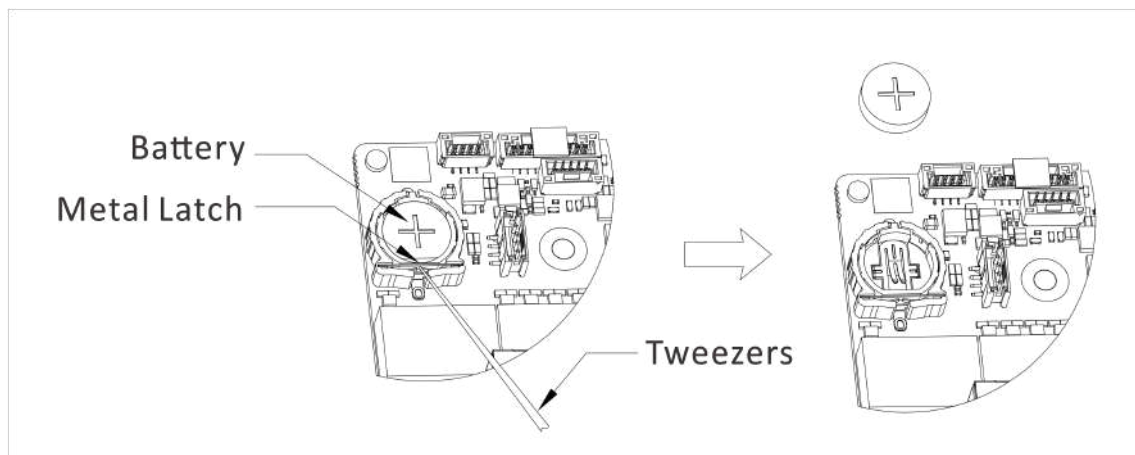


Figure 1-11 Remove Battery

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

Note

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

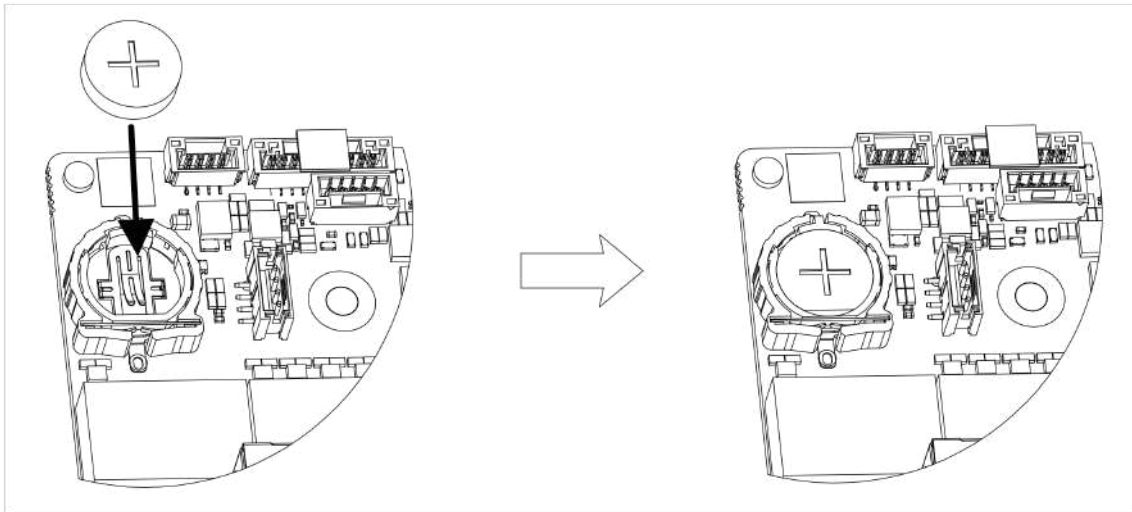


Figure 1-12 Replace Battery

5. Reinstall the device chassis cover.

What to do next

If the system time is incorrect, please go to configure the time.

Contents

Chapter 1 Startup	1
1.1 Activate Your Device	1
1.2 Login	3
1.2.1 Log in via Unlock Pattern	3
1.2.2 Log in via Password	3
Chapter 2 Live View	5
2.1 GUI Introduction	5
2.2 PTZ Control	6
2.2.1 Configure PTZ Parameter	6
2.2.2 PTZ Control Panel Introduction	8
2.2.3 Customize Preset	8
2.2.4 Customize Patrol	8
2.2.5 Customize Pattern	9
Chapter 3 Playback	10
3.1 GUI Introduction	10
3.2 Normal Playback	11
3.3 Event Playback	12
3.4 Back up Clip	13
3.5 Backup Device Playback	13
Chapter 4 Search File	14
4.1 Search Human by Face Picture	14
4.2 Quick Backup	16
Chapter 5 Configuration (Easy Mode)	17
5.1 System Configuration	17
5.1.1 General	17
5.1.2 User	17

5.1.3 Exception	19
5.2 Network Configuration	20
5.2.1 General	20
5.2.2 Hik-Connect	21
5.2.3 Email	22
5.3 Camera Management	24
5.3.1 Network Camera	24
5.3.2 Motion	27
5.3.3 OSD Settings	28
5.4 Configure Alarm Linkage Action	28
5.5 Configure Arming Schedule	29
5.6 Recording Management	30
5.6.1 Storage Device	30
5.6.2 Configure Recording Schedule	31
5.6.3 Configure Recording Parameter	33
Chapter 6 Configuration (Expert Mode)	35
6.1 System Configuration	35
6.1.1 General	35
6.1.2 Live View	36
6.1.3 User	38
6.2 Network Configuration	38
6.2.1 TCP/IP	38
6.2.2 DDNS	40
6.2.3 PPPOE	40
6.2.4 NAT	41
6.2.5 Wi-Fi	42
6.2.6 NTP	43
6.2.7 Log Server Settings	44

6.2.8 Ports (More Settings)	46
6.2.9 Hik-Connect	48
6.2.10 Email	48
6.3 Camera Management	48
6.3.1 Configure Signal Input	48
6.3.2 Network Camera	49
6.3.3 Display Settings	54
6.3.4 Privacy Mask	55
6.4 Event Configuration	56
6.4.1 Normal Event	56
6.4.2 Perimeter Protection	60
6.4.3 Face Recognition	63
6.4.4 Configure Arming Schedule	67
6.4.5 Configure Alarm Linkage Action	67
6.5 Recording Management	70
6.5.1 Configure Recording Schedule	70
6.5.2 Configure Recording Parameter	72
6.5.3 Storage Device	74
6.5.4 Configure Storage Mode	75
6.5.5 Advanced Settings	77
Chapter 7 Maintenance	79
7.1 Restore Default	79
7.2 Search Log	79
7.3 System Service	79
7.4 Buzzer Switch	80
7.5 Device Maintenance	80
7.5.1 Schedule Reboot	80
7.5.2 Device Status	81

7.6 Upgrade	81
7.6.1 Local Upgrade	81
7.6.2 Online Upgrade	82
Chapter 8 Alarm	83
8.1 Set Event Hint	83
8.2 View Alarm in Alarm Center	83
Chapter 9 Web Operation	84
9.1 Introduction	84
9.2 Login	84
9.3 Live View	85
9.4 Playback	85
9.5 Configuration	86
9.6 Log	87
Chapter 10 Appendix	89
10.1 Glossary	89

Chapter 1 Startup

1.1 Activate Your Device

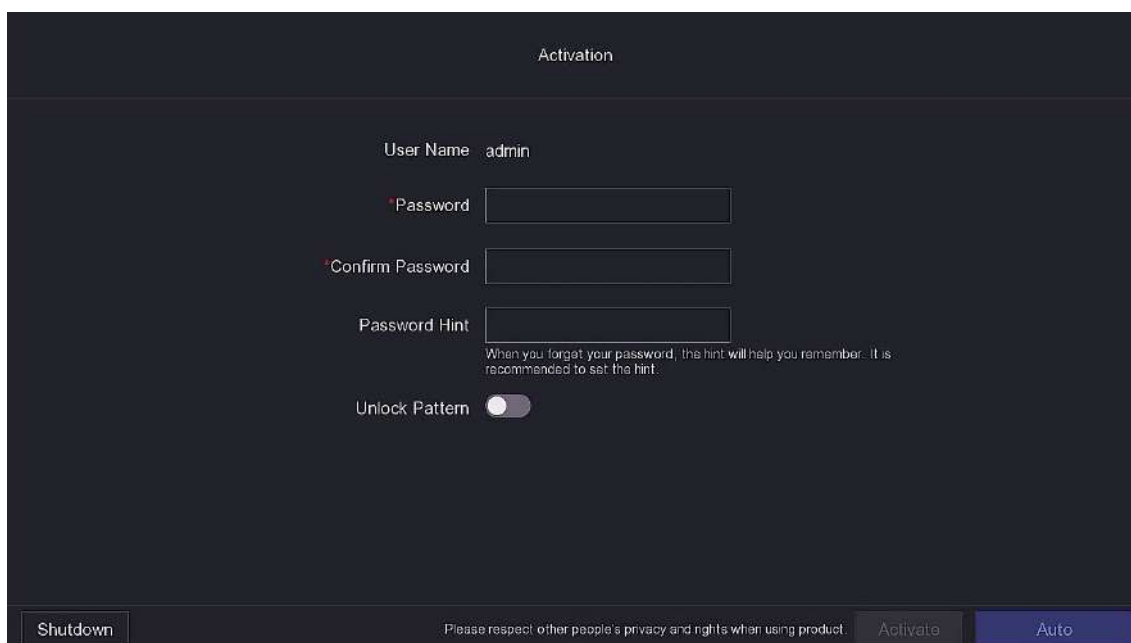
For the first-time access, you need to activate the video recorder by setting an admin password. No operation is allowed before activation. You can also activate the video recorder via web browser, SADP or client software.

Before You Start

- Power on your device.
- For the first-time access, if you do not move the mouse on the interface for one minute, the resolution will be set as 1280*720/60Hz (720P) automatically.

Steps

1. Select a language.
2. Click **Apply**.
3. Input the same password in **Password** and **Confirm Password**.



The screenshot shows the 'Activation' window. At the top, it says 'Activation'. Below that, there are several input fields: 'User Name' with the value 'admin', 'Password', 'Confirm Password', and 'Password Hint'. There is a note below the hint field: 'When you forget your password, the hint will help you remember. It is recommended to set the hint.' At the bottom, there is a toggle switch for 'Unlock Pattern' which is currently turned off. At the very bottom of the window, there are three buttons: 'Shutdown', 'Activate', and 'Auto'. A small disclaimer 'Please respect other people's privacy and rights when using product.' is visible between the 'Shutdown' and 'Activate' buttons.

Figure 1-1 Activation

Warning

- Strong Password recommended-We highly recommend you create a strong password of your own choosing according to the following rules in order to increase the security of your product:

- 8 to 16 characters.
- Do not contain the following characters in the password: the user name, 123, admin, no less than 4-digit continuously increasing or decreasing numbers, or no less than 4 continuously same characters.
- At least 2 of the following types are required: digits, upper-case letters, lower-case letters, and special characters.
- Risky password is not allowed.
- We recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Optional: Set Password Hint.



When you forget your password, the hint will help you remember it. It is recommended to set the password hint.

5. Optional: Set Unlock Pattern.

- 1) Enable **Unlock Pattern**.
- 2) Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.



- The pattern shall have 4 dots at least.
- Each dot can be connected for once only.

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

6. Click **Activate**.

7. Optional: Click **Auto** to automatically configure all the parameters in the wizard.

What to do next

Follow the wizard to set basic parameters.

- For basic system parameters. Refer to **General** for details.
- For general network parameters. Refer to **General** for details.
- For storage device configuration. Refer to **Storage Device** for details.
- For adding network cameras. Refer to **Network Camera** for details.
- For platform configuration. Refer **Hik-Connect** to for details.
- When you forget your password, there are three methods to reset it, including password resetting email, Hik-Connect, and security questions. You can configure the password resetting method. Refer to **Set Password Resetting Email** and **Hik-Connect** for details. If you do not set any methods, the auto login window will pop up. If you click **Yes**, you can log in without password.

1.2 Login

1.2.1 Log in via Unlock Pattern

Steps

1. Right click the mouse to select **Menu** or left click the mouse on live view.

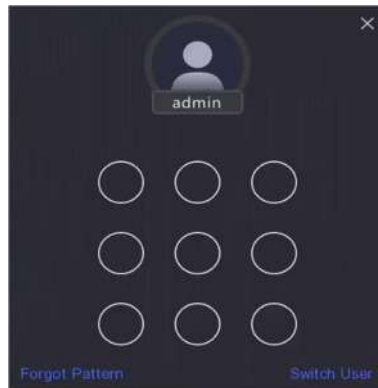


Figure 1-2 Draw the Unlock Pattern

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

Note

- If you have forgotten your pattern, you click **Forgot My Pattern** or **Switch User** to log in via password.
 - If you have drawn the wrong pattern for more than 5 times, the system will switch to the normal login mode automatically.
-

1.2.2 Log in via Password

If your video recorder has logged out, you must log in before operating the menu and other functions.

Steps

1. Select **User Name**.

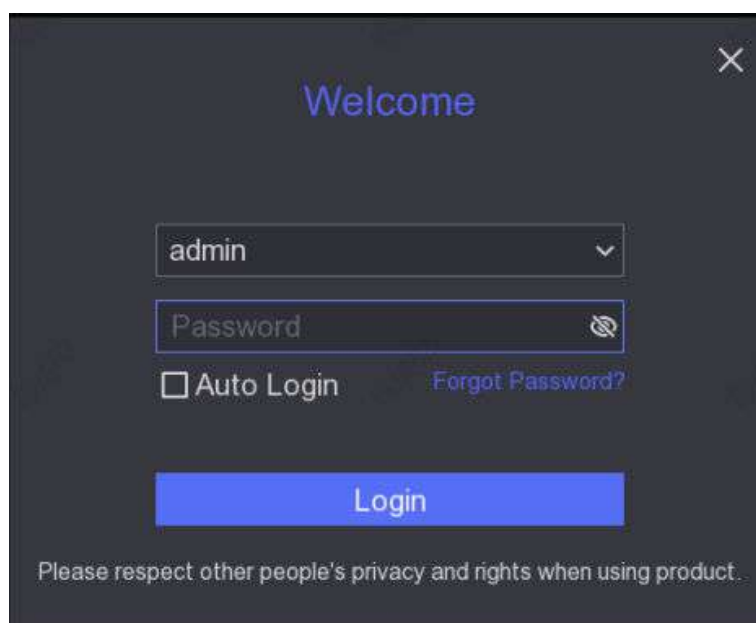


Figure 1-3 Login Interface

2. Input password.

3. Click **Login**.

 Note

- When you forget the password of the admin, you can click **Forgot Password** to reset the password.
 - If you enter the wrong password 7 times, the current user account will be locked for 60 seconds.
 - If you check **Auto Login**, you can log in without password.
-

Chapter 2 Live View

2.1 GUI Introduction

- Click **Target Detection** at the upper-left corner, and select  or  to display the specified live target detection results. For result details, click **View More**.



Note

- Target Detection** is only available for certain models.
- Target Detection** is valid when HDD is installed.
-  is valid for motion detection, line crossing detection, intrusion detection, and face capture.
- Click  to start/stop auto-switch. The screen will automatically switch to the next one.
- Click  /  /  /  /  to select the live view window division.
- Click  to enter full screen mode.
- Double click a camera to view it in single-screen mode. Double click again to exit single-screen mode.
- Change a camera live view screen by dragging it from its screen to the desired screen.
- Scroll up/down to turn to previous/next screen.
- Position the cursor on a camera to show shortcut menu.



Figure 2-1 Shortcut Menu

Table 2-1 Shortcut Menu Description

Button	Description
	Start playing videos recorded in the latest five minutes.
	Digital zoom. You can adjust zoom-in times and view the desired area.
	Click it to enter PTZ control mode.
	Turn on/off live view audio.
	Switch video stream.

- In the live view interface, there are icons at the upper-right corner of the screen for each camera, showing the camera recording and alarm status.

Table 2-2 Live View Icon Description

Icon	Description
	Alarming (normal event and smart event).
	Recording.

- Right click your mouse to display the shortcut menu.

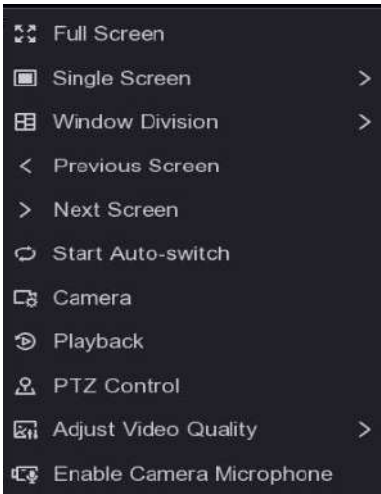


Figure 2-2 Right Click Shortcut Menu

2.2 PTZ Control

2.2.1 Configure PTZ Parameter

You shall configure PTZ parameters before controlling a PTZ camera.

