Storage Solution

Video Storage Parameters		
VideoStorage Parameters	Camera Type 1	
Channel Name	Device 1	
Channel Number	16	
Encoding Mode	H.265	
Resolution	1080P(1920×1080)	
Frame Rate	30	
Bitrate	2048	
Storage Time / Day (Hour)	24	
Storage Period (Day)	30	

NVR List Output				
NO.	Product Name	Brand	Model	Quantity
1	Storage Host	Hikvision	iDS-7616NXI-M2/16P/X(M)	1

Storage Requirements			
	Requirements	Now	Satisfaction
Storage	10TB	12TB	+2.00TB
Bandwidth	38Mbps	256Mbps	+218.00Mbps
Channel	16	16	+0.00



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
DS-9600NI-M16/R	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
DS-7700NXI-I4/P/S	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

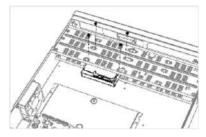


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

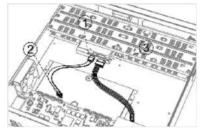


Figure 1-4 Connect Cable

INote

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.

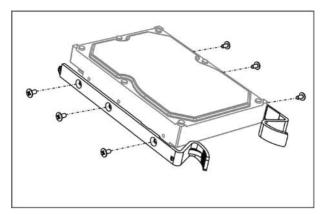


Figure 1-5 Fix Mounting Ears to HDD

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

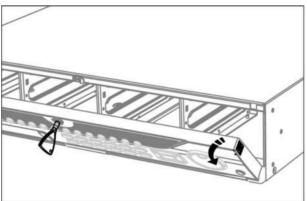


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

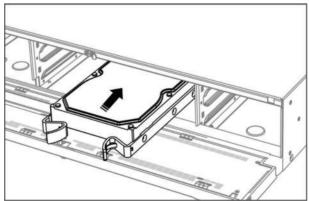


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

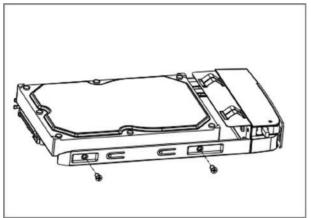


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

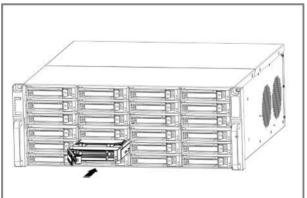


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

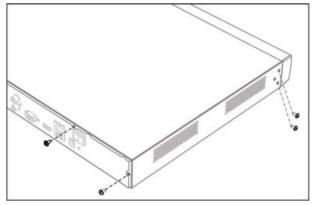


Figure 1-10 Remove Cover

- 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.

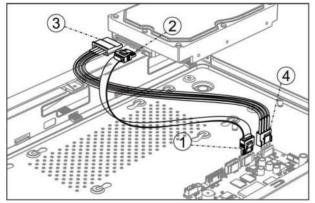


Figure 1-11 Connect Cables

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

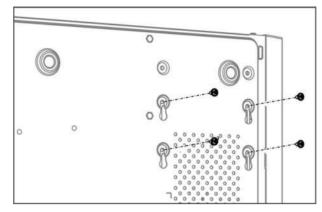


Figure 1-12 Fix HDD to Device Bottom

- 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.

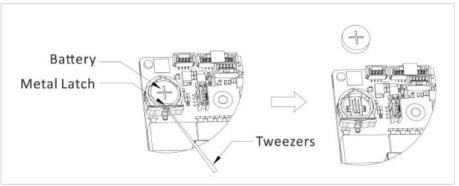


Figure 1-1 Remove Battery

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

iNote

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

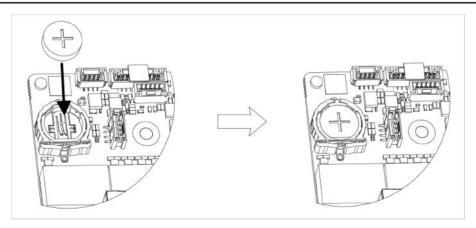


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	0
6.1 Access Video Device	0
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	0
6.1.3 Add Network Camera through PoE 2	1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	2
6.1.5 Add Network Camera via Custom Protocol 2	2
6.1.6 Add Network Camera through Camera Configuration File	4
6.2 Add Access Control Device 24	4
6.3 Add Audio Device 2	4
6.4 Add POS Device 2	5
6.5 Channel Management 2	6
Chapter 7 Device Grouping 2	7
Chapter 8 Video or Audio Device Settings 2	8
8.1 Enable H.265 Stream Access 2	8
8.2 Configure Display Settings 2	8
8.3 Configure Video Parameters 2	9
8.4 Configure Privacy Mask 2	9
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	1
8.8 Configure PoE (Power over Ethernet) Interface 3	2
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	4
9.2 RAID Configuration 3	4
9.2.1 Create Disk Array 3	5
9.2.2 Rebuild Array 3	6
9.2.3 Delete Array 3	7
9.2.4 View Firmware Info	7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library 8	85
16.4.2 Upload Face Pictures to the Library 8	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup 9	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info 9	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info 9	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
8	•••••	
A		
0		
When yo recomme	u forget your password, the hint will help you remember. It is inded to set the hint.	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)			Nore 🔲 Show Peerw	ord			O device(a) connected.
Viteo Device	Device Na. : P Addre	os = Network =	Passwor. Show Pa.	Protocol	Manage : AddesiTotal	Serial No. +	Version :
Access Control Device							
Altim Device							
Auto Device							
POS							
Device Grouping							
Device Configuration 🔗							
Device Parameter							
Access Service							
Batch Contiguration	Online Device List (0)						
			efresh:				
Menu Bar	IP Address I Device	fociel : Status	Protocol	Manage) Serial No 2	Errwan	r 3 Physical

Figure 3-2 Menu Bar Example

Destrict 09:07		e	Section of	O Parat March	(a) Property t	Contract store	÷ :
Venice Capture 2	Person Clipfure	iu:				Target Recognition	
lenu Bar	00-77	-2023 Wed 09:07:47					
	1.001.000						
				Conver	10 M T		
					SA 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP	-	Main NIC	LAN1	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

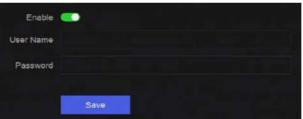


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

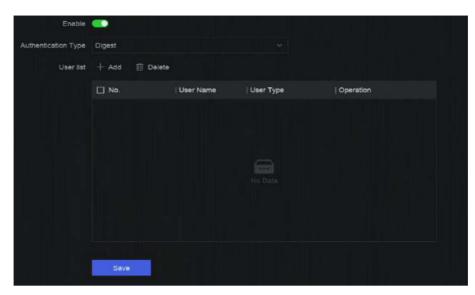


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description			
0	Set account security.			
Add	dd a new guest or operator user.			
Ū	Delete the selected user.			

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

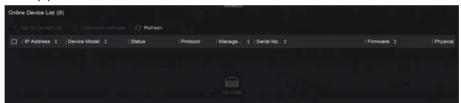


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×
Online Device List (0)	Refresh C
No. IP Address Device Model	Status Protocol Manag Serial Ne
	Data
IP Address *	Device Name *
Test	IPCamera 01
Protocol	Management Port *
ONVIF · Protocol Manag	80
User Name	Password
admin	
Transfer Protocol	Use Channel Default Password
Auto ~	

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Management						×		
HIKVISION_RTSP	Check your device URL and enter accordingly. Format [Type]//IP Address][Port/[Path]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [*Type*]://[*IP Address*]:[*Port*]/[*Resource Path*], for example, *rtsp:*//192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🗌 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click Import to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	🕳)
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

			HOWHIN HOO		Remaining capeci
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest C) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WK82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	O rigital	TYDO YZDAUNAPYS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description
One-touch Array	Click One-touch Array Configuration.
Configuration	i Note
	By default, the array type created by one-touch configuration is RAID 5.
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \boxed{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	4 68/7814 68				
+ Add Resource 🛛 🖾 🗆					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.

Parameter Name	Description
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

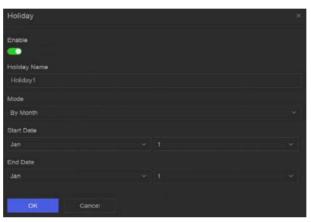


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

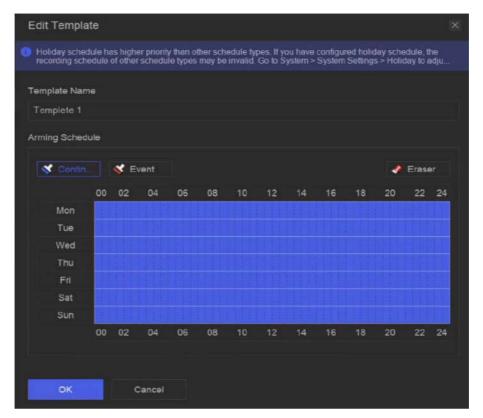


Figure 10-2 Edit Template

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

i Note

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

iNote

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

6. Click OK.

10.2 Configure Recording Schedule

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

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carnera 01		Quatom		
D2) IPCamera 02	-	Custom		
] [03] IPCamera 03	-	Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

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

INote

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

4. Click View to view the schedule.



Figure 10-4 View Schedule

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

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

7. Click Save.

10.3 Configure Picture Capture Schedule

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

Steps

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

Batch Schedule Configuration Batch Advanced Configuration Configure Template					
Channel Name	Enable	Record Schedule		Plan Details	Advanced Settings
[D1] Camera 01		Custom			
02] (02] IPCamera 02		Custom			
03] IPCamera 03		Custom			
[04] IPCamera 04		Custom			

Figure 10-5 Picture Capture Configuration

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

iNote

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

4. Click View to view the schedule.

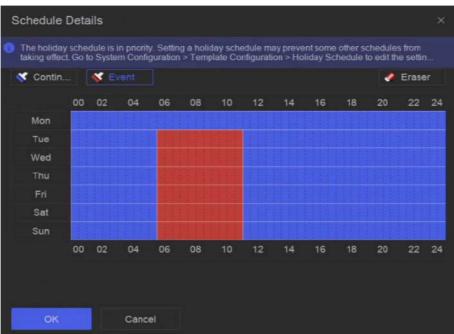


Figure 10-6 View Schedule

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

Table 10-2 Advanced Parameter Description

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

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

10.4 Configure Audio Recording

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

Steps

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

iNote

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

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

Table 10-3 Advanced Parameter Description

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

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

Chapter 11 Live View

11.1 Configure Live View Layout

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

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

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



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



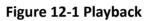


Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext.
	the corresponding event rule. Refer to the event configuration steps for details of each event type.

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

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

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

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

3. Select a date in the calendar.

iNote

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

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

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

Before You Start

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

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

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

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

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

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

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

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

12.5 Sub-Period Playback

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

Steps

1. Go to Playback \rightarrow \blacksquare .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

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

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Con	figuration
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording to configure video recording schedule.

8. Click Save.

13.1.2 Perimeter Protection

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

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V
AI by NVR	•
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shalid Area
	1 2 3 4
Rule List	
	01-62-2824 Tue: 14:68:36
	B
	Camera 01
	Save

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Rule Configuration
	be triggered when a human face is detected.	
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center
		Comparison
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.
		Non-Real-Time Mode
		For places with a high flow of people, the device processing speed may not be fast

Event Name	Event Description	Rule Configuration
		enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

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

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.

6. Click Arming Schedule to select an arming schedule type.

iNote

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

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	iNote
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
		It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description			
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.			
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).			
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.			
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.			
Sender	The sender name.			
Sender's Address	The sender's address.			
Select Receivers	Select the receiver. Up to 3 receivers can be configured.			
Attached Image	Send email with attached alarm images.			
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.			
Interval	The time interval for capturing the attached images.			

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemera 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diserming		
D3] IPCamera 03.	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disaming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
[] [D6] IPCamera 06		Disabled	Quick Diseming		
[] [D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 (010) IPCamera 10		Disabled	Quick Diseming		
[D11] IPCamera 11		Disabled	Quick Disaming		
🔲 [D12] IPCamera 12	-	Disabled	Quick Disaming		
🔲 (D13) IPCamera 13	•10	Disabled	Quick Diserming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D [D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration** or **System** \rightarrow **Event Configuration** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

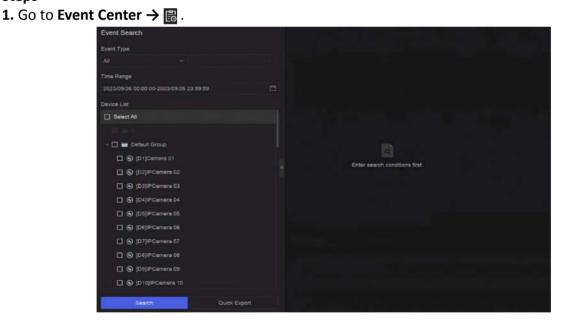


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

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

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Destruction and the second state	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August and a	DTE weeks 01 22340	CTTC-Annual III Annual	
123		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Delaut Droup					
	C (D1)Cerners 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamera 03					
	🗶 🚱 (05)/PCamers 06					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)(PCamera 05					
	🖉 💬 (010)/PCarriera 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - **5** Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

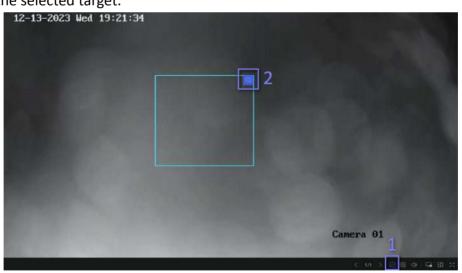


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-22003012000	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canesa 02			
🗷 🕲 (DipPCameni II)			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silarth	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

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

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

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

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

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

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

Disabled

No analysis task is enabled on the camera.

Waiting

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

Enabled

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

16.4 List library Management

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

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

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

16.4.2 Upload Face Pictures to the Library

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

Before You Start

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

Steps

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

Delete Pictures from
the Library

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

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

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

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

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

17.2 Person Check-In

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

17.2.1 Add Check-In Task

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

Before You Start

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

Steps

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

				Add Check-In Task	
Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-т Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

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

7. Click Confirm.

17.2.2 Search Check-In Records

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

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

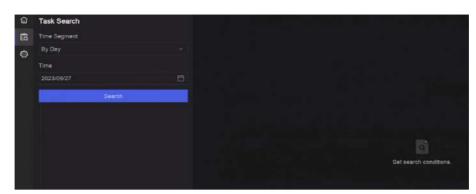


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

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

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception ~	HDD Full	
Notify Surveillance Center			
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	1.0001 > 0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

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

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- 1. Go to System → System Maintenance → Maintenance → Maintenance Tools .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

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

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Ф5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-7616NXI-M2/16P/X(M) DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 16-ch IP cameras can be connected, plug & play with 16 power-over-Ethernet (PoE) interfaces
- Intelligent analytics based on deep learning algorithm
- Up to 12-ch perimeter protection
- Up to 8-ch facial recognition for video stream, or up to 16-ch facial recognition for face picture
- Up to 6-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution

Storage and Playback

- Up to 2 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





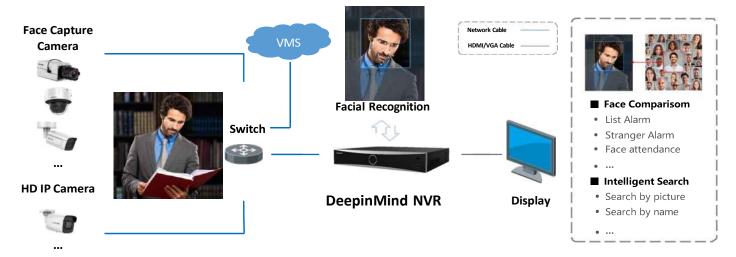
Network & Ethernet Access

- 1 self-adaptive 10M/100M/1000M Ethernet interface
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen

Typical Application

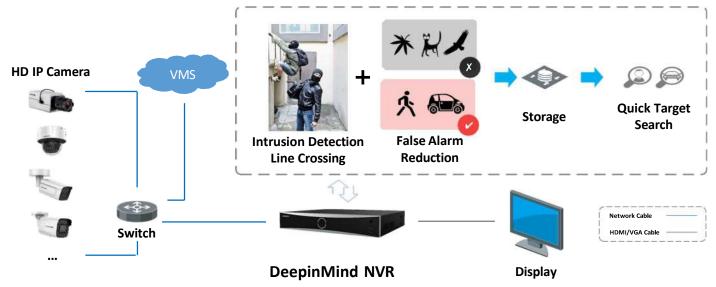
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

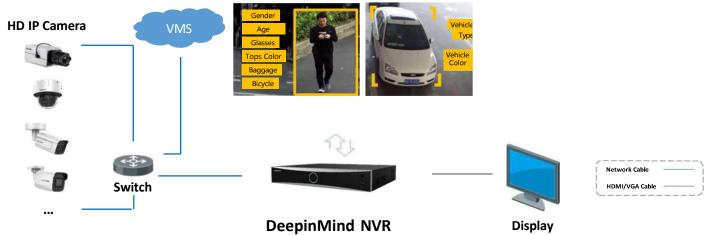
Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





. .

Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from building
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, loitering, people running
Engine	1 engine can run an intelligent algorithm, engine mode is adjustable
Operating System	Linux
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 16 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 5,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face detection.
Face Picture Comparison (Captured from Camera)	16-ch; Comparison speed: 24 pictures per second
Facial Detection and Analytics Performance	8-ch 2 MP, up to 8 MP
Perimeter Protection	
By NVR	12-ch 2 MP, up to 8 MP
By Camera	All channels
Alarms	Support generates alarms of perimeter violation
Video Structuralization	
Structured Analysis	6-ch 2 MP, up to 8 MP
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 500,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB)
Face Picture Comparison	8-ch;
Face Ficture compansion	Comparison speed: 16 pictures per second
Throwing Objects from Building	
By NVR	8-ch 2 MP, up to 8 MP
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Plate number, license plate color, license plate type
Plate Attributes	Vehicle brand, vehicle color, vehicle type



.

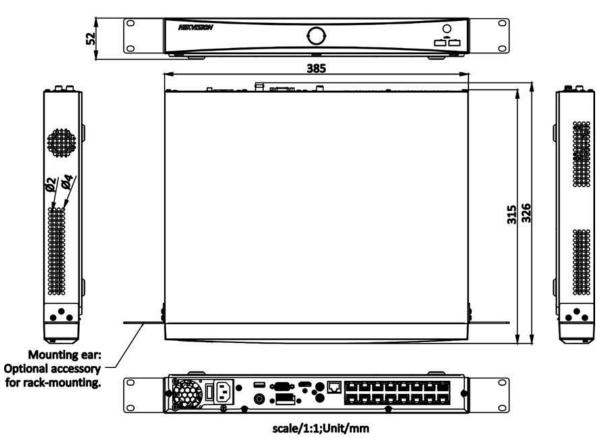
Video and Audio	
IP Video Input	16-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth	256 Mbps
Outgoing Bandwidth	256 Mbps
HDMI Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1440 × 900/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
VGA Output	1920 × 1080/60Hz, 1440 × 900/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Video Output Mode	HDMI 1.4/VGA independent output
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	1-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)
Synchronous Playback	16-ch
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTP, SADP, SMTP, SNMP, NFS, UDP, iSCSI, ISUP, UPnP™, HTTP, HTTPS
API	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	1, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)
РоЕ	
Interface	16 RJ-45 10/100 Mbps self-adaptive Ethernet interfaces
Power	≤ 200 W
Standard	IEEE 802.3 af/at



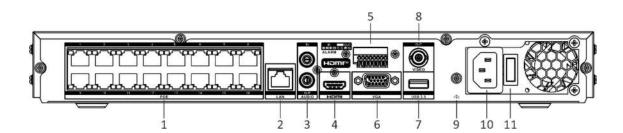
Auxiliary Interface	
SATA	2 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 14 TB capacity for each HDD
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
Alarm In/Out	4/1
General	
	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French,
	Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish
GUI Language	Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese,
	Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian,
	Kyrgyz , Brazilian Portuguese, Indonesian
Processor	32bits multi-core
Memory	RAM 8GB DDR4
Licensing	All features are fully perpetually licensed to operate standalone
File lock	Support lock and unlock recorded files
USB Video Playback	Support
Video Download	Batch and segment support
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	\leq 14 W (without HDD and PoE off and Engines off)
Working Temperature	-10 to 55° C (14 to 131° F)
Working Humidity	10 to 90%
Dimension ($W \times D \times H$)	385 × 315 × 52 mm (15.2"× 12.4" × 2.0"), 1U
Weight	≤ 3 kg (without HDD, 2.2 lb.)
Certification	
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201 9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020



Dimension



Physical Interface



No.	Description	No.	Description
1	Network interfaces with PoE function	7	USB 3.0 interface
2	LAN interface	8	CVBS video output
3	Audio out and audio in	9	GND
4	HDMI interface	10	100 to 240 VAC power supply
5	Alarm in and alarm out	11	Power switch
6	VGA output		

Available Model

iDS-7616NXI-M2/16P/X(M)

Headquarters No.555 Qianmo Road, Binjiang District, Hangzhou 310051, China T +86-571-8807-5998 www.hikvision.com

Follow us on social media to get the latest product and solution information.











(O) hikvisionhq

©Hikvision Digital Technology Co., Ltd. 2022 I Data subject to change without notice I

Storage Solution

Video Storage Parameters		
VideoStorage Parameters	Camera Type 1	
Channel Name	Device 1	
Channel Number	32	
Encoding Mode	H.265	
Resolution	1080P(1920×1080)	
Frame Rate	30	
Bitrate	2048	
Storage Time / Day (Hour)	24	
Storage Period (Day)	30	

NVR List Output				
NO.	Product Name	Brand	Model	Quantity
1	Storage Host	Hikvision	iDS-9632NXI-M8/X(M)	1

Storage Requirements			
	Requirements	Now	Satisfaction
Storage	20TB	24TB	+4.00TB
Bandwidth	76Mbps	320Mbps	+244.00Mbps
Channel	32	32	+0.00



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

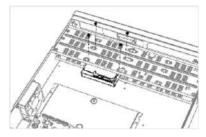


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

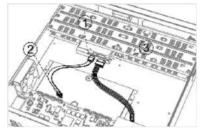


Figure 1-4 Connect Cable

INote

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.

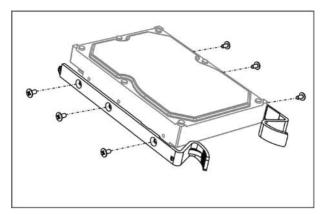


Figure 1-5 Fix Mounting Ears to HDD

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

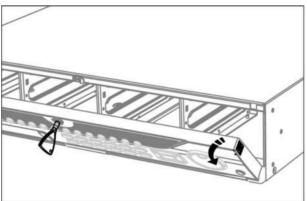


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

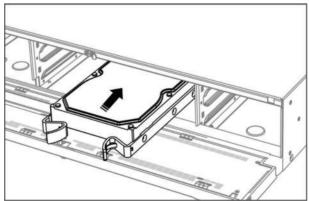


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

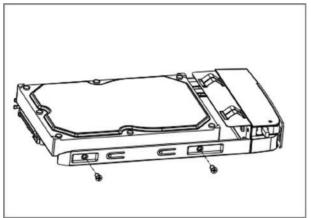


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

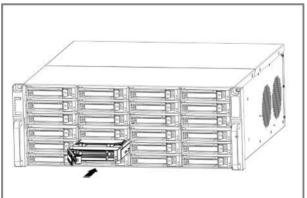


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

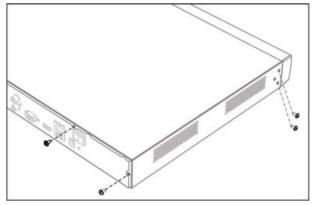


Figure 1-10 Remove Cover

- 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.

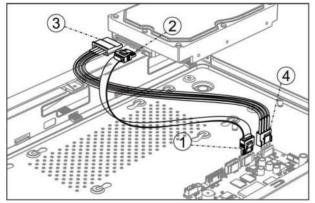


Figure 1-11 Connect Cables

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

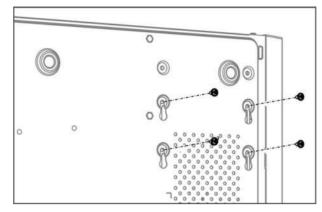


Figure 1-12 Fix HDD to Device Bottom

- 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.

