



Network Video Recorder

User Manual



Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

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

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

HDMITM : The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF

Network Video Recorder User Manual

PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Regulatory Information

FCC Information

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

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

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

FCC Conditions

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

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

EU Conformity Statement



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

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see:

<http://www.recyclethis.info>

Network Video Recorder User Manual



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

Industry Canada ICES-003 Compliance

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

Applicable Model

This manual is applicable to the following models.

Table 1-1 Applicable Model

Series	Model
DS-9600NI-I8(B)	DS-9608NI-I8(B)
	DS-9616NI-I8(B)
	DS-9632NI-I8(B)
	DS-9664NI-I8(B)
DS-9600NI-I16(B)	DS-9616NI-I16(B)
	DS-9632NI-I16(B)
	DS-9664NI-I16(B)
DS-9600NI-I8	DS-9608NI-I8
	DS-9616NI-I8
	DS-9632NI-I8
	DS-9664NI-I8
DS-9600NI-I16	DS-9616NI-I16
	DS-9632NI-I16
	DS-9664NI-I16
DS-8600NI-I8	DS-8608NI-I8
	DS-8616NI-I8
	DS-8632NI-I8
	DS-8664NI-I8
DS-8600NI-I8/24P	DS-8632NI-I8/24P
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P

Network Video Recorder User Manual

Series	Model
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4(B)	DS-7716NI-I4(B)
	DS-7732NI-I4(B)
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7700NI-I4/P(B)	DS-7716NI-I4/16P(B)
	DS-7732NI-I4/16P(B)
DS-7800NI-I2	DS-7808NI-I2
	DS-7816NI-I2
	DS-7832NI-I2
DS-7800NI-I2/P	DS-7808NI-I2/8P
	DS-7816NI-I2/16P
	DS-7832NI-I2/16P
DS-7900NI-I4	DS-7916NI-I4
	DS-7932NI-I4
DS-7900NI-I4/P	DS-7916NI-I4/16P
	DS-7932NI-I4/16P
	DS-7932NI-I4/24P
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

Network Video Recorder User Manual

Series	Model
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P
	DS-7716NI-M4/16P
	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

Safety Instruction

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- ⚡ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Never place the equipment in an unstable location. The equipment may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This product contains a coin/button cell battery. If the battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- 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 equipment shall not be exposed to dripping or splashing and that no objects filled with liquids shall be placed on the equipment, such as vases.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains, etc. The openings shall never be blocked by placing the equipment on a bed, sofa, rug or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Use only power supplies listed in the user manual or user instruction.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Use only power supplies listed in the user manual or user instruction.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.

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

Contents

Chapter 1 Basic Operation	1
1.1 Activate Your Device	1
1.1.1 Default User and IP Address	1
1.1.2 Activate via Local Menu	1
1.1.3 Activate via SADP	2
1.1.4 Activate via Client Software	3
1.1.5 Activate via Web Browser	6
1.2 Configure TCP/IP	7
1.3 Configure HDD	9
1.4 Add Network Camera	9
1.4.1 Add Automatically Searched Online Network Camera	10
1.4.2 Add Network Camera Manually	10
1.4.3 Add Network Camera Through PoE	11
1.4.4 Add Solar-Powered Camera Through OTAP Protocol	14
1.4.5 Add Network Camera via Customized Protocol	15
1.5 Connect to Platform	16
1.5.1 Configure ISUP	16
1.5.2 Configure Hik-Connect	18
1.5.3 Configure OTAP	19
Chapter 2 Camera Settings	21
2.1 Configure OSD	21
2.2 Configure Image Parameters	22
2.3 Configure Privacy Mask	22
2.4 Configure IP Camera Time Sync	23
2.5 Configure Camera Microphone Settings	24
2.6 Configure Solar-Powered Camera Parameters	25
2.7 Import Network Camera Certificate	25
2.8 Import/Export IP Camera Configuration Files	25
2.9 Save Camera VCA Data	26

Network Video Recorder User Manual

2.10 Upgrade IP Cameras.....	26
Chapter 3 Live View	28
3.1 Start Live View	28
3.1.1 Configure Live View Settings	29
3.1.2 Configure Live View Layout	30
3.1.3 Switch Main/Auxiliary Port	32
3.2 Digital Zoom.....	32
3.3 Fisheye View	33
3.4 3D Positioning	33
3.5 Configure Channel-Zero Encoding.....	34
3.6 Configure Transcoded Live View	34
3.7 PTZ Control	36
3.7.1 Configure PTZ Parameters.....	36
3.7.2 Set a Preset	36
3.7.3 Call a Preset.....	37
3.7.4 Set a Patrol	37
3.7.5 Call a Patrol	39
3.7.6 Set a Pattern.....	40
3.7.7 Call a Pattern	41
3.7.8 Set Linear Scan Limit	41
3.7.9 One-Touch Park.....	42
Chapter 4 Recording and Playback	43
4.1 Recording.....	43
4.1.1 Configure Recording Parameters	43
4.1.2 Enable H.265 Stream Access.....	45
4.1.3 ANR	45
4.1.4 Manual Recording	45
4.1.5 Configure Recording Schedule	45
4.1.6 Configure Holiday Recording.....	47
4.2 Playback.....	48
4.2.1 Instant Playback	48

Network Video Recorder User Manual

4.2.2 Play Normal Video.....	49
4.2.3 Play Smart Searched Video	50
4.2.4 Play Custom Searched Files	51
4.2.5 Play Tag Files	51
4.2.6 Play by Sub-periods.....	52
4.2.7 Play External Files	53
4.3 Playback Operations	53
4.3.1 Edit Video Clips	53
4.3.2 Configure Transcoded Playback	53
4.3.3 Thumbnails View.....	54
Chapter 5 Picture Capture	56
5.1 Configure Parameters	56
5.2 Configure Capture Schedule.....	56
5.3 Configure Holiday Capture Schedule	56
Chapter 6 Event	58
6.1 Normal Event Alarm.....	58
6.1.1 Configure Motion Detection Alarms	58
6.1.2 Configure Video Loss Alarms.....	58
6.1.3 Configure Video Tampering Alarms	59
6.1.4 Configure Sensor Alarms	59
6.1.5 Configure Exceptions Alarms.....	59
6.1.6 Flashing Light Alarm Output.....	60
6.1.7 Audio Alarm Output.....	61
6.1.8 Configure Combined Alarm	61
6.2 VCA Event Alarm	62
6.2.1 Temperature Screening.....	63
6.2.2 Transparent Transmission	63
6.2.3 Hard Hat Detection	64
6.2.4 Face Capture	64
6.2.5 Line Crossing Detection	65
6.2.6 Intrusion Detection	67

6.2.7 Region Entrance Detection	68
6.2.8 Region Exiting Detection	70
6.2.9 Vehicle Detection	71
6.2.10 Multi-Target-Type Detection	71
6.2.11 Object Thrown from Building	72
6.2.12 Loitering Detection	73
6.2.13 People Gathering Detection	75
6.2.14 Fast Moving Detection	76
6.2.15 Parking Detection	77
6.2.16 Unattended Baggage Detection	78
6.2.17 Object Removal Detection	79
6.2.18 Audio Exception Detection	81
6.2.19 Defocus Detection	82
6.2.20 Sudden Scene Change Detection	83
6.2.21 PIR Alarm	83
6.2.22 Thermal Camera Detection	84
6.2.23 Queue Management	85
6.3 Target Detection	85
6.4 Configure Arming Schedule	86
6.5 Configure Linkage Actions	87
6.5.1 Configure Auto-Switch Full Screen Monitoring	87
6.5.2 Configure Buzzer	88
6.5.3 Notify Surveillance Center	88
6.5.4 Configure Email Linkage	88
6.5.5 Configure Audio Alert	89
6.5.6 Trigger Alarm Output	89
6.5.7 Configure Audio and Light Alarm Linkage	90
6.5.8 Configure PTZ Linkage	90
Chapter 7 IoT	91
7.1 Add an IoT Device	91
7.1.1 Add an Access Control Device	91

Network Video Recorder User Manual

7.1.2 Add an Alarm Device	92
7.1.3 Add Network Audio Device	93
7.2 Configure the Linkage Action and Arming Schedule	94
7.3 Configure OSD	95
7.4 Configure Audio Parameters	96
7.5 Search the IoT Record	96
7.6 IoT Video/Picture	98
7.6.1 Configure the Event Recording/Capturing	98
7.6.2 Search IoT Video	100
Chapter 8 Smart Report	102
8.1 People Counting	102
8.2 Heat Map	102
Chapter 9 Self-Learning	104
9.1 Add False Alarm Pictures to Self-Learning Library	104
9.2 Delete False Alarm Pictures in Self-Learning Library	105
Chapter 10 File Management	106
10.1 Search Files	106
10.2 Export Files	106
10.3 Quick Backup	107
10.4 Smart Search	107
10.4.1 Face Picture Search	107
10.4.2 Human Search	108
10.4.3 Vehicle Search	109
Chapter 11 Storage	110
11.1 Storage Device Management	110
11.1.1 Manage Local HDD	110
11.1.2 Add a Network Disk	112
11.1.3 Configure Cloud Storage	113
11.1.4 Manage eSATA	114
11.1.5 Dynamically Adjust Recording Writing Buffer	116
11.2 Disk Array	117

Network Video Recorder User Manual

11.2.1 Create a Disk Array	117
11.2.2 Rebuild an Array	120
Chapter 12 Hot Spare Device Backup	123
12.1 Set Working Device	123
12.2 Set Hot Spare Device	124
12.3 Manage Hot Spare System	124
Chapter 13 Network Settings	127
13.1 Configure DDNS	127
13.2 Configure PPPoE	127
13.3 Configure SNMP	128
13.4 Configure Email	130
13.5 Configure Port Mapping (NAT)	131
13.6 Configure Port	132
13.7 Configure ONVIF	134
Chapter 14 POS Configuration	135
14.1 Configure POS Connection	135
14.2 Configure POS Text Overlay	138
14.3 Configure POS Alarm	139
Chapter 15 User Management and Security	141
15.1 Manage User Accounts	141
15.1.1 Add a User	141
15.1.2 Edit the Admin User	142
15.1.3 Edit an Operator/Guest User	143
15.2 Manage User Permissions	144
15.2.1 Set User Permissions	144
15.2.2 Set Live View Permission on Lock Screen	146
15.2.3 Set Double Verification Permission for Non-admin Users	147
15.3 Configure Password Security	148
15.3.1 Export GUID File	148
15.3.2 Configure Security Questions	149
15.3.3 Configure Reserved Email	150

15.4 Reset Password	151
15.4.1 Reset Password by GUID	151
15.4.2 Reset Password by Security Questions	152
15.4.3 Reset Password by Reserved Email	152
15.4.4 Reset Password by Hik-Connect	153
Chapter 16 System Management	154
16.1 Configure Device	154
16.2 Configure Time	154
16.2.1 Manual Time Synchronization	155
16.2.2 NTP Synchronization	155
16.2.3 DST Synchronization	155
16.3 Audio Management	156
16.4 Configure Enhanced SVC Mode	156
16.5 Network Detection	157
16.5.1 Network Traffic Monitoring	157
16.5.2 Test Network Delay and Packet Loss	157
16.5.3 Export Network Packet	158
16.5.4 Network Resource Statistics	158
16.6 Storage Device Maintenance	159
16.6.1 Bad Sector Detection	159
16.6.2 S.M.A.R.T. Detection	160
16.6.3 HDD Health Detection	161
16.6.4 Configure Disk Clone	161
16.6.5 Repair Database	162
16.7 Upgrade Device	163
16.7.1 Upgrade by Local Backup Device	163
16.7.2 Upgrade by FTP	163
16.7.3 Upgrade by Hik-Connect	164
16.8 Import/Export Device Configuration Files	164
16.9 Log Management	165
16.9.1 Log Storage	165

16.9.2 Search & Export Log Files	166
16.9.3 Upload Logs to the Server	167
16.9.4 One-Way Authentication	168
16.9.5 Two-Way Authentication	168
16.10 Restore Default Settings	169
16.11 Schedule Reboot	170
16.12 Security Management	170
16.12.1 Configure ONVIF	170
16.12.2 IP/MAC Address Filter	171
16.12.3 RTSP Authentication	172
16.12.4 RTSP Digest Algorithm	173
16.12.5 ISAPI Service	173
16.12.6 HTTP Authentication	173
16.12.7 HTTP/Web Digest Algorithm	173
16.12.8 Picture URL Digest Authentication	174
16.12.9 Serial Port Authentication Service	174
Chapter 17 Appendix	175
17.1 Glossary	175
17.2 Frequently Asked Questions	176
17.2.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?	176
17.2.2 Why is the video recorder notifying the stream type is not supported?	177
17.2.3 Why is the video recorder notifying risky password after a network camera is added?	177
17.2.4 How to improve the playback image quality?	177
17.2.5 How to confirm the video recorder is using H.265 to record video?	177
17.2.6 Why is the timeline at playback not constant?	178
17.2.7 Why is the video recorder notifying the network is unreachable when a network camera is being added?	178
17.2.8 Why is the IP address of network camera being changed automatically?	178
17.2.9 Why is the video recorder notifying IP conflict?	179
17.2.10 Why is image getting stuck when playing back by single or multi-channel	

cameras?	179
17.2.11 Why does my video recorder make a beeping sound after booting?	179
17.2.12 Why is there no recorded video after the motion detection is set?	179
17.2.13 Why is the video sound quality not good?	180

Chapter 1 Basic Operation

1.1 Activate Your Device

1.1.1 Default User and IP Address

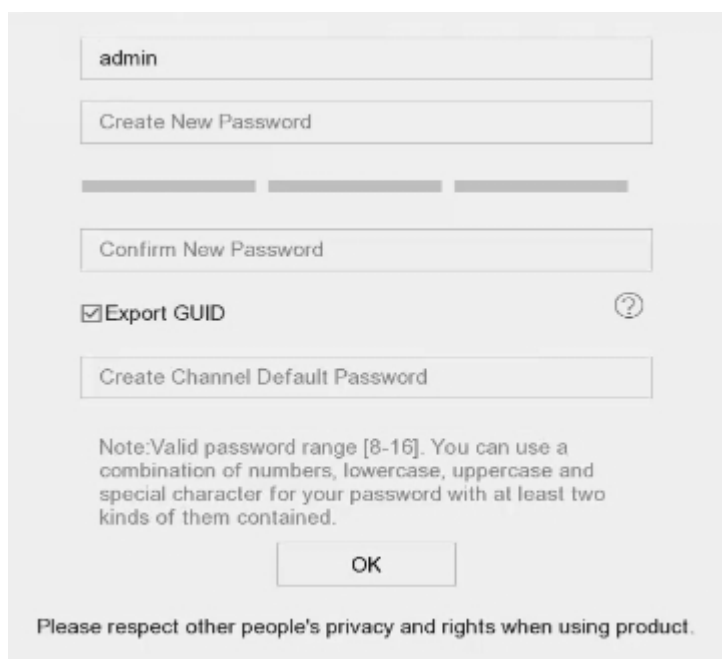
- Default administrator account: admin.
- Default IPv4 address: 192.168.1.64.

1.1.2 Activate via Local Menu

For the first-time access, you 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.

Steps

1. Enter the admin password twice.



The screenshot shows a local menu interface for activating the device. It includes the following elements:

- A text field containing "admin".
- A button labeled "Create New Password".
- A horizontal separator line.
- A text field labeled "Confirm New Password".
- A checkbox labeled "Export GUID" with a question mark icon to its right.
- A button labeled "Create Channel Default Password".
- A note: "Note: Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained."
- An "OK" button.
- A footer text: "Please respect other people's privacy and rights when using product."

Figure 1-1 Activate via Local Menu

Network Video Recorder User Manual

Warning

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

2. Enter a password to activate network cameras that are connected to the device.
 3. Click **OK**.
-



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

What to do next

Follow the wizard to set basic parameters.

- There are methods to reset your password when you forget. You have to configure at least one password resetting method after activation.
- For Hik-Connect configuration, refer to [**Configure Hik-Connect**](#) for details.

1.1.3 Activate via SADP

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

Before You Start

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

Steps

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



-
- Note**

5. Click **Activate**.

1.1.4 Activate via Client Software

Before You Start

Steps

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

Network Video Recorder User Manual

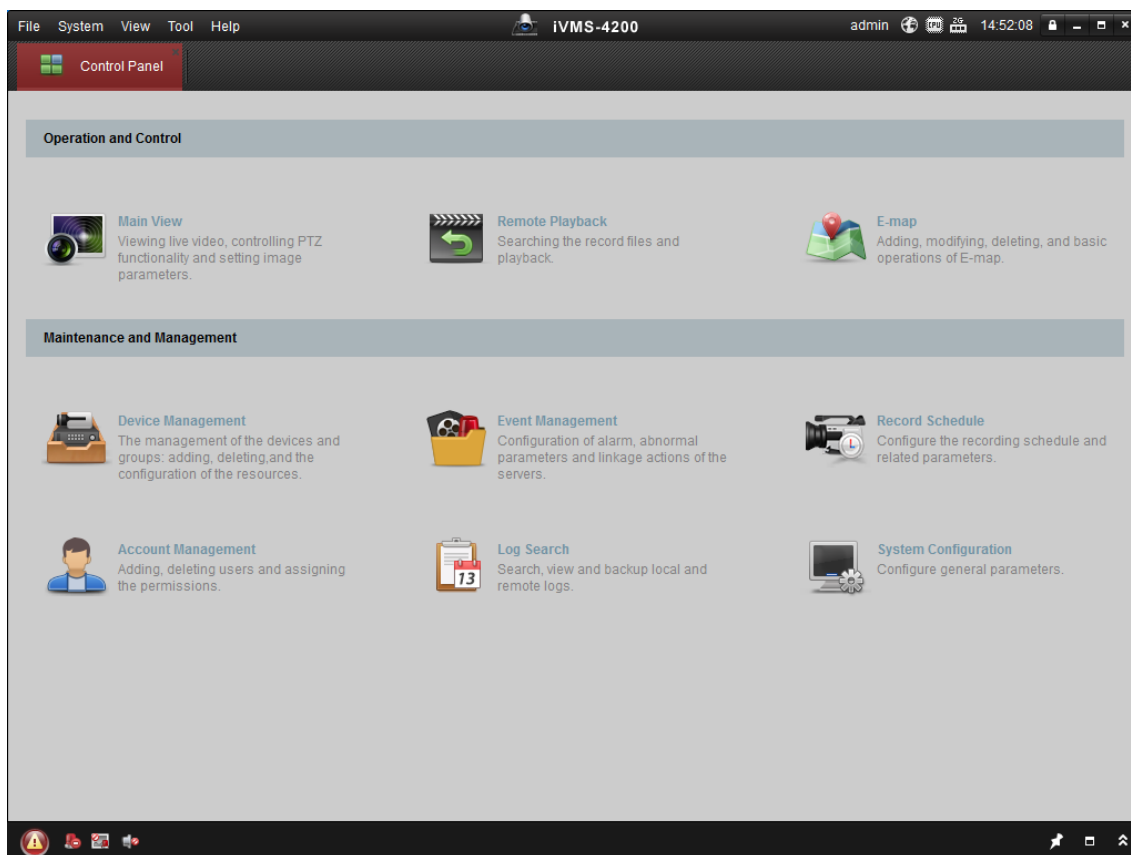


Figure 1-3 Control Panel

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

Network Video Recorder User Manual

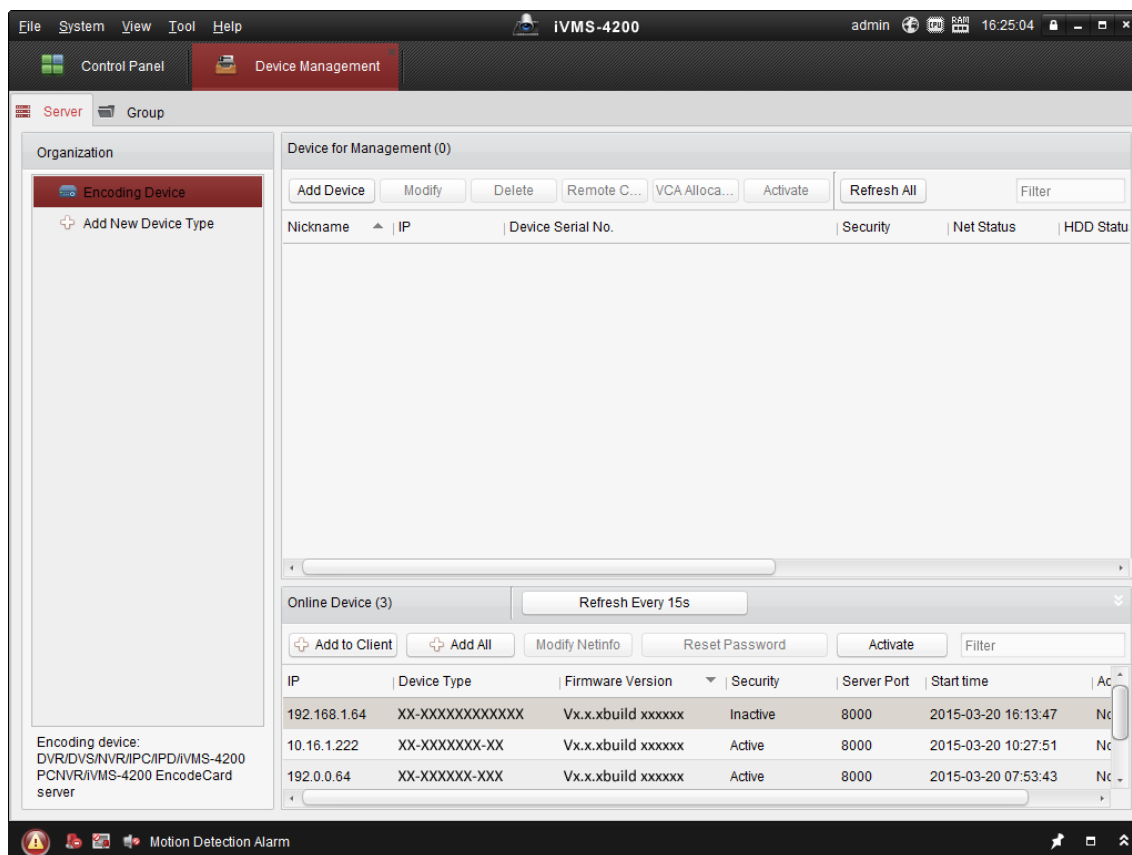
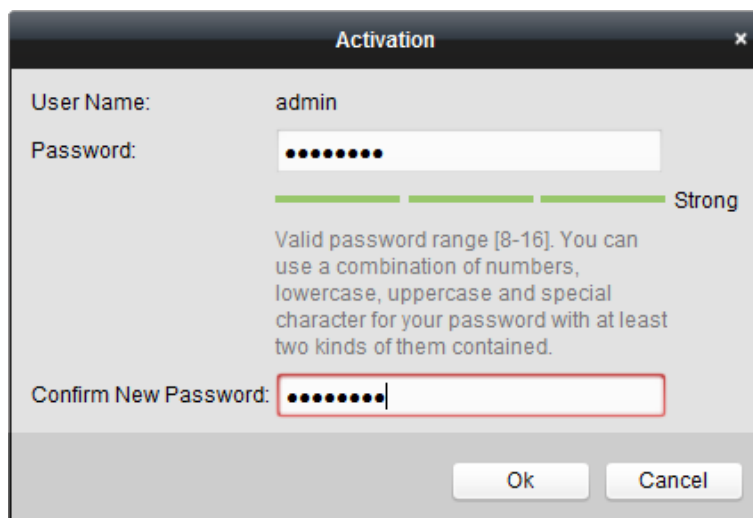


Figure 1-4 Device Management Interface

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

Note

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

The 'Activation' dialog box has a title bar with a close button. It contains a 'User Name' field with 'admin' entered. The 'Password' field is masked with dots and has a strength indicator below it showing three green bars and the word 'Strong'. A text message below the password field states: 'Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' The 'Confirm New Password' field is also masked with dots and is highlighted with a red border. At the bottom are 'Ok' and 'Cancel' buttons.

Activation

User Name: admin

Password: [masked] Strong

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

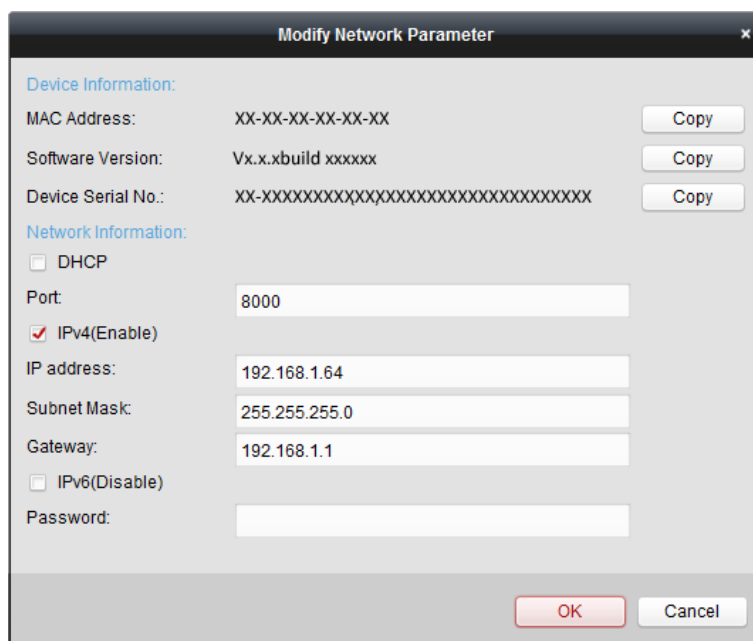
Confirm New Password: [masked]

Ok Cancel

Figure 1-5 Activation

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

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

The 'Modify Network Parameter' dialog box has a title bar with a close button. It is divided into two sections: 'Device Information' and 'Network Information'. 'Device Information' includes fields for 'MAC Address' (XX-XX-XX-XX-XX-XX), 'Software Version' (Vx.x.xbuild xxxxxx), and 'Device Serial No.' (XX-XXXXXXXXXX-XXXXXXXXXXXXXXXXXXXX), each with a 'Copy' button. 'Network Information' includes a 'DHCP' checkbox (unchecked), a 'Port' field (8000), an 'IPv4(Enable)' checkbox (checked), an 'IP address' field (192.168.1.64), a 'Subnet Mask' field (255.255.255.0), a 'Gateway' field (192.168.1.1), an 'IPv6(Disable)' checkbox (unchecked), and a 'Password' field. At the bottom are 'OK' and 'Cancel' buttons.

Modify Network Parameter

Device Information:

MAC Address: XX-XX-XX-XX-XX-XX Copy

Software Version: Vx.x.xbuild xxxxxx Copy

Device Serial No.: XX-XXXXXXXXXX-XXXXXXXXXXXXXXXXXXXX Copy

Network Information:

☐ DHCP

Port: 8000

☒ IPv4(Enable)

IP address: 192.168.1.64

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

☐ IPv6(Disable)

Password: [empty]

OK Cancel

Figure 1-6 Modify Network Parameters

8. Change the recorder IP address to the same subnet with your computer.

Modify the IP address manually. Check **Enable DHCP**.

9. Input the password to activate your IP address modification.

1.1.5 Activate via Web Browser

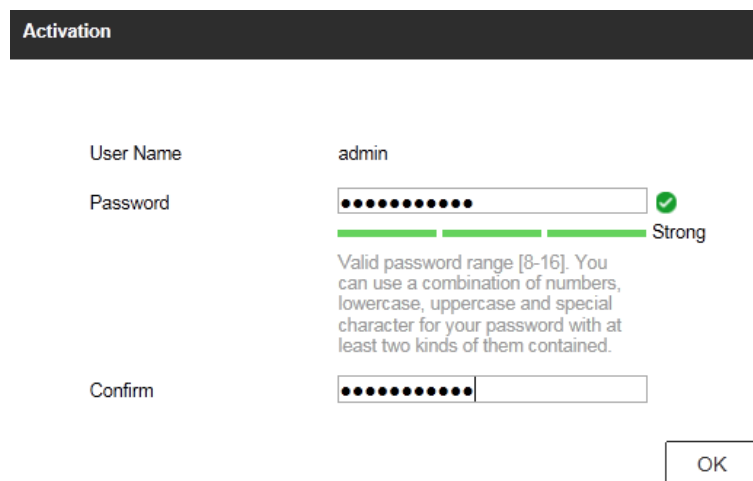
You can get access to the recorder via web browser. You may use one of the following web browsers: Internet Explorer 6.0 and above, Apple Safari, Mozilla Firefox, and Google Chrome. The

Network Video Recorder User Manual

supported resolutions include 1024 × 768 and above.

Steps

1. Enter the IP address in web browser, and then press **Enter**. The default IP address is 192.168.1.64.



The image shows a web browser activation form. At the top, there is a dark header bar with the word "Activation" in white. Below this, the form has three main input sections: "User Name" with the value "admin", "Password" with a masked input (dots) and a green checkmark indicating it is "Strong", and "Confirm" with a masked input. A green progress bar is visible below the password field. A text box provides instructions: "Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained." At the bottom right, there is an "OK" button.

Figure 1-7 Web Browser Activation

2. Set the password for the admin user account.

Note

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

3. Click **OK**.

1.2 Configure TCP/IP

TCP/IP must be properly configured before operating your device over a network. Both IPv4 and IPv6 are available.

Steps

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

Network Video Recorder User Manual

Figure 1-8 TCP/IP Settings

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

Net-Fault Tolerance

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

Multi-Address Mode

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

3. Click **IPv4** or **IPv6** as you required.
4. Optional: Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available on the network.
5. Set related parameters.

Note

Valid MTU value range is from 500 to 1500.

