Network Video Recorder

User Manual

User Manual

About this Manual

This Manual is applicable to Network Video Recorder (NVR).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND OUR COMPANY MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL OUR COMPANY, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF OUR COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

Regulatory Information

FCC Information

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

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

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

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

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

Industry Canada ICES-003 Compliance

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

Symbol Conventions

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

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

Safety Instructions

- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
- Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100~240 VAC, 48 VDC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
- Please make sure that the plug is firmly connected to the power socket.
- 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.

Preventive and Cautionary Tips

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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.

- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- When installing the device into a cabinet over 2U height, it is suggested to use rack shelf to bear the weight. If the cabinet height is over 4U, it is suggest to use slide rails or rack shelf to bear the weight.

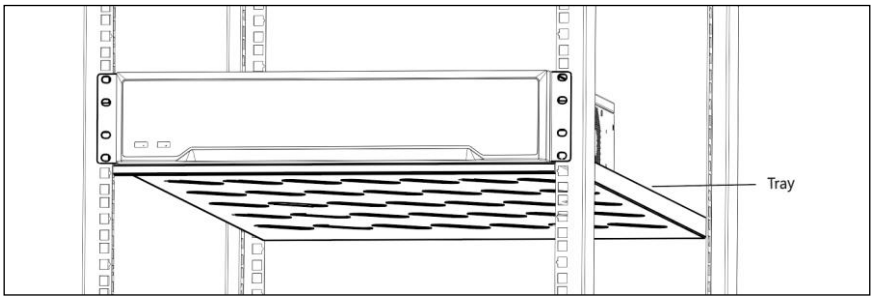


TABLE OF CONTENTS

Chapter 1 Introduction 13
1.1 Front Panel 13
1.2 IR Remote Control Operations 28
1.3 USB Mouse Operation 32
1.4 Rear Panel 33
Chapter 2 Getting Started 38
2.1 Start up the Device 38
2.2 Activate the Device 38
2.3 Configure Login Unlock Pattern 40
2.4 Login to the Device 41
2.4.1 Log in via Unlock Pattern 41
2.4.2 Log in via a Password 43
2.5 Start Setup Wizard 44
2.6 Enter Main Menu 47
2.7 System Operation 49
2.7.1 Log out 49
2.7.2 Shut Down the Device 49
2.7.3 Reboot the Device 49
Chapter 3 Camera Management 51
3.1 Add IP Cameras 51
3.1.1 Add IP Cameras Manually 51
3.1.2 Add the Automatically Searched Online IP Cameras 52
3.2 Manage Cameras for PoE Device 53
3.2.1 Add PoE Cameras 53
3.2.2 Add Non-PoE IP Cameras 53
3.2.3 Configure PoE Interface 54
3.3 Enable the H.265 Stream Access 55
3.4 Upgrade the IP Camera 56
3.5 Configure the Customized Protocols 56
Chapter 4 IoT 58
4.1 Add IoT Device 58
4.1.1 Add Access Control Device 58

4.1.2 Add Alarm Device 60
4.2 Configure Linkage Action and Arming Schedule 61
4.3 Configure OSD 62
4.4 Search IoT Record 63
4.5 IoT Video/Picture 64
4.5.1 Configure Event Recording/Capturing 65
4.5.2 Search IoT Video/Picture 66
Chapter 5 Camera Settings 68
5.1 Configure OSD Settings 68
5.2 Configure Privacy Mask 69
5.3 Configure the Image Parameters 70
5.4 Configure the Day/Night Switch 70
5.5 Configure IP Camera Time Sync 70
5.6 Configure Other Camera Parameters 71
Chapter 6 Live View 72
6.1 Start Live View 72
6.1.1 Digital Zoom 72
6.1.2 Fisheye View 72
6.1.3 3D Positioning 73
6.1.4 Live View Strategy 74
6.1.5 Switch Main/Auxiliary Port 74
6.2 Target Detection 74
6.3 Configure Live View Settings 75
6.4 Configure Live View Layout 76
6.4.1 Configure Custom Live View Layout 76
6.4.2 Configure Live View Mode 77
6.5 Configure Camera Auto-Switch 78
6.6 Configure Channel-Zero Encoding 78
Chapter 7 PTZ Control 80
7.1 PTZ Control Wizard 80
7.2 ConfigurePTZ Parameters 80
7.3 Set PTZ Presets, Patrols & Patterns 81
7.3.1 Set a Preset 81
7.3.2 Call a Preset 82
7.3.3 Set a Patrol 83

7.3.4 Call a Patrol 84
7.3.5 Set a Pattern 85
7.3.6 Call a Pattern 86
7.3.7 Set Linear Scan Limits 86
7.3.8 Call Linear Scan 87
7.3.9 One-touch Park 87
7.4 Auxiliary Functions 88
Chapter 8 Storage 89
8.1 Storage Device Management 89
8.1.1 Install the HDD 89
8.1.2 Add the Network Disks 89
8.1.3 Configure eSATA for Data Storage 91
8.1.4 Configure eSATA for Auto Backup 92
8.2 Storage Mode 93
8.2.1 Configure HDD Groups 93
8.2.2 Configure HDD Quota 95
8.3 Recording Parameters 97
8.3.1 Main Stream 97
8.3.2 Sub-Stream 97
8.3.3 Picture 97
8.3.4 ANR 98
8.3.5 Configure Advanced Recording Settings 98
8.4 Configure Recording Schedule 99
8.5 Configure Continuous Recording 101
8.6 Configure Motion Detection Triggered Recording 101
8.7 Configure Event Triggered Recording 101
8.8 Configure Alarm Triggered Recording 102
8.9 Configure POS Event Triggered Recording 102
8.10 Configure Picture Capture 103
8.11 Configure Holiday Recording and Capture 103
8.12 Configure Redundant Recording and Capture 105
Chapter 9 Disk Array (RAID) 107
9.1 Create a Disk Array 107
9.1.1 Enable a RAID 107
9.1.2 One-Touch Creation 108

9.1.3 Manual Creation....108
9.2 Rebuild an Array....110
9.2.1 Configure a Hot Spare Disk....110
9.2.2 Automatically Rebuild an Array....110
9.2.3 Manually Rebuild an Array....111
9.3 Delete an Array....112
9.4 Check and Edit Firmware....113
Chapter 10 File Management....114
10.1 Search and Export All Files....114
10.1.1 Search Files....114
10.1.2 Export Files....114
10.2 Search and Export Human Files....115
10.2.1 Search Human Files....115
10.2.2 Export Human Files....115
10.3 Search and Export Vehicle Files....115
10.3.1 Search Vehicle Files....115
10.3.2 Export Vehicle Files....116
10.4 Search History Operation....117
10.4.1 Save Search Conditions....117
10.4.2 Call Search History....117
Chapter 11 Playback....118
11.1 Play Video Files....118
11.1.1 Instant Playback....118
11.1.2 Play Normal Video....118
11.1.3 Play Smart Searched Video....119
11.1.4 Play Custom Searched Files....120
11.1.5 Play Tag Files....121
11.1.6 Play Event Files....123
11.1.7 Play Video Synopsis....125
11.1.8 Play by Sub-periods....125
11.1.9 Play Log Files....126
11.1.10 Play External Files....127
11.2 Playback Operations....127
11.2.1 Set Play Strategy in Smart/Custom Mode....127
11.2.2 Edit Video Clips....128

11.2.3 Switch between Main Stream and Sub-Stream 128
11.2.4 Thumbnails View 129
11.2.5 Fisheye View 129
11.2.6 Fast View 130
11.2.7 Digital Zoom 130
11.2.8 POS Information Overlay 131
Chapter 12 Event and Alarm Settings 132
12.1 Configure Arming Schedule 132
12.2 Configure Alarm Linkage Actions 132
12.3 Configure Motion Detection Alarms 134
12.4 Configure Video Loss Alarms 137
12.5 Configure Video Tampering Alarms 139
12.6 Configure Sensor Alarms 140
12.6.1 Configure Alarm Inputs 140
12.6.2 Configure One-Key Disarming 142
12.6.3 Configure Alarm Outputs 143
12.7 Configure Exceptions Alarms 145
12.8 Configure Combined Alarm 147
12.9 Setting Alarm Linkage Actions 148
12.9.1 Configure Auto-Switch Full Screen Monitoring 148
12.9.2 Configure Audio Warning 149
12.9.3 Notify Surveillance Center 149
12.9.4 Configure E-mail Linkage 149
12.9.5 Trigger Alarm Outputs 150
12.9.6 Configure PTZ Linkage 150
12.10 Trigger or Clear Alarm Output Manually 151
Chapter 13 VCA Event Alarm 152
13.1 Face Detection 152
13.2 Vehicle Detection 153
13.3 Line Crossing Detection 154
13.4 Intrusion Detection 156
13.5 Region Entrance Detection 157
13.6 Region Exiting Detection 158
13.7 Loitering Detection 159
13.8 People Gathering Detection 161

13.9 Fast Moving Detection 162
13.10 Parking Detection 163
13.11 Unattended Baggage Detection 164
13.12 Object Removal Detection 165
13.13 Audio Exception Detection 166
13.14 Sudden Scene Change Detection 168
13.15 Defocus Detection 169
13.16 PIR Alarm 169
13.17 Thermal Camera Detection 171
13.18 Queue Management 171
Chapter 14 Smart Analysis 172
14.1 People Counting 172
14.2 Heat Map 172
Chapter 15 POS Configuration 174
15.1 Configure POS Settings 174
15.1.1 Configure POS Connection 174
15.1.2 Configure POS Text Overlay 178
15.2 Configure POS Alarm 179
Chapter 16 Network Settings 180
16.1 Configure TCP/IP Settings 180
16.1.1 Device with Dual Network Interface 180
16.1.2 Device with a Single Network Interface 181
16.2 Configure Guarding Vision 181
16.3 Configure EHome 182
16.4 Configure DDNS 184
16.5 Configure PPPoE 185
16.6 Configure NTP 185
16.7 Configure SNMP 186
16.8 Configure Email 187
16.9 Configuring NAT 188
16.10 Configure Ports 190
Chapter 17 Hot Spare Device Backup 192
17.1 Set Hot Spare Device 192
17.2 Set Working Device 193

17.3 Manage Hot Spare System 193
Chapter 18 User Management and Security 195
18.1 Manage User Accounts 195
18.1.1 Add a User 195
18.1.2 Edit the Admin User 197
18.1.3 Edit an Operator/Guest User 198
18.1.4 Delete a User 199
18.2 Manage User Permissions 199
18.2.1 Set User Permissions 199
18.2.2 Set Local Live View Permission for Non-Admin Users 201
18.2.3 Set Live View Permission on Lock Screen 202
18.2.4 Set Double Verification Permission for Non-Admin Users 203
18.3 Configure Password Security 204
18.3.1 Export GUID File 204
18.3.2 Configure Security Questions 205
18.3.3 Configure Reserved Email 206
18.4 Reset Password 207
18.4.1 Reset Password by GUID 207
18.4.2 Reset Password by Security Questions 208
18.4.3 Reset Password by Reserved Email 208
Chapter 19 System Service Maintenance 210
19.1 Storage Device Maintenance 210
19.1.1 Configure Disk Clone 210
19.1.2 S.M.A.R.T. Detection 211
19.1.3 Bad Sector Detection 212
19.1.4 HDD Health Detection 213
19.1.5 Repair Database 214
19.2 Search and Export Log Files 214
19.2.1 Search the Log Files 214
19.2.2 Export the Log Files 216
19.3 Import/Export IP Camera Configuration Files 217
19.4 Import/Export Device Configuration Files 219
19.5 Configure System Services 219
19.5.1 Network Security Settings 219
19.5.2 Manage ONVIF User Accounts 223

19.5.3 Configure Stream Encryption 224
19.6 Configure Stream Encryption 225
19.7 Upgrade the System 226
19.7.1 Upgrade with a Local Backup Device 226
19.7.2 Upgrade by FTP 226
19.7.3 Upgrade by Guarding Vision 227
19.8 Restore Default Settings 228
Chapter 20 General System Settings 229
20.1 Configure General Settings 229
20.2 Configure Date & Time 230
20.3 Configure DST Settings 231
Chapter 21 Appendix 232
21.1 Glossary 232
21.2 Troubleshooting 233

Chapter 1 Introduction

1.1 Front Panel

Front Panel 1:

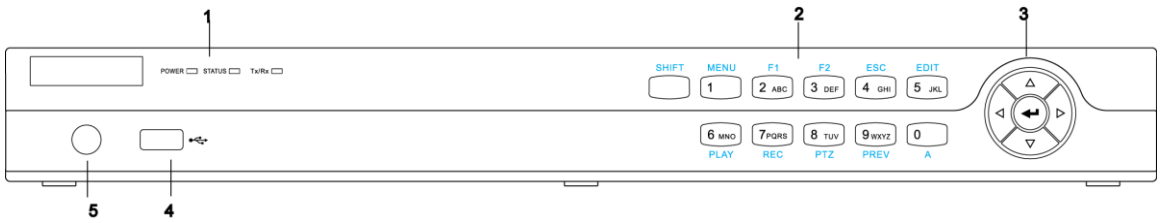


Figure 1-1 Front Panel

Table 1-1 Description of Front Panel

No.	Name		Function Description
1	**POWER**		Turns yellow when the device s running.
	STATUS		Flickers red when data is being read from or written to HDD, and turns yellow when the SHIFT function is realized.
	Tx/Rx		Flickers yellow when network connection is functioning properly.
2	**Composite Keys**	**SHIFT**	Switches between the numeric or letter input and functions of the composite keys.
		1/MENU	Enters numeral “1”; Accesses the main menu interface.
		2/ABC/F1	Enters numeral “2”;
			Enters letters “ABC”;
			Uses the F1 button to select all items in a list field;
			Turns on/off PTZ light in PTZ Control mode, and use it to zoom out the image;

No.	Name		Function Description
			Switches between main and spot video output in live view or playback mode.
		3/DEF/F2	Enters numeral “3”;
			Enters letters “DEF”;
			Uses the F2 button to change the tab pages;
			Zooms in the image in PTZ control mode.
		4/GHI/ESC	Enters numeral “4”;
			Enters letters “GHI”;
			Exits and back to the previous menu.
		5/JKL/EDIT	Enters numeral “5”;
			Enters letters “JKL”;
			Deletes characters before cursor;
			Checks the checkbox and select the ON/OFF switch;
			Starts/stops record clipping in playback.
		6/MNO/PLAY	Enters numeral “6”;
			Enters letters “MNO”;
			Accesses to playback interface in Playback mode.
		7/PQRS/REC	Enters numeral “7”;
			Enters letters “PQRS”;
			Accesses to manual record interface; Manually enables/disables record.
			Enters numeral “8”;

No.	Name		Function Description
		8/TUV/PTZ	Enters letters “TUV”;
			Accesses PTZ control interface.
		9/WXYZ/PREV	Enters numeral “9”;
			Enters letters “WXYZ”;
			Multi-channel display in live view.
		0/A	Enters numeral “0”;
			Shifts the input methods in the editing text field. (Upper and lowercase, alphabet, symbols or numeric input).
3	**DIRECTION**		Navigates between different fields and items in menus.
			Uses the Up and Down buttons to speed up and slow down the playing of video files in Playback mode. The Left and Right button will select the next and previous record files.
			Cycles through channels in Live View mode.
			Controls the movement of the PTZ camera in PTZ control mode.
	ENTER		Confirms selection in any of the menu modes.
			Checks the checkbox.
			Plays or pauses the playing of video files in Playback mode.
			Advances the video by a single frame in single-frame Playback mode.
			Stops/starts auto switch in Auto-switch mode.
4	**USB Interface**		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
5	**IR Receiver**		Receiver for IR remote control.

Front Panel 2:

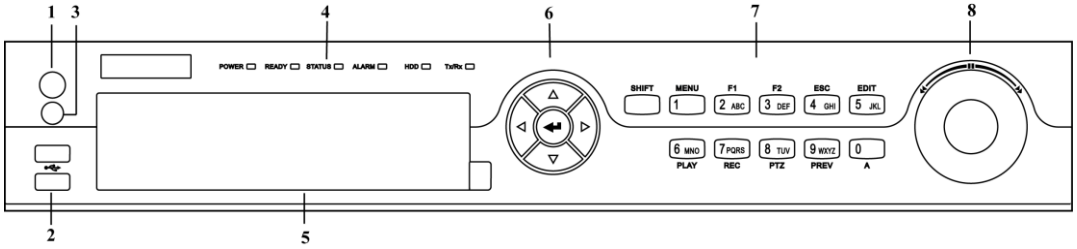


Figure 1-2 Front Panel

Table 1-2 Description of Front Panel

No.	Name	Function Description
1	**POWER ON/OFF**	Power on/off switch.
2	**USB Interface**	Connect to USB mouse or USB flash memory.
3	**IR Receiver**	Receiver for IR remote control. devices.
4	**POWER**	Power indicator lights in green when DVR is powered up.
	READY	Ready indicator is normally green, indicating that the DVR is functioning properly.
	STATUS	Indicator turns green when DVR is controlled by an IR remote control with the address from 1~254; Indicator turns red when the SHIFT button is used; Indicator does not light when the DVR is controlled by a keyboard or by the IR remote control with the address of 255; Indicator turns green when the DVR is controlled by IR remote control (with the address from 1~254) and keyboard at the same time , and the SHIFT button is not used; Indicator turns orange : (a) when the DVR is controlled by IR remote control (with the address from 1~254) and keyboard at the same time and the SHIFT button is used as well; (b) when the DVR is controlled by IR remote control (with the address from 1~254) and the SHIFT button is used.
	ALARM	Alarm indicator turns red when a sensor alarm is detected.
	HDD	HDD indicator blinks in red when data is being read from or written to HDD.
	Tx/Rx	TX/RX indictor blinks in green when network connection is

		functioning properly.
5	**DVD-ROM**	Slot for DVD-ROM.
6	**DIRECTION**	The DIRECTION buttons are used to navigate between different fields and items in menus. In Playback mode, the Up and Down button is used to speed up and slow down recorded video. In All-day Playback mode, the Left/Right button can be used to select the recorded video of next/previous day; in Playback by Normal Video Search, the Left/Right button can be used to select the next/previous recorded file. In Live View mode, the directional buttons can be used to cycle through channels. In PTZ control mode, it can control the movement of the PTZ camera.
	ENTER	Confirm selection in any of the menu modes. It can also be used to tick checkbox fields. In Playback mode, it can be used to play or pause the video. In Single-frame Playback mode, pressing the ENTER button will advance the video by a single frame. In Auto-switch mode, it can be used to stop /start auto switch.
7	**SHIFT**	Switch of compound keys between the numeric/letter input and functional control.
	1/MENU	Enter numeral “1”; Access the main menu interface.
	2ABC/F1	Enter numeral “2”; Enter letters “ABC”; The F1 button can be used to select all items on the list; In PTZ Control mode, the F1 button can be used to zoom out (zoom-) the PTZ camera; In live view or playback mode, the F1 button can be used to switch between main and spot video output.
	3DEF/F2	Enter numeral “3”; Enter letters “DEF”; In PTZ Control mode, the F1 button can be used to zoom in (zoom+) the PTZ camera; The F2 button can be used to cycle through tab pages.

	4GHI/ESC	Enter numeral “4”; Enter letters “GHI”; Exit and back to the previous menu.
	5JKL/EDIT	Enter numeral “5”; Enter letters “JKL”; Delete characters before cursor; Select the checkbox and ON/OFF switch; Start/stop record clipping in playback.
	6MNO/PLAY	Enter numeral “6”; Enter letters “MNO”; In Playback mode, it is used for direct access to playback interface.
	7PQRS/REC	Enter numeral “7”; Enter letters “PQRS”; Manual record, for direct access to manual record interface; manually enable/disable record.
	8TUV/PTZ	Enter numeral “8”; Enter letters “TUV”; Access PTZ control interface.
	9WXYZ/PREV	Enter numeral “9”; Enter letters “WXYZ”; Multi-camera display in live view; In Playback mode or Menu→Playback→Tag playback interface, this button can be used to delete the selected tag.
	0/A	Enter numeral “0”; Switch between input methods (upper and lowercase alphabet, symbols and numeric input). In Playback mode, this button can be used to add the default tag.
8	**JOG SHUTTLE Control**	Move the active selection in a menu. The inner ring will move the selection up and down; the outer ring will move it left and right. In Playback mode, the inner ring is used to jump 30s forward/backward in video files. The outer ring can be used to

		speed up/slow down the video. In Live View mode, it can be used to cycle through different channels. In PTZ control mode, in can control the movement of the PTZ camera.

Front Panel 3:

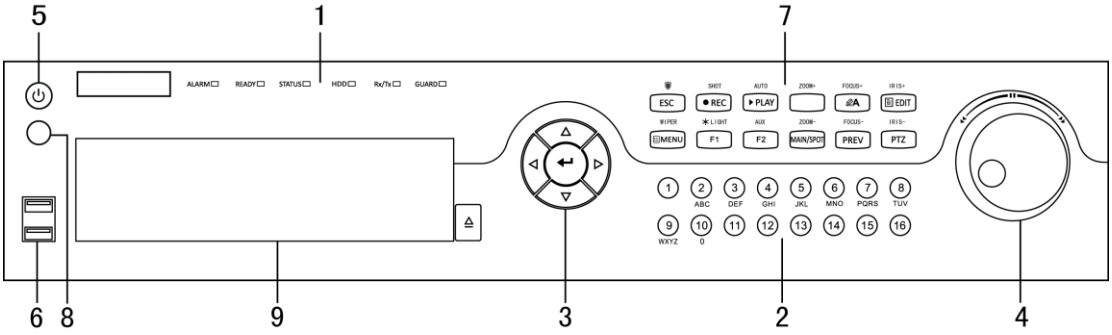


Figure 1-3 Front Panel

Table 1-3 Description of Front Panel

No.	Name		Function Description
1	**Status Indicators**	**ALARM**	Alarm indicator turns red when a sensor alarm is detected.
		READY	Turs blue when the device is functioning properly.
		STATUS	Indicator turns blue when the device is controlled by an IR remote. Indicator turns red when controlled by a keyboard and orange when IR remote and keyboard is used at the same time. Indicator does not light when the device is controlled by the IR remote control with the address of 255.
		HDD	HDD indicator blinks in red when data is being read from or written to HDD.
		TX/RX	TX/RX indictor blinks in blue when network connection is functioning properly.

No.	Name		Function Description
		GUARD	Indicator turns blue when the device is armed; Indicator does not light when the device is disarmed; The arm/disarm state can be initiated by pressing and holding on the ESC button for more than 3 seconds in live view mode.
2	**Alphanumeric Buttons**		Switch to the corresponding channel in Live view or PTZ Control mode.
			Input numbers and characters in Edit mode.
			Switch between different channels in Playback mode.
			The light of the button is blue when the corresponding channel is recording; it is red when the channel is in network transmission status; it is pink when the channel is recording and transmitting.
3	**Control Buttons**	**DIRECTION**	The DIRECTION buttons are used to navigate between different fields and items in menus.
			In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
			In Live View mode, these buttons can be used to cycle through channels.
			In PTZ control mode, it can control the movement of the PTZ camera.
		ENTER	The ENTER button is used to confirm selection in any of the menu modes.
			It can also be used to tick checkbox fields.

No.	Name		Function Description
			In Playback mode, it can be used to play or pause the video.
			In single-frame Playback mode, pressing the button will advance the video by a single frame.
			In Auto-switch mode, it can be used to stop /start auto switch.
4	**JOG SHUTTLE Control**		Move the active selection in a menu. It will move the selection up and down.
			In Live View mode, it can be used to cycle through different channels.
			In the Playback mode: the outer ring is used to speed up or slow down the record files and the inner ring is used to jump 30s forward/backward in records files.
			In PTZ control mode, it can control the movement of the PTZ camera.
5	**POWER**		Power on/off switch.
6	**USB Interfaces**		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	**Composite Keys**	**ESC**	Exit and back to the previous menu.
			Arm/disarm the device in live view mode.
		REC/SHOT	Enter the Manual Record setting menu.
			In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
			It is also used to turn audio on/off in the Playback mode.

No.	Name		Function Description
		PLAY/AUTO	Enter the Playback menu;
			Auto scan in the PTZ Control mode.
		ZOOM+	Zoom in the PTZ camera in the PTZ Control setting.
		A/FOCUS+	Adjust focus in the PTZ Control menu.
			It is also used to switch between input methods (upper and lowercase alphabet, symbols and numeric input).
		EDIT/IRIS+	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor.
			On checkbox fields, pressing the button will tick the checkbox.
			In PTZ Control mode, the button adjusts the iris of the camera.
			In Playback mode, it can be used to generate video clips for backup.
			Enter/exit the folder of USB device and eSATA HDD.
		MAIN/SPOT/ ZOOM-	Switch between main and spot output.
			In PTZ Control mode, it can be used to zoom out the image.
		F1/ LIGHT	Select all items on the list when used in a list field.
			In PTZ Control mode, it will turn on/off PTZ light (if applicable).

No.	Name		Function Description
			In Playback mode, it is used to switch between play and reverse play.
		F2/ AUX	Cycle through tab pages.
			In synchronous playback mode, it is used to switch between channels.
		MENU/WIPER	Press the button will help you return to the Main menu (after successful login).
			Press and hold the button for 5 seconds will turn off audible key beep.
			In PTZ Control mode, the MENU/WIPER button will start wiper (if applicable).
			In Playback mode, it is used to show/hide the control interface.
		PREV/FOCUS-	Switch between single screen and multi-screen mode.
			In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
		PTZ/IRIS-	Enter the PTZ Control mode.
			In the PTZ Control mode, it is used to adjust the iris of the PTZ camera.
8	**IR Receiver**		Receiver for IR remote control.
9	**DVD-R/W**		Slot for DVD-R/W.

Front Panel 4:

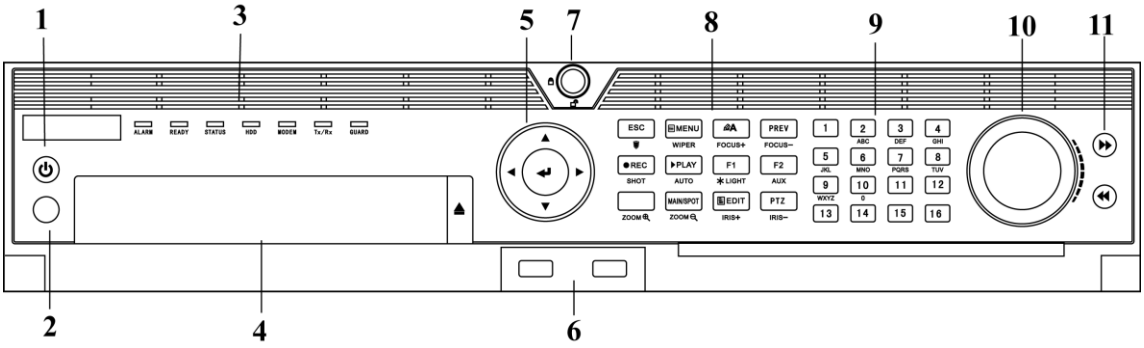


Figure 1-4 Front Panel

Table 1-4 Description of Front Panel

No.	Name		Function Description
1	**POWER ON/OFF**		Power on/off switch.
2	**IR Receiver**		Receiver for IR remote
3	**Status Indicators**	**ALARM**	Turns red when a sensor alarm is detected.
		READY	Ready LED is normally blue, indicating that the device is functioning properly.
		STATUS	Turns blue when device is controlled by an IR remote.
			Turns red when controlled by a keyboard and purple when IR remote and keyboard is used at the same time.
		HDD	Flashes red when data is being read from or written to HDD.
		MODEM	Reserved for future usage.
		TX/RX	Flashes blue when network connection is functioning properly.
		GUARD	Guard LED turns blue when the device is in armed status; at this time, an alarm is enabled when an event is detected.

No.	Name		Function Description
			The LED turns off when the device is unarmed. The arm/disarm status can be changed by pressing and holding on the ESC button for more than 3 seconds in live view mode.
4	**DVD-R/W**		Slot for DVD-R/W.
5	**Control Buttons**	**DIRECTION**	The DIRECTION buttons are used to navigate between different fields and items in menus.
			In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
			In Live View mode, these buttons can be used to cycle through channels.
			In PTZ control mode, it can control the movement of the PTZ camera.
		ENTER	The ENTER button is used to confirm selection in any of the menu modes.
			It can also be used to tick checkbox fields.
			In Playback mode, it can be used to play or pause the video.
			In single-frame Playback mode, pressing the button will advance the video by a single frame.
			In Auto-switch mode, it can be used to stop /start auto switch.
6	**USB Interfaces**		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	**Front Panel Lock**		You can lock or unlock the panel by the key.

No.	Name		Function Description
8	**Composite Keys**	**ESC**	Back to the previous menu.
			Press for Arming/disarming the device in Live View mode.
		REC/SHOT	Enter the Manual Record setting menu.
			In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
			It is also used to turn audio on/off in the Playback mode.
		PLAY/AUTO	The button is used to enter the Playback mode.
			It is also used to auto scan in the PTZ Control menu.
		ZOOM+	Zoom in the PTZ camera in the PTZ Control setting.
		A/FOCUS+	Adjust focus in the PTZ Control menu.
			It is also used to switch between input methods (upper and lowercase alphabet, symbols and numeric input).
		EDIT/IRIS+	Edit text fields. When editing text fields, it will also function as a Backspace button to delete the character in front of the cursor.
			On checkbox fields, pressing the button will tick the checkbox.
			In PTZ Control mode, the button adjusts the iris of the camera.
			In Playback mode, it can be used to generate video clips for backup.

No.	Name		Function Description
			Enter/exit the folder of USB device and eSATA HDD.
		MAIN/SPOT/ZOOM-	Switch between main and spot output.
			In PTZ Control mode, it can be used to zoom out the image.
		F1/ LIGHT	Select all items on the list when used in a list field.
			In PTZ Control mode, it will turn on/off PTZ light (if applicable).
			In Playback mode, it is used to switch between play and reverse play.
		F2/ AUX	Cycle through tab pages.
			In synchronous playback mode, it is used to switch between channels.
		MENU/WIPER	Press the button will help you return to the Main menu (after successful login).
			Press and hold the button for 5 seconds will turn off audible key beep.
			In PTZ Control mode, the MENU/WIPER button will start wiper (if applicable).
			In Playback mode, it is used to show/hide the control interface.
		PREV/FOCUS-	Switch between single screen and multi-screen mode.
			In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.
		PTZ/IRIS-	Enter the PTZ Control mode.

No.	Name	Function Description
		In the PTZ Control mode, it is used to adjust the iris of the PTZ camera.
9	**Alphanumeric Buttons**	Switch to the corresponding channel in Live view or PTZ Control mode.
		Input numbers and characters in Edit mode.
		Switch between different channels in Playback mode.
		The light of the button is blue when the corresponding channel is recording; it is red when the channel is in network transmission status; it is pink when the channel is recording and transmitting.
10	**JOG SHUTTLE Control**	Move the active selection in a menu. It will move the selection up and down.
		In Live View mode, it can be used to cycle through different channels.
		In the Playback mode: the ring is used to jump 30s forward/backward in video files.
		In PTZ control mode, it can control the movement of the PTZ camera.
11	**SLOW DOWN/SPEED UP**	Slow down/speed up in playback mode.

1.2 IR Remote Control Operations

The NVR may also be controlled with the included IR remote control.

NOTE

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

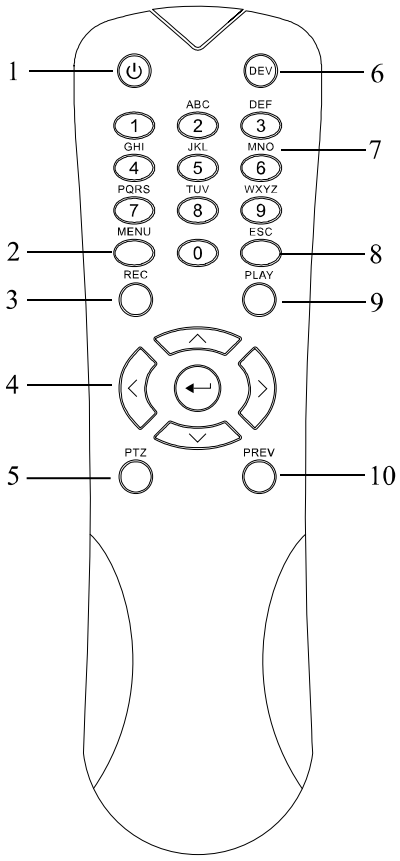


Figure 1-5 Remote Control

The keys on the remote control closely resemble the ones found on the front panel. Refer to Table 1-5, they include:

Table 1-5 Description of the IR Remote Control Buttons

No.	Name	Description
1	**POWER**	Power on/off the device.
		Power on/off the device by pressing and holding the button for 5 seconds.
2	**MENU Button**	Press the button to return to the main menu (after successful login).
		Press and hold the button for 5 seconds will turn off audible key beep.
		In PTZ Control mode, the MENU button will start wiper (if applicable).
		In Playback mode, it is used to show/hide the control interface.
		Enter the Manual Record setting menu.

No.	Name	Description
3	**REC Button**	In PTZ control settings, press the button and then you can call a PTZ preset by pressing Numeric button.
		It is also used to turn audio on/off in the Playback mode.
4	**DIRECTION Button**	Navigate between different fields and items in menus.
		In the Playback mode, the Up and Down button is used to speed up and slow down recorded video. The Left and Right button will select the next and previous record files.
		In Live View mode, these buttons can be used to cycle through channels.
		In PTZ control mode, it can control the movement of the PTZ camera.
	ENTER Button	Confirm selection in any of the menu modes.
		It can also be used to *tick* checkbox fields.
		In Playback mode, it can be used to play or pause the video.
		In single-frame Playback mode, pressing the button will advance the video by a single frame.
5	**PTZ Button**	In Auto-switch mode, it can be used to stop /start auto switch.
6	**DEV**	Enables/Disables Remote Control.
7	**Alphanumeric Buttons**	Switch to the corresponding channel in Live view or PTZ Control mode.
		Input numbers and characters in Edit mode.
		Switch between different channels in the Playback mode.
8	**ESC Button**	Back to the previous menu.
		Press for Arming/disarming the device in Live View mode.
		The button is used to enter the All-day Playback mode.

No.	Name	Description
9	**PLAY Button**	It is also used to auto scan in the PTZ Control menu.
10	**PREV Button**	Switch between single screen and multi-screen mode.
		In PTZ Control mode, it is used to adjust the focus in conjunction with the A/FOCUS+ button.

Troubleshooting Remote Control:

NOTE

Make sure you have installed batteries properly in the remote control. And you have to aim the remote control at the IR receiver on the front panel.

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

Step 1 Go to **Menu > Configuration > General > More Settings** by operating the front control panel or the mouse.

Step 2 Check and remember the NVR No. The default NVR No. is 255. This number valid for all IR remote controls.

Step 3 Press the DEV button on the remote control.

Step 4 Enter the NVR No. in step 2.

Step 5 Press the ENTER button on the remote.

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

Step 6 Batteries are installed correctly and the polarities of the batteries are not reversed.

Step 7 Batteries are fresh and not out of charge.

Step 8 IR receiver is not obstructed.

If the remote still cannot function properly, please change the remote and try again, or contact the device provider.

1.3 USB Mouse Operation

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

Step 1 Plug USB mouse into one of the USB interfaces on the front panel of the device.

Step 2 The mouse should automatically be detected. If in a rare case that the mouse is not detected, the possible reason may be that the two devices are not compatible, please refer to the recommended the device list from your provider.

The operation of the mouse:

Table 1-1 Description of the Mouse Control

Name	Action	Description
Left-Click	Single-Click	Live view: Select channel and show the quick set menu. Menu: Select and enter.
	Double-Click	Live view: Switch between single-screen and multi-screen.
	Click and Drag	PTZ control: pan, tilt and zoom. Video tampering, privacy mask and motion detection: Select target area. Digital zoom-in: Drag and select target area. Live view: Drag channel/time bar.
Right-Click	Single-Click	Live view: Show menu. Menu: Exit current menu to upper level menu.
Scroll-Wheel	Scrolling up	Live view: Previous screen. Menu: Previous item.
	Scrolling down	Live view: Next screen. Menu: Next item.

1.4 Rear Panel

NOTE

The rear panel vaires according to different models. Please refer to the actual product. The following figures are for reference only.

Rear Panel 1:

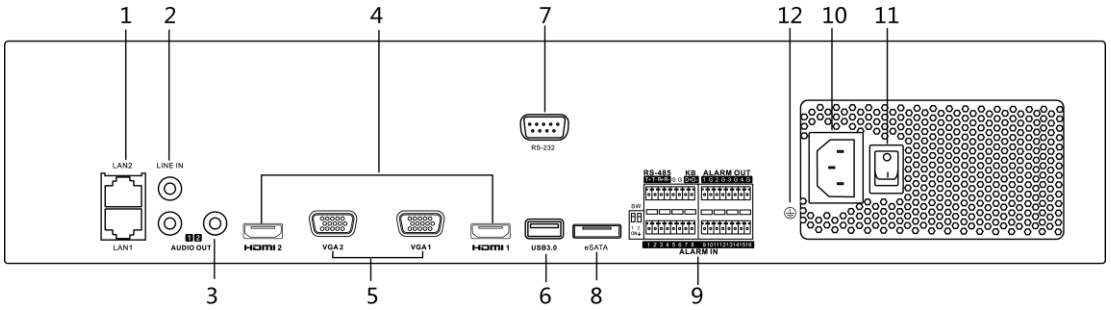


Figure 1-6 Rear Panel

Rear Panel 2:

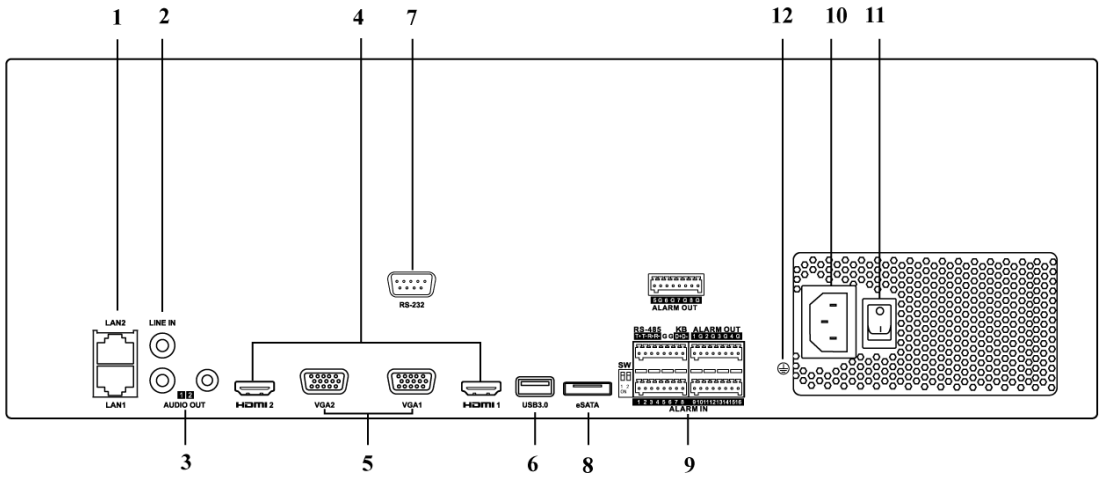


Figure 1-7 Rear Panel

Table 1-2 Panel Description

No.	Name	Description
1	LAN1/LAN2 Interface	2 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
2	LINE IN	RCA connector for audio input.
3	AUDIO OUT	2 RCA connectors for audio output.
4	HDMI1/HDMI2	HDMI video output connector.
5	VGA1/VGA2	DB9 connector for VGA output. Display local video output and menu.
6	USB 3.0 interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	RS-232 Interface	Connector for RS-232 devices.
8	eSATA	Connects external SATA HDD, CD/DVD-RM.
9	Controller Port	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first device's D+, D- pin should be connected with the D+, D- pin of the next device.
	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	100 to 240 VAC	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.
12	GROUND	Ground (needs to be connected when device starts up).

Rear Panel 3:

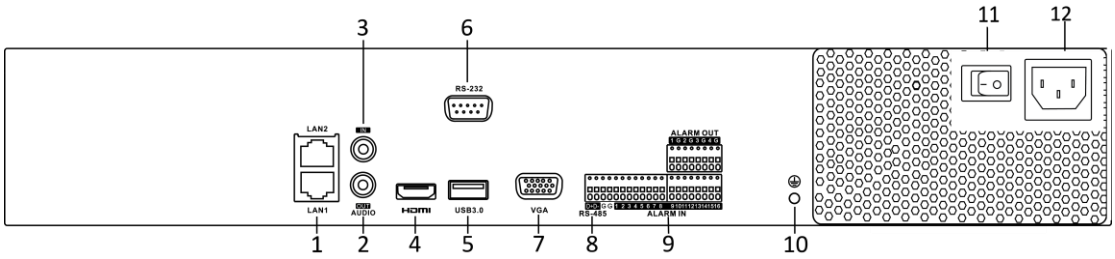


Figure 1-8 Rear Panel

Rear Panel 4:

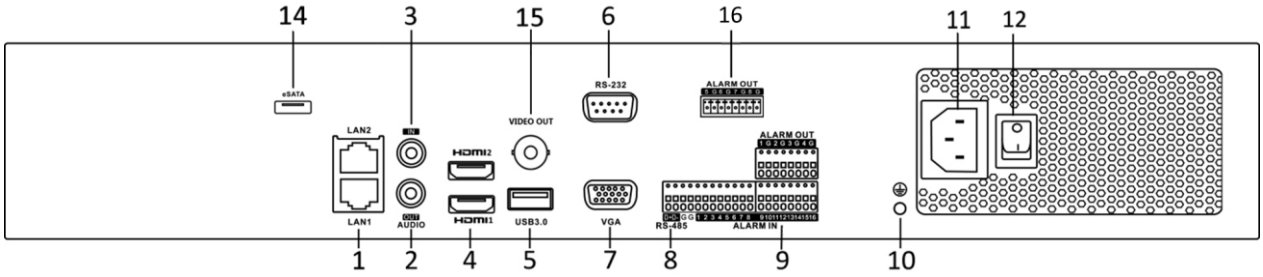


Figure 1-9 Rear Panel

Rear Panel 5:

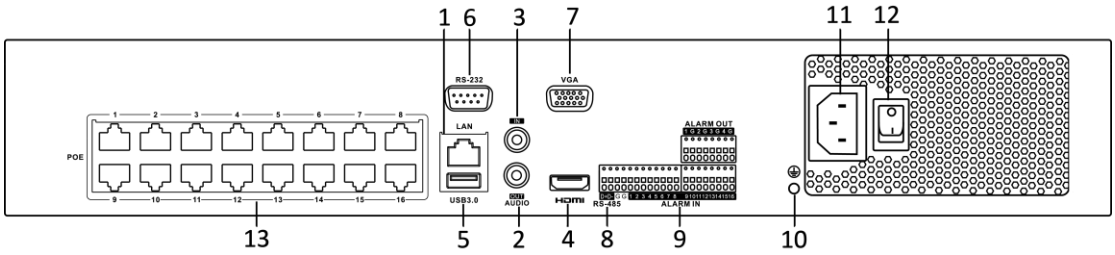


Figure 1-10 Rear Panel

Rear Panel 6:

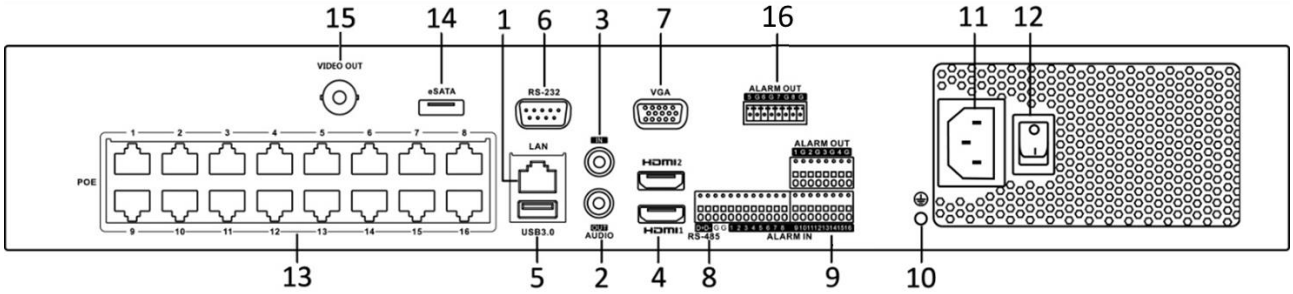


Figure 1-11 Rear Panel

NOTE

8-channel PoE NVR provides 8 network Interfaces with PoE function.

Table 1-3 Panel Description

No.	Name	Description
1	LAN Interface	1 network interface provided for PoE NVR, and 2 network interfaces for non- PoE NVR.
2	AUDIO OUT	RCA connector for audio output.

3	LINE IN	RCA connector for audio input.
4	HDMI	HDMI video output connector.
5	USB 3.0 interface	Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	RS-232 Interface	Connector for RS-232 devices.
7	VGA	DB9 connector for VGA output. Display local video output and menu.
8	RS-485 Interface	Half-duplex connector for RS-485 devices.
9	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	GROUND	Ground (needs to be connected when device starts up).
11	AC 100V ~ 240V	100V to 240VAC power supply.
12	Power Switch	Switch for turning on/off the device.
13	Network Interfaces with PoE function (for PoE NVR)	Network interfaces for the cameras and to provide power over Ethernet.
14	eSATA	Connects external SATA HDD, CD/DVD-RW.
15	VIDEO OUT	BNC connector for video output.
16	ALARM OUT (Optional)	Connector for alarm output.

Rear Panel 7

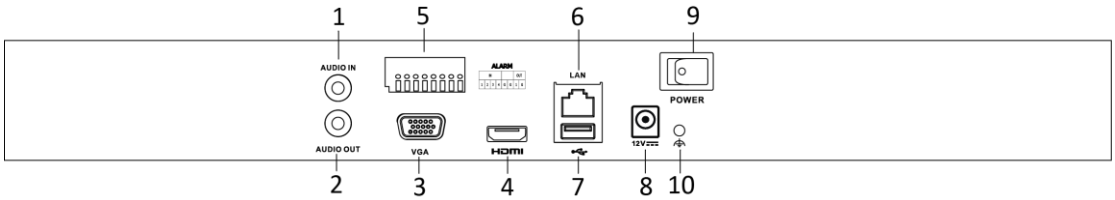


Figure 1-12 Rear Panel

Rear Panel 8

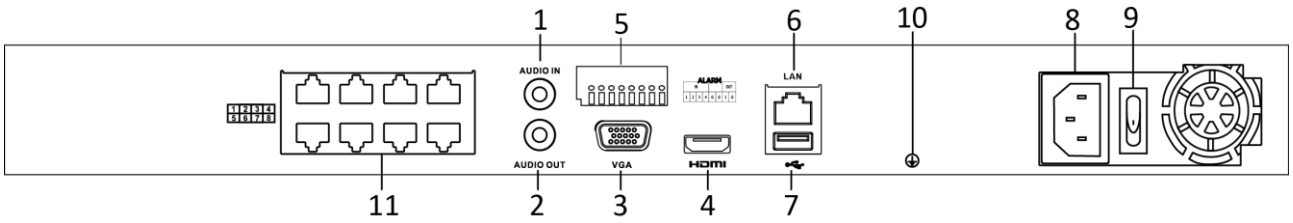


Figure 1-13 Rear Panel

NOTE

16-channel PoE NVR provide 16 network Interfaces with PoE function.

Table 1-4 Panel Description

No.	Name	Description
1	Audio In	RCA connector for audio input.
2	Audio Out	RCA connector for audio output.
3	VGA Interface	DB9 connector for VGA output. Display local video output and menu.
4	HDMI Interface	HDMI video output connector.
5	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
6	LAN Network Interface	1 10/100/1000 Mbps self-adaptive Ethernet interface
7	USB Interface	Universal Serial Bus (USB 3.0) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
8	Power Supply	12 VDC power supply for non-PoE NVR, and 100 to 240 VAC for PoE NVR.
9	Power Switch	Switch for turning on/off the device.
10	Ground	Ground (needs to be connected when NVR starts up).
11	Network Interfaces with PoE function (supported by PoE NVR)	Network interfaces for the cameras and to provide power over Ethernet.

Chapter 2 Getting Started

2.1 Start up the Device

Purpose:

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

Before you start:

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

Start up the device:

Step 1 Check the power supply is plugged into an electrical outlet. It is HIGHLY recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device gets the power supply.

Step 2 Press the POWER button on the front panel. The Power indicator LED should turn blue indicating that the unit begins to start up.

Step 3 After startup, the Power indicator LED remains blue. A splash screen with the status of the HDD appears on the monitor. The row of icons at the bottom of the screen shows the HDD status. 'X' means that the HDD is not installed or cannot be detected.

2.2 Activate the Device

Purpose:

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

Step 1 Enter the admin password twice.

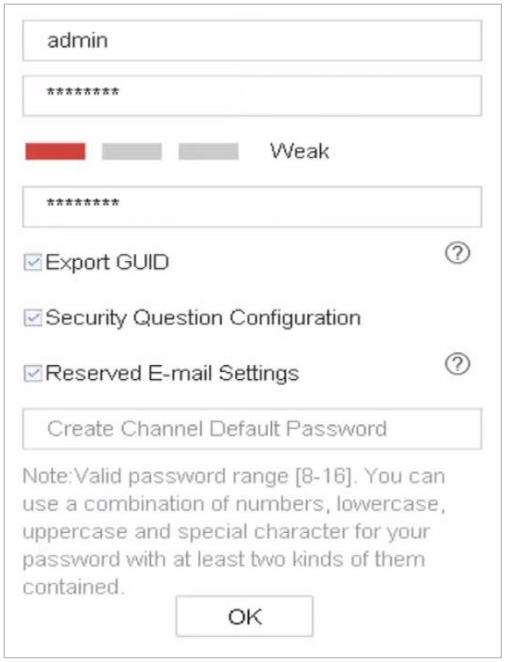


Figure 2-1 Activate the Device

WARNING

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. 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.

Step 2 Enter the password to activate the IP camera(s) connected to the device.

Step 3 (Optional) Check **Export GUID**, **Security Question Configuration,** or **Reserved E-mail**

Step 4 Click **OK**.

What to do next:

- When you have enabled the **Export GUID**, continue to export the GUID file to the USB flash driver for the future password resetting.
- When you have enabled the **Security Question Configuration**, continue to set the security questions for the future password resetting.
- When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

NOTE

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

2.3 Configure Login Unlock Pattern

You can configure a device login unlock pattern for the admin user.

Step 1 After the device is activated, enter the following interface to configure the device unlock pattern.

Step 2 Use the mouse to draw a pattern among the 9 dots on the screen. Release the mouse when the pattern is done.

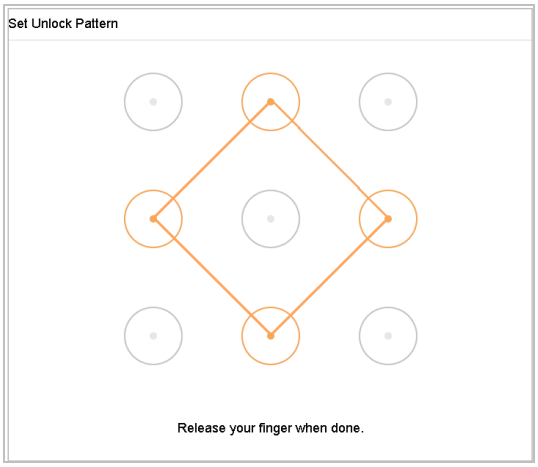


Figure 2-2 Draw the Pattern

NOTE

- Connect at least 4 dots to draw the pattern.
- Each dot can be connected for once only.

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

NOTE

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

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

NOTE

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

Before you Start

Configure the unlock pattern before unlocking. Refer to Chapter 2.2 Activate the Device

Purpose:

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

Step 1 Enter the admin password twice.

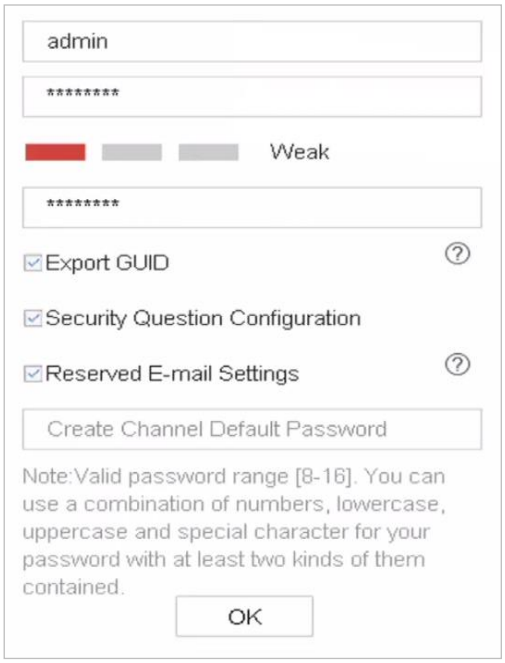


Figure 2-3 Activate the Device

WARNING

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. 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.

Step 2 Enter the password to activate the IP camera(s) connected to the device.

Step 3 (Optional) Check **Export GUID**, **Security Question Configuration,** or **Reserved E-mail**

Step 4 Click **OK**.

What to do next:

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

- When you have enabled **Reserved E-mail Settings**, continue to set the reserved email for the future password resetting.

NOTE

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

Configure Login Unlock Pattern.

Step 5 Right click the mouse and select the menu to enter the interface.

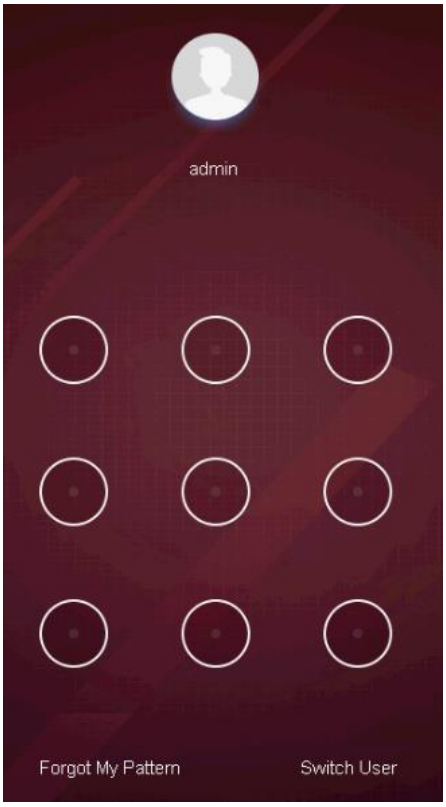


Figure 2-4 Draw the Unlock Pattern

Step 6 Draw the pre-defined pattern to unlock and enter the menu operation.

NOTE

- If you have forgotten your pattern, select **Forgot My Pattern** or **Switch User** to enter the normal login dialog box.
- If the pattern you draw is different from the pattern you configured, try again.
- If you draw the wrong pattern more than five times, the system will switch to the normal login mode automatically.