Steps

1. Preview a camera in live view and click  on shortcut menu.

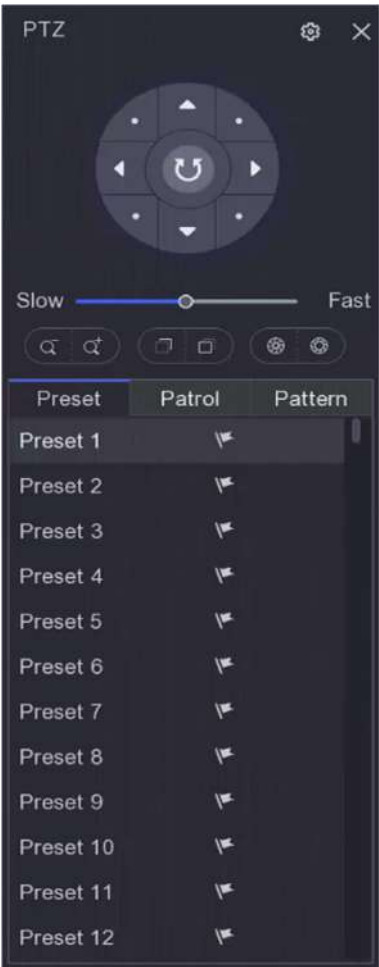


Figure 2-3 PTZ Settings

- 2. Click .
- 3. Set the PTZ camera parameters.

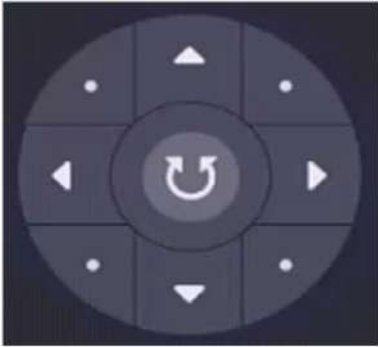
 Note

All parameters should be the same as the PTZ camera.

- 4. Click **OK**.

2.2.2 PTZ Control Panel Introduction

Table 2-3 PTZ Panel Description

Icon	Description
	Direction buttons, and the auto-cycle button.
	The speed of the PTZ movement.
	Zoom -/+.
	Focus -/+.
	Iris -/+.

2.2.3 Customize Preset

Set a preset location where the PTZ camera would point to when an event occurs.

Steps

- 1. Preview a camera in live view and click  on shortcut menu.
- 2. Select a desired preset in preset list.
- 3. Use direction buttons to wheel the camera to required locations. Adjust zoom and focus as your desire.
- 4. Click .

What to do next

Double click a preset in the preset list to call it.

2.2.4 Customize Patrol

Patrol refers to a path consists of a series of presets with designated sequence. It provides dynamic live image for monitoring several presets.

Steps

- 1. Preview a camera in live view and click on  shortcut menu.

2. Click **Patrol**.
3. Click  of a desired patrol.
4. Click .
5. Configure key point parameters, such as the key point No., duration of staying for one key point and speed of patrol. The key point is corresponding to the preset. The preset number determines the order at which the PTZ will follow while cycling through the patrol. **Duration** refers to the time span to stay at the corresponding key point. **Speed** defines the speed at which the PTZ will move from one key point to the next.

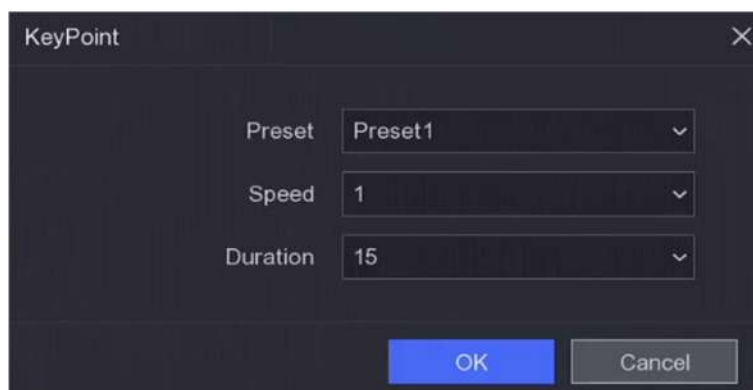


Figure 2-4 Patrol Settings

6. Click **OK**.
7. Click **Save**.

What to do next

Select a patrol and click  to call it. The PTZ camera will move according the predefined patrol path.

2.2.5 Customize Pattern

A pattern records the movement path and dwell time in a certain position. When you call a pattern, the PTZ camera will move according to the recorded path.

Steps

1. Preview a camera in live view and click  on shortcut menu.
2. Click **Pattern**.
3. Select a pattern.
4. Click .
5. Use direction buttons to wheel the camera to required locations. Adjust zoom and focus as your desire.
6. Click . The previous PTZ camera moving path is recorded as a pattern.

What to do next

Select a pattern and click  to call it. The PTZ camera will move according the predefined pattern.

Chapter 3 Playback

3.1 GUI Introduction

Go to **Playback** .

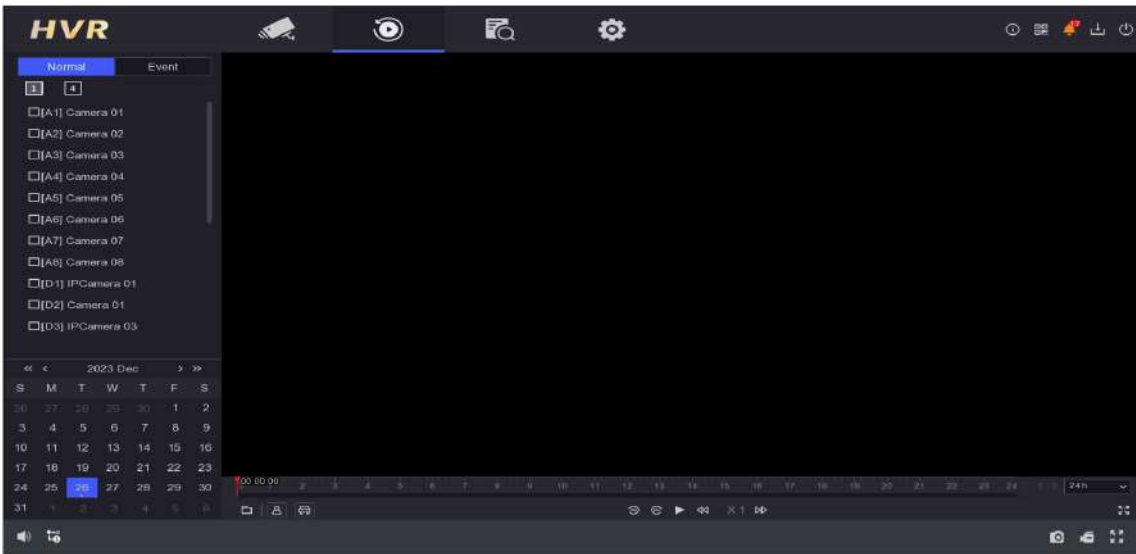


Figure 3-1 Playback

Table 3-1 Playback Interface Description

Button	Operation	Button	Operation
	30 s reverse.		30 s forward.
	Full screen.		Start playback.
	Speed down.		Speed up.
	Speed.		

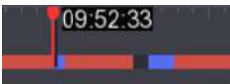


Figure 3-2 Timeline

- Position the cursor on the timeline, drag the timeline to position to a certain time.
- Period marked with blue bar contains video. Red bar indicates the video in the period is event video.
- Scroll up/down to zoom out/in timeline.

3.2 Normal Playback

Play back normal videos.

Steps

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



The blue triangle at the calendar date corner indicates there are available videos. For example, **10** means video is available. **11** means no video.

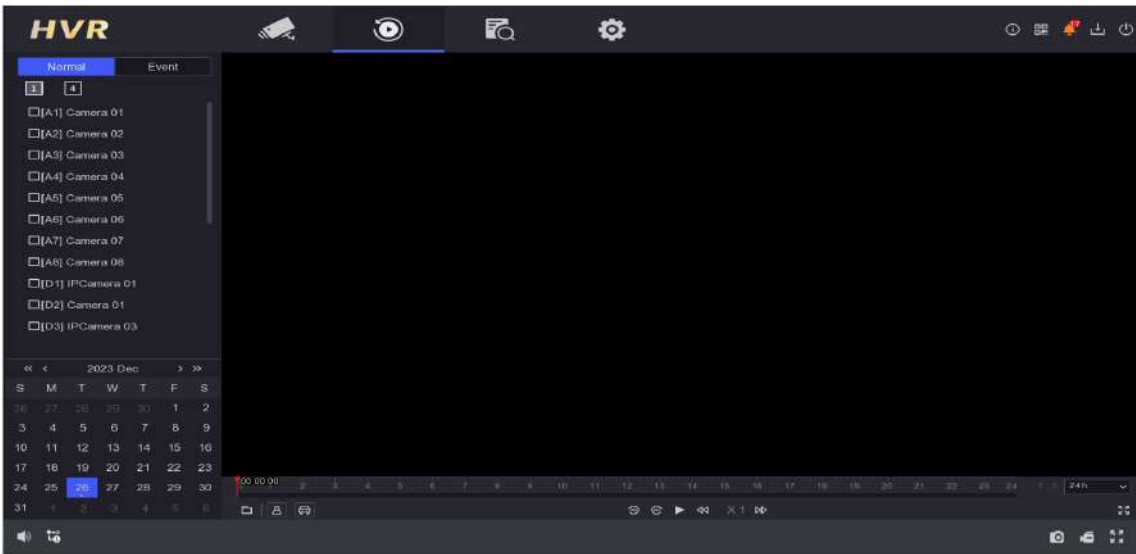


Figure 3-3 Normal Playback

- 4. **Optional:** Position the cursor on playback window to show control bar.



Figure 3-4 Control Bar

Table 3-2 Button Description

Button	Description	Button	Description
	Adjust definition.		Zoom in/out playback image.
	Turn on/off audio.		Add tag.
	Lock/unlock video.		Clip video.

3.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information, .

Before You Start

- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration → Video/Audio → Display Info. on Stream** .
- Ensure your video recorder has enabled **Save Camera VCA Data**. You can enable it in **Configuration → Record → Advanced** .

Steps

1. Go to **Playback** .
2. Click **Event**.
3. Select a camera.
4. Position the cursor on playback window to show control bar.

Table 3-3 Button Description

Button	Description	Button	Description
	Add tag.		Zoom in/out playback image.
	Clip video.		Lock/unlock video.
	Configure detection area.		Turn on/off audio.

5. Click  to set detection areas of line crossing detection, intrusion detection, or motion detection.
6. Click  to search videos. Videos meet the detection rule requirement will be marked in red.
7. Click  to configure the play strategy.

Skip Normal Videos

If it is enabled, videos without smart information will not be played.

Normal Video

Set normal video playback speed. The option is only valid when **Do not Play Normal Videos** is unchecked.

Play Speed of Smart/Custom Video

Set playback speed of videos with smart information. The option is only valid when **Do not Play Normal Videos** is enabled.

3.4 Back up Clip

You can clip videos during playback. Video clips can be exported to the backup device (USB flash drive, etc.).

Before You Start

Connect a backup device to your video recorder.

Steps

1. Start playback. Refer to **Normal Playback** for details.
2. Click .
3. Set the start and end time.
4. Click **Save**.
5. Select the backup device and folder.
6. Click **Save** to export the clip to backup device.

3.5 Backup Device Playback

You can replay the videos which are stored in the backup device (USB flash drives, USB HDDs, USB writer, SATA writer, etc.).

Before You Start

Please make sure the videos are exported from your video recorder and the format is MP4.

Steps

1. Connect a backup device to your video recorder.
2. Click  on the playback interface.
3. Click  or double click the video.

Chapter 4 Search File

Steps

1. Go to **Search**.
2. Select a search type (video, picture, event, etc.).
3. Set search conditions.
4. **Optional:** Click **Quick Backup** to quickly export videos to the device.



Note

Quick backup is available for video and event search.

5. Click **Search**.
 - Click  to lock the file. Locked file will not be overwritten.
 - Select file(s), and click **Export** to export file(s) to backup device.

4.1 Search Human by Face Picture

You can search human records by the provided face picture.

Before You Start

Ensure you have enabled face picture comparison.

Steps

1. Go to **Search → Human** .

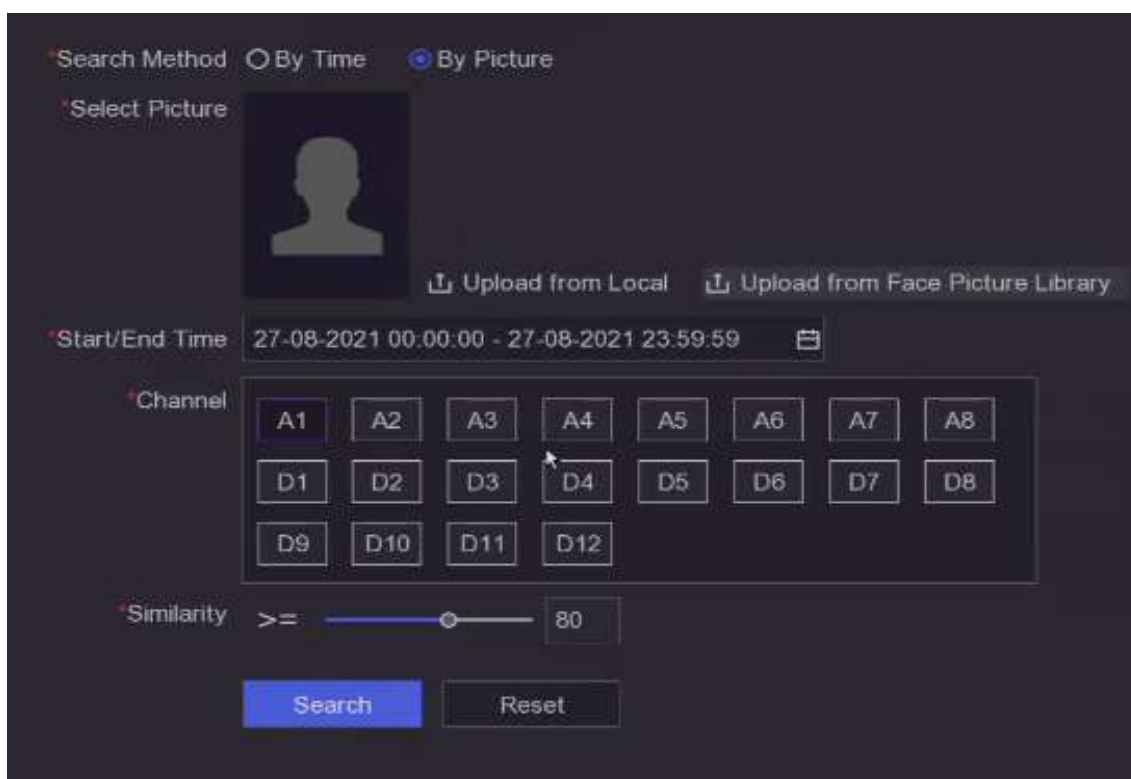


Figure 4-1 Search Human by Face Picture

2. Set **Search Method** by **By Picture**.

3. Upload a face picture.

- Click **Upload from Local** to upload a face picture from a local storage device, such as USB flash drive.
- Click **Upload from Face Picture Library** to upload a face picture from a face picture library.



Note

- Only JPG and JPEG formats are supported.
- Each picture size should be less than 1 MB.
- The picture resolution shall be between 80 × 80 and 1920 × 1080.

4. Set the start time and end time.

5. Set **Similarity**.

Similarity

Similarity value ranges from 0 to 100. Device will analyze the similarity between the detected face picture and face pictures in the library. When the similarity reaches the threshold value, the face picture comparison succeeded, and the face picture is recognized.

6. Click **Search**.

4.2 Quick Backup

Before You Start

Connect a backup device to your video recorder.

Steps

1. Go to **Search** .
2. Set search conditions.
3. Click **Quick Export**.
4. Select backup device and path.
5. Click **OK** to start exporting.

Chapter 5 Configuration (Easy Mode)

Easy mode contains basic configurations. Go to **Configuration** , and click **Easy Mode**.

5.1 System Configuration

5.1.1 General

You can configure the output resolution, system time, etc.

Steps

1. Go to **Configuration** → **System** → **General** .
2. Configure the parameters as your desire.

Wizard

The wizard will pop up after the device starts up.

Local Auto Login

You can log in without password.

NTP Time Sync

Network time protocol (NTP) is a networking protocol for time synchronization. The device can connect to NTP (network time protocol) server to sync time.

Interval (min)

Time interval between two time synchronization with NTP server.

NTP Server

IP address of the NTP server.

3. Click **Apply**.

5.1.2 User

Add User

There is a default account: Administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest user only has live view, playback, and log search permission.

Steps

1. Go to **Configuration** → **System** → **User** .
2. Click **Add** and confirm your admin password.

The screenshot shows the 'Add User' dialog box. It has a title bar with 'Add User' and a close button. The main area contains four input fields: 'User Name', 'User Level' (a dropdown menu showing 'Guest'), 'Create Password', and 'Confirm'. Below these fields are three tabs: 'Local Permission', 'Remote Permission', and 'Camera Permission'. The 'Local Permission' tab is selected and shows five checkboxes: 'Local Parameter Configuration' (unchecked), 'Local Log Search' (checked), 'Local Upgrade/HDD Initialization/Video Advanced Settings' (unchecked), 'Local Camera Management' (unchecked), and 'Local Shutdown / Reboot' (unchecked). At the bottom right are 'OK' and 'Cancel' buttons.

Figure 5-1 Add User

3. Enter user name.
4. Enter the same password in **Create Password** and **Confirm**.

 Warning

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

-
5. Set **Local Permission**, **Remote Permission** and **Camera Permission** according to the actual needs.
 6. Click **OK**.
 - Click  /  to edit/delete user.

Set Password Resetting Email

When you forgot your login pattern and password, the device will send an email contains verification code to your email for password resetting.

Steps

1. Go to **Configuration → System → User** .
2. Click **Password Resetting Email**.
3. Enter admin password for authorization.
4. Enter an email address.
5. Click **OK**.

Reset Password

You can reset your password when you forgot your login pattern and password.

