Network Video Recorder v4.x

User Manual

About this Manual

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

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

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

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

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION 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.

Applicable Models

This manual applies to the models listed in the following table:

Series	Model
DS-9600NI-I8	DS-9608NI-I8
	DS-9616NI-I8
	DS-9632NI-I8
	DS-9664NI-I8
DS-9600NI-I16	DS-9616NI-I16
	DS-9632NI-I16
	DS-9664NI-I16
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P

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. 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 to 240 VAC or 12 VDC according to the IEC60950-1 Standard. Refer to technical specifications for detailed information.
- Do not connect several devices to one power adapter as adapter overload may cause overheating or a fire hazard.
- 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, unplug the power cable, and then contact the service center.

Preventive and Cautionary Tips

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

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with a UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.

Product Key Features

General

- Connectable to network cameras, network domes, and encoders
- Connectable to third-party network cameras, including ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, Panasonic, Pelco, Samsung, Sanyo, Sony, Vivotek, Zavio, and cameras that adopt the ONVIF or PSIA protocol
- Connectable to smart IP cameras
- H.265+/H.265/H.264+/H.264/MPEG4 video formats
- PAL/NTSC adaptive video inputs
- Each channel supports dual streams
- Up to 8/16/32/64 network cameras can be added according to model
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable

Local Monitoring

- HDMI/VGA1 and HDMI2/VGA2 outputs provided
- HDMI video output at up to 4K resolution
- Multiple screen display in Live View is supported, and the display sequence of channels is adjustable
- Live view screen can be switched in groups. Manual switch and auto-switch are provided and the auto-switch interval is configurable.
- 3D positioning supported by I Series devices in Live View
- Configurable main stream and sub-stream for Live View
- Quick setting menu is provided for Live View
- POS information overlay on Live View
- Motion detection, video tampering, video exception alert, and video loss alert functions
- Privacy mask
- Multiple PTZ protocols supported; PTZ preset, patrol, and pattern
- Zooming in by clicking the mouse and PTZ tracing by dragging the mouse

HDD Management

- Up to 16 SATA hard disks and 1 eSATA disk can be connected for DS-9600NI-M8 and DS-96128NI-I16/C, and up to 8 SATA hard disks and 1 eSATA disk can be connected for DS-9600NI-M8
- Up to 8 TB storage capacity for each disk supported
- Supports 8 network disks (NAS/IP SAN disk)
- Supports S.M.A.R.T. and bad sector detection
- HDD group management
- Supports HDD standby function
- HDD property: redundancy, read-only, read/write (R/W)
- HDD quota management; different capacities can be assigned to different channels
- RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10 are supported
- Hot-swappable RAID storage scheme, can be enabled and disabled upon demand. 16 arrays can be configured.
- Disk clone to the eSATA disk
- HDD health monitoring

Recording, Capture, and Playback

- Holiday recording schedule configuration
- Continuous and event video recording parameters
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm VCA, and POS
- Eight recording time periods with separated recording types
- POS information overlay on image by I Series devices
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording

- Searching record files and captured pictures by events (alarm input/motion detection)
- Tag adding for record files, searching and playing back by tags
- Locking and unlocking record files
- Local redundant recording and capture
- Normal/important/custom video playback mode
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Supports playback by main stream or sub stream.
- Smart search for the selected area in the video
- Zooming in when playback
- Reverse playback of multi-channels
- Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse
- Supports thumbnails view and fast view during playback
- Up to 16-ch synchronous playback at 1080p real time
- Supports playback by transcoded stream
- Manual capture, continuous capture of video images, and playback of captured pictures.
- Supports enabling H.264+ to ensure high video quality with lowered bitrate.

Files Management

- Search and export important files
- Search and export vehicle detection files and human appearance files
- Export video data by USB, SATA, or eSATA device
- Export video clips when playback
- Either Normal or Hot Spare working mode is configurable to constitute an N+1 hot spare system

Alarm and Exception

- Configurable arming time of alarm input/output
- Alarm for video loss, motion detection, tampering, abnormal signal, video input/output standard mismatch, illegal login, network disconnected, IP confliction, abnormal record/capture, HDD error, and HDD full, etc.
- POS triggered alarms supported by I Series devices
- VCA detection alarm is supported
- Smart analysis for people counting and heat map
- Connectable to the thermal network camera
- Supports advanced search for fire/ship/temperature/temperature difference detection triggered alarm and the recorded video files and pictures
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending e-mail, and alarm output.
- Automatic restore when system is abnormal

Other Local Functions

- Operable by front panel, mouse, remote control, or control keyboard
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel
- Admin password resetting by exporting/importing a GUID file
- Operation, alarm, exceptions, and log recording and searching
- Manually triggering and clearing alarms
- Import and export device configuration information

Network Functions

- Two self-adaptive 10M/100M/1000 Mbps network interfaces
- IPv6 is supported
- TCP/IP protocol, DHCP, DNS, DDNS, NTP, SADP, SMTP, NFS, and iSCSI are supported
- TCP, UDP, and RTP for unicast
- Auto/Manual port mapping by UPnP™
- Supports access by Hik-Connect
- Remote Web browser access by HTTPS ensures high security
- ANR (Automatic Network Replenishment) function is supported, which enables the IP camera to save the recording files in the local storage when the network is disconnected, then synchronizes the files to the device when the network is resumed
- Remote reverse playback via RTSP
- Supports accessing the platform via ONVIF
- Remote search, playback, download, locking and unlocking of the record files, and supports downloading files upon broken transfer resume
- Remote parameters setup; remote import/export of device parameters
- Remote viewing of the device status, system logs, and alarm status
- Remote keyboard operation
- Remote HDD formatting and program upgrading
- Remote system restart and shutdown
- RS-232, RS-485 transparent channel transmission
- Alarm and exception information can be sent to the remote host
- Remotely start/stop recording
- Remotely start/stop alarm output
- Remote PTZ control
- Remote JPEG capture
- Virtual host function to access and manage the IP camera directly
- Two-way audio and voice broadcasting
- Embedded Web server

Development Scalability

- SDK for Windows system
- Source code of application software for demo
- Development support and training for application system

TABLE OF CONTENTS

Chapter 1 Introduction

1.1 Front Panel

1.1.1 DS-9600NI Series

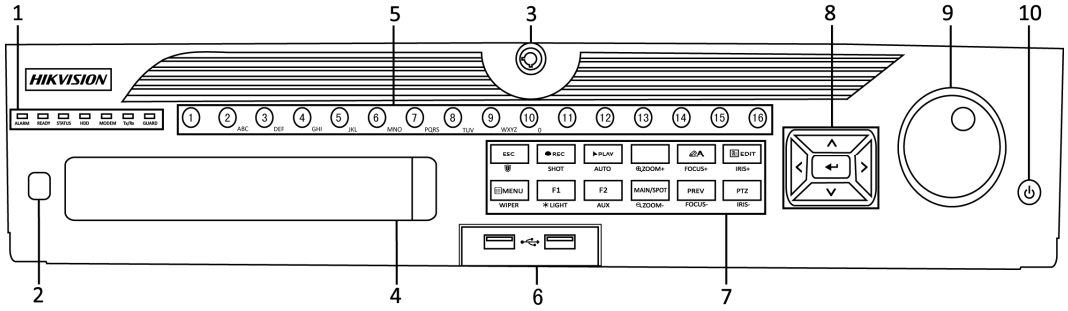


Figure 1-1 DS-9600NI-I8 Series

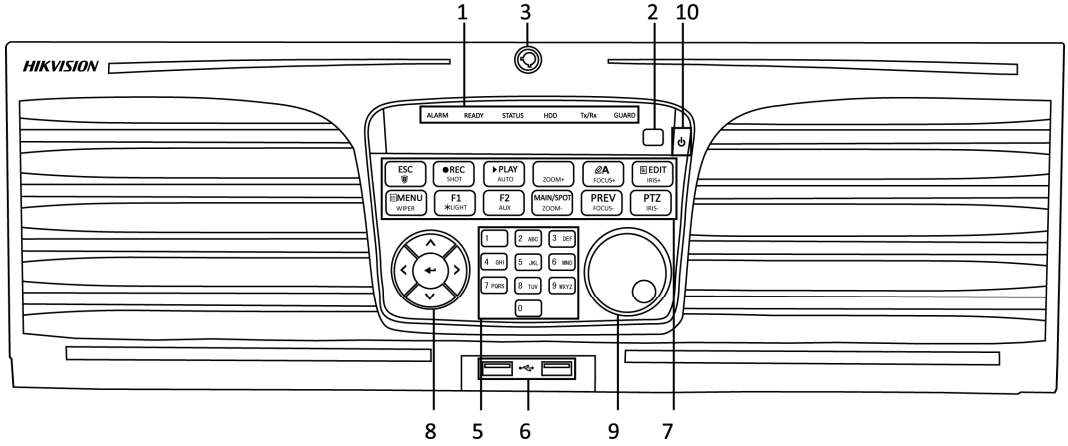


Figure 1-2 DS-9600NI-I16 Series

Table 1-1 Panel Description

No.	Name		Function Description
1	Status Indicators	ALARM	Red when a sensor alarm is detected
		READY	Blue when the device is functioning properly
		STATUS	Blue when device is controlled by an IR remote
			Red when controlled by a keyboard, purple when IR remote and keyboard used at same time
		HDD	Flickers red when data is being read from or written to HDD
		MODEM	Reserved for future usage
		Tx/Rx	Flickers blue when network connection is functioning properly
		GUARD	Blue when the device is in armed status; at this time, an alarm is enabled when an event is detected.
			Off when the device is unarmed. The arm/disarm status can be changed by pressing and holding the ESC button for more than 3 seconds in Live View mode.
2	IR Receiver		Receiver for IR remote control
3	Front Panel Lock		Locks or unlocks the panel by the key
4	DVD-R/W		Slot for DVD-R/W disk
5	Alphanumeric Buttons		Switches to the corresponding channel in Live View or PTZ control mode
			Inputs numbers and characters in edit mode
			Switches between channels in playback mode
			Blue when the corresponding channel is recording; red when the channel is in network transmission status; pink when the channel is recording and transmitting
6	USB Interfaces		Universal Serial Bus (USB) ports for devices such as USB mouse and USB Hard Disk Drive (HDD)
7	Composite Keys	ESC	Returns to the previous menu
			Press to arm/disarm the device in Live View mode
		REC/SHOT	Enters the Manual Record settings menu
			Press followed by a numeric button to call a PTZ preset in PTZ control settings
			Turns audio on/off in playback mode
		PLAY/AUTO	Enters playback mode
			Automatically scans in the PTZ control menu
		ZOOM+	Zooms in the PTZ camera in the PTZ control setting
		A/FOCUS+	Adjusts focus in the PTZ Control menu
			Switches input method (upper and lower case alphabet, symbols, numeric)
		EDIT/IRIS+	Edits text fields. When editing text fields, also deletes character in front of cursor.
			Checks the checkbox in checkbox fields.
			Adjusts the camera iris in PTZ control mode
			Generates video clips for backup in playback mode
			Enters/exits the USB device and eSATA HDD folder
		MAIN/SPOT/ ZOOM-	Switches between main and spot output
			Zooms out the image in PTZ control mode
		F1/LIGHT	Selects all items used in a list field
			Turns on/off PTZ light (if applicable) in PTZ control mode
			Switches between play and reverse play in playback mode
		F2/AUX	Cycles through tab pages
			Switches between channels in synchronous playback mode
		MENU/WIPER	Returns to the Main menu (after successful login)
			Press and hold button for five seconds to turn off audible key beep
			Starts wiper (if applicable) in PTZ control mode
			Shows/hides the control interface in playback mode
		PREV/FOCUS-	Switches between single screen and multi-screen mode
			Adjusts the focus in conjunction with the A/FOCUS+ button in PTZ control mode
		PTZ/IRIS-	Enters the PTZ Control mode
			Adjusts the PTZ camera iris in PTZ control mode
8	Control Buttons	DIRECTION	Navigates between menu fields and items
			In playback mode, use the Up and Down buttons to speed up and slow down recorded video. Use the Left and Right buttons to select the next and previous video files.
			Cycles through channels in Live View mode
			Controls PTZ camera movement in PTZ control mode
		ENTER	Confirms selection in any menu mode
			Checks the checkbox fields
			Plays or pauses the video playing in playback mode
			Advances the video by a single frame in single-frame playback mode
			Stops/starts auto switch in auto-switch mode
9	JOG SHUTTLE Control		Moves the active selection up and down in a menu
			Cycles through channels in Live View mode
			Jumps 30s forward/backward in video files in playback mode
			Controls PTZ camera movement in PTZ control mode
10	POWER ON/OFF		Long press for more than 3 seconds to turn on/off the device

1.1.2 DS-7700NI Series

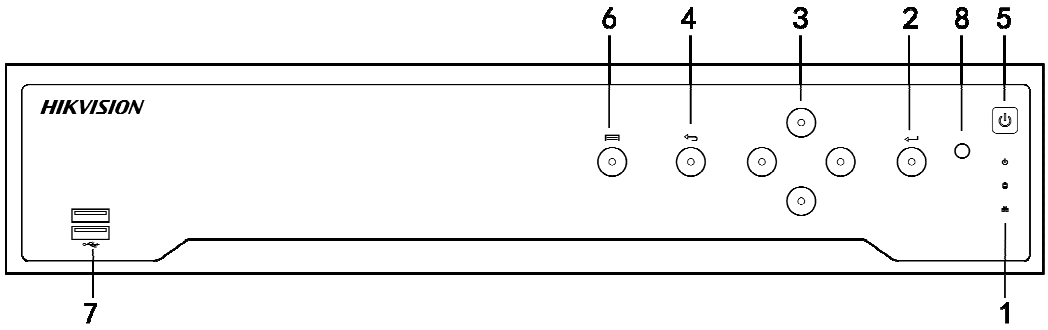


Figure 1-3 DS-7700NI Series

Table 1-2 Panel Description

No.	Name		Function Description
1	Status Indicators	POWER	Green when device is powered up
		HDD	Blinks red when HDD is reading/writing
		Tx/Rx	Blinks green when network connection is functioning normally
2	ENTER		Confirms selection in menu mode; or used to check checkbox fields and ON/OFF switch
			Play/pause video in playback mode
			Play video by a single frame in single-frame play mode
			Pause/resume auto sequence in auto sequence view mode
3	DIRECTION		Navigate between fields and items and select setting parameters in menu mode
			Up/Down buttons speed up and slow down record playing, and Left/Right buttons move the recording 30s forwards or backwards, in playback mode
			Up/Down buttons adjust the image parameters level bar in the image setting interface. Buttons switch channels in Live View mode.
4	Back		Back to previous menu
5	POWER ON/OFF		Power on/off switch
6	MENU		Access the main menu interface
7	USB Interface		Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD)

1.1.3 DS-7600NI Series

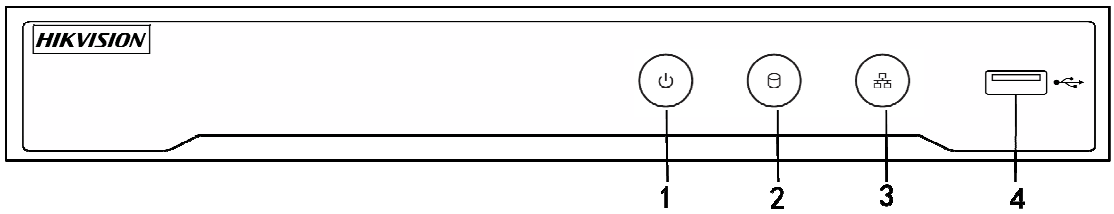


Figure 1-4 DS-7600NI Series

Table 1-3 Panel Description

No.	Name	Connections
1	POWER	Green when device is powered up
2	HDD	Flickers red when data is being read from or written to HDD
3	Tx/Rx	Flickers blue when network connection is functioning properly
4	USB Interface	Universal Serial Bus (USB) port for additional devices such as USB mouse and USB Hard Disk Drive (HDD)

1.2 IR Remote Control Operations

The device may be controlled with the included IR remote control, shown in Figure 1-5.

NOTE

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

The IR remote control is set at the factory to control the device (using default Device ID# 255) without any additional steps. Device ID# 255 is the default universal device identification number shared by the devices. You may also pair an IR remote control to a specific device by changing the Device ID#, as follows:

Pairing (Enabling) the IR Remote Control to a Specific Device (optional)

You can pair an IR remote control to a specific device by creating a user-defined Device ID#. This feature is useful when using multiple IR remote controls and devices.

On the NVR:

Step 1 Go to System > General.

Step 2 Type a number (255 digits maximum) into the Device No. field.

On the IR Remote Control:

Step 1 Press the **DEV** button.

Step 2 Use the number buttons to enter the Device ID# that was entered into the device.

Step 3 Press the **Enter** button to accept the new Device ID#.

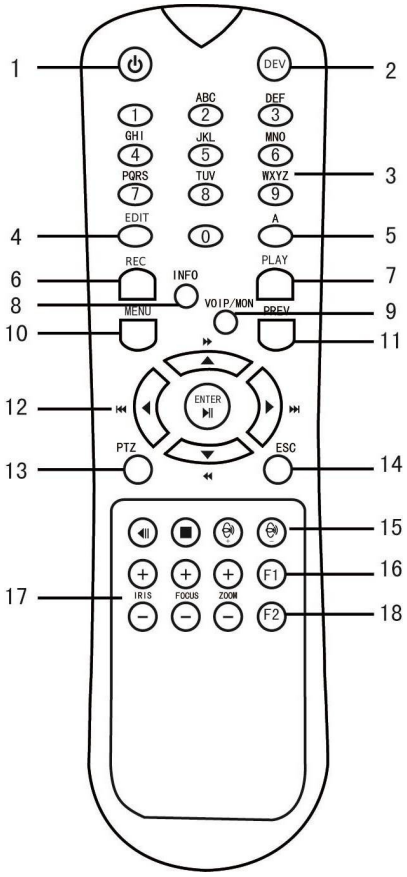


Figure 1-5 Remote Controller

Unpairing (Disabling) an IR Remote Control from a Device

To unpair an IR remote control from a device so that the unit cannot control any device functions, proceed as follows:

Press the DEV key on the IR remote control. Any existing Device ID# will be erased from the unit's memory and it will no longer function with the device.

NOTE

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

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

Table 1-4 IR Remote Functions

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

Troubleshooting the Remote Control

Make sure you have installed batteries properly in the remote control. Also, 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 **System** > **General** by operating the front control panel or the mouse.

Step 2 Check and remember device ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.

Step 3 Press the **DEV** button on the remote control.

Step 4 Enter the device ID# you set 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, check the following:

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

If the remote still doesn't function properly, change to a different 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 the 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, refer to the recommended device list from your provider.

The operation of the mouse:

Table 1-5 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

1.4.1 DS-9600NI Series

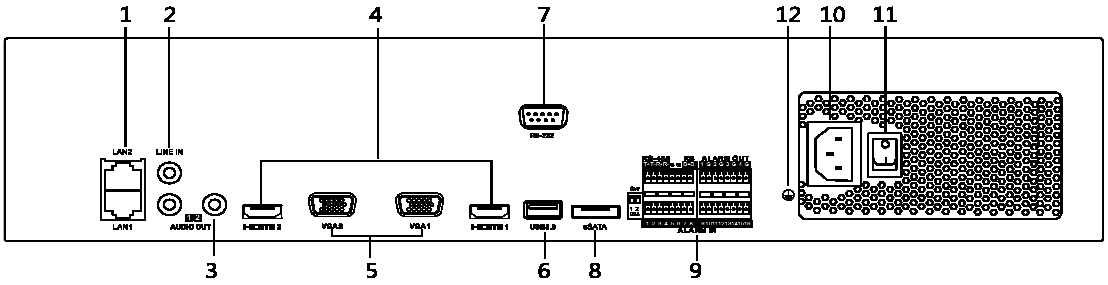


Figure 1-6 DS-9600NI-I8 Series

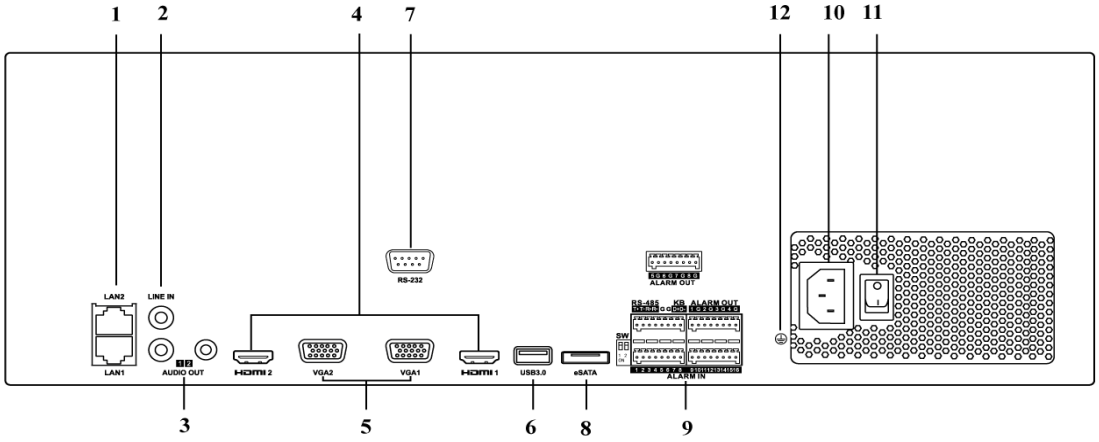


Figure 1-7 DS-9600NI-I16 Series

Table 1-6 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	DB-9 connector for VGA output. Display local video output and menu.
6	USB 3.0 interface	Universal Serial Bus ports for devices such as USB mouse, 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- pins connect to Ta, Tb pins of controller. For cascading devices, the first device's D+, D- pin should be connected to 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)

1.4.2 DS-7600NI Series

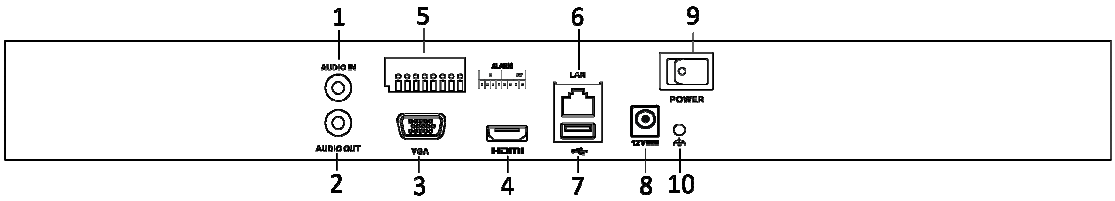


Figure 1-8 DS-7600NI-I2 Series

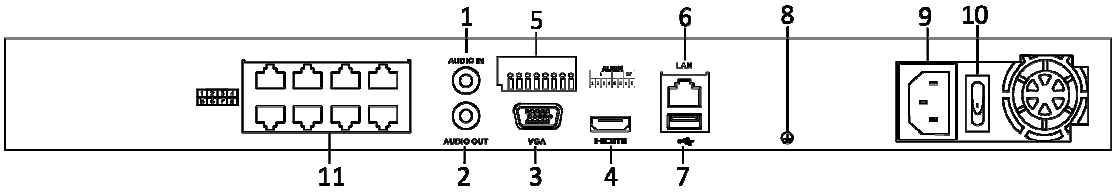


Figure 1-9 DS-7600NI-I2/8P Series

NOTE

DS-7616NI-I2/16P provides 16 network Interfaces with PoE.

Table 1-7 Panel Description

No.	Name	Description
1	Audio In	RCA connector for audio input
2	Audio Out	RCA connector for audio output
3	VGA Interface	DB-9 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	Ground	Ground (needs to be connected when device starts)
9	Power Supply	12 VDC power supply for DS-7600NI-I4, and 100 to 240 VAC for DS-7600NI-I4/P
10	Power Switch	Switch for turning on/off the device
11	Network Interfaces with PoE function (supported by DS-7600NI-I2/P)	Network interfaces for the cameras and to provide power over Ethernet

1.4.3 DS-7700NI Series

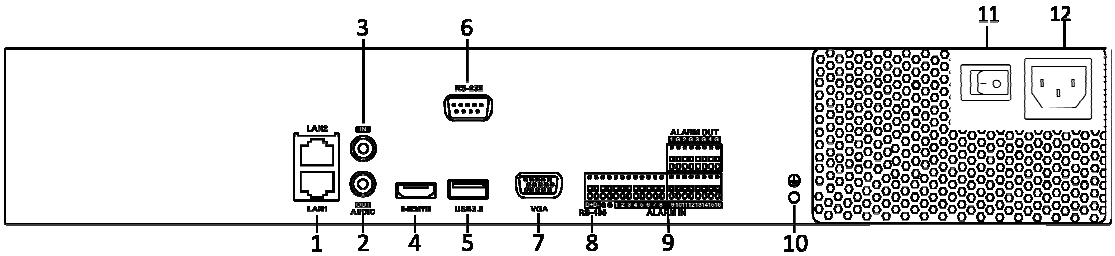


Figure 1-10 DS-7700NI-I4 Series

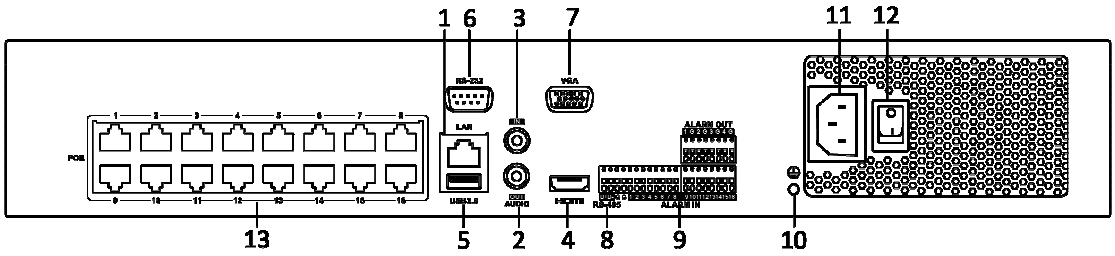


Figure 1-11 DS-7700NI-I4/16P Series

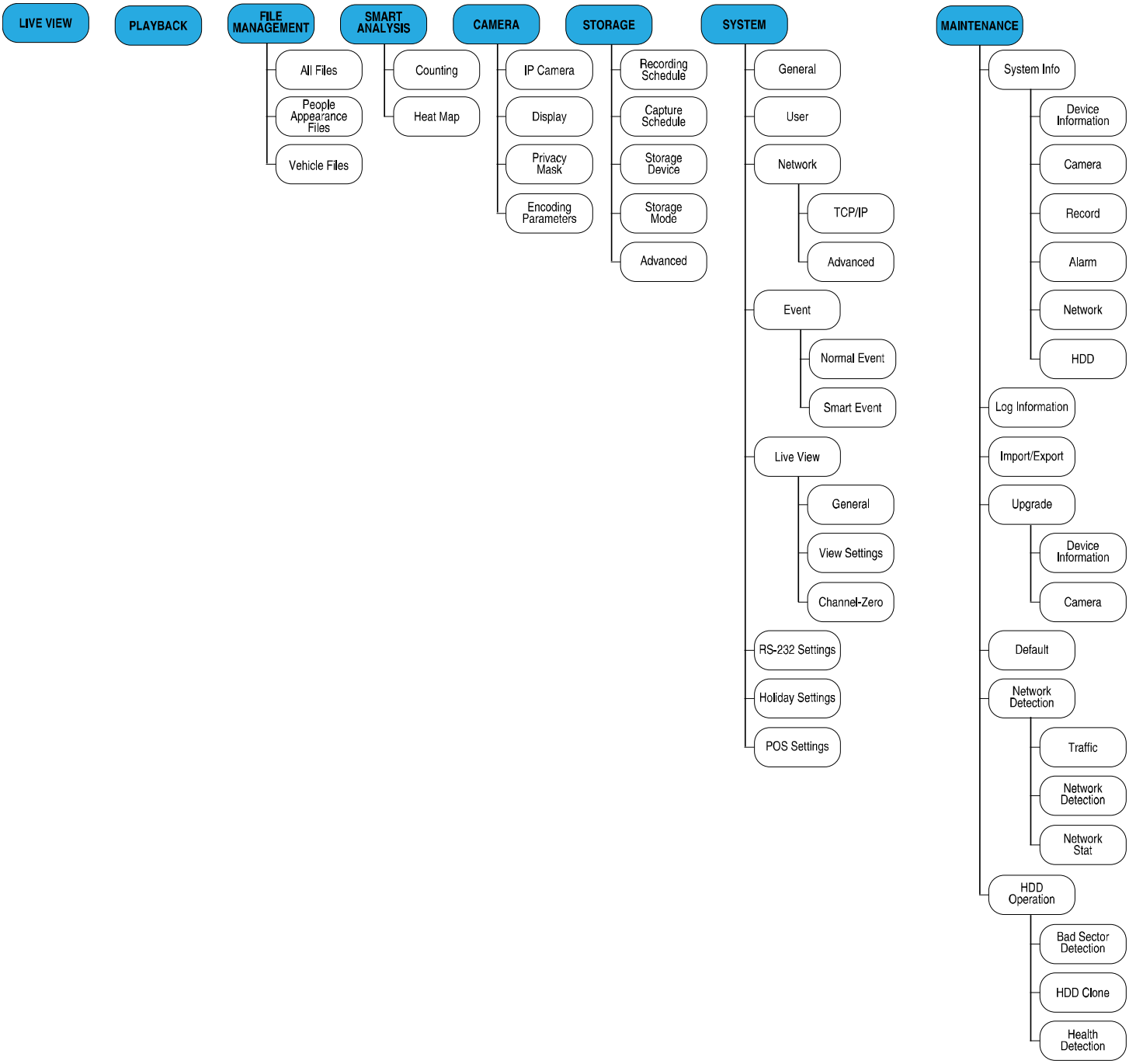
NOTE

DS-7708NI-I4/8P provides eight network Interfaces with PoE.

Table 1-8 Panel Description

No.	Name	Description
1	LAN Interface	1 network interface provided for DS-7700NI-I4/P, and 2 network interfaces for DS-7700NI-I4
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	DB-9 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)
11	AC 100V to 240V	100 to 240 VAC power supply
12	Power Switch	Switch for turning on/off the device
13	Network Interfaces with PoE function (supported by DS-7700NI-I4/P)	Network interfaces for the cameras and to provide power over Ethernet

Chapter 2 Menu Tree



Chapter 3 Getting Started

3.1 Starting 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 matches the device's requirement and the ground connection is working properly.

Powering Up the Device

Step 1 Check that 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 is receiving power.

Step 2 Press **POWER** on the front panel. The Power indicator LED should turn blue indicating that the unit is starting.

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.

3.2 Activating 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 Input the same password in the **Create New Password** and **Confirm New Password** text fields.

NOTE

Click to show the characters input.

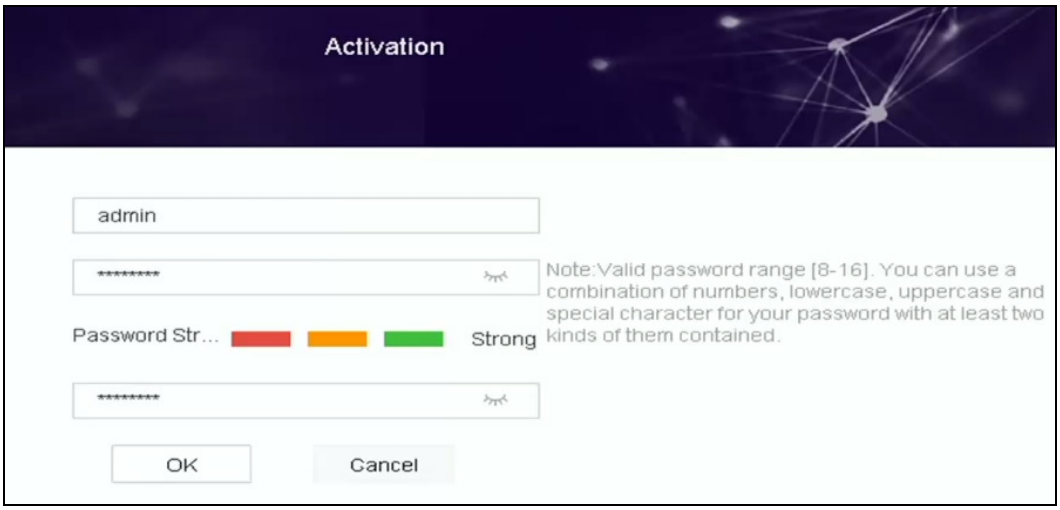


Figure 3-1 Setting Admin Password

WARNING

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

Step 2 Click **OK** to save the password and activate the device.

Step 3 When the device is activated, the system pops up a message box to remind you to properly keep the password. Click **OK** to export the GUID file for future password resetting.

Figure 3-2 Properly Keep Your Password Reminder

NOTE

If Admin's password is modified, a dialog box pops up. Optionally, click **Yes** to duplicate the password to connected IP cameras.

3.3 Configuring the 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 nine dots on the screen. Release the mouse when the pattern is done.

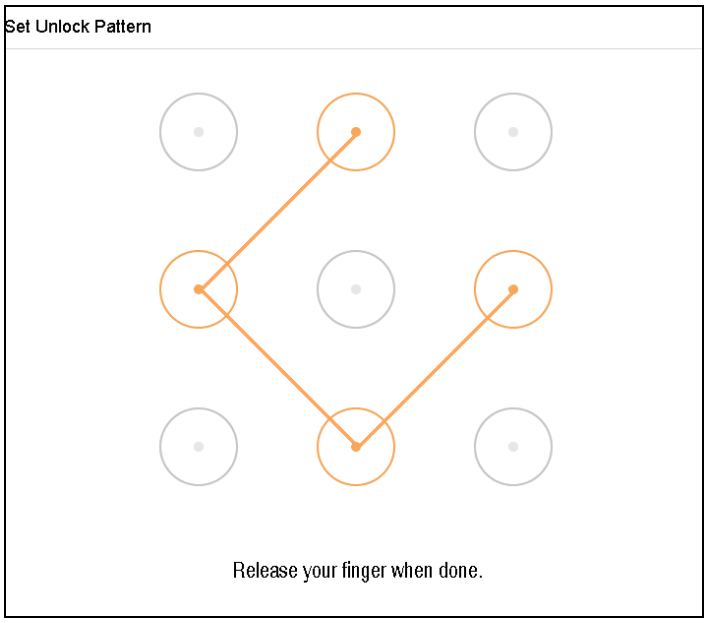


Figure 3-3 Draw the Pattern

NOTE

Connect at least four dots to draw the pattern.

Each dot can be connected only once.

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.

3.4 Log In to the Device

3.4.1 Log In via the Unlock Pattern

NOTE

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

Configure the pattern before unlocking. Refer to Chapter 3.3 Configuring the Login Unlock Pattern.

Step 1 Right-click the mouse and select the menu to enter the interface.

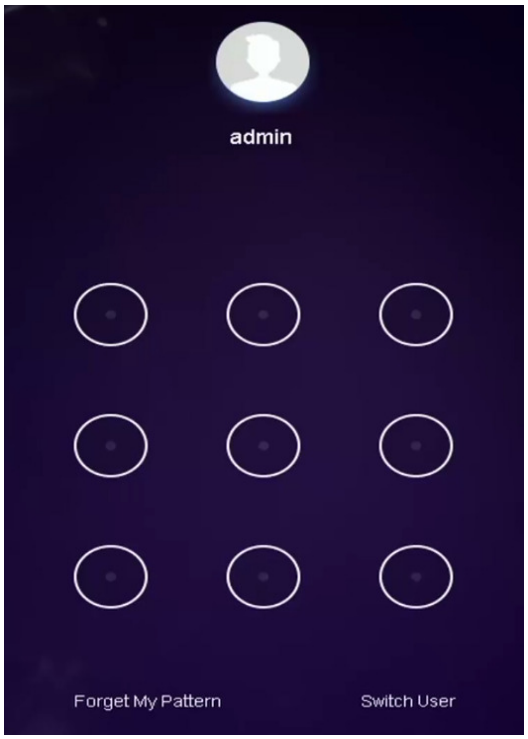


Figure 3-4 Draw the Unlock Pattern

Step 2 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.

3.4.2 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.

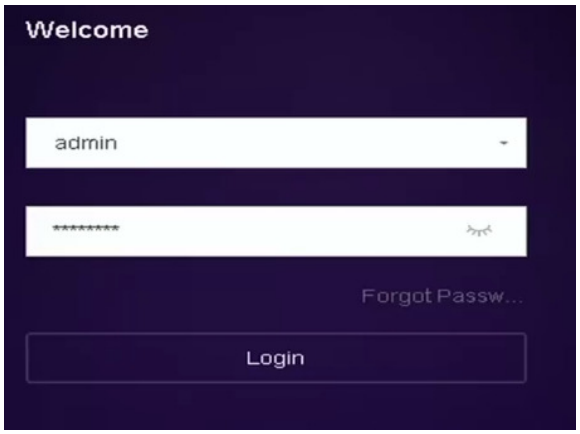


Figure 3-5 Login Interface

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 seven times, the current user account will be locked for 60 seconds.

3.5 Starting the Setup Wizard

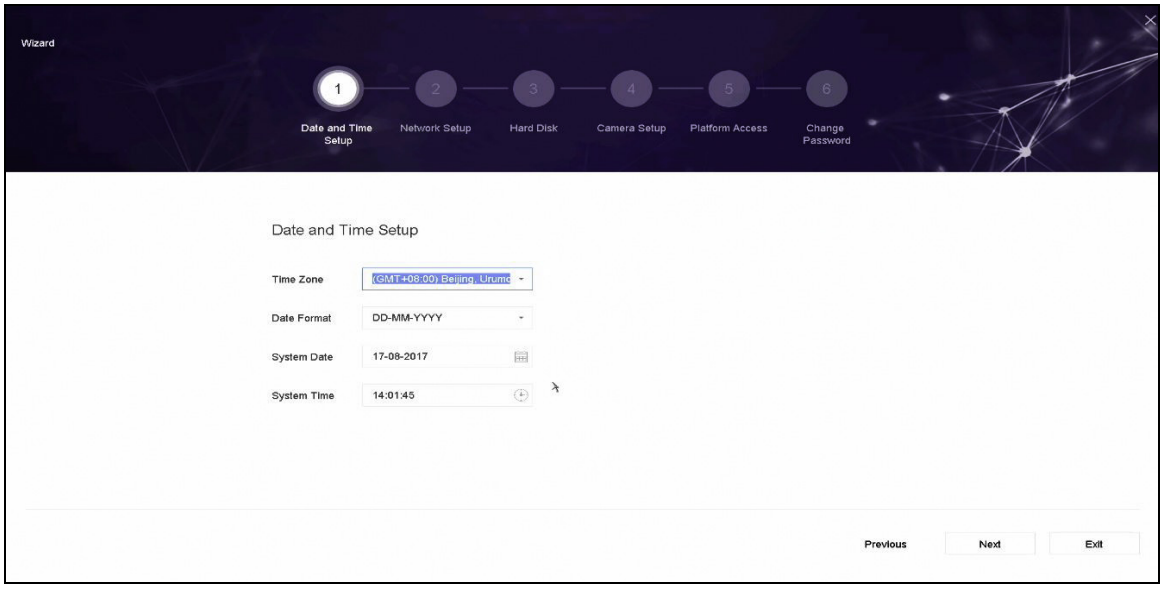


Figure 3-6 Setup Wizard

By default, the Setup Wizard starts once the device has loaded.

The Setup Wizard walks you through some important basic device settings. If you don't want to use the Setup Wizard at that moment, click **Exit**.

Step 2 Configure the date and time on the Date and Time Setup interface.

Figure 3-7 Date and Time Settings

Step 3 After the time settings, click **Next** to enter the Network Setup Wizard window, as shown in the following figure.

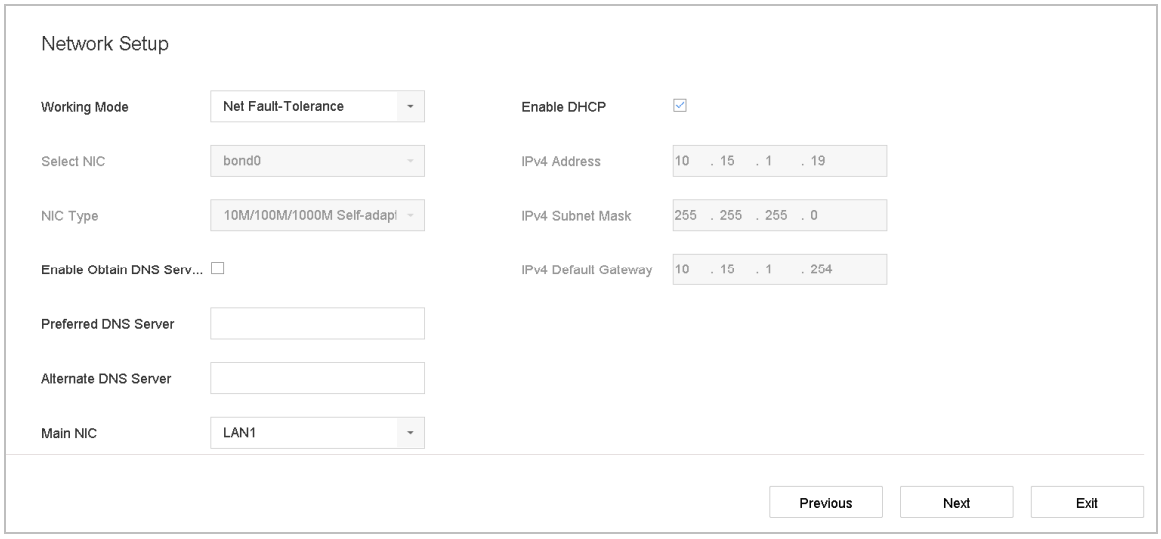


Figure 3-8 Network Settings

Step 4 Click **Next** after configuring the network parameters, which takes you to the **HDD Management** window.

