Network Video Recorder

User Manual

User Manual

About this Manual

This Manual is applicable to Network Video Recorder (NVR).
The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).
Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
Other trademarks and logos mentioned below are the properties of their respective owners.
HDMI : The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, 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 is applicable to the models listed in the following table.

Series	Model
iDS-6700NXI-I/8F(B)	iDS-6708NXI-I/8F(B)
iDS-6716NXI-I/16S(B)	iDS-6716NXI-I/16S(B)
iDS-7700NXI-I4/16P/16S(B)	iDS-7716NXI-I4/16P/16S(B)
	iDS-7732NXI-I4/16P/16S(B)
iDS-7700NXI-I4/16P/X(B)	iDS-7716NXI-I4/16P/X(B)
	iDS-7732NXI-I4/16P/X(B)
iDS-7700NXI-I4/16S(B)	iDS-7716NXI-I4/16S(B)
	iDS-7732NXI-I4/16S(B)
iDS-7700NXI-I4/X(B)	iDS-7716NXI-I4/X(B)
	iDS-7732NXI-I4/X(B)
iDS-9600NXI-I8/4F(B)	iDS-9608NXI-I8/4F(B)
	iDS-9616NXI-I8/4F(B)
	iDS-9632NXI-I8/4F(B)

iDS-9600NXI-I8/8F(B)	iDS-9616NXI-I8/8F(B)
	iDS-9632NXI-I8/8F(B)
	iDS-9664NXI-I8/8F(B)
iDS-9600NXI-I8/X(B)	iDS-9616NXI-I8/X(B)
	iDS-9632NXI-I8/X(B)
	iDS-9664NXI-I8/X(B)
iDS-9600NXI-I8/16S(B)	iDS-9616NXI-I8/16S(B)
	iDS-9632NXI-I8/16S(B)
	iDS-9664NXI-I8/16S(B)
iDS-9600NXI-I16/8F(B)	iDS-9616NXI-I16/8F(B)
	iDS-9632NXI-I16/8F(B)
	iDS-9664NXI-I16/8F(B)
iDS-9600NXI-I16/X(B)	iDS-9616NXI-I16/X(B)
	iDS-9632NXI-I16/X(B)
	iDS-9664NXI-I16/X(B)
iDS-9600NXI-I16/16S(B)	iDS-9616NXI-I16/16S(B)
	iDS-9632NXI-I16/16S(B)
	iDS-9664NXI-I16/16S(B)
iDS-96000NXI-I16(B)	iDS-96064NXI-I16(B)
	iDS-96128NXI-I16(B)
iDS-96000NXI-I24(B)	iDS-96128NXI-I24(B)
	iDS-96256NXI-I24(B)

Symbol Conventions

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

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

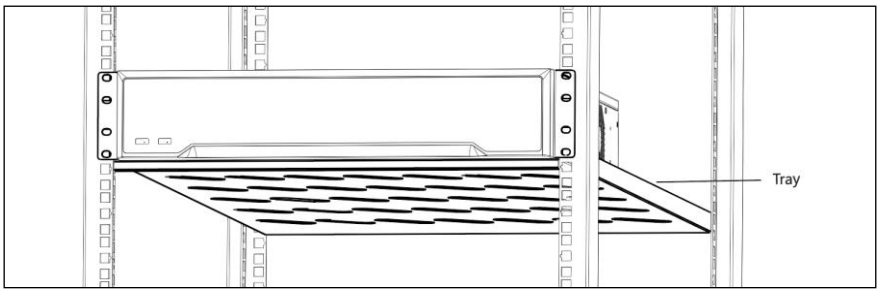
Safety Instructions

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

Preventive and Cautionary Tips

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

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


Tray

-

Product Key Features

General

- Connectable to network cameras, network dome and encoders.
- Connectable to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF protocol.
- Connectable to the smart IP cameras.
- H.265+/H.265/ H.264+/H.264/MPEG4 video formats
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 32 network cameras can be added according to different models.
- 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

- Provide HDMI/VGA1 and HDMI2/VGA2 outputs (except iDS-6716NXI-I/16S(B) series).
- HDMI Video output at up to 4K resolution (except iDS-6716NXI-I/16S(B) series).
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable.
- Live view screen can be switched in group. Manual switch and auto-switch are provided and the auto-switch interval is configurable.
- 3D positioning.
- Configurable main stream and sub-stream for the live view.
- Quick setting menu is provided for 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 mouse.

HDD Management

- Up to 16 SATA hard disks and 1 eSATA disk can be connected.
- 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 capacity can be assigned to different channel.
- RAID0, RAID1, RAID5, RAID6 and RAID 10 are supported.
- Hot-swappable RAID storage scheme, and can be enabled and disabled on your demand. And 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, and VCA.
- 8 recording time periods with separated recording types.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files 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.
- Normal/important/custom video playback mode.
- Searching and playing back record files by channel number, recording type, start time, end time, etc.
- Supports the playback by main stream or sub stream.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
- 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.
- Supports enabling H.264+ to ensure high video quality with lowered bitrate.

Files Management

- Important files search and export.
- Vehicle detection files and human appearance files search and export.
- 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, HDD error, and HDD full, etc.
- VCA detection alarm is supported.
- Smart analysis for people counting and heat map.
- Connectable to the thermal network camera.
- Supports the 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 email 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 the GUID file.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

Network Functions

- Two self-adaptive 10M/100M/1000Mbps 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™.
- Support 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 save the recording files in the local storage when the network is disconnected, and synchronizes the files to the device when the network is resumed.
- Remote reverse playback via RTSP.

- Supports accessing by the platform via ONVIF.
- Remote search, playback, download, locking and unlocking of the record files, and support downloading files 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 is provided to get 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 iDS-9600NXI-I8/8F(B), iDS-9600NXI-I8/X(B) and iDS-9600NXI-I8/16S(B) Series

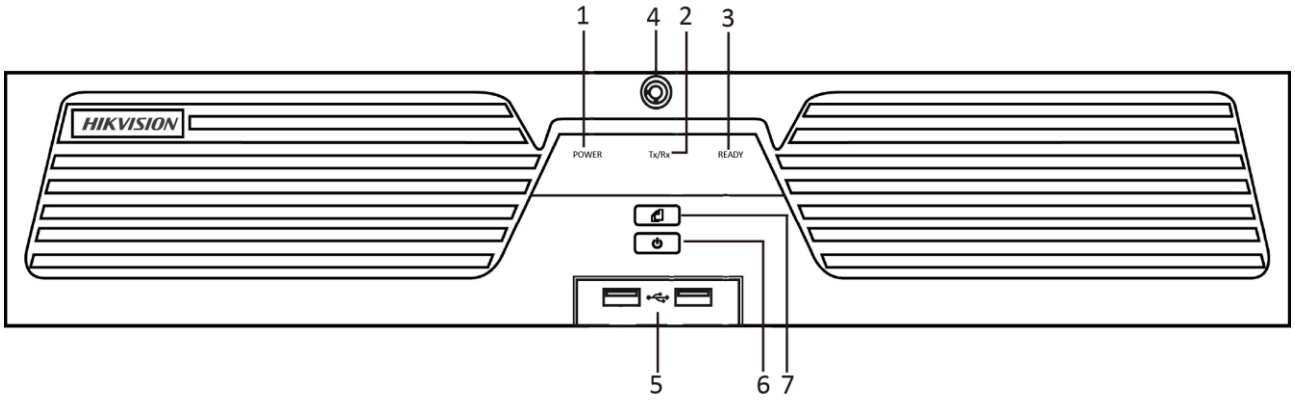


Figure 1-1 Front Panel

Table 1-1 Panel Description

No.	Name	Function Description
1	POWER	Turns red when the power is connected but the system isn't running; turns blue when the power is connected and the system is running.
2	Tx/Rx	Flickers blue when network connection is functioning properly.
3	READY	Turns blue when the device is functioning properly.
4	Front Panel Lock	Locks or unlocks the panel by the key.
5	USB Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	POWER ON/OFF	Long press the button for more than 3 seconds to turn on/off the NVR.
7	Backup	Back up video files.

1.1.2 iDS-9600NXI-I16/8F(B), iDS-9600NXI-I16/X(B) and iDS-9600NXI-I16/16S(B) Series

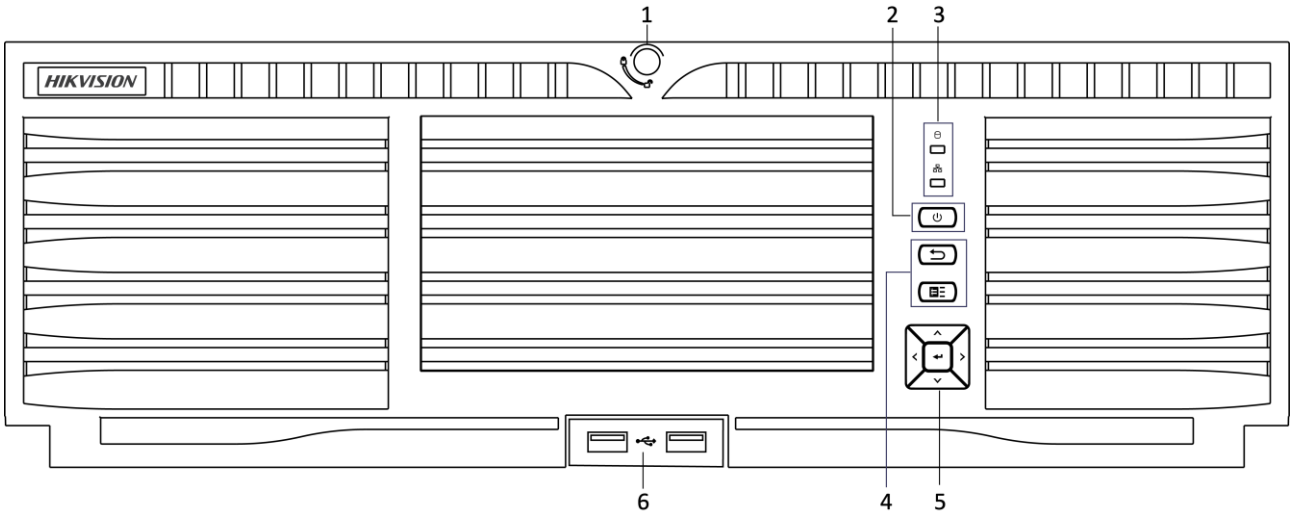


Figure 1-2 Front Panel

Table 1-2 Description

No.	Name		Description
1	Panel Lock		Locks or unlocks the panel by the key.
2	Power Switch		Powers on/off device. Solid blue indicates device is powered on. Solid red indicates device is shut down.
3	Status Indicator	HDD	• Solid red: At least one HDD is installed. • Unlit: No HDD is detected. • Flashing red: HDD is reading/writing.
		Tx/Rx	Flashing blue indicates network communication is normal.
4	Shortcut Button	Exit	• Returns to the previous menu. • Press it twice quickly to switch the main and auxiliary port. • In live view mode, press it to enter PTZ control interface.
		Menu	• Press it to pop up main menu. • Hold it for 5 seconds to turn on/off button sound. • During playback, press it to show/hide control panel.
5	Control	ENTER	• Confirms selection in any of the menu modes.

	Button		• Checks the checkbox fields. • Switches on/off status. • 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.
		DIRECTION	• Navigates between different fields and items in menus. • In the 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 the movement of the PTZ camera in PTZ control mode.
6	USB Interface		Universal Serial Bus (USB) interfaces for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

1.1.3 iDS-7700NXI-I4(/16P)/16S(B) and iDS-7700NXI-I4(/16P)/X(B) Series

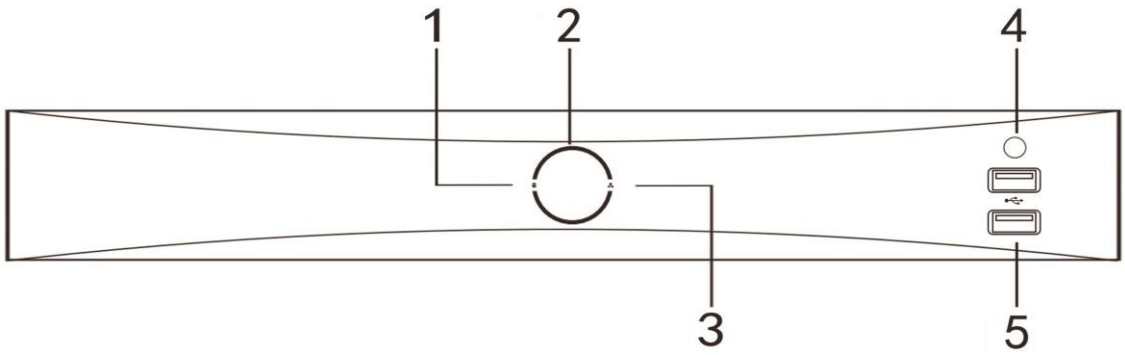


Figure 1-3 Front Panel

No.	Name	Function Description
1	HDD	Flashing white: HDD is reading/writing.
2	POWER	Turns white when the power is connected and the system is running.
3	Tx/Rx	Flickers white when network connection is functioning properly.

4	IR Receiver	Receiver for IR remote.
5	USB Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

1.1.4 iDS-6700NXI-I/8F(B) and iDS-6700NXI-I/16S(B) Series

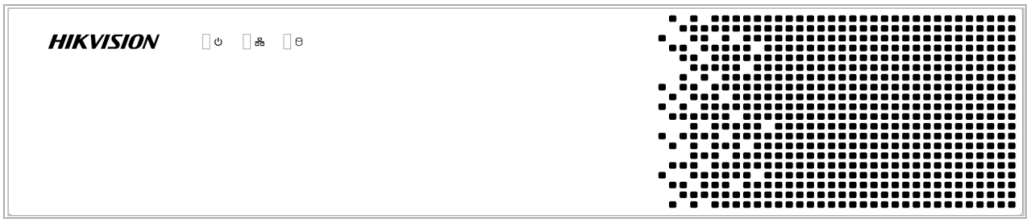


Figure 1-4 Front Panel

Table 1-3 Indicator Description

Item	Description
	Turns red when device is powered up.
	Turns red when data is being read from or written to HDD.
	Flickers blue when network connection is functioning properly.

1.1.5 iDS-9600NXI-I8/4F(B)

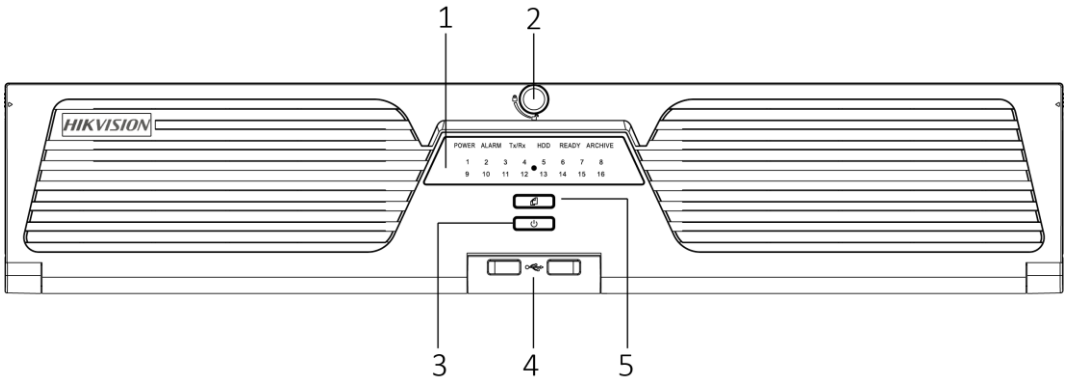


Figure 1-5 Front Panel

Table 1-4 Panel Description

No.	Name	Function Description
1	POWER	Turns red when the power is connected but the system is not running; turns blue when the power is connected and the system is running.
	ALARM	Solid red indicates alarm occurs.
	Tx/Rx	Flickers blue when network connection is functioning properly.
	HDD	• Solid red: At least one HDD is installed. • Unlit: No HDD is detected. • Flashing red: HDD is reading/writing.
	READY	Turns blue when the device is functioning properly.
	ARCHIVE	Reserved.
	Channel Status Indicator	Blue indicates recording, red indicates network connection, and purple indicates recording and network connection.
2	Front Panel Lock	Locks or unlocks the panel by the key.
3	Power Button	Long press the button for more than 3 seconds to turn on/off the NVR.
4	USB Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
5	Backup	Reserved.

1.1.6 iDS-96000NXI-I16(B)

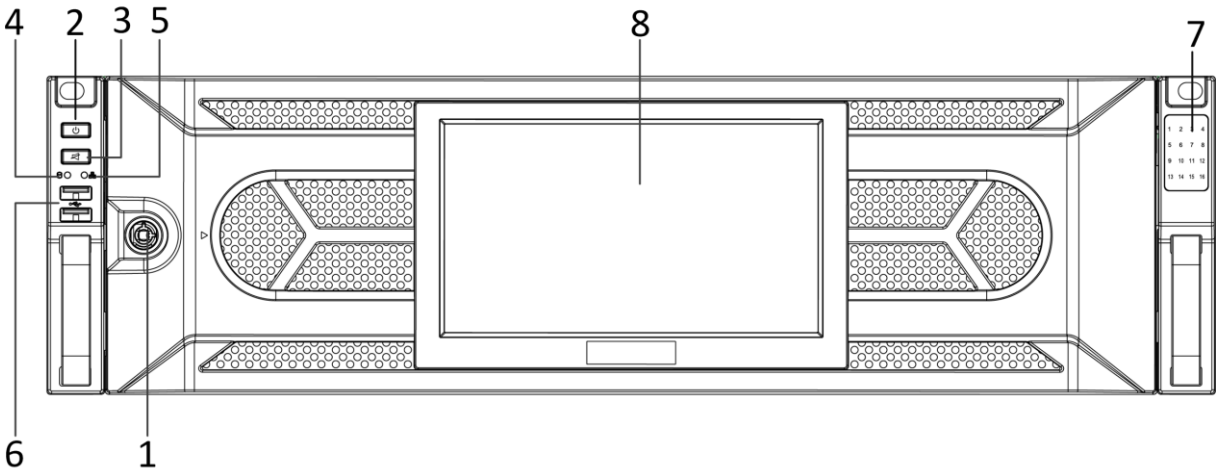


Figure 1-6 Front Panel

Table 1-5 Panel Description

No.	Name	Function Description
1	Front Panel Lock	Locks or unlocks the panel by the key.
2	Power Button	Turn on/off device. Solid blue: Device is on. Solid red: Device is off.
3	Mute Button	Turn on/off alarm beep. Solid blue: Alarm sound is off. Unlit: Alarm sound is on.
4	HDD Indicator	Solid red: At least one HDD is installed. Unlit: No HDD is detected. Flashing red: HDD is reading/writing.
5	Tx/Rx	Flashing blue: Network transmission is normal.
6	USB Interface	USB 2.0 interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	HDD Sequence Indicator	Shows the HDD sequence.
8	LCD	7-inch LCD for live-view image and menu operation.

1.1.7 iDS-96000NXI-I24(B)

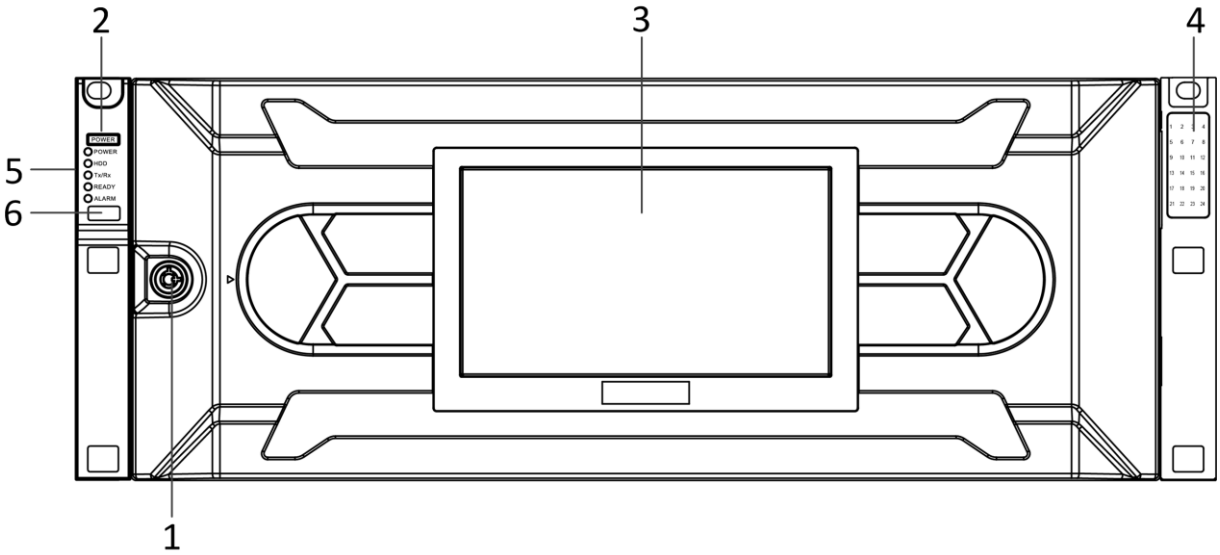


Figure 1-7 Front Panel

Table 1-6 Panel Description

No.	Name	Function Description
1	Front Panel Lock	Locks or unlocks the panel by the key.
2	Power Button	Turn on/off device. Solid blue: Device is on. Solid red: Device is off.
3	LCD	7-inch LCD for live-view image and menu operation.
4	HDD Sequence Indicator	Shows the HDD sequence.
5	Power Indicator	Flashing blue: Network transmission is normal.
	HDD Indicator	Solid red: At least one HDD is installed. Unlit: No HDD is detected. Flashing red: HDD is reading/writing.
	Tx/Rx Indicator	Flashing blue: Network transmission is normal.
	Ready Indicator	Solid blue: Device in running normally.
	Alarm Indicator	Solid red: Relay alarm occurs.
6	USB Interface	USB interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).

1)
2)
3)

1.2 IR Remote Control Operations

The device may also be controlled with the included IR remote control, shown in Figure 1-8.

NOTE

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

The IR remote 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 to a specific device by changing the Device ID#, as follows:

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

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

On the device:

Step 1 Go to System > General.

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

On the IR Remote:

Step 3 Press the DEV button.

Step 4 Use the Number buttons to enter the Device ID# that was entered into the device.

Step 5 Press Enter button to accept the new Device ID#.

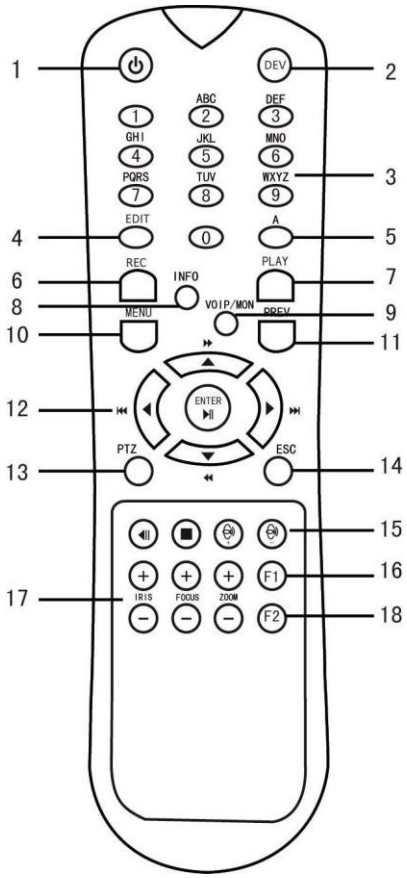


Figure 1-8 Remote Control

1.2.2 Unpairing (Disabling) an IR Remote from a Device

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

Press the DEV key on the IR Remote. 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 requires pairing to a device. See "Pairing the IR Remote to a Specific device (optional)," above.

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

Table 1-7 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 the "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 for five seconds to display the 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 Enter button (12) to accept selection. User name/password prompt depends on device is configuration. See "System Configuration" section.

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 the 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.
		Use Up/Down buttons to speed up/slow down recorded video, and Left/Right buttons to advance/rewind 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 Remote Control:

NOTE

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

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

Step 2 Go to **System** > **General** by operating the front control panel or the mouse.

Step 3 Check and remember device ID#. The default ID# is 255. This ID# is valid for all the IR remote controls.

Step 4 Press the DEV button on the remote control.

Step 5 Enter the device ID# you set in step 2.

Step 6 Press the ENTER button on the remote.

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

- 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 can’t function properly, please change a remote and try again, or contact the device provider.

1.3 USB Mouse Operation

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

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

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

The operation of the mouse:

Table 1-8 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 iDS-9600NXI-I8/8F(B), iDS-9600NXI-I8/X(B) and iDS-9600NXI-I8/16S(B) Series

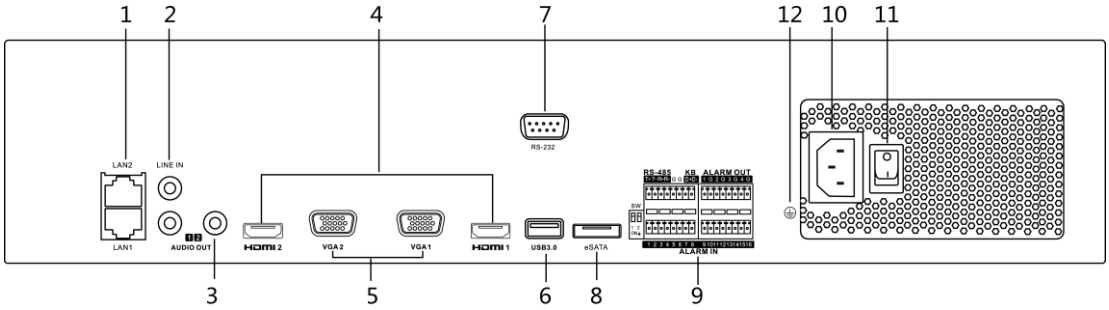


Figure 1-9 Rear Panel

Table 1-9 Panel Description

No.	Name	Description
1	LAN1/LAN2 Interface	2 RJ45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
2	LINE IN	RCA connector for audio input.
3	AUDIO OUT	2 RCA connectors for audio output.
4	HDMI1/HDMI2	HDMI video output connector.
5	VGA1/VGA2	DB9 connector for VGA output. Display local video output and menu.
6	USB 3.0 Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	RS-232 Interface	Connector for RS-232 devices.
8	eSATA	Connects external SATA HDD, CD/DVD-RM.
9	Controller Port	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next NVR.
	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	Power Supply	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.

12	GROUND	Ground (needs to be connected when NVR starts up).

1.4.2 iDS-9600NXI-I16/8F(B), iDS-9600NXI-I16/X(B) and iDS-9600NXI-I16/16S(B) Series

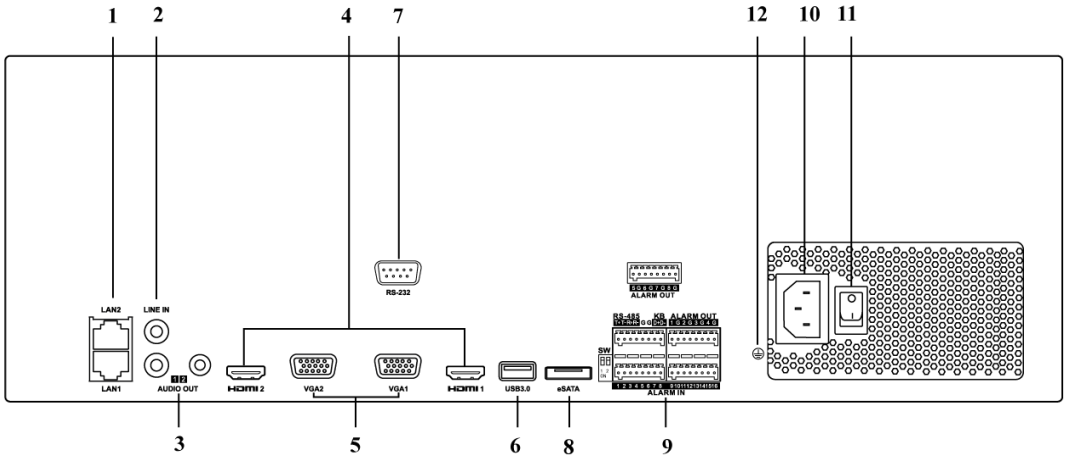


Figure 1-10 Rear Panel

Table 1-10 Panel Description

No.	Name	Description
1	LAN1/LAN2 Interface	2 RJ45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
2	LINE IN	RCA connector for audio input.
3	AUDIO OUT	2 RCA connectors for audio output.
4	HDMI1/HDMI2	HDMI video output connector.
5	VGA1/VGA2	DB9 connector for VGA output. Display local video output and menu.
6	USB 3.0 Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	RS-232 Interface	Connector for RS-232 devices.
8	eSATA	Connects external SATA HDD, CD/DVD-RM.
9	Controller Port	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next NVR.
	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.

10	Power Supply	100 to 240 VAC power supply.
11	Power Switch	Switch for turning on/off the device.
12	GROUND	Ground (needs to be connected when NVR starts up).

1.4.3 iDS-7700NXI-I4(/16P)/16S(B) and iDS-7700NXI-I4(/16P)/X(B) Series

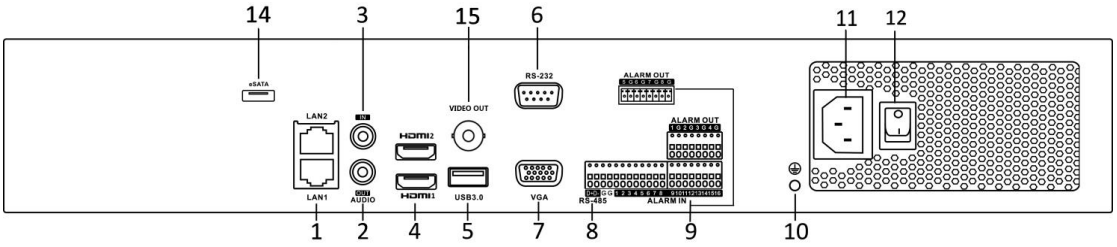


Figure 1-11 iDS-7700NXI-I4/16S(B) and iDS-7700NXI-I4/X(B) Series Rear Panel

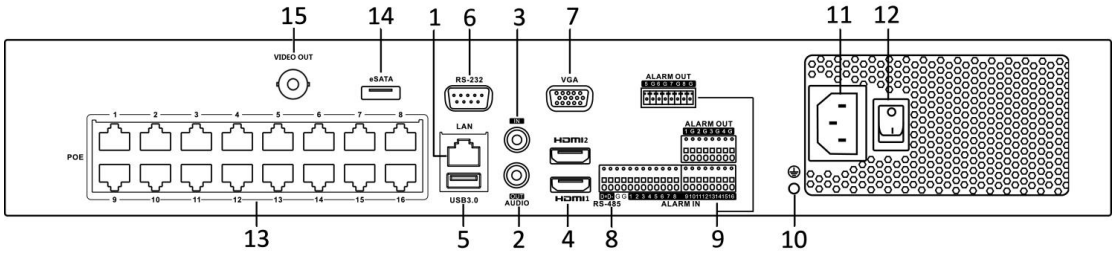


Figure 1-12 iDS-7700NXI-I4/16P/16S(B) and iDS-7700NXI-I4/16P/X(B) Series Rear Panel

Table 1-11 Panel Description

No.	Name	Description
1	LAN Interface	1 network interface provided by iDS-7700NXI-I4/16P/16S(B) and iDS-7700NXI-I4/16P/X(B) series, and 2 network interfaces by iDS-7700NXI-I4/16S(B) and iDS-7700NXI-I4/X(B) series.
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) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
6	RS-232 Interface	Connector for RS-232 devices.

7	VGA	DB9 connector for VGA output. Display local video output and menu.
8	RS-485 Interface	Half-duplex connector for RS-485 devices.
9	ALARM IN	Connector for alarm input.
	ALARM OUT	Connector for alarm output.
10	GROUND	Ground (needs to be connected when NVR starts up).
11	Power Supply	100 to 240 VAC power supply.
12	Power Switch	Switch for turning on/off the device.
13	Network Interfaces with PoE Function	Network interfaces for the cameras and to provide power over Ethernet.
14	eSATA Interface	Connects external SATA HDD, CD/DVD-RM.
15	VIDEO OUT	BNC connector for video output.

1.4.4 iDS-6700NXI-I/16S(B) and iDS-6700NXI-I/8F(B) Series

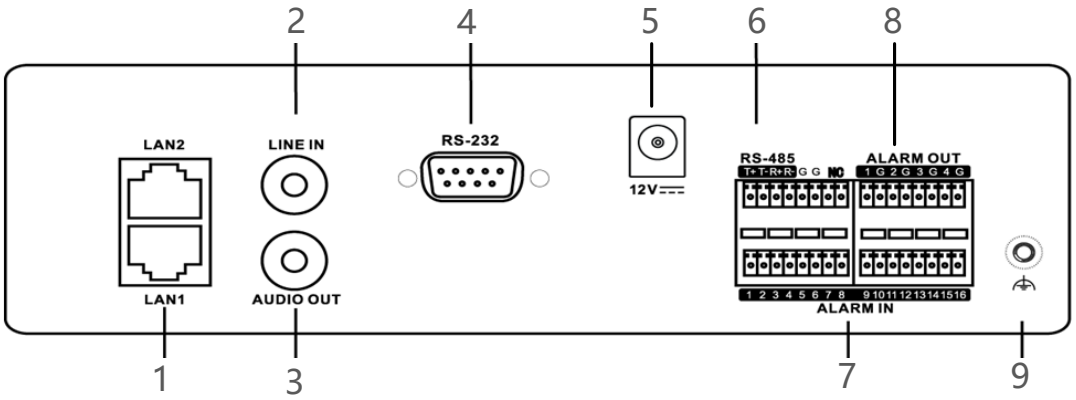


Figure 1-13 iDS-6700NXI-I/16S(B) Series Rear Panel

Table 1-12 Interface Description

Index	Item	Description
1	LAN1/LAN2	10M/100Mbps adaptive Ethernet interface.
2	LINE IN	3.5mm interface for line in; connect to audio input device or active pick-up, microphone, etc.
3	AUDIO OUT	3.5mm interface; connect to audio output device, e.g., loudspeaker, etc.
4	RS-232	Serial interface for configuration of device's parameters or used as transparent channel.
5	Power Supply	12 VDC power supply.
6	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
7	ALARM IN	Relay alarm input.
8	ALARM OUT	Relay alarm output.
9	GND	Grounding.

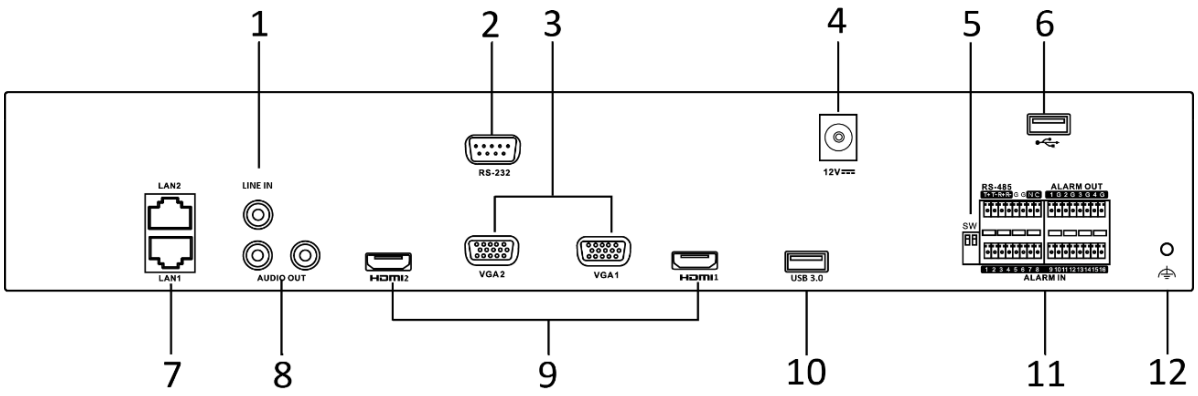


Figure 1-14 iDS-6700NXI-I/8F(B) Series Rear Panel

Table 1-13 Interface Description

Index	Item	Description
1	LINE IN	3.5mm interface for line in; connect to audio input device or active pick-up, microphone, etc.
2	RS-232	Serial interface for configuration of device's parameters or used as transparent channel.
3	VGA	DB9 connector for VGA output. Display local video output and menu.
4	Power Supply	12 VDC power supply.
5	SW	SW dial switch.
6	USB 2.0 Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	LAN1/LAN2	10/100/1000 Mbps self-adaptive Ethernet interface.
8	AUDIO OUT	3.5mm interface; connect to audio output device, e.g., loudspeaker, etc.
9	HDMI	HDMI video output connector.
10	USB 2.0 Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
11	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
	ALARM IN	Relay alarm input.
	ALARM OUT	Relay alarm output.
12	GND	Grounding.

1.4.5 iDS-9600NXI-I8/4F(B)

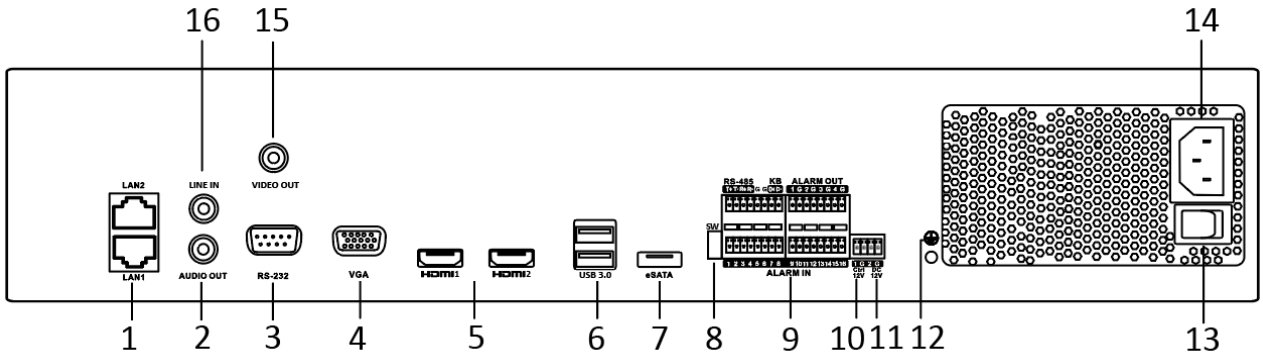


Figure 1-15 Rear Panel

Table 1-14 Panel Description

No.	Name	Description
1	LAN1/LAN2 interface	2 RJ45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
2	AUDIO OUT	2 RCA connectors for audio output.
3	RS-232 Interface	Connector for RS-232 devices.
4	VGA	DB9 connector for VGA output. Display local video output and menu.
5	HDMI1/HDMI2	HDMI video output connector.
6	USB 3.0 Interfaces	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
7	eSATA	Connects external SATA HDD, CD/DVD-RM.
8	SW	SW dial switch.
9	Controller Port	D+, D- pin connects to Ta, Tb pin of controller. For cascading devices, the first NVR's D+, D- pin should be connected with the D+, D- pin of the next NVR.
	RS-485	RS-485 serial interface; connect to pan/tilt unit, speed dome, etc.
	ALARM IN	Alarm input interface.
	ALARM OUT	Alarm output interface.
10	Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device. The power will be turned on when the

		alarm output is triggered. If the device has 4 alarm outputs, the Ctrl 12V power is controled by alarm output 5. If the device has 8 alarm outputs, the Ctrl 12V power is controled by alarm output 9. Connect positive pole to number (1) of Ctrl 12V, and connect negative pole to G of Ctrl 12V.
11	DC 12V	12 VDC, 1 A power output for external device. Connect positive pole to number (1) of DC 12V, and connect negative pole to G of DC 12V.
12	GND	Ground (needs to be connected when NVR starts up).
13	Power Switch	Switch for turning on/off the device.
14	Power Supply	100 to 240 VAC power supply.
15	VIDEO OUT	BNC connector for video output.
16	LINE IN	RCA connector for audio input.

1.4.6 iDS-96000NXI-I16(B) and iDS-96000NXI-I24(B)

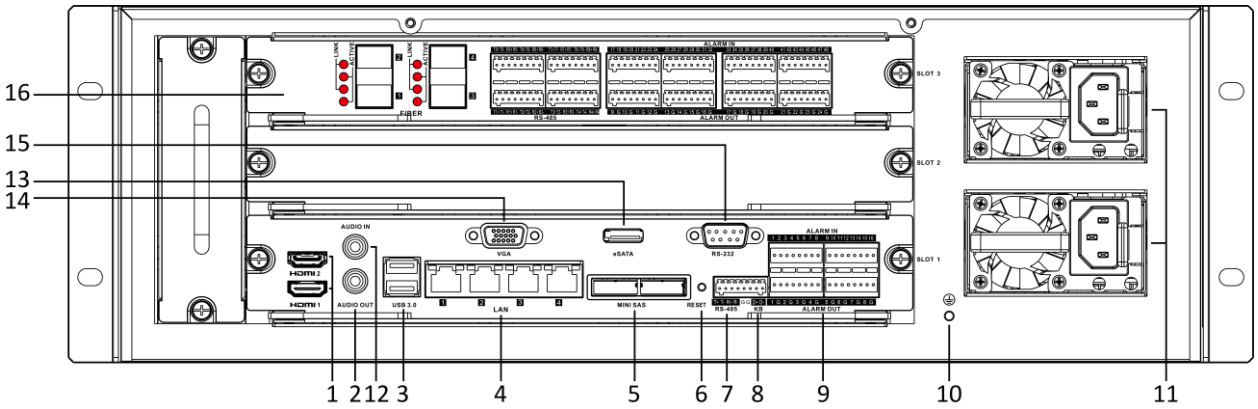


Figure 1-16 iDS-96000NXI-I16(B) Series Rear Panel

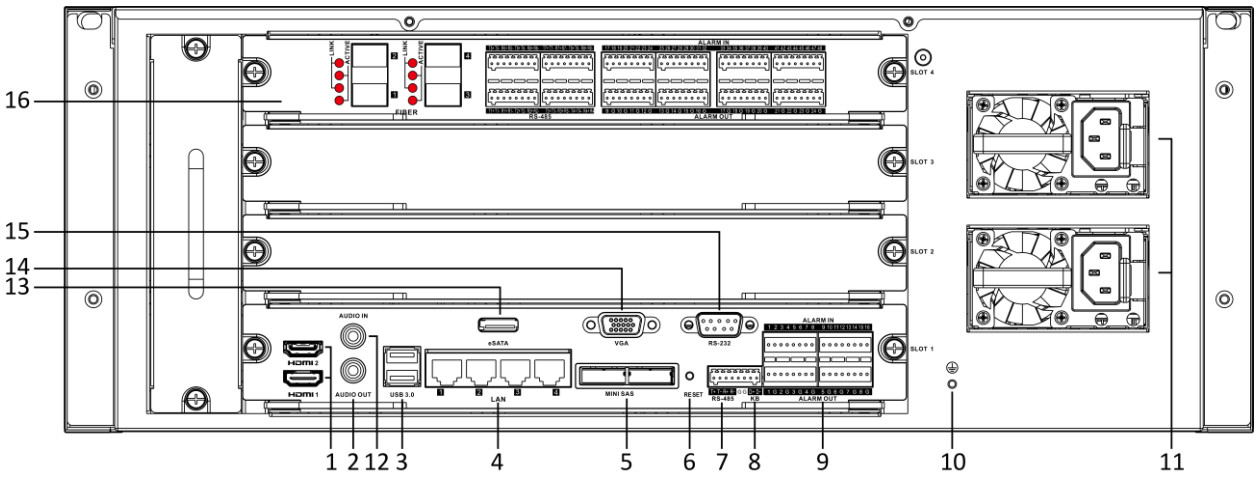


Figure 1-17 iDS-96000NXI-I24(B) Series Rear Panel

Table 1-15 Panel Description

No.	Name	Description
1	HDMI1/HDMI2	HDMI video output connector.
2	AUDIO OUT	RCA connector for audio output.
3	USB 3.0 Interface	Universal Serial Bus (USB) interface for additional devices such as USB mouse and USB Hard Disk Drive (HDD).
4	LAN Interface	4 RJ45 10/100/1000 Mbps self-adaptive Ethernet interfaces provided.
5	MiniSAS Interface	2 miniSAS interfaces
6	Reset	Reset button.
7	RS-485	RS-485 interface.

8	KB	Keyboard interface.
9	ALARM IN/OUT	Connector for alarm input/output.
10	GND	Ground (needs to be connected when NVR starts up).
11	Power Supply	100 to 240 VAC power supply.
12	AUDIO IN	RCA connector for audio input.
13	eSATA	Connects external SATA HDD, CD/DVD-RM.
14	VGA	DB9 connector for VGA output. Display local video output and menu.
15	RS-232 Interface	Connector for RS-232 devices.
16	Extension Board	4 RJ45 10/100/1000 Mbps self-adaptive optical interface, 8 × RS-485 (full-duplex), Alarm input/output: 32/16.

Chapter 2 Getting Started

2.1 Start up the Device

Purpose:

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

Before you start:

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

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

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

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

2.2 Activate the Device

Purpose:

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

Step 1 Input the same password in the text field of **Create New Password** and **Confirm New Password**.

NOTE

You can click  to show the characters input.

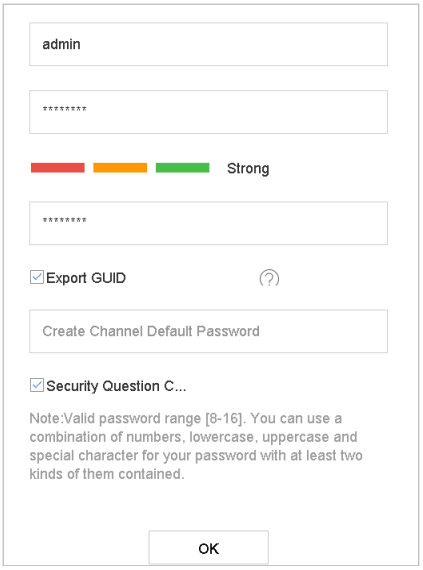


Figure 2-1 Activating the Device

WARNING

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

Step 2 In the **Create Channel Default Password** text field, create a login password for IP camera (s) connected to the device.

Step 3 (Optional) Check Export GUID and Security Question Configuration.

- **Export GUID:** export the GUID for future password resetting.
- **Security Question Configuration:** configure the security questions which can be used for resetting the password.

Step 4 Click **OK**.

What to do next:

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

NOTE

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

2.3 Configure Unlock Pattern for Login

For the admin user, you can configure the unlock pattern for device login.

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

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

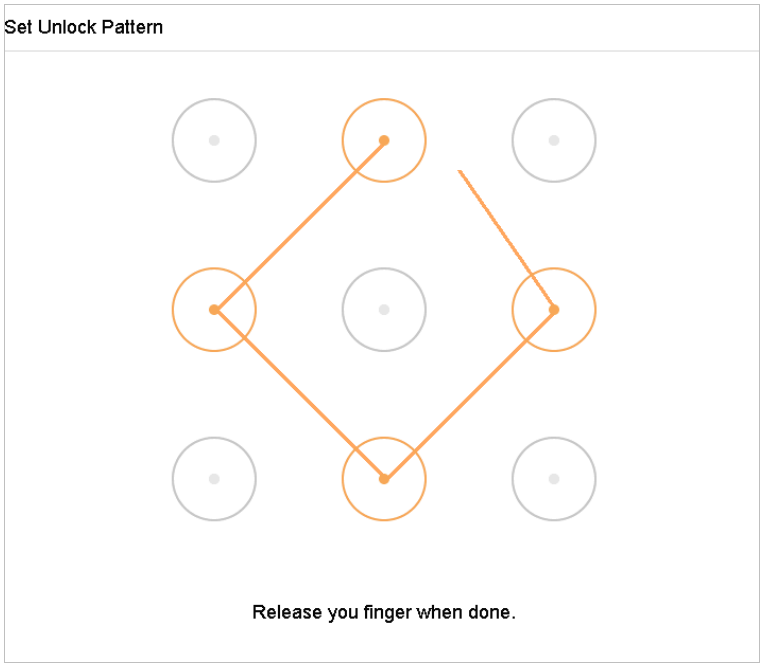


Figure 2-2 Draw the Pattern

NOTE

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

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

NOTE

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

2.4 Login to the Device

2.4.1 Log in via Unlock Pattern

NOTE

- Only the *admin* user has the permission to unlock the device.
- Please configure the pattern first before unlocking. Please refer to Chapter 2.3 Configure Unlock Pattern for Login.