6. Click **Apply**.

1.3 Configure HDD

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

1.4 Add Network Camera

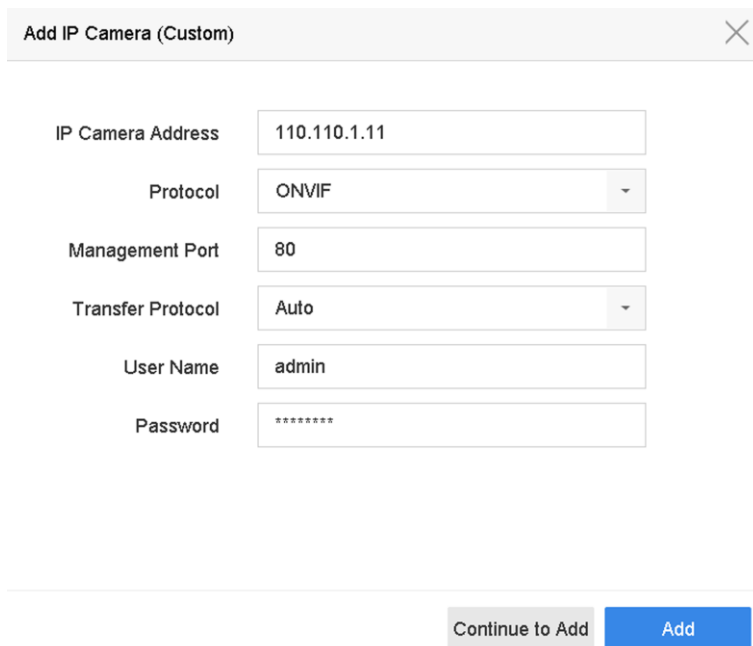
Before you can get live video or record the video files, you must add the network cameras to the connection list of the device.

Before You Start

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

Steps

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



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

Continue to Add Add

Figure 1-9 Add IP Camera

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

1.4.1 Add Automatically Searched Online Network Camera

Steps

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

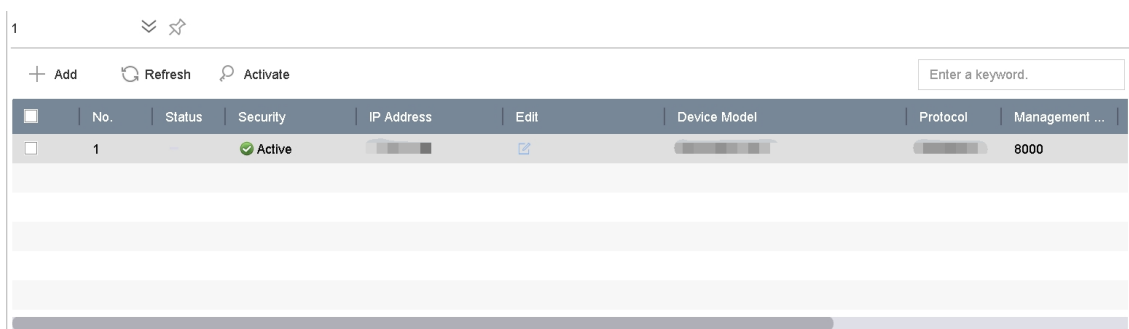


Figure 1-10 Add Automatically Searched Online Network Camera

Note

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

1.4.2 Add Network Camera Manually

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

Before You Start

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

Steps

1. Click  on the main menu.
2. Click **Custom Add**.
3. Set the parameters. For example, **IP Camera Address**, **Protocol**, etc.

Note

Management port ranges from 1 to 65535.

Network Video Recorder User Manual

Figure 1-11 Add Network Camera

4. Optional: Check **Use Channel Default Password** to use the default password to add the camera.
5. Optional: Check **Enable IP Camera Time Sync** to synchronize the time of the connected IP camera automatically. For details, refer to [**Configure IP Camera Time Sync.**](#)
6. Optional: Check **Use Default Port** to use the default management port to add the camera. For SDK service, the default port value is 8000. For enhanced SDK service, the default value is 8443.

Note

The function is only available when you use HIKVISION protocol.

7. Optional: Check **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function. For details, refer to [**Import Network Camera Certificate.**](#)

Note

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

8. Optional: Click **Search** to search other network cameras.
9. Optional: Click **Continue to Add** to add other network cameras.
10. Click **Add**.

1.4.3 Add Network Camera Through PoE

The PoE interfaces enable the device system to pass electrical power safely, along with data, on Ethernet cabling to the connected PoE cameras. Supported PoE camera number varies with device module. If you disable the PoE interface, you can also connect to the online network cameras. And

the PoE interface supports the Plug-and-Play function.

Add PoE Camera

Steps

1. Go to **Camera** → **Camera** → **PoE Settings**.
2. Enable or disable long network cable mode by selecting **Long Distance** or **Short Distance**.

Long Distance

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

Short Distance

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

Note

- The PoE ports 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.
-

Network Video Recorder User Manual

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

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

Apply

Figure 1-12 Add PoE Camera

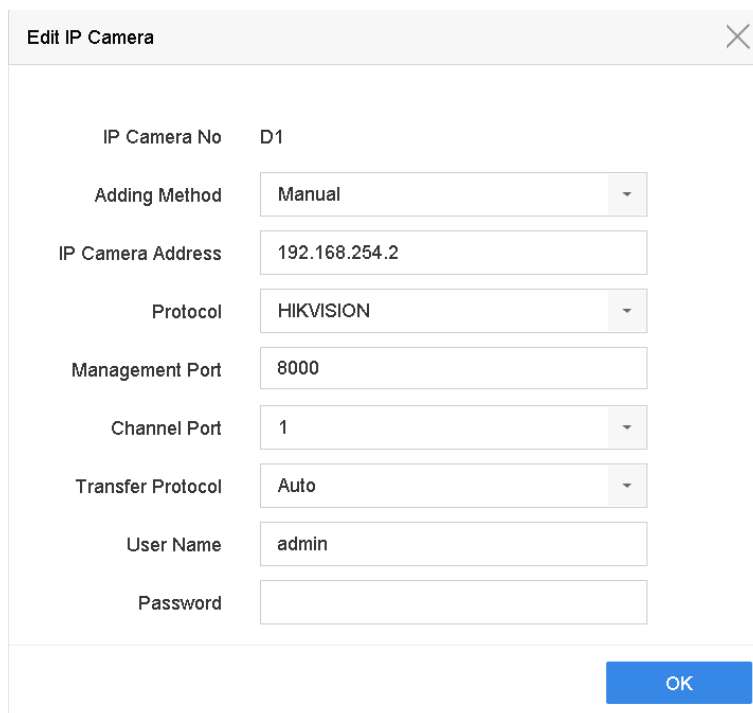
3. Click **Apply**.
4. Connect PoE cameras to device PoE ports with network cables.
5. Go to **Camera → Camera → IP Camera** to view camera image and information.

Add Non-PoE Network Camera

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

Steps

1. Go to **Camera → Camera → IP Camera**.
2. Position the cursor on a window with no linked network camera and click .



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

OK

Figure 1-13 Edit Network Camera

3. Select **Adding Method** as **Manual**.

Plug-and-Play

The camera is physically connected to the PoE interface. Its parameters cannot be edited. You can go to **System** → **Network** → **TCP/IP** to change IP address of PoE port.

Manual

Add IP camera without physical connection via network.

4. Enter **IP address**, **User Name**, and **Password**.
5. Click **OK**.

1.4.4 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.

Steps

1. Go to **Maintenance** → **System Service** → **System Service** to enable **Enable OTAP Network Camera Service**.
2. Go to **Camera** → **Camera** → **IP Camera** → **More Settings** → **OTAP** to set **OTAP Server Port** and **Encryption Key**.

Network Video Recorder User Manual

Figure 1-14 Set OTAP Parameters

3. Optional: Enable **Auto Add IP Camera**.**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.

4. Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.

Note

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

5. Add solar-powered camera(s) to your device.

- If you have enabled **Auto Add IP Camera** in **Camera → Camera → IP Camera → More Settings → OTAP**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
- Select solar-powered camera(s) from **Number of Unadded Online Device** list, and click **Add**.
- Click **Custom Add**, 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 [**ANR**](#).

1.4.5 Add Network Camera via Customized Protocol

For network cameras that are not using standard protocols, you can configure customized

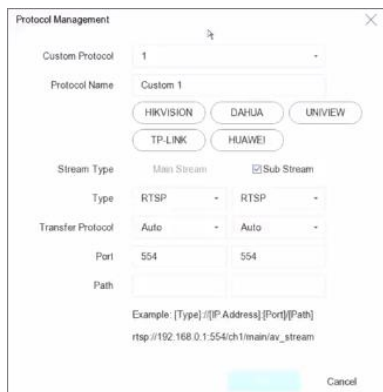
Network Video Recorder User Manual

protocols to add them. The system provides 8 customized protocols.

Steps

1. Click  on the main menu.
2. Go to **More Settings** → **Protocol**.

Note



Protocol Management

Custom Protocol: 1

Protocol Name: Custom 1

Stream Type: ☐ Main Stream ☒ Sub Stream

Type: RTSP

Transfer Protocol: Auto

Port: 554

Path:

Example: [Type]://[IP Address]:[Port]/[Path]
rtsp://192.168.0.1:554/ch1/main/av_stream

Cancel

3. Set protocol parameters.

Type

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

Path

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

Note

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

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

1.5 Connect to Platform

1.5.1 Configure ISUP

SDK is based on Intelligent Security Uplink Protocol (ISUP). It provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the

Network Video Recorder User Manual

third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System** → **Network** → **Advanced** → **Platform Access**.



Access Type	ISUP
Enable	☒
Server Address	
Server Port	7660
Registration Status	Offline
Device ID	720251740
Version	ISUP5.0
Encryption Password	*****

Figure 1-15 ISUP Settings

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

 Note

Enabling ISUP will disable other platform access.

4. Set the related parameters.

Server Address

The platform server IP address.

Server Port

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

Device ID

Device ID shall be provided by the platform.

Version

ISUP protocol version, only V5.0 is available.

Encryption Password

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is

registered to the ISUP platform. It cannot be empty, or "ABCDEF".

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

What to do next

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

1.5.2 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** → **Network** → **Advanced** → **Platform Access**.
2. Check **Enable** to activate the function. Then the service terms will pop up.
 - 1) Enter **Verification Code**.
 - 2) Scan the QR code to read the service terms and privacy statement.
 - 3) Check **The Hik-Connect service will require Internet access. Please read Service Terms and Privacy Statement before enabling the service.** if you agree with the service terms and privacy statement.
 - 4) Click **OK**.

Note

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

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



Figure 1-16 Download Hik-Connect

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

 Note

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

5. Click **Apply**.

What to do next

You can access your video recorder via Hik-Connect.

1.5.3 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 protocol.

Steps

1. Go to **System** → **Network** → **Advanced** → **Platform Access**.
2. Set **Access Type** as **OTAP**.

Network Video Recorder User Manual

Access Type	OTAP
Enable	☒
Server Address	
Server Port	7800
Registration Status	Offline
Device ID	L20545343
Encryption Password	*****

Figure 1-17 OTAP

3. Check **Enable**.
4. Set the parameters.
5. Click **Apply**.

Chapter 2 Camera Settings

2.1 Configure OSD

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

Steps

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

Camera

[D2] IPdome

Camera Name

IPdome



Apply

OSD Settings

☒ Display Name

☒ Display Date

☒ Display Week

Date Format

MM-DD-YYYY

Time For...

24-hour

Display M...

Non-Transparent & No

OSD Font

16x16

Image Settings

>

Exposure

>

Day/Night Switch

>

Backlight

>

Image Enhancement

>

Figure 2-1 OSD Settings

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

2.2 Configure Image Parameters

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

Image Settings

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

Exposure

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

Day/Night Switch

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

Supplement Light

For certain models, you can configure supplement light and the light brightness.

Backlight

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

Image Enhancement

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

2.3 Configure Privacy Mask

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

Steps

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

Network Video Recorder User Manual

Camera

08-23-2017 Wed 11:52:49



☒ Enable

☐ Clear Area 1

☐ Clear Area 2

☐ Clear Area 3

☐ Clear Area 4

Figure 2-2 Privacy Mask Settings

Note

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

5. Click **Apply**.

2.4 Configure IP Camera Time Sync

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

Steps

1. Go to **Camera** → **Camera** → **IP Camera**.

Network Video Recorder User Manual

2. Position the cursor on the window of the IP camera and click .
3. Check **Enable IP Camera Time Sync**.
4. Click **OK**.
5. Optional: All IPC channels can be enabled/disabled with shortcuts.
 - 1) Go to **Maintenance** → **System Service** → **More Settings**.
 - 2) Click **Time Sync Configuration**, select **Enable IPC Time Sync** or **Disable IPC Time Sync** to enable/disable scheduled time sync for all IPC/IoT channels.

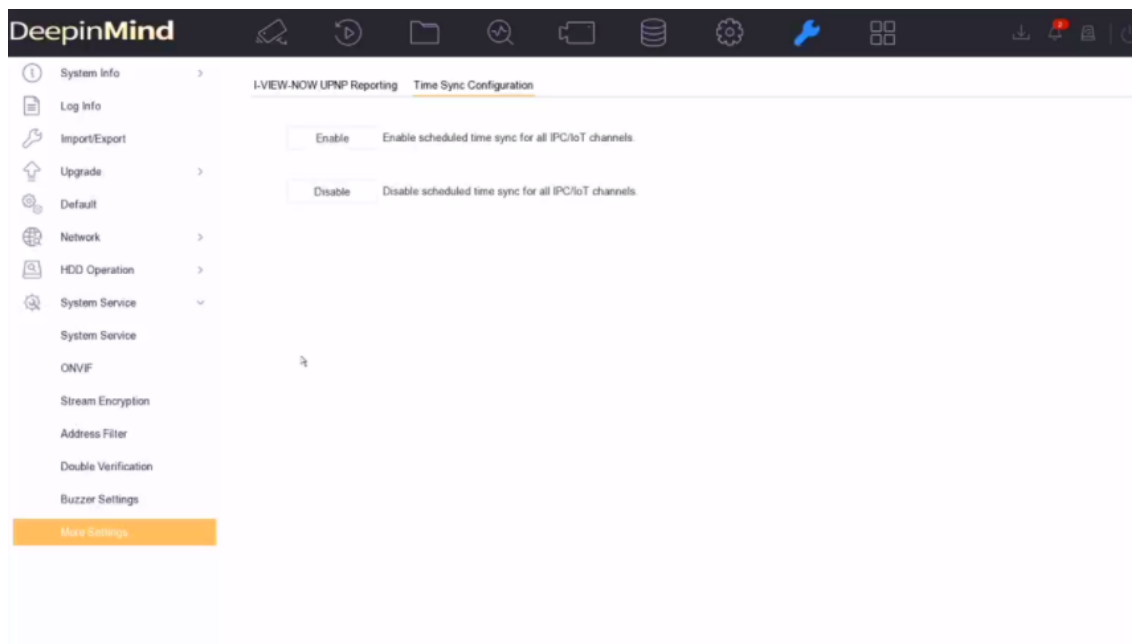


Figure 2-3 IP Camera Time Sync

 Note

This function is only available for the admin user.

2.5 Configure Camera Microphone Settings

The camera microphone can be enabled to record audio.

Go to **Camera** → **Camera** → **IP Camera** → **More Settings** → **Camera Microphone Settings**.

 Note

After enabling, the camera would record audio, which may collect personal information and violate privacy. Please comply with the local laws and regulations and the related rules.

2.6 Configure Solar-Powered Camera Parameters

After a solar-powered camera is added to your device, you can configure its parameters through web browser.

Before You Start

Ensure a solar-powered camera is added to your device.

Steps

1. Log in to the device through web browser.
2. Go to **Configuration** → **Low Power Consumption**.
3. Select the solar-powered camera.
4. Set the camera mode as your desire.
5. Click **Save**.

2.7 Import Network Camera Certificate

Import the network camera certificate to the video recorder.

Steps

1. Log in the network camera via web browser.
2. Go to **Configuration** → **Network** → **Advanced Settings** → **HTTPS** on the web browser to export its certificate.
3. Click **Export** at **Export Certificate** to save the certificate.
4. Log in the video recorder by web browser.
5. Go to **Configuration** → **System** → **Security** → **Trusted Root Certification Authorities** → **Import**.
6. Click **Import** to import the network camera certificate.

2.8 Import/Export IP Camera Configuration Files

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

Before You Start

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

Steps

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

Network Video Recorder User Manual

- To import a configuration file, select the file from the selected backup device and click **Import**.

Note

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

2.9 Save Camera VCA Data

After saving camera VCA data to your device, you will be able to search the camera VCA data.

Go to **Storage** → **Advanced** to enable **Save VCA Data** via local GUI interface.

Go to **Configuration** → **Video and Audio** → **Display Info. on Scream** to turn on **Enable Dual-VCA** via web browser.

2.10 Upgrade IP Cameras

The IP camera can be upgraded through the device.

Steps

1. Go to **Camera** → **Camera** → **IP Camera** → **More Settings** → **Upgrade**.

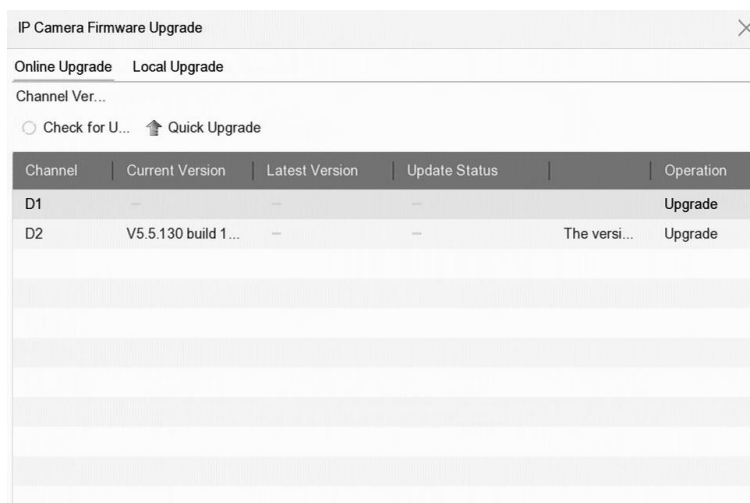


Figure 2-4 Upgrade IP Cameras

2. Select a method to upgrade your camera.

Online Upgrade

Click **Online Upgrade**, and click **Check for Updates** or **Quick Upgrade** to upgrade your cameras.

Note

Your device shall be properly connected to Hik-Connect.

Local Upgrade

Inserted a USB flash drive that contains the firmware to your device. Click **Local Upgrade**, and select the camera and firmware file for upgrade.

The IP camera will automatically restart after it is upgraded.

3. Click **Upgrade**.

Chapter 3 Live View

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

3.1 Start Live View

Click  on the main menu bar.

- Select a window and double click a camera from the channel list to play the live image of the camera.
 - Double click a window to view it in single-screen mode. Double click again to exit single-screen mode.
 - Use the toolbar at the playing window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.
-

Note

- Click  at the lower right corner to stop all-day continuous recordings.
 - If you have added audio device(s) to the recorder, you can move the cursor to  to select an audio source. But this selection is used for live view only, it will not affect the audio recording settings.
-
- Click  to start/stop auto-switch. The screen will automatically switch to the next one.
 - Single click  to enable VCA information display. Double click  to disable VCA information display.
-

Note

Click  at the lower right corner to enable/disable VCA information display for all channels. VCA information of 16 channels (maximum) is available.

- Move the cursor to a window, and right click your mouse to display the shortcut menu of the window. The shortcut menu will be different according to the window.

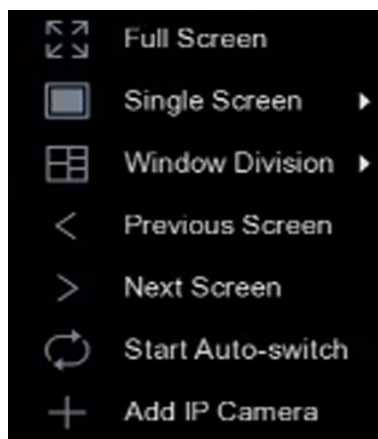


Figure 3-1 Shortcut Menu

Note

If exception occurs, error information will be displayed on the screen. Click  to edit the parameters of different channel(s).

3.1.1 Configure Live View Settings

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

Steps

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

Figure 3-2 Live View-General

2. Configure the live view parameters.

Video Output Interface

Select the video output to configure.

Live View Mode

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

Dwell Time

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

Enable Audio Output

Enable/disable audio output for the selected video output.

Volume

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

Event Output

Select the output to show event video.

Full Screen Monitoring Dwell Time

Set the time in seconds to show alarm event screen.

3. Click **OK**.

3.1.2 Configure Live View Layout

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

Configure Custom Live View Layout

Steps

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

Network Video Recorder User Manual

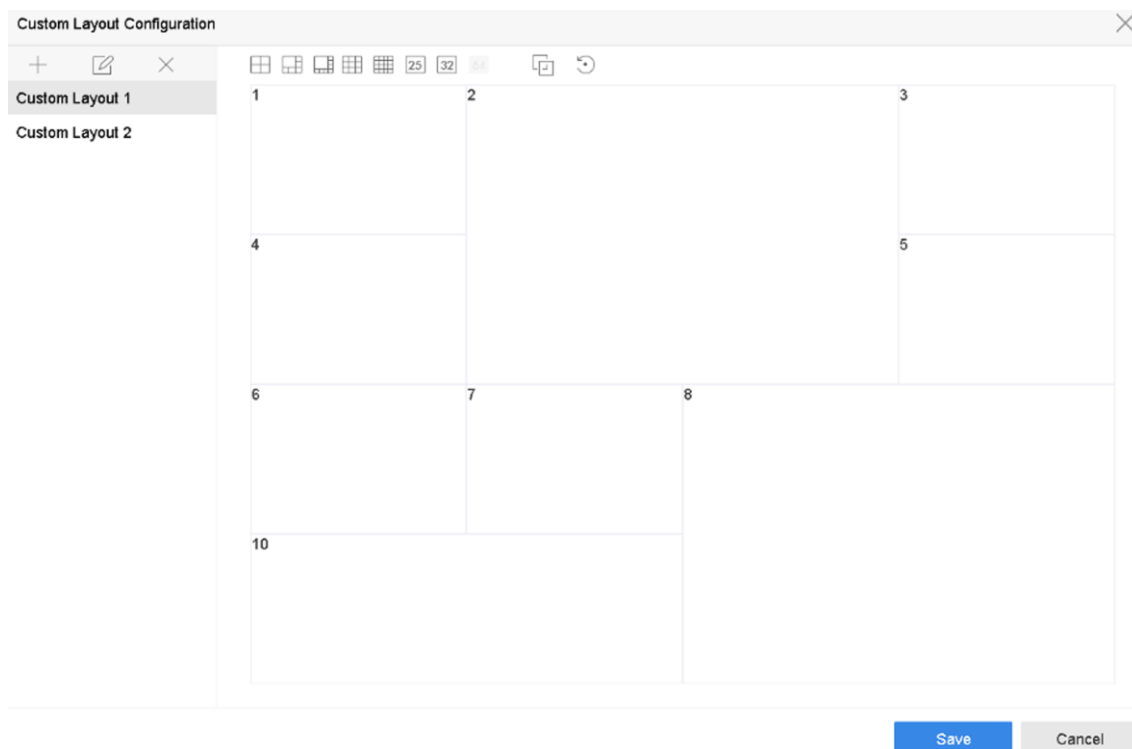


Figure 3-3 Configure Live View Layout

6. Select multiple windows and click  to joint the windows. The selected windows must be in rectangle area.
7. Click **Save**.
The successfully configured layout is displayed in the list.
8. Optional: Select a live view layout from the list and click  to edit the name, or click  to delete the name.

Configure Live View Mode

Steps

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

Note

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

5. Click **Apply**.

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

3.1.3 Switch Main/Auxiliary Port

Only the image displaying at the main port can enter main menu and achieve device operation. You can click  in Live View mode, or go to **System** → **Live View** → **General** to switch the main/auxiliary port

If your device has 2 HDMI interfaces and 2 VGA interfaces. HDMI1 and VGA1 are the main ports, and videos output are provided simultaneously. HDMI2 and VGA2 are auxiliary ports, and videos output are provided simultaneously.

3.2 Digital Zoom

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

Steps

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



Figure 3-4 Digital Zoom

3.3 Fisheye View

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

Before You Start

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

Steps

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

Table 3-1 Fisheye View Icon Description

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

3.4 3D Positioning

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

Steps

1. Start live view, and click .

2. Zoom in/out the image.

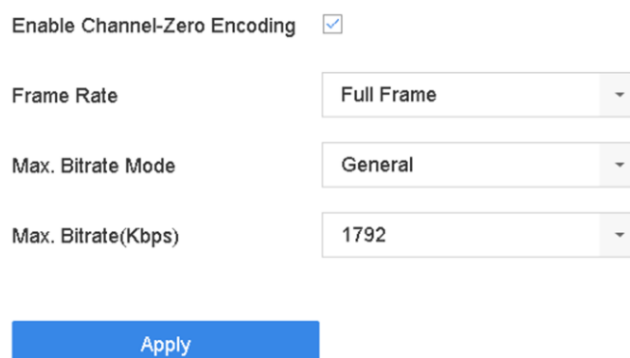
- Zoom in: Click on the desired position in the video image and drag a rectangle area in the lower right direction to zoom in.
- Zoom out: Drag a rectangle area in the upper left direction to move the position to the center and enable the rectangle area to zoom out.

3.5 Configure Channel-Zero Encoding

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

Steps

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



Enable Channel-Zero Encoding ☒

Frame Rate Full Frame

Max. Bitrate Mode General

Max. Bitrate(Kbps) 1792

Apply

Figure 3-5 Channel-Zero Encoding

3. Configure **Frame Rate**, **Max. Bitrate Mode**, and **Max. Bitrate**.

Note

The higher frame rate and bitrate require the higher bandwidth.

4. Click **Apply**.

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

3.6 Configure Transcoded Live View

When your network bandwidth is overloaded, and stuttering occurs in the remote live view main-stream image, the transcoded live view function may help to lower the live view network

Network Video Recorder User Manual

bandwidth requirement and improve image fluency.

Steps



Note

This function is only available for certain models.

1. Go to **Smart Analysis** → **Smart Encoding** → **Virtual Stream** → **Transcoded Live View**.

Figure 3-6 Transcoded Live View

2. Select a channel.
3. Turn on **Enable Live View Compression**.
4. Click **Basic Settings** to set the basic parameters, including resolution, bitrate, frame rate, etc.



Note

The transcoded stream resolution should not be higher than the original stream resolution.

5. Optional: Click **Advanced Settings** to draw ROI (Region of Interest) areas.

ROI

ROI is an encoding technology which helps to discriminate the interested region and the background information in video compression. The interested region would be assigned with more encoding resource to lossless compression while the background information will be showed in lossy compression.

6. Click **Apply**.

What to do next

Use sub-stream or transcoded stream to remotely view the live image.

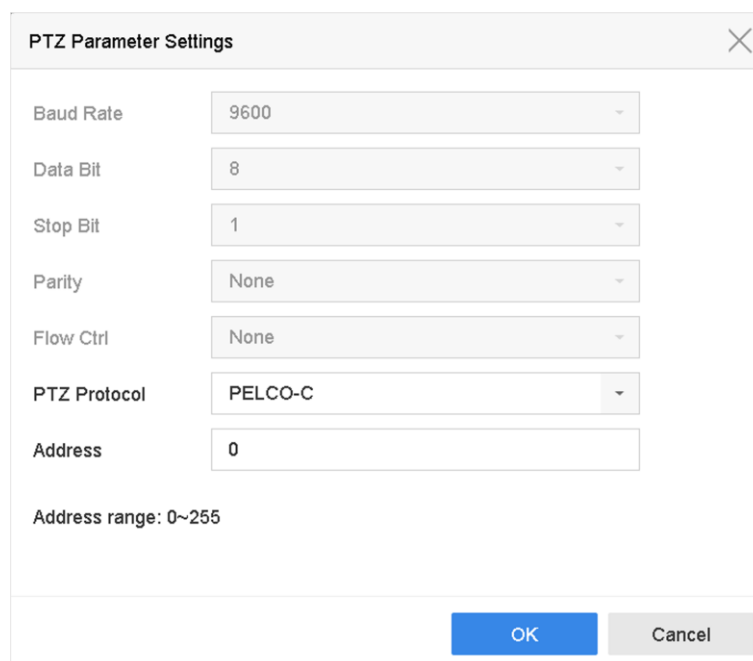
3.7 PTZ Control

3.7.1 Configure PTZ Parameters

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

Steps

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



The image shows a 'PTZ Parameter Settings' dialog box with a close button (X) in the top right corner. It contains several configuration fields: 'Baud Rate' (9600), 'Data Bit' (8), 'Stop Bit' (1), 'Parity' (None), 'Flow Ctrl' (None), 'PTZ Protocol' (PELCO-C), and 'Address' (0). Below the 'Address' field, it states 'Address range: 0~255'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

Address range: 0~255

OK Cancel

Figure 3-7 PTZ Parameters Settings

3. Edit the PTZ parameters.

Note

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

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

3.7.2 Set a Preset

Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.

Steps

1. Click  on the quick settings toolbar of the PTZ camera's live view.

2. Click directional buttons to wheel the camera to a location.
3. Adjust the zoom, focus and iris status.
4. Click  in the lower right corner of Live View to set the preset.

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

Figure 3-8 Set Preset

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



Figure 3-9 View the Configured Presets

3.7.3 Call a Preset

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

Steps

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

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

Figure 3-10 Call Preset (1)

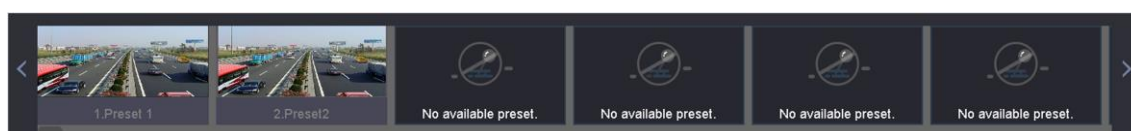


Figure 3-11 Call Preset (2)

3.7.4 Set a Patrol

Patrols can be set to move the PTZ to key points and have it stay there for a set duration before

moving on to the next key point. The key points are correspond to the presets.