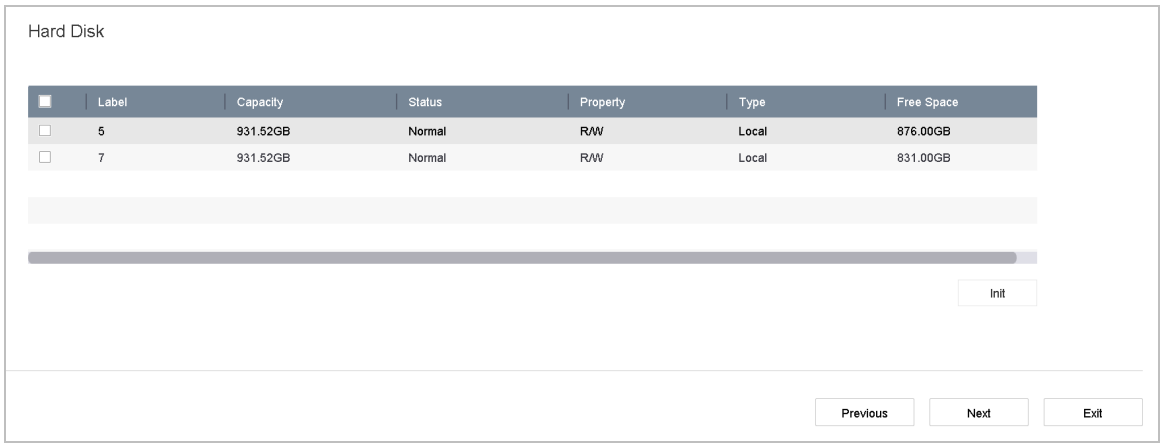


Figure 3-9 HDD Management

Step 5 To initialize the HDD, click **Init**. Initialization deletes all data saved in the HDD.

Step 6 Click **Next** to enter the **Camera Setup** interface to add IP cameras.

1) Click **Search** to search online IP cameras. 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**.

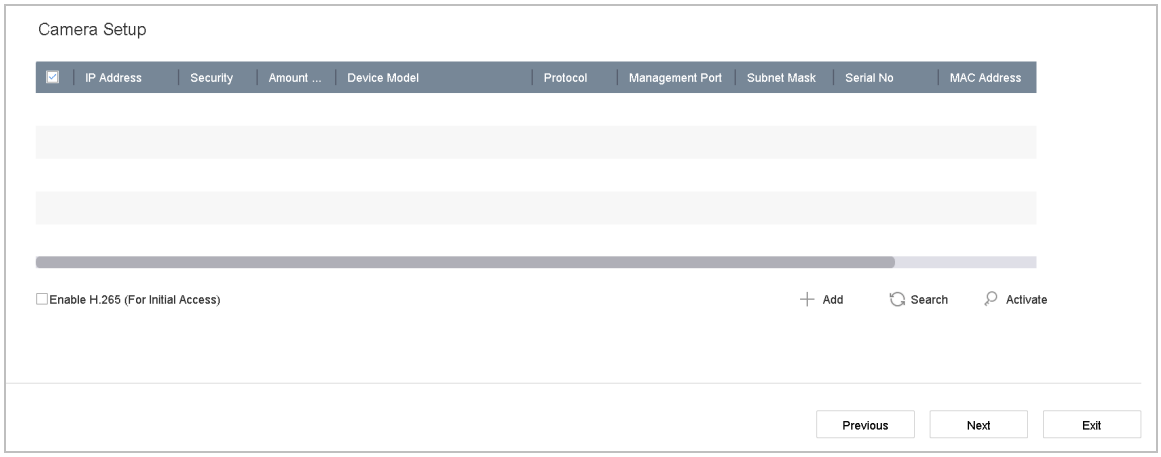


Figure 3-10 Search for IP Cameras

Step 7 Enter Platform Access and configure the Hik-Connect settings.

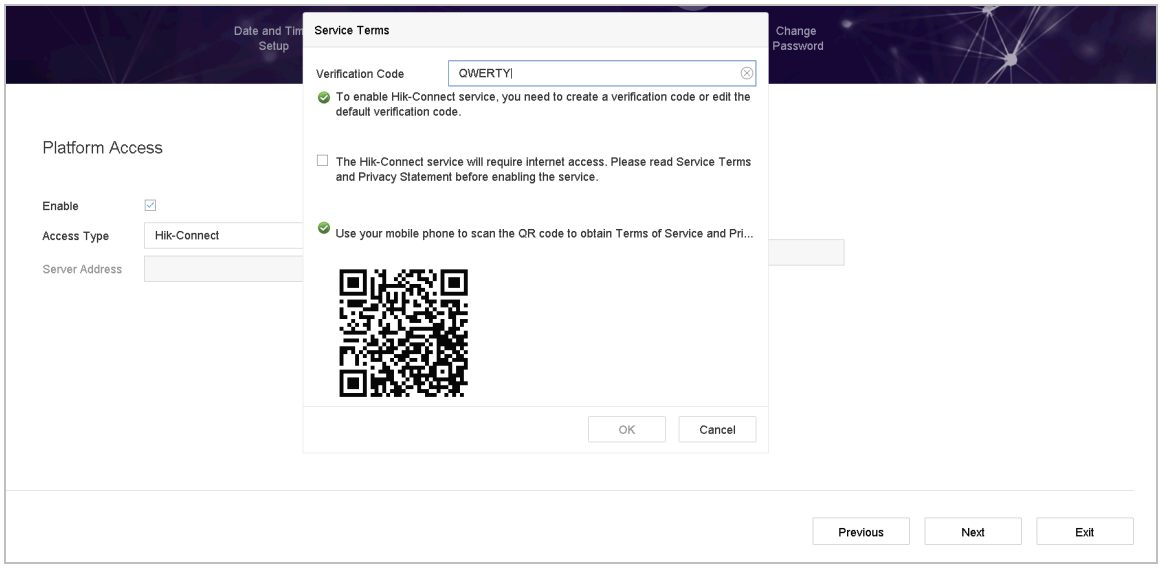


Figure 3-11 Hik-Connect Access

Step 8 Click **Next** to enter the **Change Password** interface to create a new admin password if required.

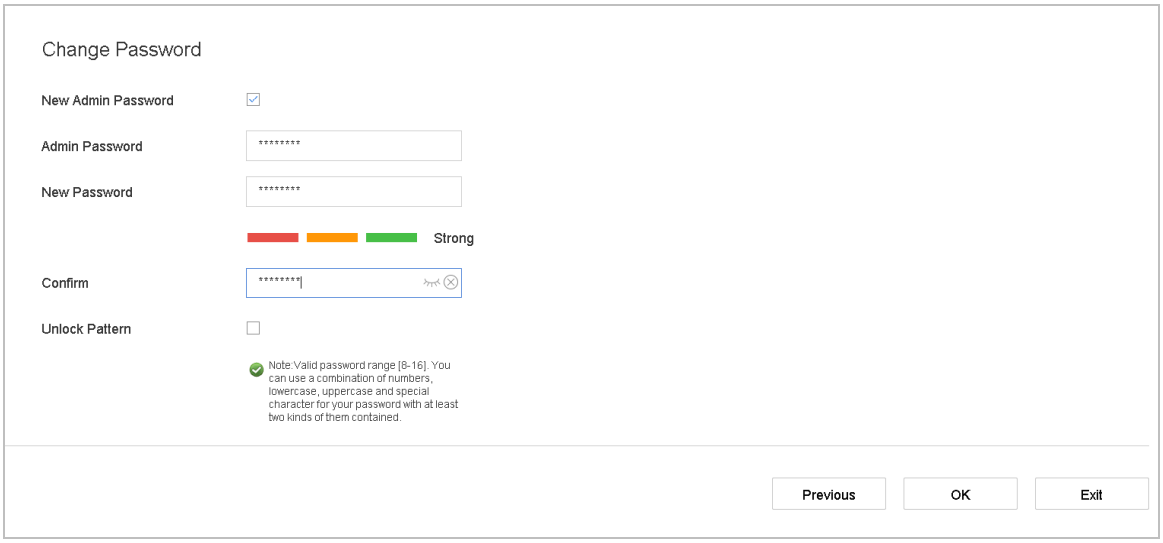


Figure 3-12 Change Password

NOTE

Click to show the characters input.

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

WARNING

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

Step 9 Click **OK** to complete the startup Setup Wizard.

3.6 Entering the Main Menu

Step 1 After you have completed the Setup Wizard, right-click on the screen to enter the main menu bar. Refer to the following figure and table for descriptions of the main menu and sub-menus.

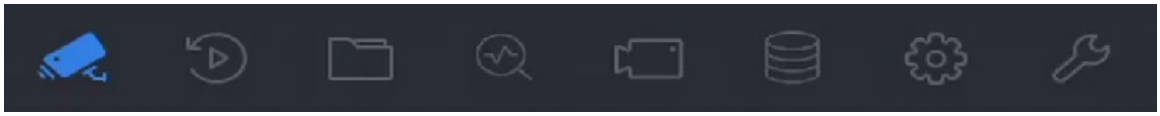


Figure 3-13 Main Menu Bar

Table 3-1 Description of Icons

Icon	Description
	Live View
	Playback
	File Management
	Smart Analysis
	Camera Management
	Storage Management
	System Management
	System Maintenance:

3.7 System Operation

3.7.1 Logging 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.

Figure 3-14 Logout

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.

3.7.2 Shutting Down the Device

Step 1 Click  on the menu bar.

Figure 3-15 Shutdown Menu

Step 2 Click Shutdown.

Step 3 Click **Yes**.

NOTE

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

3.7.3 Rebooting 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 4 Camera Management

4.1 Adding IP Cameras

4.1.1 Adding IP Cameras Manually

Purpose

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

Before You Start

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

Step 1 Click  on the main menu bar to enter the Camera Management interface.

Step 2 Click the **Custom Add** tab on the title bar to enter the Add IP Camera interface.

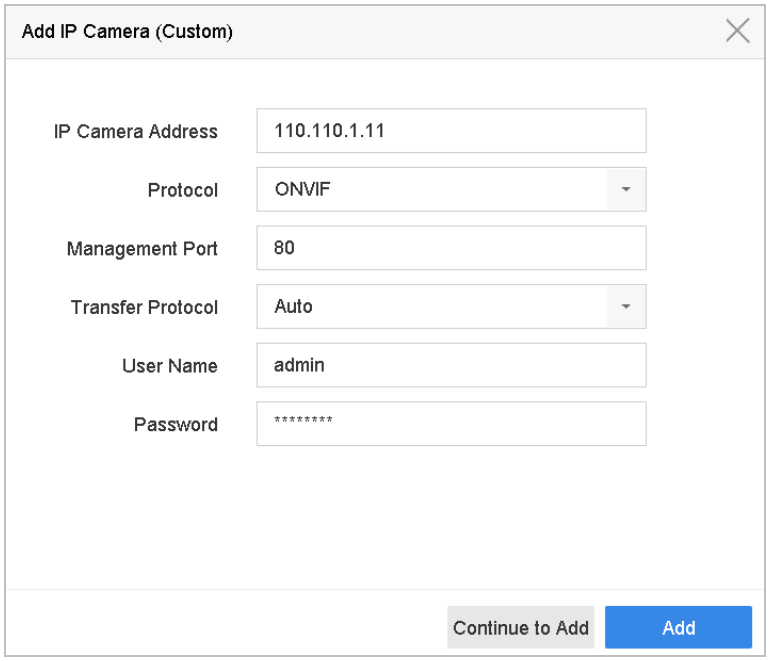


Figure 4-1 Add IP Camera

Step 3 Input the IP address, protocol, management port, and other information.

Step 4 Enter the IP camera's login user name and password.

Step 5 Click **Add** to finish adding the IP camera.

Step 6 (Optional) Click **Continue to Add** to add additional IP cameras.

4.1.2 Adding 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 devices.

Step 3 Click **Add**.

NOTE

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

4.2 Managing PoE Cameras

NOTE

This chapter is applicable only to the following models: DS-7600NI-I2/P, DS-7700NI-I4/P Series.

Purpose

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

If you disable the PoE interface, you can connect to online network cameras. Also, the PoE interface supports the Plug-and-Play function.

For example, for DS-7608NI-I2/8P, to connect six network cameras via PoE interfaces and two online cameras, disable two PoE interfaces in the Edit IP Camera menu.

Follow the steps to add network cameras for devices that support the PoE function.

4.2.1 Adding PoE Cameras

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

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

4.2.2 Adding Non-PoE IP Cameras

You can disable the PoE interface by selecting 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  .

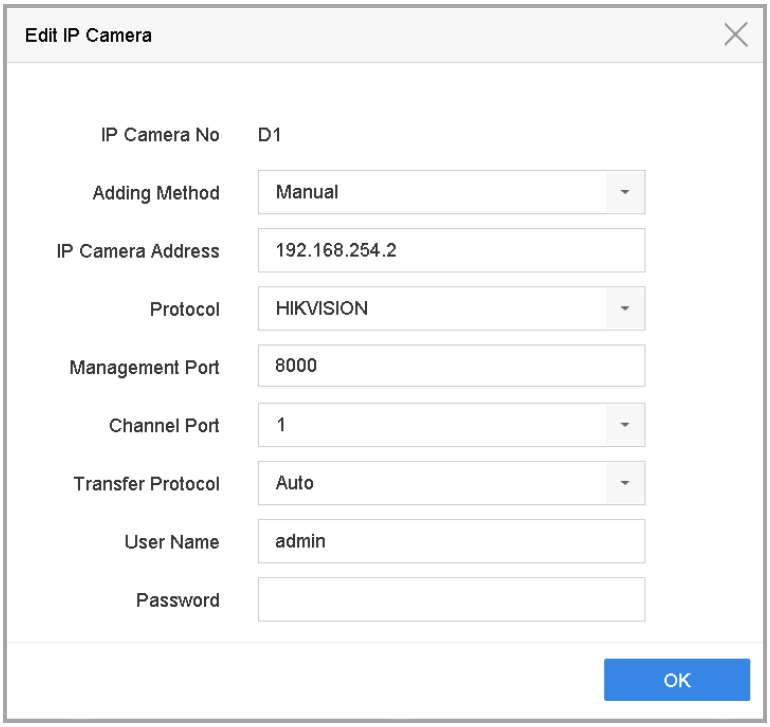


Figure 4-2 Edit IP Camera

Step 3 Set Adding Method to **Manual**.

- **Plug-and-Play:** The camera is physically connected to the PoE interface. Its parameters cannot be edited. You can go to **System > Network > TCP/IP** to change the IP address of the PoE port.
- **Manual:** Add IP camera without a physical connection, via the network.

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

Step 5 Click **OK**.

4.2.3 Configuring PoE Interfaces

Purpose

When long-distance PoE transmission (100 to 300 m) is required, 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.

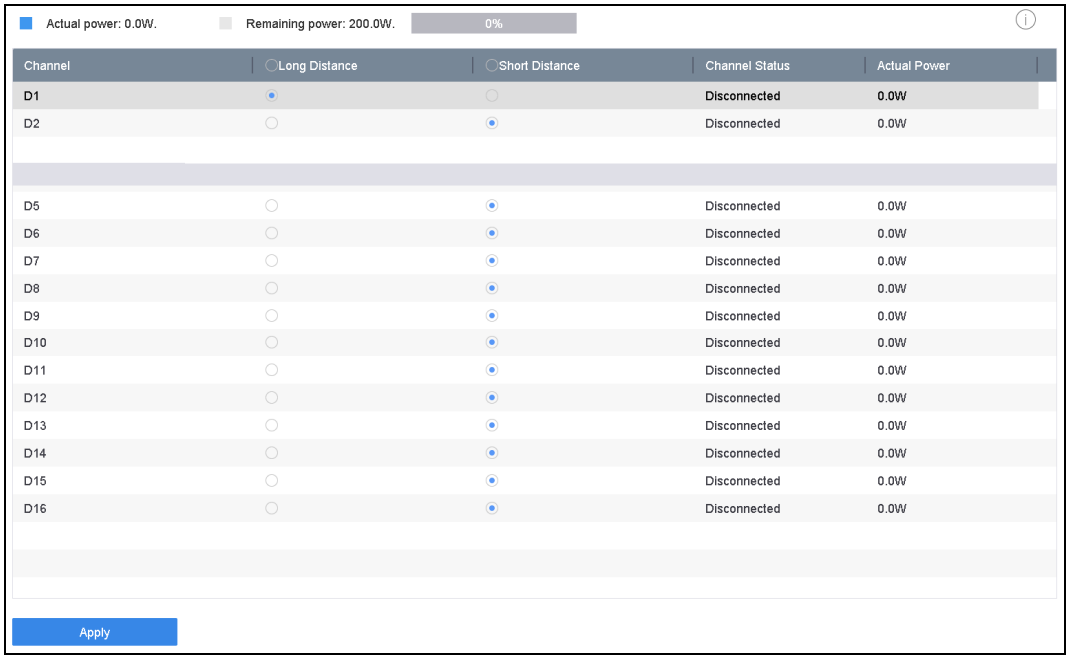


Figure 4-3 PoE Settings

NOTE

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

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

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

When the transmission distance reaches 100 to 250 meters, you must use CAT-5E or CAT-6 network cable to connect with the PoE interface.

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

Refer to Appendix **Error! Reference source not found.Error! Reference source not found.** for the list of IP cameras.

Step 3 Click **Apply**.

4.3 Configuring Customized Protocols

Purpose

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

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

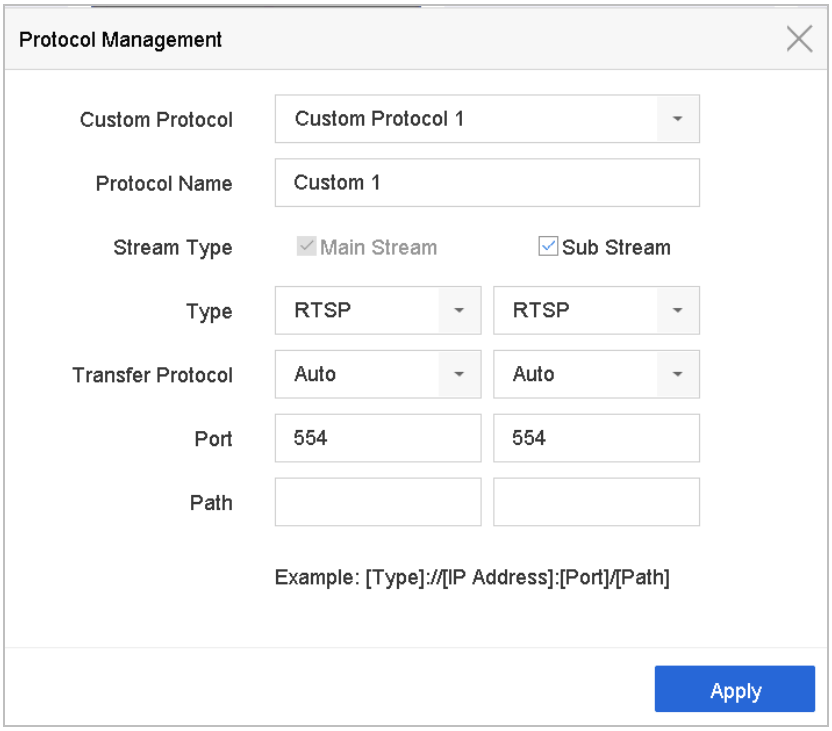


Figure 4-4 Protocol Management

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

- **Type:** The network camera adopting custom protocols must support getting streams through standard RTSP.
- **Path:** Contact the network camera manufacturer 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.

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

Chapter 5 Camera Settings

5.1 Configuring 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 the **Camera Name** text field.

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

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

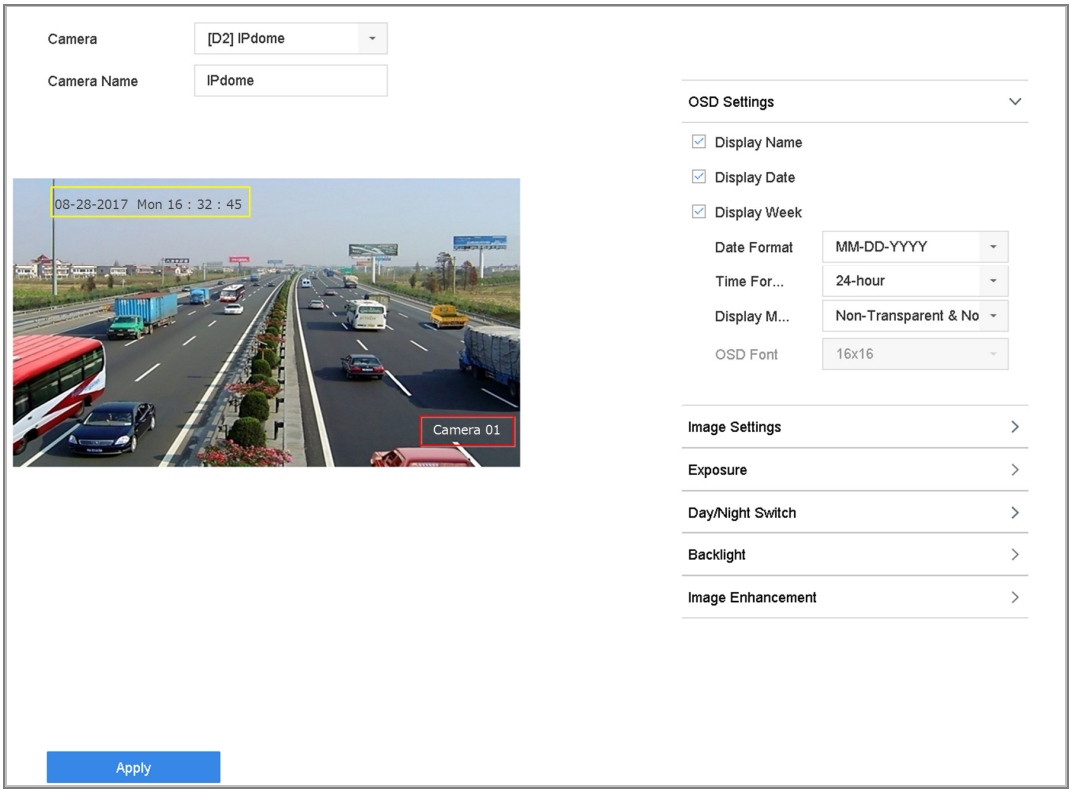


Figure 5-1 OSD Configuration Interface

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** to apply the settings.

5.2 Configuring 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 on which to set the privacy mask.

Step 3 Click the **Enable** checkbox 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.

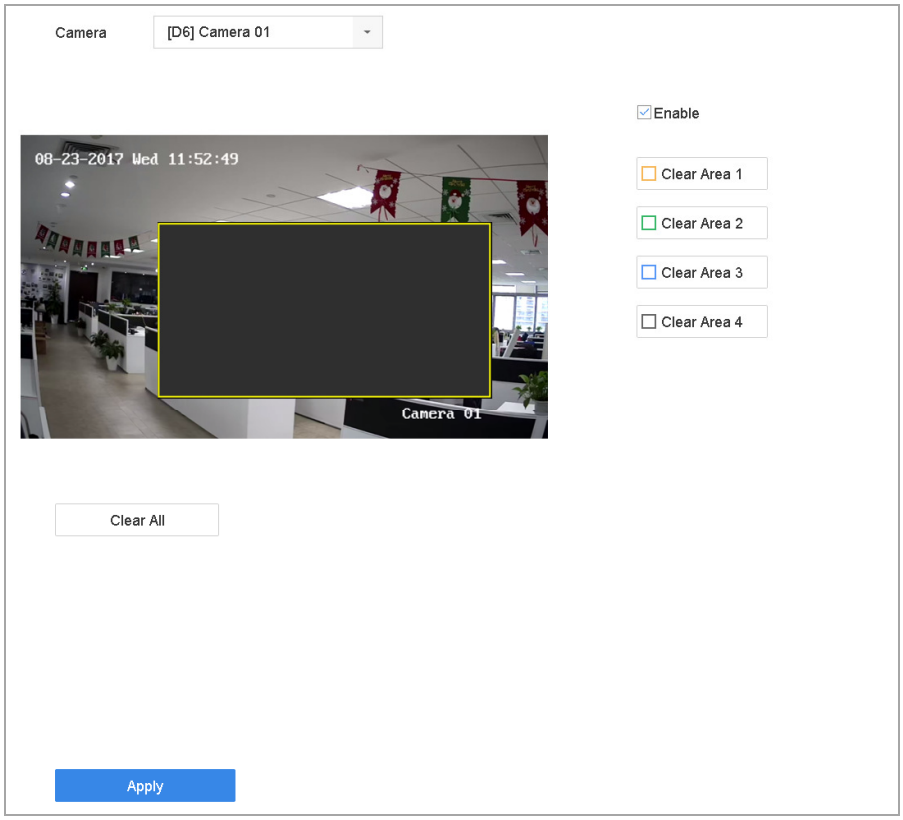


Figure 5-2 Privacy Mask Settings Interface

NOTE

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

Clear the configured privacy mask zones on the window by clicking the corresponding Clear Zone 1-4 icons on the right of the window, or click **Clear All** to clear all zones.

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

5.3 Configuring Video 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**.

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** to save the settings.

5.4 Configuring the Day/Night Switch

Step 1 The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Step 2 Go to **Camera > Display**.

Step 3 Select the camera from the drop-down list.

Step 4 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 between the day/night switch. You can set it from five 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 5 Click **Apply** to save the settings.

5.5 Configuring 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** to save the settings.

Chapter 6 Live View

Live View displays the video image from each camera in real time. The device automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy, thus pressing **ESC** many times brings you back to Live View mode.

6.1 Starting Live View

Step 1 The system automatically enters the Live View interface when starting, or you can click  on the main menu bar to enter the Live View interface.

Step 2 Click to select a window for Live View.

Step 3 Double-click the IP camera on the left list to start playing the live video.

Figure 6-1 Live View

Step 4 Use the toolbar at the window bottom for 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 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 6-2 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 DS-7600/7700/9600-I (/P) 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 180° panorama view.
- **360° Panorama (**  **)**: Switch the Live View image to 360° panorama view.

- **PTZ Expansion ():** The PTZ Expansion is the close-up view of a 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 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.

6.1.3 3D Positioning

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

Step 1 In Live View mode, click  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 interface in full screen mode.

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

6.2 Target Detection

In Live View mode, the target detection function can detect a human motion/face/vehicle/human body during the last five seconds and the following 10 seconds.

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

Step 2 Check the checkboxes to select different detection types: motion detection (), vehicle detection (), face detection (), and human body detection ().

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

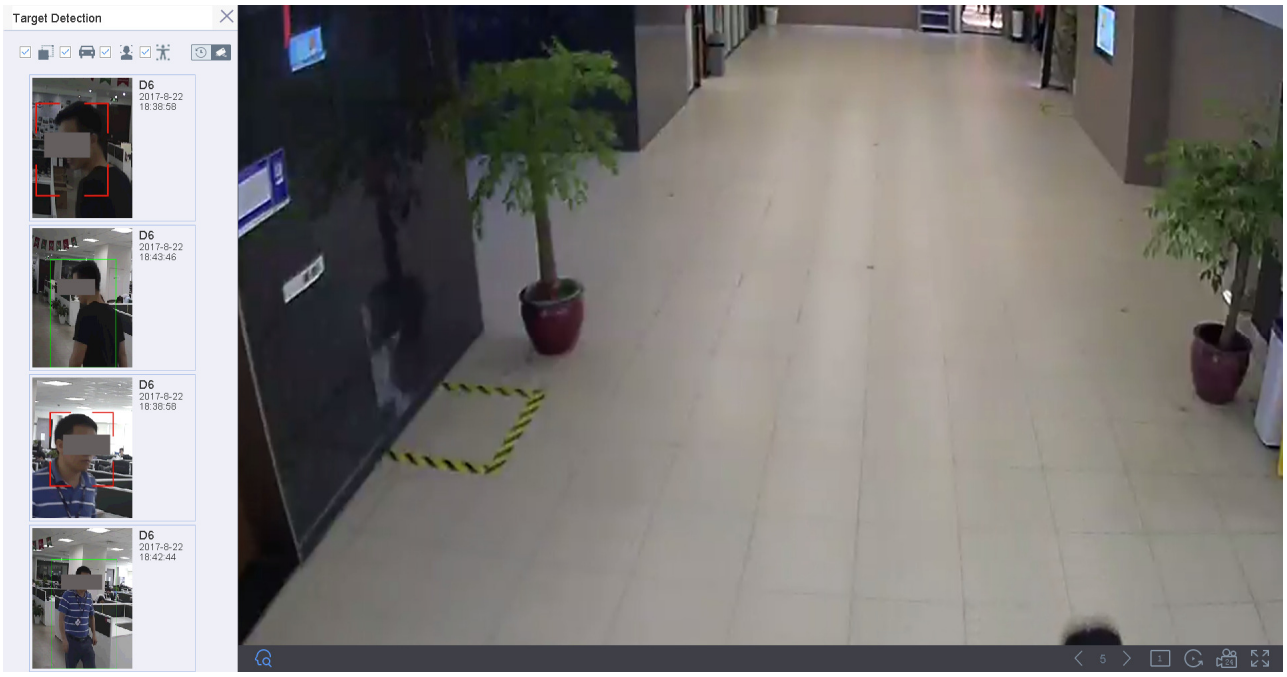


Figure 6-3 Target Detection

Step 4 The smart analysis results of the detection are displayed in the list.

6.3 Configuring 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**.

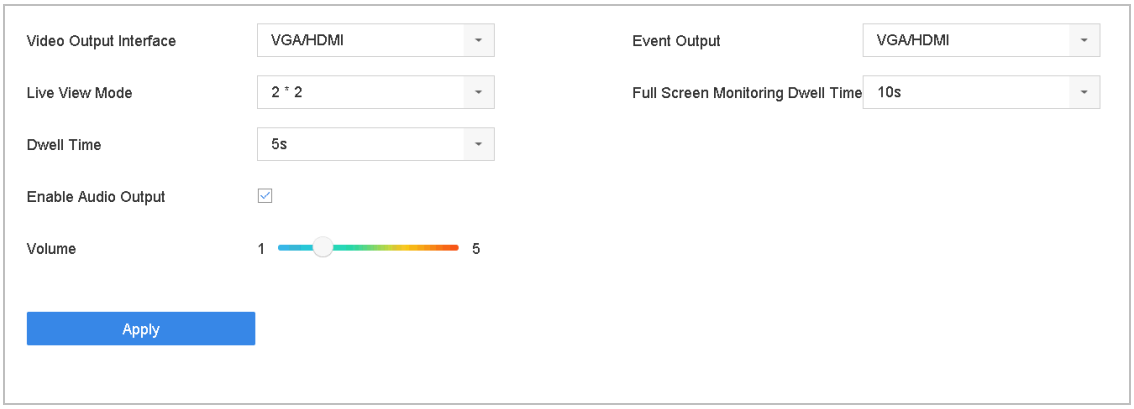


Figure 6-4 Live View-General

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 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.
- **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** to save the settings.

6.4 Configuring Live View Layout

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

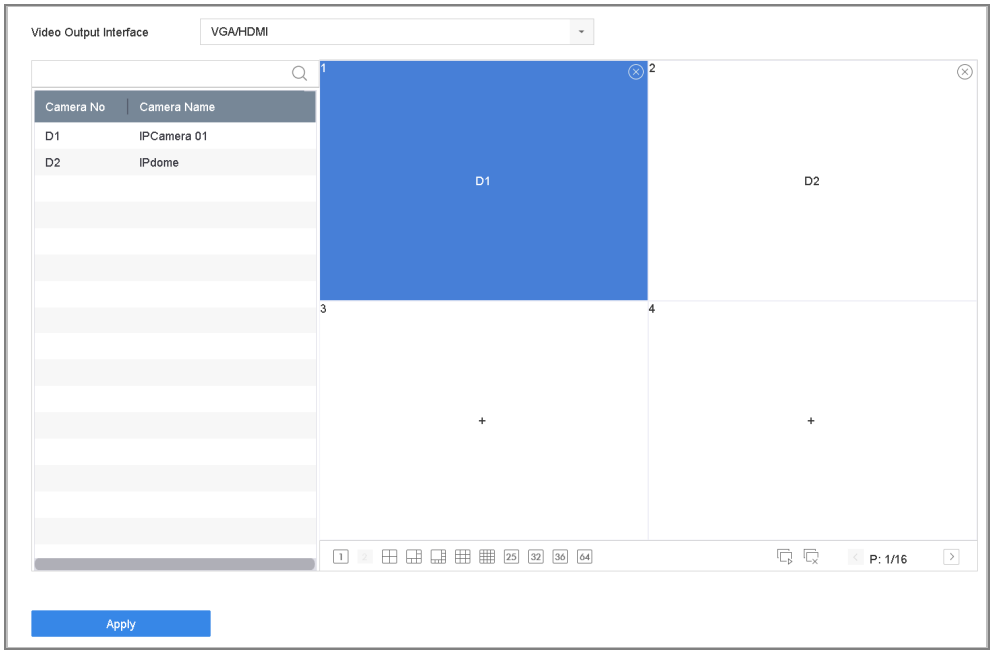


Figure 6-5 Live View

Step 2 Select the video output interface, e.g., HDMI/VGA or channel-zero.

Step 3 Select a window division mode from the toolbar.

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

Step 5 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.

Click  to start Live View for all channels.

Click  to stop all Live View channels.

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

6.5 Configuring Camera Auto-Switch

You can set the cameras' 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** to save the settings.

6.6 Configuring Channel-Zero Encoding

Purpose

Enable channel-zero encoding when you need 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 the Enable Channel-Zero Encoding checkbox.

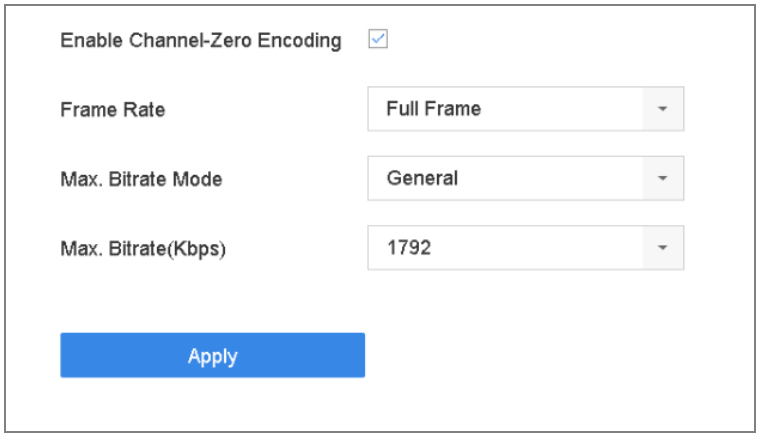


Figure 6-6 Live View, Channel-Zero Encoding

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

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 operations.

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View. The PTZ Control Wizard pops up as below.

Figure 7-1 PTZ Control Wizard

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

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

Step 4 Click **OK** to exit.

7.2 Configuring PTZ Parameters

Purpose

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

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View. The PTZ control panel displays on the right of the interface.

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

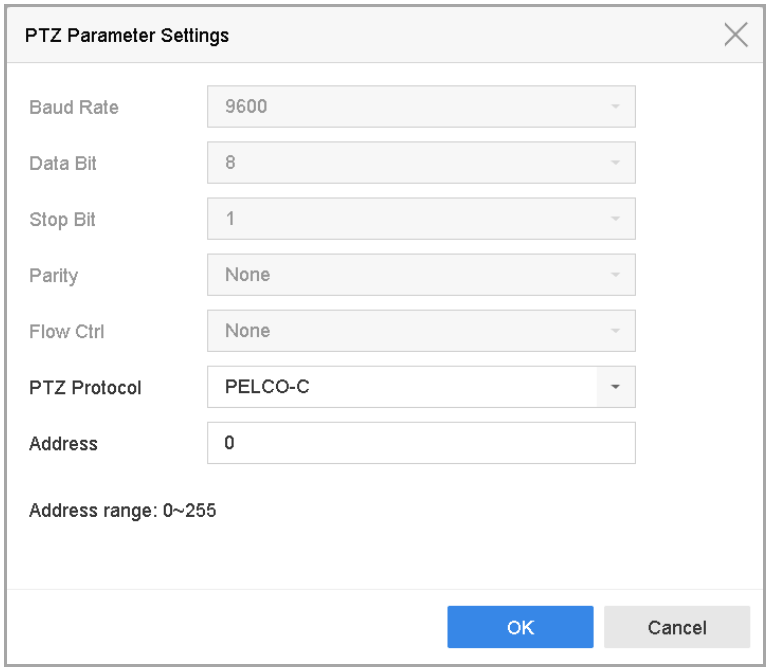


Figure 7-2 PTZ Parameters Settings

Step 3 Edit the PTZ camera parameters.

NOTE

All the parameters should match the PTZ camera parameters.

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

7.3 Setting PTZ Presets, Patrols, and Patterns

Before You Start

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

7.3.1 Setting Presets

Purpose

Follow these steps to set the preset location that 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's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Use the directional buttons on the PTZ control panel to wheel the camera to the location where you want to set a preset, and the zoom and focus operations can be recorded in the preset as well.

Step 4 Click  in the lower right corner of Live View to set the preset.

Figure 7-3 Set Preset

Step 5 Select the preset No. (1 to 255) from the drop-down list.

Step 6 Enter the preset name in the text field.

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

Step 8 Repeat steps 2-6 to save more presets.

Step 9 (Optional) Click **Cancel** to cancel the location information of the preset.

Step 10 (Optional) Click  in the lower right corner of Live View to view the configured presets.

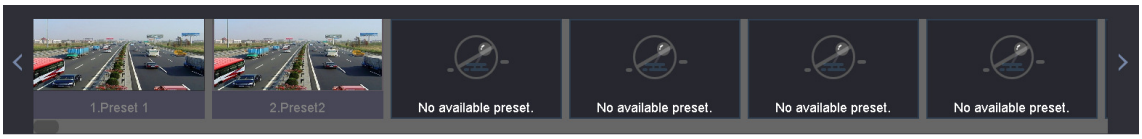


Figure 7-4 View the Configured Presets

7.3.2 Calling Presets

Purpose

A preset 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, or click  in the lower right corner of Live View, and click the configured preset to call it.

Figure 7-5 Call Preset (1)

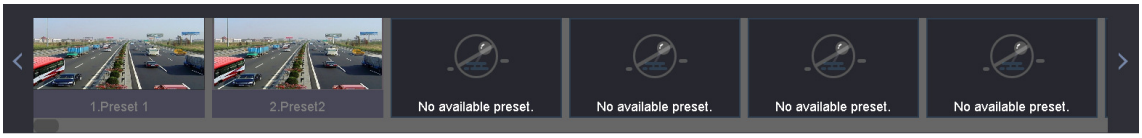


Figure 7-6 Call Preset (2)

7.3.3 Setting Patrols

Purpose

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

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click **Patrol** to configure patrol.

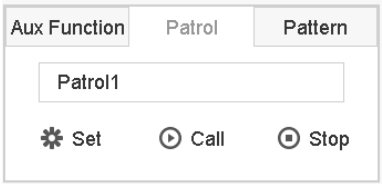


Figure 7-7 Patrol Configuration

Step 4 Select the patrol No. in the text field.

Step 5 Click **Set** to enter the Patrol Settings interface.

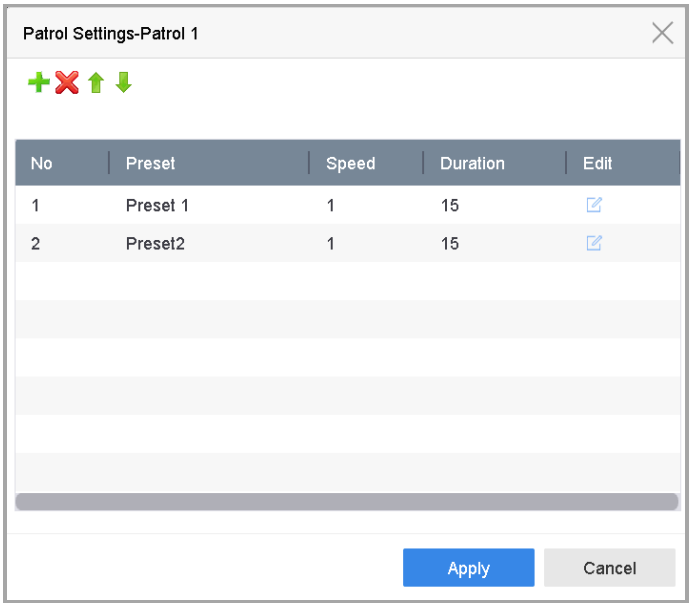


Figure 7-8 Patrol Settings

Step 6 Click  to add a key point to the patrol.

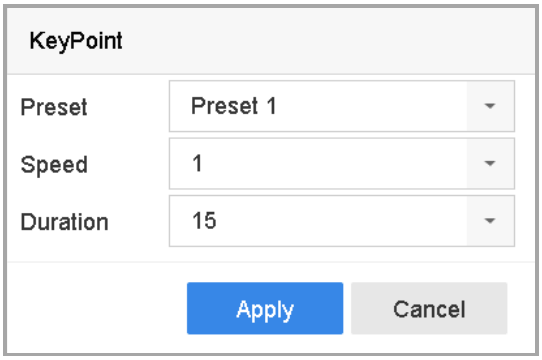


Figure 7-9 Key Point Configuration

1) Configure key point parameters.

   - **Preset:** Determines the order the PTZ will follow while cycling through the patrol.
   - **Speed:** Defines the speed the PTZ will move from one key point to the next.
   - **Duration:** Refers to the duration to stay at the corresponding key point.

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

Step 7 (Optional) Click  to edit the added key point.

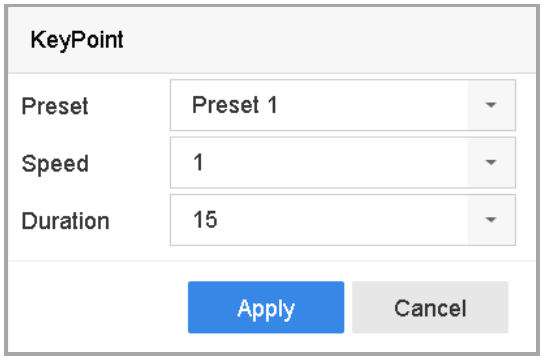


Figure 7-10 Edit Key Point

Step 8 (Optional) Select a key point and click to delete it.

Step 9 (Optional) Click or to adjust the key point order.

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

Step 11 Repeat steps 3-9 to set more patrols.

7.3.4 Calling a Patrol

Purpose

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

Step 1 Click on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click **Patrol** on the PTZ control panel.

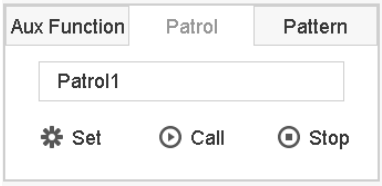


Figure 7-11 Patrol Configuration

Step 4 Select a patrol in the text field.

Step 5 Click **Call** to start the patrol.

Step 6 (Optional) Click **Stop** to stop the patrol.

7.3.5 Setting a Pattern

Purpose

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

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click **Pattern** to configure a pattern.

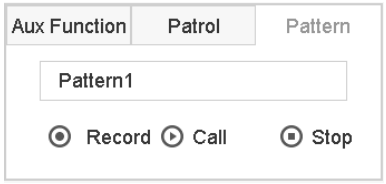


Figure 7-12 Pattern Configuration

Step 4 Select the pattern No. in the text field.