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

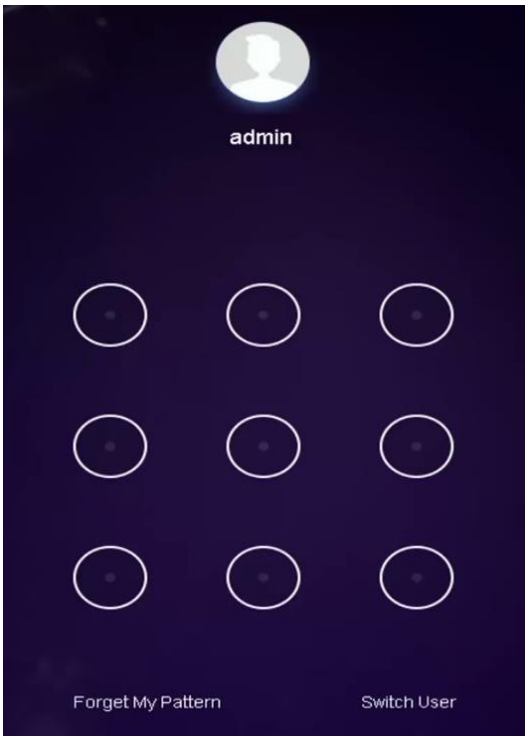


Figure 2-3 Draw the Unlock Pattern

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

NOTE

- If you have forgotten your pattern, you can select the **Forgot My Pattern** or **Switch User** option to enter the normal login dialog box.
- When the pattern you draw is different from the pattern you have configured, you should try again.
- If you have drawn the wrong pattern for more than 5 times, the system will switch to the normal login mode automatically.

2.4.2 Log in via Password

Purpose:

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

Step 1 Select the **User Name** in the dropdown list.

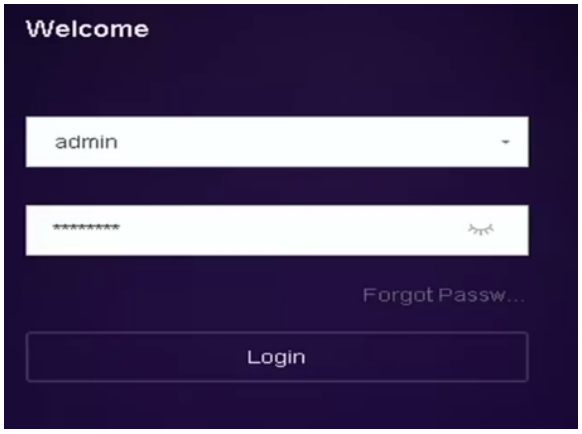


Figure 2-4 Login Interface

Step 2 Input password.

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

NOTE

- When you forget the password of the admin, you can click **Forgot Password** to reset the password.
- In the Login dialog box, if you enter the wrong password 7 times, the current user account will be locked for 60 seconds.

2.5 Enter Wizard to Configure Quick Basic Settings

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

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

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

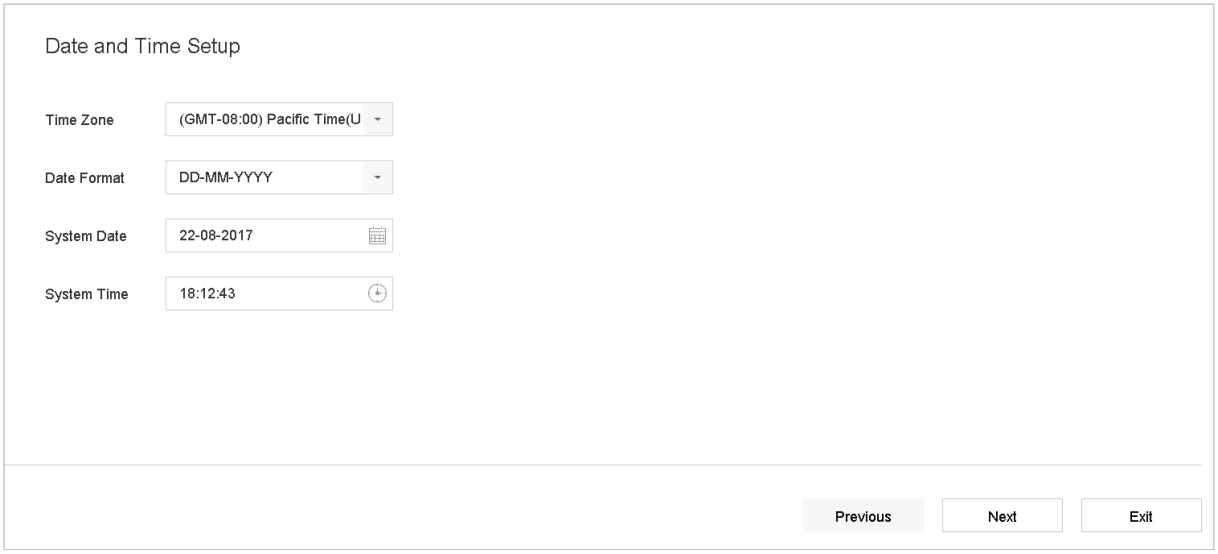


Figure 2-5 Date and Time Settings

Step 2 After the time settings, click **Next** to enter the Network Setup Wizard window, as shown in the following figure.

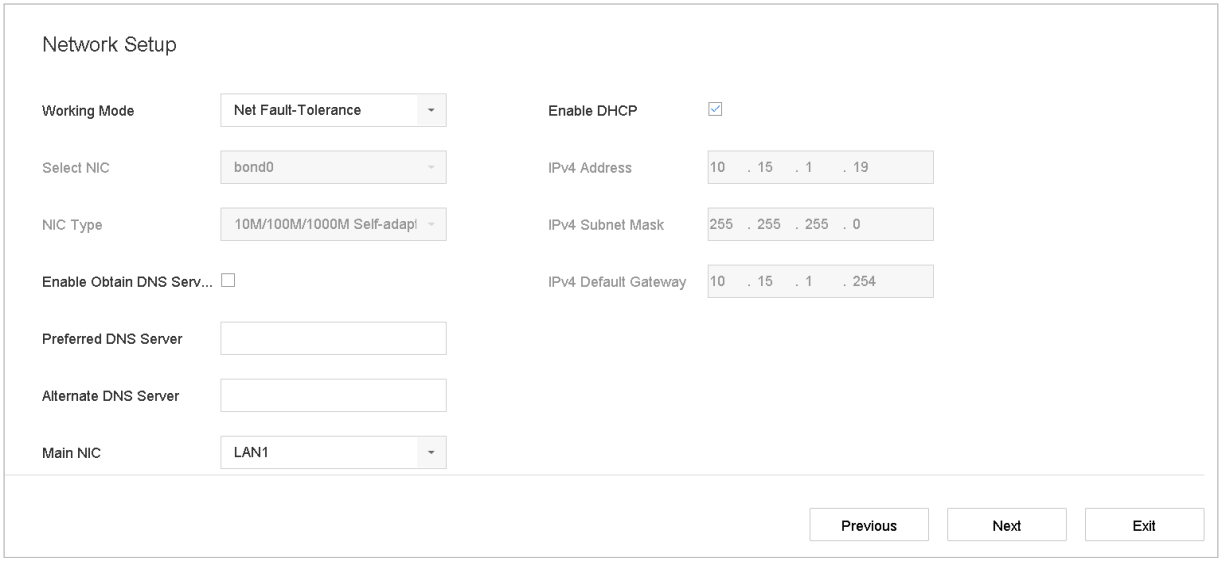


Figure 2-6 Network Settings

Step 3 Click **Next** after you configured the network parameters, which takes you to the **HDD Management** window.

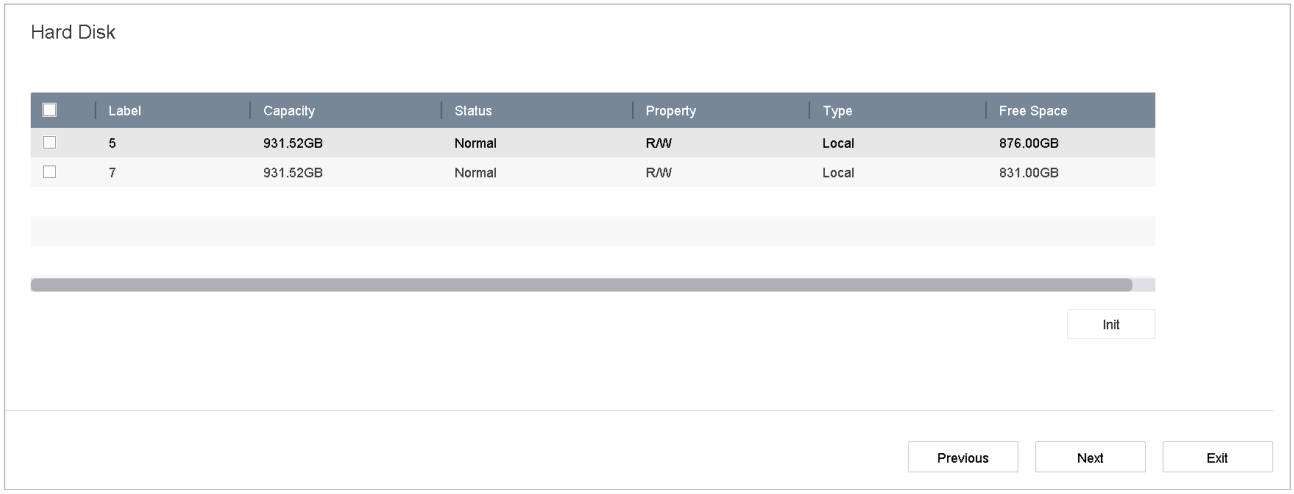


Figure 2-7 HDD Management

Step 4 To initialize the HDD, click the **Init** button. Initialization removes all the data saved in the HDD.

Step 5 Click **Next**. You enter the **Camera Setup** interface to add the IP cameras.

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

NOTE

If the camera is in inactive status, you can select the camera from the list and click **Activate** to activate the cameras.

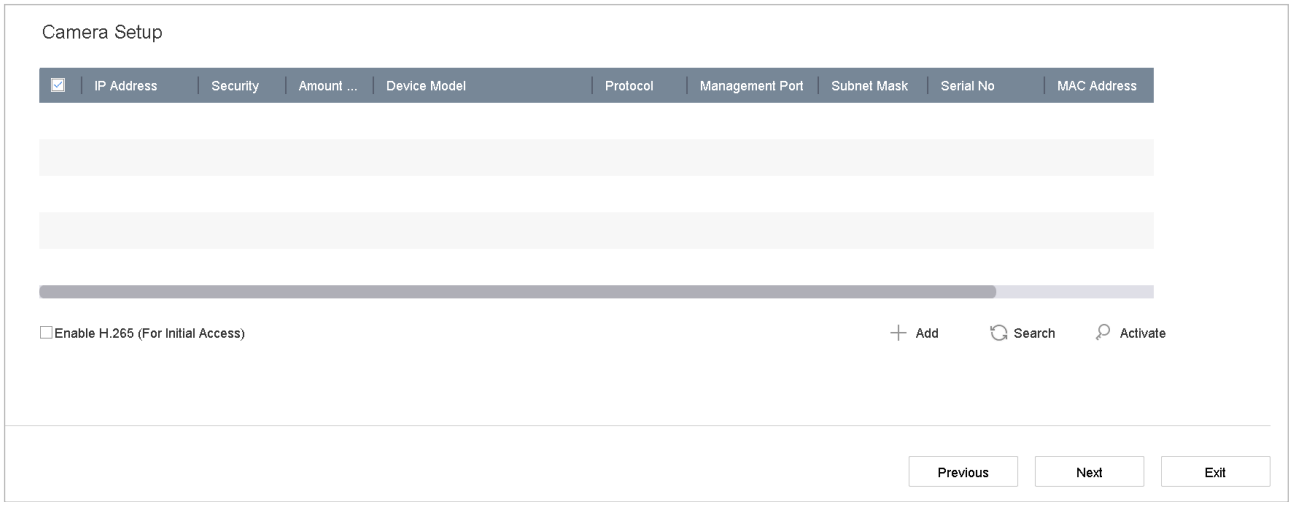


Figure 2-8 Search for IP Cameras

Step 6 Enter the Platform Access and configure the Hik-Connect settings.

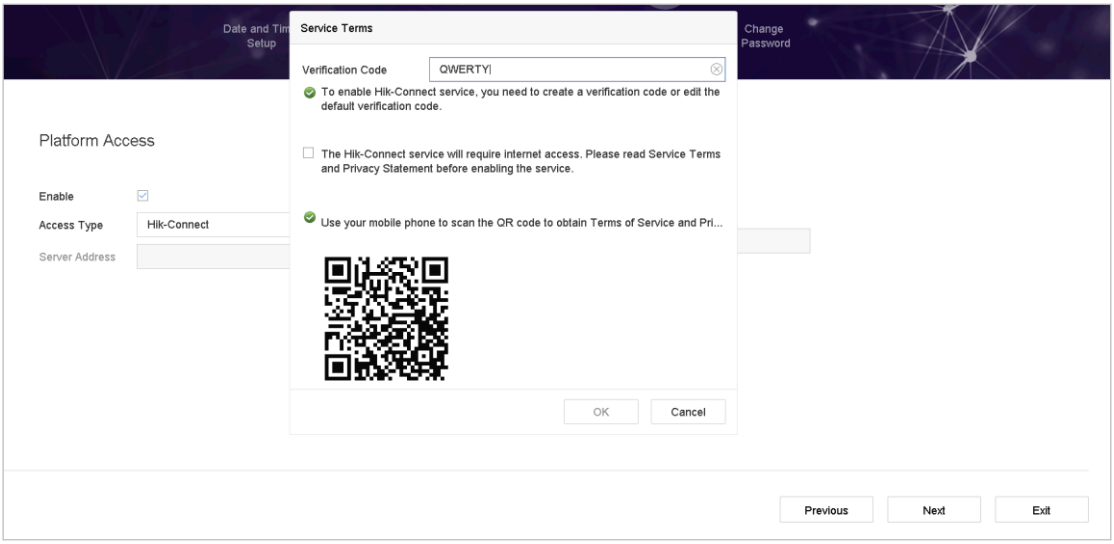


Figure 2-9 Hik-Connect Access

Step 7 Click **Next** to enter the **Change Password** interface to create the new admin password if required.

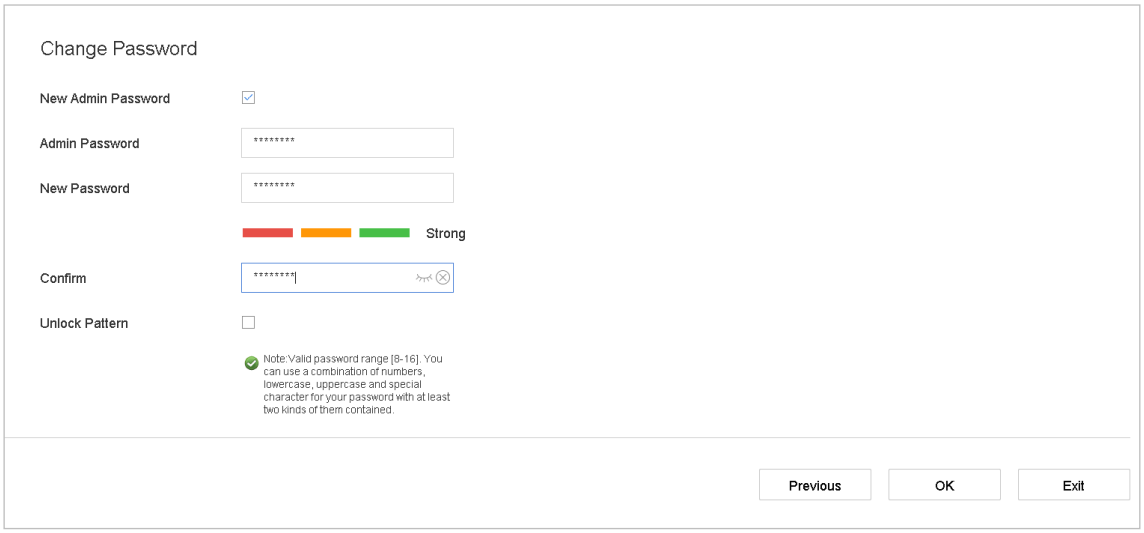


Figure 2-10 Change Password

NOTE

You can enter click the to show the characters input.

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

WARNING

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

Step 8 Click **OK** to complete the startup Setup Wizard.

2.6 Enter Main Menu

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

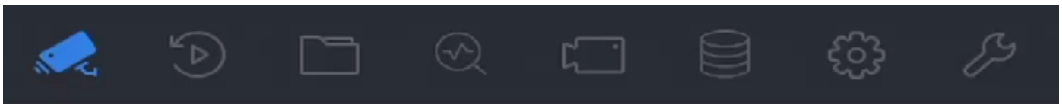


Figure 2-11 Main Menu Bar

Table 2-1 Description of Icons

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

	System Maintenance

2.7 System Operation

2.7.1 Log out

Purpose:

After logging out, the monitor turns to the live view mode and if you want to perform any operations, you need to enter user name and password log in again.

Step 1 Click  on the menu bar.

Figure 2-12 Logout

Step 2 Click **Logout**.

NOTE

After you have logged out the system, menu operation on the screen is invalid. It is required to input a user name and password to unlock the system.

2.7.2 Shut Down the Device

Step 1 Click  on the menu bar.

Figure 2-13 Shutdown Menu

Step 2 Click the **Shutdown** button.

Step 3 Click the **Yes** button.

NOTE

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

2.7.3 Reboot the Device

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

Step 1 Click  on the menu bar.

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

Chapter 3 Camera Management

3.1 Add the IP Cameras

3.1.1 Activate IP Camera

Purpose:

Before adding an IP camera, make sure the IP camera to be added is in active status.

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

Step 2 Click **Number of Unadded Online Device** on the bottom of IP camera interface.

Step 3 Check inactive cameras and click **Activate**.

Step 4 Enter the same password in Create New Password and Confirm New Password.

Or you can check Use Channel Default Password to activate the camera with channel default password.

Step 5 Click **OK.**

3.1.2 Add the IP Camera Manually

Purpose:

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

Before you start:

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

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

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

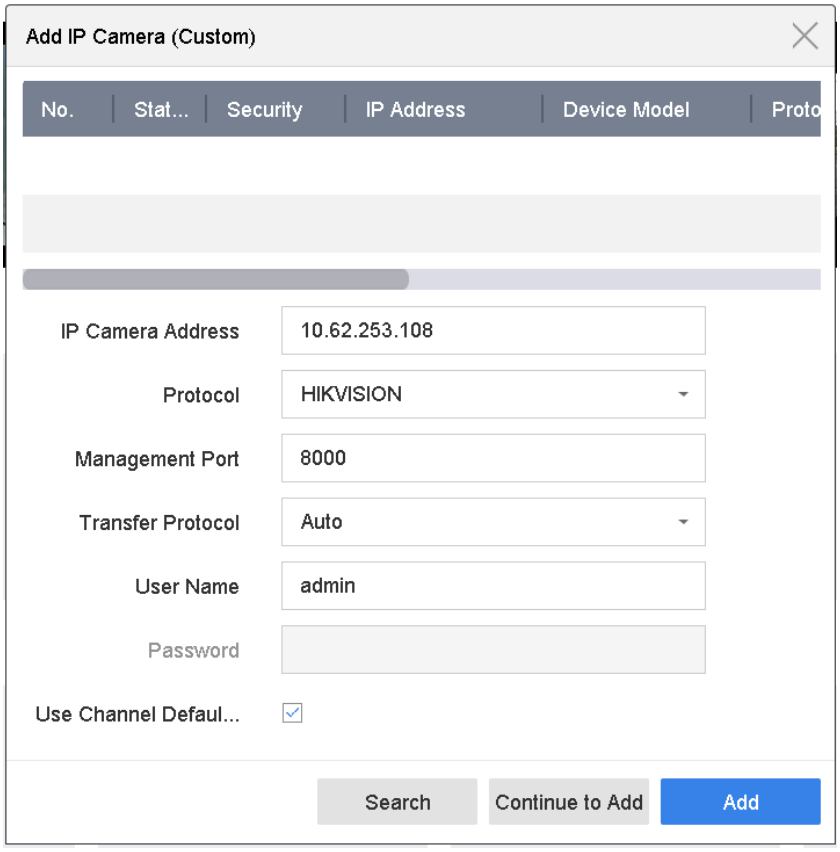


Figure 3-1 Add IP Camera

Step 3 Enter IP address, protocol, management port, and other information of the IP camera to add.

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

Or you can check **Use Channel Default Password** to add the camera with channel default password.

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

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

3.1.3 Add the Automatically Searched Online IP Cameras

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

Step 2 Select the automatically searched online devices.

Step 3 Click **Add**.

NOTE

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

3.2 Enable H.265 Stream Access

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

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

Step 2 Check Enable H.265 (For Initial Access).

Step 3 Click **OK**.

3.3 Upgrade the IP Camera

The IP camera can be remotely upgraded through the device.

NOTE

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

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

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

Step 3 Select the firmware upgrade file from the USB flash drive.

Step 4 Click **Upgrade**.

Step 5 The IP camera will reboot automatically after the upgrading completes.

3.4 Edit Channel Default Password

Purpose:

You can activate and add IP camera by the channel default password.

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

Step 2 Go to More Settings > Channel Default Password Management at the top taskbar.

Step 3 Check Change Password.

Step 4 Edit Channel Default Password.

WARNING

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

Step 5 Click **OK**.

3.5 Configure the Customized Protocols

Purpose:

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

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

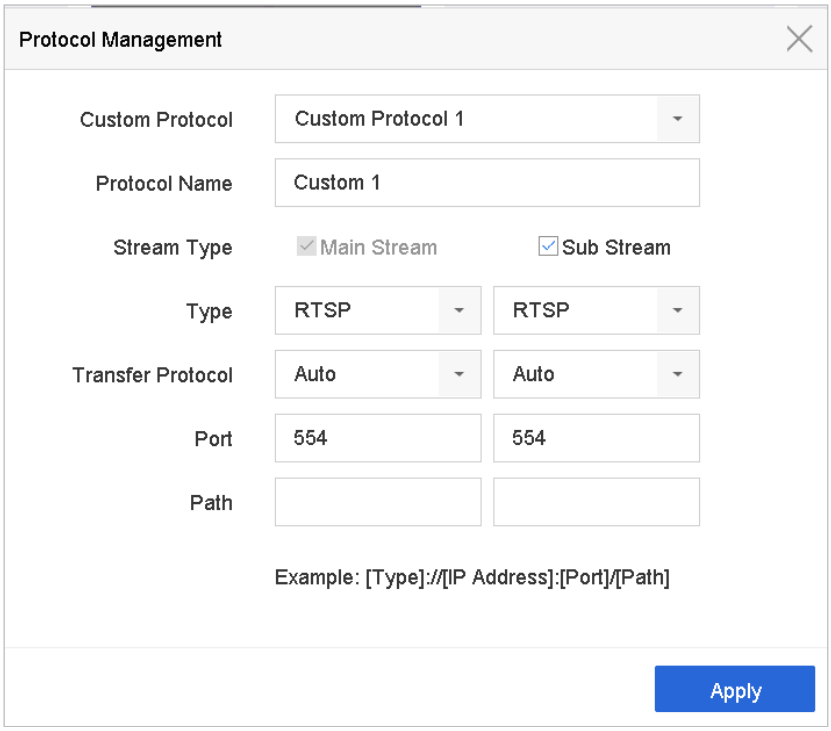


Figure 3-2 Protocol Management

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

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

NOTE

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

Result:

Step 3 After adding the customized protocols, you can see the protocol name is listed in the drop-down list.

Chapter 4 Camera Settings

4.1 Configure OSD Settings

Purpose:

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

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

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

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

Step 4 Check the checkbox of the **Display Name**, **Display Date** and **Display Week** if you want to show the information on the image.

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

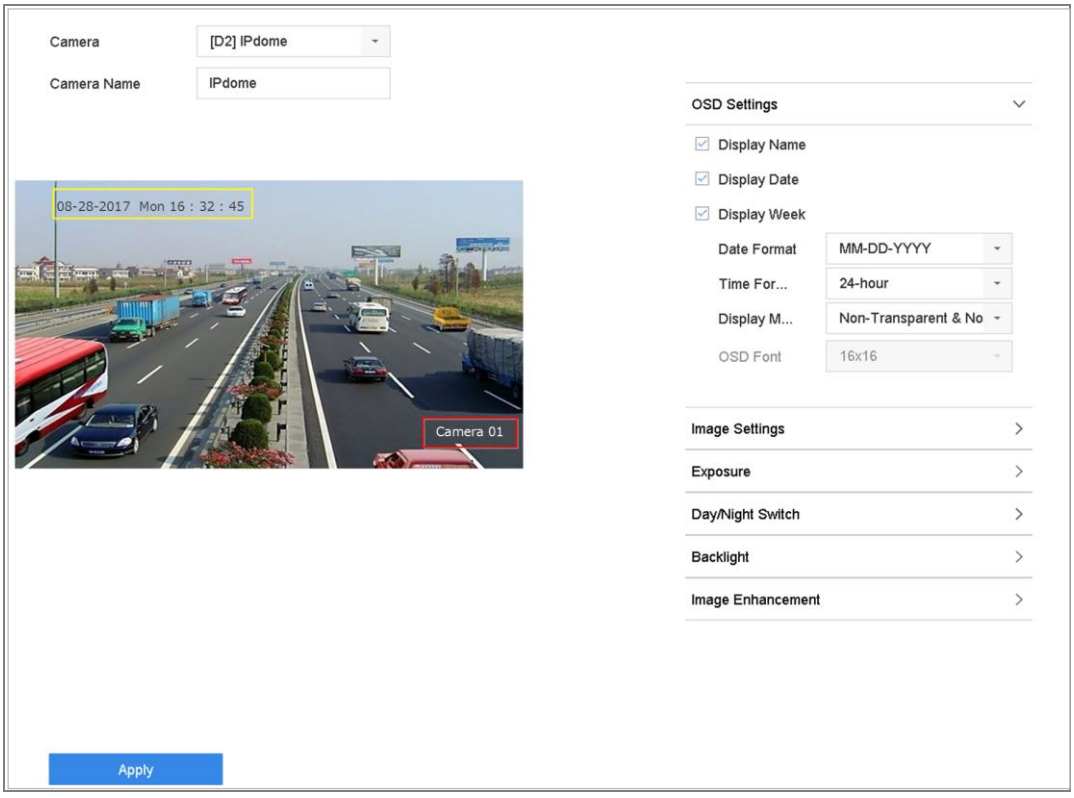


Figure 4-1 OSD Configuration Interface

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

Step 7 Click the **Apply** button to apply the settings.

4.2 Configure Privacy Mask

Purpose:

The privacy mask can be used to protect personal privacy by concealing parts of the image from view or recording with a masked area.

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

Step 2 Select the camera to set privacy mask.

Step 3 Click the checkbox of **Enable** to enable this feature.

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

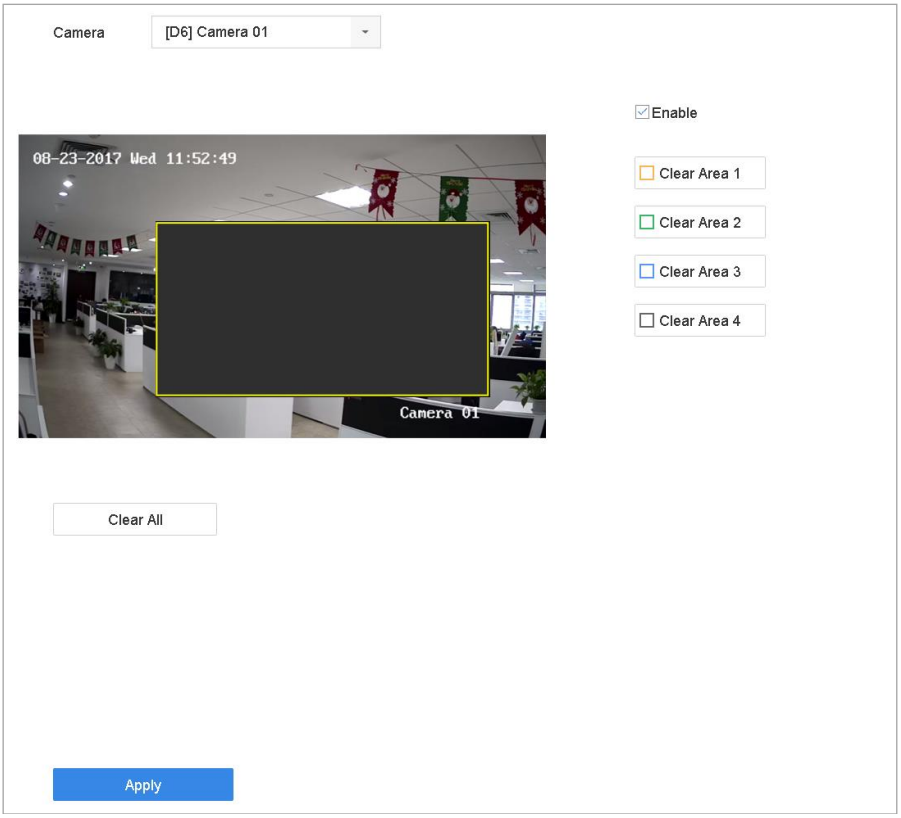


Figure 4-2 Privacy Mask Settings Interface

NOTE

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

Related Operation:

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

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

4.3 Configure the Video Parameters

Purpose:

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

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

Step 2 Select the 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.

4.4 Configure the Day/Night Switch

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

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

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

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

Auto: The camera switches between the day mode and the night mode according to the illumination automatically.

The sensitivity ranges from 0 to 7, and the higher sensitivity results in the more easily to trigger the mode switch.

The switch time refers to the interval time between the day/night switch. You can set it from 5 sec to 120 sec.

Auto-Switch: The camera switches the day mode and the night mode according to the start time and end time you set.

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

4.5 Configure Other Camera Parameters

For the 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 the camera from the drop-down list.

Step 3 Configure the camera parameters.

Exposure: Set the exposure time (1/10000 to 1 sec) of camera. The larger exposure value results in the brighter image.

Backlight: Set the wide dynamic range (0 to 100) of the camera. When the surrounding illumination and the object have larger difference in brightness, you should set the WDR value.

Image Enhancement: For optimized image contrast enhancement.

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

Chapter 5 Live View

Live view shows you the video image getting 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 the ESC many times (depending on which menu you're on) brings you to the Live View mode.

5.1 Start Live View

Step 1 The system automatically enters the live view interface when starts up, or you can click the  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 5-1 Live View

Step 4 You can use the toolbar at the window bottom to realize the capture, instant playback, audio on/off, digital zoom, live view strategy, show information and start/stop recording, etc.

5.1.2 Digital Zoom

Digital Zoom is for zooming in the live image. You can zoom in the image to different proportions (1 to 16X).

Step 1 In the live view mode, click  from the toolbar to enter the digital zoom interface.

Step 2 You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to 16X).

Figure 5-2 Digital Zoom

5.1.3 Fisheye View

The device supports the fisheye expansion for the connected fisheye camera in live view or playback mode.

NOTE

- The connected camera must support the fisheye view.
- iDS-9600NXI-I8/4F(B) series do not support fisheye view.

Step 1 In the live view mode, click the  to enter the fisheye expansion mode.

Step 2 Select the expansion view mode.

- **180° Panorama ()**: Switch the live view image to the 180° panorama view.
- **360° Panorama ()**: Switch the live view image to the 360° panorama view.
- **PTZ Expansion ()**: The PTZ Expansion is the close-up view of some defined area in the fisheye view or panorama expansion, 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.

5.1.4 3D Positioning

3D Positioning is for zooming in/out the specific area of live image.

Step 1 In the live view mode, click the  to enter the 3D positioning mode.

Step 2 Operate the zoom in/out in the image.

- Zoom in

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

- Zoom out

  Use the left key of mouse 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.

5.1.5 Live View Strategy

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

Step 2 Select the live view strategy to **Real-time**, **Balanced** or **Fluency**.

5.1.6 Target Tracking

Purpose:

The function is only available for PanoVu series network camera.

Before you start:

Add a 24 MP PanoVu series network camera to channel 1, 2, 3, or 4.

Step 1 Enter live view interface and click the  of PanoVu series network camera. The live view window will be divided into 1+5 window to show details.

Step 2 Click  to start auto-tracking.

Or click  and drag to select five area in PanoVu series network camera.

5.2 Target Detection

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

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

Step 2 Check the checkbox to select different detection types: smart detection ( ), vehicle detection ( ), facial detection ( ), and human body detection ( ).

Step 3 Select the historical analysis ( ) or real-time analysis ( ) to obtain the results. The detection results are displayed in the list.

Step 4 (Optional) Click a result in list to play the related video.

5.3 Configure Live View Settings

Live View settings can be customized according to different needs. 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**.

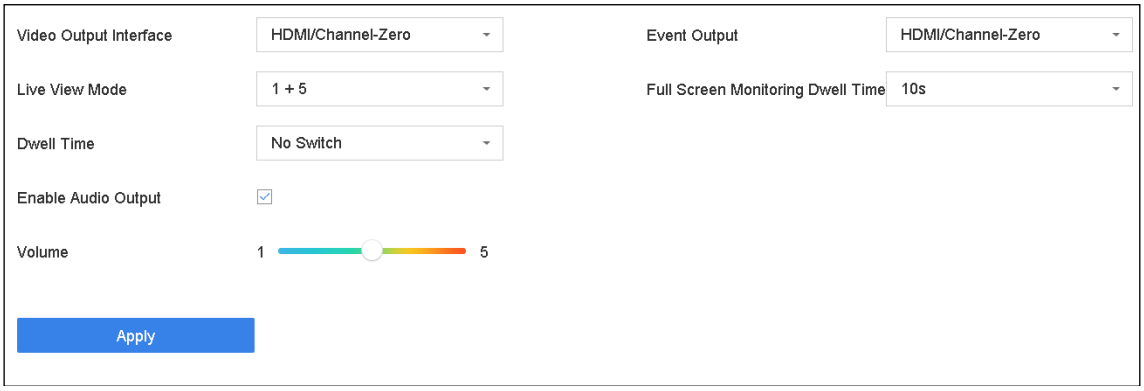


Figure 5-3 Live View-General

Step 2 Configure the live view parameters.

- **Video Output Interface:** Select the video output to configure.
- **Live View Mode:** Select the display mode for live view.
- **Dwell Time:** The time in seconds to dwell between switching of cameras when enabling auto-switch in Live View.
- **Enable Audio Output:** Enable/disable audio output for the selected video output.
- **Volume:** Adjust the volume of live view, playback and two-way audio for the selected output interface.
- **Event Output:** Select the output to show event video.
- **Full Screen Monitoring Dwell Time:** Set the time in seconds to show alarm event screen.

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

5.4 Configure Live View Layout

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

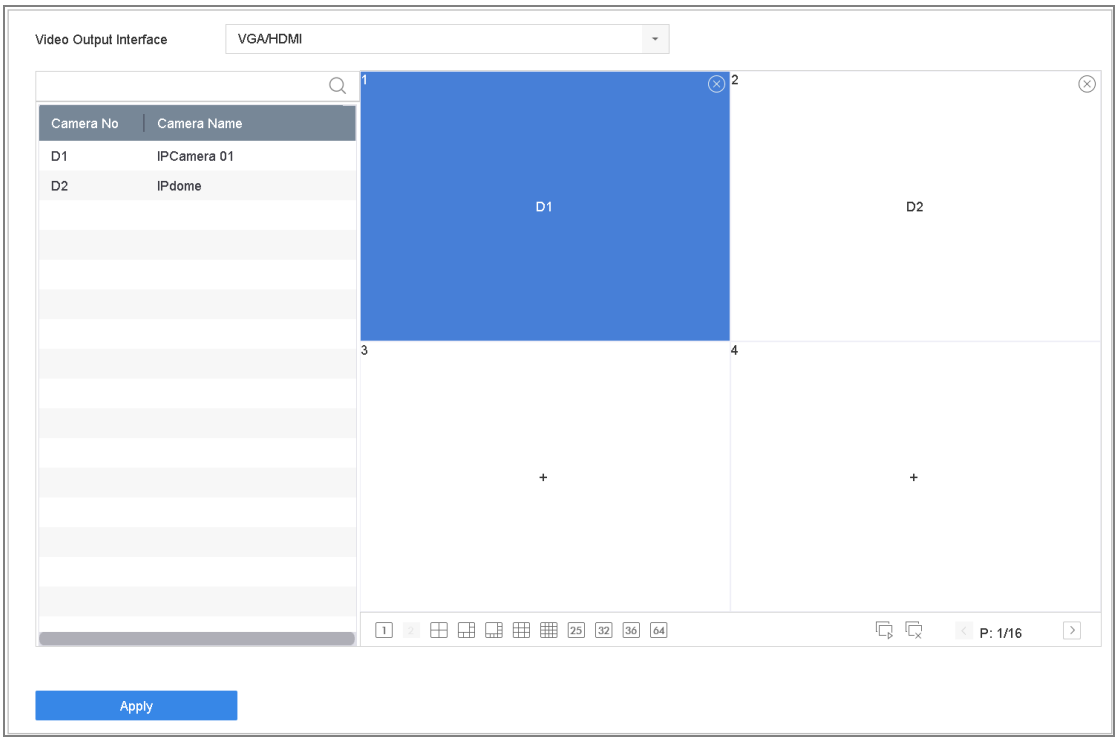


Figure 5-4 Live View

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 the camera from the list to set the camera to the window.

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

NOTE

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

Related Operation:

- Click  button to start live view for all the channels.
- Click  to stop all the live view.

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

5.5 Configure Auto-Switch of Cameras

You can set the auto-switch of cameras 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.
- **Dwell Time:** The time in seconds to dwell between switching of cameras when enabling auto-switch. The range is from 5s to 300s.

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

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

5.6 Configure Channel-Zero Encoding

Purpose:

You can enable the channel-zero encoding when you need to get a remote view of many channels in real time from 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 Select the video output interface to **Channel-Zero**.

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

Step 4 Check the checkbox to enable the channel-zero.

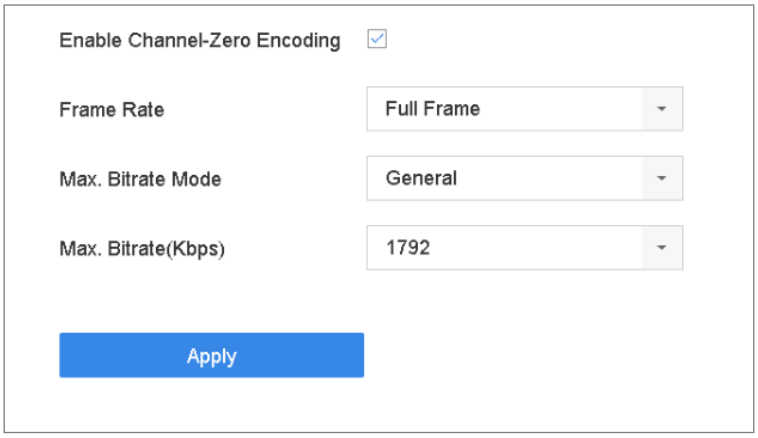


Figure 5-5 Live View- Channel-Zero Encoding

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

Step 6 Click Apply.

Result:

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

5.7 Main and Auxiliary Ports Strategy

There are five video output types: HDMI, VGA, LCD, HDMI2, and CVBS. Priority of video outputs: HDMI > VGA/LCD > HDMI2.

You can go to **System > General** to configure HDMI/VGA/LCD simultaneous output and menu output mode.

For iDS-9600NXI-I8/4F(B) series, HDMI1 and VGA are simultaneous output, HDMI1, VGA, HDMI2, CVBS cannot provide video output at the same time. When HDMI1, HDMI2, VGA, and CVBS are all connected, CVBS does not provide video output, the main port is HDMI2, and the aux port is HDMI1 and VGA. You can enable CVBS in **System > General**, it requires to switch menu output mode to HTMI2, and disable HDMI1/VGA.

For other series, the following table shows the main and auxiliary ports strategy when video cables for HDMI, HDMI2, and VGA are connected.

- **Main port**: All operations are available for main port.
- **Aux port**: You can switch to aux port to do some basic operations, like playback, switching live view image.
- **Third port**: You can only preview camera image in third port.

Table 5-1 Main and Auxiliary Ports Strategy

HDMI/VGA/LCD simultaneous output	Menu output mode	HDMI	HDMI2	VGA/LCD
On	Auto	Main port	Aux port	Main port
Off	Auto	Main port	Aux port	Third port
On	HDMI 2	Aux port	Main port	Aux port
Off	HDMI 2	Aux port	Main port	Third port
On	HDMI/VGA/LCD	Main port	Aux port	Main port
Off	VGA/LCD	Aux port	Third port	Main port
	HDMI	Main port	Third port	Aux port

5.8 Facial Recognition

Purpose:

You can enter facial recognition interface to view real-time facial recognition and stranger recognition results.

Before you start

Ensure you have configured facial detection and face picture comparison function, refer to *12.1 Facial Detection* and *Chapter 15 Face Picture Comparison* for details.

Step 1 Go to live view interface and click in toolbar.

Step 2 (Optional) Click to select window division.

Step 3 Select a window as you desired.

Step 4 Double click a camera from **Camera** list in the bottom left.

Figure 5-6 Facial Recognition

Step 5 Click **Records** to view the real-time facial recognition records of selected camera. The records will also be shown in the window on the right. You can view the facial detection number at the top, including the total number, succeeded number and failed number.

Step 6 (Optional) For the unregistered face picture, you can double click it in **Records** list, and add it to face picture library.

NOTE

For guest and operator user, it requires Local Parameters Settings permission to add unregistered face picture to face picture library.

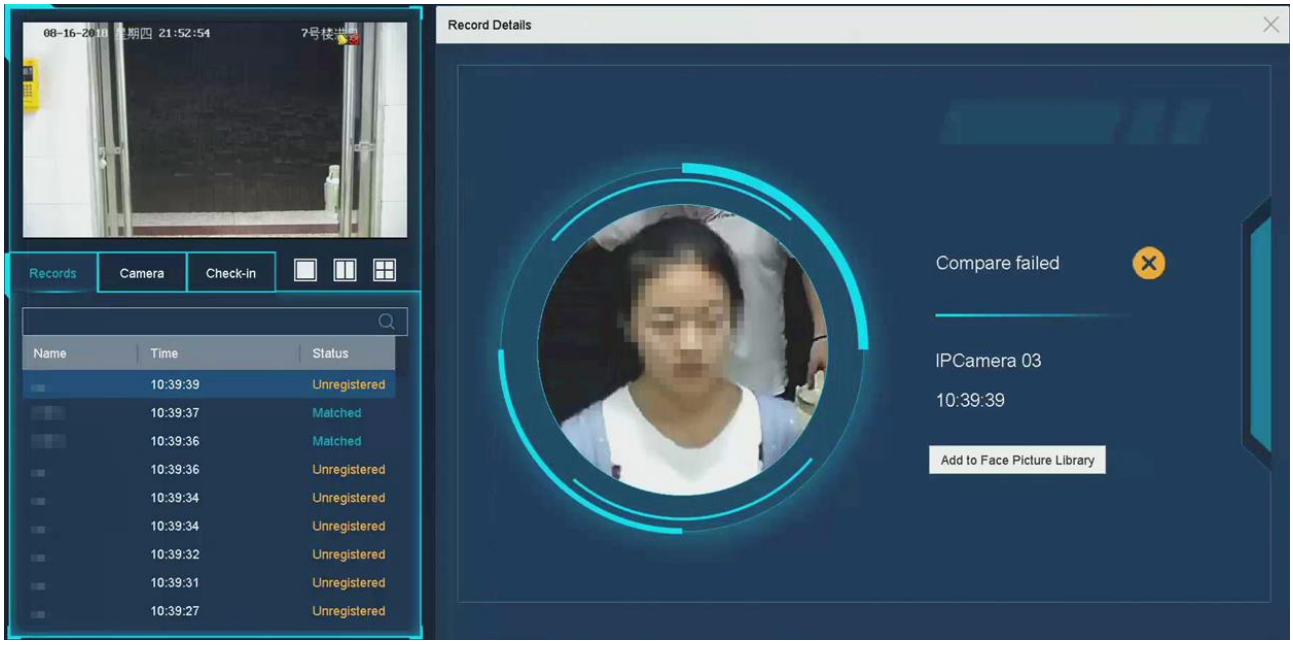


Figure 5-7 Add Unregistered Face Picture

Step 7 (Optional) You can click **Check-in** to view face picture library check-in record, including **Total No., Checked In** and **Unchecked In**.

Step 8 (Optional) Click on the upper right corner to configure the display settings as you desired.

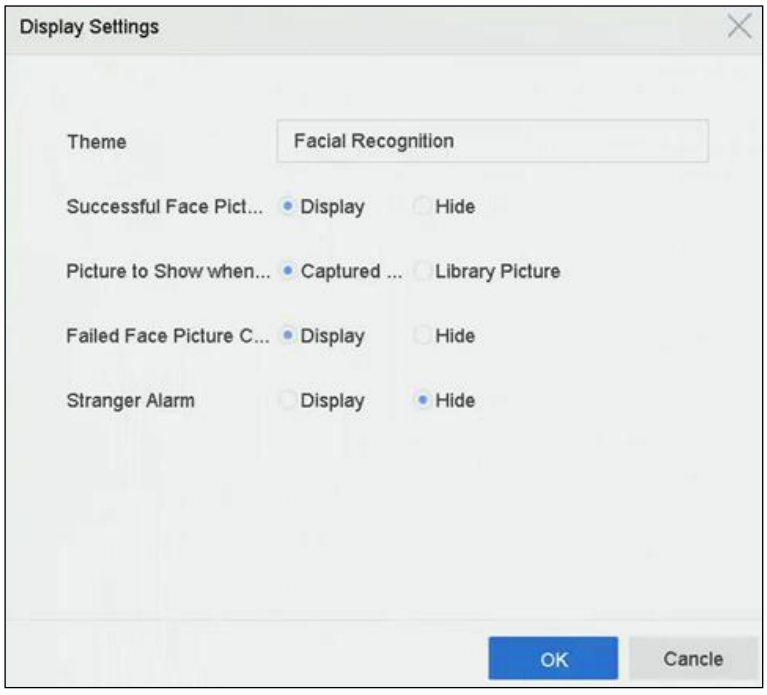


Figure 5-8 Facial Recognition Display Settings

Step 9 (Optional) Click on the upper right corner to search and export record.

1) Set the search parameters as you desired.

2) Click **Search**.
3) Click **Export Attendance Record** or **Export Check-in Record**

NOTE

- Ensure you have inserted USB flash drive before export.
- You can click a record to review the attendance information of this individual in calendar.
- For guest and operator user, it requires **Local Video Export** permission (in **Camera Permission**) to search and export record.

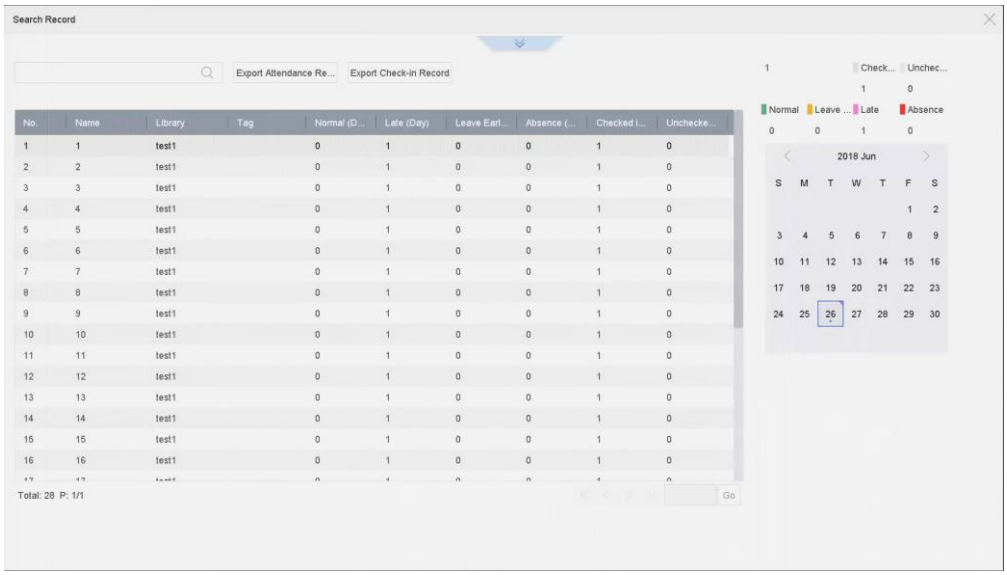


Figure 5-9 Face Recognition Search Record

Chapter 6 PTZ Control

6.1 PTZ Control Wizard

Before you start

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

Purpose

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

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

Figure 6-1 PTZ Control Wizard

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

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

Step 4 Click **OK** to exit.