Steps

1. Click **Forgot Password** at the password login interface.
2. Click **Next** if you agree the Privacy Policy, you can scan the QR code to read it.
3. Follow the wizard to reset password.

5.1.3 Exception

You can receive exception events hint in alarm center, and set exception linkage actions.

Steps

1. Go to **Configuration → System → Exception** .
2. **Optional:** Configure event hint. When the set events occur, you will receive hints in alarm center.
 - 1) Enable **Event Hint**.
 - 2) Click  at the upper-right corner of local menu to enter alarm center.
 - 3) Select an event type.
 - 4) Click **Set** to select events to hint.
3. Set **Exception Type**
4. Select **Normal Linkage** and **Trigger Alarm Output** type for exception linkage actions.

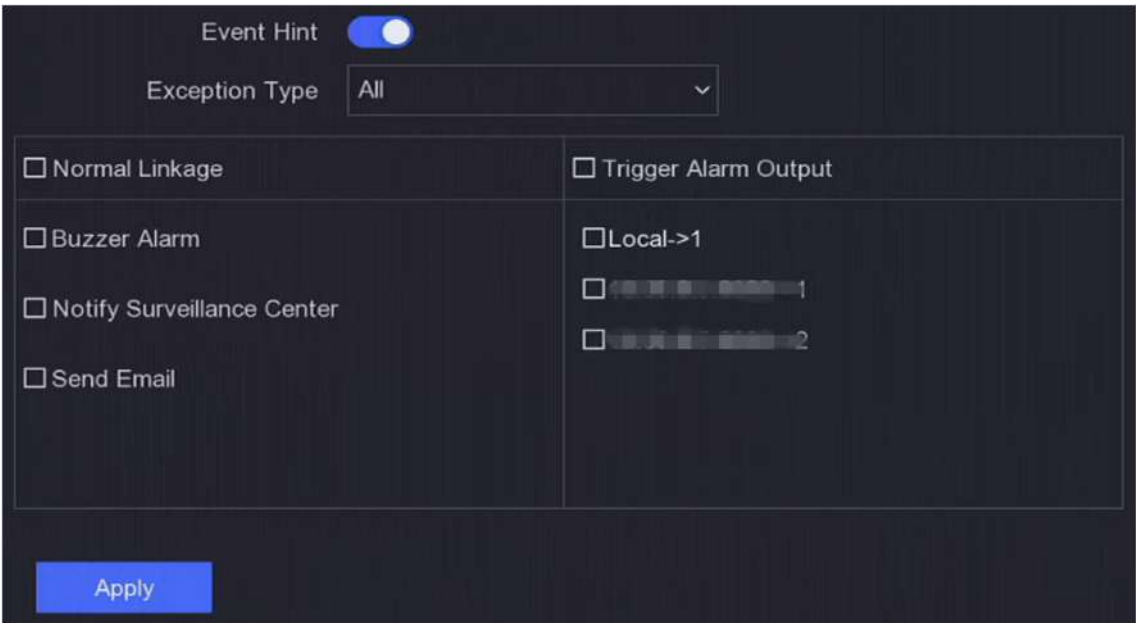


Figure 5-2 Exceptions

5. Click **Apply**.

5.2 Network Configuration

5.2.1 General

You shall properly configure the network settings before operating the device over network.

Steps

1. Go to **Configuration → Network → General** .

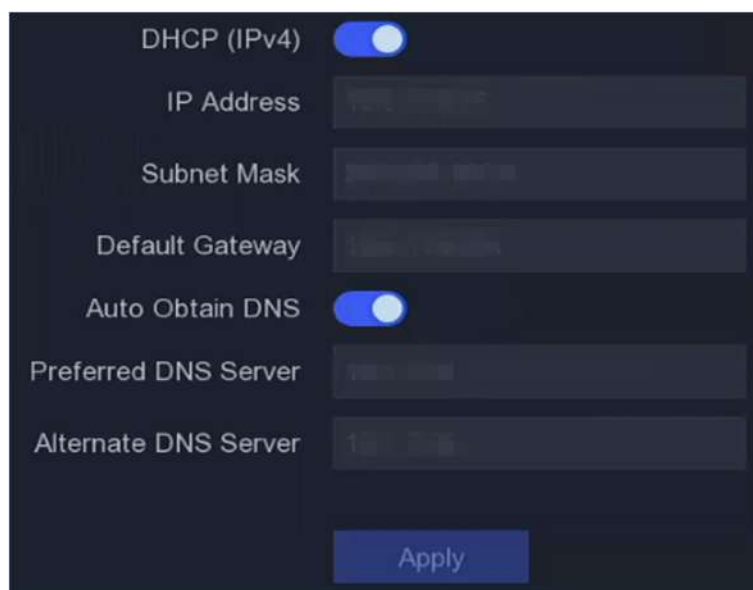


Figure 5-3 Network

2. Set network parameters.

DHCP

If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

Auto Obtain DNS

If **DHCP** is enabled. You can enable **Auto Obtain DNS** to automatically obtain **Preferred DNS Server** and **Alternate DNS Server**.

3. Click **Apply**.

5.2.2 Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your connected devices, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **Configuration → Network → Hik-Connect**.
2. Turn on **Enable**. The service terms will pop up.
 - 1) Read the service terms and privacy statement.
 - 2) Check **I have read and agree to Service Terms and Privacy Statement**. if you agree with the service terms and privacy statement.
 - 3) Click **OK**.
3. Click  to set verification code.

4. **Optional:** Enable **Platform Time Sync**, the device will sync time with the platform server instead of NTP server.
5. **Optional:** Enable **Stream Encryption**. It requires to enter verification code in remote access and live view after this function is enabled.
6. **Optional:** Edit **Server IP**.
7. **Optional:** Enable **Sub-Stream Self-Adaptive Bitrate**. When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.
8. Bind your device with a Hik-Connect account.
 - 1) Use a smart phone to scan the QR code, and download Hik-Connect app. You can also download it from <https://appstore.hikvision.com> , or the QR code below. Refer to *Hik-Connect Mobile Client User Manual* for details.



Figure 5-4 Download Hik-Connect

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



Note

- If the device is already bound with an account, you can click **Unbind** to unbind with the current account.
- You can also use the QR code in  at the upper-left corner to download Hik-Connect and bind your device.

-
9. Click **Apply**.

Result

- If your device is connected with Hik-Connect platform, **Connection Status** will be **Online**.
- If your device is bound with a Hik-Connect account, **Bind Status** will be **Yes**.

What to do next

You can access your video recorder via Hik-Connect.

5.2.3 Email

Set an email account to receive event notification.

Before You Start

- Ensure SMTP service is available for your email.
- Configure your network parameters. Refer to **General** for details.

Steps

1. Go to **Configuration → Network → Email** .

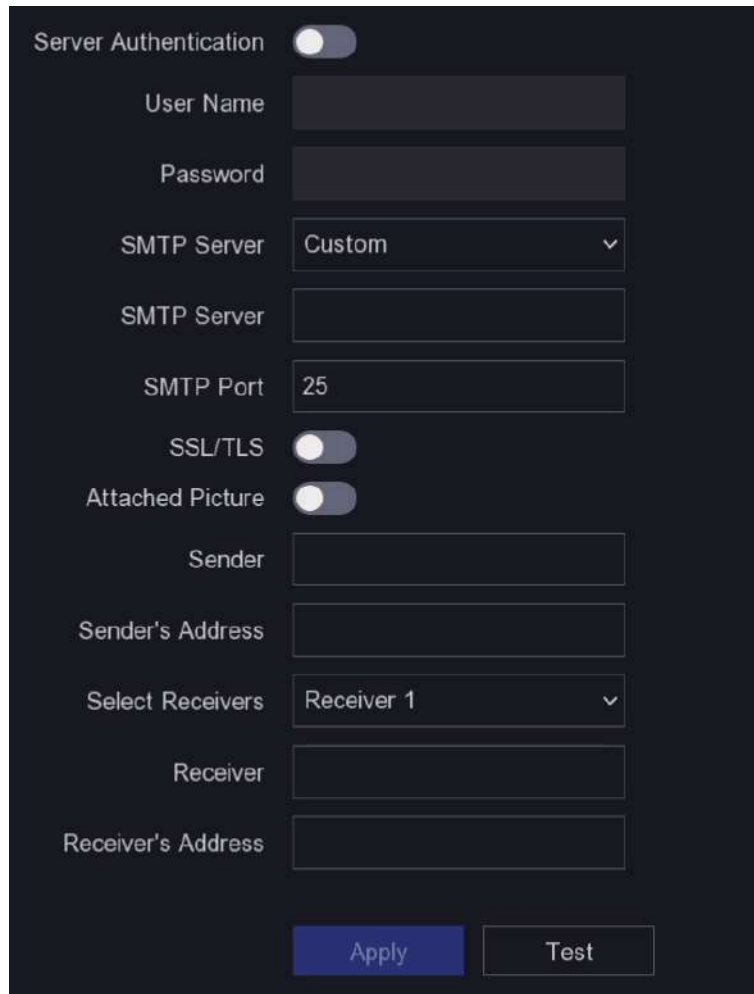


Figure 5-5 Email

2. Set email parameters

Server Authentication

Check it to enable the server authentication feature.

User Name

The user account of email sender for SMTP server authentication.

Password

The password of email sender for SMTP server authentication.

SMTP Server/SMTP Port

After selecting the **SMTP Server**, its address and port will be showed automatically. You can also edit them according to actual needs.

SSL/TLS

(Optional) Enable SSL/TLS if it is required by the SMTP server.

Attached Picture

(Optional) If events are triggered, it will send images as email attachment.

Sender

The sender name.

Sender's Address

The sender's email address.

Select Receiver

Select a receiver. Up to 3 receivers are available.

Receiver

The receiver name.

Receiver's Address

The receiver's email address.



Note

For network cameras, the event images are directly sent as the email attachment. One network camera only sends one picture.

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

4. Click **Apply**.

5.3 Camera Management

5.3.1 Network Camera

Configure Signal Input

For certain digital video recorder models, you can configure the analog and IP signal input types.

Steps

1. Go to **Configuration → Camera → Analog → Analog**.
2. Select signal input type as **HD/CVBS** or **IP** for each channel.

HD/CVBS

Four types of analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be connected randomly for the channel.

IP

Network camera can be connected for the channel.

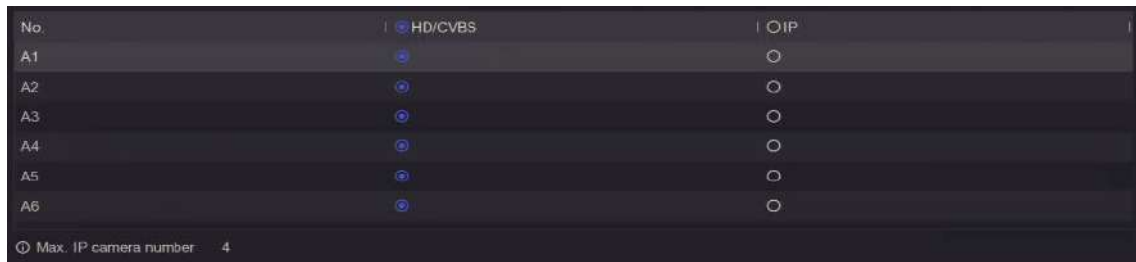


Figure 5-6 Signal Input Type

3. Click **Apply**. You can view the maximum network camera accessible number in **Max. IP Camera Number**.

Add Network Camera by Device Password

Add network cameras which the password is the same as your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with your video recorder.
- Ensure the network connection is valid and correct. Refer to **General** for details.
- Ensure the network camera password is the same as your video recorder.

Steps

1. Go to **Configuration → Camera → IP Camera**. The online cameras on the same network segment with your video recorder are displayed in **Online Device List**.
2. Select a desired network camera.
3. Click **+** to add the camera.



Note

If the camera is inactive, the device will activate it automatically with the password you have set during device activation.

4. **Optional:** If your network camera is not on the same network segment with the DVR and supports ONVIF protocol, click **Advanced Search** and fill in the first three octets of the camera IP address to add the camera(s).

Add Network Camera Manually

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **Configuration → Camera → IP Camera**.
2. Click **+** in **Added Device List**.
3. Set network camera parameters, including IP address, protocol, management port, etc.
4. **Optional:** Double click **Camera Name** to edit name.



Note

Camera name can be edited only when the camera status is online.

5. **Optional:** Enable **Use Camera Activation Password** to use the device password to add network camera(s).
6. **Optional:** Click **Add More** to add another network camera.
7. Click **Add**.

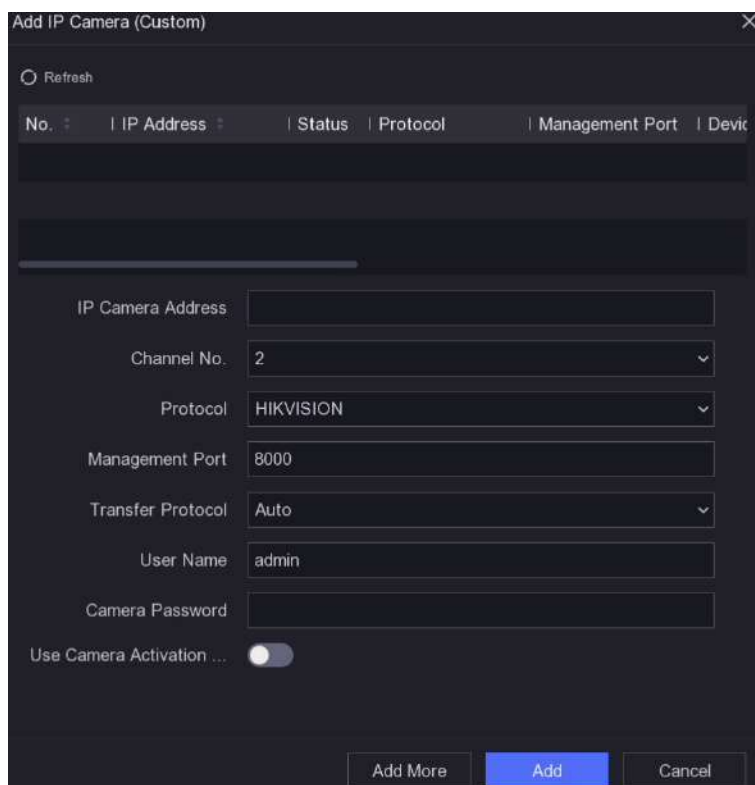


Figure 5-7 Add Network Camera

Edit Connected Network Camera

You can edit the IP address, protocol and other parameters of the added network cameras.

Steps

1. Go to **Configuration → Camera → IP Camera**.
2. Click  to edit the selected camera.

Channel Port

If the connected device is an encoding device with multiple channels, you can select the channel port No. to choose a connecting channel.

3. Click **OK**.

5.3.2 Motion

Motion enables the video recorder to detect the moving objects in the monitored area and trigger alarms.

Steps

1. Go to **Configuration → Camera → Motion**.
2. Select a camera.
3. Check **Enable**.
4. Set the motion area : Click **Draw Area** or **Clear** to draw or clear areas.



Note

The operation may differ according to different models.

5. Adjust **Sensitivity**. Sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion.
6. Set analysis mode as **AI** or **PIR**.

AI

The motion event will be analyzed by your device.

PIR

The motion event will be analyzed by certain analog PIR cameras.

7. **Optional:** Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle.
8. Set the arming schedule. Refer to **Configure Arming Schedule** for details.
9. Set the linkage actions. Refer to **Configure Alarm Linkage Action** for details.
10. Click **Apply**.

5.3.3 OSD Settings

Configure OSD (On-Screen Display) settings for the camera, including date format, camera name, etc.

Steps

1. Go to **Configuration → Camera → OSD**.
2. Select a camera.



Figure 5-8 OSD

3. Set parameters as your desire.
4. Drag the text frames on the preview window to adjust the OSD position.
5. Click **Apply**.

5.4 Configure Alarm Linkage Action

Alarm linkage actions will be activated when an alarm or exception occurs.

Steps

1. Click **Linkage Action**.

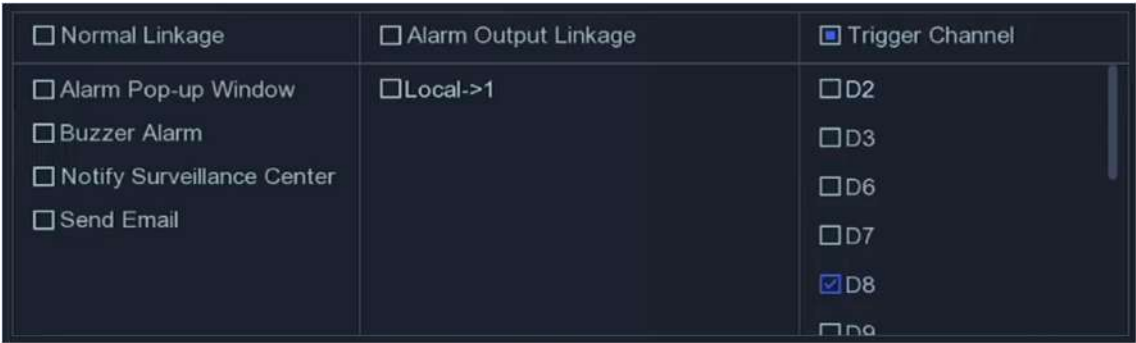


Figure 5-9 Linkage Actions

2. Set normal linkage actions, alarm output linkage actions, trigger channel, etc.

Alarm Pop-up Window

The local monitor will pop up the alarming channel image when an alarm is triggered. It requires to select the alarming channel(s) in **Trigger Channel**.