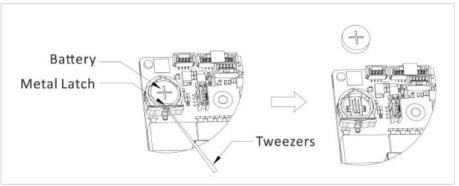


Figure 1-1 Remove Battery

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

iNote

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

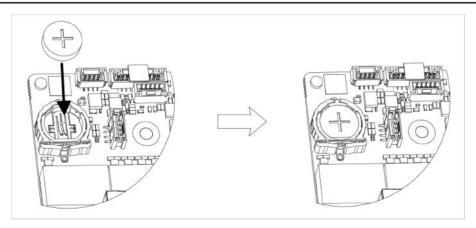


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	0
6.1 Access Video Device	0
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	0
6.1.3 Add Network Camera through PoE 2	1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	2
6.1.5 Add Network Camera via Custom Protocol 2	2
6.1.6 Add Network Camera through Camera Configuration File	4
6.2 Add Access Control Device 24	4
6.3 Add Audio Device 2	4
6.4 Add POS Device 2	5
6.5 Channel Management 2	6
Chapter 7 Device Grouping 2	7
Chapter 8 Video or Audio Device Settings 2	8
8.1 Enable H.265 Stream Access 2	8
8.2 Configure Display Settings 2	8
8.3 Configure Video Parameters 2	9
8.4 Configure Privacy Mask 2	9
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	1
8.8 Configure PoE (Power over Ethernet) Interface 3	2
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	4
9.2 RAID Configuration 3	4
9.2.1 Create Disk Array 3	5
9.2.2 Rebuild Array 3	6
9.2.3 Delete Array 3	7
9.2.4 View Firmware Info	7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	-3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library	85
16.4.2 Upload Face Pictures to the Library	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
8	•••••	
A		
0		
When yo recomme	u forget your password, the hint will help you remember. It is inded to set the hint.	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)							O device(#) connected
Viteo Device	Device Na : IP Address	+ Network +	Passwor. Show Pa.	Protocol	Manage_ : AddedTotal	Serial No. +	Version :
Access Control Device							
Atom Device							
Audio Device							
POS							
Device Grouping							
Device Configuration							
Device Parameter							
Access Service							
Batch Configuration	Online Device List (0)						
		en la come					
Menu Bar	IP Address 1 Device Mo	chel 2 Ditations	: Protocol	Manage	1 Serial No. 1	LFirmware	: Physical

Figure 3-2 Menu Bar Example

Destring Cardina		e	Section of	O Parat March	(a) Property t	Contract store	÷ :
Venice Capture 2	Person Clipfure	iu:				Target Recognition	
lenu Bar	00-77	-2023 Wed 09:07:47					
	1.001.000						
				Conver	10 M T		
					SA 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP	-	Main NIC	LAN1	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

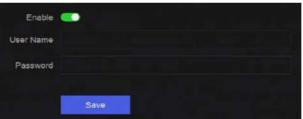


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

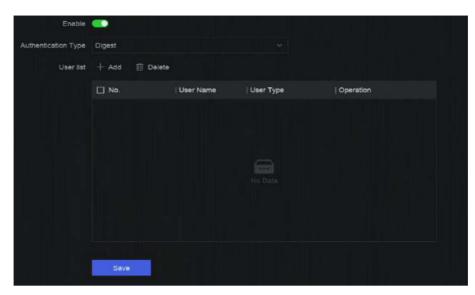


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description			
0	Set account security.			
Add	dd a new guest or operator user.			
Ū	Delete the selected user.			

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

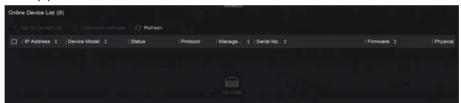


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×
Online Device List (0)	Refresh C
No. IP Address Device Model	Status Protocol Manag Serial Ne
	Data
IP Address *	Device Name *
Test	IPCamera 01
Protocol	Management Port *
ONVIF · Protocol Manag	80
User Name	Password
admin	
Transfer Protocol	Use Channel Default Password
Auto ~	

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Management						×		
HIKVISION_RTSP	Check your device URL and enter accordingly. Format [Type]//IP Address][Port/[Path]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [Type]://[IP Address]:[Port]/[Resource Path], for example, rtsp://192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🔲 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	🕳)
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

			HOWHIN HOO		Remaining capeci
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest C) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WKAND1472762 WD-WX82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	O rigital	TYDG YESHDINNAPTS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description
One-touch Array	Click One-touch Array Configuration.
Configuration	i Note
	By default, the array type created by one-touch configuration is RAID 5.
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \boxed{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	4 68/7814 68				
+ Add Resource 🛛 🖾 🗆					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description				
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.				
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.				
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .				
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.				
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after t scheduled time.				

Parameter Name	Description			
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag. 			
eSATA	For devices with eSATA interface at the rear panel.			
Usage	Set the usage for eSATA.			

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

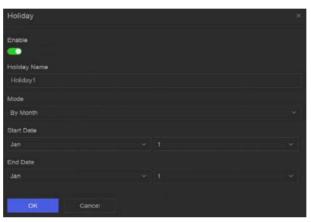


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

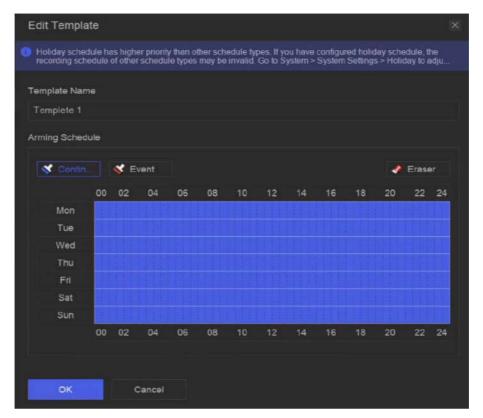


Figure 10-2 Edit Template

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

i Note

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

iNote

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

6. Click OK.

10.2 Configure Recording Schedule

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

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carriera 01		Quatom		
D2] IPCamera 02	-	Custom		
] (03) IPCemere 03		Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

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

INote

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

4. Click View to view the schedule.



Figure 10-4 View Schedule

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

Table 10-1 Advanced Parameter Description

Parameter	Description	
Record Audio	Enable or disable audio recording.	

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

7. Click Save.

10.3 Configure Picture Capture Schedule

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

Steps

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

Batch Schedule Configuration	Batch Advanced Configuration	Z Configure Template		
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01		Custom		
02] (02] IPCamera 02		Custom		
03] IPCamera 03		Custom		
[D4] IPCamera 04		Custom		

Figure 10-5 Picture Capture Configuration

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

iNote

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

4. Click View to view the schedule.

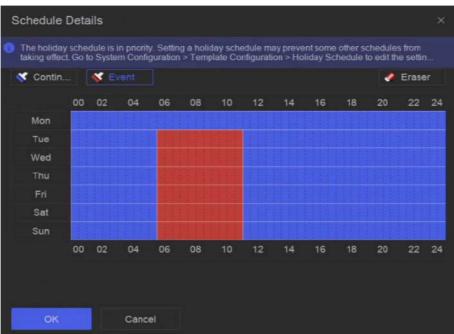


Figure 10-6 View Schedule

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

Table 10-2 Advanced Parameter Description

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

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

10.4 Configure Audio Recording

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

Steps

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

iNote

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

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

Table 10-3 Advanced Parameter Description

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

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

Chapter 11 Live View

11.1 Configure Live View Layout

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

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

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



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



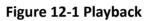


Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext.
	the corresponding event rule. Refer to the event configuration steps for details of each event type.

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

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

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

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

3. Select a date in the calendar.

iNote

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

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

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

Before You Start

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

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

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

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

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

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

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

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

12.5 Sub-Period Playback

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

Steps

1. Go to Playback → 🔜 .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

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

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Detection the moving obj	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Configuration	
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click Save.

13.1.2 Perimeter Protection

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

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V
AI by NVR	•
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shalid Area
	1 2 3 4
Rule List	
	01-62-2824 Tue: 14:68:36
	B
	Camera 01
	Save

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Rule Configuration
	be triggered when a human face is detected.	
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center
		Comparison
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.
		Non-Real-Time Mode
		For places with a high flow of people, the device processing speed may not be fast

Event Name	Event Description	Rule Configuration
		enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

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

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.

6. Click Arming Schedule to select an arming schedule type.

iNote

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

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	iNote	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
		It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemera 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diserming		
D3] IPCamera 03.	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disaming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
[] [D6] IPCamera 06		Disabled	Quick Diseming		
[] [D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 (010) IPCamera 10		Disabled	Quick Diseming		
[D11] IPCamera 11		Disabled	Quick Disaming		
🔲 [D12] IPCamera 12	-	Disabled	Quick Disaming		
🔲 (D13) IPCamera 13	•10	Disabled	Quick Diserming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D [D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration** or **System** \rightarrow **Event Configuration** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

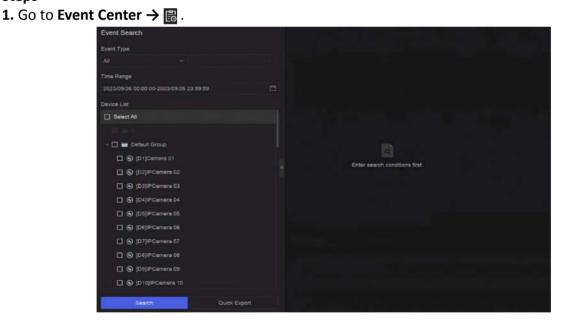


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

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

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Sand Services - Constraint State	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August and a	DTE weeks 01 22340	CTTC-Annual III Annual	
123		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Delauf Droup					
	C (D1)Cerners 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamers 03					
	🗶 🚱 (D5)PCamers 96					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)PCamera 05					
	🖉 💬 (010)/PCarriera 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

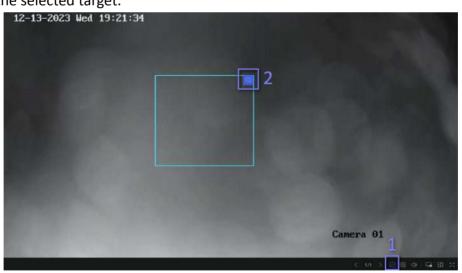


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-2200 101208.01	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canesa 02			
🗷 🕲 (DipPCameni II)			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silenty	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

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

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

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

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

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

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

Disabled

No analysis task is enabled on the camera.

Waiting

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

Enabled

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

16.4 List library Management

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

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

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

16.4.2 Upload Face Pictures to the Library

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

Before You Start

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

Steps

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

Delete Pictures from
the Library

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

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

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

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

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

17.2 Person Check-In

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

17.2.1 Add Check-In Task

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

Before You Start

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

Steps

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

				Add Check-In Task	
🗆 Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-ті Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

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

7. Click Confirm.

17.2.2 Search Check-In Records

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

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

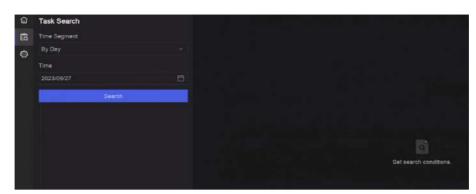


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

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

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception ~	HDD Full	
Notify Surveillance Center			
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	1.0001 > 0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

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

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- 1. Go to System → System Maintenance → Maintenance → Maintenance Tools .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

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

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-9632NXI-M8/X(M) DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 32-ch IP cameras can be connected, plug & play
- Intelligent analytics based on deep learning algorithm
- Up to 24-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 32-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading, support adding digital watermarks, and checks video integrity
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 8 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





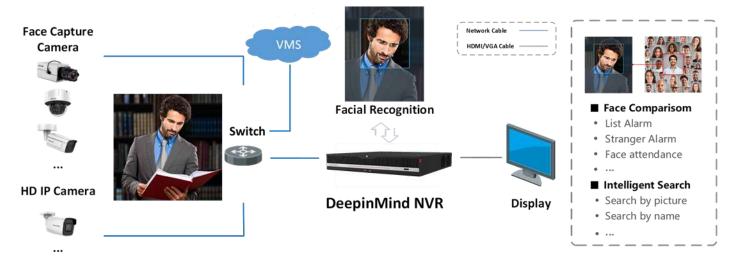
Network & Ethernet Access

- 2 self-adaptive 10M/100M/1000M Ethernet interfaces, with load balancing and multi-IP address
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen

Typical Application

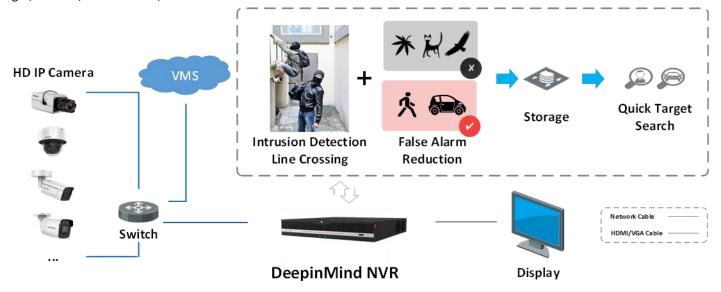
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

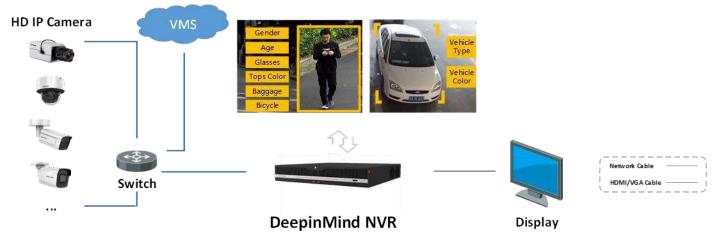
Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





.

Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from building
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, loitering, people running
Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Operating System	Linux
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face detection.
Face Picture Comparison (Captured from Camera)	32-ch (16-ch for each engine); Comparison speed: 48 pictures per second
Facial Detection and Analytics Performance	16-ch 2 MP (8-ch for each engine), up to 8 MP
Perimeter Protection	
By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
By Camera	All channels
Alarms	Support generates alarms of perimeter violation
Video Structuralization	
Structured Analysis	12-ch 2 MP (6-ch for each engine), up to 8 MP
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB)
Face Picture Comparison	16-ch; Comparison speed: 32 pictures per second
Throwing Objects from Building	
By NVR	16-ch 2 MP (8-ch for each engine), up to 8 MP)
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Vehicle brand, vehicle color, vehicle type
Plate Attributes	Plate number, license plate color, license plate type



.

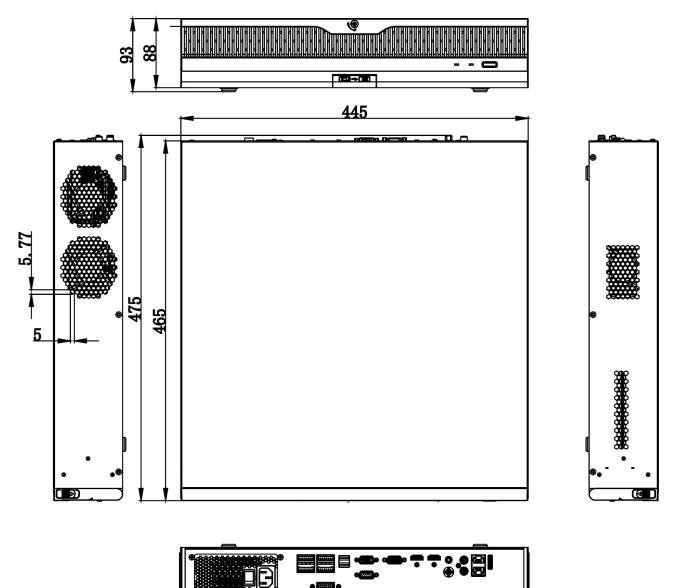
Video and Audio		
IP Video Input	32-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.	
Incoming Bandwidth	320 Mbps	
Outgoing Bandwidth	400 Mbps	
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.	
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz	
Video Output Mode	HDMI1 2.0/VGA1 simultaneous output, HDMI2 2.0/VGA2 simultaneous output	
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480	
Audio Output	2-ch, RCA (Linear, 1 KΩ)	
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)	
Decoding		
Decoding Format	H.265/H.265+/H.264/H.264+/MJPEG	
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25	
	fps)/16-ch@4 MP (30 fps)/32-ch@1080p (30 fps)	
Synchronous Playback	16-ch	
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x	
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.	
Recording Modes	Manual, schedule and event	
Network		
Remote Connection	128	
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTP, RTCP, SADP, SMTP, SNMP, SSH, FTP, SFTP, NFS, UDP, ISCSI, ISUP, UPnP™, HTTP, HTTPS	
API	ONVIF (profile S/G); SDK; ISAPI	
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version	
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface	
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)	



RAID	
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10
Auxiliary Interface	
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.
DC 12V	12 VDC, 1 A power output
SATA	8 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 14 TB capacity for each HDD
Serial Interface	1 RS-232, 1 RS-485 (full-duplex), 1 keyboard
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
Alarm In/Out	16/9
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian
Processor	64bits multi-core
Memory	RAM 16GB DDR4
Licensing	All features are fully perpetually licensed to operate standalone
File Lock	Support lock and unlock recorded files
Video Download	Batch and segment support
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others
Fans	Smart fan control
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	≤ 7 W (standby mode) (without HDD)
Working Temperature	-10 to 55° C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	445 × 465 × 93 mm (17.5"× 18.3" × 3.7"), 2U's
Weight	≤ 10 kg (without HDD, 28.7 lb.)
Certification	
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201
CE	9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020



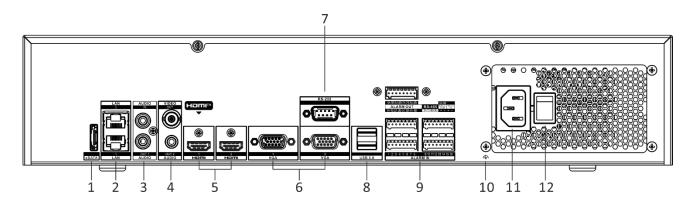
Dimension



scale/1:1;Unit/mm



Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces	8	USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface, Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

iDS-9632NXI-M8/X(M)



Follow us on social media to get the latest product and solution information.











Hikvision Corporate Channel



@Hikvision Digital Technology Co., Ltd. 2022 I Data subject to change without notice I

Storage Solution

Video Storage Parameters		
VideoStorage Parameters	Camera Type 1	
Channel Name	Device 1	
Channel Number	64	
Encoding Mode	H.265	
Resolution	1080P(1920×1080)	
Frame Rate	30	
Bitrate	2048	
Storage Time / Day (Hour)	24	
Storage Period (Day)	30	

NVR List Output				
NO.	Product Name	Brand	Model	Quantity
1	Storage Host	Hikvision	iDS-9664NXI-M8/X	1

Storage Requirements			
	Requirements	Now	Satisfaction
Storage	40TB	48TB	+8.00TB
Bandwidth	153Mbps	400Mbps	+247.00Mbps
Channel	64	64	+0.00



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-14/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

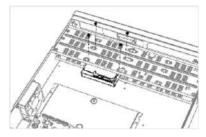


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

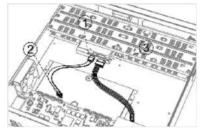


Figure 1-4 Connect Cable

INote

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.

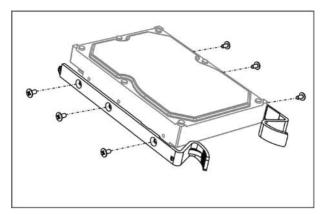


Figure 1-5 Fix Mounting Ears to HDD

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

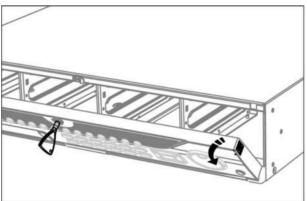


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

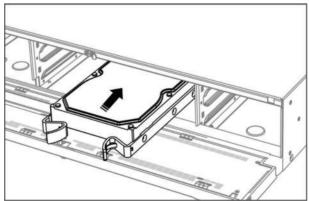


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

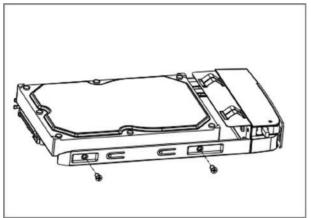


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

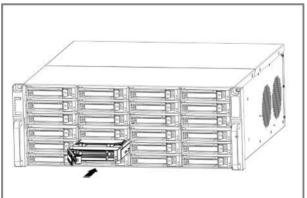


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

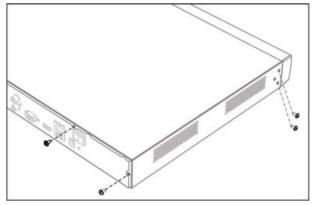


Figure 1-10 Remove Cover

- 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.

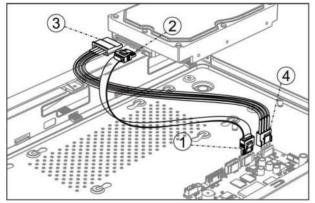


Figure 1-11 Connect Cables

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

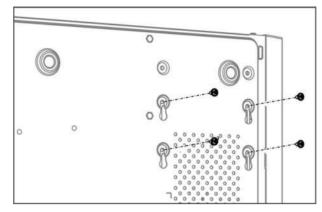


Figure 1-12 Fix HDD to Device Bottom

- 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.

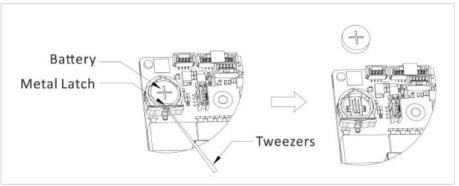


Figure 1-1 Remove Battery

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

iNote

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

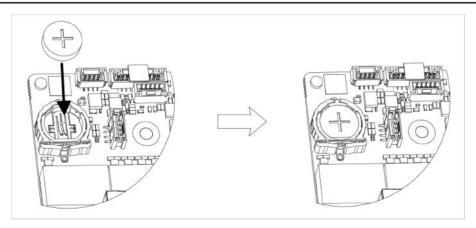


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	0
6.1 Access Video Device	0
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	0
6.1.3 Add Network Camera through PoE 2	1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	2
6.1.5 Add Network Camera via Custom Protocol 2	2
6.1.6 Add Network Camera through Camera Configuration File	4
6.2 Add Access Control Device 24	4
6.3 Add Audio Device 2	4
6.4 Add POS Device 2	5
6.5 Channel Management 2	6
Chapter 7 Device Grouping 2	7
Chapter 8 Video or Audio Device Settings 2	8
8.1 Enable H.265 Stream Access 2	8
8.2 Configure Display Settings 2	8
8.3 Configure Video Parameters 2	9
8.4 Configure Privacy Mask 2	9
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	1
8.8 Configure PoE (Power over Ethernet) Interface 3	2
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	4
9.2 RAID Configuration 3	4
9.2.1 Create Disk Array 3	5
9.2.2 Rebuild Array 3	6
9.2.3 Delete Array 3	7
9.2.4 View Firmware Info	7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	-3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library	85
16.4.2 Upload Face Pictures to the Library	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
8	•••••	
A		
0		
When yo recomme	u forget your password, the hint will help you remember. It is inded to set the hint.	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)			Nore 🔲 Show Peerw	ord			O device(a) connected.
Viteo Device	Device Na. : P Addre	os = Network =	Passwor. Show Pa.	Protocol	Manage : AddesiTotal	Serial No. +	Version :
Access Control Device							
Altim Device							
Auto Device							
POS							
Device Grouping							
Device Configuration 🔗							
Device Parameter							
Access Service							
Batch Contiguration	Online Device List (0)						
			efresh:				
Menu Bar	IP Address I Device	fociel : Status	Protocol	Manage) Serial No 2	Errwan	r 3 Physical

Figure 3-2 Menu Bar Example

Destrict 09:07		e	Section of	O Parat March	(a) Property t	Contract store	e ::
Venice Capture 2	Person Clipfure	iu:				Target Recognition	
lenu Bar	00-77	-2023 Wed 09:07:47					
	1.001.000						
				Conver	2010-		
					SA 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP		Main NIC	LANI	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

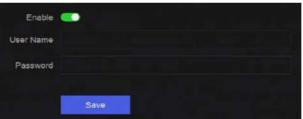


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

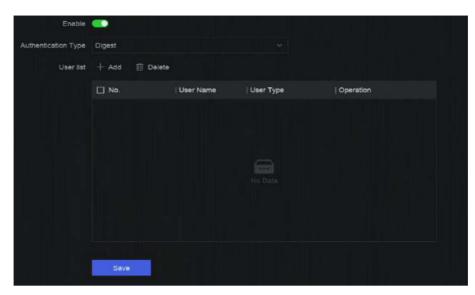


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description				
0	Set account security.				
Add	dd a new guest or operator user.				
Ū	Delete the selected user.				