2.4.2 Log in via a Password

Purpose:

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

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

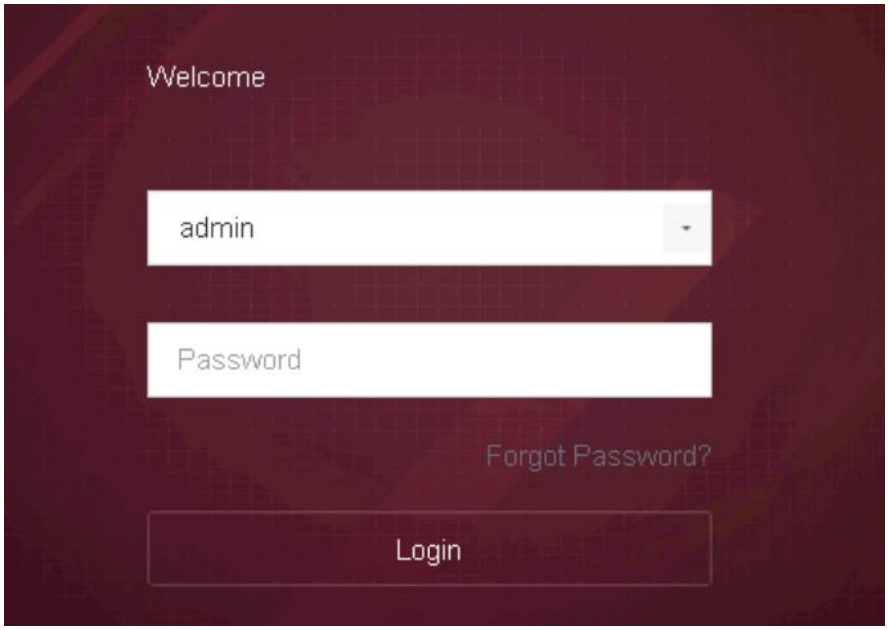


Figure 2-5 Login Interface

Step 2 Input password.

Step 3 Click **Login** to log in.

NOTE

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

NOTE

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

2.5 Start Setup Wizard

The Setup Wizard walks you through some important basic device settings.

By default, the Setup Wizard starts once the device has loaded. If you don't want to use the Setup Wizard at that moment, click **Exit**.

Step 1 Set the date and time on the **Date and Time Setup** interface.

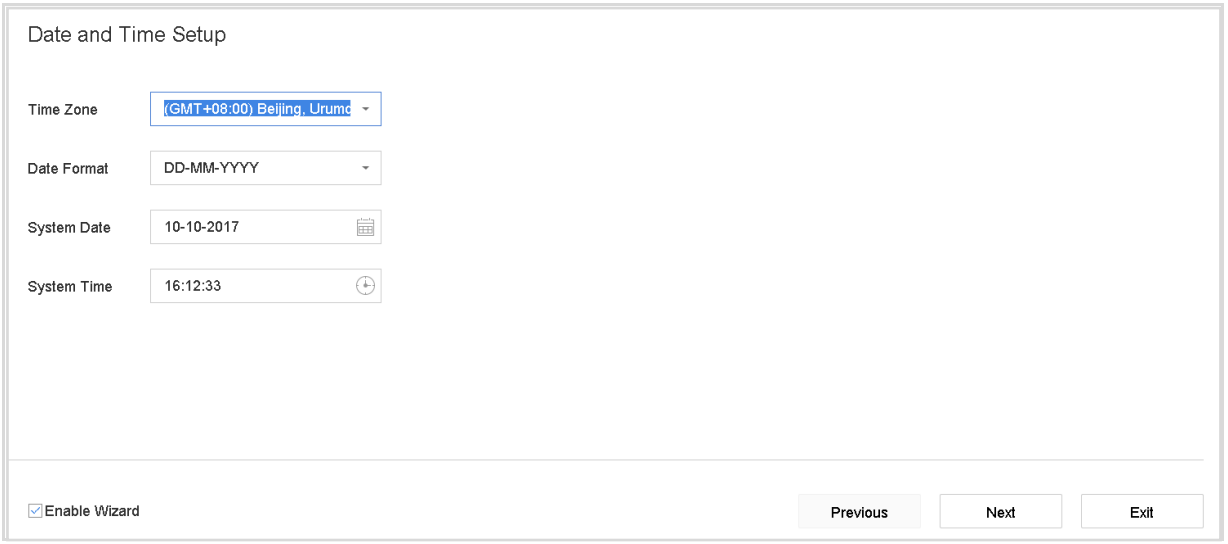


Figure 2-6 Date and Time Settings

Step 2 Set the basic network parameters on the **Network Setup** interface.

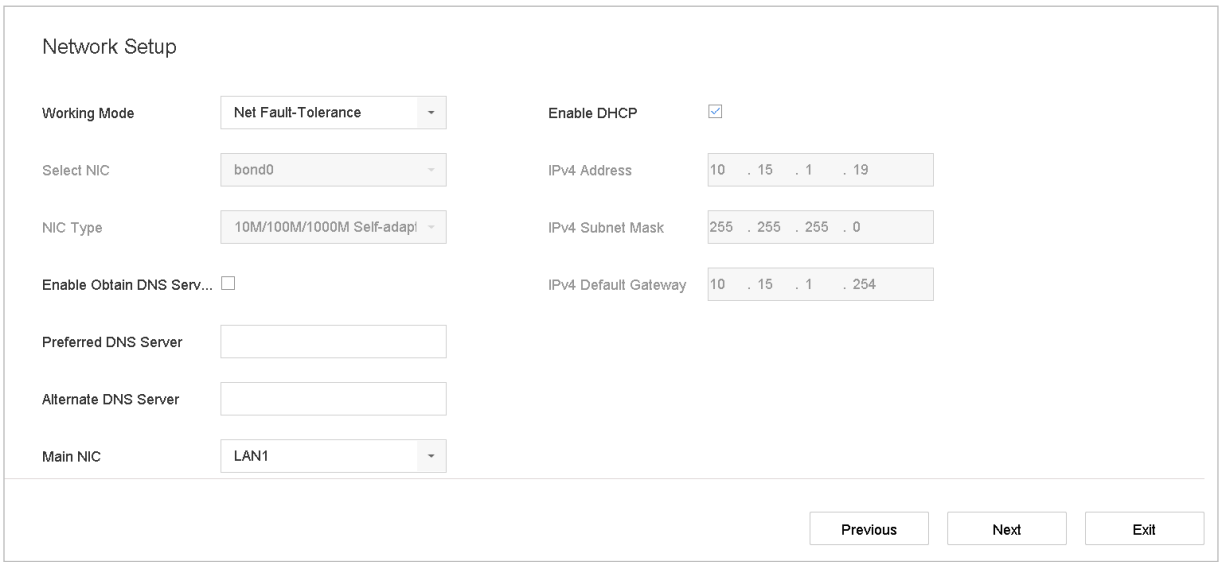


Figure 2-7 Network Settings

Step 3 Select a HDD and click **Init** to initialize it as demand on the **Hard Disk** interface.

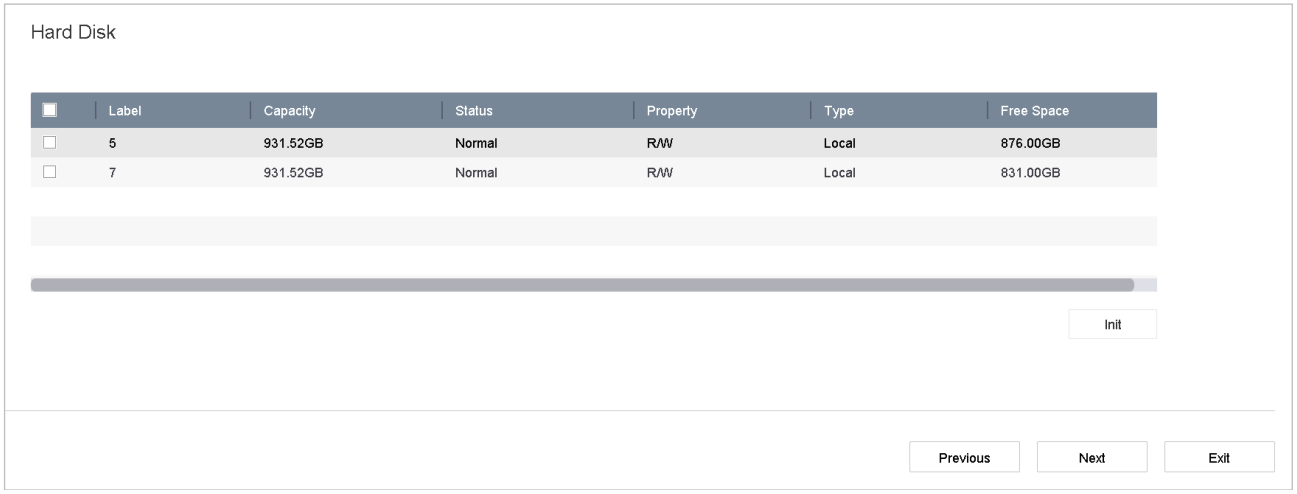


Figure 2-8 HDD Management

Step 4 Add IP cameras on the **Camera Setup** interface.

1) Click **Search** to search online IP camera. Before adding a camera, make sure the IP camera to be added is in active status.
2) Click **Add** to add the camera.

NOTE

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

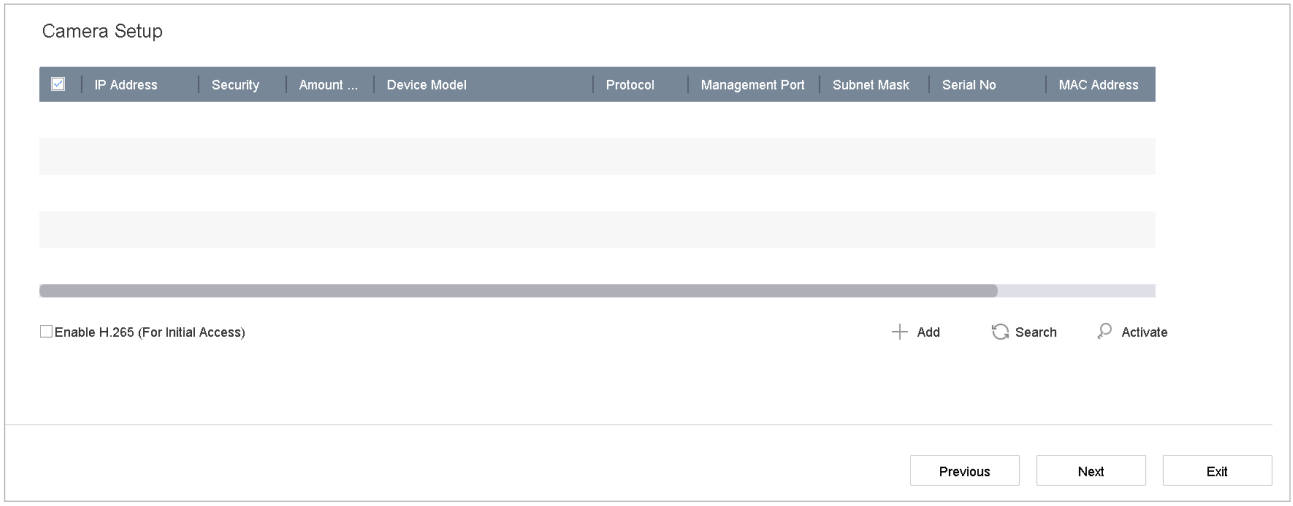


Figure 2-9 Search for IP Cameras

Step 5 Enter **Platform Access** interface and configure the Guarding Vision settings.

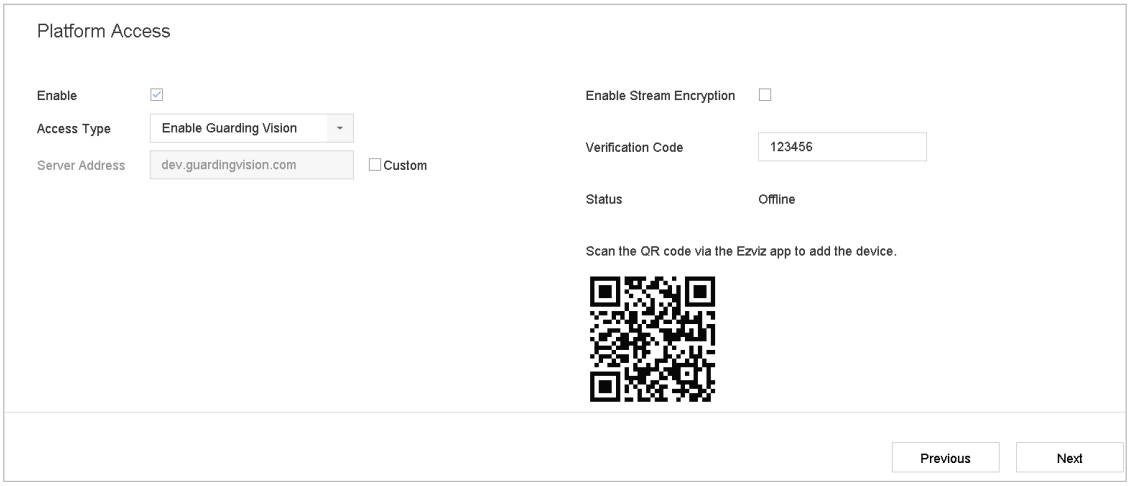


Figure 2-10 Guarding Vision Access

Step 6 Enter the **Change Password** interface to create a new admin password if required.



Figure 2-11 Change Password

NOTE

You can enter click the to show the characters input.

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

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.

Step 7 Click **OK** to complete the startup Setup Wizard.

2.6 Enter Main Menu

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

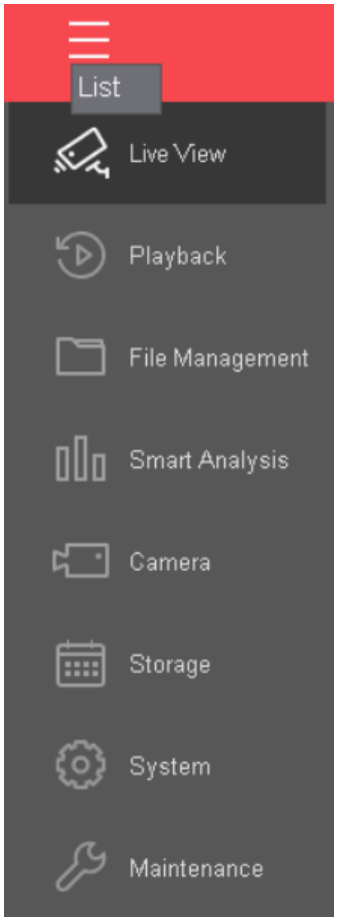


Figure 2-12 Main Menu Bar

Table 2-1 Description of Icons

Icon	Description
	Live View
	Playback
	File Management
	Smart Analysis
	Camera Management

	Storage Management
	System Management
	System Maintenance:

2.7 System Operation

2.7.1 Log out

Purpose:

After logging out, the monitor turns to live view mode. To perform any operations, you need to log in again.

Step 1 Click  on the menu bar.

Step 2 Click **Logout**.

NOTE

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

2.7.2 Shut Down the Device

Step 1 Click  on the menu bar.

Step 2 Click **Shutdown**.

Step 3 Click **Yes**.

NOTE

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

2.7.3 Reboot the Device

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

Step 1 Click  on the menu bar.

Step 2 Click **Reboot** to reboot the device.

Chapter 3 Camera Management

3.1 Add IP Cameras

3.1.1 Add IP Cameras Manually

Purpose:

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 the IP camera has been activated.

Step 1 Click  on the main menu.

Step 2 Click **Custom Add**.

Step 3 Set **IP Camera Address**, **Protocol**, **Management Port**, **Transfer Protocol**, **User Name**, and **Password**. **Management Port** ranges from 1 to 65535.

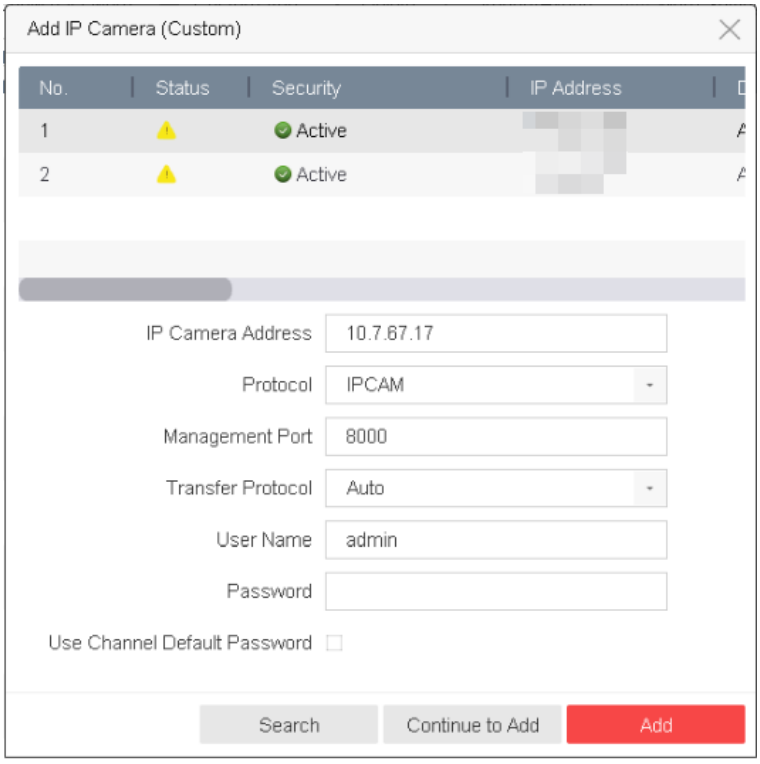


Figure 3-1 Add IP Camera

Step 4 (Optional) Check **Use Channel Default Password** to use the default password to add the camera.

Step 5 (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 IPCAM protocol.

Step 6 (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 IP camera certificate to the NVR first when you use this function.

1) Log in the IP camera by web browser.
2) Go to **Configuration** > **Network** > **Advanced Settings** > **HTTPS** on the web browser o to export its certificate.
3) Click **Export** at **Export Certificate** to save the certificate.
4) Log in the NVR by web browser.
5) Go to Configuration > System > Security > Trusted Root Certification Authorities > Import
6) Click **Import** to import the IP camera certificate.

NOTE

The function is only available when you use IPCAM protocol.

Step 7 Click **Add** to finish adding the IP camera.

Step 8 (Optional) Click **Continue to Add** to continue to add other IP cameras.

3.1.2 Add the Automatically Searched Online IP Cameras

Step 1 On the Camera Management interface, click the **Online Device** panel to expand the Online Device interface.

Step 2 Select the automatically searched online device.

Step 3 Click **Add** to add the camera which has the same login password with the device.

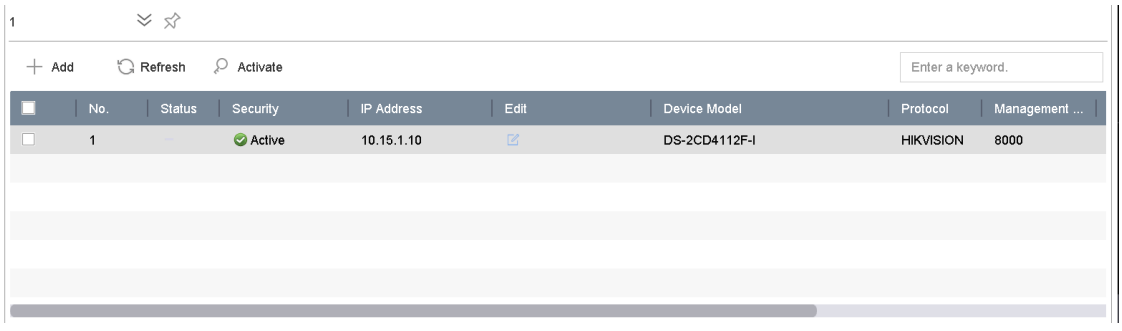


Figure 3-2 Add IP Camera

NOTE

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

3.2 Manage Cameras for PoE Device

NOTE

This chapter is only applicable for the following models: Pro Series Device.

Purpose:

The PoE interfaces enables 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 model

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.

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

3.2.1 Add PoE Cameras

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

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

3.2.2 Add Non-PoE IP Cameras

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.

Step 1 Go to **Camera > Camera > IP Camera**.

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

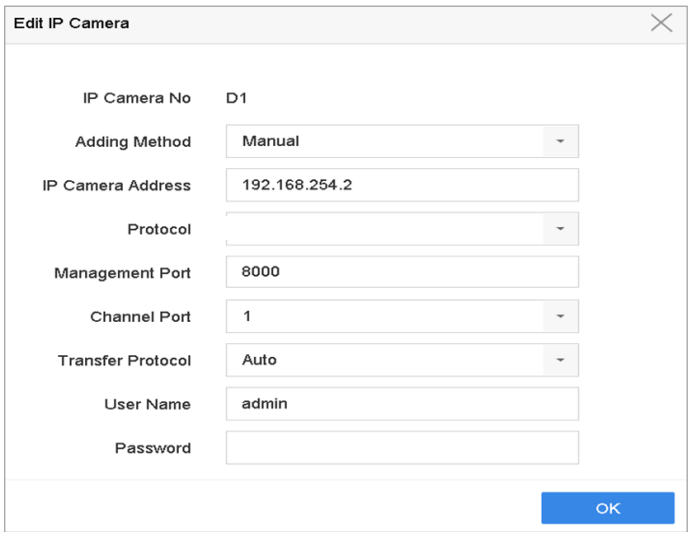


Figure 3-3 Edit IP Camera

Step 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.

Step 4 Enter the IP address, the user name and password of administrator manually.

Step 5 Click **OK**.

3.2.3 Configure PoE Interface

Purpose:

When it requires long-distance PoE transmission (100 to 300 m), you can enable long distance mode for the PoE channel.

Step 1 Go to **Camera > Camera >PoE Settings**.

Step 2 Enable or disable long network cable mode by selecting **Long Distance** or **Short Distance** radio.

- **Long Distance**: Long-distance (100 to 300 meters) network transmissions via POE interface.
- **Short Distance**: Short-distance (< 100 meters) network transmission via POE interface.

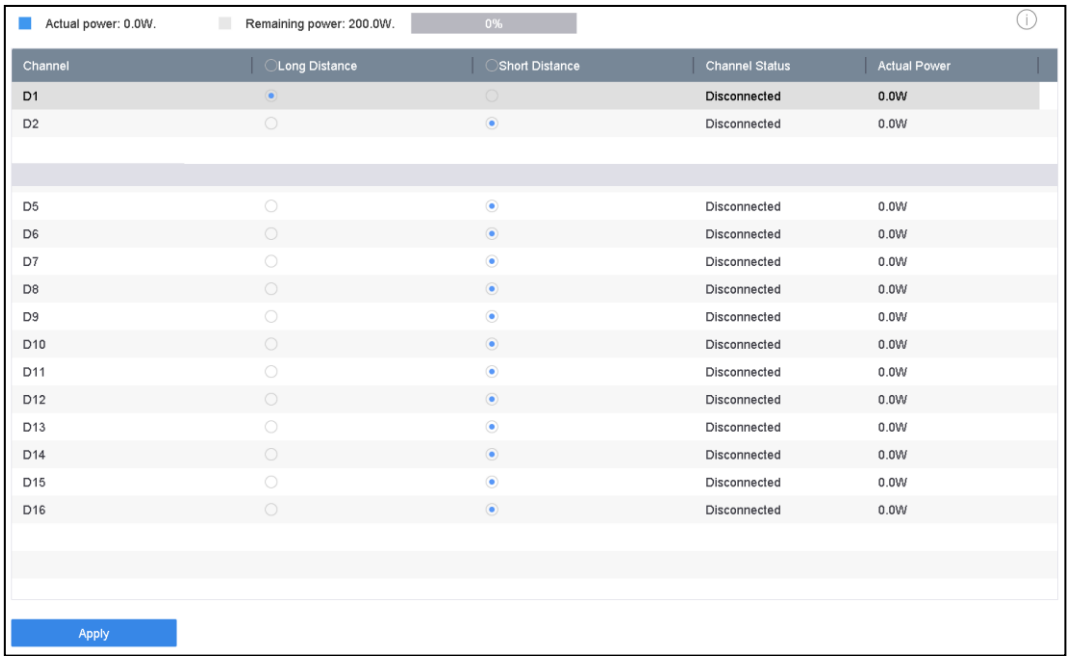


Figure 3-4 PoE Settings

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.

Step 3 Click **Apply**.

3.3 Enable the 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.

Step 1 Go to **More Settings** > **H.265 Auto Switch Configuration** at the top taskbar.

Step 2 Check the checkbox of **Enable H.265 (For Initial Access)**.

Step 3 Click **OK**.

3.4 Upgrade the IP Camera

The IP camera can be remotely upgraded through the device.

NOTE

Plug the U-flash drive with the IP camera's firmware upgrade file to the device.

Step 1 On the camera management interface, select a camera.

Step 2 Go to **More Settings** > **Upgrade** at the top taskbar.

Step 3 Select the firmware upgrade file from the U-flash drive.

Step 4 Click **Upgrade**.

Result:

The IP camera will reboot automatically after the upgrading completes.

3.5 Configure the Customized Protocols

Purpose

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

Step 1 Go to **More Settings** > **Protocol** at the top taskbar to enter the protocol management interface.

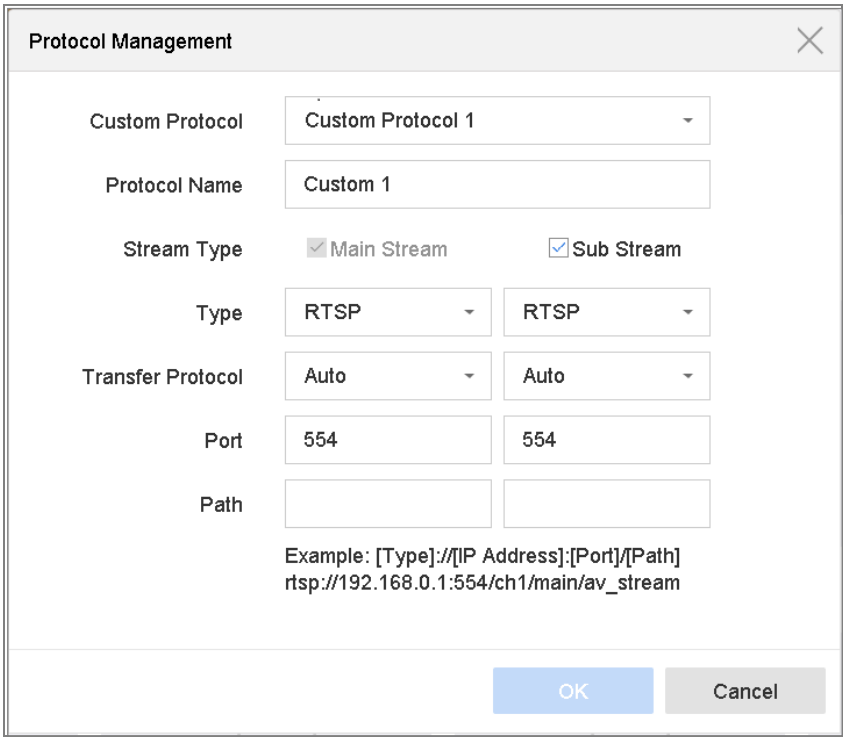


Figure 3-5 Protocol Management

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

- **Type:** The network camera adopting custom protocol must support getting stream through standard RTSP.
- **Path:** you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.
- The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path].
- ***Example:*** rtsp://192.168.1.55:554/ch1/main/av_stream.

NOTE

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

Step 3 Click **OK** to save the settings.

Result:

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

Chapter 4 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.

4.1 Add IoT Device

NOTE

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

4.1.1 Add Access Control Device

Purpose

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

Before your start

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

Step 1 Go to **Business Application > IoT > Access Control > Device Management**.

Step 2 Click **Add**.



Figure 4-1 Access Control

Step 3 Enter access control device information. **Device IP**, **Port**, **User Name**, and **Password** must be the same with access control device.

Step 4 (Optional) For device with multiple access control channels or video channels, check the access control channel and video channel as your desire.

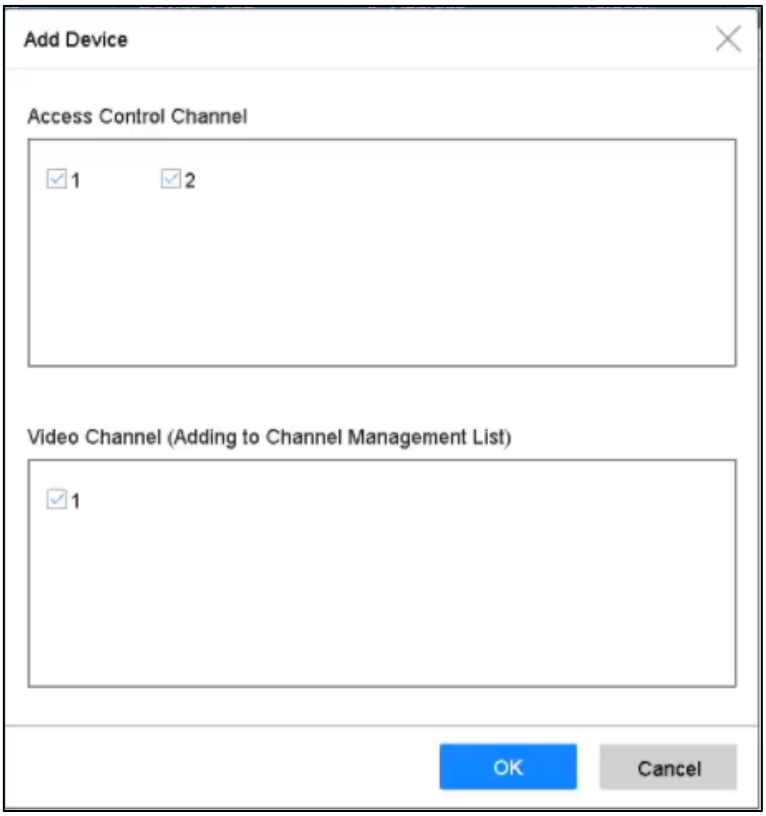


Figure 4-2 Add Device

Step 5 Click **Add**.

Related operations:

- Click to view the live video of related channel.

NOTE

For access control devices without the video channel. You need to select trigger channel in linkage action configuration first. For details, refer to *4.2 Configure Linkage Action*.

- Click to edit added access control device information.

4.1.2 Add Alarm Device

Purpose

Add alarm devices of Hikvision, Luminite, GJD, or OPTEX manufacturer to receive their alarms. You can configure linkage actions like triggering recording and full screen monitoring, when an alarm occurs.

Before your start

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

Step 1 Go to **Business Application > IoT > Alarm > Device Management**.

Step 2 Click **Add**.

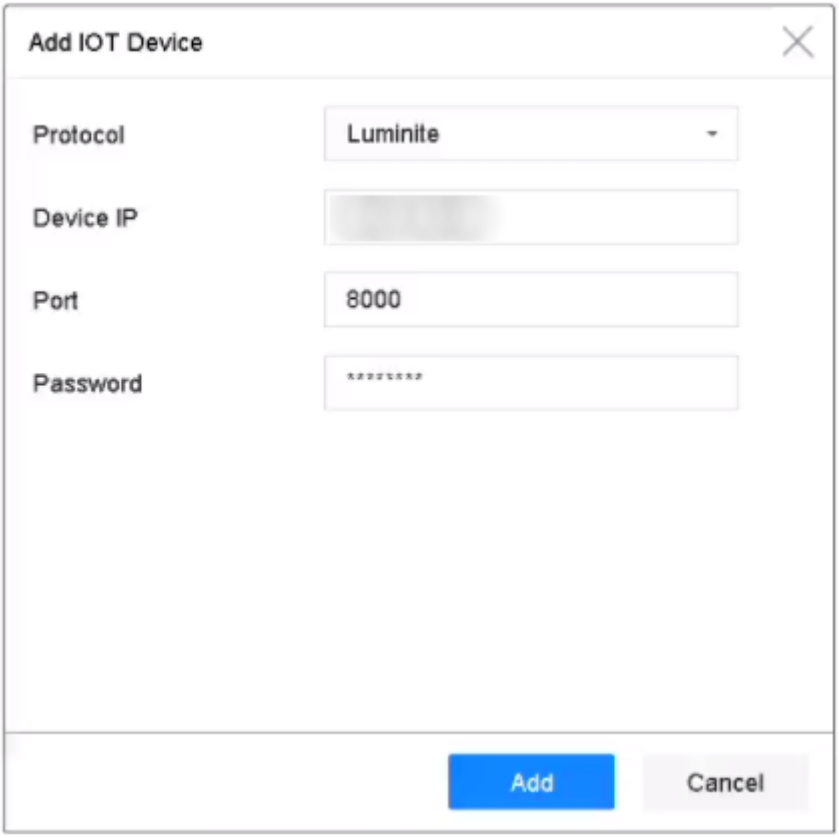


Figure 4-3 Alarm Device

Step 3 Enter access control device information. The information must be the same with alarm device to add.

Step 4 Click **Add**.

Related operations:

- Click to view the live video of related channel.

NOTE

You need to select trigger channel in linkage action configuration first. For details, refer to *4.2 Configure Linkage Action*.

- Click to edit added alarm device information.

4.2 Configure Linkage Action and Arming Schedule

Purpose

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

Step 1 Click  of an added IoT device.

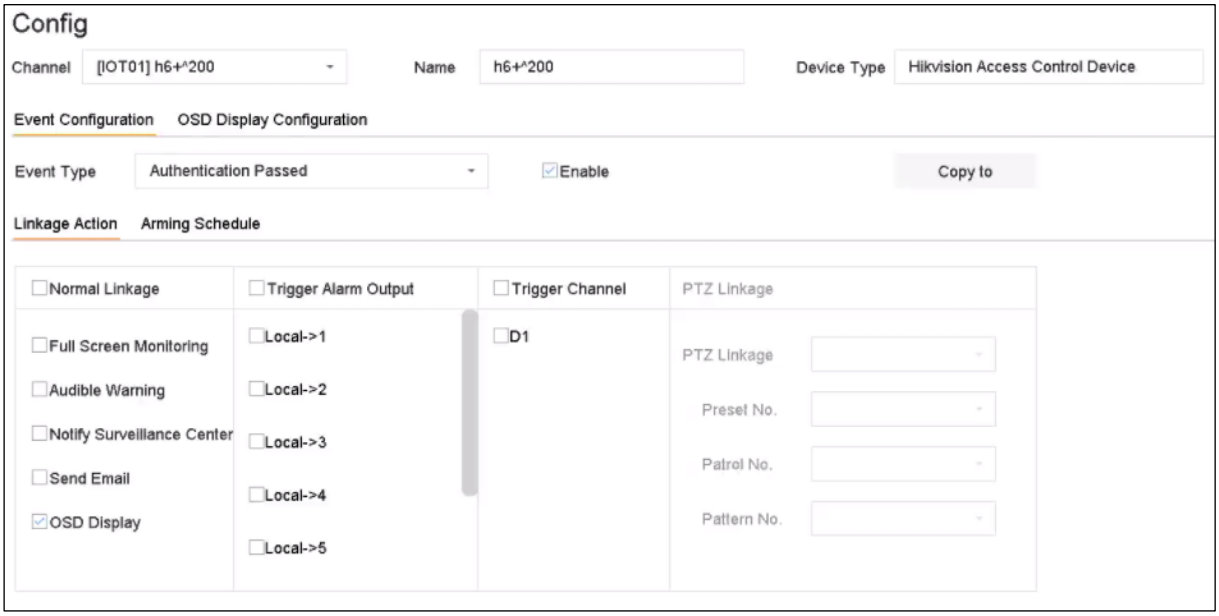


Figure 4-4 Configure IoT

Step 2 Select **Event Type.** The following configuration is only valid for the selected event type.

Step 3 Check **Enable**.

Step 4 Check linkage actions as your desire. For detailed steps, refer to *12.9 Configure Combined Alarm*.

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

Step 5 Click **Arming Schedule**.

Step 6 Configure arming schedule. For detailed steps, refer to *12.1 Configure Arming Schedule*. Linkage action is only valid during the set schedule.

Step 7 Click **Apply**.

4.3 Configure OSD

Purpose

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

Step 1 Click  of an added IoT device.

Step 2 Check **OSD Display** on Event Configuration interface.

Step 3 Select **Trigger Channel**.

Step 4 Click **OSD Display Configuration**.

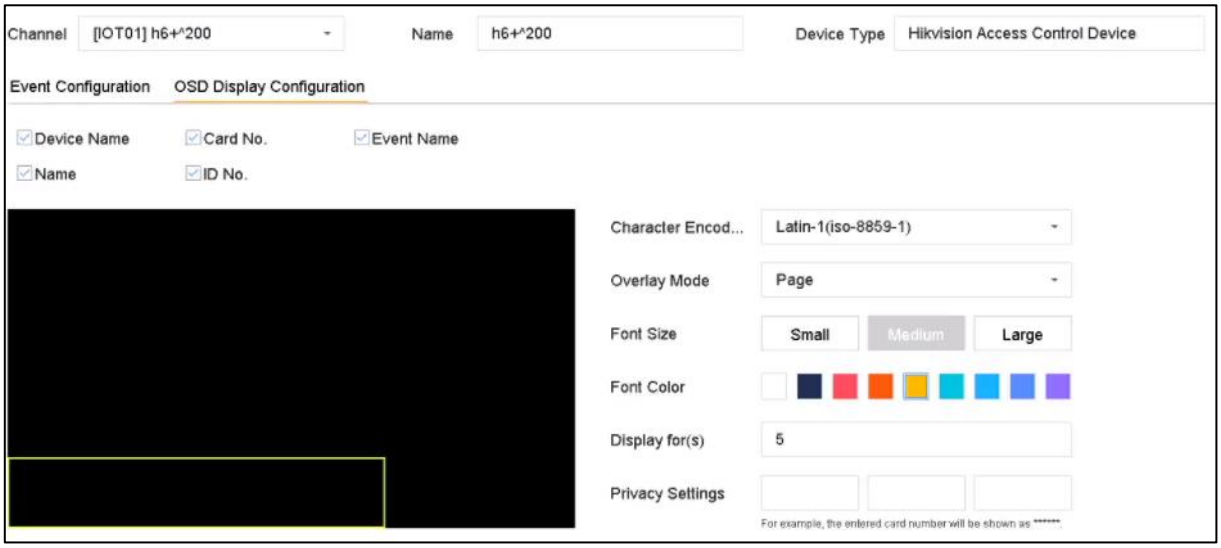


Figure 4-5 OSD Configuration

Step 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.

Step 6 Configure OSD properties.

- **Overlay Mode**:

  − **Scroll**: The OSD will automatically scroll to show the new alarm information.

  − **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**.

Step 7 Adjust the quadrilateral of yellow frame on the preview window to adjust IoT OSD size and position.

Step 8 Click **Apply**.

4.4 Search IoT Record

Purpose

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

Step 1 Go to event record interface.

- Access control: Go to **Business Application > IoT > Access Control > Card Swiping Record**.
- Alarm device: Go to **Business Application > IoT > Alarm > Search Data.**

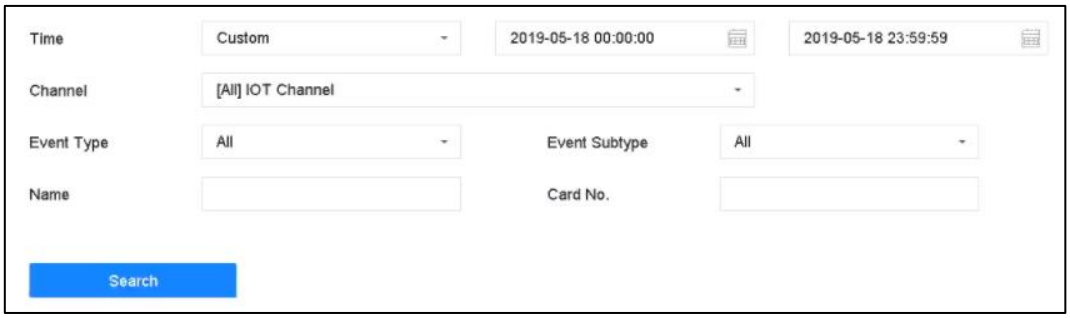


Figure 4-6 Search Event Record (Access Control)

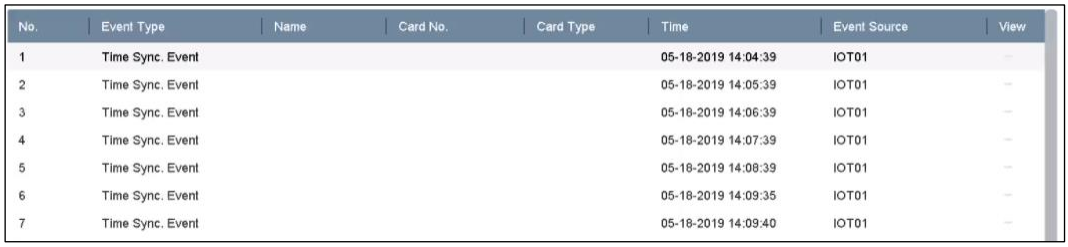


Figure 4-7 Search Event Record (Alarm Device)

Step 2 Specify search conditions.

Name and **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.

Step 3 Click **Search.**



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	

Figure 4-8 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 4-9 Search Result (Alarm Device)

4.5 IoT Video/Picture

Purpose

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.

4.5.1 Configure Event Recording/Capturing

Purpose:

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

Step 1 Click  of an added IoT device.

Step 2 Select desired **Event Type**.

Step 3 Check **Enable**.

Step 4 Check **Trigger Channel** you want to record event videos or capture pictures when an alarm occurs.

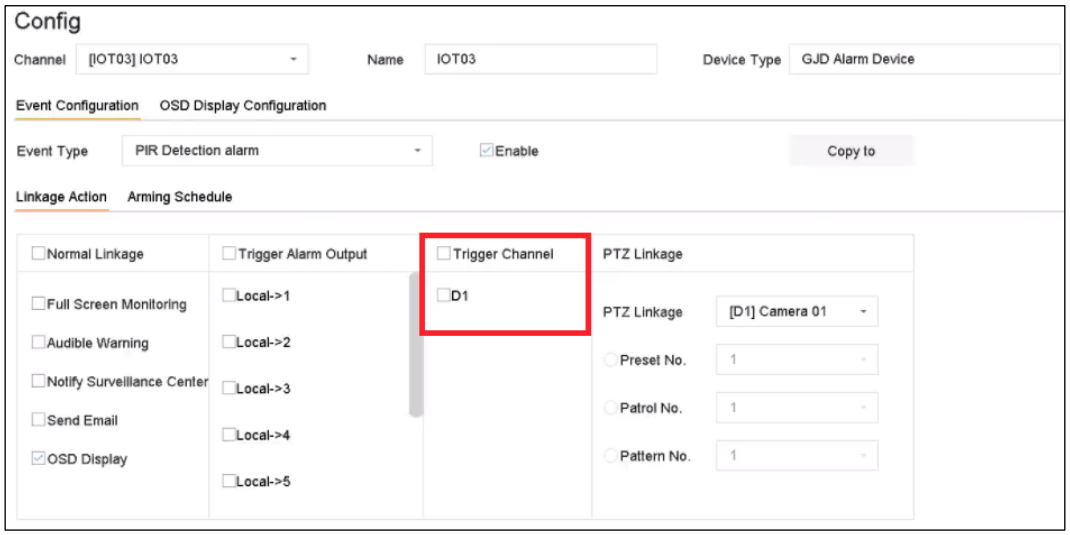


Figure 4-10 Trigger Channel

Step 5 Click **Apply**.

Step 6 Configure event recording or capturing schedule. Choose from:

- Recording

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 *8.4 Configure Recording Schedule* for details.
5) Click **OK**.

- Capturing

1) Go to **Storage > Schedule > Capture**.
2) Select **Camera No.** and check **Enable Schedule**. The camera should be the camera you select in step 4.

6) Select the capturing type as **Event**.
7) Drag the mouse on the time bar to set the event detection capturing schedule. Refer to *8.4 Configure Recording Schedule* for details.
8) Click **OK**.

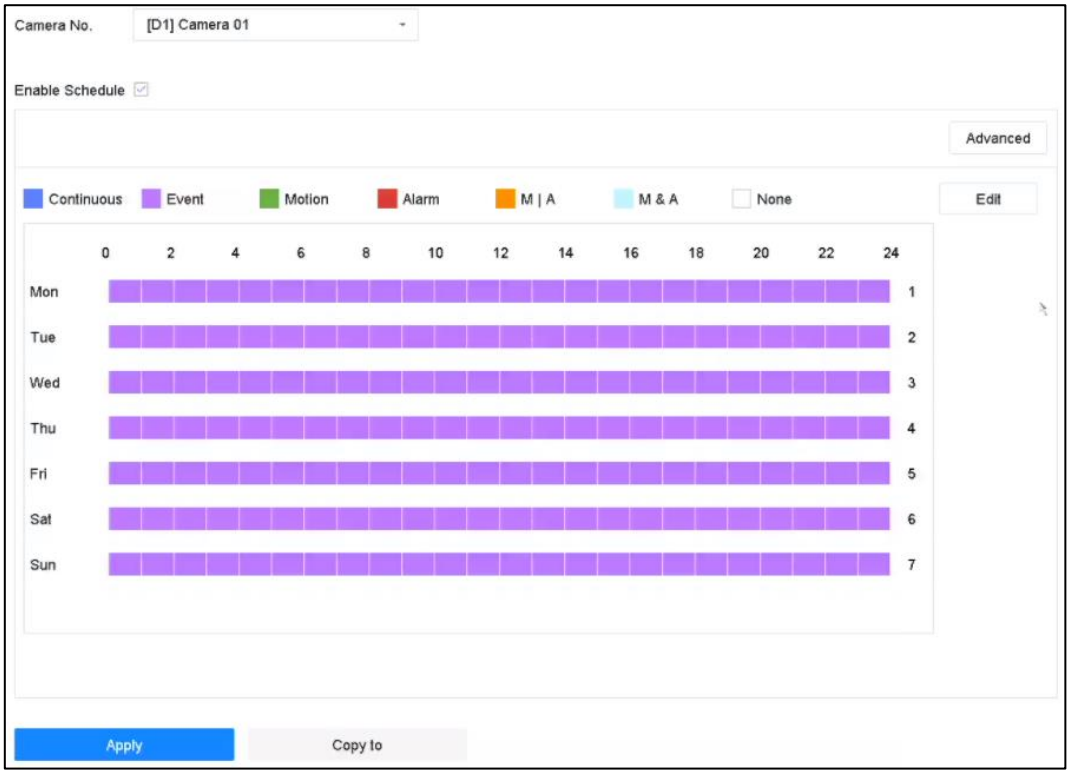


Figure 4-11 Event Recording

Step result:

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

4.5.2 Search IoT Video/Picture

Purpose

Search IoT event triggered videos or pictures.

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

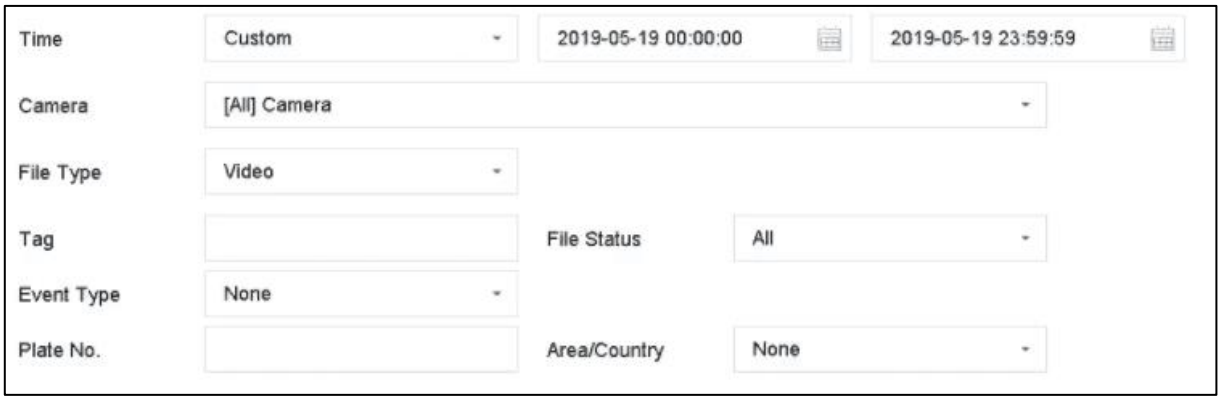


Figure 4-12 Search Event Video/Picture

Step 2 Set search conditions.

- **Camera**: Select it as the selected trigger channels in IoT linkage action configuration.
- **Event Type**: Select the desired IoT event.
- **File Type**: You can search the IoT video or picture.

Step 3 Click **Search**.

Chapter 5 Camera Settings

5.1 Configure OSD Settings

Purpose

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

Step 1 Go to **Camera** >**Display.**

Step 2 Select the camera from the drop-down list.

Step 3 Edit the name in **Camera Name**.

Step 4 Check **Display Name**, **Display Date** and **Display Week** to show the information on the image.

Step 5 Set the date format, time format, and display mode.

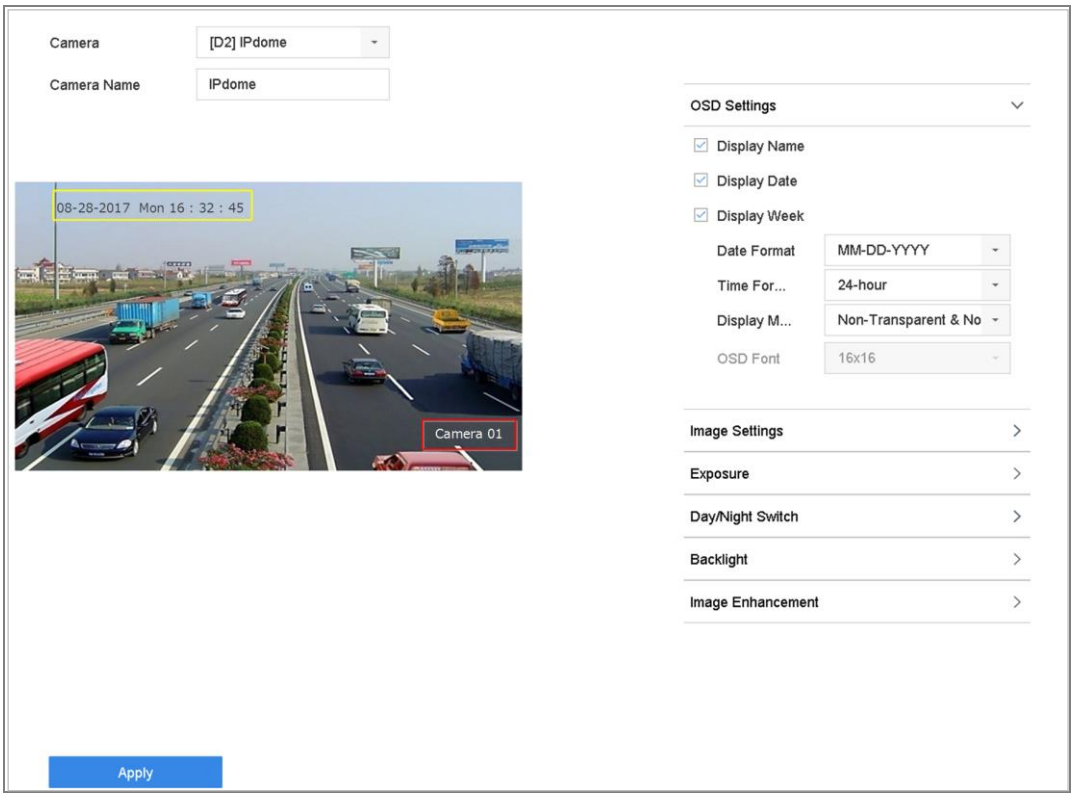


Figure 5-1 OSD Configuration Interface

Step 6 Use the mouse to click and drag the text frame on the preview window to adjust the OSD position.

Step 7 Click **Apply**.

5.2 Configure Privacy Mask

Purpose

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

Step 1 Go to **Camera** >**Privacy Mask**.

Step 2 Select the camera to set privacy mask.

Step 3 Click **Enable** to enable this feature.

Step 4 Use the mouse to draw a zone on the window. The zones will be marked by different frame colors.

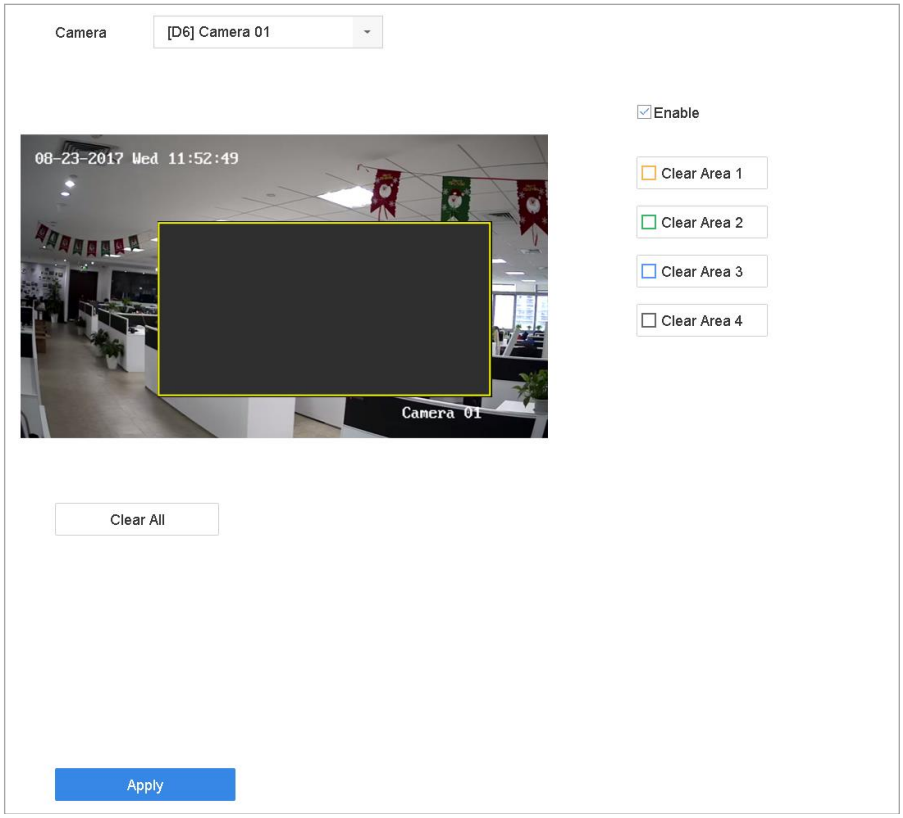


Figure 5-2 Privacy Mask Settings Interface

NOTE

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

Related Operation:

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

Step 5 Click **Apply**.

5.3 Configure the Image Parameters

Purpose

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

Step 1 Go to **Camera**>**Display > Image Settings.**

Step 2 Select a camera from the drop-down list.