Step 5 Set the pattern.

1) Click **Record** to start recording.
2) Click corresponding buttons on the control panel to move the PTZ camera.
3) Click **Stop** to stop recording. The PTZ movement is recorded as the pattern.

Step 6 Repeat steps 3-4 to set more patterns.

7.3.6 Calling 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's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click **Pattern**.

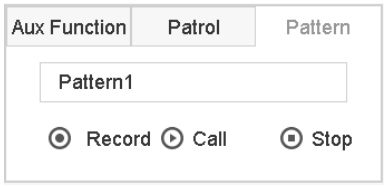


Figure 7-13 Pattern Configuration

Step 4 Select a pattern in the text field.

Step 5 Click **Call** to start the pattern.

Step 6 (Optional) Click **Stop** to stop the pattern.

7.3.7 Setting Linear Scan Limits

Before You Start

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

Purpose

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

NOTE

This function is supported only by certain models.

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click the **directional buttons** to wheel the camera to the location of 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 linear scans from the left limit to the right limit, and you must set the left limit on the left side of the right limit. Also, the angle from the left limit to the right limit must be no more greater than 180°.

7.3.8 Calling Linear Scan

NOTE

Before operating this function, make sure the connected camera supports linear scan and is in HIKVISION 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's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click **Linear Scan** to start the linear scan and click it again to stop it.

Step 4 (Optional) Click **Restore** to clear the defined left limit and right limit data.

NOTE

Reboot the camera to have the settings take effect.

7.3.9 One-Touch Park

NOTE

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

Purpose

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

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click Park (Quick Patrol), Park (Patrol 1), or Park (Preset 1) to activate the park action.

- **Park (Quick Patrol):** The dome starts patrolling from the predefined preset 1 to preset 32 in order after the park time. Undefined presets will be skipped.
- **Park (Patrol 1):** The dome starts moving according to the predefined patrol 1 path after the park time.
- **Park (Preset 1):** The dome moves to the predefined preset 1 location after the park time.

NOTE

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

Step 4 Click Stop Park (Quick Patrol), Stop Park (Patrol 1), or Stop Park (Preset 1) to inactivate it.

7.4 Auxiliary Functions

Before You Start

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

Purpose

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

Step 1 Click  on the quick settings toolbar of the PTZ camera's Live View.

Step 2 The PTZ control panel displays on the right of the interface.

Step 3 Click Aux Function.

Figure 7-14 Aux Function Configuration

Step 4 Click the icons to operate the aux functions. See the table for the icon descriptions.

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 Installing the HDD

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

8.1.2 Adding Network Disks

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

Adding a NAS

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.

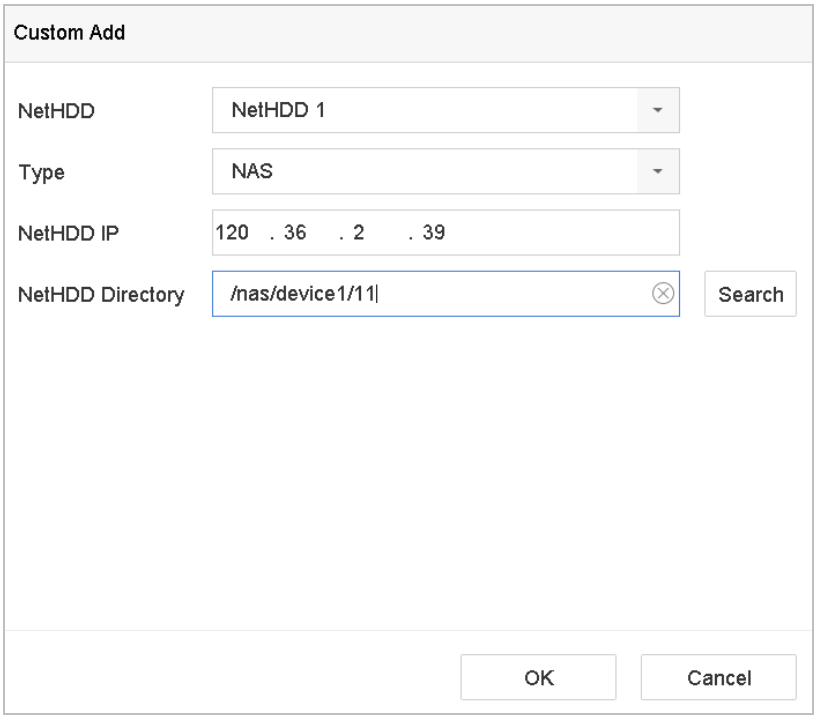


Figure 8-1 Add NAS Disk

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

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

Step 9 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 Set 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 the IP SAN disk.

NOTE

A single IP SAN disk can be added.

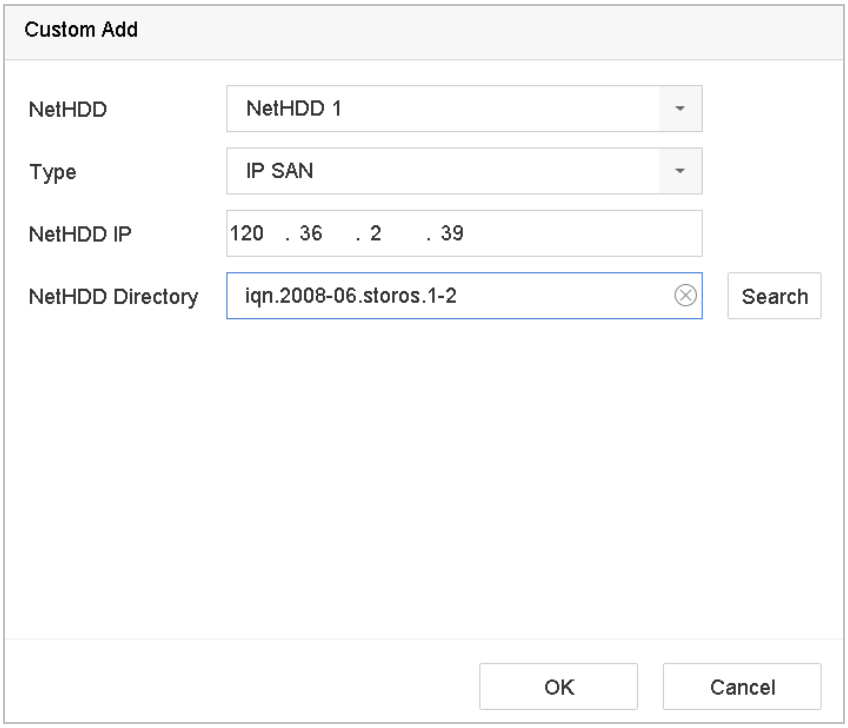


Figure 8-2 Add IP SAN Disk

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.

NOTE

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

8.1.3 Configuring eSATA for Data Storage

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

Step 1 Click Storage > Advanced.

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

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

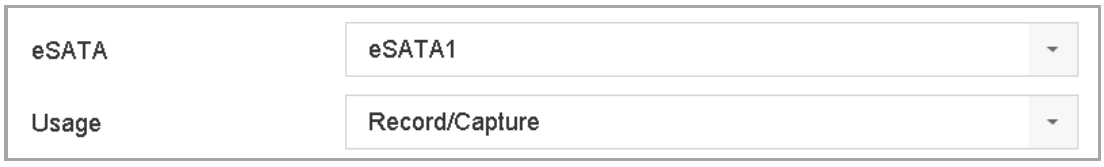


Figure 8-3 Set eSATA Mode

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.

8.2 Storage Mode

8.2.1 Configuring 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.

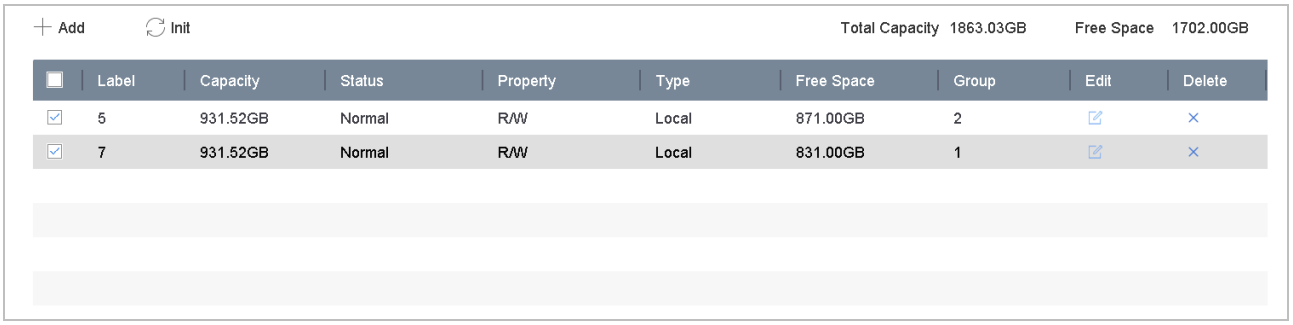


Figure 8-4 Storage Device

Step 3 Click  to enter the Local HDD Settings interface.

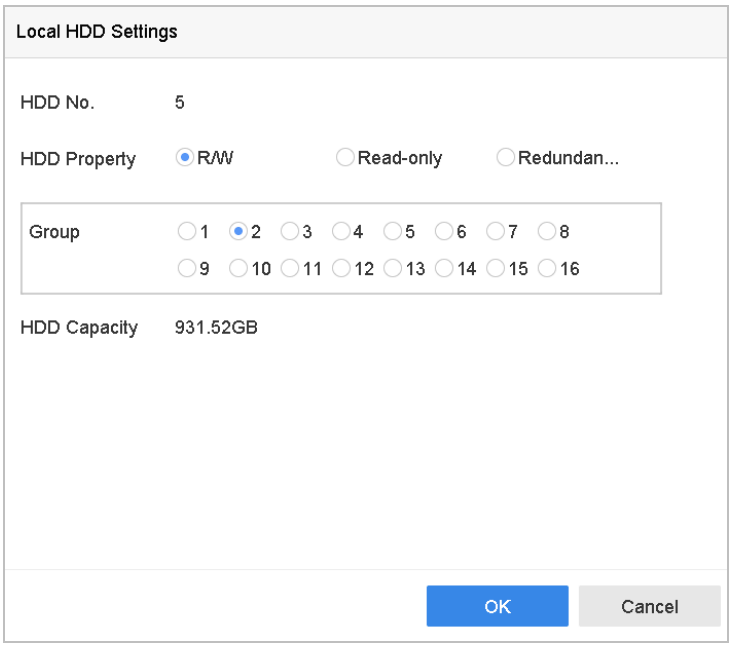


Figure 8-5 Local HDD Settings

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 the **Group** tab checkbox.

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.

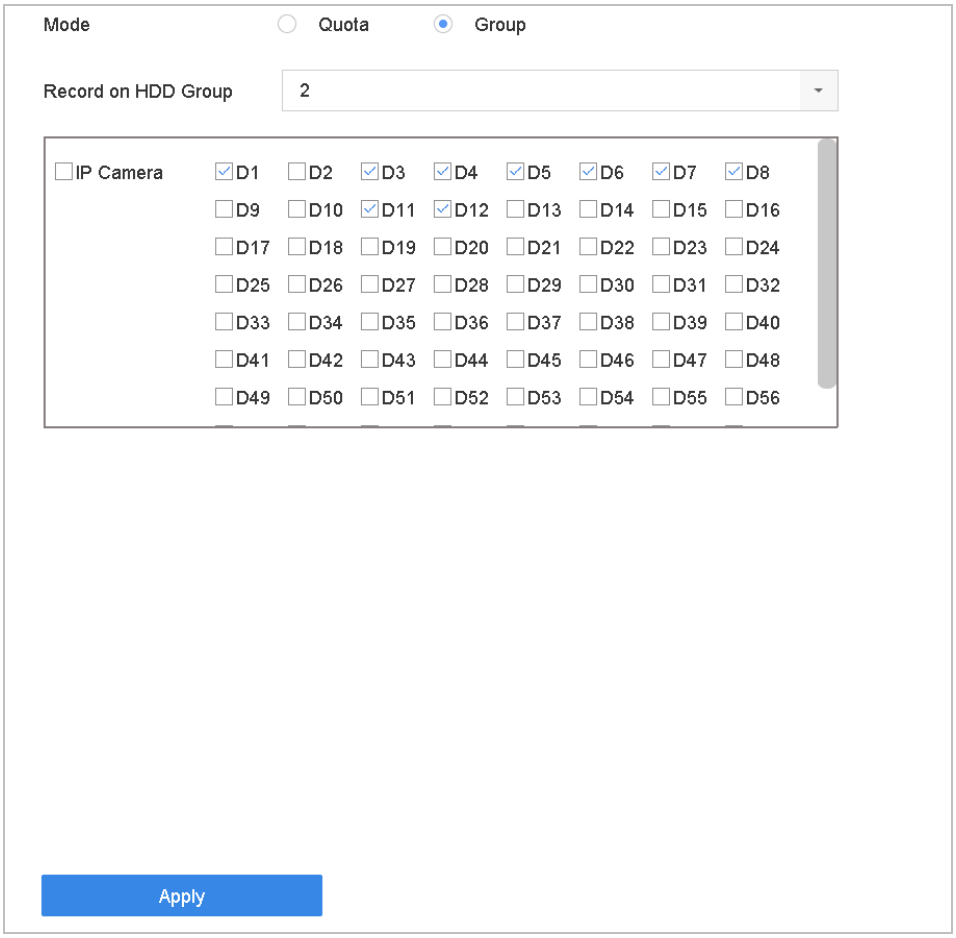


Figure 8-6 Storage Mode-HDD Group

Step 10 Click **Apply**.

NOTE

Reboot the device to activate the new storage mode settings.

8.2.2 Configuring 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 **Quota** tab checkbox.

Step 3 Select a camera for which to set the quota.

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

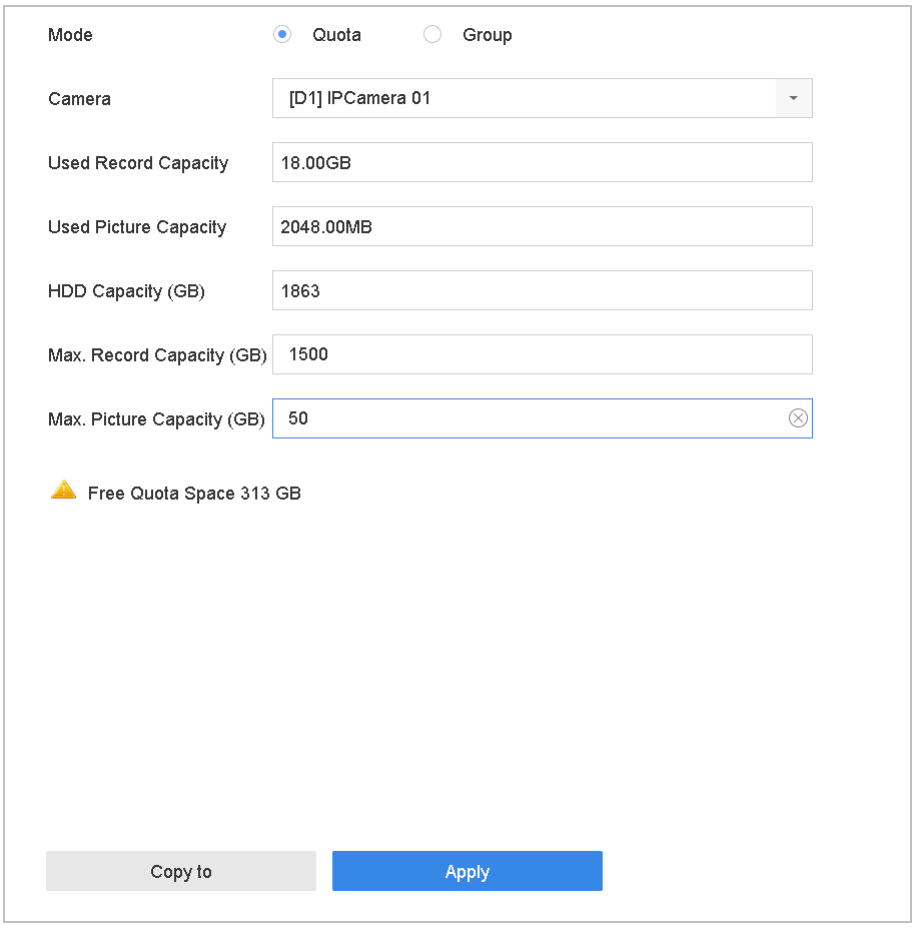


Figure 8-7 Storage Mode-HDD Quota

Step 5 (Optional) Click **Copy to** to copy the quota settings of the current camera to other cameras.

Step 6 Click **Apply** to apply the settings.

NOTE

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

NOTE

Reboot the device to activate the new storage mode settings.

8.3 Recording Parameters

8.3.1 Main Stream

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

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

Step 1 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.

Step 2 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.

Step 3 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.

Step 4 Enable H.264+ Mode: The H.264+ mode helps to ensure high video quality with a lowered bitrate. It effectively reduces the need of bandwith and HDD storage space.

NOTE

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

8.3.2 Sub-Stream

The sub-stream is a second codec that runs alongside the main stream. It reduces the outgoing Internet bandwidth without sacrificing the direct recording quality.

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

8.3.3 Picture

Step 1 Picture refers to live picture capture in continuous or event recording type.

Step 2 **Picture Quality**: Set the picture quality to low, medium, or high. Higher picture quality requires more storage space.

Step 3 **Interval**: The interval of capturing live pictures.

8.3.4 ANR

ANR (Automatic Network Replenishment) function enables IP cameras to save the recording files in local storage when the network is disconnected. When the network is re-connected, it uploads the files to the device.

Step 1 Enable the ANR (Automatic Network Replenishment) function via a Web browser (**Configuration** > **Storage** > **Schedule Settings** > **Advanced**).

8.3.5 Configuring Advanced Recording Settings

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

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

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

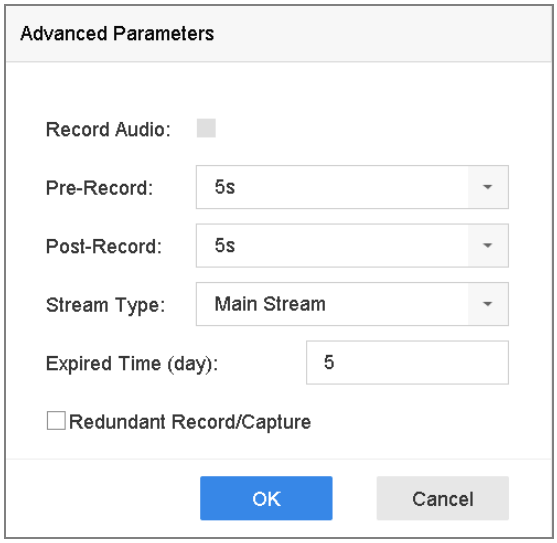


Figure 8-8 Advanced Record Settings

- **Record Audio**: Check the checkbox to enable or disable audio recording.
- **Pre-record**: The time set to record before the scheduled time or event. For example, if an alarm triggers the recording at 10:00, and the pre-record time is 5 seconds, the device will start to record at 9:59:55.

- **Post-record:** The time set to record after the event or scheduled time. For example, if an alarm triggered recording ends at 11:00, and the post-record time is 5 seconds, the device will record until 11:00:05.
- **Expired Time**: The period of time for a recorded file to be kept in the HDD. When the deadline is reached, the file will be deleted. If the expired time is set to 0, the file will not be deleted. The actual keeping time for the file should be determined by the HDD capacity.
- **Redundant Record/Capture**: Enable redundant record or capture to save the record and captured picture in the redundant HDD. See *Chapter Configuring Redundant Recording and Capture*.
- **Stream Type**: Main stream and sub-stream are selectable for recording. Select sub-stream to record for a longer time with the same storage space.

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

8.4 Configuring Recording Schedules

The camera automatically starts/stops recording according to the configured schedule.

Before You Start

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

Refer to the *Quick Start Guide* for HDD installation instructions. Refer to Chapter 8.1.2 Adding Network Disk for network HDD connections.

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

Step 2 Select a camera.

Step 3 Check Enable Schedule.

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

- **Continuous:** Scheduled recording
- **Event**: Recording triggered by an event triggered alarm
- **Motion**: Recording triggered by motion detection
- **Alarm:** Recording triggered by an alarm
- **M/A:** Recording triggered by either motion detection or an alarm
- **M&A:** Recording triggered by motion detection and an alarm
- **POS:** Recording triggered by POS and an alarm

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

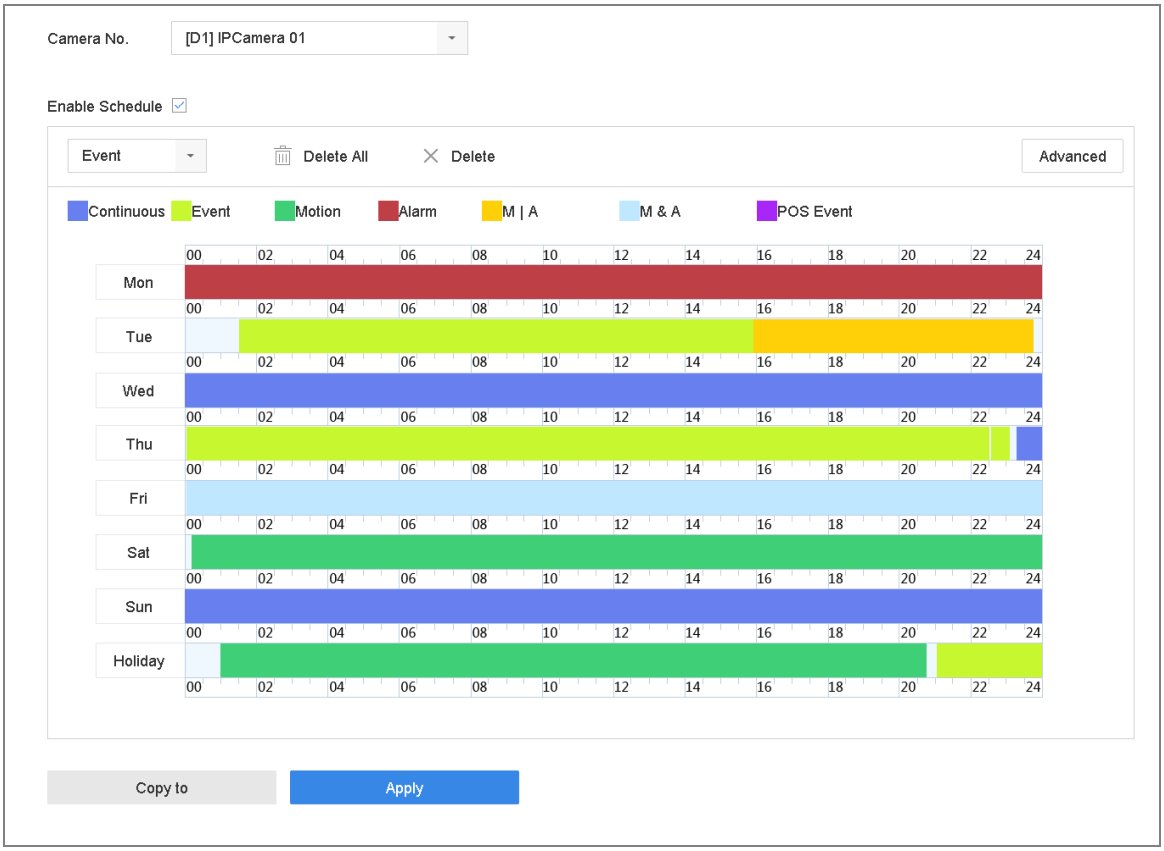


Figure 8-9 Record Schedule

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

NOTE

All-day continuous recording is the factory default.

Step 7 (Optional) Copy the schedule settings of the 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**.

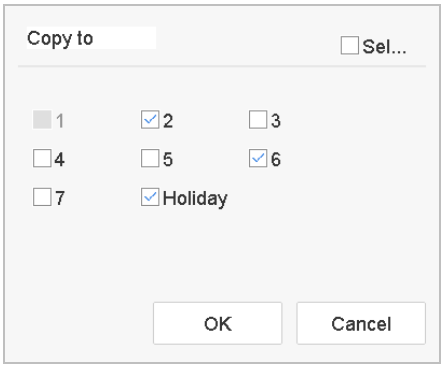


Figure 8-10 Copy Schedule to Other Days

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

NOTE

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

Event and Alarm Settings and Chapter 13 VCA Event Alarm for details.

8.5 Configuring 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 Set the record type to **Continuous**.

Step 5 Set the schedule for the continuous recording. Refer to Chapter 8.4 Configuring Recording Schedule for details.

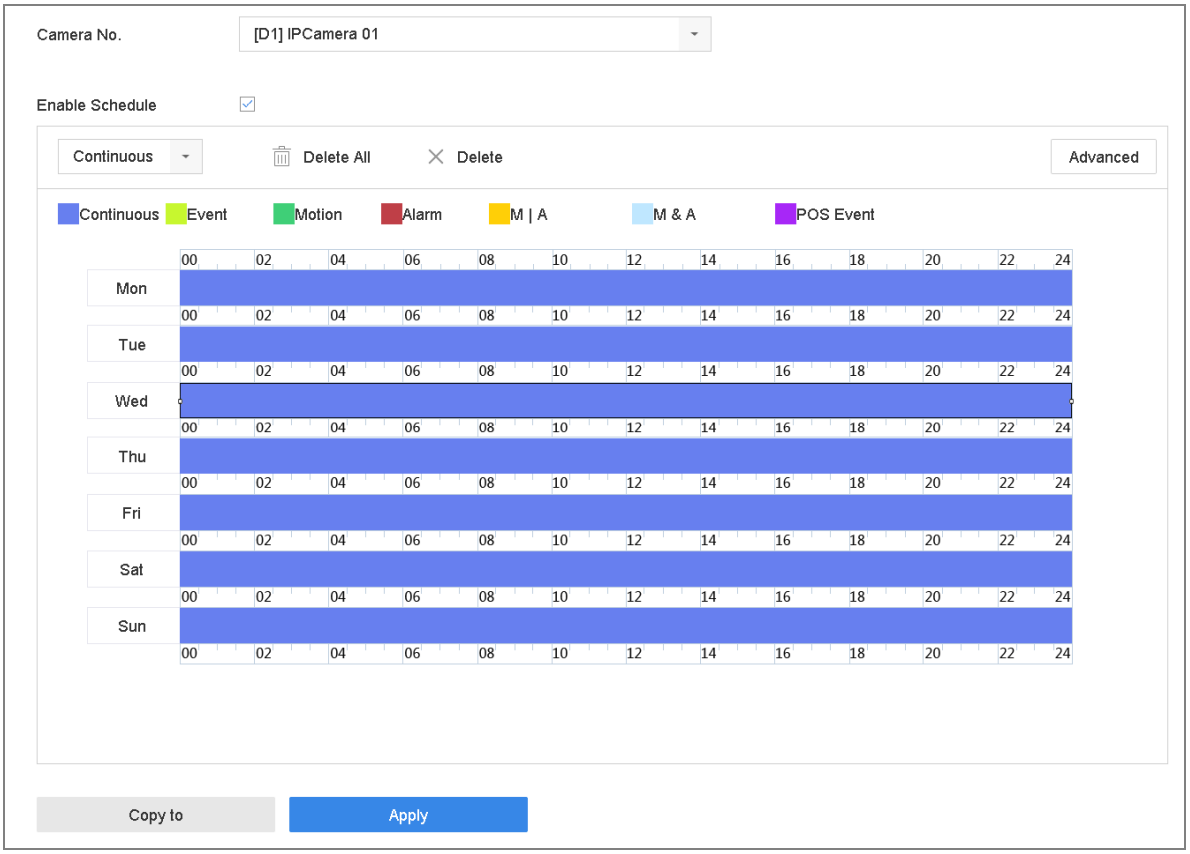


Figure 8-11 Record Schedule

8.6 Configuring Motion Detection Triggered Recordings

You can configure recordings triggered by motion detection events.

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

Step 2 Configure motion detection and select the channel(s) to trigger the recording when a motion event occurs. Refer to Chapter 12.3 Configuring 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 Set the record type to **Motion**.

Step 7 Set the schedule for the motion detection triggered recording. Refer to Chapter 8.4 Configuring Recording Schedule for details.

8.7 Configuring Event Triggered Recordings

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

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

Step 2 Configure event detection and select the channel(s) to trigger the recording when an 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 Set the record type to **Event**.

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

8.8 Configuring Alarm Triggered Recordings

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 an alarm 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 Set the record type to **Alarm**.

Step 7 Set the schedule for the alarm triggered recording. Refer to Chapter 8.4 Configuring Recording Schedule for details.

8.9 Configuring POS Event Triggered Recordings

You can configure recordings triggered by connected POS events such as transactions, etc.

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

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

Step 3 Refer to Chapter 14 Smart Analysis for details.

Step 4 Go to **Camera > Encoding Parameters > Recording Parameters**.

Step 5 Set the event main stream/sub-stream recording parameters for the camera.

Step 6 Go to **Storage > Recording Schedule**.

Step 7 Set the record type to **POS Event**.

Step 8 Set the schedule for the POS event triggered recording. Refer to Chapter 8.4 Configuring Recording Schedule for details.

8.10 Configuring Picture Capture

Step 1 Picture refers to live picture capture in continuous or event recordings.

Step 2 Go to **Camera > Encoding Parameters > Capture**.

Step 3 Set the picture parameters.

- **Resolution**: Set the resolution of the picture to capture.
- **Picture Quality**: Set the picture quality to low, medium, or high. A higher picture quality requires more storage space.
- **Interval**: The interval of capturing live pictures.

Step 4 Go to **Storage > Capture Schedule**.

Step 5 Select the camera for which to configure picture capture.

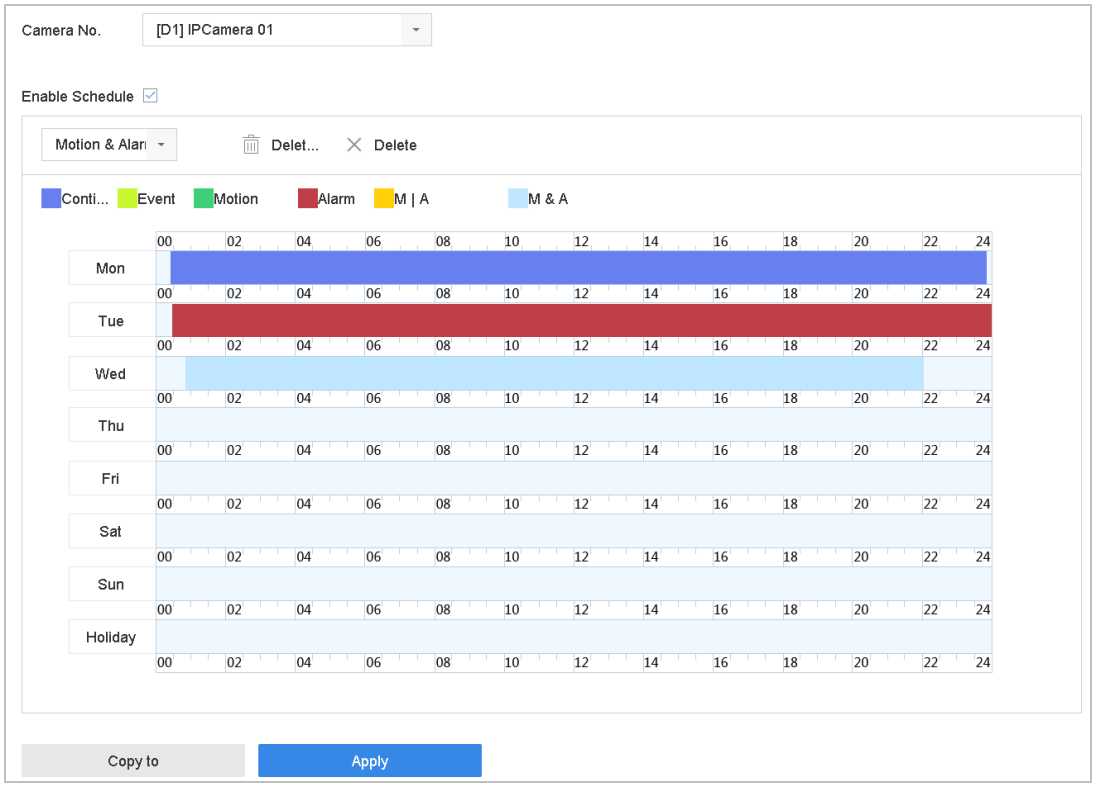


Figure 8-12 Set Picture Capture Schedule

Step 6 Set the picture capture schedule. See Chapter 8.4 Configuring Recording Schedule.

8.11 Configuring Holiday Recording and Capture

Purpose

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

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

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

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

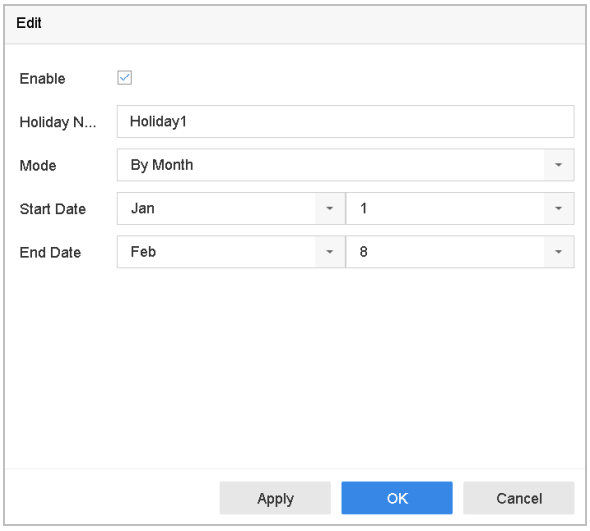


Figure 8-13 Edit Holiday Settings

1) Edit the holiday name.
2) Set 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 Configuring Recording Schedule for details.

8.12 Configuring 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, refer to Chapter 8.2.1 Configuring 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 an HDD from the list and click  to enter the Local HDD Settings interface.

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

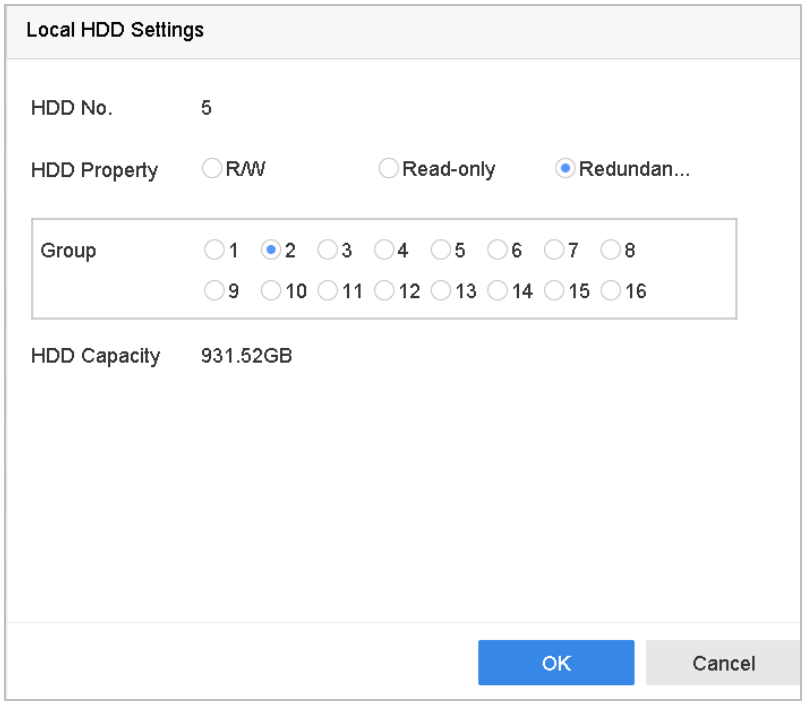


Figure 8-14 HDD Property-Redundancy

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

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

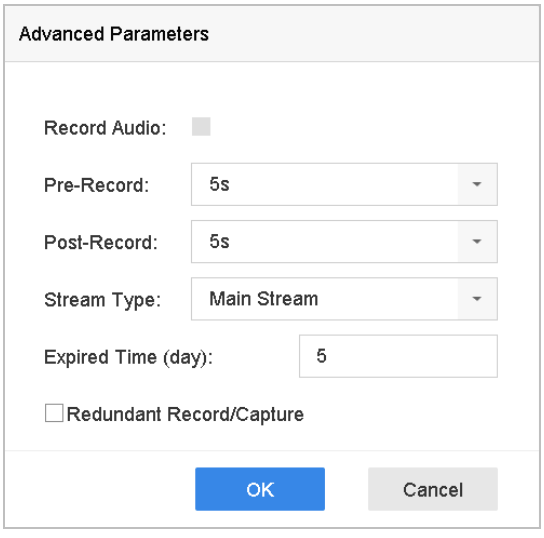


Figure 8-15 Record Parameters

Step 6 Check the Redundant Record/Capture checkbox.

Step 7 Click **OK** to save the 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 DS-9600NI-I Series devices only.

9.1 Creating 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.

9.1.1 Enabling a RAID

Purpose

Perform the following steps to enable the disk array function.

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

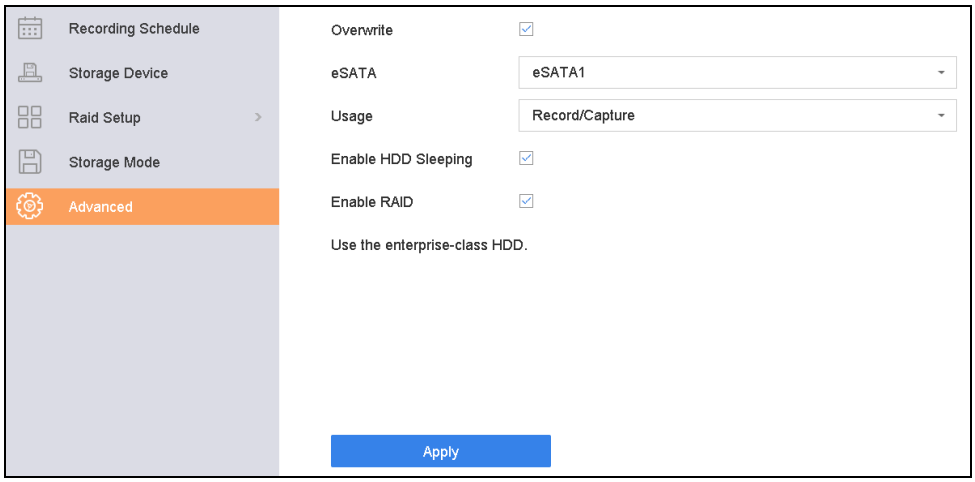


Figure 9-1 Advanced

Step 2 Check Enable RAID.

Step 3 Click **Apply**.

Step 4 Reboot the device to have the settings take effect.

9.1.2 One-Touch Creation

Purpose

One-touch configuration quickly creates a 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 Enabling a RAID.

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

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

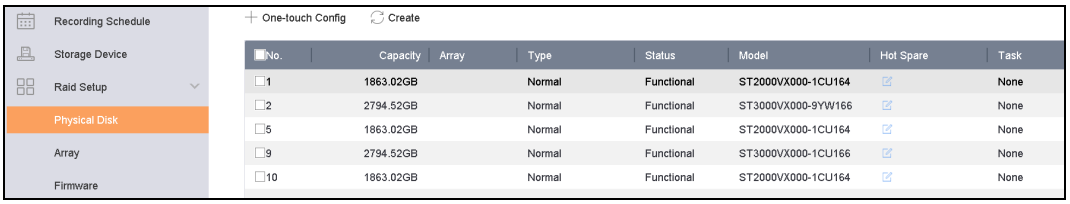


Figure 9-2 Physical Disk

Step 2 Click One-touch Config.

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

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

NOTE

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

Step 5 When a message box pops up when the array creation is complete, click **OK**.

Step 6 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**.

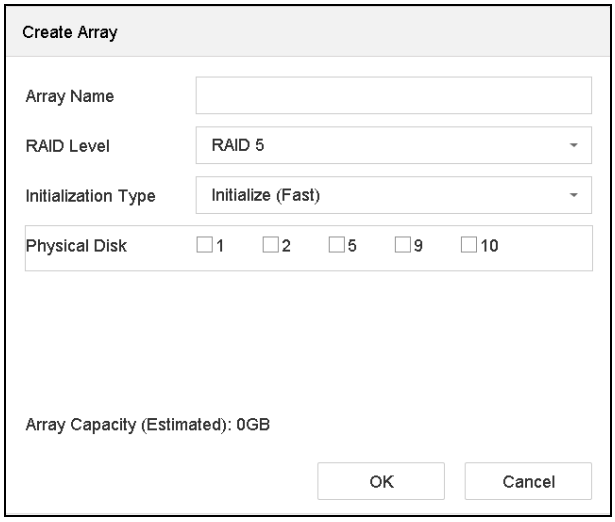


Figure 9-3 Create Array Window

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 9-1 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 HDDs must be an even range 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 array.

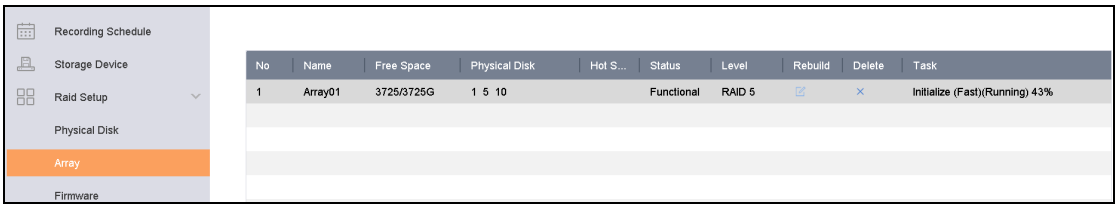


Figure 9-4 Array List

9.2 Rebuilding 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 array 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 Configuring 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 9-5 Physical Disk

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

9.2.2 Automatically Rebuilding 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 Configuring a Hot Spare Disk.

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

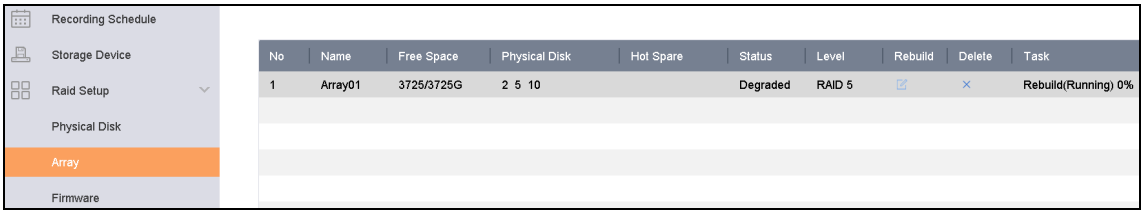


Figure 9-6 Array List

9.2.3 Manually Rebuilding 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**.

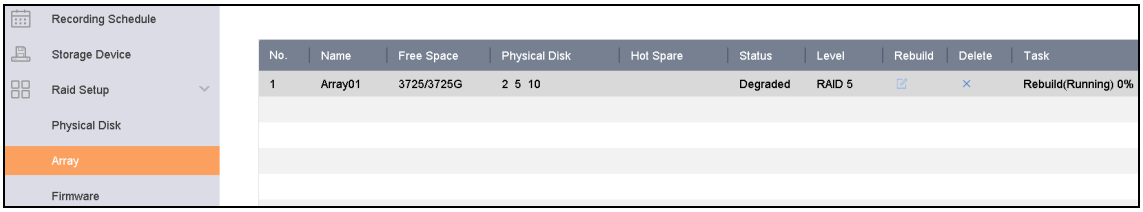


Figure 9-7 Array List

Step 2 Click  of the degraded array.