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

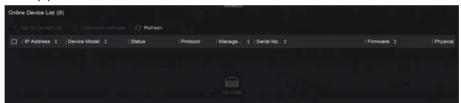


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×
Online Device List (0)	Refresh C
No. IP Address Device Model	Status Protocol Manag Serial Ne
	Data
IP Address *	Device Name *
Test	IPCamera 01
Protocol	Management Port *
ONVIF · Protocol Manag	80
User Name	Password
admin	
Transfer Protocol	Use Channel Default Password
Auto ~	

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Management					×			
HIKVISION_RTSP	Check your device URL and enter accordingly. Format [Type]//IP Address][Port]/Path]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [*Type*]://[*IP Address*]:[*Port*]/[*Resource Path*], for example, *rtsp:*//192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🗌 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click Import to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	👄)
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

			HOWHIN HOO		Remaining capeci
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WK82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	O rigital	TYDG YESHDINNAPTS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description		
One-touch Array Configuration	Click One-touch Array Configuration.		
	i Note		
	By default, the array type created by one-touch configuration is RAID 5.		
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.		

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \boxed{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	4 68/7814 68				
+ Add Resource 🛛 🖾 🗆					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.

Parameter Name	Description	
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag. 	
eSATA	For devices with eSATA interface at the rear panel.	
Usage	Set the usage for eSATA.	

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

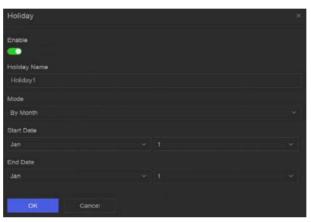


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

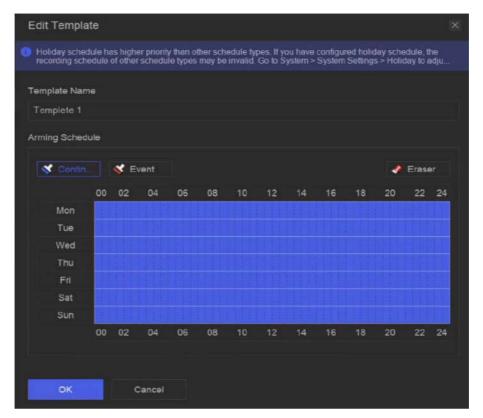


Figure 10-2 Edit Template

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

i Note

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

iNote

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

6. Click OK.

10.2 Configure Recording Schedule

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

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carnera 01		Oustom		
D2) IPCamera 02		Custom		
] [03] IPCamera 03		Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

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

INote

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

4. Click View to view the schedule.



Figure 10-4 View Schedule

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

Table 10-1 Advanced Parameter Description

Parameter	Description	
Record Audio	Enable or disable audio recording.	

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

7. Click Save.

10.3 Configure Picture Capture Schedule

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

Steps

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

Batch Schedule Configuration	Batch Advanced Configuration	Z Configure Template		
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01		Custom		
02] (02] IPCamera 02		Custom		
03] IPCamera 03		Custom		
[04] IPCamera 04		Custom		

Figure 10-5 Picture Capture Configuration

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

iNote

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

4. Click View to view the schedule.

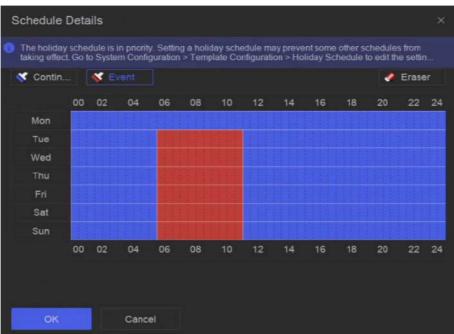


Figure 10-6 View Schedule

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

Table 10-2 Advanced Parameter Description

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

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

10.4 Configure Audio Recording

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

Steps

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

iNote

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

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

Table 10-3 Advanced Parameter Description

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

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

Chapter 11 Live View

11.1 Configure Live View Layout

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

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

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



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



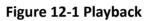


Table 12-1 Interface Description

No.	Description	
1	Area for selecting playback type.	
2	Channel list.	
3	Calendar for time selection.	
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext. 	
	the corresponding event rule. Refer to the event configuration steps for details of each event type.	

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

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

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

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

3. Select a date in the calendar.

iNote

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

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

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

Before You Start

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

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

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

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

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

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

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

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

12.5 Sub-Period Playback

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

Steps

1. Go to Playback → 🔜 .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

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

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Detection the mov	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Con	figuration
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording to configure video recording schedule.	

8. Click Save.

13.1.2 Perimeter Protection

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

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V		
AI by NVR	•		
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting		
Enable			
	Rule Settings Arming Schedule Linkage Method Shalid Area		
	1 2 3 4		
Rule List			
	01-62-2824 Tue: 14:68:36		
	B		
	Camera 01		
	Save		

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record When an alarm is detected, the selected channel would revideos.		
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Description Rule Configuration	
	be triggered when a human face is detected.		
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center	
		Comparison	
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.	
		Non-Real-Time Mode	
		For places with a high flow of people, the device processing speed may not be fast	

Event Name	Event Description	Rule Configuration		
		 enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed 		
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .		
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-		

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

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

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description	
Fire Detection	An alarm would be triggered when fire is detected in the arming area.	
Temperature Detection	An alarm would be triggered when the temperature exceed the threshold value.	

6. Click Arming Schedule to select an arming schedule type.

iNote

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

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	iNote	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
	It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemere 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diserming		
D3] IPCamera 03	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disarming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
D6] IPCamera 06		Disabled	Quick Diseming		
[D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 [010] IPCamera 10		Disabled	Quick Disaming		
🔲 (D11) IPCamera 11		Disabled	Quick Diseming		
[] [D12] IPCamera 12	-	Disabled	Quick Disaming		
[D13] IPCamera 13	•0	Disabled	Quick Disaming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration** or **System** \rightarrow **Event Configuration** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

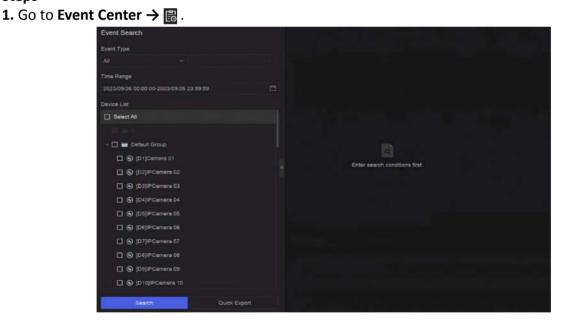


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

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

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Sand Services - Constraint State	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August and a	DTE weeks 01 22340	CTTC-Annual III Annual	
13		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Delauf Droup					
	C (D1)Cerners 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamera 03					
	🗶 🚱 (05)/PCamers 06					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)(PCamera 05					
	🖉 💬 (010)/PCarrent 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

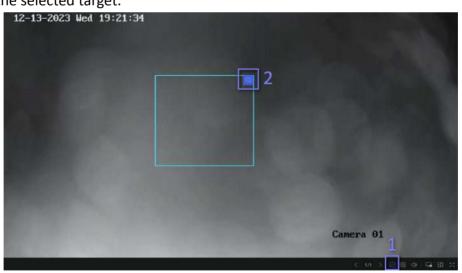


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-2200 101208.01	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canesa 02			
🗷 🕲 (DipPCament Di			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silenty	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

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

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

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

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

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

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

Disabled

No analysis task is enabled on the camera.

Waiting

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

Enabled

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

16.4 List library Management

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

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

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

16.4.2 Upload Face Pictures to the Library

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

Before You Start

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

Steps

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

Delete Pictures from
the Library

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

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

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

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

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

17.2 Person Check-In

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

17.2.1 Add Check-In Task

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

Before You Start

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

Steps

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

				Add Check-In Task	
Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-т Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

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

7. Click Confirm.

17.2.2 Search Check-In Records

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

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

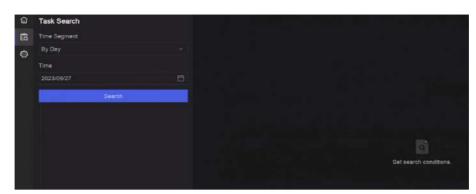


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

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

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception ~	HDD Full	
Notify Surveillance Center	•		
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	1.0001 > 0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

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

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- **1.** Go to **System → System Maintenance → Maintenance → Maintenance Tools** .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

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

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Ф5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-9664NXI-M8/X DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 64-ch IP cameras can be connected, plug & play
- Intelligent analytics based on deep learning algorithm
- Up to 24-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 48-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading and AES256 encription
- Support adding digital watermarks, and checks video integrity
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 8 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





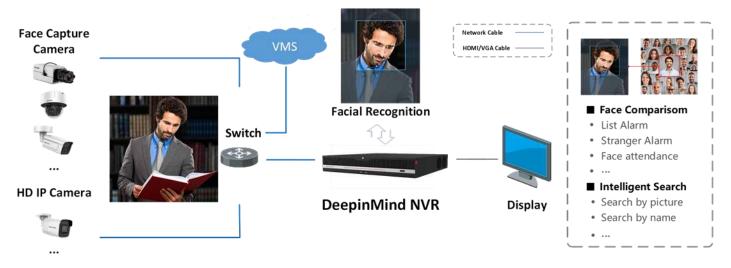
Network & Ethernet Access

- 2 self-adaptive 10M/100M/1000M Ethernet interfaces, with load balancing and multi-IP address
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen
- Operates with Video Wall over network

Typical Application

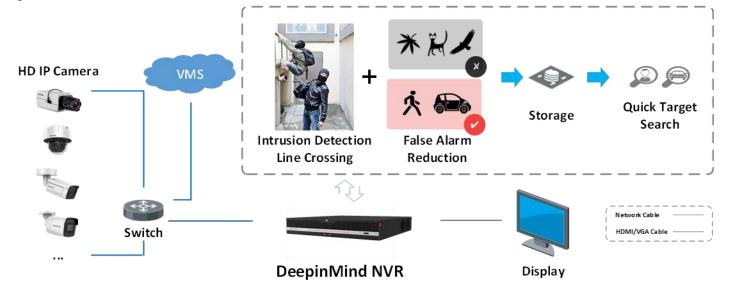
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

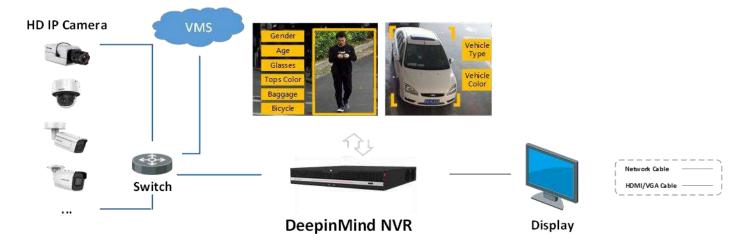
Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





.

Specification

Al by NNRFicial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCAQ lottering, people runningGPU Engine2, each engine can run an intelligent algorithm, engine mode is adjustableGPU Engine2, each engine can run an intelligent algorithm, engine mode is adjustableGPU Engine2, each engine can run an intelligent algorithm, engine mode is adjustableGPU Engine6Gradareognition5Facial Detection and AnalyticsFacial cace true is stranger library, up to 10,000,006 face pictures in face capture (each picture 4 ANB, total capacity 5 20 GB), Generates alarms for list library, up to 10,000,006 face pictures in face capture (each picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of size capture (each picture 4 ANB, total capacity 5 20 GB), Generates alarms for list motion of Generates and and total capacity 5 20 GB).Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection6Portection	Intelligent Analytics	
Al by Camerabuilding, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, 	AI by NVR	
Operating SystemLinuxFacial RecognitionFacial Detection and AnalyticsFace picture comparison, human face capture, face picture searchFace Picture LibraryUp to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000Face Picture Library& Sace (24-ch for each engine); Comparison speed: 48 pictures per secondFace Picture Comparison& Ch (24-ch for each engine), up to 8 MPPerimeter Protection& Support generates alarms of primeter violationBy NVR24-ch 2 MP (8-ch for each engine), up to 8 MPPorture LibraryUp to 32 face picture sin generates alarms of primeter violationYoure Structuralization21-ch 2 MP (6-ch for each engine), up to 8 MPPorture Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPStructure Analysis12-ch 2 MP (6-ch for each engine), up to 0,000 face pictures in list library, up to 10,000Face Picture LibraryUp to 32 face picture library in to 10,000 face pictures in list library, up to 10,000Face Picture Comparison12-ch 2 MP (6-ch for each engine), up to 8 MPOptimum Structuralization12-ch 2 MP (6-ch for each engine), up to 10,000,000 face pictures in face capture (each picture si natioger library library) up to 10,000,000 face pictures in face capture (each picture si a structure domains)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondRational Comparison Speed: 32 pictures per second16-ch; Comparison speed: 32 pictures per secondRational Comparison16-ch; Comparison speed: 32 pictures per secondRational Comparison16-ch; Comparison speed: 32 pictu	AI by Camera	building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA,
Facial RecognitionFacial Detection and AnalyticsFace picture comparison, human face capture, face picture searchFace Picture LibraryUp to 32 face picture libraries, up to 10,000 face pictures in fist library, up to 10,000Face Picture LibraryUp to 32 face picture libraries, up to 10,000,000 face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB). Generates alarms for list match and strange face detection.Face Picture Comparison48-ch (24-ch for each engine); Comparison speed: 48 pictures per secondFacial Detection and Analytics16-ch 2 MP (8-ch for each engine), up to 8 MPPerimance9PorimanceAll channelsSupport generates alarms of perimeter violationYote Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 0,000 face pictures in list library, up to 10,000Face Picture Library10 to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondFace Picture Comparison16-ch; Comparison speed: 32 pictures per secondFace Picture Comparison16-ch; Comparison speed: 32 pictures per secondFace Picture Comparison16-ch 2 MP (8-ch for each engine), up to 3,000,000 face pictures in face capture (each picture s 4 MB, total capacity s 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondFace Picture Comparison16-ch; Comparison speed: 32 pictures per secondRums0 Support generates alarms based on the Video Struc	GPU Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Facial Detection and Analytics Face picture comparison, human face capture, face picture search Pace Picture Library Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in list capture (each picture ≤ 4 MB, total capacity ≤ 20 GB). Generates alarms for list match and strange face detection. Face Picture Comparison d8-ch (24-ch for each engine); Comparison speed: 48 pictures per second Facial Detection and Analytics B-ch 2 MP (8-ch for each engine), up to 8 MP Perimeter Protection All channels Ry NNR 24-ch 2 MP (12-ch for each engine), up to 8 MP By Camera All channels Alarms Support generates alarms of perimeter violation Face Picture Library 10-ch 2 MP (6-ch for each engine), up to 8 MP Face Picture Library 10-ch 2 MP (6-ch for each engine), up to 8 MP Support generates alarms of perimeter violation 10-ch 2 MP (6-ch for each engine), up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB) Face Picture Comparison 16-ch 2 MP (6-ch for each engine), up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB) Face Picture Comparison 16-ch 2 Comparison speed: 32 pictures per second Comparison speed: 32 pictures per second Comparison speed: 32 pictures per second Aures Suport g	Operating System	Linux
Face Picture LibraryUp to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB). Generates alarms for list match and strange face detection.Face Picture Comparison48-ch (24-ch for each engine); 	Facial Recognition	
Face Picture Libraryface pictures in stranger library, up to 10,000,000 face pictures in face capture (each discussion discussion)Face Picture Comparisondetection.facial Detection and Analyticcomparison speed: 48 pictures per secondFeriormancecomparison speed: 48 pictures per secondPerimeter Protectiondetection.Pay NVR24-ch 2 MP (8-ch for each engine), up to 8 MPBy NVR24-ch 2 MP (12-ch for each engine), up to 8 MPAuransdu IchanelsAuransduport genetes alarms of perimeter violationPreturet Protection12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 9,0000 face pictures in face capture (each engine), up to 32 face picture in stranger library, up to 10,0000 face pictures in face capture (each engine), up to 32 face picture in stranger library, up to 10,0000 face pictures in face capture (each engine), up to 32 face picture si mass alarms based on the Video Structuralization features detectionFace Picture Comparison6-ch;Graphardy16-ch 2 MP (8-ch for each engine), up to 8 MPFace Picture Strometure16-ch 2 MP (8-ch for each engine), up to 8 MP<	Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
(Captured from Camera)Comparison speed: 48 pictures per secondFacial Detection and Analytics Performance16-ch 2 MP (8-ch for each engine), up to 8 MPPerimeter Protection24-ch 2 MP (12-ch for each engine), up to 8 MPBy NVRAll channelsBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Changysis12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in fiscl library, up to 10,000 face pictures in stranger library, up to 100,000 face pictures in face capture (each picture 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmssupport generates alarms based on the Video Structuralization features detectionMNR6-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsBy CameraAll channelsAurona16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsBy CameraAll channelsBy CameraAll channelsBy CameraAll channelsAuronaStructure all color, license plate type	Face Picture Library	face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face
Performance16-ch 2 MP (8-ch for each engine), up to 8 MPPerimeter ProtectionBy NVR44-ch 2 MP (12-ch for each engine), up to 8 MPBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPStructured Analysis12-ch 2 MP (6-ch for each engine), up to 10,0000 face pictures in list library, up to 10,000Face Picture LibraryUp to 32 face picture libraries, up to 100,0000 face pictures in stranger library, up to 10,0000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture ComparisonSupport generates alarms based on the Video Structuralization features detection omparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detectionBy NVR16-ch; comparison speed: 32 pictures per secondBy NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens16-ch 2 MP (8-ch fo	···· · ···	
By NVR24-ch 2 MP (12-ch for each engine), up to 8 MPBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Analysis12-ch 2 MP (6-ch for each engine), up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 100,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison6-ch; comparison speed: 32 pictures per secondAlarmssupport generates alarms based on the Video Structuralization features detectionFrowing Objects from Buildie16-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens10-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurensMI channelsPlate AttributesPlate number, license plate color, license plate type	-	16-ch 2 MP (8-ch for each engine), up to 8 MP
By CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo StructuralizationStructured Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detectionThrowing Objects from Building By CameraAll channelsANPRAll channelsBy CameraAll channelsPlate number, license plate color, license plate type	Perimeter Protection	
AlarmsSupport generates alarms of perimeter violationAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPStructured Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detectionPareman16-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsANPR11 channelsBy CameraAll channelsPlate number, license plate color, license plate type	By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
Video Structuralization Structured Analysis 12-ch 2 MP (6-ch for each engine), up to 8 MP Face Picture Library Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in face capture (each picture S 4 MB, total capacity S 20 GB) Face Picture Comparison 16-ch; Comparison speed: 32 pictures per second Alarms Support generates alarms based on the Video Structuralization features detection Throwing Objects from Building 16-ch 2 MP (8-ch for each engine), up to 8 MP) By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR Il channels By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By Camera	All channels
Structured Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture < 4 MB, total capacity < 20 GB)	Alarms	Support generates alarms of perimeter violation
Face Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detectionFhrowing Objects from Building16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsBy CameraAll channelsPlate AttributesPlate number, license plate color, license plate type	Video Structuralization	
Face Picture Libraryface pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detection Throwing Objects from Building 16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channels ANPR Plate number, license plate color, license plate type	Structured Analysis	12-ch 2 MP (6-ch for each engine), up to 8 MP
Face Picture ComparisonComparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detection Throwing Objects from Building By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channels ANPR By CameraAll channelsPlate AttributesPlate number, license plate color, license plate type	Face Picture Library	face pictures in stranger library, up to 10,000,000 face pictures in face capture (each
Throwing Objects from Building By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR International statements By Camera All channels Plate Attributes Plate number, license plate color, license plate type	Face Picture Comparison	/
By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR International All channels Plate Attributes Plate number, license plate color, license plate type	Alarms	Support generates alarms based on the Video Structuralization features detection
By Camera All channels ANPR By Camera By Camera All channels Plate Attributes Plate number, license plate color, license plate type	Throwing Objects from Building	
ANPR By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By NVR	16-ch 2 MP (8-ch for each engine), up to 8 MP)
By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By Camera	All channels
Plate Attributes Plate number, license plate color, license plate type	ANPR	
	By Camera	All channels
Vehicle Attributes Vehicle brand, vehicle color, vehicle type	Plate Attributes	Plate number, license plate color, license plate type
	Vehicle Attributes	Vehicle brand, vehicle color, vehicle type



Video and Audio	
IP Video Input	64-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth	400 Mbps
Outgoing Bandwidth	400 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Video Output Mode	HDMI1 2.0/VGA1 simultaneous output, HDMI2 2.0/VGA2 simultaneous output
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	2-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+/MJPEG
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)/32-ch@1080p (30 fps)/ 64-ch@720p (30 fps)
Synchronous Playback	16-ch
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Recording Modes	Manual, schedule and event
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTP, RTCP, SADP, SMTP, SNMP, SSH, FTP, SFTP, NFS, UDP, iSCSI, ISUP, UPnP™, HTTP, HTTPS
API	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)
RAID	
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10

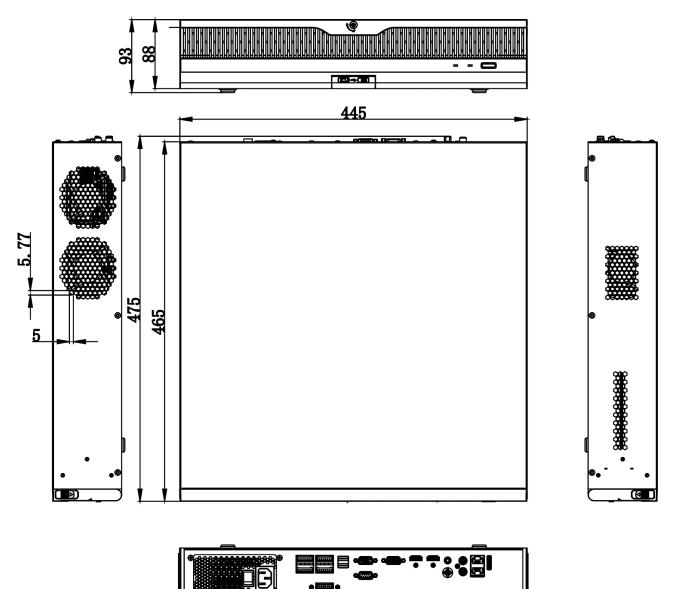


- •

Auxiliary Interface		
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.	
DC 12V	12 VDC, 1 A power output	
SATA	8 SATA interfaces; 3.5-inch HDD	
eSATA	1 eSATA interface	
Capacity	Up to 14 TB capacity for each HDD	
Serial Interface	1 RS-232, 1 RS-485 (full-duplex), 1 keyboard	
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0	
Alarm In/Out	16/9	
General		
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian	
Power Supply	100 to 240 VAC, 50 to 60 Hz	
Processor	64bits multi-core	
Memory	RAM 8GB DDR4	
Compute Power	2 TOPS	
Licensing	All features are fully perpetually licensed to operate standalone	
File Lock	Support lock and unlock recorded files	
Video Download	Batch and segment support	
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others	
Fans	Smart fan control	
Consumption	≤ 100 W	
Working Temperature	-10 to 55° C (14 to 131° F)	
Working Humidity	10 to 90%	
Dimension ($W \times D \times H$)	445 × 465 × 93 mm (17.5"× 18.3" × 3.7"), 2U's	
Weight	\leq 10 kg (without HDD, 28.7 lb.)	
Certification		
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS	
FCC	Part 15 Subpart B, ANSI C63.4-2014	
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201	
	9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020	



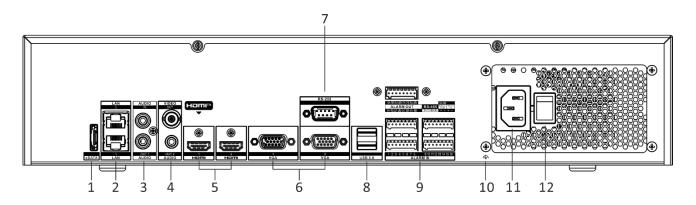
Dimension



scale/1:1;Unit/mm



Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces	8	USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface, Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

iDS-9664NXI-M8/X



Follow us on social media to get the latest product and solution information.











Hikvision Corporate Channel



@Hikvision Digital Technology Co., Ltd. 2022 | Data subject to change without notice |

Storage Solution

Video Storage Parameters			
VideoStorage Parameters	Camera Type 1		
Channel Name	Device 1		
Channel Number	16		
Encoding Mode	H.265		
Resolution	1080P(1920×1080)		
Frame Rate	30		
Bitrate	2048		
Storage Time / Day (Hour)	24		
Storage Period (Day)	30		

NVR List Output				
NO.	Product Name	Brand	Model	Quantity
1	Storage Host	Hikvision	iDS-9616NXI-M8/X	1

Storage Requirements			
	Requirements	Now	Satisfaction
Storage	10ТВ	12TB	+2.00TB
Bandwidth	38Mbps	320Mbps	+282.00Mbps
Channel	16	16	+0.00



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-14/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

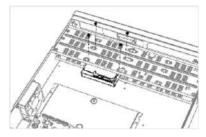


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

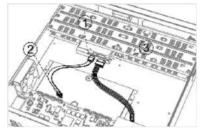


Figure 1-4 Connect Cable

INote

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.