Step 3 Adjust the slider or click on the up/down arrow to set the value of the brightness, contrast, or saturation.

Step 4 Click **Apply**.

5.4 Configure the Day/Night Switch

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

Step 1 Go to **Camera**>**Display > Day/Night Switch.**

Step 2 Select the camera from the drop-down list.

Step 3 Set the day/night switch mode to **Day**, **Night**, **Auto,** or **Auto-Switch**.

- **Auto**: The camera automatically switches between day mode and night mode according to the illumination.
  - The sensitivity ranges from 0 to 7, and higher sensitivity more easily triggers the mode switch.
  - The switch time refers to the interval time between the day/night switch. You can set it from 5 sec to 120 sec.
- **Auto-Switch**: The camera switches the day mode and the night mode according to the start time and end time you set.

Step 4 Click the **Apply**.

5.5 Configure IP Camera Time Sync

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

Step 1 Go to **Camera > Camera > IP Camera**.

Step 2 Position the cursor on the window of the IP camera and click .

Step 3 Check **Enable IP Camera Time Sync**.

Step 4 Click **OK**.

5.6 Configure Other Camera Parameters

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

Step 1 Go to **Camera**>**Display.**

Step 2 Select a camera from the drop-down list.

Step 3 Configure the camera parameters.

- Exposure: Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.
- Backlight: Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.
- Image Enhancement: For optimized image contrast enhancement.

Step 4 Click **Apply**.

Chapter 6 Live View

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

6.1 Start Live View

Click  on the main menu bar to enter the Live View.

- Select a window and double click a camera from the list to play the video from the camera in the selected window.
- 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.

6.1.1 Digital Zoom

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

Step 1 In the Live View mode, click  from the toolbar to enter the digital zoom interface.

Step 2 Move the sliding bar or scroll the mouse wheel to zoom in/out the image to different magnifications (1x to 16x).



Figure 6-1 Digital Zoom

6.1.2 Fisheye View

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

NOTE

- The fisheye expansion view feature is supported only by the Pro Series.

- The connected camera must support the fisheye view.

Step 1 In the Live View mode, click  to enter the fisheye expansion mode.

Step 2 Select the expansion view mode.

- **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.
- **Fisheye + 3PTZ ():** The camera will be divided into a fisheye view and 3 PTZ views. The PTZ views are the three different close-ups of the fisheye view. You can drag the PTZ images to adjust its view.
- **Cylinder ():** The camera image will be displayed as a cylinder. You can drag the image to adjust its view or scroll to zoom in/out.
- **Hemisphere ():** The camera image will be displayed as a hemisphere. You can drag the image to adjust its view or scroll to zoom in/out.
- **4 PTZ ():** The camera will be divided into 4 PTZ views. The PTZ views are the four different close-ups of the fisheye view. You can drag the PTZ images to adjust its view.

6.1.3 3D Positioning

3D Positioning (for I series device) zooms in/out of a specific live image area.

Step 1 In Live View mode, click the  to enter the 3D positioning mode.

Step 2 Zoom in/out of the image.

- **Zoom In**

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

- **Zoom Out**

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

6.1.4 Live View Strategy

Step 1 In Live View mode, click  to enter the digital zoom operation interface in full screen mode.

Step 2 Select the Live View strategy to **Real-time**, **Balanced** or **Fluency**.

6.1.5 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 to switch the main/auxiliary port.

6.2 Target Detection

I 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.

Step 1 In Live View mode, click **Target Detection** to enter the target detection interface.

Step 2 Select different detection types: smart detection (), vehicle detection (), face detection (), and human body detection ().

Step 3 Select the historical analysis () or real-time analysis () to obtain the results.



Figure 6-2 Target Detection

Step 4 Optionally, you can select channels that require picture capture. The unselected channels will not capture picture.

1. Click  at the left bottom of live view interface.
2. Select channel(s), the checked channel(s) will capture picture. All channels are selected as default.

Step 5 Click **Finish**.

Step 6 The smart analysis results of the detection are displayed in the list. Optionally, click a result in list to play the related video.

6.3 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.

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

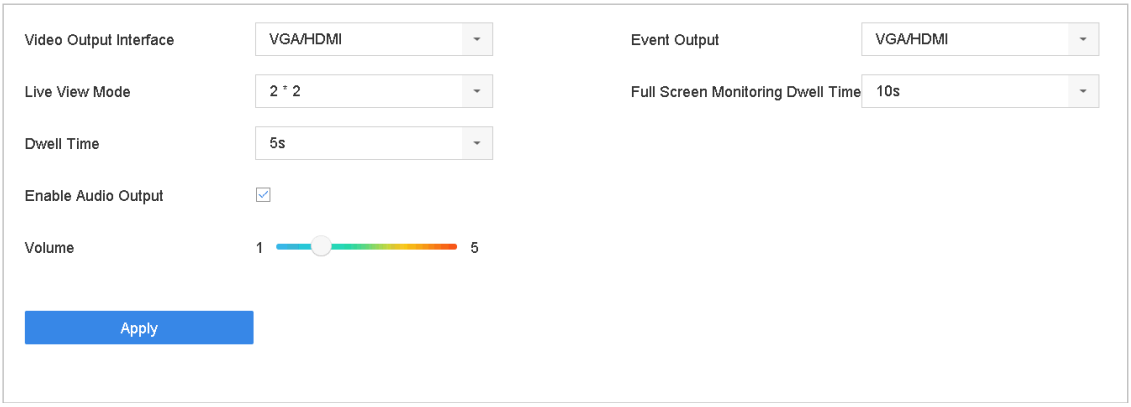


Figure 6-3 Live View-General

Step 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.

Step 3 Click **OK**.

6.4 Configure Live View Layout

6.4.1 Configure Custom Live View Layout

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

Step 2 Click **Set Custom Layout**.

Step 3 Click  on **Custom Layout Configuration**.

Step 4 Edit the layout name.

Step 5 Select a window division mode.

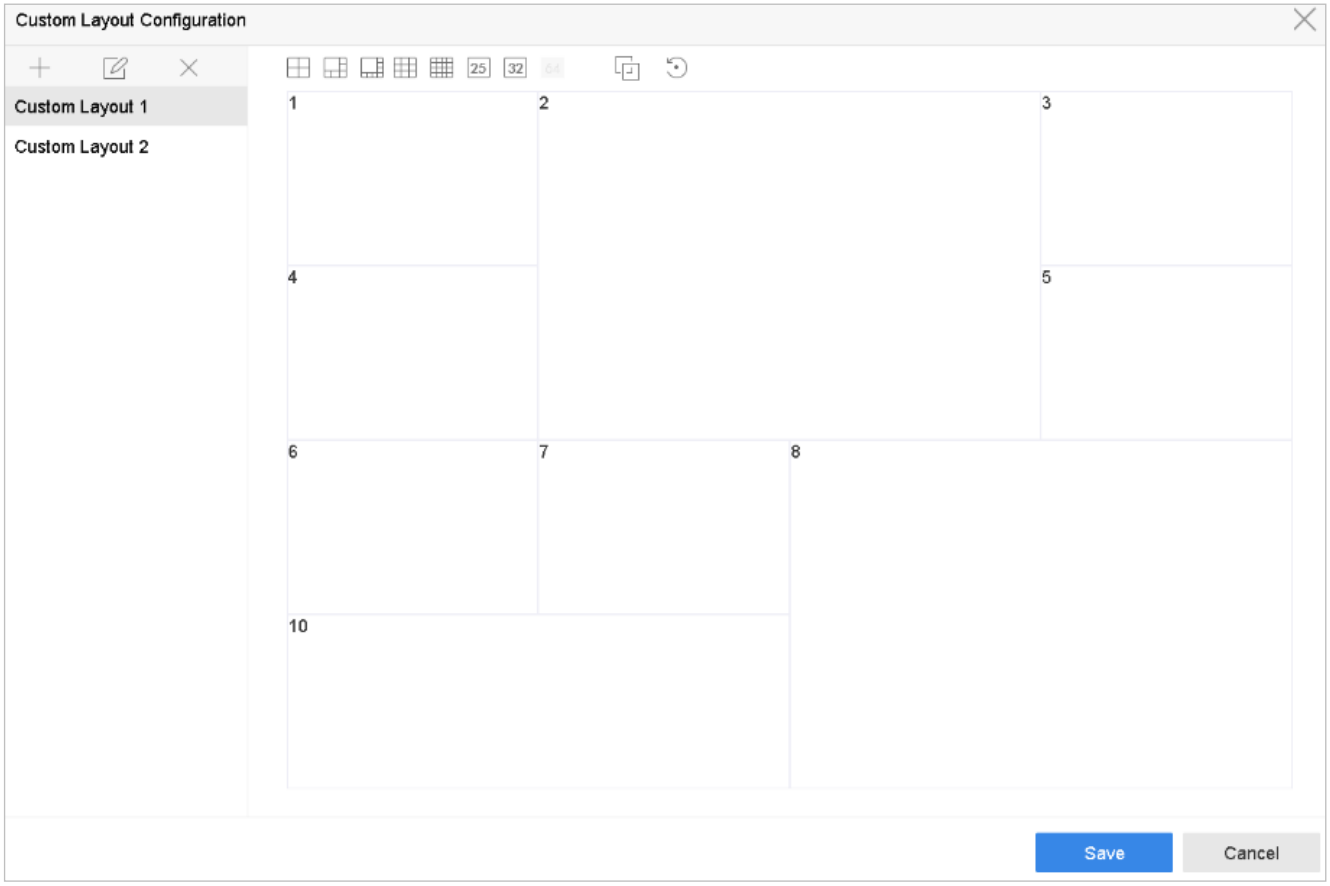


Figure 6-4 Configure Live View Layout

Step 6 Select multiple windows and click  to join the windows. The selected windows must be in rectangle area.

Step 7 Click **Save**.

Result:

The successfully configured view layout is displayed in the list.

Related Operations:

- Select a live view layout from the list and click  to edit the name.
- Select a live view layout from the list and click  to delete the name.

6.4.2 Configure Live View Mode

Step 1 Go to **System** > **Live View** > **View**

Step 2 Select the video output interface.

Step 3 Select a constant window-division layout or custom layout from the toolbar.

Step 4 Select a division window, and double-click on a camera in the list to link the camera to the window.

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

NOTE

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

Step 5 Click **Apply**.

Related Operations:

- Click  to start Live View for all channels.
- Click  to stop all Live View channels.

6.5 Configure Camera Auto-Switch

You can set the camera's auto-switch to play in different display modes.

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

Step 2 Set the video output interface, Live View mode and dwell time.

- **Video Output Interface:** Select the video output interface.
- **Live View Mode:** Select the display mode for Live View, e.g., 2*2, 1*5, etc.
- **Dwell Time:** The time in seconds to wait between switching of cameras when in auto-switch. The range is from 5s to 300s.

Step 3 Go to **View Settings** to set the view layout.

Step 4 Click **OK**.

6.6 Configure Channel-Zero Encoding

Purpose

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.

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

Step 2 Set the video output interface to **Channel-Zero**.

Step 3 Go to **System**>**Live View**>**Channel-Zero**.

Step 4 Check **Enable Channel-Zero Encoding**.

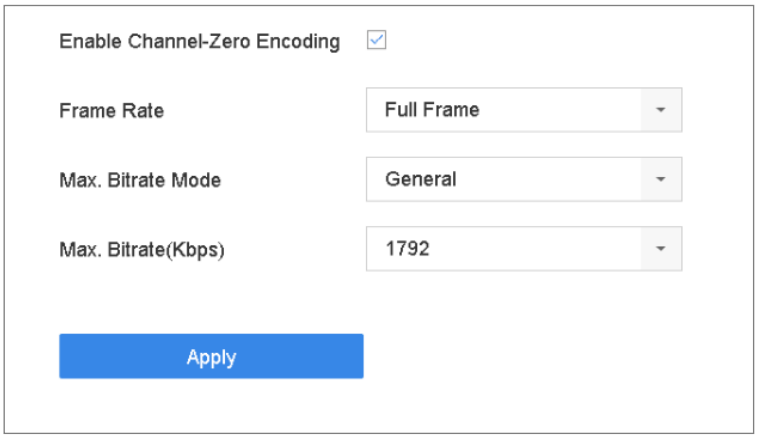


Figure 6-5 Live View, Channel-Zero Encoding

Step 5 Configure the **Frame Rate**, **Max. Bitrate Mode,** and **Max. Bitrate**. The higher frame rate and bitrate settings result in higher bandwidth requirement.

Step 6 Click **Apply.**

Result:

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

Chapter 7 PTZ Control

7.1 PTZ Control Wizard

Before you start

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

Purpose

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

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

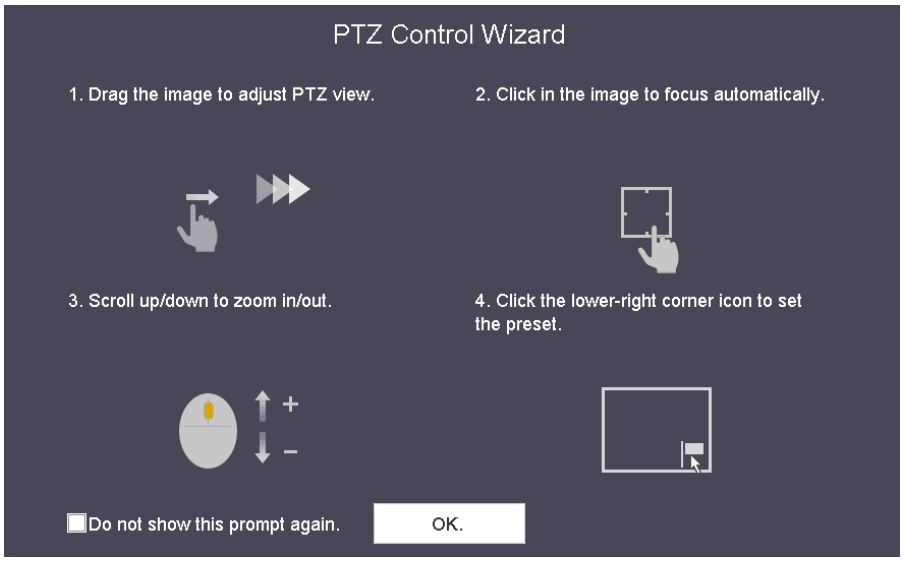


Figure 7-1 PTZ Control Wizard

Step 2 Follow the wizard to adjust the PTZ view, focus, and zoom in/out the camera.

Step 3 (Optional) Check *Do not show this prompt again.*

Step 4 Click **OK** to exit.

7.2 ConfigurePTZ Parameters

Purpose

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

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

Step 2 Click **PTZ Parameters Settings** to set the PTZ parameters.

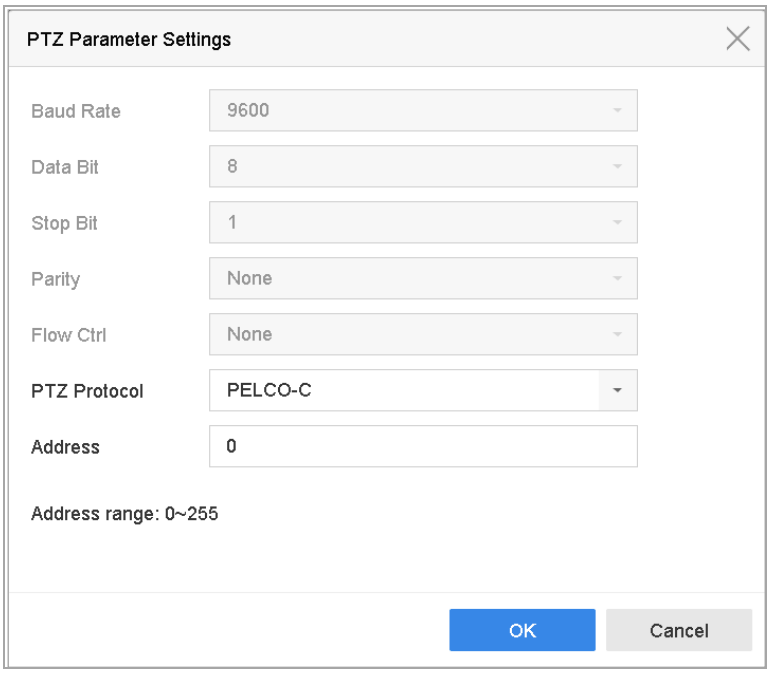


Figure 7-2 PTZ Parameters Settings

Step 3 Edit the parameters of the PTZ camera.

NOTE

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

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

7.3 Set PTZ Presets, Patrols & Patterns

Before you start:

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

7.3.1 Set a Preset

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Use the directional buttons on the PTZ control panel to wheel the camera to the location where you want to set preset, and the zoom and focus operations can be recorded in the preset as well.

Step 3 Click  in the lower right corner of live view to set the preset.



Figure 7-3 Set Preset

Step 4 Select the preset No. (1~255) from the drop-down list.

Step 5 Enter the preset name in the text field.

Step 6 Click **Apply** to save the preset.

Step 7 Repeat steps 2-6 to save more presets.

Step 8 (Optional) Click **Cancel** to cancel the location information of the preset.

Step 9 (Optional) Click  in the lower right corner of live view to view the configured presets.

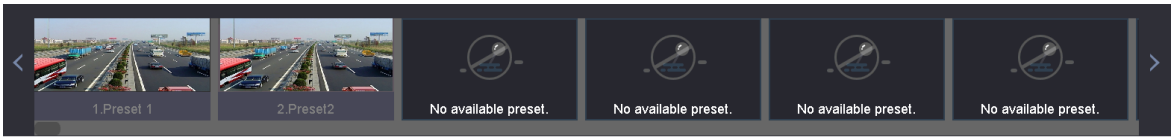


Figure 7-4 View the Configured Presets

7.3.2 Call a Preset

Purpose:

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

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

Step 2 Click  in the lower right corner of live view.

Step 3 Select the preset No. from the drop-down list.

Step 4 Click **Call** to call it.

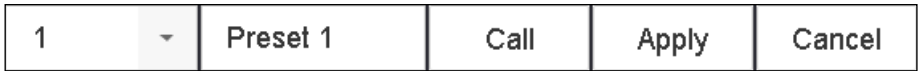


Figure 7-5 Call Preset (1)

Or click  in the lower right corner of live view, and click the configured preset to call it.

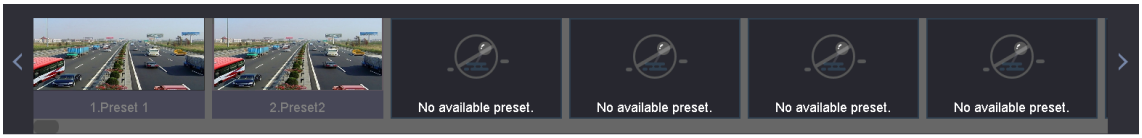


Figure 7-6 Call Preset (2)

7.3.3 Set a Patrol

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Patrol** to configure patrol.

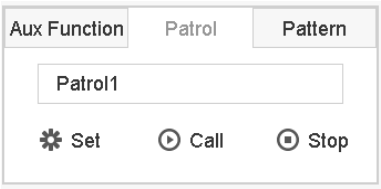


Figure 7-7 Patrol Configuration

Step 3 Select the patrol No. in the text field.

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

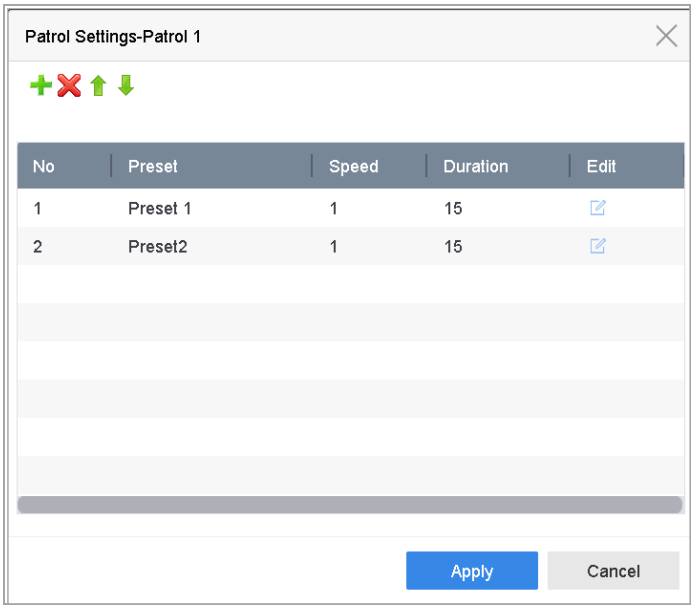


Figure 7-8 Patrol Settings

Step 5 Click  to add key point for the patrol.

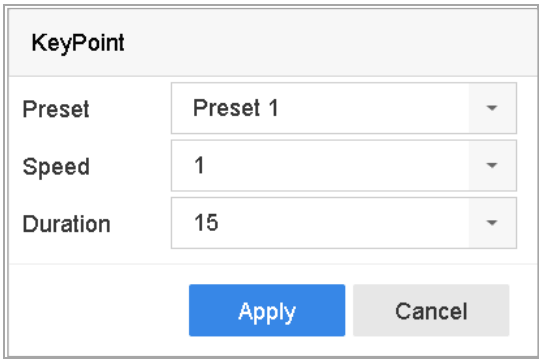


Figure 7-9 Key Point Configuration

1) Configure key point parameters.

Preset: It determines the order at which the PTZ will follow while cycling through the patrol.

Speed: It defines the speed at which the PTZ will move from one key point to the next.

Duration: It refers to the time span to stay at the corresponding key point.

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

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

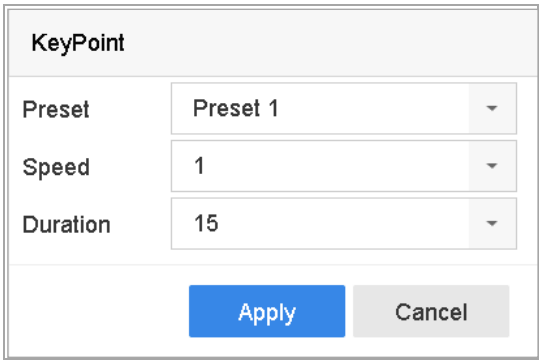


Figure 7-10 Edit Key Point

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

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

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

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

7.3.4 Call a Patrol

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Patrol** on the PTZ control panel.

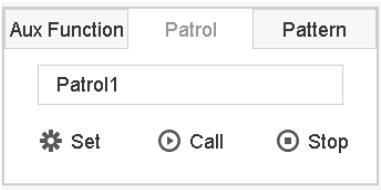


Figure 7-11 Patrol Configuration

Step 3 Select a patrol in the text field.

Step 4 Click **Call** to call it.

Step 5 (Optional) Click **Stop** to stop calling it.

7.3.5 Set a Pattern

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Pattern** to configure pattern.

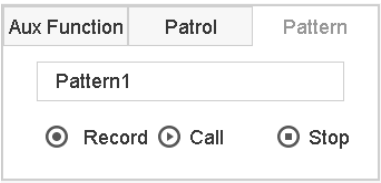


Figure 7-12 Pattern Configuration

Step 3 Select the pattern No. in the text field.

Step 4 Set the pattern.

1) Click **Record** to start recording.
2) Click corresponding buttons on the control panel to move the PTZ camera.
3) Click **Stop** to stop recording.

The movement of the PTZ is recorded as the pattern.

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

7.3.6 Call a Pattern

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Pattern** to configure pattern.

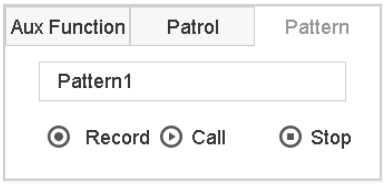


Figure 7-13 Pattern Configuration

Step 3 Select a pattern in the text field.

Step 4 Click **Call** to call it.

Step 5 (Optional) Click **Stop** to stop calling it.

7.3.7 Set Linear Scan Limits

Before you start:

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

Purpose:

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

NOTE

This function is supported by some certain models.

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

The PTZ control panel displays on the right of the interface.

Step 2 Click the directional buttons to wheel the camera to the location where you want to set the limit, and click **Left Limit** or **Right Limit** to link the location to the corresponding limit.

NOTE

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

7.3.8 Call Linear Scan

NOTE

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

Purpose:

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Linear Scan** to start the linear scan and click it again to stop it.

Step 3 (Optional) Click **Restore** to clear the defined left limit and right limit data.

NOTE

Reboot the camera to take the settings into effect.

7.3.9 One-touch Park

NOTE

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

Purpose

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Park (Quick Patrol)**, **Park (Patrol 1)** or **Park (Preset 1)** to activate the park action.

Park (Quick Patrol): The dome starts patrol from the predefined preset 1 to preset 32 in order after the park time. The undefined preset will be skipped.

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

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

NOTE

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

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

7.4 Auxiliary Functions

Before you start

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

Purpose

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

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

The PTZ control panel displays on the right of the interface.

Step 2 Click **Aux Function**.



Figure 7-14 Aux Function Configuration

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

Table 7-1 Description of Aux Functions Icons

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

Chapter 8 Storage

8.1 Storage Device Management

8.1.1 Install the HDD

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

8.1.2 Add the Network Disks

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

Adding a NAS

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

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

Step 3 Select NetHDD from the drop-down list.

Step 4 Set the type to NAS.

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

Step 6 Click **Search** to search the available NAS disks.

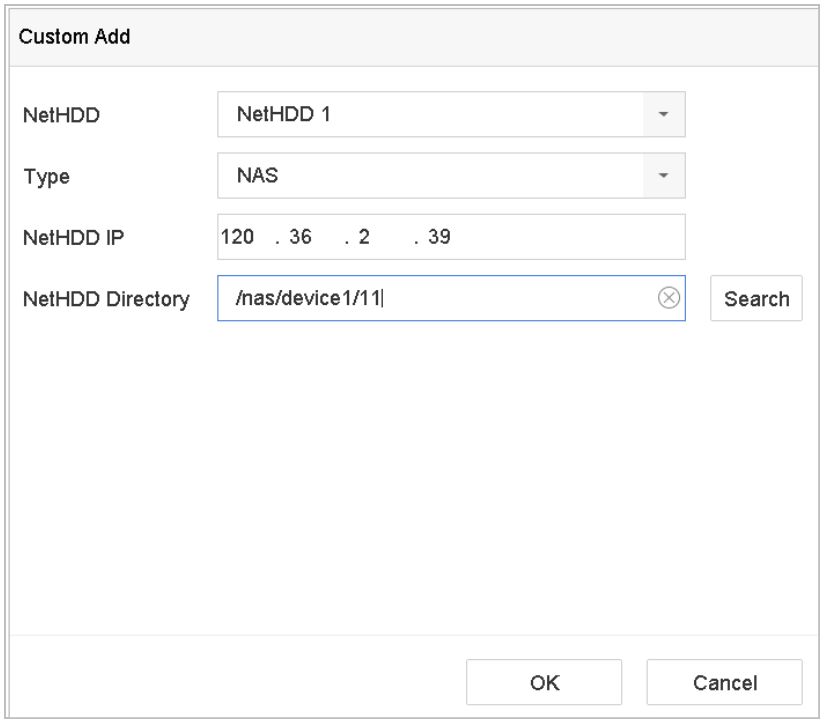


Figure 8-1 Add NAS Disk

Step 7 Select the NAS disk from the list shown below, or manually enter the directory in the NetHDD Directory text field.

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

Result:

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

Adding an IP SAN

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

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

Step 3 Select NetHDD from the drop-down list.

Step 4 Select the type to IP SAN.

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

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

Step 7 Select the IP SAN disk from the list.

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

NOTE

A single IP SAN disk can be added.

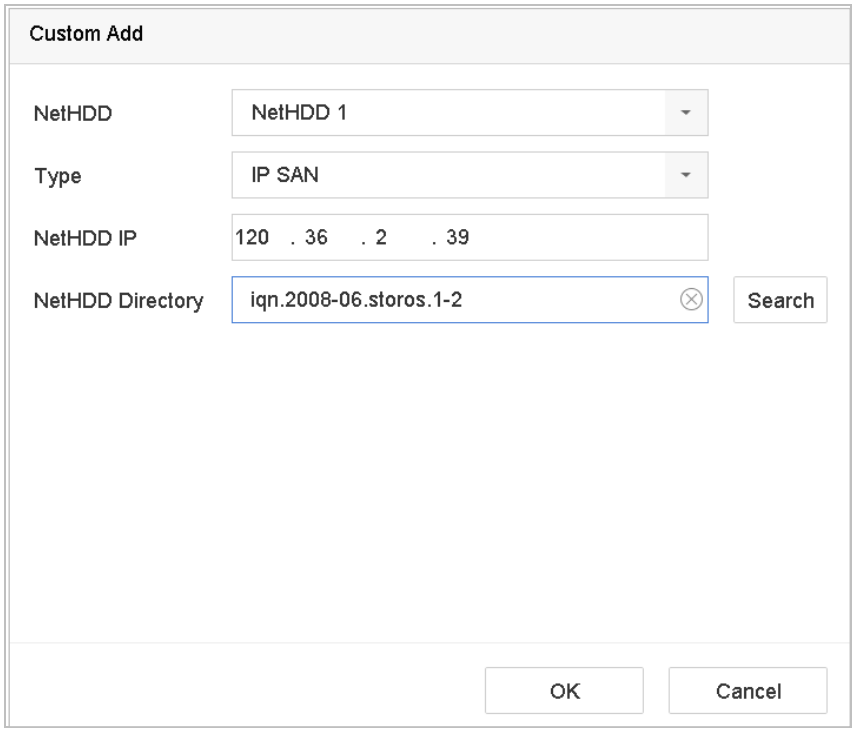


Figure 8-2 Add IP SAN Disk

Step 9 After having successfully added the IP SAN disk, return to the HDD Information menu. The added NetHDD will be displayed in the list.

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

8.1.3 Configure eSATA for Data Storage

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

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

Step 2 Select the eSATA type to Export or Record/Capture from **eSATA**.

Export: Use the eSATA for backup.

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



Figure 8-3 Set eSATA Mode

Step 3 When the eSATA type is set to Record/Capture, enter the storage device interface.

Step 4 Edit the property of the selected eSATA, or initialize it as required.

8.1.4 Configure eSATA for Auto Backup

After you set an auto backup plan, the system will back up the local record files to eSATA. It will back up the record files 24 hours ahead of the backup start time.

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 *8.1.3 Configure eSATA for Data Storage* for details.

Step 1 Go to **Storage** > **Auto Backup.**

Step 2 Check **Auto Backup**.

Step 3 Set the backup start time in **Start Backup at**.

NOTE

If the day experiences a failed backup, the device will back up the record files 48 hours ahead of the backup start time in the next day.

Step 4 Select channel(s) for backup.

Step 5 Select **Backup Stream Type** as your desire.

Step 6 Select **Overwrite** type.

Disable: When hard drive is full, it will stop writing.

Enable: When hard drive is full, it will continue to write new files by deleting the oldest files.

Step 7 Click **Apply** to finish.

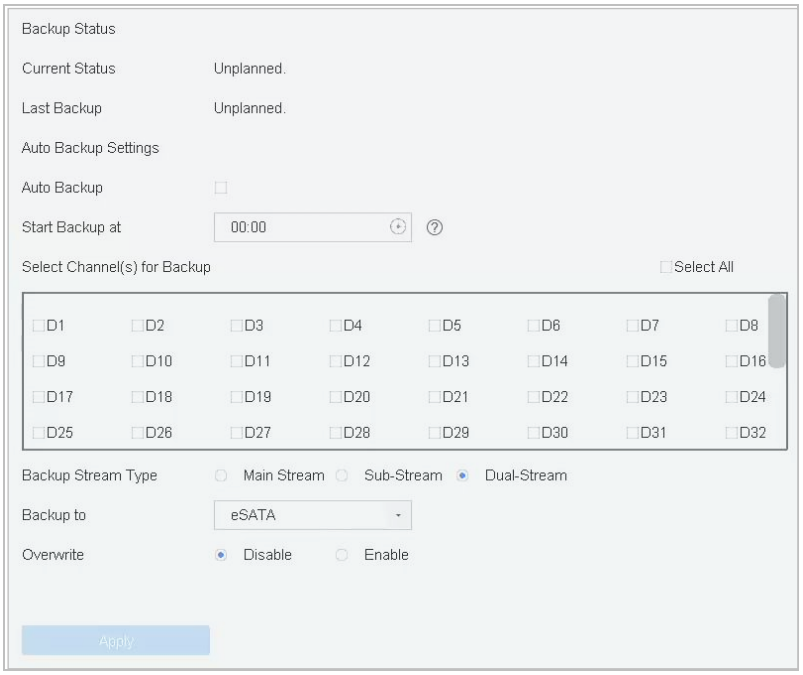


Figure 8-4 Configure eSATA for Auto Backup

8.2 Storage Mode

8.2.1 Configure HDD Groups

Purpose

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

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

Step 2 Check the checkbox to select the HDD to set the group.

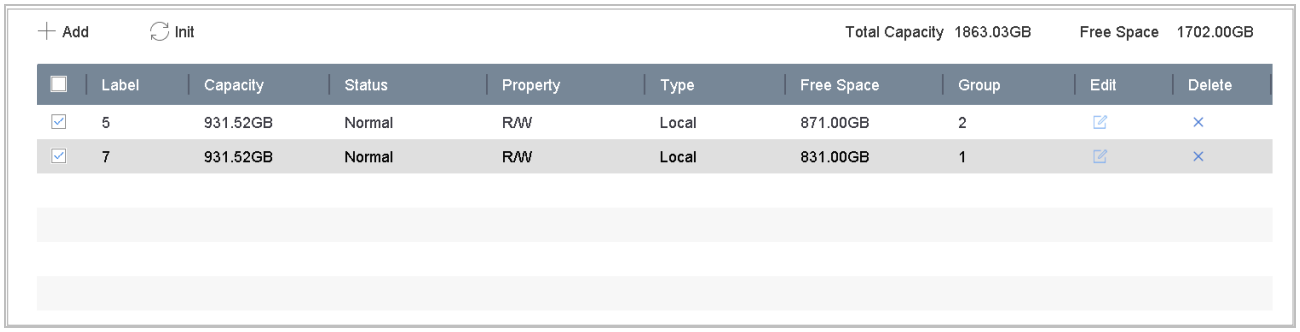


Figure 8-5 Storage Device

Step 3 Click  to enter the Local HDD Settings interface.

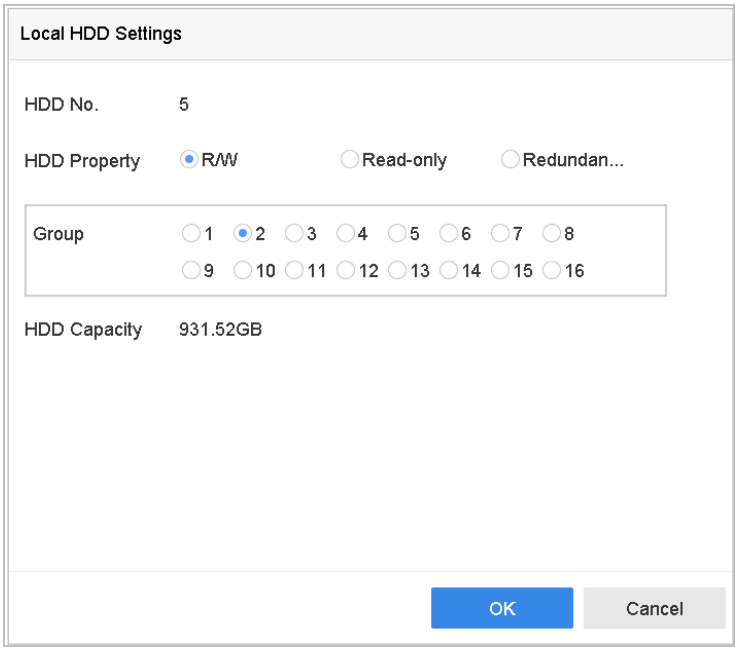


Figure 8-6 Local HDD Settings

Step 4 Select the Group number for the current HDD.

Step 5 Click **OK**.

NOTE

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

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

Step 7 Check **Group** tab.

Step 8 Select the group No. from the list.

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

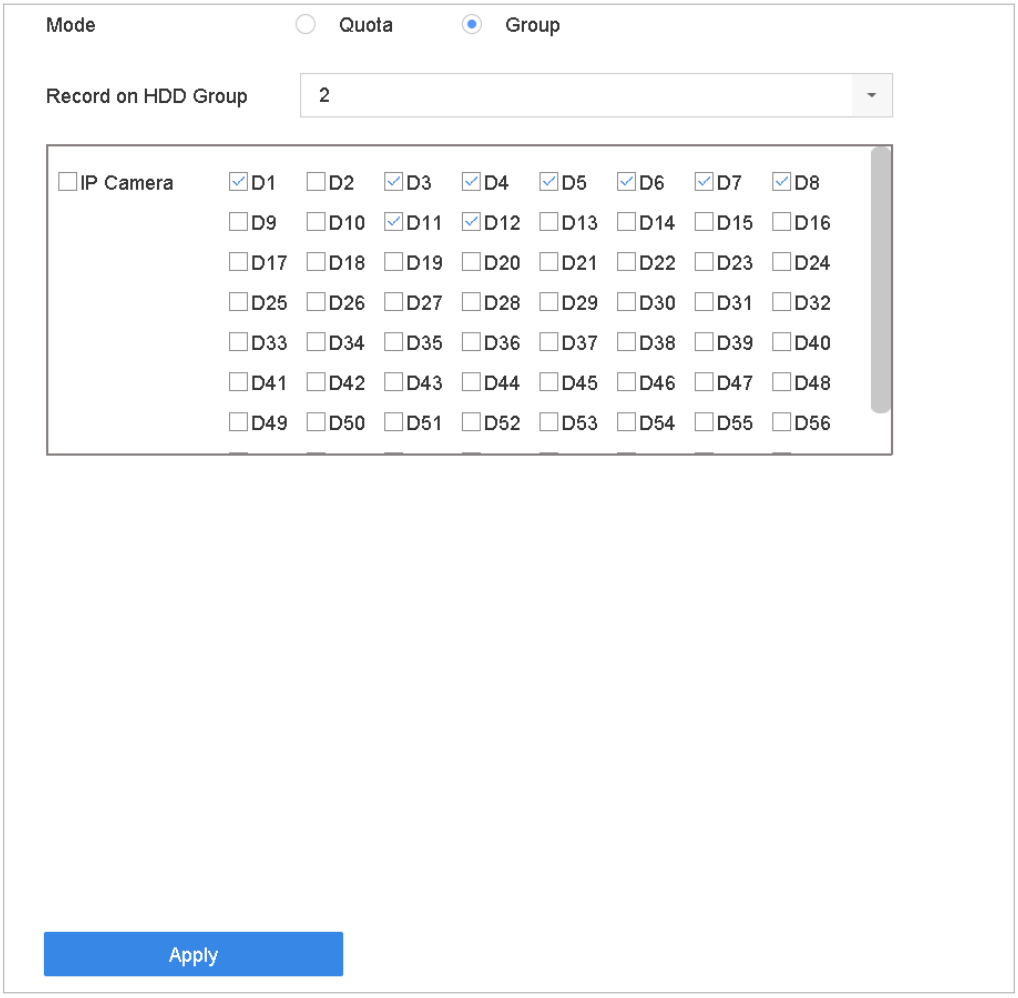


Figure 8-7 Storage Mode-HDD Group

Step 10 Click **Apply**.

NOTE

Reboot the device to activate the new storage mode settings.

8.2.2 Configure HDD Quota

Purpose

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

Step 1 Go to **Storage**> **Storage Mode**.

Step 2 Check the checkbox of **Quota** tab.

Step 3 Select a camera to set quota.

Step 4 Enter the storage capacity in the text fields of **Max. Record Capacity (GB)** and **Max. Picture Capacity (GB)**.

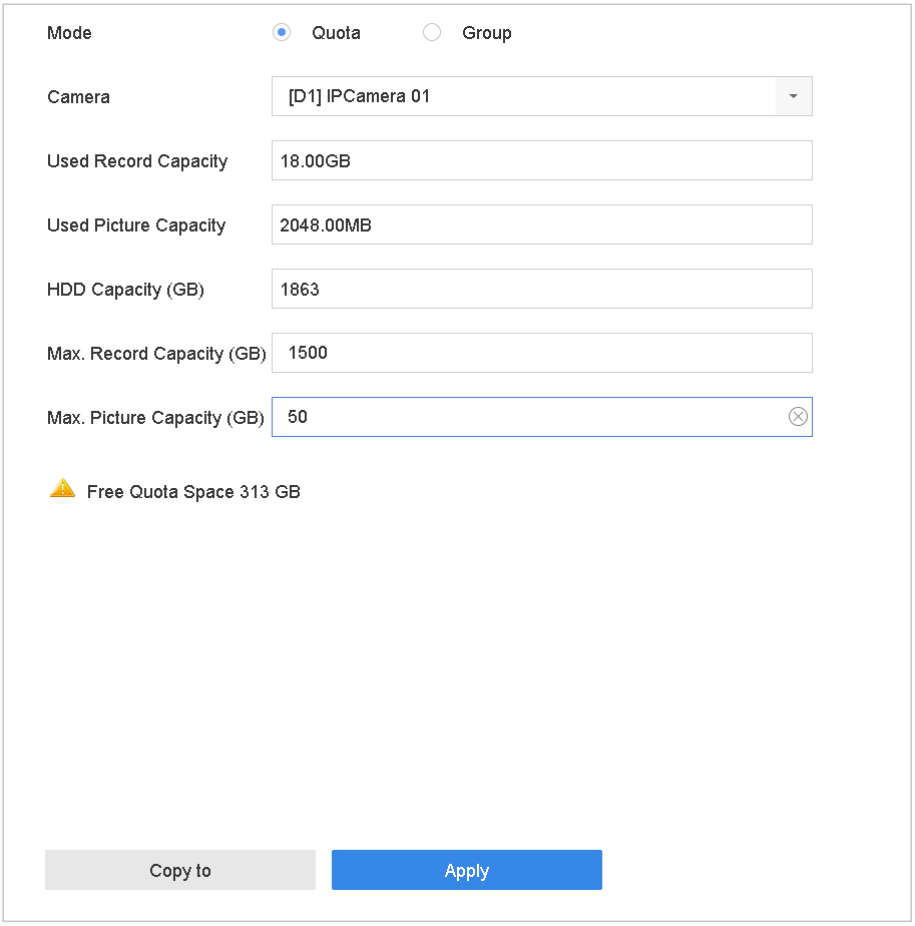


Figure 8-8 Storage Mode-HDD Quota

Step 5 (Optional) You can click **Copy to** if you want to copy the quota settings of the current camera to other cameras.

Step 6 Click **Apply**.

NOTE

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

NOTE

Reboot the device to activate the new storage mode settings.

8.3 Recording Parameters

8.3.1 Main Stream

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

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

Frame Rate (FPS - Frames Per Second): refers to how many frames are captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

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

Bitrate: The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit and not distance/time unit.

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

NOTE

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

8.3.2 Sub-Stream

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

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

8.3.3 Picture

The picture refers to the live picture capture in continuous or event recording type. (**Storage** > **Capture Schedule** > **Advanced**)

Picture Quality: Set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.

Interval: The interval of capturing live picture.

Capture Delay Time: The duration of capturing pictures.

8.3.4 ANR

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

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

8.3.5 Configure Advanced Recording Settings

Step 1 Go to **Storage** > **Schedule Settings > Record Schedule/Capture Schedule**.

Step 2 Check **Enable** to enable scheduled recording.

Step 3 Click **Advanced** to set the recording parameters.

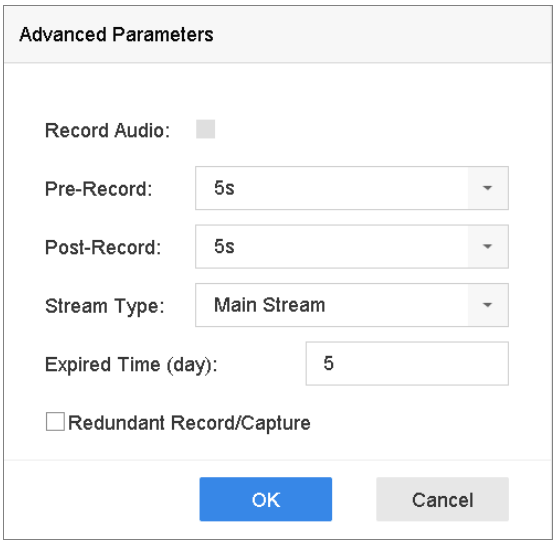


Figure 8-9 Advanced Record Settings

Record Audio: Check the checkbox to enable or disable audio recording.

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

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

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

Redundant Record/Capture: By enabling redundant record or capture you save the record and captured picture in the redundant HDD. See *Chapter Configure Redundant Recording and Capture*.

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

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

8.4 Configure Recording Schedule

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

Before you start

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

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

Refer to *Chapter 8.1.2* Add the Network Disk for network HDD connections.

Step 1 Go to **Storage** > **Recording Schedule**.

Step 2 Select a camera.

Step 3 Check the **Enable Schedule**.

Step 4 Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

Different recording types are configurable.

Continuous: scheduled recording.

Event: recording triggered by all event triggered alarm.

Motion: recording triggered by motion detection.

Alarm: recording triggered by alarm.

M/A: recording triggered by either motion detection or alarm.

M&A: recording triggered by motion detection and alarm.

POS: recording triggered by POS and alarm.

Step 5 Select a day and click-and-drag the mouse on the time bar to set the record schedule.

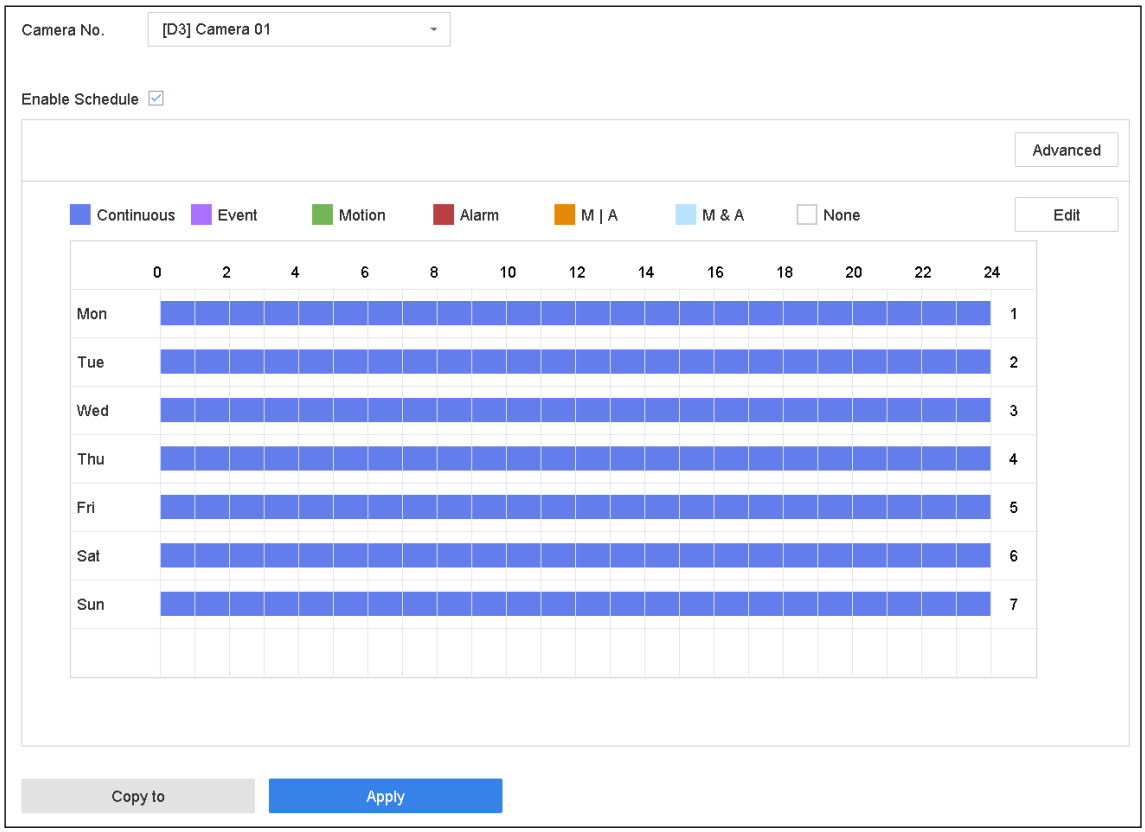


Figure 8-10 Record Schedule

Step 6 Repeat the above steps to schedule recording or capture for other days in the week.

NOTE

The all-day continuous recording is configured for the device by factory default.

Step 7 (Optional) Copy the schedule settings of the one day to the other days of the week or holiday.

1) Click the  tab.
2) Select the day (s) to duplicate with the same schedule settings.
3) Click **OK**.

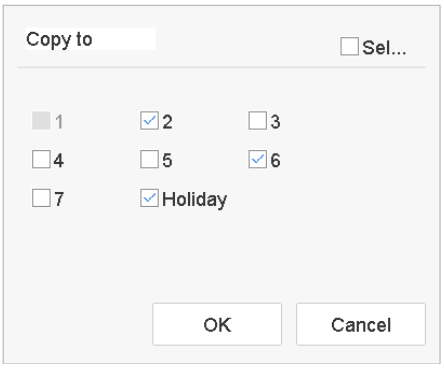


Figure 8-11 Copy Schedule to Other Days

Step 8 Click **Apply**.

NOTE

To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and Event triggered recording and capture, you must configure the motion detection settings, alarm input settings and other events as well. Please refer to Chapter 12 Event and Alarm Settings and Chapter 13 VCA Event Alarm for details for details.

8.5 Configure Continuous Recording

Step 1 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 2 Set the continuous main stream/sub-stream recording parameters for the camera.

Step 3 Go to **Storage** > **Recording Schedule**.

Step 4 Select the recording type to **Continuous**.

Step 5 Drag the mouse on the time bar to set the continuous recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.6 Configure Motion Detection Triggered Recording

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

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

Step 2 Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to Chapter 12.3 Configure Motion Detection Alarm for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Motion**.

Step 7 Drag the mouse on the time bar to set the motion detection recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.7 Configure Event Triggered Recording

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

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

Step 2 Configure the event detection and select the channel (s) to trigger the recording when event occurs. Refer to Chapter 12 Event and Alarm Settings and Chapter 13 VCA Event Alarm for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Event**.

Step 7 Drag the mouse on the time bar to set the event detection recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.8 Configure Alarm Triggered Recording

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

Step 1 Go to **System** > **Event** > **Normal Event > Alarm Input**.

Step 2 Configure the alarm input and select the channel (s) to trigger the recording when alarm occurs.

Refer to Chapter 12 Event and Alarm Settings and Chapter 13 VCA Event Alarm for details for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the recording type to **Alarm**

Step 7 Drag the mouse on the time bar to set the alarm recording schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.9 Configure POS Event Triggered Recording

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

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

Step 2 Configure the POS and select the channel (s) in the **Event Linkage** to trigger the recording when POS event occurs.

Refer to Chapter 13 VCA Event Alarm for details.

Step 3 Go to **Camera** > **Encoding Parameters** > **Recording Parameters**.

Step 4 Set the event main stream/sub-stream recording parameters for the camera.

Step 5 Go to **Storage** > **Recording Schedule**.

Step 6 Select the record type to **POS Event**.

Step 7 Set the schedule for the POS event triggered recording. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.10 Configure Picture Capture

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

Step 1 Go to **Storage** > **Capture Schedule > Advanced**.

Step 2 Set the picture parameters.

- **Resolution**: Set the resolution of the picture to capture.
- **Picture Quality**: Set the picture quality to low, medium or high. The higher picture quality results in more storage space requirement.
- **Interval**: The interval of capturing live picture.
- **Capture Delay Time**: The duration of capturing pictures.

Step 3 Go to **Storage** > **Capture Schedule**.

Step 4 Select the camera to configure the picture capture.

Step 5 Set the picture capture schedule. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.11 Configure Holiday Recording and Capture

Purpose:

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

Step 1 Go to **System** > **Holiday Setting**s.

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

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

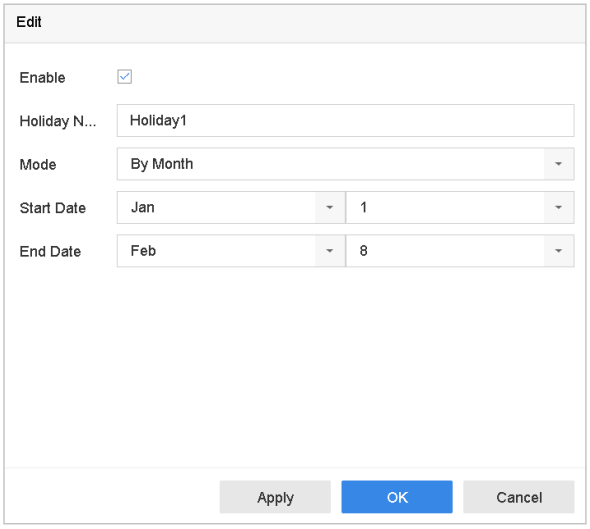


Figure 8-12 Edit Holiday Settings

1) Edit the holiday name.
2) Select the mode to by date, by week or by month.
3) Set the start and end date of the holiday.
4) Click **OK**.

Step 4 Set the schedule for the holiday recording. Refer to Chapter 8.4 Configure Recording Schedule for details.

8.12 Configure Redundant Recording and Capture

Purpose:

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

NOTE

You must set the storage mode to *Group* before you set the HDD property to Redundancy. For detailed information, please refer to Chapter 8.2.1 Configure HDD Group. There should be at least another HDD which is in Read/Write status.

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

Step 2 Select a **HDD** from the list and Click  to enter the Local HDD Settings interface.

Step 3 Set the HDD property to **Redundancy**.

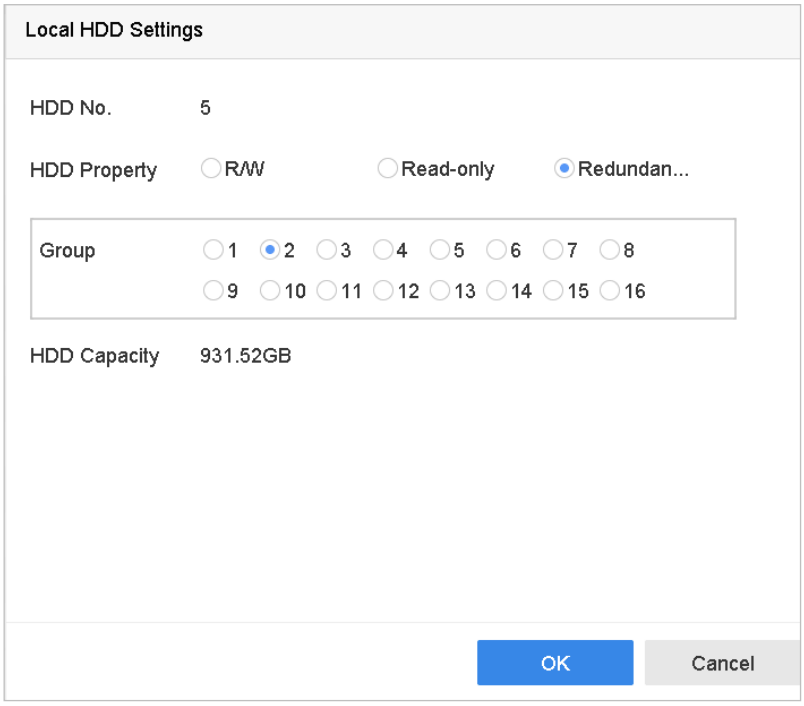


Figure 8-13 HDD Property-Redundancy

Step 4 Go to **Storage** > **Schedule Settings > Record Schedule/Capture Schedule**.