Steps

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

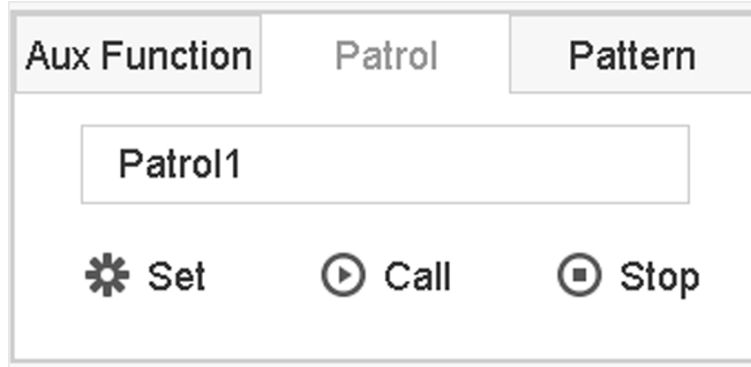


Figure 3-12 Patrol Configuration

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

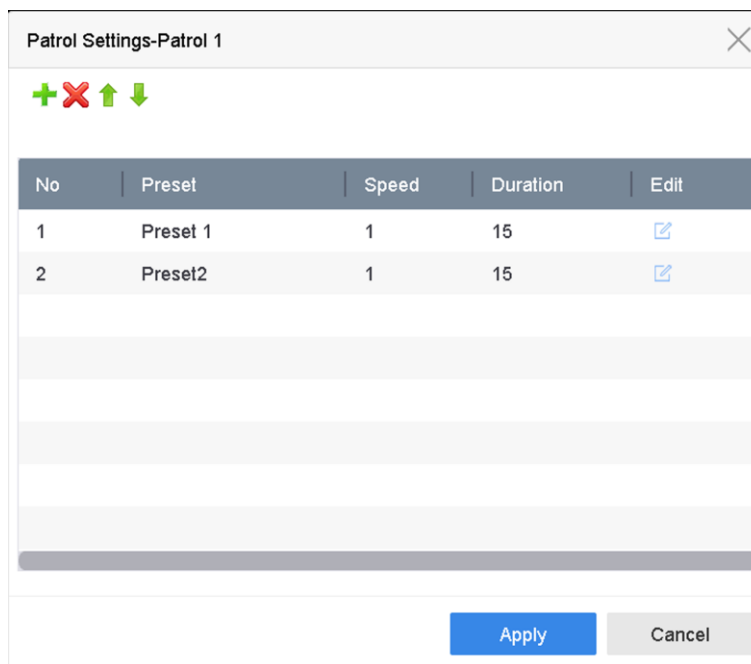


Figure 3-13 Patrol Settings

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

KeyPoint	
Preset	Preset 1 ▾
Speed	1 ▾
Duration	15 ▾

Apply
Cancel

Figure 3-14 Key Point Configuration

1) Configure key point parameters.

Preset

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

Speed

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

Duration

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

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

6. Other operation is as follows.

Table 3-2 Operation Description

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

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

3.7.5 Call a Patrol

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

Steps

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

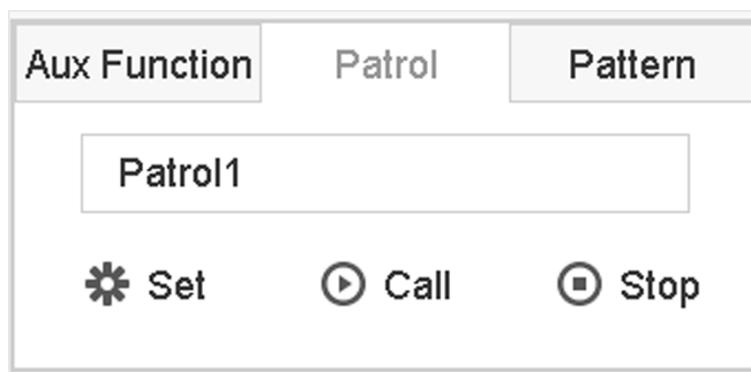


Figure 3-15 Patrol Configuration

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

3.7.6 Set a Pattern

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

Steps

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

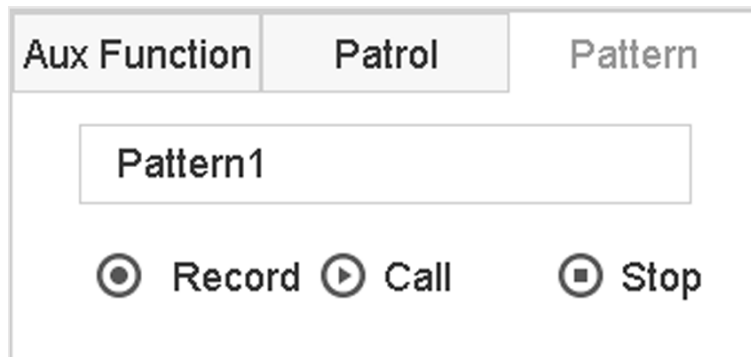


Figure 3-16 Pattern Configuration

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

3.7.7 Call a Pattern

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

Steps

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

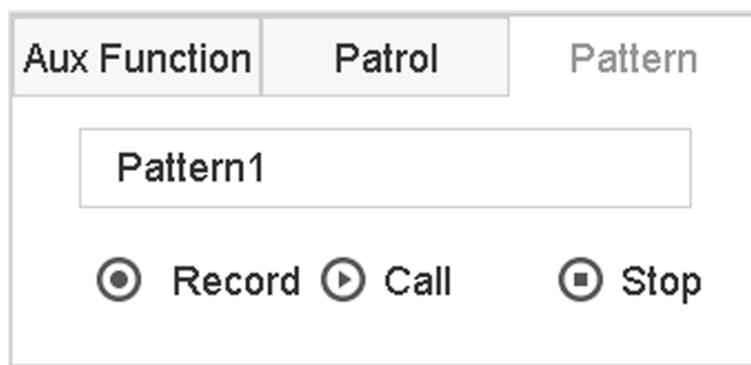


Figure 3-17 Pattern Configuration

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

3.7.8 Set Linear Scan Limit

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

Before You Start

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

Note

This function is supported only by certain models.

Steps

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

Note

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

3.7.9 One-Touch Park

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

Before You Start

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

Steps

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

Park (Quick Patrol)

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

Park (Patrol 1)

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

Park (Preset 1)

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

Note

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

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

Chapter 4 Recording and Playback

4.1 Recording

4.1.1 Configure Recording Parameters

Configure Video Parameters

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

Main Stream

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

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

Frame Rate (FPS - Frames per Second)

It refers to 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.

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.

Enable H.265+

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

Note

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

Sub-Stream

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

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

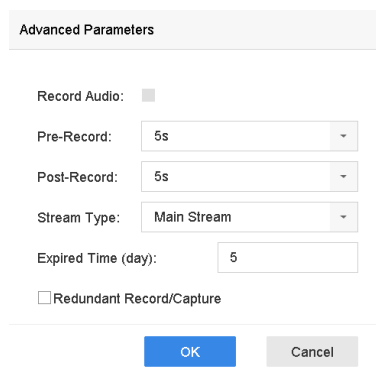
Video Quality

Set the video quality as you desire. The higher video quality results in more storage space requirement.

Configure Advanced Parameters

Steps

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



The screenshot shows a dialog box titled "Advanced Parameters". It contains the following settings:

- Record Audio:** A checkbox that is currently unchecked.
- Pre-Record:** A dropdown menu set to "5s".
- Post-Record:** A dropdown menu set to "5s".
- Stream Type:** A dropdown menu set to "Main Stream".
- Expired Time (day):** A text input field containing the number "5".
- Redundant Record/Capture:** An unchecked checkbox.

At the bottom of the dialog are two buttons: "OK" (in blue) and "Cancel" (in grey).

Figure 4-1 Advanced Record Settings

Record Audio

Enable or disable audio recording.

Pre-record

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

Post-record

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

Stream Type

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

Expired Time

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

Redundant Record/Capture

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

4.1.2 Enable H.265 Stream Access

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

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

4.1.3 ANR

ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.

Before You Start

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

Steps

1. Log in your device via web browser.
2. Go to **Configuration** → **Storage** → **Schedule Settings** → **Advanced Parameter**.
3. Check **Enable ANR**.
4. Optional: For certain camera types, set **ANR Cycle**.

ANR Cycle

The camera would follow the time cycle to synchronize videos with the video recorder.

5. Click **OK**.

4.1.4 Manual Recording

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

4.1.5 Configure Recording Schedule

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

schedule.

Before You Start

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

Steps

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

Continuous

Scheduled recording.

Event

Recording triggered by all event triggered alarm.

Motion

Recording triggered by motion detection.

Alarm

Recording triggered by alarm.

M/A

Recording triggered by either motion detection or alarm.

M&A

Recording triggered by motion detection and alarm.

POS

Recording triggered by POS and alarm.

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

Network Video Recorder User Manual

Camera No. [D3] Camera 01

Enable Schedule ☒

Advanced

Continuous Event Motion Alarm M | A M & A None

Edit

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

Copy to Apply

Figure 4-2 Record Schedule

Note

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

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

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

7. Click **Apply**.

4.1.6 Configure Holiday Recording

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

Steps

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

4. Check **Enable**.

The screenshot shows a web-based configuration interface for editing holiday settings. It features a title bar labeled 'Edit'. Below it, there is a section with the following fields:

- Enable:** A checkbox that is currently checked.
- Holiday Name:** A text input field containing the value 'Holiday1'.
- Mode:** A dropdown menu currently showing 'By Month'.
- Start Date:** A date picker showing 'Jan' for the month and '1' for the day.
- End Date:** A date picker showing 'Feb' for the month and '8' for the day.

At the bottom of the dialog, there are three buttons: 'Apply' (disabled), 'OK' (active), and 'Cancel' (disabled).

Figure 4-3 Edit Holiday Settings

5. Set **Holiday Name**, **Mode**, **Start Date**, and **End Date**.
6. Click **OK**.
7. Set the schedule for holiday recording. Refer to [***Configure Recording Schedule***](#) for details.

4.2 Playback

4.2.1 Instant Playback

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

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



Figure 4-4 Playback

4.2.2 Play Normal Video

Go to **Playback**, select date and camera(s). 1 4 8 9 16 is the window division shortcut for grouping cameras and playing videos. You can also select camera(s) from the list to achieve simultaneous playback of multiple camera(s).

Position the cursor on playback window, and use the toolbar at the bottom to perform playback operations. Refer to **Playback Operations** for details.

Note

256x playing speed is supported.

Network Video Recorder User Manual



Figure 4-5 Play Normal Video

4.2.3 Play Smart Searched Video

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

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

For certain cameras that have enabled human and vehicle of motion detection, you can click  or  to search human and vehicle targets. When you are playing back videos that contain human or vehicle targets, the device cannot use the videos (that contain human or vehicle targets) to apply a double analysis of line crossing detection () or intrusion detection () .



Figure 4-6 Payback by Smart Search

4.2.4 Play Custom Searched Files

You can play video by customized search conditions.

Steps

1. Go to **Playback**.
2. Select camera(s) from the list.
3. Click **Custom Search** at the lower-left corner.
4. Select a search method. For example, **Search by Appearance**.
5. Set search conditions
6. Click **Start Search**. The search result list displays 1 channel.
7. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
8. Optional: Click  to play a video.
9. Click  to lock a file. The locked file will not be overwritten.
10. Optional: Export search results to a backup device.
 - 1) Select file(s) in the search result list, or check **Select All** to select all files.
 - 2) Click **Export** to export the selected file(s) to a backup device.

Note

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

4.2.5 Play Tag Files

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

Add Tag Files

Steps

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

Note

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

Play Tag Files

Steps

1. Go to **Playback**.
2. Click **Custom Search** at the lower-left corner.
3. Click **Search by Tag**.
4. Set search conditions, including time and tag keyword.
5. Click **Start Search**. The search result list displays 1 channel.
6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
7. Click  to play a video.
8. Optional: Export search results to a backup device.
 - 1) Select file(s) in the search result list, or check **Select All** to select all files.
 - 2) Click **Export** to export the selected file(s) to a backup device.

Note

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

4.2.6 Play by Sub-periods

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

Steps

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

Note

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

4.2.7 Play External Files

You can play files from external storage devices.

Before You Start

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

Steps

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

4.3 Playback Operations

4.3.1 Edit Video Clips

You can cut and export video clips during playback.

Steps

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

4.3.2 Configure Transcoded Playback

When your network bandwidth is overloaded, and stuttering occurs in the remote playback main-stream image, the transcoded playback function may help to lower the live view network bandwidth requirement and improve image fluency.

Steps



This function is only available for certain models.

1. Go to **Smart Analysis** → **Smart Encoding** → **Virtual Stream** → **Transcoded Playback**.

Network Video Recorder User Manual

The screenshot shows the 'Basic Settings' tab for transcoded playback. At the top, there is a 'Channel' dropdown menu set to '[D1] IPCamera 01' and an 'Enable Playba...' checkbox. Below this, the 'Basic Settings' tab is selected, showing various configuration options:

Resolution	1280*720 (HD720P)	
Bitrate Type	Constant	
Image Quality	Medium	
Frame Rate	15	fps
Max. Bitrate M...	General	
Max. Bit Rate	1024	kbps
Video Encoding	H.265 Pro	

Figure 4-7 Transcoded Playback

2. Select a channel.
3. Turn on **Enable Playback Compression**.
4. Click **Basic Settings** to set the basic parameters, including resolution, bitrate, frame rate, etc.

Note

The transcoded stream resolution should not be higher than the original stream resolution.

5. Optional: Click **Advanced Settings** to draw ROI (Region of Interest) areas.

ROI

ROI is an encoding technology which helps to discriminate the interested region and the background information in video compression. The interested region would be assigned with more encoding resource to lossless compression while the background information will be showed in lossy compression.

6. Click **Apply**.

What to do next

Use sub-stream or transcoded stream to remotely view the playback image.

4.3.3 Thumbnails View

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

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

Figure 4-8 Thumbnails View

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

Chapter 5 Picture Capture



Note

This chapter is only available for certain models.

5.1 Configure Parameters

The picture refers to the live picture captured in continuous or event recording. You can edit picture parameters in **Storage** → **Schedule** → **Capture** → **Advanced**.

Resolution

Set the picture resolution.

Picture Quality

Set picture quality to low, medium or high. Higher quality requires more storage space.

Interval

The live picture capture interval.

Capture Delay Time

The duration of capturing pictures.

5.2 Configure Capture Schedule

The device will automatically capture picture according to the schedule.

Before You Start

Ensure you have installed HDDs, or added network disks for storage.

Steps

1. Go to **Storage** → **Schedule** → **Capture**.
2. Select a camera.
3. Set the picture capture schedule. Refer to [Configure Recording Schedule](#) for schedule setting details.

5.3 Configure Holiday Capture Schedule

You can set the capture schedule on holidays of the year. The recorder will follow holiday capture

Network Video Recorder User Manual

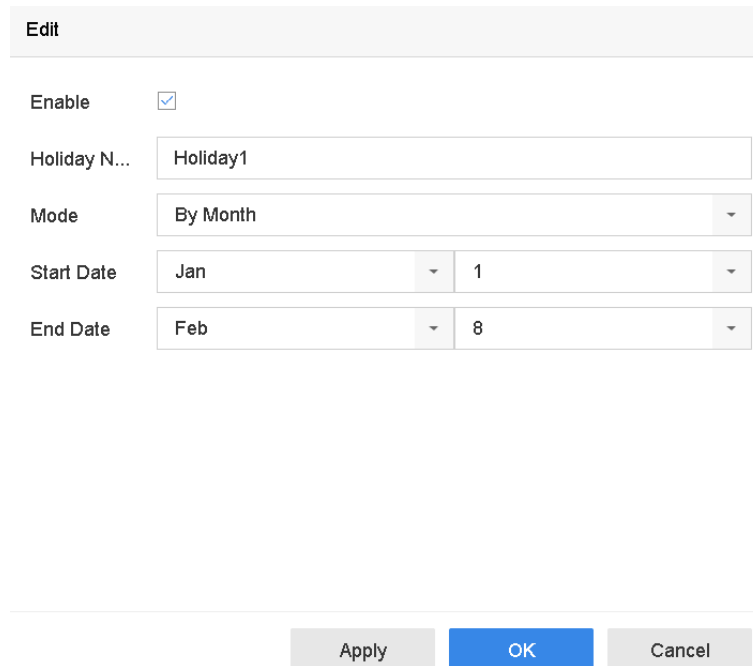
plan as its capture priority during holidays.

Before You Start

Ensure you have installed HDDs, or added network disks for storage.

Steps

1. Go to **System** → **Holiday**.
2. Select a holiday item from the list and click .
3. Check **Enable**.
4. Edit holiday parameters, including name, mode, and date.



Edit	
Enable	☒
Holiday N...	Holiday1
Mode	By Month
Start Date	Jan 1
End Date	Feb 8
Apply OK Cancel	

Figure 5-1 Edit Holiday Settings

5. Click **OK**.
6. Set the holiday capture schedule. Refer to [***Configure Recording Schedule***](#) for schedule setting details.

Chapter 6 Event

6.1 Normal Event Alarm

6.1.1 Configure Motion Detection Alarms

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

Steps

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

For cameras have human and vehicle detection function.

Click **Draw Area** to draw the detection area(s) on the preview screen. Set **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.

For cameras do not have human and vehicle detection function.

Click **Full screen** to set the full-screen as the detection area, or drag on the preview screen to draw the customized detection area.

5. Set **Sensitivity**

Sensitivity

Sensitivity ranges from 0 to 100. It allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.

6. Set the arming schedule. Refer to [Configure Arming Schedule](#).
7. Set linkage actions. Refer to [Configure Linkage Actions](#).

6.1.2 Configure Video Loss Alarms

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

Steps

1. Go to **System** → **Event** → **Normal Event** → **Video Loss**.
2. Select a camera.
3. Check **Enable**.
4. Set the arming schedule. Refer to [Configure Arming Schedule](#).

5. Set linkage actions. Refer to [**Configure Linkage Actions**](#).

6.1.3 Configure Video Tampering Alarms

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

Steps

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

6.1.4 Configure Sensor Alarms

Set the handling action of an external sensor alarm.

Steps

1. Go to **System** → **Event** → **Normal Event** → **Alarm Input**.
2. Select an alarm input item from the list and click .
3. Select the alarm input type.
4. Edit the alarm name.
5. Set **Settings** as **Input** to enable the function.



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

6. Set the arming schedule. Refer to [**Configure Arming Schedule**](#).
7. Set linkage actions. Refer to [**Configure Linkage Actions**](#).
8. Optional: Set combined alarm. Refer to [**Configure Combined Alarm**](#).

6.1.5 Configure Exceptions Alarms

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

Steps

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

2. Optional: Enable the event hint to display it in the live view window.

1) Check **Enable Event Hint**.

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

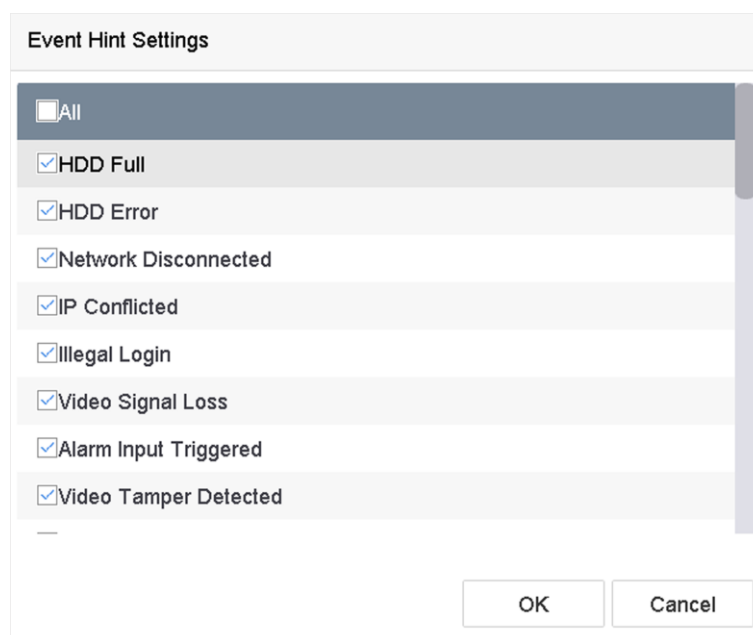


Figure 6-1 Event Hint Settings

3. Select an exception type.

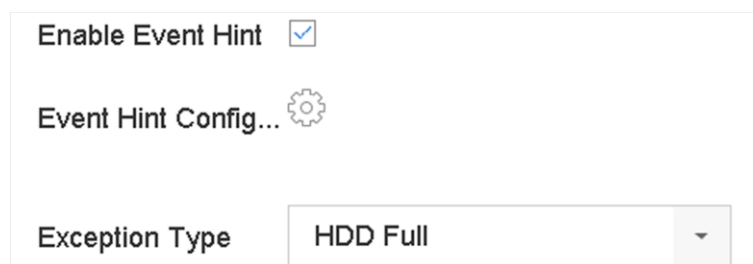


Figure 6-2 Exceptions Handling

4. Set the linkage actions. Refer to [**Configure Linkage Actions**](#).

6.1.6 Flashing Light Alarm Output

After configuring flashing light alarm output, the camera flashing light can be activated when an alarm is triggered.

Before You Start

Ensure a camera with flashing light alarm function is connected.

Steps

1. Go to **System** → **Event** → **Normal Event** → **Flashing Light Alarm Output**.
2. Select a camera.

3. Set **Flashing Duration** and **Flashing Frequency**.

Flashing Duration

The time period the flashing lasts when one alarm happens.

Flashing Frequency

The flashing speed of the light.

4. Set arming schedule.

5. Click **Save**.

6.1.7 Audio Alarm Output

After configuring audio alarm output, the camera speaker can be activated when an event is triggered.

Before You Start

Ensure a camera with audio alarm function is connected.

Steps

1. Go to **System** → **Event** → **Normal Event** → **Audio Alarm Output**.
2. Select a camera.
3. Set **Audio Type**, **Alarm Times** and **Sound Volume**.
4. Set arming schedule.
5. Click **Save**.

6.1.8 Configure Combined Alarm

Combined alarm combines events with alarm input. The combined alarm will be triggered when it receives alarms from both alarm input and events. Event types include motion detection, video tampering detection, and other smart events such as line crossing detection, intrusion detection, etc.

Before You Start

Ensure the channel has been assigned with event alarm as your desire, and the alarm input has been configured (refer to [**Configure Sensor Alarms**](#)).

Steps

1. Go to **System** → **Event** → **Normal Event** → **Alarm Input**.
2. Select an alarm input item from the list and click .
3. Select **Settings** as **Input**.
4. Click **Combined Alarm**.
5. Select a channel as your desire.
6. Select **Combined Alarm Event**.
7. Click **Apply**.

Note

The combined alarm arming schedule and linkage action are the same as the selected event(s).

The screenshot shows the 'Edit' window for a Combined Alarm. At the top, there's a close button (X). Below it, 'Alarm Input No.' is set to 'Local<-1' and 'Type' is 'N.C'. There's an empty 'Alarm Name' field. Under 'Settings', the 'Input' radio button is selected. The 'Combined Alarm' tab is active, displaying a list of events: Video Tampering, Motion, Face (Face Capture), Vehicle, Line Crossing, Intrusion, Region Entrance, and Region Exit. The 'Select Channel' dropdown is set to '[D4] IPCamera 04'. An 'Apply' button is at the bottom right.

Figure 6-3 Combined Alarm

6.2 VCA Event Alarm

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

Note

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

6.2.1 Temperature Screening

After specified thermography cameras are connected, the device can display temperature measurement results, and notify you with audio alert when normal or abnormal temperature is detected.

Before You Start

Ensure your thermography camera supports this function, and it is properly configured.

Steps

1. Go to **System** → **Event** → **Smart Event**.
2. Select the optical channel of thermography camera.
3. Click **Face Capture**.
4. Optional: Check **Save VCA Picture** to save the captured pictures of face detection.
5. Set the arming schedule. Refer to [Configure Arming Schedule](#).
6. Set linkage actions. Refer to [Configure Linkage Actions](#). If you require to implement linkage actions only when the thermography camera detects abnormal temperature, check **Abnormal Body Temperature** in **Rule Settings**.



Note

The abnormal temperature is detected and defined by the thermography camera.

7. Click **Apply**.

What to do next

- You can check  of **Target** in live view to view detection results.
- You can go to **File Management** → **Smart Search** → **Search by Appearance** to search detection results.

6.2.2 Transparent Transmission

Transparent transmission makes a large variety of events configurable, and the event alarms from cameras can be directly transmitted. For events which are not listed in smart event, they will be listed in the transparent transmission list. The list will only display events which the connected cameras support. You can custom the event description as your desire. Transparent transmission is configurable via web browser.

Before You Start

Ensure you have correctly connected camera(s) that supports transparent transmission.

Steps

1. Go to **Configuration** → **Event** → **More Events** → **Transparent Transmission Configuration**. The available events are listed in **Event Description List**.
2. Click **Template List** to export the template list file.

 Note

The template list is for reference only. It cannot be deleted or edited.

3. Edit **Event Description** according to your camera and the template list.

Event Type

The event type shall be the same as your camera event.

Event Description

The event description can be customized. After the event type is recognized, the device will display the event description as the event name.

4. Click **Save**.

What to do next

Go to **Configuration** → **Event** → **Smart Event** → **More Events** to configure events.

6.2.3 Hard Hat Detection

Hard hat detection detects people who are not wearing hard hats. You can configure the arming schedule and linkage actions. Hard hat detection is configurable via web browser.

6.2.4 Face Capture

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

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Facial Recognition**.
2. Click **Face Capture**.

Network Video Recorder User Manual

☐ Enable Face... Sensitivity 1  5 3

Arming Schedule Linkage Action

☒ Continuous ☐ None Edit

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

Apply

Figure 6-4 Face Capture

3. Select a camera to configure.
4. Check **Enable Face Capture**.
5. Optional: Check **Save VCA Picture** to save the captured pictures of face detection.
6. Set the detection sensitivity.

Note

Sensitivity range: [1-5]. The higher the value is, the easier faces will be detected.

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

6.2.5 Line Crossing Detection

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

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection**.
2. Select a camera.
3. Click **Line Crossing**.

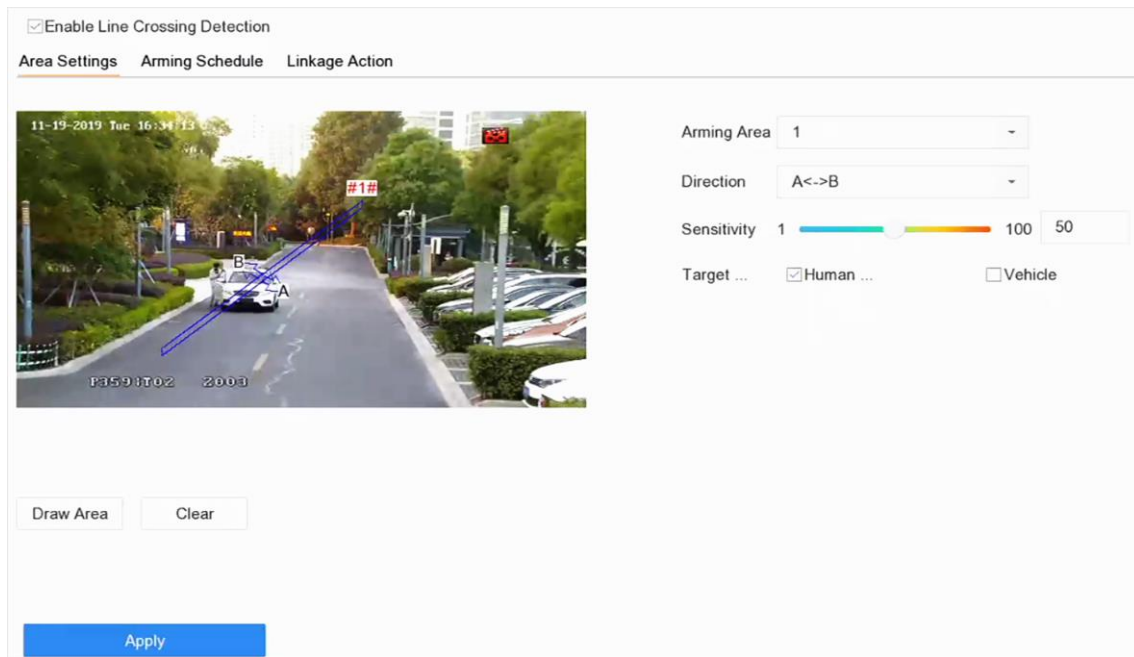


Figure 6-5 Line Crossing Detection

4. Check **Enable Line Crossing Detection**.
5. Optional: Check **Save VCA Picture** to save the captured pictures of line crossing detection.
6. Set the line crossing detection rules and detection areas.
 - 1) Select an arming area.
 - 2) Select **Direction** as **A<->B**, **A->B**, or **A<-B**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both 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.

- 3) Set the detection sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
- 4) Click **Draw Region**.
- 5) Draw a virtual line in the preview window.
7. Optional: Draw the maximum size/minimum size for targets.

Note

Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.

- 1) Click **Max. Size/Min. Size**.

- 2) Draw an area in preview window.
- 3) Click **Stop Drawing**.
8. Optional: Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
9. Set the arming schedule. Refer to [Configure Arming Schedule](#).
10. Set linkage actions. Refer to [Configure Linkage Actions](#).
11. Click **Apply**.

6.2.6 Intrusion Detection

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

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection**.
2. Select a camera.
3. Click **Intrusion**.