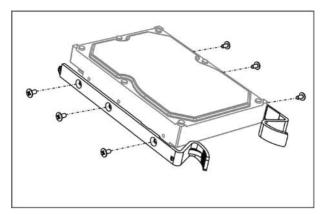


Figure 1-5 Fix Mounting Ears to HDD

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

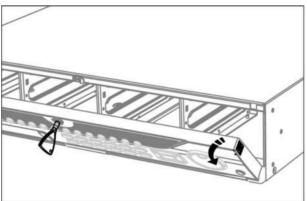


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

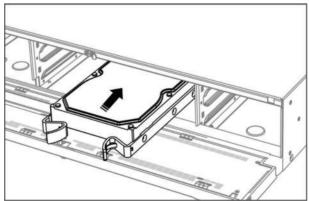


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

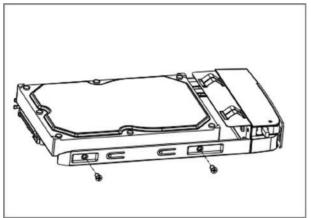


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

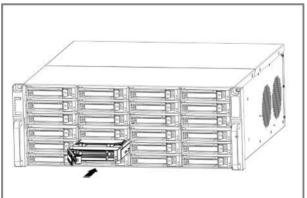


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

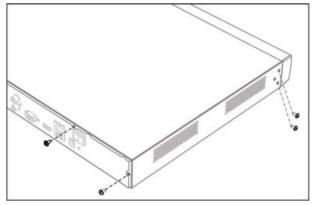


Figure 1-10 Remove Cover

- 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.

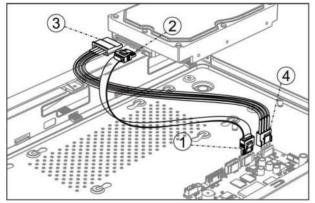


Figure 1-11 Connect Cables

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

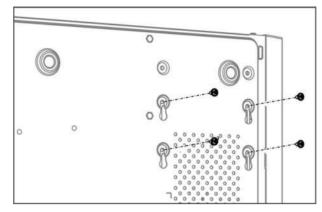


Figure 1-12 Fix HDD to Device Bottom

- 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.

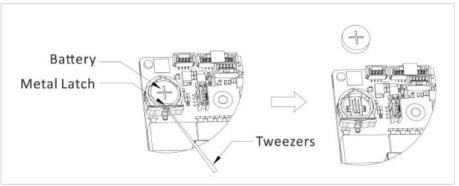


Figure 1-1 Remove Battery

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

iNote

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

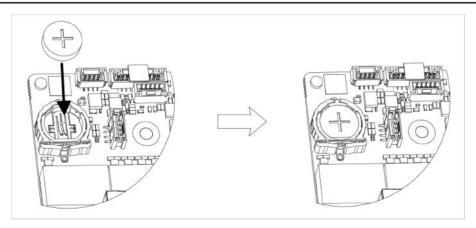


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	0
6.1 Access Video Device	0
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	0
6.1.3 Add Network Camera through PoE 2	1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	2
6.1.5 Add Network Camera via Custom Protocol 2	2
6.1.6 Add Network Camera through Camera Configuration File	4
6.2 Add Access Control Device 24	4
6.3 Add Audio Device 2	4
6.4 Add POS Device 2	5
6.5 Channel Management 2	6
Chapter 7 Device Grouping 2	7
Chapter 8 Video or Audio Device Settings 2	8
8.1 Enable H.265 Stream Access 2	8
8.2 Configure Display Settings 2	8
8.3 Configure Video Parameters 2	9
8.4 Configure Privacy Mask 2	9
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	1
8.8 Configure PoE (Power over Ethernet) Interface 3	2
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	4
9.2 RAID Configuration 3	4
9.2.1 Create Disk Array 3	5
9.2.2 Rebuild Array 3	6
9.2.3 Delete Array 3	7
9.2.4 View Firmware Info	7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library	85
16.4.2 Upload Face Pictures to the Library	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
8	•••••	
A		
0		
When yo recomme	u forget your password, the hint will help you remember. It is inded to set the hint.	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)			Nore 🔲 Show Peerw	ord			O device(a) connected.
Viteo Device	Device Na. : P Addre	os = Network =	Passwor. Show Pa.	Protocol	Manage : AddesiTotal	Serial No. +	Version :
Access Control Device							
Altim Device							
Auto Device							
POS							
Device Grouping							
Device Configuration 🔗							
Device Parameter							
Access Service							
Batch Contiguration	Online Device List (0)						
			efresh:				
Menu Bar	IP Address I Device	fociel : Status	Protocol	Manage) Serial No 2	Errwan	r 3 Physical

Figure 3-2 Menu Bar Example

Destring Cardina		e	Section of	O Parat March	(a) Property t	Contract store	e ::
Venice Capture 2	Person Clipfure	iu:				Target Recognition	
lenu Bar	00-77	-2023 Wed 09:07:47					
	1.001.000						
				Conver	2010-		
					SA 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP		Main NIC	LANI	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

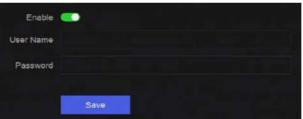


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

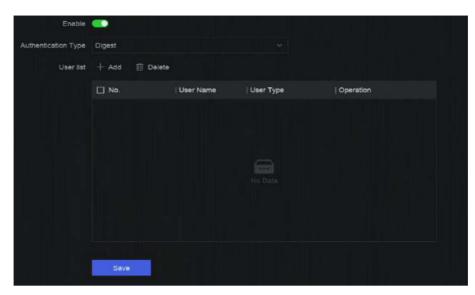


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description	
0	Set account security.	
Add	Add a new guest or operator user.	
Ū	Delete the selected user.	

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

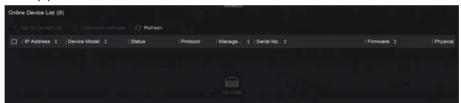


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×
Online Device List (0)	Refresh C
No. IP Address Device Model	Status Protocol Manag Serial Ne
	Data
IP Address *	Device Name *
Test	IPCamera 01
Protocol	Management Port *
ONVIF · Protocol Manag	80
User Name	Password
admin	
Transfer Protocol	Use Channel Default Password
Auto ~	

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Mana	gement							×
HIKVISION_RTSP	Check your device URL and enter accordingly. Format: [Type]//[P.Address][Port/[Path]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [Type]://[IP Address]:[Port]/[Resource Path], for example, rtsp://192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🗌 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	👄)
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

			HOWHIN HOO		Remaining capeci
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WK82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	O rigital	TYDG YESHDINNAPTS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description		
One-touch Array	Click One-touch Array Configuration.		
Configuration	i Note		
	By default, the array type created by one-touch configuration is RAID 5.		
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.		

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \boxed{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	4 68/7814 68				
+ Add Resource 🛛 🖾 🗆					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.

Parameter Name	Description		
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag. 		
eSATA	For devices with eSATA interface at the rear panel.		
Usage	Set the usage for eSATA.		

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

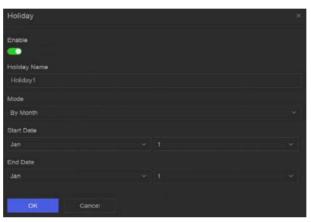


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

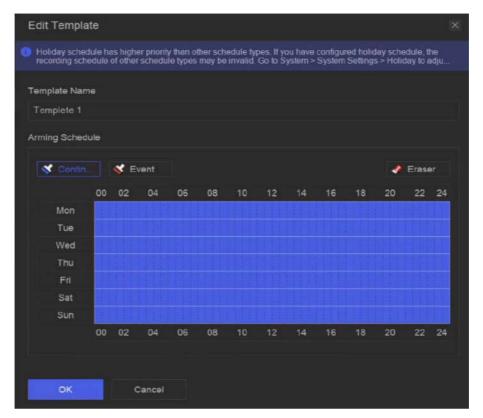


Figure 10-2 Edit Template

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

i Note

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

iNote

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

6. Click OK.

10.2 Configure Recording Schedule

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

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carnera 01		Oustom		
D2) IPCamera 02		Custom		
] [03] IPCamera 03		Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

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

INote

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

4. Click View to view the schedule.



Figure 10-4 View Schedule

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

Table 10-1 Advanced Parameter Description

Parameter	Description	
Record Audio	Enable or disable audio recording.	

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

7. Click Save.

10.3 Configure Picture Capture Schedule

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

Steps

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

Batch Schedule Configuration	Batch Advanced Configuration	Z Configure Template		
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01		Custom		
02] (02] IPCamera 02		Custom		
03] IPCamera 03		Custom		
[04] IPCamera 04		Custom		

Figure 10-5 Picture Capture Configuration

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

iNote

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

4. Click View to view the schedule.

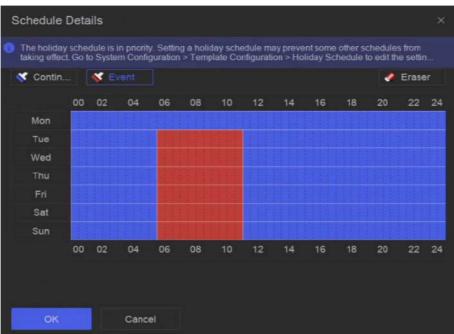


Figure 10-6 View Schedule

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

Table 10-2 Advanced Parameter Description

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

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

10.4 Configure Audio Recording

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

Steps

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

iNote

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

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

Table 10-3 Advanced Parameter Description

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

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

Chapter 11 Live View

11.1 Configure Live View Layout

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

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

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



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



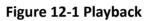


Table 12-1 Interface Description

No.	Description	
1	Area for selecting playback type.	
2	Channel list.	
3	Calendar for time selection.	
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext. 	
	the corresponding event rule. Refer to the event configuration steps for details of each event type.	

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

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

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

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

3. Select a date in the calendar.

iNote

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

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

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

Before You Start

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

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

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

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

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

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

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

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

12.5 Sub-Period Playback

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

Steps

1. Go to Playback \rightarrow \blacksquare .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

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

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Detection the mov	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Con	figuration
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording to configure video recording schedule.	

8. Click Save.

13.1.2 Perimeter Protection

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

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V		
AI by NVR	•		
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting		
Enable			
	Rule Settings Arming Schedule Linkage Method Shalid Area		
	1 2 3 4		
Rule List			
	01-62-2824 Tue: 14:68:36		
	B		
	Camera 01		
	Save		

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record When an alarm is detected, the selected channel would revideos.		
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Description Rule Configuration	
	be triggered when a human face is detected.		
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center	
		Comparison	
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.	
		Non-Real-Time Mode	
		For places with a high flow of people, the device processing speed may not be fast	

Event Name	Event Description	Rule Configuration		
		 enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed 		
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .		
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-		

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

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

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description	
Fire Detection	An alarm would be triggered when fire is detected in the arming area.	
Temperature Detection	An alarm would be triggered when the temperature exceed the threshold value.	

6. Click Arming Schedule to select an arming schedule type.

iNote

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

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	iNote	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
		It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemere 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diserming		
[D3] IPCamera 03	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disarming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
D6] IPCemere 06	•10	Disabled	Quick Diseming		
[D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 [010] IPCamera 10		Disabled	Quick Disaming		
🔲 (D11) IPCamera 11		Disabled	Quick Diseming		
[] [D12] IPCamera 12	-	Disabled	Quick Disaming		
[D13] IPCamera 13	•0	Disabled	Quick Disaming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration** or **System** \rightarrow **Event Configuration** $\rightarrow \bigotimes \rightarrow$ **Event Configuration** \rightarrow **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

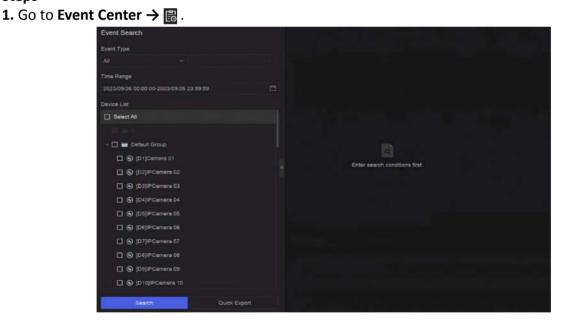


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

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

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Sand Services - Constraint State	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August a	DTE weeks 01 22340	CTTC-Annual III Annual	
123		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Delauf Droup					
	C (D1)Cerners 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamera 03					
	🗶 🚱 (05)/PCamers 06					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)(PCamera 05					
	🖉 💬 (010)/PCarrent 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

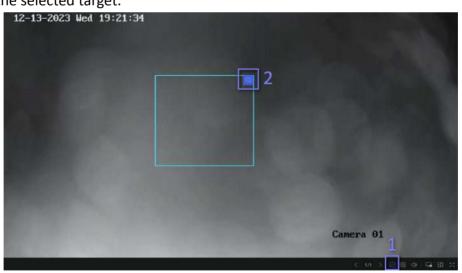


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-22003012000	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canesa 02			
🗷 🕲 (DipPCameni II)			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silenty	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

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

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

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

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

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

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

Disabled

No analysis task is enabled on the camera.

Waiting

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

Enabled

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

16.4 List library Management

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

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

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

16.4.2 Upload Face Pictures to the Library

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

Before You Start

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

Steps

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

Delete Pictures from
the Library

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

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

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

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

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

17.2 Person Check-In

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

17.2.1 Add Check-In Task

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

Before You Start

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

Steps

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

				Add Check-In Task	
Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-т Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

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

7. Click Confirm.

17.2.2 Search Check-In Records

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

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

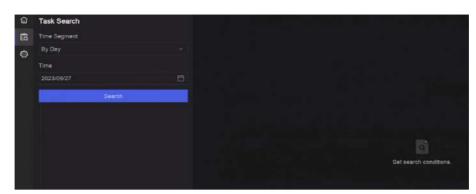


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

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

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception	HDD Full	
lotify Surveillance Center	•		
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	I anal >0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

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

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- **1.** Go to **System → System Maintenance → Maintenance → Maintenance Tools** .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

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

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Ф5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-9616NXI-M8/X DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 16-ch IP cameras can be connected, plug & play
- Intelligent analytics based on deep learning algorithm
- Up to 16-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 16-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading, support adding digital watermarks, and checks video integrity
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 8 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





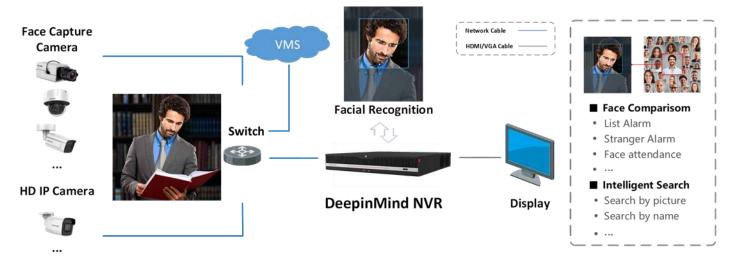
Network & Ethernet Access

- 2 self-adaptive 10M/100M/1000M Ethernet interfaces, with load balancing and multi-IP address
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen

Typical Application

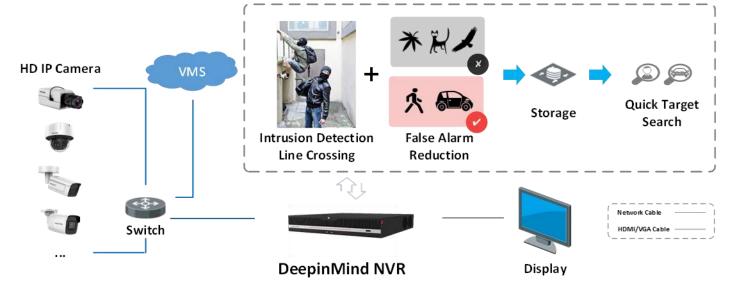
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





- •

Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from building
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, loitering, people running
Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Operating System	Linux
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face detection.
Face Picture Comparison (Captured from Camera)	16-ch (8-ch for each engine); Comparison speed: 48 pictures per second
Facial Detection and Analytics Performance	16-ch 2 MP (8-ch for each engine), up to 8 MP
Perimeter Protection	
By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
By Camera	All channels
Alarms	Support generates alarms of perimeter violation
Video Structuralization	
Structured Analysis	12-ch 2 MP (6-ch for each engine), up to 8 MP
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB)
Face Picture Comparison	16-ch; Comparison speed: 32 pictures per second
Throwing Objects from Building	
By NVR	16-ch 2 MP (8-ch for each engine), up to 8 MP)
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Vehicle brand, vehicle color, vehicle type
Plate Attributes	Plate number, license plate color, license plate type



.

Video and Audio	
IP Video Input	16-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth	320 Mbps
Outgoing Bandwidth	400 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Video Output Mode	HDMI1 2.0/VGA1 simultaneous output, HDMI2 2.0/VGA2 simultaneous output
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	2-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+/MJPEG
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)
Synchronous Playback	16-ch
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Recording Modes	Manual, schedule and event
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTCP, RTP, SADP, SMTP, SNMP, SSH, FTP, SFTP, NFS, UDP, ISCSI, ISUP, UPnP™, HTTP, HTTPS
ΑΡΙ	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)

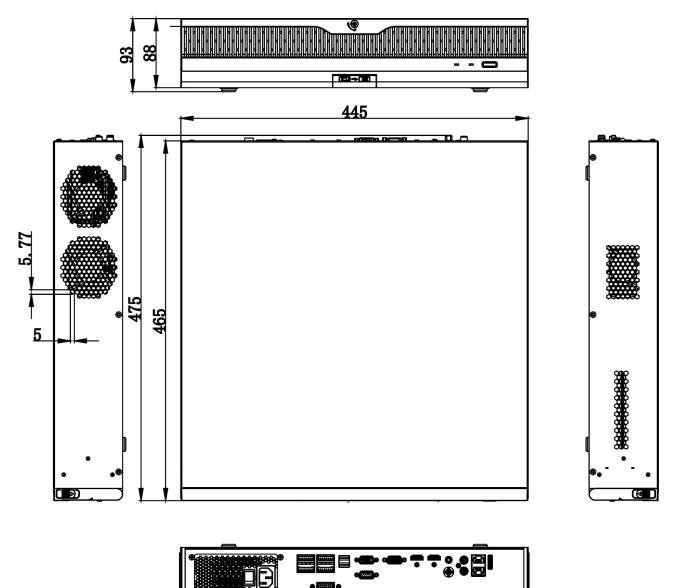


- •

RAID	
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10
Auxiliary Interface	
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.
DC 12V	12 VDC, 1 A power output
SATA	8 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 14 TB capacity for each HDD
Serial Interface	1 RS-232, 1 RS-485 (full-duplex), 1 keyboard
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0
Alarm In/Out	16/9
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian
Processor	64bits multi-core
Memory	RAM 8GB DDR4
Compute Power	2 TOPS
Licensing	All features are fully perpetually licensed to operate standalone
File Lock	Support lock and unlock recorded files
Video Download	Batch and segment support
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others
Fans	Smart fan control
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	≤ 100 W
Working Temperature	-10 to 55° C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	445 × 465 × 93 mm (17.5"× 18.3" × 3.7"), 2U's
Weight	≤ 10 kg (without HDD, 28.7 lb.)
Certification	
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201
	9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020



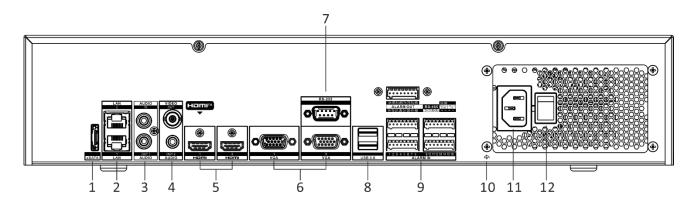
Dimension



scale/1:1;Unit/mm



Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces	8	USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface, Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

iDS-9616NXI-M8/X



Follow us on social media to get the latest product and solution information.











Hikvision Corporate Channel



@Hikvision Digital Technology Co., Ltd. 2022 I Data subject to change without notice I

Storage Solution

Video Storage Parameters		
VideoStorage Parameters	Camera Type 1	
Channel Name	Device 1	
Channel Number	32	
Encoding Mode	H.265	
Resolution	1080P(1920×1080)	
Frame Rate	30	
Bitrate	2048	
Storage Time / Day (Hour)	24	
Storage Period (Day)	30	

NVR List Output				
NO.	Product Name	Brand	Model	Quantity
1	Storage Host	Hikvision	iDS-9632NXI-M8/X	1

Storage Requirements				
	Requirements	Now	Satisfaction	
Storage	20ТВ	24TB	+4.00TB	
Bandwidth	76Mbps	320Mbps	+244.00Mbps	
Channel	32	32	+0.00	



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-14/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

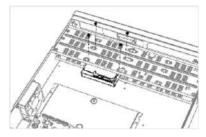


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

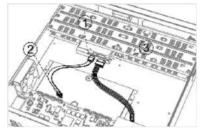


Figure 1-4 Connect Cable

INote

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.

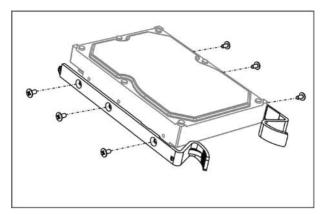


Figure 1-5 Fix Mounting Ears to HDD

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

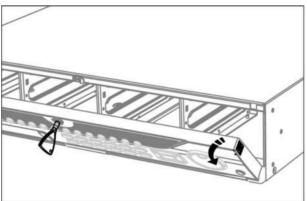


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

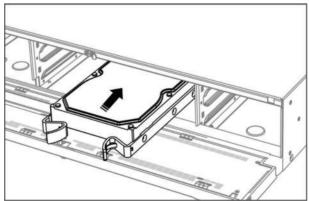


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

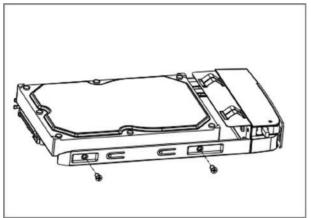


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

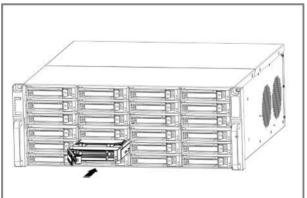


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

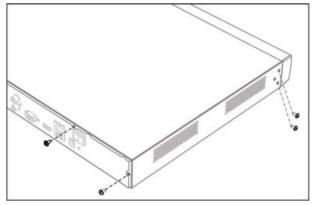


Figure 1-10 Remove Cover

- 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.

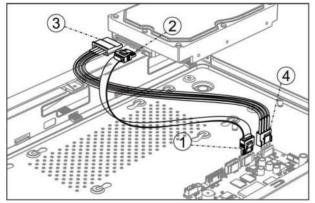


Figure 1-11 Connect Cables

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

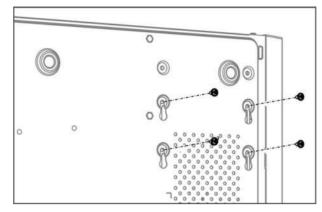


Figure 1-12 Fix HDD to Device Bottom

- 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.