Step 5 Click **Advanced** to set the camera recording parameters.

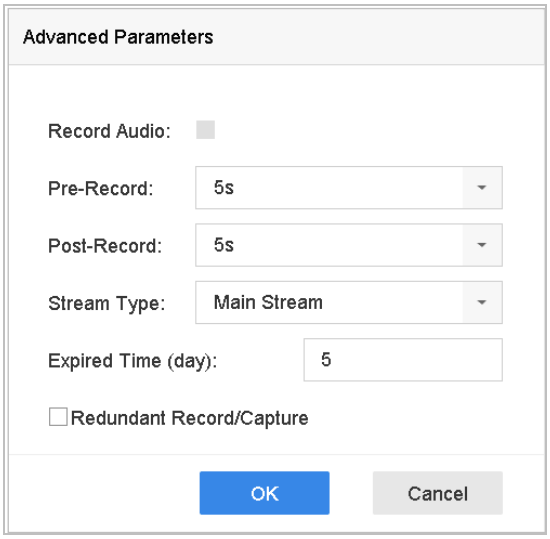


Figure 8-14 Record Parameters

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

Step 7 Click **OK** to save settings.

Chapter 9 Disk Array (RAID)

Purpose

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

Disk arrays are supported by Ultra Series device only.

9.1 Create a Disk Array

Purpose

The device supports software-based disk arrays. Enable the RAID function as required. Two ways are available for creating an array: one-touch configuration and manual configuration. The following flow chart shows the process of creating array.

9.1.1 Enable a RAID

Purpose

Perform the following steps to enable the disk array function.

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

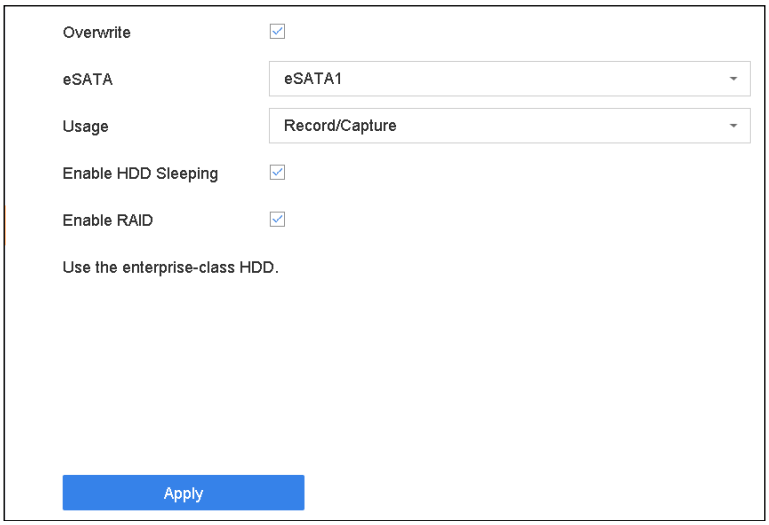


Figure 9-1 Advanced

Step 2 Check **Enable RAID**.

Step 3 Click **Apply**.

Step 4 Reboot the device to have settings take effect.

9.1.2 One-Touch Creation

Purpose

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

Before You Start

- Enable the RAID function. For details, refer to Chapter 9.1.1 Enable a RAID.
- 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.

Step 1 Go to **Storage > RAID Setup > Physical Disk**.

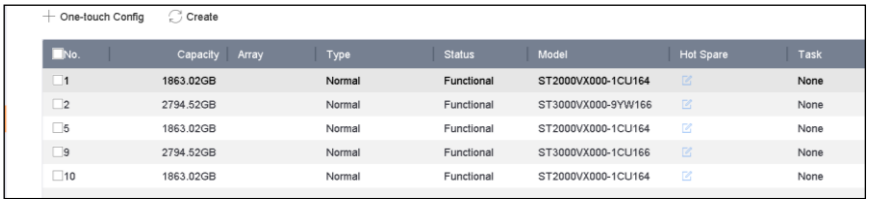


Figure 9-2 Physical Disk

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

Step 3 Edit the array name in **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.

Step 4 When a message box pops up when the array creation is completed, click **OK** on it.

Step 5 Optionally, the device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** to view the information of the created arrray.

9.1.3 Manual Creation

Purpose

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

Step 1 Go to **Storage > RAID Setup > Physical Disk**.

Step 2 Click **Create**.

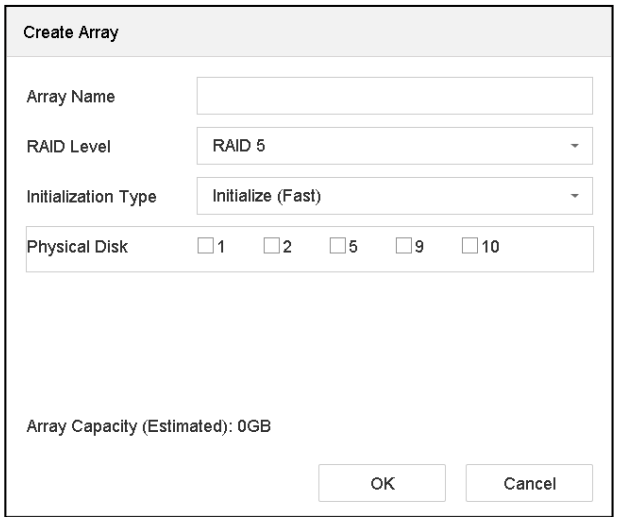


Table 9-1 Create Array Window

Step 3 Input the array name.

Step 4 Select **RAID Level** as **RAID 0, RAID 1, RAID 5, RAID 6**, or **RAID 10** as required.

Step 5 Select the physical disks to constitute the array.

Table 9-2 Required Number of HDDs

RAID Level	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.

Step 6 Click **OK**.

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

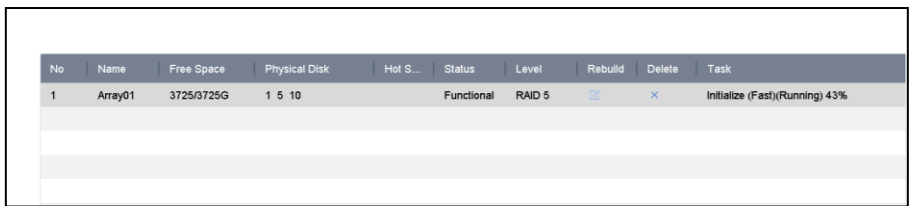


Figure 9-3 Array List

9.2 Rebuild an Array

Purpose:

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

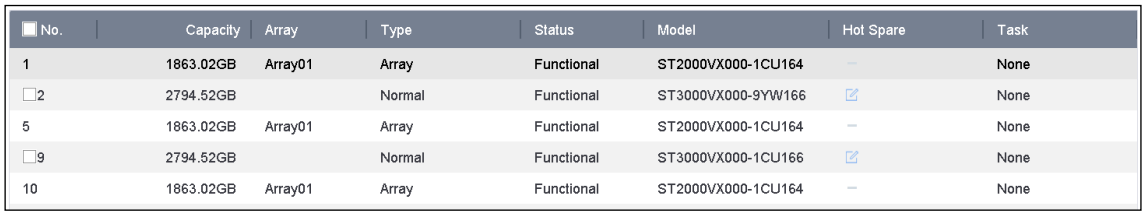
- Functional: No disk loss in the array.
- Offline: The number of lost disks has exceeded the limit.
- Degraded: If any HDD fails in the array, the array degrades. Restore it to Functional status by rebuilding the array.

9.2.1 Configure a Hot Spare Disk

Purpose

Hot spare disks are required for disk array automatic rebuilding.

Step 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 9-4 Physical Disk

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

9.2.2 Automatically Rebuild an Array

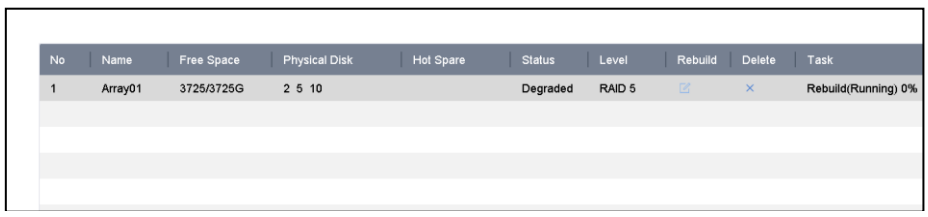
Purpose

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

Before You Start

Create hot spare disks. For details, refer to Chapter 9.2.1 Configure a Hot Spare Disk.

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



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

Figure 9-5 Array List

9.2.3 Manually Rebuild an Array

Purpose

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.

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

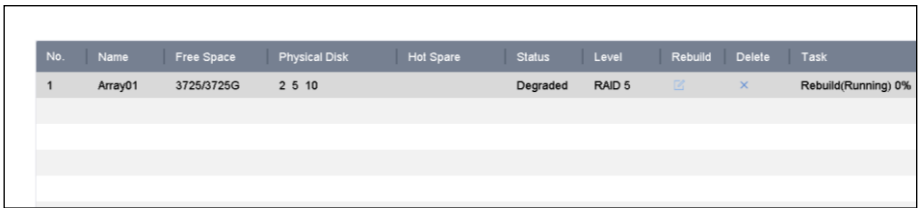


Figure 9-6 Array List

Step 2 Click of the degraded array.

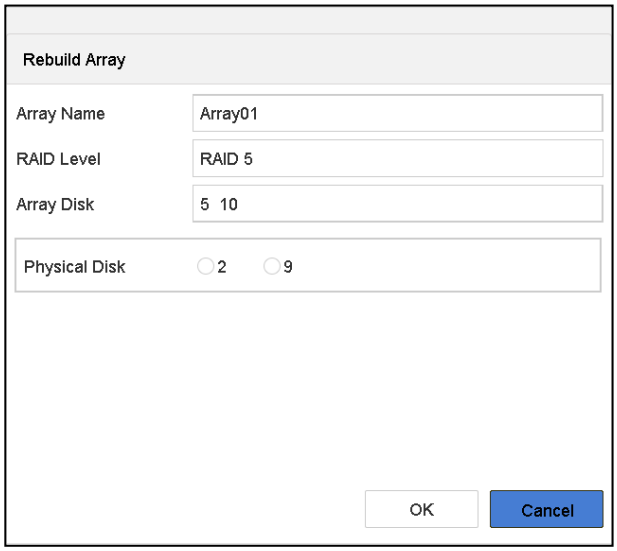


Figure 9-7 Rebuild Array

Step 3 Select the available physical disk.

Step 4 Click **OK**.

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

9.3 Delete an Array

NOTE

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

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

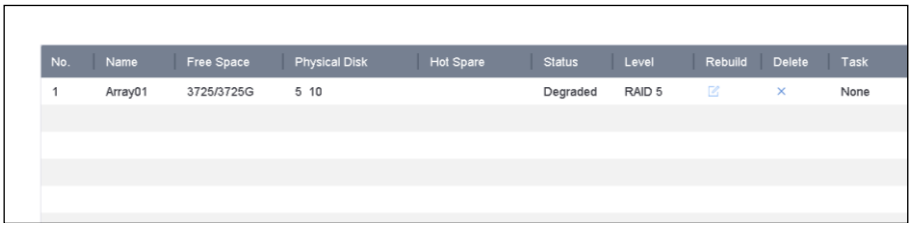


Figure 9-8 Array List

Step 2 Click ✕ of the array to delete it.

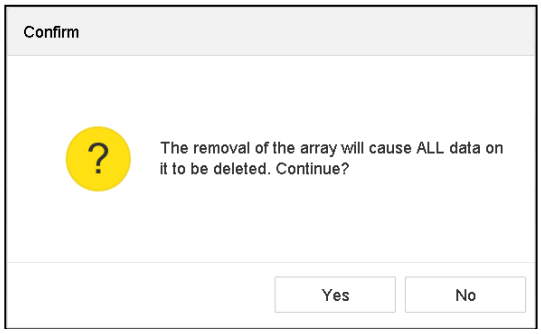


Figure 9-9 Attention

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

9.4 Check and Edit Firmware

Purpose

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

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

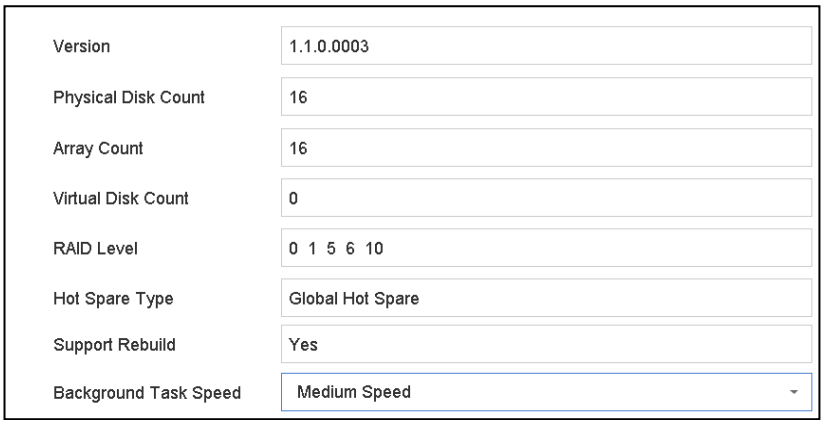


Figure 9-10 Firmware

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

Step 3 Click **Apply**.

Chapter 10 File Management

10.1 Search and Export All Files

10.1.1 Search Files

Purpose

Specify detailed conditions to search videos and pictures.

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

Step 2 Specify detailed conditions, including time, camera, event type, etc.

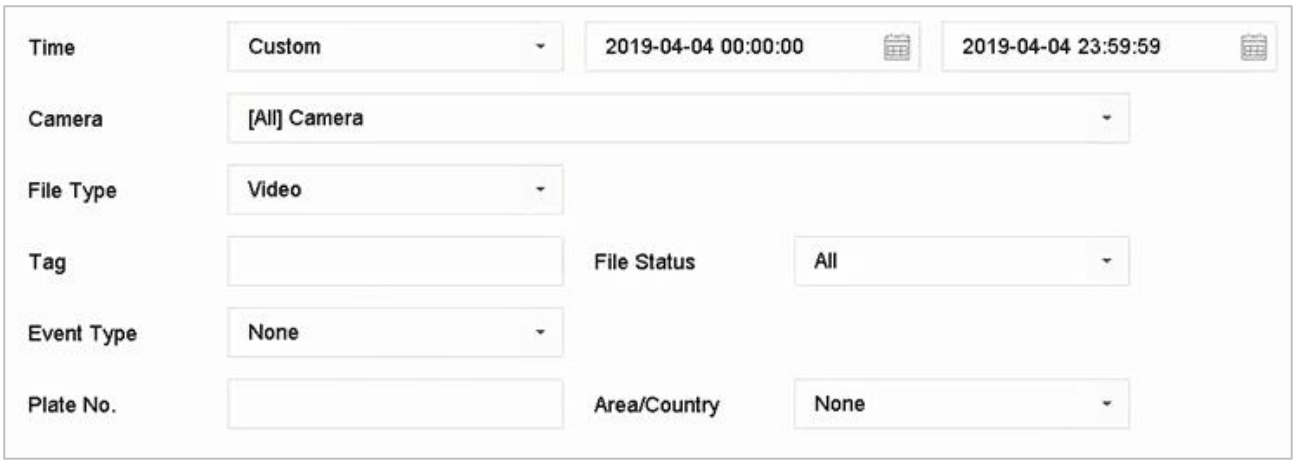


Figure 10-1 Search All Files

Step 3 Click **Search** to display results. The matched files will be displayed.

10.1.2 Export Files

Purpose

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

Step 1 Search files to export. For details, see *10.1.1 Search Files*.

Step 2 Click files to select and click **Export**.

Step 3 Select the file to export as **Video and Log** and click **OK**.

Step 4 Click **OK** to export files to backup device.

10.2 Search and Export Human Files

10.2.1 Search Human Files

Purpose

Specify detailed conditions by which to search human pictures and videos.

Before You Start

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

Step 1 Go to **File Management** > **Human Files**.

Step 2 Select **Time** and **Camera** to search.

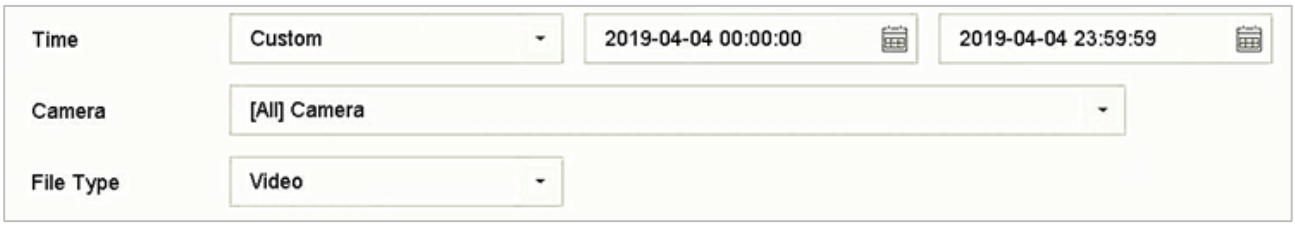


Figure 10-2 Search Human Files

Step 3 Click **Search** to display results. The matched files are displayed in thumbnails or a list.

Step 4 Select **Target Picture** or **Source Picture** in the menu bar to display related pictures only.

- **Target Picture**: Display the search results of people close-ups.
- **Source Picture**: Display the search results of original pictures captured by the camera.

10.2.2 Export Human Files

Purpose

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

Step 1 Search for the human files to export. For details, see *10.2.1 Search Human Files*.

Step 2 Click to select files and click **Export**.

Step 3 Select the file to export as **Video and Log** and click **OK**.

Step 4 Click **OK** to export files to backup device.

10.3 Search and Export Vehicle Files

10.3.1 Search Vehicle Files

Purpose

Specify detailed conditions by which to search vehicle pictures and videos.

Before You Start

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

Step 1 Go to **File Management** > **Vehicle Files**.

Step 2 Specify detailed conditions, including **Time, Camera**, **Plate No.**, and **Area/Country**.

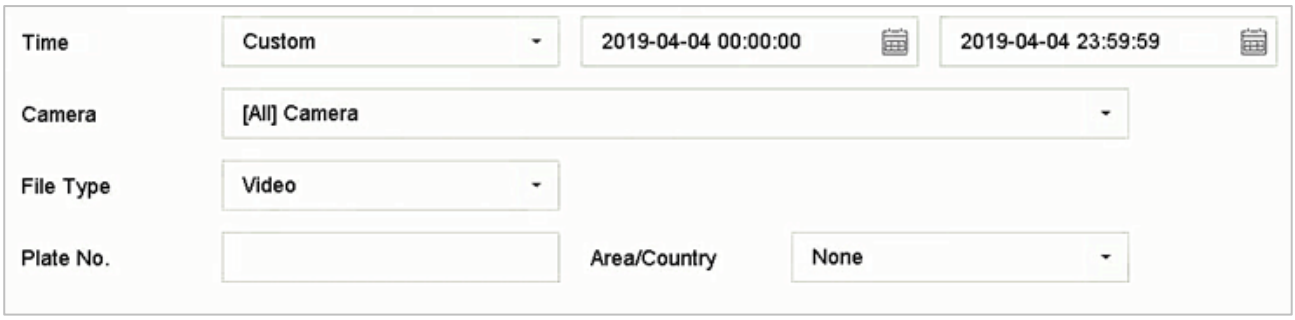


Figure 10-3 Search Vehicle Files

Step 3 Click **Search** to display results. The matched files are displayed in thumbnails or a list.

Step 4 Select **Target Picture** or **Source Picture** in the menu bar to display related pictures only. Select **Video** or **Picture** to specify the file type.

- **Target Picture**: Display the search results of vehicle close-ups.
- **Source Picture**: Display the search results of original pictures captured by the camera.

10.3.2 Export Vehicle Files

Purpose

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

Step 1 Search for the vehicle files to export. For details, see *10.3.1 Search Vehicle Files*.

Step 2 Optionally, Check **Backup License Plate Statistics Info** to export license plate statistics information later.

Step 3 Select files as your desire.

Step 4 Click **Export**.

Step 5 Select the file to export as **Video and Log** and click **OK**.

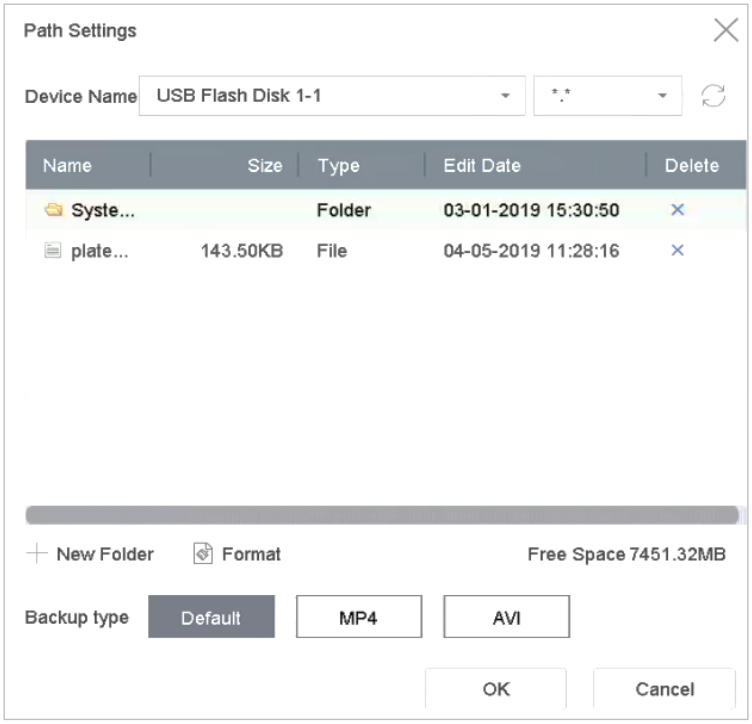


Figure 10-4 Export Vehicle File

Step 6 Click **OK** to export files to backup device.

10.4 Search History Operation

10.4.1 Save Search Conditions

Purpose

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

Step 1 Go to **File Management** > **All Files/People Appearance File/Vehicle File**.

Step 2 Set the search conditions.

Step 3 Click **Save**.

Step 4 Enter a name in text field and click **Finished**. The saved search conditions will be displayed in search history list.

10.4.2 Call Search History

Purpose

You can quickly search files by calling the search history.

Step 1 Go to **File Management** > **All Files/Human Files/Vehicle Files**.

Step 2 Click a search conditon to search files quickly.

Chapter 11 Playback

11.1 Play Video Files

11.1.1 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.

Step 1 On the Live View window of the selected camera, move the cursor to the window bottom to access the toolbar.

Step 2 Click  to start instant playback.



Figure 11-1 Playback Interface

11.1.2 Play Normal Video

Step 1 Go to **Playback.**

Step 2 Check one or more cameras in the camera list to start playing the video.

Step 3 Select a date in the calendar to start playing the video.

Step 4 Use the toolbar in the bottom part of the playback interface to control the playing and perform a series of operations. Refer to Chapter 10.2 Playback Operations 8.2.

Step 5 Click the channel(s) to execute simultaneous playback of multiple channels.



Figure 11-2 Playback Interface

NOTE

256x playing speed is supported.

11.1.3 Play Smart Searched Video

In smart playback mode, the device can analyze the video containing the motion, line, or intrusion detection information, mark it in red, and play the smart searched video.

NOTE

The smart playback must be in the single-channel playing mode.

Step 1 Go to **Playback**.

Step 2 Start playing the video of camera.

Step 3 Click **Smart**.

Step 4 From the toolbar at the bottom of the playing window, click the motion/line crossing/ intrusion icon for search.



Figure 11-3 Playback by Smart Search

Step 5 Set the rules and areas for smart search of line crossing detection, intrusion detection or motion detection event triggered recording.

●Line Crossing Detection

1) Click the icon.
2) Click on the image to specify the start point and end point of the line.

●Intrusion Detection

1) Click the icon.
2) Specify 4 points to set a quadrilateral region for intrusion detection. Only one region can be set.

●Motion Detection

1) Click the icon.
2) Hold the mouse on the image to draw the detection area manually.
3) Click Search to search the matched video and start to play it.

11.1.4 Play Custom Searched Files

You can play the files by custom search with different conditions.

Step 1 Go to **Playback**.

Step 2 Select a camera or cameras from the list.

Step 3 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 4 Enter the search conditions for the files, e.g., time, file status, event type, etc.

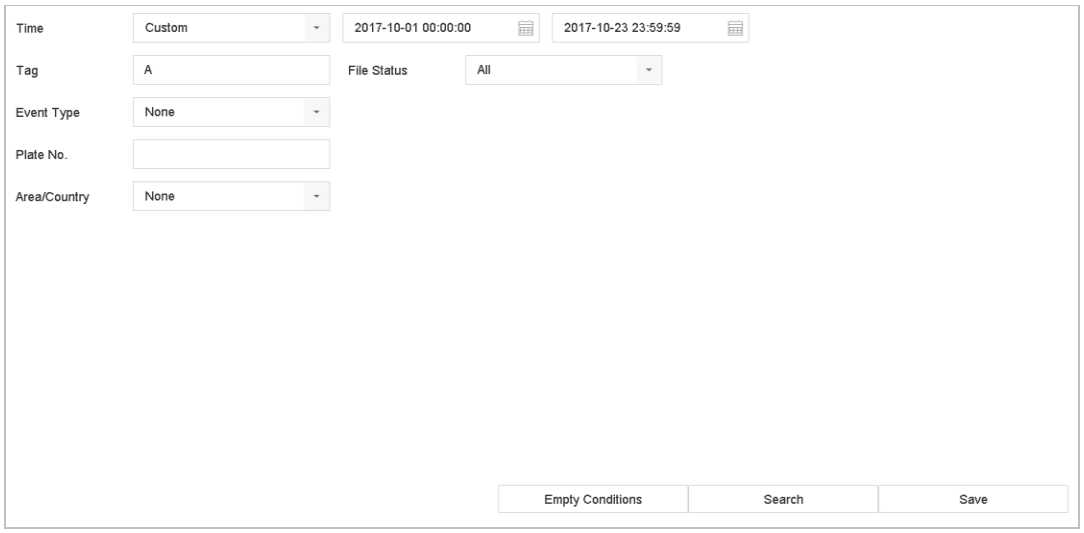


Figure 11-4 Custom Search

Step 5 Click **Search.**

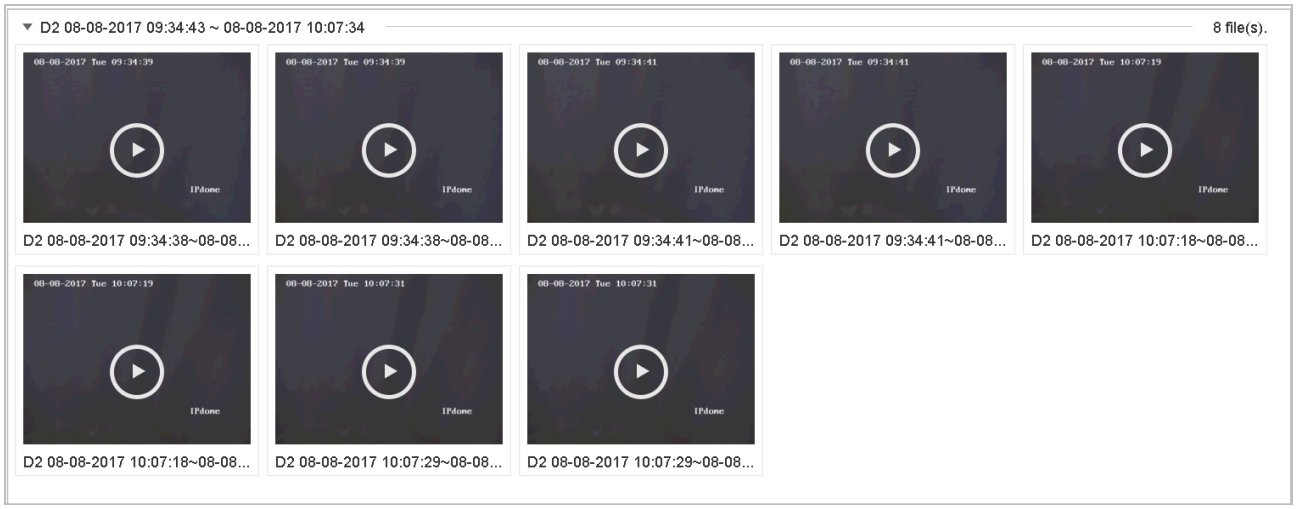


Figure 11-5 Custom Searched Video Files

Step 6 On the search results interface, select a file and click to start playing the video.

11.1.5 Play Tag Files

Purpose

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

Before playing back by tag:

Add Tag Files

Step 1 Go to **Playback**.

Step 2 Search and play back the video file(s).

Step 3 Click  to add the tag.

Step 4 Edit the tag information.

Step 5 Click **OK**.

NOTE

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

Edit Tag Files

You can edit the tag information for the existed tag video.

Step 1 Go to **Playback**.

Step 2 Click **Tag**.

The available tags are white marked and displayed in the time bar.

Step 3 Point the white marked tag in the time bar to access the tag information.

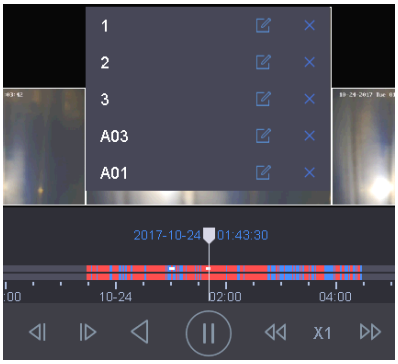


Figure 11-6 Edit Tag Files

Step 4 Click  to edit the tag name.

Step 5 Click **OK**.

Play Tag Files

Step 1 Go to **Playback**.

Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the tag files, including the time and the tag keyword.

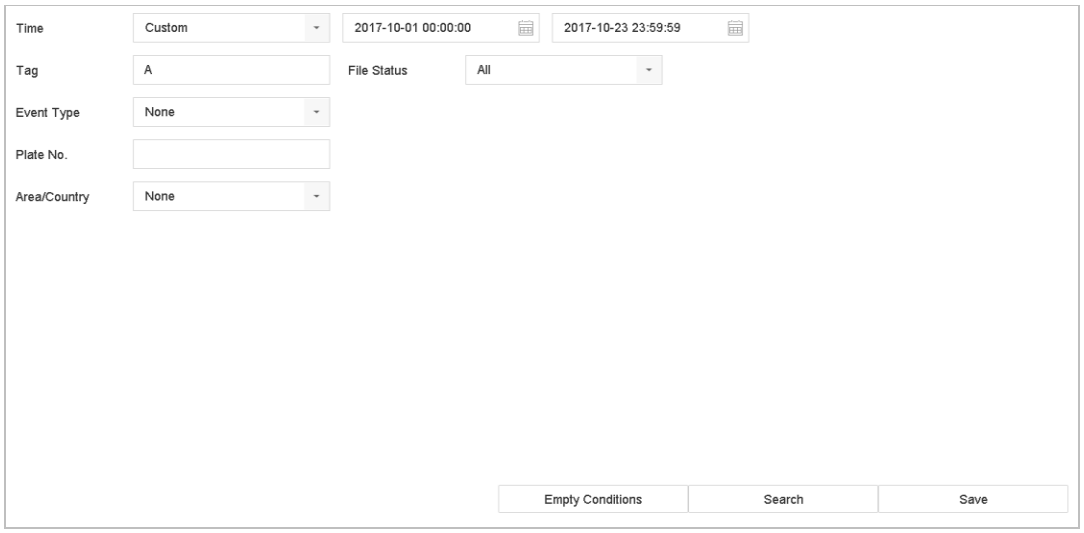


Figure 11-7 Tag Search

Step 4 Click **Search.**

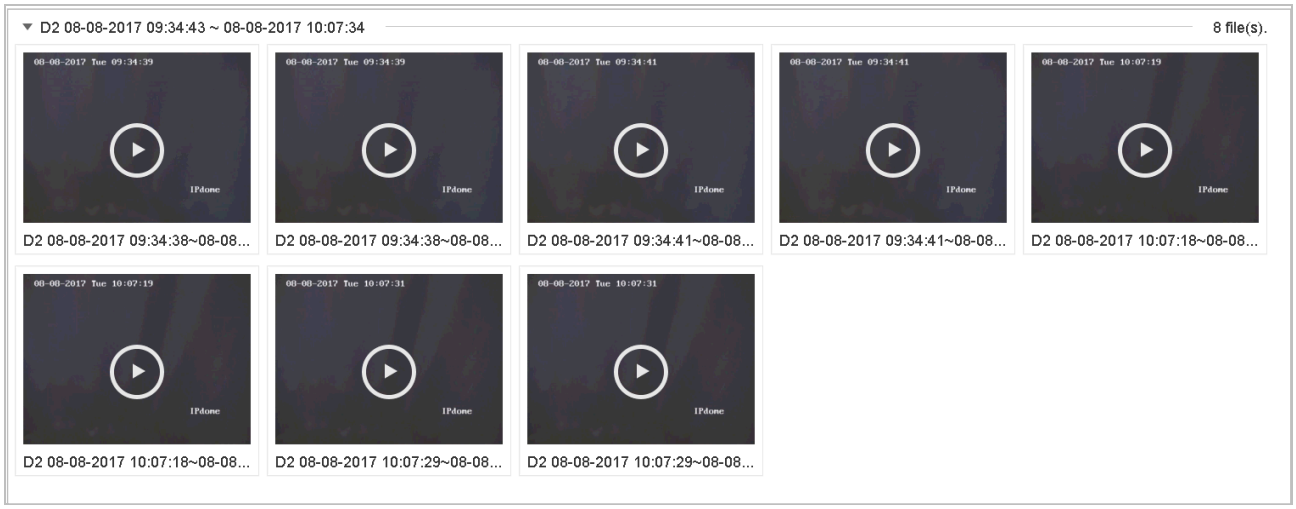


Figure 11-8 Searched Tag Files

Step 5 On the search results interface, select a tag file and click to start playing the video.

11.1.6 Play Event Files

Purpose

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

Step 1 Go to **Playback**.

Step 2 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 3 Enter the search conditions for the event files, e.g., time, event type, file status, vehicle information (for vehicle detection event), etc.

Step 4 Click **Search.**

Step 5 On the search results interface, select an event video file/picture file and double click to start playing the video.

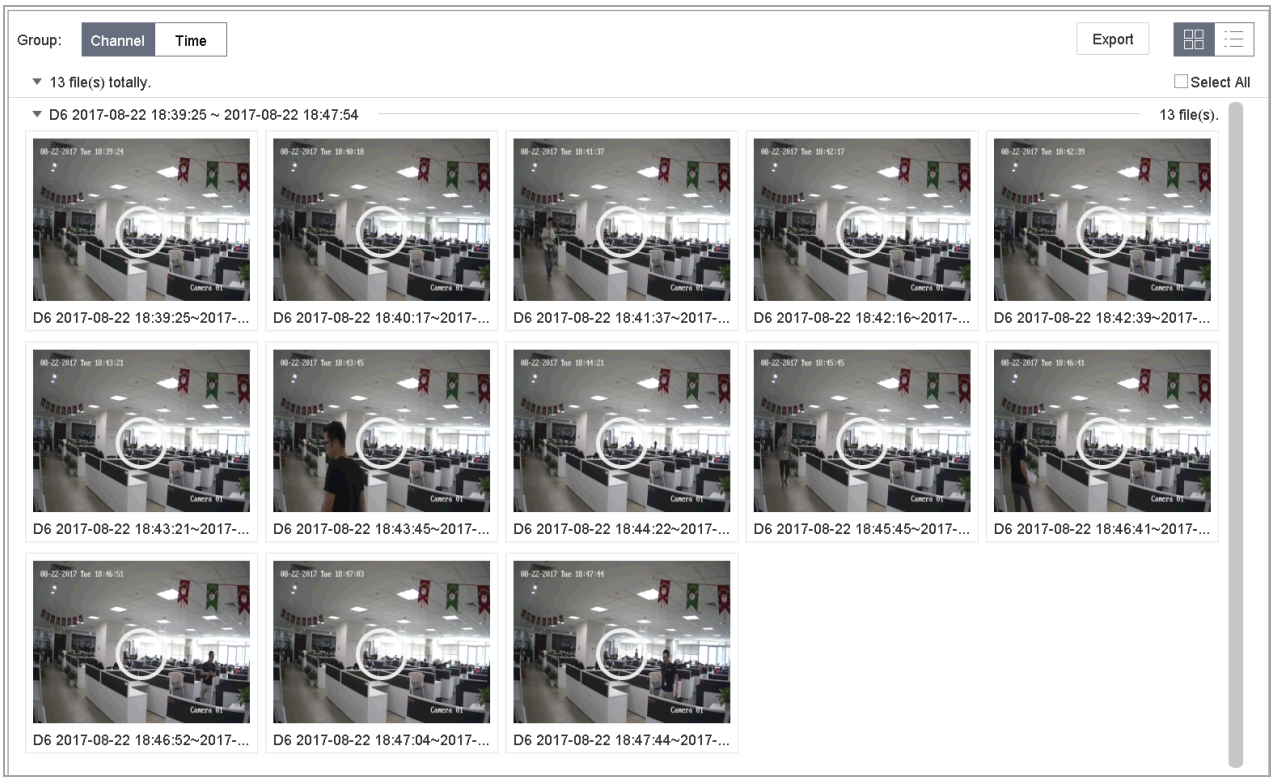


Figure 11-9 Event Files

You can click  or  button to play 30s backward or forward.

NOTE

- Refer to Chapter 12

Event and Alarm Settings and Chapter 13 VCA Event Alarm for details for event and alarm settings.

- Refer to Chapter 8.7 Configure Event Triggered Recording for the event triggered recording/capture settings.

11.1.7 Play Video Synopsis

Purpose:

Video synopsis is an approach to create a short video summary of a long video. It tracks and analyzes moving objects (also called events), and converts video streams into a database of objects and activities.

Before you start:

Enable Dual-VCA and intrusion detection/line crossing detection on the network camera.

Step 1 Go to **Playback** interface.

Step 2 Click  in toolbar.

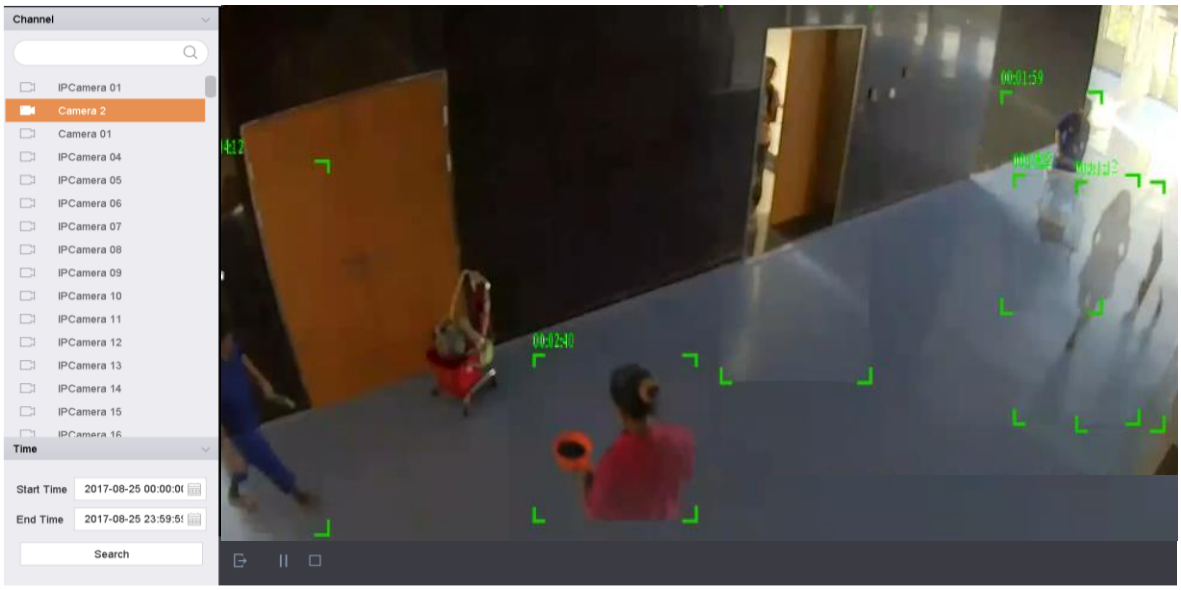


Figure 11-10 Synopsis Playback

Step 3 Select a camera in channel list.

Step 4 Specify **Start Time** and **End Time**. The duration must be within 24 hours.

Step 5 Click **Search** to start play.

Step 6 Optionally, double click a target on the playback window. A 60-second video of 30 seconds before and after the time will be played.

11.1.8 Play by Sub-periods

Purpose:

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

Step 1 Go to **Playback**.

Step 2 Select  icon at the left bottom corner to enter the sub-period playing mode.

Step 3 Select a camera.

Step 4 Set the start time and end time for searching video.

Step 5 Select the different multi-period at the right bottom 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.

11.1.9 Play Log Files

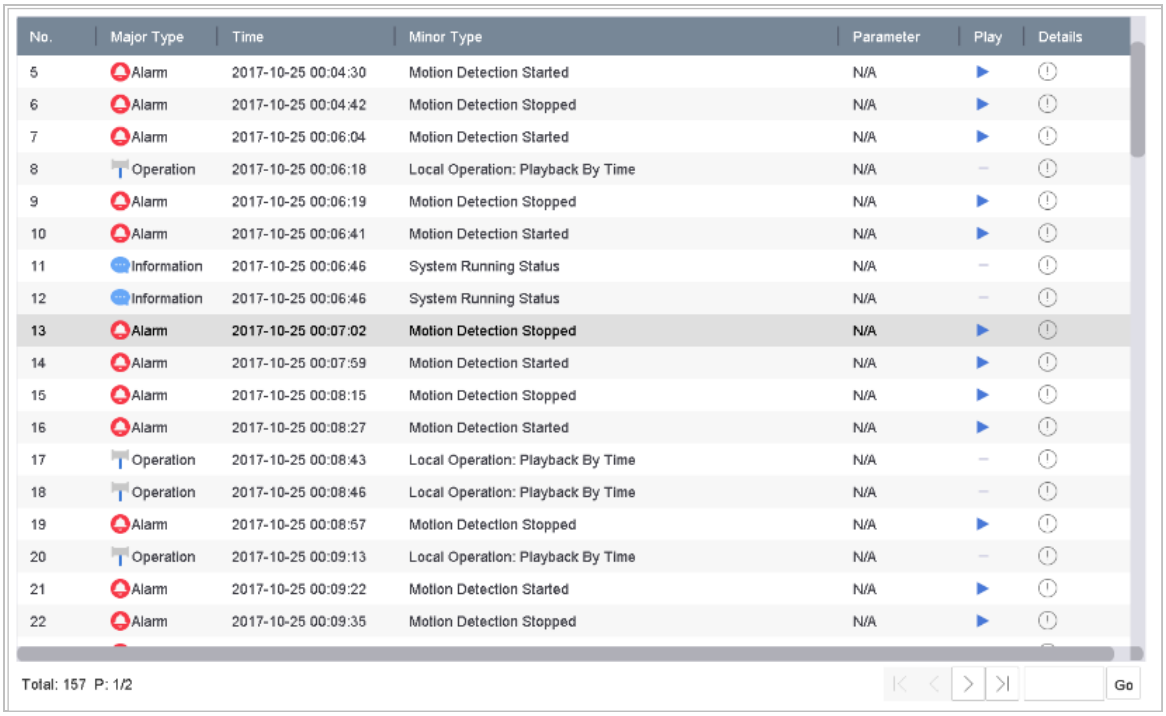
Purpose

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

Step 1 Go to **Maintenance**>**Log Information**.

Step 2 Click **Log Search**.

Step 3 Set search time and type and click **Search**.



No.	Major Type	Time	Minor Type	Parameter	Play	Details
5	Alarm	2017-10-25 00:04:30	Motion Detection Started	N/A	▶	
6	Alarm	2017-10-25 00:04:42	Motion Detection Stopped	N/A	▶	
7	Alarm	2017-10-25 00:06:04	Motion Detection Started	N/A	▶	
8	Operation	2017-10-25 00:06:18	Local Operation: Playback By Time	N/A	–	
9	Alarm	2017-10-25 00:06:19	Motion Detection Stopped	N/A	▶	
10	Alarm	2017-10-25 00:06:41	Motion Detection Started	N/A	▶	
11	Information	2017-10-25 00:06:46	System Running Status	N/A	–	
12	Information	2017-10-25 00:06:46	System Running Status	N/A	–	
13	Alarm	2017-10-25 00:07:02	Motion Detection Stopped	N/A	▶	
14	Alarm	2017-10-25 00:07:59	Motion Detection Started	N/A	▶	
15	Alarm	2017-10-25 00:08:15	Motion Detection Stopped	N/A	▶	
16	Alarm	2017-10-25 00:08:27	Motion Detection Started	N/A	▶	
17	Operation	2017-10-25 00:08:43	Local Operation: Playback By Time	N/A	–	
18	Operation	2017-10-25 00:08:46	Local Operation: Playback By Time	N/A	–	
19	Alarm	2017-10-25 00:08:57	Motion Detection Stopped	N/A	▶	
20	Operation	2017-10-25 00:09:13	Local Operation: Playback By Time	N/A	–	
21	Alarm	2017-10-25 00:09:22	Motion Detection Started	N/A	▶	
22	Alarm	2017-10-25 00:09:35	Motion Detection Stopped	N/A	▶	

Total: 157 P: 1/2 Go

Figure 11-11 System Log Search Interface

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

11.1.10 Play External Files

Purpose

You can play files from external storage devices.

Before You Start

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

Step 1 Go to **Playback**.

Step 2 Click  at the left bottom corner.

Step 3 Select and click t  or double click to play the file.

11.2 Playback Operations

11.2.1 Set Play Strategy in Smart/Custom Mode

Purpose:

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

In the Smart/Custom video playback mode, click  to set the play strategy.

- When **Do not Play Normal Videos** is checked, the device will skip the normal video and play the smart (motion/line crossing/intrusion) video and the custom (searched video) only in the normal speed (X1).
- When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video the smart/custom video separately. The speed range is from X1 to XMAX.

NOTE

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

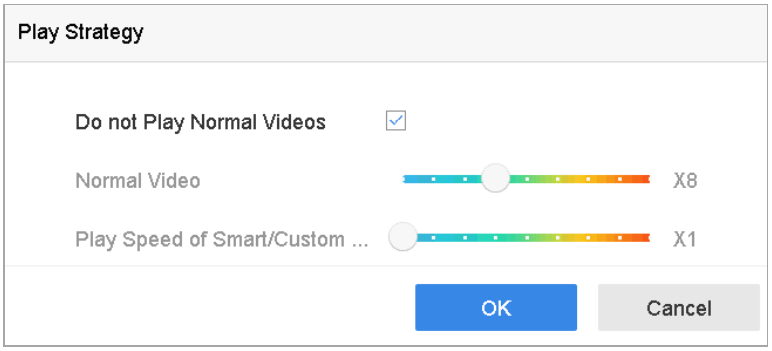


Figure 11-12 Play Strategy

11.2.2 Edit Video Clips

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

In the Video Playback mode, click  to start the video clipping operation.

- : Set the start time and end time of the video clipping.
- : Export the video clips to the local storage device.

11.2.3 Switch between Main Stream and Sub-Stream

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

: Play the video in main stream.

: Play the video in sub-stream.

NOTE

The encoding parameters for the main stream and sub-stream can be configured in **Storage** > **Encoding Parameters**.

11.2.4 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, move the mouse to the time bar to get the preview thumbnails of the video files.

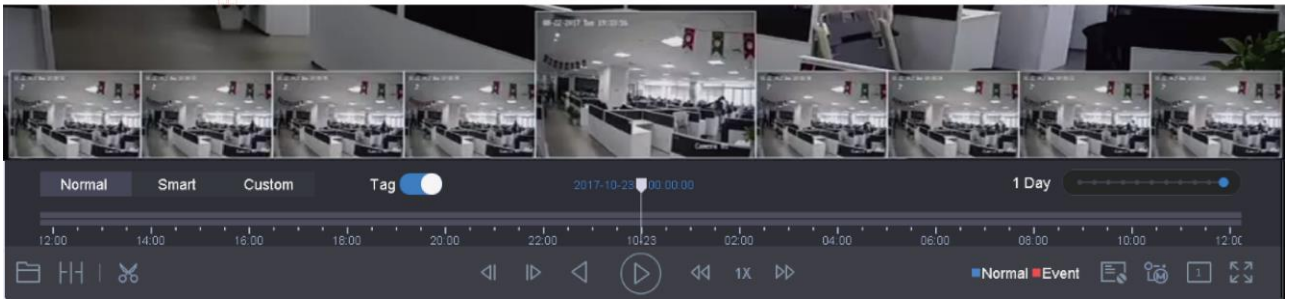


Figure 11-13 Thumbnails View

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

11.2.5 Fisheye View

You can enter the fisheye expansion view during the video playback.

Click the  to enter the fisheye expansion mode.

- **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 a defined area in the fisheye view or panorama expansion, and it supports the electronic PTZ function, which is also called e-PTZ.
- **Radial Expansion ():** In the 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.

- **Fisheye + 3PTZ ( ):** The camera will be divided into a fisheye view and 3 PTZ views. The PTZ views are the three different close-ups of the fisheye view. You can drag the PTZ images to adjust its view.
- **Cylinder ( ):** The camera image will be displayed as a cylinder. You can drag the image to adjust its view or scroll to zoom in/out.
- **Hemisphere ( ):** The camera image will be displayed as a hemisphere. You can drag the image to adjust its view or scroll to zoom in/out.
- **4 PTZ ( ):** The camera will be divided into 4 PTZ views. The PTZ views are the four different close-ups of the fisheye view. You can drag the PTZ images to adjust its view.

11.2.6 Fast View

Hold the mouse to drag on the time bar to get a fast view of the video files.

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

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

11.2.7 Digital Zoom

Digital zoom adopts encoding technology to enlarge the image which will result in image quality damage.

In the Video Playback mode, click in the toolbar to enter the digital zoom interface.

Move the sliding bar or scroll the mouse wheel to zoom in/out of the image to different magnifications (1 to16X).



Figure 11-14 Digital Zoom

11.2.8 POS Information Overlay

The device can be connected with the POS machine/server, and receive the transaction message for overlay on the image during playback.

In the video playback mode, click  to overlay the POS transaction information on the playback video.

NOTE

When the playing speed is higher than 2x, the POS information cannot be overlaid on the video.

Chapter 12 Event and Alarm Settings

12.1 Configure Arming Schedule

Step 1 Click **Arming Schedule**.

Step 2 Click **Edit**.

Step 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.

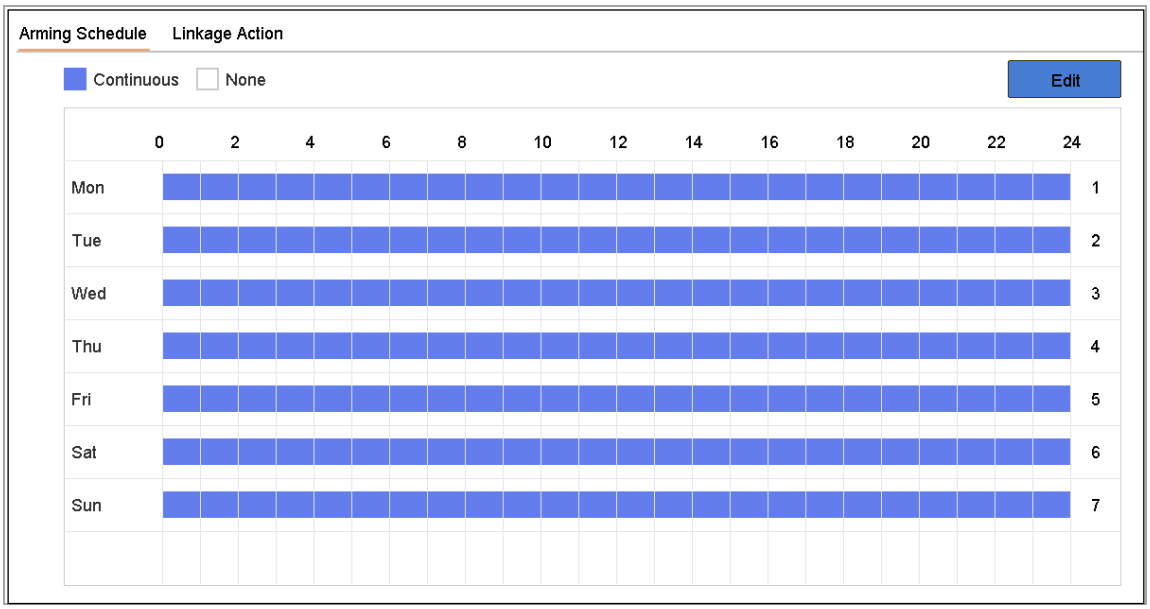


Figure 12-1 Set Arming Schedule

Step 4 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

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

12.2 Configure Alarm Linkage Actions

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

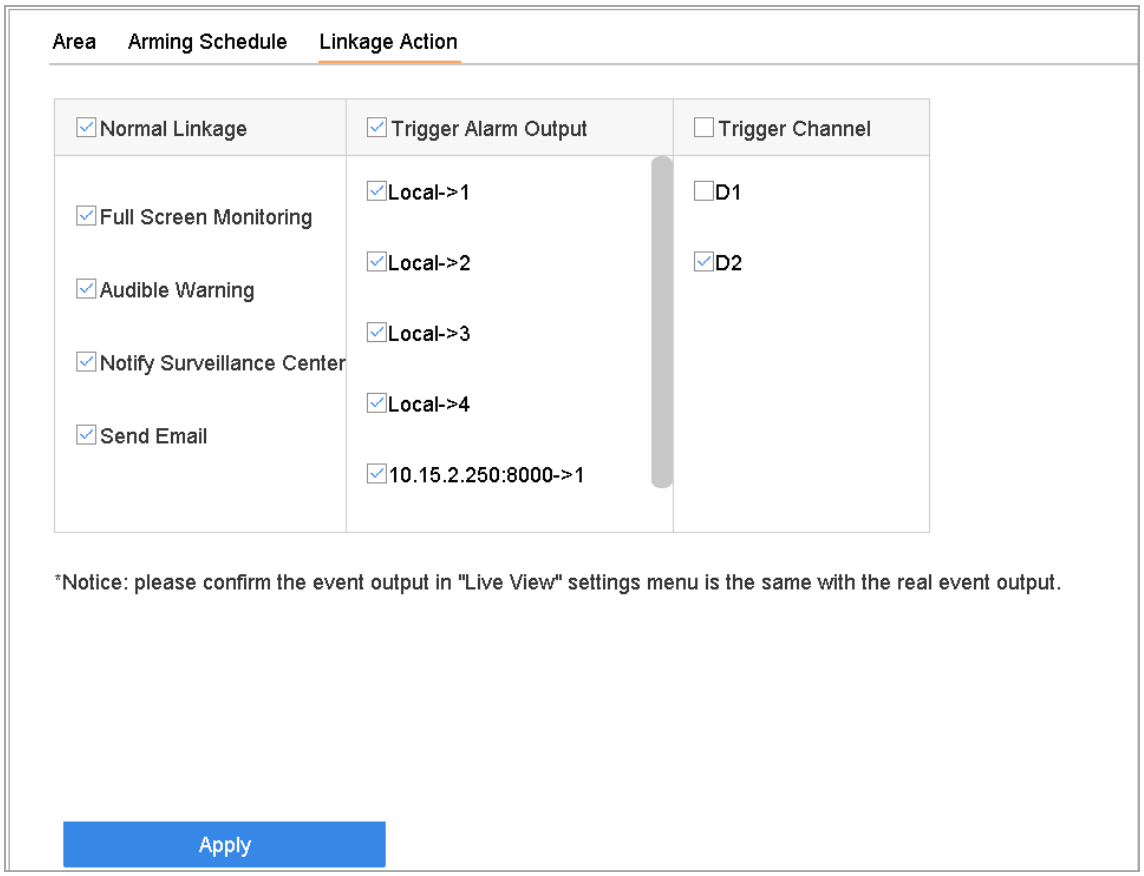


Figure 12-2 Set Linkage Actions

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

- **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.