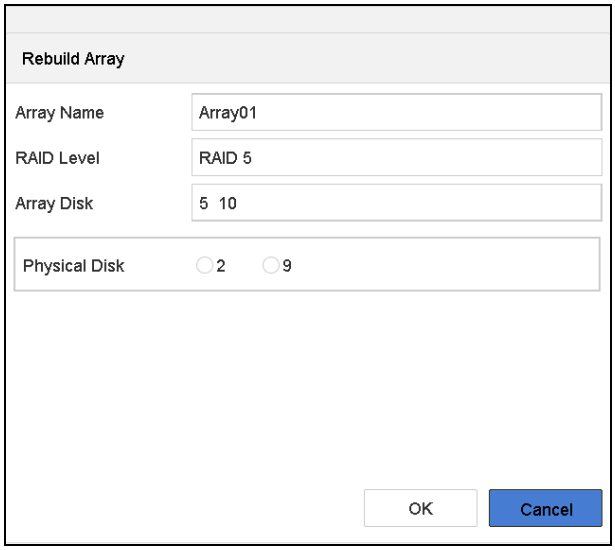


Figure 9-8 Rebuild Array

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 Deleting an Array

NOTE

Deleting an array will delete all data saved to it.

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

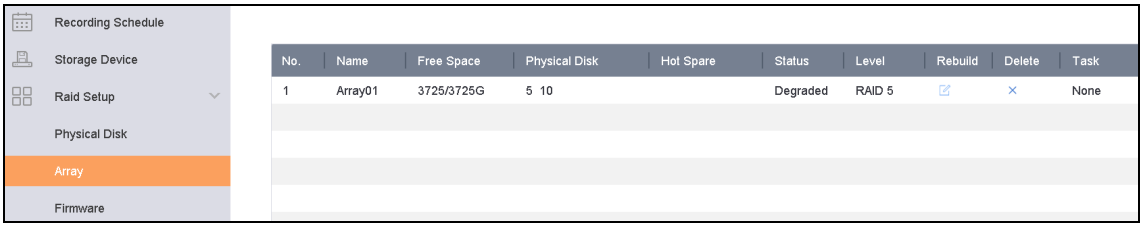


Figure 9-9 Array List

Step 2 Click ✕ of the array to delete it.

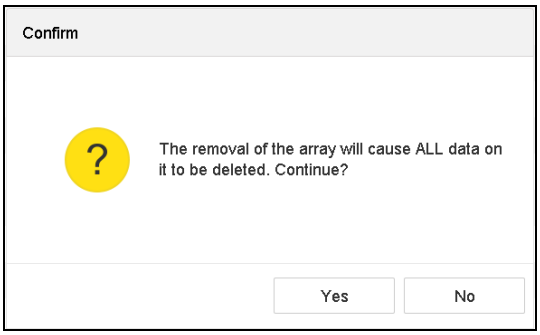


Figure 9-10 Attention

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

9.4 Checking and Editing 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**.

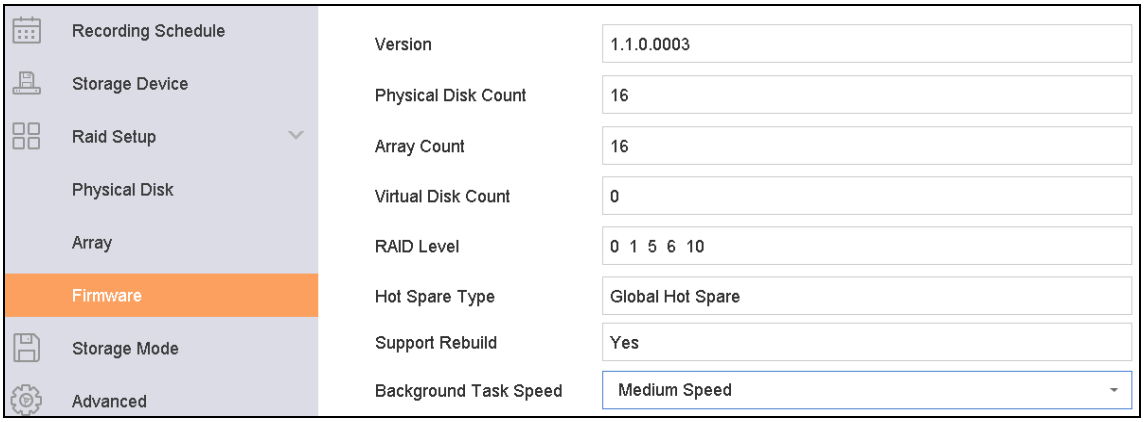


Figure 9-11 Firmware

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

Step 3 Click **Apply**.

Chapter 10 File Management

10.1 Searching and Exporting All Files

10.1.1 Searching Files

Purpose

Specify detailed conditions to search videos and pictures.

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

Step 2 Click **Advanced Search** in the menu bar to specify detailed conditions, including time, camera, event type, etc.

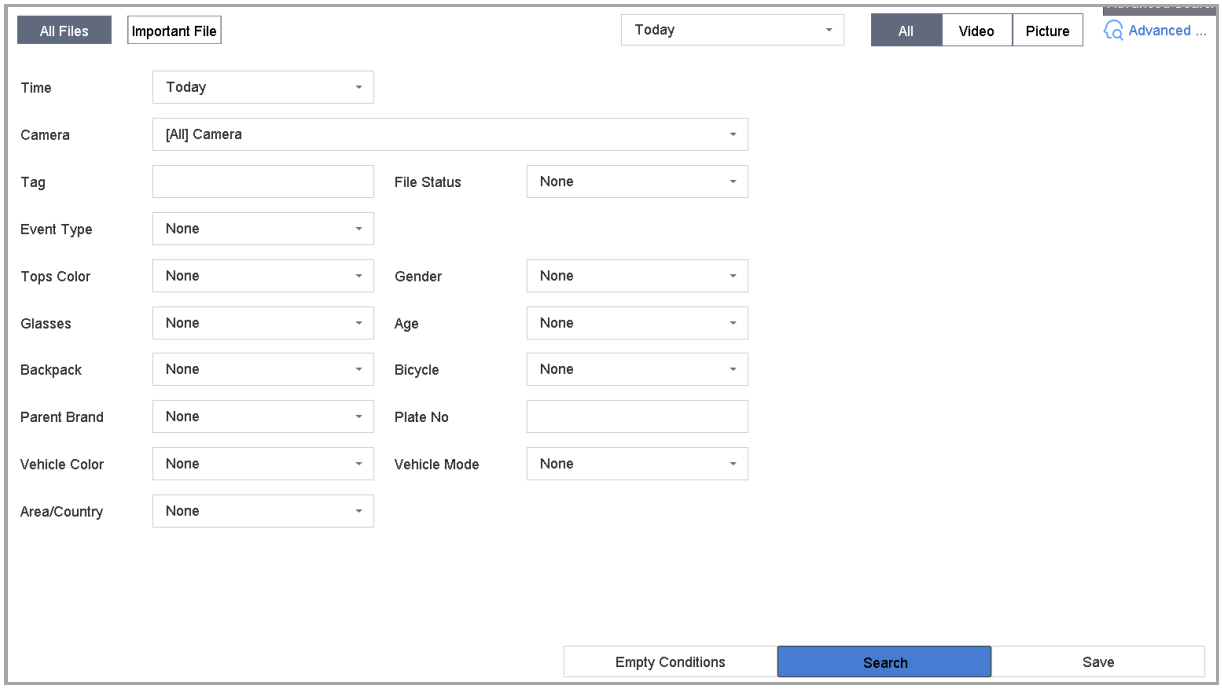


Figure 10-1 Advanced Search

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.
- **Group**: Sort the search results by the selected item.

10.1.2 Exporting 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 vehicle files to export. For details, see 10.1.1 Searching Files.

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

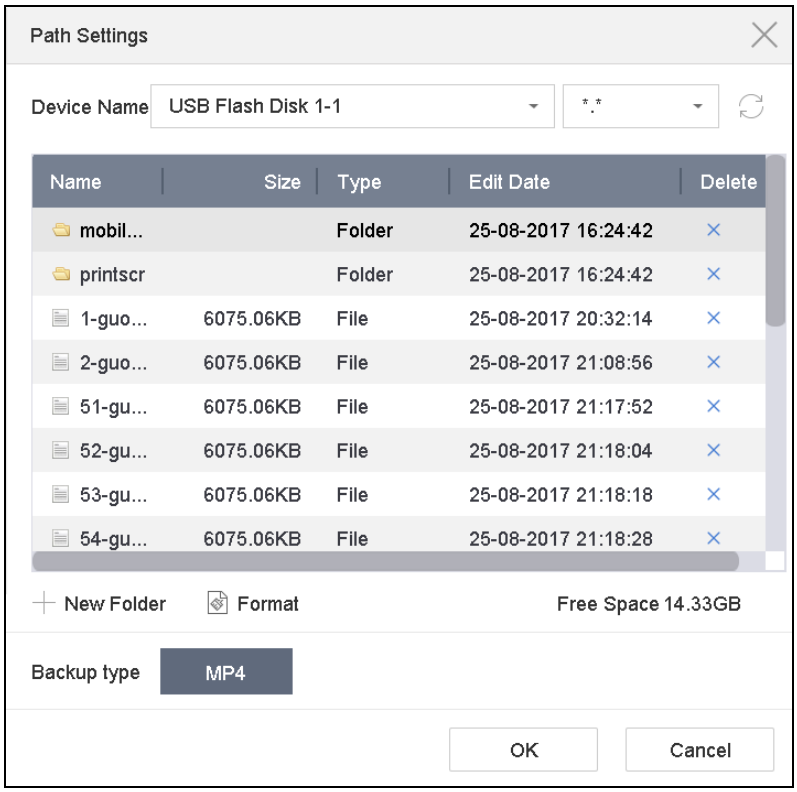


Figure 10-2 Export Files

Step 3 Click **OK** to export pictures to the backup device.

10.2 Searching and Exporting Human Pictures

10.2.1 Searching Human Pictures

Purpose

Specify detailed conditions by which to search human pictures.

Before You Start

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

Step 1 Go to **File Management > People Appearance File**.

Step 2 Click **Advanced Search** in the menu bar to specify detailed conditions, including time, camera, people appearance, etc.

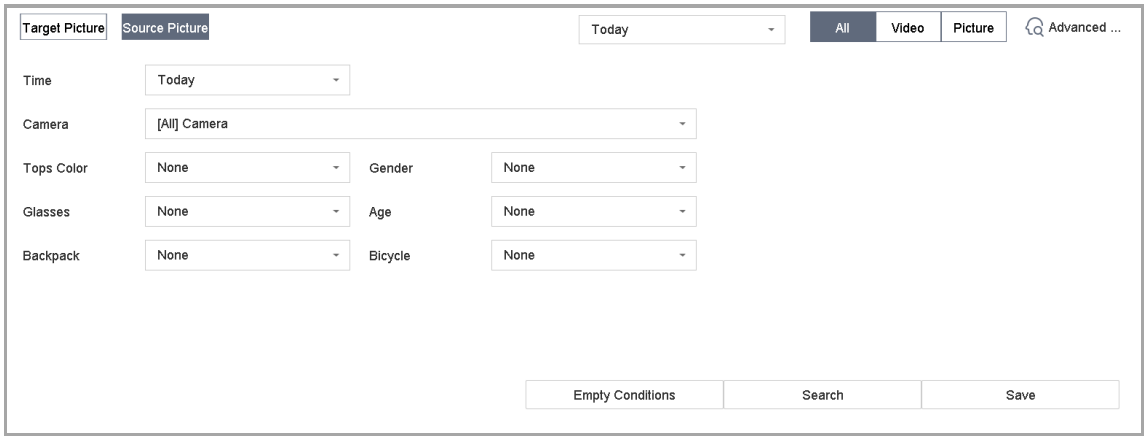


Figure 10-3 Advanced Search

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

10.2.2 Exporting Human Pictures

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 Searching Human Pictures.

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

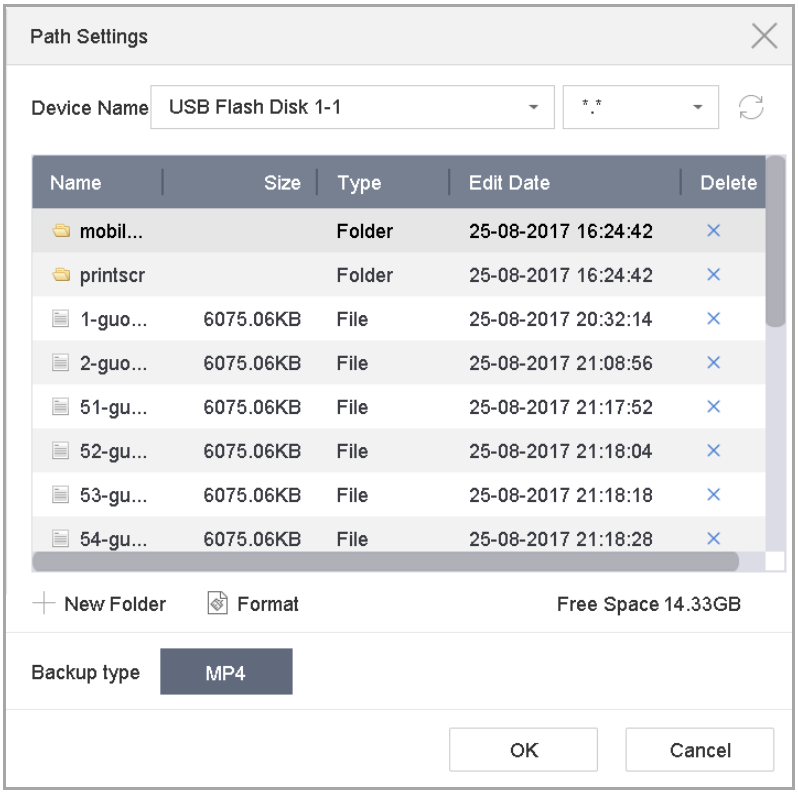


Figure 10-4 Export Files

Step 3 Click **OK** to export pictures to the backup device.

10.3 Searching and Exporting Vehicle Files

10.3.1 Searching Vehicle Pictures

Purpose

Specify detailed conditions by which to search vehicle pictures.

Before You Start

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

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

Step 2 Click **Advanced Search** in the menu bar to specify detailed conditions, including time, camera, vehicle appearance, etc.

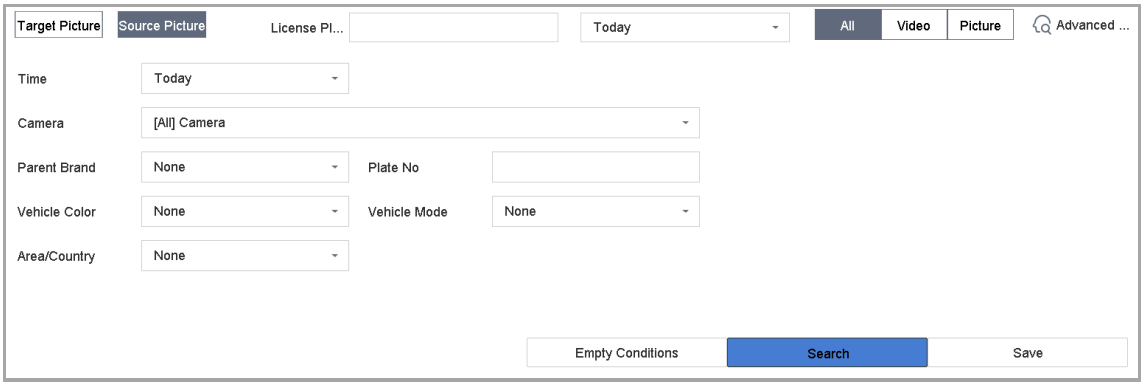


Figure 10-5 Advanced Search

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.
- **Group**: Sort the search results by selected item.

10.3.2 Exporting Vehicle Pictures

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 Searching Vehicle Pictures.

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

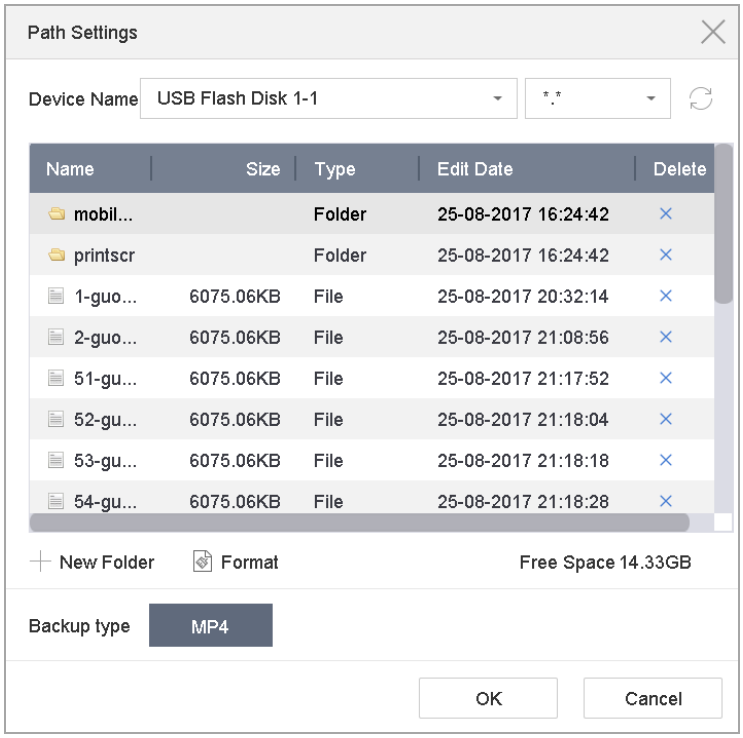


Figure 10-6 Export Files

Step 3 Click **OK** to export pictures to the backup device.

10.4 Searching History Operation

10.4.1 Saving 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 Click **Advanced Search** in the menu bar and set the search conditions.

Step 3 Click **Save**.

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

10.4.2 Calling Search History

Purpose

You can quickly search files by calling the Search History.

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

Step 2 Click a saved search conditon to search files quickly.

Chapter 11 Playback

11.1 Playing Video Files

11.1.1 Instant Playback

Instant Playback enables the device to play video files recorded in the last five minutes. If no video is found, it means there was no 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 Playing Video

Step 1 Go to **Playback**.

Step 2 Select one or more cameras in the camera list.

Step 3 Select a date in the calendar.

Step 4 Click **Play** on the toolbar to start playing the video.

Step 5 You can use the toolbar in the bottom of the playback interface to control the playing and perform a series of operations. Refer to Chapter 11.2 Playback Operations 8.2.

Figure 11-2 Playback Interface

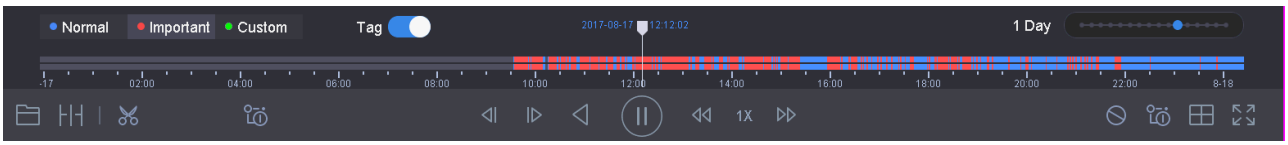


Figure 11-3 Toolbar of Playback

Step 6 You can click the channel(s) to execute simultaneous playback of multiple channels.

NOTE

256x playing speed is supported.

11.1.3 Playing 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 the time point.

Managing 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.

NOTE

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

Playing Tag Files

Step 5 Go to **Playback**.

Step 6 Click **Tag** button.

Step 7 Click **Custom Search** on the left bottom to enter the Search Condition interface.

Step 8 Click **Smart Search** on the top right corner.

Step 9 Enter the search conditions for the tag files, including the time and the tag keyword.

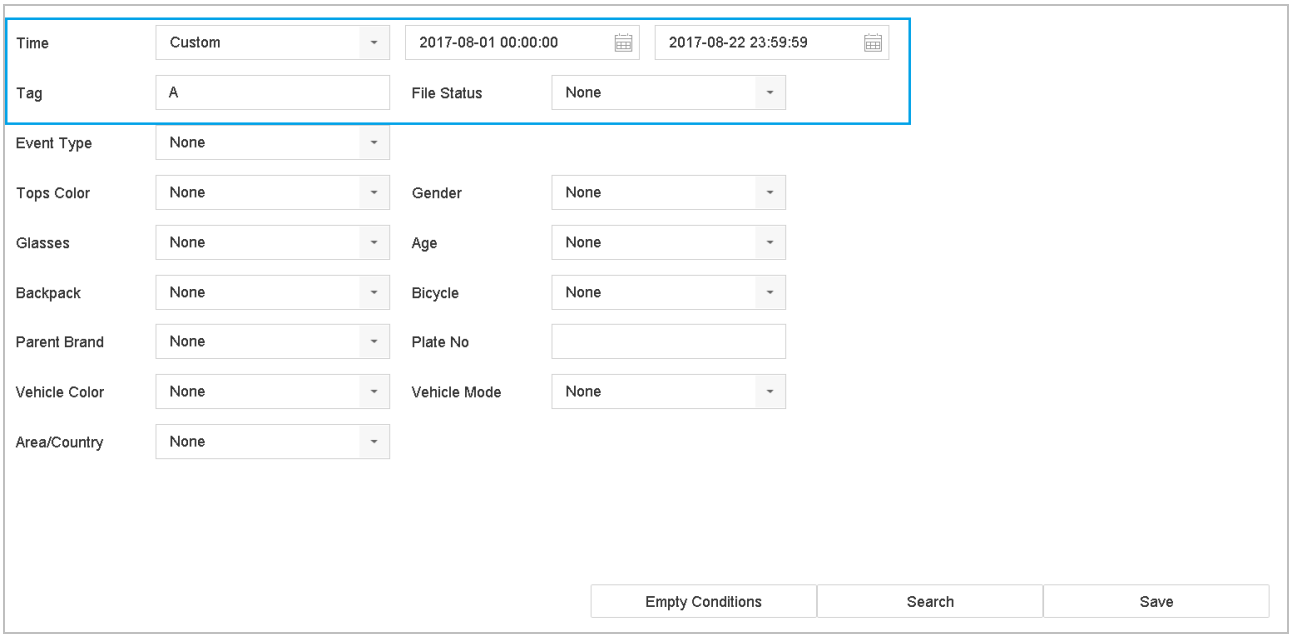


Figure 11-4 Tag Search

Step 10 Click **Search**.

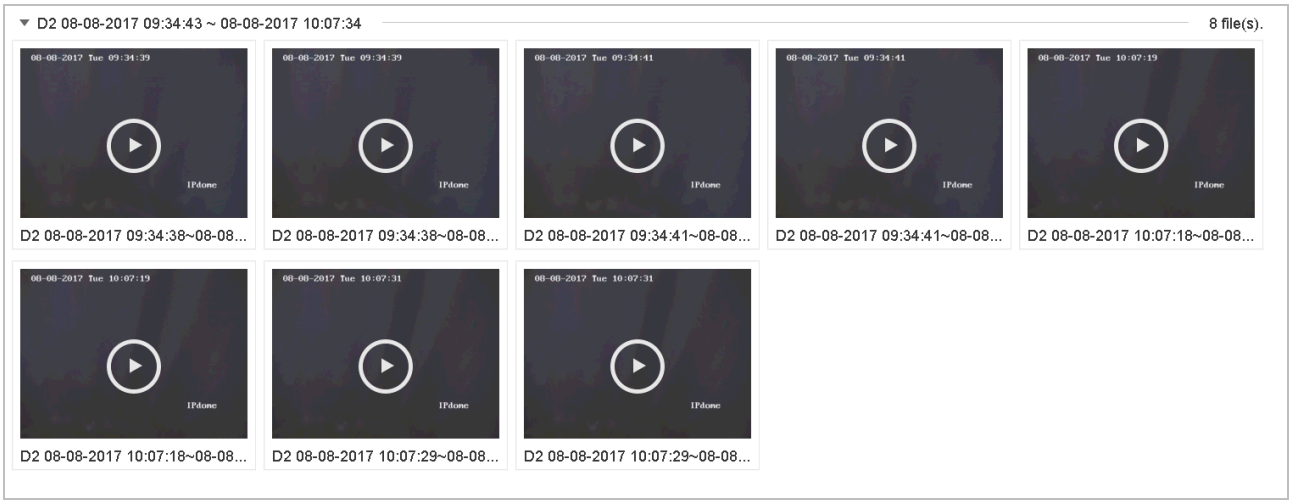


Figure 11-5 Searched Tag Files

Step 11 On the search results interface, select a tag file and click to start playing the video.

Figure 11-6 Tag Playback

11.1.4 Playing by Smart Search

Purpose

In Smart Playback mode, the device will analyze the video containing the motion, line, or intrusion detection information, mark it in green, and play it at normal speed. Video without motion will be played in at 16x speed.

The smart playback rules and areas are configurable.

Step 1 Go to **Playback**.

Step 2 Start playing the video files by channel or by time.

Step 3 From the toolbar at the bottom of the playing window, click the motion/line crossing/intrusion icon for search.

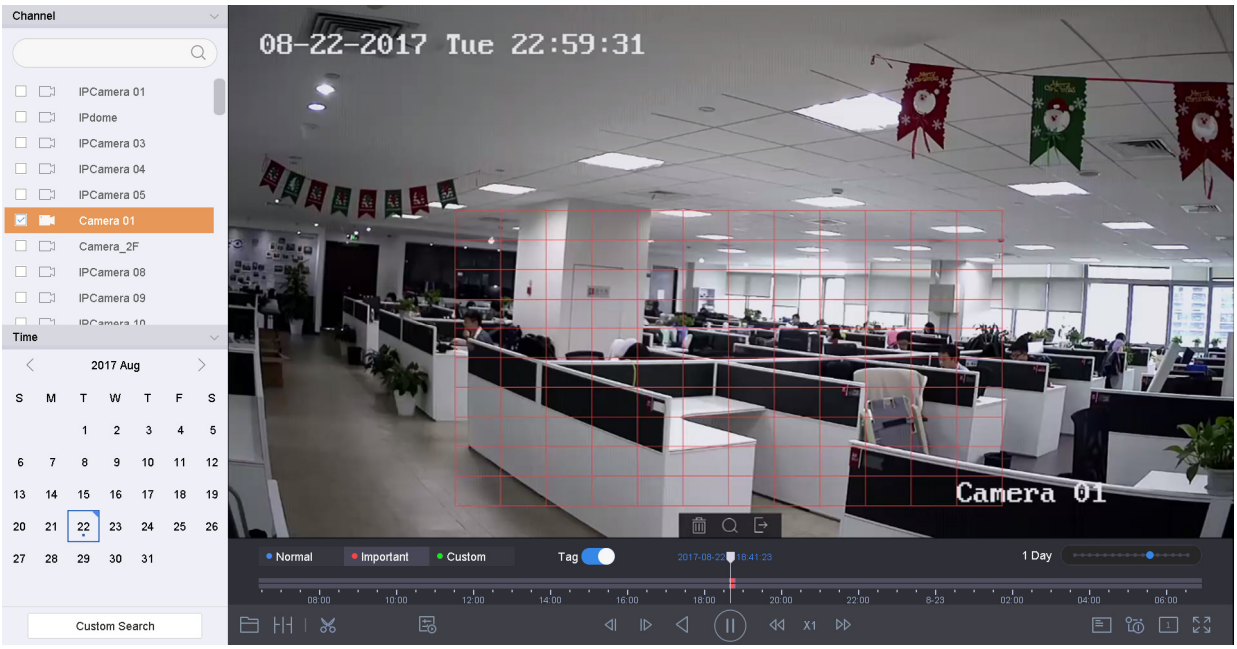


Figure 11-7 Playback by Smart Search

Step 4 Set the rules and areas for smart search by line crossing detection, intrusion detection or motion detection event triggered recording.

- **Line Crossing Detection**

  1) Click the  icon.

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

- **Intrusion Detection**

  1) Click the  icon.

  2) Specify four points to set a quadrilateral region for 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  to search the matched video and start to play it.

11.1.5 Playing Event Files

Purpose

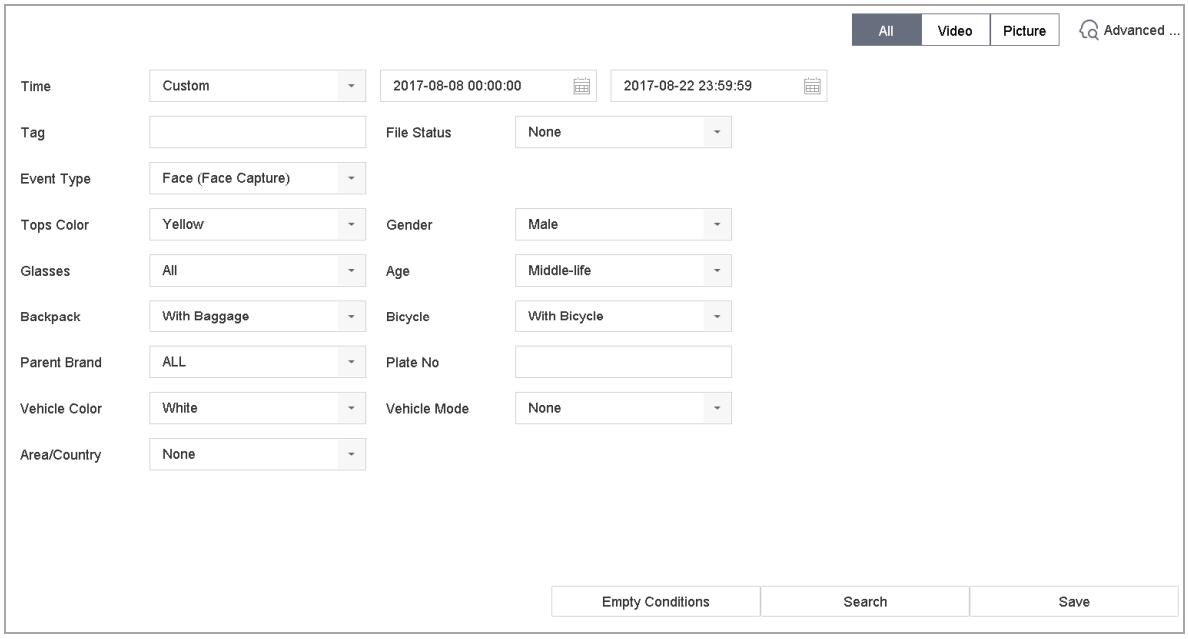
Play back video files on one or several channels searched by event type (e.g., alarm input, motion detection, line crossing detection, face detection, vehicle detection, etc.).

Step 1 Go to **Playback**.

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

Step 3 Click **Smart Search** on the top right corner.

Step 4 Enter the search conditions for the event files, e.g., time, event type, file status, people appearance (for face detection, human detection, etc.), and vehicle information (for vehicle detection event).



Step 5 Click **Search**.

Step 6 On the search results interface, select an event video file/picture file and click it to start playing the video or double-click it to play the picture.

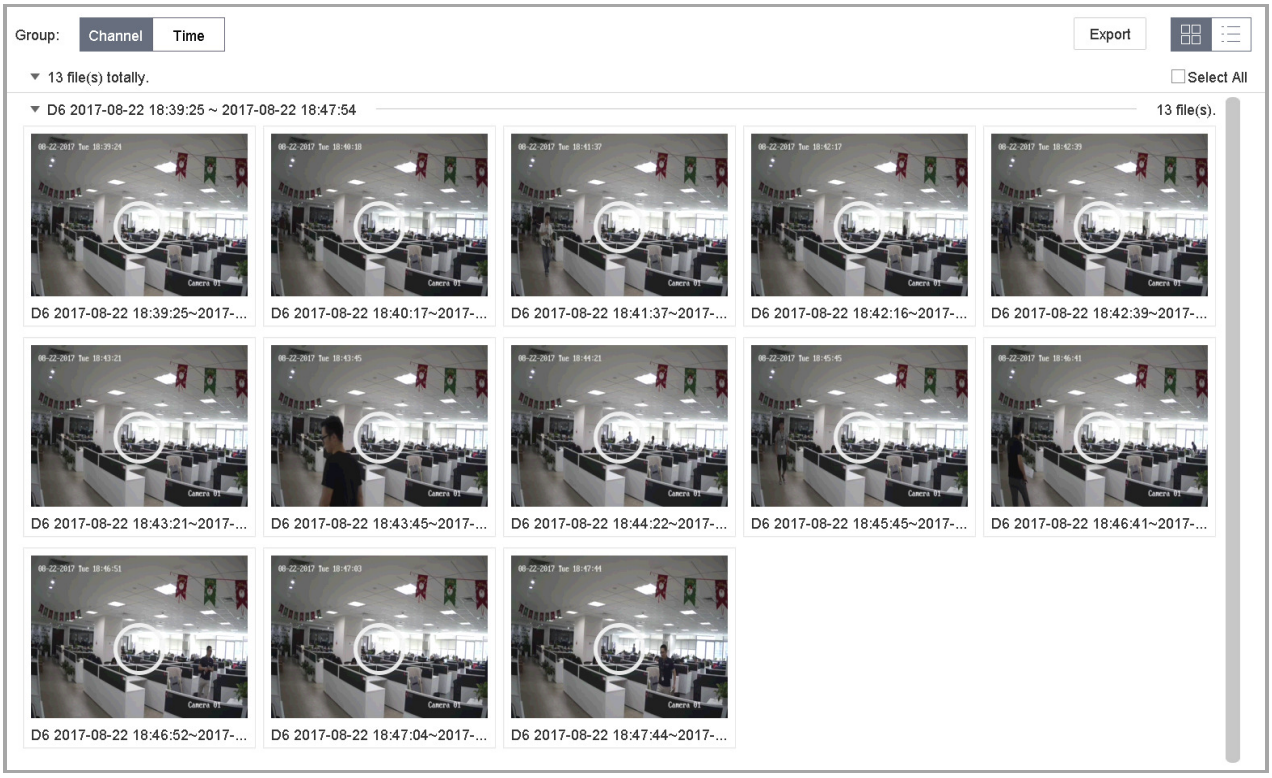


Figure 11-8 Event Files

Step 7 Click  or  to select the previous or next event.

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

Configuring Event Triggered Recording for the event triggered recording/capture settings.

11.1.6 Playing 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 **Sub-periods** from the drop-down list in the upper-left corner of the page to enter the Sub-Periods Playback interface.

Step 3 Select a date and start playing the video file. Select the Split-Screen Number from the drop-down list. Up to 16 screens are configurable.

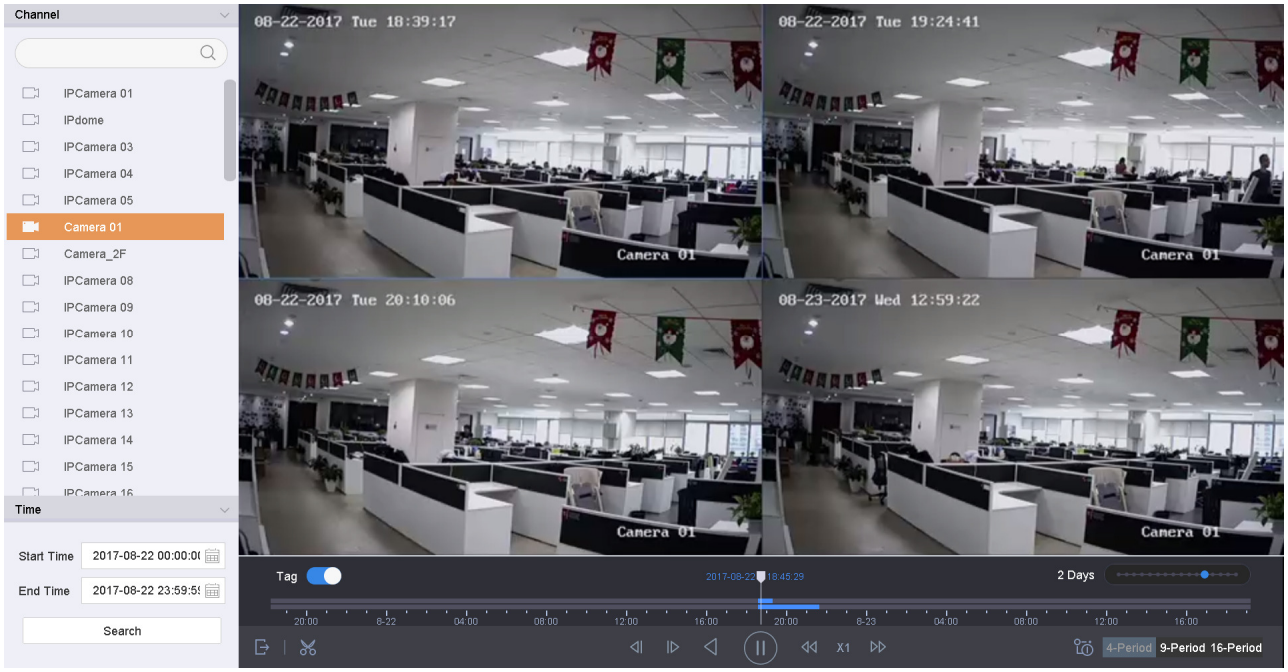


Figure 11-9 Interface of Sub-periods Playback

NOTE

According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if 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.

11.1.7 Playing 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 the **Log Search** tab to enter Playback by System Logs.

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

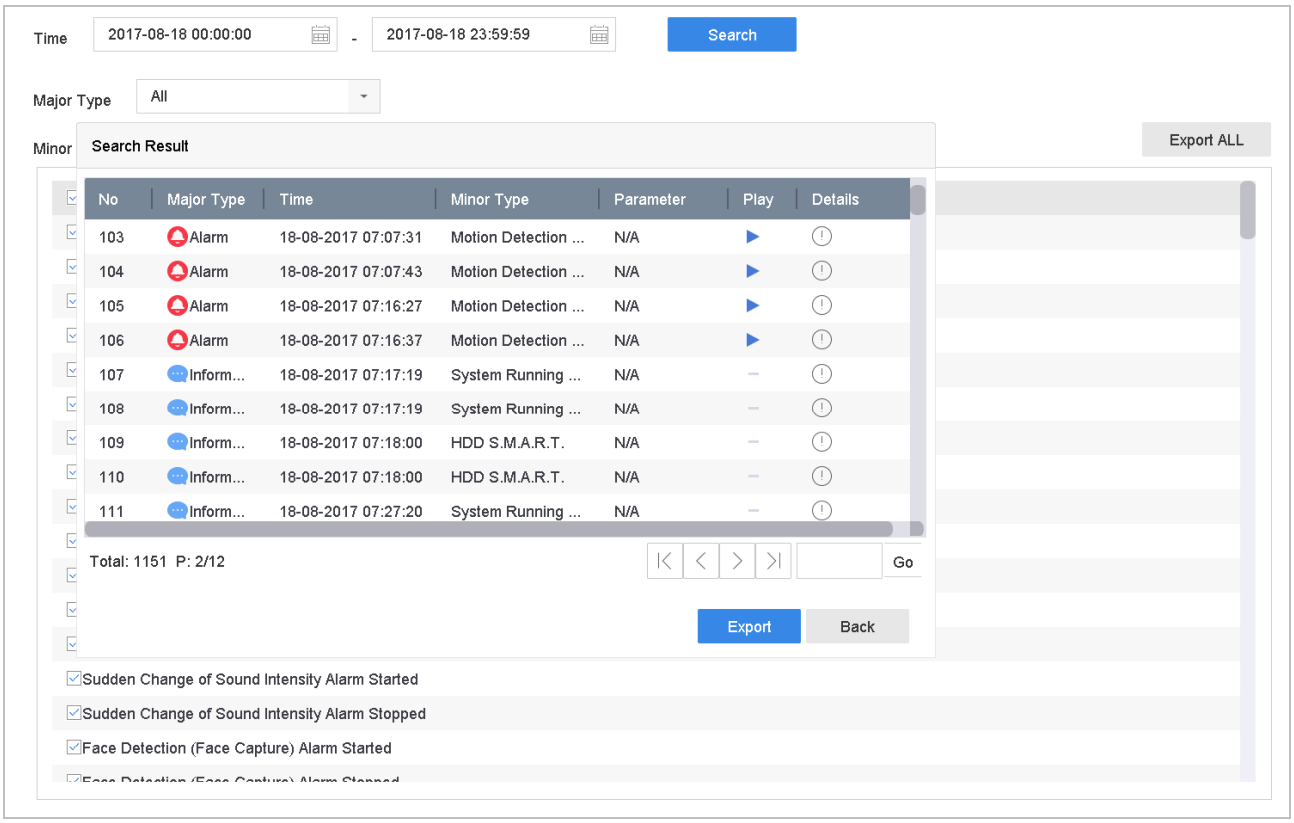


Figure 11-10 System Log Search Interface

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

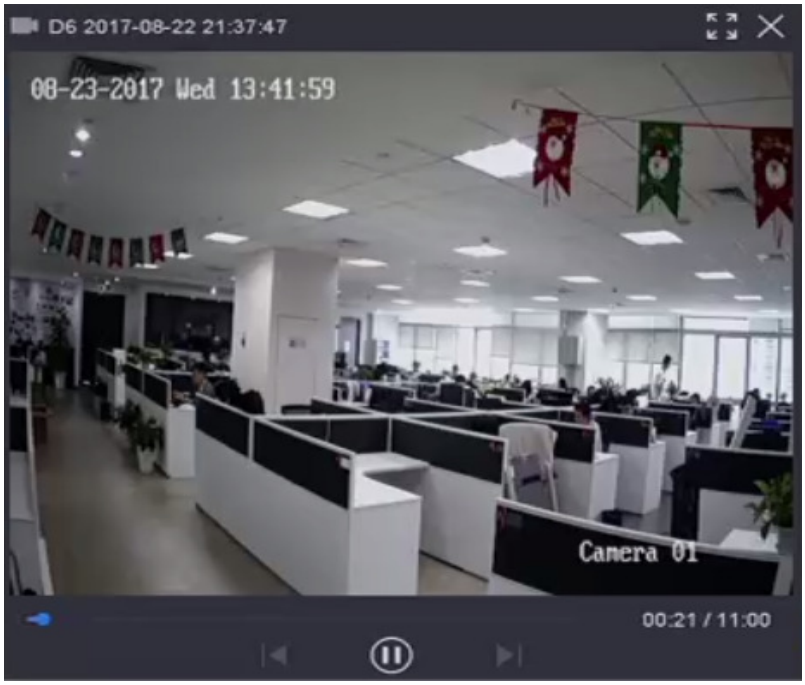


Figure 11-11 Interface of Playback by Log

11.1.8 Playing 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  or double-click to play the file.

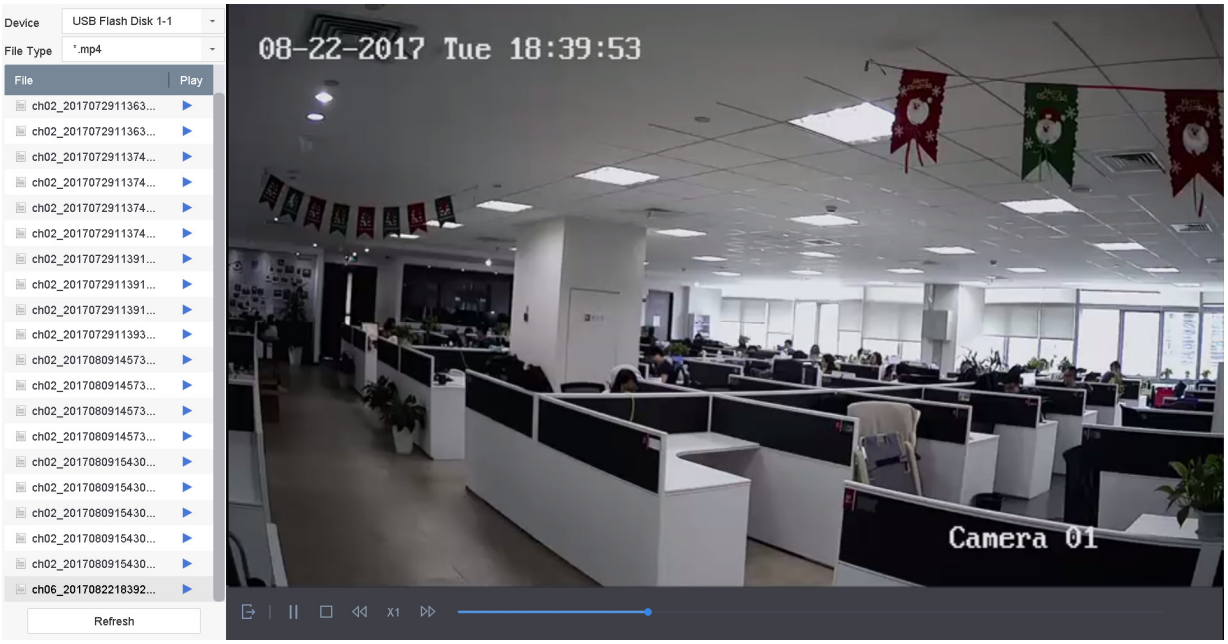


Figure 11-12 External File Playback

11.2 Playback Operations

11.2.1 Normal/Important/Custom Video

During playback, you can select the following three modes to play the video.