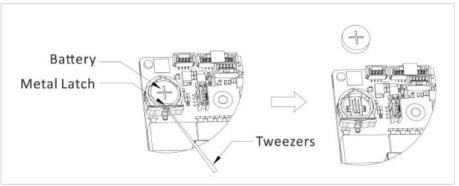


Figure 1-1 Remove Battery

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

iNote

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

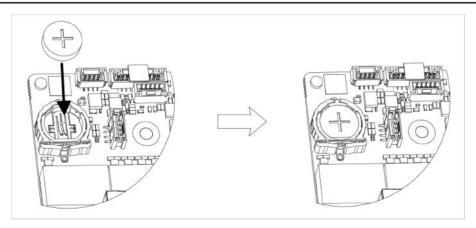


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	0
6.1 Access Video Device	0
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	20
6.1.3 Add Network Camera through PoE 2	!1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	22
6.1.5 Add Network Camera via Custom Protocol 2	22
6.1.6 Add Network Camera through Camera Configuration File	24
6.2 Add Access Control Device 2	24
6.3 Add Audio Device 2	24
6.4 Add POS Device 2	25
6.5 Channel Management 2	26
Chapter 7 Device Grouping 2	27
Chapter 8 Video or Audio Device Settings 2	28
8.1 Enable H.265 Stream Access 2	28
8.2 Configure Display Settings 2	28
8.3 Configure Video Parameters 2	29
8.4 Configure Privacy Mask 2	29
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	\$1
8.8 Configure PoE (Power over Ethernet) Interface 3	32
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	\$4
9.2 RAID Configuration 3	\$4
9.2.1 Create Disk Array 3	\$5
9.2.2 Rebuild Array	6
9.2.3 Delete Array 3	57
9.2.4 View Firmware Info	;7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters 3	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library	85
16.4.2 Upload Face Pictures to the Library	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
8	•••••	
A		
0		
When yo recomme	u forget your password, the hint will help you remember. It is inded to set the hint.	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)	+ Add Comment G Export G Import -	More D Show Paseword		0	devica() connected.
Viteo Device	Device Na. : IP Address : Network :	Passwor. Show Pa., Protocol	Manage_ : AddesiTotal	Serial No. : Verse	
Access Control Device					
Altim Device					
Auto Device					
POS					
Device Grouping					
Device Configuration 🔗					
Device Parameter					
Access Service					
Batch Configuration	Online Device List (0)				
Menu Bar					
Menu Bar	IP Address 1 Device Model 1 Status	Protocol Manage	8 Seriel No. 2	Firmware 2	Physical

Figure 3-2 Menu Bar Example

Description Construe		Constant of the second	and the second second	O Parant March	() Pasiers >	And States over	
Venice Capture	Person Clipture					 Target Recognition 	
enu Bar	09-77	-2023 Wed 09:07:47					
	RTA:	7.00.3 MEM 03.07.47					
					0000		
				Conce	w 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP		Main NIC	LANI	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

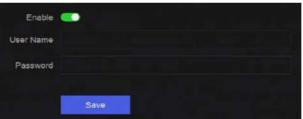


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

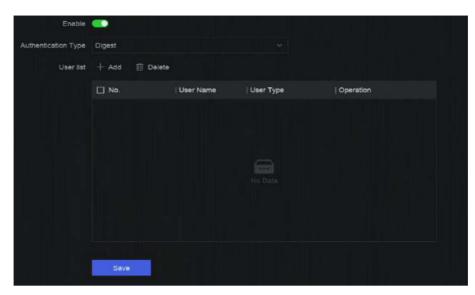


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description						
0	Set account security.						
Add	Add a new guest or operator user.						
Ū	Delete the selected user.						

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

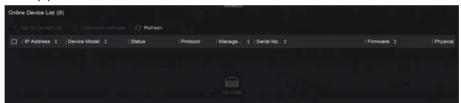


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×
Online Device List (0)	Refresh C
No. IP Address Device Model	Status Protocol Manag Serial Ne
	Data
IP Address *	Device Name *
Test	IPCamera 01
Protocol	Management Port *
ONVIF · Protocol Manag	80
User Name	Password
admin	
Transfer Protocol	Use Channel Default Password
Auto ~	

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Mana	gement							×
HIKVISION_RTSP	Check your device URL and enter accordingly. Format (Type)//IP Address)[Port/(Path)]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [Type]://[IP Address]:[Port]/[Resource Path], for example, rtsp://192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🗌 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click Import to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	👄)
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

			HOWHIN HOO		Remaining capeci
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WK82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	Constant	TYDG YESHDINNAPTS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description
One-touch Array Configuration	Click One-touch Array Configuration.
	i Note
	By default, the array type created by one-touch configuration is RAID 5.
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \boxed{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	M 68/7814 08				
+ Add Resource 🛛 🖾 🕬					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.

Parameter Name	Description
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

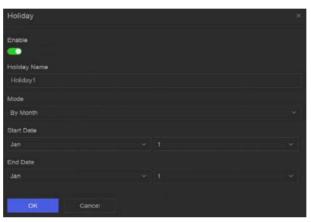


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

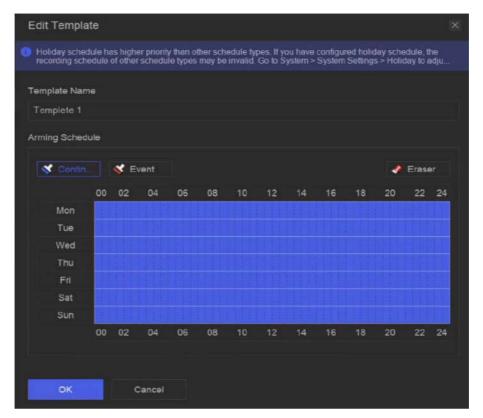


Figure 10-2 Edit Template

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

i Note

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

iNote

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

6. Click OK.

10.2 Configure Recording Schedule

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

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carnera 01		Oustom		
D2) IPCamera 02		Custom		
] [03] IPCamera 03		Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

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

INote

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

4. Click View to view the schedule.



Figure 10-4 View Schedule

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

Table 10-1 Advanced Parameter Description

Parameter	Description	
Record Audio	Enable or disable audio recording.	

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

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

7. Click Save.

10.3 Configure Picture Capture Schedule

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

Steps

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

Batch Schedule Configuration	Batch Advanced Configuration	Z Configure Template		
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01		Custom		
02] (02] IPCamera 02		Custom		
03] IPCamera 03		Custom		
[04] IPCamera 04		Custom		

Figure 10-5 Picture Capture Configuration

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

iNote

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

4. Click View to view the schedule.

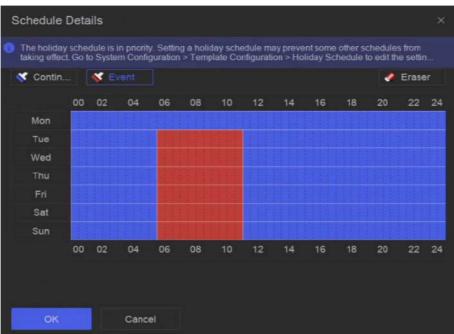


Figure 10-6 View Schedule

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

Table 10-2 Advanced Parameter Description

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

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

10.4 Configure Audio Recording

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

Steps

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

iNote

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

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

Table 10-3 Advanced Parameter Description

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

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

Chapter 11 Live View

11.1 Configure Live View Layout

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

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

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



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



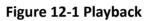


Table 12-1 Interface Description

No.	Description	
1	Area for selecting playback type.	
2	Channel list.	
3	Calendar for time selection.	
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext. 	
	the corresponding event rule. Refer to the event configuration steps for details of each event type.	

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

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

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

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

3. Select a date in the calendar.

iNote

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

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

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

Before You Start

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

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

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

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

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

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

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

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

12.5 Sub-Period Playback

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

Steps

1. Go to Playback → 🔜 .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

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

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Detection the mov	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Con	figuration
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording to configure video recording schedule.	

8. Click Save.

13.1.2 Perimeter Protection

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

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V		
AI by NVR	•		
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting		
Enable			
	Rule Settings Arming Schedule Linkage Method Shalid Area		
	1 2 3 4		
Rule List			
	01-62-2824 Tue: 14:68:36		
	B		
	Camera 01		
	Save		

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record When an alarm is detected, the selected channel would revideos.		
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

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

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

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

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Description Rule Configuration	
	be triggered when a human face is detected.		
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center	
		Comparison	
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.	
		Non-Real-Time Mode	
		For places with a high flow of people, the device processing speed may not be fast	

Event Name	Event Description	Rule Configuration		
		 enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed 		
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .		
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-		

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

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

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description	
Fire Detection	An alarm would be triggered when fire is detected in the arming area.	
Temperature Detection	An alarm would be triggered when the temperature exceed the threshold value.	

6. Click Arming Schedule to select an arming schedule type.

iNote

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

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	iNote	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
		It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	i Note	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemere 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diseming		
[D3] IPCamera 03	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disarming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
D6j iPCemere 06	•10	Disabled	Quick Diseming		
[D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 [010] IPCamera 10		Disabled	Quick Disaming		
🔲 (D11) IPCamera 11		Disabled	Quick Diseming		
🔲 [D12] IPCamera 12	-	Disabled	Quick Disaming		
[D13] IPCamera 13	•0	Disabled	Quick Disaming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of Notify Surveillance Center can be enabled or disabled in batches through Event Center $\rightarrow \bigotimes \rightarrow$ Event Configuration \rightarrow Batch Configuration or System \rightarrow Event Configuration $\rightarrow \bigotimes \rightarrow$ Event Configuration \rightarrow Batch Configuration. After an event is enabled, please click Go to Event Configuration to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

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

Steps

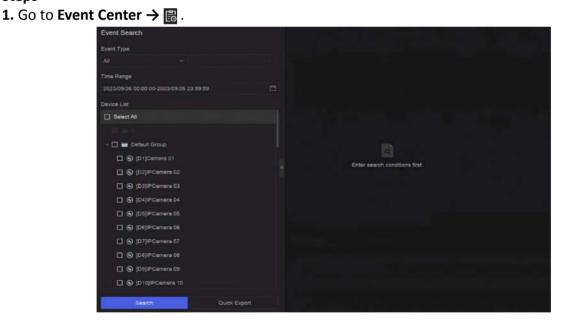


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

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

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Sand Services - Constraint State	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August and a	DTE weeks 01 22340	CTTC-Annual III Annual	
13		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Default Droup					
	C (D1)Cemere 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamera 03					
	🗶 🚱 (05)/PCamers 06					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)PCamera 05					
	🖉 💬 (010)/PCarrent 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - **5** Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

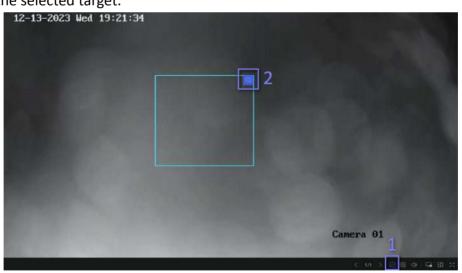


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-2200 101208.01	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canesa 02			
🗷 🕲 (DipPCameni II)			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silenty	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

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

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

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

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

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

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

Disabled

No analysis task is enabled on the camera.

Waiting

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

Enabled

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

16.4 List library Management

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

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

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

16.4.2 Upload Face Pictures to the Library

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

Before You Start

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

Steps

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

Delete Pictures from
the Library

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

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

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

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

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

17.2 Person Check-In

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

17.2.1 Add Check-In Task

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

Before You Start

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

Steps

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

				Add Check-In Task	
🗆 Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-ті Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

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

7. Click Confirm.

17.2.2 Search Check-In Records

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

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

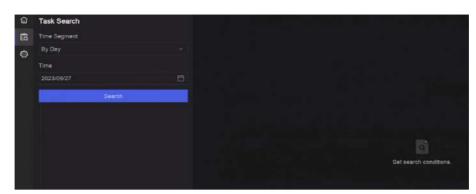


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

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

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception	HDD Full	
lotify Surveillance Center	•		
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	I anal >0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

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

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- **1.** Go to **System → System Maintenance → Maintenance → Maintenance Tools** .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

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

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Ф5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-9632NXI-M8/X DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 32-ch IP cameras can be connected, plug & play
- Intelligent analytics based on deep learning algorithm
- Up to 24-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 32-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading, support adding digital watermarks, and checks video integrity
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 8 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





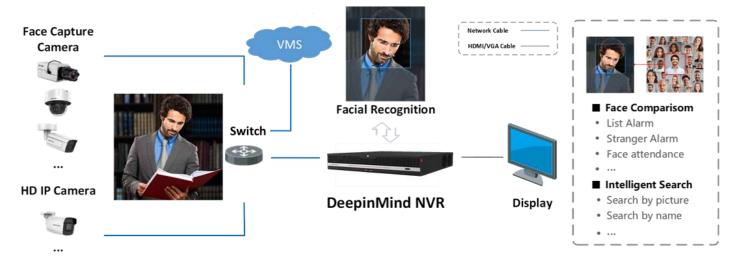
Network & Ethernet Access

- 2 self-adaptive 10M/100M/1000M Ethernet interfaces, with load balancing and multi-IP address
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen

Typical Application

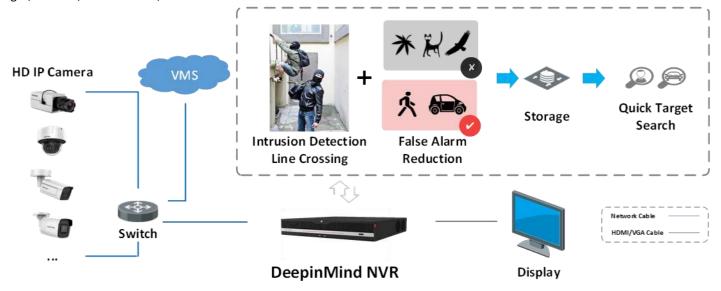
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

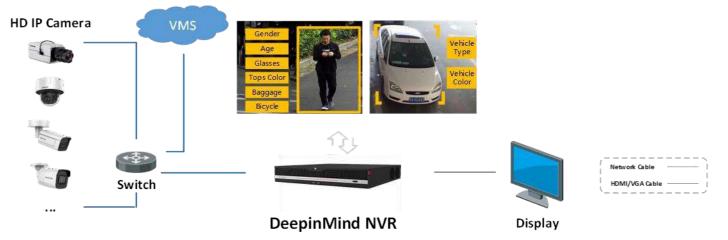
Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





. .

Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization, throwing objects from building
AI by Camera	Facial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, loitering, people running
Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable
Operating System	Linux
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face detection.
Face Picture Comparison (Captured from Camera)	32-ch (16-ch for each engine); Comparison speed: 48 pictures per second
Facial Detection and Analytics Performance	16-ch 2 MP (8-ch for each engine), up to 8 MP
Perimeter Protection	
By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP
By Camera	All channels
Alarms	Support generates alarms of perimeter violation
Video Structuralization	
Structured Analysis	12-ch 2 MP (6-ch for each engine), up to 8 MP
Face Picture Library	Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB)
Face Picture Comparison	16-ch; Comparison speed: 32 pictures per second
Throwing Objects from Building	
By NVR	16-ch 2 MP (8-ch for each engine), up to 8 MP)
By Camera	All channels
ANPR	
By Camera	All channels
Vehicle Attributes	Vehicle brand, vehicle color, vehicle type
Plate Attributes	Plate number, license plate color, license plate type



.

Video and Audio	
IP Video Input	32-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Incoming Bandwidth	320 Mbps
Outgoing Bandwidth	400 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Video Output Mode	HDMI1 2.0/VGA1 simultaneous output, HDMI2 2.0/VGA2 simultaneous output
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	2-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+/MJPEG
Deservice Construction	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25
Decoding Capability	fps)/16-ch@4 MP (30 fps)/32-ch@1080p (30 fps)
Synchronous Playback	16-ch
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.
Recording Modes	Manual, schedule and event
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTP, RTCP, SADP, SMTP, SNMP, SSH, FTP, SFTP, NFS, UDP, iSCSI, ISUP, UPnP™, HTTP, HTTPS
ΑΡΙ	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)

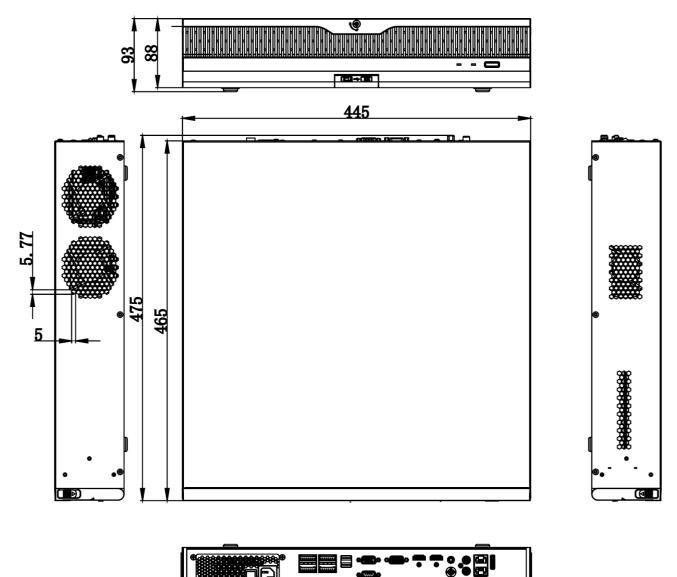


- •

2412		
RAID		
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10	
Auxiliary Interface		
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.	
DC 12V	12 VDC, 1 A power output	
SATA	8 SATA interfaces; 3.5-inch HDD	
eSATA	1 eSATA interface	
Capacity	Up to 14 TB capacity for each HDD	
Serial Interface	1 RS-232, 1 RS-485 (full-duplex), 1 keyboard	
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0	
Alarm In/Out	16/9	
General		
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian	
Processor	64bits multi-core	
Memory	RAM 16GB DDR4	
Licensing	All features are fully perpetually licensed to operate standalone	
File Lock	Support lock and unlock recorded files	
Video Download	Batch and segment support	
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others	
Fans	Smart fan control	
Power Supply	100 to 240 VAC, 50 to 60 Hz	
Consumption	\leq 50 W (without HDD), \leq 7 W (standby mode)	
Working Temperature	-10 to 55° C (14 to 131° F)	
Working Humidity	10 to 90%	
Dimension (W × D × H)	445 × 465 × 93 mm (17.5"× 18.3" × 3.7"), 2U's	
Weight	≤ 10 kg (without HDD, 28.7 lb.)	
Certification		
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS	
FCC	Part 15 Subpart B, ANSI C63.4-2014	
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201	
	9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020	



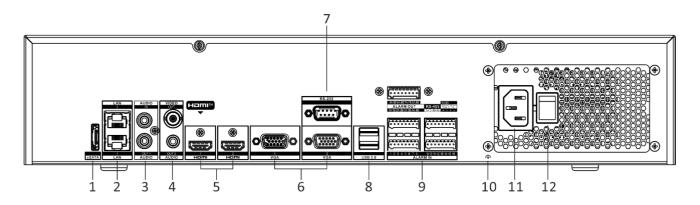
Dimension



scale/1:1;Unit/mm



Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces	8	USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface,
			Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

iDS-9632NXI-M8/X



@Hikvision Digital Technology Co., Ltd. 2022 | Data subject to change without notice |

Storage Solution

Video Storage Parameters		
VideoStorage Parameters	Camera Type 1	
Channel Name	Device 1	
Channel Number	64	
Encoding Mode	H.265	
Resolution	1080P(1920×1080)	
Frame Rate	30	
Bitrate	2048	
Storage Time / Day (Hour)	24	
Storage Period (Day)	30	

		NVR Lis	t Output		
NO.	NO. Product Name Brand Model Quantity				
1	1 Storage Host Hikvision iDS-9664NXI-M8/X 1				

Storage Requirements			
	Requirements	Now	Satisfaction
Storage	40TB	48TB	+8.00TB
Bandwidth	153Mbps	400Mbps	+247.00Mbps
Channel	64	64	+0.00



Network Video Recorder

User Manual

Legal Information

About this Document

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

About this Product

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



Acknowledgment of Intellectual Property Rights

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

LEGAL DISCLAIMER

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

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

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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



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

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



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: <u>http://www.recyclethis.info</u>.

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Series	Model
DS-7600NI-I2	DS-7608NI-12
	DS-7616NI-I2
	DS-7632NI-12
DS-7600NI-I2/P	DS-7608NI-12/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-14
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P

Table 1-1 Applicable Model

Series	Model
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro

Series	Model
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-12/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-12/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-14/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-18/S	DS-8616NXI-I8/S
	DS-8632NXI-18/S
	DS-8664NXI-18/S
DS-8600NXI-18/24P/S	DS-8632NXI-18/24P/S
DS-9600NXI-18/S	DS-9616NXI-I8/S
	DS-9632NXI-18/S
	DS-9664NXI-18/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X

Series	Model
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X

Safety Instruction

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

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
- (+ identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- 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 <u>A</u> or <u>m</u>, 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.

Content Convention

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

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

Symbol Conventions

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

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

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.

iNote

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

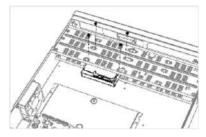


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

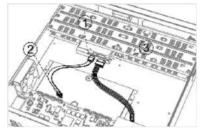


Figure 1-4 Connect Cable

INote

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.

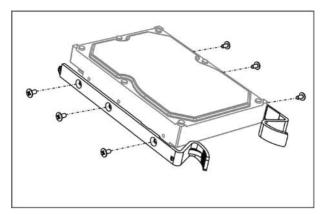


Figure 1-5 Fix Mounting Ears to HDD

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

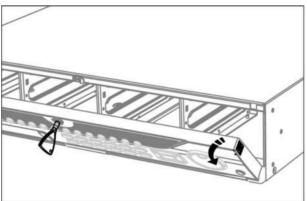


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

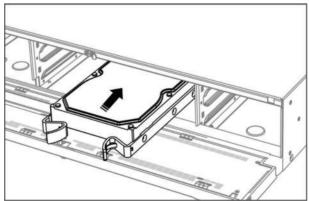


Figure 1-7 Insert HDD

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

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

- 1. Unlock the front panel with panel key.
- 2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

- **3.** Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
- **4.** Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

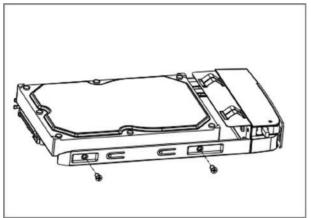


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

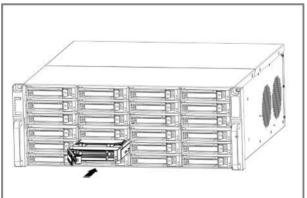


Figure 1-9 Push HDD Case into Slot

- **6.** Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
- 7. Close the front panel, and lock it with the panel 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.

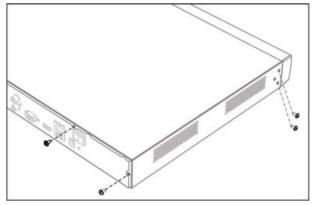


Figure 1-10 Remove Cover

- 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.

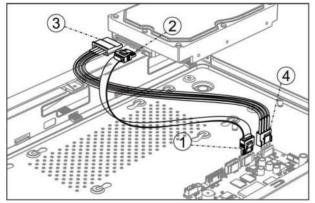


Figure 1-11 Connect Cables

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

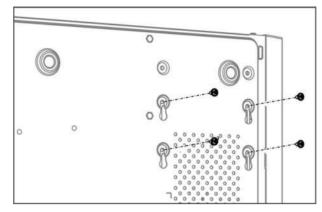


Figure 1-12 Fix HDD to Device Bottom

- 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.