6.2 Configure PTZ Parameters

Purpose

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

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

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

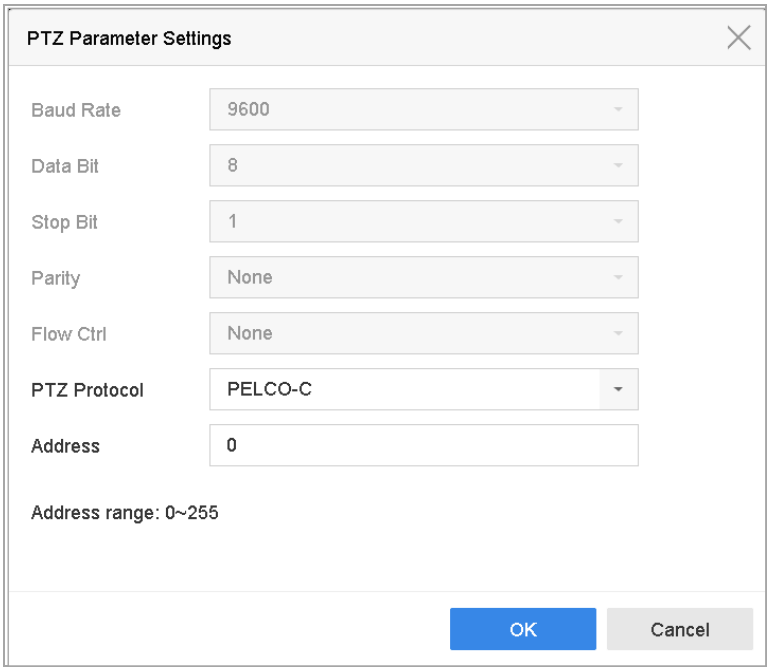


Figure 6-2 PTZ Parameters Settings

Step 3 Edit the parameters of the PTZ camera.

NOTE

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

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

6.3 Set PTZ Presets, Patrols & Patterns

Before you start:

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

6.3.1 Set a Preset

Purpose:

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

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

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

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

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

Figure 6-3 Set Preset

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

Step 5 Enter the preset name in the text field.

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

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

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

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

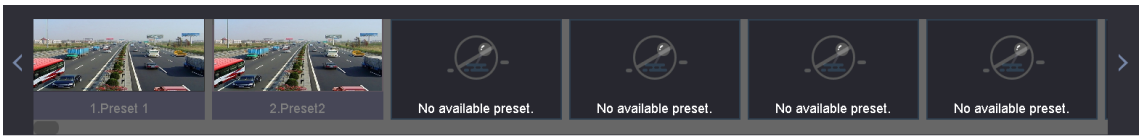


Figure 6-4 View the Configured Presets

6.3.2 Call a Preset

Purpose:

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

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

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

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

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

Figure 6-5 Call Preset (1)

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

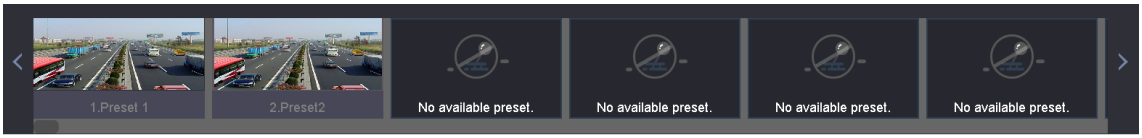


Figure 6-6 Call Preset (2)

6.3.3 Set a Patrol

Purpose:

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

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

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

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

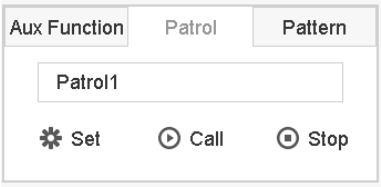


Figure 6-7 Patrol Configuration

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

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

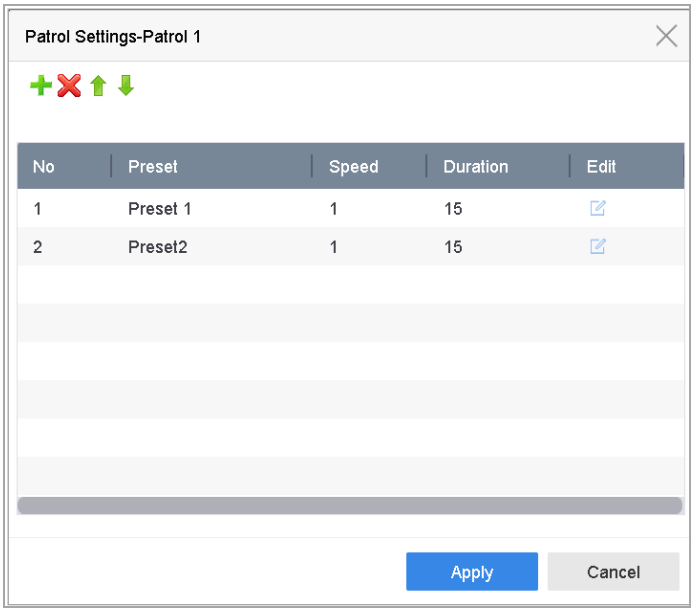


Figure 6-8 Patrol Settings

Step 5 Click  to add key point for the patrol.

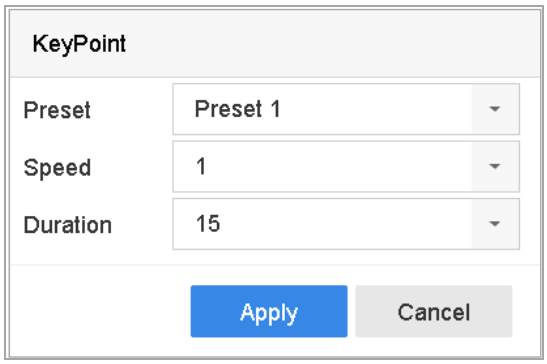


Figure 6-9 Key Point Configuration

1) Configure key point parameters.

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

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

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

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

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

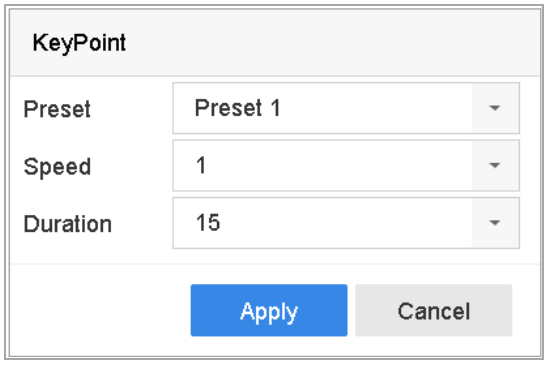


Figure 6-10 Edit Key Point

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

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

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

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

6.3.4 Call a Patrol

Purpose:

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

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

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

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

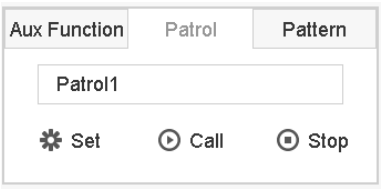


Figure 6-11 Patrol Configuration

Step 3 Select a patrol in the text field.

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

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

6.3.5 Set a Pattern

Purpose:

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

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

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

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

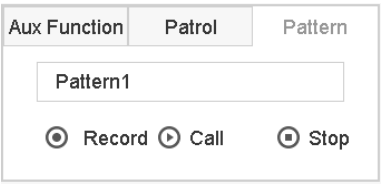


Figure 6-12 Pattern Configuration

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

Step 4 Set the pattern.

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

The movement of the PTZ is recorded as the pattern.

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

6.3.6 Call a Pattern

Purpose:

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

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

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

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

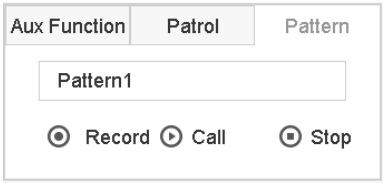


Figure 6-13 Pattern Configuration

Step 3 Select a pattern in the text field.

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

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

6.3.7 Set Linear Scan Limits

Before you start:

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

Purpose:

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

NOTE

This function is supported by some certain models.

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

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

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

NOTE

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

6.3.8 Call Linear Scan

NOTE

Before operating this function, make sure the connected camera supports the 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 live view.

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

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

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

NOTE

Reboot the camera to take the settings into effect.

6.3.9 One-touch Park

NOTE

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

Purpose

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

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

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

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

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

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

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

NOTE

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

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

6.4 Auxiliary Functions

Before you start

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

Purpose

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

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

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

Step 2 Click Aux Function.

Figure 6-14 Aux Function Configuration

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

Table 6-1 Description of Aux Functions Icons

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

Chapter 7 Storage

7.1 Storage Device Management

7.1.1 Install the HDD

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

7.1.2 Add the Network Disk

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

Add NAS

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

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

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

Step 4 Select 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.

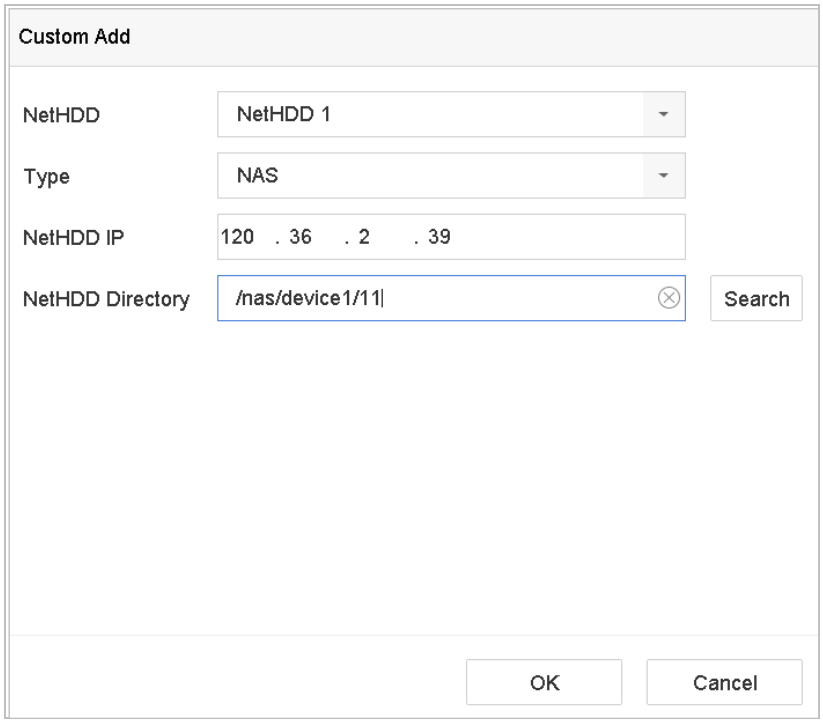


Figure 7-1 Add NAS Disk

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

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

Result:

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

Add IP SAN

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

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

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

Step 4 Select the type to IP SAN.

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

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

Step 7 Select the IP SAN disk from the list shown below.

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

NOTE

Up to 1 IP SAN disk can be added.

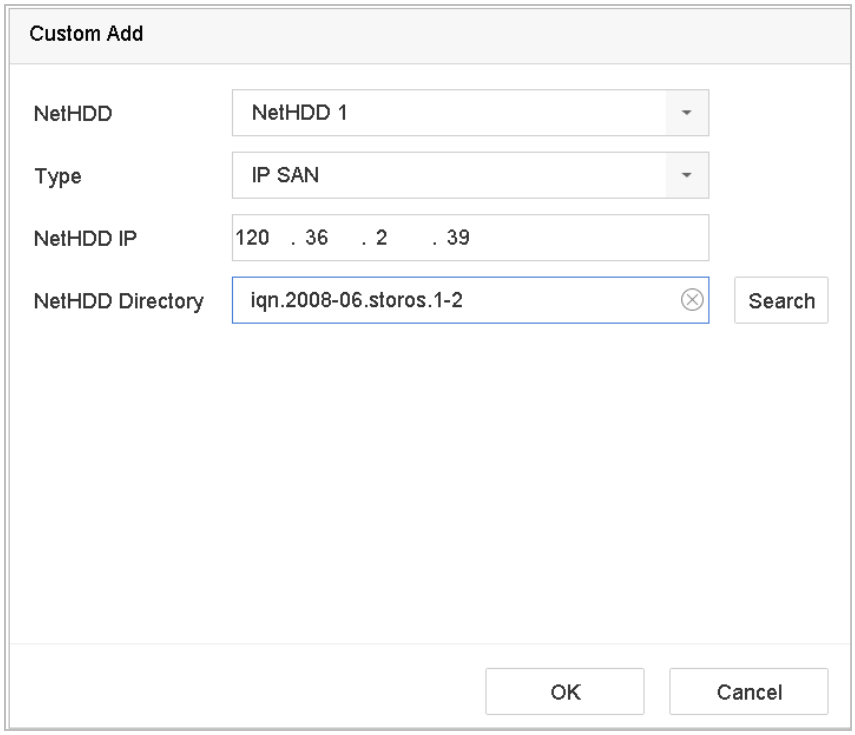


Figure 7-2 Add IP SAN Disk

Result:

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, please select it and click the **Init** button for initialization.

7.1.3 Initialize SSD

For the device that has pre-installed SSD on main board, you can view the SSD space distribution or initialize the SSD.

Step 1 Go to **Storage** > **Storage Management** > **SSD Management**.

Figure 7-3 Initialize SSD

Step 2 Click **Format**.

Step 3 Click **Yes** to initialize SSD.

NOTE

Initializing SSD will erase its data, including those in face picture library, and cancel the alarms linked to the library. The device will restart after initialization.

7.1.4 Configure eSATA for Data Storage

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

Step 1 Click Storage>Advanced.

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

Export: use the eSATA for backup.

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

Figure 7-4 Set eSATA Mode

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

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

7.2 Storage Mode

7.2.1 Configure HDD Group

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.

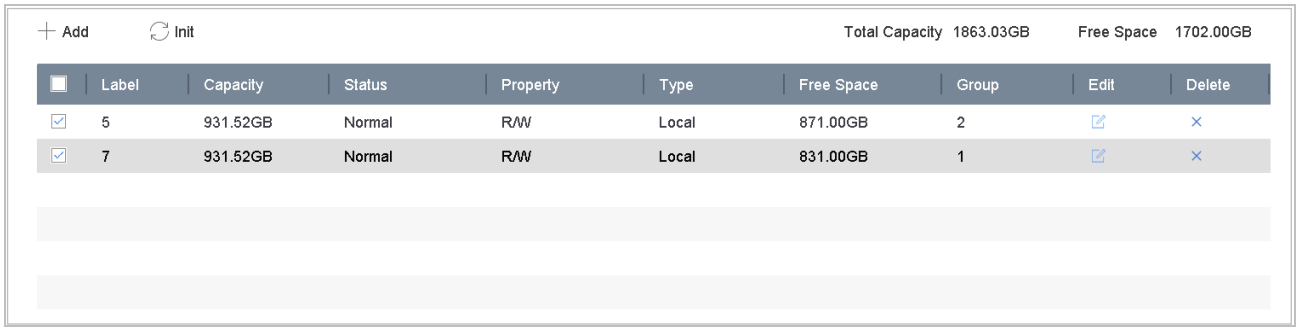


Figure 7-5 Storage Device

Step 3 Click  to enter the Local HDD Settings interface.

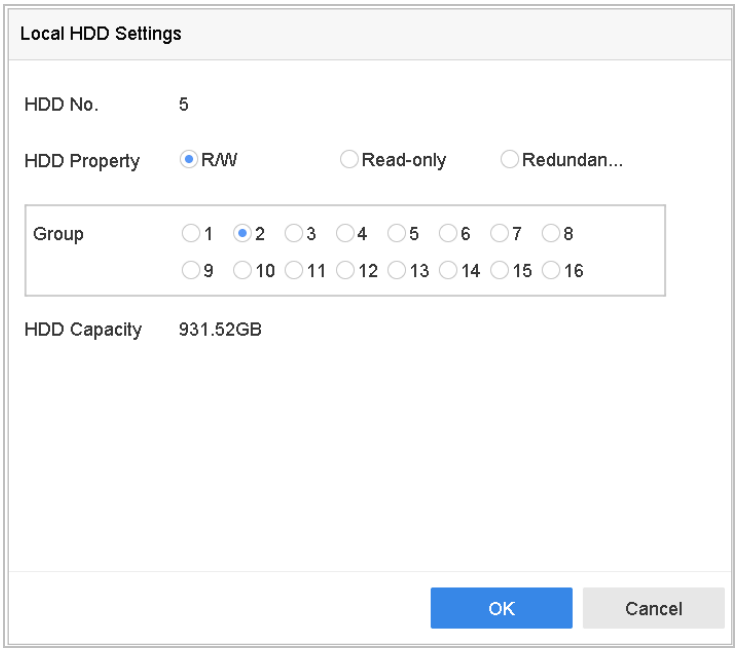


Figure 7-6 Local HDD Settings

Step 4 Select the Group number for the current HDD.

Step 5 Click **OK**.

NOTE

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

Step 6 Go to Storage> Storage Mode.

Step 7 Check the checkbox of **Group** tab.

Step 8 Select the group No. from the list.

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

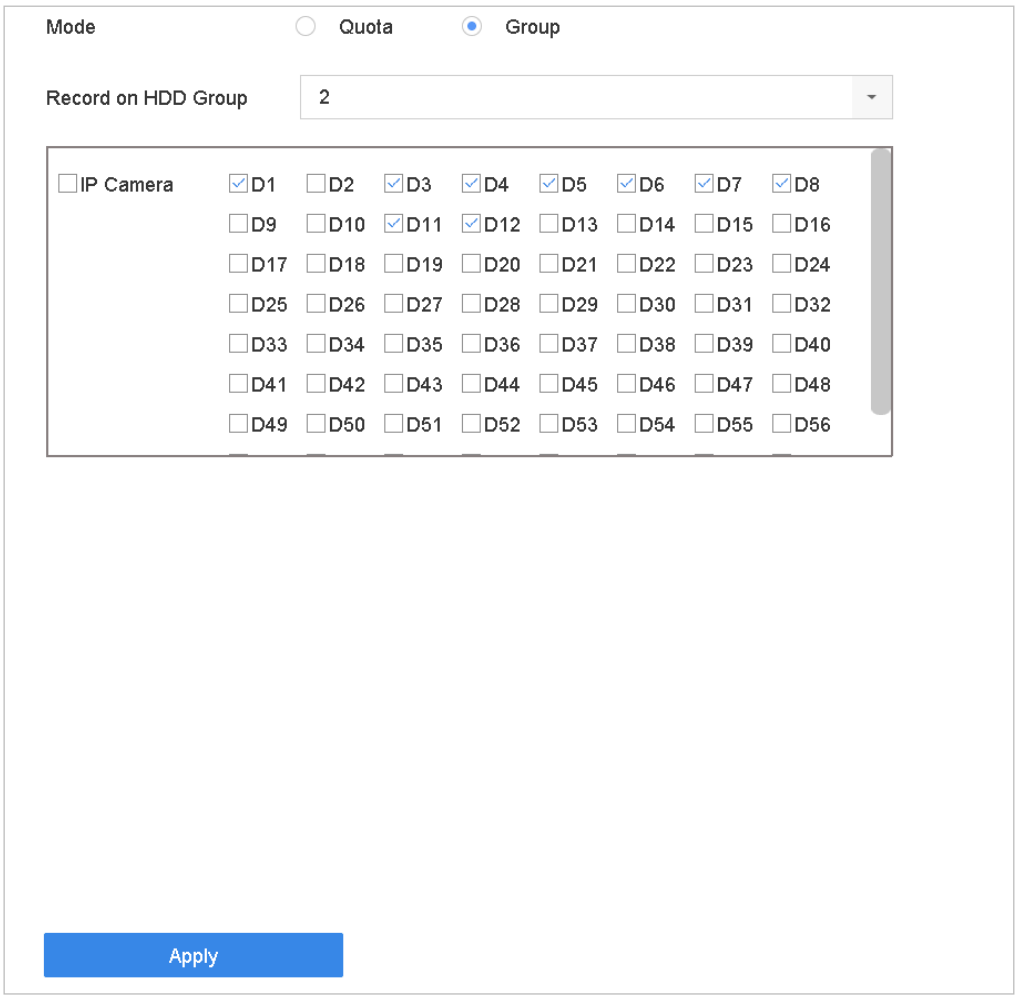


Figure 7-7 Storage Mode-HDD Group

Step 10 Click **Apply**.

NOTE

Reboot the device to activate the new storage mode settings.

7.2.2 Configure HDD Quota

Purpose:

Each camera can be configured with allocated quota for the storage of recorded files.

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

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

Step 3 Select a camera to set quota.

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

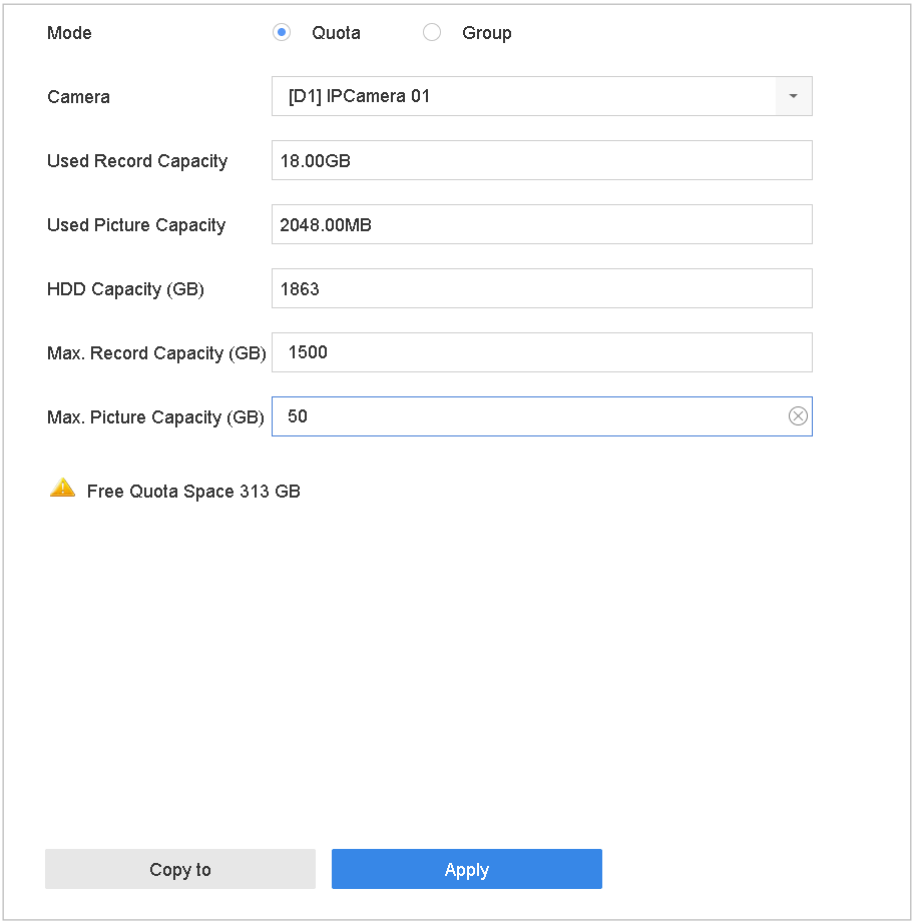


Figure 7-8 Storage Mode-HDD Quota

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

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

NOTE

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

NOTE

Reboot the device to activate the new storage mode settings.

7.3 Recording Parameters

7.3.1 Main Stream

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

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

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

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

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

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

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

7.3.2 Sub-Stream

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

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

7.3.3 ANR

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

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

7.3.4 Configure Advanced Recording Settings

Step 1 Go to Storage > Recording Schedule.

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

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

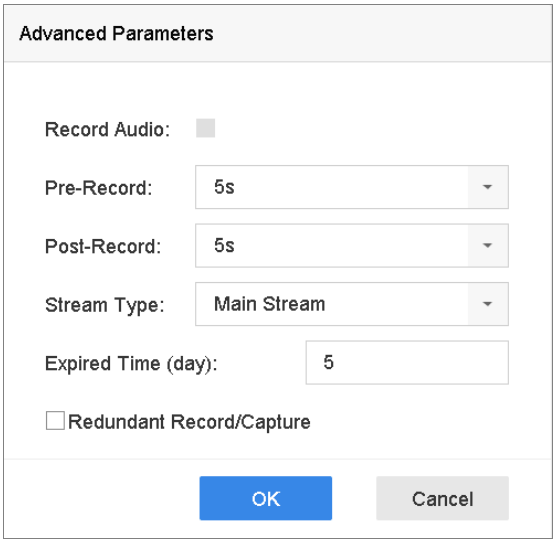


Figure 7-9 Advanced Record Settings

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

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

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

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

Redundant Record/Capture: By enabling redundant record you save the record and captured picture in the redundant HDD. See 7.11 *Configure Redundant Recording*.

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

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

7.4 Configure Recording Schedule

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

Before you start

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

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

Refer to *Chapter 7.1.2* Add the Network Disk for network HDD connections.

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

Step 2 Select a camera.

Step 3 Check Enable Schedule.

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

Different recording types are configurable.

- **Continuous:** scheduled recording.
- **Event**: recording triggered by all event triggered alarm.
- **Motion**: recording triggered by motion detection.
- **Alarm:** recording triggered by alarm.
- **M/A:** recording triggered by either motion detection or alarm.
- **M&A:** recording triggered by motion detection and alarm.

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

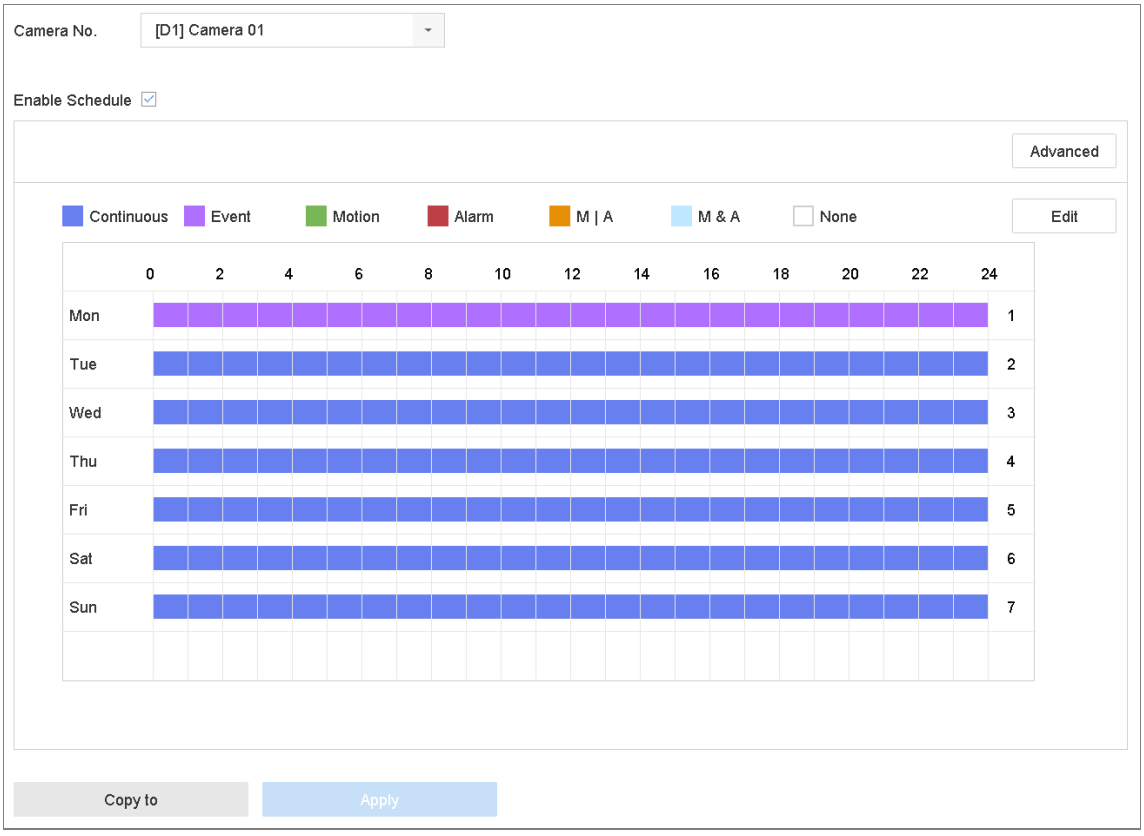


Figure 7-10 Record Schedule

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

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

NOTE

To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and Event triggered recording, you must configure the motion detection settings, alarm input settings and other events as well. Please refer to Chapter 11 Event and Alarm Settings

Event and Alarm Settings and Chapter 12 VCA Event Alarm for details.

7.5 Configure Continuous Recording

Step 1 Go to **Camera** > **Video Parameters**.

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

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

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

Step 5 Set the schedule for the continuous recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.6 Configure Motion Detection Triggered Recording

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

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

Step 2 Configure the motion detection and select the channel (s) to trigger the recording when motion event occurs. Refer to Chapter 11.2 Configure Alarm Linkage Actions for details.

Step 3 Go to **Camera** > **Video Parameters**.

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

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

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

Step 7 Set the schedule for the motion detection triggered recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.7 Configure Event Triggered Recording

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

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

Step 2 Configure the event detection and select the channel (s) to trigger the recording when event occurs. Refer to Chapter 11 Event and Alarm Settings and Chapter 12 VCA Event Alarm for details.

Step 3 Go to **Camera** > **Video Parameters**.

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

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

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

Step 7 Set the schedule for the event triggered recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.8 Configure Alarm Triggered Recording

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

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

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

Refer to Chapter 11 and Chapter 12 VCA Event Alarm for details.

Step 3 Go to Camera > Video Parameters.

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

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

Step 6 Select the record type to **Alarm**.

Step 7 Set the schedule for the alarm triggered recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.9 Configure Picture Capture

Purpose:

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

NOTE

Only iDS-9600NXI-I8/4F(B) series support this function.

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

Step 2 Set the picture parameters.

Resolution: set the resolution of the picture to capture.

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

Interval: the interval of capturing live picture.

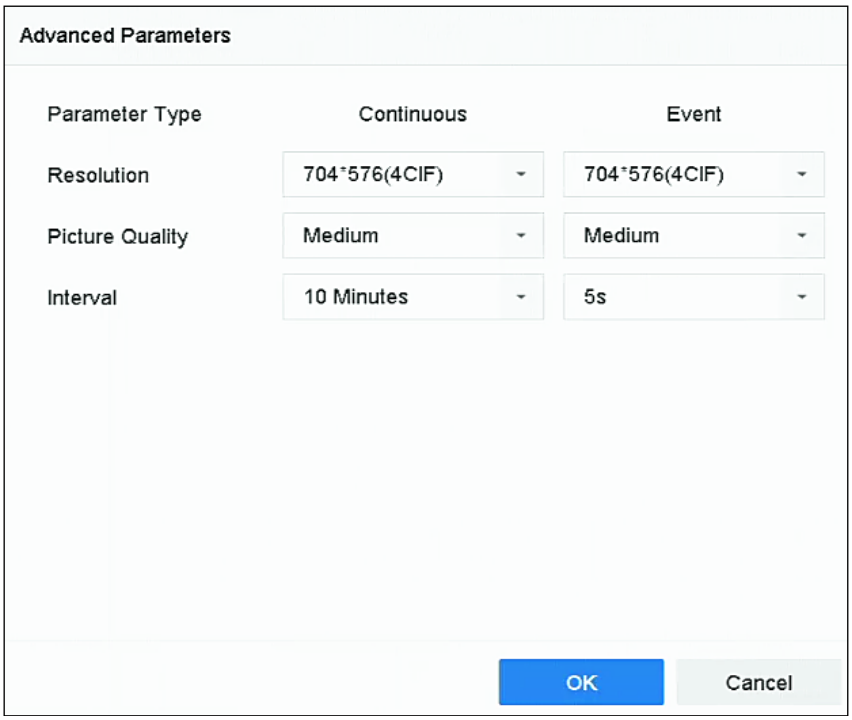


Figure 7-11 Picture Parameters

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

Step 4 Select the camera to configure the picture capture.

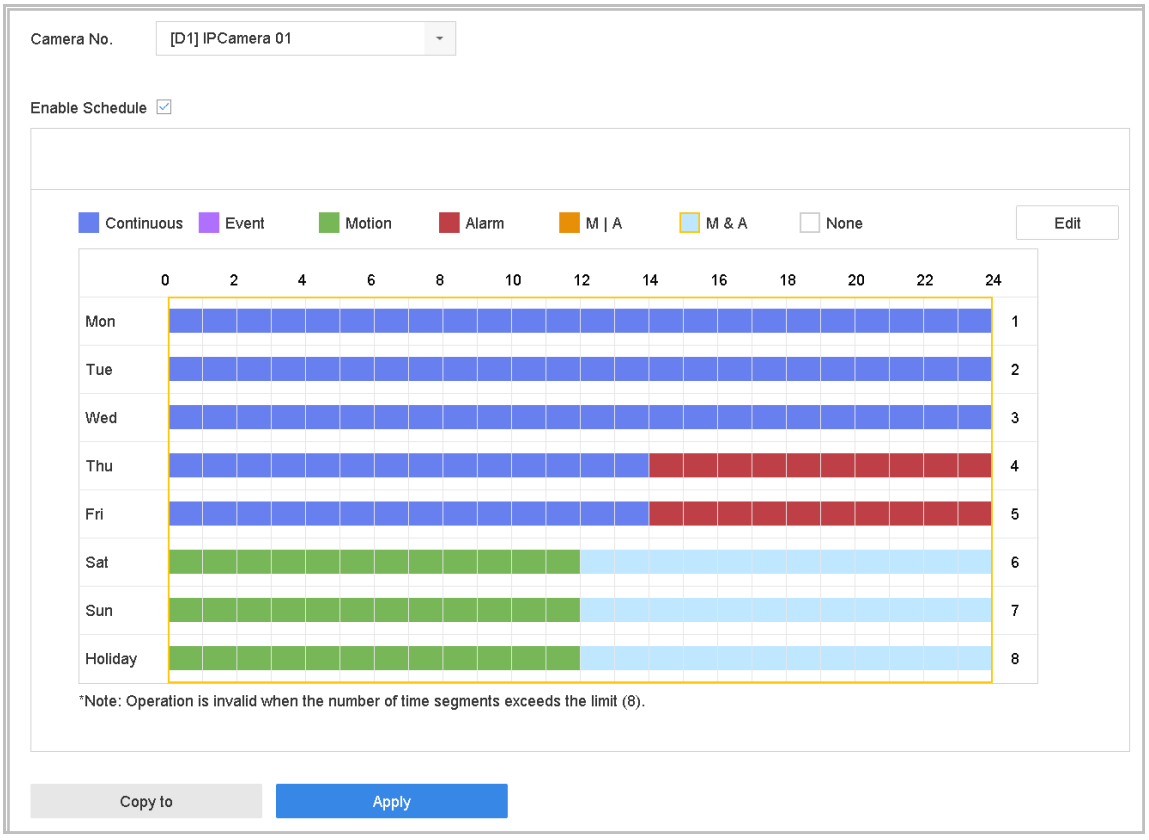


Figure 7-12 Set Picture Capture Schedule

Step 5 Set the picture capture schedule. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.10 Configure Holiday Recording

Purpose:

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

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

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

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

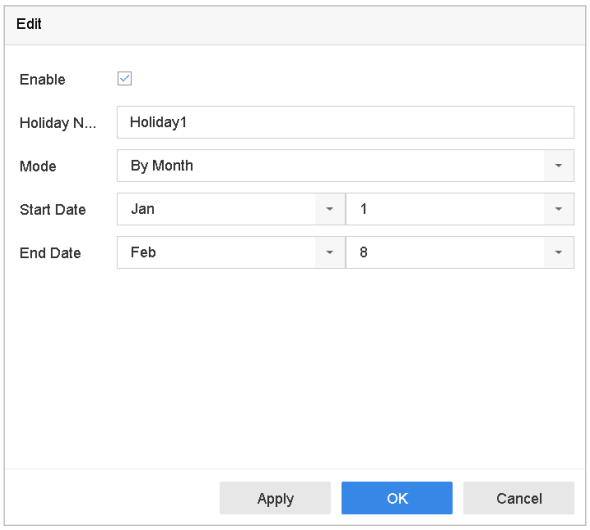


Figure 7-13 Edit Holiday Settings

1) Edit the holiday name.

Select the mode to by date, by week or by month.

Set the start and end date of the holiday.

Click **OK**.

Step 4 Set the schedule for the holiday recording. Refer to Chapter 7.4 Configure Recording Schedule for details.

7.11 Configure Redundant Recording

Purpose:

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

NOTE

You must set the storage mode to *Group* before you set the HDD property to Redundancy. For detailed information, please refer to Chapter 7.2.1 Configure HDD Group. There should be at least another HDD which is in Read/Write status.

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

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

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

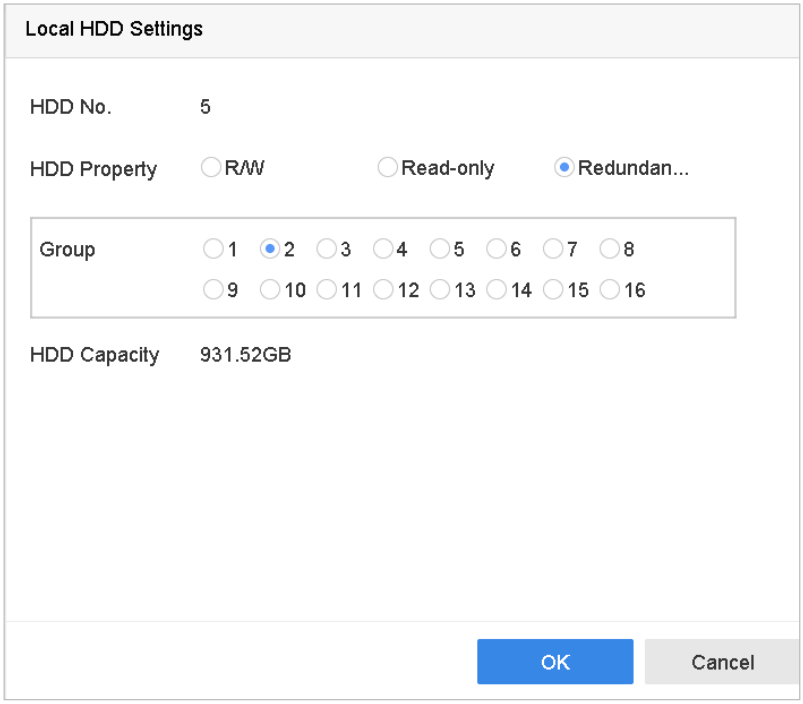


Figure 7-14 HDD Property-Redundancy

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

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

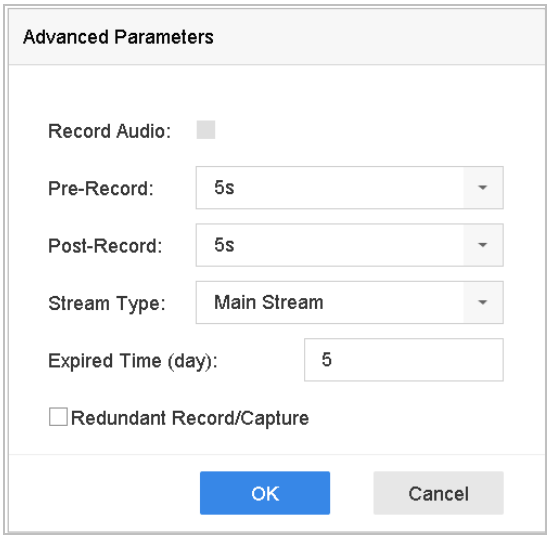


Figure 7-15 Record Parameters

Step 6 Check the checkbox of Redundant Record/Capture.

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

Chapter 8 Disk Array

Purpose:

Disk array is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit. 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", depending on what level of redundancy and performance is required.

8.1 Create Disk Array

Purpose:

The device supports the disk array that is realized by software. You can enable the RAID function as required. Two ways are available for creating array: one-touch configuration and manual configuration. The following flow chart shows the process of creating array.

8.1.1 Enable RAID

Purpose:

Perform the following steps to enable the disk array function.

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

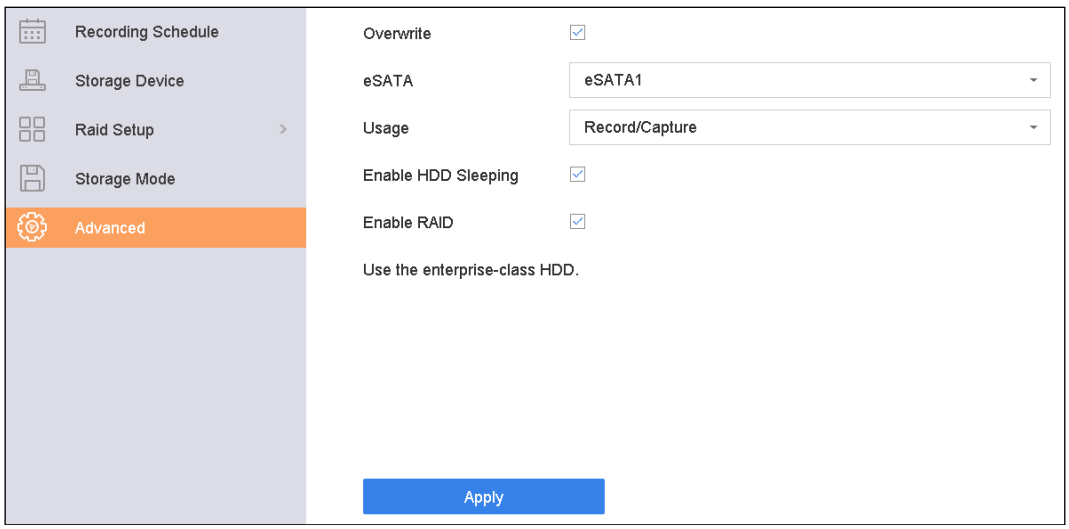


Figure 8-1 Advanced

Step 2 Check Enable RAID.

Step 3 Click **Apply**.

Step 4 Reboot device to take effect the settings.

8.1.2 One-Touch Creation

Purpose:

One-touch configuration helps you to quickly create the disk array. By default, the array type created by one-touch configuration is RAID 5.

Before you start:

- Enable RAID function. For details, refer to Chapter 8.1.1 Enable RAID.
- Install at least 3 HDDs. If more than 10 HDDs are installed, 2 arrays will be created. To maintain reliable and stable running of the HDDs, it is recommended to use enterprise-level HDDs with the same model and capacity.

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

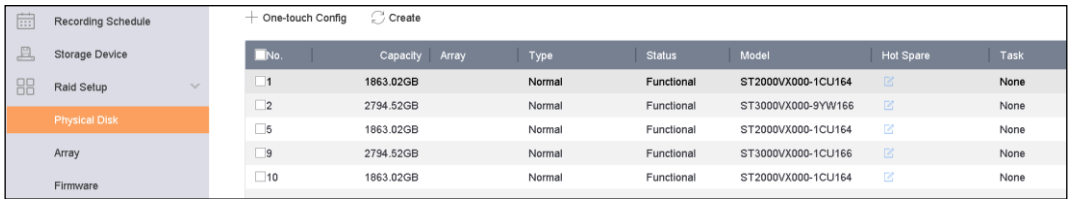


Figure 8-2 Physical Disk

Step 2 Click One-touch Config.

Step 3 Edit the array name in **Array Name** text filed and click **OK** to start configuring.

NOTE

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

Step 4 A message box will pop up when the array creation is completed, click **OK** on it.

Step 5 (Optional) The device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** view the information of created arrray.

8.1.3 Manual Creation

Purpose:

Manually create the array of RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10.

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

Step 2 Click **Create**.

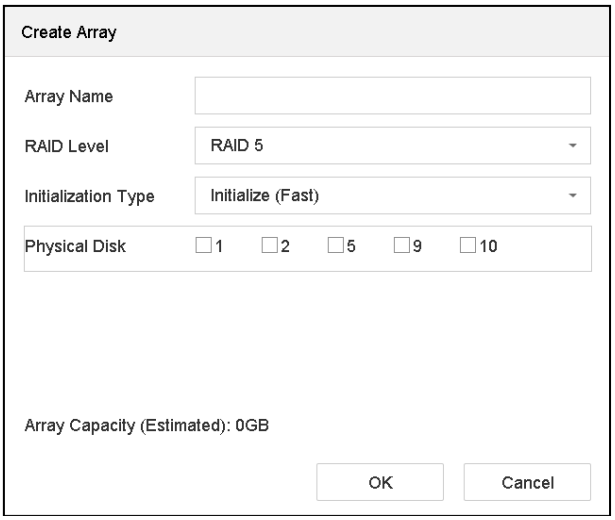


Table 8-1 Create Array

Step 3 Enter 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 array.

Table 8-2 Required Number of HDD

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

Step 6 Click **OK**.

Step 7 (Optional) The device will automatically initialize the created array. Go to **Storage > RAID Setup > Array** view the information of created arrray.

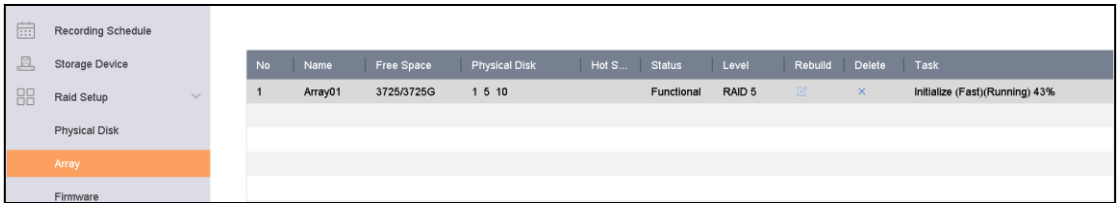


Figure 8-3 Array List

8.2 Rebuild Array

Purpose:

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

- Functional: No disk loss in the array.
- Offline: The number of lost disks has exceeded the limit.
- Degraded: If amount of HDD fail in array, array degrades. You should recover it to Functional by array rebuilding.

8.2.1 Configure 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 8-4 Physical Disk

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

8.2.2 Automatically Rebuild 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 8.2.1 Configure Hot Spare Disk.

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

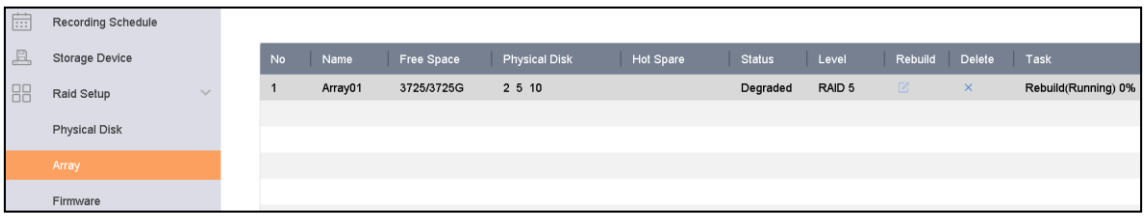


Figure 8-5 Array List

8.2.3 Manually Rebuild Array

Purpose:

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

Before you start:

At least one available physical disk should exist for rebuilding the array.

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

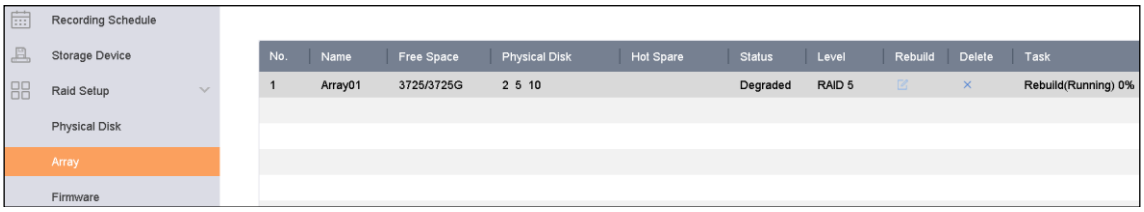


Figure 8-6 Array List

Step 2 Click  of degraded array.