- **Normal:** Video files from continuous recordings
- **Important**: Video files from event and alarm recording triggered recordings
- **Custom**: Video files searched by custom conditions

11.2.2 Setting Play Strategy in Important/Custom Mode

Purpose

In the Important/Custom video playback mode, you can set the playing speed separately for normal video and important/custom video, or you can select to skip the normal video.

Step 1 In the Important/Custom video playback mode, click  to set the play strategy.

- When **Do not Play Normal Videos** is checked, the device will skip the normal video and play the important (event) video and the custom (searched video) only, in normal speed (x1).
- When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video and the important/custom video separately. The speed range is from x1 to xMAX.

NOTE

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

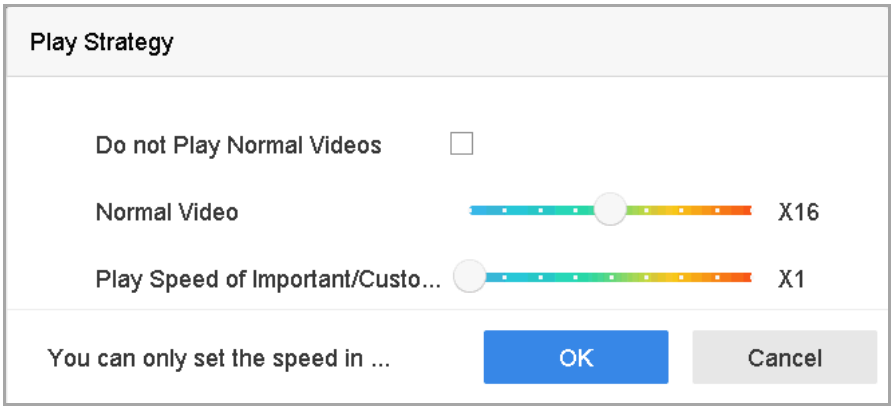


Figure 11-13 Play Strategy

11.2.3 Editing Video Clips

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

Step 1 In Video Playback mode, click  to start the video clipping operation.

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

11.2.4 Switching 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**.

11.2.5 Thumbnails View

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

In the Video Playback mode, move the mouse to the time bar to preview thumbnails of the video files.

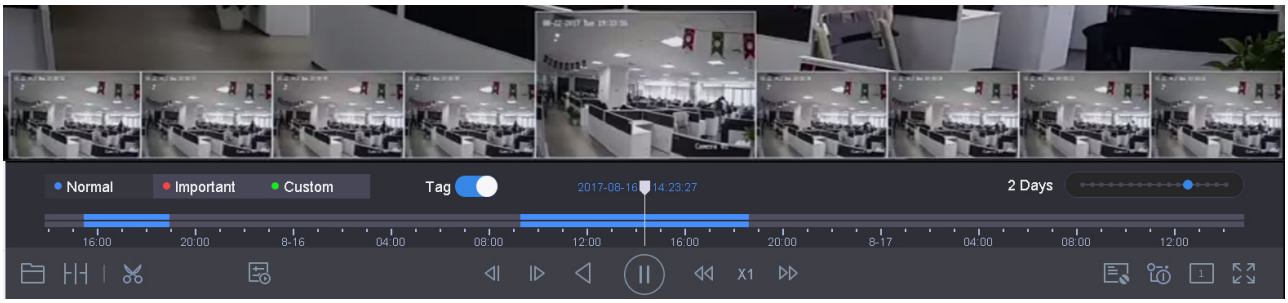


Figure 11-14 Thumbnails View

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

NOTE

Thumbnail view is supported only in 1x single-camera playback mode.

11.2.6 Fisheye View

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

Step 1 Click to enter the fisheye expansion mode.

- **180° Panorama ( ):** Switch the Live View image to the 180° panorama view.

- **360° Panorama (** **)**: Switch 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.

11.2.7 Fast View

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

Step 1 In Video Playback mode, hold and drag the mouse through the playing time bar to fast view the video files.

Step 2 Release the mouse at the required time point to enter full-screen playback.

NOTE

Fast view is supported only in the 1x single-camera playback mode.

11.2.8 Digital Zoom

Step 1 In Video Playback mode, click in the toolbar to enter the digital zoom interface.

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

Figure 11-15 Digital Zoom

11.2.9 POS Information Overlay

In 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 overlayed on the video.

Chapter 12 Event and Alarm Settings

12.1 Configuring Arming Schedule

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

Step 2 Choose 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 overlap.

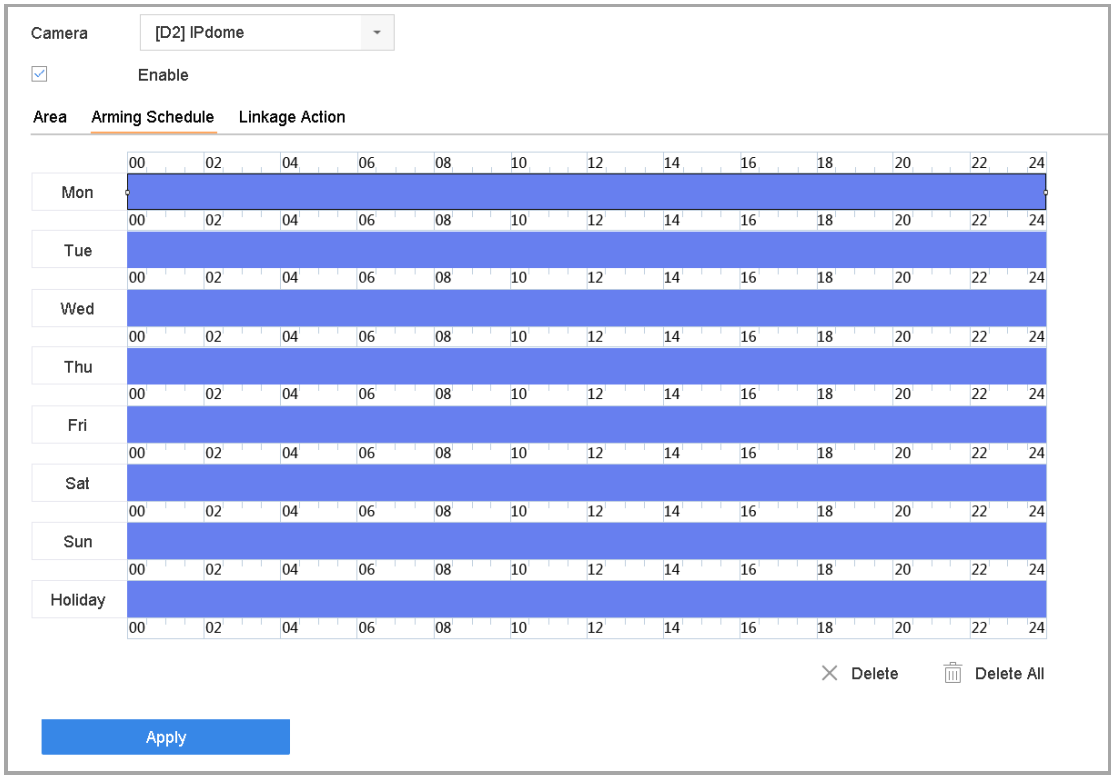


Figure 12-1 Set Arming Schedule

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

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

12.2 Configuring Alarm Linkage Actions

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

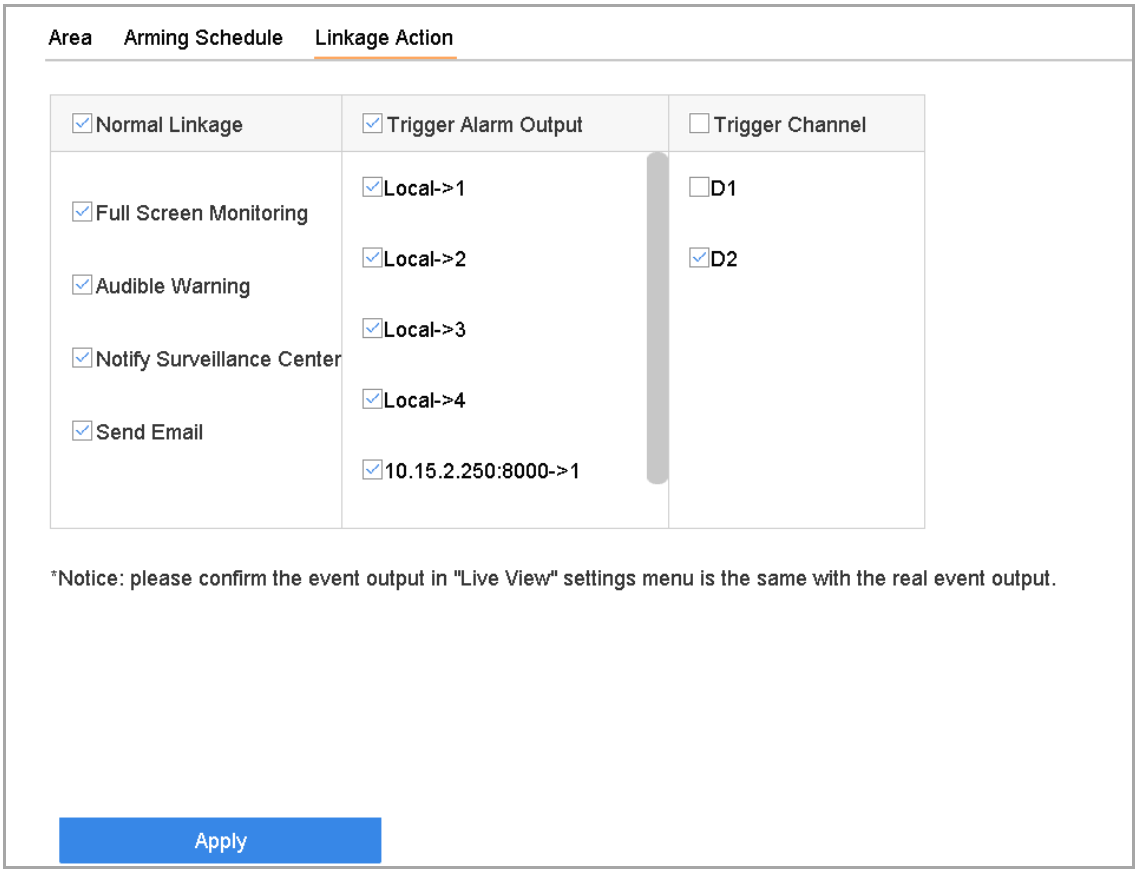


Figure 12-2 Set Linkage Actions

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. Refer to Chapter 16.8 Configure Ports for alarm host configuration.

- **Send Email**

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

  Refer to 16.7 Configuring E-Mail for 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, refer to Chapter 12.6.3 Configuring 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 Configuring Recording Schedule for setting the recording schedule.

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

12.3 Configuring Motion Detection Alarms

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

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

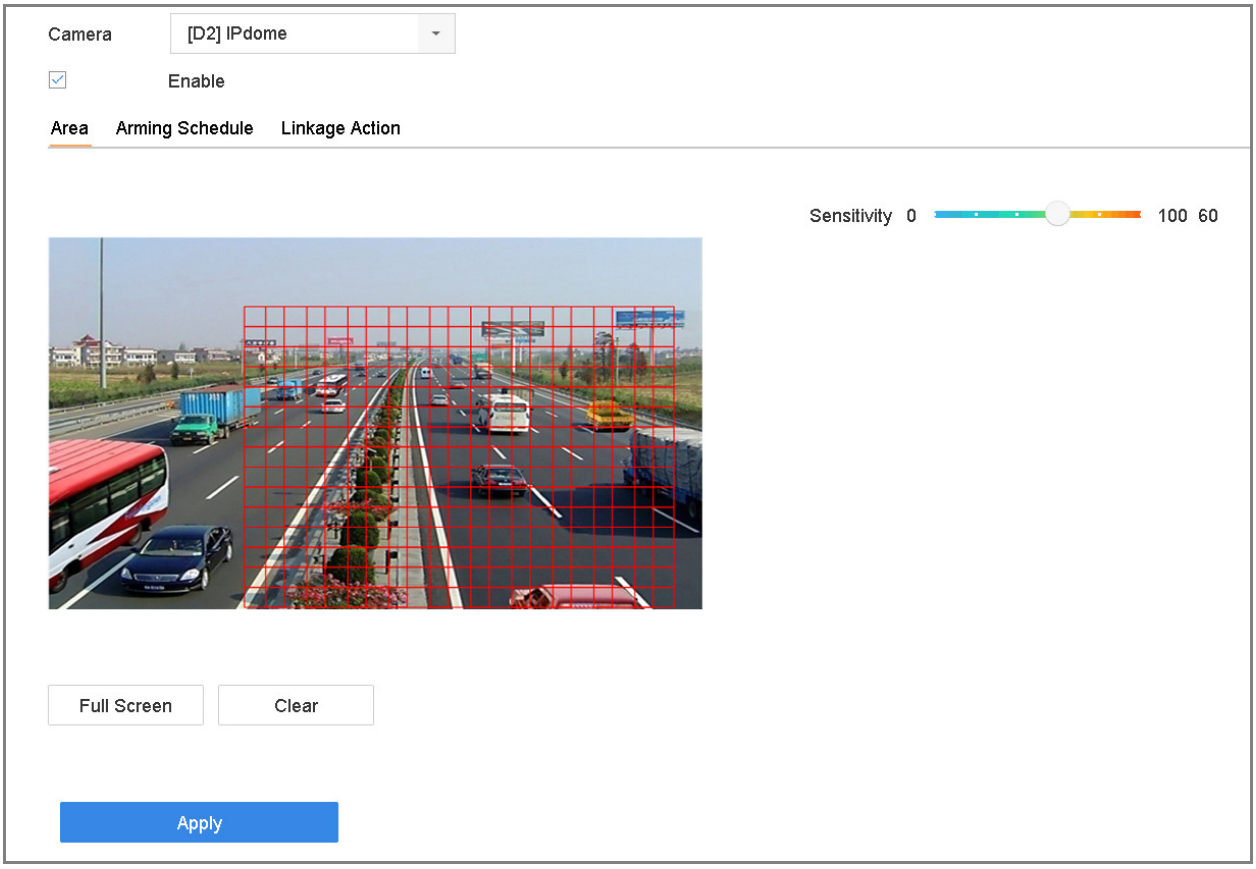


Figure 12-3 Set Motion Detection

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 full-screen motion detection for the image.
- **Customized area:** Click-and-drag the mouse 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 more readily triggers motion detection.

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

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

12.4 Configuring 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**.

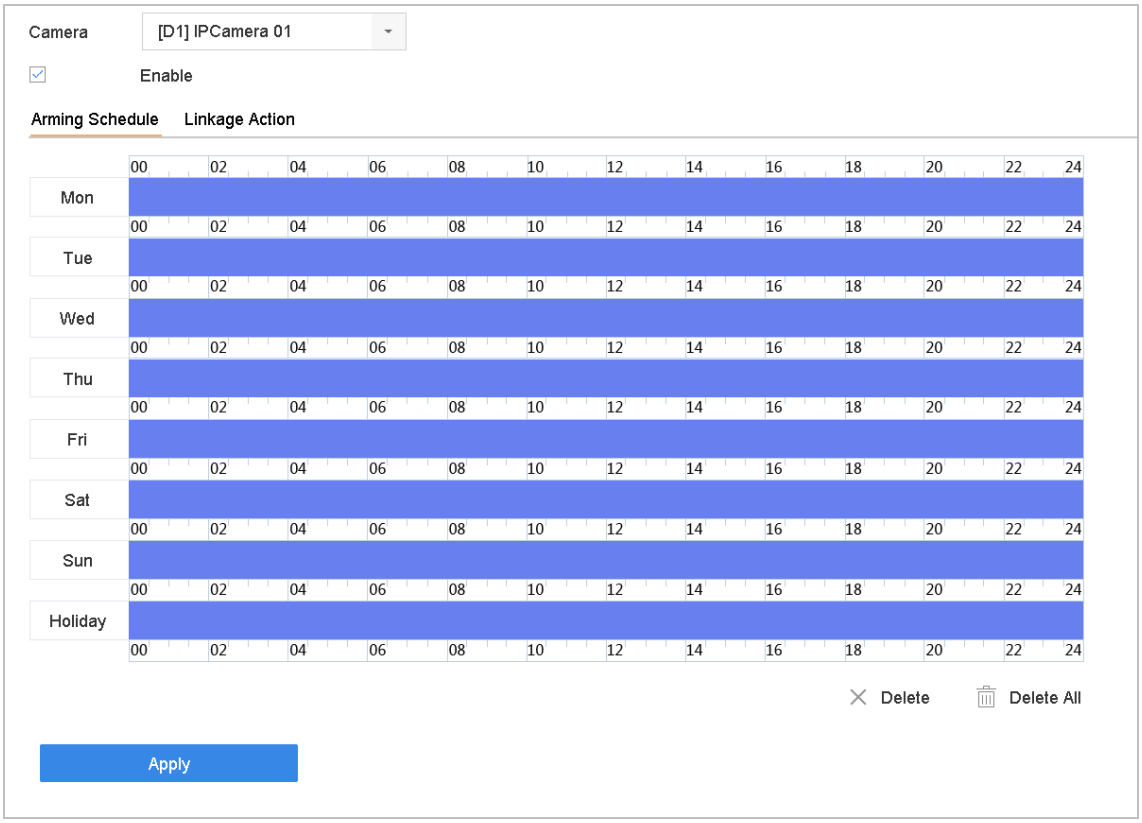


Figure 12-4 Set Video Loss Detection

Step 2 Select the camera to configure video loss detection.

Step 3 Check **Enable**.

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

Step 5 Set the linkage actions. Refer to Chapter 12.2 Configuring Alarm Linkage Actions.

12.5 Configuring Video Tampering Alarms

Purpose

Video Tampering Detection triggerd 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.

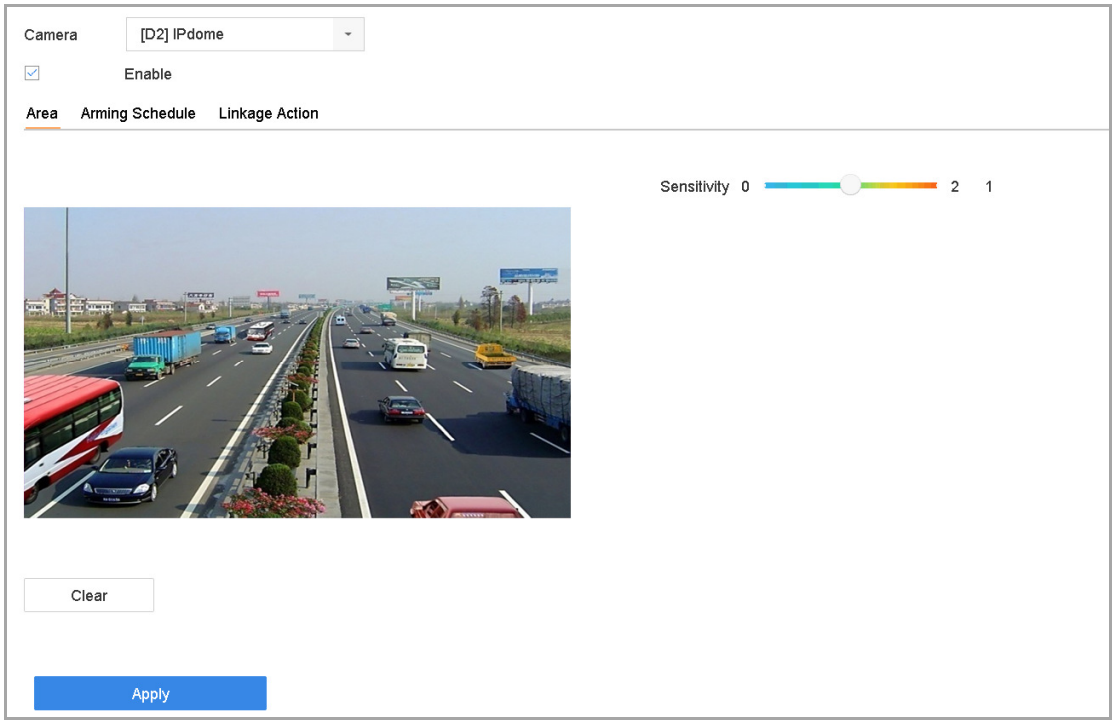


Figure 12-5 Set Video Tampering Setting

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). Three 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 Configuring Arming Schedule.

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

12.6 Configuring Sensor Alarms

Purpose

Set the handling action of an external sensor alarm.

12.6.1 Configuring Alarm Inputs

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

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

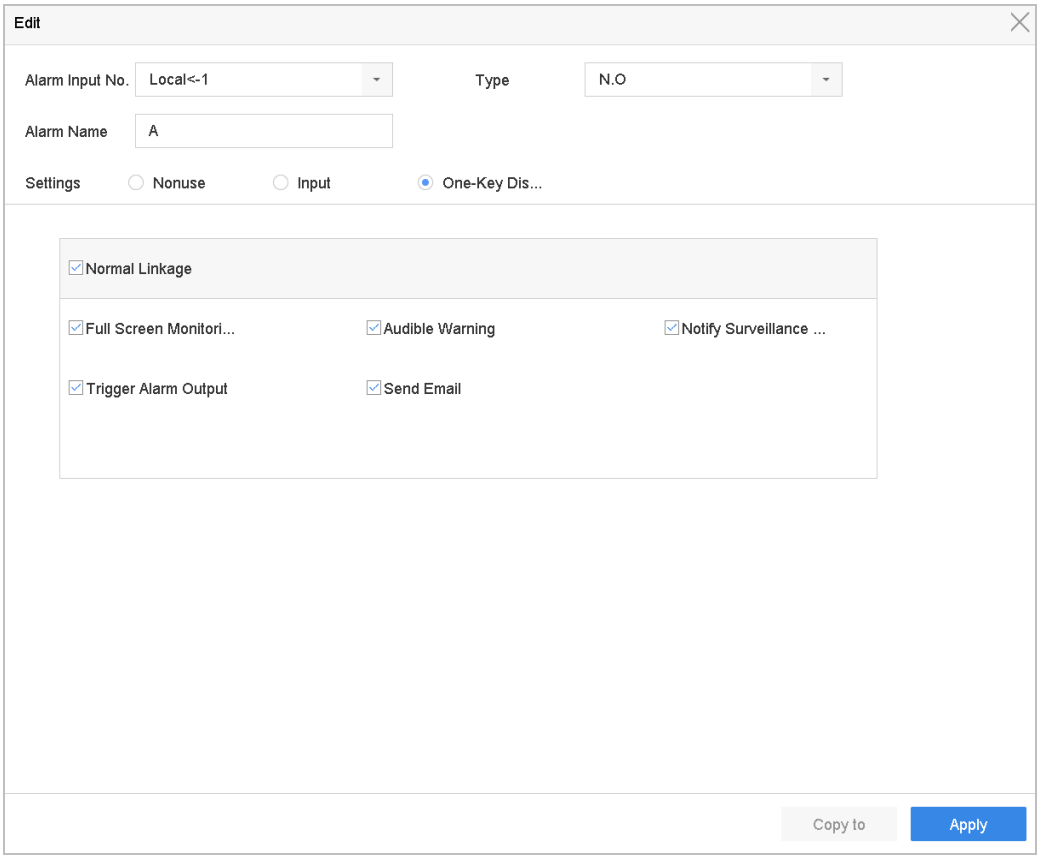


Figure 12-6 Alarm Input

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

Step 4 Edit the alarm name.

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

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

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configuring Alarm Linkage Actions.

12.6.2 Configuring One-Key Disarming

One-Key Disarming disarms 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 the **Enable One-Key Disarming** radio button.

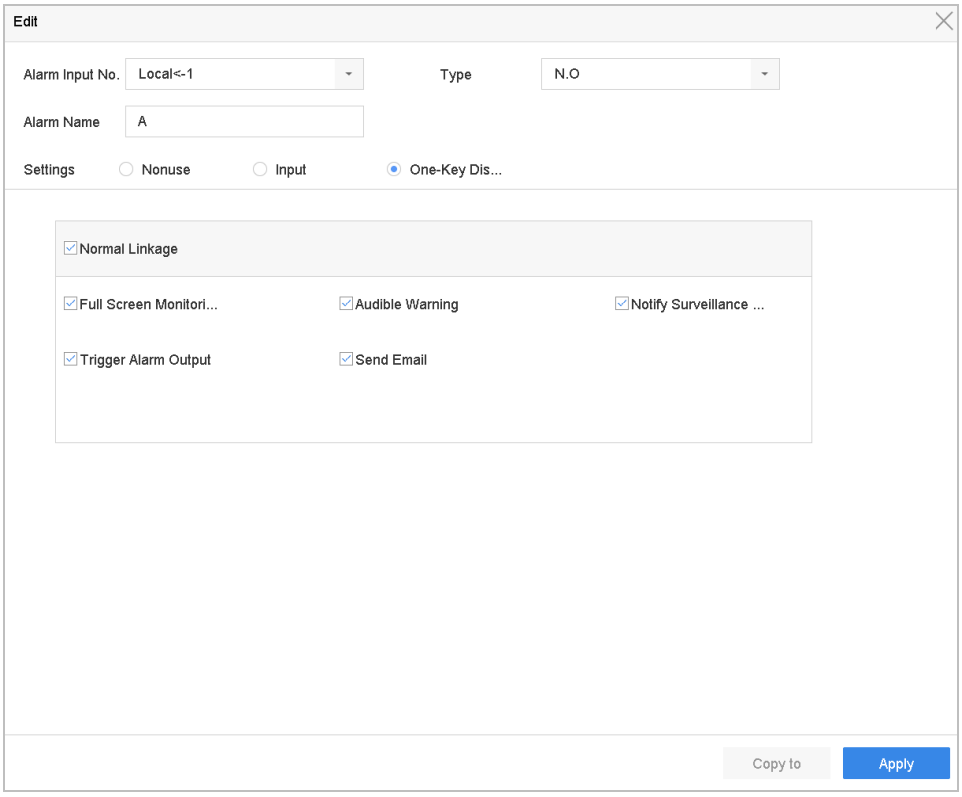


Figure 12-7 One-Key Alarm Disarming

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 Configuring 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**.

Step 5 **Manually Clear**: You should manually clear the alarm when the alarm occurs. Refer to Chapter 12.9 Triggering or Clearing Alarm Output Manually for detailed instructions.

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

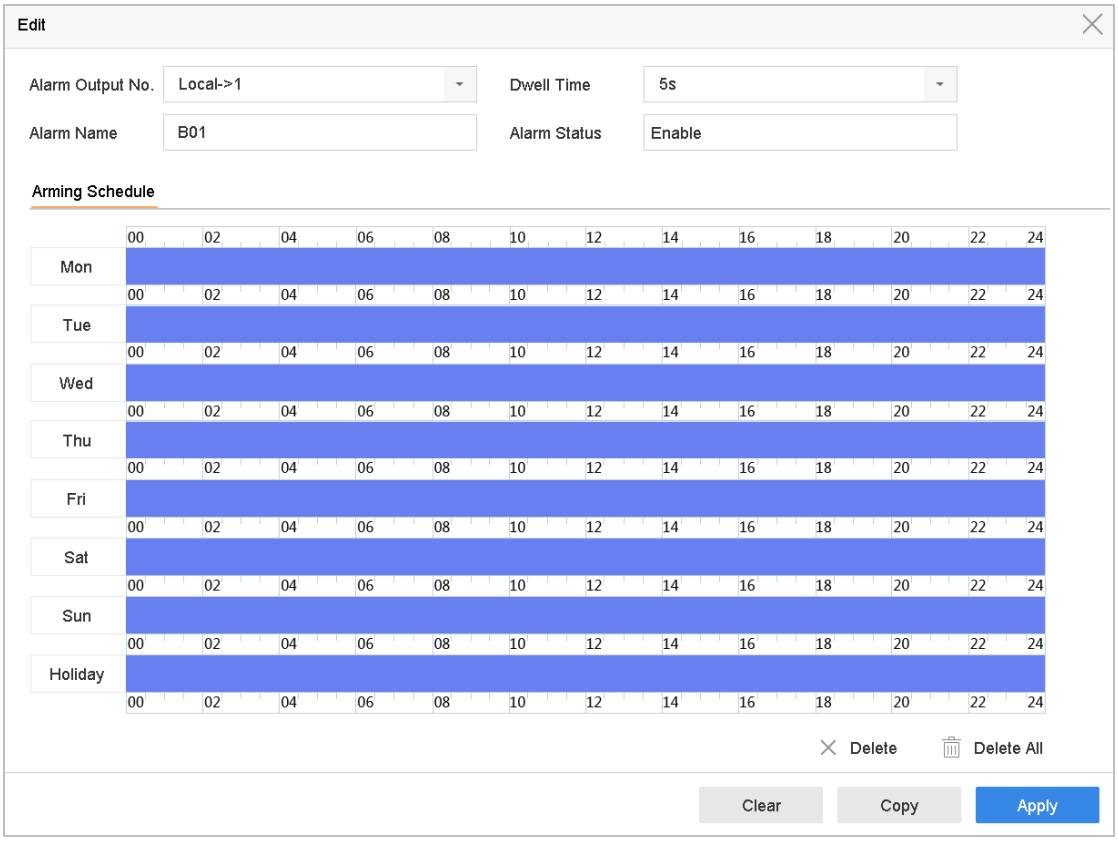


Figure 12-8 Alarm Output

Step 7 (Optional) Click **Copy** to copy the same settings to other alarm output(s).

12.7 Configuring 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 the **Enable Event Hint** checkbox.

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

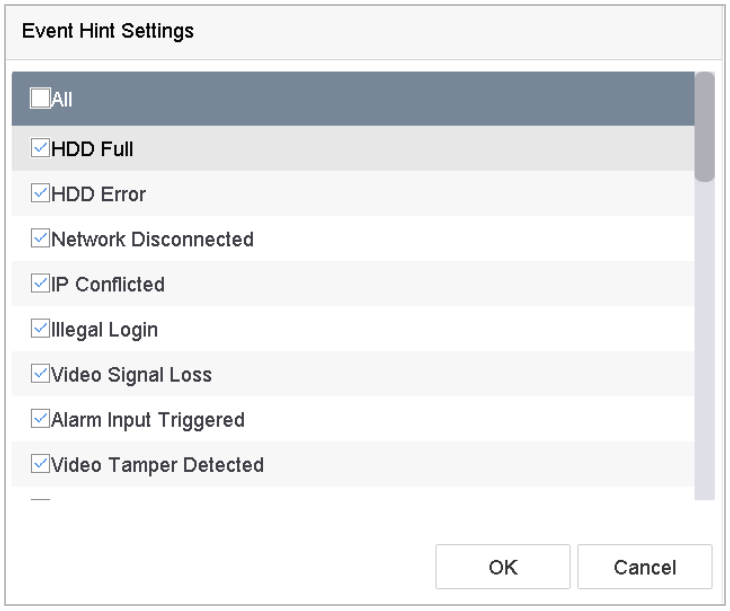


Figure 12-9 Event Hint Settings

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

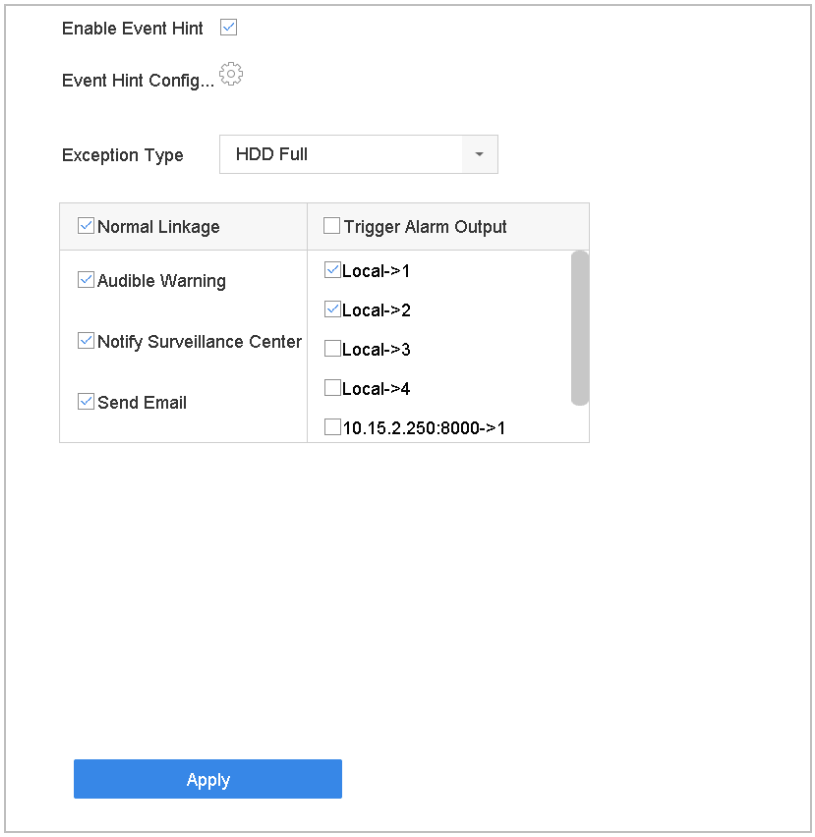


Figure 12-10 Exceptions Handling

Step 4 Set the normal linkage and alarm output triggering. Refer to Chapter 10.2 Setting Alarm Linkage Actions.

12.8 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.

12.8.1 Configuring 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) you want for full screen monitoring in **Trigger Channel** settings.

NOTE

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

12.8.2 Configuring Audio Warning

The audio warning has the system 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.

12.8.3 Notifying Surveillance Center

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

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.

12.8.4 Configuring E-Mail Linkage

The system can send an e-mail with alarm information to a user or users when an alarm is detected. Refer to Chapter 16.7 Configuring E-Mail for details of e-mail 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.

12.8.5 Triggering Alarm Outputs

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

Step 1 Go to the **Linkage Action** interface of the alarm input or event 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.

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

12.8.6 Configuring PTZ Linkage

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

NOTE

Make sure the connected PTZ or speed dome 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.

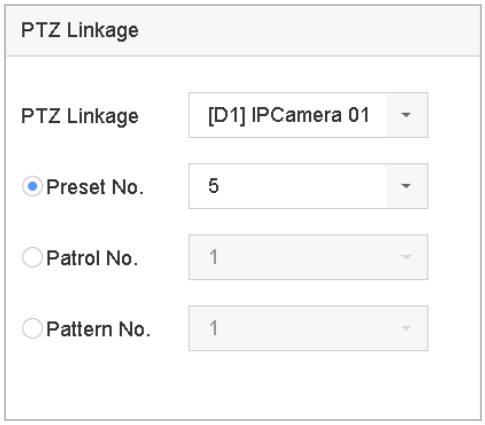


Figure 12-11 PTZ Linkage

NOTE

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

12.9 Triggering or Clearing Alarm Output Manually

Purpose

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

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.

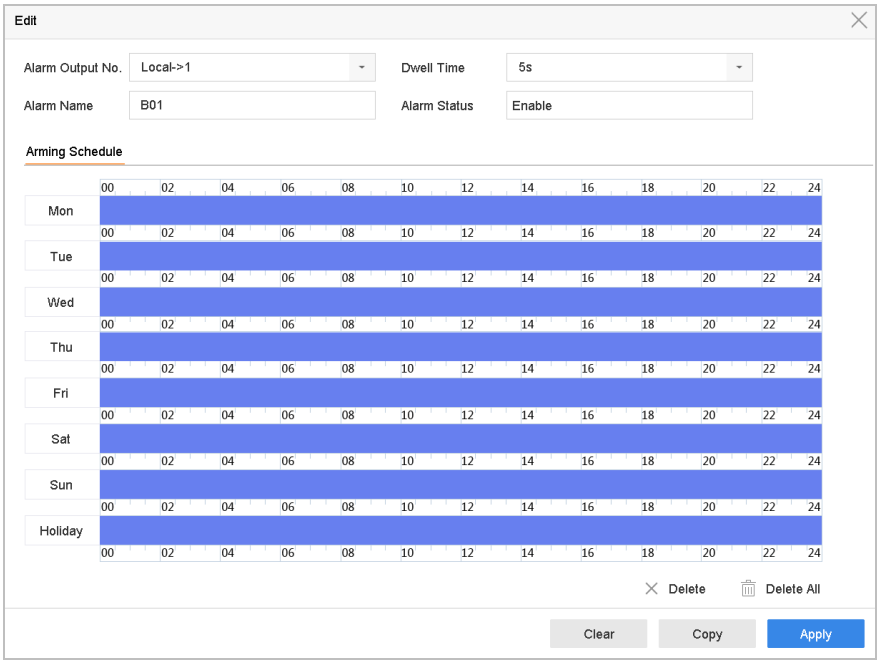


Figure 12-12 Alarm Output

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 faces 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 Click Face Detection.

Figure 13-1 Face Detection

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

Step 4 Check Enable Face Detection.

Step 5 Optionally, 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, the more easily the face will be detected.

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

Step 8 Set the linkage actions. Refer to Chapter 12.2 Configuring 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 Click **Vehicle**.

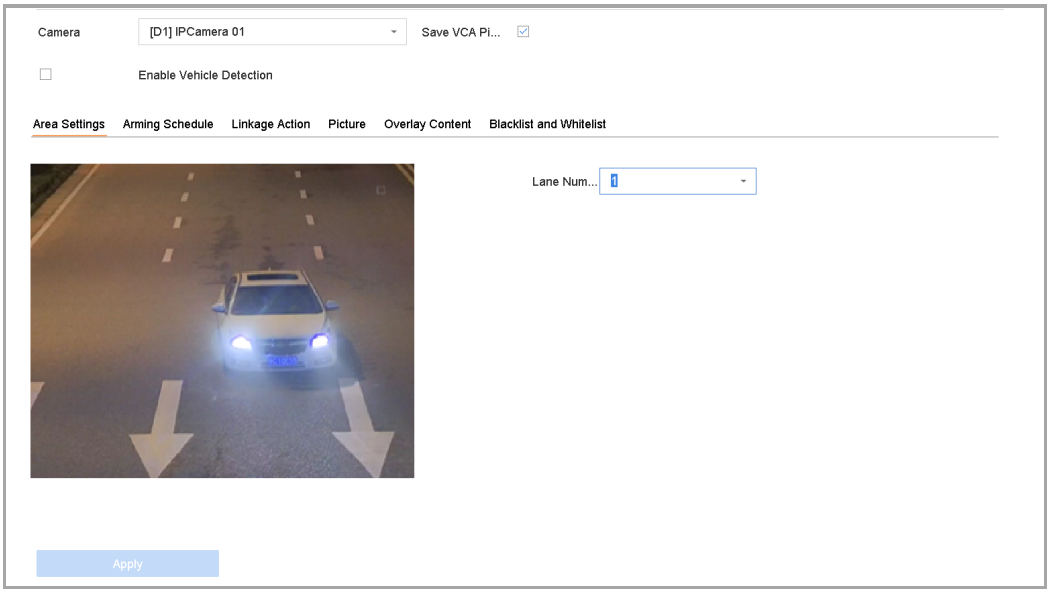


Figure 13-2 Vehicle Detection

Step 3 Select a camera to configure.