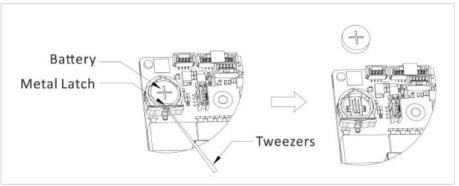


Figure 1-1 Remove Battery

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

iNote

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

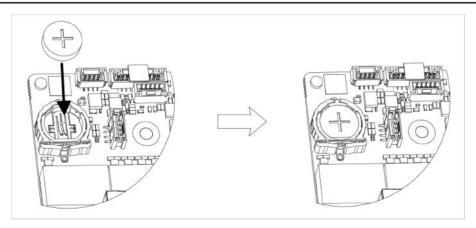


Figure 1-2 Replace Battery

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 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	8
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP 1	1
4.2.3 Configure ISUP 1	1
4.2.4 Configure SDK Service 12	2
4.2.5 Enable ISAPI 1	3
4.2.6 Configure ONVIF 1	3
4.2.7 Configure Log Server 14	4
4.3 Network Service Settings 1	5
4.3.1 Configure HTTP(S) 1	5
4.3.2 Configure RTSP 10	6
4.3.3 Configure WebSocket(s) 10	6
4.3.4 Configure Port Mapping (NAT) 1	7
Chapter 5 User Management 19	9
Chapter 6 Device Access 20	D
6.1 Access Video Device 20	D
6.1.1 Add Automatically Searched Online Network Camera	0

6.1.2 Add Network Camera Manually 2	20
6.1.3 Add Network Camera through PoE 2	!1
6.1.4 Add Solar-Powered Camera through OTAP Protocol	22
6.1.5 Add Network Camera via Custom Protocol 2	22
6.1.6 Add Network Camera through Camera Configuration File	24
6.2 Add Access Control Device 2	24
6.3 Add Audio Device 2	24
6.4 Add POS Device 2	25
6.5 Channel Management 2	26
Chapter 7 Device Grouping 2	27
Chapter 8 Video or Audio Device Settings 2	28
8.1 Enable H.265 Stream Access 2	28
8.2 Configure Display Settings 2	28
8.3 Configure Video Parameters 2	29
8.4 Configure Privacy Mask 2	29
8.5 Configure Audio Parameter 3	0
8.6 Configure OTAP Service	0
8.7 Batch Configuration 3	\$1
8.8 Configure PoE (Power over Ethernet) Interface 3	32
Chapter 9 Storage Management 3	4
9.1 Manage HDD 3	\$4
9.2 RAID Configuration 3	\$4
9.2.1 Create Disk Array 3	\$5
9.2.2 Rebuild Array	6
9.2.3 Delete Array 3	57
9.2.4 View Firmware Info	;7
9.3 Configure Storage Mode 3	8
9.4 Configure Other Storage Parameters 3	8

9.5 Mange USB Flash Drive 3	9
Chapter 10 Schedule Configuration 4	0
10.1 Configure Schedule Template 4	0
10.2 Configure Recording Schedule 4	1
10.3 Configure Picture Capture Schedule 4	3
10.4 Configure Audio Recording 4	-5
Chapter 11 Live View 4	6
11.1 Configure Live View Layout 4	6
11.2 GUI Introduction 4	6
11.3 PTZ Control 4	7
Chapter 12 Playback 4	9
12.1 GUI Introduction 4	9
12.2 Normal Playback 5	0
12.3 Event Playback 5	51
12.4 Slice Playback 5	51
12.5 Sub-Period Playback 5	52
Chapter 13 Event Center 5	3
13.1 Event Settings 5	3
13.1.1 Basic/Generic Event 5	53
13.1.2 Perimeter Protection 5	5
13.1.3 Abnormal Behavior Event 6	5
13.1.4 Target Event	57
13.1.5 Thermal Camera Detection 7	0'
13.1.6 Alarm Input Event 7	'1
13.1.7 Audio Analysis Event 7	'3
13.2 Linkage Configuration	'5
13.3 Disarming Configuration7	6
13.4 Batch Configuration 7	7

13.5 Event Search	78
13.6 View Alarms	79
Chapter 14 Search and Backup	80
Chapter 15 AcuSearch 8	82
Chapter 16 Smart Settings 8	84
16.1 Algorithm Management 8	84
16.2 Engine Status 8	84
16.3 Task Plan Management 8	84
16.4 List library Management 8	84
16.4.1 Add a List Library	85
16.4.2 Upload Face Pictures to the Library	85
Chapter 17 Application Center 8	87
17.1 Human and Vehicle Detection 8	87
17.2 Person Check-In 8	87
17.2.1 Add Check-In Task 8	87
17.2.2 Search Check-In Records 8	88
17.3 Statistic Report 8	89
Chapter 18 System Parameter Settings	90
Chapter 19 Hot Spare Device Backup	92
19.1 Set Working Device	92
19.2 Set Hot Spare Device	92
Chapter 20 Configure Exception Event	94
Chapter 21 View System Info	96
Chapter 22 System Maintenance	97
22.1 Schedule Reboot	97
22.2 Upgrade Device	97
22.3 Backup and Restore	97
22.4 Log Info	98

22.5 Configure Log Server		98
22.6 Maintenance Tools		98
Chapter 23 Security Manageme	nt 10	00
23.1 Address Filter		00
23.2 Stream Encryption		00
23.3 Select TLS Version		00
Chapter 24 Appendix		01
24.1 List of Applicable Powe	r Adapter 10	01
24.2 Glossary		02
24.3 Frequently Asked Ques	tions 10	03
	rt of channels displaying "No Resource" or turning black screen in 10	
•	recorder notifying risky password after a network camera is addec	
24.3.3 Why is the video	recorder notifying the stream type is not supported? 10	04
24.3.4 How to confirm tl	ne video recorder is using H.265 to record video? 10	04
24.3.5 Why is the video	recorder notifying IP conflict? 10	04
	ing stuck when playing back by single or multi-channel cameras?	05
24.3.7 Why is the device	not able to control PTZ camera via coaxitron? 10	05
24.3.8 Why does the PTZ	seem unresponsive via RS-485? 10	05
24.3.9 Why is the video	sound quality not good?10	05
24.4 Notification for Corrosi	ve Gas 10	06

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

- **1.** Power on your device.
- 2. Select a system language.
- 3. Enter the admin password twice.

ACaution

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

Devi	ce Activation	
Do		
۵	••••••	
A		
0		
When yo tecomme	u forget your password, the hint will help you remember. It is inded to set the hint	
	Activate	

Figure 1-1 Activate via Local Menu

4. Optional: Enter a password hint. It will help you remember your password when you forget.5. Click Activate.

iNote

After the device is activated, you should properly keep the password.

6. Optional: Draw an unlock pattern.

7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

- 1. Power on your device.
- 2. Right click to display the shortcut menu.
- **3.** Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

Welcome	
8 admin	
A Password	
Login	
Please respect other people's priv	ary and rights when using product

Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

iNote

- Unlock pattern is only available for admin user.
- If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

Device (2)	+ Add Comment Concerning Export	More D Show Paseword		0	devica() connected.
Viteo Device	Device Na. : IP Address : Network :	Passwor. Show Pa., Protocol	Manage_ : AddesiTotal	Serial No. : Verse	
Access Control Device					
Altim Device					
Auto Device					
POS					
Device Grouping					
Device Configuration 🔗					
Device Parameter					
Access Service					
Batch Configuration	Online Device List (0)				
Menu Bar					
Menu Bar	IP Address 1 Device Model 1 Status	Protocol Manage	8 Seriel No. 2	Farriware 2	Physical

Figure 3-2 Menu Bar Example

Description Construe		Constant of the second	and the second second	O Parant March	() Pasiers >	And States to a	
Venice Capture	Person Clipture					 Target Recognition 	
enu Bar	09-77	-2023 Wed 09:07:47					
	87-61	7.00.3 MEM 03.07.47					
					0000		
				Conce	w 01		

Figure 3-3 Human and Vehicle Detection Example of Application Center

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab.
	Icon introduction :
	 • If a constraint of the second sec
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.
	i Note
	For applications in Application Center , you can click 👿 , or right click to display the menu bar.

Table 3-1 Interface Introduction

Chapter 4 Network Settings

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

4.1 Network Parameter Settings

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

4.1.1 Configure TCP/IP

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

Steps

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

Working Mode	Net Fault-Tolerance	DNS Server Settings		
Select NIC		Auto Obtain DNS Server	•	
NIC Type		Preferred DNS Server		
	IPv4 IPv6	Alternate DNS Server		
DHCP		Main NIC	LANI	
IPv4 Address				
IPv4 Subnet Mask				
IPv4 Default Gateway				
MAC Address				
MTU(Bytes)				

Figure 4-1 TCP/IP Settings

2. Set Working Mode and Select NIC.

Multi-address

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

Net-fault Tolerance

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

iNote

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

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

MTU

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

Auto Obtain DNS Server

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

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click Save.

4.1.2 Configure DDNS

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

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to System → System Settings → Network → Network → DDNS .

Enable		
DDNS Type	DynDNS	
Server Address		
Device Domain Name		
User Name		
Password		
Status	DDNS is disabled.	
	Save	

Figure 4-2 DDNS

- 2. Turn on Enable.
- 3. Select a DDNS type.
- 4. Set parameters, including service address, domain name, etc.
- 5. Click Save.

4.1.3 Configure PPPoE

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

Steps

1. Go to System → System Settings → Network → Network → PPPoE .

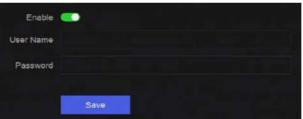


Figure 4-3 PPPoE

2. Turn on Enable.

- **3.** Enter user name and password.
- 4. Click Save.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

- 1. Go to System → System Settings → Network → Network → Other .
- 2. Set Multicast parameters.

iNote

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is
 recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When
 adding a device to the CMS software, the multicast address must be the same as that of the
 device.
- 3. Click Save.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

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

Steps

```
1. Go to System → System Settings → Network → Hik-Connect.
```

En	able 💽		
	atus 🛕 Offline(0xe0000102)		
Scan QR Code to Bind			
 Scan to Download the App 	2 Register Your Account	Use the App to Scan the C Code	DR 4 Bind Your Device
Mahde cleat	2	+ Vericatur Cade	+
		 ∠®	

Figure 4-4 Hik-Connect

- 2. Turn on Enable, and the service terms will pop up.
- **3.** Accept the service terms.
- 4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.

- Download the app from *https://appstore.hikvision.com* .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.

6. Optional: Click More Settings to enable Stream Encryption, Platform Time Sync, and Adaptive Bitrate Streaming, or edit Server IP Address.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

- 7. Click Z to set verification code.
- **8.** Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.

iNote

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

Result

- If your device is connected with Hik-Connect, Connection Status will be Online.
- If your device is bound with a Hik-Connect account, Account Status will be Linked.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

```
1. Go to System → System Settings → Network → Platform Access → OTAP .
```

Enable	
Server Address	
Access Service Port	
Device ID	
Encryption Password	
Registration Status	Offline
	<u>de noisean</u> de la de la constante de
	Save

Figure 4-6 OTAP

- 2. Turn on OTAP.
- 3. Set the parameters.
- 4. Click Save.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the thirdparty platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ISUP .

Enable		
Server Address		
Access Service Port		
Device ID		
Protocol Version	ISUP5.0	
Encryption Key		
Registration Status	Offline	
	Save	

Figure 4-7 ISUP

2. Turn on Enable.

iNote

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click Save.

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

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to System → System Settings → Network → Platform Access → SDK.

SDK	
Enable	<u></u>
Port	8000
Enhanced SDK Service	
Enable	
Port	8443
Enable Stream Over TLS	
	Save

Figure 4-8 SDK Service

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

iNote

The port for Enhanced SDK Service is 8443 by default.

- **3. Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
- 4. Click Save.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to System \rightarrow System Settings \rightarrow Network \rightarrow Platform Access \rightarrow ISAPI to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to System → CX → System Settings → Network → Platform Access → ONVIF .

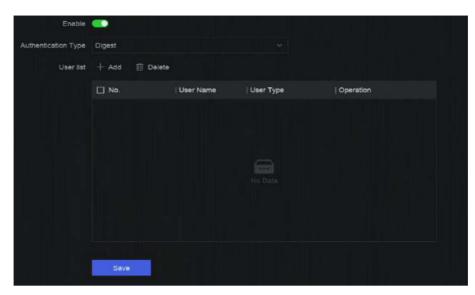


Figure 4-9 ONVIF

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

Caution

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

6. Click Save.

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to System → System Settings → Network → Platform Access → Log Server.



Figure 4-10 Log Server

- 2. Turn on Enable.
- 3. Set Upload Time Interval, Server IP Address, and Port.
- 4. Optional: Click Test to check if parameters are valid.
- 5. Click Save.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

```
1. Go to System → System Settings → Network → Network Service → HTTP(S).
```

HTTP		
Enable	•	
Port	80	
HTTPS		
Enable	 Image: A second s	
	Ensure the client TLS version is enabled.	TLS Settings
Port	443	
Enable HTTPS Browsing	•	
HTTP/HTTPS Authentication		
Authentication Type	Digest	
Digest Algorithm	MD5	
	Authentication type and digest algorithm are	

Figure 4-11 HTTP(S)

- **2. Optional:** Turn on HTTP or HTTPS.
- 3. View or edit Port of HTTP or HTTPS.
- 4. Set HTTP/HTTPS Authentication.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click Save.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

```
1. Go to System → System Settings → Network → Network Service → RTSP .
```

Enable	•	
Port	554	
Authentication Type	Digest	
Digest Algorithm	MD5	

Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

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

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click Save.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to System → System Settings → Network → Network Service → WebSocket(s).

- 2. Turn on Enable.
- 3. Set Port.
- 4. Click Save.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP[™] (Universal Plug and Play), and manual mapping. UPnP[™] can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP[™] function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

If you want to enable the UPnP[™] function of the device, you must enable the UPnP[™] function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the Default Route of the device should be in the same network segment as that of the LAN IP address of the router.

Steps

Operation

1. Go to System \rightarrow System Settings \rightarrow Network \rightarrow Network Service \rightarrow NAT.

Figure 4-13 Port Mapping (NAT)

2. Turn on Enable.

3. Set Mapping Mode.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If Mapping Mode is selected as Manual, click 🖉 to edit corresponding ports.

iNote

• The value of the RTSP port number should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from

each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

• External Port indicates the internal port number for port mapping in the router.

5. Click Save.

What to do next

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

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to System \rightarrow System Settings \rightarrow User Management .



Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
0	Set account security.
Add	Add a new guest or operator user.
Ū	Delete the selected user.

iNote

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to System → Device Access → Device → Video Device → Online Device List .

2. Select the device(s) from the list.

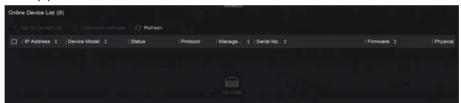


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click Add to Device List.

iNote

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

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

Steps

1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .

Add Device	×					
Online Device List (0)	Refresh C					
No. IP Address Device Model	Status Protocol Manag Serial Ne					
	Data					
IP Address *	Device Name *					
Test	IPCamera 01					
Protocol	Management Port *					
ONVIF · Protocol Manag	80					
User Name	Password					
admin						
Transfer Protocol	Use Channel Default Password					
Auto ~						

Figure 6-2 Add Network Camera Manually

- 2. Click Add.
- 3. Enter network camera parameters.

Use Channel Default Password

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

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

- 4. Optional: Click Continue to Add to add other network cameras.
- 5. Click Add.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to *Configure PoE (Power over Ethernet) Interface* for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

- 1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.
- 2. Turn on Enable.
- 3. Set OTAP Server Port and Encryption Key.
- **4. Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
- **5.** Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



The solar-powered camera OTAP protocol parameters shall be the same as the device.

- 6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from Online Device List, and click Quick Add.
- 7. Click Add in System → Device Access → Device → Video Device, select Protocol as OTAP, and click Add.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to <u>Configure Recording</u> <u>Schedule</u>.

6.1.5 Add Network Camera via Custom Protocol

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

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click More → Custom Protocol Management , or Add → Protocol Management .

Custom Protocol Management ×								
HIKVISION_RTSP	Check your device URL and enter accordingly. Format: [Type] //IP Address][Port](Path]							
DAHUA_RTSP	Example rtsp://1	192,16	8.0.1:554/ch1/mair	nviav_st	ream			
UNIVIEW_RTSP	Protocol Name							
TPLINK_RTSP	HIKVISION_RT	SP						
	HIKVISION	DAHU	IA UNIVIEW		TP-LINK	HUAWEI		
HUAWEI_RTSP	Main Stream							
Custom 6	Туре		Transfer Protoc	:oi	Port		Path	
Custom 7	RTSP		Auto		554			
Custom 8	Sub Stream							
Custom 9	Enable							
Custom 10								
Custom 11	Туре		Transfer Protoc		Port		Path	
	RTSP		Auto		554			

Figure 6-3 Add Network Camera via Customized Protocol

- **3.** Select a protocol type at the left side.
- **4.** Set protocol parameters.

Туре

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

Transfer Protocol

3 types are selectable, including Auto, UDP, and RTP Over RTSP.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and substream. The general format is [*Type*]://[*IP Address*]:[*Port*]/[*Resource Path*], for example, *rtsp:*//192.168.0.1:554/ch1/main/av_stream.

iNote

- Protocol Name and Path can be automatically generated if you click a brand name below Protocol Name.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.
- 5. Click OK.
- 6. Click Add in System → Device Access → Device → Video Device to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

- **1.** Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
- 2. Click Import to import the configuration file in USB flash drive.
- 3. Set the folder path.
- 4. Click Confirm.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with Access Video Device .

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with <u>Access Video Device</u>. If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

- **1.** Go to **System** \rightarrow **Device** Access \rightarrow **Device** \rightarrow **POS**.
- 2. Click Add to add a POS device.

Add POS			×
POS Protocol			
Universal Protocol			
POS Name			
POS2			
Connection Mode			
TCP Reception			
Add	Continue to Add	Cancel	

Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

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

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click Add.

iNote

After a POS device is add, you can click in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System** \rightarrow **Device Access** \rightarrow **Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to System \rightarrow Device Access \rightarrow Device Grouping .

+∠ ⊡	Video Channel (0)	Access Control Channel (0)	Audio Cł	nannel (0)
E Default Group	🗈 Import 🖂 Ren			
	🔲 🛛 Camera No.	Camera Name	IP Address	Device

Figure 7-1 Device Grouping

2. Click + to add a group.



After a group is added, you can click 🗾 / 🛅 to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

```
1. Go to System \rightarrow Device Access \rightarrow Device \rightarrow Video Device .
```

- 2. Click More → Auto Switch to H.265 .
- Enable this function.
- 4. Click Save.

8.2 Configure Display Settings

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

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Display Settings. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

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

Exposure Time

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

Day/Night Switch

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

Backlight

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

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to System \rightarrow Device Access \rightarrow Device Configuration \rightarrow Device Parameter \rightarrow Video Device \rightarrow Video Parameters. Select a camera, and configure parameters as your desire.

Main Stream

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

Sub-Stream

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

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

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

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask.



Figure 8-1 Privacy Mask

- 2. Select a camera.
- 3. Turn on Enable.
- **4.** Draw mask areas on the preview window. The areas will be marked with different frame colors.

iNote

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

5. Click Save.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** \rightarrow **Device Access** \rightarrow **Device Configuration** \rightarrow **Device Parameter** \rightarrow **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of HikVision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to System → Device Access → Device Configuration → Access Service → OTAP Service.

Enable	-
Service Port	7800
Encryption Key	
Auto Add IP Camera	🕳 ()
Enable External Mapping	•
External IP Address	
External Service Port	7800
External Alarm Port	
External Alarm Picture	6011
() External Streaming Start	58002
	Save

Figure 8-2 Configure OTAP Service

- 2. Turn on Enable.
- 3. Set the parameters.
- 4. Click Save.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

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

Batch Configure IP Address	Batch Time Sync	Batch OSD Config	Batch Upgrade			nin in	
Menual Time Sync							
Manual Time Sync	Sync Time Now						
Schedule Time Sync							
Enable	-						
	Alter security (1) (1000)						
	Vitted Device	Access Control Device	Alarm Device	IP Speaker	Microphone		
Select Device	Refresh						
	Device Name		🛛 🗹 Time Sync		Status		
	Camera 01				Enabled		
	IPGamera 01				Enabled		

Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule. **3.** For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

- 1. Go to System → Device Access → Device Configuration → PoE.
- 2. Enable Plug-and-Play function of PoE interfaces according to your requirement.
- 3. Select the device type as IP Speaker of Camera.
- **4.** If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.

iNote

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click Save.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

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

Before You Start

Ensure the HDD is properly installed to your device.

Steps

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

				Remaining capac	
	D No. Free Space (GB)	Capacity (GB)	Status	Property	Operation
۵ I			C Electing		
п. э.	3685		S Denting		
D 14	3685		C Steeping		

Figure 9-1 Manage HDD

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

Add Network HDD	Add a NAS or IP SAN.
Format	Format the selected HDD.
Repair Database	Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.
	 Note Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc. Do not pull out the drive, or shut down the device during the process.
a / b	Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed across the drives in one of several ways called "RAID levels", based the redundancy and performance required.

A Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

RAID Type	Required Number of HDDs
RAIDO	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8

Table 9-1 HDD Requirement for Each RAID Type

iNote

- The function is only available for certain models.
- When array exception event occurs, the corresponding linkage actions can be configured in System → System Settings → Exception .

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- Storage Mode is set to Quota in System → Storage Management → Storage Mode .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

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



Figure 9-2 Enable RAID

- **3.** Wait for the device to restart.
- 4. Go to System → Storage Management → Storage HDD → Array Management again.

+ Create	G Retest C) Firmware into							Array Mode
	Name	Capacity	Physical Disk	Туре	Status	Hot Spare	Tesk		Operation
		7450.05GB		RAIDS	🗢 Normal).	None	None		
Physical D	iek.								
	ouch Array Configuratio	in 🗇 Refresh							
	Capacity	Array Name	Туре	Status	Model		Serial	Task	Operati
	465.770B	i Allay Northe		 Normal 	WDC WD5000YS-01		WD-WMANU1472762	i i i i i i i i i i i i i i i i i i i	Z
	465.7705 3726.03GB		Алтау	Normal	WDC WD40PURX-7		WD-WKAND1472762 WD-WX82DA1ESYSA		
	3726.03G8			 Normal 	WDC WD40HKAI-78		V1HLX0GG	None	
	5478109/9B		Array	O rigital	TYDG YESHDINNAPTS	AND TH	withe Aug G	Presta	

Figure 9-3 Array Management

5.	Create	an	array.
----	--------	----	--------

Creation Method	Description		
One-touch Array	Click One-touch Array Configuration.		
Configuration	i Note		
	By default, the array type created by one-touch configuration is RAID 5.		
Manual Creation	Click Create to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.		

9.2.2 Rebuild Array

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

Steps

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

2. Rebuild an array.

Table S	9-2	Rebuilding	Method
----------------	-----	------------	--------

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click in Operation column under Physical Disk to set a hot spare disk.
	When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.
	i Note
	After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array.
	Go to System → Storage Management → Storage HDD → Array Management , and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to System \rightarrow Storage Management \rightarrow Storage HDD to click \overline{m} to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

- **1.** Go to System \rightarrow Storage Management \rightarrow Storage HDD \rightarrow Array Management .
- 2. Click Firmware Info.
- 3. Optional: Set Back Ground Task Speed.

9.3 Configure Storage Mode

Steps

1. Go to System → Storage Management → Storage Mode .

Quota					
Group	M 68/7814 08				
+ Add Resource 🛛 🖾 🕬					
Resource Name	Capacity (GB)	Free Space (GB)	Storage Content	Storage Object	Operation

Figure 9-4 Storage Mode

2. Select Quota or Group.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

- 3. Set corresponding parameters.
 - Quota: Allocate space for storage objects.
 - Group: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to System \rightarrow Storage Management \rightarrow Advanced Settings .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.

Parameter Name	Description
	 ▶ Note You can click ■ during live view or playback to add a tag. ▶ For searching tag videos, go to ➡ → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon displayed at the upper-right corner.

Chapter 10 Schedule Configuration

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

10.1 Configure Schedule Template

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

Steps

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

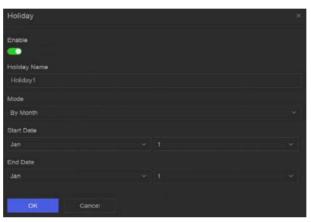


Figure 10-1 Add Holiday

3. Turn on Enable.

4. Configure the holiday.

i Note

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

5. Set Storage Schedule.

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

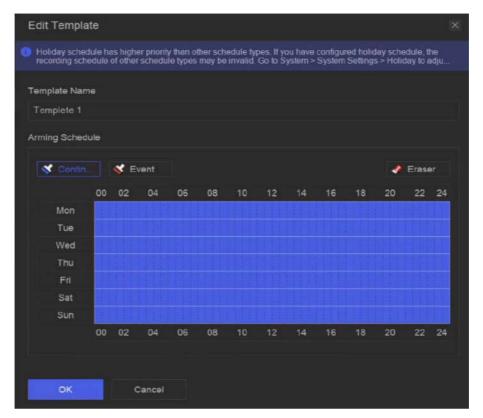


Figure 10-2 Edit Template

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

i Note

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

iNote

You can also click **Configure Template** to configure template in **System** → **Storage Management** → **Storage Schedule** → **Video Recording / Picture Capture / Audio Recording**.

6. Click OK.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording .

Batch Schedule Configuration	Batch Advanced Configuration			
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Carnera 01		Oustom		
D2) IPCamera 02		Custom		
] [03] IPCamera 03		Custom		
[04] IPCamera 04	-	Custom		

Figure 10-3 Video Recording Configuration

- 2. Turn on Enable for a camera.
- 3. Select a schedule type.

INote

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

4. Click View to view the schedule.



Figure 10-4 View Schedule

5. Optional: Click on under Advanced Settings to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.

Parameter	Description
	Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

6. Optional: Select channels in the list, and use Batch Schedule Configuration and Batch Advanced Settings to configure channels in a batch.