Buzzer Alarm

It will trigger a buzzer beep when an alarm is triggered.

Notify Surveillance Center

The device will send an exception or alarm signal to the remote client software when an alarm is triggered.

Send Email

It will send an email with alarm information when an alarm is triggered.

PTZ Linkage

It will trigger PTZ actions (e.g., call preset/patrol/pattern) when smart events occur.

Audio and Light Alarm Linkage

For certain network cameras, you can set the alarm linkage action as audio alarm or light alarm.



Note

- Ensure your camera supports audio and light alarm linkage.
- Ensure the audio output and volume are properly configured.
- If you require to set audio and light parameters, please log into the network camera via web browser to configure them.

3. Click **Apply**.

5.5 Configure Arming Schedule

Steps

1. Select **Arming Schedule**.

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



Note

Time periods shall not be repeated or overlapped.

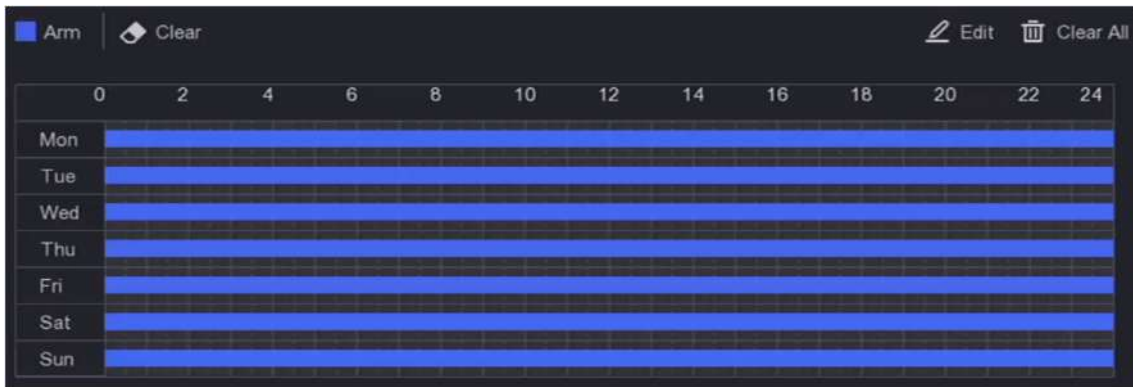


Figure 5-10 Set Arming Schedule

3. Click **Apply**.

5.6 Recording Management

5.6.1 Storage Device

Initialize HDD

A newly installed hard disk drive (HDD) must be initialized before it can be used to save videos and information.

Before You Start

Install at least an HDD to your video recorder. For detailed steps, refer to Quick Start Guide.

Steps

1. Go to **Configuration → Record → Storage**.
2. Select an HDD.
3. Click **Init**.

Repair Database

Repair an HDD that with error in database. Please operate it with the help of professional technical support.

Secure Erase

Secure Erase will delete videos in the selected disk(s).

Add Network Disk

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

Steps

1. Go to **Configuration → Record → Storage**.
2. Click **Add**.
3. Select **NetHDD**.
4. Set **Type** as **NAS** or **IP SAN**.
5. Enter **NetHDD IP** address.
6. Click  to search the available disks.

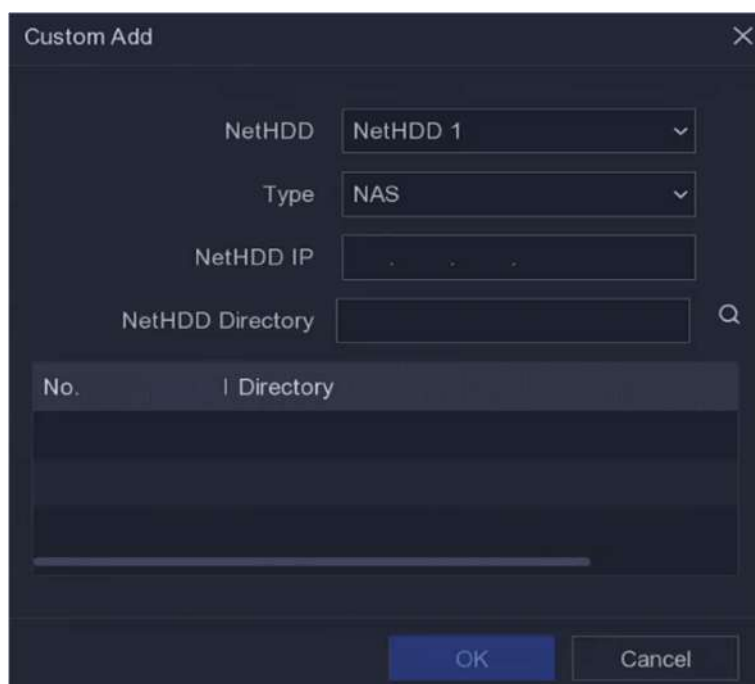


Figure 5-11 Add NetHDD

7. Select NAS disk from the list, or manually enter the directory in **NetHDD Directory**.
8. Click **OK**. The added NetHDD will be displayed in the storage device list.

5.6.2 Configure Recording Schedule

Video recorder will automatically start/stop recording according to the configured schedule.

Configure Continuous Recording

Steps

1. Go to **Configuration → Record → Parameter** .
2. Set the continuous main stream/sub-stream recording parameters for the camera. Refer to **Configure Recording Parameter** for details.
3. Go to **Configuration → Record → Schedule** .
4. Select recording type as **Continuous**. Refer to **Edit Schedule** for details.

Configure Event Recording

You can configure the recording triggered by the motion detection, line crossing detection, and intrusion detection.

Steps

1. Go to **Configuration → Event** .
2. Configure the event detection and select the channels to trigger the recording when an event occurs.
3. Go to **Configuration → Record → Parameter** .
4. Set the continuous main stream/sub-stream recording parameters for the camera. Refer to **Configure Recording Parameter** for details.
5. Go to **Configuration → Record → Schedule** .
6. Select recording type as **Event**. Refer to **Edit Schedule** for details.

Edit Schedule

Steps

1. Go to **Configuration → Record → Schedule** .



Figure 5-12 Recording Schedule

Continuous

Continuous recording.

Event

Recording is triggered by events.

- 2. Select a camera in **Camera No.**
- 3. Turn on **Enable**.
- 4. Configure the recording schedule.

Edit

Schedule

- a. Click **Edit**.
- b. Select a day to configure in **Weekday**.
- c. To set an all-day recording schedule, check **All Day** and select schedule type.
- d. To set other schedules, uncheck **All Day**, and set **Start/End Time** and schedule type.



Note

Up to 8 periods can be configured for each day. And the time periods cannot be overlapped with each other.

- e. Click **OK** to save the settings and go back to upper level menu.

Draw

Schedule

- a. Click to select schedule type as **Continuous** or **Event**.
- b. On the table, drag the mouse on the desired period to draw a colored bar.

- 5. Click **Apply**.

5.6.3 Configure Recording Parameter

Steps

- 1. Go to **Configuration → Record → Parameter** .

2. Configure recording parameters.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Frame Rate

Frame rate 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.



Note

Higher resolution, frame rate, and bitrate provide you better video quality, but it also requires more internet bandwidth and uses more storage space on the hard disk drive.

3. Click **Apply**.

Chapter 6 Configuration (Expert Mode)

Go to **Configuration** , and click **Expert Mode** at the lower-left corner.

6.1 System Configuration

6.1.1 General

Configure Basic Settings

You can configure the language, system time, output resolution, mouse pointer speed, lock screen password, etc.

Go to **Configuration** → **System** → **General** → **Basic Settings** , configure the parameters as your desire, and click **Apply**.

Language

The default language is **English**.

VGA/HDMI Resolution

Select the output resolution, which must be the same with the resolution of the VGA/HDMI display.

Video Quality Mode

The default mode is standard.

Local Auto Login

You can log in without password.

Mouse Pointer Speed

Set the speed of mouse pointer. 4 levels are configurable.

Wizard

The wizard will pop up after the device starts up.

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.

Go to **Configuration** → **System** → **General** → **DST Settings** , configure the parameters as your desire, and click **Apply**.

Configure More Settings

You can configure your device name, lock screen time, output mode, etc.

Go to **Configuration → System → General → More Settings**, configure the parameters as your desire, and click **Apply**.

Device Name

Edit the video recorder name.

Device No.

The number is required in the connection with remote control, network keyboard, etc. Edit the serial number of video recorder. The device number ranges from 1 to 255, and the default value is 255.

Lock Screen

Set timeout time for lock screen.

Menu Output Mode

Choose output to display local menu.

Enhanced IP Mode

Enabling enhanced IP mode will allow you to connect to the maximum number of cameras, but disable 2K/4K output resolution, and make perimeter protection, human or vehicle detection of motion, face capture and face picture comparison functions unavailable in analog channel.

6.1.2 Live View

Configure General Parameters

You can configure the output interface, mute or turning on the audio, event output interface, etc.

Steps

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

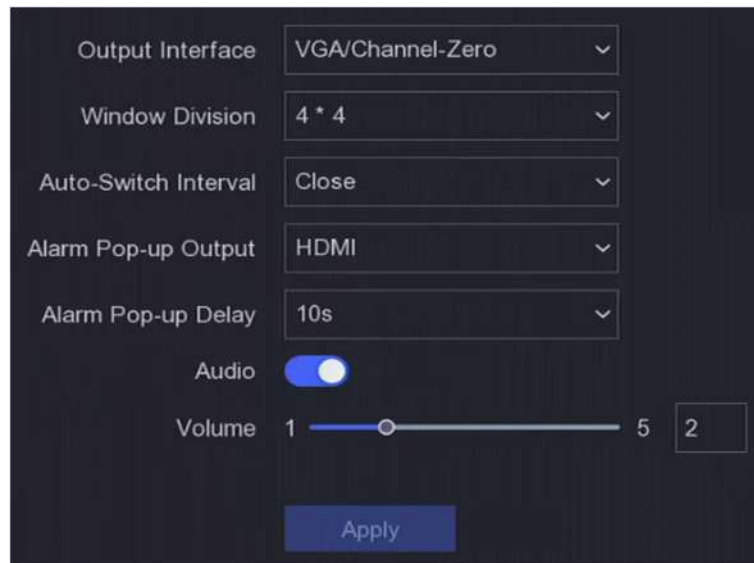


Figure 6-1 Live View-General

2. Configure the Live View parameters.

Window Division

Select the live view window division.

Auto Switch Interval

The time to dwell in a camera before switching to next camera when auto-switch in live view is enabled.

Alarm Pop-up Output

Select the output to show alarm video.

Alarm Pop-up Delay

Set the time to show alarm event image.

Audio

Turn on/off audio output for the selected video output.

Volume

Adjust the live view, playback, and two-way audio volume for the selected video output interface.

3. Click **Apply**.

Configure Live View Layout

Steps

1. Go to **Configuration → System → Live View → View**.
2. Set **Output Interface**.

3. Select a window, and double click a camera the list you would like to display. + means no camera is displayed on the window.
4. **Optional:** Click  or  to start or stop live view of all cameras.
5. Click **Apply**.

Configure Channel-Zero Encoding

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

Steps

1. Go to **Configuration → System → Live View → Channel-Zero** .

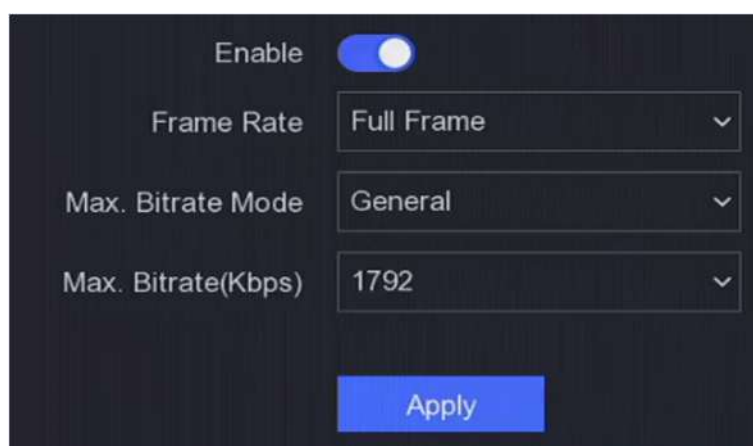


Figure 6-2 Channel-Zero

2. Turn on **Enable**.
3. Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**. The higher frame rate and bitrate require higher bandwidth requirement.
4. Click **Apply**.

6.1.3 User

Refer to [User](#) for details.

6.2 Network Configuration

6.2.1 TCP/IP

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

Steps

1. Go to **Configuration → Network → General → TCP/IP**.
2. Configure network parameters.

Working Mode

Multi-address Mode

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

Net-fault Tolerance Mode

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

Load Balance Mode

By using the same IP address and two NIC cards share the load of the total bandwidth, which enables the system to provide two Gigabit network capacity.



Note

Working mode is only available for certain models.

NIC Type

Select NIC type as your desire. If your device supports Wi-Fi dongle function, the NIC of Wi-Fi dongle would be selectable after a suitable Wi-Fi dongle is installed.

DHCP

If the DHCP server is available, you can check **Enable DHCP** to automatically obtain an IP address and other network settings from that server.

MTU

The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

Default Route

Select a route as your desire. If your device supports Wi-Fi dongle function, the route of Wi-Fi dongle would be selectable after a suitable Wi-Fi dongle is installed.

Auto Obtain DNS

If **DHCP** is checked. You can check **Obtain DNS Automatically** to obtain **Preferred DNS Server** and **Alternate DNS Server**.

3. Click **Apply**.

6.2.2 DDNS

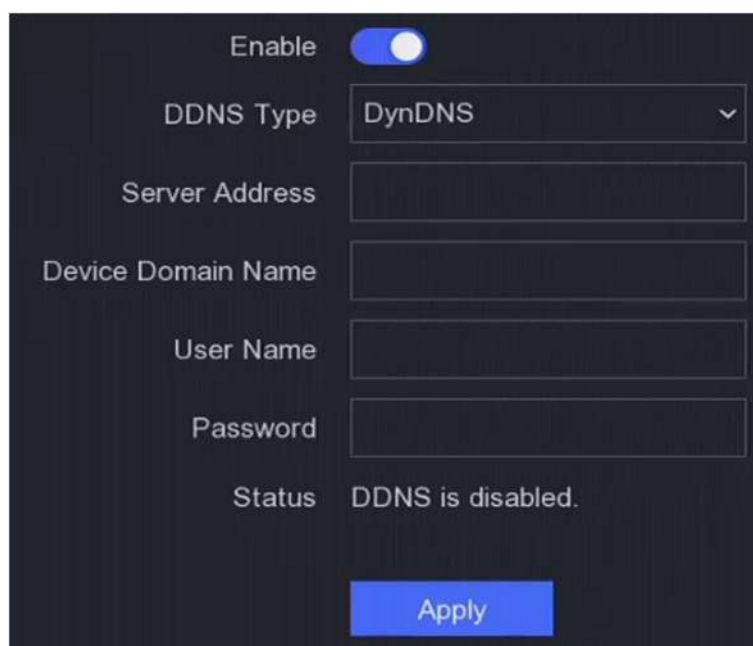
Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Register DynDNS, PeanutHull and NO-IP services with your ISP.

Steps

1. Go to **Configuration → Network → General → DDNS**.



Enable ☒

DDNS Type DynDNS ▼

Server Address

Device Domain Name

User Name

Password

Status DDNS is disabled.

Apply

Figure 6-3 DDNS

2. Turn on **Enable**.
3. Select a DDNS type.
4. Enter parameters including service address, domain name, etc.
5. Click **Apply**.

What to do next

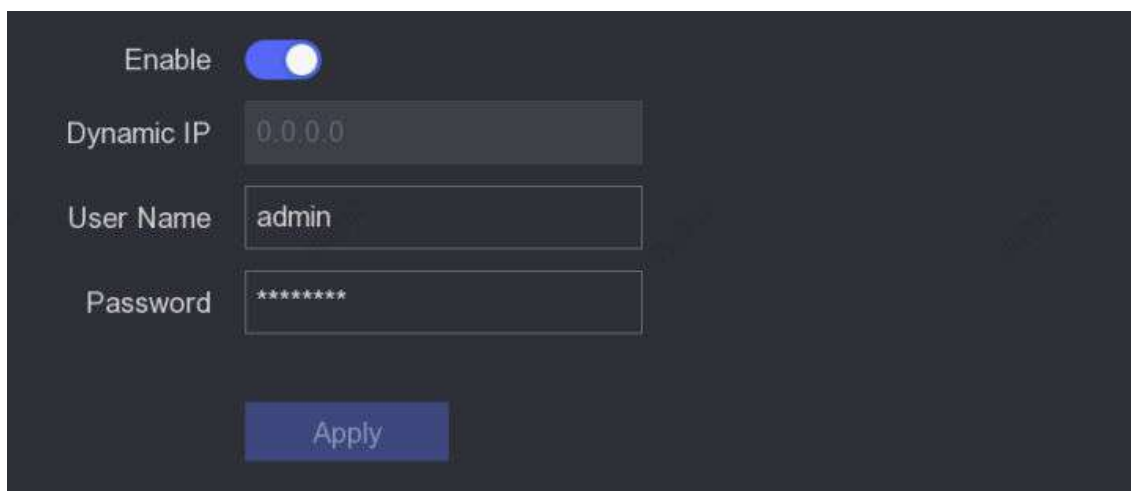
You can view DDNS status in **Status**.

6.2.3 PPPOE

If the device is going to connect to Internet through PPPOE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPOE service.