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 Configuring Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configuring Alarm Linkage Actions.

Step 8 Configure rules, including **Area Settings, Picture, Overlay Content**, and **Blacklist and Whitelist**. Area Settings: Up to four lanes are selectable.

Step 9 Click **Save**.

NOTE

Refer to the Network Camera user manual for detailed instructions for 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 Click Line Crossing.

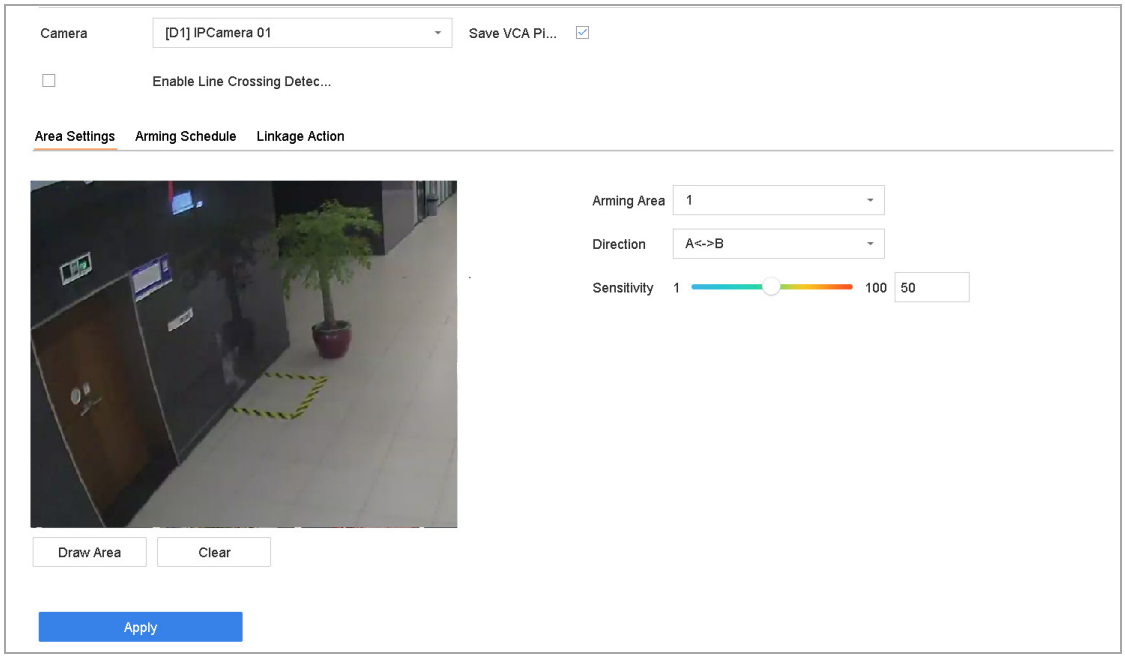


Figure 13-3 Line Crossing Detection

Step 3 Select a camera to configure.

Step 4 Check the Enable Line Crossing Detection checkbox.

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

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

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

2) 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) Drag the Sensitivity slider to set the detection sensitivity. The higher the value, the more easily the detection alarm will be triggered.

4) Click Draw Region and set two points in the preview window to draw a virtual line.

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

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

Step 9 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 Click Intrusion.

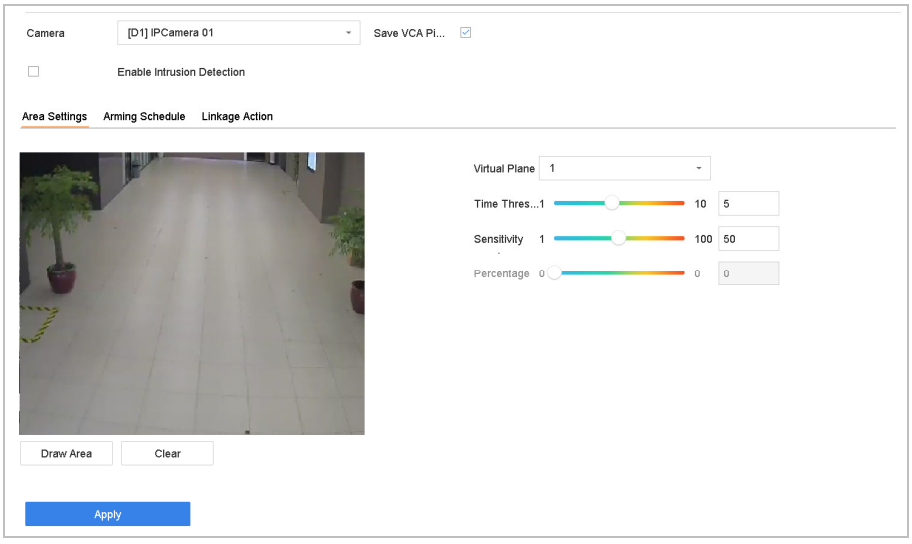


Figure 13-4 Intrusion Detection

Step 3 Select a camera to configure.

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 a Virtual Panel to configure. Up to four virtual panels are selectable.

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

Time Threshold: The time an object can 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, 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 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 Configuring Arming Schedule.

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

Step 9 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 the **Region Entrance Detection** item.

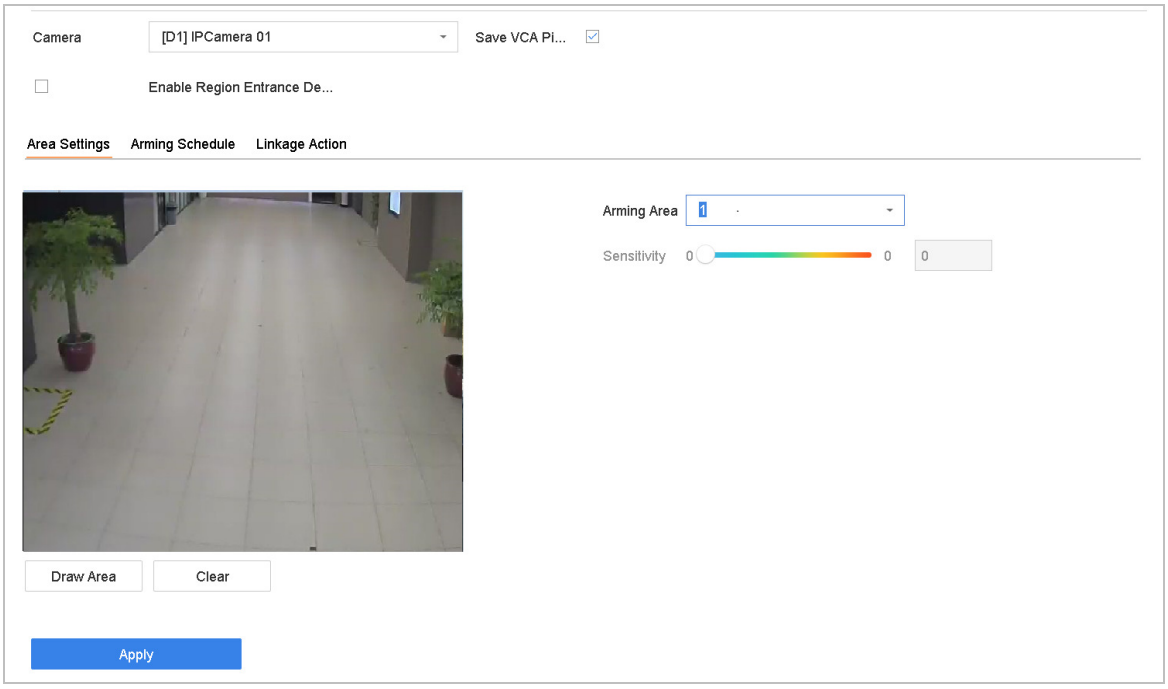


Figure 13-5 Region Entrance Detection

Step 3 Select a camera to configure.

Step 4 Check the Enable Region Entrance Detection checkbox.

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

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

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

2) Drag the sliders to set Sensitivity.

Sensitivity: The higher the value, the more easily the detection alarm 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 a pre-defined virtual region.

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

Step 2 Click **Region Exiting**.

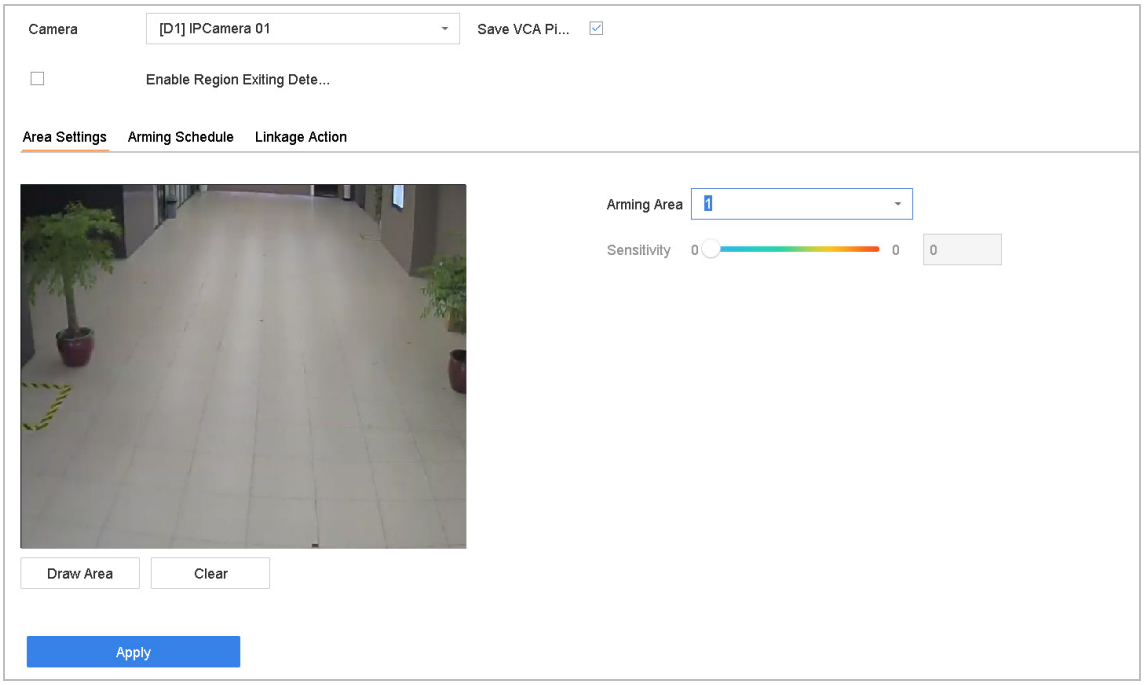


Figure 13-6 Region Exiting Detection

Step 3 Select a camera to configure.

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 an Arming Region to configure. Up to four regions are selectable.

2) Drag the sliders to set Sensitivity.

Sensitivity: The higher the value, the more easily the detection alarm 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 Set the arming schedule. Refer to Chapter 12.1 Configuring Arming Schedule.

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

Step 9 Click **Apply**.

13.7 Unattended Baggage Detection

Purpose

The Unattended Baggage Detection function detects objects left in a pre-defined region such as 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 Click **Unattended Baggage**.

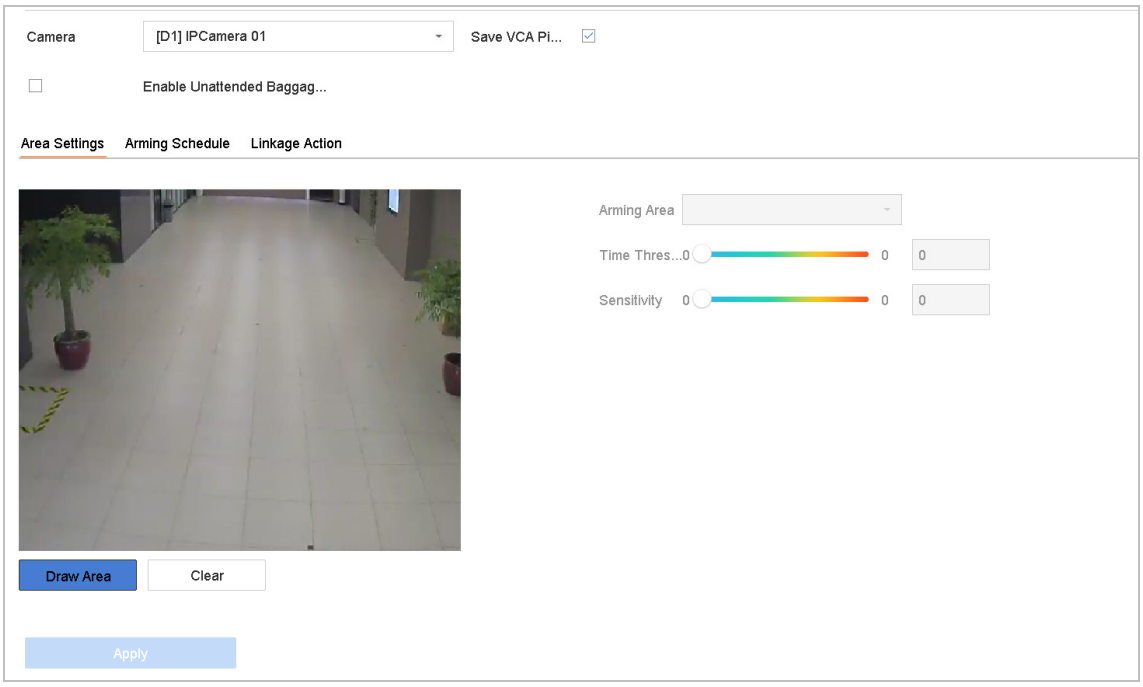


Figure 13-7 Unattended Baggage Detection

Step 3 Select a camera to configure.

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 an **Arming Region** to configure. Up to four regions are selectable.

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

Time Threshold: The time the objects are left in the region. If the value is 10, an alarm is triggered after the object is left in the region for 10s. Its range is [5s-20s].

Sensitivity: Similarity of the background image to the object. The higher the value, the more easily 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 Configuring Arming Schedule.

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

Step 9 Click **Apply**.

13.8 Object Removal Detection

Purpose

The Object Removal Detection function detects objects removed from a pre-defined region such as exhibits on display, and a series of actions can be taken when the alarm is triggered.

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

Step 2 Click **Object Removable**.

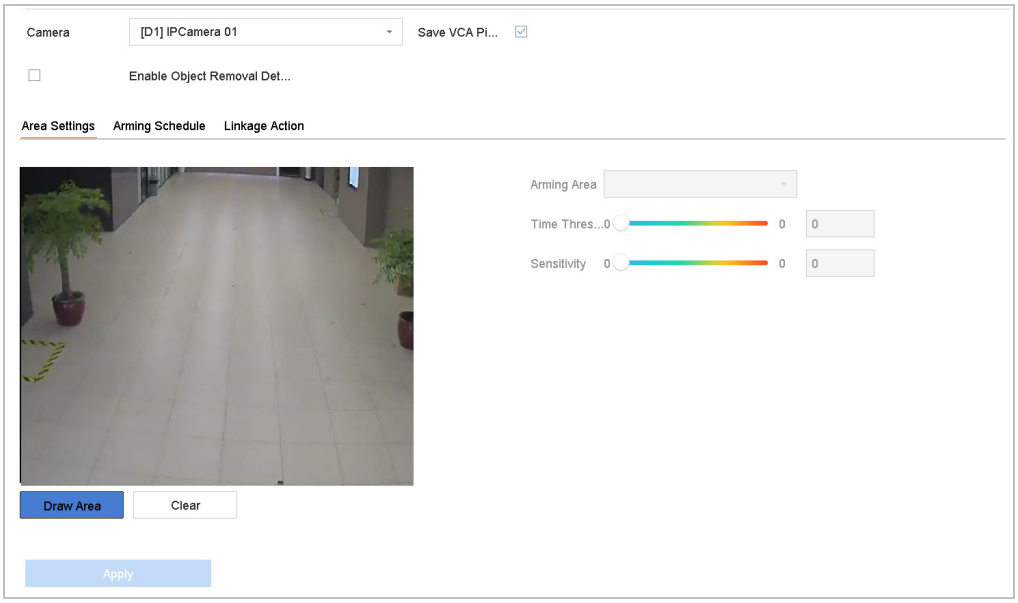


Figure 13-8 Object Removal Detection

Step 3 Select a camera to configure.

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 an Arming Region to configure. Up to four regions are selectable.

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

Time Threshold: The time of the objects 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 of the background image. If the sensitivity is high, a very small object taken from the region will trigger the alarm.

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 Configuring Arming Schedule.

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

Step 9 Click **Apply**.

13.9 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 Click **Audio Exception**.

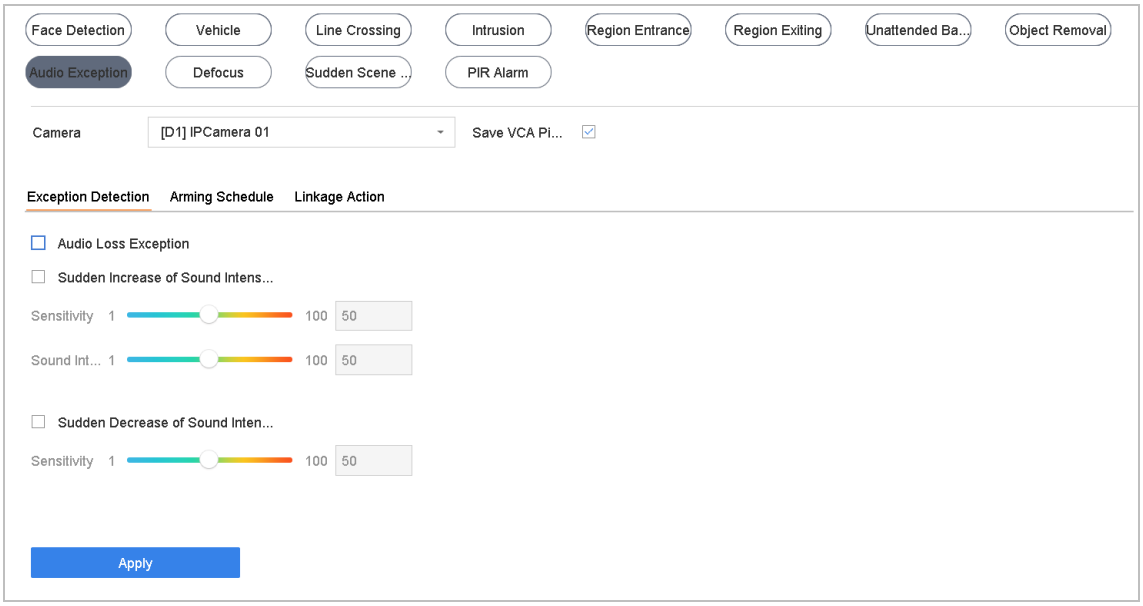


Figure 13-9 Audio Exception Detection

Step 3 Select a camera to configure.

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

Step 5 Set the detection rules:

1) Select the **Exception Detection** tab.

2) Check the **Audio Loss Exception**, **Sudden Increase of Sound Intensity Detection**, and/or **Sudden Decrease of Sound Intensity Detection** checkbox(es).

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 Configuring Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configuring Alarm Linkage Actions.

Step 8 Click **Apply**.

13.10 Sudden Scene Change Detection

Purpose

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

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

Step 2 Click **Sudden Scene Change**.

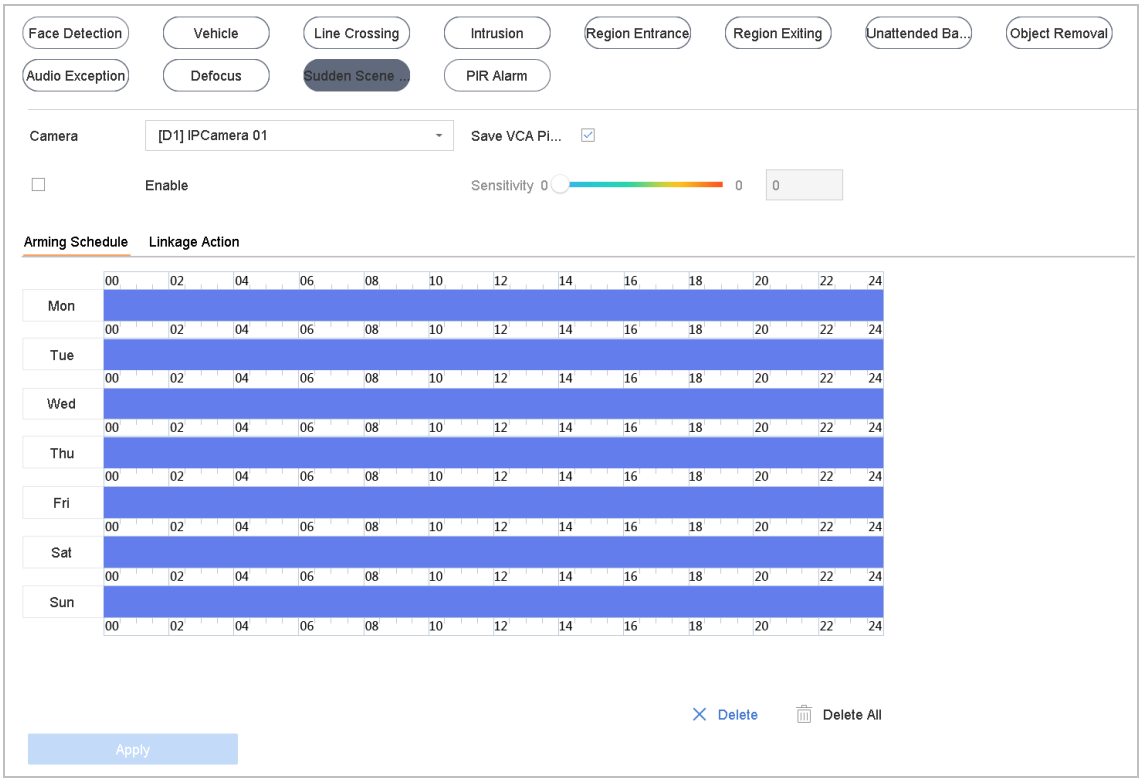


Figure 13-10 Sudden Scene Change

Step 3 Select a camera to configure.

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

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

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

Step 9 Click **Apply**.

13.11 Defocus Detection

Purpose

Image blur caused by lens defocus can be detected.

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

Step 2 Click **Defocus**.

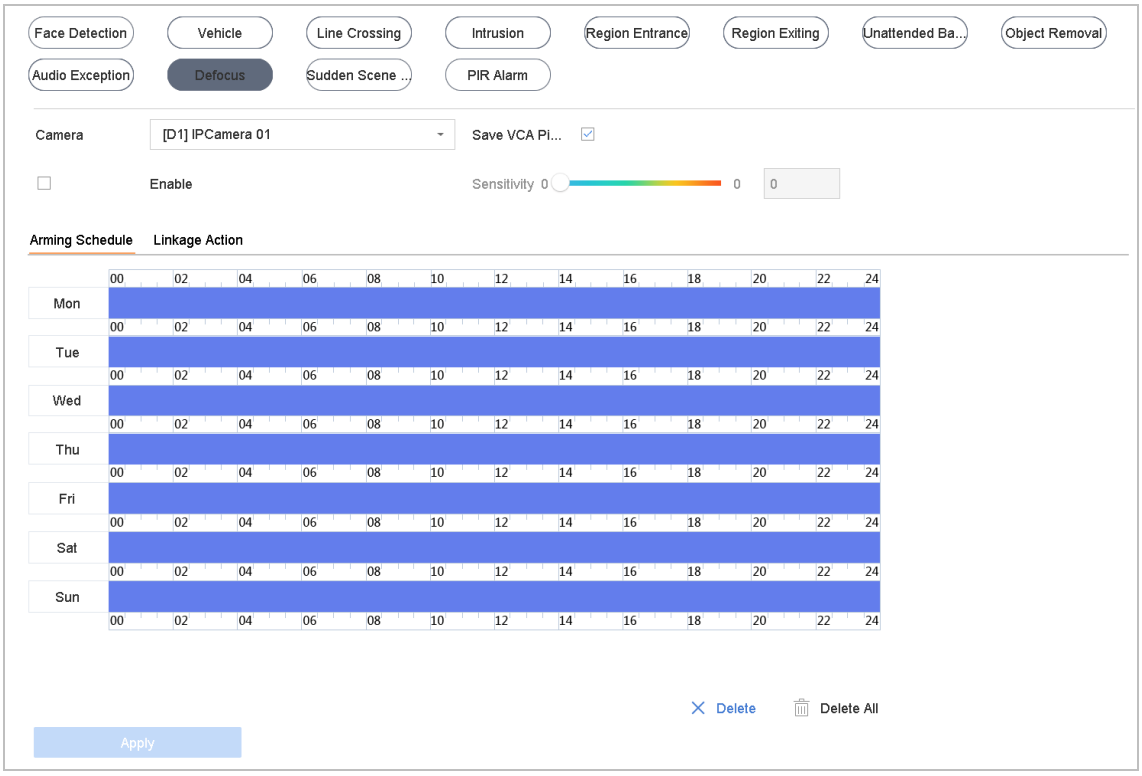


Figure 13-11 Defocus Detection

Step 3 Select a camera to configure.

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 Configuring Arming Schedule.

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

Step 9 Click **Apply**.

13.12 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 Click **PIR Alarm**.

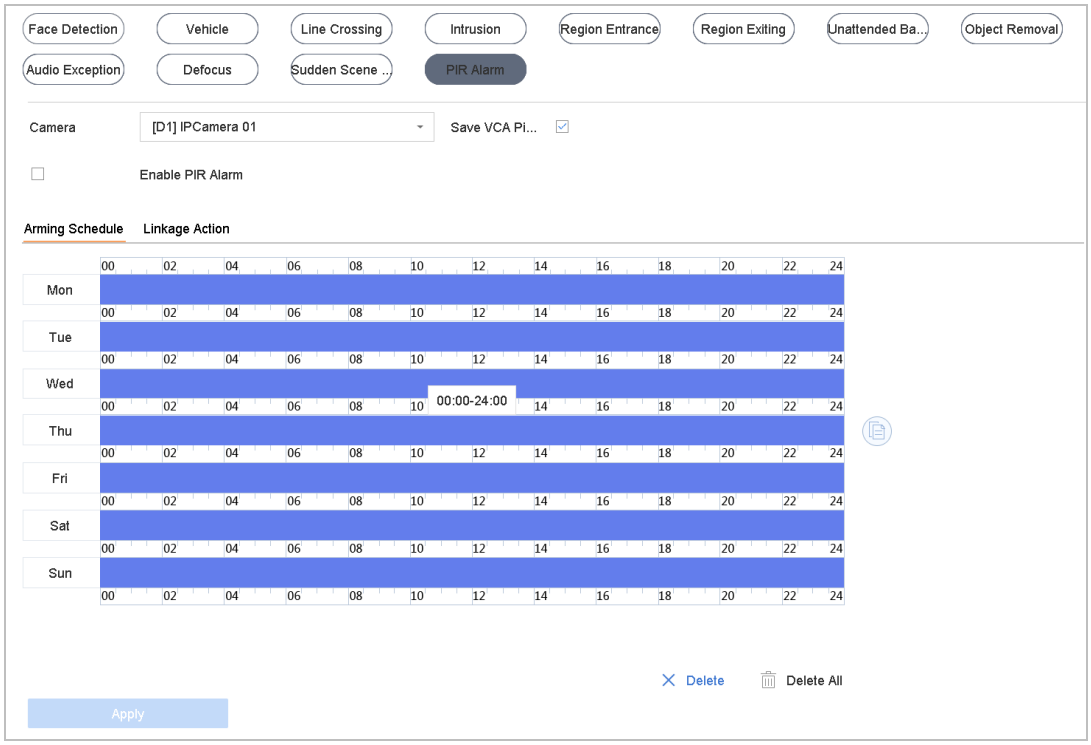


Figure 13-12 FIR Alarm

Step 3 Select a camera to configure.

Step 4 Check PIR Alarm.

Step 5 Optionally, check **Save VCA Picture** to save the captured PIR alarm pictures.

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

Step 7 Set the linkage actions. Refer to Chapter 12.2 Configuring Alarm Linkage Actions.

Step 8 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 configured area and creates daily/weekly/monthly/annual reports for analysis.

Step 1 Go to **Smart Analysis > Counting**.

Step 2 Select the camera.

Step 3 Set the report type to Daily Report, Weekly Report, Monthly Report, or Annual Report.

Step 4 Set the **Date** to analyze. Then the people counting graphic will show.

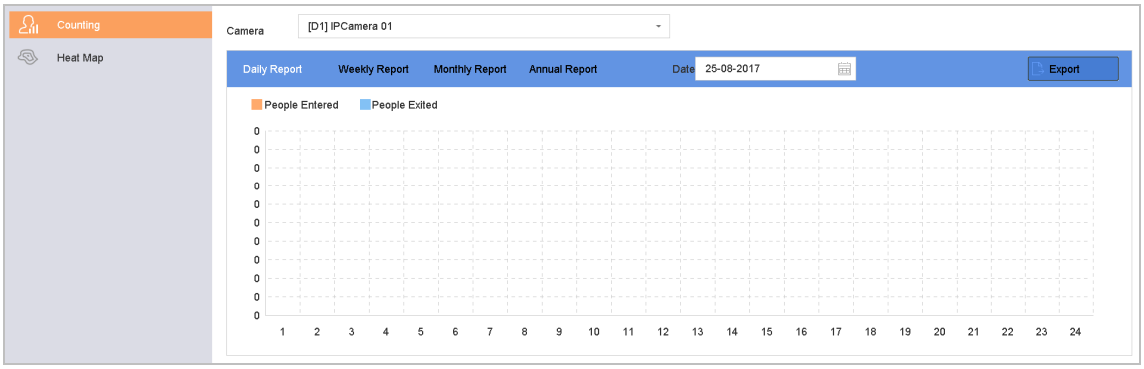


Figure 14-1 People Counting Interface

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.

NOTE

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

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

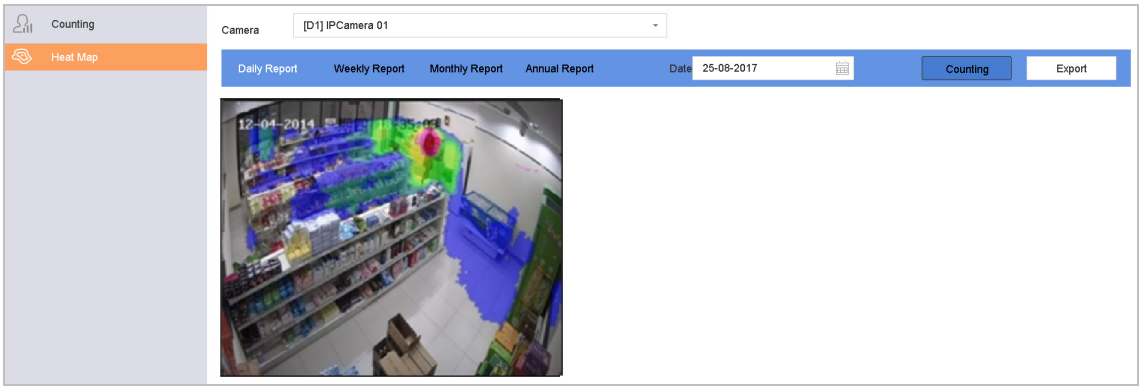


Figure 14-2 Heat Map Interface

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 DS-9600/7700/7600-I (/P) Series devices only.

15.1 Configuring POS Settings

15.1.1 Configuring POS Connection

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

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 half of its number of channels, e.g., Eight POS devices are supported by the DS-9616NI-I8 model.

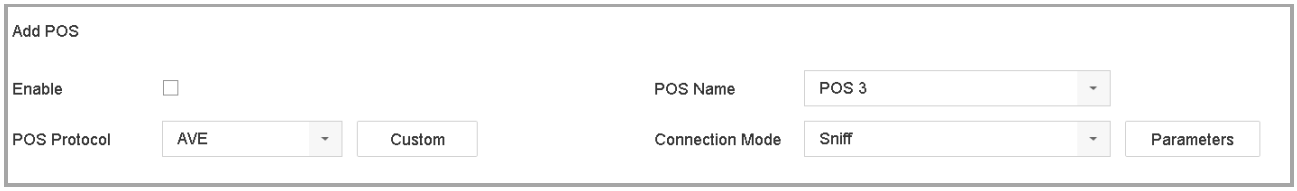


Figure 15-1 POS Settings

Step 5 Set 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.

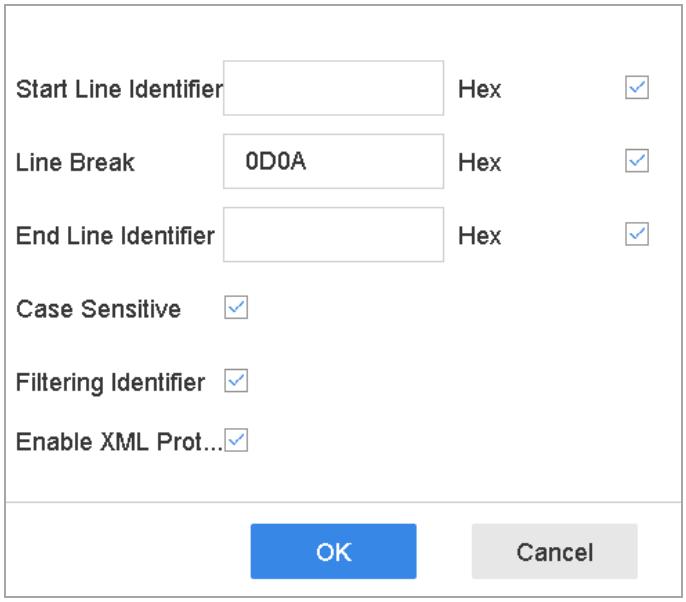


Figure 15-2 Universal Protocol Settings

- **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.

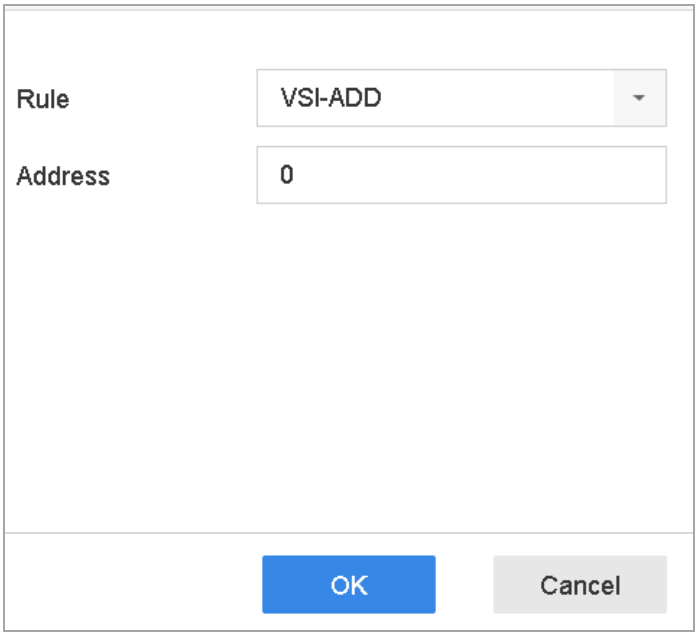


Figure 15-3 AVE Settings

- **NUCLEUS**

  1) Click **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.

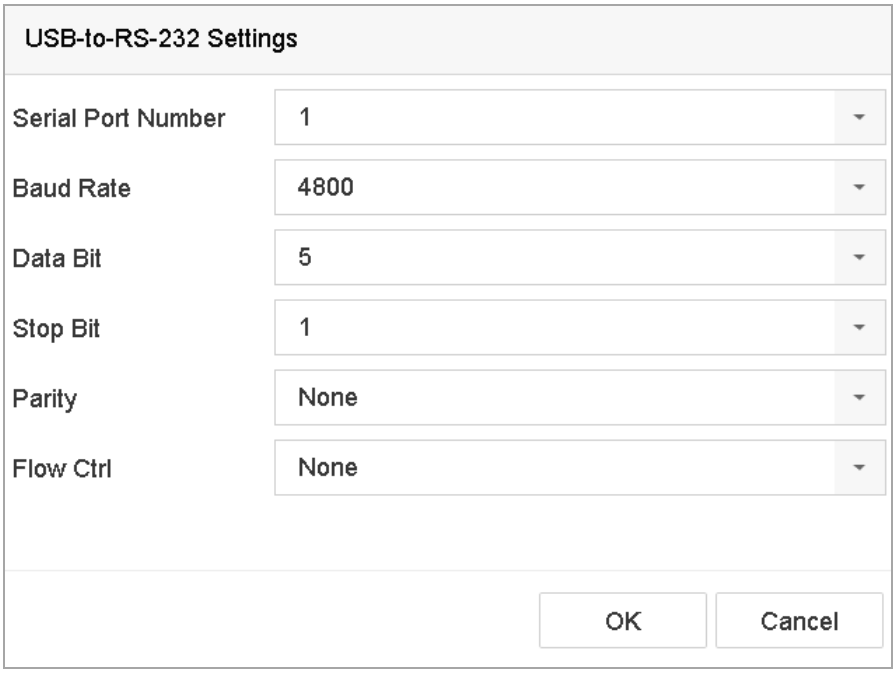


Figure 15-5 USB-to-RS-232 Settings

- **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.

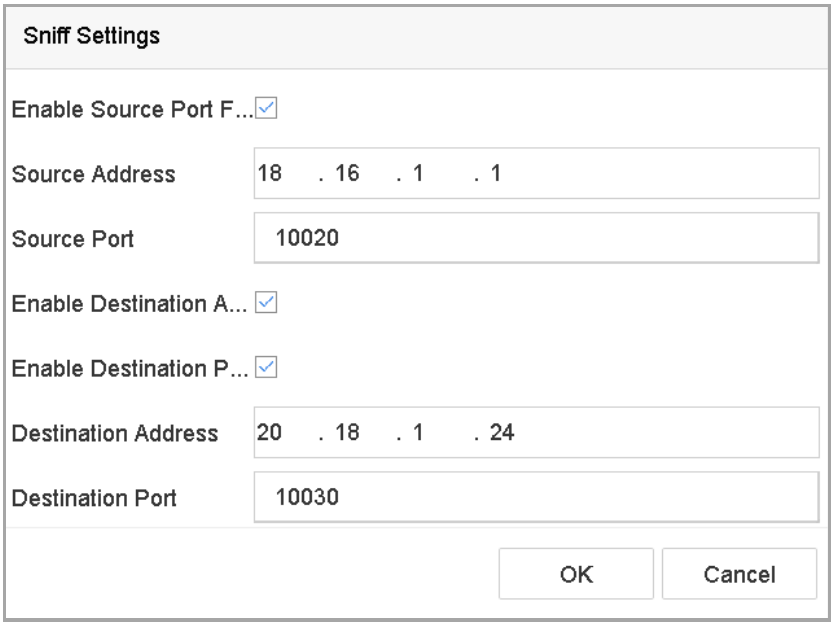


Figure 15-6 Sniff Settings

15.1.2 Configuring POS Text Overlay

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

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 mode
- 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.

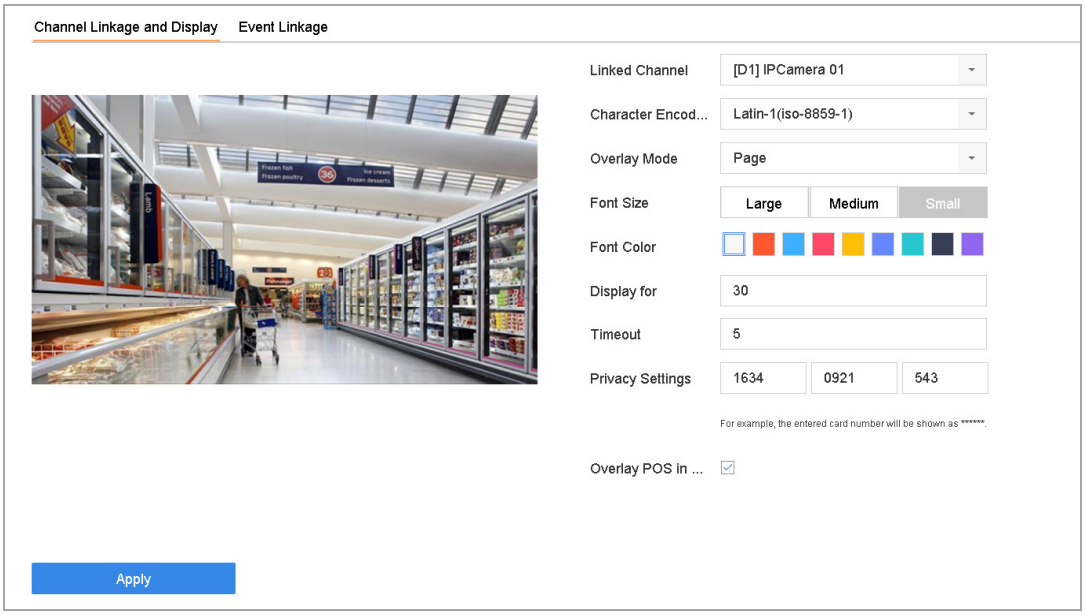


Figure 15-7 Overlay Character Settings

NOTE

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

Step 8 Click **Apply** to activate the settings.

15.2 Configuring POS Alarm

Purpose

A POS event can trigger channels to start recording, trigger full screen monitoring or an audio warning, notify 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 Settings**.

Step 4 Click **the Event Linkage** tab 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.