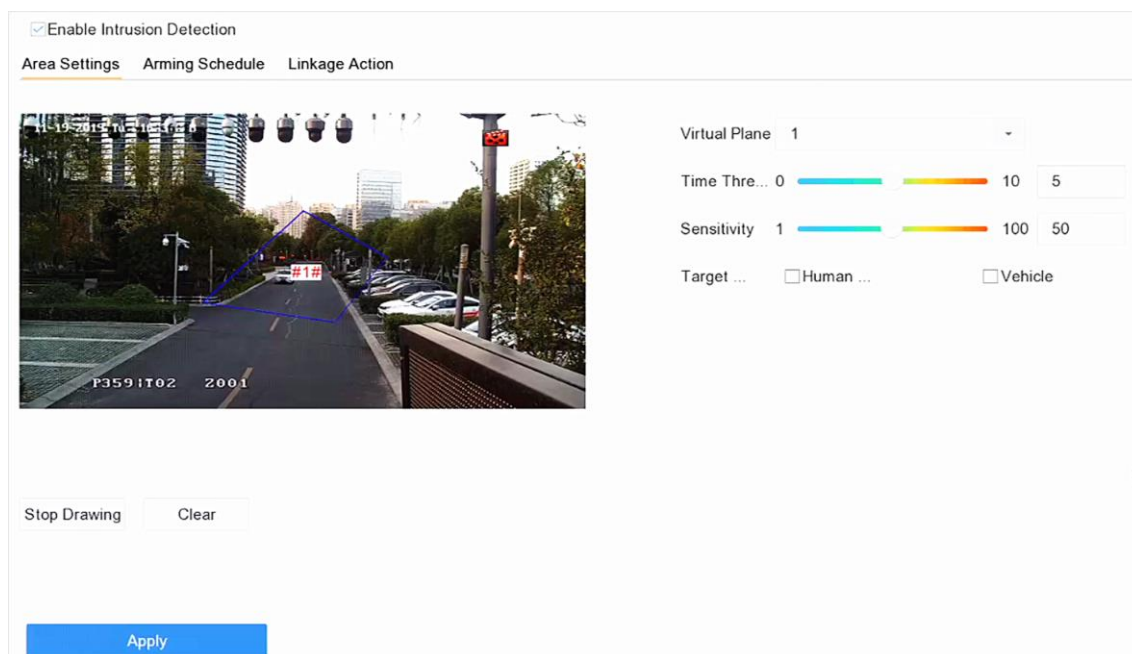


Figure 6-6 Intrusion Detection

4. Check **Enable Intrusion Detection**.
5. Optional: Check **Save VCA Picture** to save the captured intrusion detection pictures.
6. Set the detection rules and detection areas.
 - 1) Select a virtual panel. Up to 4 virtual panels are selectable.
 - 2) Set **Time Threshold**, and **Sensitivity**.

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

Sensitivity is the object size which is able to trigger an alarm. The higher the sensitivity is, the more easily the detection alarm will be triggered.

- 3) Click **Draw Area**.
- 4) Draw a quadrilateral in the preview window.
7. Optional: Draw the maximum size/minimum size for targets.

**Note**

Only the targets in the size ranging from maximum size to minimum size will trigger Intrusion detection.

- 1) Click **Max. Size/Min. Size**.
- 2) Draw an area in preview window.
- 3) Click **Stop Drawing**.
8. Optional: Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
9. Set the arming schedule. Refer to [Configure Arming Schedule](#).
10. Set linkage actions. Refer to [Configure Linkage Actions](#).
11. Click **Apply**.

6.2.7 Region Entrance Detection

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

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection**.
2. Select a camera.
3. Click **Region Entrance Detection**.

Network Video Recorder User Manual

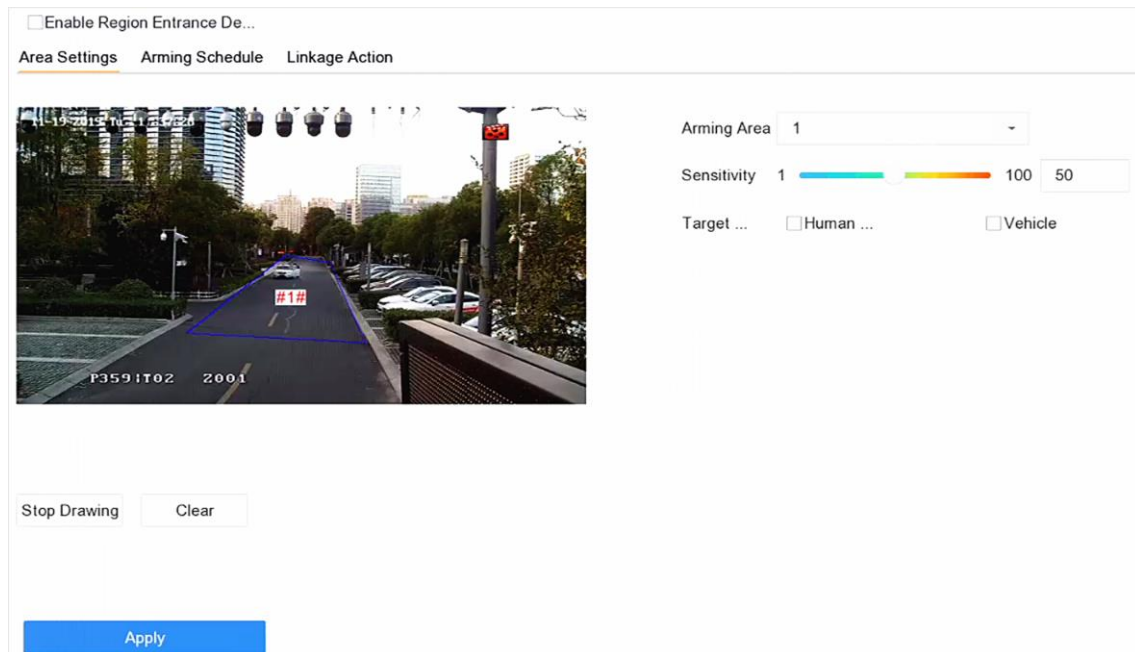


Figure 6-7 Region Entrance Detection

4. Check **Enable Region Entrance Detection**.
5. Optional: Check **Save VCA Picture** to save the captured pictures of region entrance detection pictures.
6. Set detection rules and detection areas.
 - 1) Select **Arming Region**.

Note

Up to 4 regions are selectable.

- 2) Set **Sensitivity**.

Sensitivity

The higher the value is, the easier the detection alarm will be triggered. Its range is [0-100].

- 3) Click **Draw Region**, and draw a quadrilateral in the preview window.
7. Optional: Draw the maximum size/minimum size for targets. Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.
 - 1) Click **Max. Size/Min. Size**.
 - 2) Draw an area in preview window.
 - 3) Click **Stop Drawing**.
8. Optional: Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
9. Set the arming schedule. Refer to [Configure Arming Schedule](#).
10. Set linkage actions. Refer to [Configure Linkage Actions](#).
11. Click **Apply**.

6.2.8 Region Exiting Detection

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

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Perimeter Protection**.
2. Select a camera.
3. Click **Region Exiting**.

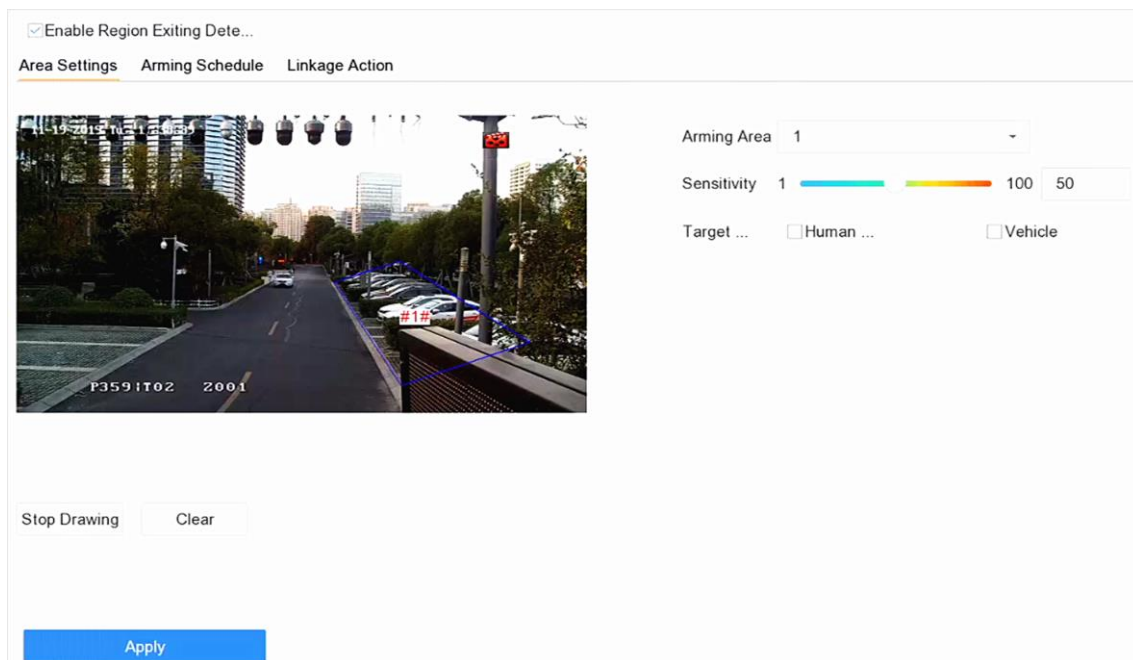


Figure 6-8 Region Exiting Detection

4. Check **Enable Region Exiting Detection**.
5. Optional: Check **Save VCA Picture** to save the captured region exiting detection pictures.
6. Follow these steps to set the detection rules and detection areas.
 - 1) Select **Arming Region**. Up to 4 regions are selectable.
 - 2) Set **Sensitivity**. The higher the value is, the more easily the detection alarm will be triggered. Its range is [0-100].
 - 3) Click **Draw Region** and draw a quadrilateral in the preview window.
7. Optional: Draw the maximum size/minimum size for targets. Only the targets in the size ranging from maximum size to minimum size will trigger line crossing detection.
 - 1) Click **Max. Size/Min. Size**.
 - 2) Draw an area in preview window.
 - 3) Click **Stop Drawing**.
8. Optional: Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human body or vehicle.
9. Set the arming schedule. Refer to [Configure Arming Schedule](#).
10. Set linkage actions. Refer to [Configure Linkage Actions](#).
11. Click **Apply**.

6.2.9 Vehicle Detection

Vehicle detection, available in the road traffic monitoring, is tend to detect the passed vehicle on the road, and capture its license plate at the same time.

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Vehicle Detection**.
2. Select a camera.
3. Click **Vehicle**.
4. Check **Enable Vehicle Detection**.
5. Optional: Check **Save VCA Picture** to save the captured vehicle detection pictures.
6. Configure rules, including **Area Settings**, **Picture**, **Overlay Content**, and **Blocklist and Allowlist**.

Area Settings

Up to 4 lanes are selectable.

Blocklist and Allowlist

You can export the file first to see its format, and edit it and import it to the device.

7. Click **Apply**.



Note

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

8. Set the arming schedule. Refer to [**Configure Arming Schedule**](#).
9. Set the linkage actions. Refer to [**Configure Linkage Actions**](#).

6.2.10 Multi-Target-Type Detection

Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.

Steps

1. Go to **Smart Analysis** → **Smart Event Settings** → **Video Structuralization**.
2. Select a camera.
3. Check **Enable Multi-Target-Type Detection**.
4. Optional: Check **Save VCA Picture** to save the captured intrusion detection pictures.
5. Set detection area.
 - 1) Click **Draw Area**.
 - 2) Adjust the red frame on the image to draw the detection area. It is full screen by default.
 - 3) Click **Stop Drawing**.
6. Set the arming schedule. Refer to [**Configure Arming Schedule**](#).
7. Set linkage actions. Refer to [**Configure Linkage Actions**](#).
8. Click **Apply**.

6.2.11 Object Thrown from Building

This function can identify the event of throwing objects from building and identify the real target.

Before You Start

Ensure your camera supports this function.

Steps

1. Go to **Configuration** → **VCA** → **Object Thrown from Building** via web browser.
2. Select a camera.
3. Check **Enable Object Thrown from Building**.
4. Click **Area Settings** and click  to draw rule area.

Note

1. Click  to start drawing, left click each time on the screen to determine a vertex, right click to stop drawing. The inside of the drawn polygon is the shielded area. If you make a mistake, you can click  and redraw.
2. It is recommended to draw the detection area according to the outline of the building in the screen.

-
5. Enter **Rule Name**. The default name is rule 1.
 6. Set the detection parameters.

Sensitivity

Used to detect and filter object(s) that are definitely not thrown from the building. The higher the value, the greater the possibility of a false alarm. Default value of 50 is recommended.

Detection Confidence

Used to detect suspicious object(s) in the detection area. The lower the value, the easier it is to detect the object in the video and make a judgment. Default value of 50 is recommended.

Target Confidence

Used to determine if the target is a real object thrown from building. The lower the value, the easier it is for a detected object in the video to be determined as an object thrown from building, and the greater the likelihood of a false alarm. Default value of 50 is recommended.

Note

Default value is recommended at first. Adjustment can be made if false alarm is triggered frequently during the operation. Target confidence is recommended to be adjusted initially, and detection confidence is recommended to be adjusted later if no sound detection results provided. If still, there is no obvious effect, then adjust the sensitivity.

7. Click **Save**.
8. Click **Arming Schedule**. Refer to [Configure Arming Schedule](#).

9. Click **Linkage Method**. Refer to **Configure Linkage Actions**.

10. Configure **Shield Region**.

- 1) Click **Shield Region**.
 - 2) Draw the region.
-

Note

1. If there are parts of the screen (either within or outside the detection area) that do not need to be detected (such as an area where the light jumps from time to time or leaves often drift by and trigger false alarms, etc.), you can draw it as a shield region.
 2. Click  to start drawing, left click each time on the screen to determine a vertex, right click to stop drawing. The inside of the drawn polygon is the shielded area. If you make a mistake, you can click  and redraw.
 3. 8 shield regions are supported.
-

11. Click **Save**.

6.2.12 Loitering Detection

Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.

Steps

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

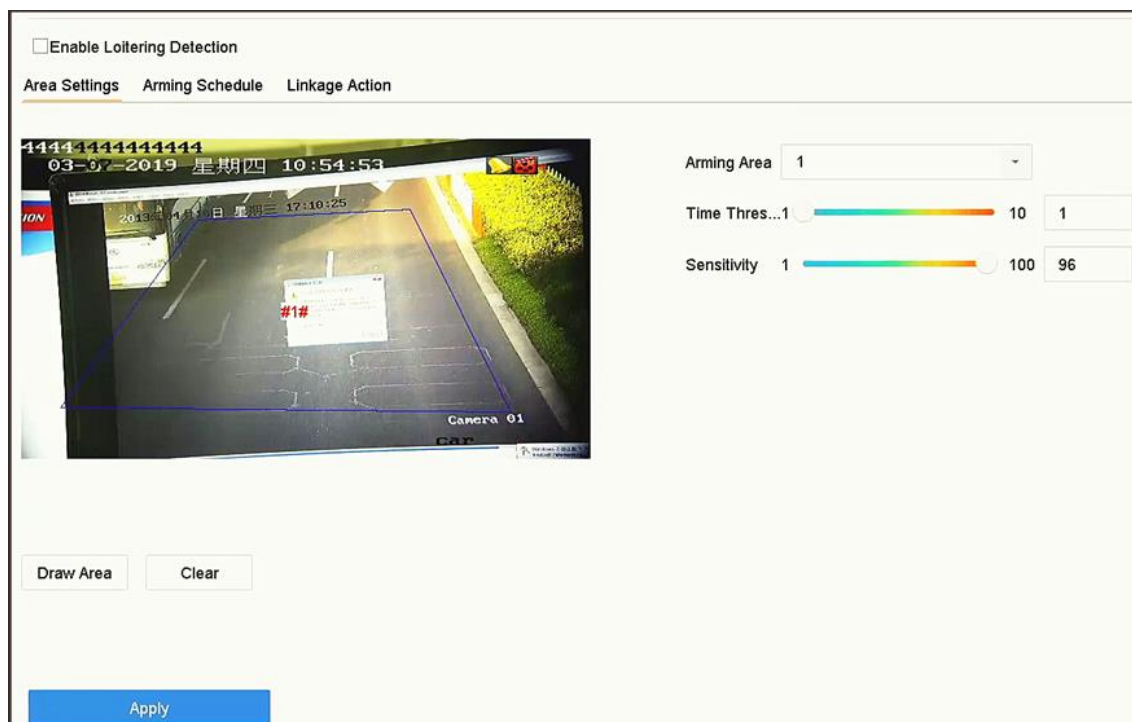


Figure 6-9 Loitering Detection

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

Note

Up to 4 areas are selectable.

- 2) Set **Time Threshold**.

Time Threshold

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

- 3) Set **Sensitivity**.

Sensitivity

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

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

6.2.13 People Gathering Detection

People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.

Steps

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

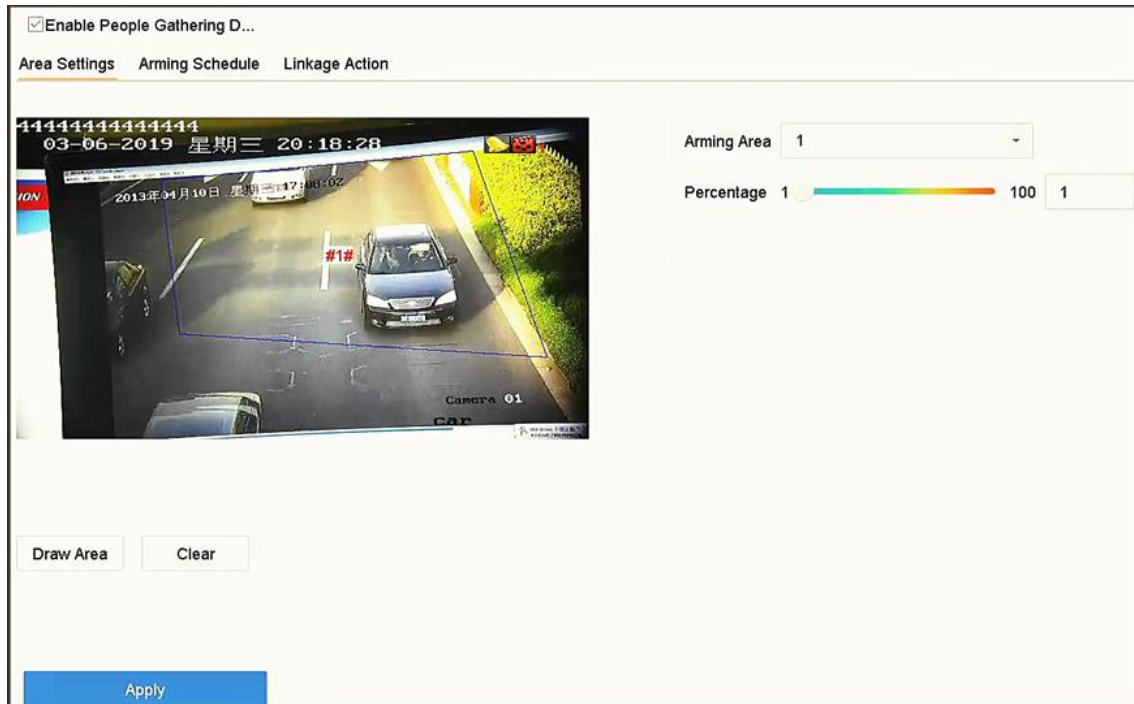


Figure 6-10 People Gathering Detection

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

Note

Up to 4 areas are selectable.

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

Percentage

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

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

6.2.14 Fast Moving Detection

Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.

Steps

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

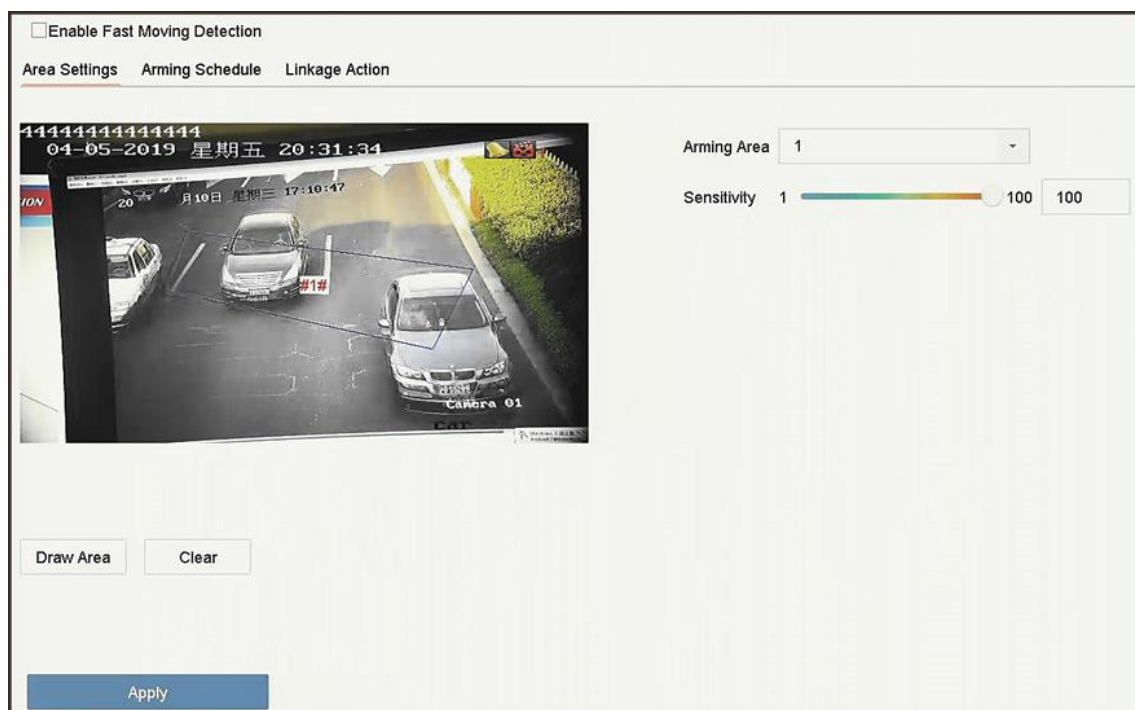


Figure 6-11 Fast Moving Detection

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

Sensitivity

Similarity of the background image to the object. The higher the value is, more easily the

detection alarm will be triggered.

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

6.2.15 Parking Detection

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

Steps

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

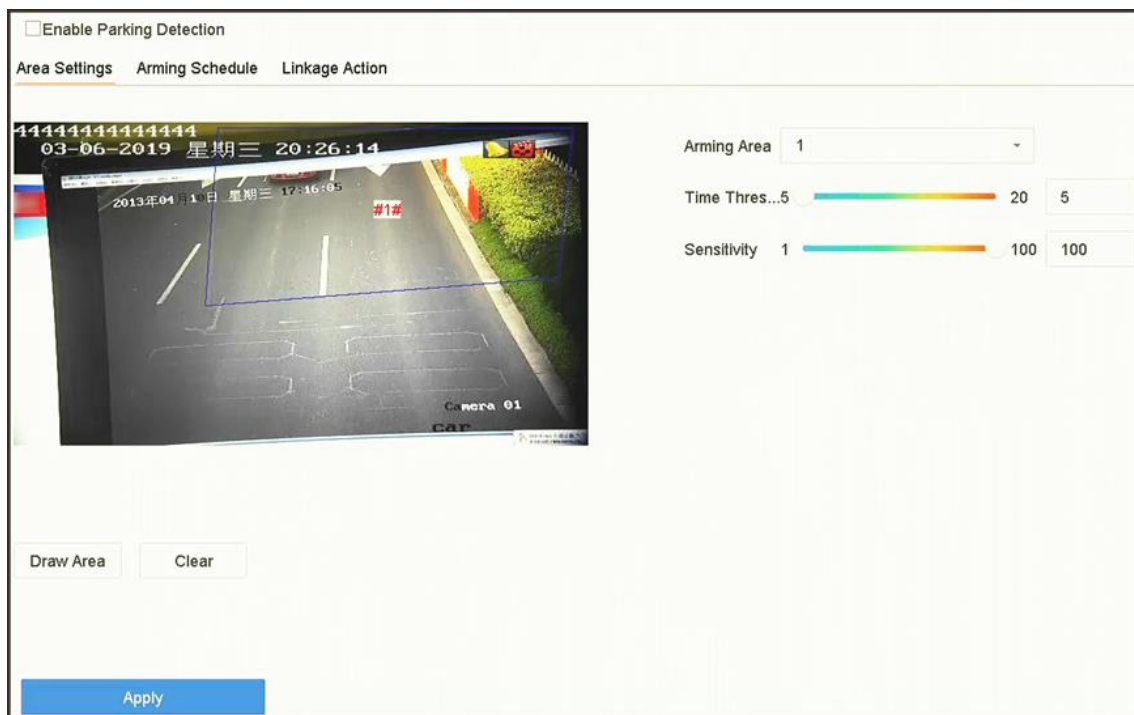


Figure 6-12 Parking Detection

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

Note

Up to 4 areas are selectable.

- 2) Set **Time Threshold**.

Time Threshold

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

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

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

7. Set the arming schedule. Refer to [**Configure Arming Schedule**](#).

8. Set the linkage actions. Refer to [**Configure Linkage Actions**](#).

9. Click **Apply**.

6.2.16 Unattended Baggage Detection

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

Steps

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

☐ Enable Unattended Baggage...

Area Settings Arming Schedule Linkage Action



Arming Area 1

Time Thres...5  3600 5

Sensitivity 1  100 50

Stop Drawing Clear

Apply

Figure 6-13 Unattended Baggage Detection

4. Check **Enable Unattended Baggage Detection**.
5. Optional: Check **Save VCA Picture** to save the captured unattended baggage detection pictures.

6. Set the detection rules and detection areas.

1) Select **Arming Area**.



Up to 4 areas are selectable.

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

Time Threshold

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

Sensitivity

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

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

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

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

9. Click **Apply**.

6.2.17 Object Removal Detection

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

Steps

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

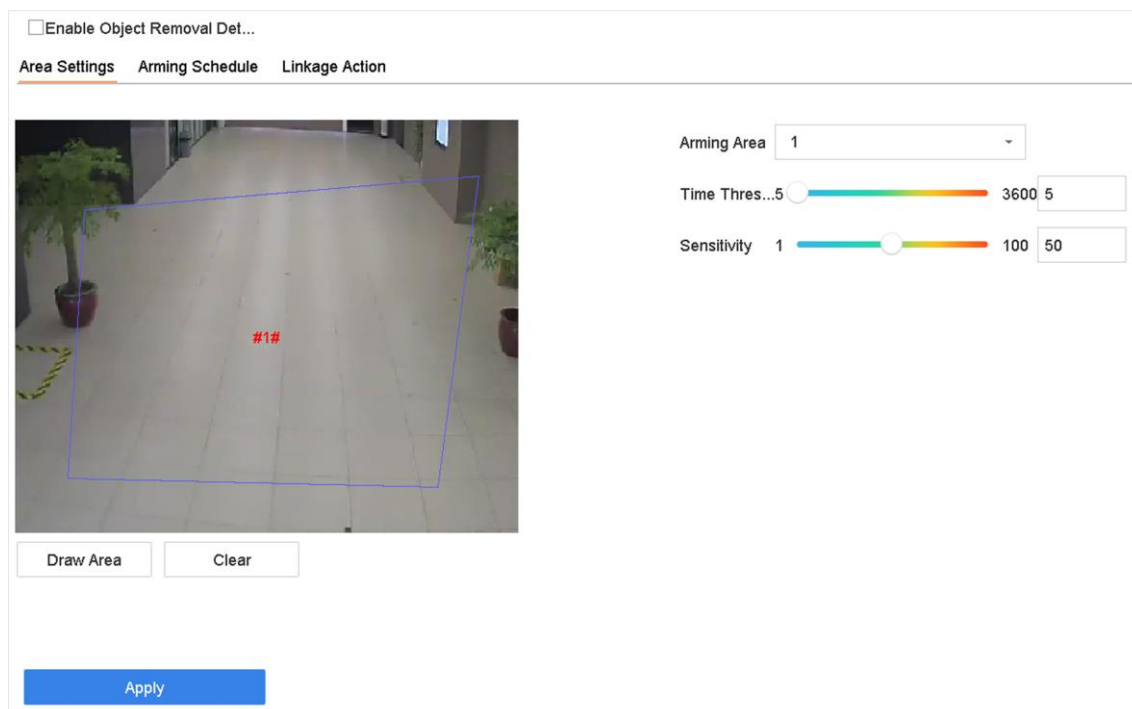


Figure 6-14 Object Removal Detection

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

Note

Up to 4 areas are selectable.

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

Time Threshold

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

Sensitivity

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

- 3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection region.
7. Set the arming schedule. Refer to [Configure Arming Schedule](#).
8. Set the linkage actions. Refer to [Configure Linkage Actions](#).
9. Click **Apply**.

6.2.18 Audio Exception Detection

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

Steps

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

Figure 6-15 Audio Exception Detection

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

Audio Loss Exception

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

Sensitivity

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

Sound Intensity Threshold

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

Sudden Decrease of Sound Intensity Detection

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

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

6.2.19 Defocus Detection

Image blur caused by lens defocus can be detected.

Steps

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

The screenshot shows the 'Defocus Detection' configuration window. At the top, there is an 'Enable' checkbox and a 'Sensitivity' slider set to 100. Below this, there are tabs for 'Arming Schedule' and 'Linkage Action'. Under 'Arming Schedule', there are radio buttons for 'Continuous' (selected) and 'None', and an 'Edit' button. The main area is a grid for the arming schedule, with columns for time slots (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) and rows for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun). Each cell in the grid is currently filled with blue, indicating the detection is armed for all times and days. At the bottom left, there is an 'Apply' button.

Figure 6-16 Defocus Detection

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

Sensitivity

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

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

6.2.20 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.

Steps

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

☐ Enable

Sensitivity 1 100 50

Arming Schedule Linkage Action

☒ Continuous ☐ None Edit

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

Apply

Figure 6-17 Sudden Scene Change

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

Sensitivity

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

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

6.2.21 PIR Alarm

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector vision field.

Network Video Recorder User Manual

The heat energy dissipated by a person or any other warm blooded creature such as dogs, cats, etc., can be detected.