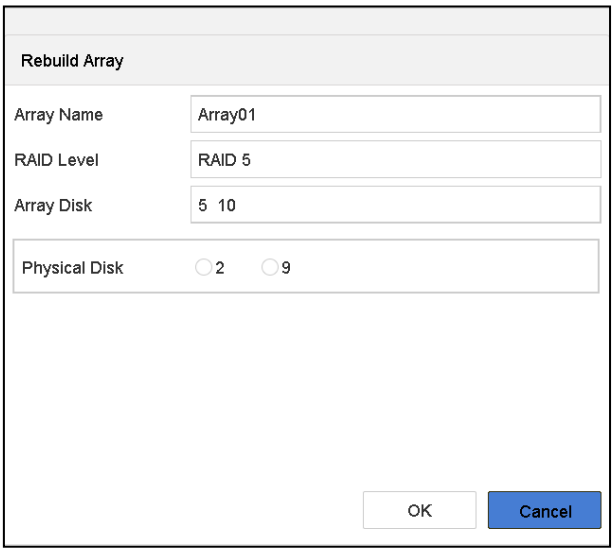


Figure 8-7 Rebuild Array

Step 3 Select the available physical disk.

Step 4 Click **OK**.

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

8.3 Delete Array

NOTE

Deleting array will delete all the data saved in it.

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

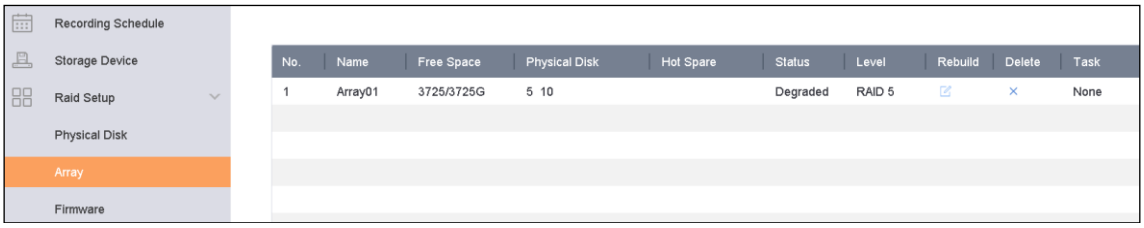


Figure 8-8 Array List

Step 2 Click ✕ of array to delete.

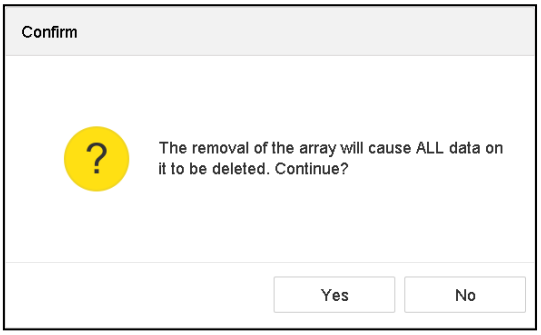


Figure 8-9 Attention

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

8.4 Check and Edit Firmware

Purpose:

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

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

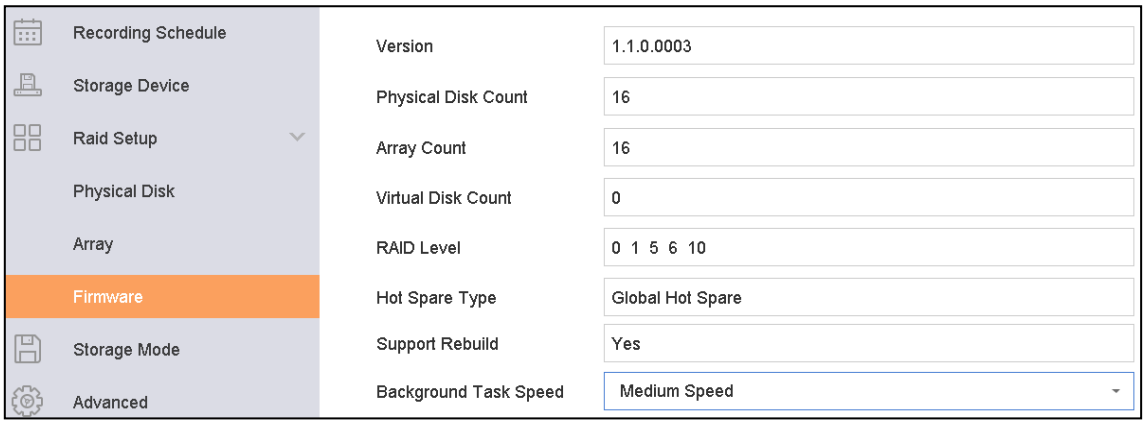


Figure 8-10 Firmware

Step 2 (Optional) Set the **Background Task Speed**.

Step 3 Click **Apply**.

Chapter 9 File Management

9.1 Search Video

Purpose

Specify detailed conditions to search videos.

Step 1 Go to **File Management** > **Video**.

Step 2 Set search conditions.

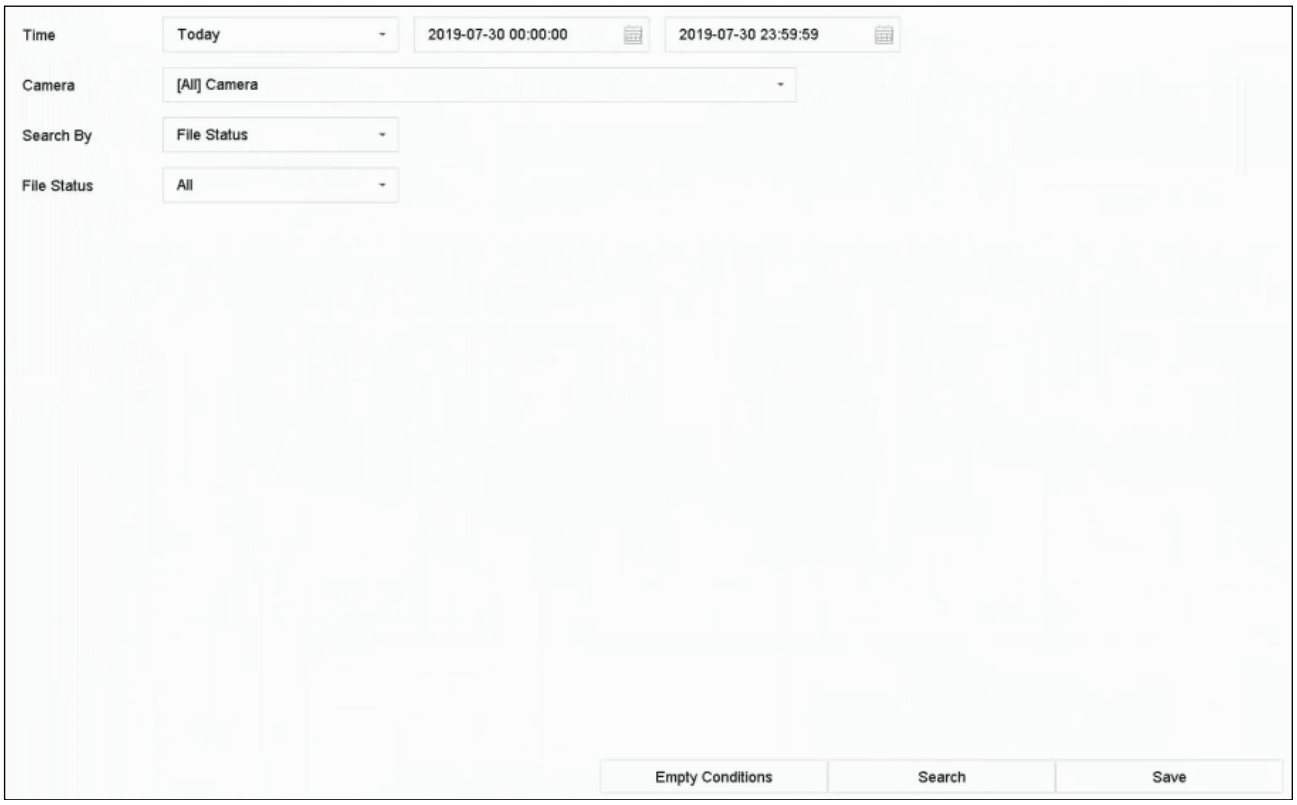


Figure 9-1 Search Video

Step 3 (Optional) Save search conditions.

1) Click **Save**.
2) Enter a name.
3) Click **Finish**.

Step 4 Click **Search**. The search result list displays 1 channel.

Step 5 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Step 6 (Optional) Click  or  to switch view mode.

Step 7 (Optional) Click  or  in different view mode to lock a video. The locked video will not be overwritten.

Step 8 (Optional) Export search results.

1) Select result file(s) from the search result interface, or check **Select All** to select all files.
2) Click **Export** to export the selected file(s) to a backup device.

NOTE

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

9.2 Search Picture

Purpose

Specify detailed conditions to search pictures.

Step 1 Go to **File Management** > **Picture**.

Step 2 Set search conditions.

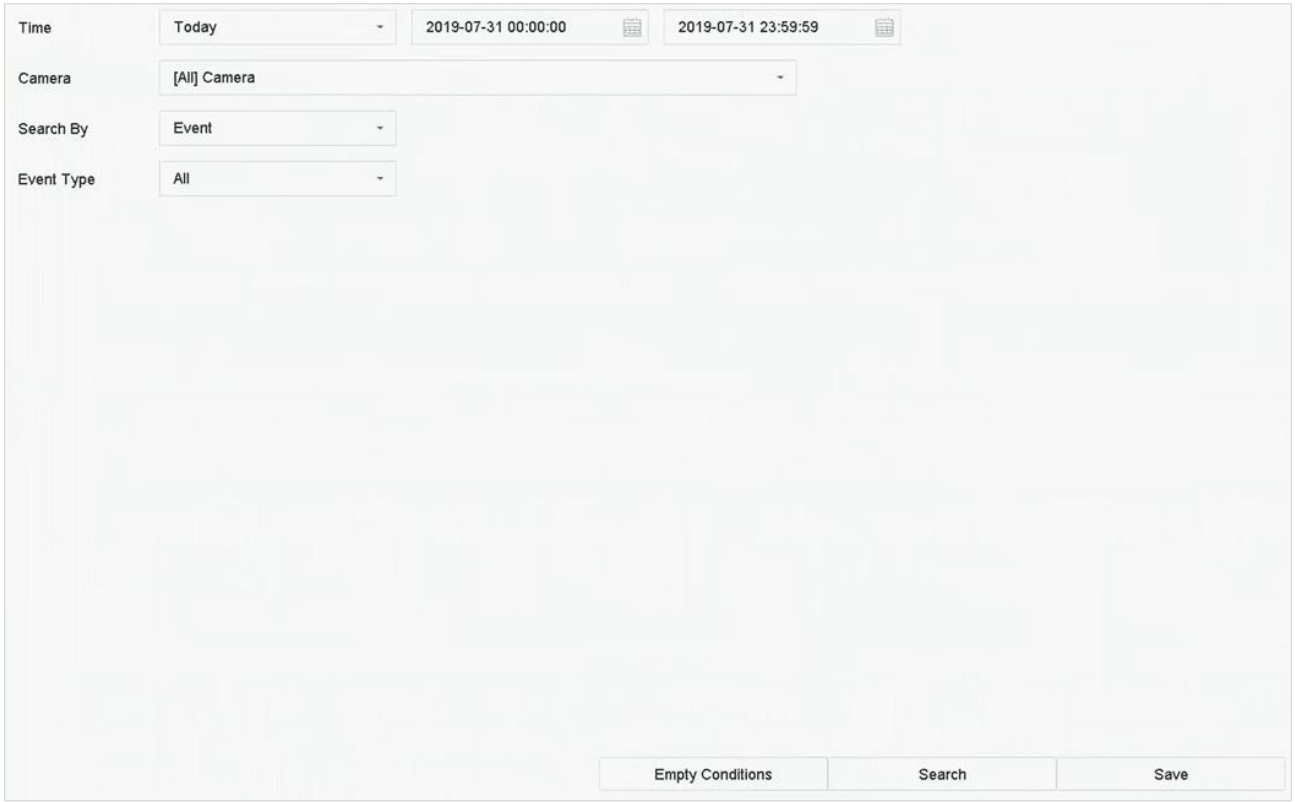


Figure 9-2 Search Picture

Step 3 (Optional) Save search conditions.

1) Click **Save**.
2) Enter a name.
3) Click **Finish**.

Step 4 Click **Search**. The search result list displays 1 channel.

Step 5 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Step 6 (Optional) Click  or  to switch view mode.

Step 7 (Optional) Export search results.

1) Select result file(s) from the search result interface, or check **Select All** to select all files.
2) Click **Export** to export the selected file(s) to a backup device.

NOTE

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

9.3 Smart Search

You can search human body files, face files and vehicles in **File Management** > **Smart Search**. Refer to *14.3 Human Body Search*, *15.4 Face Picture Search,* and *13.4 Vehicle Search* for details.

Chapter 10 Playback

10.1 Playing Video Files

10.1.1 Instant Playback

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

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

Step 2 Click  to start instant playback.

Figure 10-1 Playback Interface

10.1.2 Play Normal Video

Purpose:

In the normal playback mode, you can achieve the advanced playback operations which will satisfy more complicated requirements.

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 the play button on the toolbar to start playing the video.

Step 5 You can use the toolbar in the bottom part of playback interface to control the playing and realize a series of operations. Refer to Chapter 10.2 Playback Operations.

Figure 10-2 Playback Interface

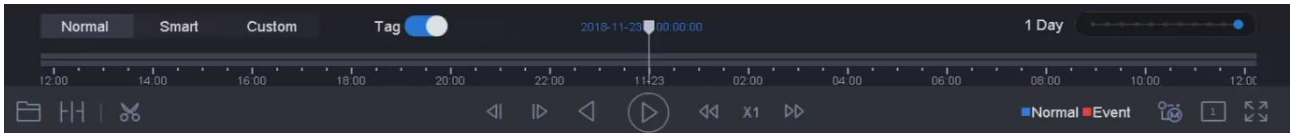


Figure 10-3 Toolbar of Playback

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

NOTE

The playing speed of 256X is supported.

10.1.3 Play Tag Files

Purpose:

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

Before playing back by tag:

Manage Tag Files

Step 1 Go to **Playback**.

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

Step 3 Positioning mouse on playback window and click  to add the tag.

Step 4 Edit the tag information.

NOTE

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

Play Tag Files

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

Step 2 Enter the search conditions for the tag files, including the time and the tag keyword.

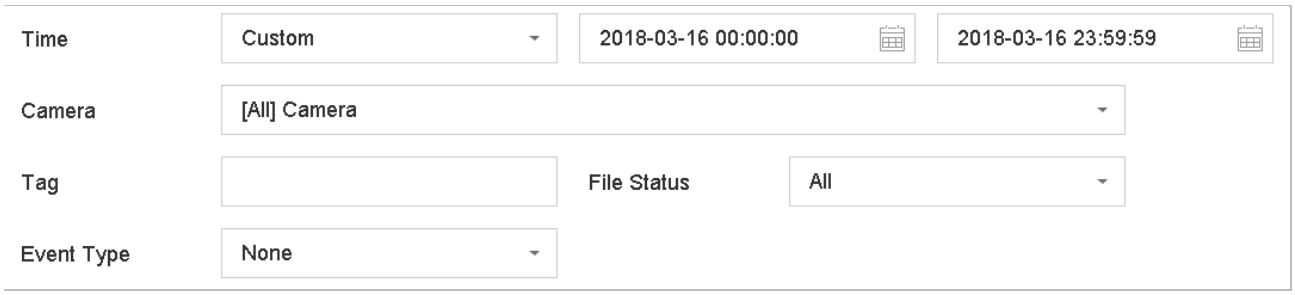


Figure 10-4 Tag Search

Step 3 Click **Search**.

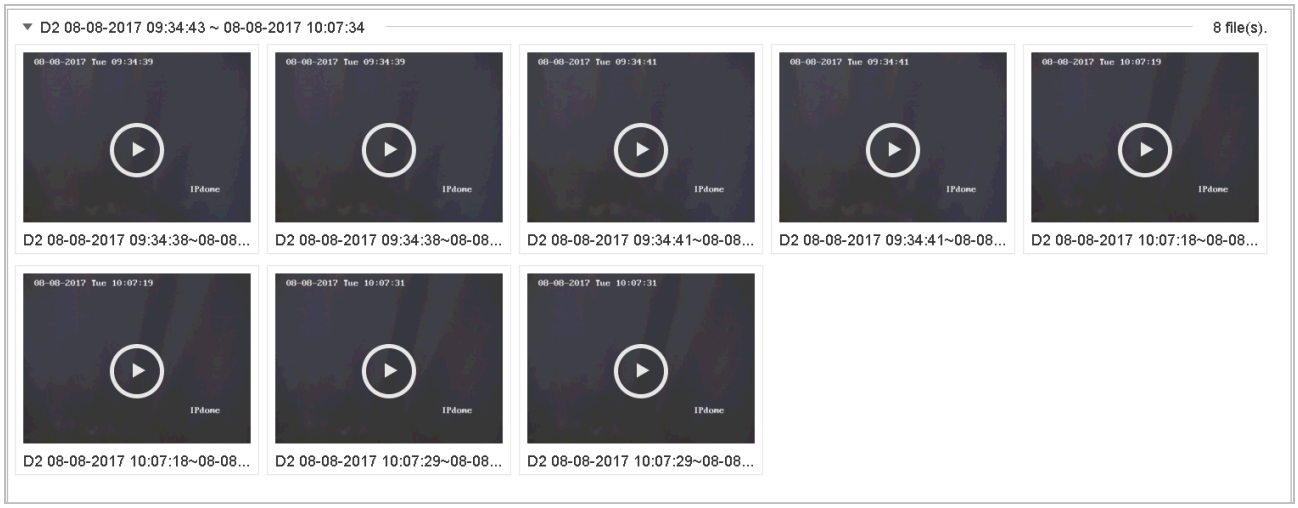


Figure 10-5 Searched Tag Files

Step 4 On the search results interface, select a tag file and click to start playing the video.

10.1.4 Play by Smart Search

Purpose

In the smart playback mode, the device will analyze the video containing the motion, line or intrusion detection information, mark it with green color and play it in the normal speed. And the video without motion will be played in the 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 Click **Smart**.

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

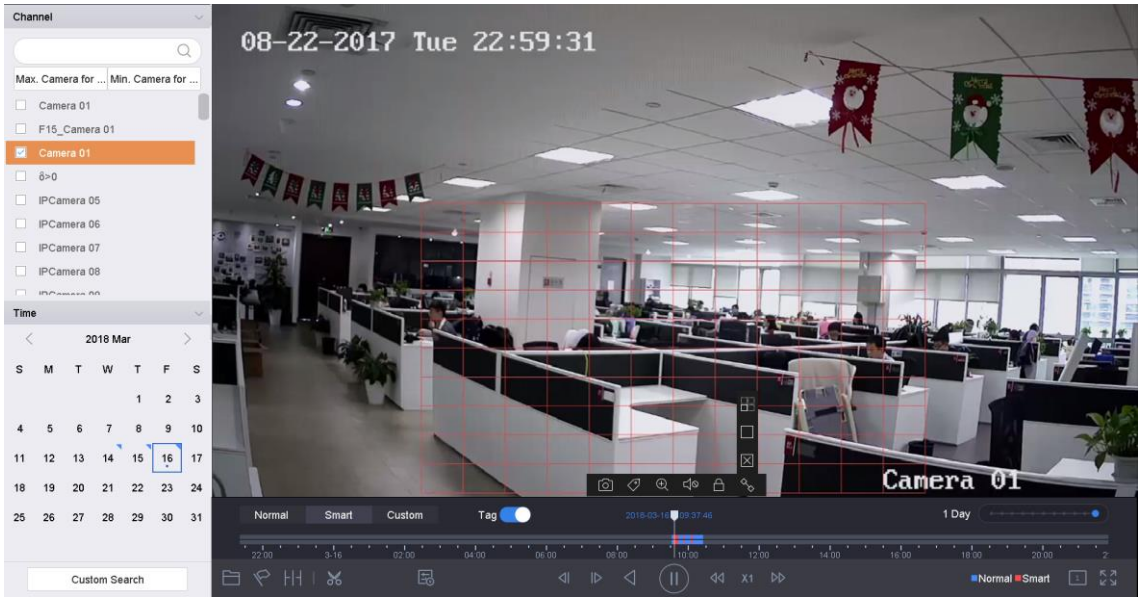


Figure 10-6 Playback by Smart Search

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

- Line Crossing Detection

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

- Intrusion Detection

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

- Motion Detection

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

10.1.5 Play Event Files

Purpose

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

Step 1 Go to **Playback**.

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

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

Step 4 Click Search.

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

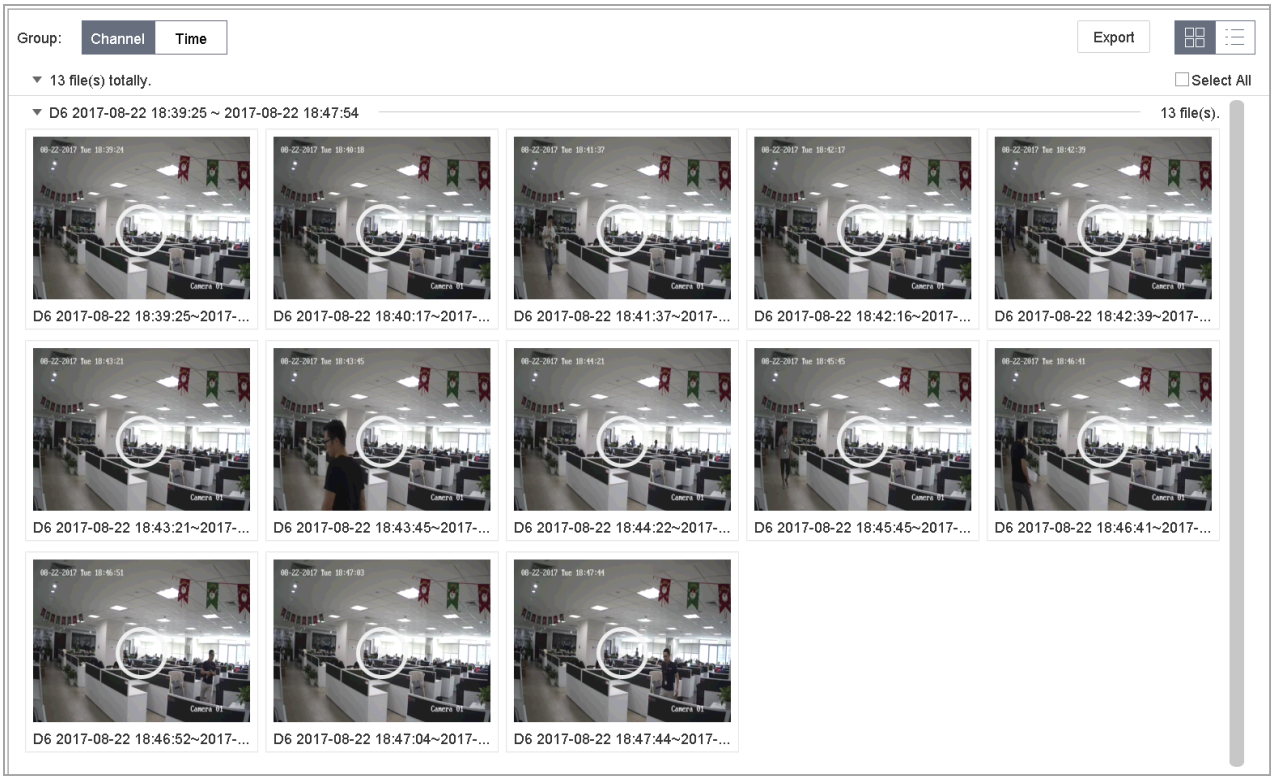


Figure 10-7 Event Files

Step 6 You can click  or  button to select the previous or next event.

NOTE

- Refer to Chapter 11 and Chapter 12 VCA Event Alarm for details for event and alarm settings.
- Refer to Chapter 7.7 Configure Event Triggered Recording for the event triggered recording settings.

10.1.6 Play by Sub-periods

Purpose:

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

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 dropdown list. Up to 16 screens are configurable.

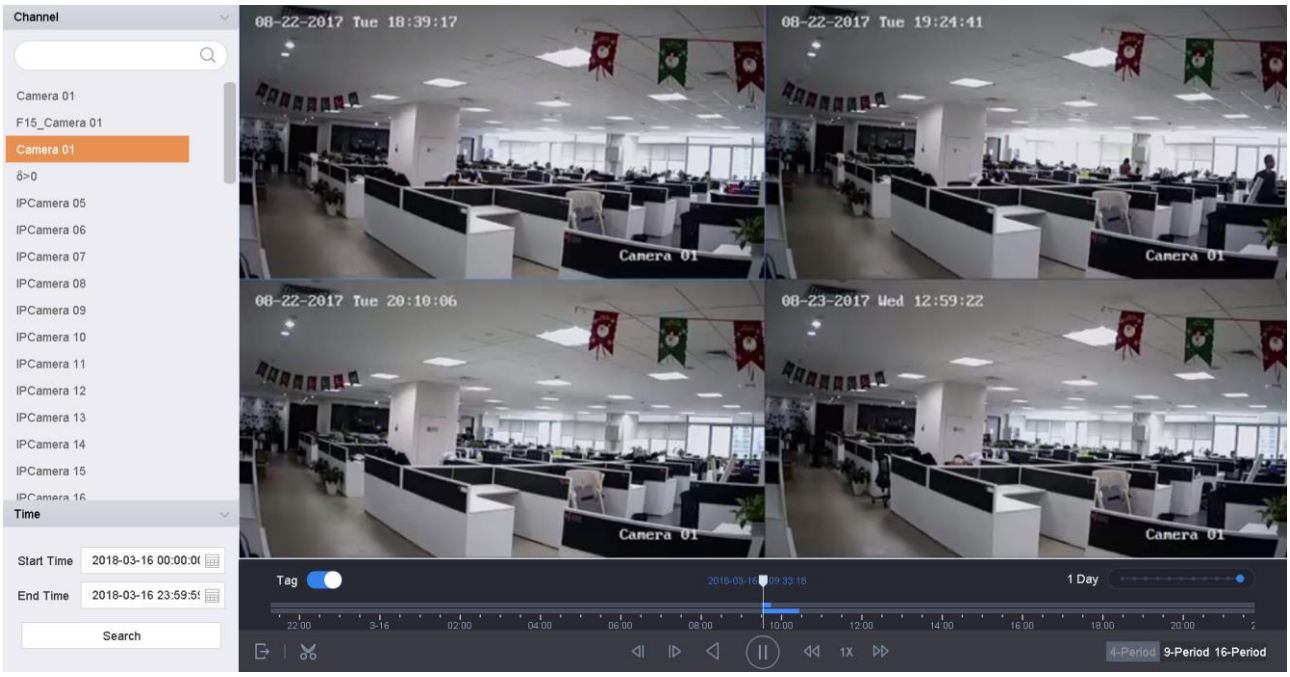


Figure 10-8 Interface of Sub-periods Playback

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.

10.1.7 Play Log Files

Purpose:

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

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

Step 2 Click **Log Search** tab to enter Playback by System Logs.

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

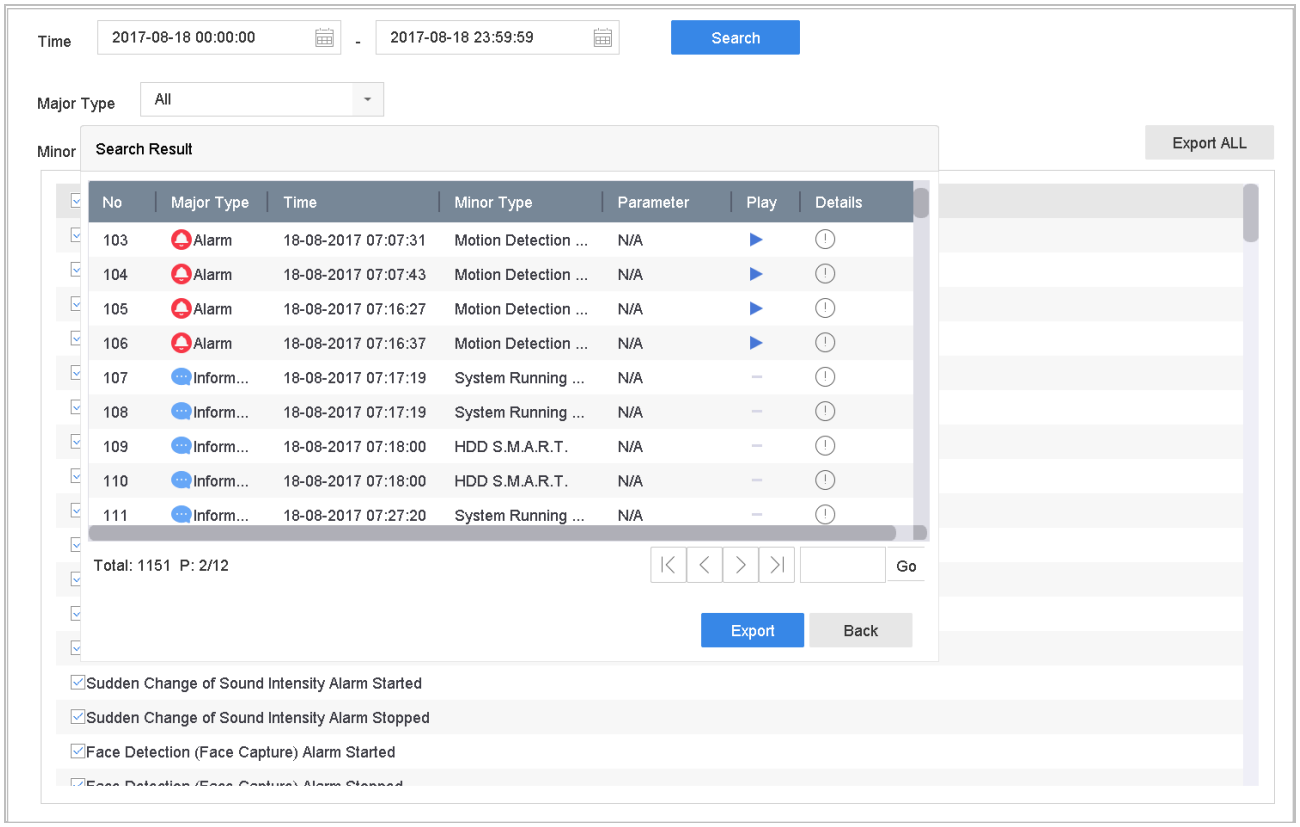


Figure 10-9 System Log Search Interface

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

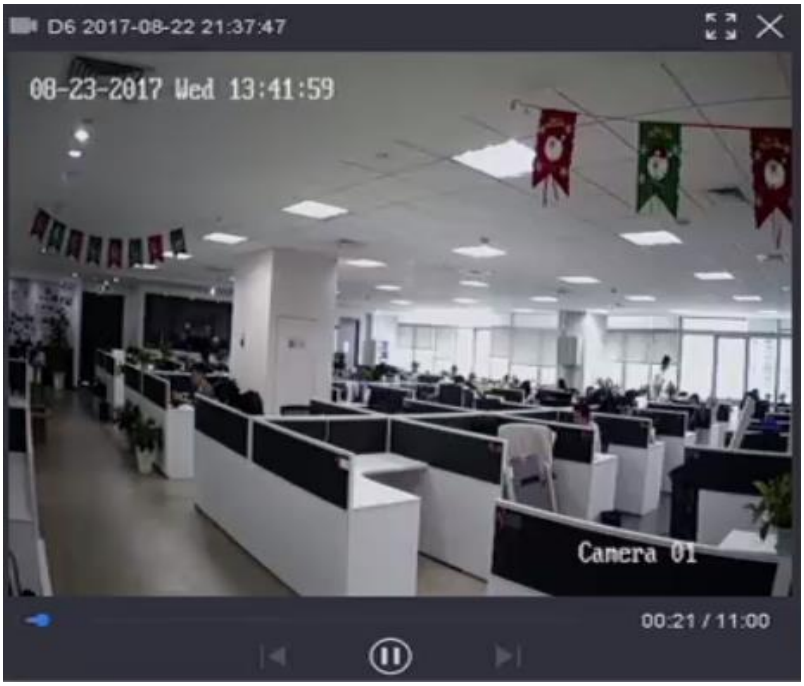


Figure 10-10 Interface of Playback by Log

10.1.8 Play External File

Purpose:

You can play files from the 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 the  icon at the left bottom corner.

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

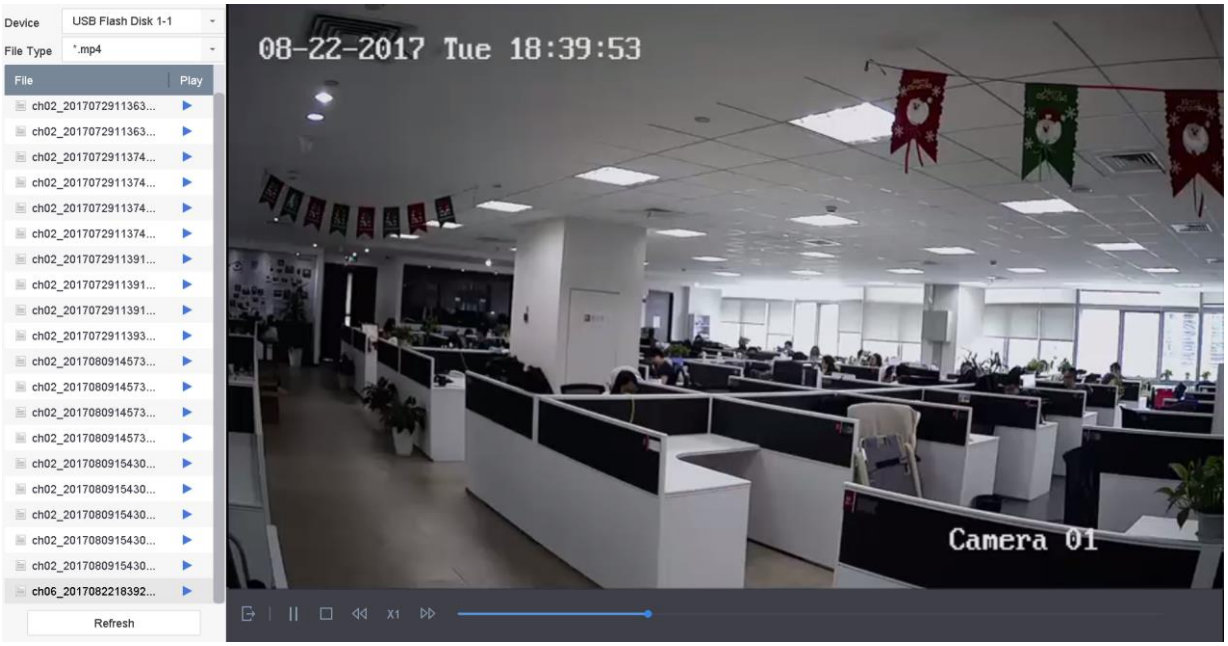


Figure 10-11 External File Playback

10.2 Playback Operations

10.2.1 Normal/Important/Custom Video

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

Normal: video files from the continuous recording.

Important: video files from the event and alarm recording triggered recording.

Custom: video files searched by custom conditions.

10.2.2 Set Play Strategy in Important/Custom Mode

Purpose:

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

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 the normal speed (X1).

When **Do not Play Normal Videos** is unchecked, you can set the play speed for the normal video the important/custom video separately. The speed range is from X1 to XMAX.

NOTE

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

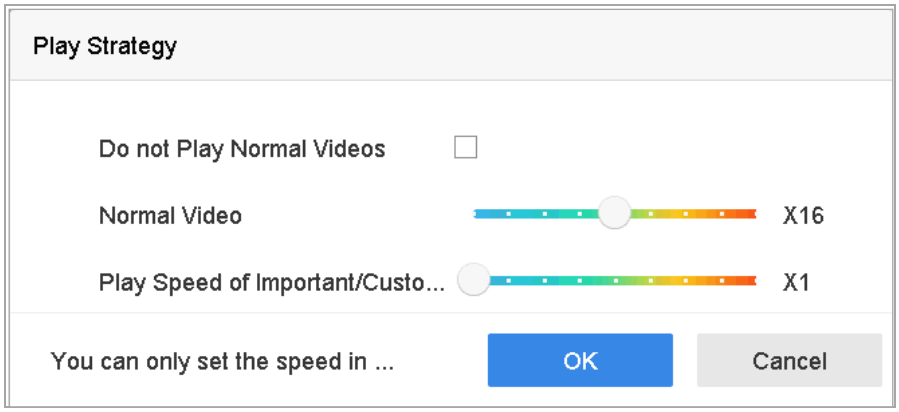


Figure 10-12 Play Strategy

10.2.3 Edit Video Clips

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

In the video playback mode, click  to start video clipping operation.

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

10.2.4 Switch between Main Stream and Sub-Stream

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

10.2.5 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 get the preview thumbnails of the video files.

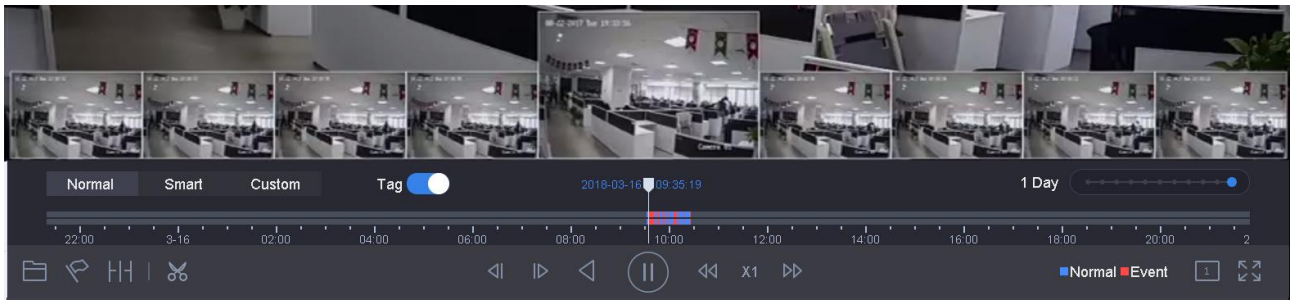


Figure 10-13 Thumbnails View

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

NOTE

The thumbnail view is supported only in the 1X single-camera playback mode.

10.2.6 Fisheye View

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

Click the  to enter the fisheye expansion mode.

- **180° Panorama ()**: Switch the live view image to the 180° panorama view.
- **360° Panorama ()**: Switch the live view image to the 360° panorama view.
- **PTZ Expansion ()**: The PTZ Expansion is the close-up view of some 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.

NOTE

iDS-9600NXI-I8/4F(B) series do not support fisheye view.

10.2.7 Fast View

You can hold the mouse to drag on the time bar to get the fast view of the video files.

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

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

NOTE

The fast view is supported only in the 1X single-camera playback mode.

10.2.8 Digital Zoom

In the video playback mode, click  from the toolbar to enter the digital zoom interface.

You can move the sliding bar or scroll the mouse wheel to zoom in/out the image to different proportions (1 to16X).

Figure 10-14 Digital Zoom

Chapter 11 Event and Alarm Settings

11.1 Configure Arming Schedule

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

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

NOTE

Time periods shall not be repeated or overlapped.

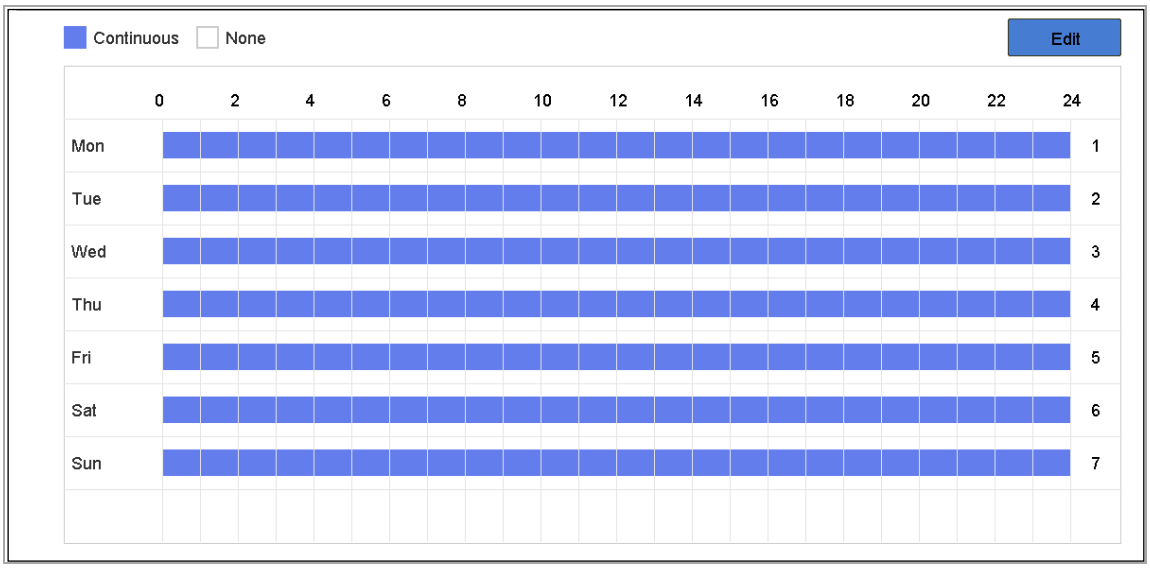


Figure 11-1 Set Arming Schedule

Step 3 (Optional) If you want to copy the same arming schedule of the current day to the other day (s) of the week or holiday, you can click the icon to copy arming schedule settings.

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

11.2 Configure 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.

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

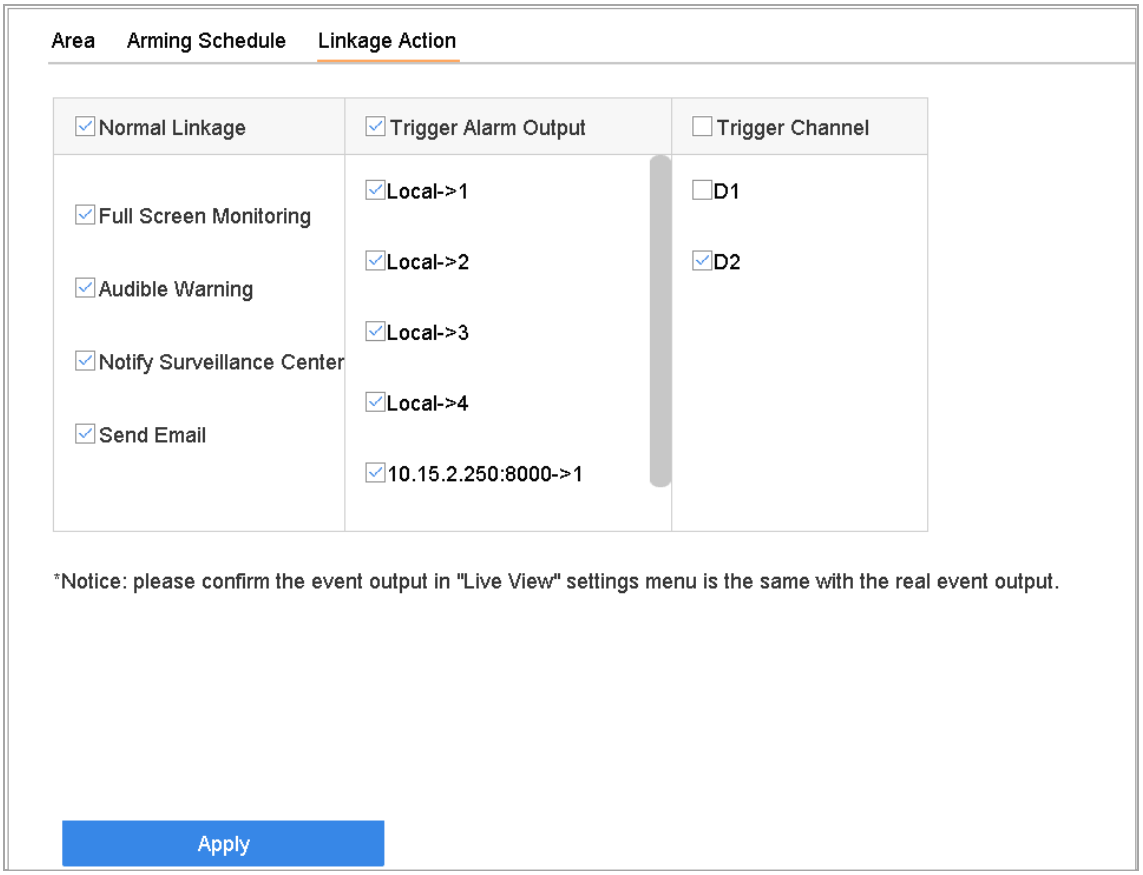


Figure 11-2 Set Linkage Actions

Step 2 Select the normal linkage actions, trigger alarm output or trigger recording channel. For details, refer to Chapter 11.2.1 to 11.2.6 .

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

11.2.1 Configure Auto-Switch Full Screen Monitoring

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

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

Step 2 Set the event output and dwell time.

Event Output: Select the output to show event video.

Full Screen Monitoring Dwell Time: Set the time in seconds to show 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, facial detection, etc.).

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

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

NOTE

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

11.2.2 Configure Audio Warning

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

Step 1 Go to **System** > **Live 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, facial detection, etc.).

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

11.2.3 Notify Surveillance Center

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

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, facial detection, etc.).

Step 4 Select the Notify Surveillance Center.

11.2.4 Configure Email Linkage

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

Please refer to Chapter 17.7 Configure Email for details of Email configuration.

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

Step 2 Configure the Email settings.

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

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

11.2.5 Trigger Alarm Output

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

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

Step 2 Click the Trigger Alarm Output tab.

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

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

Step 5 Select an alarm output item from the list.

NOTE

Refer to Chapter 11.6.3 Configure Alarm Output for the alarm output settings.

11.2.6 Configure PTZ Linkage

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

NOTE

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

Step 1 Go to the **Linkage Action** interface of the alarm input or VCA detection (e.g., facial 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.

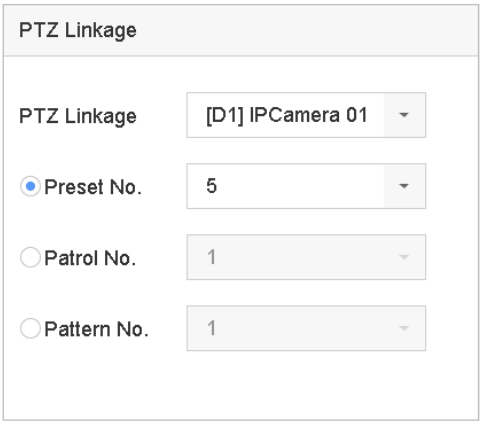


Figure 11-3 PTZ Linkage

NOTE

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

11.3 Configure Motion Detection Alarm

The motion detection enables the device to detect the moving objects in the monitoring area and trigger the alarm.