  If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to **System>Live View > Full Screen Monitoring Dwell Time**.

  Auto-switch will terminate once the alarm stops and return to the Live View interface.

NOTE

Select the channel(s) you want to trigger full screen monitoring in **Trigger Channel** settings.

- **Audible Warning**

  It will trigger an audible *beep* when an alarm is detected.

- **Notify Surveillance Center**

  It will send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with Remote Client.

NOTE

The alarm signal will be transmitted automatically at detection mode when a remote alarm host is configured.

- **Send Email**

  It will send an e-mail with alarm information to the user when an alarm is detected.

  Refer to 16.8 Configure Email for details of e-mail configuration details.

Step 3 Check the checkbox to select the alarm output when an alarm is triggered.

NOTE

To trigger an alarm output when an event occurs, please refer to Chapter 12.6.3 Configure Alarm Output to set the alarm output parameters.

Step 4 Click **Trigger Channel** and select one or more channels that will record/capture or perform full-screen monitoring when a motion alarm is triggered.

NOTE

You have to set the recording schedule to realize this function. Refer to Refer to Chapter 8.4 Configure Recording Schedule for setting the recording schedule.

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

12.3 Configure Motion Detection Alarms

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

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

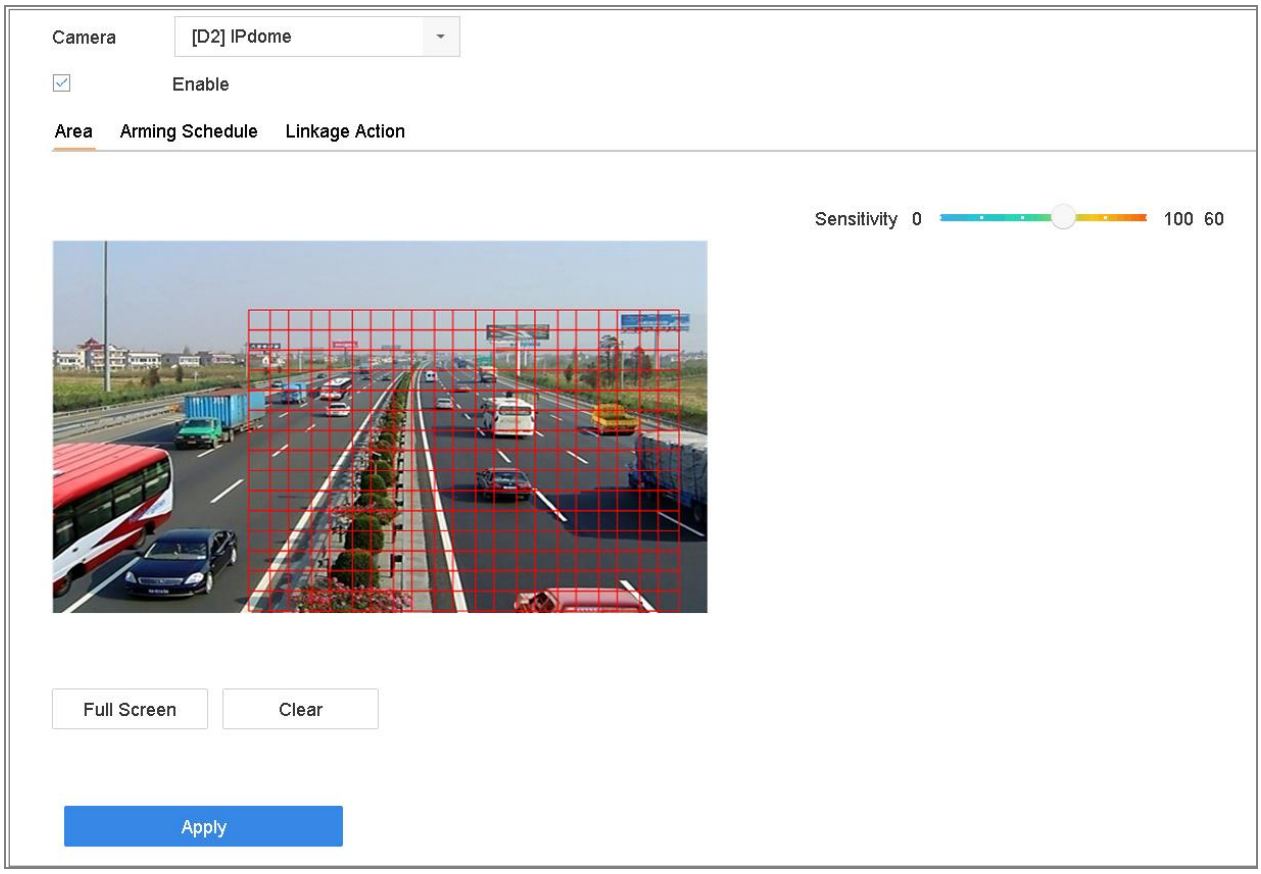


Figure 12-3 Set Motion Detection

Step 2 Select the camera to configure the motion detection.

Step 3 Check **Enable**.

Step 4 Set the motion detection area.

- Full screen: Click to set the full-screen motion detection for the image.
- Customized area: Click-and drag the mouse to click and drag on the preview screen to draw the customized motion detection area (s).

Step 5 Click **Clear** to clear the current motion detection area settings and draw again.

Step 6 Set sensitivity (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. A higher value results in the more readily to triggers motion detection.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.1 Configure Arming Schedule

Step 9 Click **Arming Schedule**.

Step 10 Click **Edit**.

Step 11 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.

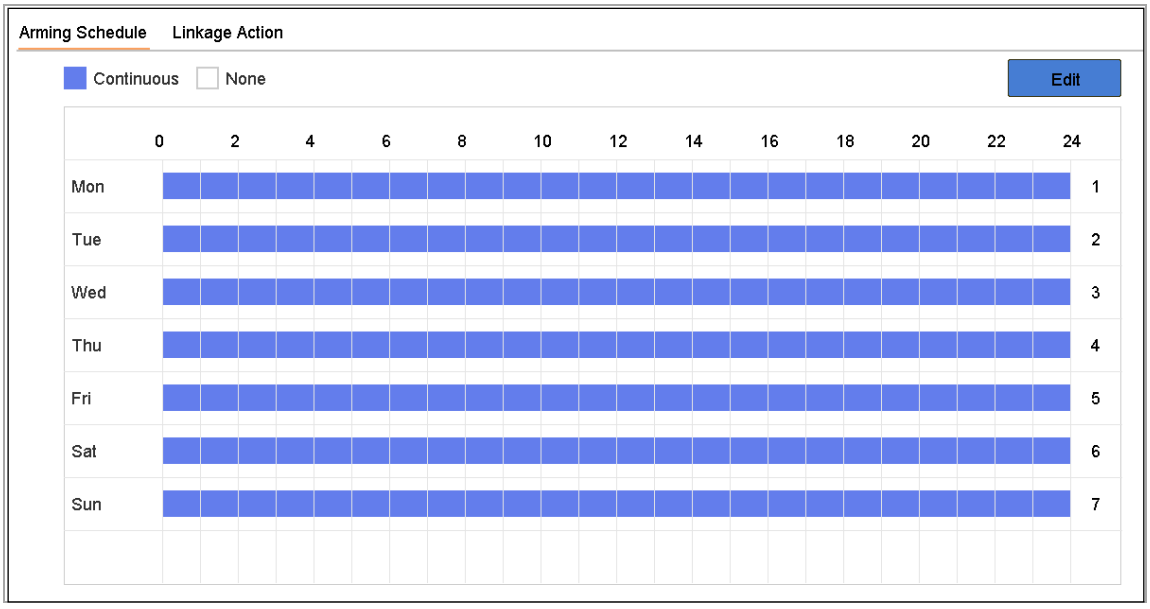


Figure 12-4 Set Arming Schedule

Step 12 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

Step 13 Click **Apply** to save the settings.

Step 14 Configure Alarm Linkage Actions.

12.4 Configure Video Loss Alarms

Purpose

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

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

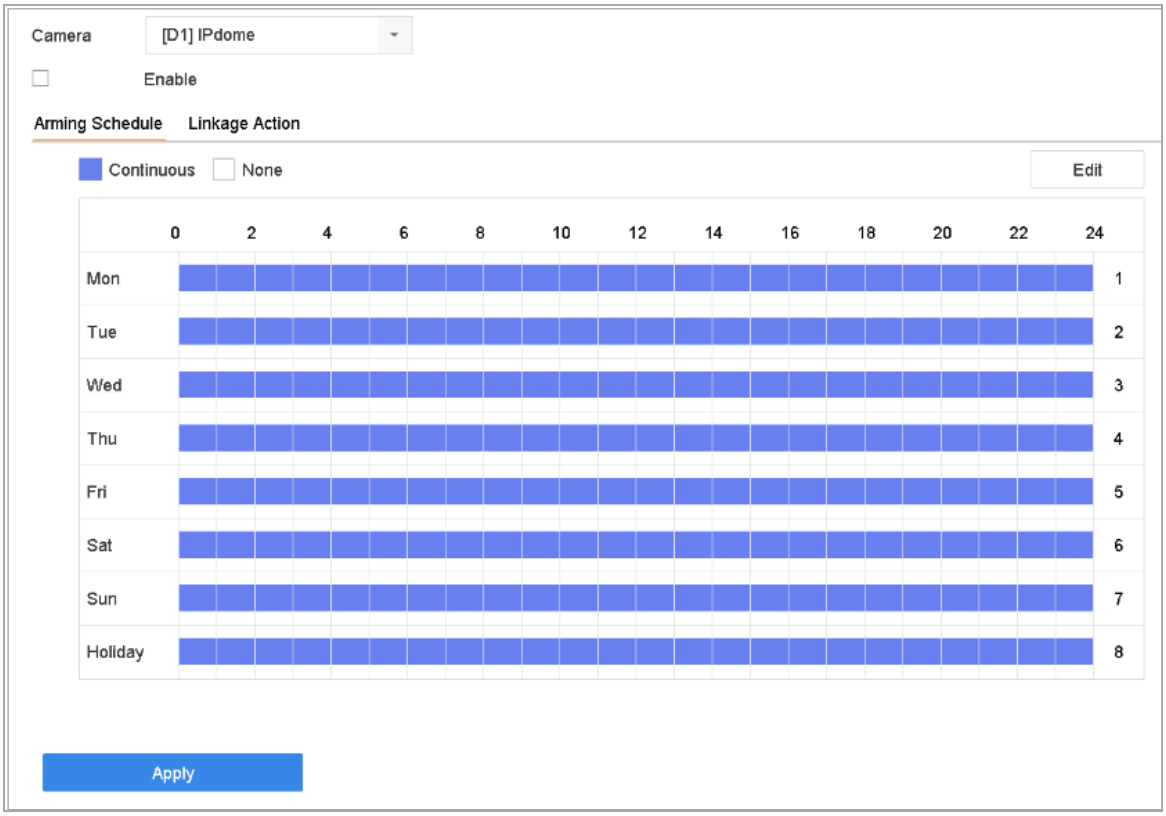


Figure 12-5 Set Video Loss Detection

Step 2 Select the camera to configure the video loss detection.

Step 3 Check **Enable**.

Step 4 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 5 Set the linkage actions. Refer to Chapter 12.1 Configure Arming Schedule

Step 6 Click **Arming Schedule**.

Step 7 Click **Edit**.

Step 8 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.

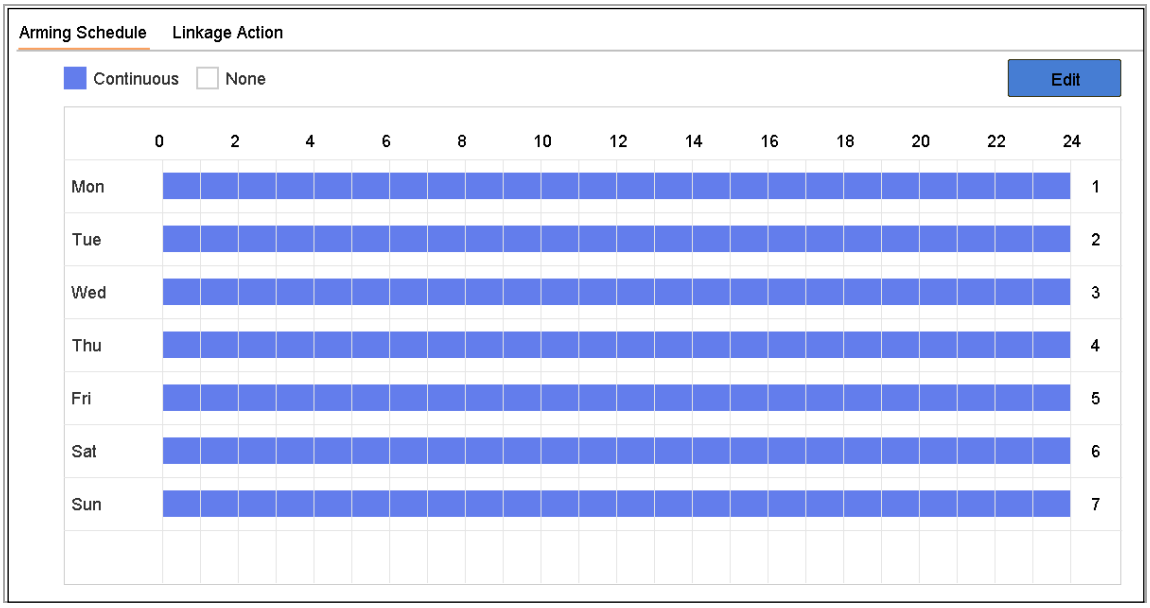


Figure 12-6 Set Arming Schedule

Step 9 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

Step 10 Click **Apply** to save the settings.

Step 11 Configure Alarm Linkage Actions.

12.5 Configure Video Tampering Alarms

Purpose

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

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

Step 2 Select the camera to configure the video tampering detection.

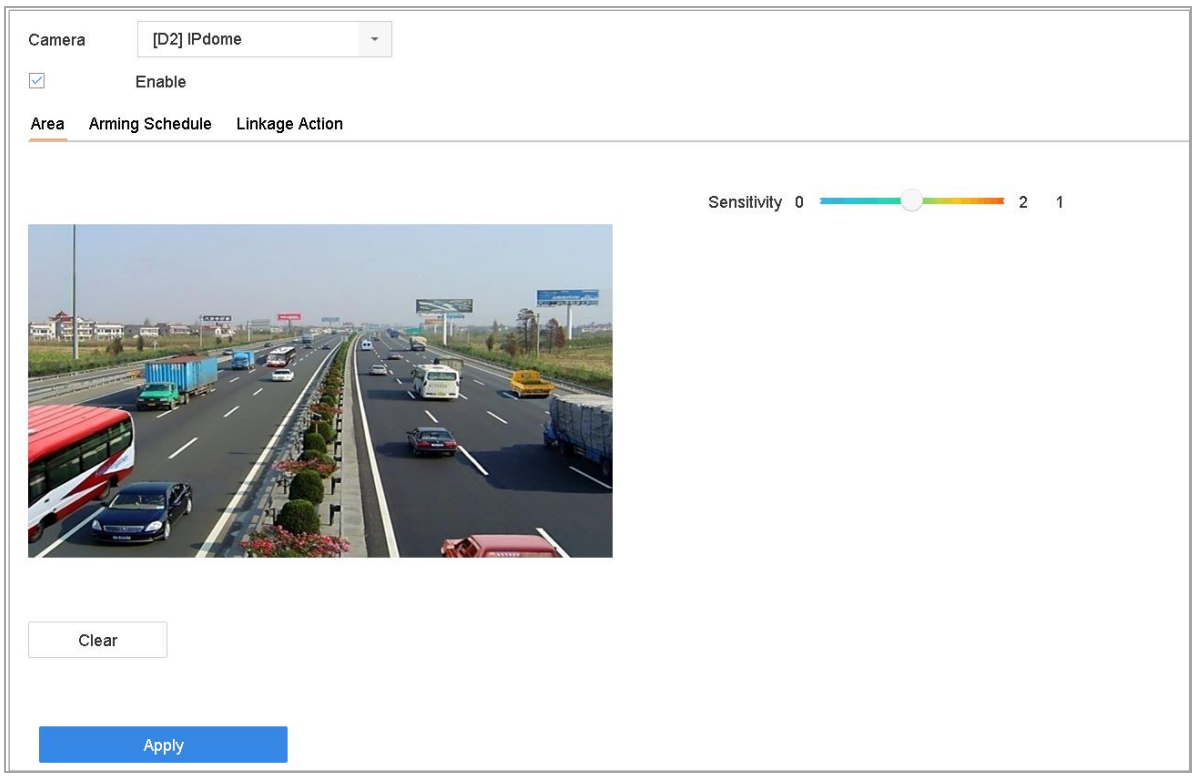


Figure 12-7 Set Video Tampering Setting

Step 3 Check **Enable**.

Step 4 Set the video tampering area. Click-and-drag the mouse on the preview screen to draw the customized video tampering area.

Step 5 Click **Clear** to clear the current area settings and draw again.

Step 6 Set sensitivity level (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.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.1 Configure Arming Schedule

Step 9 Click **Arming Schedule**.

Step 10 Click **Edit**.

Step 11 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.

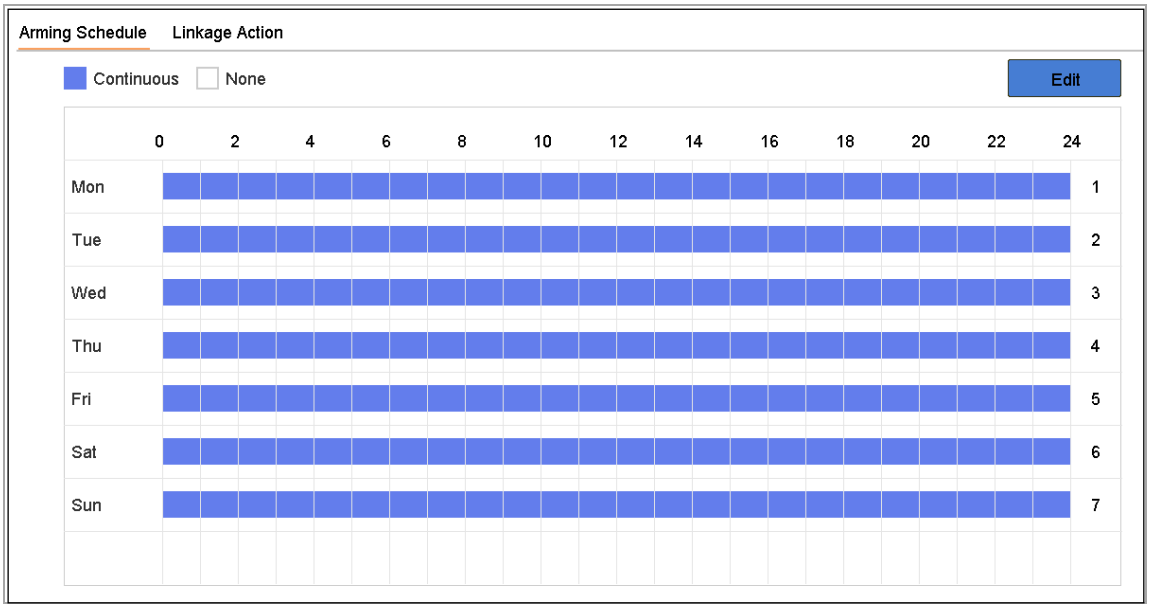


Figure 12-8 Set Arming Schedule

Step 12 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

Step 13 Click **Apply** to save the settings.

Step 14 Configure Alarm Linkage Actions.

12.6 Configure Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

12.6.1 Configure Alarm Inputs

Step 1 Go to **System> Event>Normal Event>Alarm Input**

Step 2 Select an alarm input item from the list and click .

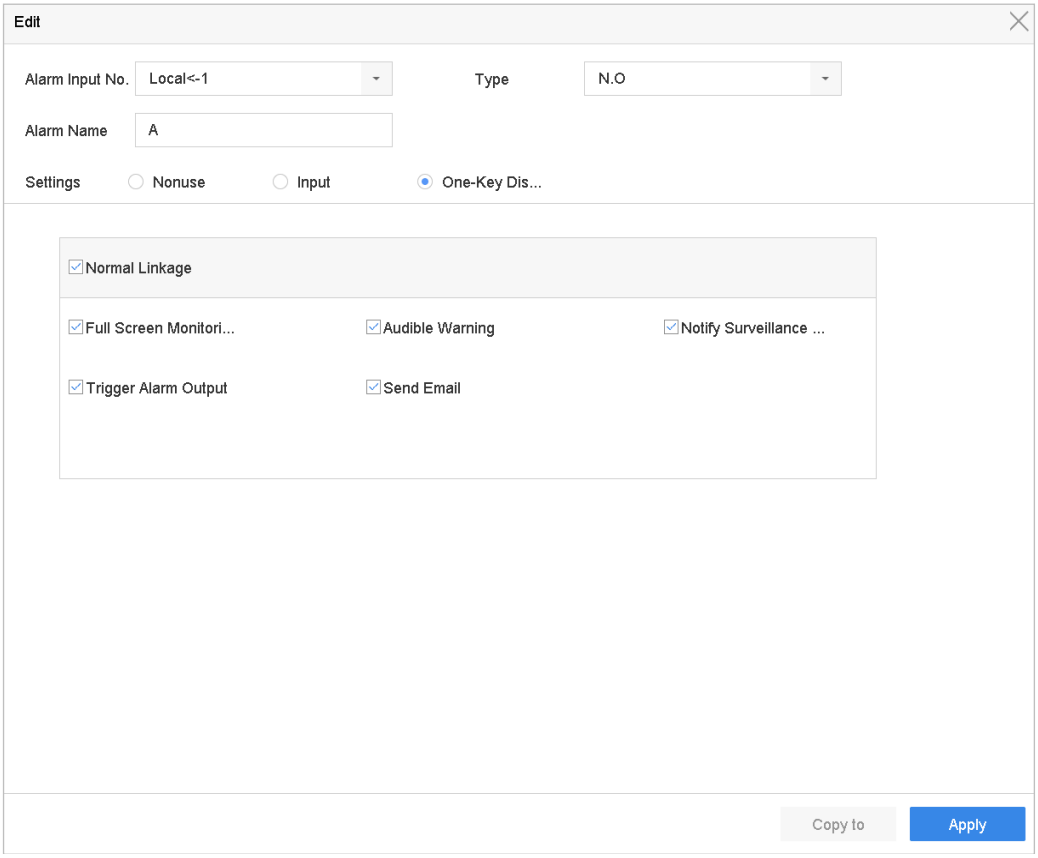


Figure 12-9 Alarm Input

Step 3 Select the alarm input type to N.C or N.O.

Step 4 Edit the alarm name.

Step 5 Check **Input**.

Step 6 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 12.1 Configure Arming Schedule

Step 8 Click **Arming Schedule**.

Step 9 Click **Edit**.

Step 10 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.

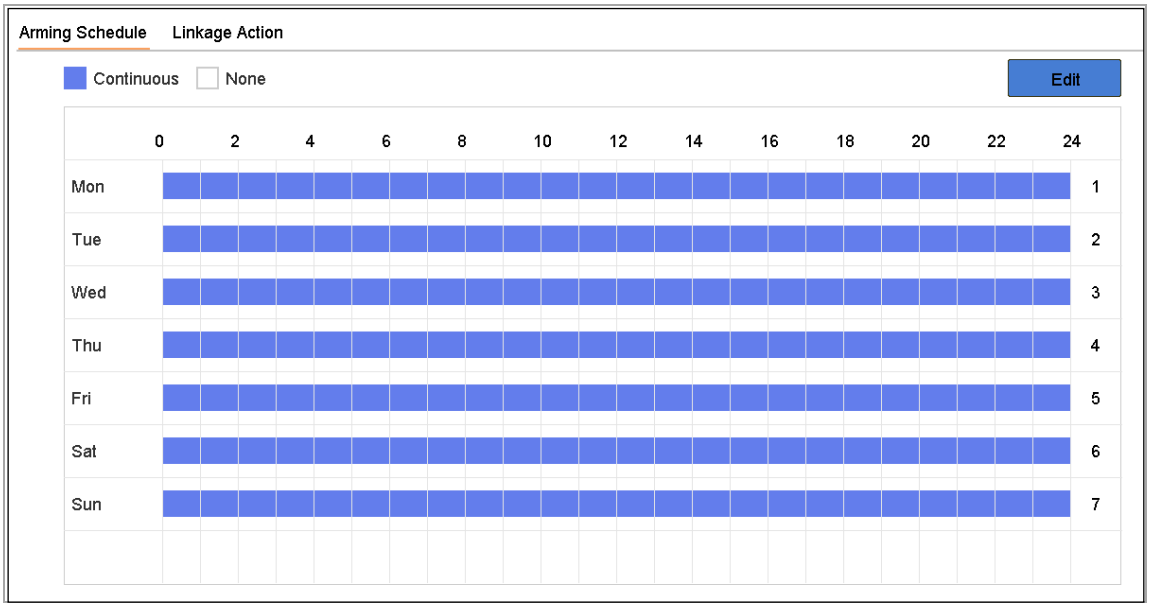


Figure 12-10 Set Arming Schedule

Step 11 (Optional) You can click **Copy** to copy the current day arming schedule settings to other day(s).

Step 12 Click **Apply** to save the settings.

Step 13 Configure Alarm Linkage Actions.

12.6.2 Configure One-Key Disarming

One-Key Disarming disarm Alarm Input 1 by one-key operation.

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Input**

Step 2 Select Alarm Input 1 from the list and click .

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

Step 4 Edit the alarm name.

Step 5 Check **Enable One-Key Disarming**.

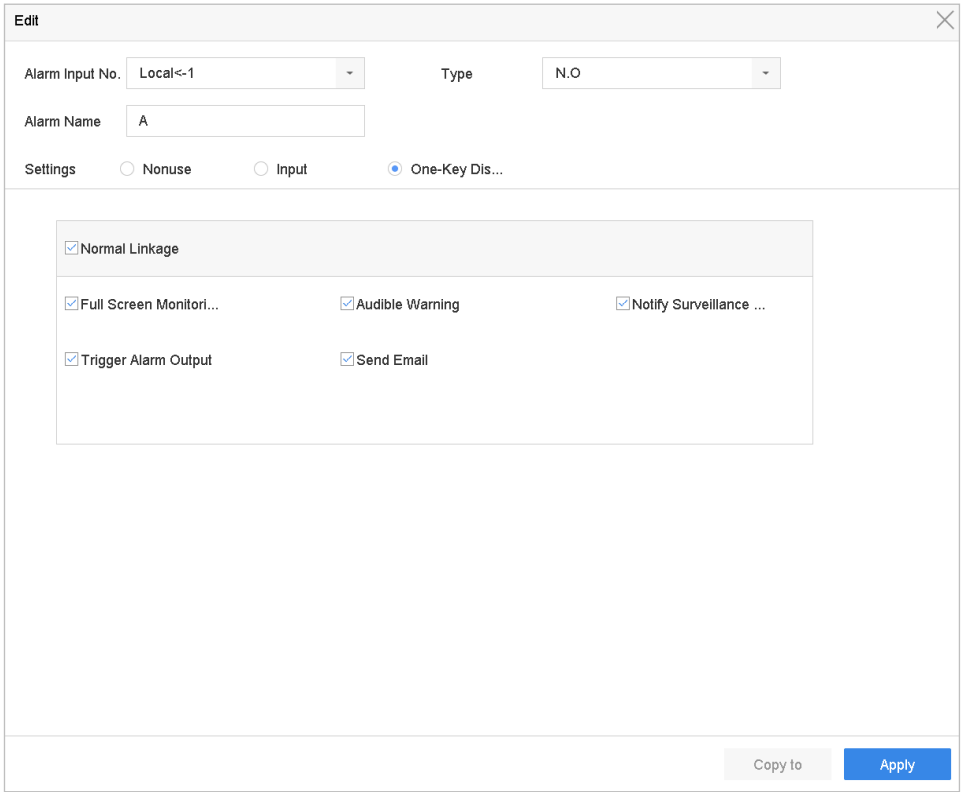


Figure 12-11 One-Key Alarm Disarming

Step 6 Select the alarm linkage action(s) you want to disarm for the local Alarm Input.

NOTE

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

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

12.6.3 Configure Alarm Outputs

Trigger an alarm output when an alarm is triggered.

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Output**.

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

Step 3 Edit the alarm name.

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

Manually Clear: You should manually clear the alarm when the alarm occurs. Refer to Chapter 12.10 Trigger or Clear Alarm Output Manually for detailed instructions.

Step 5 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

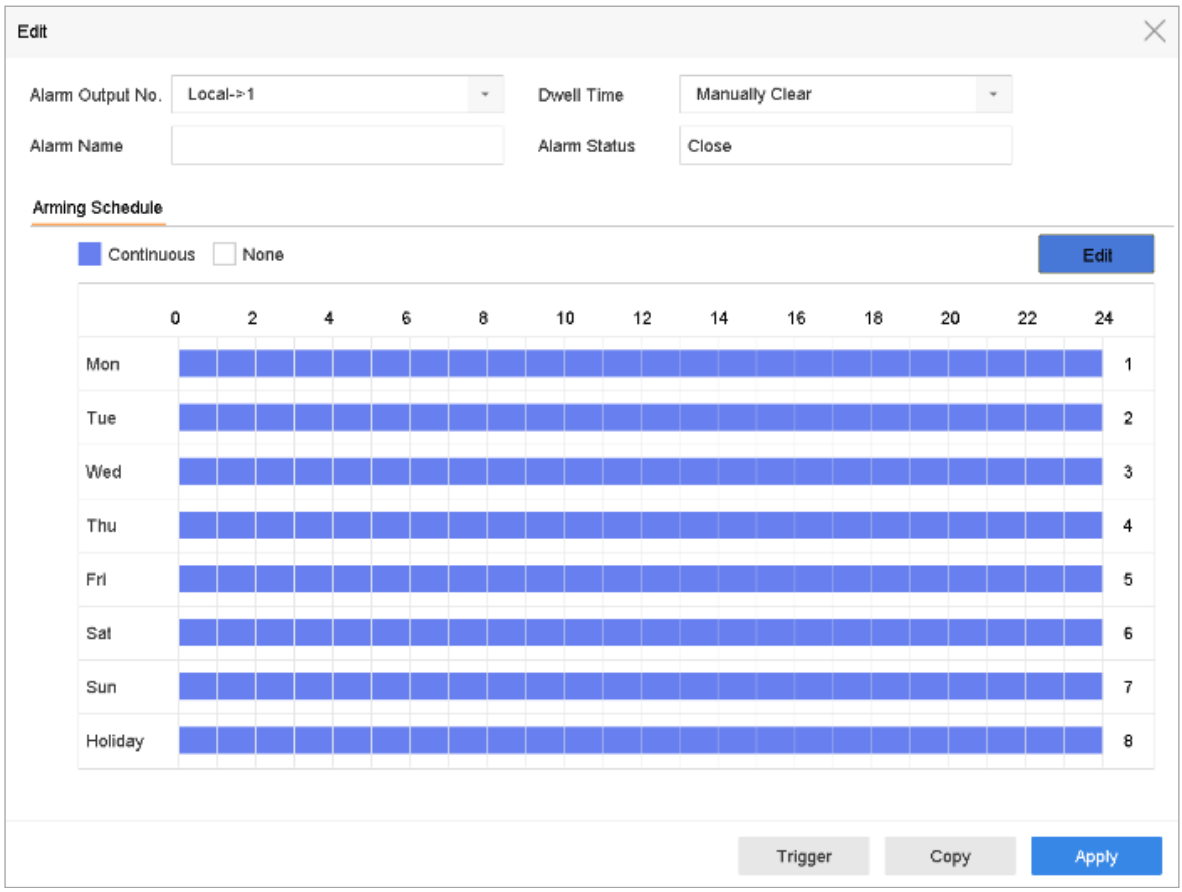


Figure 12-12 Alarm Output

Step 1 (Optional) Click **Copy** to copy the same settings to other alarm output (s).

12.7 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.

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

Step 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.

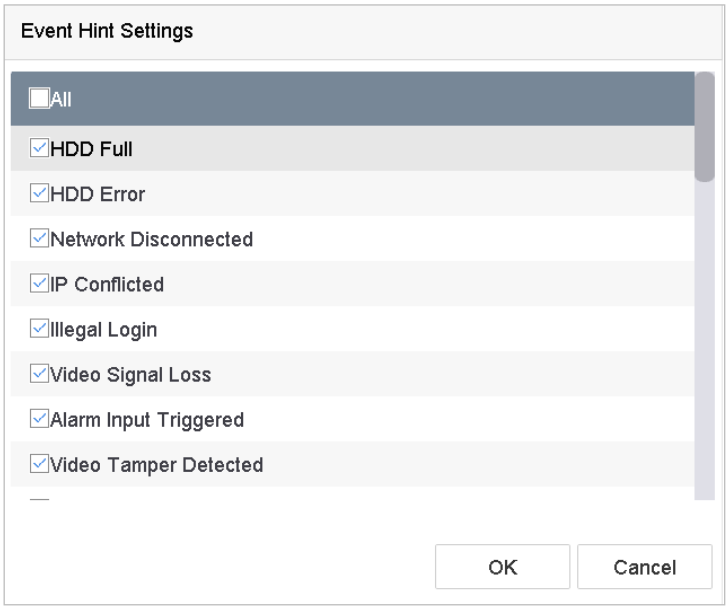


Figure 12-13 Event Hint Settings

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

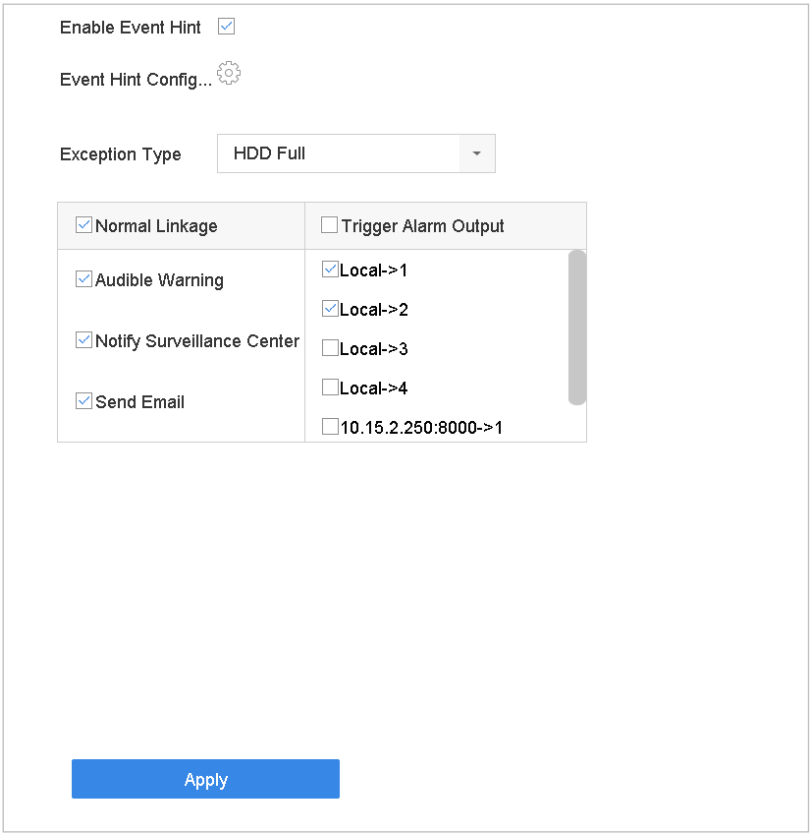


Figure 12-14 Exceptions Handling

Step 4 Set the normal linkage and alarm output triggering. Refer to Chapter 11.8 Setting Alarm Linkage Actions

12.8 Configure Combined Alarm

Purpose

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 12.6.1 Configure Alarm Inputs).

Step 1 Go to **System** > **Event** > **Normal Event** > **Alarm Input**.

Step 2 Select an alarm input item from the list and click .

Step 3 Select **Settings** as **Input**.

Step 4 Click **Combined Alarm**.

Step 5 Select channel as your desire.

Step 6 Select **Combined Alarm Event**.

Step 7 Click **Apply**.

NOTE

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

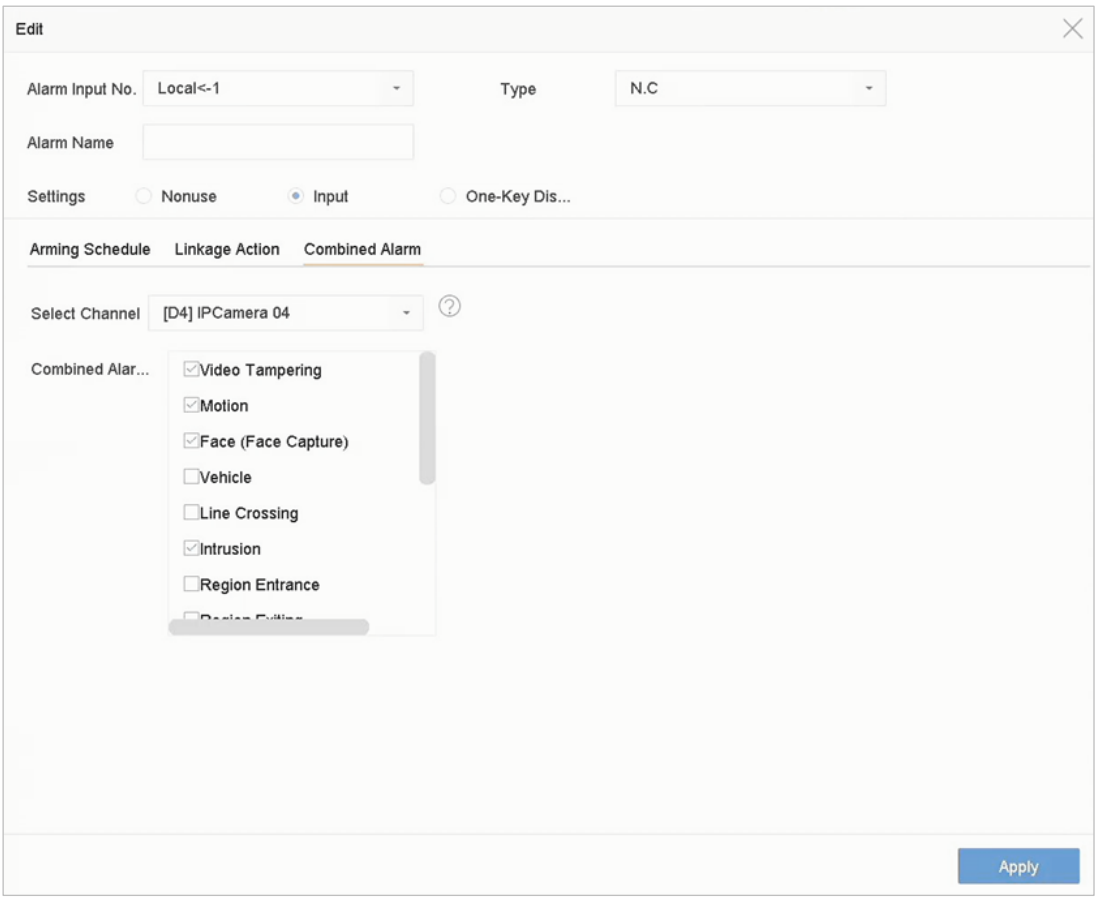


Figure 12-15 Combined Alarm

12.9 Setting Alarm Linkage Actions

Purpose

Alarm linkage actions will be activated when an alarm or exception occurs, including Event Hint Display, Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Trigger Alarm Output, and Send Email.

12.9.1 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.

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

Step 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).

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the **Full Screen Monitoring** alarm linkage action.

Step 5 Select the channel(s) in **Trigger Channel** settings you for make full screen monitoring in Trigger Channel Settings.

NOTE

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

12.9.2 Configure Audio Warning

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

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

Step 2 Enable the audio output and set the volume.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the **Audio Warning** alarm linkage action.

12.9.3 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., CMS, Guarding Vision).

Step 1 Go to **System** > **Network** > **Advanced** > **More Settings**.

Step 2 Set the alarm host IP and alarm host port.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the **Notify Surveillance Center**.

12.9.4 Configure E-mail Linkage

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

Please refer to Chapter 16.8 Configure Email for details of Email configuration.

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

Step 2 Configure the e-mail settings.

Step 3 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, video tampering, face detection, etc.).

Step 4 Select the **Send Email** alarm linkage action.

12.9.5 Trigger Alarm Outputs

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.

Step 1 Go to the **Linkage Action** interface of the alarm detection (e.g., motion detection, face detection, line crossing detection, intrusion detection, etc.).

Step 2 Click the **Trigger Alarm Output** tab.

Step 3 Select the alarm output (s) to trigger.

Step 4 Go to **System**> **Event**>**Normal Event>Alarm Output**.

Step 5 Select an alarm output item from the list.

NOTE

Refer to Chapter 12.6.3 Configure Alarm Output for the alarm output settings.

12.9.6 Configure PTZ Linkage

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

NOTE

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

Step 1 Go to the **Linkage Action** interface of the alarm input or VCA detection (e.g., face detection, line crossing detection, intrusion detection, etc.).

Step 2 Select the **PTZ Linkage**.

Step 3 Select the camera to perform the PTZ actions.

Step 4 Select the preset/patrol/pattern No. to call when the alarm events occur.

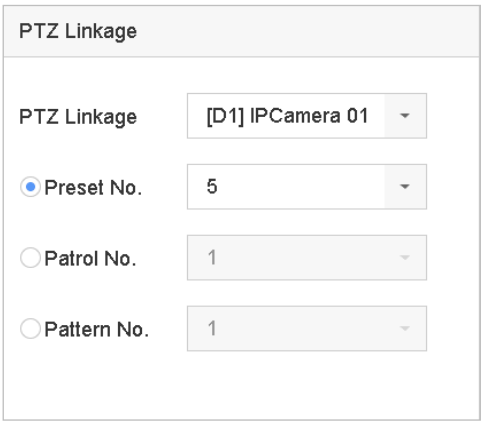


Figure 12-16 PTZ Linkage

NOTE

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

12.10 Trigger or Clear Alarm Output Manually

Purpose

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

Step 1 Go to **System**> **Event**>**Normal Event>Alarm Output**.

Step 2 Select the alarm output you want to trigger or clear.

Step 3 Click **Trigger/Clear** to trigger or clear an alarm output.

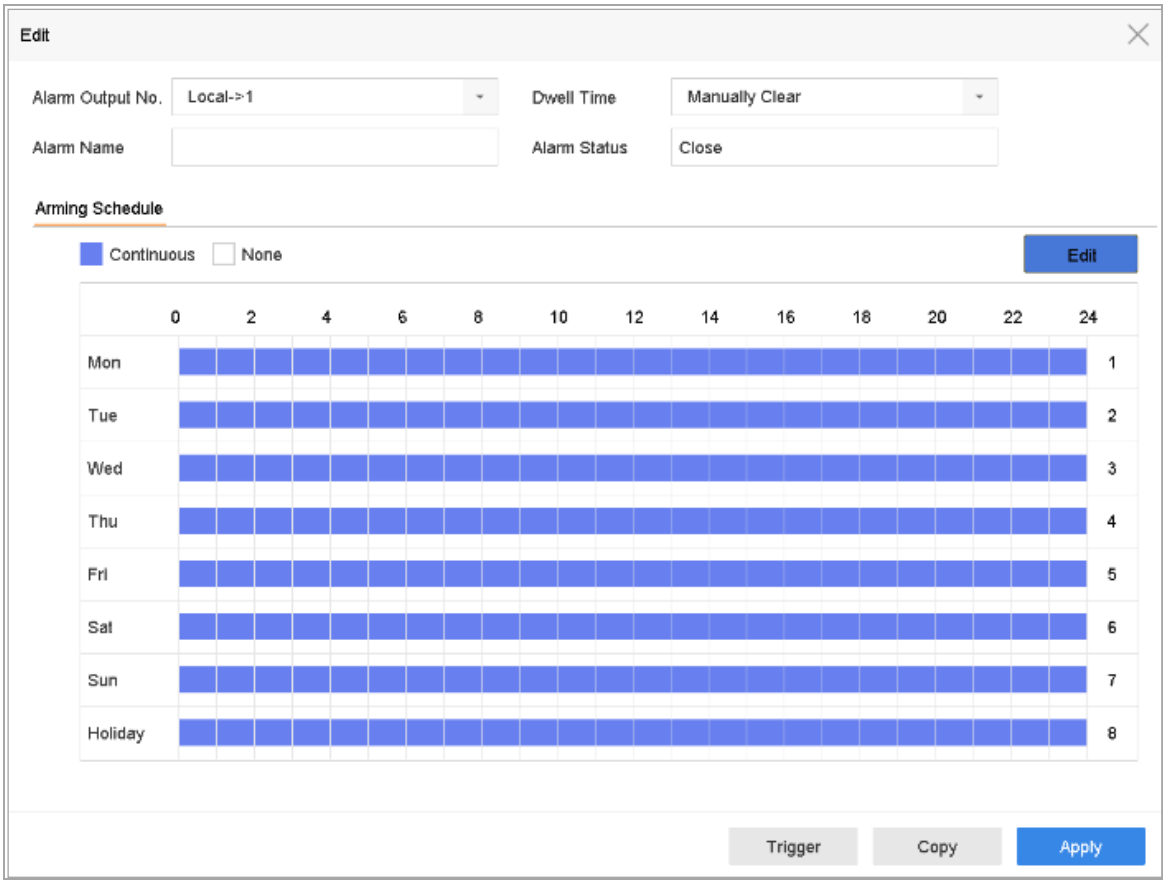


Figure 12-17 Alarm Output

Chapter 13 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's user manual for detailed VCA detection instructions.

13.1 Face Detection

Purpose

The face detection function detects the face appearing in the surveillance scene. Linkage actions can be triggered when a human face is detected.

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

Step 2 Select a camera to configure.

Step 3 Click **Face Detection**.

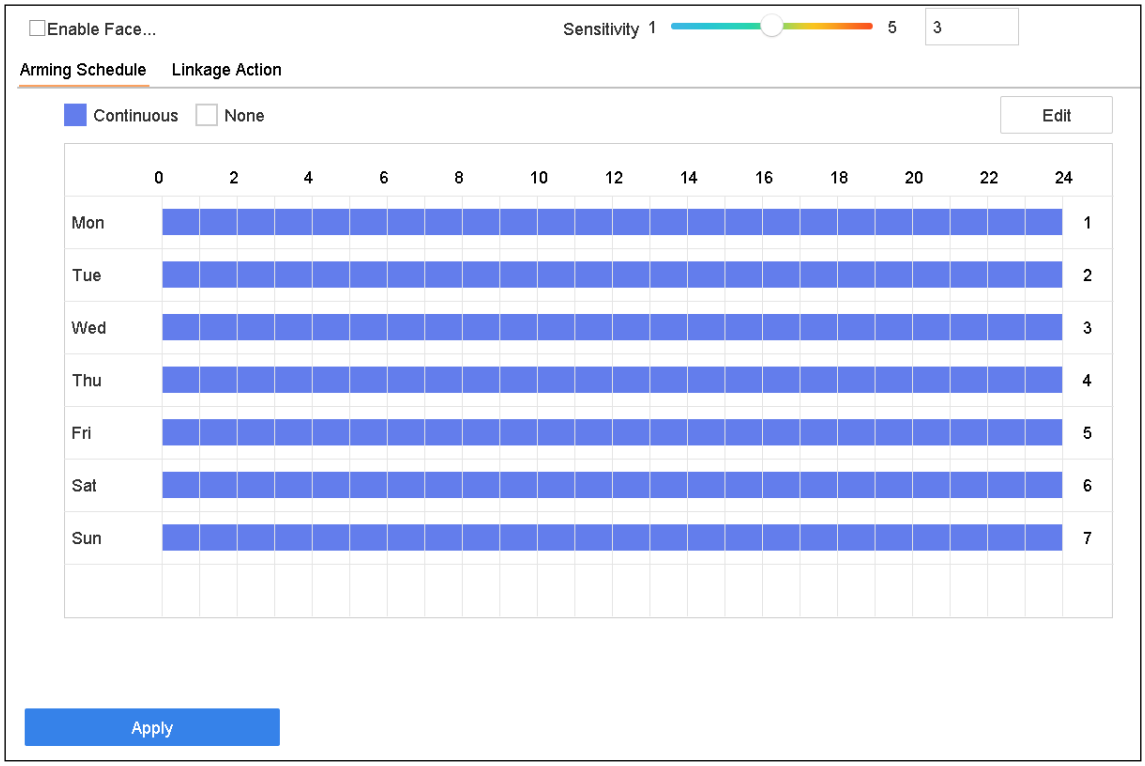


Figure 13-1 Face Detection

Step 4 Check **Enable Face Detection**.

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

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

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.2 Vehicle Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Vehicle**.

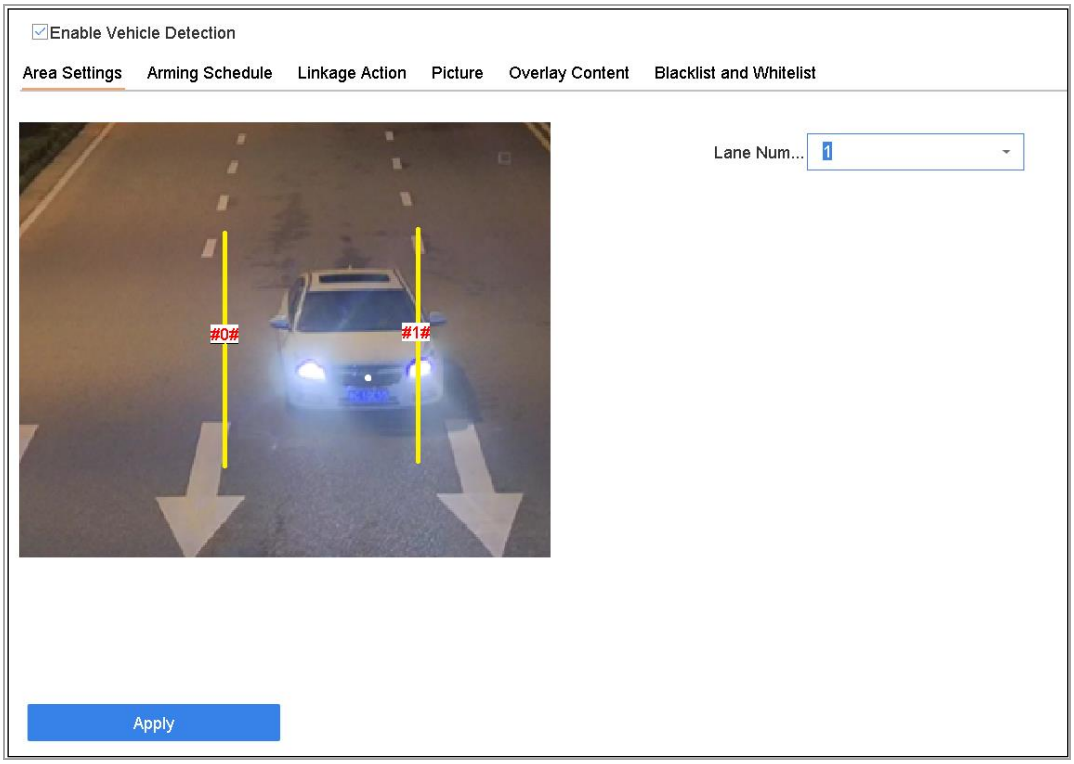


Figure 13-2 Vehicle Detection

Step 4 Check **Enable Vehicle Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured vehicle detection pictures.

Step 6 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 7 Set the linkage actions. You can configure the linkage action for black list, whitelist and other license plate respectively. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 8 Configure rules, including **Area Settings, Picture, Overlay Content**, and **Blacklist and Whitelist**.

Area Settings: Up to 4 lanes are selectable.

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

Step 9 Click **Apply**.

NOTE

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

13.3 Line Crossing Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Line Crossing**.

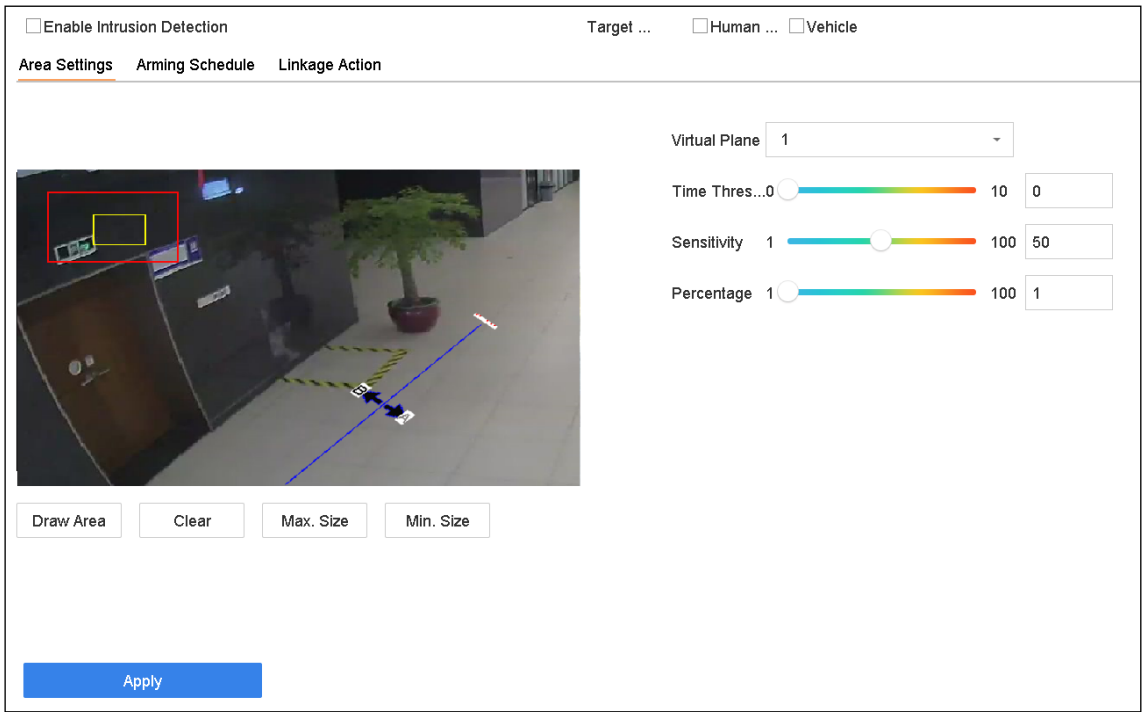


Figure 13-3 Line Crossing Detection

Step 4 Check **Enable Line Crossing Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of line crossing detection pictures.