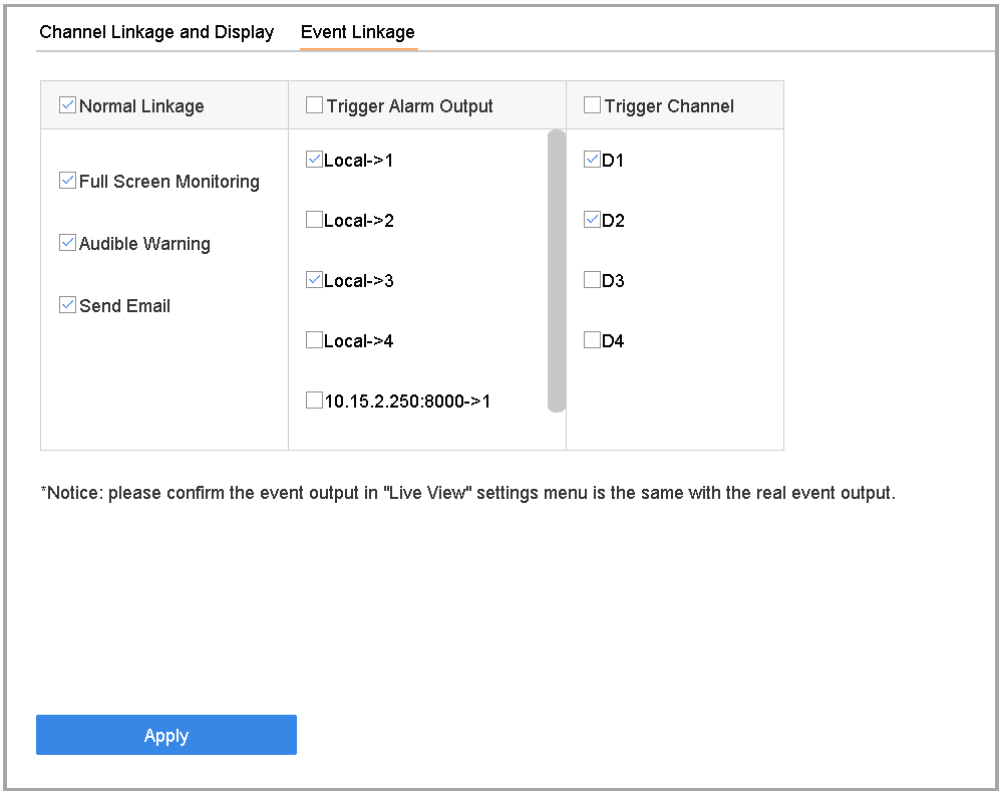


Figure 15-8 Set Trigger Cameras of POS

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

Chapter 16 Network Settings

16.1 Configuring TCP/IP Settings

Purpose

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

16.1.1 Device with Dual Network Interface

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

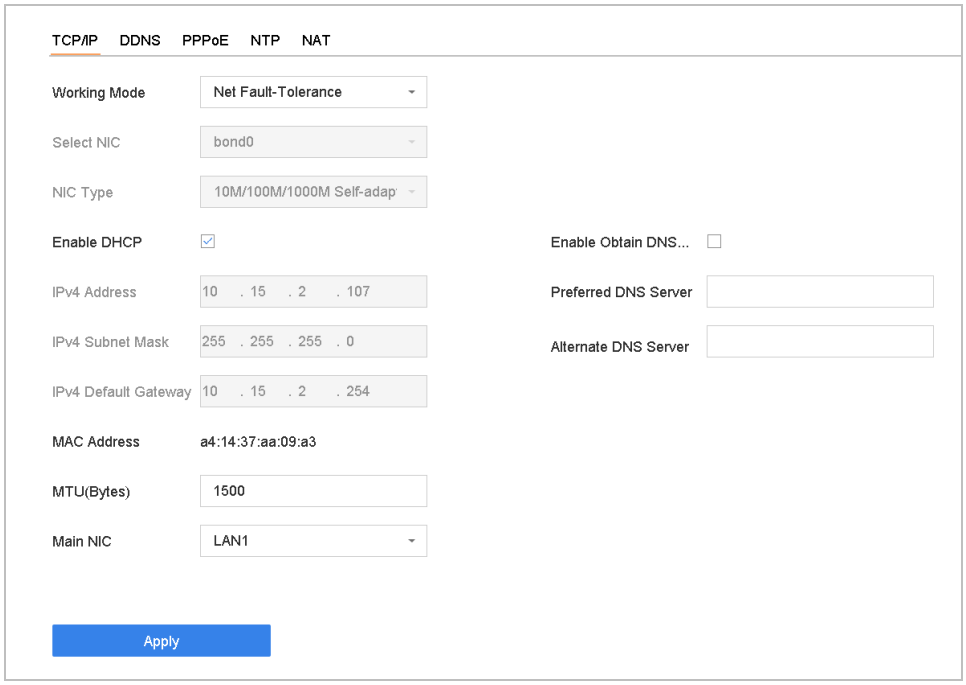


Figure 16-1 TCP/IP Settings

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 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 the **Enable DHCP** checkbox 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**.

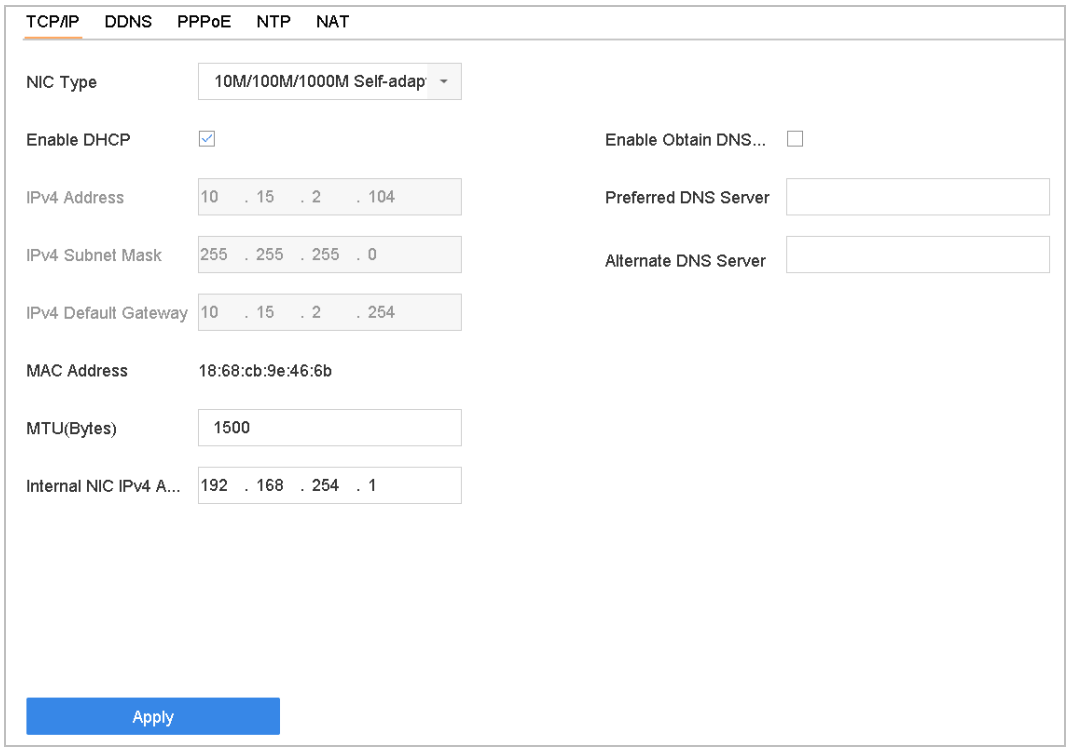


Figure 16-2 TCP/IP Settings

Step 2 Configure network parameters as needed.

NOTE

Check the **Enable DHCP** checkbox 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 Configuring Hik-Connect

Purpose

Hik-Connect provides the mobile phone application as well as the service platform to access and manage your connected devices with remote access to the surveillance system.

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

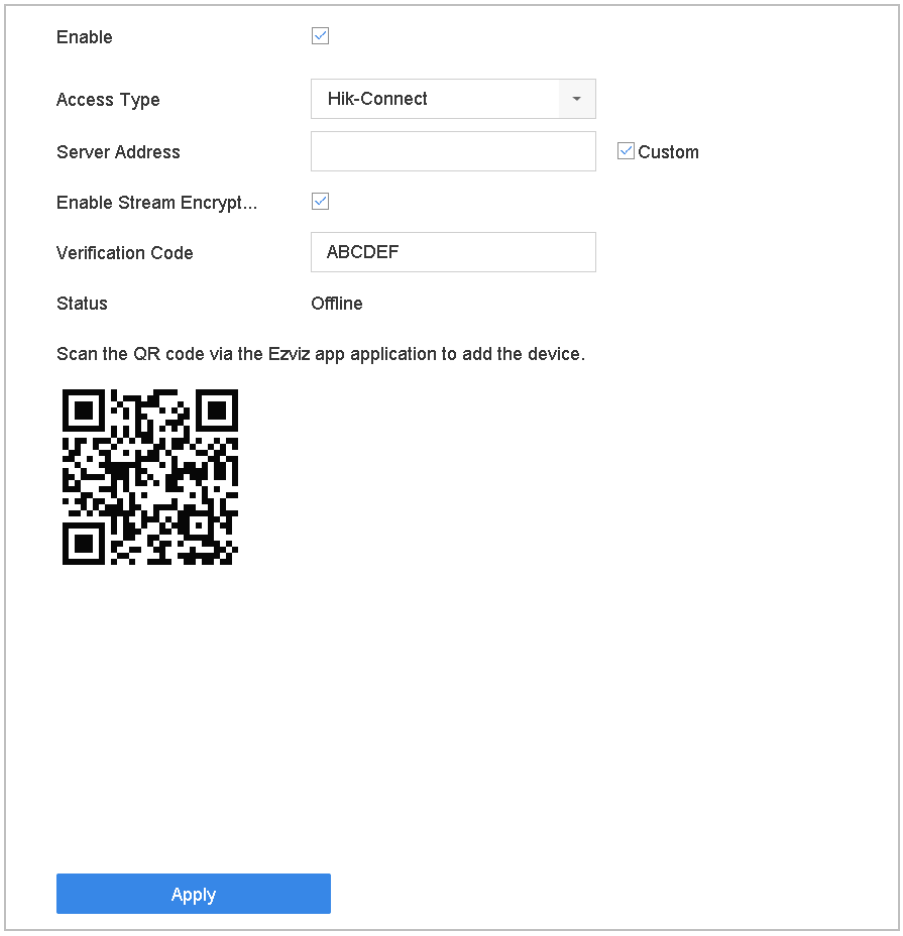


Figure 16-3 Hik-Connect Settings

Step 2 Check the **Enable** checkbox and a **Service Terms** window will pop up. Create your verification code, check to agree to the service terms, and click **OK**.

Step 3 (Optional) Check the **Custom** checkbox and enter the server address as needed. The default server address is dev.hik-connect.com.

Step 4 (Optional) Check the **Enable Stream Encryption** checkbox and a verification code will be required for remote access and Live View.

Step 5 Click **Apply**.

NOTE

After configuration, you can access and manage your devices through Hik-Connect app or **www.hik-connect.com**.

For more detailed instructions of Hik-Connect, refer to help on **www.hik-connect.com**.

16.3 Configuring 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 service 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.

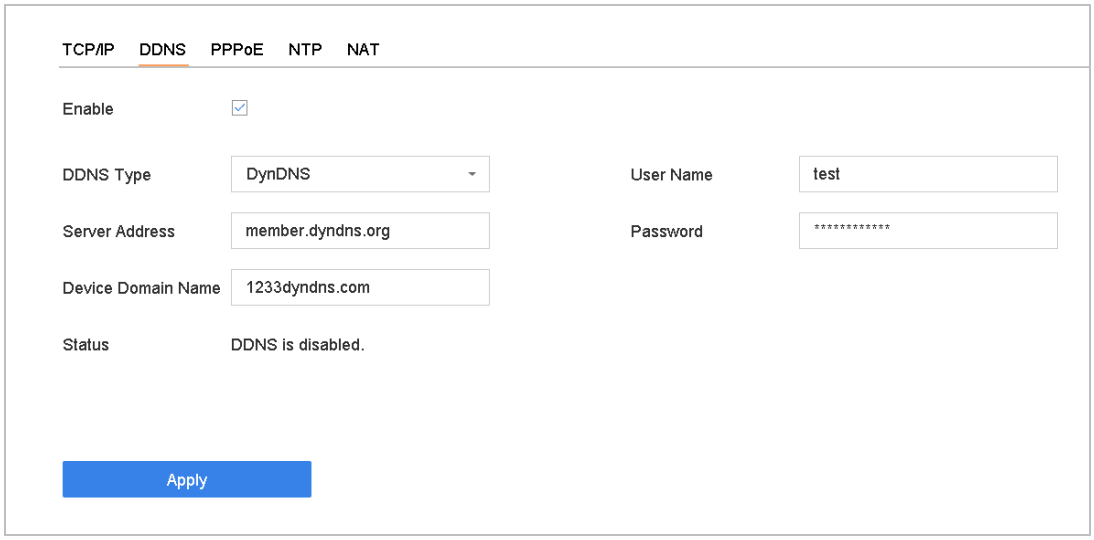


Figure 16-4 DDNS Settings

Step 7 Click **Apply**.

16.4 Configuring 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.

16.5 Configuring 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**.

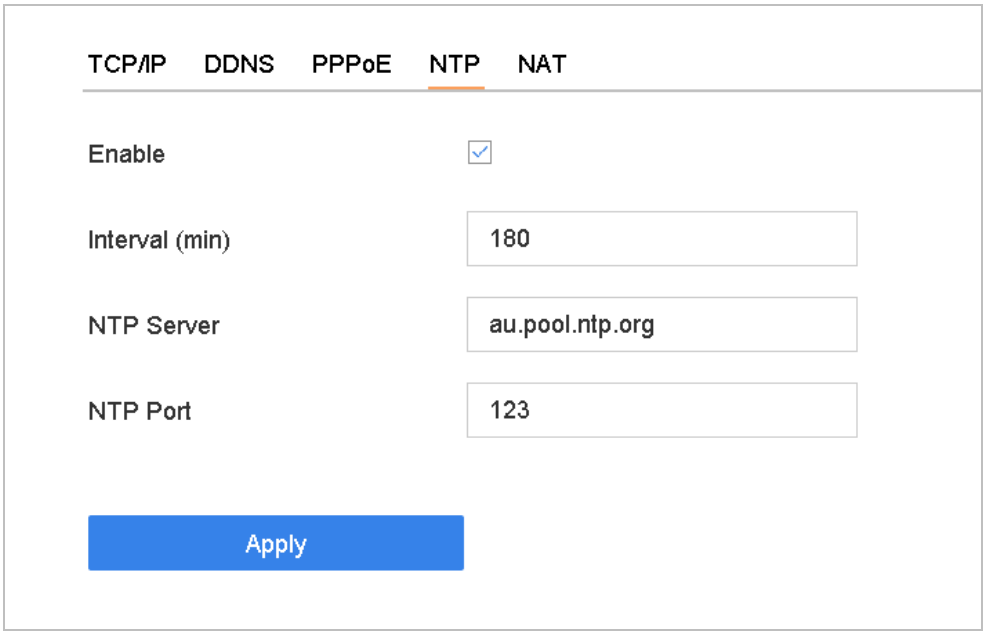


Figure 16-5 NTP Settings

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**.

16.6 Configuring 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**.

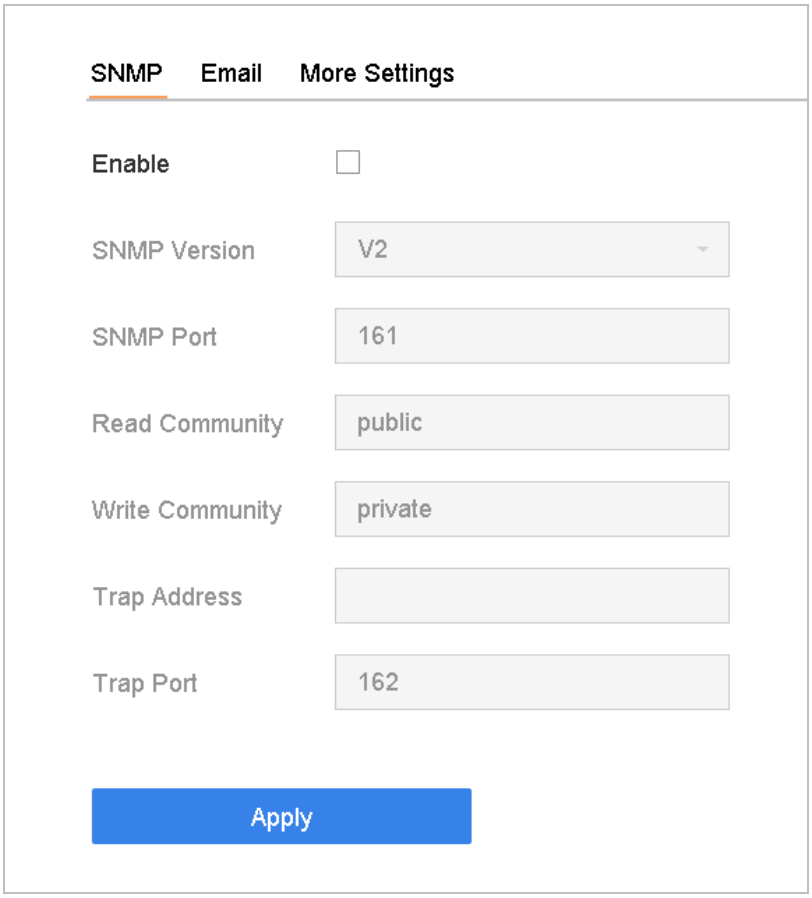


Figure 16-6 SNMP Settings

Step 2 Check the **Enable** checkbox. 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**: SNMP host port.

Step 4 Click **Apply**.

16.7 Configuring E-Mail

Purpose

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

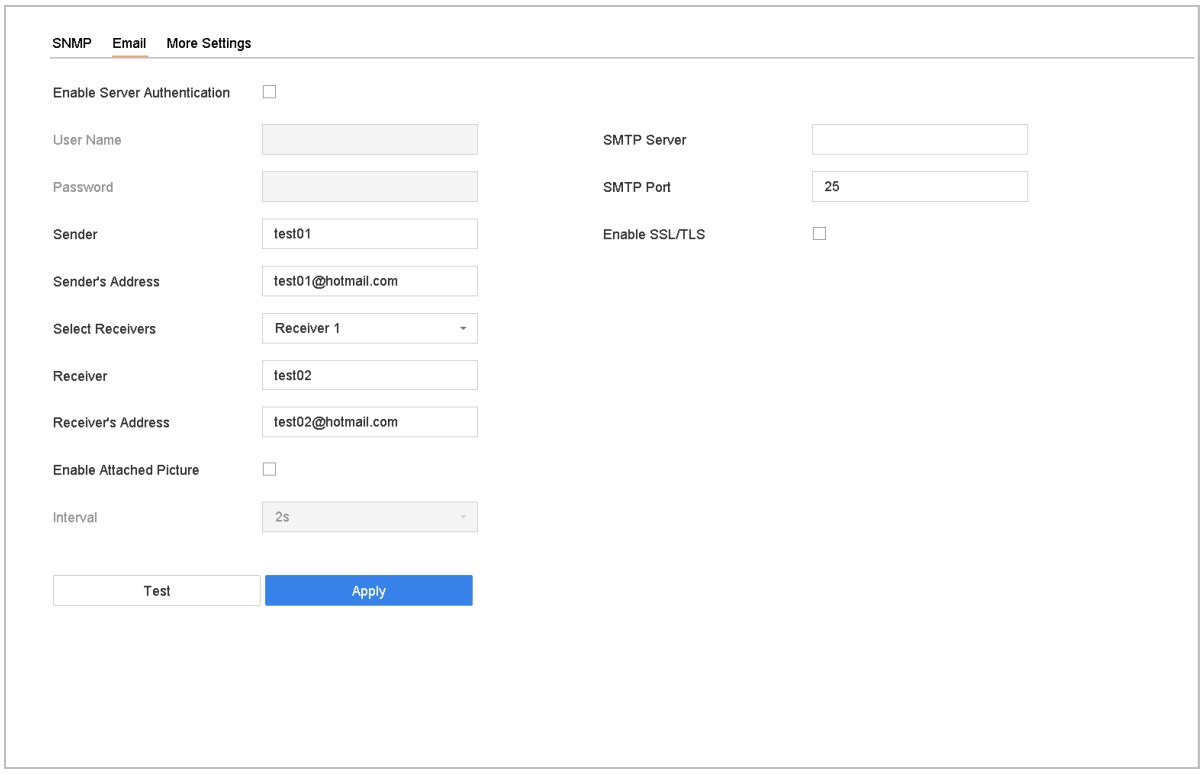


Figure 16-7 E-mail Settings

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 three 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.

16.8 Configure Ports

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

Step 1 Go to **System > Network > Advanced > More Settings** and configure port settings as needed.

- **Alarm Host IP/Port**: With a remote alarm host configured, the device will send the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the client management system (CMS) software installed.

  The Alarm Host IP refers to the IP address of the remote PC on which the CMS software (e.g., iVMS-4200) is installed, and the Alarm Host Port (7200 by default) must be the same as the alarm monitoring port configured in the software.

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

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

- **Multicast IP**: Multicast can be configured to enable Live View for cameras that exceed the maximum number allowed through network. 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.

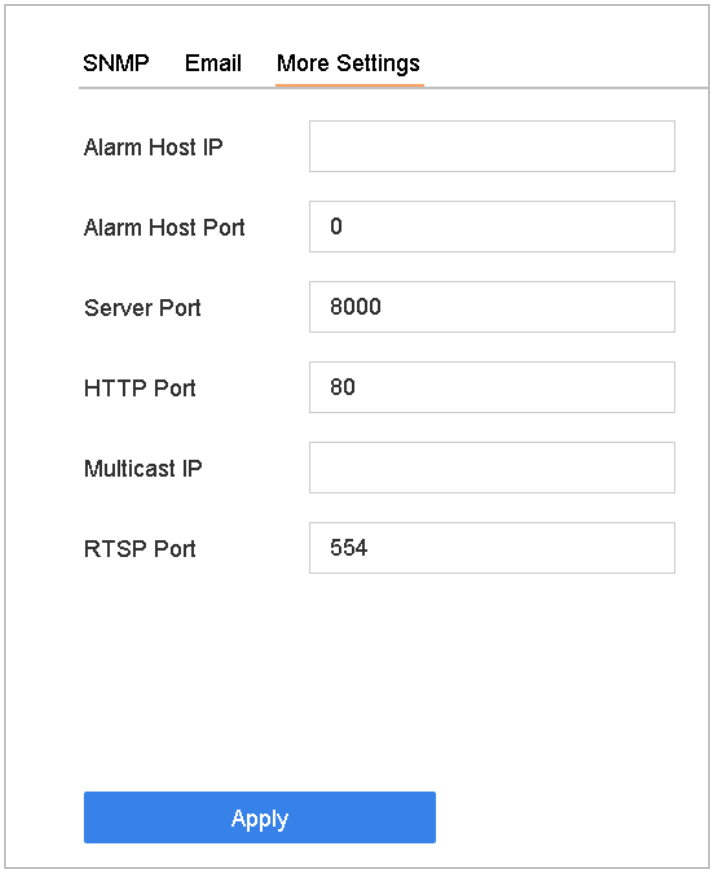


Figure 16-8 Port Settings

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.

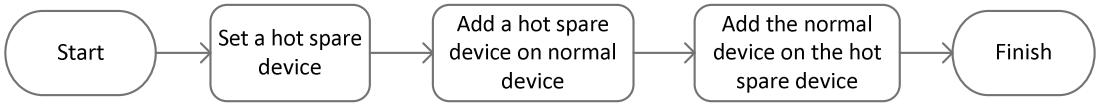


Figure 17-1 Building a Hot Spare System

Before You Start

At least two devices must be online.

17.1 Set Hot Spare Device

Purpose

Hot spare devices take over device tasks when working devices fail.

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

Step 2 Set the Work Mode to **Hot Spare Mode**.

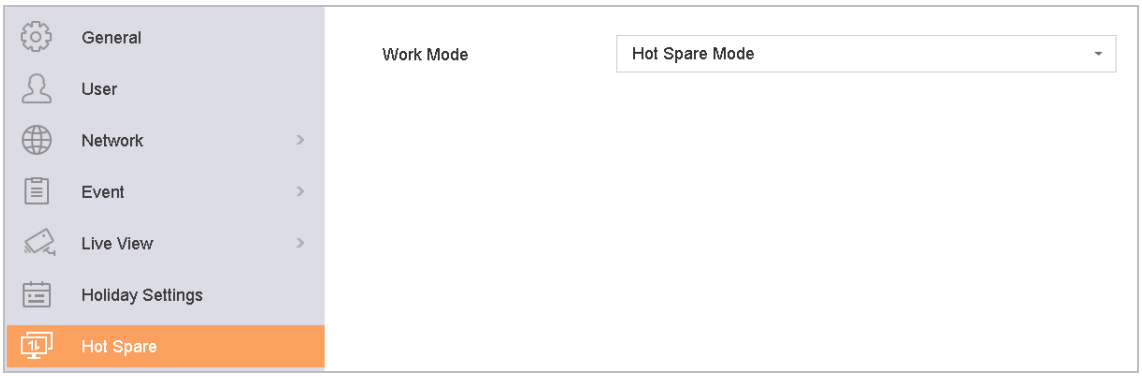


Figure 17-2 Hot Spare

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 the device defaults after switching the working mode of the hot spare device to normal mode to ensure 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 and admin password of the hot spare device.

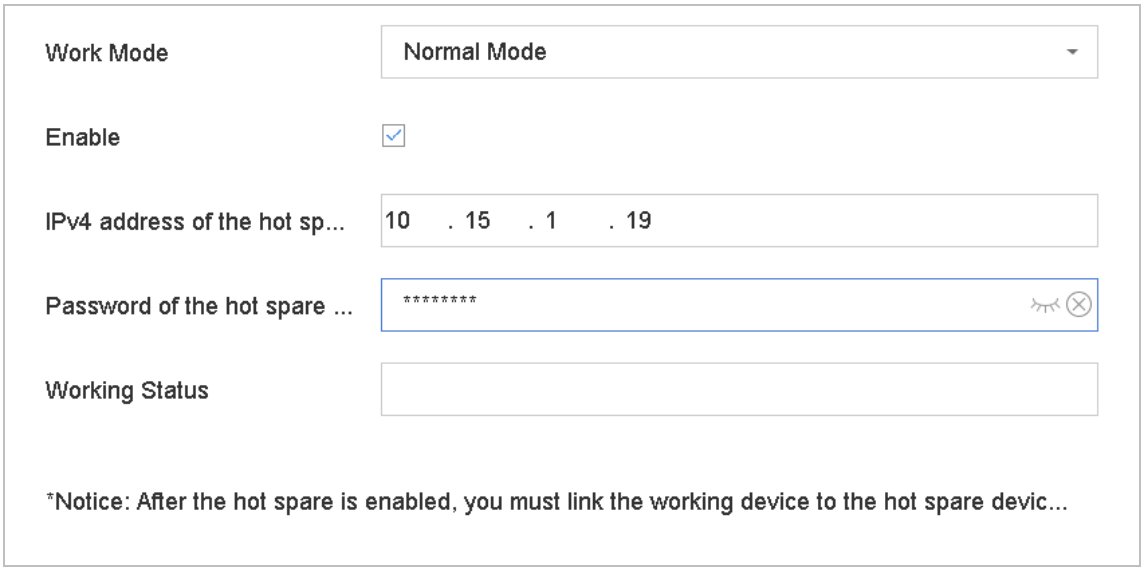


Figure 17-3 Hot Spare

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.

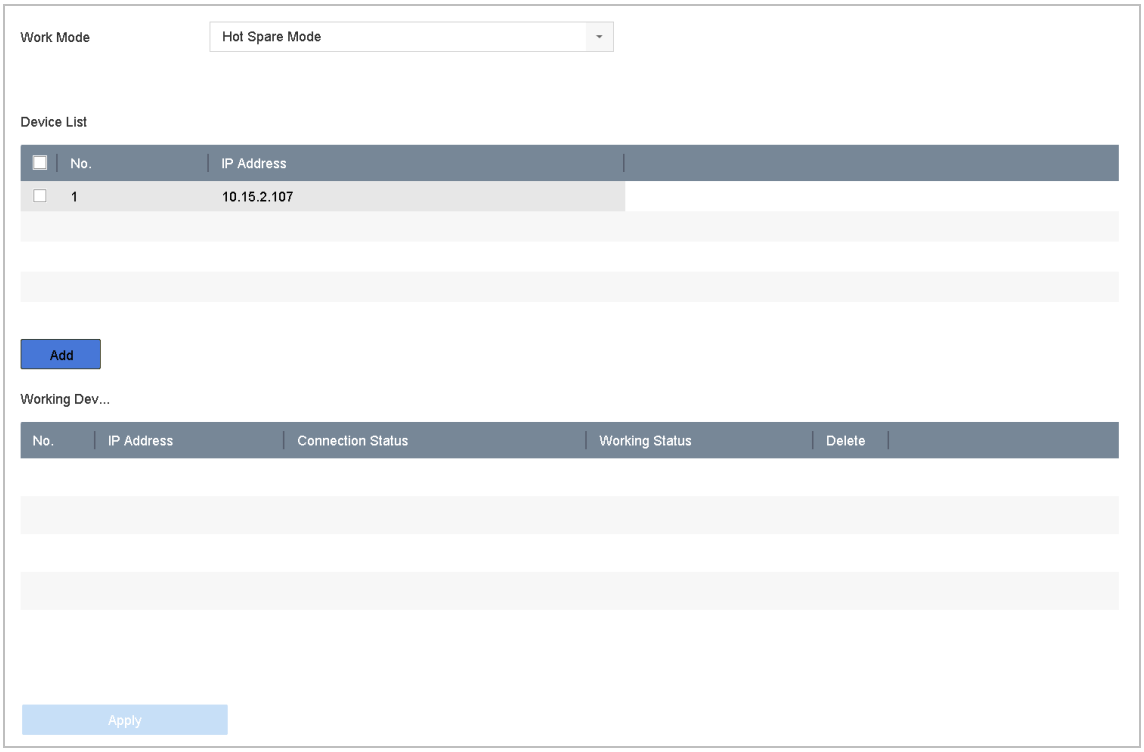


Figure 17-4 Add Working Device

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 one 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 one working device at a time.

Chapter 18 System Maintenance

18.1 Storage Device Maintenance

18.1.1 Configuring 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**.

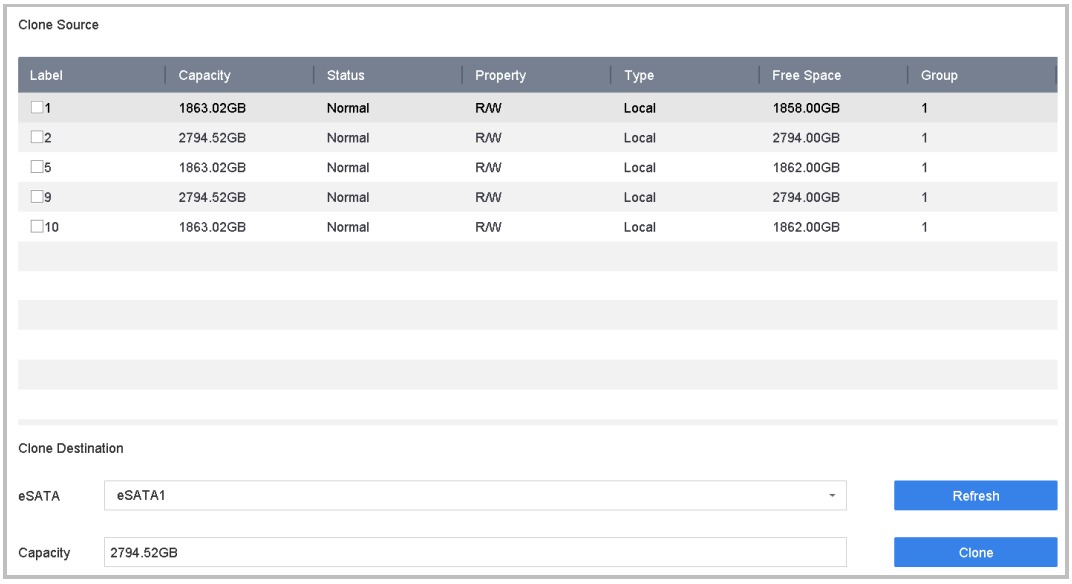


Figure 18-1 HDD Clone

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 continue creating the clone.

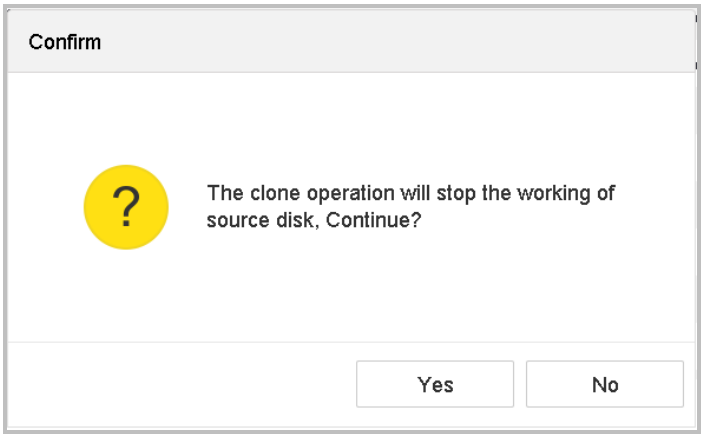


Figure 18-2 Message Box

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

Purpose

HDD detection functions such as S.M.A.R.T. and 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 Conveyance Test.

Step 4 Click **Self-Test** to start the S.M.A.R.T. HDD self-evaluation.

Step 5 The related S.M.A.R.T. information is shown, and you can check the HDD status.

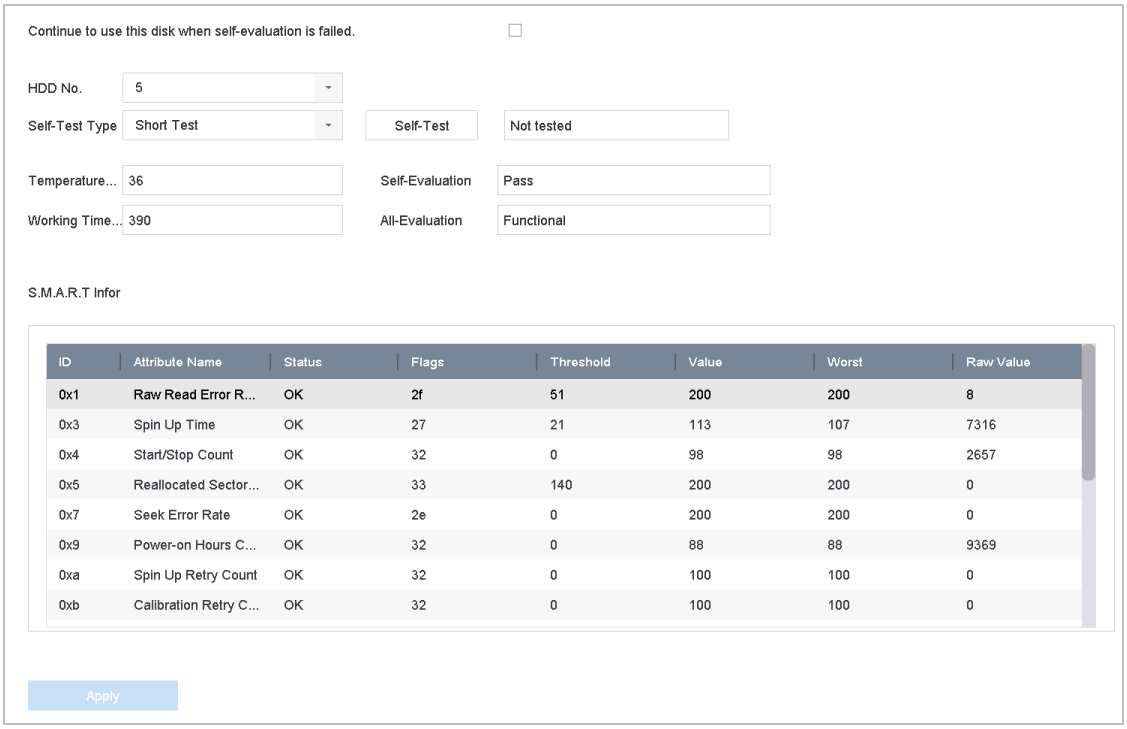


Figure 18-3 S.M.A.R.T. Settings Interface

NOTE

To use the HDD even when S.M.A.R.T. checking has failed, check the **Continue to use the disk when self-evaluation is failed** checkbox.

18.1.3 Bad Sector Detection

Step 1 Go to **Maintenance > HDD Operation > Bad Sector Detection**.

Step 2 Select the HDD No. you want to configure in the drop-down list.

Step 3 Select **All Detection** or **Key Area Detection** as the detection type.

Step 4 Click **Self-Test** to start the detection.

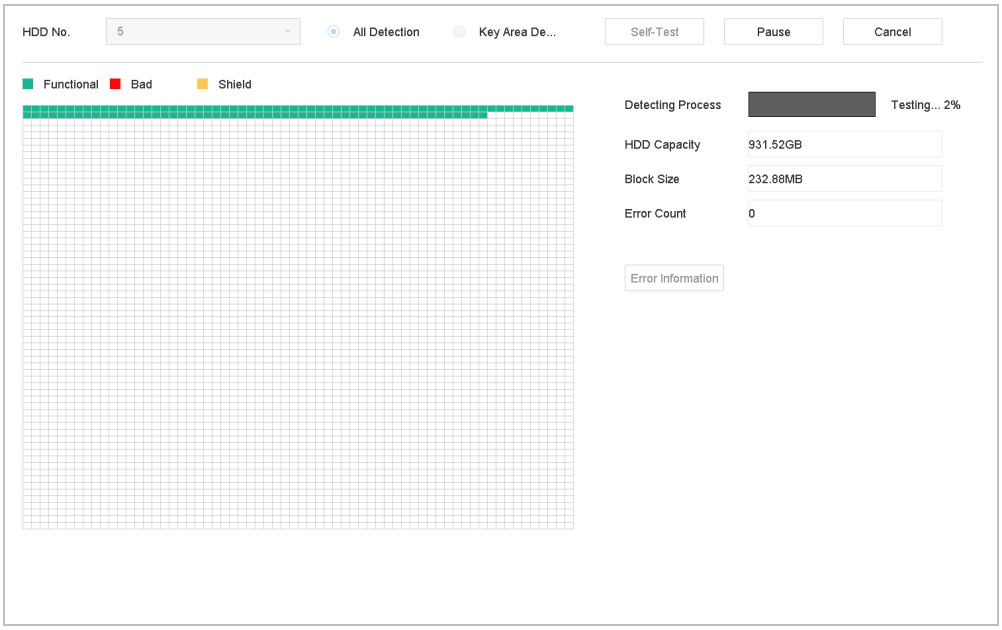


Figure 18-4 Bad Sector Detection

Step 5 You can pause/resume or cancel the detection.

Step 6 After testing has been completed, click **Error Information** to see the detailed damage information.

18.1.4 HDD Health Detection

Purpose

You can view the health status of a 4 TB to 8 TB Seagate HDD manufactured 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 18-5 Health Detection

Step 2 Click an HDD to view details.

18.2 Search and Export Log Files

Purpose

The device operation, alarm, exception, and information can be stored in log files, which can be viewed and exported at any time.

18.2.1 Searching the Log Files

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

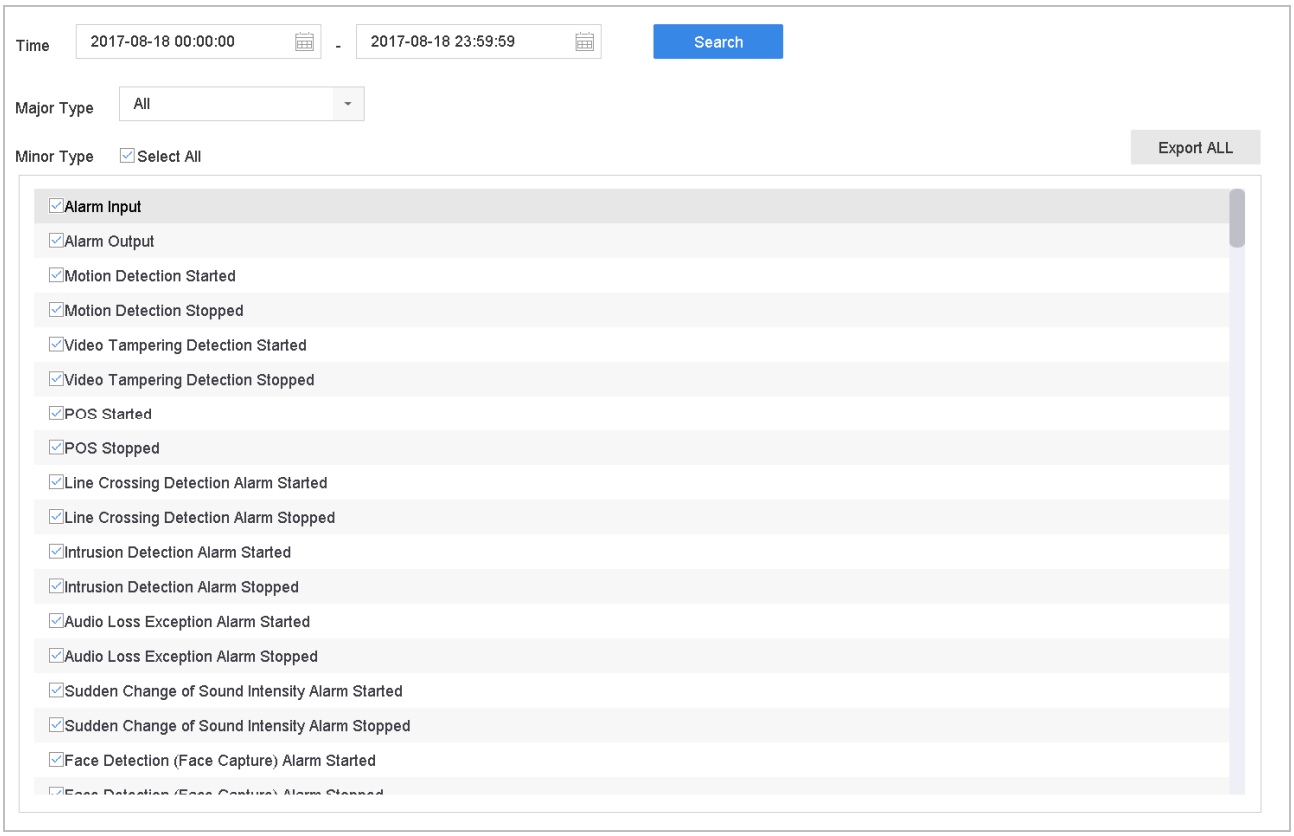


Figure 18-6 Log Search Interface

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.