7. Click Save.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

1. Go to System → Storage Management → Storage Schedule → Picture Capture .

Batch Schedule Configuration	Batch Advanced Configuration	Z Configure Template		
Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01		Custom		
02] (02] IPCamera 02		Custom		
03] IPCamera 03		Custom		
[04] IPCamera 04		Custom		

Figure 10-5 Picture Capture Configuration

- 2. Turn on Enable for a camera.
- **3.** Select a schedule type.

iNote

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

4. Click View to view the schedule.

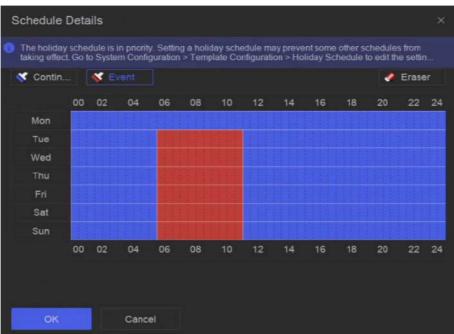


Figure 10-6 View Schedule

5. Click under Advanced Settings to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

- 6. Optional: Select channels in the list, and use Batch Schedule Configuration and Batch Advanced Settings to configure channels in a batch.
- 7. Click Save.

10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

- 1. Go to System → Storage Management → Storage Schedule → Audio Recording .
- 2. Turn on Enable for a channel.
- 3. Select a schedule type.

iNote

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

- 4. Click View to view the schedule.
- 5. Optional: Click under Advanced Settings to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records at 9:59:55.
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

- 6. Optional: Select channels in the list, and use Batch Schedule Configuration and Batch Advanced Settings to configure channels in a batch.
- 7. Click Save.

Chapter 11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

- 1. Go to Live View.
- 2. Click 📰 at the lower-right corner.
- **3.** Select a window division type, or click **Custom** to customize a new type as your desire.
- 4. Move the cursor on **Default View** in **View**.
- 5. Click 🔯 at the right side of View.
- 6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
- 7. Click 🧮 .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.



Figure 11-1 Live View (Type 1)



Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	 Channel tool bar. Click
4	Live view tool bar. Functions like Voice Broadcast, Display VCA Info and Switch Output can be performed here.

iNote

If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	 Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click Call a preset: Click Call a preset: Click
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click ⊇ . 3. Add presets for the patrol. 4. Click OK. Call a patrol: Click ⊙ .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	 Set a pattern: 1. Click . 2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click .

Table 11-2 PTZ Operation

INote

If the PTZ panel cannot be used, please click 🔯 to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



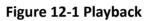


Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	 Channel tool bar. Click ■ to add a tag go the channel. After adding, you can go to → Backup → By Tag to search videos by tag. Click ■ to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to → Backup → By Tag to search videos by lock. Select ■ → Dual-VCA to search videos that can trigger the corresponding event rule. Defer to the overtext.
	the corresponding event rule. Refer to the event configuration steps for details of each event type.

No.	Description
	 Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. You can select → Show VCA Info to display rule frames.
5	 Playback 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.
6	 Playback tool bar. Click A / the to show videos that contain human/ vehicle. In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. Click to set normal video and smart video (the video that contains smart data) playback strategy. Click to search videos that can trigger the corresponding event. The operations are similar with Dual-VCA function. Click to perform AcuSearch function. Refer to <u>AcuSearch</u> for details.

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

- **1.** Go to **Playback** \rightarrow O.
- 2. Select channel(s) in the list at the left side.

iNote

Group playback: Select a group in the list, and channels in the group can be played back.

3. Select a date in the calendar.

iNote

The blue triangle at the calendar date corner indicates there are available videos.

- 4. Optional: Play back videos that contain human or vehicle targets.
 - 🔄 : Videos that contain human would be marked in red.
 - 🔄 : Videos that contain vehicle would be marked in red.

12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start

- Ensure the camera has enabled Dual-VCA. You can enable it via the camera web browser interface in Configuration → Video/Audio → Display Info. on Stream.
- Ensure your video recorder has enabled Save Camera VCA Data in Storage management → Advanced Settings .

Steps

- **1.** Select **Playback** \rightarrow 🐻 .
- 2. Select a date in the calendar.

iNote

The blue triangle at the calendar date corner indicates there are available videos.

- 3. Click → Dual-VCA at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
- 4. Click Search.

Videos meet the detection rule requirement will be marked in red.

5. Click 🔯 to set normal video and smart video (the video that contains smart data) playback strategy.

iNote

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

- **1.** Go to **Playback** \rightarrow **E** .
- 2. Select a camera from the camera list.
- **3.** Select a date on the calendar.
- 4. Click Search.

The retrieved video will be divided into one-hour slices for playback.

5. Optional: Select an one-hour slice and click 🖪 to divide it into one-minute slices for playback.

12.5 Sub-Period Playback

The video files can be played in multiple sub-periods simultaneously on the screen.

Steps

1. Go to Playback \rightarrow \blacksquare .

- 2. Select a camera.
- 3. Set the start time and end time.
- 4. Click Search.



Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.

iNote

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to Event Center → 🔯 → Event Configuration → Basic Event / Generic Event .

- 2. Select a channel.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Con	figuration
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. AI by NVR The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects.	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.
		AI by Camera	
		The motion detection event will be analyzed by camera.	
		Detection Target	
		Human and Vehicle are selectable, apart	

Event Name	Event Description	Rule Configuration	
		from false alarms, only the selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> (c) to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System \rightarrow Storage Management \rightarrow Storage Schedule \rightarrow Video Recording to configure video recording schedule.

8. Click Save.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure 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.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

i Note

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

The device will analyze the video, and cameras only transmit video stream.

- 4. Select Line Crossing.
- 5. Turn on Enable.

Channel	(D1) Camera 01 V
AI by NVR	•
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shalid Area
	1 2 3 4
Rule List	
	01-62-2824 Tue: 14:68:36
	B
	Camera 01
	Save

Figure 13-1 Line Crossing Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set Direction, Sensitivity, and Detection Target.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from the A side to the B side can be detected.

B->A

Only the object crossing the configured line from the B side to the A side can be detected.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click i / in to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-3 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Intrusion Detection

Intrusion detection function detects people, vehicles or other objects that enter and loiter in a predefined virtual region. Specific actions can be taken when an alarm is triggered.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System → Smart Settings → Algorithm Configuration → Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

The device will analyze the video, and cameras only transmit video stream.

- 4. Select Intrusion.
- 5. Turn on Enable.

Channel	[D1] Camera 01 V
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Scheld Area
Rule List	
	P1-02-2021 Tue 11:16:10 #1# Concra 01
	Save

Figure 13-2 Intrusion Detection

6. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select 1.
- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Time Threshold, Sensitivity, and Detection Target.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click / to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-4 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

The device will analyze the video, and cameras only transmit video stream.

- 4. Select Region Entrance.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Schedd Area
Rule List	
	01-02-2021 Tue 14:59:21
	Canera 01
	Save

Figure 13-3 Region Entrance Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.
 - 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
 - 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-5 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Before You Start

If your device supports AI by NVR function, and its corresponding functions are required, please go to System \rightarrow Smart Settings \rightarrow Algorithm Configuration \rightarrow Algorithm Management to enable Perimeter Protection algorithm.

Steps

iNote

A part of the following steps are only available for certain NVR or camera models.

- 1. Go to Event Center → 🔯 → Event Configuration → Perimeter Protection.
- 2. Select a camera.
- 3. Optional: Turn on Enable AI by NVR.

The device will analyze the video, and cameras only transmit video stream.

- 4. Select Region Exiting.
- 5. Turn on Enable.

Channel	[D1] Camera 01 ~
AI by NVR	
Sub Event	Line Crossing Intrusion Region Entrance Region Exiting
Enable	
	Rule Settings Arming Schedule Linkage Method Shield Area
Rule List	
	01-02-2024 Tue 15:03:58
	Contraction of the second s
	Contraction of the Contraction o
	Contraction of the Contraction o
	Camera 01
	Save

Figure 13-4 Region Exiting Detection

- 6. Click Rule Settings to detection rules.
 - 1) Select a rule number. For example, select 1.

- 2) Click and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set Sensitivity and Detection Target.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
- 7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-6 Linkage Method Description

9. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

10. Click Save.

What to do next

You can go to Live View and click Target to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

- 2. Select a camera
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10].
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	 Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined	

Event Name	Event Description	Rule Configuration
	region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	 a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	

Linkage Method	Description	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **System** \rightarrow **Smart Settings** \rightarrow **Algorithm Configuration** \rightarrow **Algorithm Management**.

Steps

1. Go to Event Center \rightarrow **[as a determination of the set of th**

- 2. Select a camera.
- 3. Select an event.
- 4. Turn on Enable.
- 5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can	-

Event Name	Event Description	Rule Configuration	
	be triggered when a human face is detected.		
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	Start Configure Face Picture Library Enable Target Recognition or Video Structuralization Algorithm Configure Event Rules and Parameters Configure Arming Schedule and Linkage Method Optional: View Real-Time Alarms in Live View or Application Center	
		Comparison	
		Target Grading Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.	
		Non-Real-Time Mode	
		For places with a high flow of people, the device processing speed may not be fast	

Event Name	Event Description	Rule Configuration
		enough, Non-Real-Time Mode will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison. Non-Real-Time Mode will not trigger real-time alarm, so Arming Schedule is unavailable. Linkage Succeeded / Linkage Failed
		When comparison succeeded or failed, the corresponding linkage actions would be triggered. You can view the real-time comparison result in Target of Live View .
Multi-Target- Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	I Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click Save.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to Event Center → 🔯 → Event Configuration → Thermal Event .

- 2. Select a camera.
- 3. Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature DetectionAn alarm would be triggered when the temperature e the threshold value.	

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description	
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).	
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.	
Buzzer	When an alarm is detected, the buzzer will make an audible beep.	
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.	
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.	
Record	When an alarm is detected, the selected channel would record videos.	
	iNote	
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.	

8. Click Save.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Alarm Input Event .

2. Select an alarm input name.

Edit Alarm Input	×
Alarm Input No.	
Local<-1	٣
Alarm Name	
Enable	
•••	
Link to Quick Disarming ①	
Oulck Disarming Configuration	
Alarm Type	
N.0	~
Arming Schedule	
All-Day Arming	View
Template Configuration	

Figure 13-6 Configure Alarm Input

iNote

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

- 3. Edit Alarm Name.
- 4. Turn on Enable.
- 5. Set Quick Disarming. Quick disarming can disable the selected alarm linkage methods in a batch.
- 6. Set Alarm Type.

iNote

Refer to the alarm source to correctly configure the alarm type.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

7. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00.00-24:00</u> to set specified time schedule.

8. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

9. Click Save.

13.1.7 Audio Analysis Event

Steps

- **1.** Go to Event Center \rightarrow **[6]** \rightarrow Event Configuration \rightarrow Audio Analysis .
- 2. Select a channel.
- **3.** Select an event type.
- 4. Turn on Enable.
- 5. Click Rule Settings to set the rule.

Event Name	Event Description	Rule Configuration
Audio	Audio exception	Sudden Increase of Sound Intensity Detection
Exception	detection detects	Detects a steep sound increase in the scene.
Detection	abnormal sounds in	Sudden Decrease of Sound Intensity Detection

Event Name	Event Description	Rule Configuration
	the scene, such as a sudden increase/ decrease in sound intensity.	Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered.
		Sound Intensity Threshold
		It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click Arming Schedule to select an arming schedule type.

iNote

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click <u>00:00-24:00</u> to set specified time schedule.

7. Click Linkage Method to set linkage methods.

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.
	i Note
	Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

Table 13-14 Linkage Method Description

8. Click Save.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- 1. Go to Event Center → → Event Configuration → Linkage Configuration or System → Event Configuration → → Event Configuration → Linkage Configuration.
- 2. Click Email to configure email parameters.

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp. 263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click Audio Management to manage audio files for alarm linkage.

iNote

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

iNote

- This linkage action is only available for few event types.
- The uploaded audio file shoud be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.
- 5. Click Alarm Output to set alarm output parameters.

iNote

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, Local->1 means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.

iNote

This linkage action is only available for few event types.

7. Click Security Control Panel to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

Channel Name	Allow Disarming 🔘	Disarming Status	Disarming Method	Disarming Template	Details
[D1] Cemere 01		Disabled	Quick Diserming	Mute Disarming	
D2] IPCamera 02		Disabled	Quick Diseming		
[D3] IPCamera 03	•0	Disabled	Quick Disarming		
D4] IPCamera 04	•	Disabled	Quick Disarming		
🔲 [D5] IPCamera 05	-	Disabled	Quick Disaming		
D6j iPCemere 06	•10	Disabled	Quick Diseming		
[D7] IPCamera 07		Disabled	Quick Disarming		
[] [D8] IPCamera 08	•	Disabled	Quick Disarming		
[D9] IPCamera 09		Disabled	Quick Disaming		
🖸 [010] IPCamera 10		Disabled	Quick Disaming		
🔲 (D11) IPCamera 11		Disabled	Quick Diseming		
🔲 [D12] IPCamera 12	-	Disabled	Quick Disaming		
[D13] IPCamera 13	•0	Disabled	Quick Disaming		
[] [D14] IPCemera 14	•10	Disabled	Quick Diserming		
D15] IPCamera 15		Disabled	Quick Disarming		

Figure 13-7 Disarming Configuration

- 2. Select channel(s) that are allowed for disarming.
- 3. Click Batch Schedule Configuration.
- 4. Turn on Enable.
- 5. Select Disarming Template. Only two types are available

INote

Currently, only two template types are available and each template parameters cannot configured.

6. Click OK.

13.4 Batch Configuration

The listed events and the corresponding linkage action of Notify Surveillance Center can be enabled or disabled in batches through Event Center $\rightarrow \bigotimes \rightarrow$ Event Configuration \rightarrow Batch Configuration or System \rightarrow Event Configuration $\rightarrow \bigotimes \rightarrow$ Event Configuration \rightarrow Batch Configuration. After an event is enabled, please click Go to Event Configuration to set rules.

Channel	Enable Event	Notify

Figure 13-8 Batch Configuration

13.5 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

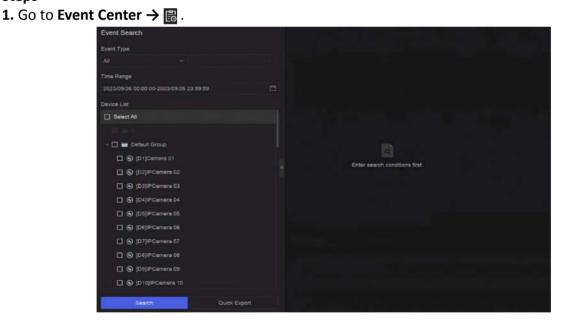


Figure 13-9 Event Search

- 2. Specify detailed conditions, including event type, time, channel, etc.
- 3. Click Search.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

- 1. Go to Event Center → 🛃 .
- 2. Click Real-Time Alarm.
- **3.** Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

- 4. Click Playback, and the alarm recording video would be played back.
- 5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to Backup.

64 355 0 Perice List ★6 00 00 00 00 00 00 00 00 00 0	By Lock By Teg 00.00.00-2023/09/26 23:59:59 Image: Comparison of the second sec	f	Enter search cond	Bons fret.	
	Search	Ouick Export			

Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, 7 types are supported.

INote

The searching conditions would vary according to the selected searching method.

- 3. Set the searching conditions.
- 4. Click Search.

	Video File		Destruction and the second state	Export All		4 🗆 🔳
	By Time Dy Lock Dy Tag			1		5
	Time Period		August and a	DTE weeks 01 22340	CTTC-Annual III Annual	
13		B 8		Concert .	inniger (
10	Device List	2	3			
	NI NI	Z	2			
Ť						
A	- 📰 🖿 Default Droup					
	C (D1)Cemere 01					
	C (03)PCamera 03					7
	C (DI)PCamira 04					
	💌 🛞 (DS)PCamera 03					
	🗶 🚱 (05)/PCamers 06					
	🖉 🛞 (57)PCamere 87					
	O (DB)PCamera DB O					
	🔳 🚱 (05)(PCamera 05					
	🖉 💬 (010)/PCarriera 10					
	🖉 😡 (D11]/PCarriera 11					
	Seetly Oulek Expert	Total 3 here(s			6	1 / 00

Figure 14-2 Searching Result

- **5. Optional:** Perform the following operations.
 - 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - **3** Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - **6** Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6. Insert a USB flash drive to the device for backup.
- **7.** Export files to the USB flash drive.
 - Select files(s) in the result list and click **Export**.
 - Click Export All to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

- **1.** Go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable AcuSearch algorithm.
 - Al by Camera: The camera will perform the AcuSearch analysis.
 - AI by NVR: The device will perform the AcuSearch analysis, and engine resource is required for analysis.
- 2. Go to Live View or Playback, and click 🔤 at the lower-left corner during video playing.

i Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** (<a>[in]) to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking 🔄 , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.
- **3.** Click of the selected target.

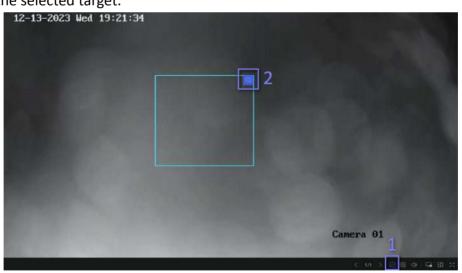


Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

rsh			
Peta			- Entany
e Kange	NA ANALISES IN DOMINING	TTN 0-22003012000	TN PRODUCT
Default Group			
😸 🚱 (D1)Canela D1			
🗶 🛞 (D2p+Canena 02			
🗷 🕲 (DipPCament Di			
🗹 🛞 (D4)/PCamera 04			
🗷 😡 (DS)/PCamera 05			
C (DE)PCamera DE			
Silenty	Total + Iterrita)		

Figure 15-2 AcuSearch Result

- **5. Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
- **6. Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Algorithm Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Algorithm Management. The available algorithms would be listed, and you can click the required algorithm to link engine(s).

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Engine Status. If you need to switch the algorithm, refer to <u>Algorithm Management</u>.

16.3 Task Plan Management

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Go to System \rightarrow Event Configuration \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management or Event Center \rightarrow Event Configuration \rightarrow Smart Settings \rightarrow Task Plan Management. For Non-Real-Time Target Comparison, you can view the progress of each day.

Task status mainly includes 3 conditions: Disabled, Waiting, and Enabled.

Disabled

No analysis task is enabled on the camera.

Waiting

The analysis task of the camera is enabled. Device is waiting to analyze data.

Enabled

The analysis task of the camera is enabled and device is analyzing data of the camera.

16.4 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers** library is used to store pictures for strangers, and it cannot be deleted.

16.4.1 Add a List Library

Steps

- 1. Go to System → Event Configuration → Event Configuration → Data Archive → List Library or Event Center \rightarrow Event Configuration \rightarrow Data Archive \rightarrow List Library.
- 2. Click Add.
- **3.** Enter the library name.
- 4. Click Confirm.

iNote

- After a list library, you can move the cursor on the library to edit or delete it.
- You can click Delete in Batch to delete selected libraries, or clear all pictures in the selected libraries.

16.4.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

- 1. Double click a list library.
- 2. Optional: Click Custom Tag to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.
- 3. Click Add or Import.
- 4. Import picture(s).
 - Add: Click to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
 - Import: Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.
- 5. Optional: Perform the following operations.

Delete Pictures from
the Library

- Select a picture and delete it.
- Select pictures and click Delete in Batch to delete the select ones.

Search Pictures in the Library

Click at the tool bar to search pictures.

Copy Pictures to Another Library	Select pictures and click Copy to to copy the uploaded pictures of the current library to another library.
Edit Pictures	Click the picture name, and edit its attributes.
Export Pictures	Select pictures, and click Export to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time.

Human and vehicle detection should be configured in advance. Go to **Event Center** \rightarrow **[2]** to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

No.	Description
1	Right-click shortcut menu.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

17.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

17.2.1 Add Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to System → Smart Settings → Algorithm Configuration → Algorithm Management .
 Allocate Target Recognition to at least one engine.
- The list library for check-in comparison is properly configured. Refer to <u>Add a List Library</u> for details.

Steps

- 1. Click Person Check-In .
- 2. Right click to display the menu at left side.
- **3.** Click 🔯 .
- 4. Click Add.

				Add Check-In Task	
🗆 Teek Name	Status	Checked In People	Recog		
				Task Type	
				O Repeat	
				Title of Daplay Page	
				Display Mode	
				No more than 100 persons can be improved at the survey display model. If the particle of pengle ecce	
				Слисний-ті Ресри	
				Ci Select At	
				Carden Carcel	

Figure 17-2 Add Check-In Task

5. Set Task.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

6. Configure other parameters, including Task Name, Check-In Time, Recognition Channel, etc.

7. Click Confirm.

17.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to Person Check-In .

2. Right click to display the menu at the left side.

3. Click 🐻 .

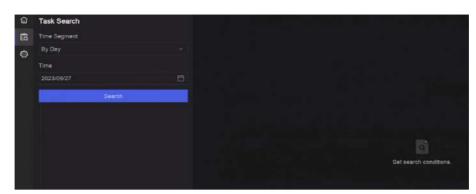


Figure 17-3 Search Check-In Records

- 4. Set time.
- 5. Click Search.

17.3 Statistic Report

You can view reports of people counting and heat map.

Function Name	lcon	Condition	Description
People Counting	8	 The function must be supported by the connected IP camera. For example, a people counting camera is connected to your device. Camera statistic data can be stored to the device HDD. 	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/ monthly/annual reports for analysis.
Heat Map		 The function must be supported by the connected IP camera. Camera statistic data can be stored to the device HDD. 	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Table 17-2 Statistic Report Introduction

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Туре	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time	Time Sync Mode	NTP Time Sync
Configuration		You can select NTP Time Sync and configure NTP Server , NTP Server Port , NTP Client Port , and Interval . Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization.
		Manual Time Sync
		Manually set the system time.
		Hik-Connect Server Time Sync
		The device will sync time with Hik-Connect instead of NTP server.
		DST
		DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).

Table 18-1 Parameter Description

Туре	Parameter Name	Description
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console
		After connecting it to PC with a convertor, PC can set the device parameters.
		Transparent Channel
		It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System

i Note

- Up to 32 working devices and 32 hot spare devices are allowed.
- It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
- Only certain models support this function.

19.1 Set Working Device

Steps

- 1. Go to System → System Management → N+M Hot Spare .
- 2. Set Working Mode as Normal Mode.
- 3. Turn on Enable.
- 4. Click Save.
- 5. Optional: View Hot Spare Device IP Address and Hot Spare Device Working Status.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

- **1.** Go to System \rightarrow System Management \rightarrow N+M Hot Spare .
- 2. Set Working Mode as Hot Spare Mode.
- 3. Click Save. Your device will restart automatically.

i Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

4. Go to System → System Management → N+M Hot Spare again.

- **5.** Add working devices to the hot spare system.
- 6. Add hot spare devices to the hot spare system.
- 7. Click Save.

Chapter 20 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System** \rightarrow **System** Settings \rightarrow Exception .

Main Type Exception	HDD Exception ~	HDD Full	
Notify Surveillance Center	•		
Send Email	Configure Email		
Buzzer	•		
Alarm Output	Select All		Configure Alarm Output
	Local->1		
	Local->2		
	Local->3		
	Local->4		
	Local->5		
	Local->6		
	Local->7		
	1.0001 > 0		

Figure 20-1 Exception Event Configuration

- 2. Select exception type.
- **3.** Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.

Linkage Method	Description
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.

iNote

When exception events occur, in at the upper-right corner would notify, and you can click it to view.

4. Click Save.

Chapter 21 View System Info

Go to System → System Maintenance → Running Info → System Info to view the system

information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to System \rightarrow System Maintenance \rightarrow Maintenance \rightarrow Schedule Reboot to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

The device configuration files can be exported to a local device for backup, and the configuration files of one device can be imported to multiple devices if they are to be configured with the same parameters.

Simple Restore

Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the device to the inactive status, and leave all settings unchanged except restoring user accounts.

22.4 Log Info

Go to **System** \rightarrow **System Maintenance** \rightarrow **Maintenance** \rightarrow **Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

- **1.** Go to System \rightarrow CX \rightarrow System Settings \rightarrow Network \rightarrow Network \rightarrow Log Server .
- 2. Turn on Enable.
- 3. Set Upload Time, Server IP Address, and Port.
- 4. Optional: Click Test to test if parameters are valid.
- 5. Click Save.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

- **1.** Go to **System → System Maintenance → Maintenance → Maintenance Tools** .
- 2. Select tools according to your requirement.

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping
	The ping test is used to detect whether the destination IP address is reachable.
	NIC Packet Capture

Table 22-1 Tool Description

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.
 Note	

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

- 1. Go to System → System Maintenance → Security Management → Address Filter .
- 2. Turn on Enable.
- 3. Set Filtering Type. Choose to filter by IP address or MAC Address.
- **4.** Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
- 5. Optional: Set Restriction List. You can add, edit or delete address.
- 6. Click Save.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

- 1. Go to System → System Maintenance → Security Management → Stream Encryption .
- 2. Turn on Enable.
- 3. Set Encryption Key.