Steps

1. Go to **Network → General → PPPOE**.



Enable ☒

Dynamic IP

User Name

Password

Figure 6-4 PPPOE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

If you can get the dynamic IP, the PPPOE status is normal.

6.2.4 NAT

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

Before You Start

Enable the UPnP™ function of your router if UPnP™ is required. When the device network working mode is multi-address, the default device route should be on the same network segment as the LAN IP address of the router.

Steps

1. Go to **Configuration → Network → General → NAT**.

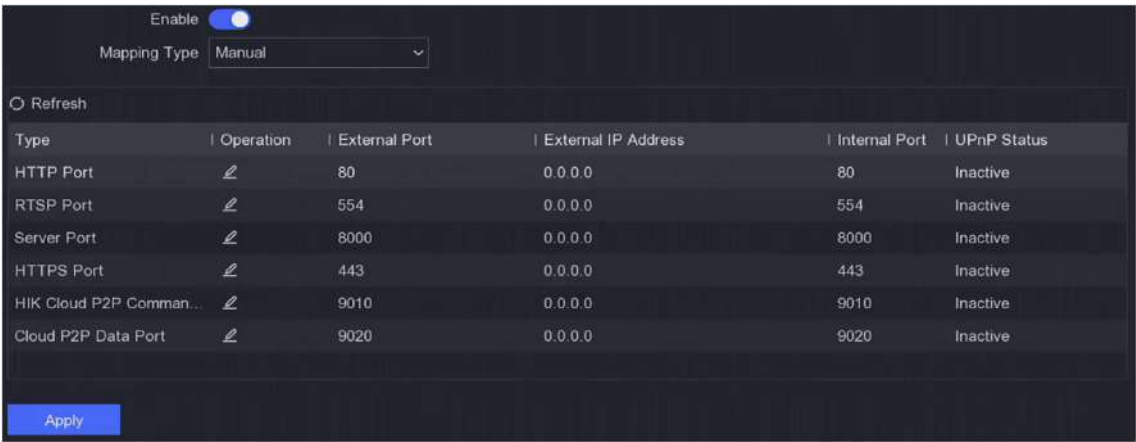


Figure 6-5 NAT

- 2. Turn on **Enable**.
- 3. Select **Mapping Type** as **Manual** or **Auto**
 - Auto** The port mapping items are read-only, and the external ports are set by the router automatically. You can click **Refresh** to get the latest status of the port mapping.
 - Manual** Select an external port type. Click to edit **External Port**. You can use the default external port No., or change it according to actual requirements. **External Port** indicates the port No. for port mapping in the router.

The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.
- 4. Set the virtual server of your router, including internal source port, external source port, etc. The virtual server parameters shall be corresponding with your device port.

6.2.5 Wi-Fi

For certain models, after installing a Wi-Fi dongle to your device, the device would be able to connect to a wireless network, and the channels in your device can be viewed thorough Wi-Fi. For example, if your device is connected with several network cameras or analog cameras (Wi-Fi network cameras currently cannot be connected), after the device is connected to a wireless network, you would be able to access your device and view the connected channels through Wi-Fi.

Before You Start

- Prepare a suitable Wi-Fi dongle, and insert it in to the USB interface at the rear panel.
- Ensure your device support this function.

Steps

- 1. Go to **Configuration → Network → General → Wi-Fi** .



Note

The Wi-Fi setting interface will automatically pop up when you insert the Wi-Fi dongle for the first time.

2. Connect to a wireless network.

Connect to an Automatically Searched Wireless Network

- a. Double click the wireless network from the list as you desired.
- b. Set wireless network parameters.
- c. Click **OK**.

Connect to a Customized Wireless Network

- a. Click **Custom Adding**.
- b. Set wireless network parameters.
- c. Click **OK**.

Connect to a Wireless Network with WPS (Wi-Fi Protected Setup)

- a. Click **WPS Settings**.
 - b. Check **Enable WPS**.
 - c. Set wireless network parameters.
 - d. Click **Apply**.
-



Note

If you requires to edit or forget the network, double click the connected network, and edit it as your desire.

After connecting to an available wireless network, you can view the connection result in **Connection Status**.

3. Go to **Configuration → Network → General → TCP/IP**.
4. Set **Select NIC** and **Default Route** as **WLAN0**.
5. Check **Enable Wi-Fi**.
6. Set other network parameters.
7. Click **Apply**.

6.2.6 NTP

Your device can connect to a network time protocol (NTP) server to ensure that the system time is accurate.

Steps

1. Go to **Configuration → Network → General → NTP**.
2. Turn on **Enable**.
3. Enter the parameters.

Interval

Time interval between two time synchronization with NTP server.

NTP Server

IP address of the NTP server.

4. Click **Apply**.

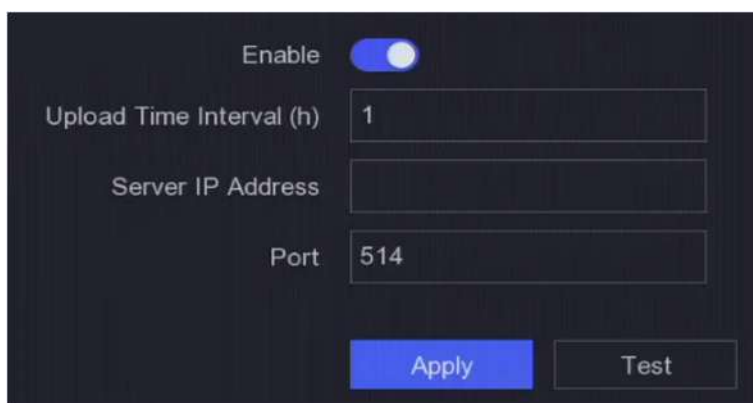
6.2.7 Log Server Settings

Upload Logs to the Server

You can upload system logs to the server for backup.

Steps

1. Go to **Configuration → Network → General → Log Server Settings** .



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

Figure 6-6 Log Server Settings

2. Turn on **Enable**

3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.

4. **Optional:** Click **Test** to test if parameters are valid.

5. Click **Apply**.

One-Way Authentication

You can install a CA certificate (from the server) to your device to authorize the server via web browser. It would improve the log communication security.

Before You Start

- Download the CA certificate from the server.
- Ensure log server parameters are valid.

Steps

1. Go to **Configuration → Network → Advanced Settings → Log Server Configuration** .

The screenshot shows a web interface for configuring log server settings. At the top, there is a checkbox labeled 'Enable' which is checked. Below it are three input fields: 'Log Server Address' containing '192.168.1.100', 'Log Server Port' containing '8080', and 'Upload Time Interval (h)' containing '1'. A 'Test' button is positioned below these fields. The 'Client Certificate' section includes a 'Create Certificate Request' button (labeled 'Create') with a 'No file.' status, a 'Download Certificate Request' button (labeled 'Download'), and a 'Delete Certificate Request' button (labeled 'Delete'). Below these is an 'Install Generated Certificate' section with a file input field, a 'Browse' button, and an 'Install' button. The 'CA Certificate' section has an 'Install' label, a file input field, a 'Browse' button, and an 'Install' button. At the bottom left is a large red 'Save' button with a floppy disk icon.

Figure 6-7 One-Way Authentication

2. Install the CA certificate in **CA Certificate**.
3. **Optional:** Click **Test** to test if the connection is valid.
4. Click **Save**.

Two-Way Authentication

You can install a CA certificate (from the server) to your device to authorize the server, and create a certificate (from your device) to authorize your device by the server. This would improve the log communication security. Two-way authentication can be configured via web browser.

Before You Start

- Download the CA certificate from the server.
- Ensure log server parameters are valid.

Steps

1. Go to **Configuration → Network → Advanced Settings → Log Server Configuration**.

The screenshot shows a web-based configuration interface for Two-Way Authentication. At the top, there is a checkbox labeled 'Enable' which is checked. Below it are three input fields: 'Log Server Address' with the value '192.168.1.100', 'Log Server Port' with the value '8080', and 'Upload Time Interval (h)' with the value '1'. A 'Test' button is located below these fields. The 'Client Certificate' section contains four buttons: 'Create' (with a 'No file.' status), 'Download', 'Delete', and 'Install Generated Certificate' (with a 'Browse' button next to it). The 'CA Certificate' section contains an 'Install' button (with a 'Browse' button next to it). A large red 'Save' button is at the bottom left.

Figure 6-8 Two-Way Authentication

2. Install the CA certificate in **CA Certificate**.
3. Click **Create** in **Client Certificate**, and follow the pop-up to create the certificate.
4. Click **Download** to download the certificate file to a desired location.
5. Upload the downloaded certificate file to the server, and the server will return the certificate key.
6. Open the certificate as a text file, and modify it by the certificate key as the server returned.
7. Install the modified certificate in **Client Certificate**.
8. **Optional:** Click **Test** to test if the connection is valid.
9. Click **Save**.

6.2.8 Ports (More Settings)

Set different port types to enable relevant functions as your desire.

Go to **Configuration → Network → General → More Settings**.

Alarm Host IP/Port

The device will send the alarm event or exception message to the alarm 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

For remote client software access. Ranges from 2000 to 65535. The default value is 8000.

HTTP Port

For remote web browser access. The default value is 80.

Multicast IP

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

When adding a device to the CMS software, the multicast address must be the same as that of the device.

RTSP Port

RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The port is 554 by default.

Output Bandwidth Limit

You can check the checkbox to enable output bandwidth limit.

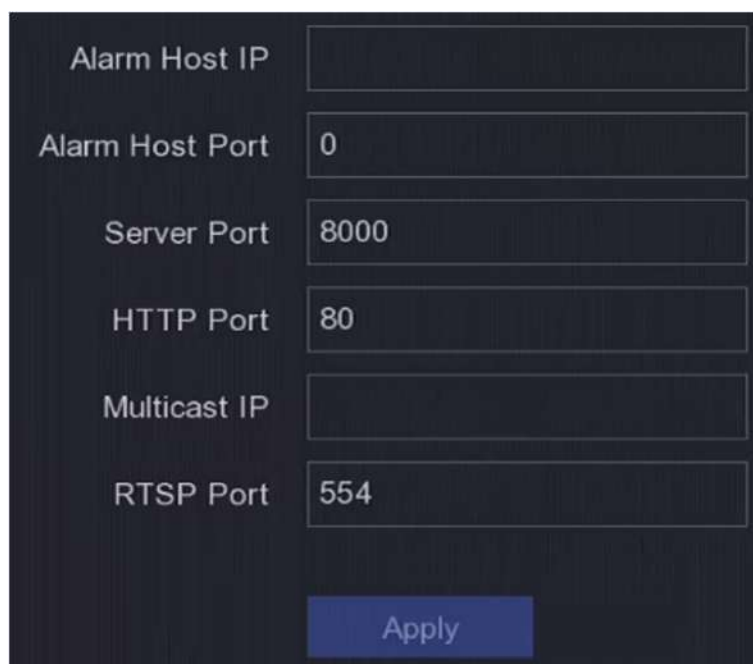
Output Bandwidth

After enable the output bandwidth limit, input the output bandwidth.



Note

- The output bandwidth limit is used for the remote live view and playback.
 - The default output bandwidth is the maximum limit.
-



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

Figure 6-9 Port Settings

6.2.9 Hik-Connect

Go to **Configuration → Network → Platform Access** . Refer to [**Hik-Connect**](#) for details.

6.2.10 Email

Go to **Configuration → Network → Email** . Refer to [**Email**](#) for details.

6.3 Camera Management

6.3.1 Configure Signal Input

For certain digital video recorder models, you can configure the analog and IP signal input types.

Steps

1. Go to **Configuration → Camera → Analog** , or click **Edit** at the upper-right corner in **Configuration → Camera → Camera** .
2. Select signal input type as **HD/CVBS** or **IP**.
HD/CVBS

Four types of analog signal inputs including Turbo HD, AHD, HDCVI, and CVBS can be connected randomly for the channel.

IP

Network camera can be connected for the channel.

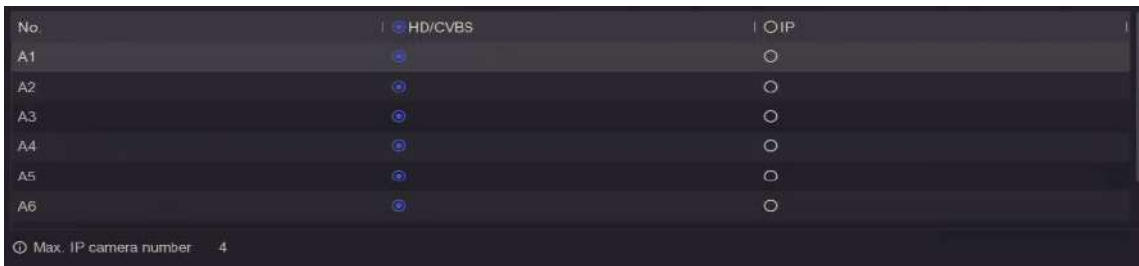


Figure 6-10 Signal Input Type

3. Click **Apply**. You can view the maximum network camera accessible number in **Max. IP Camera Number**.

6.3.2 Network Camera

Add Automatically Searched Online Network Camera

Add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera password is the same as your video recorder.

Steps

1. Go to **Configuration → Camera → Camera**.
2. Click **Online Device List**. The online cameras on the same network segment will be displayed in the list.

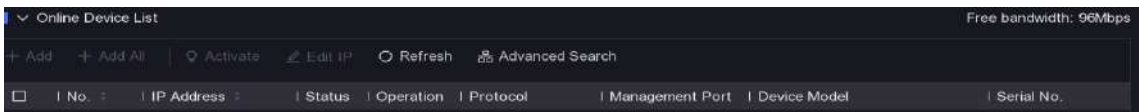


Figure 6-11 Online Device

3. **Optional:** Click **Edit IP** to edit camera IP addresses in batch. The system will allocate IP addresses to the selected cameras in order.

 Note

- Ensure the selected cameras are activated.
- When the network camera is online, you can double click camera name to edit it.

4. Select a network camera, and click **Add** to add it.

Add Network Camera Manually

Add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **Configuration → Camera → Camera** .
2. Click  .

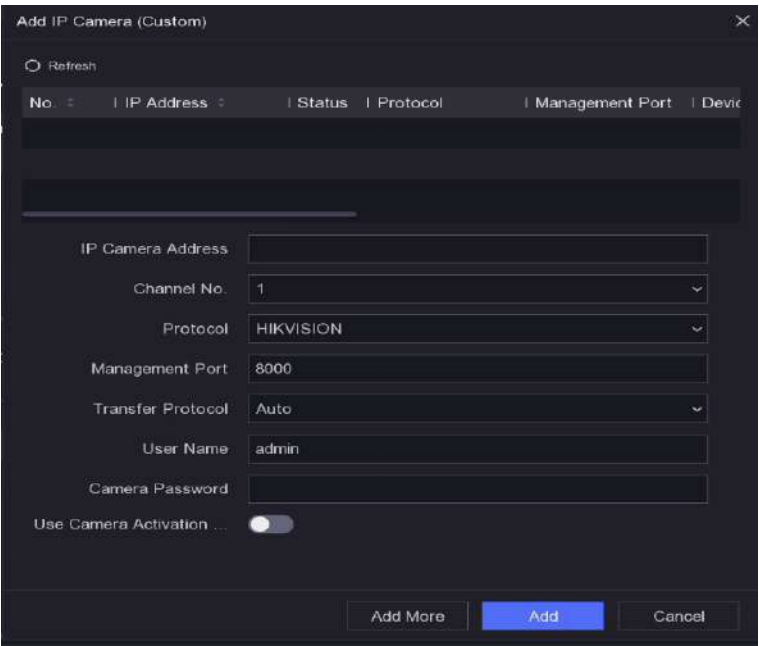


Figure 6-12 Add IP Camera

3. Enter network camera parameters.

Use Camera Activation Password

If it is enabled, the video recorder will add the camera by the set channel default password.

4. Click **Add**.

Add Network Camera on Different Network Segment

If your network camera is on a different network segment, the device can search its IP address within a range of IP addresses, and add it.

Before You Start

- Ensure the network connection is valid and correct.
- Ensure the network camera password is the same as your video recorder.

Steps

1. Go to **Configuration → Camera → Camera → IP Channel**.
2. Click **Advanced Search**.
3. Enter **Network Segment**.

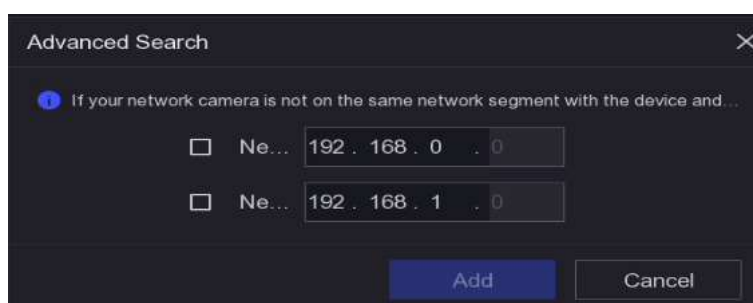


Figure 6-13 Enter Network Segment

4. Click **Add**.

Add Network Camera Through Plug-and-Play

If an inactive network camera or third party ONVIF camera is connected to your network, the video recorder may automatically detect and add the camera, or notify you to manually add it.

Steps

1. Go to **Configuration → Camera → Camera → IP Channel**.
2. Click **More**.
3. Select **Plug-and-Play**.
4. **Optional:** Enable **Auto Add Network Camera**. The video recorder would automatically detect and add the inactive network camera or third party ONVIF camera.