Steps

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

☐ Enable PIR Alarm

Arming Schedule **Linkage Action**

☒ Continuous ☐ None **Edit**

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

Apply

Figure 6-18 PIR Alarm

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

6.2.22 Thermal Camera Detection

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

Before You Start

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

Steps

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

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

6.2.23 Queue Management

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

Before You Start

Ensure the recorder have connected with queue management camera.

Steps

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

6.3 Target Detection

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

Steps

1. In live view mode, click **Target** to enter the target detection interface.
2. Select different detection types: smart detection () , vehicle detection () , facial detection () , and human body detection () .

Note

1. To enable the detection of throwing objects from building, ensure smart detection () has been checked. When the target is identified, the detected view will be displayed on the left. Meanwhile, the box will display the detected object. (If there is a suspicious target, the parabola will turn green. If there is a real target and the alarm is triggered, the parabola will turn red.)
 2. For thermal cameras, the temperature measurement event is in smart detection () , the face capture and facial temperature measurement are in facial detection () .
-

3. Click  to set alarm configuration.

1) Select IP Camera(s) and IoT channel(s), and complete access control event display settings.

Display Pop-Up

Enable this function, the pop-up including person type information, body temperature and mask-wearing status (optional) will be displayed once the alarm is triggered.

Mask Not Wearing Event

Temperature units including Celsius degree and Fahrenheit degree of the detected target are available. Enable this function, when the target does not wear mask, the pop-up will show yellow. Meanwhile, if the target has exceptional body temperature, the pop-up will turn red.

4. Select the historical analysis () or real-time analysis () to obtain the results.

Note

The smart analysis results of the detection are displayed in the list. Click a result in the list to play the related video.

6.4 Configure Arming Schedule

Steps

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

Note

Time periods cannot repeat or overlapped.

Edit	
Weekday	Mon
Start/End Time	00:00-24:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Start/End Time	00:00-00:00
Copy Apply OK Cancel	

Figure 6-19 Set Arming Schedule

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

6.5 Configure Linkage Actions

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

6.5.1 Configure Auto-Switch Full Screen Monitoring

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

Note

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

Steps

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

Event Output

Select the output to show the event video.

Full Screen Monitoring Dwell Time

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

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

6.5.2 Configure Buzzer

When an alarm is detected, the buzzer will make an audible beep.

Steps

1. Go to **System** → **Live View** → **General**.
2. Check **Enable Audio Output**.
3. Set the audio volume.
4. Click **Apply**.
5. Go to **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
6. Select **Buzzer** as the alarm linkage action.

6.5.3 Notify Surveillance Center

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

Steps

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

6.5.4 Configure Email Linkage

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

detected.

Steps

1. Go to **System** → **Network** → **Advanced** → **Email**.
2. Set the email parameters.
3. Click **Apply**.
4. Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).
5. Select **Send Email** alarm linkage action.

6.5.5 Configure Audio Alert

When an alarm is triggered, an audio file will be played as the linkage action. The audio file can be customized. Refer to [Audio Management](#) for details.

Before You Start

Ensure the audio files are imported to the device.

Steps



Note

This linkage action is only available for certain events.

1. Check **Audio Alert** in **Normal Linkage**.
2. Click  to select audio file.
3. Select an audio file.
4. Set arming schedule.
5. Click **OK**.
6. Click **Apply**.

6.5.6 Trigger Alarm Output

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

Steps

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

 Note

If the device has 8 alarm outputs, the Ctrl 12V power is controlled by alarm output 9. Connect positive pole to A of Ctrl 12V, and connect negative pole to B of Ctrl 12V. The power will be turned on when the alarm output is triggered.

6.5.7 Configure Audio and Light Alarm Linkage

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

Before You Start

- Ensure your camera supports audio and light alarm linkage.
- Ensure the audio output and volume are properly configured.

Steps

1. Go to the linkage action interface of the alarm detection (e.g., motion detection).
2. Set **Audio and Light Alarm Linkage** as your desire.
3. Click **Apply**.

6.5.8 Configure PTZ Linkage

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

Before You Start

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

Steps

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

 Note

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

Chapter 7 IoT

IoT (Internet of Things) feature allows you to build connections between your video recorder and IoT devices, including access control and alarm devices. Video recorder will receive alarms from connected IoT devices. You can configure linkage actions like triggering recording and full screen monitoring, when IoT alarm occurs.

7.1 Add an IoT Device



Maximum number of IoT channel is the half of maximum network camera number of your video recorder.

7.1.1 Add an Access Control Device

Add Hikvision alarm host and video intercom devices to receive alarms. You can configure linkage actions like triggering recording and full screen monitoring, when an alarm occurs.

Before You Start

Install access control devices. Ensure network communication between access control devices and video recorder is well.

Steps

1. Go to **Business Application** → **IoT** → **Access Control** → **Device Management**.
2. Click **Add**.

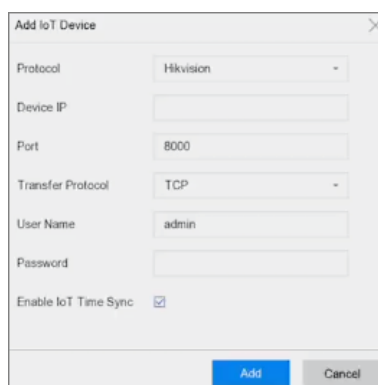


Figure 7-1 Access Control

3. Enter access control device information. **Device IP**, **Port**, **Transfer Protocol**, **User Name**, and **Password** must be the same with access control device.
4. Optional: Check **Enable IoT Time Sync** as your desire.

 Note

All IoT channels can be enabled/disabled with shortcuts.

1. Go to **Maintenance** → **System Service** → **More Settings**.

Click **Time Sync Configuration**, select **Enable IoT Time Sync** or **Disable IoT Time Sync** to enable/disable scheduled time sync for all IoT channels.

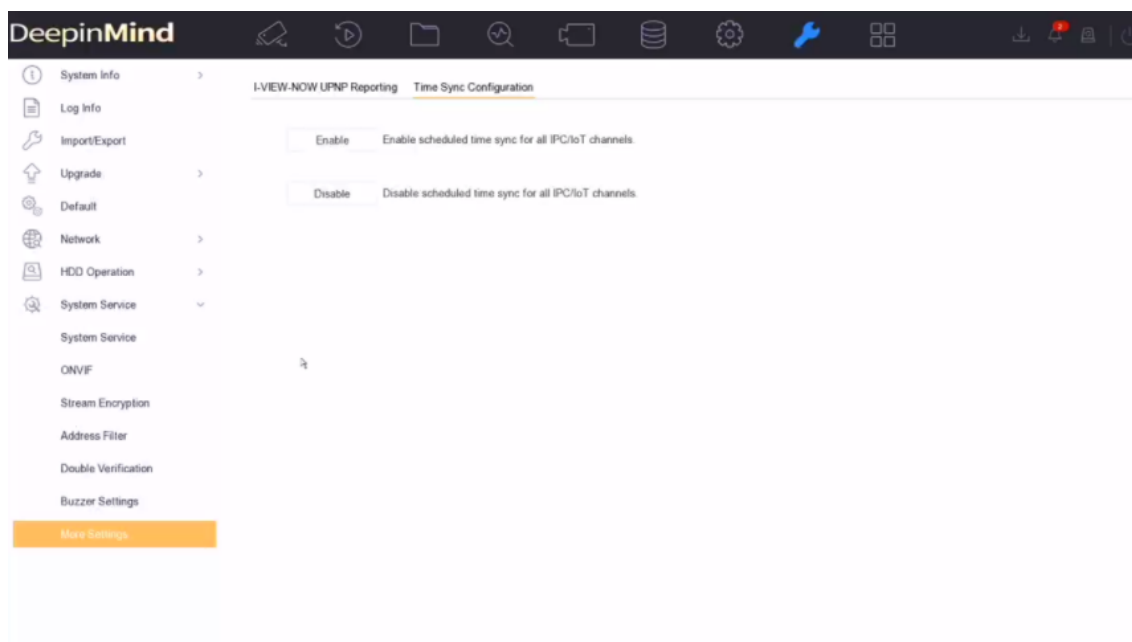


Figure 7-2 IoT Time Sync

This function is only available for the admin user.

5. Click **Add**.

7.1.2 Add an Alarm Device

Add alarm devices of various manufacturers to receive alarms. You can configure linkage actions like triggering recording and full screen monitoring, when an alarm occurs.

Before You Start

Install alarm devices. Ensure network communication between alarm devices and video recorder is well.

Steps

1. Go to **Business Application** → **IoT** → **Alarm** → **Device Management** → **Alarm Host**.
2. Click **Add**.

Figure 7-3 Alarm Device

3. Set alarm host device parameters.
4. Optional: Check **Enable IoT Time Sync** as your desire.
 - 1) Go to **Maintenance** → **System Service** → **More Settings**.
 - 2) Click **Time Sync Configuration**, select **Enable** or **Disable** to enable/disable scheduled time sync for all IoT channels.

Note

All IoT channels can only be enabled/disabled with shortcuts for the admin user.

5. Click **Add**.

7.1.3 Add Network Audio Device

Network audio devices can also be added to your recorder, and the audios can be recorded. If a network camera does not have a pick-up, or the recorded audio is not useful, an audio device can be linked with the camera to replenish the audio effect.

Before You Start

Ensure the network audio device is properly connected.

Steps

1. Go to **Business Application** → **IoT** → **Audio** → **Device Management**.
2. Click **Add**.
3. Set the device parameters, including IP address, password, etc.

Link Network Camera

You can link the audio device to a network camera. After the linkage succeeded, the audio of network camera would be replaced with this audio device.

4. Click **Add**.
5. Optional: Click  to play the real-time audio.
6. Optional: Click  to edit device parameters.
7. Optional: Click **Delete** to delete the device.

Note

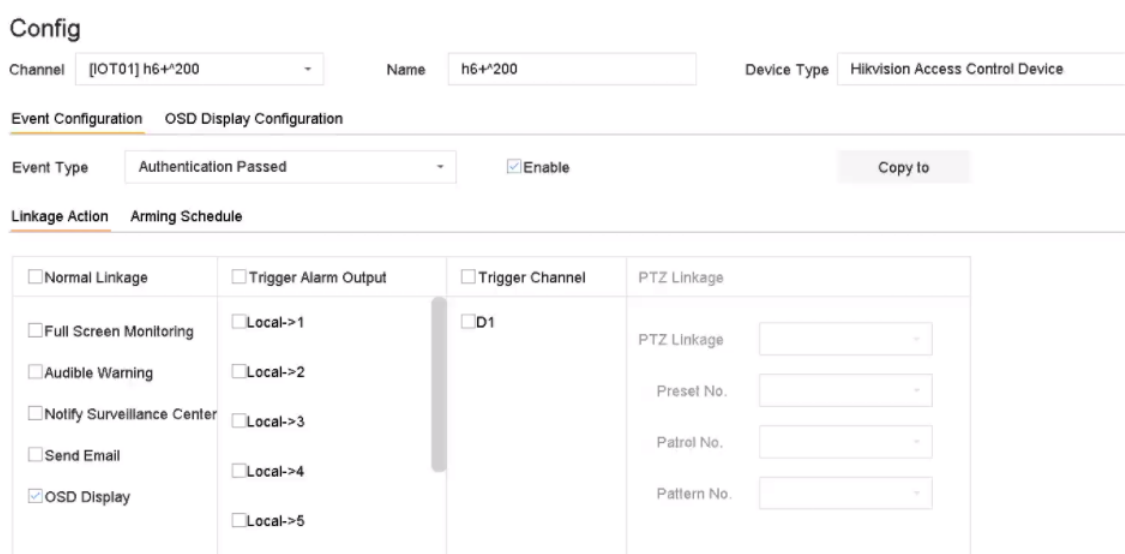
If the network audio device has linked a network camera, after the audio device is deleted, the recorder will store audio of the linked network camera itself.

7.2 Configure the Linkage Action and Arming Schedule

Configure the linkage actions and arming schedule for access control or alarm devices. Linkage actions will be triggered when the designate alarm occurs.

Steps

1. Click  of an added IoT device.



Config

Channel: [IoT01] h6+*200 Name: h6+*200 Device Type: Hikvision Access Control Device

Event Configuration OSD Display Configuration

Event Type: Authentication Passed ☒ Enable Copy to

Linkage Action Arming Schedule

☐ Normal Linkage ☐ Full Screen Monitoring ☐ Audible Warning ☐ Notify Surveillance Center ☐ Send Email ☒ OSD Display	☐ Trigger Alarm Output ☐ Local->1 ☐ Local->2 ☐ Local->3 ☐ Local->4 ☐ Local->5	☐ Trigger Channel ☐ D1	PTZ Linkage PTZ Linkage: Preset No.: Patrol No.: Pattern No.:
---	--	---	--

Figure 7-4 Configure IoT

2. Select **Event Type**. The following configuration is only valid for the selected event type.
3. Check **Enable**.
4. Check linkage actions as your desire. For detailed steps, refer to [Configure Linkage Actions](#).

Note

Full Screen Monitoring and **OSD Display** are only valid for the selected **Trigger Channel**.

5. Click **Arming Schedule**.
6. Configure arming schedule. For detailed steps, refer to [Configure Arming Schedule](#). Linkage action is only valid during the set schedule.
7. Click **Apply**.

7.3 Configure OSD

You can display alarm information received from IoT devices on live view image.

Steps

1. Click  of an added IoT device.
2. Check **OSD Display** on Event Configuration interface.
3. Select **Trigger Channel**.
4. Click **OSD Display Configuration**.

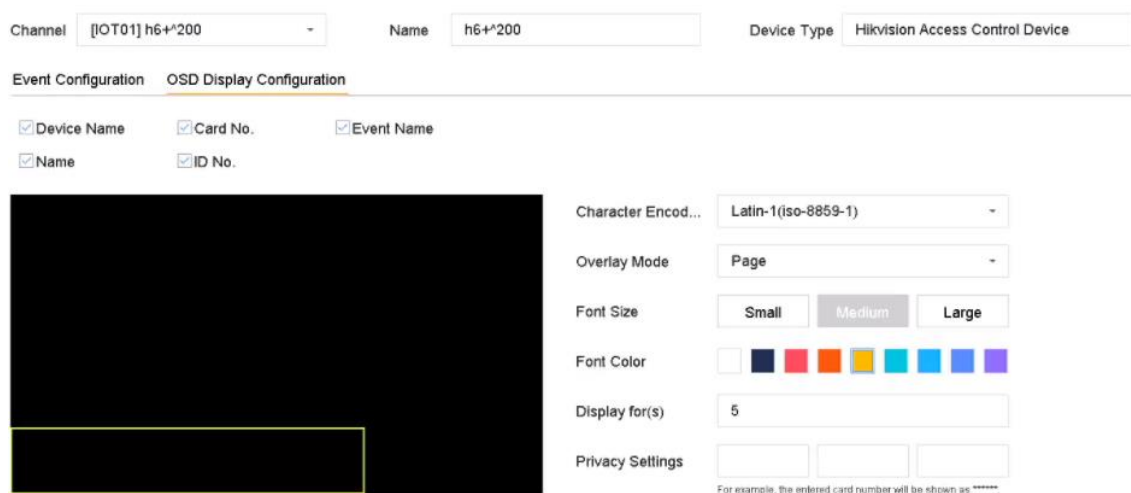


Figure 7-5 OSD Configuration

5. Select items, including **Device Name**, **Card No.**, **Event Name**, **Name**, and **ID No.**, to display on live view image. The items are only for access control devices.
6. Configure OSD properties.

Overlay Mode - Scroll

The OSD will automatically scroll to show the new alarm information.

Overlay Mode - Page

When the current OSD cannot show more alarm information, it will automatically turn to new page.

Privacy Settings

Enter privacy information you want to mask. Masked privacy information will be replaced by *. Privacy information includes **Event**, **Device**, **Card**, **Name**, and **ID**.

7. Adjust the quadrilateral of yellow frame on the preview window to adjust IoT OSD size and position.
8. Click **Apply**.

7.4 Configure Audio Parameters

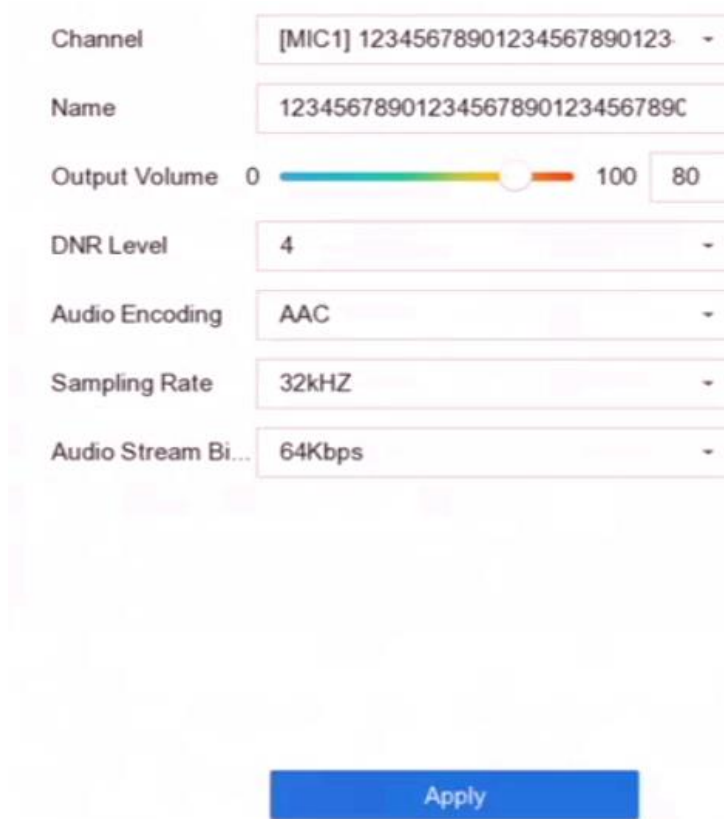
After an network audio device is added, you can configure its parameters, including output volume, sampling rate, DNR (digital noise reduction) level, etc.

Before You Start

Ensure you an audio device is added to your recorder, and the network connection is valid.

Steps

1. Go to **Business Application** → **IoT** → **Audio** → **Audio Parameters**.



Channel	[MIC1] 12345678901234567890123
Name	12345678901234567890123456789C
Output Volume	0 <input type="range"/> 100 80
DNR Level	4
Audio Encoding	AAC
Sampling Rate	32kHz
Audio Stream Bi...	64Kbps

Apply

Figure 7-6 Configure Audio Parameters

2. Set the parameters as your desire.
3. Click **Apply**.

7.5 Search the IoT Record

Search alarms by time, by event type, or by channel.

Steps

1. Go to event record interface.
 - Access control: Go to **Business Application** → **IoT** → **Access Control** → **Card Swiping Record**.

Network Video Recorder User Manual

- Alarm device: Go to **Business Application** → **IoT** → **Alarm** → **Search Data**.

Time: Custom | 2019-05-18 00:00:00 | 2019-05-18 23:59:59

Channel: [All] IOT Channel

Event Type: All | Event Subtype: All

Name: | Card No.:

Search

Figure 7-7 Search Event Record (Access Control)

Time: Custom | 2019-05-19 00:00:00 | 2019-05-19 23:59:59

Channel: [All] IOT Channel

Main Type: GJD Alarm Event | Sub Type: All

Search

Figure 7-8 Search Event Record (Alarm Device)

2. Specify search conditions.

 Note

Name/Card No.: When card swiping event occurs, the access control device will upload card name and card No. to video record. You can search event by card name or card No.

3. Click **Search**.

Network Video Recorder User Manual

No.	Event Type	Name	Card No.	Card Type	Time	Event Source	View
1	Time Sync. Event				05-18-2019 14:04:39	IOT01	—
2	Time Sync. Event				05-18-2019 14:05:39	IOT01	—
3	Time Sync. Event				05-18-2019 14:06:39	IOT01	—
4	Time Sync. Event				05-18-2019 14:07:39	IOT01	—
5	Time Sync. Event				05-18-2019 14:08:39	IOT01	—
6	Time Sync. Event				05-18-2019 14:09:35	IOT01	—
7	Time Sync. Event				05-18-2019 14:09:40	IOT01	—
8	Time Sync. Event				05-18-2019 14:10:39	IOT01	—
9	Time Sync. Event				05-18-2019 14:11:40	IOT01	—
10	Time Sync. Event				05-18-2019 14:12:40	IOT01	—
11	Time Sync. Event				05-18-2019 14:13:39	IOT01	—
12	Time Sync. Event				05-18-2019 14:14:40	IOT01	—
13	Time Sync. Event				05-18-2019 14:14:41	IOT01	—
14	Time Sync. Event				05-18-2019 14:15:40	IOT01	—
15	Time Sync. Event				05-18-2019 14:16:40	IOT01	—
16	Time Sync. Event				05-18-2019 14:17:40	IOT01	—
17	Time Sync. Event				05-18-2019 14:18:40	IOT01	—
18	Time Sync. Event				05-18-2019 14:19:40	IOT01	—
19	Time Sync. Event				05-18-2019 14:19:46	IOT01	—
20	Time Sync. Event				05-18-2019 14:20:40	IOT01	—

Total: 22 P: 1/1

Figure 7-9 Search Result (Access Control)

No.	Channel	Time	Main Type	Sub Type	Status	Data	View
1	IOT03	05-18-2019 14:49:56	GJD Alarm Event	PIR Detection alarm			—

Figure 7-10 Search Result (Alarm Device)

7.6 IoT Video/Picture

Configure the event recording or capturing schedule for the selected trigger channel, the channel will automatically record videos or capture pictures when IoT alarm occurs.

7.6.1 Configure the Event Recording/Capturing

The video recorder can record videos or capture pictures when an IoT alarm occurs.

Steps

1. Click  of an added IoT device.
2. Select desired **Event Type**.
3. Check **Enable**.
4. Check **Trigger Channel** you want to record event videos or capture pictures when an alarm occurs.

Network Video Recorder User Manual

Config

Channel: [IOT03] IOT03 Name: IOT03 Device Type: GJD Alarm Device

Event Configuration OSD Display Configuration

Event Type: PIR Detection alarm ☒ Enable Copy to

Linkage Action Arming Schedule

☐ Normal Linkage ☐ Full Screen Monitoring ☐ Audible Warning ☐ Notify Surveillance Center ☐ Send Email ☒ OSD Display	☐ Trigger Alarm Output ☐ Local->1 ☐ Local->2 ☐ Local->3 ☐ Local->4 ☐ Local->5	☐ Trigger Channel ☐ D1	PTZ Linkage PTZ Linkage: [D1] Camera 01 Preset No.: 1 Patrol No.: 1 Pattern No.: 1
---	--	---	---

Figure 7-11 Trigger Channel

5. Click **Apply**.
6. Configure the event recording or capturing schedule. Here we take the example of configuring event recording to describe the steps.
 - 1) Go to **Storage** → **Schedule** → **Record**.
 - 2) Select **Camera No.** and check **Enable Schedule**. The camera should be the camera you select in step 4.
 - 3) Select the recording type as **Event**.
 - 4) Drag the mouse on the time bar to set the event detection recording schedule. Refer to **Configure Recording Schedule** for details.
 - 5) Click **OK**.

Network Video Recorder User Manual

Camera No. [D1] Camera 01

Enable Schedule ☒

Advanced

Continuous Event Motion Alarm M | A M & A None

Edit

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

Apply Copy to

Figure 7-12 Event Recording

Result

When an alarm occurs, the selected trigger channel will start event recording.

7.6.2 Search IoT Video

Search IoT event triggered videos.

Steps

1. Go to **File Management** → **Video** → **Search by Event**.

Network Video Recorder User Manual

Time: Today, 2020-11-25 00:00:00, 2020-11-25 23:59:59

Camera: [All] Camera

Event Type: All

- PIR Alarm
- Fire Source Detection
- Temperature Detection
- Temperature Difference Detection
- Regional People Queuing-Up
- Waiting Time Detection
- Human Body Detection
- POS Event
- Stranger Detection Alarm
- Successful Face Picture Comparison
- Failed Face Picture Comparison
- Multi-Target-Type Detection
- Temperature Measurement Pre-Alarm
- Access Control Event**
- Video Intercom Event
- GJD Alarm Event
- Luminite Alarm Event

Start Search

Figure 7-13 Search Event Video

2. Set search conditions.

Camera

Select it as the selected trigger channels in IoT linkage action configuration.

Event Type

Select the desired IoT event.

3. Click **Start Search**.

Chapter 8 Smart Report

8.1 People Counting

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

Steps

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

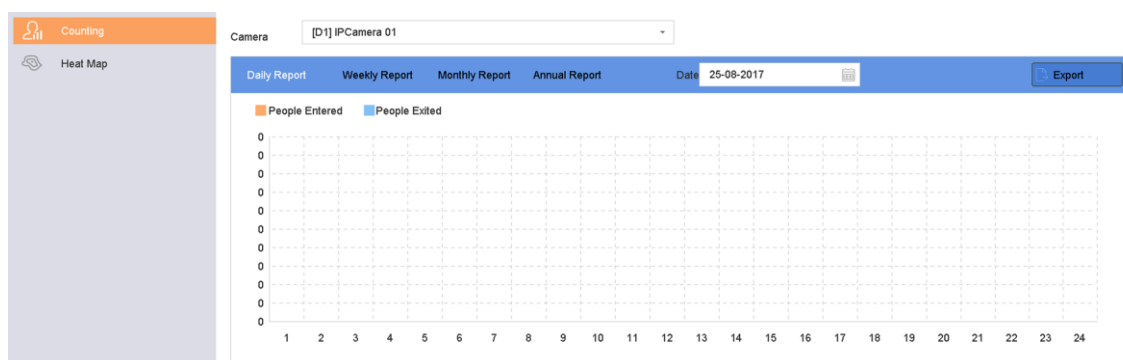


Figure 8-1 People Counting

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

8.2 Heat Map

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

Before You Start

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

Steps

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

Network Video Recorder User Manual

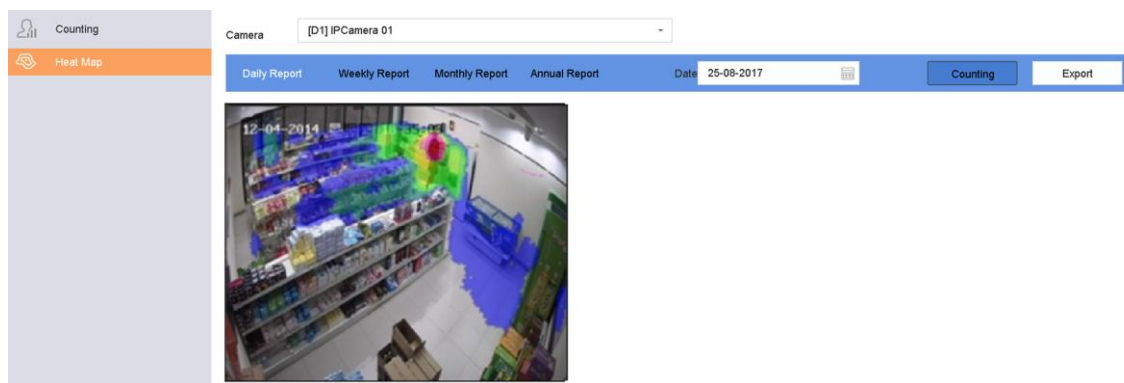


Figure 8-2 Heat Map

5. Click **Counting**.

Note

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

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

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

Chapter 9 Self-Learning

After your camera has enabled self-learning, the camera will learn the false alarm examples in the self-learning library. When the amount of false alarm examples in the self-learning library is large enough, the false alarms would be significantly reduced.

Note

- The chapter is only available for M series and certain event types.
- Ensure your camera supports and has enabled this function.

9.1 Add False Alarm Pictures to Self-Learning Library

For certain event types, when you have found false alarms in target detection of live view or searching results, you can add them in to self-learning library to reduce the reappearances of these false alarms.

Before You Start

- Ensure the event supports this function.
- Ensure the false alarm pictures are generated by the camera that supports self-learning.

Steps

1. Find false alarms in **Live View** → **Target**, **File Management** → **Smart Search**, or the search interfaces in **Smart Analysis**.
2. Select false alarm pictures from searching results.
3. Click **Import to Self-Learning Library**.

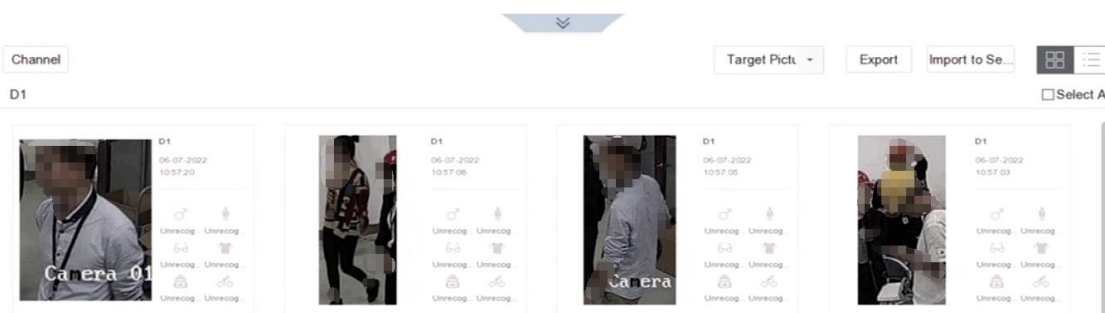


Figure 9-1 Add Examples to Self-Learning Library

Note

- For certain types of search interfaces, you have to click  to display the import button.
- Do not import the correct alarm pictures of human/vehicle targets to the self-learning library.

4. Optional: Go to **Smart Analysis** → **AI Training** → **Self-Learning Library** to view or delete false alarm examples.

9.2 Delete False Alarm Pictures in Self-Learning Library

You can view or delete false alarm pictures in the self-learning library.

Steps

1. Go to **Smart Analysis** → **Self-Learning Library**.
2. Select false alarm pictures.
3. Click **Delete**.

Chapter 10 File Management

10.1 Search Files

Specify detailed conditions to search videos and pictures.