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

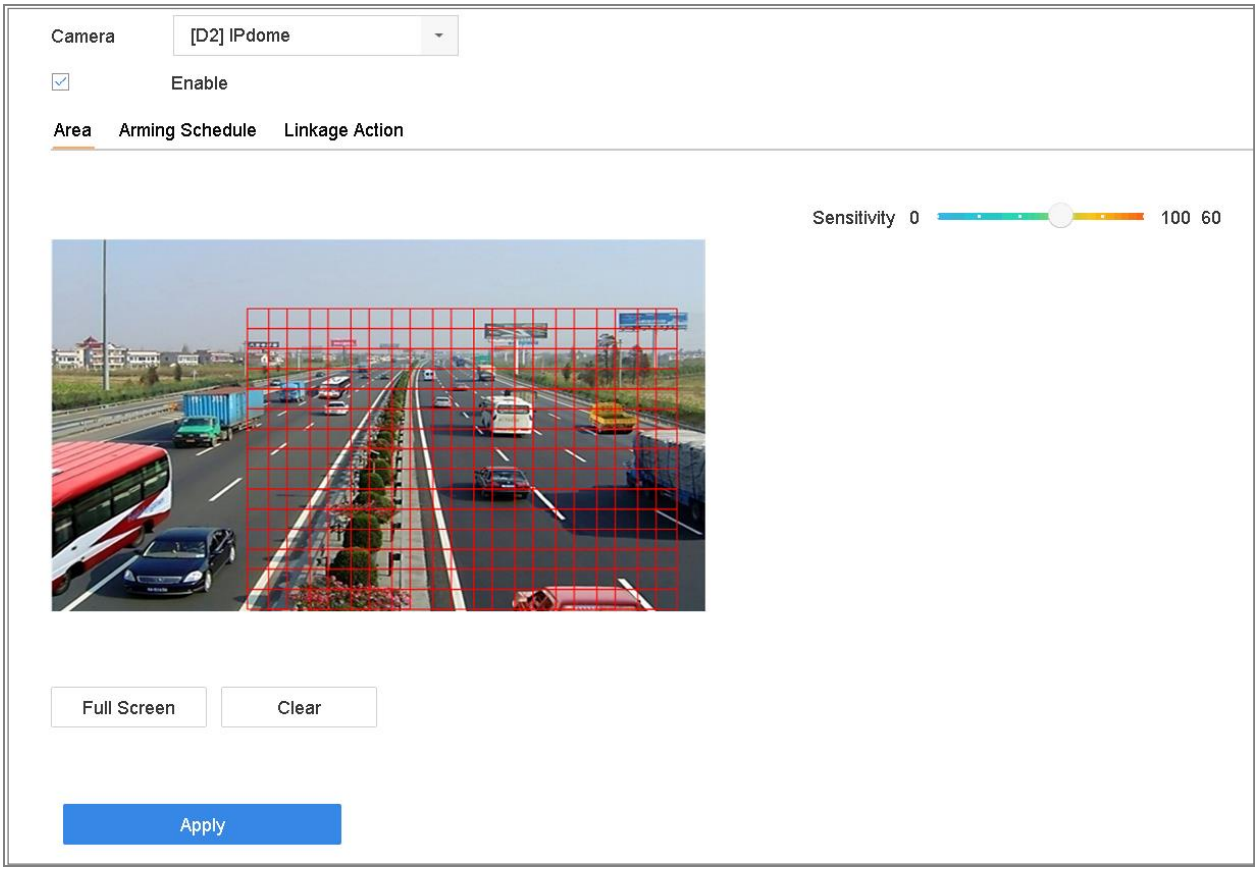


Figure 11-4 Set Motion Detection

Step 2 Select the camera to configure the motion detection.

Step 3 Check **Enable**.

Step 4 Set the motion detection area.

Full screen: click to set the full-screen motion detection for the image.

Customized area: use the mouse to click and drag on the preview screen to draw the customized motion detection area (s).

You can click **Clear** to clear the current motion detection area settings and draw again.

Step 5 Set sensitivity (0-100). The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the motion detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.4 Configure Video Loss Alarm

Purpose:

The video loss detection enables to detect video loss of a channel and take alarm response action(s).

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

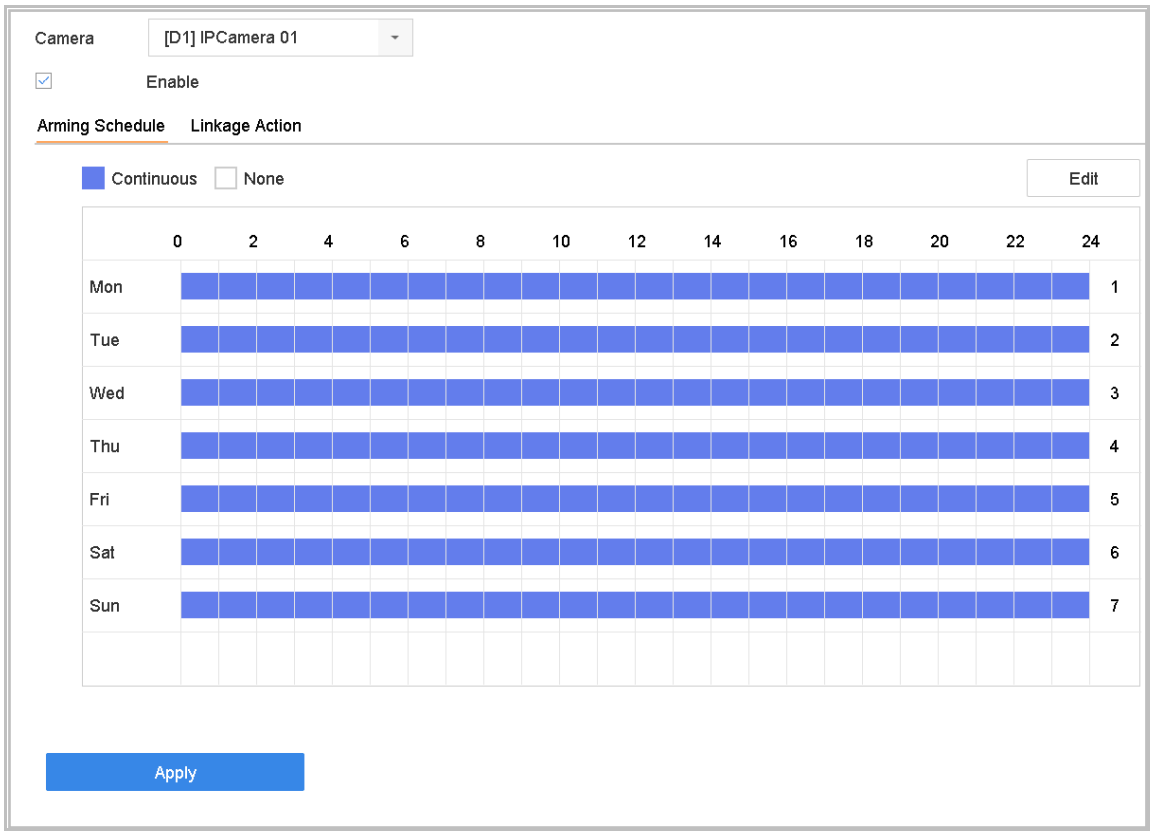


Figure 11-5 Set Video Loss Detection

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

Step 3 Check **Enable**.

Step 4 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 5 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.5 Configure Video Tampering Alarm

Purpose:

The video tampering detection enables to trigger alarm when the camera lens is covered and take 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.

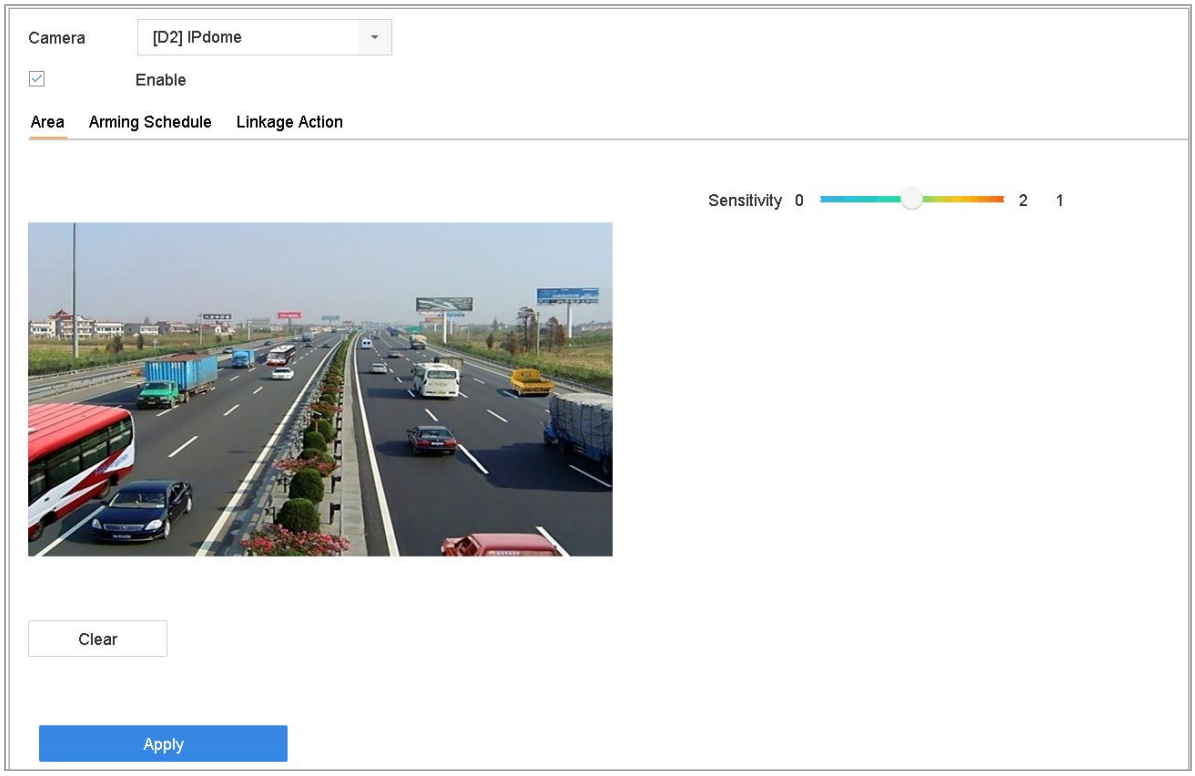


Figure 11-6 Set Video Tampering Setting

Step 3 Check **Enable**.

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

You can click **Clear** to clear the current area settings and draw again.

Step 5 Set sensitivity level (0-2). 3 levels are available. The sensitivity allows you to calibrate how readily movement triggers the alarm. The higher value results in the more readily to trigger the video tampering detection.

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.6 Configure Sensor Alarms

Purpose:

Set the handling action of an external sensor alarm.

11.6.1 Configure Alarm Input

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

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

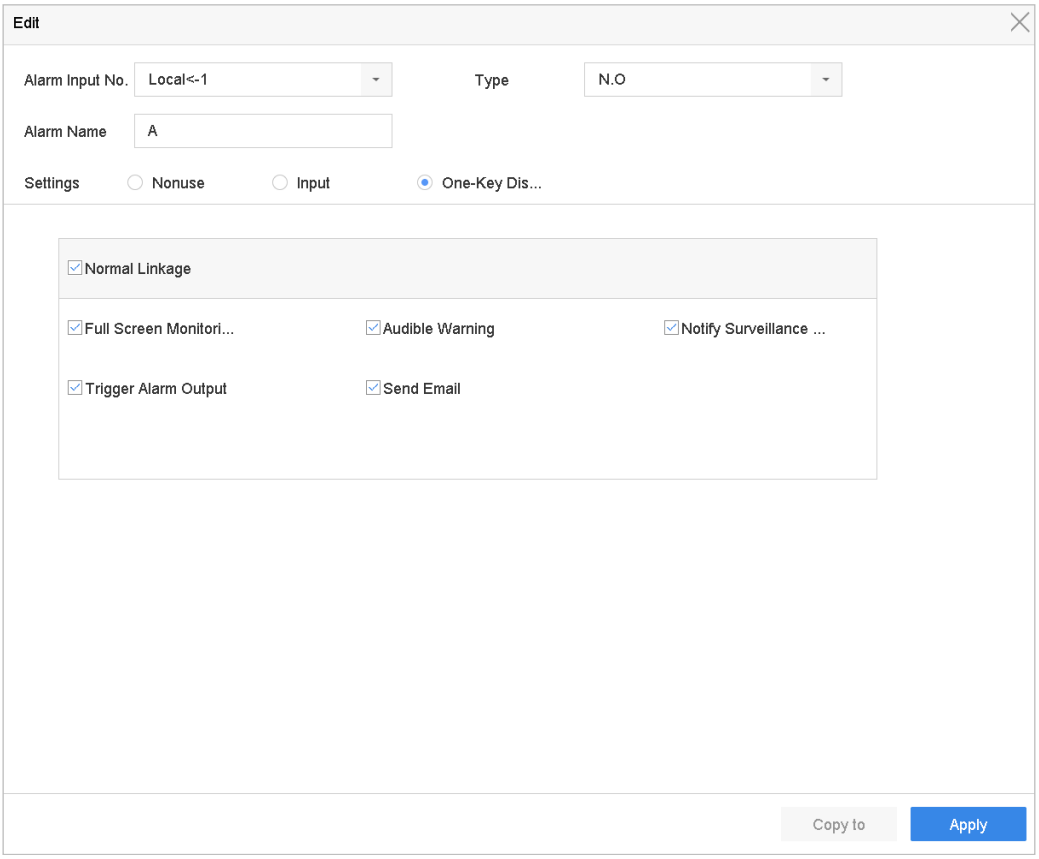


Figure 11-7 Alarm Input

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

Step 4 Edit the alarm name.

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

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

11.6.2 Configure One-Key Disarming

The one-key disarming enables the device to disarm the alarm input 1 by one-key operation.

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

Step 2 Select the alarm input1 item from the list and click .

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

Step 4 Edit the alarm name.

Step 5 Check the radio button of **Enable One-Key Disarming**.

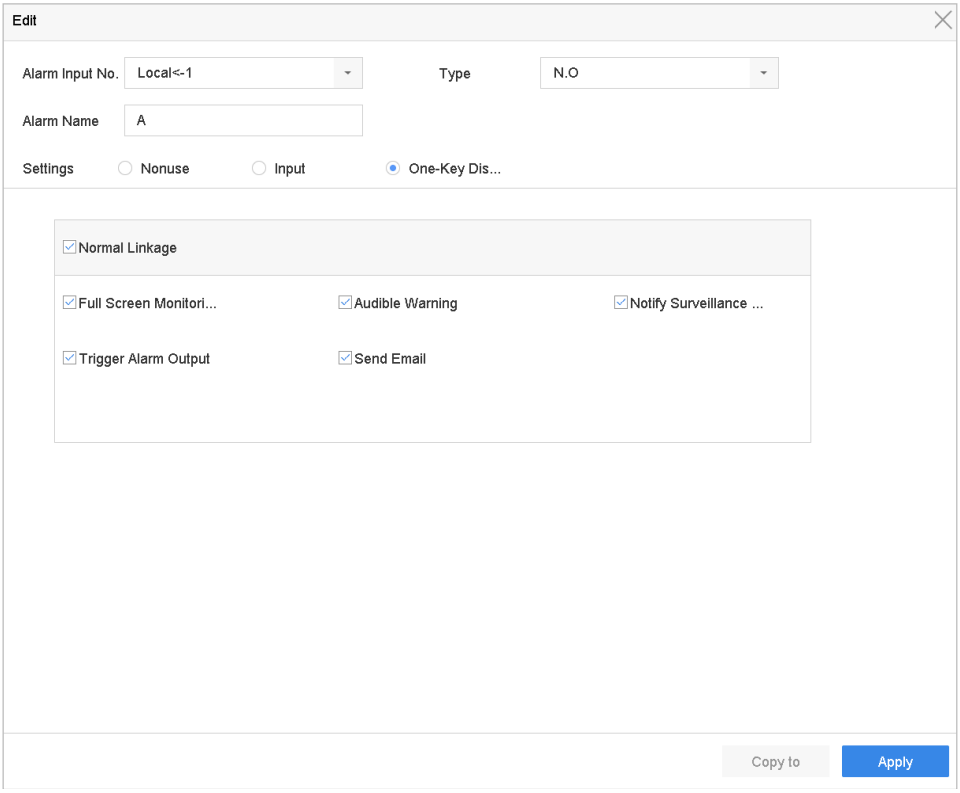


Figure 11-8 One-Key Alarm Disarming

Step 6 Select the alarm linkage action (s) you want to disarm for the local alarm input1.

NOTE

When the 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.

11.6.3 Configure Alarm Output

Trigger an alarm output when an alarm is triggered.

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

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

Step 3 Edit the alarm name.

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

Manually Clear: you should manually clear the alarm when the alarm occurs. Refer to Chapter 11.8 Trigger or Clear Alarm Output Manually for detailed instructions.

Step 5 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

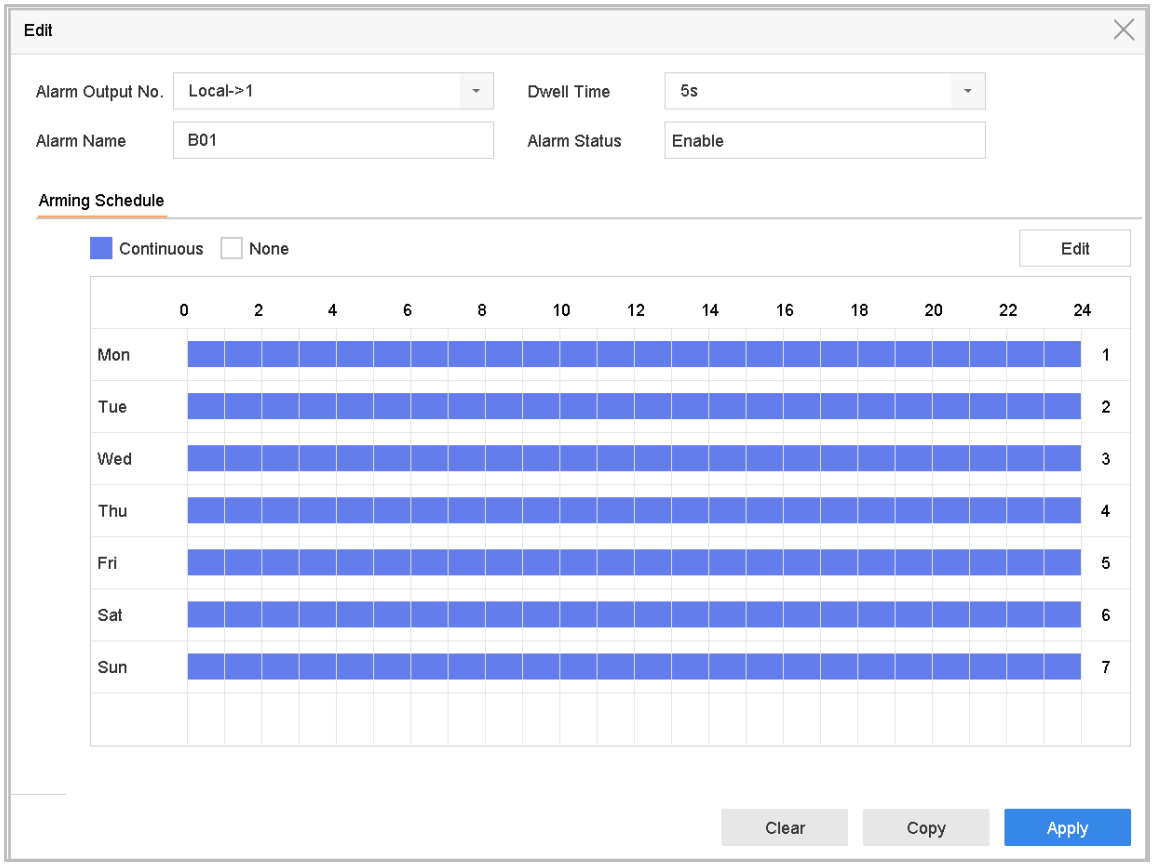


Figure 11-9 Alarm Output

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

11.7 Configure Exceptions Alarm

The exception events can be configured to take the event hint in the live view window, trigger alarm output and linkage actions.

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

Step 2 (Optional) Enable the event hint if you want to display the event hint in the live view window.

1) Check the checkbox of **Enable Event Hint.**

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

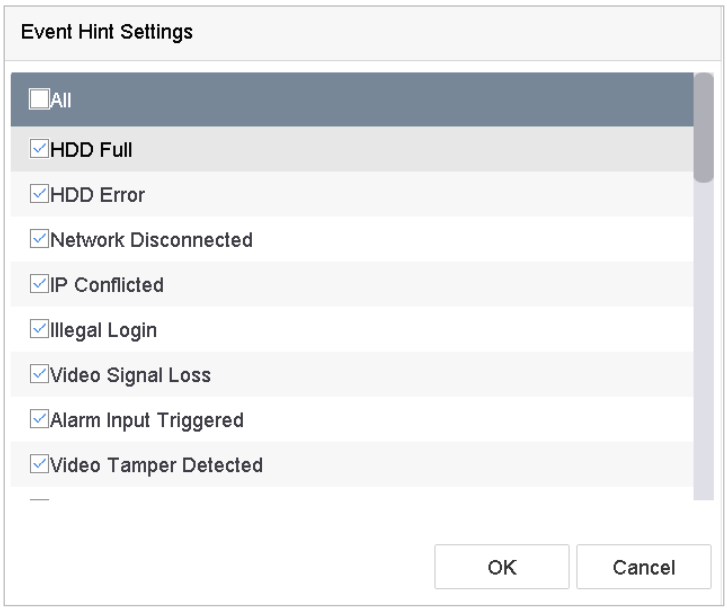


Figure 11-10 Event Hint Settings

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

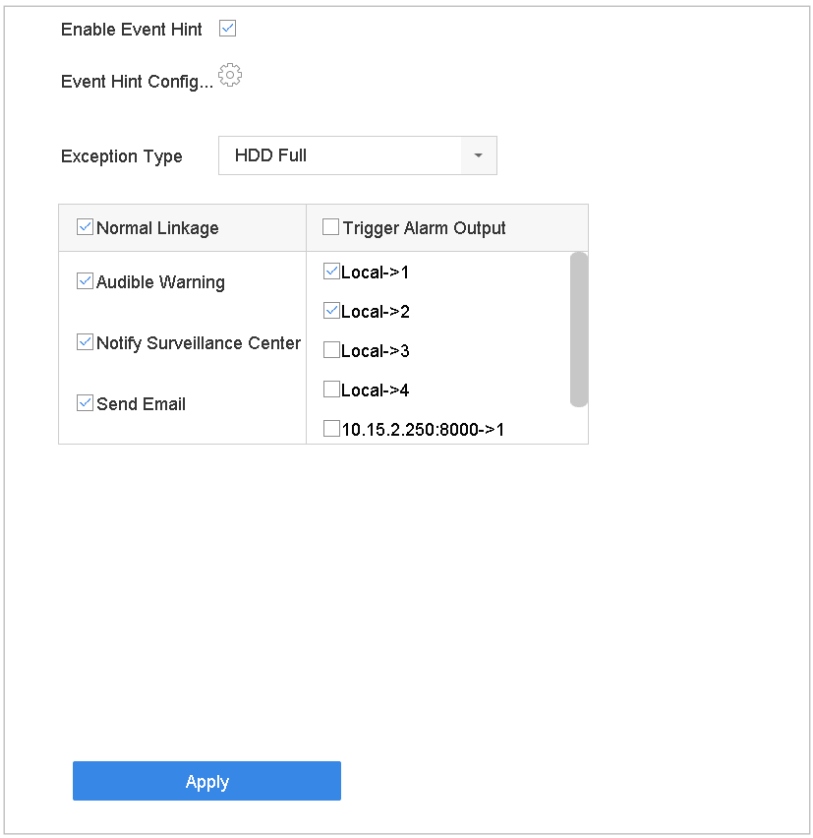


Figure 11-11 Exceptions Handling

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

11.8 Trigger or Clear Alarm Output Manually

Purpose:

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

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

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

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

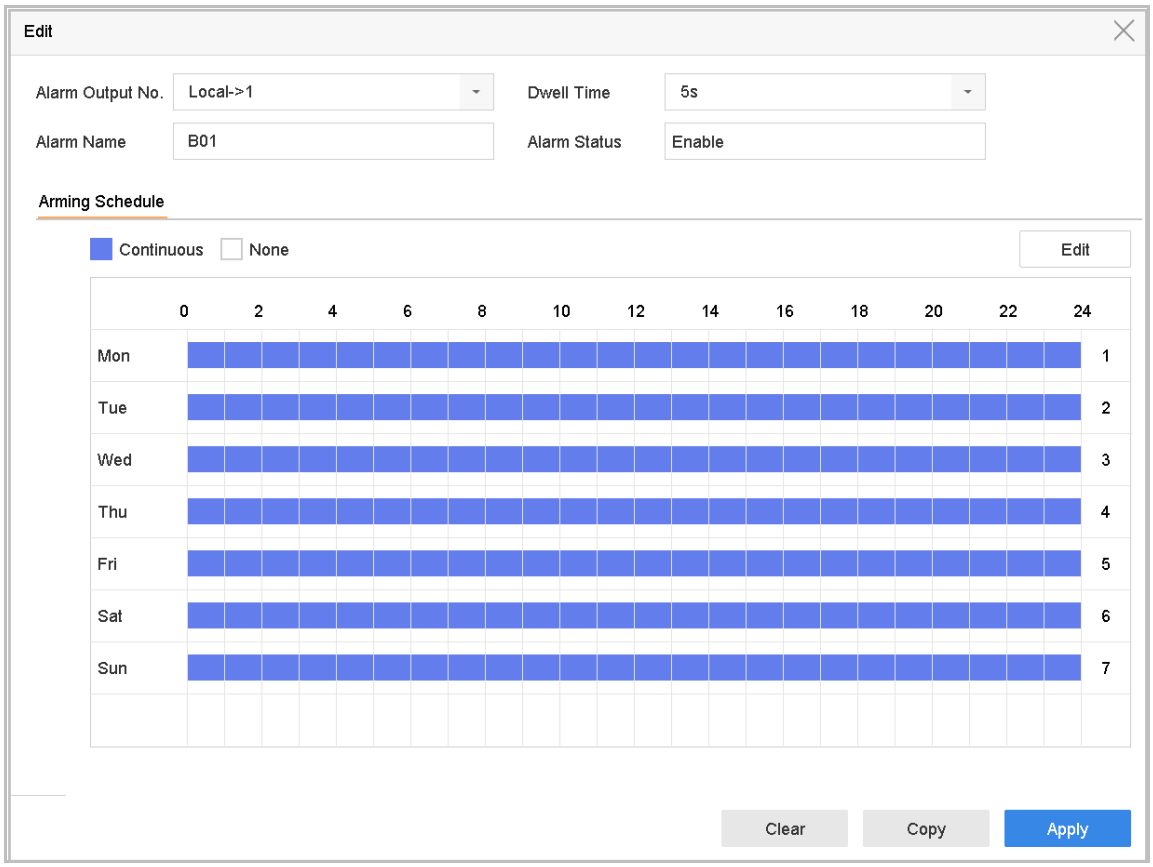


Figure 11-12 Alarm Output

Chapter 12 VCA Event Alarm

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

NOTE

- VCA detections must be supported by the connected IP camera.
- Refer to the User Manual of Network Camera for the detailed instructions for the VCA detection.

12.1 Facial Detection

Purpose:

Facial detection function detects the face appears in the surveillance scene. Linkage actions will be triggered when a human face is detected.

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

Step 2 Select a **Camera**.

Step 3 Click **Facial Detection**.

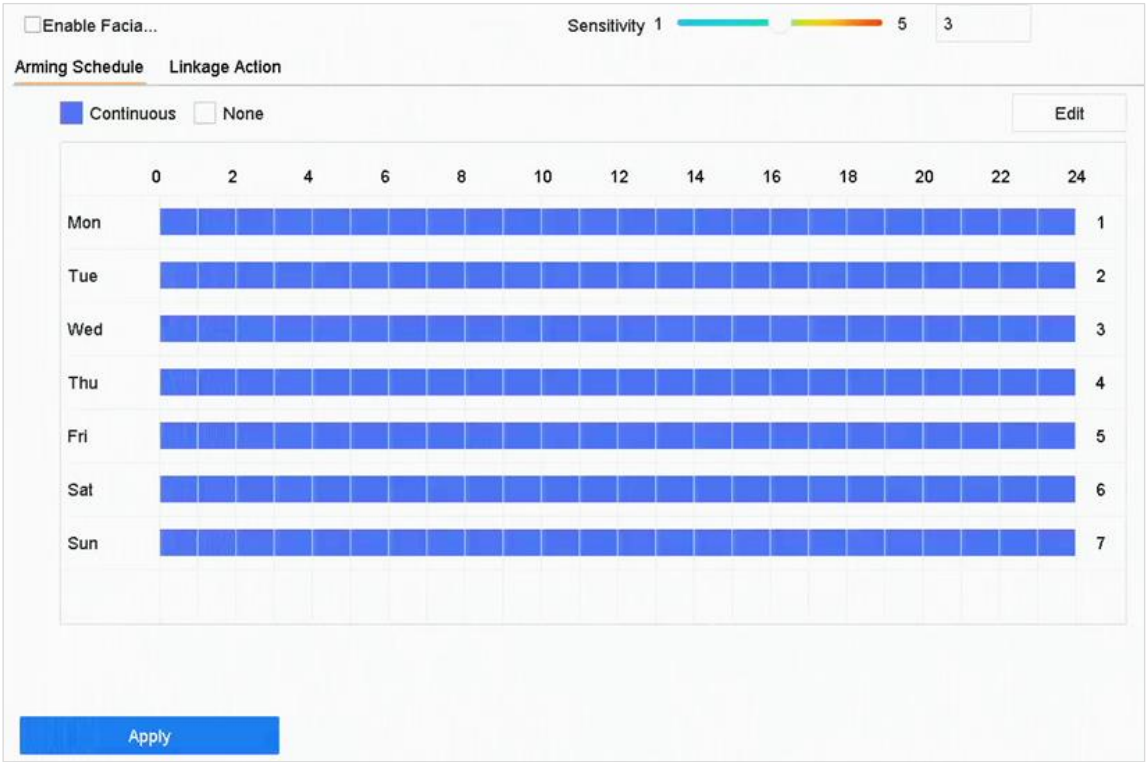


Figure 12-1 Facial Detection

Step 4 Check **Enable Facial Detection**.

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

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

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.2 Vehicle Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Vehicle**.

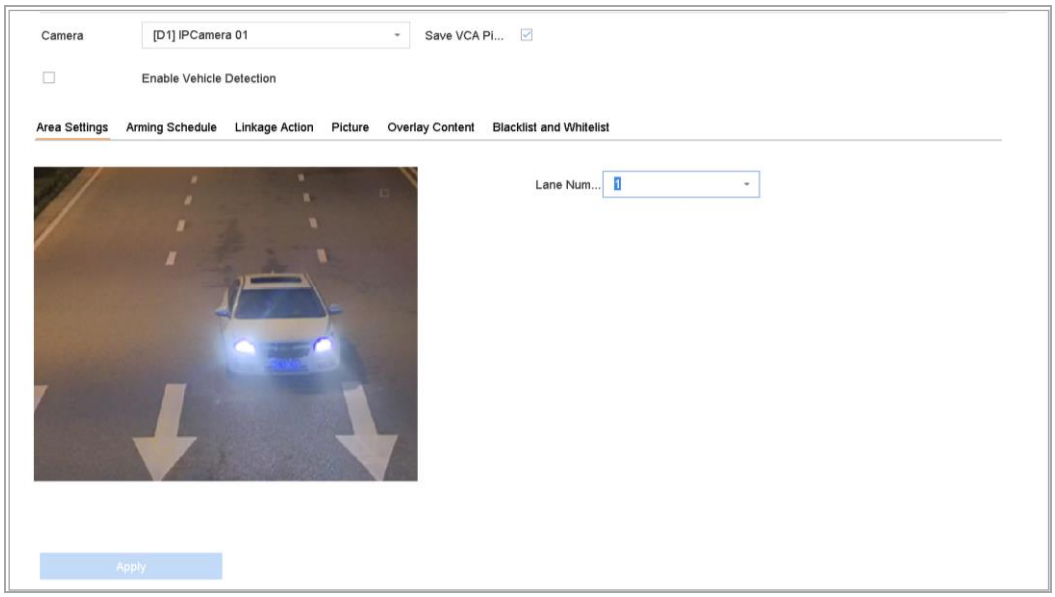


Figure 12-2 Vehicle Detection

Step 4 Check **Enable Vehicle Detection**.

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

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Configure rules, including **Area Settings, Picture, Overlay Content**, and **Blacklist and Whitelist**. Area Settings: Up to 4 lanes are selectable.

Step 9 Click **Save**.

NOTE

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

12.3 Line Crossing Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Line Crossing**.

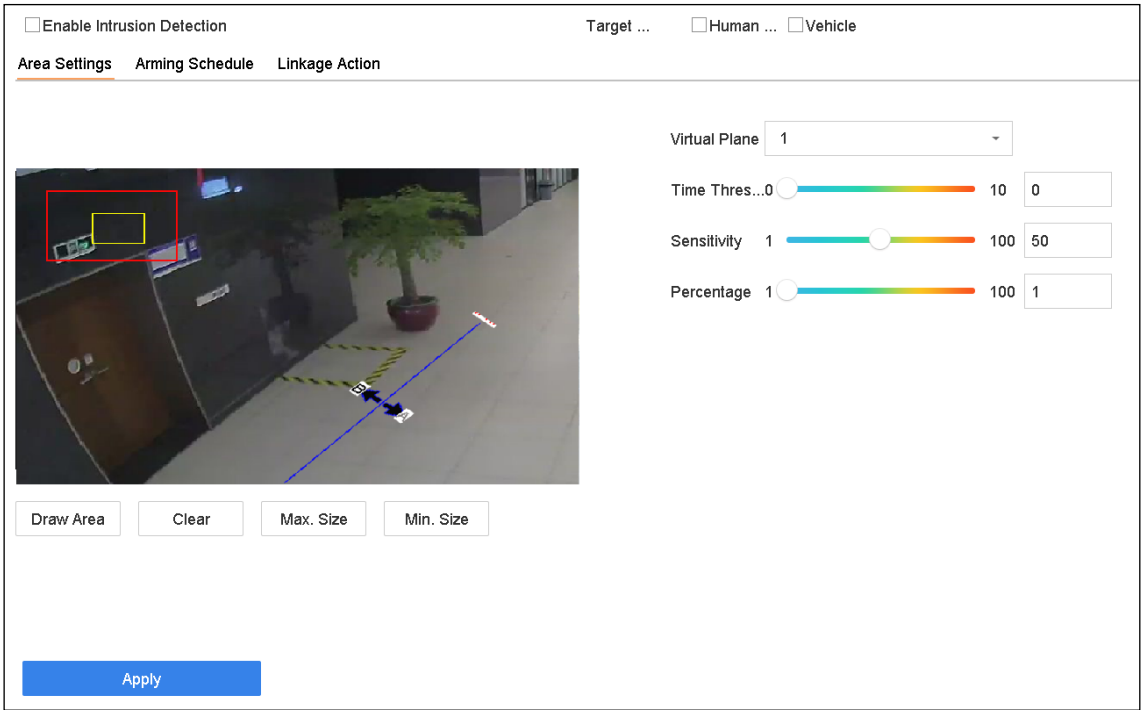


Figure 12-3 Line Crossing Detection

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

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

Step 6 Select **Target of Interest** as **Human Body** or **Vehicle** to discard line crossing detection pictures and video files which are not triggered by human body or vehicle.

Step 7 Follow the steps to set the line crossing detection rules and detection areas.

1) Select an Arming Region to configure. Up to 4 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. When an object goes across the configured line with both directions can be detected and alarms are triggered.

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

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

3) Drag the Sensitivity slider to set the detection sensitivity. Sensitivity range: sensitivity. The higher the value is, the more easily the detection alarm can be triggered.
4) Click Draw Region and set two points in the preview window to draw a virtual line.

Step 8 Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger line crossing detection.

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

Step 9 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 10 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 11 Click **Apply**.

12.4 Intrusion Detection

Purpose:

Intrusion detection function detects people, vehicle or other objects which enter and loiter in a pre-defined virtual region, and some certain actions can be taken when the alarm is triggered.

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Intrusion**.

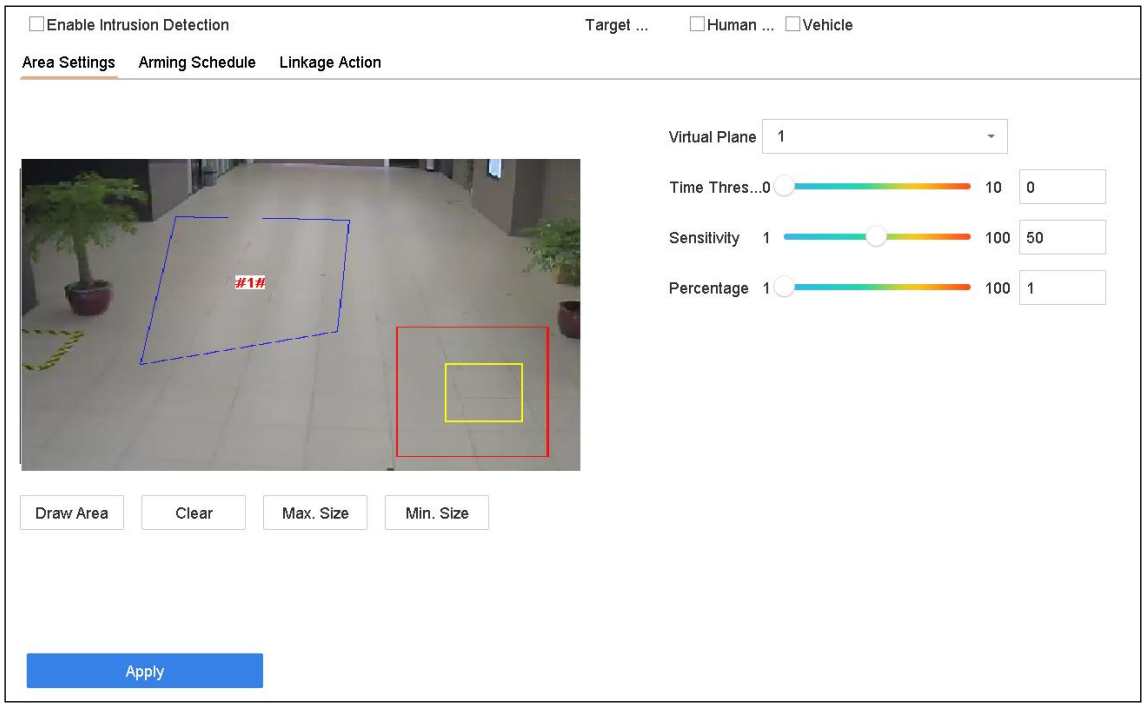


Figure 12-4 Intrusion Detection

Step 4 Check **Enable Intrusion Detection**.

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

Step 6 Select **Target of Interest** as **Human Body** or **Vehicle** to discard intrusion detection pictures and video files which are not triggered by human body or vehicle.

Step 7 Follow the steps to set the detection rules and detection areas.

1) Select a Virtual Panel to configure. Up to 4 virtual panels are selectable.
2) Drag the sliders to set Time Threshold, Sensitivity, and Percentage.

   Time Threshold: The threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the threshold, device will trigger an alarm. Its range is [1s-10s].

   Sensitivity: The size of the object that can trigger the alarm. The higher the value is, the more easily the detection alarm can 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, 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 vertexes of the detection region.

Step 8 Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger line crossing detection.

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

2) Draw an area in preview window.
3) Click **Stop Drawing**.

Step 9 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 10 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 11 Click **Apply**.

12.5 Region Entrance Detection

Purpose:

Region entrance detection function detects objects that enter a pre-defined virtual region from the outside place.

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Region Entrance Detection**.

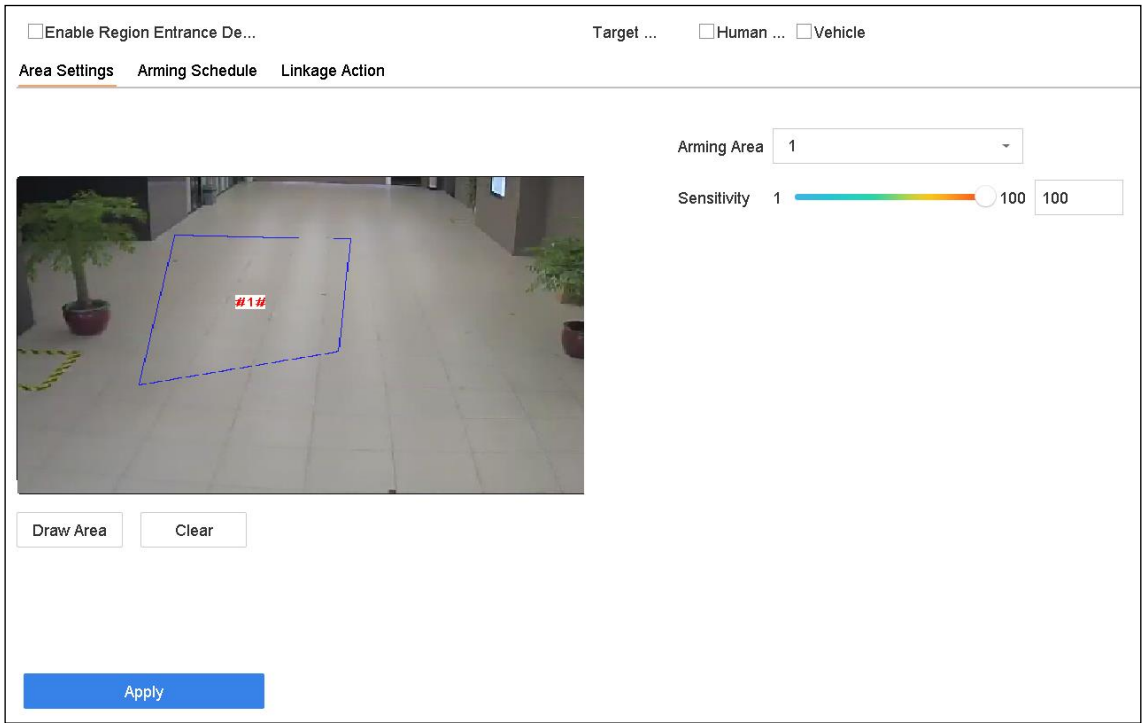


Figure 12-5 Region Entrance Detection

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

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

Step 6 Select **Target of Interest** as **Human Body** or **Vehicle** to discard region entrance pictures and video files which are not triggered by human body or vehicle.

Step 7 Follow the steps to set the detection rules and detection areas.

1) Select an Arming Region to configure. Up to 4 regions are selectable.
2) Drag the sliders to set Sensitivity.

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

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

Step 8 Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger line crossing detection.

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

Step 9 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 10 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 11 Click **Apply**.

12.6 Region Exiting Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Region Exiting**.

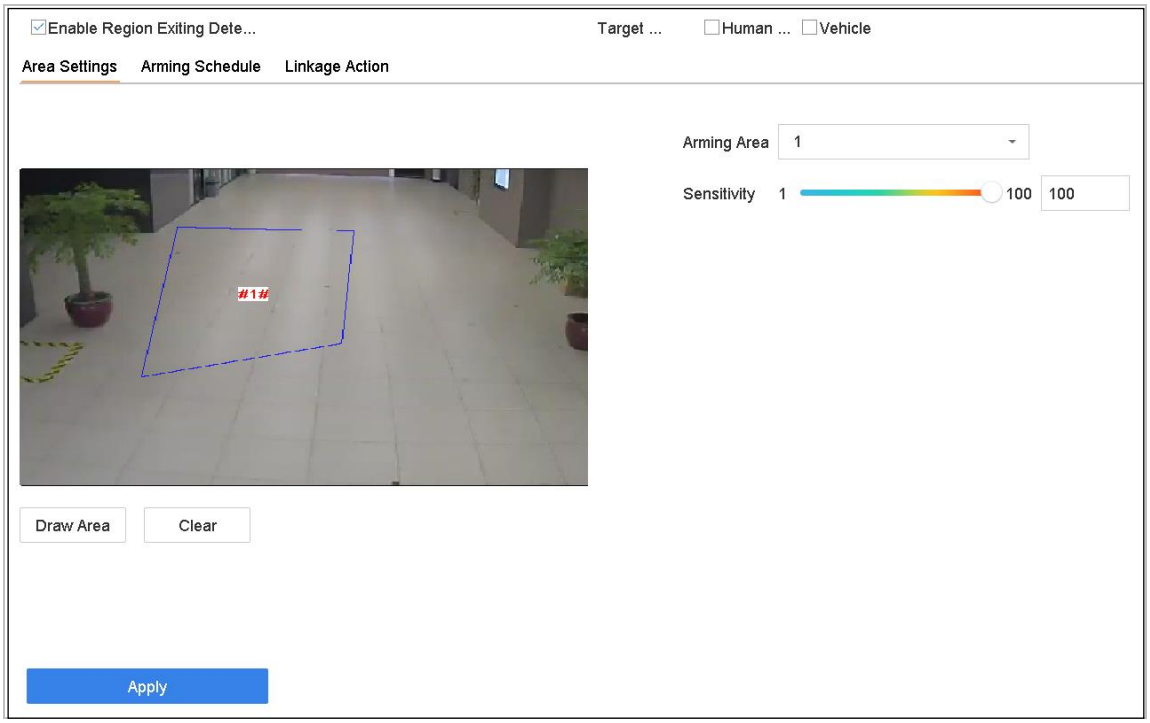


Figure 12-6 Region Exiting Detection

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

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

Step 6 Select **Target of Interest** as **Human Body** or **Vehicle** to discard region exiting pictures and video files which are not triggered by human body or vehicle.

Step 7 Follow the steps to set the detection rules and detection areas.

1) Select an Arming Region to configure. Up to 4 regions are selectable.
2) Drag the sliders to set Sensitivity.

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

3) Click Draw Region and draw a quadrilateral in the preview window by specifying four vertexes of the detection region.

Step 8 Draw the maximum size/minimum size for targets. Only target the size of which is rangers from max. size and min. size will be trigger line crossing detection.

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

Step 9 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 10 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 11 Click **Apply**.

12.7 Unattended Baggage Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Unattended Baggage**.

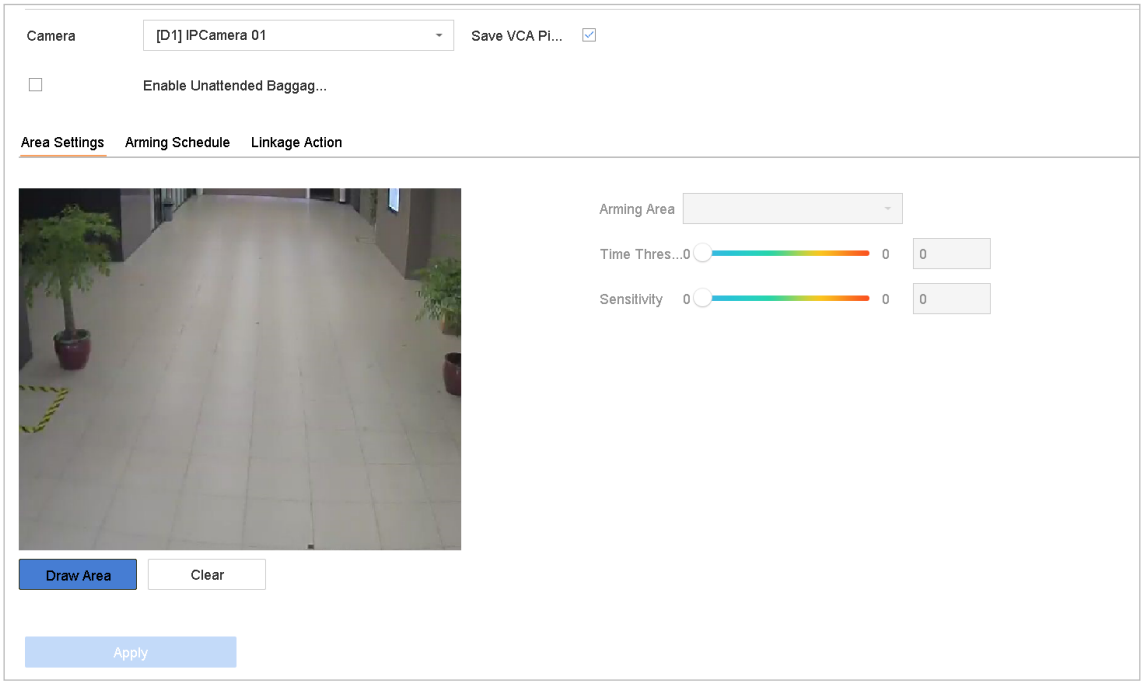


Figure 12-7 Unattended Baggage Detection

Step 4 Check Enable **Unattended Baggage Detection**.

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

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

1) Select an **Arming Region** to configure. Up to 4 regions are selectable.
2) Drag the sliders to set **Time Threshold** and **Sensitivity**.

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

Sensitivity: Similarity degree of the background image. The higher the value is, the more easily the detection alarm can be triggered.

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

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.8 Object Removal Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Object Removable**.