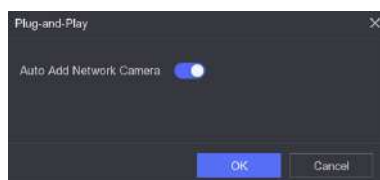


Figure 6-14 Auto Add Network Camera



Note

If you turn off **Auto Add Network Camera**, when an inactive network camera or third party ONVIF camera is connected to your network, the video recorder would automatically detect it and notify you to add it.

Edit Network Camera

You can edit the IP address, protocol and other parameters of network cameras.

Steps

1. Go to **Configuration → Camera → Camera**.
2. Click  of an added network camera.

Channel Port

If the connected device is an encoding device with multiple channels, you can choose the channel to connect by selecting the channel port No. in the drop-down list.

3. **Optional:** Click **Edit IP** to edit camera IP addresses in batch. The system will allocate IP addresses to the selected cameras in order.
4. Click **OK**.

Upgrade Network Camera

The Network camera can be remotely upgraded through the device.

Before You Start

- Ensure you have inserted the USB flash drive to the device, and it contains the network camera upgrade firmware.
- Ensure your network camera is on the same network segment with your video recorder.
- Ensure the network connection is valid and correct.

Steps

1. Go to **Configuration → Camera → Camera**.
2. Click .
3. Click **Yes** to confirm.
4. Select the camera upgrade firmware from your storage device.
5. Click **Upgrade** to start upgrading. The camera will restarted automatically after upgrade completed.

Configure Advanced Camera Parameters

You can configure advanced camera parameters like camera IP address, camera password, etc.

Before You Start

- Ensure your network camera is on the same network segment with your video recorder.
- Ensure the network connection is valid and correct.

Steps

1. Go to **Configuration → Camera → Camera** .
2. Click  .
3. Set camera parameters like IP address, camera password, etc.
4. Click **Apply**.

Import/Export IP Camera Configuration File

The information of added network camera can be generated into an excel file and exported to the local device for backup, including the IP address, port, password of admin, etc. And the exported file can be edited on your computer, like adding or deleting the content, and copy the setting to other devices by importing the excel file to it.

Before You Start

Connect a backup device, such as a USB flash drive, to your video recorder.

Steps

1. Go to **Configuration → Camera → Camera** .
2. Click **More**.
3. Click **Export/Import** to export/import configuration files to the connected backup device.
4. Set the storage device and folder path.
5. Click **Export/Import**.

What to do next

After the importing process is completed, you must restart the video recorder.

Advanced Settings

Steps

1. Go to **Configuration → Camera → Camera** .
2. Click **More**.
3. Configure the parameters as your desire.

H.265 Auto Switch Configuration

If you enable the option, the device will automatically switch to H.265 stream for the network camera (which supports H.265 video format) for the initial access.

Upgrade

Upgrade the added network cameras.

Export/Import

The information of added network camera can be generated into an excel file and exported to the local device for backup, including the IP address, port, password of admin, etc. And the exported file can be edited on your computer, like adding or deleting the content, and copying the settings to other devices by importing the excel file to it.

Protocol

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

Camera Activation Password Settings

Change the default password for activating and adding network cameras. For network cameras that are already connected, you can choose to change their passwords to this one in the following pup-up window.

Batch Configuration

The device can enable SVC function or automatically synchronize time of the selected network cameras.

Plug-and-Play

The device can add network camera automatically.

6.3.3 Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Steps

1. Go to **Configuration → Camera → Display**.
2. Set **Camera**.
3. Configure parameters as your desire.

OSD Settings

Configure the OSD (On-screen Display) settings for the camera, including date, time, camera name, etc.

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

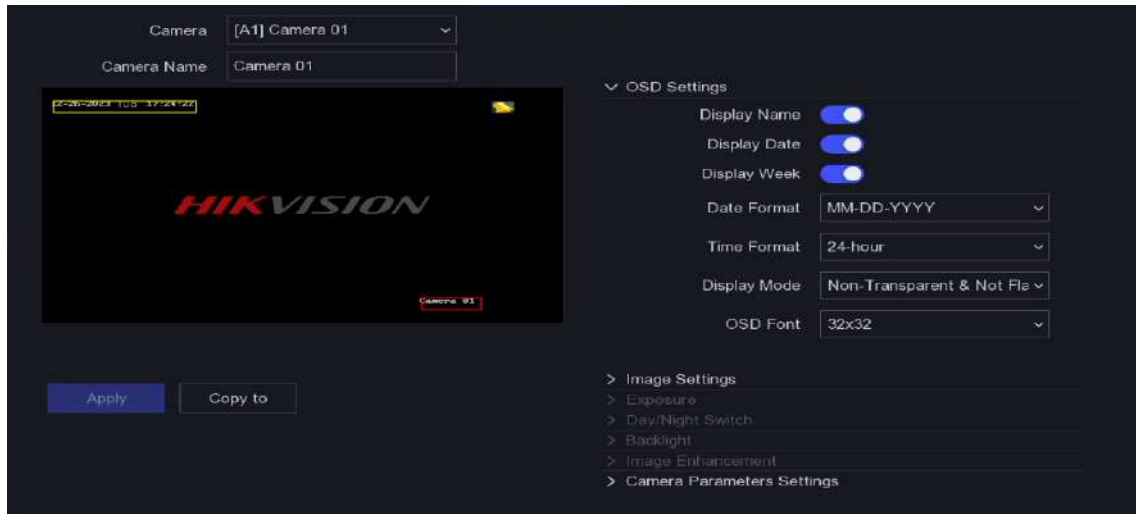


Figure 6-15 OSD

4. Drag the text frames on the preview window to adjust the OSD position.
5. Click **Apply**.

6.3.4 Privacy Mask

You are allowed to configure the privacy mask areas that cannot be viewed or recorded.

Steps

1. Go to **Configuration → Camera → Privacy Mask**.
2. Select **Camera**.
3. Turn on **Enable**.

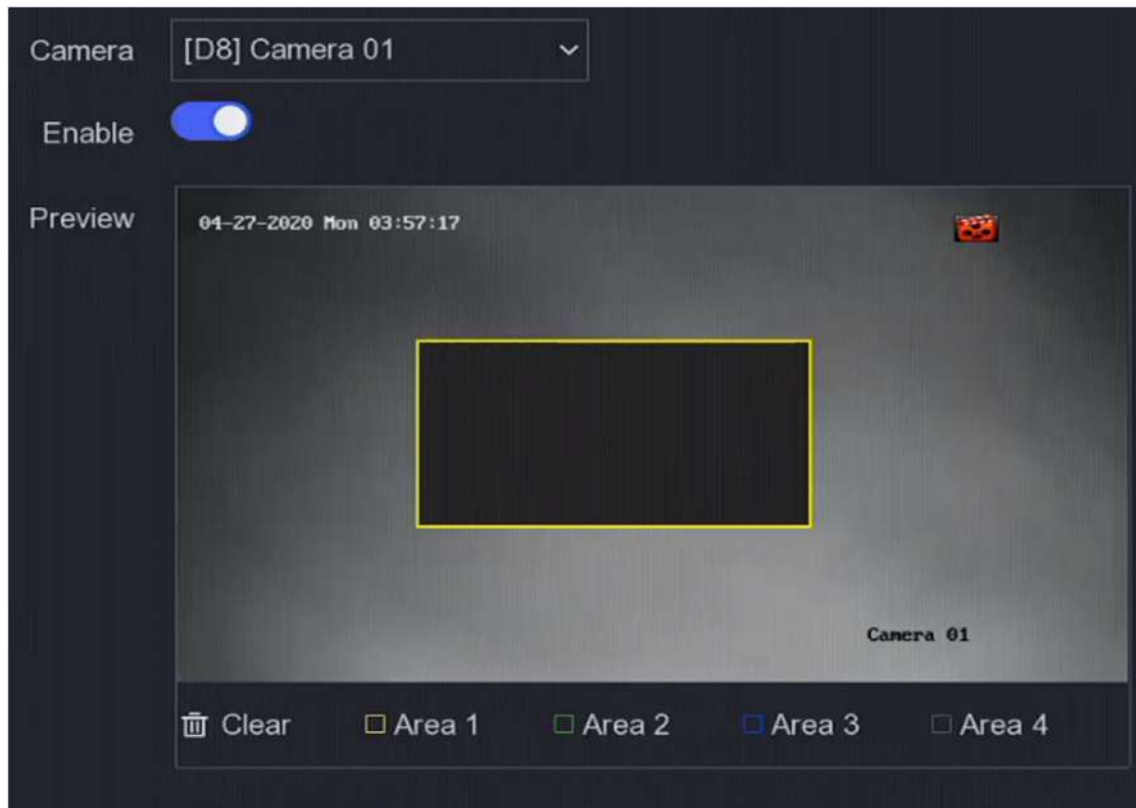


Figure 6-16 Privacy Mask

4. Drag to draw an area on the window. The frames of the areas will be marked with different colors.



Note

Up to 4 privacy mask areas can be configured. The size of each area can be adjusted.

5. Click **Apply**.

6.4 Event Configuration

6.4.1 Normal Event

Motion Detection

Motion detection enables the video recorder to detect the moving objects in the monitored area and trigger alarms. Refer to for details.

Video Tampering

Trigger alarm when the lens is covered and take alarm response actions.

Steps

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

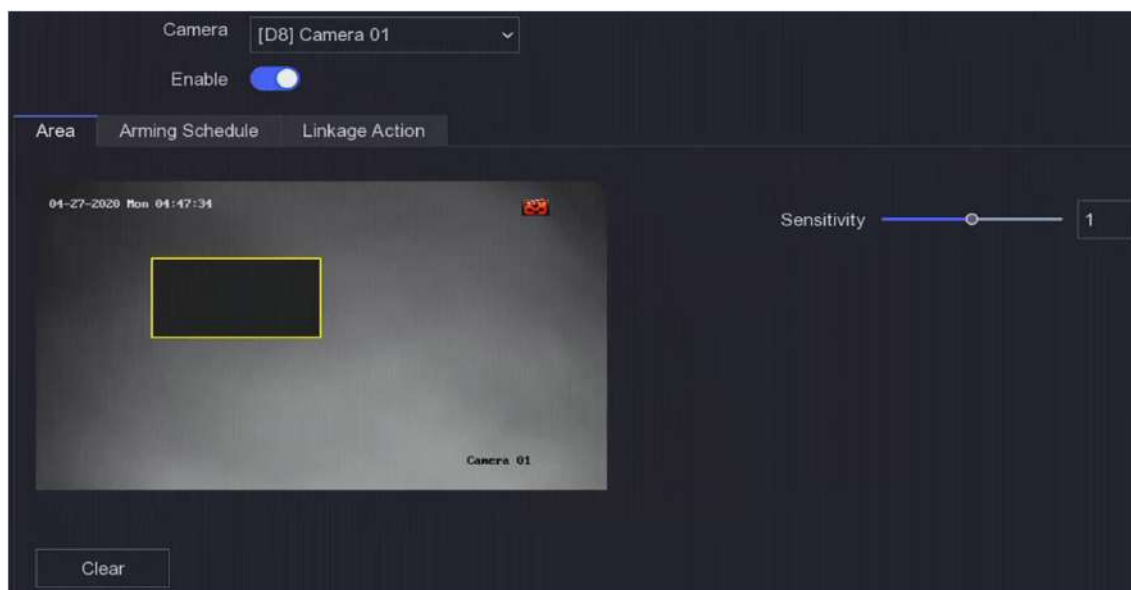


Figure 6-17 Video Tampering

2. Set **Camera**.
3. Turn on **Enable**.
4. Adjust **Sensitivity** as your desire. The higher the value is, the more easily the video tampering can be triggered.
5. Set the arming schedule. Refer to [Configure Arming Schedule](#) for details.
6. Set the linkage actions. Refer to [Configure Alarm Linkage Action](#) for details.
7. Click **Apply**.

Video Loss

Detect video loss of a camera and take alarm response actions.

Steps

1. Go to **Configuration → Event → Normal Event → Video Loss**.
2. Set **Camera**.
3. Turn on **Enable**.
4. Set the arming schedule. Refer to [Configure Arming Schedule](#) for details.
5. Set the linkage actions. Refer to [Configure Alarm Linkage Action](#) for details.
6. Click **Apply**.

Alarm Input

Set linkage actions for an external sensor alarm.

Steps

1. Go to **Configuration → Event → Normal Event → Alarm Input** .

Alarm Input No.	Alarm Name	Alarm Type	Enable	Operation
Local<-1		N.O	No	
Local<-2		N.O	No	
Local<-3		N.O	No	
Local<-4		N.O	No	

Figure 6-18 Alarm Input



Note

Local alarm input: Local alarm input is triggered by the external device that connected to the video recorder's terminal block.

2. Click of a desired alarm input.

Figure 6-19 Edit Alarm Input

3. Customize **Alarm Name**.
4. Set alarm type as **N.O** (normally open) or **N.C** (normally closed).
5. Set **Settings** as **Input** to enable the function.



Note

If you set **Settings** as **Nonuse**, the alarm input will be disabled. If you set **Settings** as **One-Key Disarming**, the selected linkage method(s) of the alarm input will be disabled.

6. Set the arming schedule. Refer to [**Configure Arming Schedule**](#) for details.
7. Set the linkage actions. Refer to [**Configure Alarm Linkage Action**](#) for details.
8. Click **Apply**.

Alarm Output

Trigger an alarm output when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Normal Event → Alarm Output** .

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

Figure 6-20 Alarm Output

- 2. Click  of a desired alarm output.
- 3. Customize **Alarm Name**.
- 4. Select **Dwell Time**.

Alarm Output No. Local->1

Dwell Time 5s

Alarm Name

Alarm Status Close

Arming Schedule

Continuous

Clear

Edit

Clear All

024681012141618202224

Mon

Tue

Wed

Thu

Fri

Sat

Sun

Copy to

Trigger

Apply

Figure 6-21 Edit Alarm Output

- 5. Set **Settings** as **Input** to enable the function.
- 6. Set the arming schedule. Refer to Configure Arming Schedule for details.
- 7. Click **Apply**.

Exception

Exception events can be configured to take the event hint in the live view window and trigger alarm outputs and linkage actions.

Steps

- 1. Go to **Configuration → Event → Normal Event → Exception** .
- 2. Configure event hint. When the set events occur, you will receive hints in alarm center.
 - 1) Enable **Event Hint**.
 - 2) Select events to hint. Choose from:
 - Click  of **Event Hint Configuration** to select events.
 - Click  in the upper-right corner of local menu to enter alarm center to select events.
- 3. Select **Exception Type** to set its linkage actions.

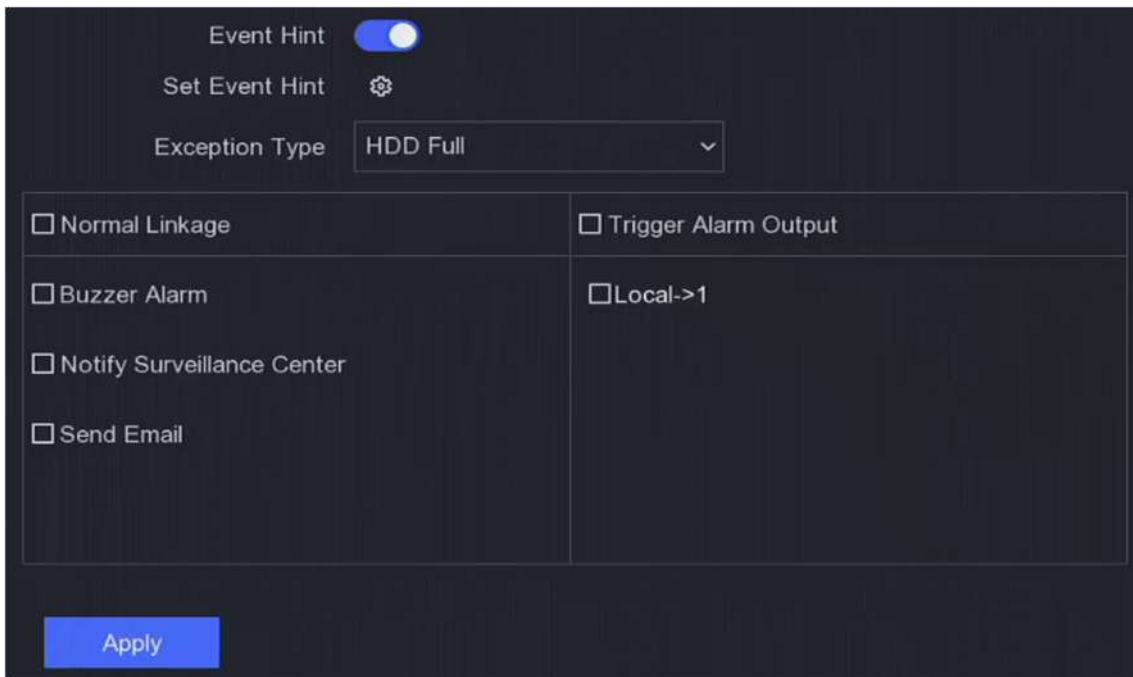


Figure 6-22 Exceptions

4. Set the arming schedule. Refer to [***Configure Arming Schedule***](#) for details.
5. Click **Apply**.

6.4.2 Perimeter Protection

Perimeter protection includes line crossing detection, intrusion detection, region entrance detection, and region exiting detection.



Note

Perimeter protection is only available for certain device models or camera models.

Line Crossing Detection

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

Steps

1. Go to **Configuration → Event → Perimeter Protection → Line Crossing**.
2. Set **Camera**.
3. Turn on **Enable**.
4. Set the detection rules and detection areas.
 - 1) Set **Arming Area**.

2) Set **Direction** as **A<->B**, **A->B**, or **A<-B**.