Steps

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

Note

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

10.2 Export Files

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

Steps

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

10.3 Quick Backup

All the videos can be backed up with a shortcut.

Steps

1. Go to **File Management** → **Video**.
2. Search video(s) by setting different conditions (appearance, event or tag).
3. Click **Quick Backup**.

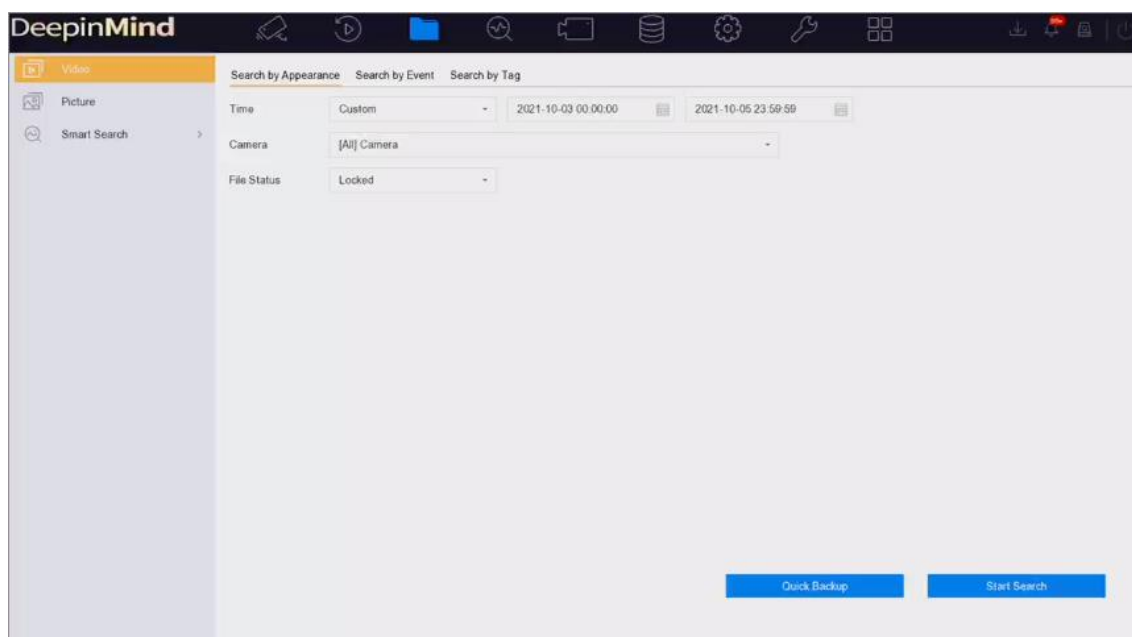


Figure 10-1 Quick Backup

10.4 Smart Search

10.4.1 Face Picture Search

Search by Face Picture Comparison Event

Search face picture by face picture comparison results.

Steps

1. Go to **File Management** → **Smart Search** → **Face** → **Search by Event**.
2. Set the start time and end time.
3. Select a channel.
4. Select **Event Type** as **Face Picture Comparison**.
5. Click **Start Search**. The search result list displays 1 channel.

6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to [**View Searching Result.**](#)

Search by Appearance

Search face picture by appearance.

Steps

1. Go to **File Management** → **Smart Search** → **Face** → **Search by Appearance**.
2. Set search conditions.
3. Click **Start Search**. The search result list displays 1 channel.
4. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

What to do next

Refer to [**View Searching Result.**](#)

View Searching Result

- Double click a file to view the related video.
- Click **Export** to export the selected file(s) to a backup device. You can click **Select All** to select all files.

 Note

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

10.4.2 Human Search

Search pictures by human body detection alarms.

Steps

1. Go to **File Management** → **Smart Search** → **Human** → **Search by Event**.
2. Set the start time and end time.
3. Select a channel.
4. Select **Event Type** as **Human Body Alarm**.
5. Click **Start Search**. The search result list displays 1 channel.
6. Click **Channel** to select a channel as your desire. It will display search results for the selected channel.
7. Optional: Export search results.
 - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
 - 2) Click **Export** to export the selected file(s) to a backup device.

 Note

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

10.4.3 Vehicle Search

You can search and view the matched vehicle pictures.

Steps

1. Go to **File Management** → **Smart Search** → **Vehicle**.
 2. Select a search method. For example, **Search by Appearance**, or **Search by Event**.
 3. Select the IP camera for the vehicle search.
 4. Set search conditions.
 5. Click **Start Search**. The search result list displays 1 channel.
 6. Click **Channel** to select a channel as your desire. It will display searching results for the selected channel.
 7. Export search results.
 - 1) Select result file(s) from the search result interface, or check **Select All** to select all files.
 - 2) Click **Export** to export the selected file(s) to a backup device.
-

 Note

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

Chapter 11 Storage

11.1 Storage Device Management

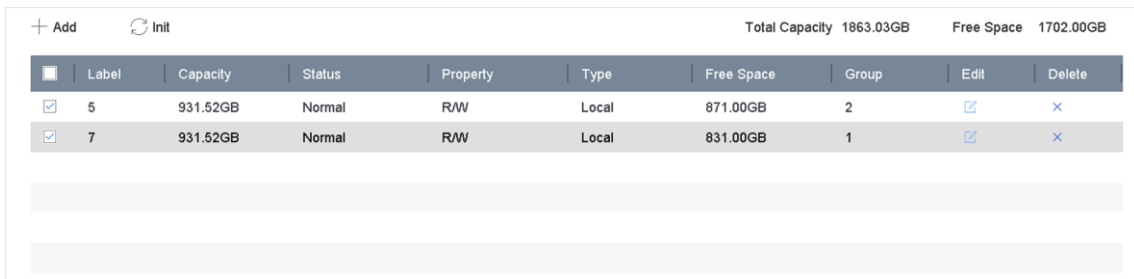
11.1.1 Manage Local HDD

Configure HDD Group

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

Steps

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



The screenshot shows a web interface for managing storage devices. At the top, there are buttons for '+ Add' and 'Init'. To the right, it displays 'Total Capacity 1863.03GB' and 'Free Space 1702.00GB'. Below this is a table with columns: Label, Capacity, Status, Property, Type, Free Space, Group, Edit, and Delete. Two HDDs are listed: Label 5 (931.52GB, Normal, R/W, Local, 871.00GB free, Group 2) and Label 7 (931.52GB, Normal, R/W, Local, 831.00GB free, Group 1). Each row has an 'Edit' icon (pencil) and a 'Delete' icon (X). Below the table are two empty rows for additional devices.

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

Figure 11-1 Storage Device

6. Click to enter Local HDD Settings interface.

Local HDD Settings

HDD No.

5

HDD Property

☒ R/W ☐ Read-only ☐ Redundan...

Group

☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8

☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16

HDD Capacity

931.52GB

OK

Cancel

Figure 11-2 Local HDD Settings

7. Select a group number for the HDD.

8. Click **OK**.

Note

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

9. Go to **Storage** → **Storage Mode**.

10. Select group number from the list.

11. Select related camera(s) to save videos and pictures on the HDD group.

12. Click **Apply**.

Configure the HDD Property

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

Before You Start

Set the storage mode to Group. For detailed steps, refer to [***Configure HDD Group***](#)

Steps

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

R/W

HDD supports both read and write.

Read-only

Files in read-only HDD will not be overwritten.

Redundant

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

4. Click **OK**.

Configure the HDD Quota

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

Steps

1. Go to **Storage** → **Storage Mode**.
2. Select **Mode** as **Quota**.
3. Select a device type.
4. Select a device.
5. Set the storage capacity for the quota.
6. Click **Copy to** to copy the quota settings of the current camera to other cameras.
7. Click **Apply**.

 Note

- When the maximum capacity is set to 0, devices will use the total HDD capacity for storing files.
 - Reboot the video recorder to activate the new settings.
-

11.1.2 Add a Network Disk

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

Steps

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

Custom Add

NetHDD

NetHDD 1

Type

NAS

NetHDD IP

120 . 36 . 2 . 39

NetHDD Directory

/nas/device1/11|

⊗

Search

OK

Cancel

Figure 11-3 Add NetHDD

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

11.1.3 Configure Cloud Storage

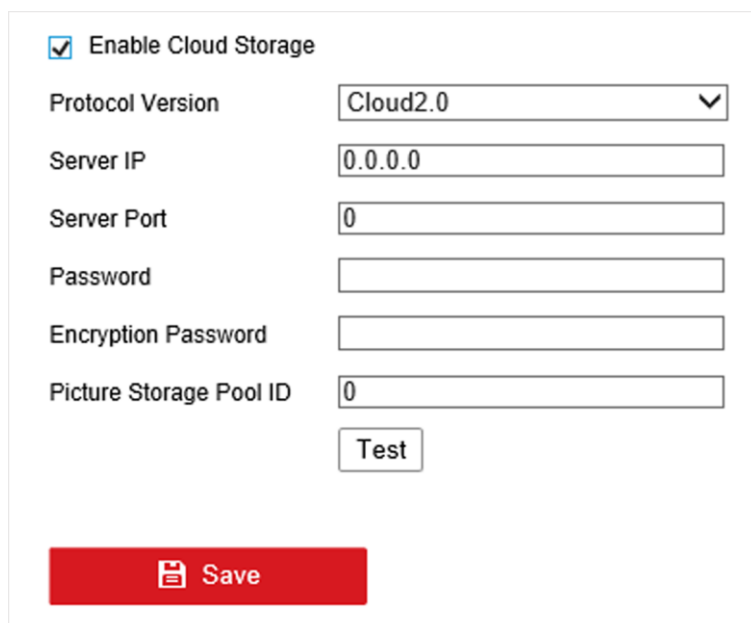
The cloud storage function enables the device to upload videos to a cloud server. It may not only save your local HDD storage space, but also let you access videos more conveniently. You can enable cloud storage via web browser.

Before You Start

Ensure your device is properly connected to Internet, and you have the correct cloud storage information.

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **Cloud Storage**.



☒ Enable Cloud Storage

Protocol Version

Server IP

Server Port

Password

Encryption Password

Picture Storage Pool ID

Figure 11-4 Cloud Storage

2. Check **Enable Cloud Storage**.
3. Set cloud storage server parameters.

 Note

There are multiple pools in a cloud storage server. A pool is like an HDD, it is used for store files. Each pool has an ID, hence you have to get the pool ID from storage server.

4. Click **Test** to test if parameters are valid.
5. Click **Save**.

11.1.4 Manage eSATA

 Note

The eSATA function is only available for certain models.

Configure eSATA for Data Storage

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

Steps

1. Go to **Storage** → **Advanced**.

2. Select eSATA **Usage** as **Export** or **Record/Capture**.

Export

Use the eSATA for backup.

Record/Capture

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

eSATA	eSATA1
Usage	Record/Capture

Figure 11-5 eSATA Mode

What to do next

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

Configure eSATA for Auto Backup

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

Before You Start

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

Steps

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

Note

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

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

Network Video Recorder User Manual

The screenshot shows the 'Backup Status' and 'Auto Backup Settings' section of a Network Video Recorder's web interface. The 'Backup Status' section shows 'Current Status' and 'Last Backup' as 'Unplanned'. The 'Auto Backup Settings' section includes a checkbox for 'Auto Backup' which is currently unchecked. Below this is a 'Start Backup at' field set to '00:00' with a '+' button and a help icon. A 'Select Channel(s) for Backup' section features a 'Select All' checkbox and a grid of 32 channels (D1 to D32), each with an unchecked checkbox. Below the channel grid, the 'Backup Stream Type' is set to 'Dual-Stream' (selected over 'Main Stream' and 'Sub-Stream'). The 'Backup to' dropdown is set to 'eSATA'. The 'Overwrite' option is set to 'Disable' (selected over 'Enable'). An 'Apply' button is at the bottom.

Backup Status	
Current Status	Unplanned.
Last Backup	Unplanned.

Auto Backup Settings

Auto Backup ☐

Start Backup at

Select Channel(s) for Backup ☐ Select All

☐ D1	☐ D2	☐ D3	☐ D4	☐ D5	☐ D6	☐ D7	☐ D8
☐ D9	☐ D10	☐ D11	☐ D12	☐ D13	☐ D14	☐ D15	☐ D16
☐ D17	☐ D18	☐ D19	☐ D20	☐ D21	☐ D22	☐ D23	☐ D24
☐ D25	☐ D26	☐ D27	☐ D28	☐ D29	☐ D30	☐ D31	☐ D32

Backup Stream Type ☐ Main Stream ☐ Sub-Stream ☒ Dual-Stream

Backup to

Overwrite ☒ Disable ☐ Enable

Figure 11-6 Configure eSATA for Auto Backup

11.1.5 Dynamically Adjust Recording Writing Buffer

Dynamically adjust recording writing buffer allows the device to adjust buffer memory dynamically when bit rate exceeds limit.

Steps

1. Go to **Storage** → **Advanced**.
2. Check **Dynamically Adjust Recording Writing Buffer** to avoid video loss when bit rate is higher than 4 Mbps.

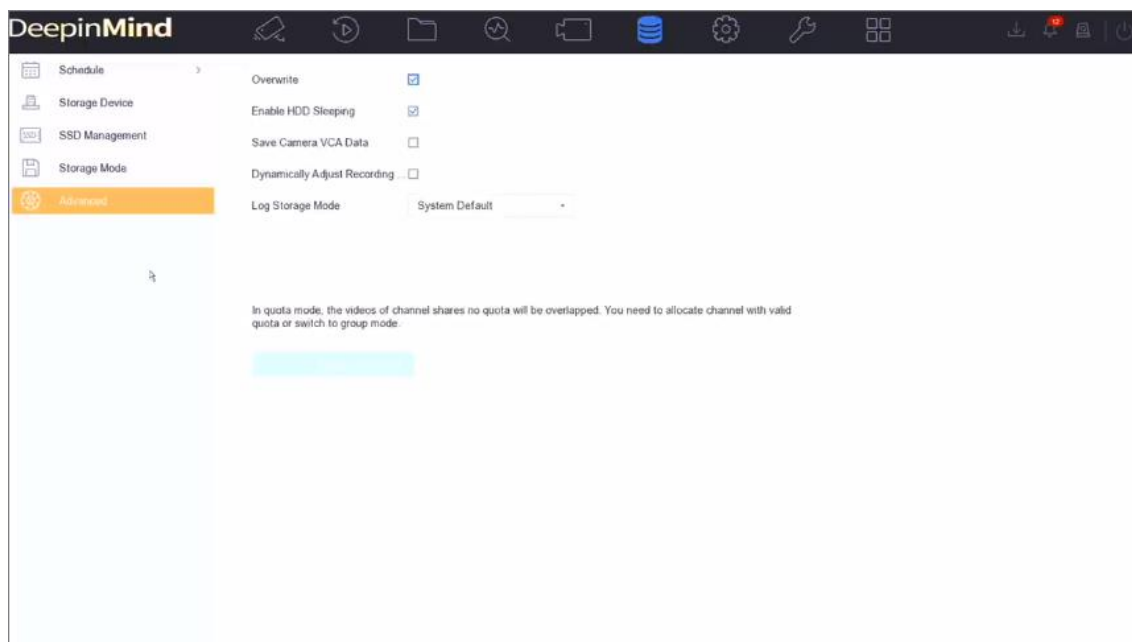


Figure 11-7 Dynamically Adjust Recording Writing Buffer

Note

This function will result in higher memory use. Restart the device after you enable/disable the function.

11.2 Disk Array

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

Note

The functions in this section are only available for certain models.

11.2.1 Create a Disk Array

The video recorder supports software-based disk arrays. Enable the RAID function as required, and ensure each HDD capacity is not less than 4 TB. If your device has no more than 16 SATA interfaces, a disk array can contain no more than 8 HDDs. If your device has 24 SATA interfaces, a disk array can contain no more than 12 HDDs. Two ways are available for creating an array: one-

touch configuration and manual configuration.

One-Touch Creation

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

Before You Start

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

Steps

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



Note

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

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

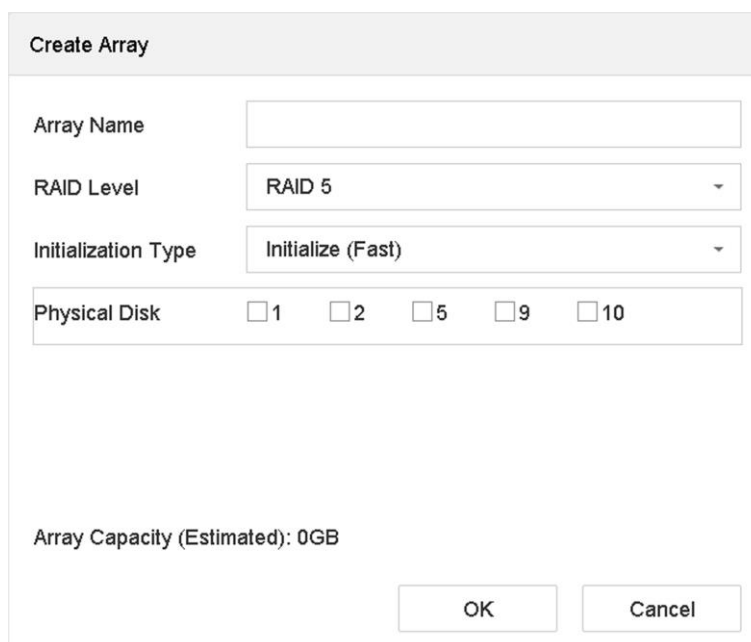
Manual Creation

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

Steps

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

Network Video Recorder User Manual



Create Array

Array Name:

RAID Level:

Initialization Type:

Physical Disk: ☐ 1 ☐ 2 ☐ 5 ☐ 9 ☐ 10

Array Capacity (Estimated): 0GB

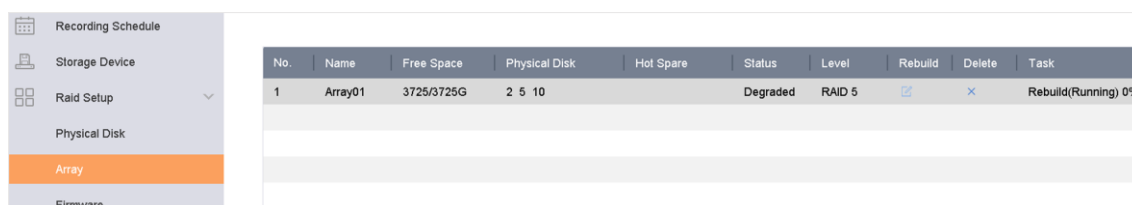
Figure 11-8 Create Array

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

Table 11-1 The Required Number of HDDs

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

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



Recording Schedule	
Storage Device	
Raid Setup	
Physical Disk	
Array	
Firmware	

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

Figure 11-9 Array List

11.2.2 Rebuild an Array

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

Functional

No disk loss in the array.

Offline

The number of lost disks has exceeded the limit.

Degraded

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

Configure a Hot Spare Disk

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

Steps

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

No.	Capacity	Array	Type	Status	Model	Hot Spare	Task
1	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
☐ 2	2794.52GB		Normal	Functional	ST3000VX000-9YW166	☒	None
5	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None
☐ 9	2794.52GB		Normal	Functional	ST3000VX000-1CU166	☒	None
10	1863.02GB	Array01	Array	Functional	ST2000VX000-1CU164	—	None

Figure 11-10 Physical Disk

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

Automatically Rebuild an Array

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

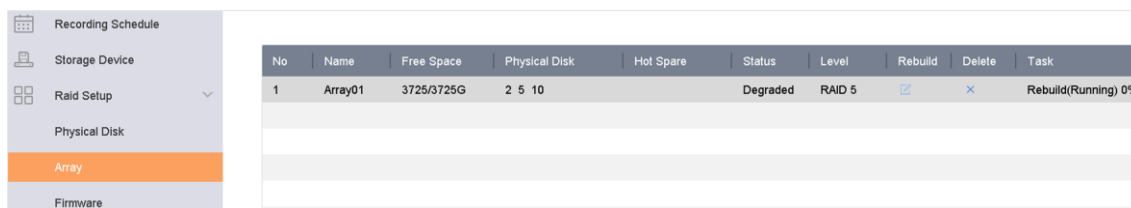
Before You Start

Create hot spare disks. For details, refer to [Configure a Hot Spare Disk](#).

Steps

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

Network Video Recorder User Manual



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

Figure 11-11 Array List

Manually Rebuild an Array

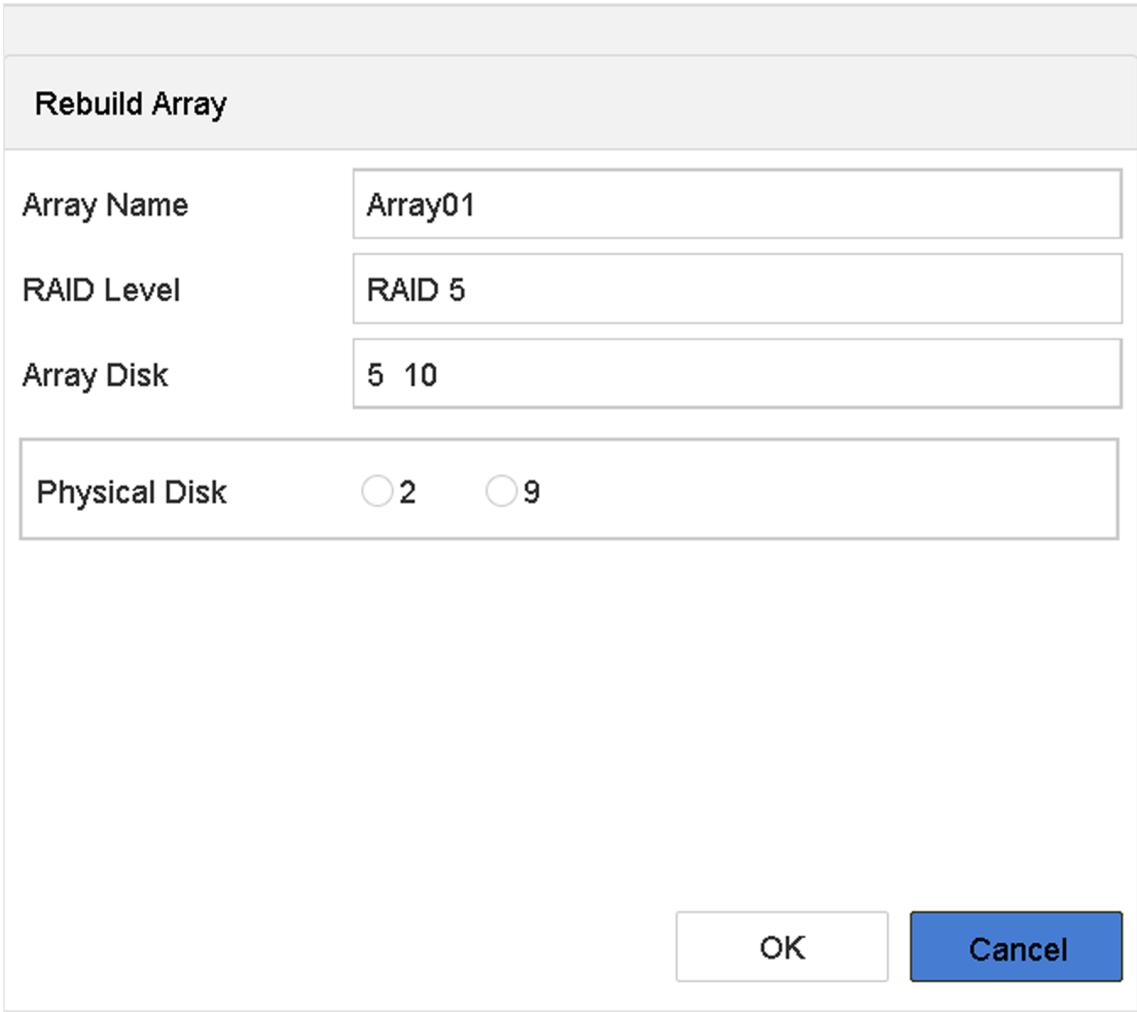
If no hot spare disks are configured, rebuild a degraded array manually.

Before You Start

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

Steps

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



The image shows a 'Rebuild Array' dialog box. It has a title bar 'Rebuild Array'. Inside, there are three text input fields: 'Array Name' with 'Array01', 'RAID Level' with 'RAID 5', and 'Array Disk' with '5 10'. Below these is a section for 'Physical Disk' with two radio buttons, '2' and '9', both of which are unselected. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Rebuild Array	
Array Name	Array01
RAID Level	RAID 5
Array Disk	5 10
Physical Disk	☐ 2 ☐ 9
OK Cancel	

Figure 11-12 Rebuild Array

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

Chapter 12 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 12-1 Building a Hot Spare System

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.
-

12.1 Set Working Device

Steps

1. Go to **System** → **Hot Spare**.
 2. Set **Work Mode** as **Normal Mode**.
-

Note

Normal Mode is set by default.

The screenshot shows a configuration window for the hot spare system. It includes a 'Work Mode' dropdown menu currently set to 'Normal Mode'. Below this is a text field for the 'IP address of the hot spare device'. A status indicator shows 'Hot Spare Device Working Status' as 'Disconnected'. A note at the bottom states: 'Note: Please configure hot spare relation in the hot spare device.'

Figure 12-2 Set Working Recorder

3. Click **Apply**.

 Note

Repeat the above steps to set other working devices.

12.2 Set Hot Spare Device

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

Steps

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

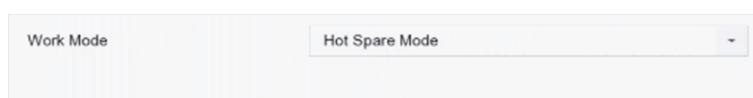


Figure 12-3 Hot Spare

3. Click **Apply**.
4. Click **Yes** in the pop-up. Your device will restart automatically.

 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 afterward.
-

12.3 Manage Hot Spare System

Steps

 Note

- Up to 32 working devices and 32 hot spare devices are allowed in the hot spare system.
 - Only one hot spare device can add working devices and other hot spare devices. You can find the hot spare device IP address from working devices.
-

1. Go to **System** → **Hot Spare** through the hot spare device.

Network Video Recorder User Manual

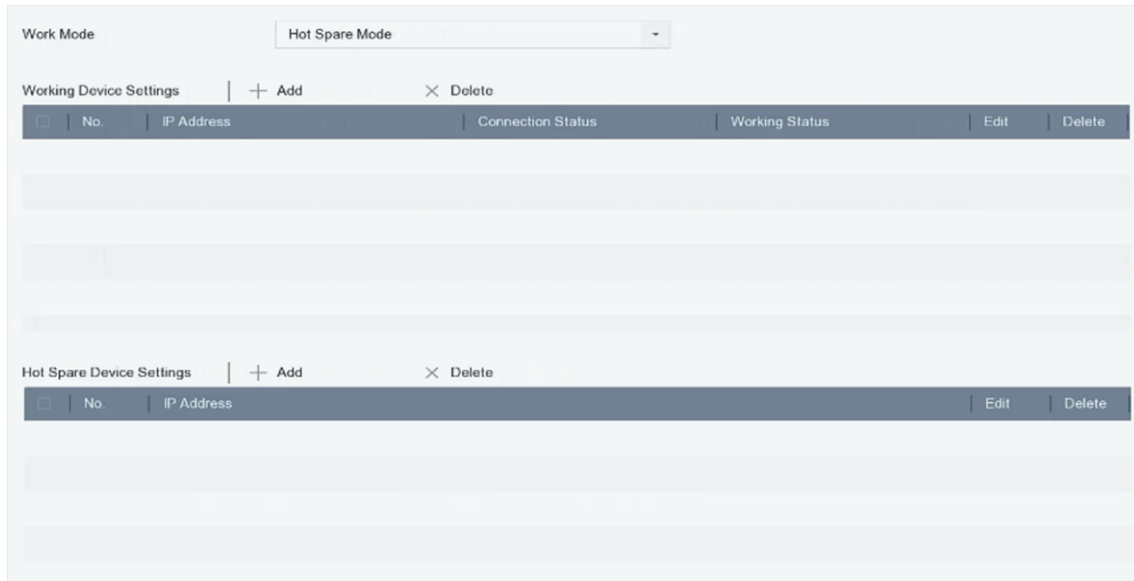


Figure 12-4 Add Working Device

2. Click **Add** in **Working Device Settings** to add working devices to the hot spare system. After refreshing the interface, you can view the working status of working devices from the hot spare device interface. Also, the working status and IP address of the hot spare device can be viewed from working device interface.

Table 12-1 Working Status of Working Device

Working Status	Description
Monitoring	Working devices are working properly.
No need for backup	The working device goes offline and has never been monitored before.
Backing up	The working device has been monitored before but goes offline. A hot spare device will take over the working device, and record the videos of network cameras connected to the working device. The video backup function can be enabled for one working device at a time.
Waiting for synchronization	The working device comes back online, and waits for the a hot spare device to sync videos.
Synchronizing	The hot spare device is restoring videos back into the working device. The synchronization function can be enabled for one working device at a time.
Synchronization finished	Videos are restored back to the working

Network Video Recorder User Manual

Working Status	Description
	device. The work device is recovered.

3. Click **Add** in **Hot Spare Device Settings** to add hot spare devices to the hot spare system.
4. Optional: Click **Delete** to delete working devices or hot spare devices as your desire.

Chapter 13 Network Settings

13.1 Configure DDNS

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

Before You Start

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

Steps

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

TCP/IP DDNS PPPoE NTP NAT

Enable ☒

DDNS Type DynDNS

User Name test

Server Address member.dyndns.org

Password *****

Device Domain Name 1233dyndns.com

Status DDNS is disabled.

Apply

Figure 13-1 DDNS Settings

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

13.2 Configure PPPoE

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

Contact your Internet service provider for details about PPPoE service.

13.3 Configure SNMP

You can configure SNMP (SNMP v2 and SNMP v3) settings to get device status and parameter information via web browser. SNMP v3 adds cryptographic security to SNMP v2, and provides security with authentication and privacy.