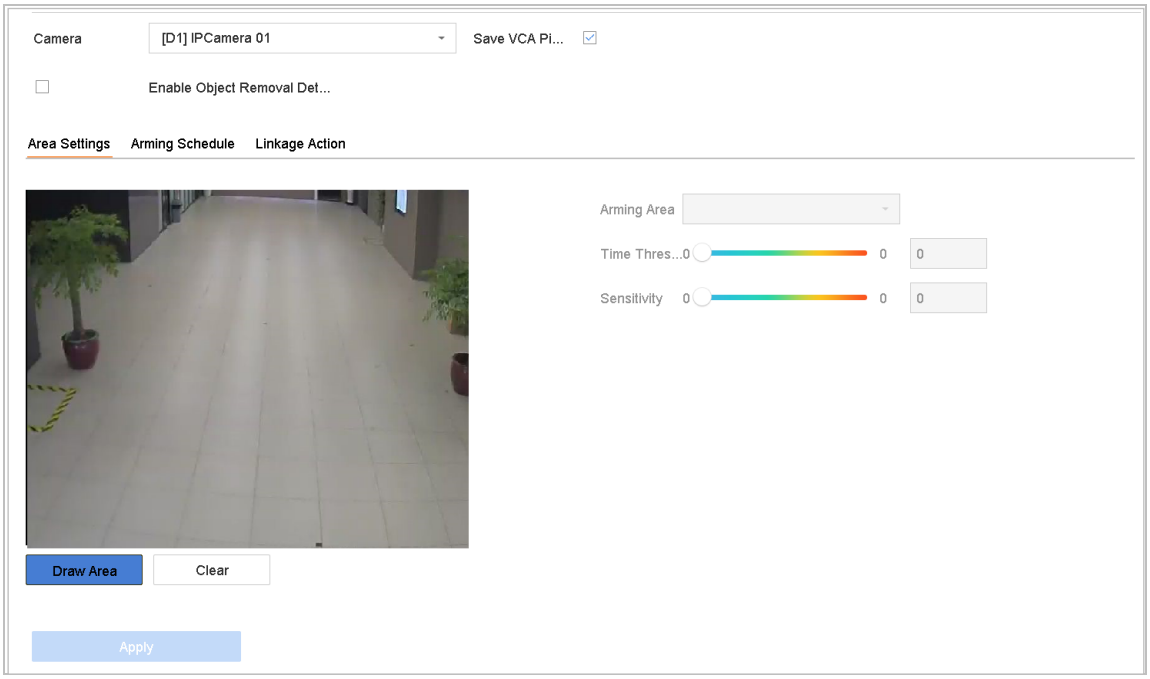


Figure 12-8 Object Removal Detection

Step 4 Check **Enable Object Removable Detection**.

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

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

1) Select an Arming Region to configure. Up to 4 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 is triggered after the object disappeared from the region for 10s. Its range is [5s-20s].

Sensitivity: The similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.

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

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.9 Audio Exception Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Audio Exception**.

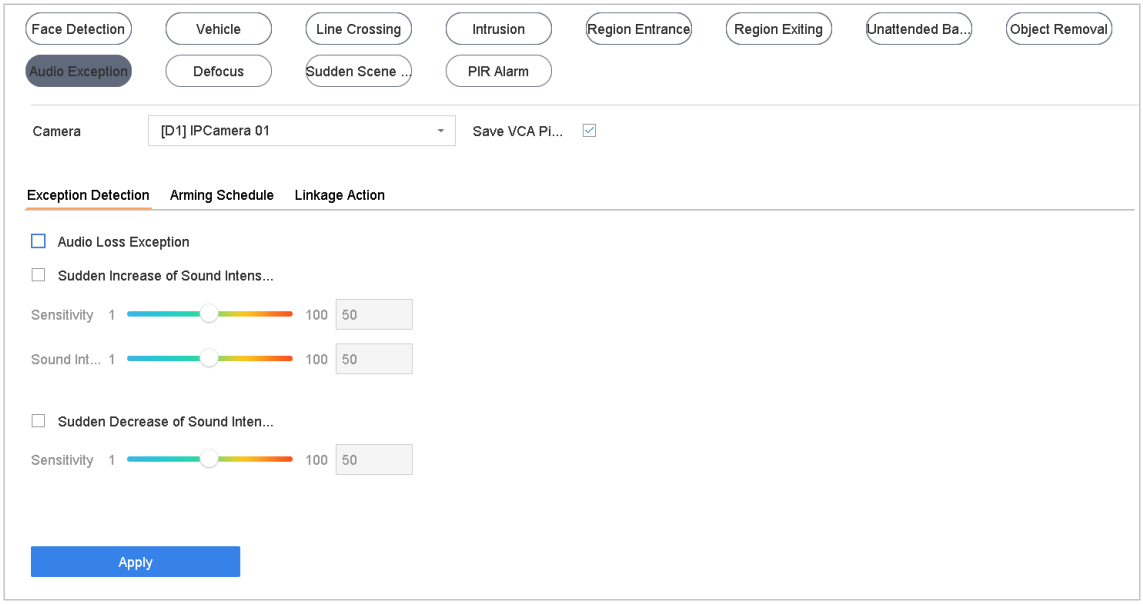


Figure 12-9 Audio Exception Detection

Step 4 (Optional) Check **Save VCA Picture** to save the captured pictures of audio exception detection.

Step 5 Follow the steps to set the detection rules.

1) Select the Exception Detection tab.
2) Check the checkboxes of Audio Loss Exception, Sudden Increase of Sound Intensity Detection, or Sudden Decrease of Sound Intensity Detection.

Audio Loss Exception: Detects the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise. You need to configure its **Sensitivity** and **Sound Intensity Threshold**.

Sensitivity: The smaller the value is, the more severe the change should 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 the sound steep drop in the surveillance scene. You need set the detection sensitivity [1-100].

Step 6 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 7 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 8 Click **Apply**.

12.10 Sudden Scene Change Detection

Purpose:

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

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

Step 2 Select a **Camera** to configure.

Step 3 Click Sudden Scene Change.

Figure 12-10 Sudden Scene Change

Step 4 Select a **Camera** to configure.

Step 5 Check **Enable Sudden Scene Change Detection**.

Step 6 (Optional) Check **Save VCA Picture** to save the captured pictures of sudden scene change detection.

Step 7 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the change of scene can trigger the alarm.

Step 8 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 9 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 10 Click **Apply**.

12.11 Defocus Detection

Purpose:

The image blur caused by defocus of the lens can be detected.

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

Step 2 Select a **Camera** to configure.

Step 3 Click **Defocus**.

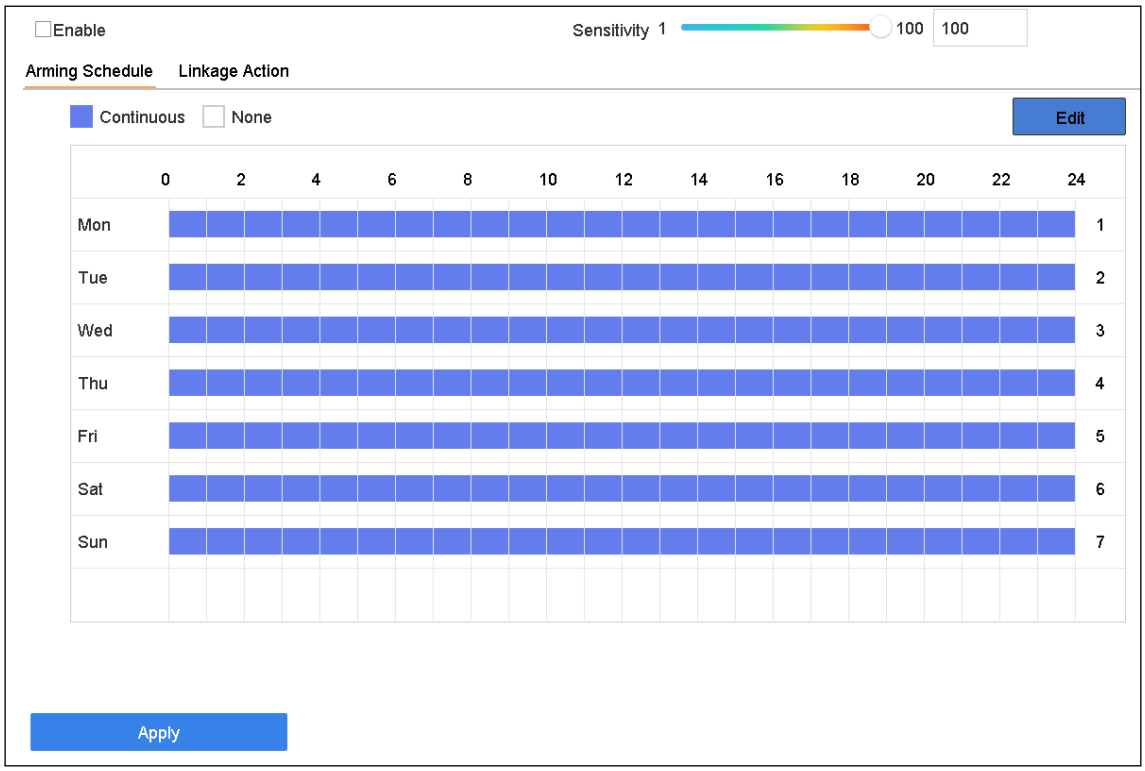


Figure 12-11 Defocus Detection

Step 4 Check **Enable Defocus Detection**.

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

Step 6 Drag the **Sensitivity** slider to set the detection sensitivity. Sensitivity range: [1-100]. The higher the value is, the more easily the defocus image can be detected.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 Click **Apply**.

12.12 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 Select a **Camera** to configure.

Step 3 Click **PIR Alarm**.

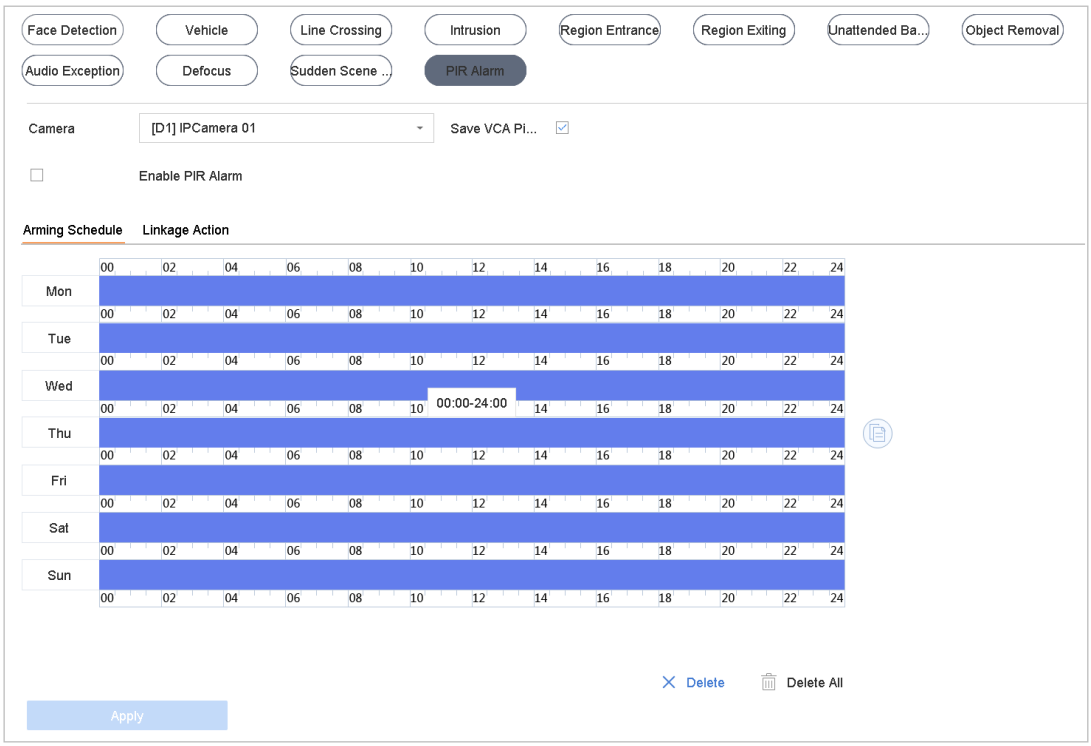


Figure 12-12 FIR Alarm

Step 4 Select a **Camera** to configure.

Step 5 Check **PIR Alarm**.

Step 6 (Optional) Check **Save VCA Picture** to save the captured pictures of PIR alarm.

Step 7 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 8 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 9 .Click **Apply**.

12.13 Thermal Camera Detection

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

Before you start

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

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

Step 2 Select a thermal camera from the camera list.

Step 3 (Optional) Check **Save VCA Picture** to save the captured pictures of detection.

Step 4 Click an event detection (Temperature A, Temperature, etc.).

Step 5 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 6 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 7 Click **Apply**.

Chapter 13 Smart Analysis

With the configured VCA detection, the device supports the smart analysis of people counting, heat map, etc.

13.1 Engine Configuration

Purpose:

Each engine processes a specified VCA type as its working mode. You can configure the engine working mode as your desire.

Step 1 Go to **Smart Analysis** > **Smart Analysis** > **Engine Configuration.**

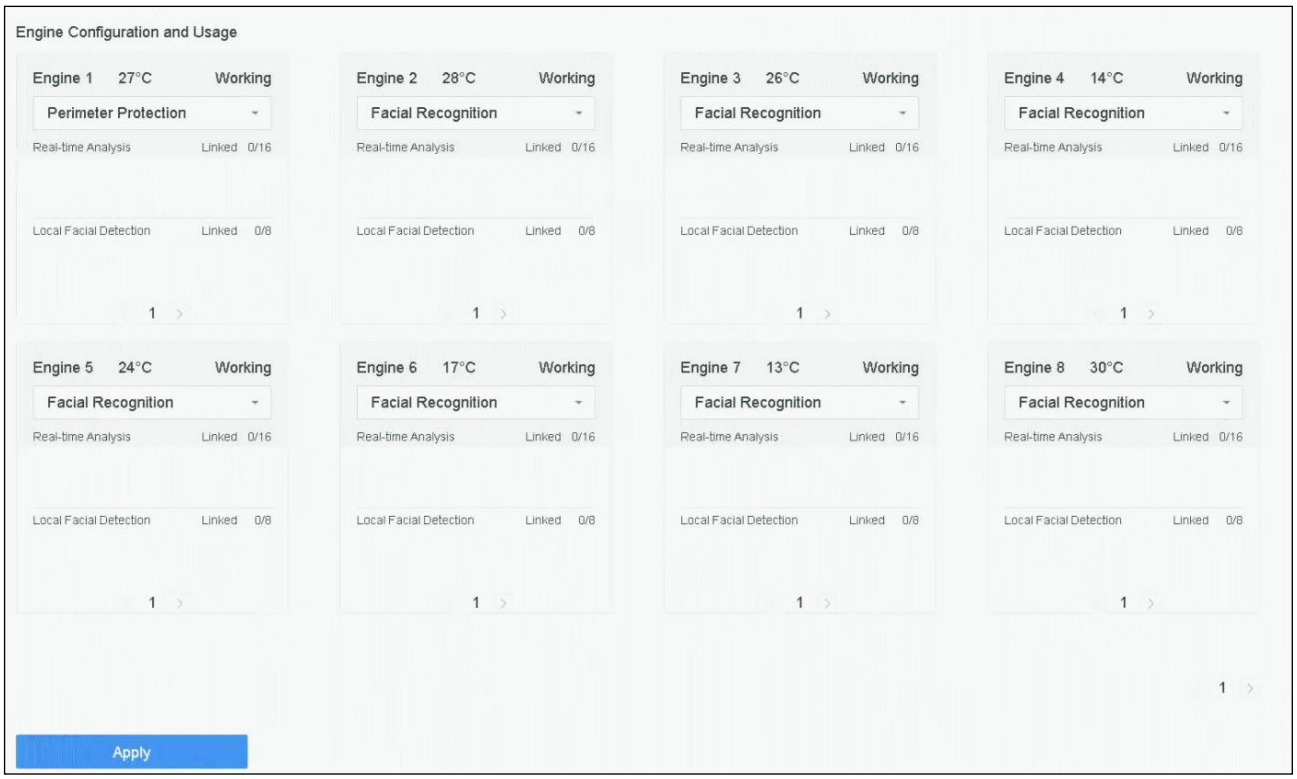


Figure 13-1 Engine Configuration

Step 2 Configure each engine usage as **Facial Recognition** or **Perimeter Protection**. You can view the engine temperature and linked channel status of each function.

NOTE

- S(B) series only support **Perimeter Protection** mode.
- If the engine has been bound with channel(s), switching engine working mode will unbind the engine and channel(s), and cancel the related smart event of the channel.

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

13.2 Task Configuration

Purpose:

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

Before you start

Check **Save VCA Pictures** for human body detection/vehicle detection, line crossing detection, intrusion detection, region entrance, or region exiting.

Step 1 Go to **Smart Analysis** > **Smart Analysis** > **Task Configuration**.

Step 2 Check cameras to enable corresponding analysis mode. Ensure engine is available for the selected analysis mode.

Step 3 Enable auto analysis.

1) Click **Edit.**
2) (Optional) Check Enable of Display Status and Notify Surveillance Center.
3) Set **Start Time** of video to analyze.
4) Click **OK**.

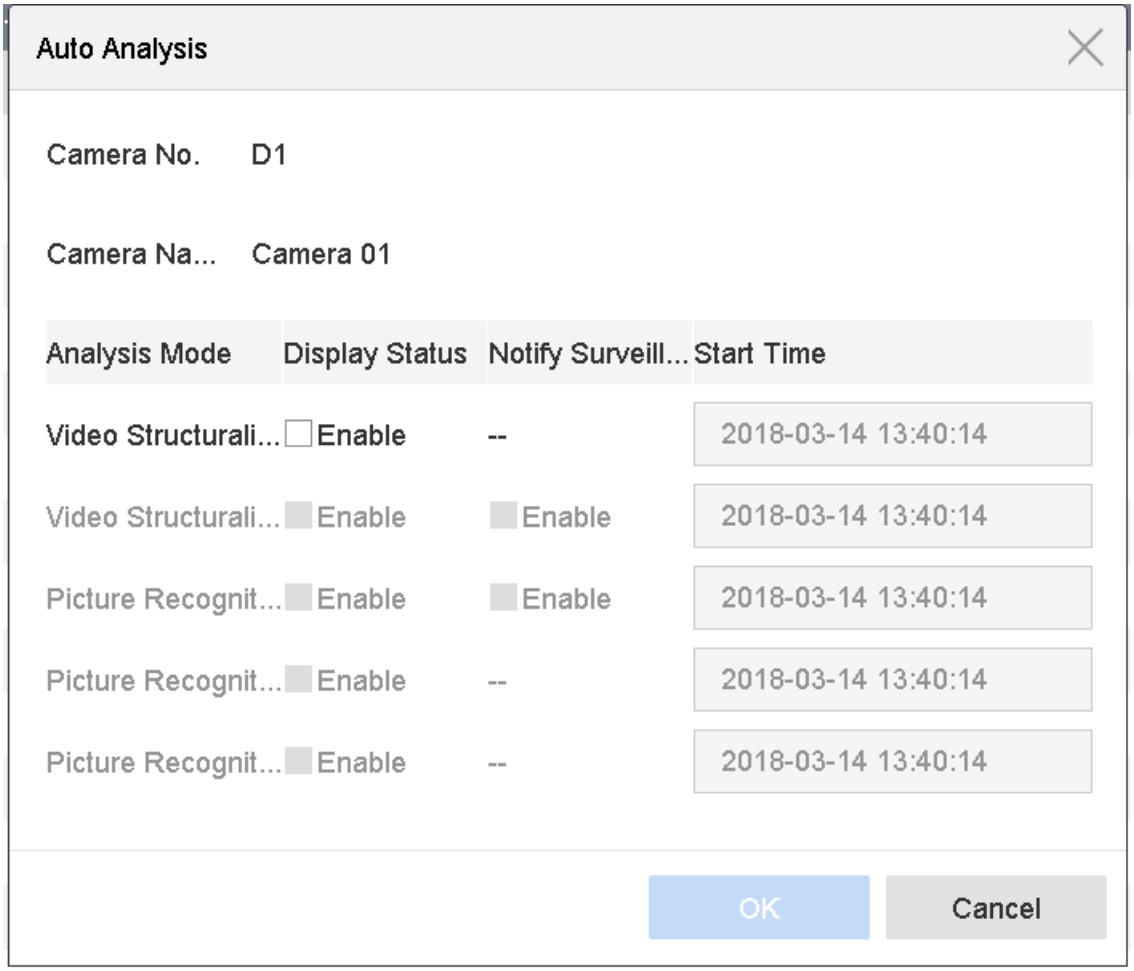


Figure 13-2 Auto Analysis

Step 4 Check cameras and click **Enabled** to start analyzing.

NOTE

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

- **Disabled**: No analysis task is enabled on the camera.
- **Waiting**: The analysis task of the camera is enabled. Device is waiting to analyze data.
- **Enabled**: The analysis task of the camera is enabled and device is analyzing data of the camera.

Step 5 (Optional) For **Non-Real-Time Face Picture Comparison** analysis mode, click **View Record** to view the progress of each day.

13.3 Face Grading Configuration

Purpose:

Face grading is used for face picture selection. According to pupil distance, tilt angle and pan angle, it only uses face pictures which satisfy grading requirement for analysis. Larger pupil distance, smaller tilt and pan angle, better it would be for analysis.

Step 1 Go to **Smart Analysis** > **Smart Analysis** > **Face Grading**.

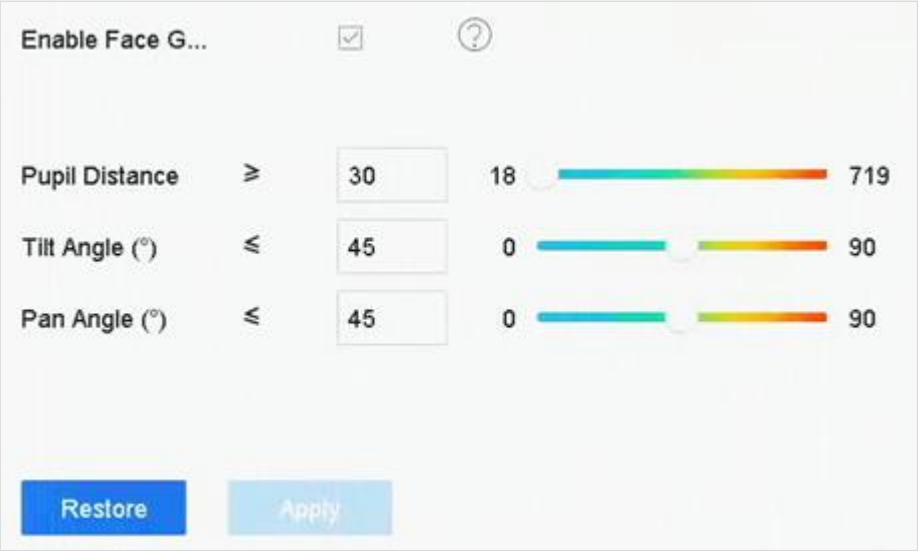


Figure 13-3 Face Grading

Step 2 Check **Enable Face Grading**.

Step 3 Set **Pupil Distance**, **Tilt Angle**, and **Pan Angle**.

- **Pupil Distance:** Pupil distance is the distance between two pupils.
- **Tilt Angle:** Tilt angle is the angle between your view and horizontal plane.
- **Pan Angle:** Pan angle is the angle between your view and vertical plane.

Step 4 Click **Apply**.

13.4 Vehicle Search

Purpose:

You can search and view the matched vehicle pictures.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Vehicle Search**.

Step 2 Select the IP camera for the vehicle search.

Step 3 Set search conditions.

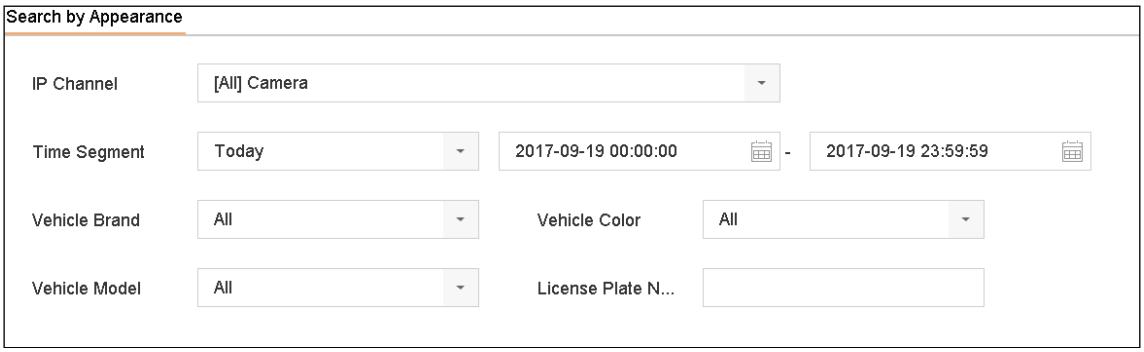


Figure 13-4 Human Body Search

Step 4 Click **Start Search**. The search result list displays 1 channel.

Step 5 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Step 6 (Optional) Export search results.

1) Select result file(s) from the search result interface, or check **Select All** to select all files.
2) Click **Export** to export the selected file(s) to a backup device.

NOTE

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

13.5 People Counting

Purpose:

The feature is used to calculate the number of people entered or left a certain configured area and generate daily/weekly/monthly/annual reports for analysis.

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

Step 2 Select the camera.

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

Step 4 Set the **Date** to generate people counting graphic.

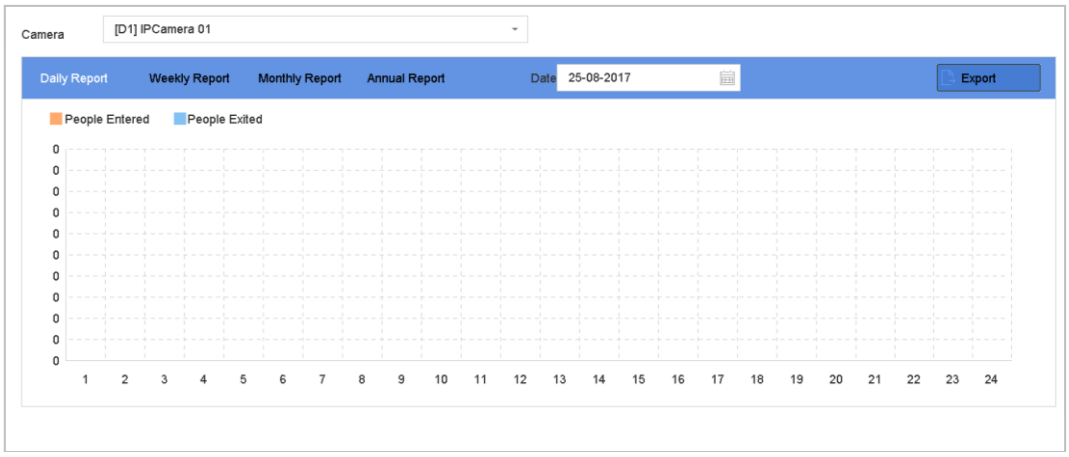


Figure 13-5 People Counting Interface

Step 5 (Optional) Click **Export** to export the report in excel format.

13.6 Heat Map

Purpose:

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

The heat map function must be supported by the connected IP camera and the corresponding configuration must be set.

Step 1 Go to **Smart Analysis** > **Heat Map**.

Step 2 Select a camera.

Step 3 Select the report type as Daily Report, Weekly Report, Monthly Report, or Annual Report.

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

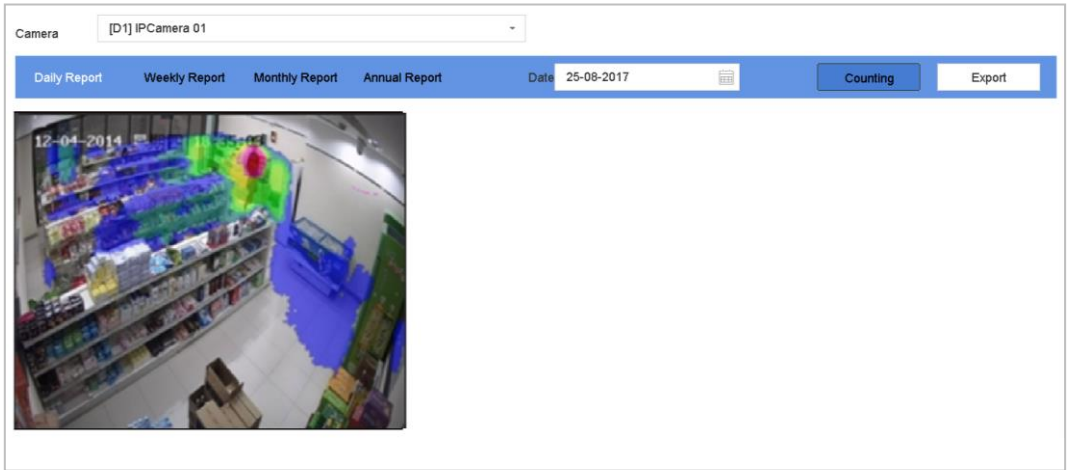


Figure 13-6 Heat Map Interface

Step 5 Click **Counting**. Then the results displayed in graphics marked in different colors will show.

NOTE

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

Step 6 (Optional) Click **Export** to export the statistics report in excel format.

Chapter 14 Human Body Detection

14.1 Human Body Detection

The human body detection enables to detect the human body appearing in the monitoring scene, and capture the human body pictures.

NOTE

This feature is available only when the connected camera supports the human body detection.

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

Step 2 Click **Human Body**.

Step 3 (Optional) For IP camera does not support human body detection, Check **Enable Local Human Body Detection**. Then NVR will consume its decoding resource to execute human body detection. Before enabling the function, go to **Smart Analysis** > **Smart Analysis** > **Engine Configuration** to select at least one engine as **Video Structuralization-Real-Time**.

Step 4 Enabling the function will change smart events supported by the camera.

Step 5 Select the camera to configure the human body detection.

Step 6 Check **Save VCA Picture** to save the captured pictures of human body detection.

Step 7 Check **Target of Interest (Human Body)** to discard non-human body pictures and videos which are not triggered by human body detection. The feature is only available for local human body detection.

Step 8 Set detection area.

1) Select the detection area to configure from the **Area** drop-down list. Up to 8 detection areas are selectable.
2) Check the checkbox of **Enable Area** to enable the selected detection area.
3) Edit the area name in the **Scene Name**. The scene name can contain up to 32 characters.

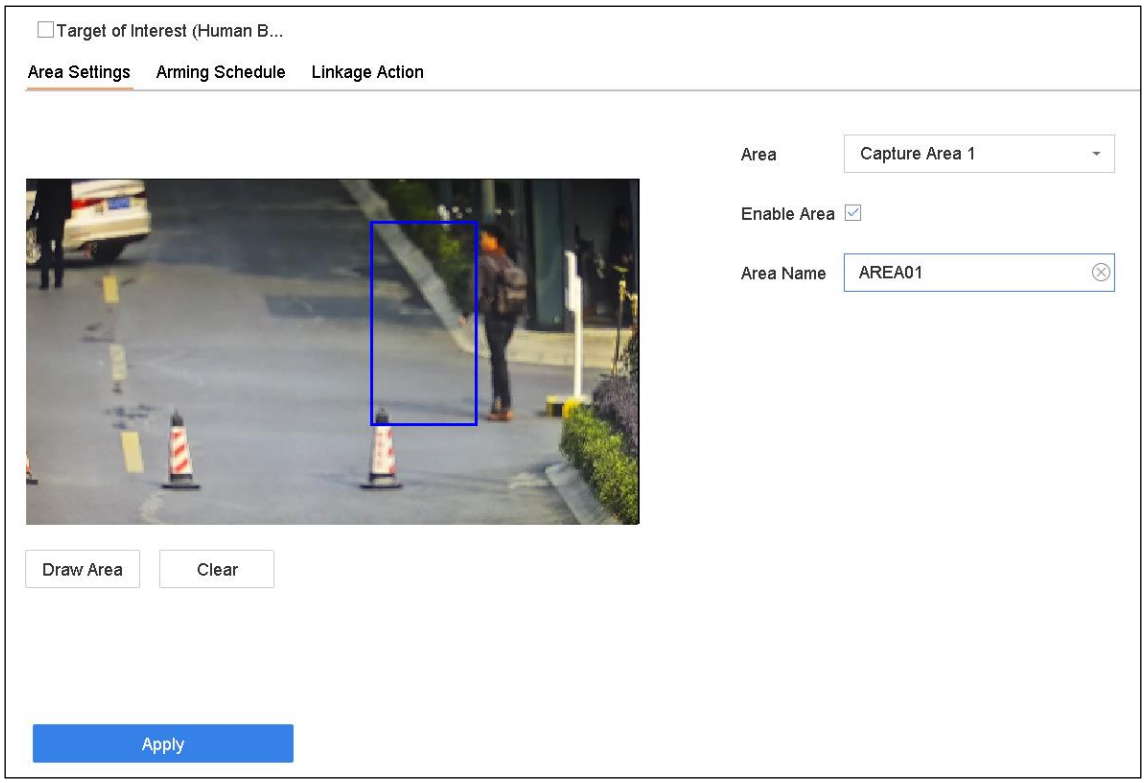


Figure 14-1 Human Body Detection

4) Click **Draw Area** to draw a quadrilateral in the preview window and then click **Stop Drawing**.

Related Operation: You can click **Clear** to clear the existing virtual line and re-draw it.

Step 9 Set the arming schedule. Refer to Chapter 11.1 Configure Arming Schedule.

Step 10 Set the linkage actions. Refer to Chapter 11.2 Configure Alarm Linkage Actions.

Step 11 Click **Apply** to activate the settings.

14.2 Enable Human Body Smart Analysis

Step 1 Go to **Smart Analysis > Smart Analysis > Engine Configuration**. Configure the engine usage of at least one engine as Picture Recognition-Human Body. For details, refer to 13.1 Engine Configuration.

Step 2 Go to **Smart Analysis > Smart Analysis > Task Configuration**. Enable the Picture Recognition-Human Body task for camera the human body detection of which is enabled. For details, refer to 13.2 Task Configuration.

14.3 Human Body Search

14.3.1 Search by Appearance

Purpose

Search human body pictures according to manually specified search conditions.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Human Body Detection** > **Search by Appearance**.

Step 2 Specify search conditions.

Step 3 Click **Start Search**. The search result list displays 1 channel.

Step 4 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Step 5 (Optional) Export search results.

1) Select result file(s) from the search result interface, or check **Select All** to select all files.
2) Click **Export** to export the selected file(s) to a backup device.

NOTE

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

14.3.2 Add Search Result as Sample Picture

Purpose

You can add searched human body pictures as sample pictures. And then search human body pictures by the sample pictures.

Step 1 Search human body pictures.

Step 2 In search result interface, click to select a picture and click **Add to Sample**.

Step 3 Return to search condition settings interface, the selected sample will be listed.

Chapter 15 Face Picture Comparison

The device supports the face picture comparison alarm and face capture for the connected camera based on face recognition feature.

15.1 Face Picture Library Management

You can add the face picture library to the system and upload the face pictures for similarity comparison with the live captured face picture.

15.1.1 Add a Face Picture Library

Step 1 Go to **Smart Analysis** > **Face Picture Database**.

Step 2 Click  .

Step 3 Enter library name and click **OK**.

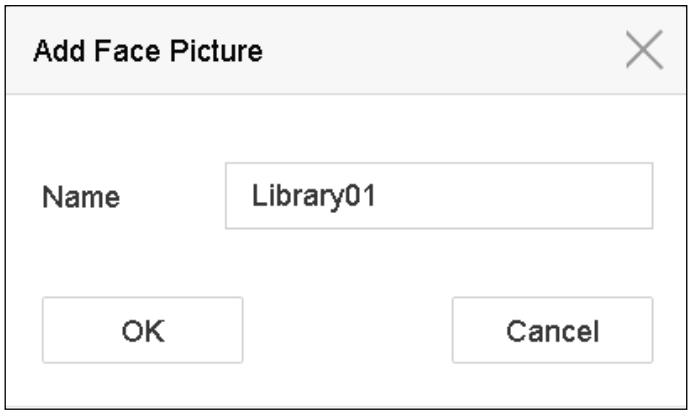


Figure 15-1 Add Face Picture

Related Operation:

You can click  or  to edit the library name or delete the library.

NOTE

Up to 4 face picture libraries can be added.

15.1.2 Upload Face Pictures to the Library

Purpose:

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

- Up to 50,000 pictures can be uploaded to the libraries.
- The picture to upload must be in *.jpeg or .jpg* format.

Before you start:

Import pictures to upload to a backup device.

Upload Single Picture

Step 1 Select a face picture library in the list.

Step 2 Click **Add**.

Step 3 Select the picture to import and click **Import**.

Import Multiple Pictures

Step 1 Select a face picture library in the list.

Step 2 Click **Import Face Picture Library**.

Step 3 On the picture importing interface, select multiple picutures to import and click **Import**.

Related Operations

- Select pictures and click **Copy to** to copy the uploaded pictures of the current library to other library.
- Select a picture and click **Edit** to modify the picture information.
- Select a picture from the list and click **Delete** to delete the picture.
- Select a library and click **Export Face Picture Library** to export library to backup device.
- Click  or  to view by figure or list.

15.1.3 Library for Strangers

All unrecognized face pictures will be added to **Strangers** library. This library cannot be deleted, and will be unavailable for stranger alarm when you select libraries.

The library name uses **Strangers** by default, you can edit the name as your desire. You can edit, delete, search, and export face pictures in this library. Face pictures in this library can be copy to other libraries. After copying face pictures to other libraries, you can delete them as your desire.

This library displays frequently appeared person frequency if you have lined this library with frequently appeared person alarm.

NOTE

Ensure you have enabled frequently appeared person alarm. Refer to *16.1 Frequently Appeared Person Alarm* for details.

15.2 Configure Engine

Go to **Smart Analysis > Smart Analysis > Engine Configuration**. Configure the engine usage of at least one engine as **Facial Recognition**. For details, refer to 13.1 Engine Configuration.

15.3 Face Picture Comparison Alarm

15.3.1 Configure Face Picture Comparison

Purpose:

Compare detected face pictures with specified face picture library. Trigger alarm when comparison succeeded.

Step 1 Go to **System** > **Event** > **Smart Event** > **Face Picture Comparison**.

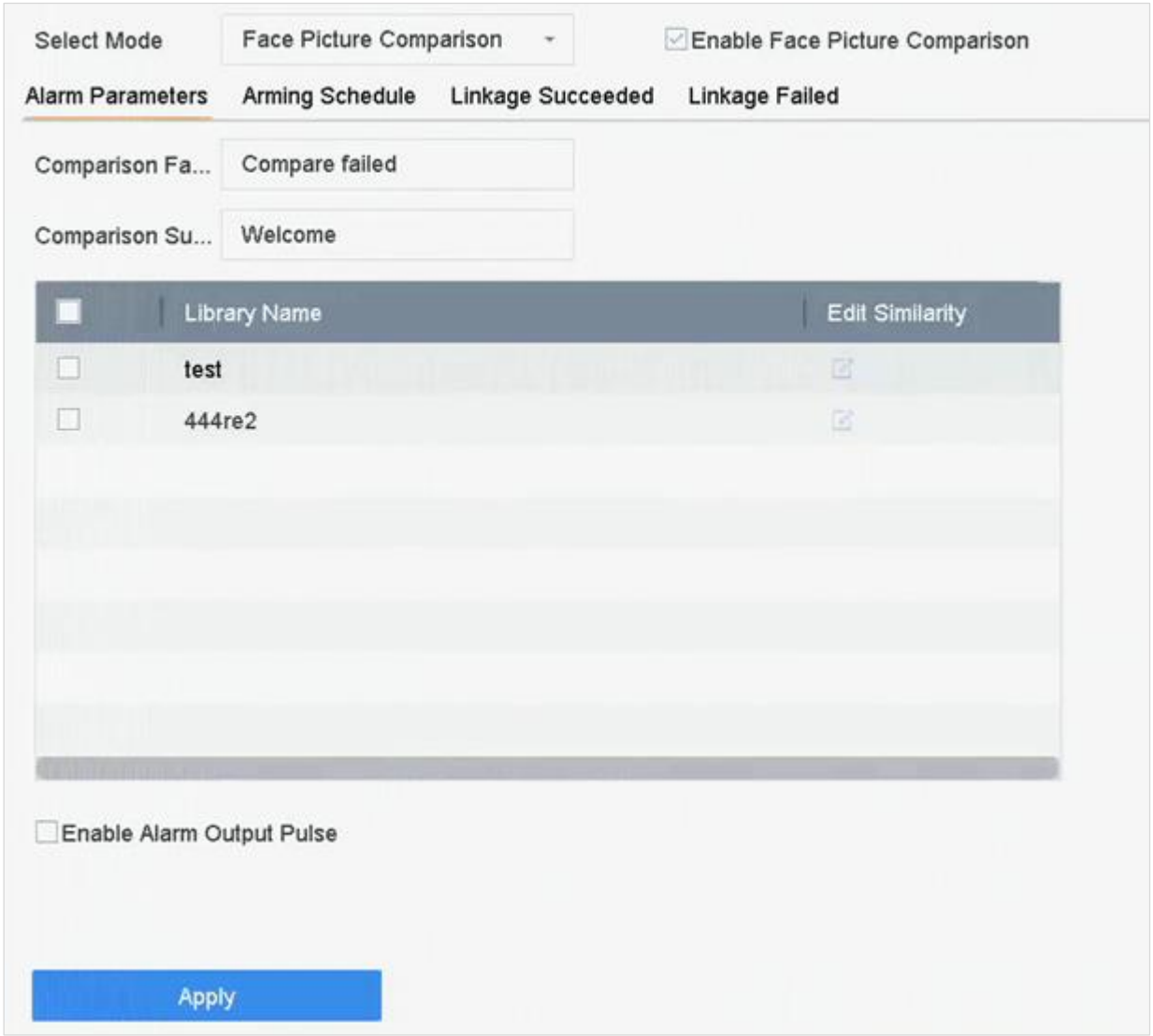


Figure 15-2 Face Picture Comparison

Step 2 Select a camera.

Step 3 Select **Mode** as **Face Picture Comparison**.

Step 4 (Optional) Check **Enable Non-Real-Time Mode**. For places with a high flow of people, the device processing speed may not be fast enough, **Non-Real-Time Mode** will save the real-time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison.

NOTE

- When **Non-Real-Time Mode** is enabled, the linkage method will only support **Notify Surveillance Center**.
- **Non-Real-Time Mode** will not trigger real-time alarm, so **Arming Schedule** is unavailable.
- You can search the comparison results in **File Management** > **All Files** > **Event Type**.

Step 5 Check **Enable Face Picture Comparison**.

Step 6 (Optional) Check **Save VCA Picture** to save the captured pictures of VCA detection**.** After the face picture comparison is enabled, the comparison results will be uploaded for face comparison alarm. If the comparison produced a match, both the real-time face picture and the target picture from the library will be uploaded. If no match is produced, the real-time face picture is uploaded to center only. Up to 6 connected cameras can be configured for face picture comparison simultaneously.

Step 7 (Optional) Set **Comparison Failed Prompt**, **Comparison Succeeded Prompt**, and **Enable Alarm Output Pulse**.

- **Comparison Failed Prompt**: It will display the prompt in live view **Target Detection** (with **Facial Detection** checked) or **Facial Recognition** when face picture comparison failed. You can click  in live view to enter Facial Recognition interface.
- **Comparison Succeeded Prompt:** It will display the prompt in **Facial Recognition** when face picture comparison succeeded. You can click  in live view to enter Facial Recognition interface.
- **Enable Alarm Output Pulse:** It is usually linked with a gate. When a person is passing a gate, if the comparison succeeded, it will trigger a pulse to open the gate. The pulse is between 100 to 900 ms. You can set **Alarm Output Pulse (ms)** in **System** > **Event** > **Normal Event** > **Alarm Output**.

Step 8 Select face picture libraries and set similarity.

Step 9 Set the arming schedule. Refer to *11.1 Configure Arming Schedule*.

Step 10 Set the linkage actions when face picture comparison succeeded or failed. Refer to *11.2 Configure Alarm Linkage Actions*.

Step 11 (Optional) Configure face grading parameters. Refer to *13.3 Face Grading Configuration* for details.

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

15.3.2 Configure Stranger Alarm

Purpose:

Compare detected face pictures with specified face picture library. Trigger alarm when comparison failed.

Step 1 Go to **System** > **Event** > **Smart Event** > **Face Picture Comparison**.

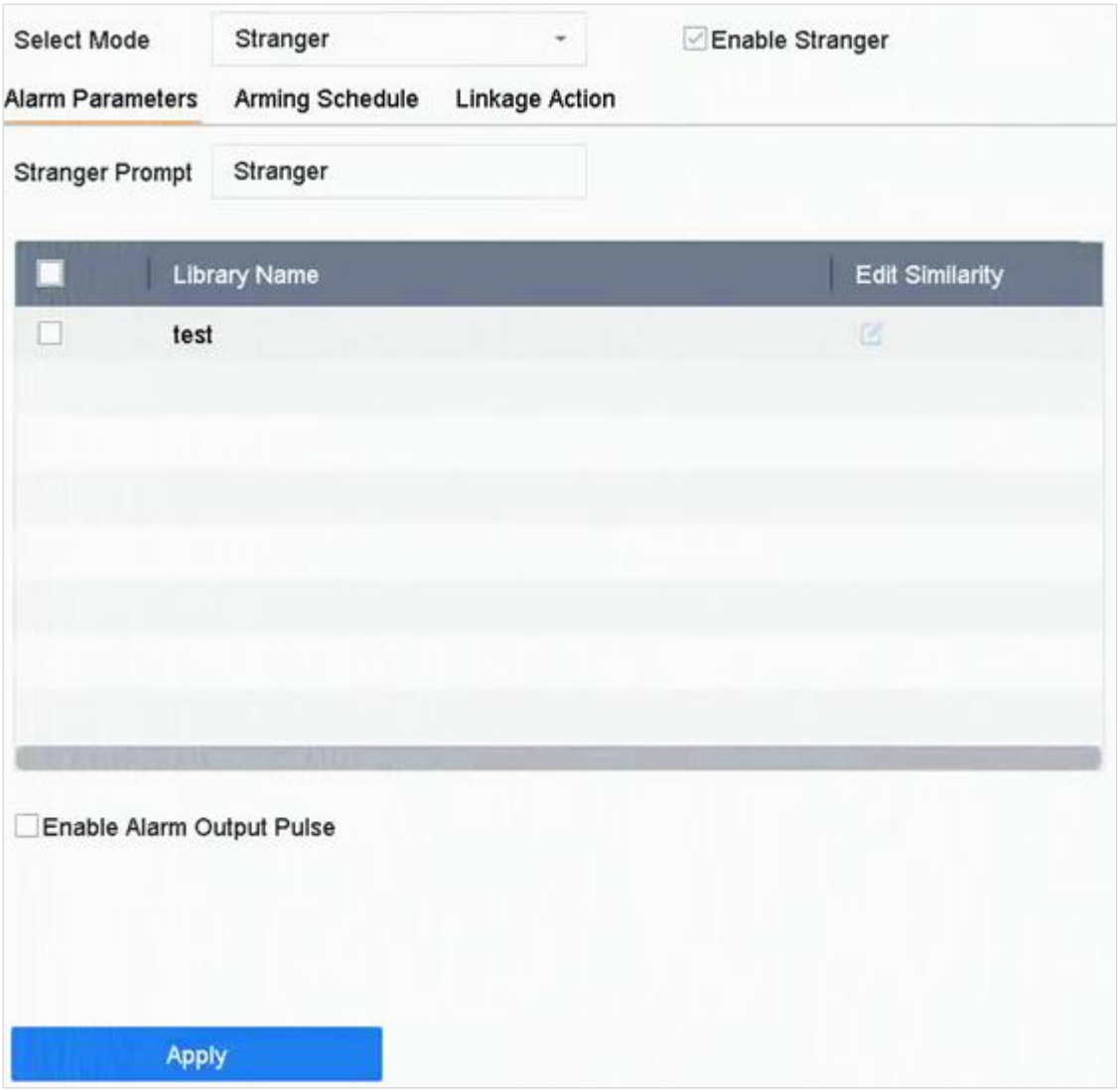


Figure 15-3 Face Picture Comparison

Step 2 Select a camera.

Step 3 Select **Mode** as **Stranger**.

Step 4 (Optional) Check **Enable Non-Real-Time Mode**. For places with a high flow of people, the device processing speed may not be fast enough, **Non-Real-Time Mode** will save the real-

time pictures as cache, and process them later when engine has free resource. After enabling this function, all channels will be able to support face picture comparison.

NOTE

- When **Non-Real-Time Mode** is enabled, the linkage method will only support **Notify Surveillance Center**.
- **Non-Real-Time Mode** will not trigger real-time alarm, so **Arming Schedule** is unavailable.
- You can search the comparison results in **File Management** > **All Files** > **Event Type**.

Step 5 Check **Enable Stranger**.

Step 6 (Optional) Check **Save VCA Picture** to save the captured pictures of VCA detection. After the face picture comparison is enabled, the comparison results will be uploaded for face comparison alarm. If the comparison produced a match, both the real-time face picture and the target picture from the library will be uploaded. If no match is produced, the real-time face picture is uploaded to center only.