Step 6 Follow the steps to set the line crossing detection rules and detection areas.

1) Select **Arming Area**. Up to 4 arming areas are selectable.
2) Select the Direction as **A<->B**, **A->B**, or **A<-B**.

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

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

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

3) Set the detection sensitivity range. The higher the value is, the easier the detection alarm will be triggered.
4) Click **Draw Area** and set two points in the preview window to draw a virtual line.

Step 7 Draw the maximum size/minimum size for targets. Only the targets in the size ranging from max.size to min. size will trigger line crossing detection.

1) Click **Max. Size/Min. Size**.
2) Draw an area in preview window.

3) Click **Stop Drawing**.

Step 8 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 9 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 10 Click **Apply**.

13.4 Intrusion Detection

Purpose

The 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.

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

Step 2 Select a camera to configure.

Step 3 Click **Intrusion**.

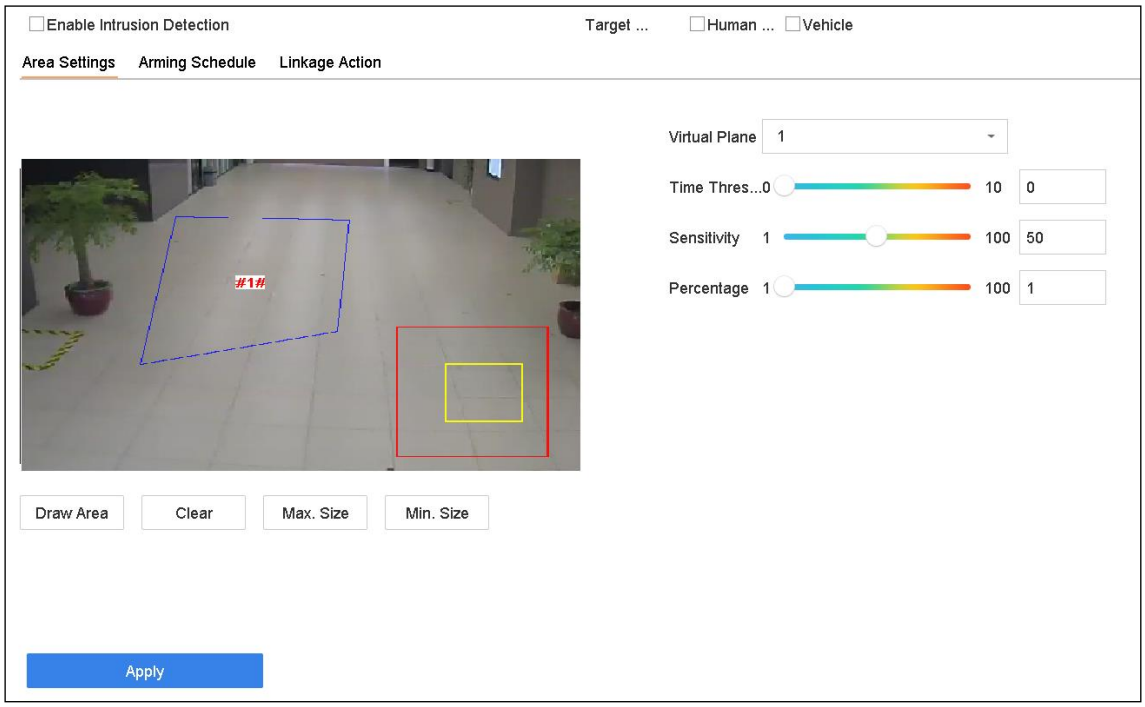


Figure 13-4 Intrusion Detection

Step 4 Check **Enable Intrusion Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured intrusion detection pictures.

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

1) Select **Virtual Panel**. Up to 4 virtual panels are selectable.
2) Set **Time Threshold**, **Sensitivity**, and **Percentage.**

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. Its range is [1s-10s].

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

Percentage: The ratio of the in-region part of the object that can trigger the alarm. For example, if the percentage is 50%, when the object enters the region and occupies half of the whole region, the device will trigger an alarm. Its range is [1-100].

3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection area.

Step 7 Draw the maximum size/minimum size for targets. Only the targets in the size ranging from max.size to min. size will trigger intrusion detection.

1) Click **Max. Size**/**Min. Size**.
2) Draw an area in preview window.
3) Click **Stop Drawing**.

Step 8 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 9 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 10 Click **Apply**.

13.5 Region Entrance Detection

Purpose

The region entrance detection function detects objects that enter a pre-defined virtual region.

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

Step 2 Click **Region Entrance Detection**.

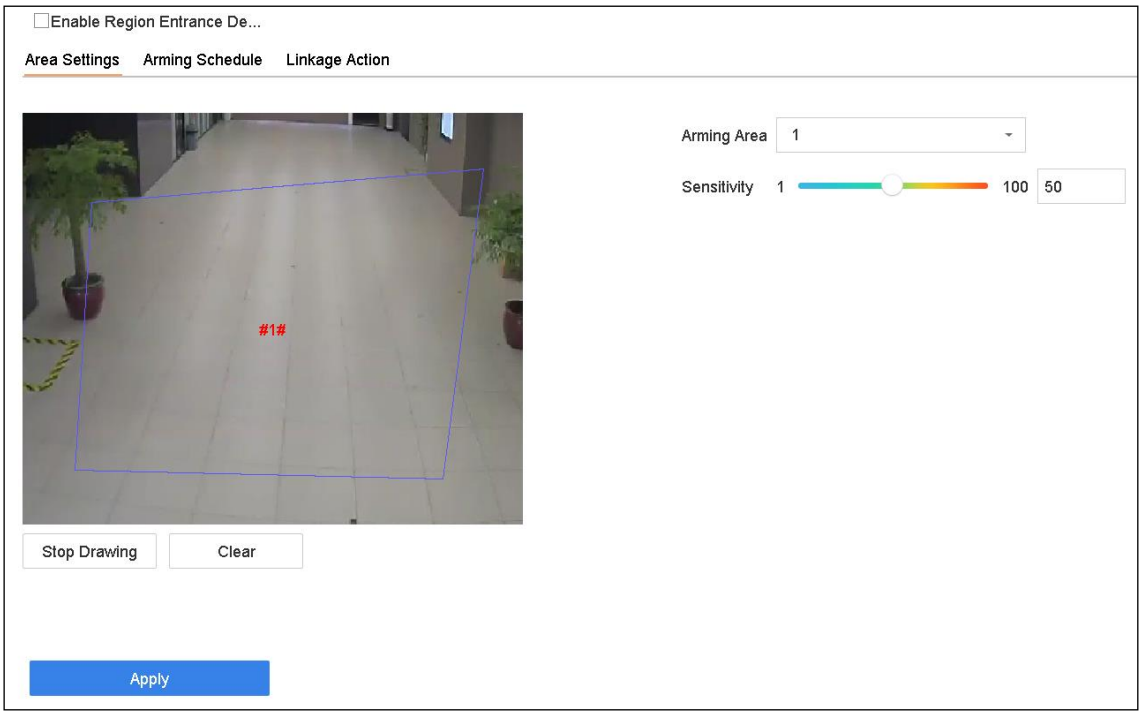


Figure 13-5 Region Entrance Detection

Step 3 Select a camera to configure.

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

Step 5 Optionally, check **Save VCA Picture** to save the captured pictures of region entrance detection pictures.

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

1) Select **Arming Area**. Up to 4 areas 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 by specifying four vertices of the detection region.

Step 7 Configure **Arming Schedule** and **Linkage Action**.

Step 8 Click **Apply**.

13.6 Region Exiting Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Region Exiting**.

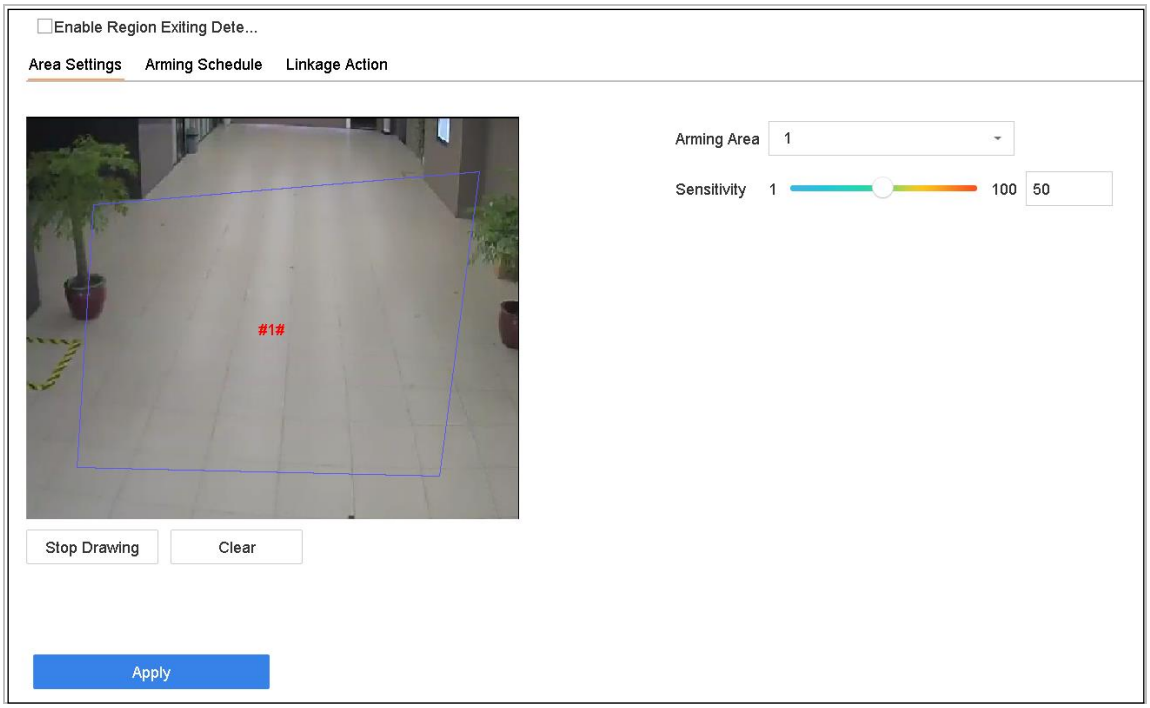


Figure 13-6 Region Exiting Detection

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

Step 5 Optionally, check **Save VCA Picture** to save the captured region exiting detection pictures.

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

1) Select **Arming Area**. Up to 4 areas are selectable.
2) Set **Sensitivity**.

   Sensitivity: The higher the value is, the more easily the detection alarm will be triggered. Its range is [0-100].

3) Click **Draw Area** and draw a quadrilateral in the preview window by specifying four vertices of the detection area.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.7 Loitering Detection

Purpose

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.

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

Step 2 Select a camera to configure.

Step 3 Click **Loitering**.

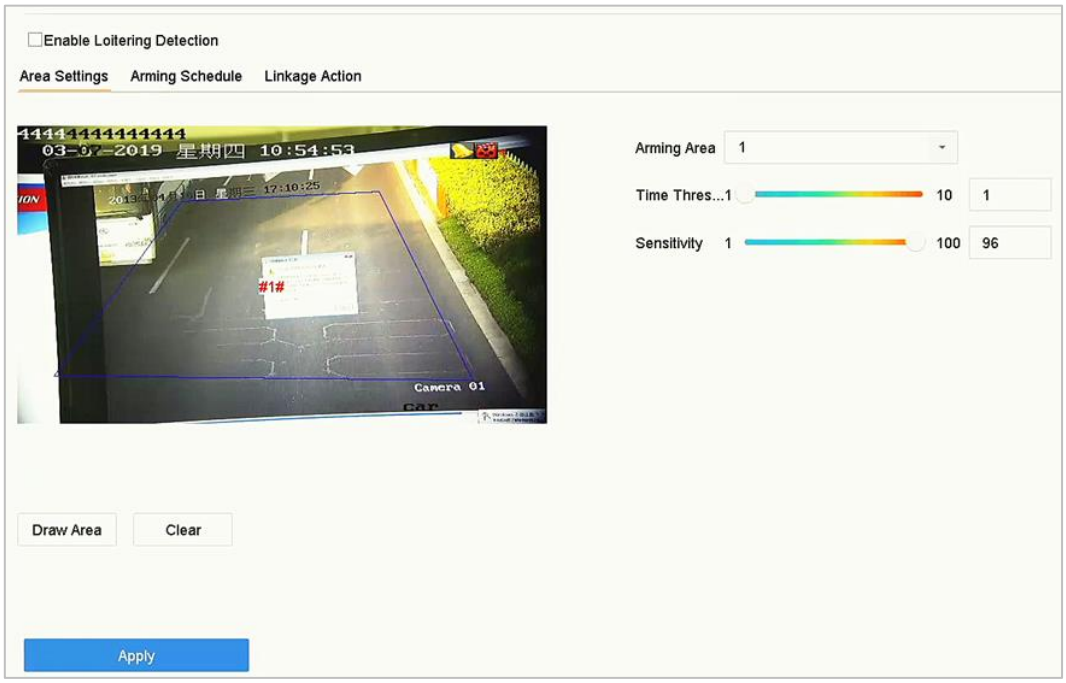


Figure 13-7 Loitering Detection

Step 4 Check **Enable Loitering Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured loitering detection pictures.

Step 6 Set loitering detection parameters.

1) Select **Arming Area**. Up to 4 areas are selectable.
2) Set Time Threshold (s).

   Time Threshold: The time of car staying in the region. If the value is 10, an alarm is triggered after the car has stayed in the region for 10s. Its range is [1s-10s].

3) Set **Sensitivity**.

   Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.8 People Gathering Detection

Purpose

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.

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

Step 2 Select a camera to configure.

Step 3 Click **People Gathering**.

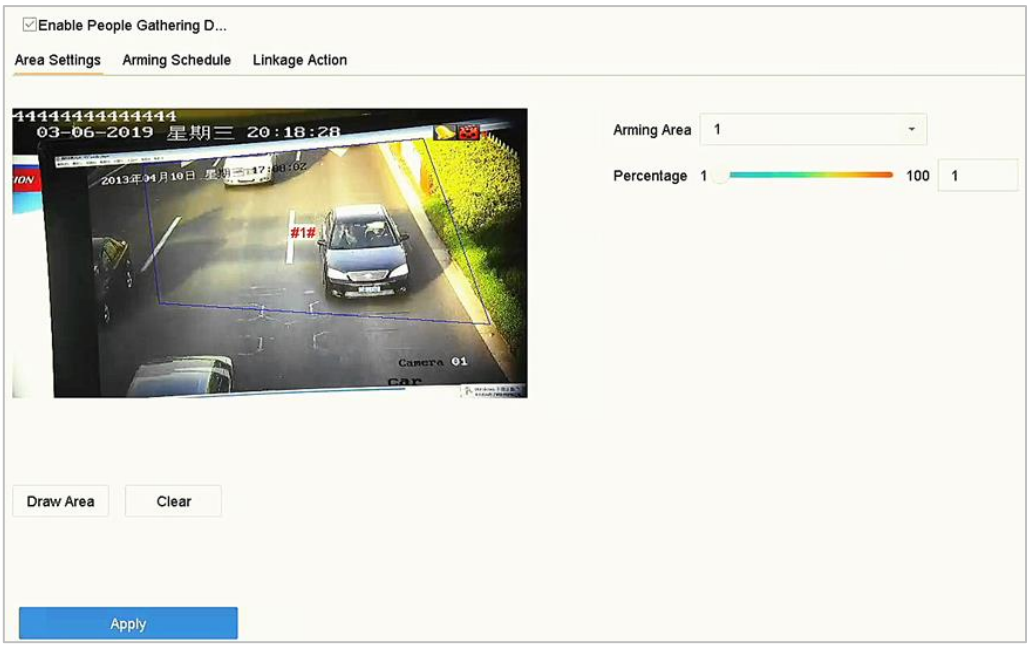


Figure 13-8 People Gathering Detection

Step 4 Check **Enable People Gathering Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured people gathering detection pictures.

Step 6 Set people gathering detection parameters.

1) Select **Arming Area**. 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 percentage refers to the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions..

Step 9 Click **Apply**.

13.9 Fast Moving Detection

Purpose

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.

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

Step 2 Select a camera to configure.

Step 3 Click **Fast Moving**.

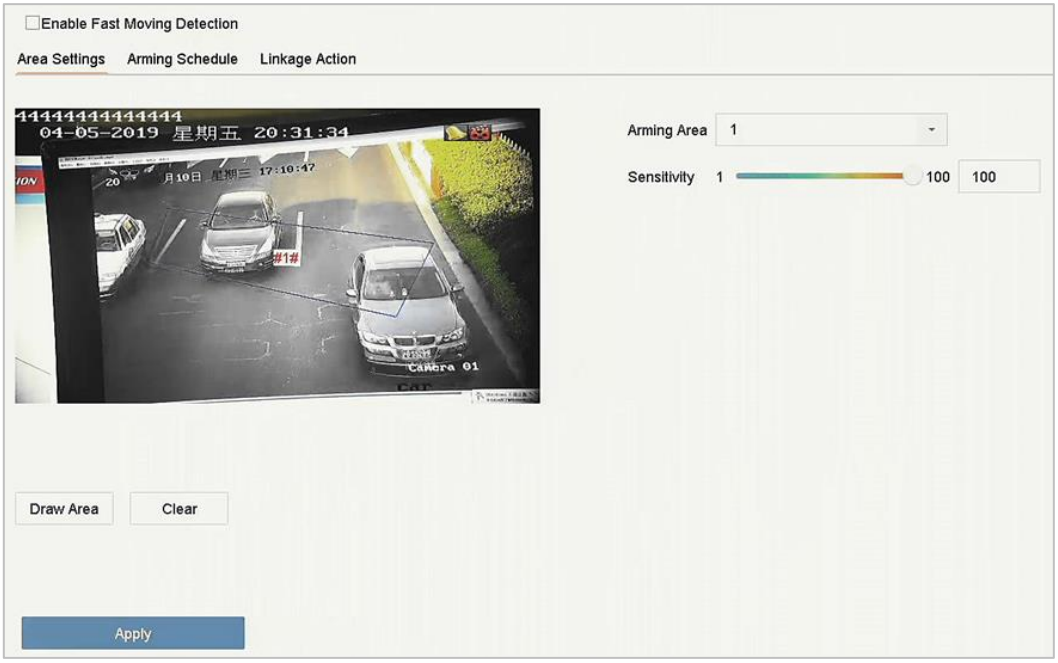


Figure 13-9 Fast Moving Detection

Step 4 Check **Enable Fast Moving**.

Step 5 Optionally, check **Save VCA Picture** to save the captured fast moving detection pictures.

Step 6 Set fast moving detection parameters.

1) Select **Arming Area**. 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 **Sensitivity**.

   Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.10 Parking Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Parking**.

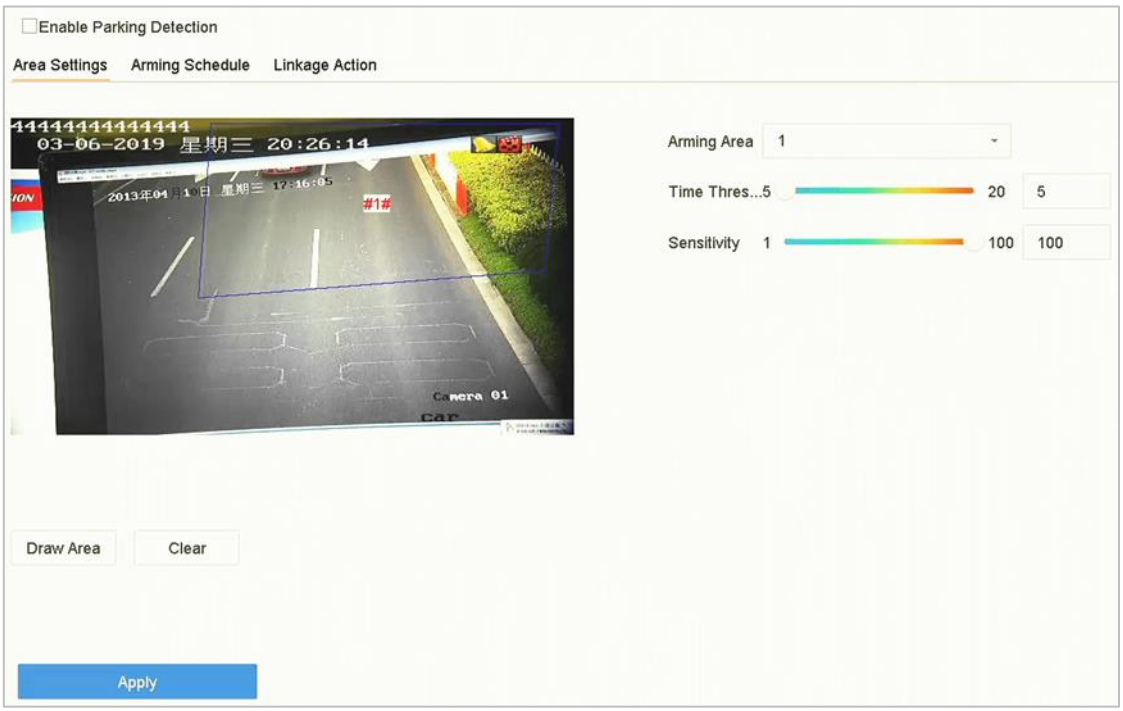


Figure 13-10 Parking Detection

Step 4 Check **Enable Parking Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured parking detection pictures.

Step 6 Set parking detection parameters.

1) Select **Arming Area**. Up to 4 areas are selectable.
2) Set **Time Threshold (s).**

   Time Threshold: The time of car staying in the region. If the value is 10, an alarm is triggered after the car has stayed in the region for 10s. Its range is [5s-20s].

3) Set **Sensitivity**.

Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.11 Unattended Baggage Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Unattended Baggage**.

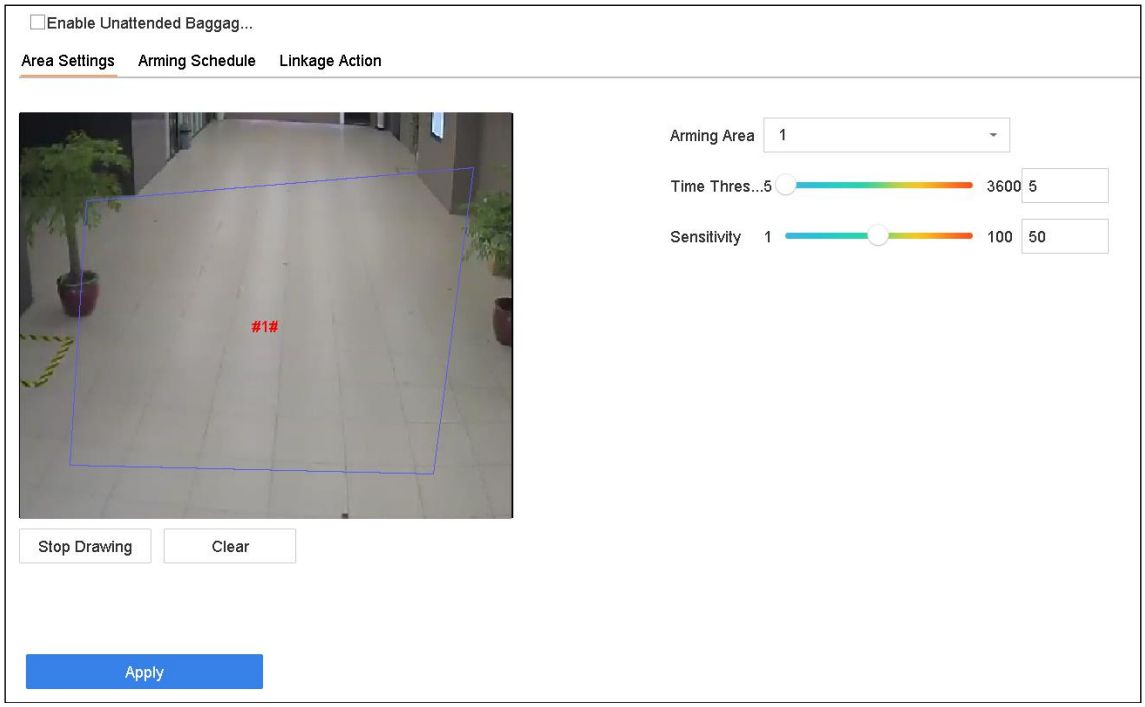


Figure 13-11 Unattended Baggage Detection

Step 4 Check **Enable Unattended Baggage Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured unattended baggage detection pictures.

Step 6 Follow these steps to 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 are left in the region. If the value is 10, an alarm is triggered after the object is left and stayed in the region for 10s. Its range is [5s-20s].

   Sensitivity: Similarity of the background image to the object. The higher the value, the easier the detection alarm will be triggered.

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

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.12 Object Removal Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Object Removable**.

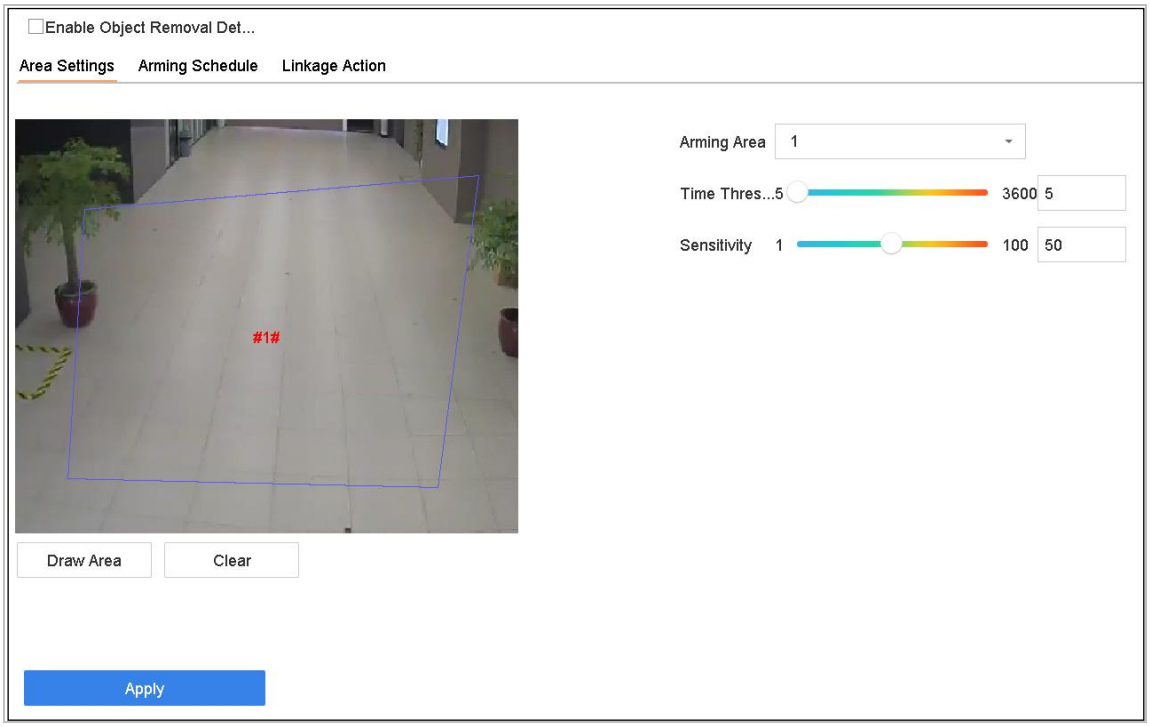


Figure 13-12 Object Removal Detection

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

Step 5 Optionally, check **Save VCA Picture** to save the captured object removable detection pictures.

Step 6 Follow these steps to 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 removed from the region. If the value is 10, alarm will be triggered after the object disappears from the region for 10s. Its range is [5s-20s].

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

3) Click **Draw area** and draw a quadrilateral in the preview window by specifying four vertices of the detection region.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.13 Audio Exception Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Audio Exception**.

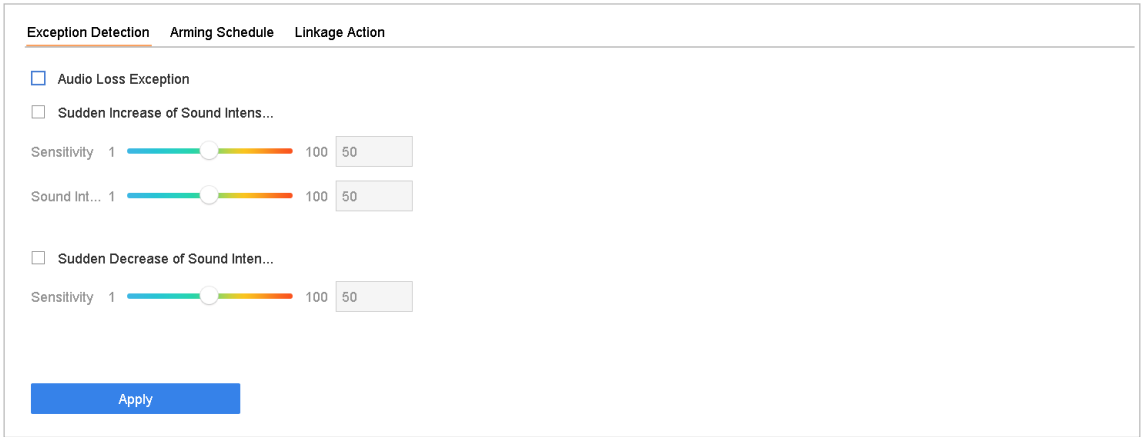


Figure 13-13 Audio Exception Detection

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

Step 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 surveillance scene. You can set the detection sensitivity and threshold for steep sound rise by configuring its **Sensitivity** and **Sound Intensity Threshold**.

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

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

   Sudden Decrease of Sound Intensity Detection: Detects a steep sound drop in the surveillance scene. You need set the detection sensitivity [1-100].

Step 6 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 8 Click **Apply**.

13.14 Sudden Scene Change Detection

Purpose

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

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

Step 2 Select a camera to configure.

Step 3 Click **Sudden Scene Change**.



Figure 13-14 Sudden Scene Change

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

Step 5 Optionally, check **Save VCA Picture** to save the captured sudden scene change detection pictures.

Step 6 Set the detection sensitivity. Sensitivity range: [1-100]. The higher the value, the more easily the change of scene can trigger the alarm.

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.15 Defocus Detection

Purpose

Image blur caused by lens defocus can be detected.

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

Step 2 Select a camera to configure.

Step 3 Click **Defocus**.

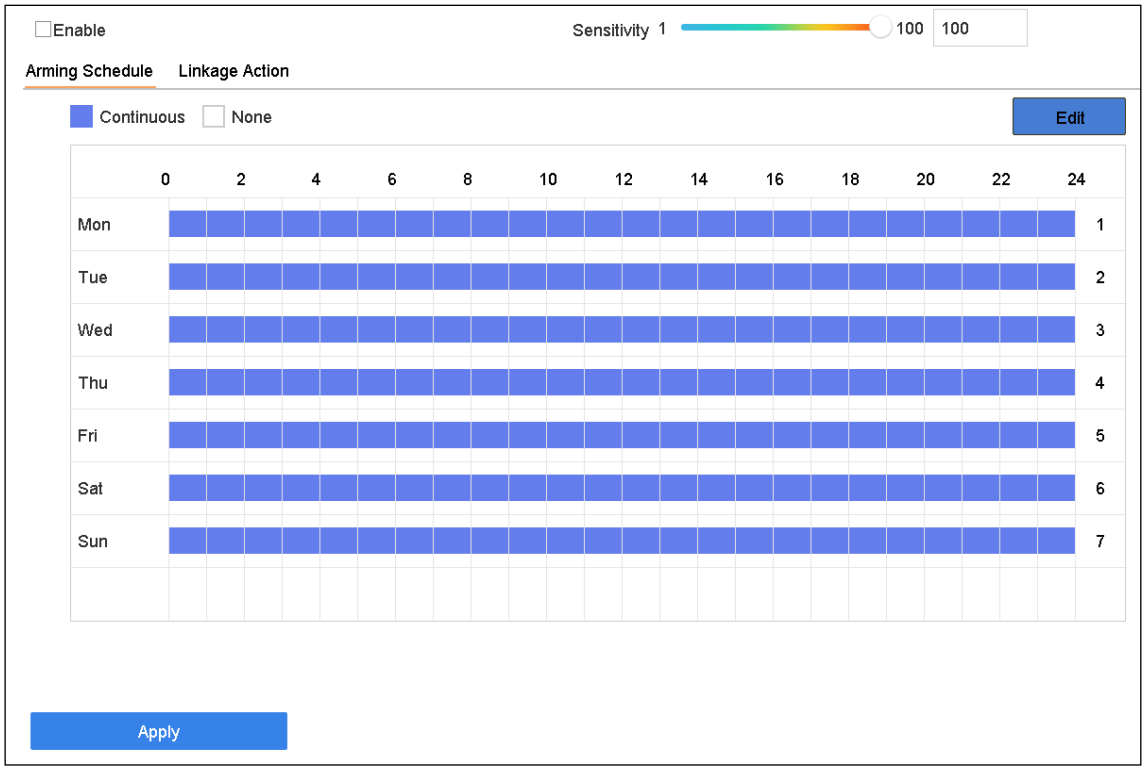


Figure 13-15 Defocus Detection

Step 4 Check **Enable Defocus Detection**.

Step 5 Optionally, check **Save VCA Picture** to save the captured defocus detection pictures.

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

Step 7 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

13.16 PIR Alarm

Purpose

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector vision field. The heat energy dissipated by a person or any other warm blooded creature such as dogs, cats, etc., can be detected.

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

Step 2 Select a camera to configure.

Step 3 Click **PIR Alarm**.

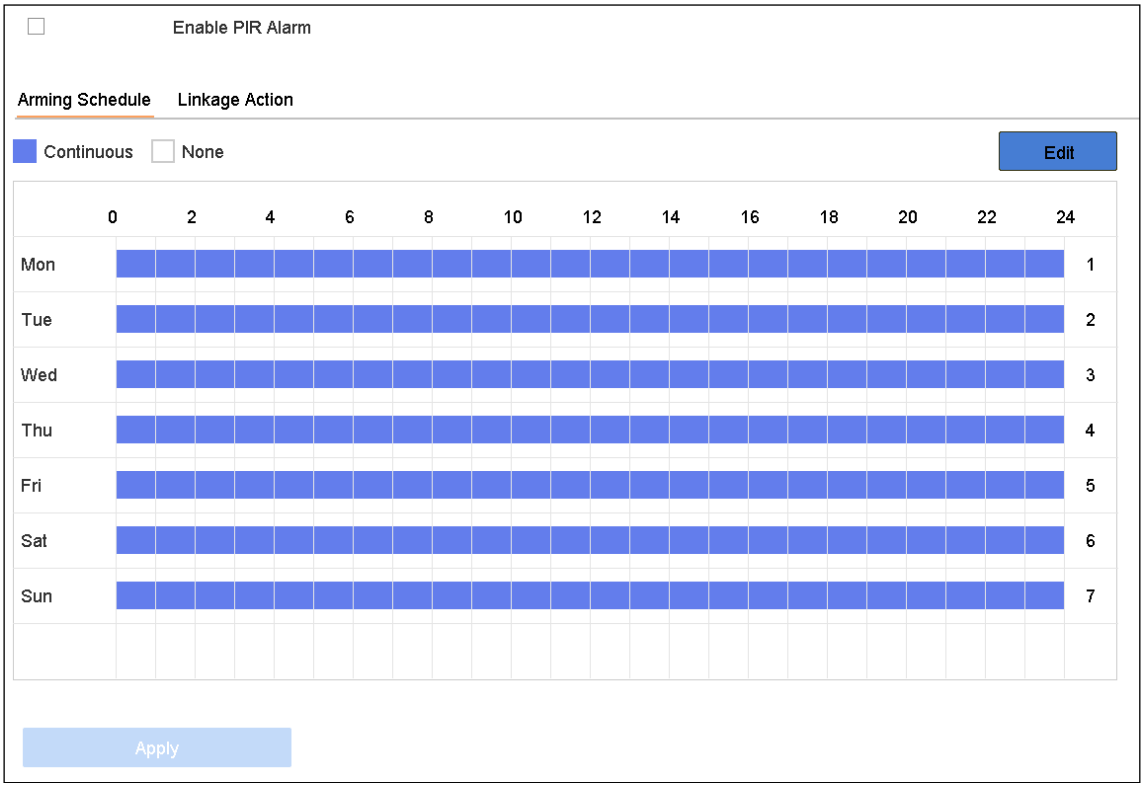


Figure 13-16 FIR Alarm

Step 4 Check **PIR Alarm**.

Step 5 Optionally, check **Save VCA Picture** to save the captured of PIR alarm pictures.

Step 6 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 8 .Click **Apply**.

13.17 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.

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

Step 2 Select a thermal camera from the camera list.

Step 3 (Optional) Check **Save VCA Picture** to save the captured pictures of detection.

Step 4 Select an event detection (Temperature, etc.).

Step 5 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 6 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 7 Click **Apply**.

13.18 Queue Management

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

Before you start

Ensure you have connected the device with queue management camera, and the camera is online.

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

Step 2 Select a queue management camera from the camera list.

Step 3 (Optional) Check **Save VCA Picture** to save the captured pictures of detection.

Step 4 Set the arming schedule. Refer to Chapter 12.1 Configure Arming Schedule.

Step 5 Set the linkage actions. Refer to Chapter 12.2 Configure Alarm Linkage Actions.

Step 6 Click **Apply**.

Chapter 14 Smart Analysis

With the configured VCA detection, the device supports smart analysis for people counting and heat map.

14.1 People Counting

Purpose

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

Step 1 Go to **Smart Analysis** > **Counting**.

Step 2 Select the camera(s).

Step 3 Select the report type to **Daily Report, Weekly Report, Monthly Report**, or **Annual Report**.

Step 4 Set the **Date** to analyze. The people counting graphic will show.

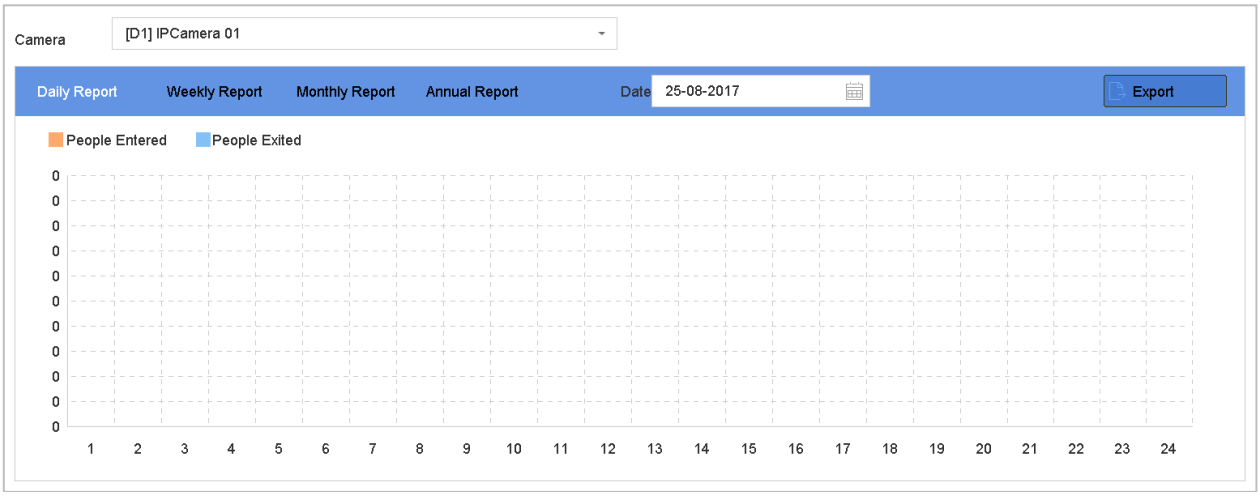


Figure 14-1 People Counting Interface

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

14.2 Heat Map

Purpose

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

The Heat Map function must be supported by the connected IP camera and the corresponding configuration must be set.

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

Step 2 Select a camera.

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

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

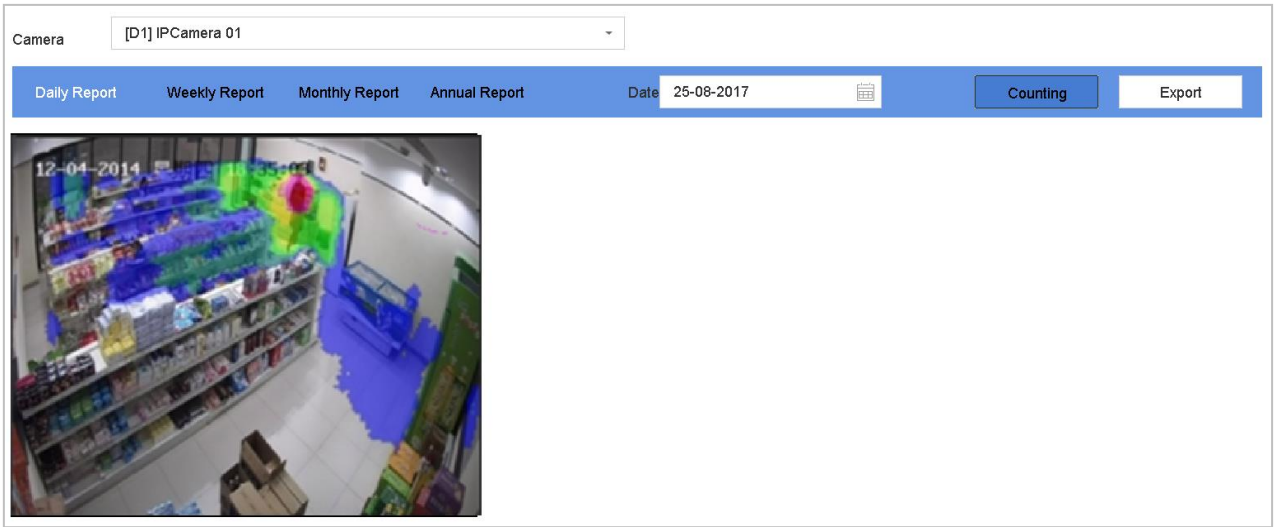


Figure 14-2 Heat Map Interface

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

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.

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

Chapter 15 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.

NOTE

The POS feature is supported by Pro Series Device only.

15.1 Configure POS Settings

15.1.1 Configure POS Connection

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

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

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

Step 4 Check **Enable**.

NOTE

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

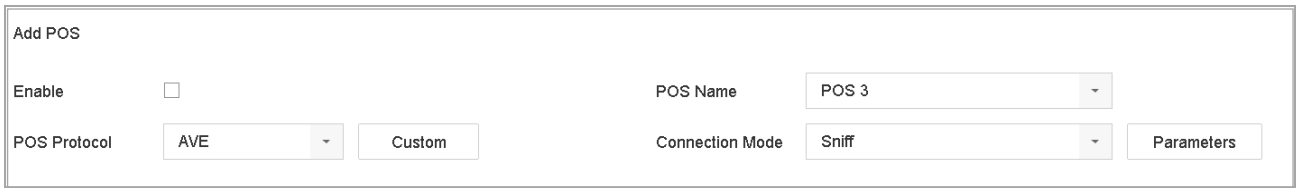


Figure 15-1 POS Settings

Step 5 Select the POS protocol to Universal Protocol, EPSON, AVE, or NUCLEUS.

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.

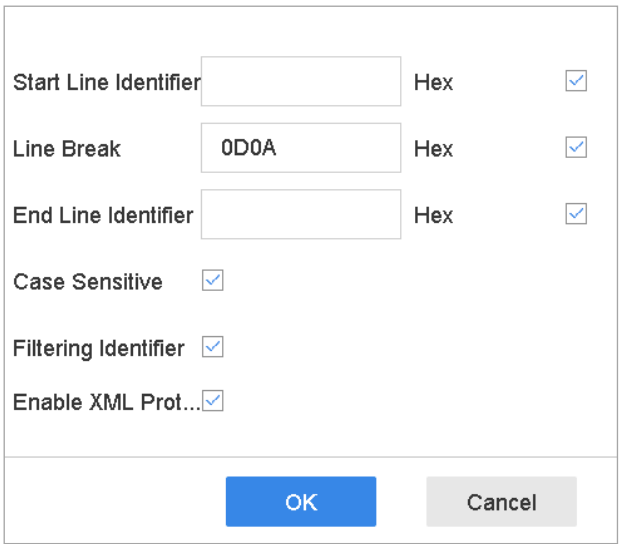


Figure 15-2 Universal Protocol Settings

- EPSON

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

- AVE

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

1) Click **Custom** to configure the AVE settings.
2) Set the rule to VSI-ADD or VNET.
3) Set the address bit of the POS message to send.
4) Click **OK** to save the settings.

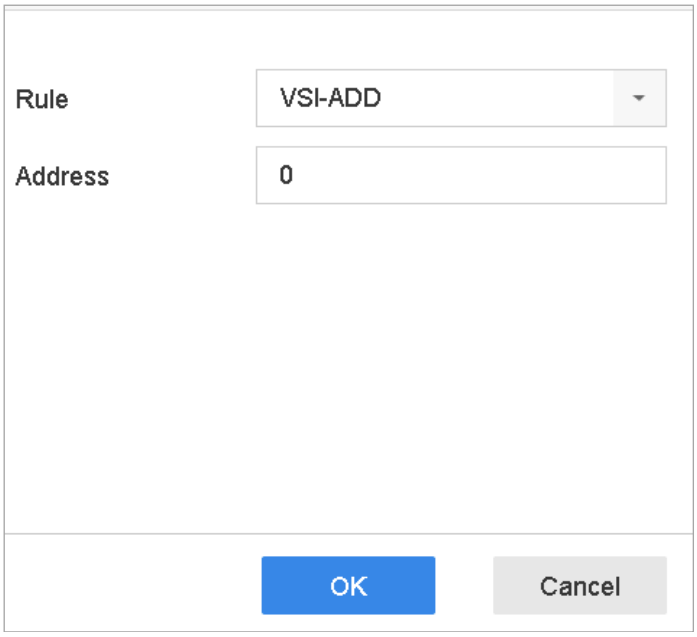


Figure 15-3 AVE Settings

- NUCLEUS
  1) Click the **Custom** to configure the NUCLEUS settings.
  2) 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.

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

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

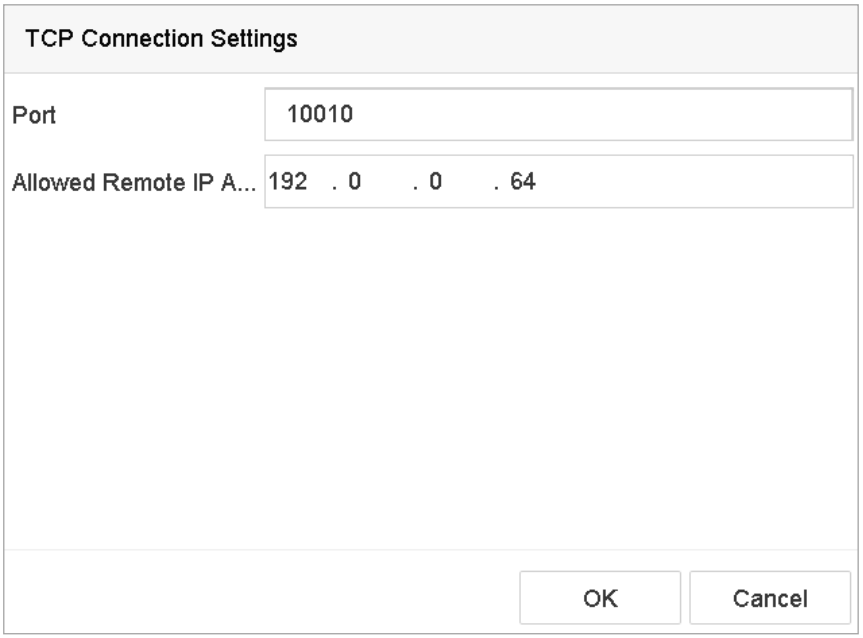


Figure 15-4 TCP Connection Settings

- UDP Connection
  1) When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.
  2) Set the **Allowed Remote IP Address** of the device sending the POS message.
- USB-to-RS-232 Connection

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

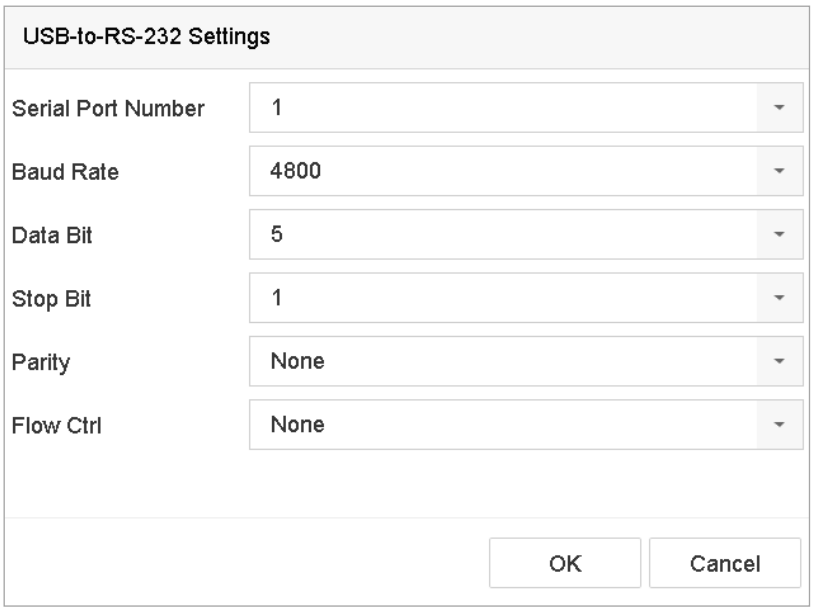


Figure 15-5 USB-to-RS-232 Settings

- RS-232 Connection

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

- Multicast Connection

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

- Sniff Connection

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

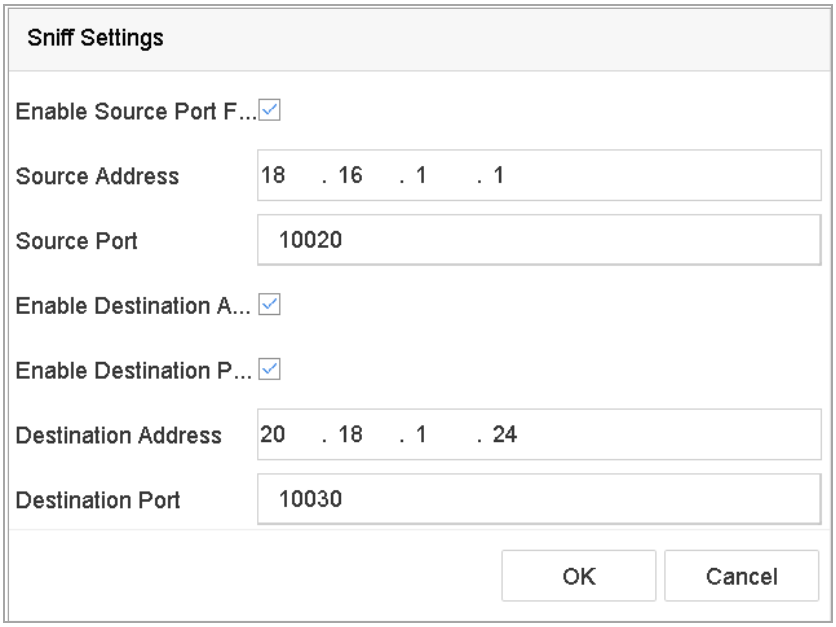


Figure 15-6 Sniff Settings

15.1.2 Configure POS Text Overlay

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

Step 2 Click **Channel Linkage and Display** tab.

Step 3 Select the linked channel to overlay the POS characters.

Step 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.

Step 5 In the **Privacy Settings**, set the POS privacy information to not display on the image, e.g., the card number, user name, etc.

Step 6 Result: The defined privacy information will be displayed using ***on the image instead.

Step 7 (optional) Check the checkbox to enable the **Overlay POS in Live View**. When this feature is enabled, the POS information is overlaid on the Live View image.

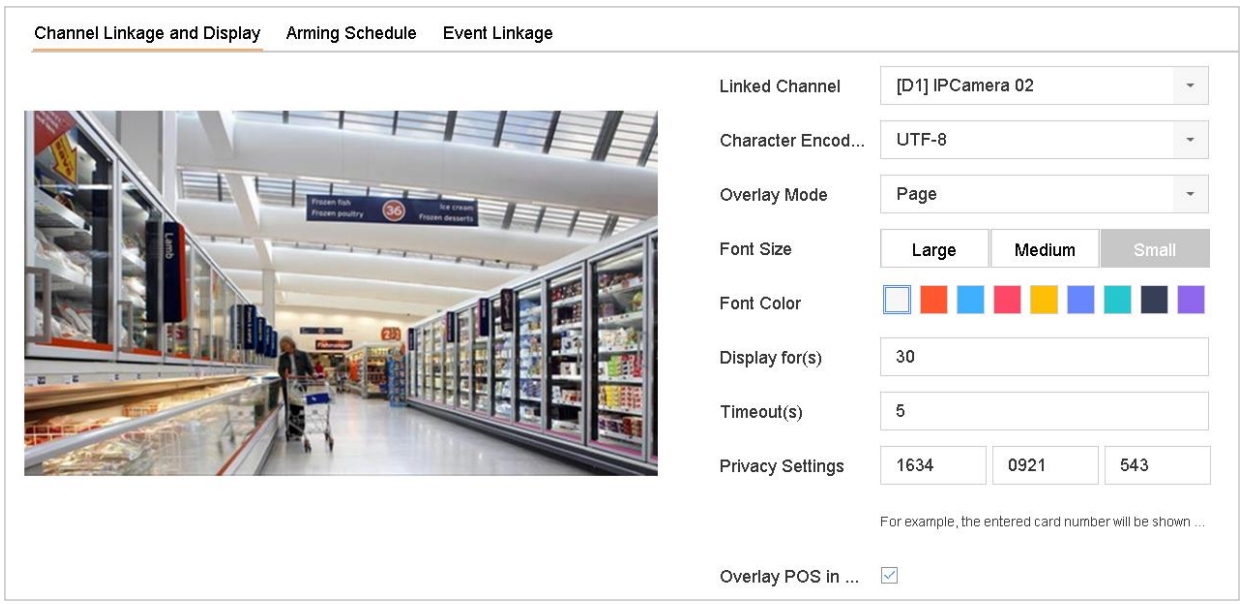


Figure 15-7 Overlay Character Settings

NOTE

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

Step 8 Click **Apply** to activate the settings.