INote

The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.

4. Click Save.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to System \rightarrow System Maintenance \rightarrow Security Management \rightarrow TLS to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, Φ5.5 × 2.1 × 10	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, Ф5.5 × 2.1 × 10	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, Φ2.1	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 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.

ΡΡΡοΕ

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.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying "No Resource" or turning black screen in multi-screen live view?

Reason

- 1. Sub-stream resolution or bitrate settings is inappropriate.
- 2. Connecting sub-stream failed.

Solution

 Go to Camera → Video Parameters → Sub-Stream. Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).

iNote

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

- 1. The camera does not support coaxitron.
- 2. The coaxitron protocol is incorrect.
- 3. The signal is affected by video optical transceiver.

Solution

- 1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
- 2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
- 3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

- 1. The RS-485 cable is not properly connected.
- 2. The RS-485 interface is broken.
- 3. The control protocol is not correct.

Solution

- 1. Check if RS-485 cable is properly connected.
- 2. Change RS-485 interface, and try again.
- 3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

- 1. The audio input device does not have a good effect in sound collection.
- 2. Interference in transmission.
- 3. The audio parameter is not properly set.

Solution

- 1. Check if the audio input device is working properly. You can change another audio input device, and try again.
- 2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
- 3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCI (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _X (Nitrogen Oxides)	0.5	1.0

 Table 24-1 Corrosive Gas Concentration Limit

iNote

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _X (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.





iDS-9664NXI-M8/X DeepinMind M Series NVR

Key Feature

- Up to 2-ch@32 MP/2-ch@24 MP/4-ch@12 MP/8-ch@8 MP/16ch@4 MP/32-ch@1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 64-ch IP cameras can be connected, plug & play
- Intelligent analytics based on deep learning algorithm
- Up to 24-ch perimeter protection
- Up to 16-ch facial recognition for video stream, or up to 48-ch facial recognition for face picture
- Up to 12-ch video structuralization



Profession and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading and AES256 encription
- Support adding digital watermarks, and checks video integrity
- ANR (Automatic Network Replenishment) technology ensures network camera video storage reliability

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K resolution or dual 4K resolution

Storage and Playback

- Up to 8 SATA interfaces for HDD connection
- Up to 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR (Automatic Number-Plate Recognition), and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm





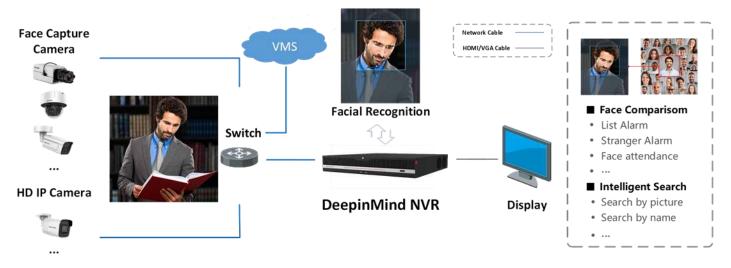
Network & Ethernet Access

- 2 self-adaptive 10M/100M/1000M Ethernet interfaces, with load balancing and multi-IP address
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in
- Manages user and group permissions and function access
- Generate manually snapshots of the cameras
- Allows playback at specific time points, fast forward and rewind, slow forward and rewind and pause
- Digital zoom during playback and live view and playback in full screen
- Operates with Video Wall over network

Typical Application

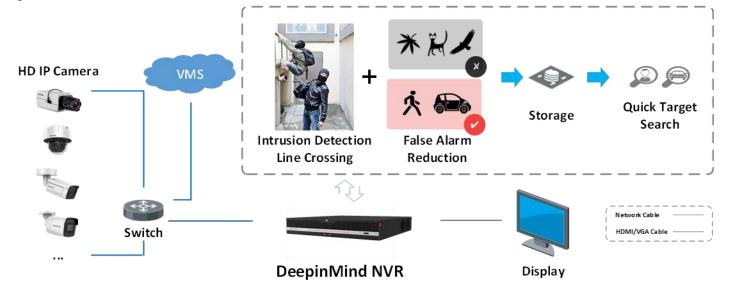
Facial Recognition and Face Picture Comparison

Modeling and analyzing face pictures captured by cameras. Realize list alarm and stranger alarm via face picture library. Search target people by picture and name features.



Perimeter Protection

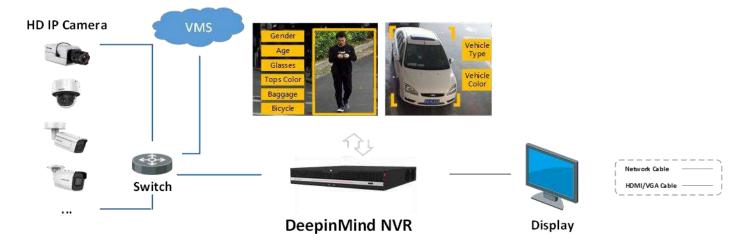
Adopt deep learning algorithm to reduce false alarm, effectively reduces the false alarm caused by tree branches, leaves, shadow, light, vehicles, small animals, etc.





Video Structuralization

Extracting the face picture, human body and vehicle features from live videos, which is used for the tracking and retrieval of human and vehicles. Extracting the following human features: age, gender, glasses, hats, masks, tops type, tops color, pants type, pants color, backpack, carrying things, riding a bicycle.





.

Specification

Al by NNRFacial recognition, perimeter protection, video structuralization, throwing objects from building, motion detection 2,0, ANPR, people counting, face capture, smart event, VCAQ lottering, people runningGPU Engine2, each engine can run an intelligent algorithm, engine mode is adjustableOperating System10Facial Detection and AnalyticsFacial recognition, perimeter protection, video structuralization, throwing objects from builtering, people runningFacial Detection and AnalyticsFace picture comparison, human face capture, face pictures in singer picture si A MB, total capacity \$20 GB), Generates alarms for list library, up to 10,000,000 face pictures in face capture (each picture si A MB, total capacity \$20 GB), Generates alarms for list match and stranger face pictures in singer piberary, up to 10,000,000 face pictures in face capture (each picture si A MB, total capacity \$20 GB), Generates alarms for list match and stranger face pictures and MB, total capacity \$20 GB), Generates alarms for list match and stranger face pictures in singer piberary, up to 10,000,000 face pictures in face capture (each picture si A MB, total capacity \$20 GB), Generates alarms for list match and stranger face pictures in singer piberary, up to 10,000,000 face pictures in face capture (each picture si A MB, total capacity \$20 GB).Facial Detection and AnalytisCabe 2AP (Pach for each engine); capture picture si and singer face pictures in singer piberary, up to 10,000,000 face pictures in face capture (each picture si A MB, total capacity 2, up to 10,000,000 face pictures in face capture (each capture si and singer pictures on singer singer singer, up to 100,000 face pictures in face capture (each capture singer s	Intelligent Analytics		
Al by Camerabuilding, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA, ditering, people runningGPU Engine2, each engine can run an intelligent algorithm, engine mode is adjustableOperating SystemLinuxFacial RecognitionFace picture comparison, human face capture, face picture searchFacial Detection and AnalyticsGace picture libraries, up to 100,000 face pictures in list library, up to 10,000Face Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in face capture (each picture s 4 MB, total capacity S 20 GB), Generates alarms for list match and strange face detection.Face Picture Comparison (Captured from Camera)Bac (24-ch for each engine); comparison speed: 48 pictures per secondFacial Detection PerformanceAll channelsBy VRa24-ch 2 MP (8-ch for each engine), up to 8 MPBy CameraMil ChannelsAlarmsSupport generates alarms of perimeter violationFace Picture LibraryUp to 32 face picture libraries, up to 10,000,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB)Face Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB)Face Picture LibraryUp to 32 face picture libraries, up to 10,000,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB)Face Picture LibraryUp to 32 face picture library, up to 10,000,000 fa	AI by NVR		
Operating SystemLinuxFacial RecognitionFacial Detection and AnalyticsFace picture comparison, human face capture, face picture searchFace Picture LibraryUp to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000Face Picture Library& 48-ch (24-ch for each engine); Comparison speed: 48 pictures per secondFace Picture Comparison& 68-ch (24-ch for each engine), up to 8 MPPerimeter Protection& 24-ch 2 MP (8-ch for each engine), up to 8 MPParmeter Protection& 24-ch 2 MP (12-ch for each engine), up to 8 MPBy NVR24-ch 2 MP (12-ch for each engine), up to 8 MPOperating System& 21-ch 2 MP (6-ch for each engine), up to 8 MPStructured Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPOperating System& 21-ch 2 MP (6-ch for each engine), up to 0,000 face pictures in list library, up to 10,000Face Picture LibraryUp to 32 face picture libraryUp to 32 face picture sin and specification& 30-port generates alarms of perimeter violationFace Picture Comparison12-ch 2 MP (6-ch for each engine), up to 0,000 face pictures in list library, up to 10,000Face Picture Comparison13-ch 2 MP (6-ch for each engine), up to 10,000,000 face pictures in face capture (each picture si and specification	Al by Camera	building, motion detection 2.0, ANPR, people counting, face capture, smart event, VCA,	
Facial Recognition Facial Detection and Analytics Face picture comparison, human face capture, face picture search Face Picture Library Up to 32 face picture libraries, up to 10,000 face pictures in fist library, up to 10,000, face pictures in face capture (each picture 5 4 MB, total capacity 5 20 GB). Generates alarms for list match and strange face detection. Face Picture Comparison 48-ch (24-ch for each engine); Comparison speed: 48 pictures per second Facial Detection and Analytics reference Performance 16-ch 2 MP (8-ch for each engine), up to 8 MP Performance All channels Support generates alarms of perimeter violation Support generates alarms of perimeter violation Yeace Picture Library 10 to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 Parimeter Protection 24-ch 2 MP (12-ch for each engine), up to 8 MP Parimeter Protection Up to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 Video Structuralization 12-ch 2 MP (6-ch for each engine), up to 8 MP Picture Library Up to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 Face Picture Comparison 16-ch; Comparison speed: 32 pictures per second Alarms Support generates alarms based on the Video Structurali	GPU Engine	2, each engine can run an intelligent algorithm, engine mode is adjustable	
Facial Detection and Analytics Face picture comparison, human face capture, face picture search Pace Picture Library Up to 32 face picture libraries, up to 100,000 face pictures in face capture (each picture s 4 MB, total capacity s 20 GB). Generates alarms for list match and strange face detection. Face Picture Comparison d8-ch (24-ch for each engine); Comparison speed: 48 pictures per second Facial Detection and Analytics Comparison speed: 48 pictures per second Perimeter Protection 16-ch 2 MP (8-ch for each engine), up to 8 MP Perimeter Protection 24-ch 2 MP (12-ch for each engine), up to 8 MP By NVR 24-ch 2 MP (12-ch for each engine), up to 8 MP Support generates alarms of perimeter violation 3000000000000000000000000000000000000	Operating System	Linux	
Face Picture LibraryUp to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture 4 MB, total capacity 5 20 GB). Generates alarms for list match and strange face detection.Face Picture Comparison48-ch (24-ch for each engine); Comparison speed: 48 pictures per secondFacial Detection and Analytic Performance16-ch 2 MP (8-ch for each engine), up to 8 MPPerimeter Protection24-ch 2 MP (12-ch for each engine), up to 8 MPBy NVR24-ch 2 MP (12-ch for each engine), up to 8 MPBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Comparison16-ch; comparison speed: 32 pictures per secondface Picture Comparison16-ch; comparison speed: 32 pictures per secondface Picture Comparison16-ch; comparison speed: 32 pictures per secondfarmsSupport generates alarms based on the Video Structuralization features detectionface Picture Comparison16-ch; comparison speed: 32 pictures per secondfarmsSupport generates alarms based on the Video Structuralization features detectiongy NVR16-ch 2 MP (8-ch for each engine), up to 8 MPgy NVR16-ch 2 MP (8-ch for each engine), up to 8 MPface Picture Comparison16-ch; 	Facial Recognition		
Face Picture Libraryface pictures in stranger library, up to 10,000,000 face pictures in face capture (each pictures 4 MB, total capacity 5 20 GB). Generates alarms for list match and strange face detection.Face. Picture Comparisond8-ch (24-ch for each engine); comparison speed: 48 pictures per secondFacial Detection and Analyticcomparison speed: 48 pictures per secondPerimeter Protectiond1-ch 2 MP (8-ch for each engine), up to 8 MPPerimeter Protectiond1-ch 2 MP (12-ch for each engine), up to 8 MPBy NVR41-ch 2 MP (12-ch for each engine), up to 8 MPAuransupper generates alarms of perimeter violationAuransupper generates alarms of perimeter violationFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPface Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPface Picture Library12-ch 2 MP (6-ch for each engine), up to 8 MPface Picture Somparison6-ch; comparison speed: 32 pictures per secondface Picture Comparison6-ch; comparison speed: 32 pictures per secondfarms0 upport generates alarms based on the Video Structuralization features detectionfarms0 cho 2 MP (8-ch for each engine), up to 8 MPfarms0 cho 2 MP (8-ch for each engine), up to 8 MPfarms0 cho 2 MP (8-ch for each engine), up to 8 MPfarms0 cho 2 MP (8-ch for each engine), up to 8 MP <td>Facial Detection and Analytics</td> <td>Face picture comparison, human face capture, face picture search</td>	Facial Detection and Analytics	Face picture comparison, human face capture, face picture search	
(Captured from Camera)Comparison speed: 48 pictures per secondFacial Detection and Analytics Performance16-ch 2 MP (8-ch for each engine), up to 8 MPPerimeter Protection24-ch 2 MP (12-ch for each engine), up to 8 MPBy NVRAll channelsBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 100,000 face pictures in face capture (each picture 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsup to rgenerates alarms based on the Video Structuralization features detectionPartonic Comparison16-ch; Comparison speed: 32 pictures per secondPartonic Comparison16-ch; Comparison speed: 32 pictures per secondPartonic Detection14 channelsPartonic Comparison16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection14 channelsPartonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP (8-ch for each engine), up to 8 MP)Partonic Detection16-ch 2 MP	Face Picture Library	face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture \leq 4 MB, total capacity \leq 20 GB). Generates alarms for list match and strange face	
Performance 16-ch 2 MP (8-ch for each engine), up to 8 MP Perimeter Protection 24-ch 2 MP (12-ch for each engine), up to 8 MP By NVR All channels Alarms Support generates alarms of perimeter violation Video Structuralization Up to 32 face picture libraries, up to 10,000 face pictures in list library, up to 10,000 Face Picture Library Up to 32 face picture libraries, up to 10,000 face pictures in face capture (each engine), up to 10,000 face pictures in face capture (each engine), up to 10,000 face pictures in face capture (each engine), up to 10,000 face pictures in face capture (each engine) face pictures 2 MB, total capacity ≤ 0 GB) Face Picture Comparison Up to 32 face pictures per second Alarms Support generates alarms based on the Video Structuralization features detection By NVR Alchannels By NVR Ich An PI (8-ch for each engine), up to 8 MP) By Camera Alchannels Aurons Ich Annels By RVR Ich Annels By Camera All channels Aurons Ich Annels By Camera All channels Aurons Ich Annels By Camera All channels	· · · · · · · · · · · · · · · · · · ·		
By NVR24-ch 2 MP (12-ch for each engine), up to 8 MPBy CameraAll channelsAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture Analysis12-ch 2 MP (6-ch for each engine), up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 100,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison6-ch; comparison speed: 32 pictures per secondAlarmssupport generates alarms based on the Video Structuralization features detectionPavNR16-ch 2 MP (8-ch for each engine), up to 8 MP)By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens12-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens10-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsAurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to 8 MP)Aurens10-ch 2 MP (8-ch for each engine), up to	•	16-ch 2 MP (8-ch for each engine), up to 8 MP	
By Camera All channels Alarms Support generates alarms of perimeter violation Video Structuralization I2-ch 2 MP (6-ch for each engine), up to 8 MP Structured Analysis 12-ch 2 MP (6-ch for each engine), up to 100,000 face pictures in list library, up to 10,000 face pictures in list capacity (each picture Library) Face Picture Library Up to 32 face picture libraries, up to 100,000 face pictures in face capture (each picture S on speed: 32 pictures per second) Face Picture Comparison 16-ch; Comparison speed: 32 pictures per second Alarms Support generates alarms based on the Video Structuralization features detection By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Qamera All channels By Camera All channels By Camera All channels By Camera All channels By Camera All channels Plate number, license plate color, license plate type	Perimeter Protection		
AlarmsSupport generates alarms of perimeter violationAlarmsSupport generates alarms of perimeter violationVideo Structuralization12-ch 2 MP (6-ch for each engine), up to 8 MPStructured Analysis12-ch 2 MP (6-ch for each engine), up to 100,000 face pictures in list library, up to 100,000 face pictures in stranger library, up to 100,000 face pictures in list library, up to 100,000 face pictures in stranger library, up to 100,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; 	By NVR	24-ch 2 MP (12-ch for each engine), up to 8 MP	
Video Structuralization Structured Analysis 12-ch 2 MP (6-ch for each engine), up to 8 MP Face Picture Library Up to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB) Face Picture Comparison 16-ch; Comparison speed: 32 pictures per second Alarms Support generates alarms based on the Video Structuralization features detection Throwing Objects from Building 16-ch 2 MP (8-ch for each engine), up to 8 MP) By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR Il channels By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By Camera	All channels	
Structured Analysis12-ch 2 MP (6-ch for each engine), up to 8 MPFace Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture < 4 MB, total capacity < 20 GB)	Alarms	Support generates alarms of perimeter violation	
Face Picture LibraryUp to 32 face picture libraries, up to 100,000 face pictures in list library, up to 10,000 face pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detectionFhrowing Objects from Building16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channelsBy CameraAll channelsPlate AttributesPlate number, license plate color, license plate type	Video Structuralization		
Face Picture Libraryface pictures in stranger library, up to 10,000,000 face pictures in face capture (each picture ≤ 4 MB, total capacity ≤ 20 GB)Face Picture Comparison16-ch; Comparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detection Throwing Objects from Building By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channels ANPR Plate AttributesPlate number, license plate color, license plate type	Structured Analysis	12-ch 2 MP (6-ch for each engine), up to 8 MP	
Face Picture ComparisonComparison speed: 32 pictures per secondAlarmsSupport generates alarms based on the Video Structuralization features detection Throwing Objects from Building By NVR16-ch 2 MP (8-ch for each engine), up to 8 MP)By CameraAll channels ANPR By CameraAll channelsPlate AttributesPlate number, license plate color, license plate type	Face Picture Library	face pictures in stranger library, up to 10,000,000 face pictures in face capture (each	
Throwing Objects from Building By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR International statements By Camera All channels Plate Attributes Plate number, license plate color, license plate type	Face Picture Comparison	/	
By NVR 16-ch 2 MP (8-ch for each engine), up to 8 MP) By Camera All channels ANPR International All channels Plate Attributes Plate number, license plate color, license plate type	Alarms	Support generates alarms based on the Video Structuralization features detection	
By Camera All channels ANPR By Camera By Camera All channels Plate Attributes Plate number, license plate color, license plate type	Throwing Objects from Building		
ANPR By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By NVR	16-ch 2 MP (8-ch for each engine), up to 8 MP)	
By Camera All channels Plate Attributes Plate number, license plate color, license plate type	By Camera	All channels	
Plate Attributes Plate number, license plate color, license plate type	ANPR		
	By Camera	All channels	
Vehicle Attributes Vehicle brand, vehicle color, vehicle type	Plate Attributes	Plate number, license plate color, license plate type	
	Vehicle Attributes	Vehicle brand, vehicle color, vehicle type	



Video and Audio			
IP Video Input	64-ch Up to 32 MP resolution *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.		
Incoming Bandwidth	400 Mbps		
Outgoing Bandwidth	400 Mbps		
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.		
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
Video Output Mode	HDMI1 2.0/VGA1 simultaneous output, HDMI2 2.0/VGA2 simultaneous output		
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480		
Audio Output	2-ch, RCA (Linear, 1 KΩ)		
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)		
Decoding			
Decoding Format	H.265/H.265+/H.264/H.264+/MJPEG		
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30 fps)/4-ch@12 MP (20 fps)/8-ch@8 MP (25 fps)/16-ch@4 MP (30 fps)/32-ch@1080p (30 fps)/ 64-ch@720p (30 fps)		
Synchronous Playback	16-ch		
Playback Speed	1/16x, 1/8x, 1/4x, 1/2x, 1x, 2x, 4x, 8x, 16x		
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA /4CIF/DCIF/ 2CIF/CIF/QCIF *: After ultra HD resolution mode is enabled, the NVR supports up to 8-ch 32 MP/24 MP IP video inputs.		
Recording Modes	Manual, schedule and event		
Network			
Remote Connection	128		
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, RTP, RTCP, SADP, SMTP, SNMP, SSH, FTP, SFTP, NFS, UDP, ISCSI, ISUP, UPnP™, HTTP, HTTPS		
API	ONVIF (profile S/G); SDK; ISAPI		
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version		
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface		
Client	iVMS-4200, Hik-Connect (iOS and Android) activated scanning the QR-Code, Hik-Central (Georeferenced on HCP maps)		
RAID			
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10		

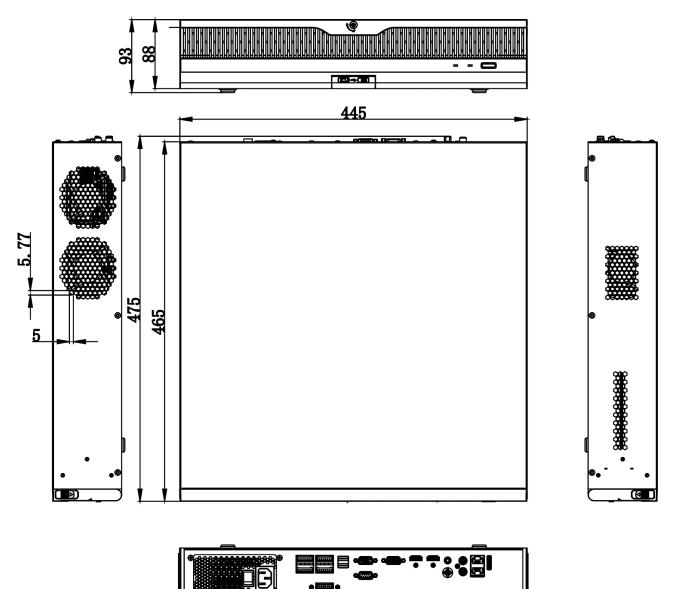


- •

Auxiliary Interface			
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.		
DC 12V	12 VDC, 1 A power output		
SATA	8 SATA interfaces; 3.5-inch HDD		
eSATA	1 eSATA interface		
Capacity	Up to 14 TB capacity for each HDD		
Serial Interface	1 RS-232, 1 RS-485 (full-duplex), 1 keyboard		
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 1 × USB 3.0		
Alarm In/Out	16/9		
General			
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish Language, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian		
Power Supply	100 to 240 VAC, 50 to 60 Hz		
Processor	64bits multi-core		
Memory	RAM 8GB DDR4		
Compute Power	2 TOPS		
Licensing	All features are fully perpetually licensed to operate standalone		
File Lock	Support lock and unlock recorded files		
Video Download	Batch and segment support		
Logs	Audit logs of operation, system, alarms, parameter changes, recordings and others		
Fans	Smart fan control		
Consumption	≤ 100 W		
Working Temperature	-10 to 55° C (14 to 131° F)		
Working Humidity	10 to 90%		
Dimension ($W \times D \times H$)	445 × 465 × 93 mm (17.5"× 18.3" × 3.7"), 2U's		
Weight	\leq 10 kg (without HDD, 28.7 lb.)		
Certification			
Obtained Certification	CE, FCC, IC, CB, KC, UL, Rohs, Reach, WEEE, RCM, UKCA, LOA, BIS		
FCC	Part 15 Subpart B, ANSI C63.4-2014		
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:201		
	9, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020		



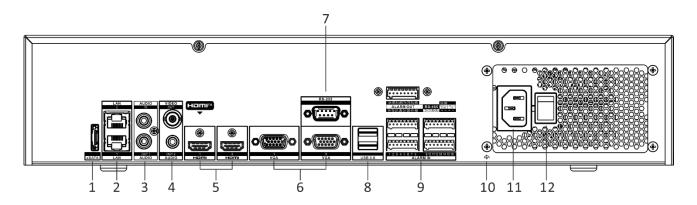
Dimension



scale/1:1;Unit/mm



Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces		USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface, Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

iDS-9664NXI-M8/X



Follow us on social media to get the latest product and solution information.











Hikvision Corporate Channel



@Hikvision Digital Technology Co., Ltd. 2022 | Data subject to change without notice |