Step 7 (Optional) Set **Stranger Prompt**. It will display the prompt in live view **Target Detection** (Facial Detection) when comparison failed.

- **Stranger Prompt**: It will display the prompt in live view **Target Detection** (with **Facial Detection** checked) when face picture comparison failed.
- **Enable Alarm Output Pulse:** It is usually linked with a gate. When a person is passing a gate, if the comparison succeeded, it will trigger a pulse to open the gate. The pulse is between 100 to 900 ms. You can set **Alarm Output Pulse (ms)** in **System** > **Event** > **Normal Event** > **Alarm Output**.

Step 8 Select face picture libraries and set similarity.

Step 9 Set the arming schedule. Refer to *11.1 Configure Arming Schedule*.

Step 10 Set the linkage actions. Refer to *11.2 Configure Alarm Linkage Actions*.

Step 11 (Optional) Configure face grading parameters. Refer to *13.3 Face Grading Configuration* for details.

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

15.4 Face Picture Search

15.4.1 Search by Face Picture Comparison Event

Purpose:

Search face picture by face picture comparison results.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Face Search** > **Search by Event**.

Step 2 Set the start time and end time.

Step 3 Select a channel.

Step 4 Select **Event Type** as **Face Picture Comparison**.

Step 5 Click **Start Search**. The search result list displays 1 channel.

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

Related Operation:

- Double click a file to view the related video.
- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to *15.4.2 Search by Uploaded Picture*.
- Click **Export** to export the selected file(s) to a backup device. You can **Select All** to select all files.

NOTE

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

15.4.2 Search by Uploaded Picture

Purpose:

You can search the face pictures by uploaded picture.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Face Search** > **Search by Picture**.

Step 2 Select a channel.

Step 3 Click **Upload Sample from Local** and select face pictures from your local directory for search.

Or you can click **Upload Sample from Face Picture Database** and select face pictures from created face picture libraries.

Step 4 Set the start time and end time.

Step 5 Set the **Similarity** value (range: 0 to 100). Device will analyze the similarity between samples and face pictures in library and show pictures the similarity of which are higher than the set one.

Step 6 Click **Start Search**. The search result list displays 1 channel.

Step 7 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Related Operation:

- Double click a file to view the related video.

- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures.
- Click **Export** to export the selected file(s) to a backup device. You can **Select All** to select all files.

NOTE

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

15.4.3 Search by Personal Name

Purpose:

Search face picture by personal name.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Face Search** > **Search by Name**.

Step 2 Set the start time and end time of the face pictures to search.

Step 3 Select a channel.

Step 4 Enter a name.

Step 5 Click **Start Search**. The search result list displays 1 channel.

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

Related Operation:

- Double click a file to view the related video.
- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to *15.4.2 Search by Uploaded Picture*.
- Click **Export** to export the selected file(s) to a backup device. You can **Select All** to select all files.

NOTE

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

15.4.4 Search by Appearance

Purpose

Search face picture by appearance.

Step 1 Go to **Smart Analysis** > **Smart Search** > **Face Search** > **Search by Appearance**.

Step 2 Set search conditions.

Step 3 Click **Start Search**. The search result list displays 1 channel.

Step 4 Click **Channel** to select a channel as your desire. It will display search results for the selected channel.

Related Operation:

- Double click a file to view the related video.
- Click **Add to Face Database** to add the selected file(s) to a face picture library.
- Click **Add to Sample** to add the select file(s) as sample picture(s). You can use the sample picture(s) to search other pictures. Refer to *15.4.2 Search by Uploaded Picture*.
- Click **Export** to export the selected file(s) to a backup device. You can **Select All** to select all files.

NOTE

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

Chapter 16 People Frequency Alarm

You can only configure people frequency alarm via web browser.

16.1 Frequently Appeared Person Alarm

Purpose

It will trigger alarm when a person has appeared at a high frequency.

Step 1 Go to **Configuration** > **Event** > **People Frequency** > **Frequently Appeared Person**.

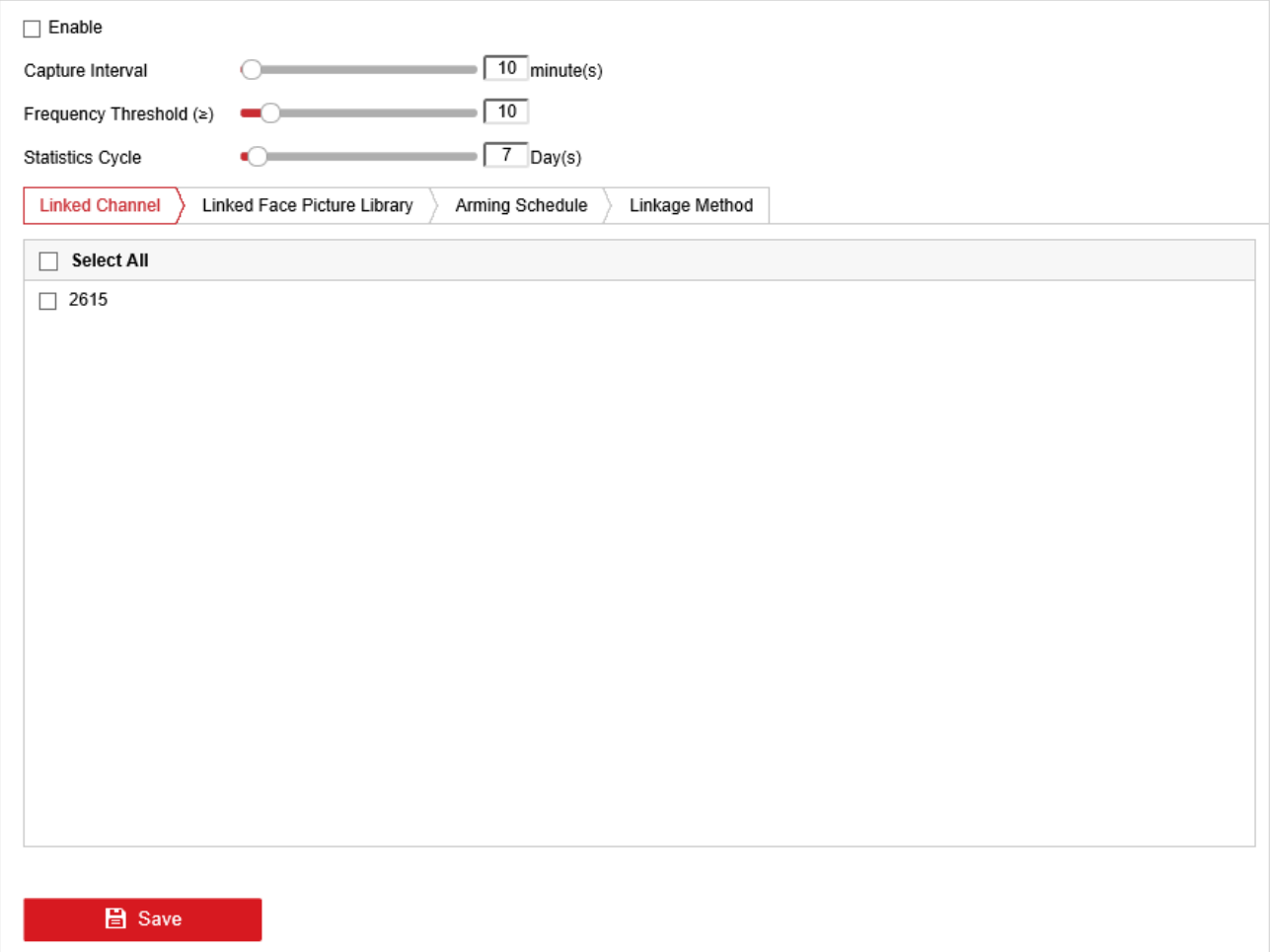


Figure 16-1 Frequently Appeared Person

Step 2 Check **Enable**.

Step 3 Set **Capture Interval**, **Frequency Threshold**, and **Statistics Cycle**.

- **Capture Interval:** When a person has appeared several times within the capture interval, it only counts 1 time for this person.
- **Frequency Threshold:** It will trigger alarm when the frequency has exceeded the threshold.

- **Statistics Cycle:** Time period for counting the people frequency. For example, if the statistics cycle is 7 days, device will count people frequency in the last 7 days, if a person has exceeded the frequency threshold in the last 7 days, it will trigger alarm.

Step 4 Select channel in **Linked Channel**.

Step 5 Select face picture library in **Linked Face Picture Library**.

Step 6 Set similarity for the selected library.

Step 7 Set strategy as **Filter** or **Alarm**.

- **Filter**: If the face picture similarity has exceeded the value, the face picture is considered as an existing member in the library, which will not trigger alarm.
- **Alarm**: It will trigger alarm when the face picture similarity and frequency has exceeded the threshold.

NOTE

All unrecognized face pictures will be added to **Strangers** library, so that strangers can also trigger the frequently appeared person alarm, and they use the similarity of **Strangers** library.

Step 8 Set the arming schedule. Refer to *11.1 Configure Arming Schedule*.

Step 9 Set the linkage method. Refer to *11.2 Configure Alarm Linkage Actions*.

Step 10 Click **Save**.

16.2 Low Frequency Person Alarm

Purpose

It will trigger alarm when a person has appeared at a low frequency.

Step 1 Go to **Configuration** > **Event** > **People Frequency** > **Low Frequency Person**.

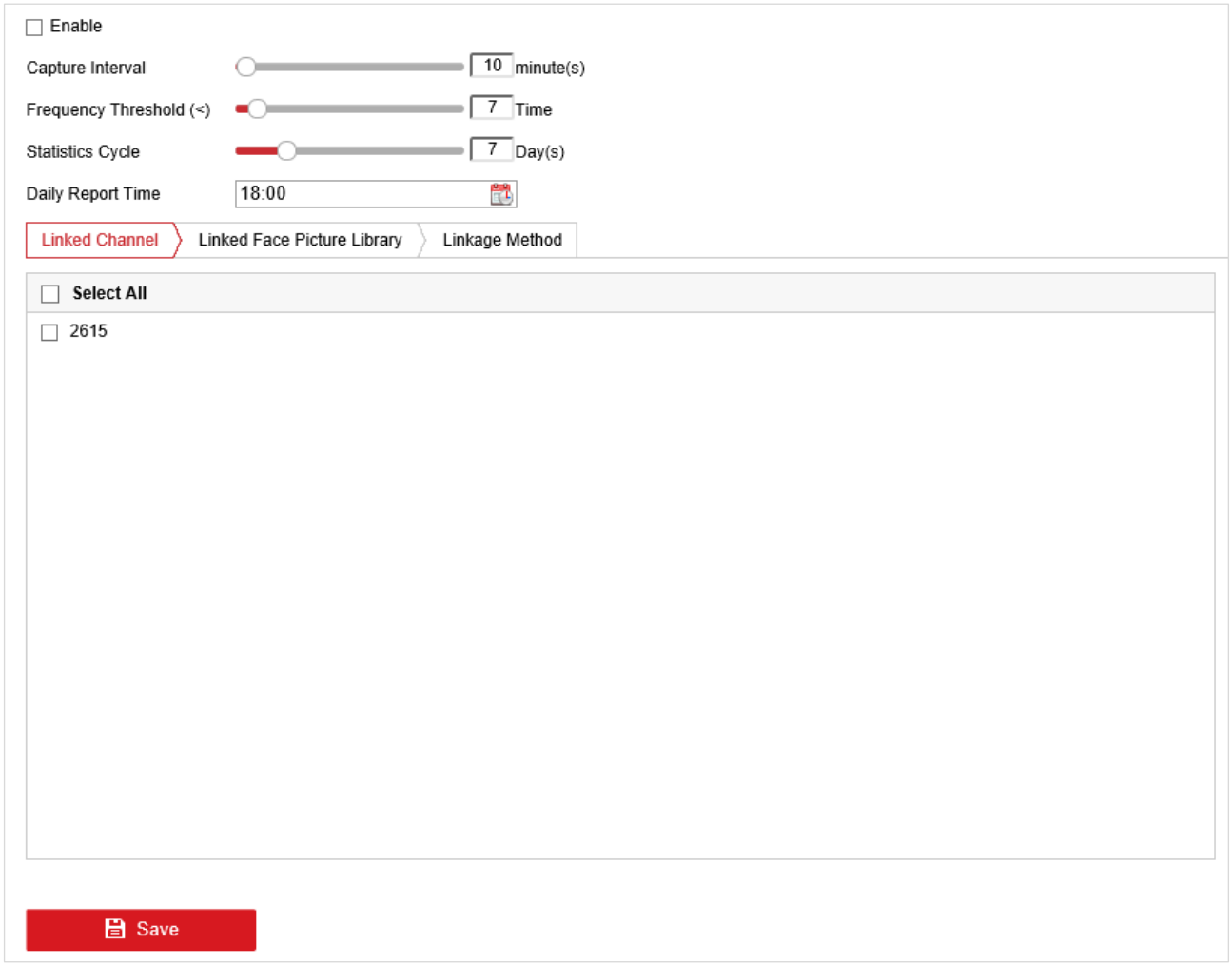


Figure 16-2 Low Frequency Person

Step 2 Check **Enable**.

Step 3 Set **Capture Interval**, **Frequency Threshold**, **Statistics Cycle**, and **Daily Report Time**.

- **Capture Interval:** When a person has appeared several times within the capture interval, it only counts 1 time for this person.
- **Frequency Threshold:** It will trigger alarm when the frequency has exceeded the threshold.
- **Statistics Cycle:** Time period for counting the people frequency. For example, if the statistics cycle is 7 days, device will count people frequency in the last 7 days, if a person has not exceeded the frequency threshold in the last 7 days, it will trigger alarm.
- **Daily Report Time:** Daily report low frequency person statistics at the predefined time.

Step 4 Select channel in **Linked Channel**.

Step 5 Select face picture library in **Linked Face Picture Library**.

Step 6 Set similarity for the selected library.

Step 7 Set the linkage method. Refer to *11.2 Configure Alarm Linkage Actions*.

Step 8 Click **Save**.

Chapter 17 Network Settings

17.1 Configure TCP/IP Settings

Purpose

TCP/IP settings must be properly configured before you can operate the device over network.

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

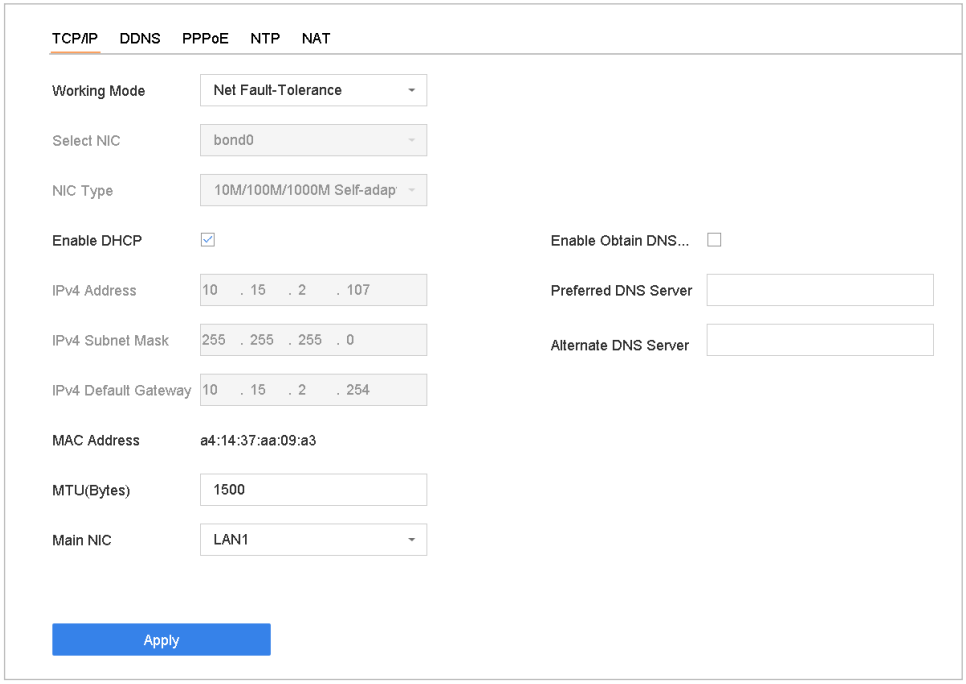


Figure 17-1 TCP/IP Settings

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. By this way, in case of one NIC card failure, the device will automatically enable the other standby NIC card so as to ensure the normal running of the whole 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. You can select one NIC card as default route. And then the system is connecting with the extranet the data will be forwarded through the default route.

Step 3 Configure other IP settings as needed.

NOTE

Check **Enable DHCP** to obtain IP settings automatically if a DHCP server is available in the network.

Valid range of MTU value is 500 to 9676.

Step 4 Click **Apply**.

17.2 Configure DDNS

Purpose

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

Before You Start

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

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

Step 2 Check **Enable**.

Step 3 Select **DynDNS** under **DDNS Type**.

NOTE

PeanutHull and NO-IP are also available under DDNS Type, and required information should be entered accordingly.

Step 4 Enter **Server Address** for **DynDNS** (i.e. members.dyndns.org).

Step 5 Under **Device Domain Name**, enter the domain name obtained from the DynDNS website.

Step 6 Enter the **User Name** and **Password** registered in the DynDNS website.

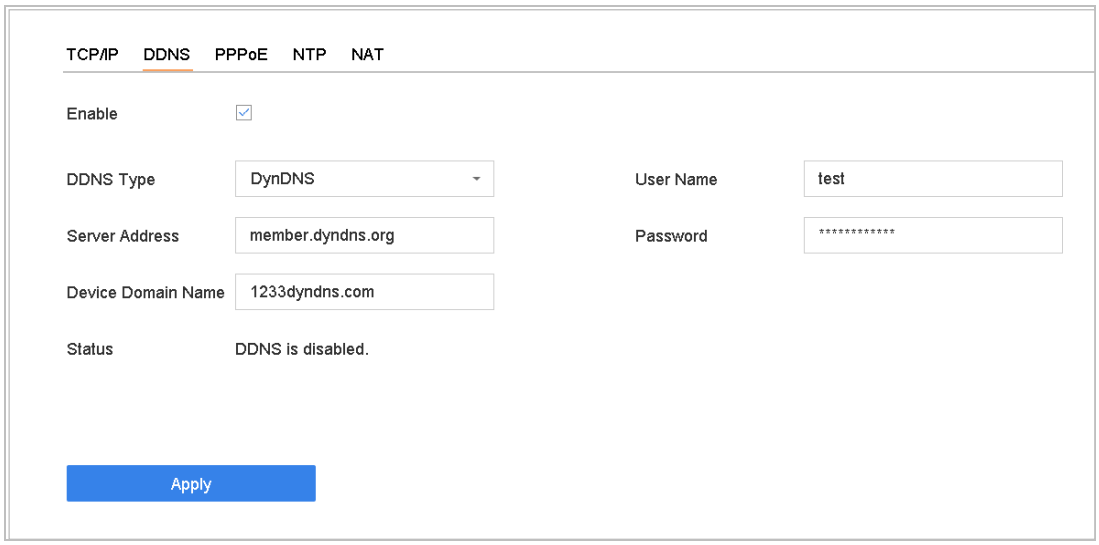


Figure 17-2 DDNS Settings

Step 7 Click **Apply**.

17.3 Configure PPPoE

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

NOTE

Contact your Internet service provider for details about PPPoE service.

17.4 Configure NTP

Purpose

Connection to a network time protocol (NTP) server can be configured on your device to ensure the accuracy of system date and time.

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

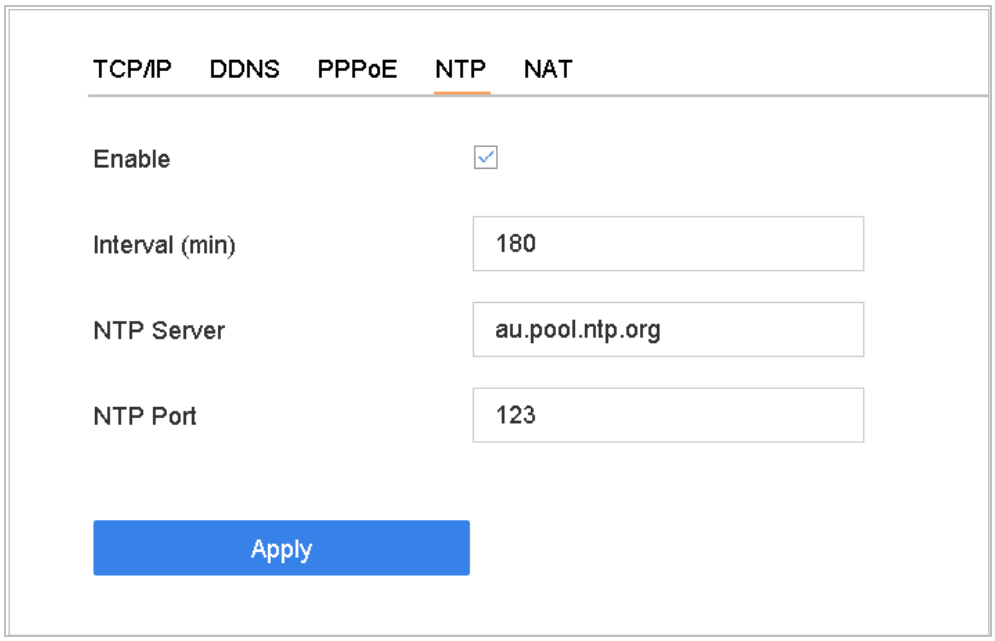


Figure 17-3 NTP Settings

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**.

17.5 Configure NAT

Purpose:

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

- **UPnP™**

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

Before you start:

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

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

Figure 17-4 UPnP™ Settings Interface

Step 2 Check **Enable UPnP**.

Step 3 Select Mapping Type as Manual or Auto.

OPTION 1: Auto

If you select **Auto**, the port mapping items are read-only, and the external ports are set by the router automatically.

NOTE

You can click **Refresh** to get the latest status of the port mapping.

OPTION 2: Manual

If you select **Manual**, you can edit the external port on your demand by clicking to activate **External Port Settings**.

NOTE

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

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

NOTE

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

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

Figure 17-5 Setting Virtual Server Item

17.6 Configure SNMP

Purpose

You can configure SNMP settings to get device status and parameter information.

Before You Start

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

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

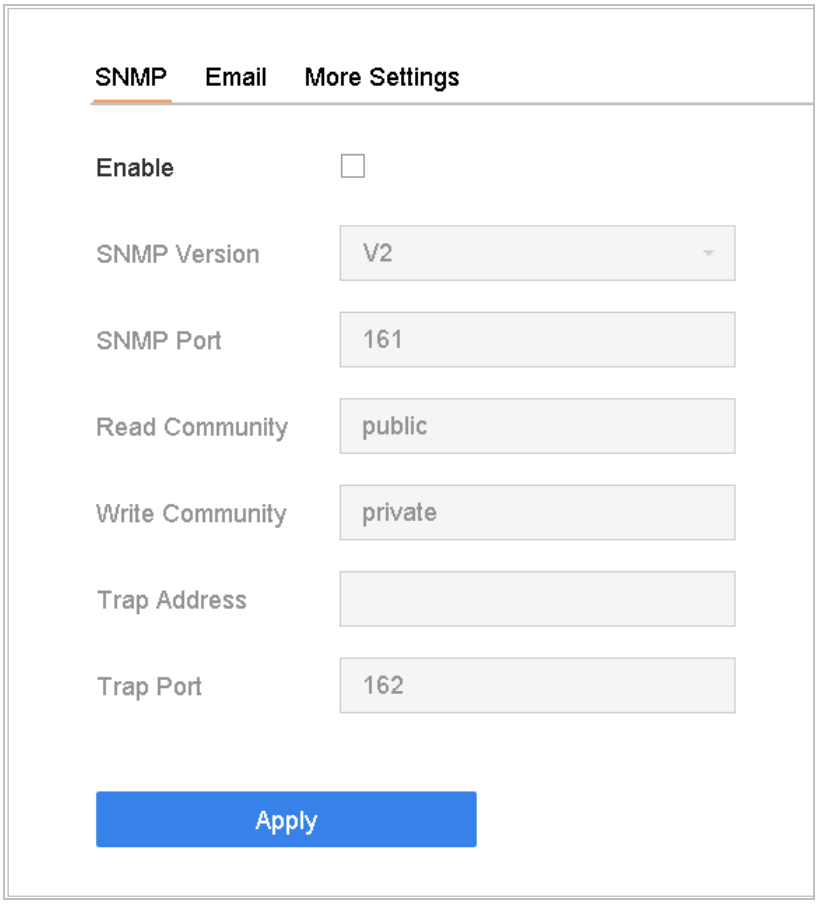


Figure 17-6 SNMP Settings

Step 2 Check **Enable**. A message will pop up to prompt possible security risk and click **Yes** to continue.

Step 3 Configure the SNMP settings as needed.

- **Trap Address**: IP address of the SNMP host.
- **Trap Port**: Port of the SNMP host.

Step 4 Click **Apply**.

17.7 Configure Email

Purpose

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

Before You Start

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

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

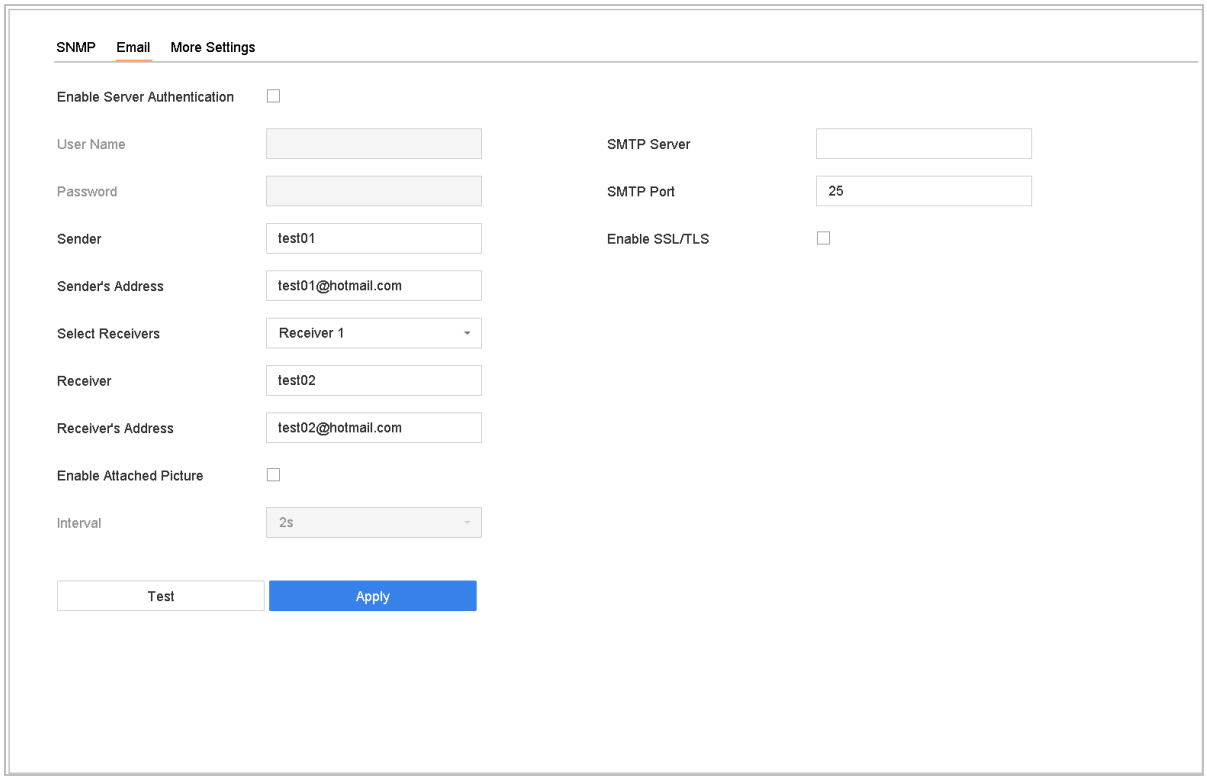


Figure 17-7 Email Settings

Step 2 Configure the following Email settings.

- **Enable Server Authentication**: Check to enable the function if the SMTP server requires user authentication and enter user name and password accordingly.
- **SMTP Server**: The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
- **SMTP Port**: The SMTP port. The default TCP/IP port used for SMTP is 25.
- **Enable SSL/TLS**: Check to enable SSL/TLS if required by the SMTP server.
- **Sender**: The name of the sender.
- **Sender's Address**: Sender's Address.
- **Select Receivers**: Select the receiver. Up to 3 receivers can be configured.
- **Receiver**: The name of the receiver.
- **Receiver's Address**: The Email address of user to be notified.
- **Enable Attached Picture**: Check to enable the function if you want to send email with attached alarm images. The interval is the time between two adjacent alarm images.

Step 3 Click **Apply**.

Step 4 (Optional) Click **Test** to send a test email.

17.8 Configure Hik-Connect

Purpose

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

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

Step 2 Check **Enable** to activate the function. Then the service terms will pop up.

1) Enter the verification code in **Verification Code**.
2) Scan the QR code to read the service terms and privacy statement.
3) Check The Hik-Connect service will require internet access. Please read Service Terms and Privacy Statement before enabling the service if you agree the service terms and privacy statement.
4) Click **OK** to save the settings.

NOTE

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

Step 3 (Optional) Check **Custom** to enter the server address as your desire.

Step 4 (Optional) Check **Enable Stream Encryption**, verification code is required for remote access and live view.

Step 5 Click **Apply**.

What to do next:

After configuration, you can access and manage your devices through Hik-Connect app or website.

17.9 Configure Ports

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

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

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

  The **Alarm Host IP** refers to the IP address of the remote PC on which the CMS software (e.g., 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 the IP address ranging from 239.252.0.0 to 239.255.255.255.

  When adding a device to the CMS software, the multicast address must be the same as that of the device.
- **RTSP Port**: RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers. The port is 554 by default.

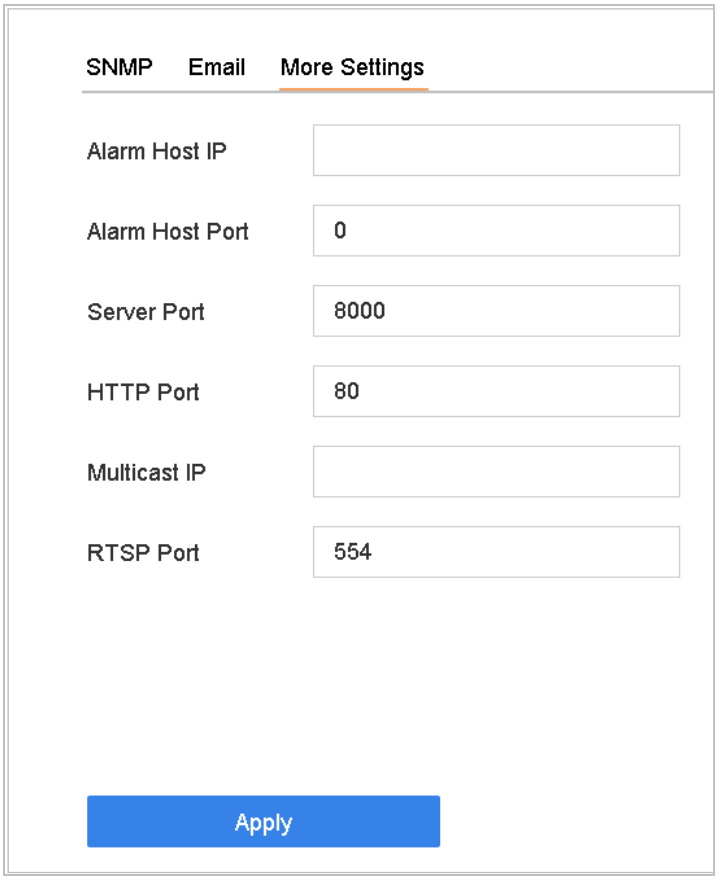


Figure 17-8 Port Settings

Chapter 18 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. Please contact dealer for details of models which 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.

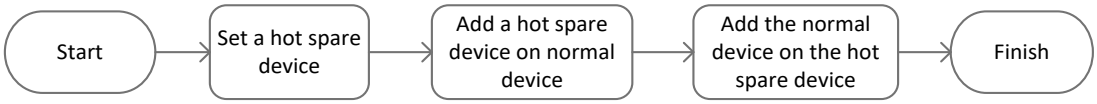


Figure 18-1 Building Hot Spare System

Before you start:

At least 2 devices are online.

18.2 Set Hot Spare Device

Purpose:

Hot spare devices takes over working device tasks when working device fails.

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

Step 2 Set the Work Mode as Hot Spare Mode.

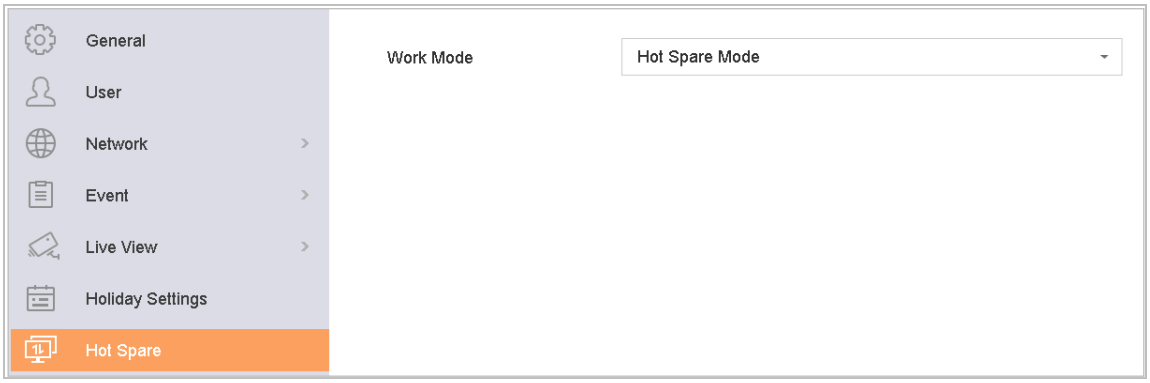


Figure 18-2 Hot Spare

Step 3 Click **Apply**.

Step 4 Click **Yes** in popup attention box to reboot the device.

NOTE

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

18.3 Set Working Device

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

Step 2 Set the Work Mode as Normal Mode.

Step 3 Check **Enable**.

Step 4 Enter the IP address and admin password of hot spare device.

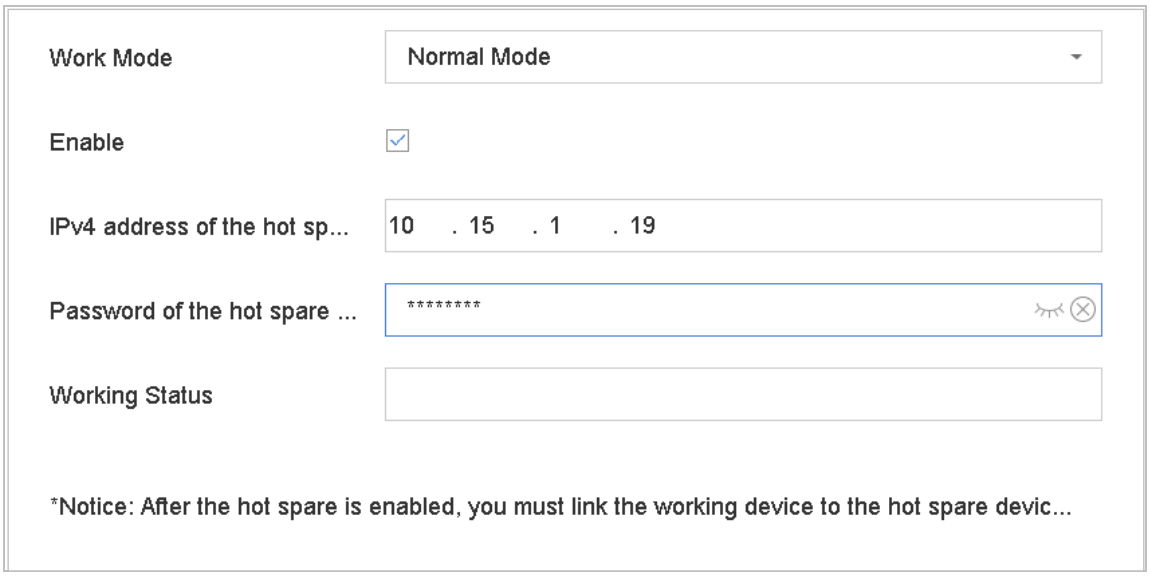


Figure 18-3 Hot Spare

Step 5 Click **Apply**.

18.4 Manage Hot Spare System

Step 1 Go to **System > Hot Spare** in hot spare device.

Step 2 Check working devices from 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.

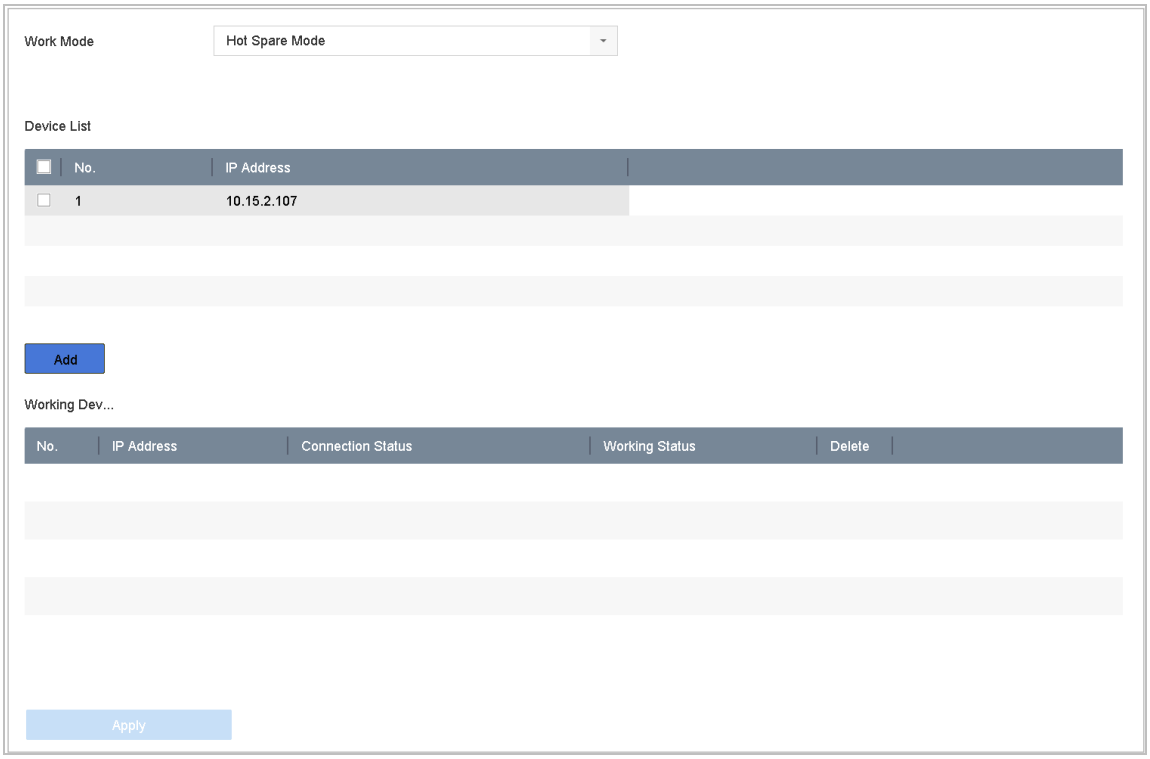


Figure 18-4 Add Working Device

Table 18-1 Working Status Descrption

Working Status	Description
No record	The working device works properly.
Backing up	The working device gets offline, the hot spare device will record the video of the IP camera connected to the working device for backup The record backing up can be functioned for 1 working device at a time.
Synchronizing	The working device comes online, the lost video files will be restored by the record synchronization function. The record synchronization function can be enabled for 1 working device at a time.

Chapter 19 System Maintenance

19.1 Storage Device Maintenance

19.1.1 Configure Disk Clone

Purpose:

Select the HDDs to clone to eSATA HDD.

Before you start:

Connect an eSATA disk to the device.

Step 1 Go to **Maintenance** > **HDD Operation** > **HDD Clone**.

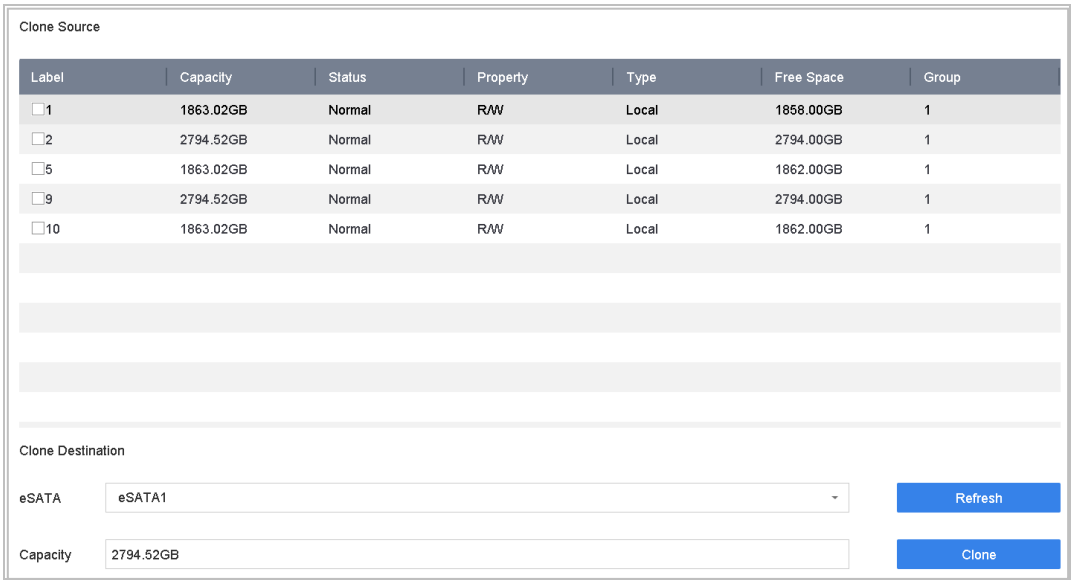


Figure 19-1 HDD Clone

Step 2 Check the HDD to clone. The capacity of selected HDD must match the capacity of clone destination.

Step 3 Click **Clone**.

Step 4 Click **Yes** on popup message box to continue clone.

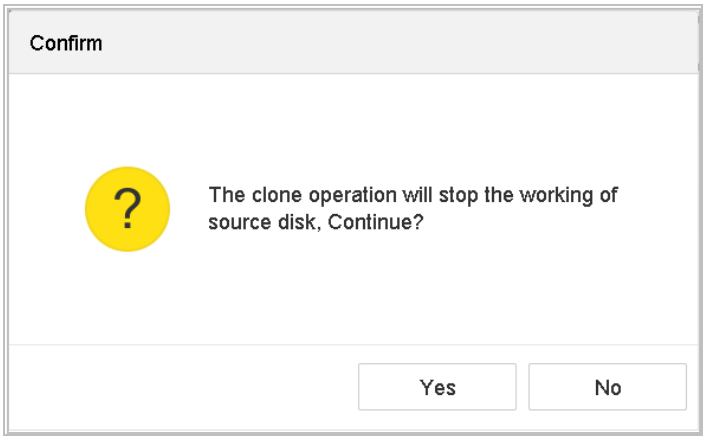


Figure 19-2 Message Box

19.1.2 S.M.A.R.T Detection

Purpose:

The device provides the HDD detection function such as the adopting of the S.M.A.R.T. and the Bad Sector Detection technique. The S.M.A.R.T. *(*Self-Monitoring, Analysis and Reporting Technology*)* is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

Step 1 Go to **Maintenance** > **HDD Operation** > **S.M.A.R.T.**.

Step 2 Select the HDD to view its S.M.A.R.T information list.

Step 3 Select the self-test types as **Short Test**, **Expanded Test** or the **Conveyance Test**.

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

Step 5 The related information of the S.M.A.R.T. is shown on the interface. You can check the HDD status.

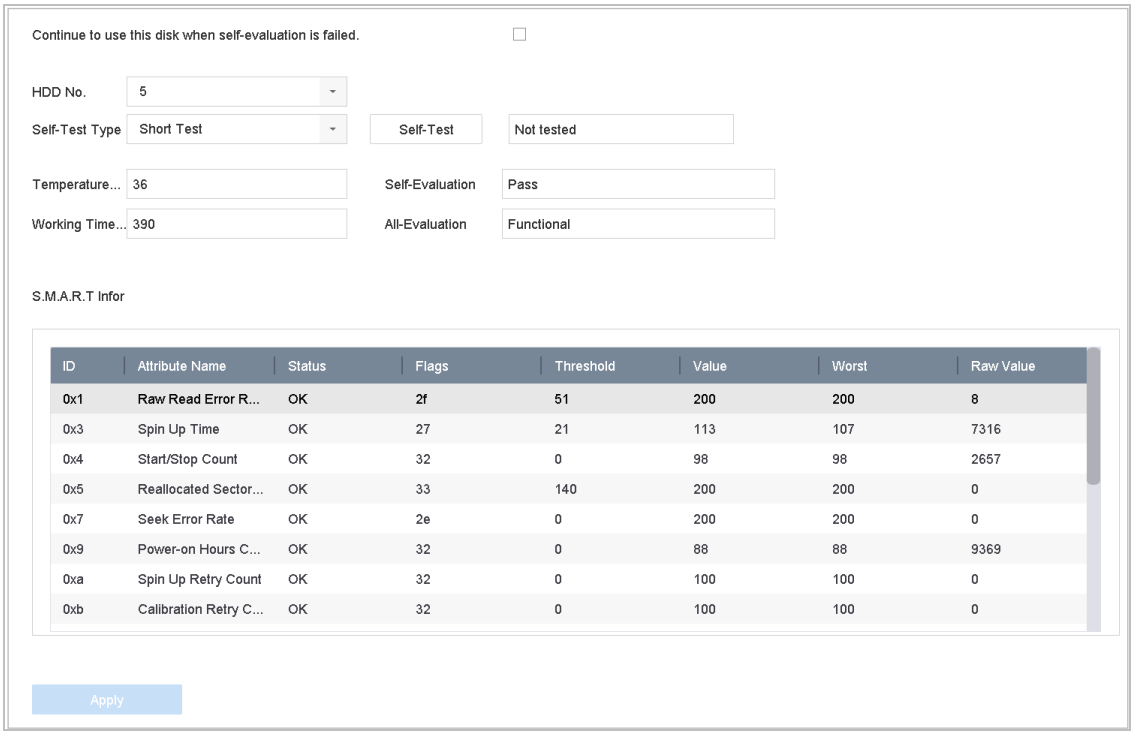


Figure 19-3 S.M.A.R.T Settings Interface

NOTE

If you want to use the HDD even when the S.M.A.R.T. checking is failed, you can check the checkbox of the **Continue to use the disk when self-evaluation is failed** item.

19.1.3 Bad Sector Detection

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

Step 2 Select the HDD No. in the dropdown list you want to configure.

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

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

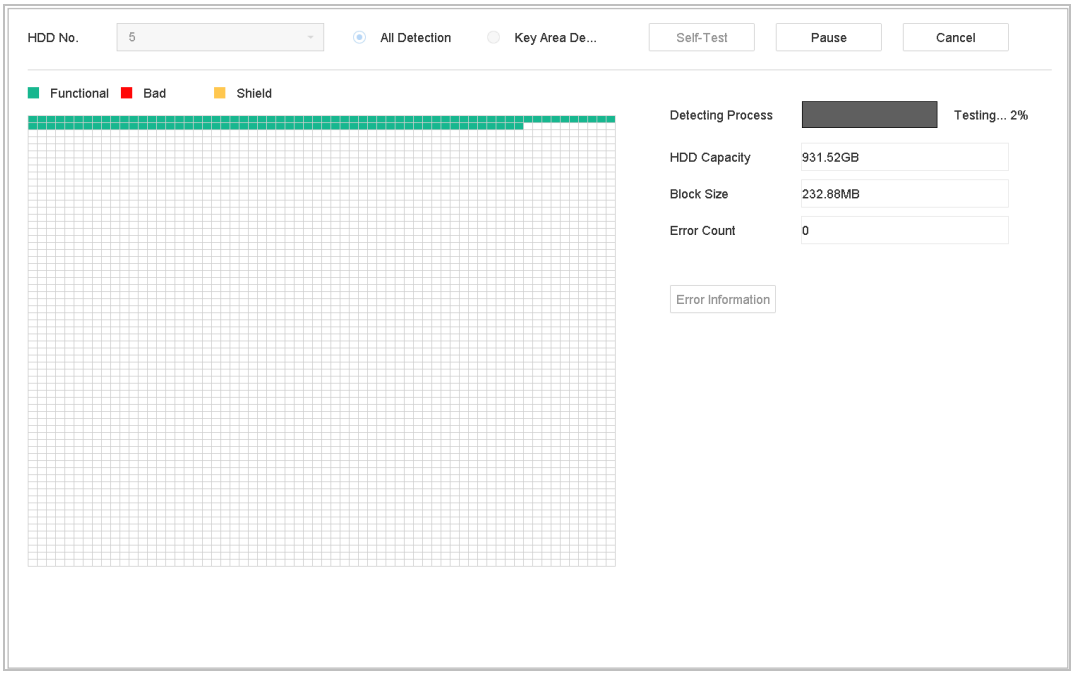


Figure 19-4 Bad Sector Detection

You can also pause/resume or cancel the detection.