15.2 Configure POS Alarm

Purpose

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

Step 1 Go to **Storage** > **Recording Schedule**.

Step 2 Set the POS event's arming schedule.

Step 3 Go to **System** > **POS**.

Step 4 Click **Event Linkage** on the POS adding or editing interface.

Step 5 Select the normal linkage actions: full screen monitoring, audio warning, or send e-mail.

Step 6 Select one or more alarm output(s) to trigger.

Step 7 Select one or more channels to record or become full-screen monitoring when a POS alarm is triggered.

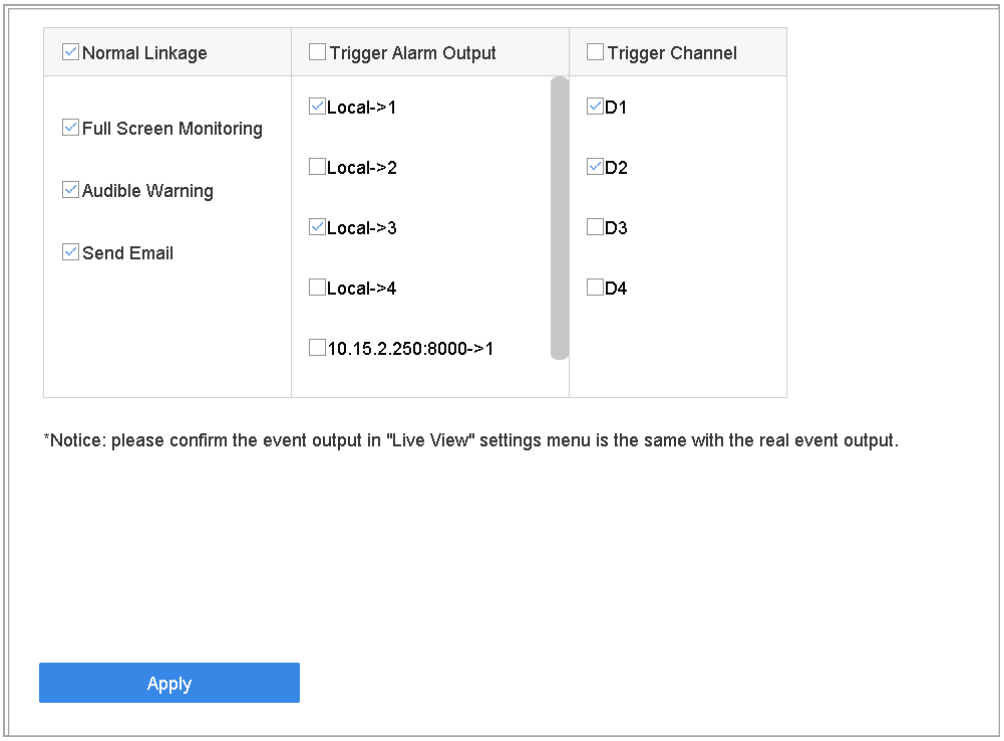


Figure 15-8 Set Trigger Cameras of POS

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

Chapter 16 Network Settings

16.1 Configure TCP/IP Settings

Purpose

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

16.1.1 Device with Dual Network Interface

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

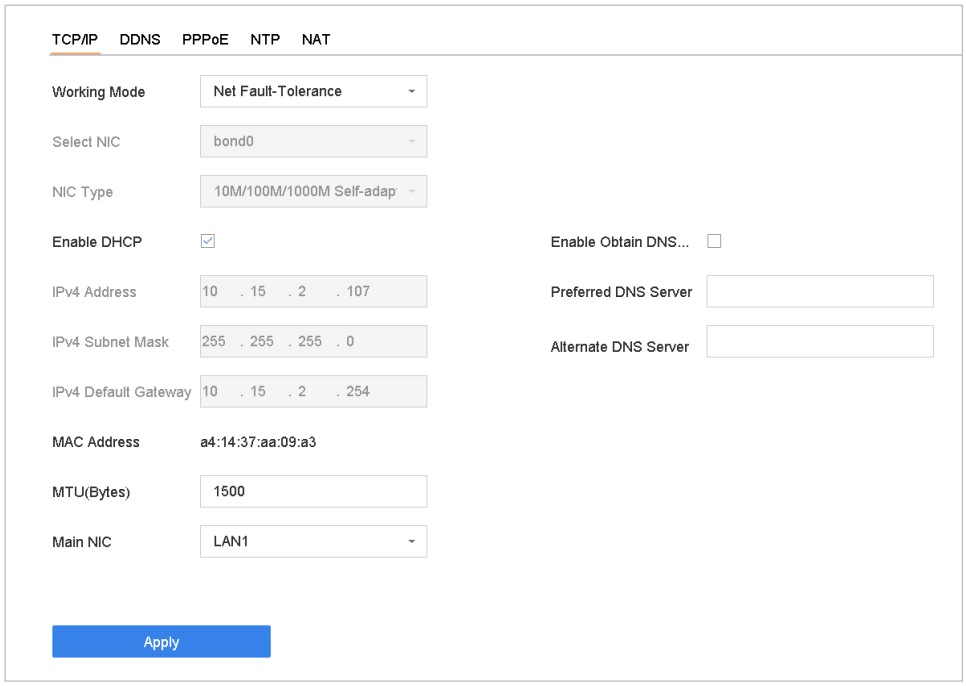


Figure 16-1 TCP/IP Settings

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

- **Net-Fault Tolerance**: The two NIC cards use the same IP address, and you can select the main NIC to LAN1 or LAN2. In this way, in case of one NIC card failure, the device will automatically enable the other 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.

Step 3 Configure other IP settings as needed.

NOTE

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

Step 4 Click **Apply**.

16.1.2 Device with a Single Network Interface

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

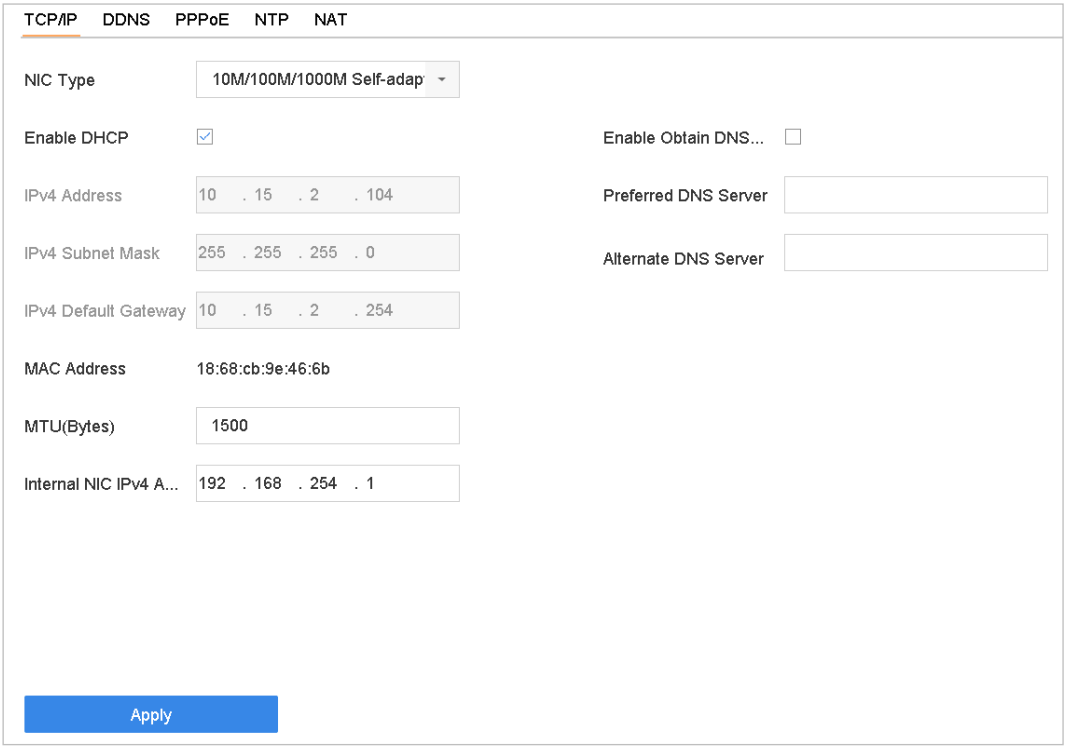


Figure 16-2 TCP/IP Settings

Step 2 Configure network parameters as needed.

NOTE

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

Step 3 Click **Apply**.

16.2 Configure Guarding Vision

Purpose

Guarding Vision provides mobile phone application and platform service to access and manage your connected devices, which enables you to get a convenient remote access to the surveillance system.

Step 1 Go to **System** > **Network** > **Advanced** > **Platform Access**.

Step 2 Check **Enable** to activate the function. Then the service terms will pop up.

1) Enter the verification code in **Verification Code**.
2) Scan the QR code to read the service terms and privacy statement.
3) Check The Guarding Vision service will require internet access. Please read Service Terms and Privacy Statement before enabling the service if you agree the service terms and privacy statement.
4) Click **OK** to save the settings.

NOTE

- Guarding Vision 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.

Step 3 (Optional) Check **Custom** to enter the server address as your desire.

Step 4 (Optional) Check **Enable Stream Encryption**, verification code is required for remote access and live view.

Step 5 (Optional) Click **Unbind** if the device requires to unbind with the current Guarding Vision account.

Step 6 Click **Apply**.

What to do next:

After configuration, you can access and manage your devices through Guarding Vision app or website.

16.3 Configure EHome

Purpose

EHome protocol is non-open and push-mode protocol based on TCP/UDP, which can realize the communication between the system and mobile devices (e.g., body camera, MNVR, etc.). The system is as a server and you can register the device to the system. The protocol is suitable for the application of dynamic device IP address.

Step 1 Go to **System** > **Network** > **Advanced** > **Platform Access**.

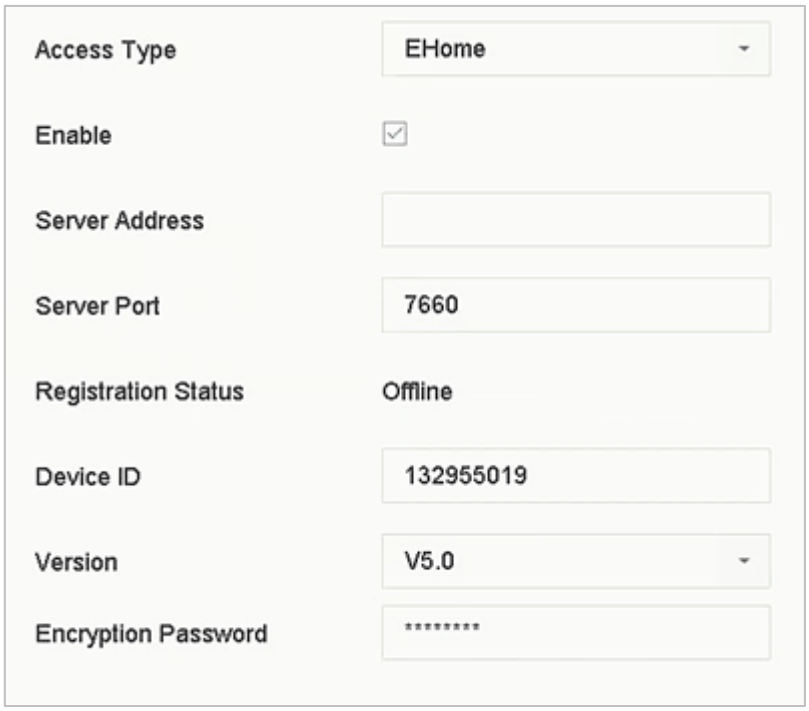


Figure 16-3 EHome Settings

Step 2 Select **Access Type** as EHome.

Step 3 Check **Enable**.

NOTE

Enabling EHome will disable Guarding Vision platform access.

Step 4 Set the related parameters, including **Server Address**, **Server Port**, **Device ID**, **Version**, and **Encryption Password**.

- **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**: The Device ID shall be provided by the platform.
- **Version**: EHome protocol version, only V5.0 is available.
- **Encryption Password**: Encryption password is required when using EHome V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the EHome platform.

Step 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.

16.4 Configure DDNS

Purpose

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

Before You Start

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

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

Step 2 Check **Enable**.

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

NOTE

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

Step 4 Enter **Server Address** for **DynDNS** (i.e., members.dyndns.org).

Step 5 Under **Device Domain Name**, enter the domain name obtained from the DynDNS Website.

Step 6 Enter the **User Name** and **Password** registered in the DynDNS Website.

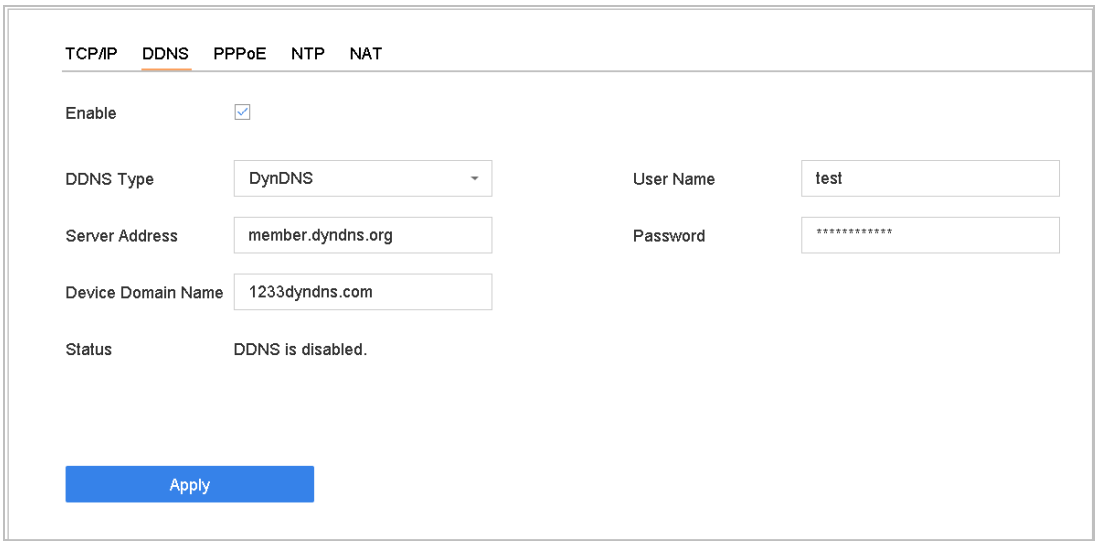


Figure 16-4 DDNS Settings

Step 7 Click **Apply**.

16.5 Configure PPPoE

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

NOTE

Contact your Internet service provider for details about PPPoE service.

16.6 Configure NTP

Purpose

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

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

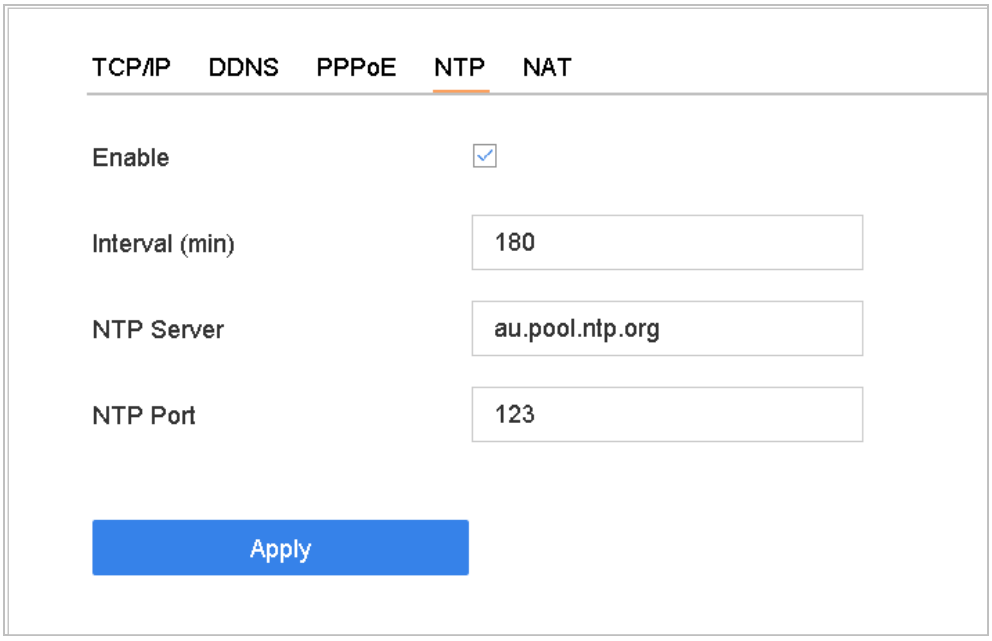


Figure 16-5 NTP Settings

Step 2 Check **Enable**.

Step 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

Step 4 Click **Apply**.

16.7 Configure SNMP

Purpose

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

Before You Start

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

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

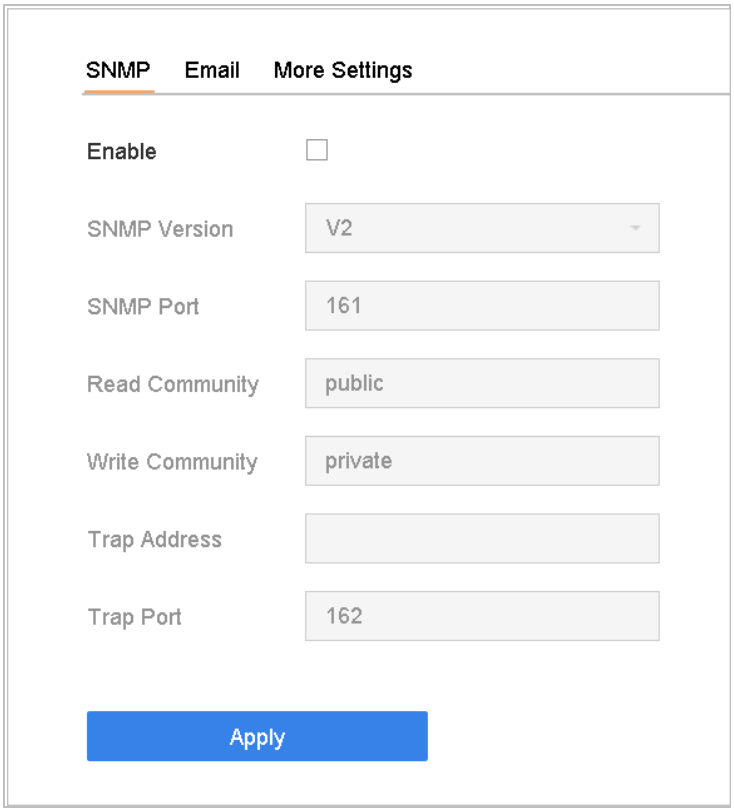


Figure 16-6 SNMP Settings

Step 2 Check **Enable**. A message will pop up to notify about a possible security risk. Click **Yes** to continue.

Step 3 Configure the SNMP settings as needed.

- **Trap Address**: SNMP host IP address.
- **Trap Port**: Port of the SNMP host.

Step 4 Click **Apply**.

16.8 Configure Email

Purpose

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

Before You Start

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

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

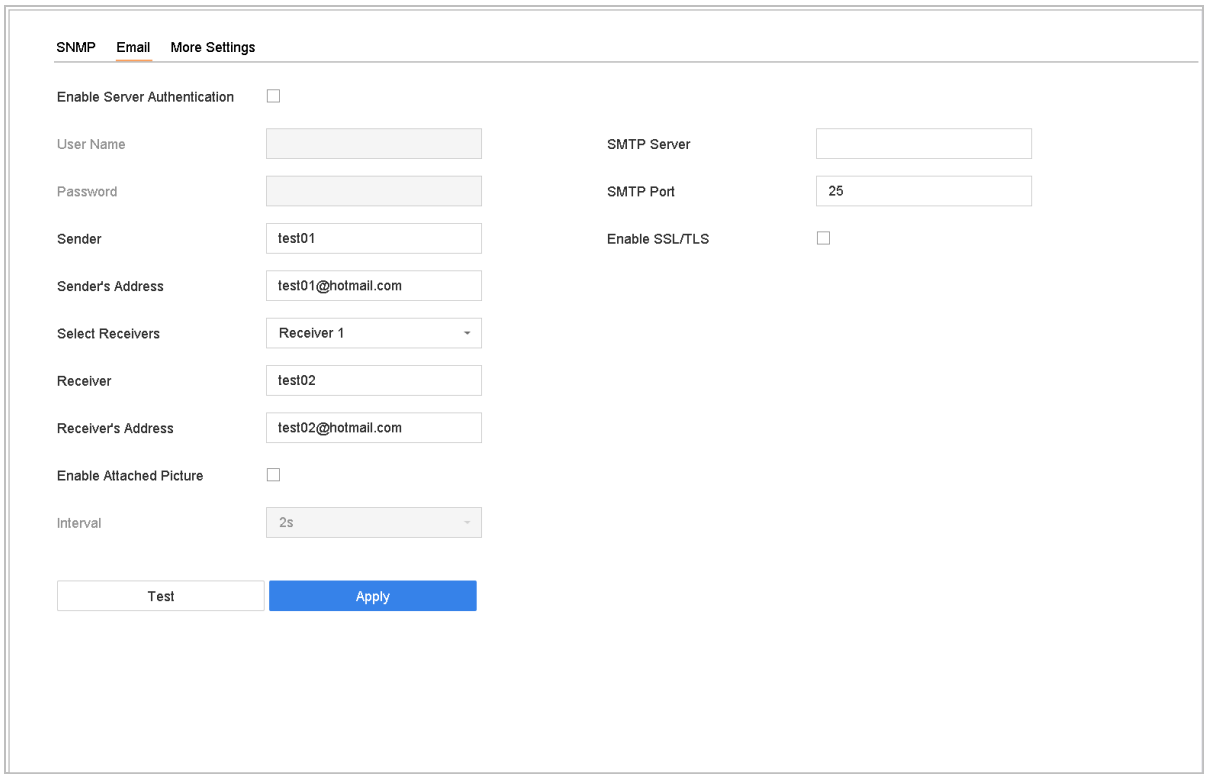


Figure 16-7 E-mail Settings

Step 2 Configure the following e-mail settings.

- **Enable Server Authentication**: Check to enable the function if the SMTP server requires user authentication, and enter the user name and password accordingly.
- **SMTP Server**: IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
- **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 e-mail address of the user to be notified.
- **Enable Attached Picture**: Check to send e-mail with attached alarm images. The interval is the time between sending two subsequent alarm images.

Step 3 Click **Apply**.

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

16.9 Configuring NAT

Purpose:

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

- **UPnP™**

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.

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.

Step 1 Go to **Menu** > **Configuration** > **Network** > **NAT**.

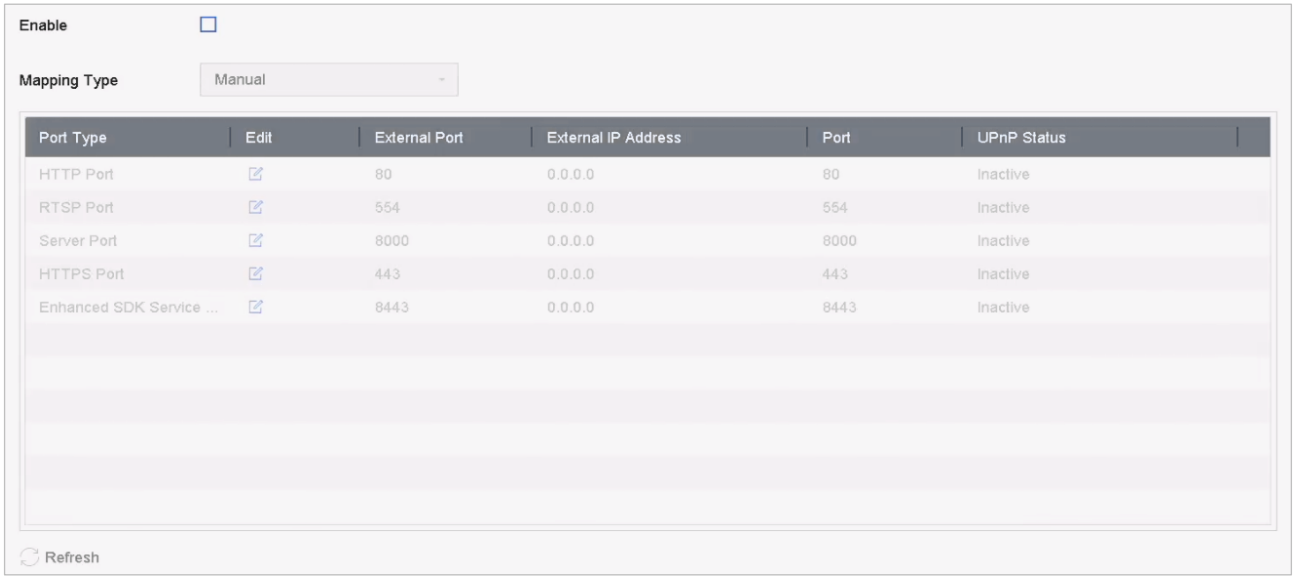


Figure 16-8 UPnP™ Settings Interface

Step 2 Check **Enable UPnP.**

Step 3 Select **Mapping Type** as **Manual** or **Auto**.

OPTION 1: Auto

If you select **Auto**, the port mapping items are read-only, and the external ports are set by the router automatically.

NOTE

You can click **Refresh** button to get the latest status of the port mapping.

OPTION 2: 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.

Step 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.

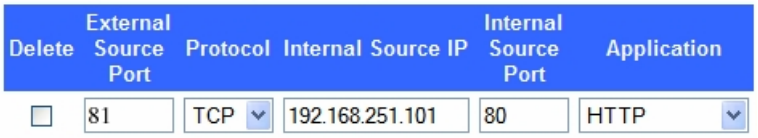


Figure 16-9 Setting Virtual Server Item

16.10 Configure Ports

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

Go to **System** > **Network** > **Advanced** > **More Settings** and configure port settings as needed.

- **Alarm Host IP/Port**: With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the client management system (CMS) software installed.

  The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS software (e.g., CMS) is installed, and the **Alarm Host Port** (7200 by default) must be the same as the alarm monitoring port configured in the software.

- **Server Port**: Server port (8000 by default) should be configured for remote client software access and its valid range is 2000 to 65535.
- **HTTP Port**: HTTP port (80 by default) should be configured for remote Web browser access.
- **Multicast IP**: Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through network. A multicast IP address covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use 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.

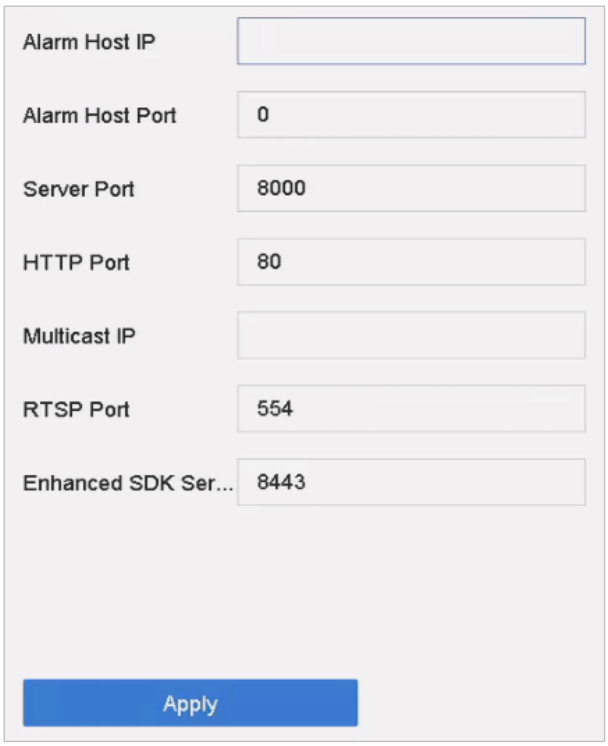


Figure 16-10 Port Settings

Chapter 17 Hot Spare Device Backup

Purpose

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

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

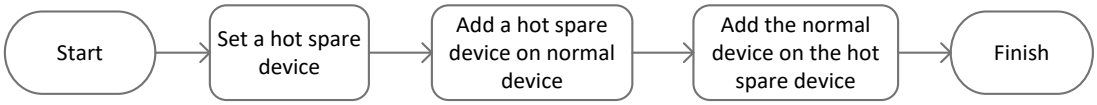


Figure 17-1 Building a Hot Spare System

Before You Start

At least 2 devices must be online.

17.1 Set Hot Spare Device

Purpose

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

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

Step 2 Set the **Work Mode** to **Hot Spare Mode**.

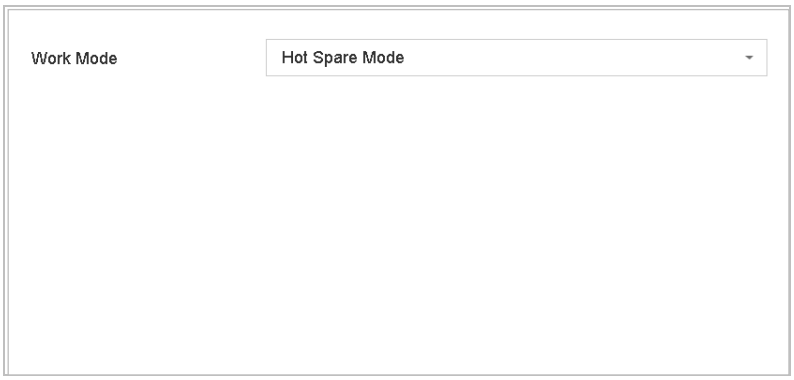


Figure 17-2 Hot Spare

Step 3 Click **Apply**.

Step 4 Click **Yes** in the popup attention box to reboot the device.

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 working mode of the hot spare device to normal mode to ensure the normal operation afterwards.

17.2 Set Working Device

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

Step 2 Set the **Work Mode** to **Normal Mode**.

Step 3 Check **Enable**.

Step 4 Enter the IP address, user name, and admin password of the hot spare device.

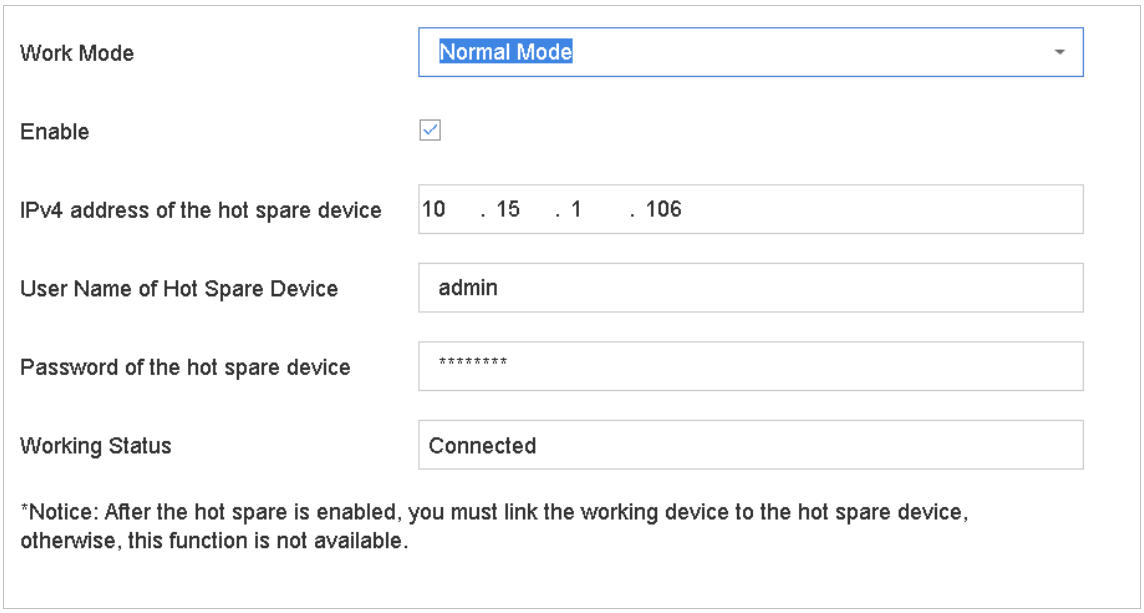


Figure 17-3 Hot Spare

Step 5 Click **Apply**.

17.3 Manage Hot Spare System

Step 1 Go to **System > Hot Spare** in the hot spare device.

Step 2 Check working devices on the device list and click **Add** to link the working device to the hot spare device.

NOTE

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

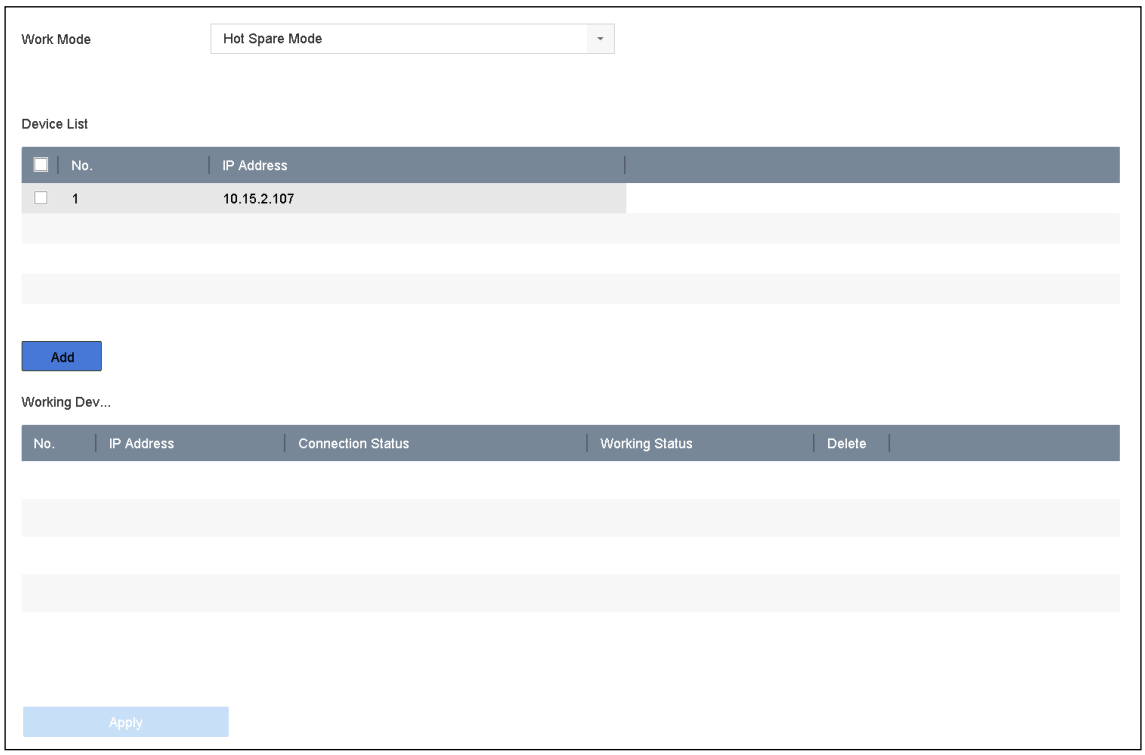


Figure 17-4 Add Working Device

Table 17-1 Working Status Descrption

Working Status	Description
No record	The working device works properly.
Backing up	If the working device goes offline, the hot spare device will record the video of the IP camera connected to the working device for backup The record back up functions for 1 working device at a time.
Synchronizing	When the working device comes back online, the lost video files will be restored by the record synchronization function. The record synchronization function can be enabled for 1 working device at a time.

Chapter 18 User Management and Security

18.1 Manage User Accounts

Purpose

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

18.1.1 Add a User

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

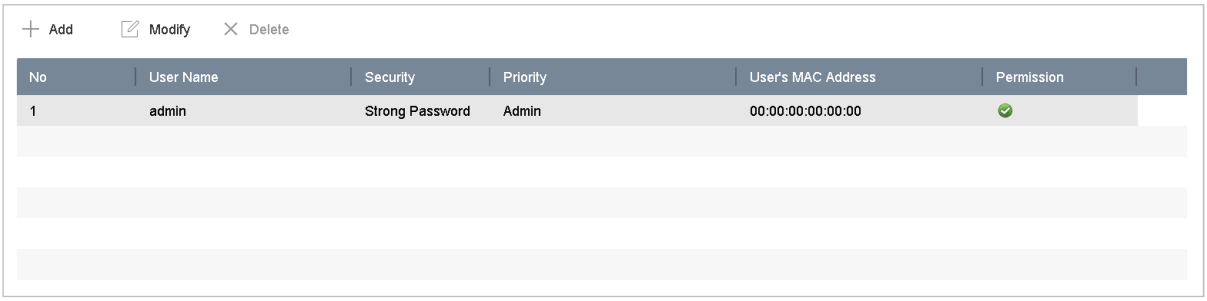


Figure 18-1 User Management Interface

Step 2 Click **Add** to enter the operation permission interface.

Step 3 Input the admin password and click **OK**.

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

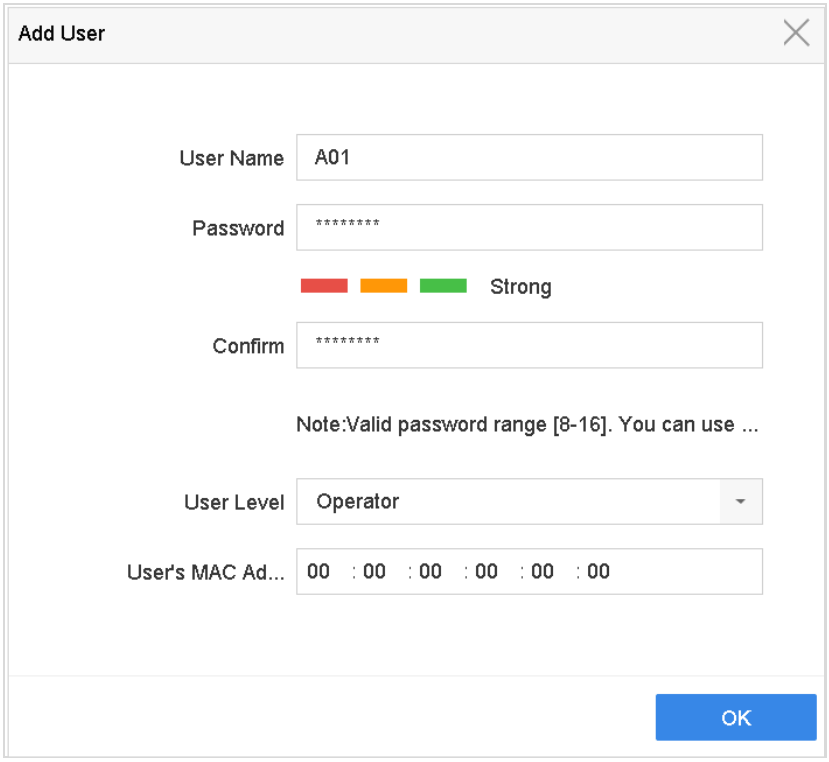


Figure 18-2 Add User

WARNING

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.

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

Step 6 In the User Management interface, the added new user is displayed on the list.

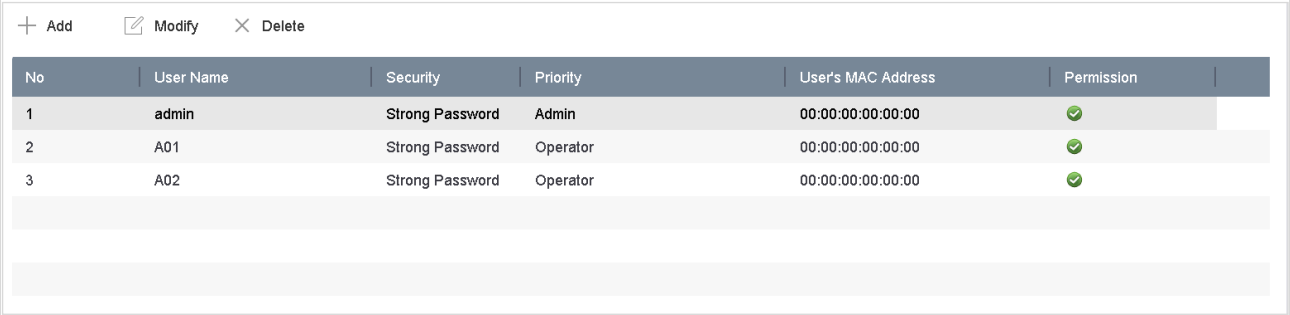


Figure 18-3 User List

18.1.2 Edit the Admin User

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

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

Step 2 Select the admin user from the list.

Step 3 Click **Modify**.

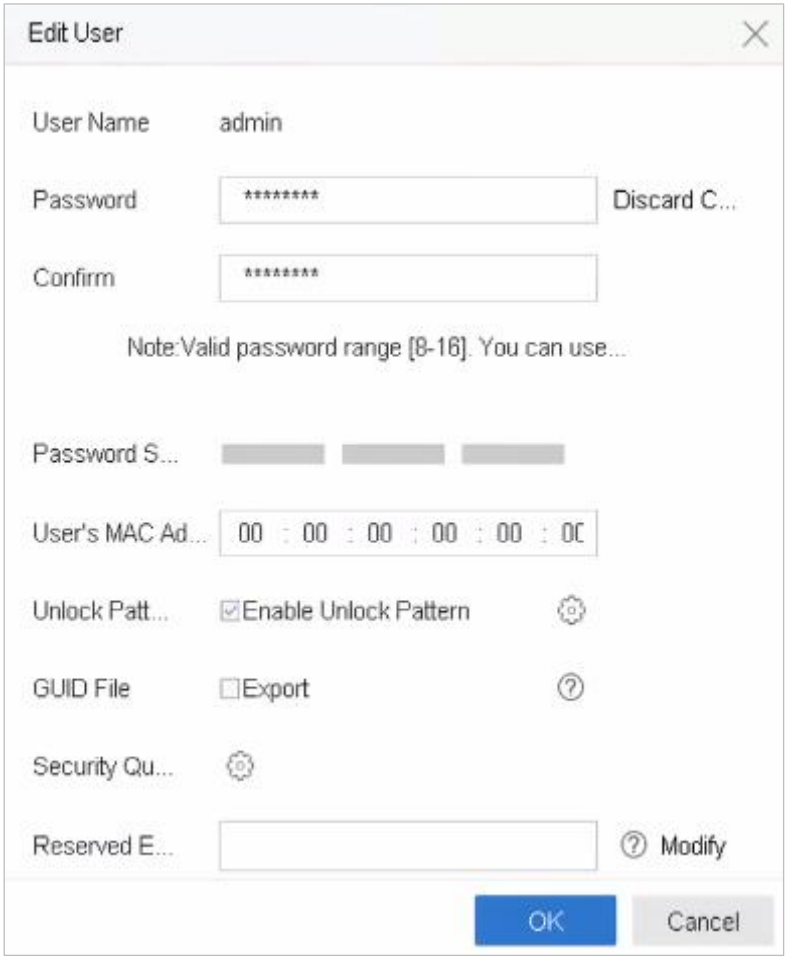


Figure 18-4 Edit User (Admin)

Step 4 Edit the admin user information as desired, including a new admin password (strong password is required) and MAC address.

Step 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.

Step 6 Check **Export** of **Export GUID** 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 disk in the Import/Export interface for the future password resetting.

Step 7 Configure security question for password resetting.

Step 8 Configure reserved email for password resetting.

Step 9 Click **OK** to save the settings.

18.1.3 Edit an Operator/Guest User

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

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

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

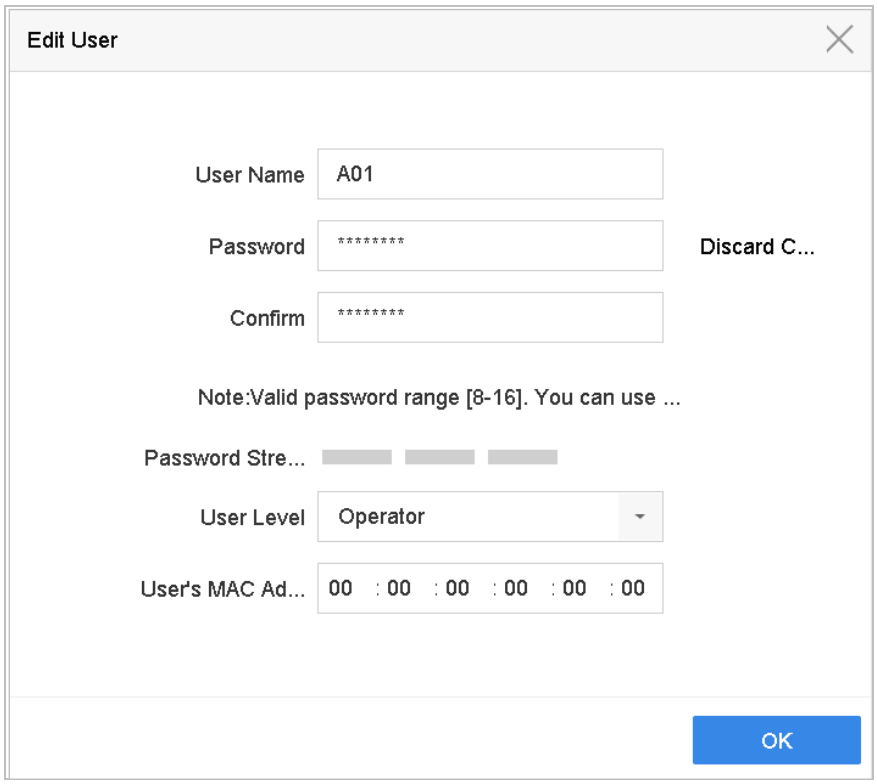


Figure 18-5 Edit User (Operator/Guest)

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

18.1.4 Delete a User

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

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

Step 2 Select a user from the list.

Step 3 Click **Delete** to delete the selected user account.

18.2 Manage User Permissions

18.2.1 Set User Permissions

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

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

Step 2 Select a user from the list, and then click to enter the permission settings interface.

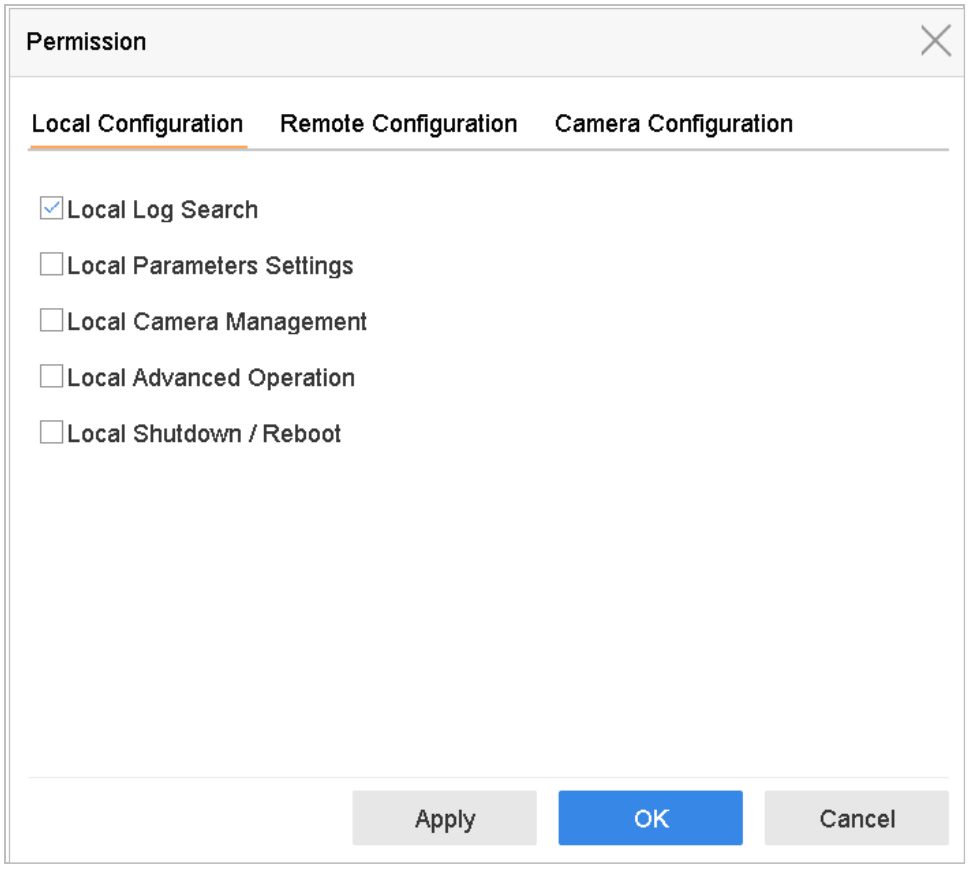


Figure 18-6 User Permission Settings Interface

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

- 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.

- 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.

- 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). Available for double verification function, refer to 18.2.4 Set Double Verification Permission for Non-Admin Users for details.

Remote Playback/Download: Remotely playing back or downloading recorded files of the selected camera(s). Available for double verification function, refer to 18.2.4 Set Double Verification Permission for Non-Admin Users for details.

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. Available for double verification function, refer to 18.2.4 Set Double Verification Permission for Non-Admin Users for details.

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

NOTE

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

18.2.2 Set Local Live View Permission for Non-Admin Users

The admin user can assign to normal users (Operator or Guest) the live view permission for specific cameras.

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

Step 2 Click .

Step 3 Input admin password and click **OK**.

Step 4 Select cameras that a non-admin user can view locally and click **OK.**

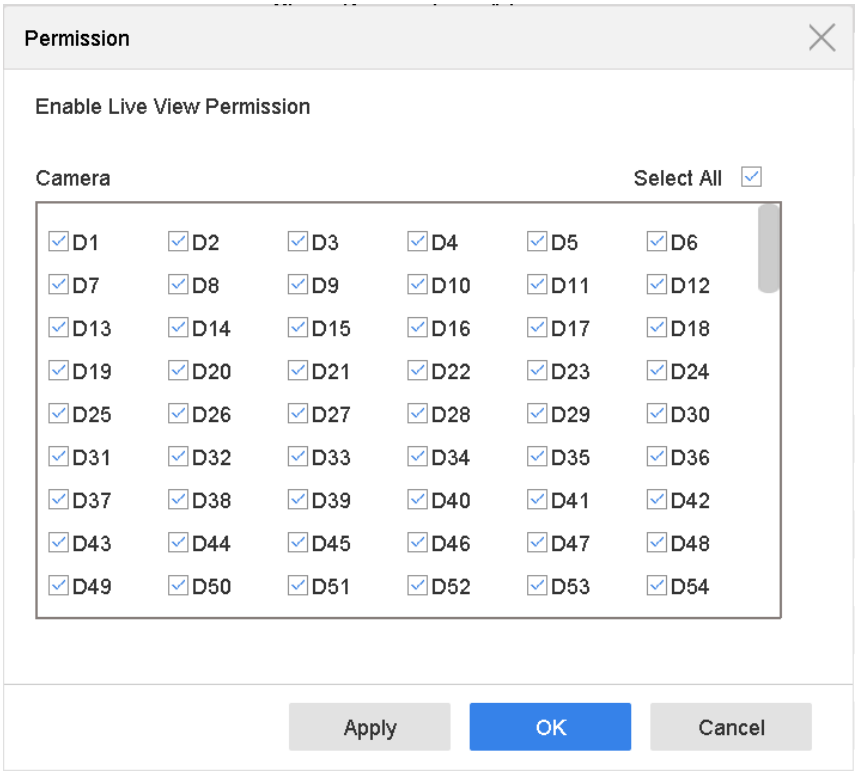


Figure 18-7 Set Live View Permissions

Step 5 Click  of non-admin user.

Step 6 Click the **Camera Configuration** tab.

Step 7 Select Camera Permission as **Local Live View**.

Step 8 Select cameras to display in Live View.

Step 9 Click **OK**.

18.2.3 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.

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

Step 2 Click **Live View Permission on Lock Screen**.

Step 3 Input admin password and click **Next.**

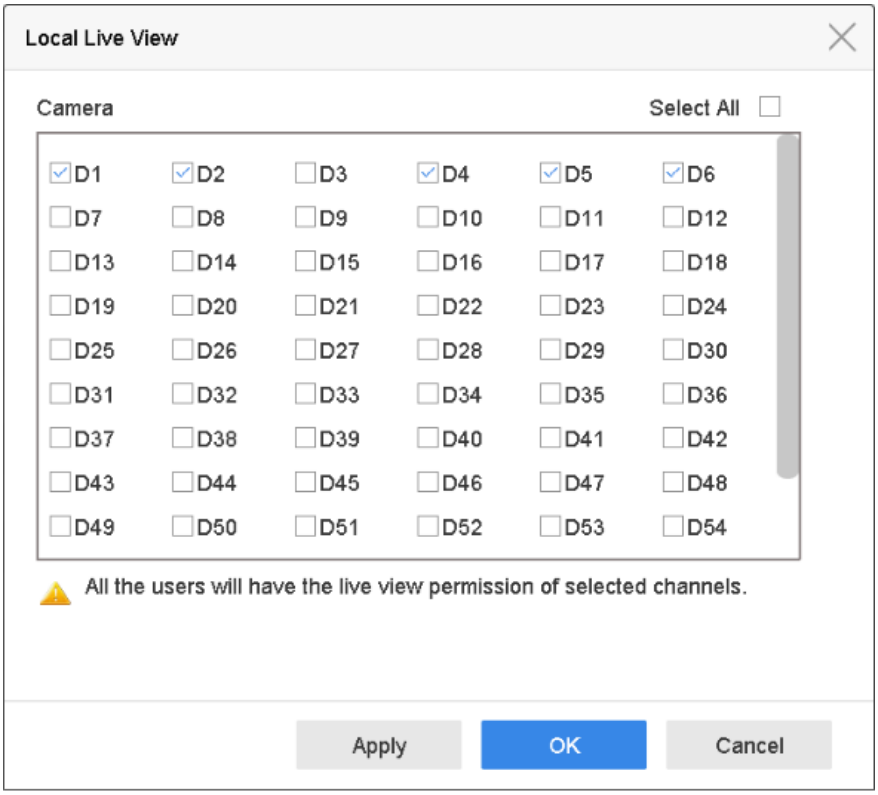


Figure 18-8 Set Live View Permissions on Lock Screen

Step 4 Set the permissions.

- Select the camera (s) to allow live view when the current user account is in logout status.
- Deselect the camera (s) to forbidden the camera (s) being viewed when the current user account is in logout status.

Step 5 Click **OK**.

NOTE

- 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) (refer to 18.2.2 Set Local Live View Permission for Non-Admin Users), the live view permission for such camera (s) on lock screen status cannot be configured (live view not allowed by default).