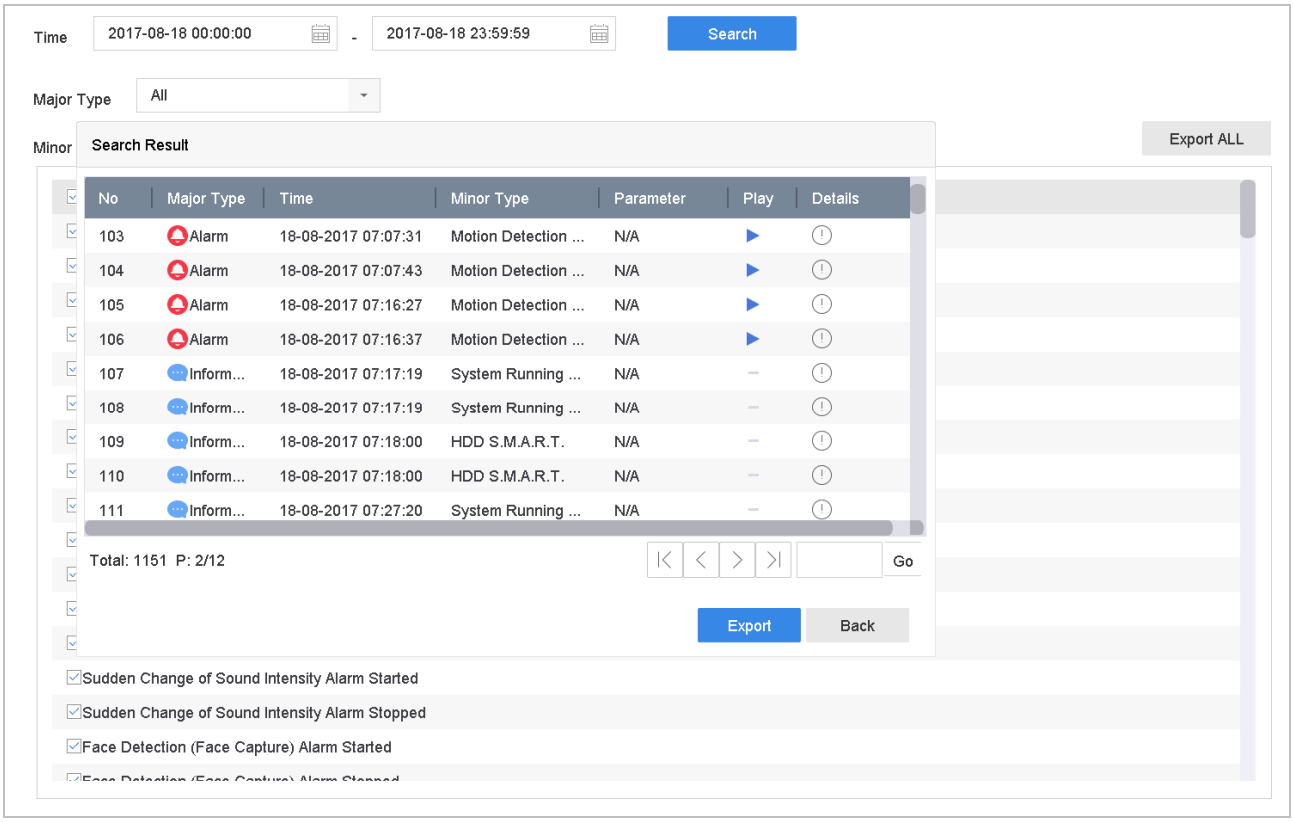


Figure 18-7 Log Search Results

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.

18.2.2 Exporting Log Files

Before You Start

Connect a storage device to the NVR.

Step 1 Search the log files. Refer to Chapter 18.2.1 Searching 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.

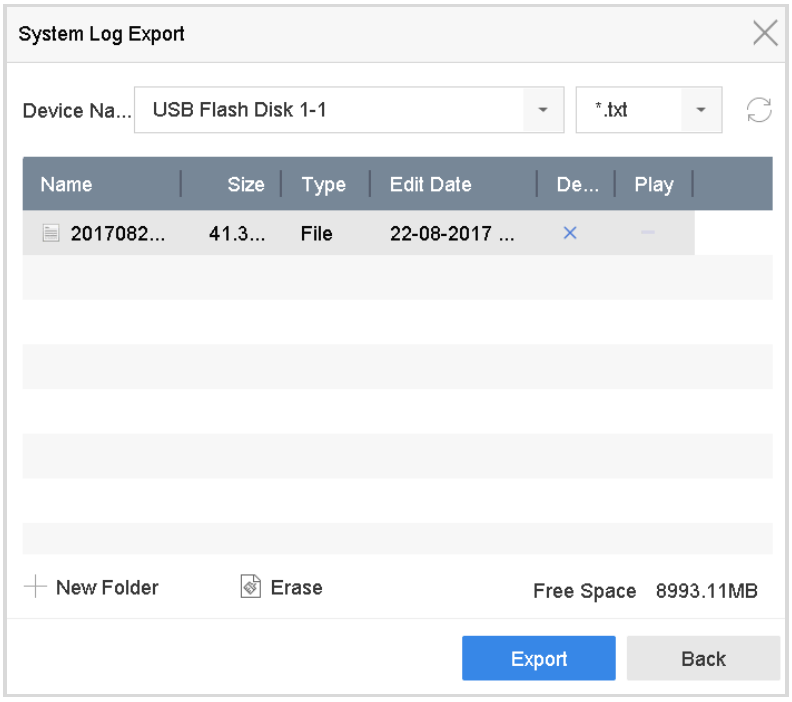


Figure 18-8 Export Log Files

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

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 **New Folder** to create a new folder in the storage device.
- Click **Format** to format the storage device before exporting the log(s).

18.3 Importing/Exporting IP Camera Configuration Files

Purpose

The IP camera information, including 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 a 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.

18.4 Importing/Exporting 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**.

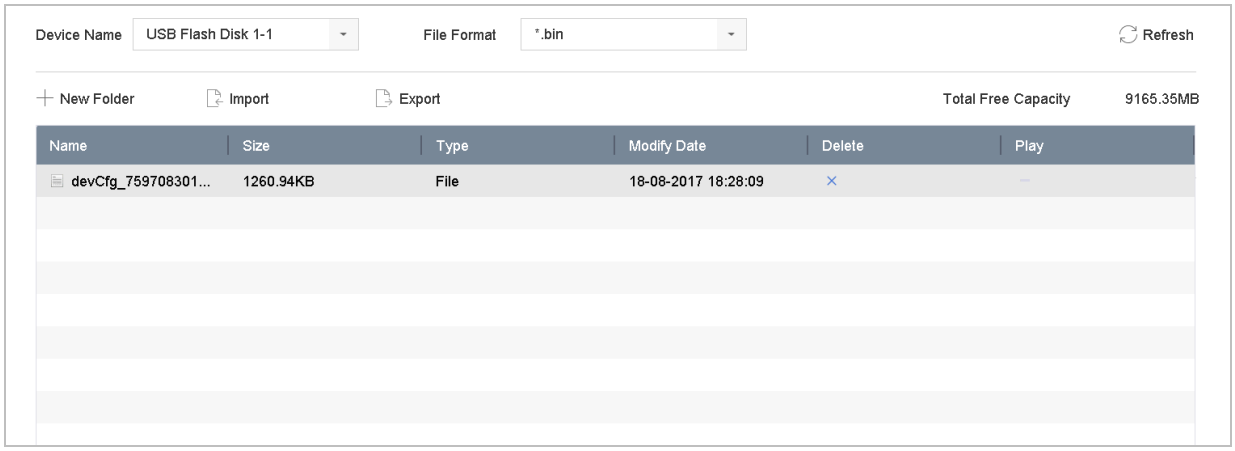


Figure 18-9 Import/Export Config File

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 **Import**.

NOTE

After having finished importing the configuration files, the device will reboot automatically.

18.5 Upgrading the System

Purpose

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

18.5.1 Upgrading with a Local Backup Device

Before You Start

Step 1 Connect your device to a local storage device that contains the firmware update file.

Step 2 Go to **Maintenance > Upgrade**.

Step 3 Click the **Local Upgrade** tab to enter the local upgrade interface.

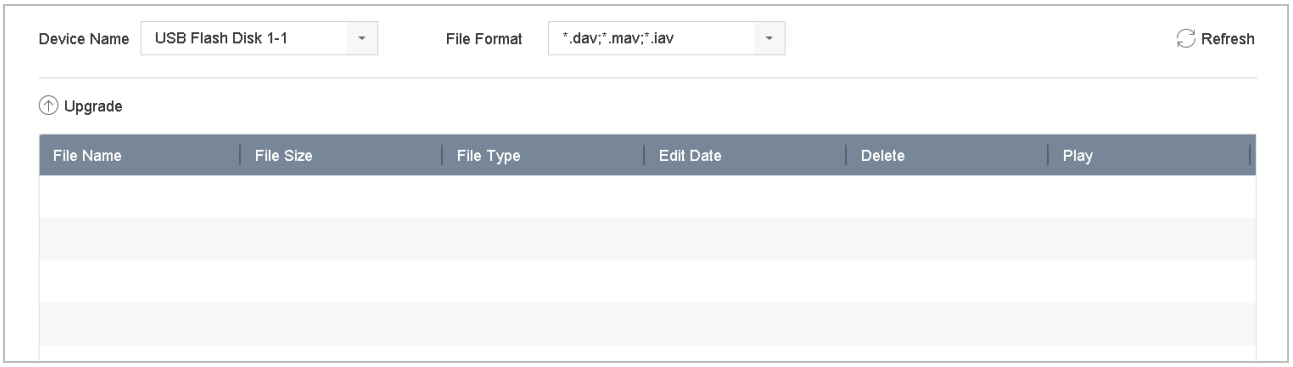


Figure 18-10 Local Upgrade Interface

Step 4 Select the firmware update file from the storage device.

Step 5 Click **Upgrade** to start upgrading.

Step 6 After the upgrade is complete, the device will reboot automatically to activate the new firmware.

18.5.2 Upgrading 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.

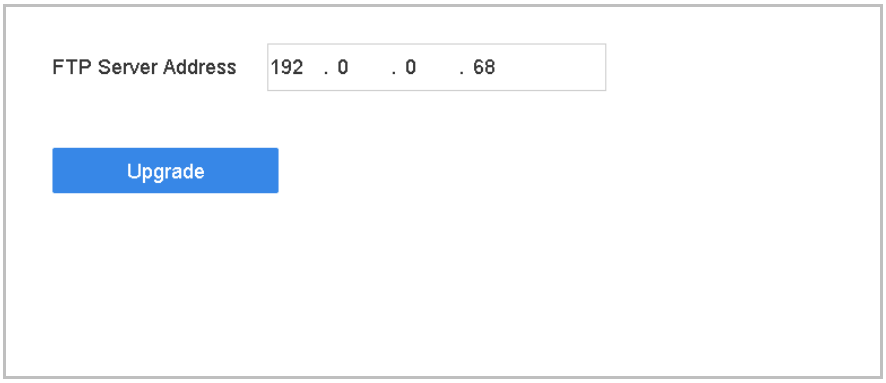


Figure 18-11 FTP Upgrade Interface

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

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

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

18.6 Restore Default Settings

Step 1 Go to **Maintenance > Default**.

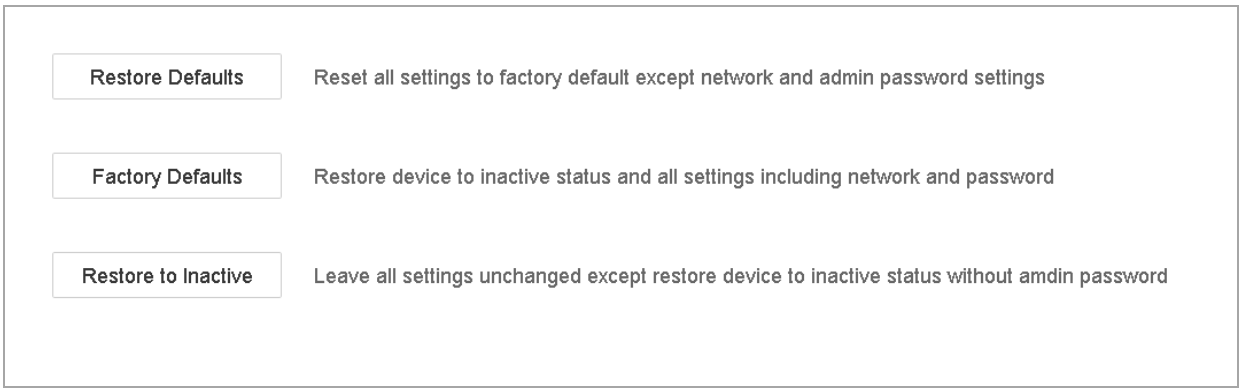


Figure 18-12 Restore Defaults

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 19 General System Settings

19.1 Configuring 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**.

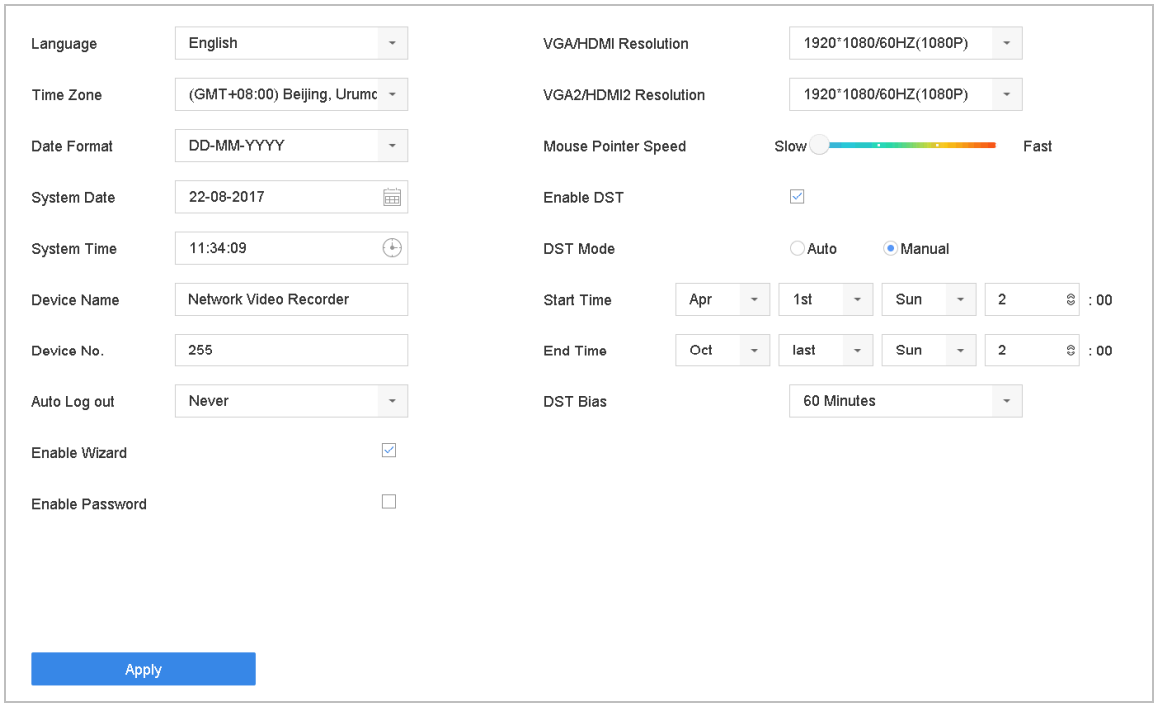


Figure 19-1 General Settings Interface

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 the video output resolution.
- **Device Name:** Edit the name of the device
- **Device No.:** Edit the device serial number. The Device No. can be set in the range of 1 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*, the system will exit from the current operation menu to the Live View screen after five minutes of menu inactivity.
- **Mouse Pointer Speed:** Set the speed of the mouse pointer; four 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.

19.2 Configuring the Date and 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.

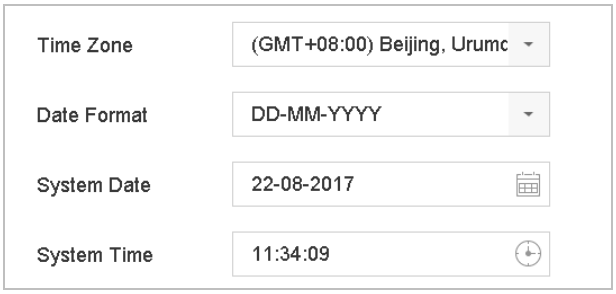


Figure 19-2 Date and Time Settings

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

19.3 Configuring the 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 the **Enable DST** checkbox.

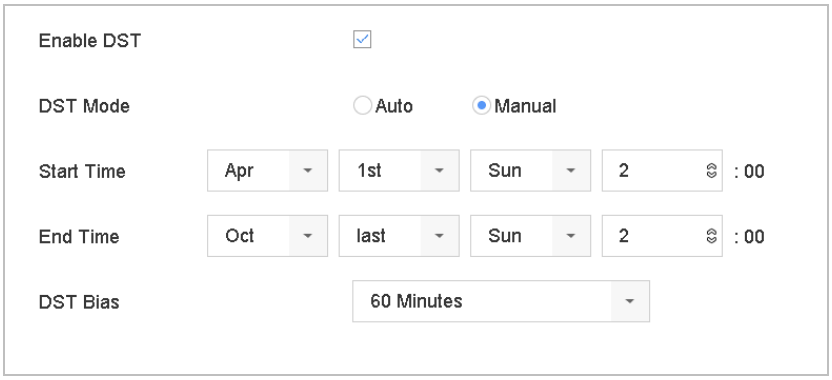


Figure 19-3 DST Settings Interface

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.

19.4 Managing User Accounts

Purpose

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

19.4.1 Adding a User

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

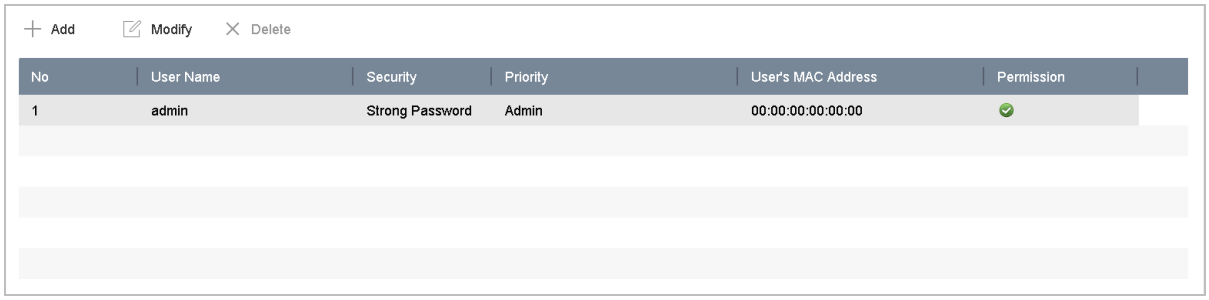


Figure 19-4 User Management Interface

Step 2 Click **Add** to enter the operation permission interface.

Step 3 Input the admin password and click **OK**.

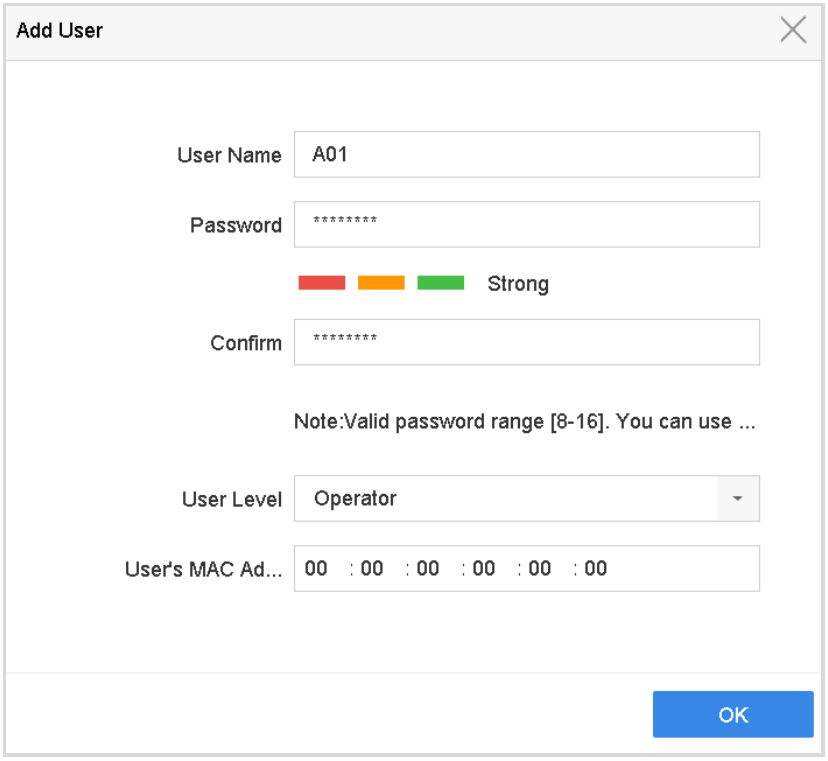


Figure 19-5 Add User

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**.

WARNING

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

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

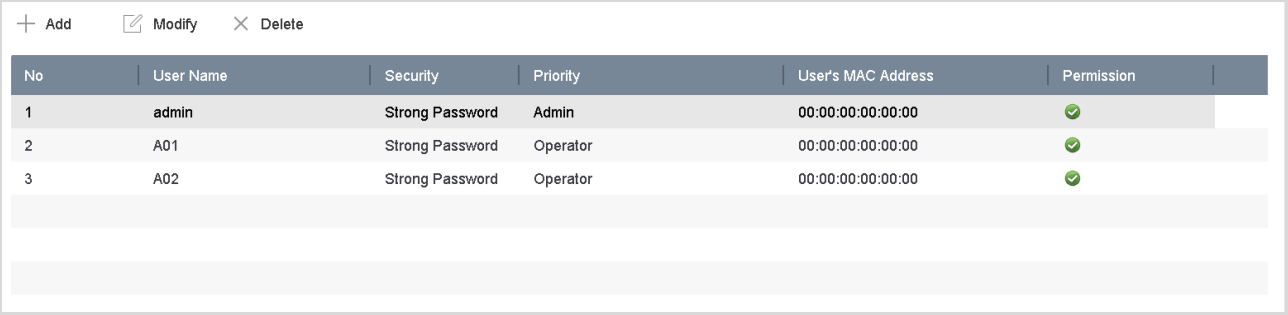


Figure 19-6 User List

19.4.2 Setting User Permissions

For an added user, you can assign 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.

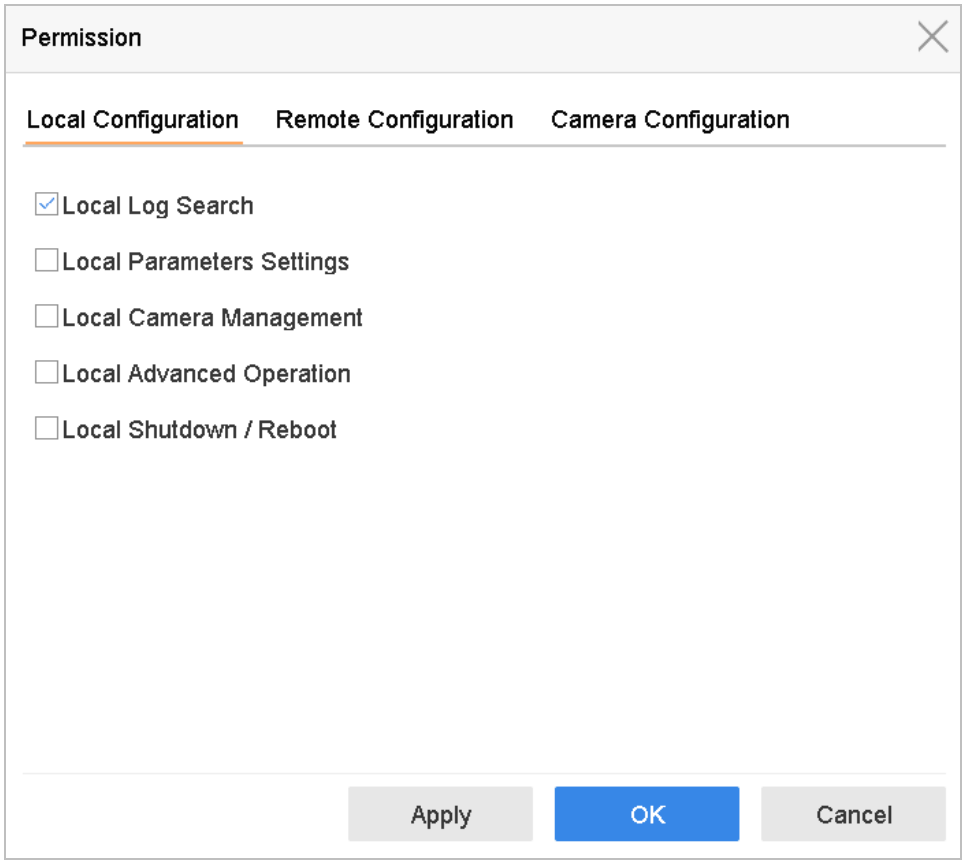


Figure 19-7 User Permission Settings Interface

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

- **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 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 IP cameras.
- **Remote Serial Port Control**: Configuring 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).
- **Remote Playback**: Remotely playing back recorded files of the selected camera(s).
- **Local PTZ Control**: Locally controlling PTZ movement of the selected camera(s).
- **Remote PTZ Control**: Remotely controlling PTZ movement of the selected camera(s).
- **Local Video Export**: Locally exporting recorded files of the selected camera(s).
- **Local Live View**: View live video of the selected camera(s) locally.

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

NOTE

Only the admin user account has the permission to restore factory default parameters.

19.4.3 Setting Local Live View Permission for Non-Admin Users

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

Step 2 Click of the admin user.

Step 3 Input admin password and click **OK**.

Step 4 Select cameras that a non-admin user can view locally, and click **OK.**

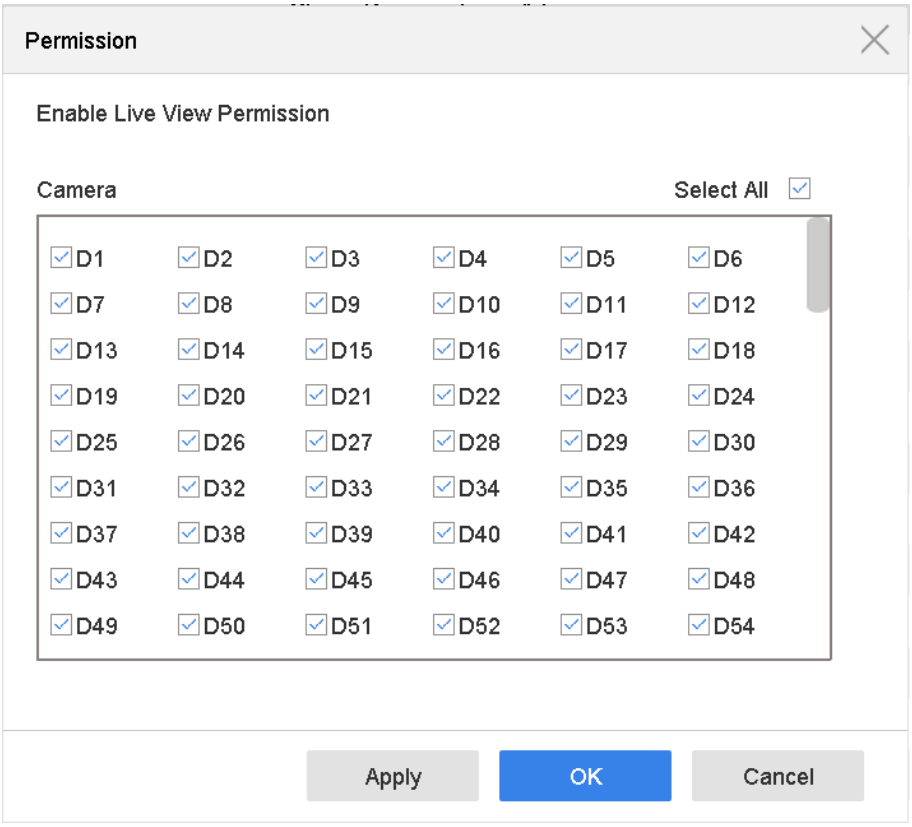


Figure 19-8 Enable Live View Permissions

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**.

19.4.4 Editing the Admin User

You can modify the admin user account's password and unlock pattern.

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

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

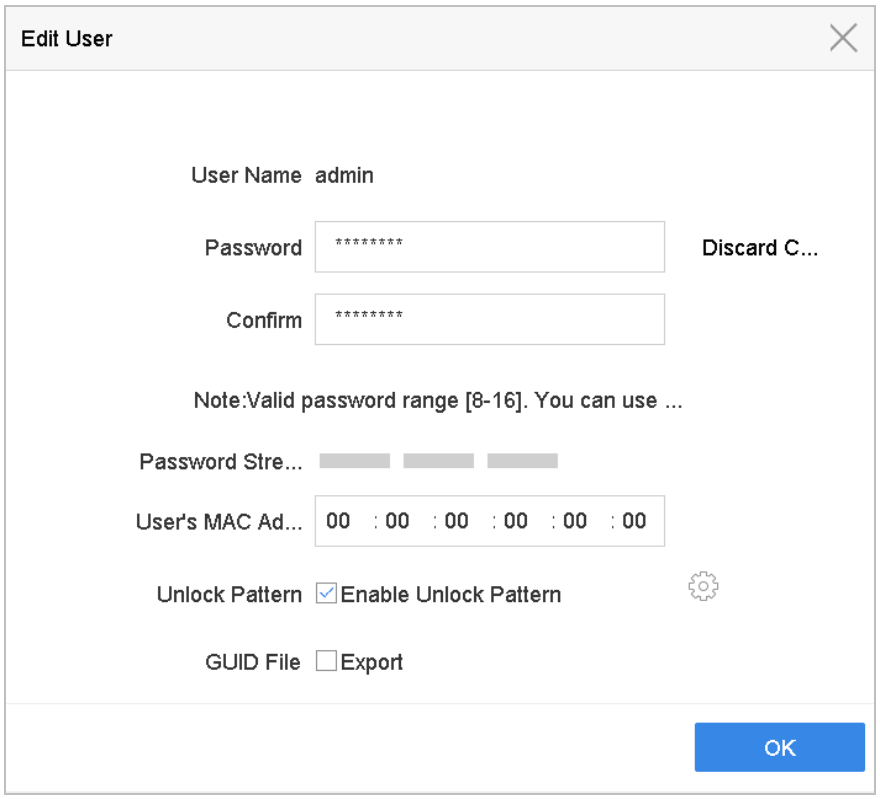


Figure 19-9 Edit User (Admin)

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

Step 4 Edit the unlock pattern for the admin user account.

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

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

NOTE

Refer to Chapter 3.3 Configuring the Login Unlock Pattern for detailed instructions.

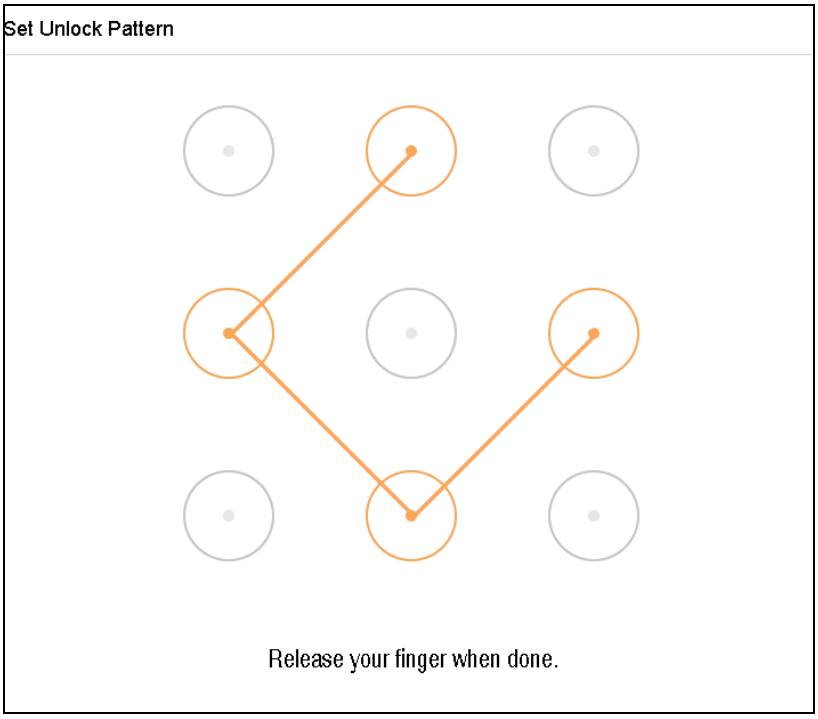


Figure 19-10 Set Admin User Unlock Pattern

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

Step 6 When the admin password is changed, export the new GUID to the connected USB flash disk in the Import/Export interface for future password resetting.

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

Step 8 For an **Operator** or **Guest** user account, click on the user management interface to edit the permissions.

19.4.5 Editing an Operator/Guest User

You can edit the user information, including user name, password, permission level, and MAC address. Check the **Change Password** checkbox to change the password, and input the new password in the **Password** and **Confirm** text fields. A strong password is recommended.

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

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

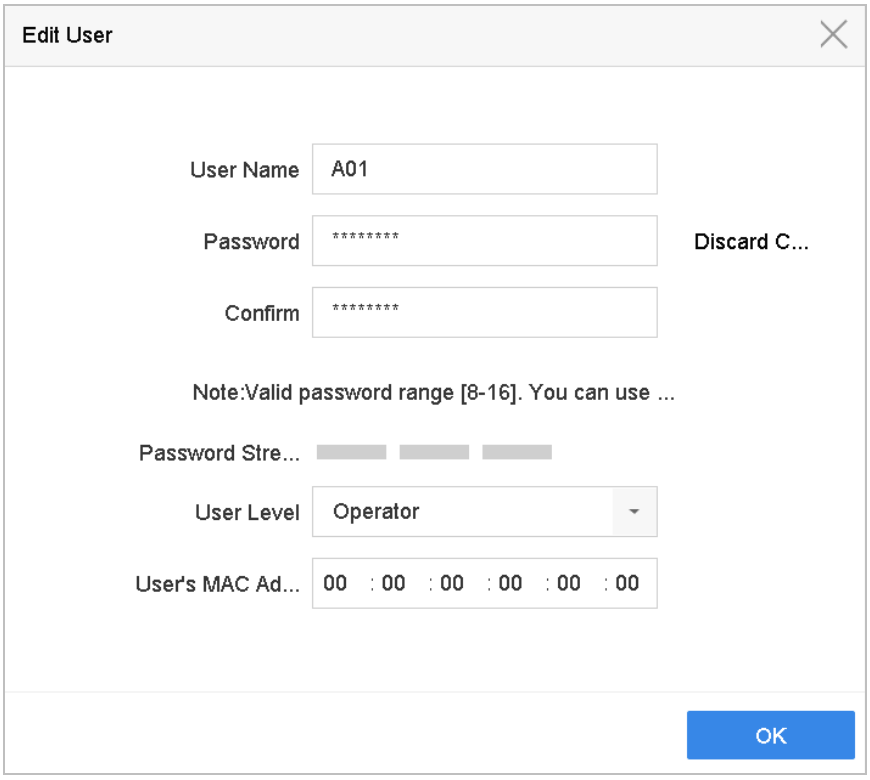


Figure 19-11 Edit User (Operator/Guest)

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

19.4.6 Deleting a User

The admin user account has 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.

Chapter 20 Appendix

20.1 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the device, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium that stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext 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 to establish a PPP connection over Ethernet protocol.
- **Hybrid device:** A hybrid device is a combination of a DVR and device.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60 Hz.
- **Device:** 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. A PAL signal contains 625 scan lines at 50 Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down, and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

20.2 Troubleshooting

- No image displayed on 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 to the monitor via HDMI or VGA cable.

  Step 2 If not, connect the device to the monitor and reboot.

  Step 3 Verify the connection cable is good.

  Step 4 If there is still no image displayed on the monitor after rebooting, check if the connection cable is good, and change the cable and connect again.

  Step 5 Verify Input mode of the monitor is correct.

  Step 6 Check that the monitor input mode matches the output mode of the device (e.g., if the device's output mode is HDMI, then the monitor input mode must be HDMI). If not, modify the monitor's input mode.

  Step 7 Check if the fault is solved by step 1 to step 3.

  Step 8 If it is solved, finish the process.

  Step 9 If not, contact a Hikvision engineer for further process.

- There is an audible warning sound "Di-Di-Di-DiDi" after a new 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.

  Step 1 Verify at least one HDD is installed in the device.

  – If not, install a compatible HDD.

  NOTE

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

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

Step 2 Verify the HDD is initialized.

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

2) If the HDD status is "Uninitialized," check the checkbox of the corresponding HDD and click **Init**.

Step 3 Verify the HDD is detected and is in good condition.

1) Select **Menu > Storage > Storage Device**.

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

Step 4 Check if the fault is solved by step 1 to step 3.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for 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 connection.

– 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).

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

3) If there exists return information and the time value is small, the network is normal.

Step 2 Verify the configuration parameters are correct.

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

2) Verify the parameters are the same as those of the connected IP devices, including IP address, protocol, management port, user name, and password.

Step 3 Verify 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 step 1 to step 3.

3) If it is solved, finish the process.

4) If not, contact a Hikvision engineer for further process.

- The IP camera frequently goes online and offline and the status displays as "Disconnected."

  Possible Reasons:

  – The IP camera and the device versions are not compatible.

  – Unstable IP camera power supply.

  – Unstable network between IP camera and device.

  – Limited flow by the switch connected with IP camera and device.

  Step 1 Verify the IP camera and the device versions are compatible.

  1) Go to **Menu > Camera**, and view the firmware version of the connected IP camera.

  2) Go to **Menu > Maintenance > System Info > Device Info** and view the firmware version of the device.

  Step 2 Verify that the IP camera power supply is stable.

  1) Verify the power indicator is normal.

  2) When the IP camera is offline, try the ping command on a PC to check if the PC connects to the IP camera.

  Step 3 Verify that the network between the IP camera and device is stable.

  1) When the IP camera is offline, connect a PC and the device with an RS-232 cable.

  2) Open the Super Terminal and use the ping command to keep sending large data packages to the connected IP camera, and check if there is packet loss.

  NOTE

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

Example: Input ping 172.6.22.131 –l 1472 –f.

Step 4 Verify the switch is not configured for flow control.

1) Check the brand and model of the switch connecting the IP camera and the device, and contact the manufacturer of the switch to check if it has a flow control function. If so, turn it down.

Step 5 Check if the fault is solved by step 1 to step 4.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for further process.

- No monitor is connected to the device locally, and when you manage the IP camera to connect with the device by Web browser remotely, the status displays as Connected. If you then connect the device with the monitor via the VGA or HDMI interface and reboot the device, there is a black screen with the mouse cursor.

- Connect the device with the monitor before startup via the VGA or HDMI interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connected. If you then connect the device with CVBS, there is a black screen.

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 local operation of the device.

Different camera orders and window-division modes can be set for different output interfaces separately, and digits such as "D1"and "D2" stand 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.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for further process.

- Live view becomes stuck when video is output locally.

Possible Reasons:

– Poor network between the device and IP camera, and there is packet loss during the transmission.

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

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

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

2) Open the Super Terminal, and execute the command "**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.

1) 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.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for further process.

- Live view is stuck when video is output remotely via 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 hardware used is not good enough, including CPU, memory, etc.

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

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

2) Open the Super Terminal, and execute the command "**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 network between the device and the PC is connected.

1) Open the cmd window in the Start menu, or press "windows + R" shortcut key to open it.

2) Use the ping command to send large packets to the device, execute the command "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 3 Verify the hardware of the PC is adequate.

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

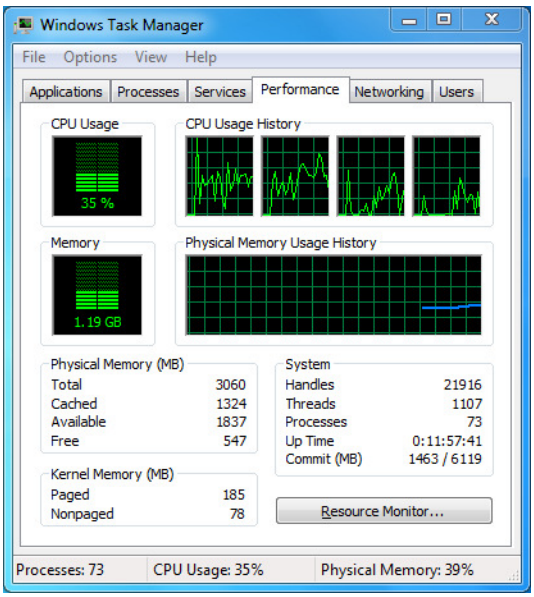


Figure 20-1 Windows task management interface

2) Select the "Performance" tab; check the status of the CPU and memory.

3) If the resource is not enough, end unnecessary processes.

Step 4 Check if the fault is solved by the above steps.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for further process.

- When using the device to get the Live View audio, there is no sound, 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 by the device.

Step 1 Verify the cable between the pickup and IP camera is connected well and impedance matches and is compatible.

1) Log in the IP camera directly, and turn the audio on. Check if the sound is normal. If not, contact the IP camera manufacturer.

Step 2 Verify the setting parameters are correct.

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

Step 3 Verify the IP camera's audio encoding standard is supported by the device.

1) 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, log in the IP camera to configure it to a supported standard.

Step 4 Check if the fault is solved by the above steps.

1) If it is solved, finish the process.

2) If not, contact a Hikvision engineer for further process.

- The image gets stuck when the device is playing back 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 4CIF resolution, if you want 16-channel synchronize playback at 720p resolution, frame extracting may occur, which leads to the image being slightly stuck.

  Step 5 Verify the network between the device and the IP camera is connected.

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

  2) Open the Super Terminal, and execute the command "**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.

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

Step 7 Verify the hardware supports the playback.

1) Reduce the channel number of playback.
2) Go to **Menu > Camera > Encoding Parameters**, and set a lower bitrate and resolution.

Step 8 Reduce the number of local playback channels.

1) Go to **Menu > Playback**, and uncheck unnecessary channel checkboxes.

Step 9 Check if the fault is solved by the above steps.

1) If it is solved, finish the process.
2) If not, contact a Hikvision engineer for further process.

- No record file is found in device's local HDD, and a "No record file found" prompt is displayed.

Possible Reasons:

– The time setting of system is incorrect.

– The search condition is incorrect.

– The HDD is in error or not detected.

Step 1 Verify the system time setting is correct.

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

Step 2 Verify the search condition is correct.

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

Step 3 Verify that the HDD status is normal.

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

Step 4 Check if the fault is solved by the above steps.

1) If it is solved, finish the process.
2) If not, contact a Hikvision engineer for further process.

First Choice for Security Professionals