A<->B

Only the arrow on the B side shows. An object crossing a configured line in both directions can be detected and trigger alarms.

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) Click **Max. Size** and draw a quadrilateral in the preview window to set the maximum draw area size of the target.

4) Click **Min. Size** and draw a quadrilateral in the preview window to set the minimum draw area size of the target.

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

5. Adjust **Sensitivity**. Sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.

6. **Optional**: Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle.



Note

This function is only available for certain models.

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

8. Set the linkage actions. Refer to ***Configure Alarm Linkage Action*** for details.

9. Click **Apply**.

Intrusion Detection

Intrusion detection function detects people, vehicles, or objects that enter and loiter in a pre-defined virtual region.

Steps

1. Go to **Configuration → Event → Perimeter Protection → Intrusion**.

2. Select **Camera** to configure.

3. Turn on **Enable**.

4. Set the detection rules and detection areas.

1) Select **Arming Area**.

2) Adjust **Time Threshold** and **Sensitivity**.

Sensitivity

The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm will be triggered. Its range is [1-100].

Time Threshold

Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.

- 3) **Optional:** Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.



Note

This function is only available for certain models.

- 4) Click **Max. Size** and draw a quadrilateral in the preview window to set the maximum draw area size of the target.
 - 5) Click **Min. Size** and draw a quadrilateral in the preview window to set the minimum draw area size of the target.
 - 6) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
5. Set the arming schedule. Refer to [**Configure Arming Schedule**](#) for details.
 6. Set the linkage actions. Refer to [**Configure Alarm Linkage Action**](#) for details.
 7. Click **Apply**.

Region Entrance Detection

For certain network cameras, region entrance detection function detects people, vehicles or other objects which enter a pre-defined virtual region from the outside place, and some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Smart Event → Region Entrance**.
2. Set **Camera**.
3. Turn on **Enable**.
4. **Optional:** Check **Save VCA Picture** to save the captured pictures of VCA detection.
5. Set the detection rules and detection areas.
 - 1) Set **Arming Area**. Up to 4 arming areas are selectable.
 - 2) Adjust **Sensitivity**. **Sensitivity**: Range [0-100]. The higher the value is, the more easily the detection alarm can be triggered.
 - 3) **Optional:** Set **Target Detection** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.



Note

This function is only available for certain models.

- 4) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
6. Set the arming schedule. Refer to [**Configure Arming Schedule**](#) for details.
 7. Set the linkage actions. Refer to [**Configure Alarm Linkage Action**](#) for details.
 8. Click **Apply**.

Region Exiting Detection

For certain network cameras, region exiting detection function detects people, vehicles or other objects which exit from a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Smart Event → Region Exiting**.
2. Set **Camera**.
3. Turn on **Enable**.
4. **Optional**: Check **Save VCA Picture** to save the captured pictures of VCA detection.
5. Set the detection rules and detection areas.
 - 1) Set **Arming Area**. Up to 4 arming areas are selectable.
 - 2) Adjust **Sensitivity**. **Sensitivity**: Range [0-100]. The higher the value is, the more easily the detection alarm can be triggered.
 - 3) **Optional**: Set **Target Detection** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.



Note

This function is only available for certain models.

- 4) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.
6. Set the arming schedule. Refer to **Configure Arming Schedule** for details.
7. Set the linkage actions. Refer to **Configure Alarm Linkage Action** for details.
8. Click **Apply**.

6.4.3 Face Recognition

Face recognition is the function that compares a captured face (in image or video stream) with those in face picture libraries and returns its identity information if the face is recognized. Based on facial feature of human being, face recognition first checks if human face exists in the input image or video stream. If there is a human face, the function compares the face data (such as position, size, and facial feature) with those in current face picture libraries to identify the person.

Before You Start

Make sure you have configured related parameters on Hik Central Professional or Hik Connect and disabled **Motion** and **Perimeter Protection**.



Note

This function is only available for certain models.

Face Capture

Face capture detects human faces appearing in the scene. Linkage actions can be triggered when a human face is detected.

Steps

1. Go to **Configuration → Event → Face Recognition → Face Capture**.



Figure 6-23 Face Capture

2. Select **Camera**.
3. Turn on **Enable**.
4. Adjust **Sensitivity**.

Sensitivity

The higher the value is, the more easily the defocus image can trigger the alarm.

5. Set the arming schedule. Refer to **Configure Arming Schedule** for details.
6. Set the linkage actions. Refer to **Configure Alarm Linkage Action** for details.
7. Click **Apply**.

Face Picture Library Management

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

Note

The section is only available for certain models.

Add a Face Picture Library

Face picture library is used to store face pictures, it is essential for face picture comparison.

Steps

1. Go to **Configuration → Face Picture Library**.
2. Enter the admin password for authorization.
3. Click **Add**.
4. Enter the face picture library name.
5. Click **Add**.



Note

You can also go to **Search → Human** to add the search results to the **Face Picture Library**.

What to do next

After a face picture library is added, you can edit its name, delete it, or upload face pictures to it.

Upload Face Pictures to the Library

You can upload a single face picture or import multiple face pictures to the library.

Before You Start

Ensure you have created a face picture library and enabled face picture comparison.

Steps

1. Go to **Configuration → Face Picture Library**.
2. Find the face picture library that you are going to upload face pictures, and click .
3. Click **Add**.
4. Import picture(s).



Add one face picture to the library.



Add multiple face pictures to the library.



Note

- Only JPG and JPEG formats are supported.
 - Each picture size should be less than 1 MB.
 - The picture resolution shall be between 80 × 80 and 1920 × 1080.
 - Only the pictures in the USB flash drive can be imported.
-

Face Picture Comparison

Face picture comparison compares the detected face pictures with face pictures in the face picture library. The device will trigger an alarm when comparison succeeded.

Before You Start

Ensure you have created at least one face picture library, and face pictures are added to the library. Refer to **Face Picture Library Management** for operation details.

Steps

1. Go to **Configuration → Face Recognition → Face Picture Comparison** .



Figure 6-24 Face Picture Comparison

2. Select a camera.
3. Turn on **Enable**.
4. Select the face picture library (or libraries) in **List Library Linkage**.
5. Set the face picture library similarity.

Similarity

Similarity value ranges from 0 to 100. Device will analyze the similarity between the detected face picture and face pictures in the library. When the similarity reaches the threshold value, the face picture comparison succeeded, and the face picture is recognized.

6. Set the arming schedule. Refer to **Configure Arming Schedule** for details.
7. Set the linkage actions for **Linkage Succeeded** and **Linkage Failed**. Refer to **Configure Alarm Linkage Action** for details.

Linkage Succeeded

The device will perform linkage actions when the face picture comparison succeeded.

Linkage Failed

The device will perform linkage actions when the face picture comparison failed.

8. Click **Apply**.

6.4.4 Configure Arming Schedule

Steps

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



Note

Time periods shall not be repeated or overlapped.

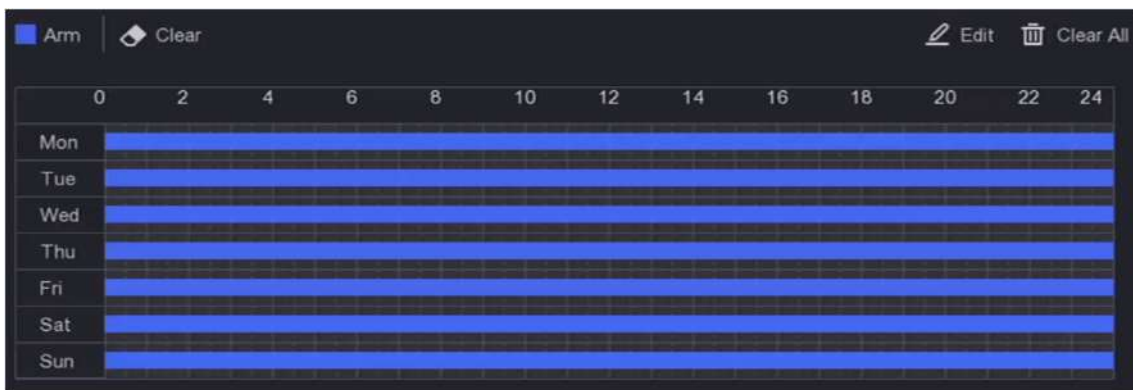


Figure 6-25 Set Arming Schedule

3. Click **Apply**.

6.4.5 Configure Alarm Linkage Action

Configure Alarm Pop-up Window

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.

Steps

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

Alarm Pop-up Output

Select the output to show event video.

Alarm Pop-up Delay

Set the time in seconds to show alarm event image. 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. Click **Linkage Action** of the alarm detection.
4. Select **Alarm Pop-up Window** 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 back to the live view interface.

Configure Buzzer Alarm

The audio warning enables the video recorder to trigger an audible beep when an alarm is detected.

Steps

1. Go to **Configuration → System → Live View → General**.
2. Turn on **Audio**, and set **Volume**.
3. Go to **Linkage Action** interface of the alarm detection.
4. Select **Buzzer Alarm** linkage action.

Notify Surveillance Center

The video recorder can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the computer installed with client software (e.g., iVMS-4200, iVMS-5200).

Steps

1. Go to **Configuration → Network → General → More Settings**.
2. Set **Alarm Host IP** and **Alarm Host Port**.
3. Go to Linkage Action interface of the alarm detection.
4. Select **Notify Surveillance Center**.

Configure Email Linkage

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

Steps

1. Go to **Configuration → Network → Email**.
2. Configure the settings.
3. Go to Linkage Action interface of the alarm detection.
4. Select **Send Email** as alarm linkage action.

Trigger Alarm Output

The alarm output can be triggered by the normal and smart events.

Steps

1. Go to **Linkage Action** interface of the alarm input or event detection.
2. Click **Alarm Output Linkage**.
3. Select the alarm outputs to trigger.
4. Go to **Configuration → Event → Normal Event → Alarm Output**.
5. Select an alarm output item from the list. Refer to **Alarm Output** for details.

Configure PTZ Linkage

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

Steps

1. Go to **Linkage Action** interface of the alarm input or VCA detection.
2. Select **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.



Figure 6-26 PTZ Linkage

Note

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

6.5 Recording Management

6.5.1 Configure Recording Schedule

Video recorder will automatically start/stop recording according to the configured schedule.

Configure Continuous Recording

Steps

1. Go to **Configuration → Record → Parameter** .
2. Set the continuous main stream/sub-stream recording parameters for the camera.
3. Go to **Configuration → Record → Schedule** .
4. Select recording type as **Continuous**.

Configure Event Recording

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

Steps

1. Go to **Configuration → Event** .
2. Configure the event detection and select the cameras to trigger the recording when event occurs.
3. Go to **Configuration → Record → Parameter** .
4. Set the continuous main stream/sub-stream recording parameters for the camera.
5. Go to **Configuration → Record → Schedule** .
6. Select recording type as **Event**.

Edit Schedule

Steps

1. Go to **Configuration → Record → Schedule** .

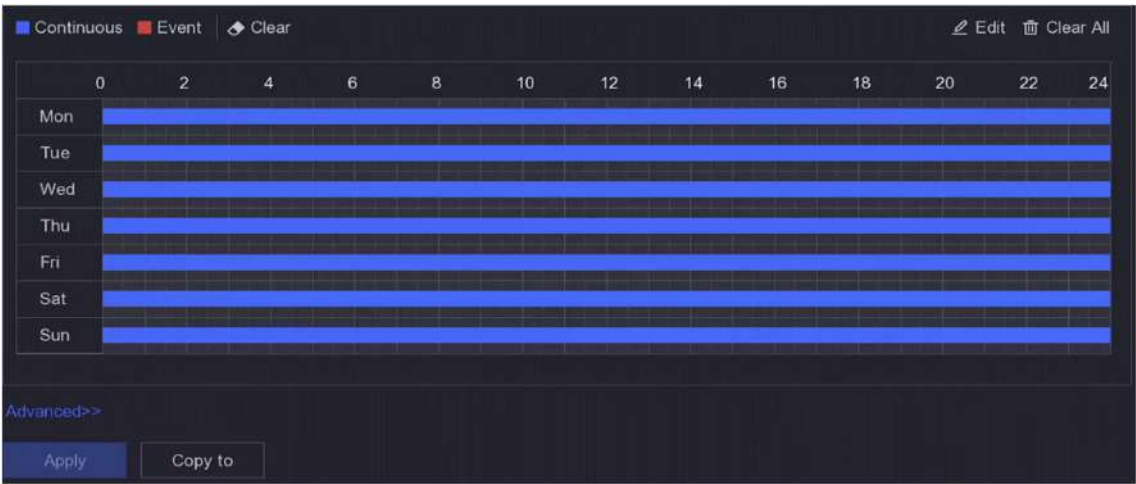


Figure 6-27 Recording Schedule

Continuous

Continuous recording.

Event

Recording triggered by all event triggered alarms.

- 2. Select a camera in **Camera No.**
- 3. Turn on **Enable**.
- 4. Configure the recording schedule.
 - 1) Click **Edit**.
 - 2) Select a day to configure in **Weekday**.
 - 3) To set an all-day recording schedule, check **All Day** and select schedule **Type**.
 - 4) To set other schedules, uncheck **All Day** and set **Start/End time** and schedule **Type**.

 Note

Up to 8 periods can be configured for each day. And the time periods cannot be overlapped with each other.

- 5) Click **OK** to save the settings and go back to upper level menu.

 Note

You can also select schedule type as **Continuous** or **Event**, and drag the cursor on the desired period to draw a colored bar.

- 5. Click **Advanced** to set advanced parameters.

Record Audio

Audio will be record to the video file.

Pre-Record

The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Post-Record

The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

Stream Type

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

Video/Picture Expiry Time

The expiry time is period for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

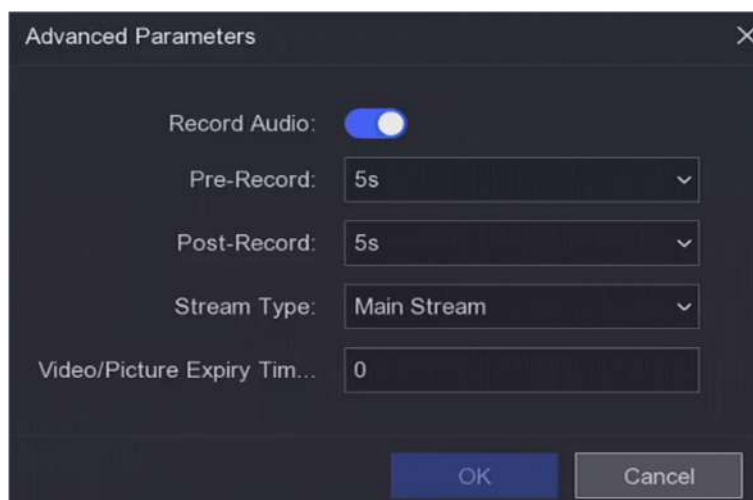


Figure 6-28 Advanced Parameters

6. Click **OK** to save the advanced settings.
7. Click **Apply**.

6.5.2 Configure Recording Parameter

Steps

1. Go to **Configuration → Record → Parameter** to configure camera main stream and sub-stream parameters.
2. Configure recording parameters.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Frame Rate

Frame rate 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), for example, 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+/Enable H.265+

The H.264+/H.265+ mode helps to ensure the high video quality with a lowered bitrate. It can effectively reduce the need of bandwidth and HDD storage space.

Audio Source

The audio input signal source. If you select **Audio Source** as **Camera**, it will transmit audio via coaxial cable, and make the local audio input signal unavailable. Ensure the camera supports to transmit audio via coaxial cable before selecting **Audio Source** as **Camera**.



Note

Audio Source is only available for certain models.

Enable Low Bitrate Mode

In order to save device bandwidth or memory, the device would automatically adjust camera video main stream bitrate according to your network condition.



Note

Low bitrate mode is only available for certain camera models. If your camera supports this function, it would be enabled by default.

3. Click **Apply**.

6.5.3 Storage Device

Initialize HDD

If it is the first time you use your HDD, please initialize it after it is installed.

Before You Start

Install at least an HDD to your video recorder.

Steps

1. Go to **Configuration → Record → Storage** .
2. Select an HDD.
3. Click **Init**.

Add Network Disk

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

Steps

1. Go to **Configuration → Record → Storage** .
2. Click **Add**.
3. Set **NetHDD**.
4. Set **Type** as **NAS** or **IP SAN**.
5. Enter NetHDD IP address.
6. Click  to search the available disks.

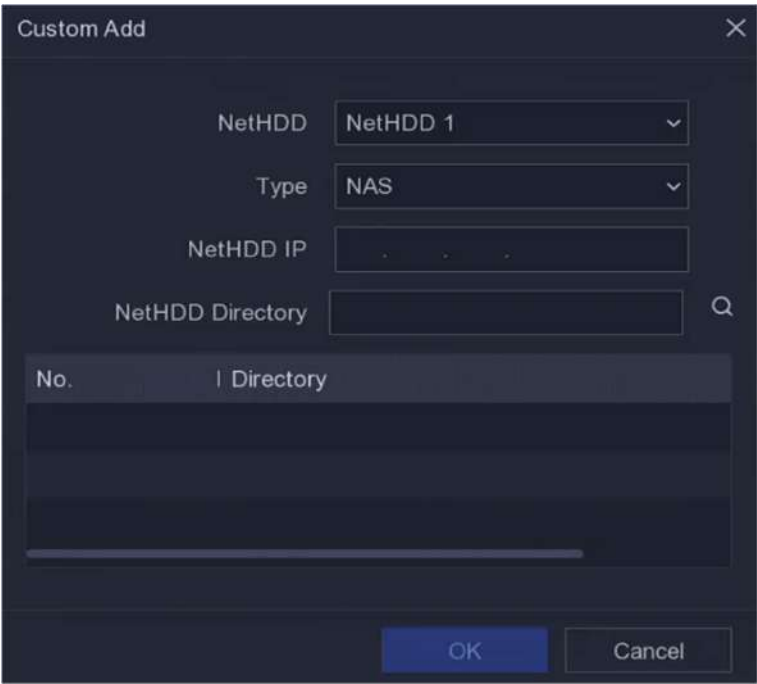


Figure 6-29 Add NetHDD

- 7. Select NAS disk from the list, or manually enter the directory in **NetHDD Directory**.
- 8. Click **OK**.