Before You Start

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

Steps

1. Go to **Configuration** → **Network** → **Advanced Settings** → **SNMP** via web browser.

SNMP v2
☐ Enable SNMP v2c
Read SNMP Community
Write SNMP Community
Trap Address
Trap Port

SNMP v3
☐ Enable SNMPv3
Read UserName
Security Level
Authentication Algorithm ☒ MD5 ☐ SHA
Authentication Password
Private-key Algorithm ☒ DES ☐ AES
Private-key password
Write UserName
Security Level
Authentication Algorithm ☒ MD5 ☐ SHA
Authentication Password
Private-key Algorithm ☒ DES ☐ AES
Private-key password
Trap Address
Trap Port

SNMP Other Settings
SNMP Port

 Save

Figure 13-2 SNMP Settings

2. Enable SNMP v2 or SNMP v3 as your desire.
3. Set related parameters.
4. Set **SNMP Port**.
5. Click **Save**.

13.4 Configure Email

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

Before You Start

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

Steps

1. Go to **System** → **Network** → **Advanced** → **Email**.
2. Configure the email settings.

Server Authentication

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

SMTP Server

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

SMTP Port

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

Enable SSL/TLS

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

Sender

The sender's name.

Sender's Address

The sender's address.

Select Receivers

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

Receiver

The receiver's name.

Receiver's Address

The email address of the user to be notified.

Attached Image

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

Interval

The time interval for capturing the attached images.

3. Optional: Enable the alternate SMTP, and configure the required parameters for alternate SMTP. When the preferred SMTP is invalid, the device will use alternate SMTP to send emails.
4. Optional: Click **Test** to send a test email.
5. Click **Apply**.

13.5 Configure Port Mapping (NAT)

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

Before You Start

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

Universal Plug and Play (UPnP™) can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Steps

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

Enable ☐

Mapping Type: Manual

Port Type	Edit	External Port	External IP Address	Port	UPnP Status
HTTP Port	✎	80	0.0.0.0	80	inactive
RTSP Port	✎	554	0.0.0.0	554	inactive
Server Port	✎	8000	0.0.0.0	8000	inactive
HTTPS Port	✎	443	0.0.0.0	443	inactive
Enhanced SDK Service ...	✎	8443	0.0.0.0	8443	inactive

[Refresh](#)

Figure 13-3 Port Mapping Setting

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

 Note

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

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

 Note

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

Delete	External Source Port	Protocol	Internal Source IP	Internal Source Port	Application
☐	81	TCP	192.168.251.101	80	HTTP

Figure 13-4 Set Virtual Server Item

13.6 Configure Port

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

Steps

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

Alarm Host IP	
Alarm Host Port	0
Server Port	8000
HTTP Port	80
Multicast IP	
RTSP Port	554
Enhanced SDK Ser...	8443
Apply	

Figure 13-5 Port Settings

2. Configure port settings as needed.

Alarm Host IP/Port

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

Server Port

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

HTTP Port

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

Multicast IP

Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through network. Both IPv4 and IPv6 are available for multicast IP address.

Network Video Recorder User Manual

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.

RTSP Port

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

Enhanced SDK Service Port

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

3. Click **Apply**.

13.7 Configure ONVIF

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

Steps

1. Go to **Maintenance** → **System Service** → **ONVIF**.
2. Check **Enable ONVIF** to enable the ONVIF access management.



Note

ONVIF protocol is disabled by default.

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



Caution

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

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

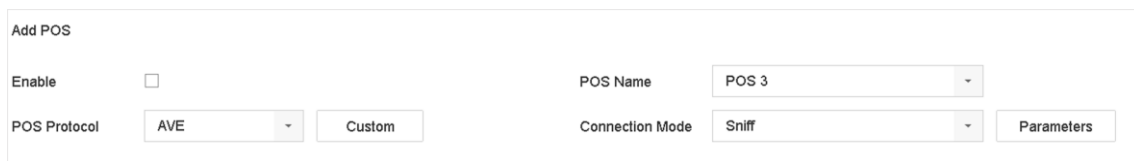
Chapter 14 POS Configuration

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

14.1 Configure POS Connection

Steps

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



The screenshot shows the 'Add POS' configuration interface. It includes an 'Enable' checkbox, a 'POS Name' dropdown menu currently showing 'POS 3', a 'POS Protocol' dropdown menu showing 'AVE' with a 'Custom' button, a 'Connection Mode' dropdown menu showing 'Sniff', and a 'Parameters' button.

Figure 14-1 POS Settings

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

Note

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

5. Select **POS Protocol**.

Note

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

Universal Protocol

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

Start Line Identifier		Hex	☒
Line Break	0D0A	Hex	☒
End Line Identifier		Hex	☒
Case Sensitive	☒		
Filtering Identifier	☒		
Enable XML Prot...	☒		
OK Cancel			

Figure 14-2 Universal Protocol Settings

EPSON

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

AVE

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

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

NUCLEUS

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

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

**Note**

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

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

TCP Connection

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

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

UDP Connection

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

machine must be unique.

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

USB-to-RS-232 Connection

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

USB-to-RS-232 Settings	
Serial Port Number	1
Baud Rate	4800
Data Bit	5
Stop Bit	1
Parity	None
Flow Ctrl	None
OK Cancel	

Figure 14-3 USB-to-RS-232 Settings

RS-232 Connection

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

Multicast Connection

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

Sniff Connection

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

Sniff Settings	
Enable Source Port F...	☒
Source Address	18 . 16 . 1 . 1
Source Port	10020
Enable Destination A...	☒
Enable Destination P...	☒
Destination Address	20 . 18 . 1 . 24
Destination Port	10030
OK Cancel	

Figure 14-4 Sniff Settings

14.2 Configure POS Text Overlay

Steps

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

Figure 14-5 Overlay Character Settings

3. Select **linked channel** to overlay the POS characters.
4. Set the characters overlay for the enabled POS.
 - Character encoding format: currently the Latin-1 format is available
 - Overlay mode of the characters to display in scrolling or page mod
 - Font size and font color
 - Display time (sec) of the characters. The value ranges 5 -3600 sec.
 - Timeout of POS event. The value ranges 5 -3600 sec. When the device has not received the POS message within the defined time, the transaction ends.
5. In **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc.
The defined privacy information will be displayed using ***on the image instead.
6. Check **Overlay POS in Live View**. When this feature is enabled, the POS information is overlaid on the Live View image.

Note

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

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

14.3 Configure POS Alarm

A POS event can trigger channels to start recording, or trigger full screen monitoring, etc.

Steps

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

Network Video Recorder User Manual

Channel Linkage and Display

Event Linkage

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

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

Apply

Figure 14-6 Set Trigger Cameras of POS

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

Chapter 15 User Management and Security

15.1 Manage User Accounts

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

15.1.1 Add a User

Steps

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

Caution

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

User Level

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

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

User's MAC Address

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

5. Click **OK**.

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

15.1.2 Edit the Admin User

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

Steps

1. Go to **System** → **User**.
2. Select the admin user from the list.
3. Click **Modify**.

The 'Edit User' dialog box contains the following fields and controls:

- User Name:** admin
- Password:** masked with asterisks. A 'Discard C...' button is next to it.
- Confirm:** masked with asterisks.
- Note:** Valid password range [8-16]. You can use...
- Password S...:** Three bars indicating strength.
- User's MAC Ad...:** 00 : 00 : 00 : 00 : 00 : 00
- Unlock Patt...:** ☒ Enable Unlock Pattern (gear icon)
- GUID File:** ☐ Export (question mark icon)
- Security Qu...:** (gear icon)
- Reserved E...:** (empty field) (question mark icon) Modify
- Buttons:** OK, Cancel

Figure 15-1 Edit User (Admin)

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

Network Video Recorder User Manual

6. Check **Export** of **GUID File** to export the GUID file for the admin user account.
-

 Note

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

7. Configure security question for password resetting.
8. Configure reserved email for password resetting.
9. Click **OK** to save the settings.

15.1.3 Edit an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address.

Steps

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

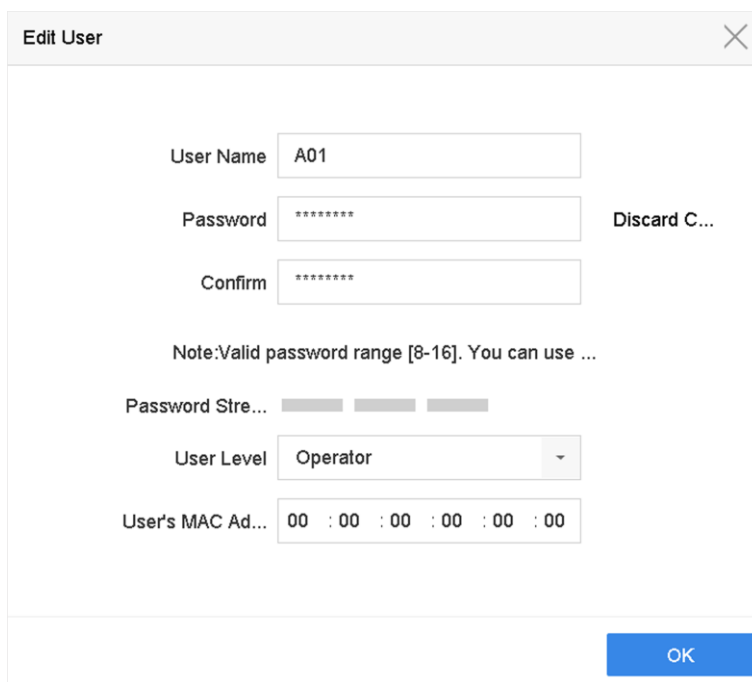


Figure 15-2 Edit User (Operator/Guest)

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

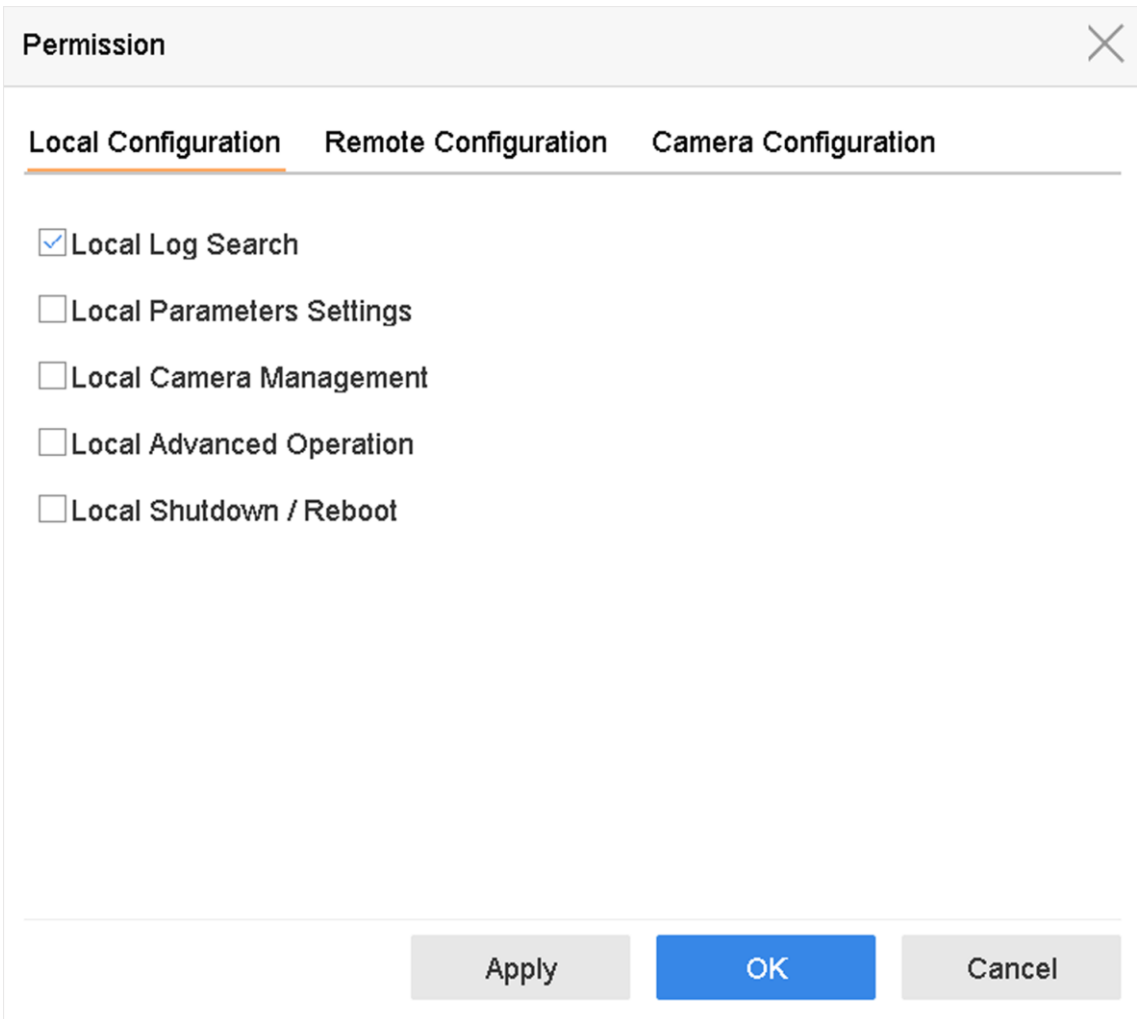
15.2 Manage User Permissions

15.2.1 Set User Permissions

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

Steps

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



The image shows a 'Permission' dialog box with a close button (X) in the top right corner. It has three tabs: 'Local Configuration' (selected), 'Remote Configuration', and 'Camera Configuration'. Under the 'Local Configuration' tab, there are five checkboxes: 'Local Log Search' (checked), 'Local Parameters Settings', 'Local Camera Management', 'Local Advanced Operation', and 'Local Shutdown / Reboot'. At the bottom, there are three buttons: 'Apply', 'OK' (highlighted in blue), and 'Cancel'.

Figure 15-3 User Permission Settings Interface

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

Local Log Search

Searching and viewing logs and system information of device.

Local Parameters Settings

Configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

Local Camera Management

Adding, deleting, and editing of IP cameras.

Local Advanced Operation

Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Local Shutdown Reboot

Shutting down or rebooting the device.

2) Set Remote Configuration

Remote Log Search

Remotely viewing logs that are saved on the device.

Remote Parameters Settings

Remotely configuring parameters, restoring factory default parameters, and importing/exporting configuration files.

Remote Camera Management

Remote adding, deleting, and editing of the IP cameras.

Remote Serial Port Control

Configuring settings for RS-232 and RS-485 port settings.

Remote Video Output Control

Sending remote button control signals.

Two-Way Audio

Operating the two-way radio between the remote client and the device.

Remote Alarm Control

Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.

Remote Advanced Operation

Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

Remote Shutdown/Reboot

Remotely shutting down or rebooting the device.

3) Set Camera Configuration

Remote Live View

Remotely viewing live video of the selected camera(s).

Local Manual Operation

Locally starting/stopping manual recording and alarm output of the selected camera(s).

Remote Manual Operation

Remotely starting/stopping manual recording and alarm output of the selected camera(s).

Local Playback

Locally playing back recorded files of the selected camera(s).

Remote Playback

Remotely playing back recorded files of the selected camera(s).

Local PTZ Control

Locally controlling PTZ movement of the selected camera(s).

Remote PTZ Control

Remotely controlling PTZ movement of the selected camera(s).

Local Video Export

Locally exporting recorded files of the selected camera(s).

Local Live View

View live video of the selected camera(s) in local.

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

15.2.2 Set Live View Permission on Lock Screen

The admin user can set live view permission for specific cameras in the screen lock status of device.

- The admin user can set this permission for user accounts.
- When the normal user (Operator or Guest) has no local live view permission for specific camera (s), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

Steps

1. Go to **System** → **User**.
2. Click **Live View Permission on Lock Screen**.
3. Input admin password and click **Next**.

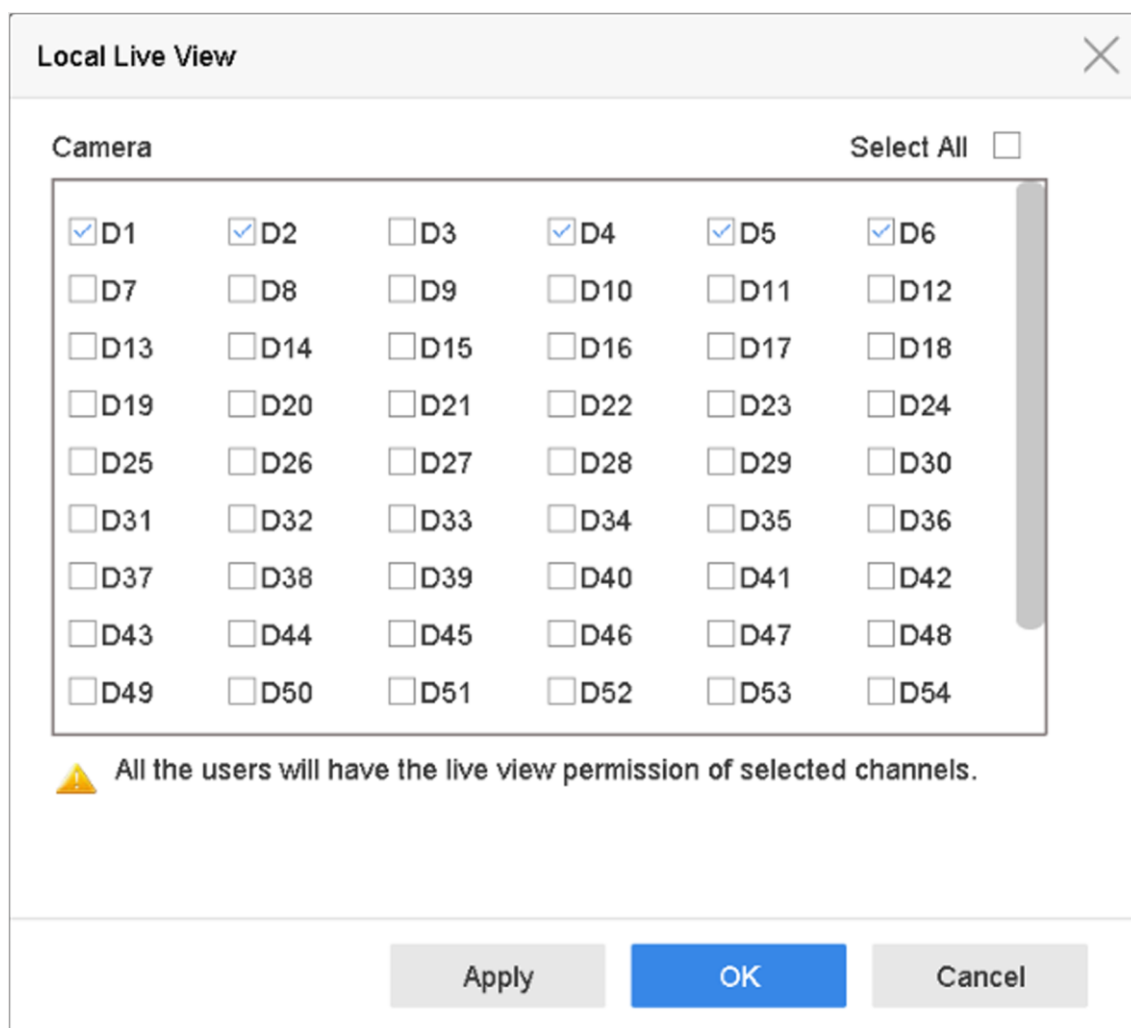


Figure 15-4 Set Live View Permissions on Lock Screen

4. Set the permissions. Select the camera (s) to allow live view when the current user account is in logout status.
5. Click **OK**.

15.2.3 Set Double Verification Permission for Non-admin Users

After double verification is enabled in the channel, a non-admin user must be verified by an authorized user to get the permission. Only admin has the authorization to set double verification.

Steps

1. Go to **Maintenance** → **System Service** → **Double Verification Settings**.

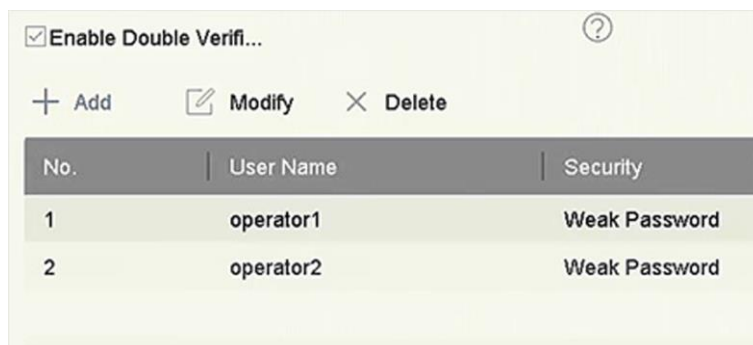


Figure 15-5 Set Double Verification User

2. Check **Enable Double Verification**.
3. Set double verification user. The double verification is different from the system user. You can add up to 8 double verification users.
 - 1) Click **Add** to add a double verification user.
 - 2) Enter the admin password.
 - 3) Set the user parameters, including user name, password, camera permission, etc.
 - 4) Click **OK**.
4. Click **Apply**.
5. Set permission for non-admin users.
 - 1) Go to **System** → **User**.
 - 2) Click  to edit user permission.
 - 3) Select **Camera Permission**. Only **Local Playback**, **Remote Playback/Download**, and **Local Video Export** are available for double verification.
 - 4) Select the channel(s) that requires double verification.
 - 5) Click **OK**.

15.3 Configure Password Security

15.3.1 Export GUID File

The GUID file can help you to reset password when you forget it. You can export GUID file via web browser. Please keep the GUID file properly.

Before You Start

Ensure you are on the same network segment with your device.

Steps

1. Go to **Configuration** → **System** → **User Management** → **User Management**.
2. Select the admin user.
3. Click **Account Security Settings**.
4. Click **Modify**.

Security Question Configuration

Security Question1 ▼

Answer

Security Question2 ▼

Answer

Security Question3 ▼

Answer

Export GUID File ?

Password Recovery via E-mail ?

Password Recovery via E-mail

Figure 15-6 Export GUID File

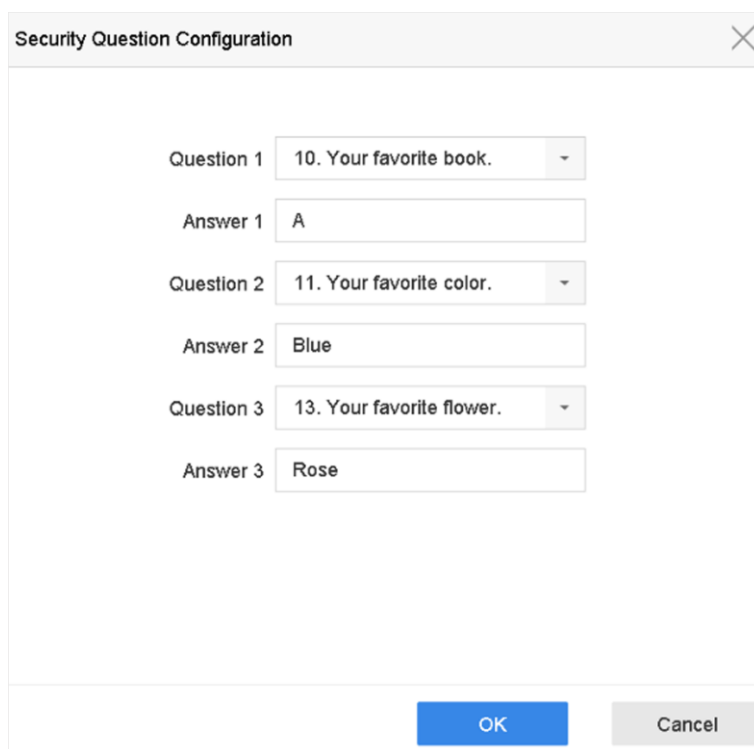
5. Click **Export** in **Export GUID File**.
6. Enter the admin password.
7. Save the GUID file to a directory as your desire.

15.3.2 Configure Security Questions

The security questions can help you to reset password when you forget your password, or encounter security issues.

Steps

1. Click **Security Question Configuration** when you are activating the device, or editing the admin user account.
2. Set the security questions and answers.

A screenshot of a 'Security Question Configuration' dialog box. The dialog has a title bar with the text 'Security Question Configuration' and a close button (X) on the right. The main area contains three sets of question and answer fields. Each set consists of a label (e.g., 'Question 1'), a dropdown menu, and a text input field (e.g., 'Answer 1'). The first set shows 'Question 1' with a dropdown value of '10. Your favorite book.' and an answer of 'A'. The second set shows 'Question 2' with a dropdown value of '11. Your favorite color.' and an answer of 'Blue'. The third set shows 'Question 3' with a dropdown value of '13. Your favorite flower.' and an answer of 'Rose'. At the bottom right, there are two buttons: 'OK' (blue) and 'Cancel' (grey).

Question	Answer
Question 1	A
Question 2	Blue
Question 3	Rose

Figure 15-7 Configure Security Questions

3. Click **OK**.

15.3.3 Configure Reserved Email

The reserved email will help you to reset password when you forget your password.

Steps

1. Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.
2. Enter reserved email address.

Figure 15-8 shows the 'Edit User' dialog box. The 'Reserved E...' field is highlighted, showing an email address 'z*****@*****.com' with a question mark icon and a 'Modify' button next to it. The 'OK' button is highlighted in blue.

Figure 15-8 Configure Reserved Email

3. Click **OK**.

15.4 Reset Password

When you forget the admin password, you can reset the password by importing the GUID file, answering security questions, or entering verification code from your reserved email.

15.4.1 Reset Password by GUID

You can reset password by GUID via web browser.

Before You Start

Ensure you have the correct GUID file.

Steps

1. On the user login interface, click **Forgot password**.
2. Select **Verification Mode** as **GUID File Verification**.
3. Click **Browse** to locate the GUID file.
4. Click **Next**.
5. Enter a new password.

Warning

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

6. Confirm the new password.
7. Click **Next**.

15.4.2 Reset Password by Security Questions

Before You Start

You have configured the security questions when you activate the device or edit the admin user account.

Steps

1. On the user login interface, click **Forgot Password**.
2. Select the **password resetting type** as **Verify by Security Question**.
3. Input the correct answers of the three security questions.
4. Click **OK**.
5. Create the new admin password on the Reset Password interface.

15.4.3 Reset Password by Reserved Email

Before You Start

Ensure you have configured the reserved email when you are activating the device or editing the admin user account. (Refer to [***Configure Reserved Email***](#))

Steps

1. On the user login interface, click **Forgot Password**.
2. On the password reset type interface, select **Verify by Reserved Email**.
3. Click **OK**.
4. Click **Next** if you accept the legal disclaimer. You can use a smartphone to scan the QR code and read the legal disclaimer.
5. Obtain the verification code. There are two ways to get the verification code.
 - Use Hik-Connect app to scan the QR code.
 - Send the QR code to email server.
 1. Insert a USB flash drive to your device.
 2. Click **Export** to export the QR code to USB flash drive.
 3. Email the QR code to [***pw_recovery@hikvision.com***](mailto:pw_recovery@hikvision.com) as attachment.
6. Check your reserved email, and you will receive a verification code within 5 minutes.

7. Enter the verification code.
8. Click **OK** to set the new password.

15.4.4 Reset Password by Hik-Connect

Before You Start

Ensure your device has enabled Hik-Connect, and bound with a registered Hik-Connect account.

Steps

1. On the user login interface, click **Forgot Password**.
2. On the password reset type interface, select **Verify by Hik-Connect**.
3. Log in to Hik-Connect app with the account that has bound with your device.
4. Use Hik-Connect to scan the QR code. Thereafter, you will have a verification code from Hik-Connect.
5. Enter the verification code.
6. Click **OK**.

Chapter 16 System Management

16.1 Configure Device

Steps

1. Go to **System** → **General**.
2. Configure the following settings.

Language

The default language used is English.

Output Standard

Set the output standard to NTSC or PAL, which must be the same as the video input standard.

Resolution

Configure video output resolution.

Device Name

Edit device name.

Device No.

Edit the device serial number. The Device No. can be set in the range of 1 to 255, and the default No. is 255. The number is used for the remote and keyboard control.

Auto Logout

Set the timeout time for menu inactivity. E.g., when the timeout time is set to 5 minutes, then the system will exit from the current operation menu to Live View screen after 5 minutes of menu inactivity.

Mouse Pointer Speed

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

Enable Wizard

Enable/disable the Wizard when the device starts up.

Enable Password

Enable/disable the use of the login password.

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

16.2 Configure Time

16.2.1 Manual Time Synchronization

Steps

1. Go to **System** → **General**.
2. Configure the date and time.
3. Click **Apply** to save the settings.

16.2.2 NTP Synchronization

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

Steps

1. Go to **System** → **Network** → **TCP/IP** → **NTP**.
2. Check **Enable**.
3. Configure NTP settings as need.

Interval (min)

Time interval between two time synchronization with NTP server

NTP Server

IP address of the NTP server

NTP Port

Port of the NTP server

4. Click **Apply**

16.2.3 DST Synchronization

DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

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

Steps

1. Go to **System** → **General**.
2. Check **Enable DST**.
3. Set **DST mode** as **Auto** or **Manual**.

Auto

Automatically enable the default DST period according to the local DST rules.

Manual

Manually set the start time and end time of the DST period, and the DST bias.

Network Video Recorder User Manual

4. Set the DST Bias. Set the time (30/60/90/120 minutes) offset from the standard time.
5. Click **Apply** to save the settings.

16.3 Audio Management

The audio files are used for alarm linkage.

You can import and manage audio files in **System** → **Audio Management**.

Note

Before importing audio files, prepare a backup device with the audio files in it.

16.4 Configure Enhanced SVC Mode

In live view or playback, enhanced SVC mode can be configured to extract frames of the video, providing better decoding capacity.

This mode can be enabled if you go to **System** → **General**.