18.2.4 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.

Step 1 Go to **Maintenance** > **System Service** > **Double Verification Settings**.

Step 2 Check **Enable Double Verification**.

Step 3 Set double verification user. The double verification is different from the system user. You can add up to 8 double verification users.

3. Click **Add** to add a double verification user.
4. Enter the admin password.
5. Set the user parameters, including user name, password, camera permission, etc.
6. Click **OK**.



Figure 18-9 Set Double Verification User

Step 4 Click **Apply**.

Step 5 Go to **System** > **User**.

Step 6 Click to edit user permission.

Step 7 Select **Camera Permission**. Only **Local Playback**, **Remote Playback/Download**, and **Local Video Export** are available for double verification.

Step 8 Select the channel(s) that requires double verification.

Step 9 Click **OK**.

18.3 Configure Password Security

18.3.1 Export GUID File

The GUID file may help you to reset password when you forget password.

Step 1 Select to export GUID file when you are activating the device, or editing the admin user account.

Step 2 Insert the U flash disk to your device, and export the GUID file to the U flash disk.

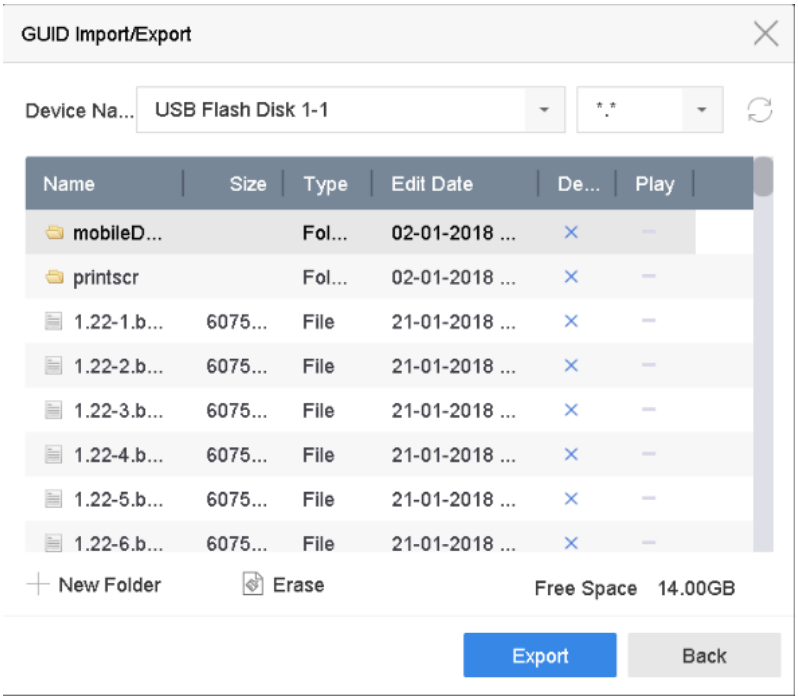


Figure 18-10 Export GUID File

NOTE

Please keep your GUID file properly for future password resetting.

18.3.2 Configure Security Questions

The security question configuration may help you to reset password when you forget your password or encounter security issues.

Step 1 Click **Security Question Configuration** when you are activating the device, or editing the admin user account.

Step 2 Select three security questions from the drop-down list and input the answers.

Step 3 Click **OK**.

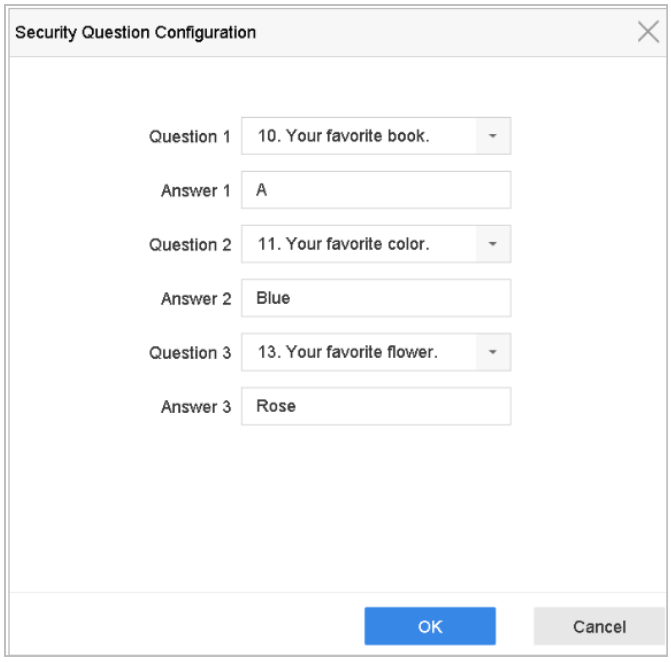


Figure 18-11 Configure Security Questions

18.3.3 Configure Reserved Email

Purpose:

The reserved email will help you to reset password when you forget your password.

Step 1 Check **Reserved E-mail** when you are activating the device, or click **Modify** when you are editing the admin user account.

Step 2 Enter reserved email address.

Step 3 Click **OK.**

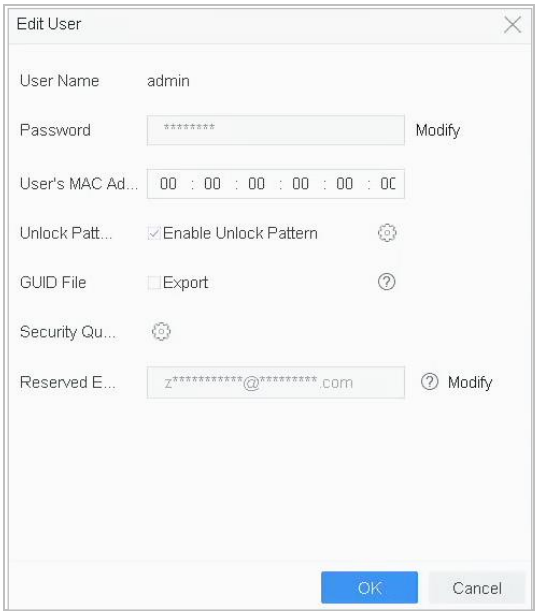


Figure 18-12 Configure Reserved Email

18.4 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 .

18.4.1 Reset Password by GUID

Before You Start

The GUID file must be exported and saved in the local U flash disk after you have activated the device or edited the admin user account. (Refer to Chapter 18.3.1 Export GUID File).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by GUID**.

NOTE

Please insert the U flash disk stored with the GUID file to the NVR before resetting password.

Step 3 Select the GUID file from the U flash disk and click **Import** to import the file to the device.

NOTE

If you have imported the wrong GUIE file for 7 times, you will be not allowed to reset the password for 30 minutes.

Step 4 After the GUID file is successfully imported, enter the reset password interface to set the new admin password.

Step 5 Click **OK** to set the new password. You can export the new GUID file to the U flash disk for future password resetting.

NOTE

When the new password is set, the original GUID file will be invalid. The new GUID file should be exported for future password resetting. You can also enter the User>User Management interface to edit the admin user and export the GUID file.

18.4.2 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. (Refer to Chapter 18.3.2 Configure Security Questions).

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by Security Question**.

Step 3 Input the correct answers of the three security questions.

Step 4 Click **OK**.

NOTE

If the answers mismatch, the verification is failed.

Step 5 Create the new admin password on the **Reset Password** interface.

18.4.3 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 18.3.3 Configure Reserved Email)

Step 1 On the user login interface, click **Forgot Password**.

Step 2 Select the password resetting type to **Verify by Reserved Email**.

Step 3 Click **OK**.

Step 4 Obtain the verification code. There are two ways to get the verification code.

- Use Guarding Vision 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@device-service.com* as attachment.

Step 5 Check your reserved email, and you will receive a verification code within 5 minutes.

Step 6 Enter the verification code.

Step 7 Click **OK** to set the new password.

Chapter 19 System Service Maintenance

19.1 Storage Device Maintenance

19.1.1 Configure Disk Clone

Purpose

Select the HDDs to clone to the eSATA HDD.

Before You Start

Connect an eSATA disk to the device.

Step 1 Go to **Maintenance > HDD Operation > HDD Clone**.

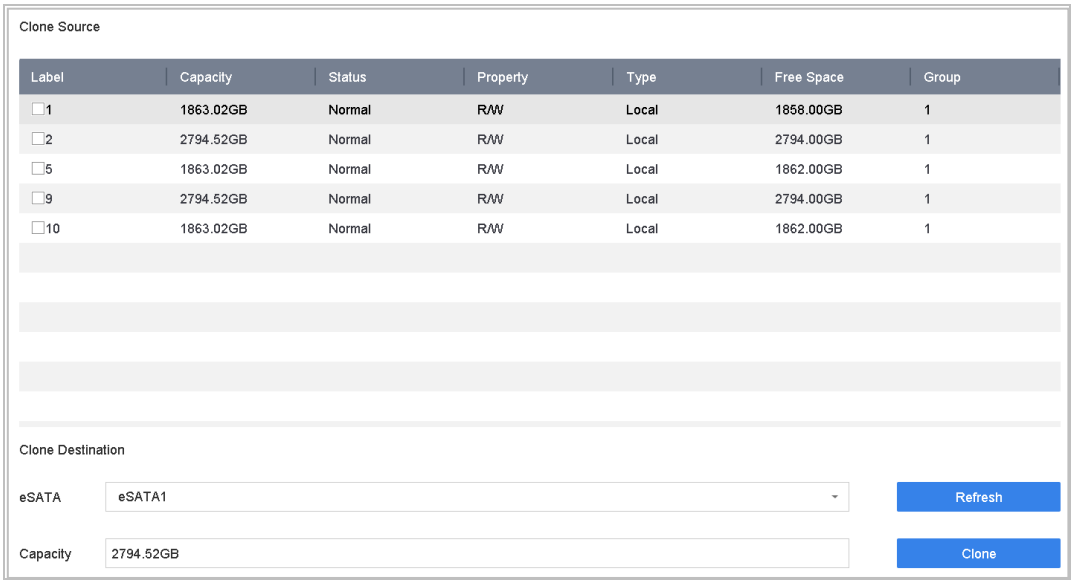


Figure 19-1 HDD Clone

Step 2 Check the HDD to clone. The capacity of the selected HDD must match the capacity of the clone destination.

Step 3 Click **Clone**.

Step 4 Click **Yes** on the popup message box to create the clone.

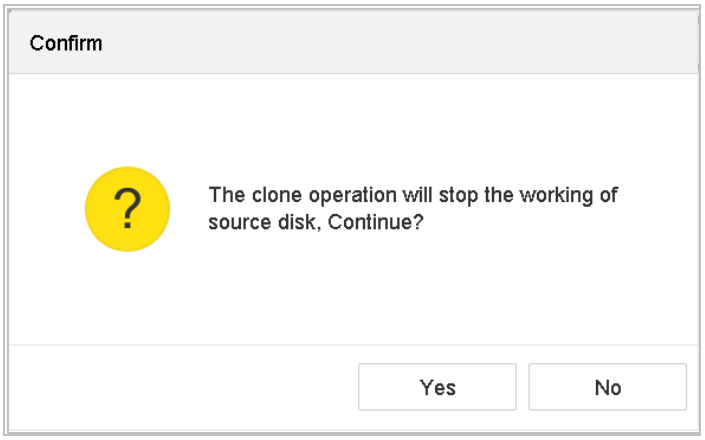


Figure 19-2 Message Box

19.1.2 S.M.A.R.T. Detection

Purpose

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.

Step 1 Go to **Maintenance** > **HDD Operation** > **S.M.A.R.T.**

Step 2 Select the HDD to view its S.M.A.R.T. information list.

Step 3 Select the self-test types as **Short Test**, **Expanded Test,** or the **Conveyance Test**.

Step 4 Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

Step 5 The related S.M.R.T. information of the S.M.A.R.T. is shown, and you can check the HDD status.

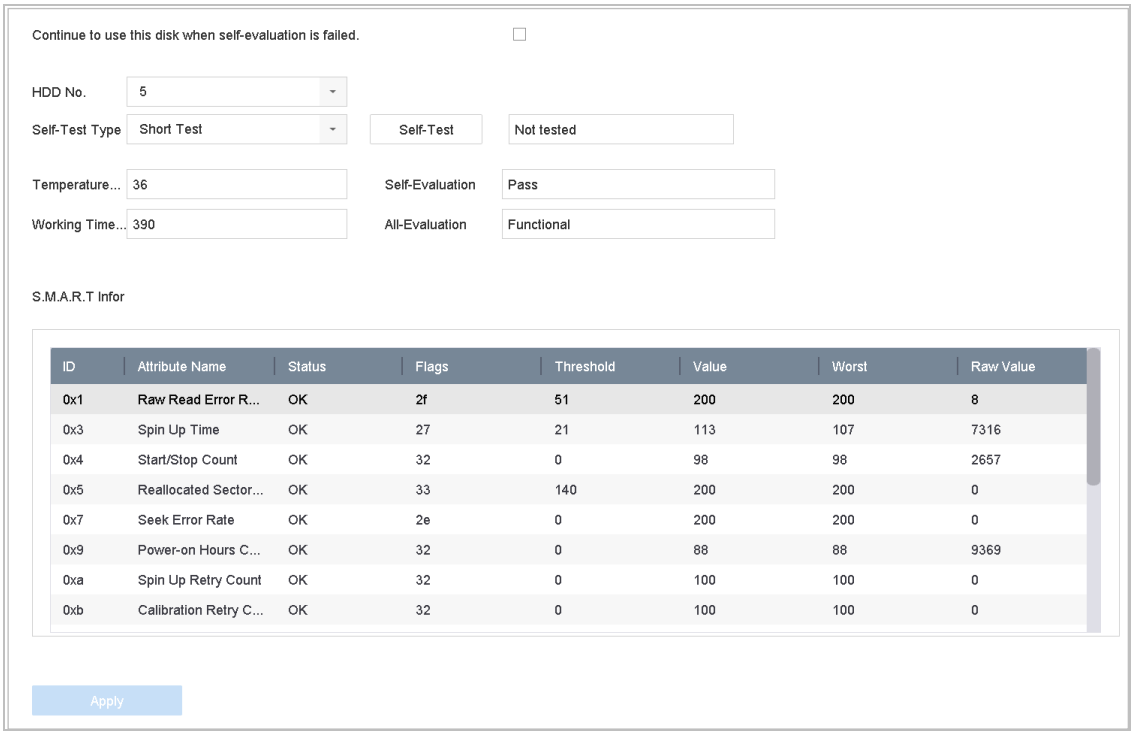


Figure 19-3 S.M.A.R.T. Settings Interface

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** checkbox.

19.1.3 Bad Sector Detection

Step 1 Go to **Maintenance** > **HDD Operation** > **Bad Sector Detection**.

Step 2 Select the HDD No. you want to configure in the dropdown list.

Step 3 Select **All Detection** or **Key Area Detection** as the detection type.

Step 4 Click the **Self-Test** button to start the detection.

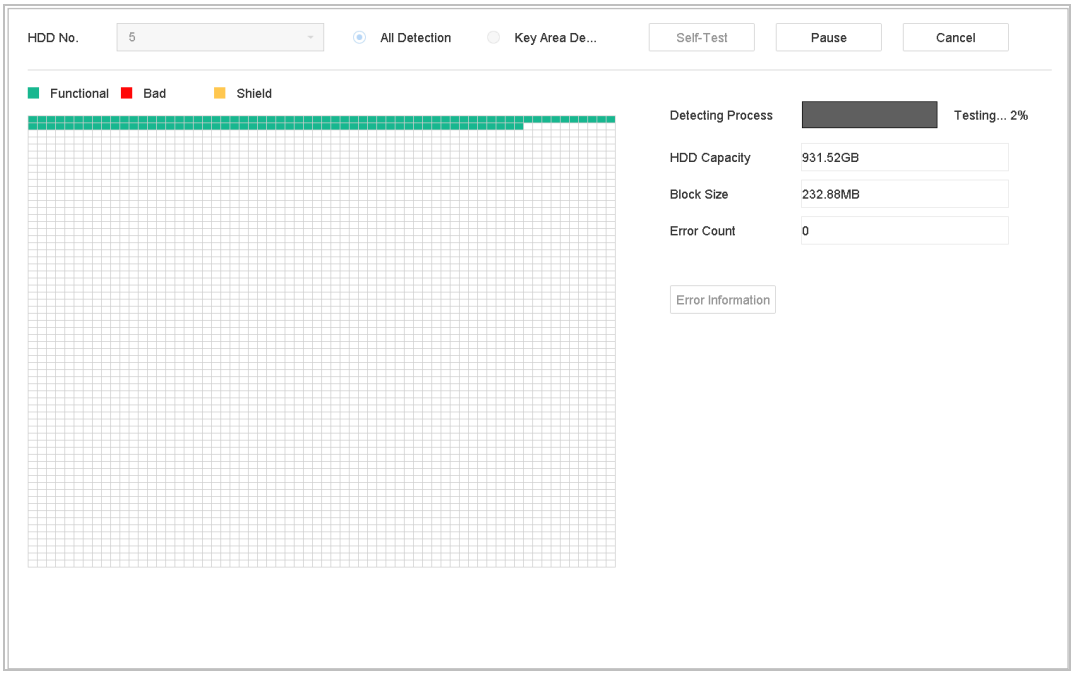


Figure 19-4 Bad Sector Detection

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

19.1.4 HDD Health Detection

Purpose

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.

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



Figure 19-5 Health Detection

Step 2 Click an HDD to view details.

19.1.5 Repair Database

Purpose

Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

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

Step 2 Select the drive.

Step 3 Click **Repair Database**.

Step 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 drive, or shut down the device during the process.
- You can see the repairing progress at **Status**.

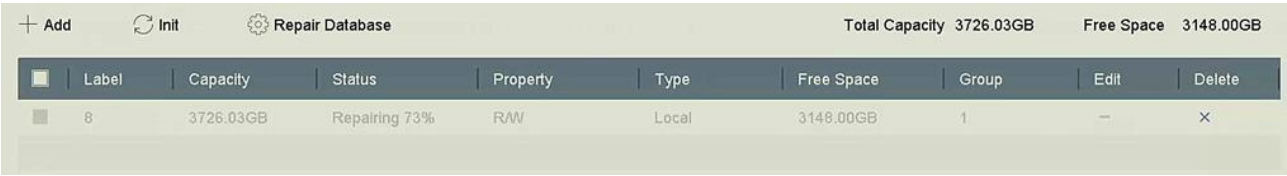


Figure 19-6 Repair Database

19.2 Search and Export Log Files

Purpose

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

19.2.1 Search the Log Files

Step 1 Go to **Maintenance** > **Log Information**.

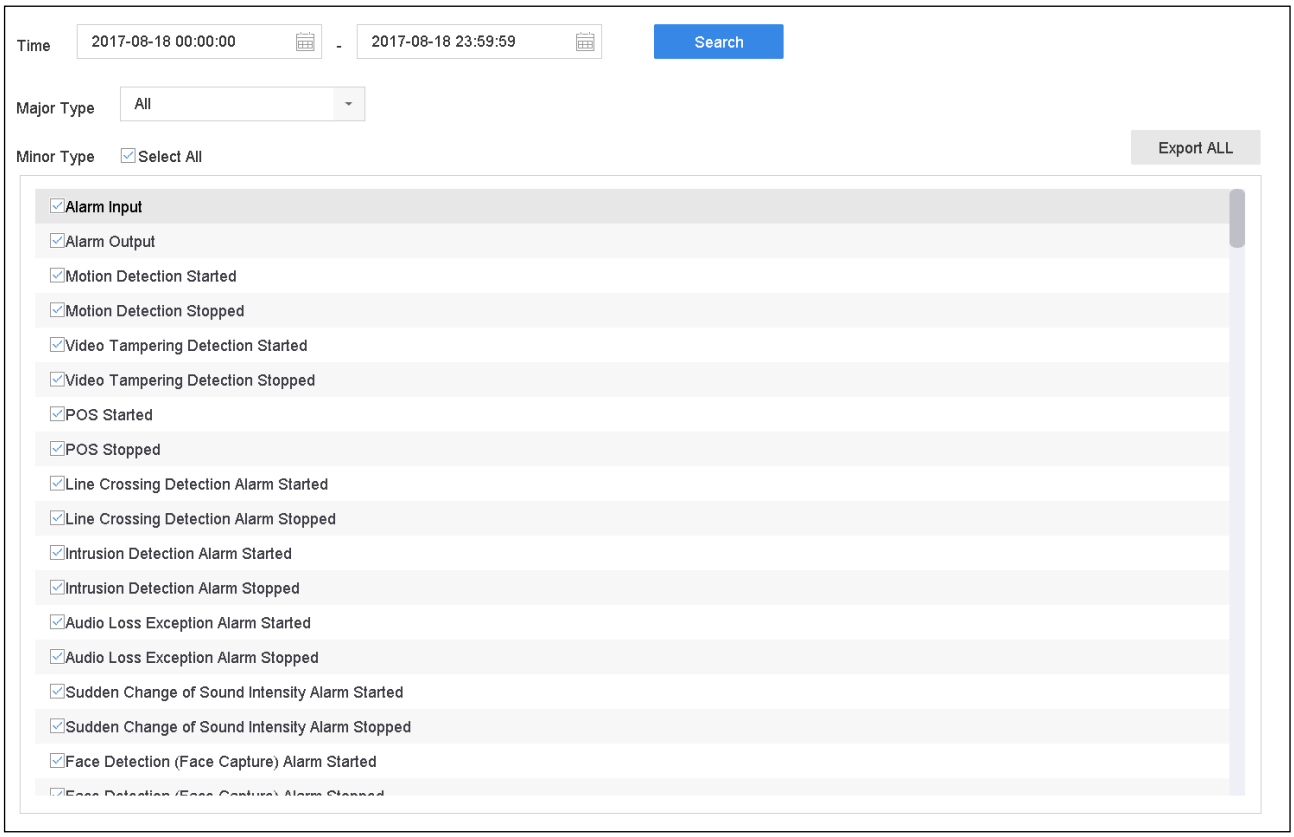


Figure 19-6 Log Search Interface

Step 2 Set the log search conditions, including the time, major type and minor type.

Step 3 Click **Search** to start searching the log files.

Step 4 The matched log files will be displayed on the list, as shown below.

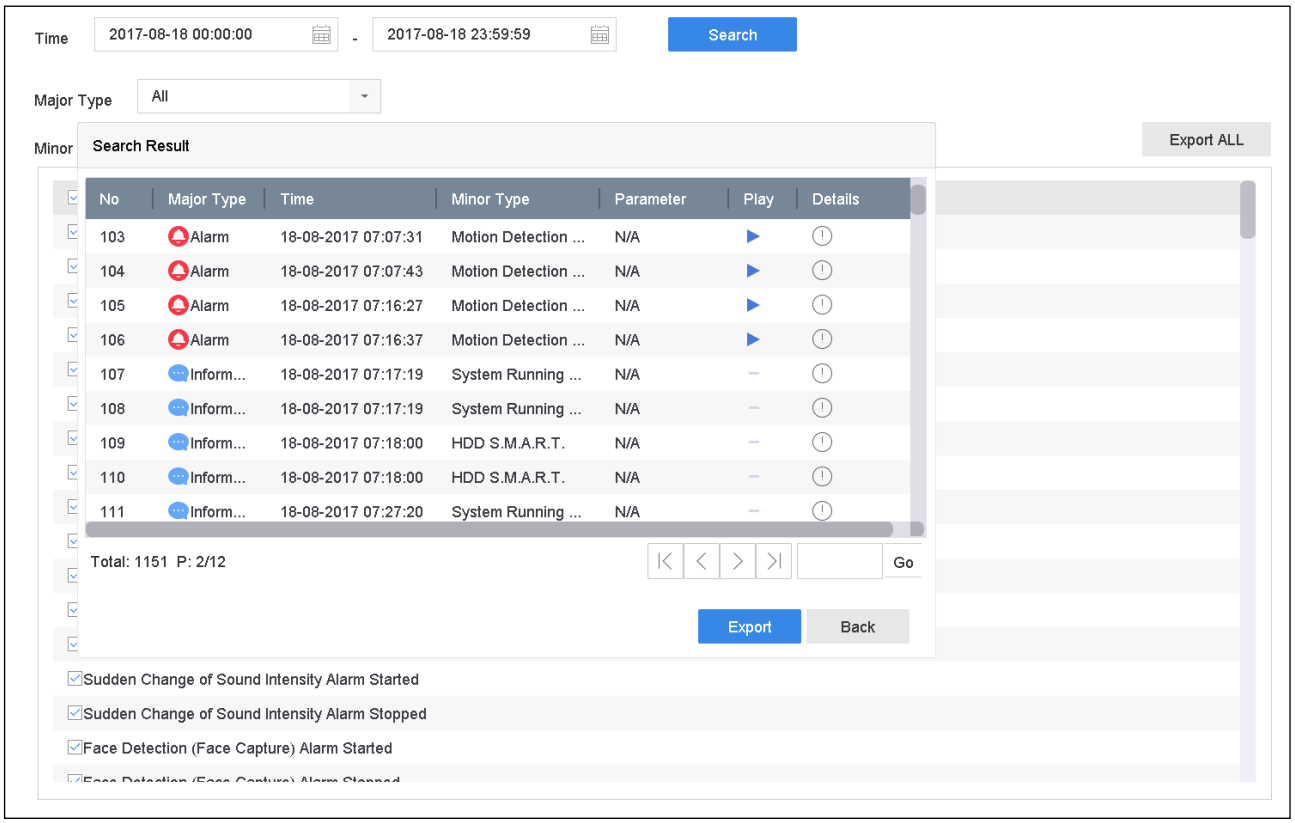


Figure 19-7 Log Search Results

NOTE

Up to 2,000 log files can be displayed each time.

Step 5 Related Operation:

- Click  or double-click it to view detailed information.
- Click  to view the related video file.

19.2.2 Export the Log Files

Before You Start

Connect a storage device to the NVR.

Step 1 Search the log files. Refer to Chapter 19.2.1 Search the Log Files.

Step 2 Select the log files you want to export, and click **Export** or click **Export ALL** on the Log Search interface to export all the system logs to the storage device.

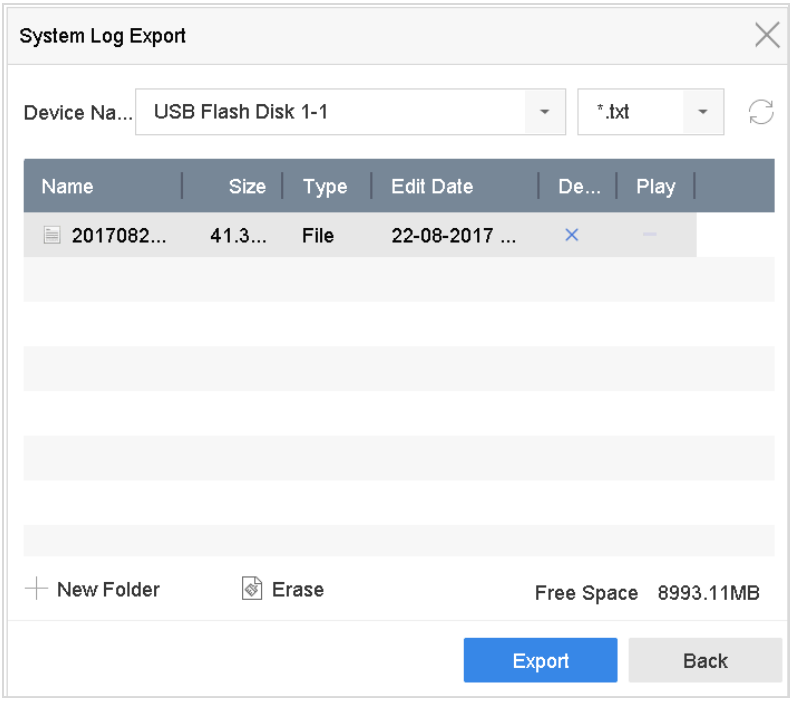


Figure 19-7 Export Log Files

Step 3 On the Export interface, select the storage device from **Device Name**.

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

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

- Click the **New Folder** button to create a new folder in the storage device.
- Click the **Format** button to format the storage device before exporting the log(s).

19.3 Import/Export IP Camera Configuration Files

Purpose

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 NVR.

Step 1 Go to **Camera** > **IP Camera Import/Export**.

Step 2 Click the **IP Camera Import/Export** tab, and the detected external device contents appear.

Step 3 Export or import the IP camera configuration files.

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

NOTE

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

19.4 Import/Export Device Configuration Files

Purpose

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

Before You Start

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

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

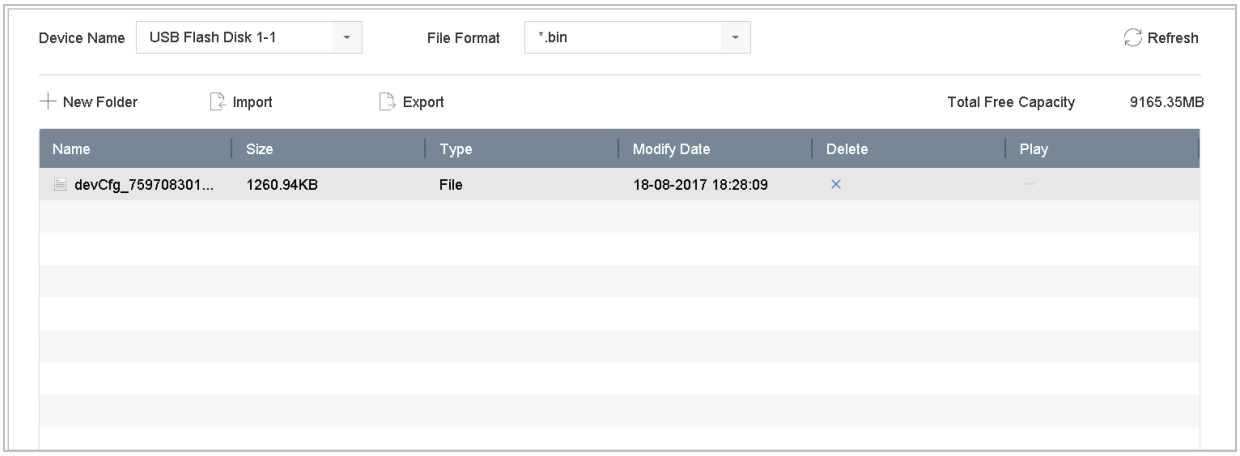


Figure 19-8 Import/Export Config File

Step 2 Export or import the device configuration files.

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

NOTE

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

19.5 Configure System Services

19.5.1 Network Security Settings

Set HTTP Authentication

Purpose

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

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



Figure 19-9 HTTP Authentication

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

Step 3 Select **HTTP Authentication**.

NOTE

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

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

Step 5 Restart the device to take effect the settings.

NOTE

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

Disable HTTP

Purpose

The admin user account can disable the HTTP service from the GUI or the web browser.

After the HTTP is disabled, all the related services, including the ISAPI, Onvif and Gennetc, will terminate as well.

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

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

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

Step 4 Restart the device to take effect the settings.

RTSP Authentication

Purpose

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

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

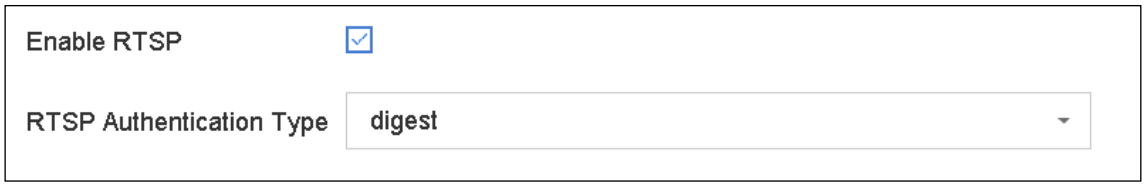


Figure 19-10 RTSP Authentication

Step 2 Select the 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.

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

Step 4 Restart the device to take effect the settings.

Enable ISAPI

Purpose

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.

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

Step 2 Check **Enable ISAPI**.

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

Step 4 Restart the device to take effect the settings.

Enable IP Camera Occupation Detection

Purpose

The function is able to detect the IP camera status. If the IP camera has been added by other device, it will show as  when you search available IP cameras in **Number of Unadded Online Device.**

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

Step 2 Check **Enable IP Camera Occupation Detection**.

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

Step 4 Restart the device to take effect the settings.

Enable SDK Service

Purpose

SDK service is used for developing applications of hardware platform, software framework, operating system, etc.

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

Step 2 Check **Enable SDK Service**.

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

Step 4 Restart the device to take effect the settings.

Enable Enhanced SDK Service

Purpose

The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

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

Step 2 Check **Enable SDK Service**.

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

Step 4 Restart the device to take effect the settings.

IP/MAC Address Filter

Purpose:

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

Step 1 Go to **Maintenance** > **System Service** > **Address Filter**.

Step 2 Check **Enable**.

Step 3 Select **Restriction Mode**. Choose to filter by IP address or MAC Address.

Step 4 Select **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.

Step 5 Set **Restriction List**. You can add, edit or delete address.

Step 6 Click **Apply** to save the settings.

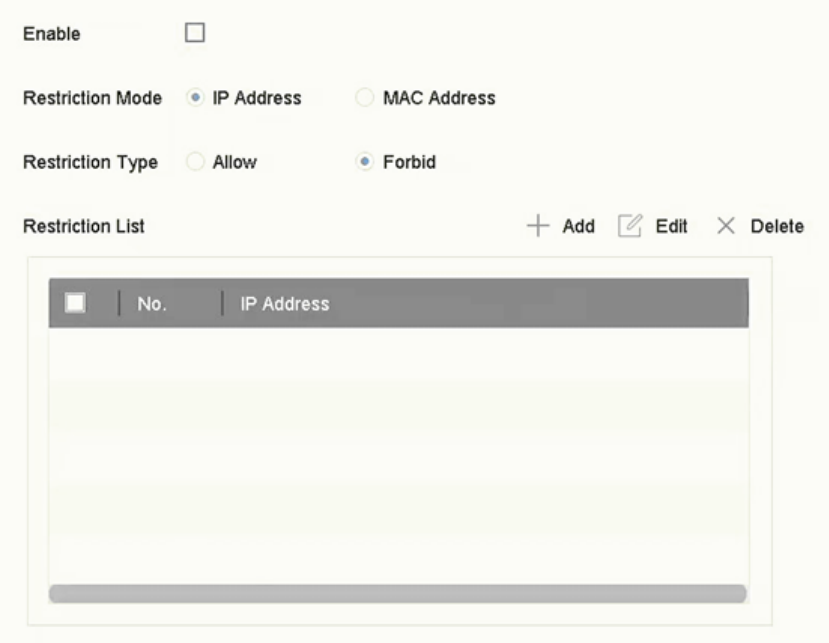


Figure 19-11 Address Filter

19.5.2 Manage ONVIF User Accounts

Purpose

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

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

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

NOTE

ONVIF protocol is disabled by default.

Step 3 Click **Add**.

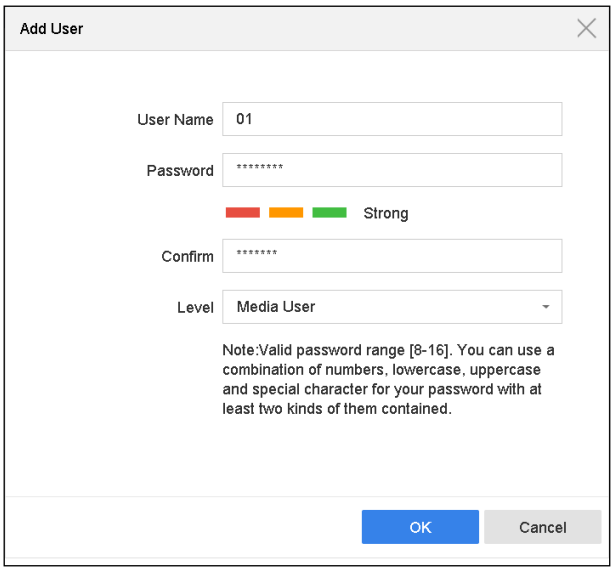


Figure 19-12 Add User

Step 4 Enter the user name, and 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.

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

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

19.5.3 Configure Stream Encryption

Purpose

The stream encryption enables to encrypt the streams for live view, playback, download, backup, etc.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **Stream Encryption**.

Step 2 Check **Enable Stream Encryption**.

Step 3 Create the encryption password.

NOTE

The stream encryption password is synchronized with the Guarding Vision service verification code. After enabling the encryption code, the Guarding Vision stream will be forcedly encrypted. Make sure the Guarding Vision service supports the stream encryption as well.

19.6 Configure Stream Encryption

The stream encryption enables to encrypt the streams for live view, playback, download, backup, etc.

Step 1 Go to **Menu** > **Maintenance** > **System Service** > **Stream Encryption**.

Step 2 Check **Enable Stream Encryption**.

Step 3 Create the encryption password.

NOTE

The stream encryption password is synchronized with the Guarding Vision service verification code. After enabling the encryption code, the Guarding Vision stream will be forcedly encrypted. Make sure the Guarding Vision service supports the stream encryption as well.

19.7 Upgrade the System

Purpose

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

19.7.1 Upgrade with a Local Backup Device

Before You Start

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

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

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

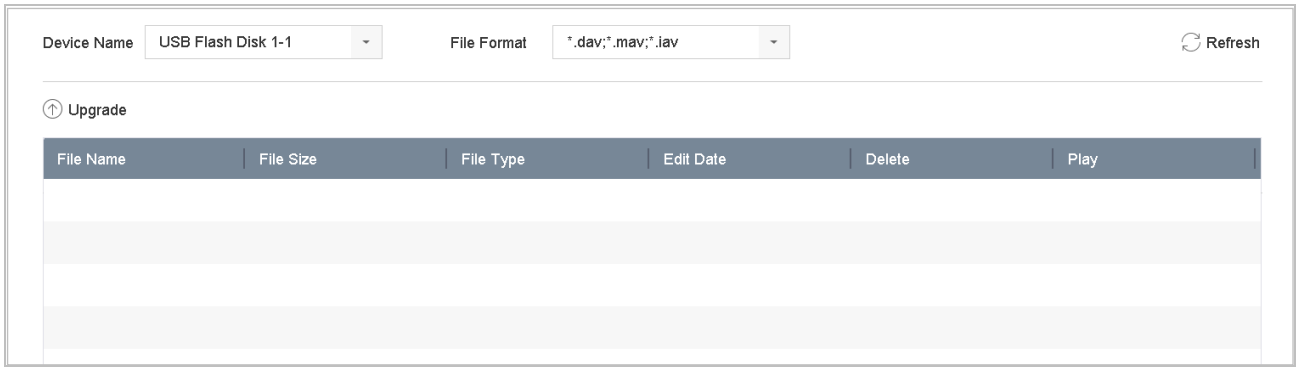


Figure 19-13 Local Upgrade Interface

Step 3 Select the firmware update file from the storage device.

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

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

19.7.2 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.

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

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

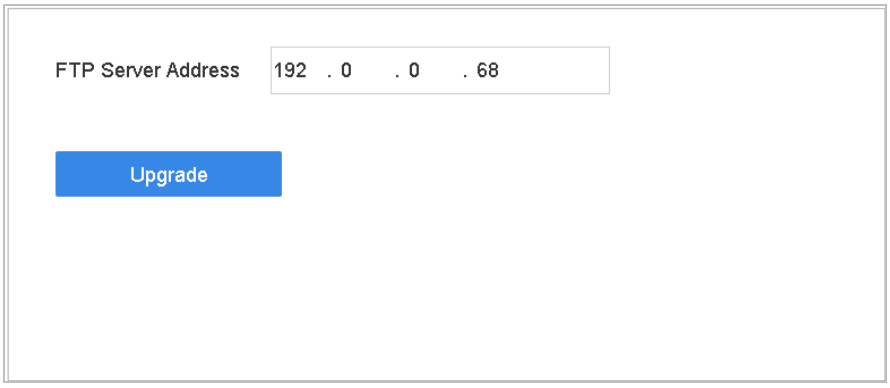


Figure 19-14 FTP Upgrade Interface

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

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

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

19.7.3 Upgrade by Guarding Vision

After logging the device into Guarding Vision, the device would periodically check for the latest firmware from Guarding Vision. 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 Guarding Vision, and it requires to install at least one read-write HDD for firmware downloading.

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

Step 2 Click **Check Upgrade** to manually check and download the latest firmware from Guarding Vision.

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.

Step 3 (Optional) You can switch on **Download Latest Package Automatically** to automatically download the latest firmware package.

Step 4 Click **Upgrade Now**.

19.8 Restore Default Settings

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

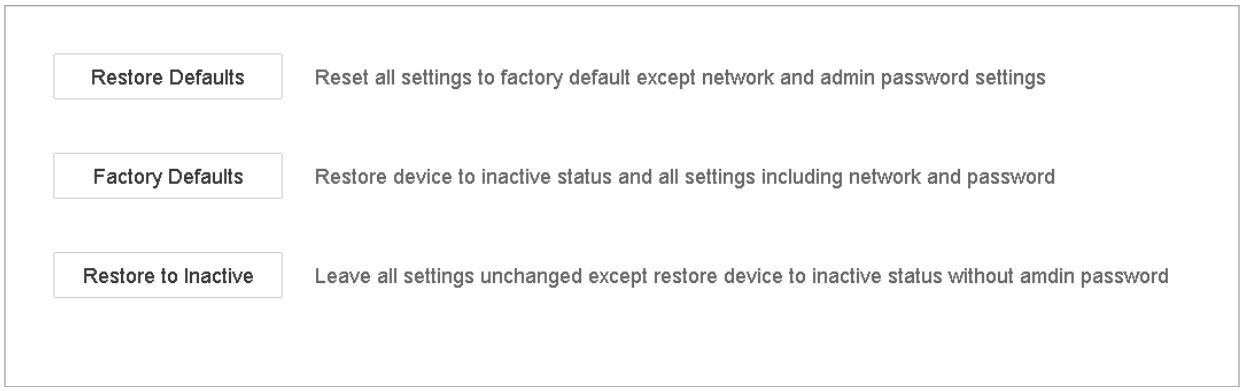


Figure 19-15 Restore Defaults

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

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

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

Restore to Inactive: Restore the device to inactive status.

NOTE

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

Chapter 20 General System Settings

20.1 Configure General Settings

Purpose:

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

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

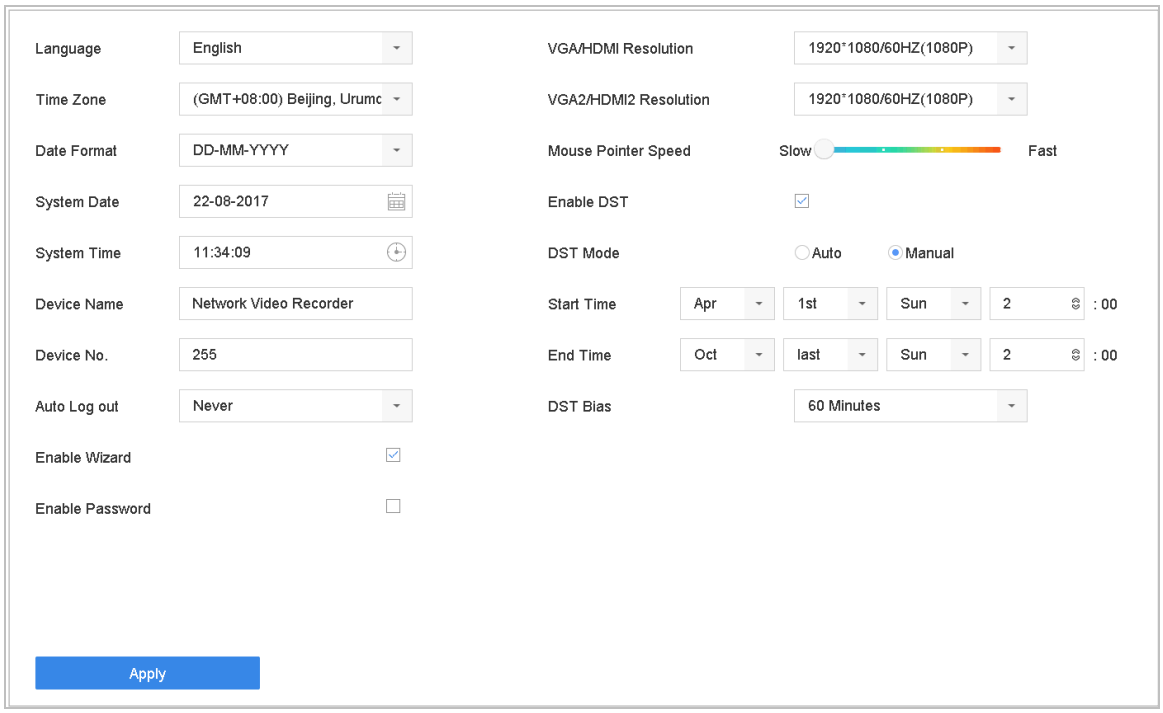


Figure 20-1 General Settings Interface

Step 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.

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

20.2 Configure Date & Time

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

Step 2 Configure the date and time.

Time Zone: Select the time zone.

Date Format: Select the date format.

System Date: Select the system date.

System Time: Set the system time.

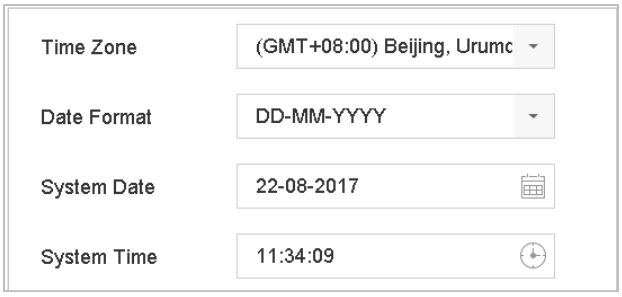


Figure 20-2 Date and Time Settings

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

20.3 Configure DST Settings

DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

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).

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

Step 2 Check **Enable DST**.

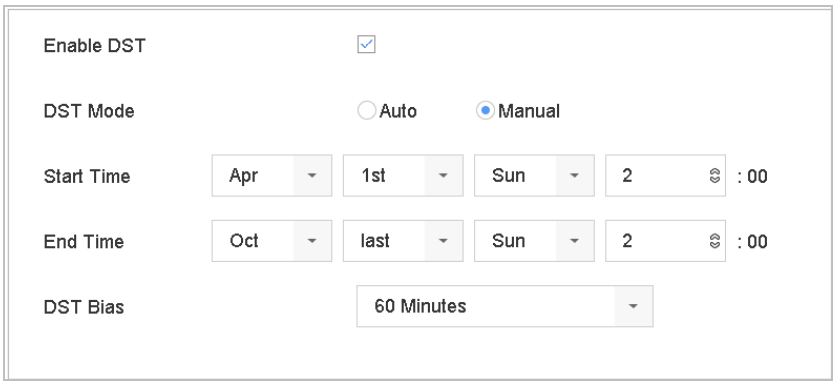


Figure 20-3 DST Settings Interface

Step 3 Set the DST mode to **Auto** or **Manual**.

- **Auto:** Automatically enable the default DST period according to the local DST rules.
- **Manual:** Manually set the start time and end time of the DST period, and the DST bias.

  DST Bias: Set the time (30/60/90/120 minutes) offset from the standard time.

  Example: DST begins at 2:00 a.m. on the second Sunday of March and ends at 2:00 a.m. on the first Sunday of November, with 60 minutes ahead.

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

Chapter 21 Appendix

21.1 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the device, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **PPPoE:** Stands for "Point-to-Point Protocol over Ethernet." PPPoE is a network configuration used for establishing a PPP connection over an Ethernet protocol.
- **Hybrid device:** A hybrid device is a combination of a DVR and device.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **Device:** Acronym for Network Video Recorder. A device can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other devices.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

21.2 Troubleshooting

- **No image displayed on the monitor after starting up normally.**

  Possible Reasons:

  − No VGA or HDMI connections.

  − Connection cable is damaged.

  − Input mode of the monitor is incorrect.

Step 1 Verify the device is connected with the monitor via HDMI or VGA cable.

Step 2 If not, please connect the device with the monitor and reboot.

Step 3 Verify the connection cable is good.

Step 4 If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.

Step 5 Verify Input mode of the monitor is correct.

Step 6 Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of device is HDMI output, then the input mode of monitor must be the HDMI input). And if not, please modify the input mode of monitor.

Step 7 Check if the fault is solved by the step 1 to step 3.

Step 8 If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **There is an audible warning sound "Di-Di-Di-DiDi" after a new bought device starts up.**

  Possible Reasons:

  − No HDD is installed in the device.

  − The installed HDD has not been initialized.

  − The installed HDD is not compatible with the device or is broken-down.

Step 1 Verify at least one HDD is installed in the device.

− If not, please install the compatible HDD.

NOTE

Please refer to the *Quick Start Guide* for the HDD installation steps.

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

Step 2 Verify the HDD is initialized.

1) Go to Menu>Storage>Storage Device.
2) If the status of the HDD is “Uninitialized”, please check the checkbox of corresponding HDD and click the “Init” button.

Step 3 Verify the HDD is detected or is in good condition.

3) Select Menu>Storage>Storage Device.
4) If the HDD is not detected or the status is “Abnormal”, please replace the dedicated HDD according to the requirement.

Step 4 Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The status of the added IP camera displays as “Disconnected” when it is connected through Private Protocol. Select “Menu>Camera>Camera>IP Camera” to get the camera status.**

Possible Reasons:

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

Step 1 Verify the network is connected.

1) Connect the device and PC with the RS-232 cable.
2) Open the Super Terminal software, and execute the ping command. Input “ping IP” (e.g. ping 172.6.22.131).

NOTE

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

If there exists return information and the time value is little, the network is normal.

Step 2 Verify the configuration parameters are correct.

1) Go to Menu>Camera.
2) Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.

Step 3 Verify the whether the bandwidth is enough.

1) Go to Menu>Maintenance>Net Detect>Network Stat..
2) Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.

Step 4 Check if the fault is solved by the step 1 to step 3.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The IP camera frequently goes online and offline and the status of it displays as "Disconnected".**

  Possible Reasons:

  − The IP camera and the device versions are not compatible.

  − Unstable power supply of IP camera.

  − Unstable network between IP camera and device.

  − Limited flow by the switch connected with IP camera and device.

Step 1 Verify the IP camera and the device versions are compatible.

1) Go to Menu>Camera, and view the firmware version of connected IP camera.
2) Go to Menu>Maintenance>System Info>Device Info and view the firmware version of device.

Step 2 Verify power supply of IP camera is stable.

1) Verify the power indicator is normal.
2) When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.

Step 3 Verify the network between IP camera and device is stable.

3) When the IP camera is offline, connect PC and device with the RS-232 cable.
4) Open the Super Terminal, use the ping command and keep sending large data packages to the connected IP camera, and check if there exists packet loss.

NOTE

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

Example: Input ping 172.6.22.131 –l 1472 –f.

Step 1 Verify the switch is not flow control.

Check the brand, model of the switch connecting IP camera and device, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.

Step 2 Check if the fault is solved by the step 1 to step 4.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **No monitor connected with the device locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via VGA or HDMI interface and reboot the device, there is black screen with the mouse cursor.**

Connect the device with the monitor before startup via VGA or HDMI interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect. And then connect the device with the CVBS, and there is black screen either.

Possible Reasons:

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

Step 1 Enable the output channel.

Step 2 Go to Menu>System>Live View>General, and select video output interface in the drop-down list and configure the window you want to view.

NOTE

- The view settings can only be configured by the local operation of device.
- Different camera orders and window-division modes can be set for different output interfaces separately, and digits like “D1”and “D2” stands for the channel number, and “X” means the selected window has no image output.

Step 3 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **Live view stuck when video output locally.**

Possible Reasons:

− Poor network between device and IP camera, and there exists packet loss during the transmission.

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

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

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

NOTE

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

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

Go to Menu>Camera>Encoding Parameters, and set the Frame rate to Full Frame.

Step 3 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **Live view stuck when video output remotely via the Internet Explorer or platform software.**

Possible Reasons:

− Poor network between device and IP camera, and there exists packet loss during the transmission.

− Poor network between device and PC, and there exists packet loss during the transmission.

− The performances of hardware are not good enough, including CPU, memory, etc..

Step 4 Verify the network between device and IP camera is connected.

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

NOTE

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

Step 5 Verify the network between device and PC is connected.

1) Open the cmd window in the Start menu, or you can press "windows+R" shortcut key to open it.
2) Use the ping command to send large packet to the device, execute the command of "ping 192.168.0.0 –l 1472 –f" (the IP address may change according to the real condition), and check if there exists packet loss.

NOTE

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

Step 6 Verify the hardware of the PC is good enough.

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

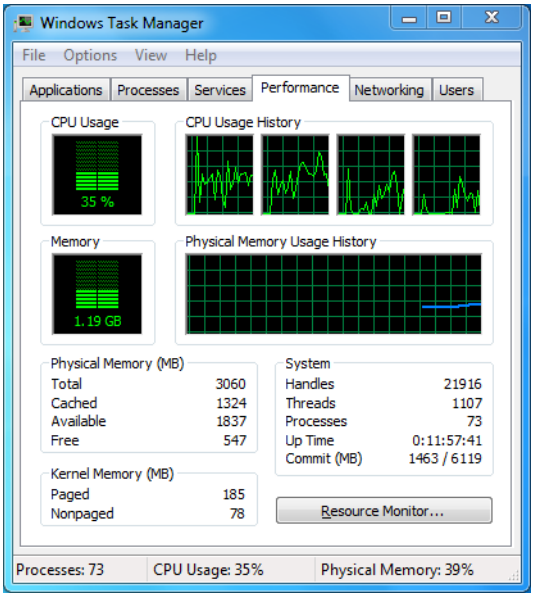


Figure 21-1 Windows task management interface

- Select the “Performance” tab; check the status of the CPU and Memory.
- If the resource is not enough, please end some unnecessary processes.

Step 7 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

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

Possible Reasons:

− Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.

− The stream type is not set as “Video & Audio”.

− The encoding standard is not supported with device.

Step 1 Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.

Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

Step 2 Verify the setting parameters are correct.

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

Step 3 Verify the audio encoding standard of the IP camera is supported by the device.

The device supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

Step 4 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **The image gets stuck when device is playing back by single or multi-channel.**

Possible Reasons:

− Poor network between device and IP camera, and there exists packet loss during the transmission.

− The frame rate is not the real-time frame rate.

− The device supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

Step 5 Verify the network between device and IP camera is connected.

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

NOTE

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

Step 6 Verify the frame rate is real-time frame rate.

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

Step 7 Verify the hardware can afford the playback.

Reduce the channel number of playback.

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

Step 8 Reduce the number of local playback channel.

Go to Menu>Playback, and uncheck the checkbox of unnecessary channels.

Step 9 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.

- **No record file found in the device local HDD, and prompt "No record file found".**

Possible Reasons:

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

Step 1 Verify the system time setting is correct.

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

Step 2 Verify the search condition is correct.

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

Step 3 Verify the HDD status is normal.

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

Step 4 Check if the fault is solved by the above steps.

If it is solved, finish the process.

If not, please contact the engineer from our company to do the further process.