 Note

Up to 8 TB storage capacity is allowed for each network disk.

Result

The added network disks will be displayed in the storage device list.

6.5.4 Configure Storage Mode

Configure HDD Groups

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

Steps

 Note

This function is only available for certain models.

- 1. Go to **Configuration → Record → Storage Mode** .

- 2. Select **Mode** as **Group**.
- 3. Select a group number.
- 4. Select IP cameras to record on the HDD group.

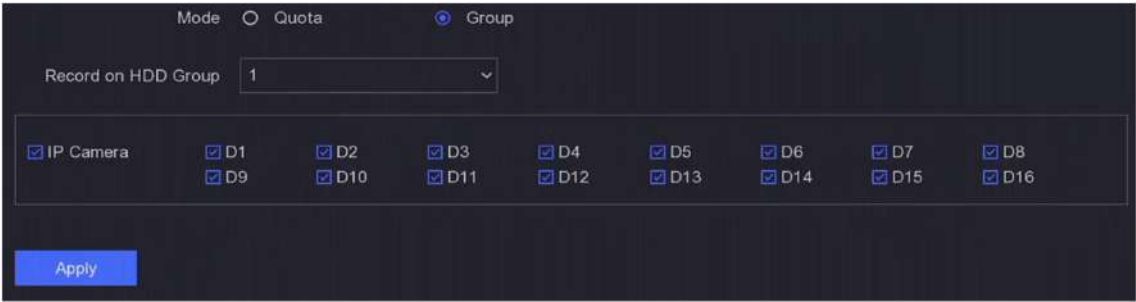


Figure 6-30 Group

- 5. Click **Apply**.
- 6. Restart the video recorder to activate the new storage mode settings.
- 7. After restart, go to **Configuration → Record → Storage**.
- 8. Click of desired HDD to set the group.
- 9. Select a group number for the current HDD.
- 10. Click **Apply**.



Note

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

Configure HDD Quota

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

Steps



Note

This function is only available for certain models.

- 1. Go to **Configuration → Record → Storage Mode**.
- 2. Set **Mode** as **Quota**.
- 3. Select a camera to set quota in **Camera**.
- 4. Enter the storage capacity in **Record Capacity**.

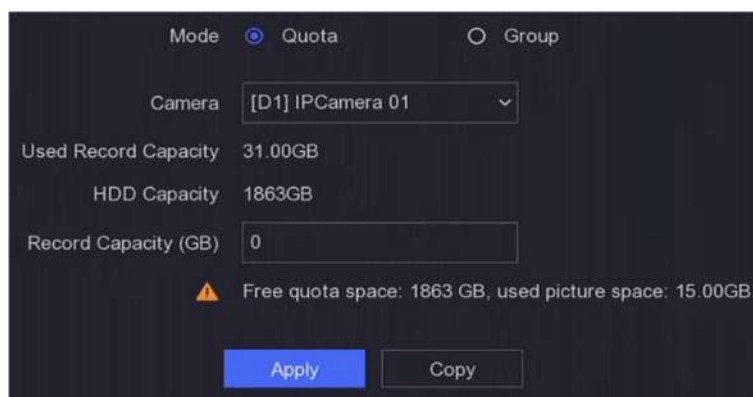


Figure 6-31 Quota



Note

When the quota capacity is set to 0, all cameras will use the total capacity of HDD for videos and pictures.

5. Click **Apply**.
6. Restart the video recorder to activate the new settings.

6.5.5 Advanced Settings

Steps

1. Go to **Configuration → Record → Advanced**.
2. Configure the parameters as your desire.

Overwrite

- Disable: When the HDD is full, video recorder will stop writing.
- Enable: When hard drive is full, video record will continue to write new files by deleting the oldest files.

Enable HDD Sleeping

HDDs which are free of working for a long time will turn into sleep status.

Save Camera VCA Data

Camera VCA data will be saved so that you can search it.



Note

Disabling **Save Camera VCA Data** will delete the existing Dual-VCA and motion detection information, and stop analyzing and storing Dual-VCA and motion detection information.

Alarm Storage

When the HDD free space is not enough, you can disable it to save space, but your device will stop storing alarm information.

Picture Storage

When the HDD free space is not enough, you can disable it to save space, but your device will stop storing pictures.

Chapter 7 Maintenance

7.1 Restore Default

Steps

1. Click  at the upper-right corner.
2. Select the restoring type.

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the device to the inactive status, and leave all settings unchanged except restoring user accounts.

3. Click **Yes**. The device will reboot automatically.

7.2 Search Log

The operation, alarm, exception and information of video recorder can be stored in logs, which can be viewed and exported at any time.

Steps

1. Click  at the upper-right corner.
2. Click **More**.
3. Click **Log Information**.
4. Set the search conditions.
5. Click **Search**.

7.3 System Service

Steps

1. Click  at the upper-right corner.
2. Click **More**.
3. Click **System Service**.
4. Configure the parameters as your desire.

RTSP

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

RTSP Authentication

Two authentication types are selectable, if you select **digest**, only the request with digest authentication can access the video stream by the RTSP protocol via the IP address. For security reasons, it is recommended to select **digest** as the authentication type.

ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.). The video recorder is used as a server, the system can find and connect the video recorder.

HTTP

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

HTTP Authentication

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security. Two authentication types are selectable. For security reasons, it is recommended to select **digest** as the authentication type.

Camera Added Detection

The function detects the network camera status. If the network camera has been added by another video recorder, the network camera status will show as  in **Online Device** list.

5. Click **Apply**.

7.4 Buzzer Switch

You can enable or disable buzzer with alarm linkage or exceptional linkage.

Steps

1. Click  at the upper-right corner.
2. Click **More**.
3. Go to **Buzzer Switch**.
4. Turn on or turn off **Enable**.

7.5 Device Maintenance

7.5.1 Schedule Reboot

The device will automatically restart according to the schedule.

Steps

1. Click  at the upper-right corner.
2. Click **More**.
3. Go to **Device Maintenance** → **Enable Schedule Reboot**.
4. Turn on **Enable**.
5. Set the reboot schedule.
6. Click **Apply**.

7.5.2 Device Status

You can mute the selected channel(s).

Steps

1. Click  at the upper-right corner.
2. Click **More**.
3. Go to **Device Maintenance** → **Device Status**.
4. In the **Mute and Not Disturb** column, check the corresponding channel(s).

Result

The selected channel(s) will be muted.

7.6 Upgrade



Warning

Do not shutdown or turn off the power during upgrade.

7.6.1 Local Upgrade

Before You Start

Store the upgrade firmware to a backup device, and connect it to your device.

Steps

1. Click  at the upper-right corner.
2. Click .
3. Click **Local Upgrade**.
4. Select a backup device in **Device Name**.
5. Select the upgrade firmware.
6. Click **Upgrade**. Your device will reboot automatically.

7.6.2 Online Upgrade

Upgrade the device with the latest online firmware.

Before You Start

Ensure Hik-Connect is enabled and properly configured. Refer to **Hik-Connect** for details.

Steps

1. Click  at the upper-right corner.
2. Click .
3. Go to **Online Upgrade**.
4. Download the latest firmware.

Auto Download The will automatically check and download the latest firmware.

Test Upgrade Click **Test Upgrade** to manually check and download the latest firmware.

5. Upgrade your device if a new firmware version is available. The device will reboot automatically.

Chapter 8 Alarm

When events occur, you can view their details in alarm center.

8.1 Set Event Hint

Select the events to hint in alarm center.

Steps

1. Click  at the upper-right corner.
2. Set **Exception**, **Basic Event**, or **Smart Event** as your desire.

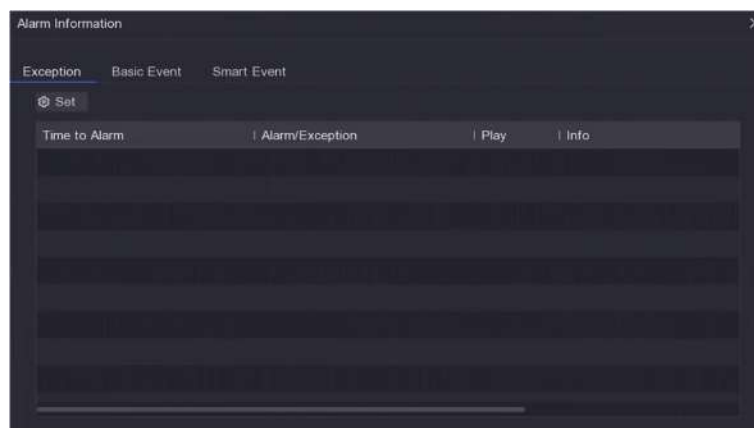


Figure 8-1 Alarm Center

3. Click  and select events to hint.
4. Click **OK**.

When the selected events occur, the alarm information will be displayed in  (locating at the upper-right corner of local menu).

8.2 View Alarm in Alarm Center

Steps

1. Click  at the upper-right corner of local menu.
2. Click **Exception**, **Basic Event**, or **Smart Event** to view as your desire.

Chapter 9 Web Operation

9.1 Introduction

You can get access to the video recorder via web browser.

You may use one of the following listed web browsers: Internet Explorer 11.0, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolutions include 1024×768 and above.

For certain models, you will have to download a web component plug-in, and install it. Otherwise, a few functions would be unavailable. The download address is <http://hikdownload.hs7.com/web/webplugin/windows/WebComponents/standard/WebComponents.exe>.

9.2 Login

You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, please contact with your dealer or the nearest service center.

Steps

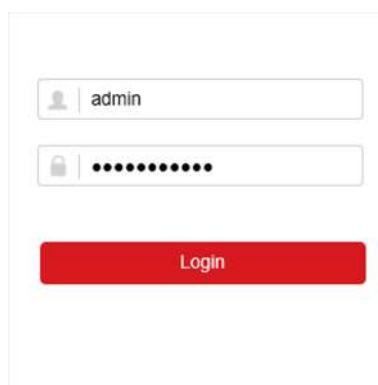
1. Open web browser, input the IP address of the video recorder and then press **Enter**.



Note

If you have changed HTTP port, enter ***http://IP address:HTTP port*** in address bar. E.g., ***http:192.168.1.64:81***.

2. Enter **user name** and **password** in the login interface.
3. Click **Login**.



The image shows a web login interface. It consists of two input fields: the first is for the username, with 'admin' entered, and the second is for the password, with ten dots representing masked characters. Below these fields is a red rectangular button with the word 'Login' in white text.

Figure 9-1 Login

4. Follow the installation prompts to install the plug-in.

Note

You may have to close the web browser to finish the installation of the plug-in.

9.3 Live View

After login, live view interface shows.



Figure 9-2 Live View

9.4 Playback

Click **Playback** to enter playback interface.

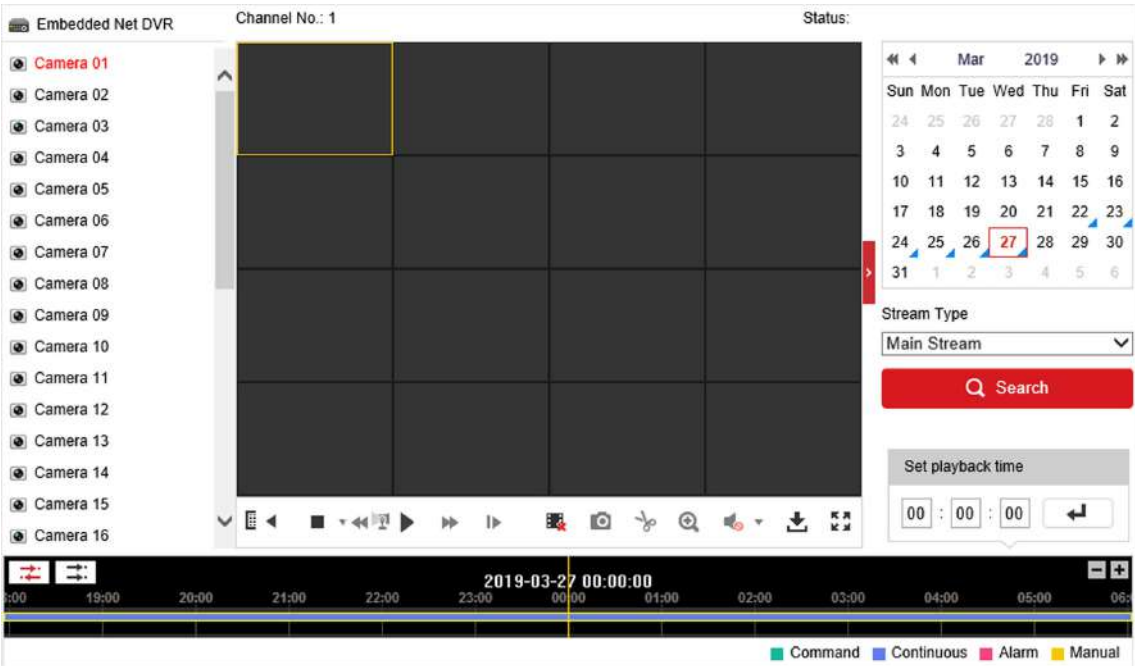


Figure 9-3 Playback

9.5 Configuration

Click **Configuration** to enter configuration interface.

Local

System

Network

Video/Audio

Image

Event

Storage

Vehicle Detection

VCA

Target Capture

Live View Parameters

Protocol

☒ TCP

☐ UDP

☐ MULTICAST

☐ HTTP

Stream Type:

☒ Main Stream

☐ Sub-stream

Play Performance

☐ Shortest Delay

☒ Balanced

☐ Fluency

Rules

☐ Enabled

☒ Disabled

Display Trajectory

☐ Enabled

☒ Disabled

POS/OSD Overlay

☒ Enabled

☐ Disabled

Image Size

☒ Auto-fill

☐ 4:3

☐ 16:9

Auto Start Live View

☐ Yes

☒ No

Image Format

☒ JPEG

☐ BMP

Encryption Key

Record File Settings

Record File Size

☐ 256M

☒ 512M

☐ 1G

Save record files to

Browse

Save downloaded files to

Browse

Picture and Clip Settings

Save snapshots in live view to

Browse

Save snapshots when playback to

Browse

Save clips to

Browse

Save

Figure 9-4 Configuration

9.6 Log

Steps

- 1. Go to Maintenance → System → Maintenance → Log .
- 2. Set the search conditions.
- 3. Click Search.

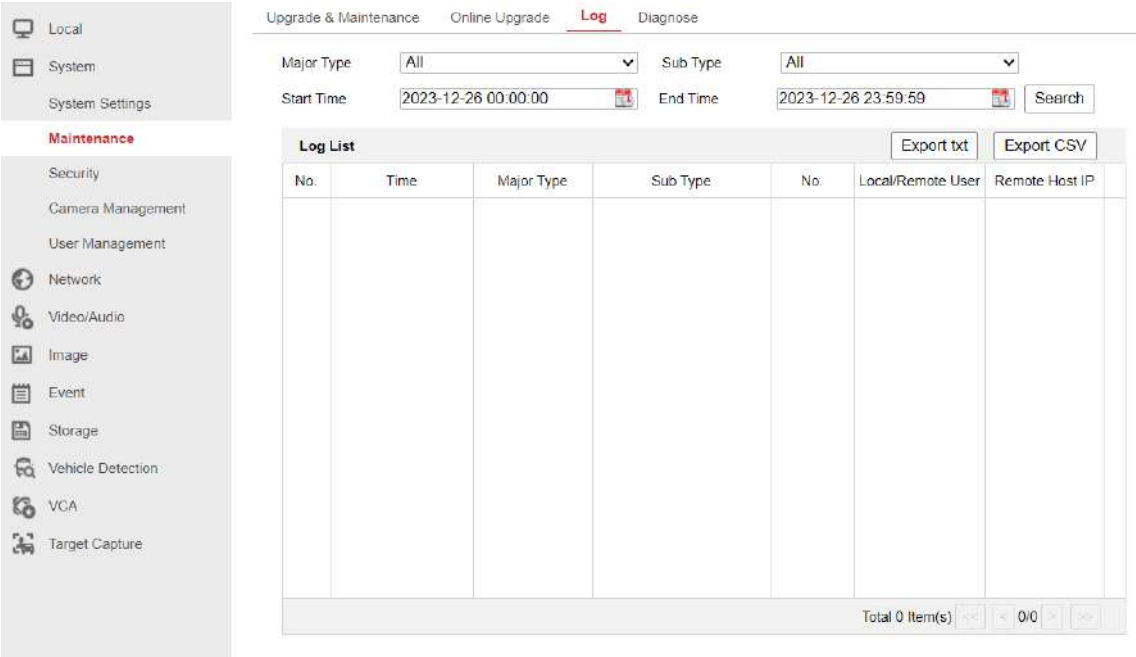


Figure 9-5 Log

Chapter 10 Appendix

10.1 Glossary

Dual-Stream

Dual-stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.

DDNS

Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.

NVR

Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.



See Far, Go Further