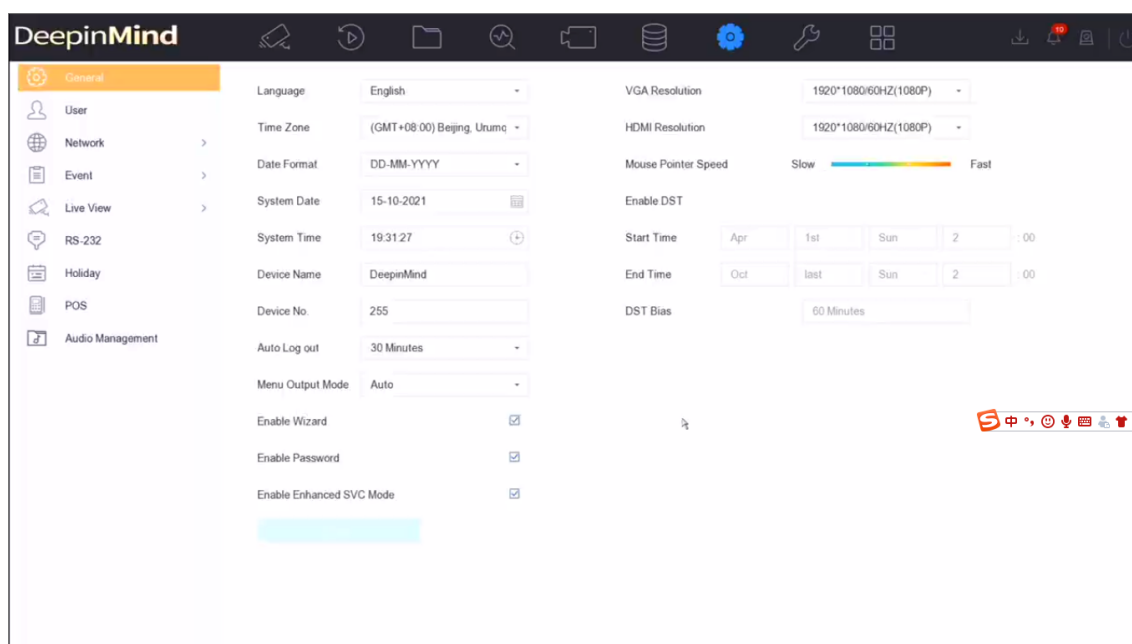


Figure 16-1 Enhanced SVC Mode

Note

If the enhanced SVC mode configuration of the device does not work, go to the Web page of the camera(s) to enable the enhanced SVC mode.

16.5 Network Detection

16.5.1 Network Traffic Monitoring

Network traffic monitoring is the process of reviewing, analyzing and managing network traffic for any abnormality or process that can affect network performance, availability and/or security.

Steps

1. Go to **Maintenance** → **Network** → **Traffic**.
2. You can view the real-time network traffic status, including MTU (Maximum Transmission Unit), and network throughput.

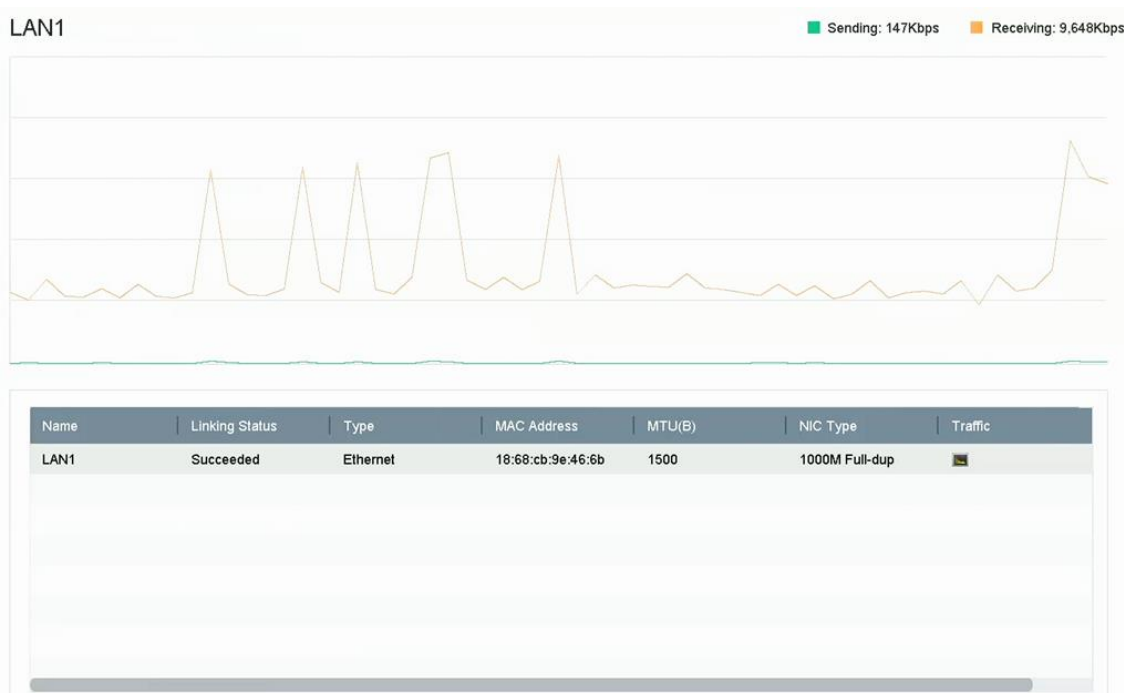


Figure 16-2 Network Traffic

16.5.2 Test Network Delay and Packet Loss

Network delay is caused by slow response of the device when oversized data information is not limited during transmission under certain network protocol, e.g. TCP/IP. Packet loss test is for testing network packet loss rate that is the ratio of lost data packet and total number of transmitted data packet.

Steps

1. Go to **Maintenance** → **Network** → **Network Detection**.
2. Select a network card in **Select NIC**.
3. Enter the destination IP address in **Destination Address**.

Network Video Recorder User Manual

4. Click **Test**.



Network Delay, Packet Loss Test

Select NIC: LAN1

Destination Address: 10.6.114.33

Test

Figure 16-3 Test Network Delay and Packet Loss

16.5.3 Export Network Packet

After the recorder accessing network, you can use USB flash drive to export network packet.

Before You Start

Prepare a USB flash drive to export network packet.

Steps

1. Insert the USB flash drive.
2. Go to **Maintenance** → **Network** → **Network Detection**.
3. Select network card in **Select NIC**.
4. Select the USB flash drive in **Device Name**. You can click **Refresh** if the connected local backup device cannot be displayed.



Network Packet Export

Device Name: USB Flash Disk 1-1

Refresh Status

LAN1	10.6.114.17	3.132Kbps
------	-------------	-----------

Export

Figure 16-4 Export Network Packet

5. Optional: Click **Status** to view the network status.
6. Click **Export**.



Note

It will export 1 MB data each time as default.

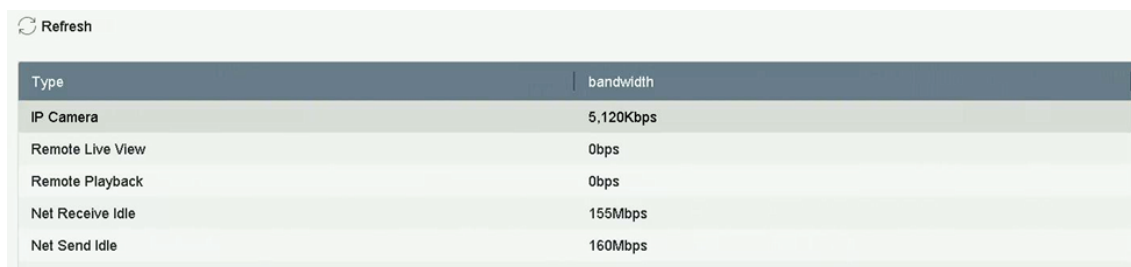
16.5.4 Network Resource Statistics

The remote access, including web browser and client software, will consume output bandwidth. You can view the real-time bandwidth statistics.

Steps

1. Go to **Maintenance** → **Network** → **Network Stat**.

Network Video Recorder User Manual



Type	bandwidth
IP Camera	5,120Kbps
Remote Live View	0bps
Remote Playback	0bps
Net Receive Idle	155Mbps
Net Send Idle	160Mbps

Figure 16-5 Network Resource Statistics

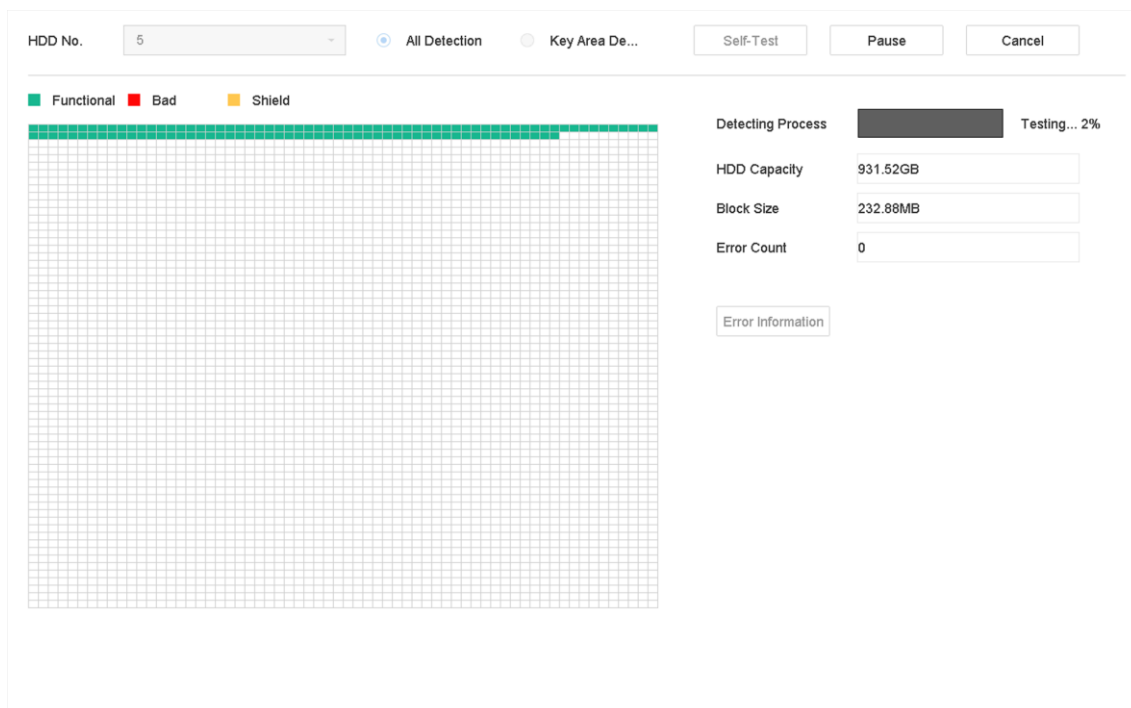
2. View the bandwidth statistics, including **IP Camera**, **Remote Live View**, **Remote Play**, **Net Total Idle**, etc.
3. Optional: Click **Refresh** to obtain the latest data.

16.6 Storage Device Maintenance

16.6.1 Bad Sector Detection

Steps

1. Go to **Maintenance** → **HDD Operation** → **Bad Sector Detection**.
2. Select the HDD No. you want to configure in the dropdown list.
3. Select **All Detection** or **Key Area Detection** as the detection type.
4. Click **Self-Test** to start the detection.



HDD No. ☒ All Detection ☐ Key Area De...

Functional Bad Shield

Detecting Process Testing... 2%

HDD Capacity

Block Size

Error Count

Figure 16-6 Bad Sector Detection

Note

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

16.6.2 S.M.A.R.T. Detection

HDD detection functions such as the adopting of the S.M.A.R.T. and the Bad Sector Detection techniques. S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.

Steps

1. Go to **Maintenance** → **HDD Operation** → **S.M.A.R.T.**
2. Select the HDD to view its S.M.A.R.T. information list.
3. Set **Self-Test Type**.
4. Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

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

HDD No.

Self-Test Type

Temperature... Self-Evaluation

Working Time... All-Evaluation

S.M.A.R.T Infor

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

Figure 16-7 S.M.A.R.T. Settings Interface

Note

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

The related information of the S.M.A.R.T. is shown, and you can check the HDD status.

16.6.3 HDD Health Detection

You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.

Steps

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

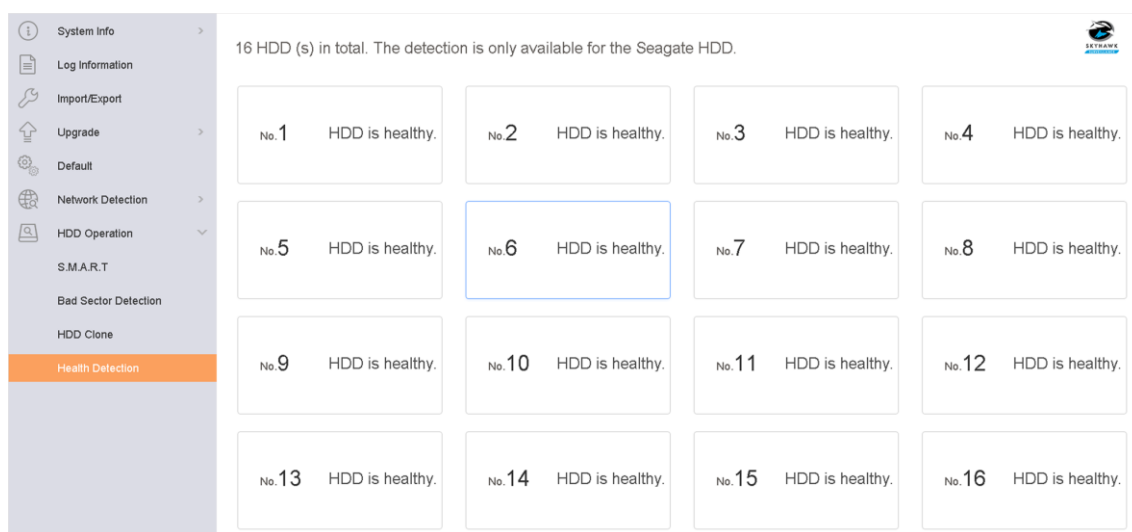


Figure 16-8 Health Detection

2. Click a HDD to view details.

16.6.4 Configure Disk Clone

Select the HDDs to clone to the eSATA HDD.

Before You Start

Connect an eSATA disk to the device.

Steps

1. Go to **Maintenance** → **HDD Operation** → **HDD Clone**.

Network Video Recorder User Manual

Clone Source

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

Clone Destination

eSATA

Capacity

Refresh

Clone

Figure 16-9 HDD Clone

2. Check the HDD to clone. The capacity of the selected HDD must match the capacity of the clone destination.
3. Click **Clone**.
4. Click **Yes** on the pop up message box to create the clone.

16.6.5 Repair Database

Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Steps

1. Go to **Storage** → **Storage Device**.
2. Select the drive.
3. Click **Repair Database**.
4. Click **Yes**.



Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.

You can see the repairing progress at **Status**.

Network Video Recorder User Manual

+ Add		Init	Repair Database				Total Capacity 3726.03GB		Free Space 3148.00GB	
	Label	Capacity	Status	Property	Type	Free Space	Group	Edit	Delete	
	8	3726.03GB	Repairing 73%	R/W	Local	3148.00GB	1	—	×	

Figure 16-10 Repair Database

16.7 Upgrade Device

Your device firmware can be upgraded with a local backup device or remote FTP server.

16.7.1 Upgrade by Local Backup Device

Before You Start

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

Steps

1. Go to **Maintenance** → **Upgrade**.
2. Click **Local Upgrade** to enter the local upgrade interface.

Device Name:
File Format:

File Name	File Size	File Type	Edit Date	Delete	Play

Figure 16-11 Local Upgrade

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

16.7.2 Upgrade by FTP

Before You Start

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

Steps

1. Go to **Maintenance** → **Upgrade**.
2. Click **FTP** to enter the local upgrade interface.



Figure 16-12 FTP Upgrade

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

16.7.3 Upgrade by Hik-Connect

After logging the device into Hik-Connect, the device would periodically check for the latest firmware from Hik-Connect. If an upgrade firmware is available, the device will notify you when you log in. You can also manually check for the latest firmware.

Before You Start

Ensure the device has successfully connected to Hik-Connect, and it requires to install at least one read-write HDD for firmware downloading.

Steps

1. Go to **Maintenance** → **Upgrade** → **Online Upgrade**.
2. Click **Check Upgrade** to manually check and download the latest firmware from Hik-Connect.

Note

The device will automatically check for the latest firmware every 24 hours. If it detects available upgrade firmware, the device will notify you when you log in.

3. Optional: You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.
4. Click **Upgrade Now**.

16.8 Import/Export Device Configuration Files

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

Before You Start

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

Network Video Recorder User Manual

contain the file.

Steps

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

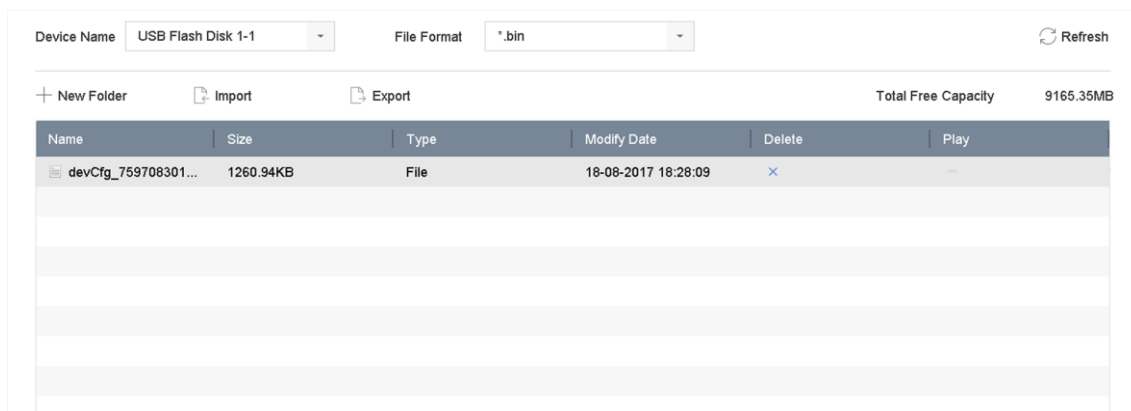


Figure 16-13 Import/Export Configuration File

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

Note

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

16.9 Log Management

16.9.1 Log Storage

You can customize the log storage disk and log storage period.

Steps

1. Go to **Storage** → **Advanced**.

Log Storage Mode: Custom

Log Storage Period: 90 Day

Log Disk/Array No.: 2

Apply

Figure 16-14 Log Storage

2. Set **Log Storage Mode**.

System Default

Each disk will allocate a certain space to store logs. Old logs will be overwritten when the space is full.

Custom

You can set **Log Storage Period** or allocate **Log Disk** for log storage. When logs exceed the period, the historical logs cannot be searched.

3. Click **Apply**.

16.9.2 Search & Export Log Files

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

Steps

1. Go to **Maintenance** → **Log Info**.

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

Major Type: All

Minor Type: ☒ Select All

Search

Export ALL

Figure 16-15 Log Search Interface

2. Set the log search conditions, including the time, major type and minor type.

3. Click **Search** to start searching the log files.

4. The matched log files will be displayed on the list, as shown below.

Network Video Recorder User Manual

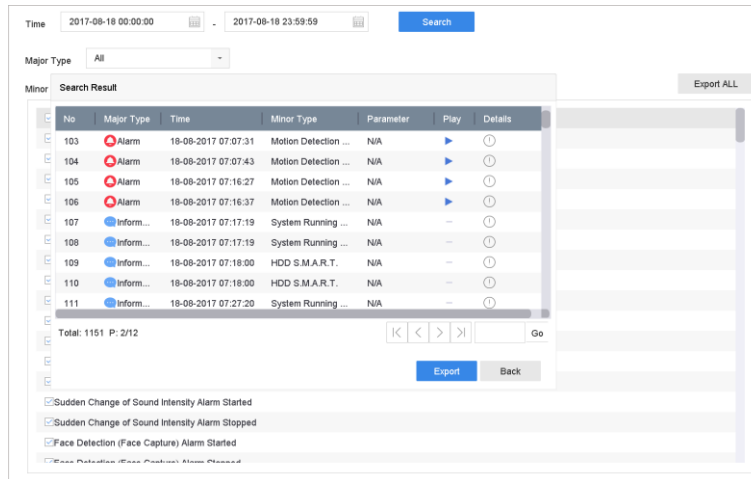


Figure 16-16 Log Search Results



Note

Up to 2,000 log files can be displayed each time.

5. Related Operation:



Click or double-click it to view detailed information.



Click it to view the related video file.

Export/Export ALL

Click it to export all the system logs to the storage device.

16.9.3 Upload Logs to the Server

You can upload system logs to the server for backup.

Steps

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

Figure 16-17 Log Server Settings

2. Check **Enable**

3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. Optional: Click **Test** to test if parameters are valid.
5. Click **Apply**.

16.9.4 One-Way Authentication

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

Before You Start

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

Steps

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

The screenshot displays the 'Log Server Configuration' web interface. At the top, there is a checkbox labeled 'Enable' which is checked. Below this are three input fields: 'Log Server Address' (containing '192.168.1.100'), 'Log Server Port' (containing '8080'), and 'Upload Time Interval (h)' (containing '1'). A 'Test' button is positioned below these fields. The 'Client Certificate' section includes three buttons: 'Create' (with the text 'No file.' next to it), 'Download', and 'Delete'. Below this is an 'Install Generated Certificate' section with a file input field and 'Browse' and 'Install' buttons. The 'CA Certificate' section has an 'Install' label, a file input field, and 'Browse' and 'Install' buttons. At the bottom of the form is a large red 'Save' button with a floppy disk icon.

Figure 16-18 One-Way Authentication

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

16.9.5 Two-Way Authentication

You can install a CA certificate (from the server) to your device to authorize the server, and create a certificate (from your device) to authorize your device by the server. This would improve the log

Network Video Recorder User Manual

communication security. Two-way authentication can be configured via web browser.

Before You Start

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

Steps

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

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

Figure 16-19 Two-Way Authentication

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

16.10 Restore Default Settings

Steps

1. Go to **Maintenance** → **Default**.

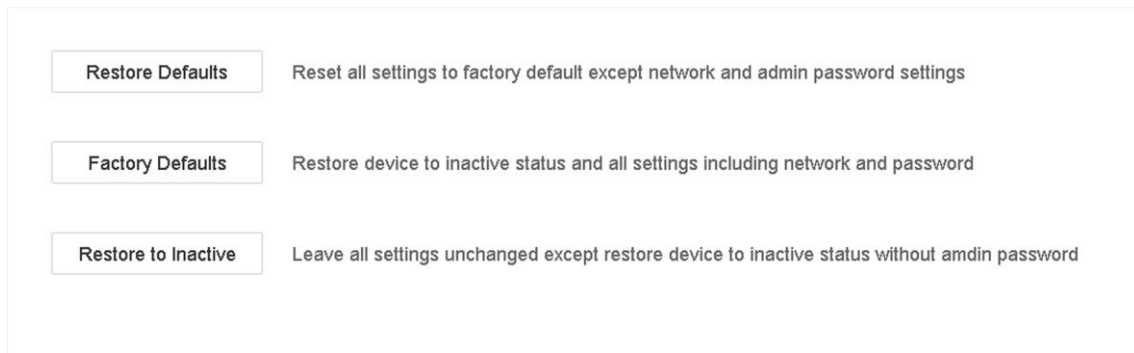


Figure 16-20 Restore Default Settings

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

Restore Defaults

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

Factory Defaults

Restore all parameters to the factory default settings.

Restore to Inactive

Restore the recorder to inactive status.



Note

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

16.11 Schedule Reboot

The device will automatically restart according to the schedule.

Steps

1. Go to **Maintenance** → **System Service** → **System Service** → **Schedule Reboot**.
2. Check **Enable**.
3. Set the reboot schedule.
4. Click **Apply**.

16.12 Security Management

16.12.1 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the

permission to connect other devices via ONVIF protocol.

Steps

1. Go to **Maintenance** → **System Service** → **ONVIF**.
2. Check **Enable ONVIF** to enable the ONVIF access management.

Note

ONVIF protocol is disabled by default.

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

Caution

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

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

16.12.2 IP/MAC Address Filter

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

Steps

1. Go to **Maintenance** → **System Service** → **Address Filter**.

Enable ☐

Restriction Mode ☒ IP Address ☐ MAC Address

Restriction Type ☐ Allow ☒ Forbid

Restriction List + Add Edit Delete

☐	No.	IP Address

Figure 16-21 Address Filter

2. Check **Enable**.
3. Select **Restriction Mode**. Choose to filter by IP address or MAC Address.
4. Select **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 **Apply** to save the settings.

16.12.3 RTSP Authentication

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

Steps

1. Go to **System** → **System Service** → **System Service**.

Enable RTSP ☒

RTSP Authentication Type digest

Figure 16-22 RTSP Authentication

2. Select **RTSP Authentication Type**.

Note

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

3. Click **Apply**.
4. Restart the device to take effect the settings.

16.12.4 RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP protocol, it is an algorithm for digest authentication of the user authentication. You can configure RTSP digest algorithm via web browser.

Go to **Configuration** → **System** → **Security** → **Authentication** via web browser to select the required RTSP digest algorithm type.

16.12.5 ISAPI Service

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

Steps

1. Go to **System** → **System Service** → **System Service**.
2. Check **Enable ISAPI**.
3. Click **Apply**.
4. Restart the device to take effect the settings.

16.12.6 HTTP Authentication

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

Steps

1. Go to **Maintenance** → **System Service** → **System Service**.



Enable HTTP ☒

HTTP Authentication Type digest

Figure 16-23 HTTP Authentication

2. Check **Enable HTTP**.
3. Select **HTTP Authentication Type**.

Note

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

4. Click **Apply** to save the settings.
5. Restart the device to take effect the settings.

16.12.7 HTTP/Web Digest Algorithm

HTTP/Web digest algorithm is based on HTTP protocol, it is an algorithm for digest authentication

of the user authentication. You can configure HTTP/web digest algorithm via web browser. Go to **Configuration** → **System** → **Security** → **Authentication** via web browser to select the required digest algorithm type.

16.12.8 Picture URL Digest Authentication

When using HTTP protocol to download the pictures which are uploaded by SDK, picture URL digest authentication controls whether the picture download process requires digest authentication or not. You can configure picture URL digest authentication via web browser. Go to **Configuration** → **System** → **Security** → **Security Service** via web browser to enable/disable picture URL digest authentication.

16.12.9 Serial Port Authentication Service

Serial port can be used to capture device information and control the device. Serial port authentication service provides the authentication for the serial port usage. Go to **Configuration** → **System** → **Security** → **Security Service** via web browser to enable/disable serial port authentication service.

Service Close Time

The serial port authentication service will be closed for a specific period. For example, if **Service Close Time** is set as **30**, the serial port authentication service will be closed for 30 days. And after 30 days, serial port authentication service will be enabled.

Chapter 17 Appendix

17.1 Glossary

Dual-Stream

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

DVR

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

HDD

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

DHCP

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

HTTP

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

PPPoE

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

DDNS

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

Hybrid DVR

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

NTP

Network Video Recorder User Manual

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.

17.2 Frequently Asked Questions

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

Reason

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

Solution

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



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.

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

Reason

The camera encoding format mismatches with the video recorder.

Solution

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

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

Reason

The camera password is too weak.

Solution

Change the camera password.

Warning

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

17.2.4 How to improve the playback image quality?

Reason

Recording parameter settings are inappropriate.

Solution

Go to **Camera** → **Video Parameters**. Increase resolution and max. bitrate, and try again.

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

video?

Solution

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

17.2.6 Why is the timeline at playback not constant?

Reason

1. When the video recorder is using event recording, it only records video when event occurs. Hence the video may not be continuous.
2. Exception occurs, such as the device offline, HDD error, record exception, network camera offline, etc.

Solution

1. Ensure the recording type is continuous recording.
2. Go to **Maintenance** → **Log Information**. Search the log file during the video time period. See if there are unexpected events, such as HDD error, record exception, etc.

17.2.7 Why is the video recorder notifying the network is unreachable when a network camera is being added?

Reason

1. The IP address or port of network camera is incorrect.
2. The network between video recorder and camera is disconnected.

Solution

1. Go to **Camera** → **Camera** → **IP Camera**. Click  of the selected camera, and edit its IP address and port. Ensure the video recorder and camera is using the same port.
2. Go to **Maintenance** → **Network** → **Detection**. Enter the IP address of network camera in **Destination Address**, and click **Test** to see if the network is reachable.

17.2.8 Why is the IP address of network camera being changed automatically?

Reason

When network camera and video recorder are using the same switch but in different subnets, the video recorder will change the IP address of network camera to the same subnet as itself.

Solution

When adding camera, click **Custom Add** to add camera.

17.2.9 Why is the video recorder notifying IP conflict?**Reason**

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

Solution

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

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

HDD read/write exception.

Solution

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

17.2.11 Why does my video recorder make a beeping sound after booting?**Reason**

1. The front panel is not fastened (for the device which its front panel is removable).
2. HDD error, or do not have HDD.

Solution

1. If it makes continuous beeps, and your device's front panel is removable, ensure the front panel is fastened.
2. If it makes non-continuous beeps (3 long, 2 short), take HDD error as an example, check if the device has installed HDD. If not, you can go to **System** → **Event** → **Normal Event** → **Exception**, and uncheck **Event Hint Configuration** to disable HDD error event hint.
Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.
Check if the HDD is broken. You can change it, and try again.

17.2.12 Why is there no recorded video after the motion detection is

set?

Reason

1. The recording schedule is incorrect.
2. The motion detection event setting is incorrect.
3. HDD exception.

Solution

1. The recording schedule is setup correctly by following the steps listed in Configuring Record/Capture Schedule.
2. The motion detection area is configured correctly. The channels are being triggered for motion detection (See Configuring Motion Detection).
3. Check if the device has installed HDD.
Check if the HDD is initialized. If not, go to Storage > Storage Device to initialize the HDD.
Check if the HDD is broken. You can change it, and try again.

17.2.13 Why is the video sound quality not good?

Reason

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

Solution

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