After testing completed, you can click **Error information** button to see the detailed damage information.

19.1.4 HDD Health Detection

Purpose:

You can view the health status of Seagate HDD that generated after October 1th, 2017 and capacity ranges from 4 TB to 8 TB. The function helps you to troubleshoot HDD problems. Compared with S.M.A.R.T function, health detection shows HDD status with more details.

Step 1 Go to **Maintenance** > **HDD Operation** > **Health Detection**.

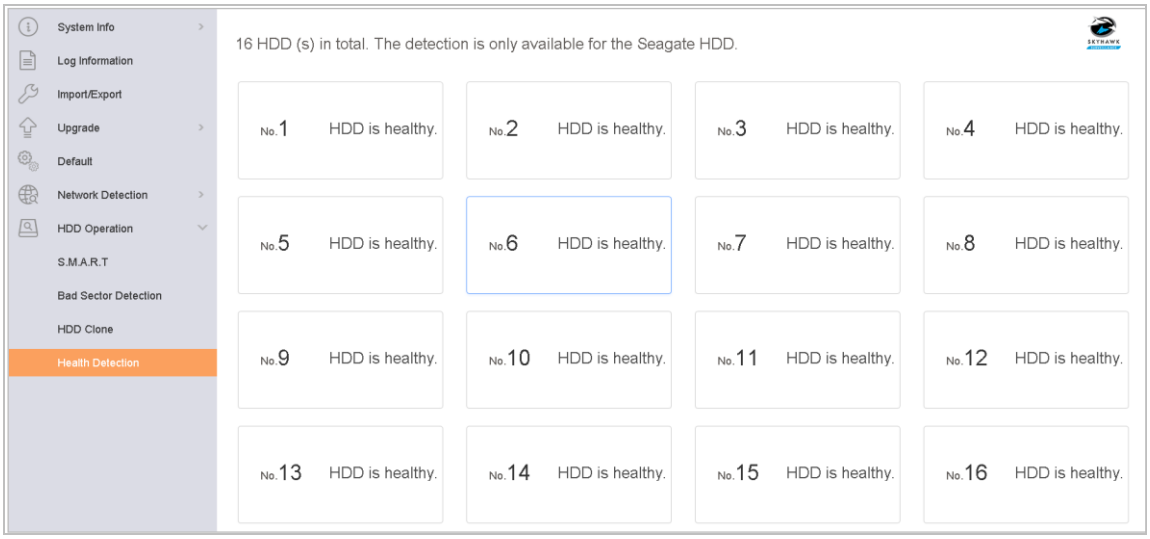


Figure 19-5 Health Detection

Step 2 Click a HDD to view details.

19.2 Search & Export Log Files

Purpose:

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

19.2.1 Search the Log Files

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

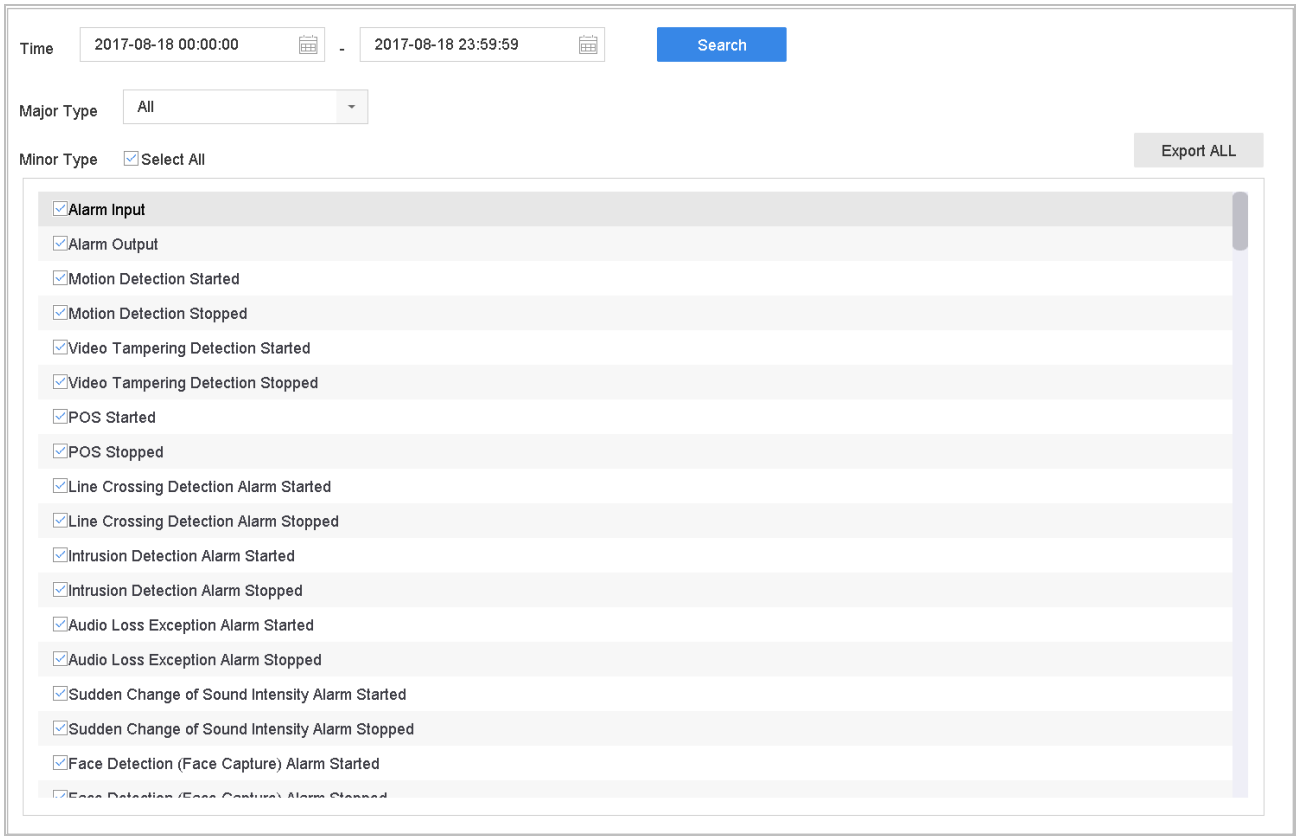


Figure 19-6 Log Search Interface

Step 2 Set the log search conditions, including the Time, Major Type and Minor Type.

Step 3 Click **Search** to start search log files.

The matched log files will be displayed on the list shown below.

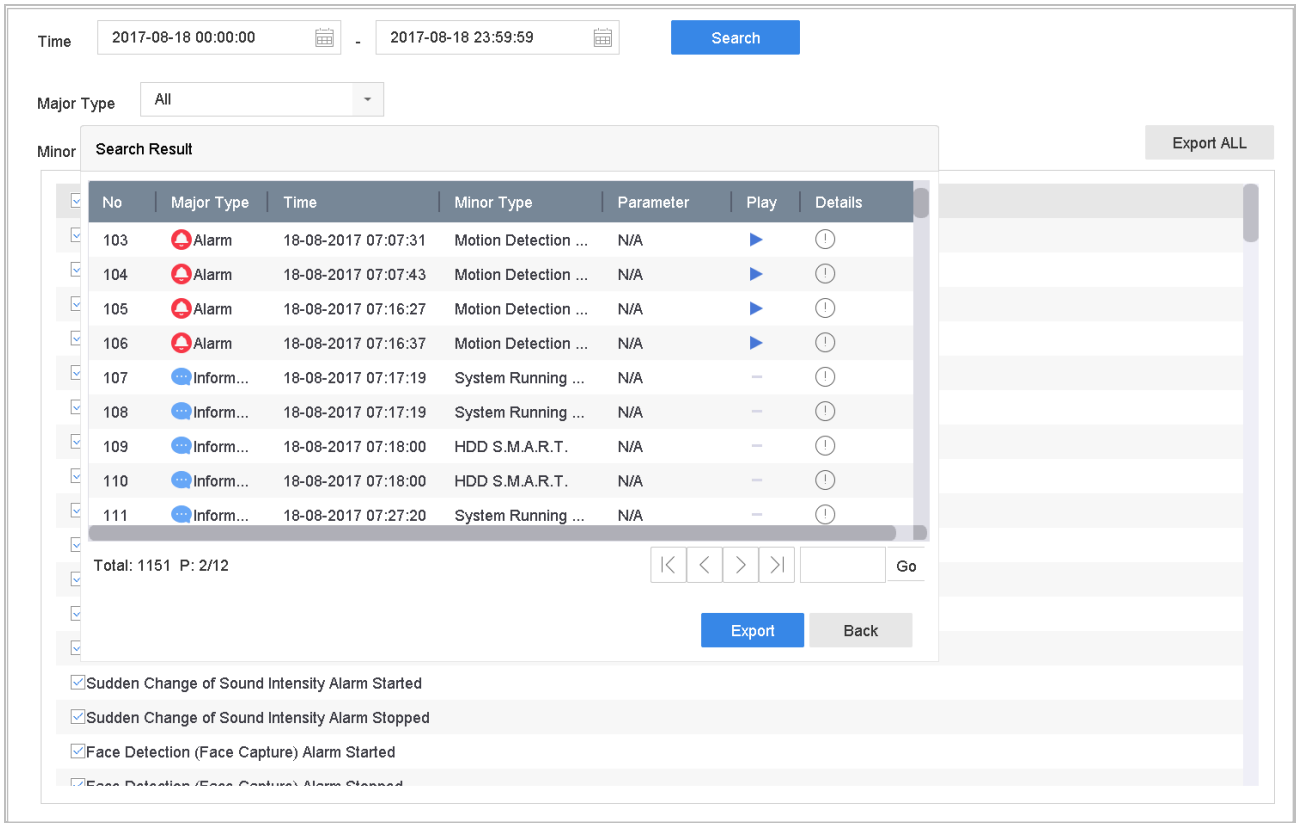


Figure 19-7 Log Search Results

NOTE

Up to 2000 log files can be displayed each time.

Related Operation:

Click the button or double click it to view its detailed information.

Click the button to view the related video file.

19.2.2 Export the Log Files

Before You Start:

Connect a storage device to your device.

Step 1 Search the log files. Refer to Chapter 19.2.1 Search the Log Files.

Step 2 Select the log files you want to export, and click **Export**.

Or you can click **Export ALL** on the Log Search interface to export all the system logs to the storage device.

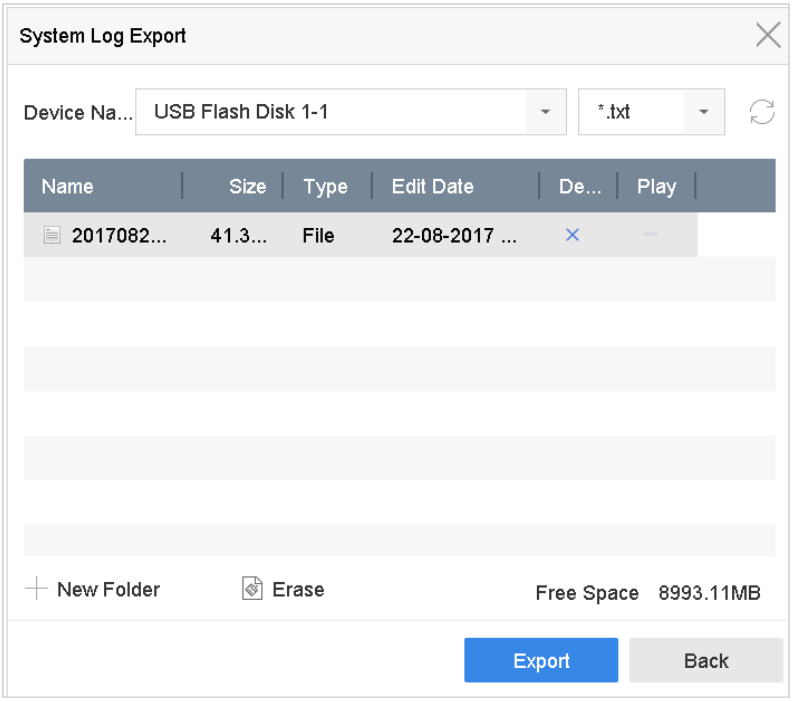


Figure 19-8 Export Log Files

Step 3 On the Export interface, select the storage device from the dropdown list of **Device Name**.

Step 4 Select the format of the log files to be exported. Up to 15 formats are selectable.

Step 5 Click the **Export** to export the log files to the selected storage device.

Related Operation:

Click the **New Folder** button to create new folder in the storage device.

Click the **Format** button to format the storage device before log export.

19.3 Import/Export IP Camera Configuration Files

Purpose:

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

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to **Camera** > **IP Camera Import/Export**.

Step 2 Click the **IP Camera Import/Export** tab, and the content of detected plugged external device appears.

Step 3 Export or import the IP camera configuration files.

Click **Export** to export configuration files to the selected local backup device.

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

NOTE

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

19.4 Import/Export Device Configuration Files

Purpose:

The configuration files of the device can be exported to 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.

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Before You Start:

Connect a storage device to your device. For importing the configuration file, the storage device must be with the file.

Step 1 Go to **Maintenance** > **Import/Export**.

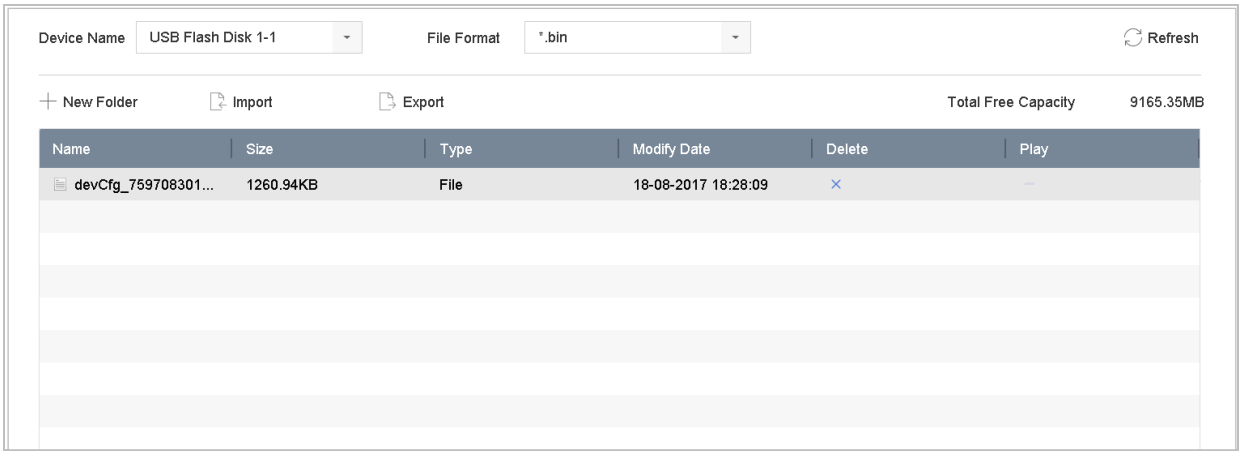


Figure 19-9 Import/Export Config File

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 the **Import** button.

NOTE

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

19.5 Upgrade System

Purpose:

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

19.5.1 Upgrade by Local Backup Device

Before You Start:

Connect your device with a local storage device with update firmware file.

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

Step 2 Click the **Local Upgrade** tab to enter the local upgrade interface.

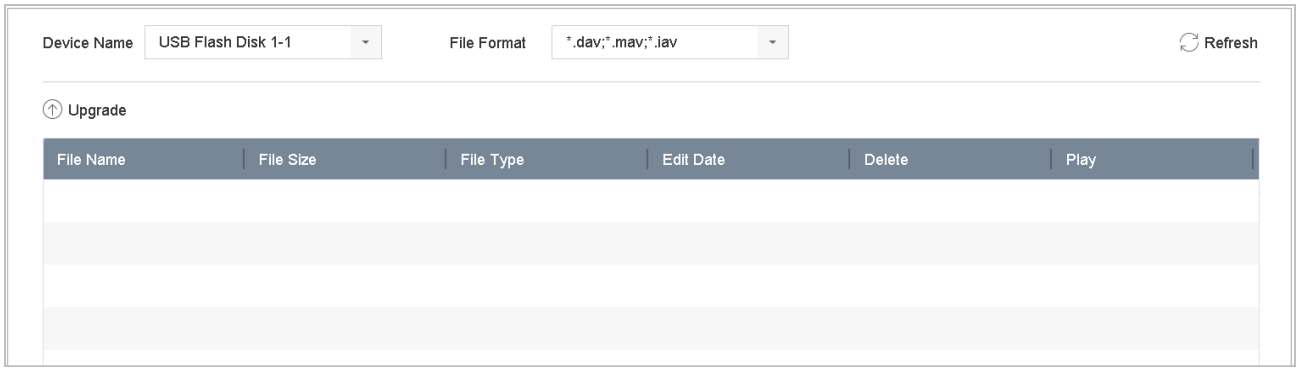


Figure 19-10 Local Upgrade Interface

Step 3 Select the update file from the storage device.

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

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

19.5.2 Upgrade by FTP

Before you start:

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

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

Step 2 Click the **FTP** tab to enter the local upgrade interface.

Figure 19-11 FTP Upgrade Interface

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

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

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

19.6 Restore Default Settings

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

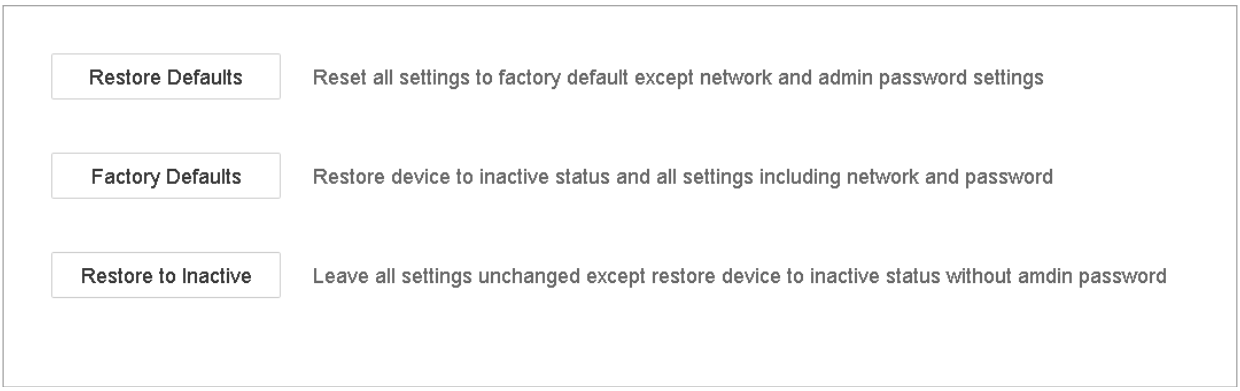


Figure 19-12 Restore Defaults

Step 2 Select the restoring 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 the inactive status.

NOTE

The device will reboot automatically after restoring to the default settings.

19.7 System Service

19.7.1 Network Security Settings

HTTP

You can choose to disable the HTTP, or set the HTTP authentication when it is enabled as demand to enhance the access security.

NOTE

By default, the HTTP service is enabled.

Set HTTP Authentication

Purpose

If you need to enable the HTTP service, you can set the HTTP authentication to enhance the access security.

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

Figure 19-13 HTTP Authentication

Step 2 Check the **Enable HTTP** to enable the HTTP service.

Step 3 Select the **digest** as the **HTTP Authentication** in the drop-down list.

Step 4 Click **Apply** to save the settings. And reboot device to take effect the settings.

NOTE

Two authentication types are selectable: **digest** and **digest/basic**. For security reasons, it is recommended to select digest as the authentication type.

Disable HTTP

Purpose

The admin user account can disable the HTTP service from the GUI or the web browser.

After the HTTP is disabled, all its related services, including the ISAPI, Onvif and Gennetc, will terminate as well.

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

Step 2 Uncheck the **Enable HTTP** to disable the HTTP service.

Step 3 Click **Apply** to save the settings. And reboot device to take effect the settings.

RTSP Authentication

Purpose

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

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

Figure 19-14 RTSP Authentication

Step 2 Select the authentication type.

NOTE

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

Step 3 Click **Apply** to save the settings. And reboot device to take effect the settings.

Enable IP Camera Occupation Detection

Purpose

After enabling the feature, when search IP camera in Number of Unadded Online Device interface, the status of IP camera the has been added by other device will show as  .

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

Step 2 Check **Enable IP Camera Occupation Detection.**

Step 3 Click **Apply** to save the settings. And reboot device to take effect the settings.

19.7.2 Managing ONVIF User Accounts

Purpose

For the third-party camera connection to the device via ONVIF, you can enable ONVIF function and manage the user accounts.

Step 1 Go to **System** > **System Service** > **ONVIF**.

Step 2 Check **Enable ONVIF** to enable the ONVIF access management.

Step 3 Click **Add** to enter the Add User interface.

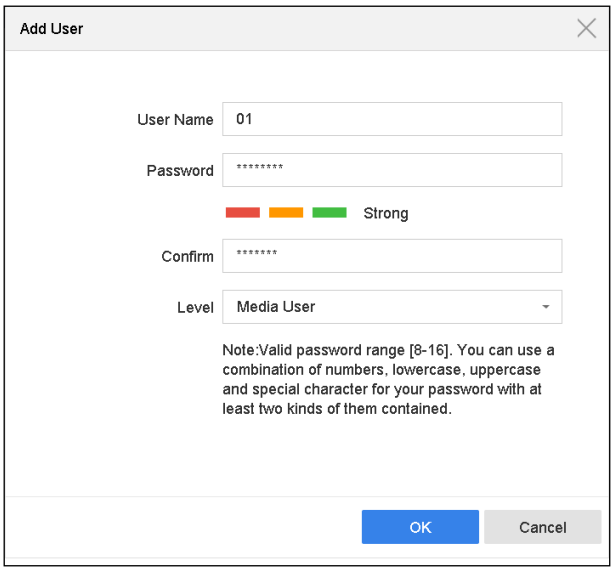


Figure 19-15 Add User

Step 4 Edit the user name, and enter the strong password.

Step 5 Select the user level to **Media User**, **Operator** and **Admin**.

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

Result:

The added user accounts have the permission to connect other devices to the device via ONVIF protocol.

NOTE

ONVIF protocol is disabled by default.

Chapter 20 General System Settings

20.1 Configure General Settings

Purpose:

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the **System** > **General**.

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

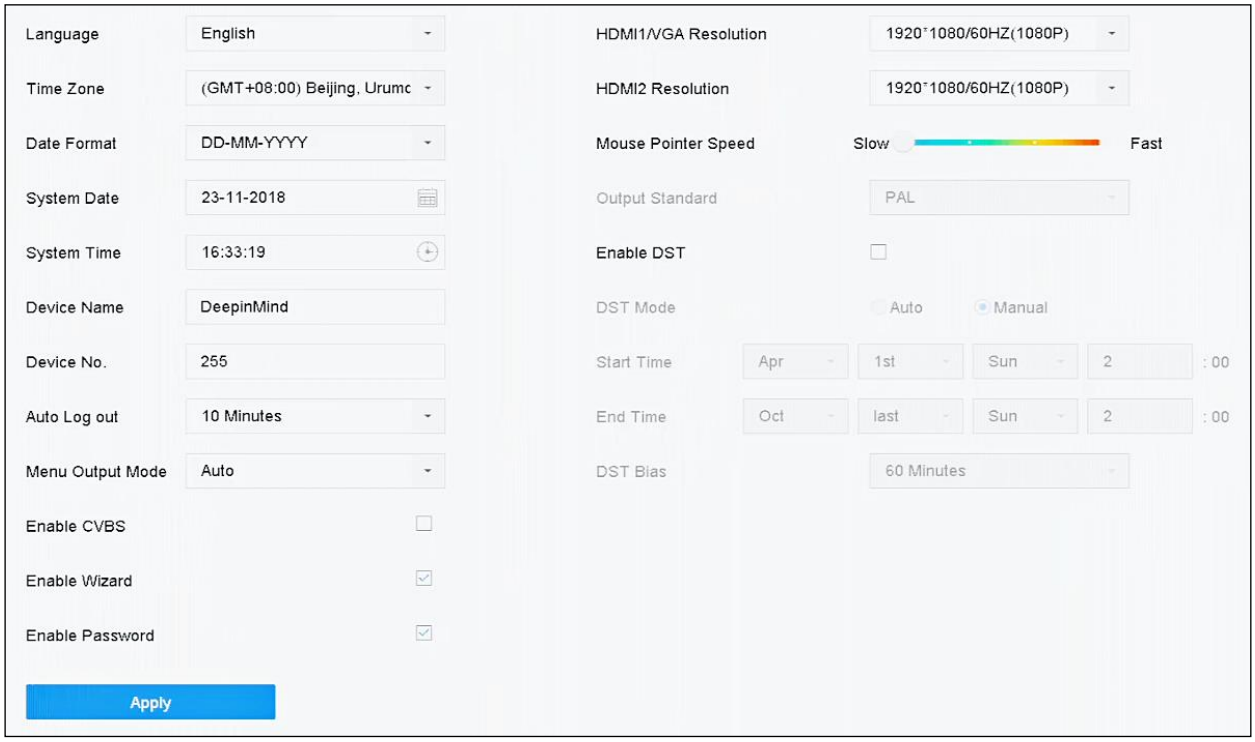


Figure 20-1 General Settings Interface

Step 2 Configure the following settings.

Language: The default language used is *English*.

Output Standard: Select the output standard to NTSC or PAL, which must be the same with the video input standard.

Resolution: Configure the resolution of the video output.

Device Name: Edit the name of the device

Device No.: Edit the serial number of the device. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.

Auto Logout: Set timeout time for menu inactivity. E.g., when the timeout time is set to *5 Minutes*, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.

Enable HDMI/VGA/LCD Simultaneous Output: Enable/disable HDMI/VGA/LCD simultaneous output. For details, refer to 5.7 Main and Auxiliary Ports Strategy.

Mouse Pointer Speed: Set the speed of mouse pointer; 4 levels are configurable.

Enable CVBS: Enable/disable CVBS output. After enabling CVBS, the menu output mode will switch to HDMI2, and it will disable HDMI1/VGA.

Enable Wizard: Enable/disable the Wizard when the device starts up.

Enable Password: Enable/disable the use of the login password.

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

20.2 Configure Date & Time

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

Step 2 Configure the date and time.

Time Zone: Select the time zone.

Date Format: Select the date format.

System Date: Select the system date.

System Time: Set the system time.

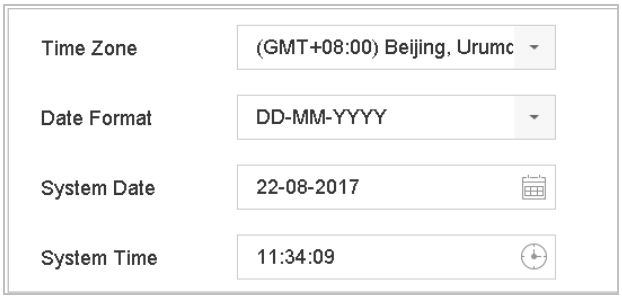


Figure 20-2 Date and Time Settings

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

20.3 Configure DST Settings

The 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**.

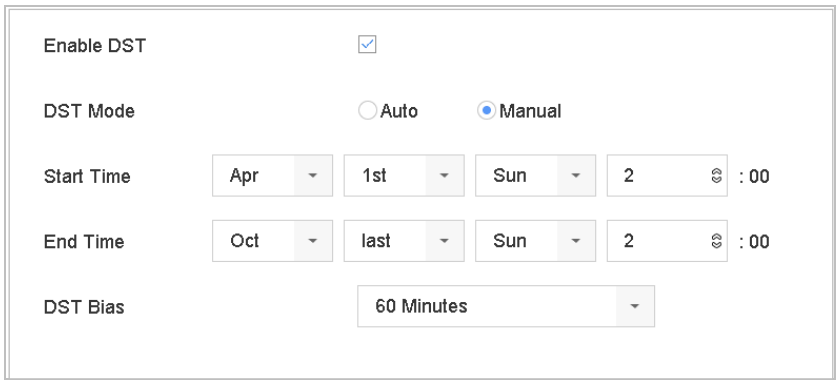


Figure 20-3 DST Settings Interface

Step 3 Select 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: The 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 the **Apply** button to save the settings.

20.4 Manage User Accounts

Purpose:

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

20.4.1 Add a User

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

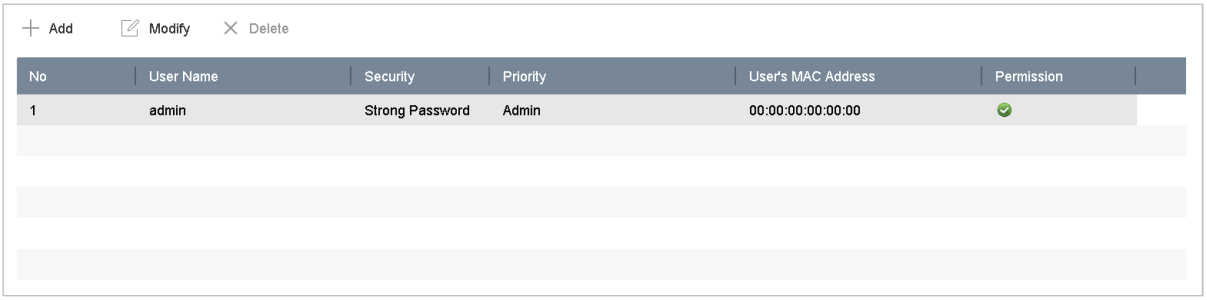


Figure 20-4 User Management Interface

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

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

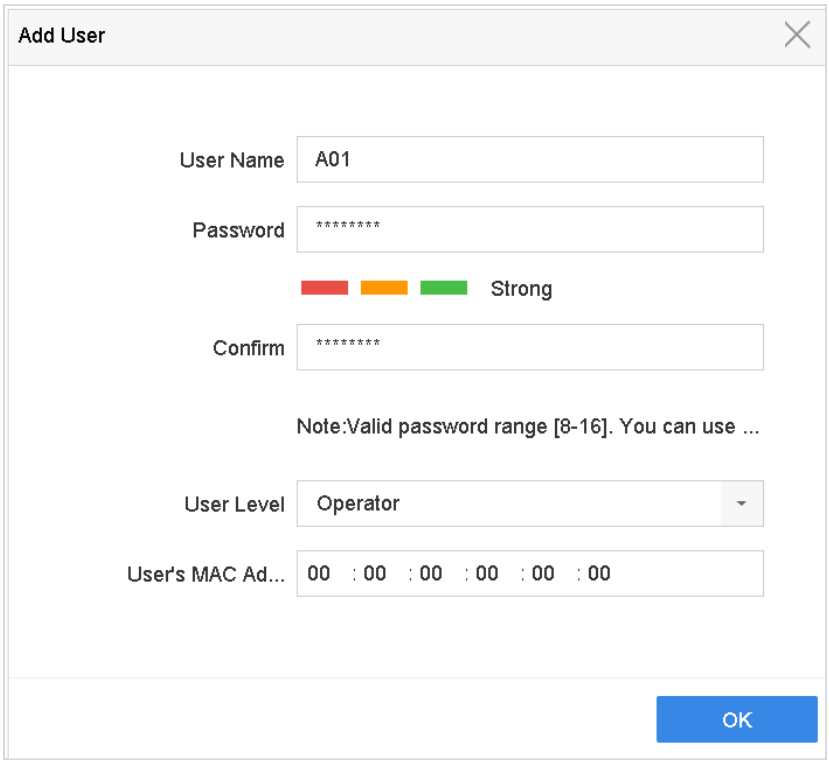


Figure 20-5 Add User

Step 4 In the Add User interface, enter the information for 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 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

Operator: The *Operator* user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.

Guest: The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

User's MAC Address: The MAC address of the remote PC which logs onto the device. If it is configured and enabled, it only allows the remote user with this MAC address to access the device.

Step 5 Click **OK** to finish the new user account adding.

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

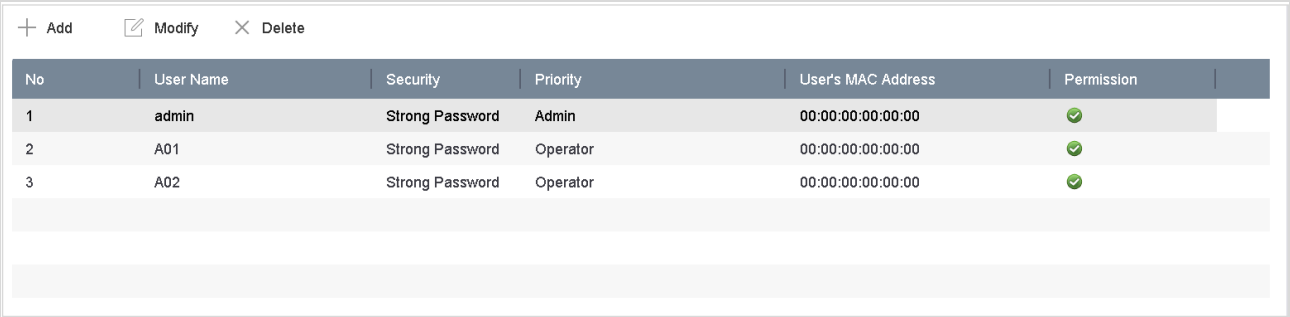


Figure 20-6 User List

20.4.2 Set the Permission for a User

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

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

Step 2 Select a user from the list and then click the button to enter the permission settings interface.

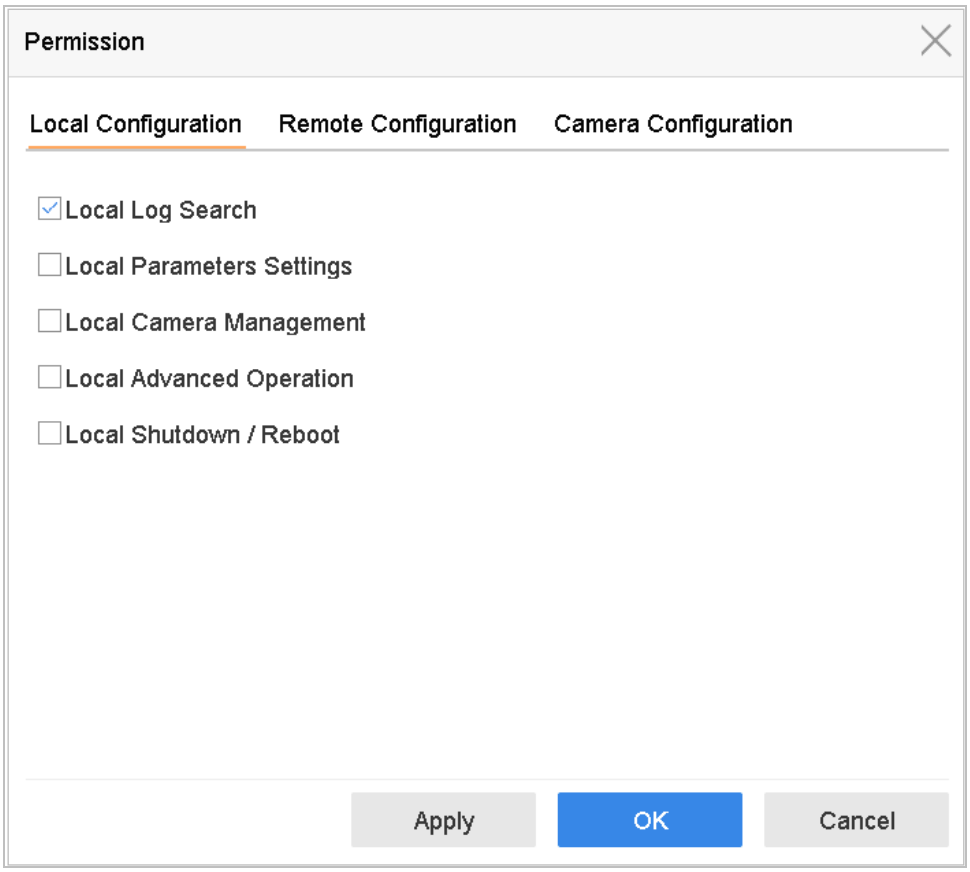


Figure 20-7 User Permission Settings Interface

Step 3 Set the operating permission of Local Configuration, Remote Configuration and Camera Configuration for the user.

Local Configuration

Local Log Search: Searching and viewing logs and system information of device.

Local Parameters Settings: Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Local Camera Management: The adding, deleting and editing of IP cameras.

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

Local Shutdown Reboot: Shutting down or rebooting the device.

Remote Configuration

Remote Log Search: Remotely viewing logs that are saved on the device.

Remote Parameters Settings: Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.

Remote Camera Management: Remote adding, deleting and editing of the IP cameras.

Remote Serial Port Control: Configuring settings for RS-232 and RS-485 ports.

Remote Video Output Control: Sending remote button control signal.

Two-Way Audio: Realizing 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) in local.

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

NOTE

Only the admin user account has the permission of restoring factory default parameters.

20.4.3 Set Local Live View Permission for Non-Admin Users

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

Step 2 Click of admin user.

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

Step 4 Select cameras that non-admin user can view in local and click **OK.**

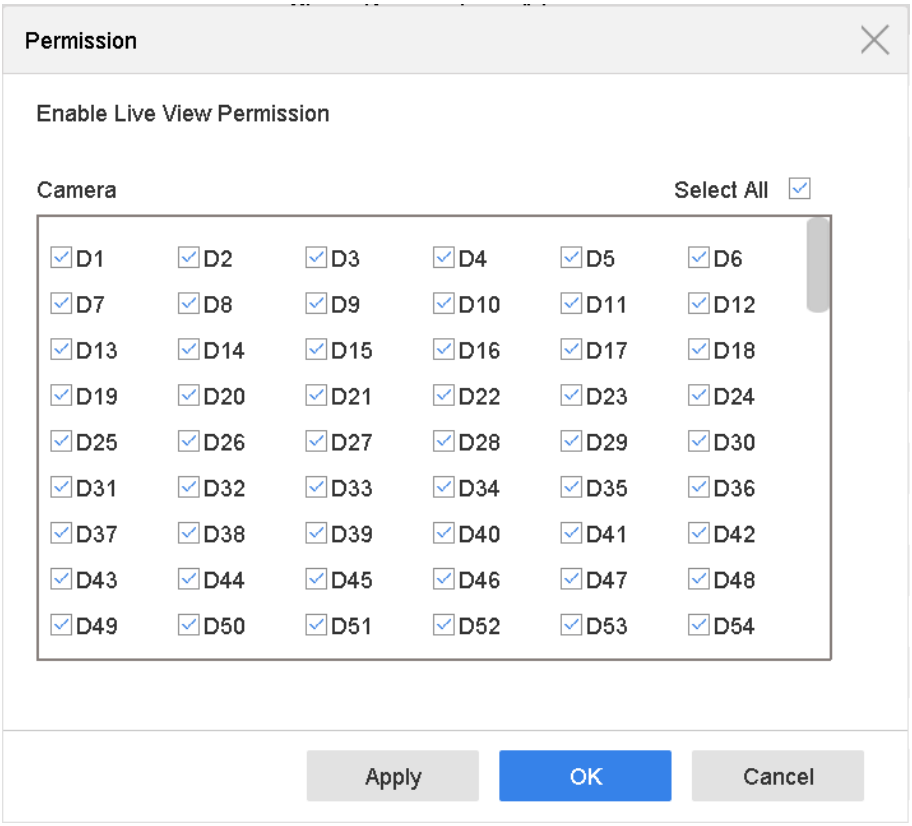


Figure 20-8 Enable Live View Permission

Step 5 Click of non-admin user.

Step 6 Enter **Camera Configuration**.

Step 7 Select **Camera Permission** as **Local Live View**.

Step 8 Select cameras to live view.

Step 9 Click **OK**.

20.4.4 Edit the Admin User

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

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

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

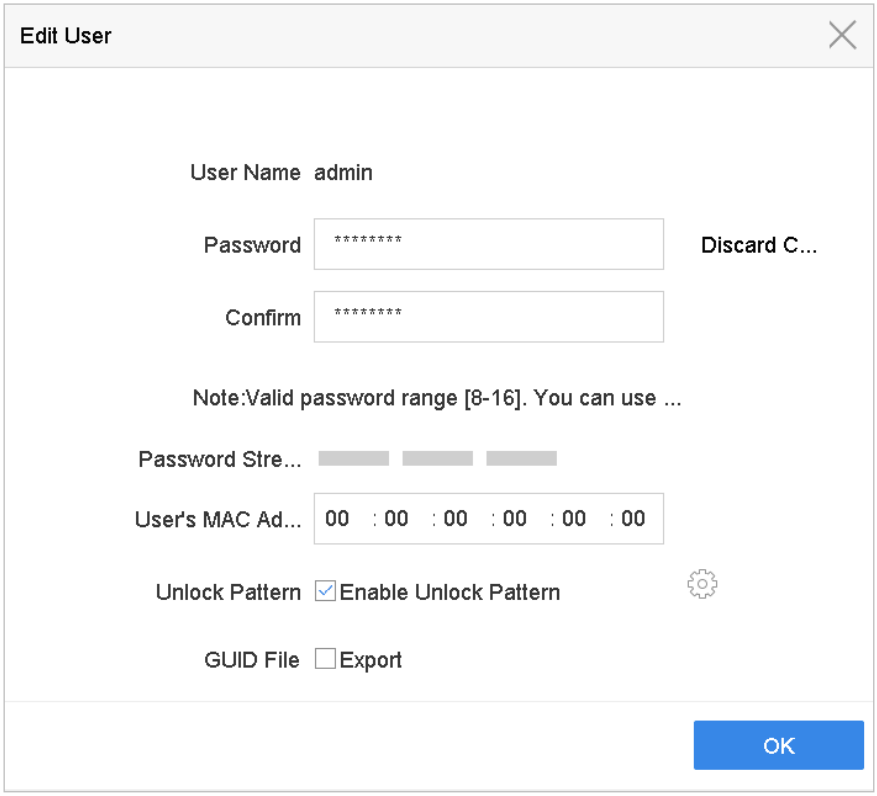


Figure 20-9 Edit User (Admin)

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

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

1) Check the checkbox of **Enable Unlock Pattern** to enable the use of unlock pattern when logging in to the device.
2) Use the mouse to draw a pattern among the 9 dots on the screen, and release the mouse when the pattern is done.

NOTE

Please refer to Chapter 2.3 Configure Unlock Pattern for Login for detailed instructions.

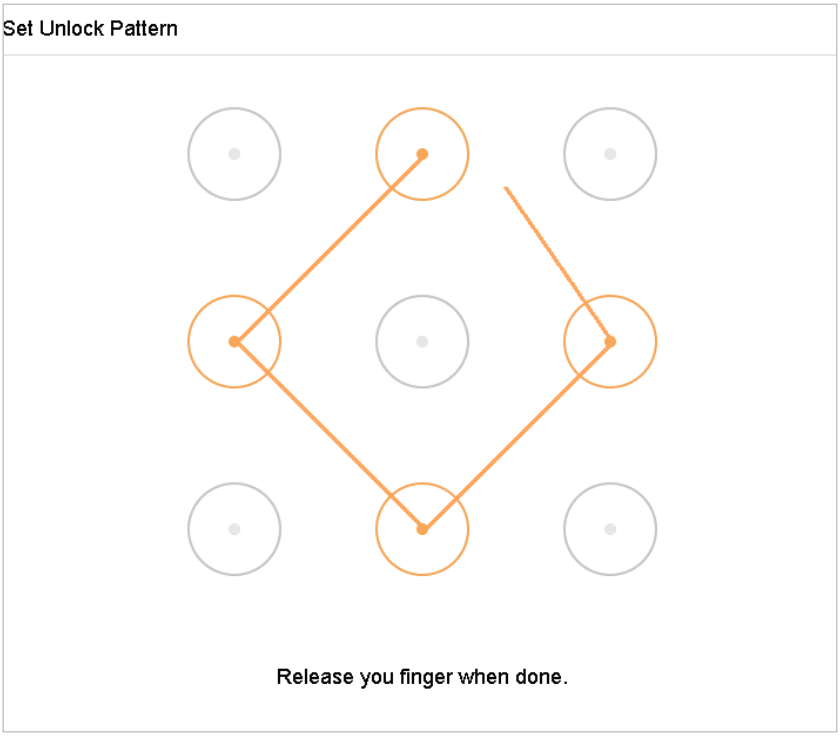


Figure 20-10 Set Unlock Patter for Admin User

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

When the admin password is changed, you can export the new GUID to the connected U flash disk in the Import/Export interface for the future password resetting.

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

Step 7 For the **Operator** or **Guest** user account, you can also click the  button on the user management interface to edit the permission.

20.4.5 Edit the Operator/Guest User

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

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

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

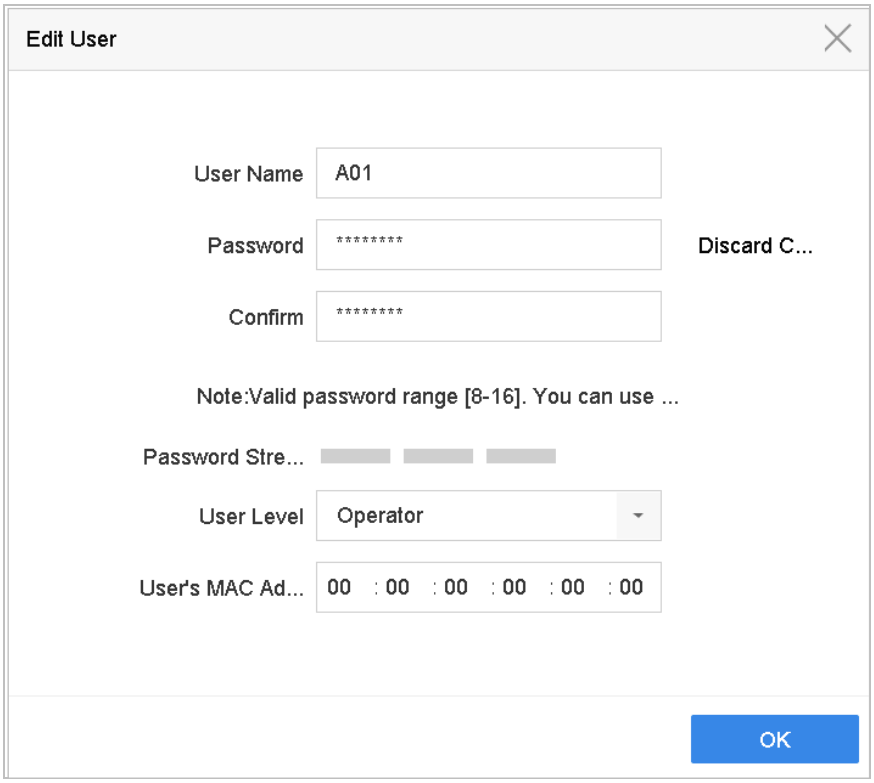


Figure 20-11 Edit User (Operator/Guest)

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

20.4.6 Delete a User

The admin user account has the permission to delete the 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 21 Appendix

21.1 Glossary

- **Dual Stream:** Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the device, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.
- **HDD:** Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.
- **DHCP:** Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- **HTTP:** Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network
- **DDNS:** Dynamic DNS is a method, protocol, or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.
- **PPPoE:** Stands for "Point-to-Point Protocol over Ethernet." PPPoE is a network configuration used for establishing a PPP connection over an Ethernet protocol.
- **Hybrid device:** A hybrid device is a combination of a DVR and device.
- **NTP:** Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.
- **NTSC:** Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.
- **Device:** Acronym for Network Video Recorder. A device can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other devices.
- **PAL:** Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.
- **PTZ:** Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.
- **USB:** Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

UD15842B