IC REALTIME

IC Realtime
Network Video Recorder

User's Manual

V4.1.1

Foreword

General

This manual introduces the functions and operations of the NVR device (hereinafter referred to as "the Device"). **Note that not all functions covered in this manual are available depending on the actual model used.**

Safety Instructions

The following categorized signal words with defined meanings might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard that, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	This indicates a potential risk that, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
⊙⌐ TIPS	Provides methods to help you solve a problem or save you time.
📖 NOTE	Provides additional information as the emphasis and supplement to the text.

About the Manual

- The manual is for reference only. If there is any inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the manual, QR code, or our official website.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact technical support for the latest program and supplementary documentation.
- There still may be a deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- All trademarks, registered trademarks, and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurring when using the device

Important Safeguards and Warnings

The following statements describe the correct application methods for the device. Read the manual carefully before use to prevent danger and property loss. Strictly conform to the manual during application and keep it properly stored after reading for future reference.

Operating Requirements

- Install the PoE front-end device indoors.
- These devices do not support wall mounts.
- Do not place and install the device in an area exposed to direct sunlight or near a heat-generating device.
- Do not install the device in a humid, dusty, or dirty area.
- Make sure the recorder is installed horizontally, at a stable location, and prevent it from falling.
- Do not drip or splash liquids onto the device; do not put on the device anything filled with liquids, in order to prevent liquids from flowing into the device.
- Install the device at well-ventilated places; do not block its ventilation opening(s).
- Power the device only within the rated input and output range.
- Do not dismantle the device arbitrarily.
- Transport, use, and store the device within the allowed humidity and temperature range.

Power Requirements

- Make sure to use the designated power type. Otherwise, there may be a risk of fire or explosion.
- Make sure to use power according to requirements. Otherwise, it may result in fire, explosion, or burning risks of batteries!
- To replace batteries, only the same type of batteries can be used.
- Make sure to dispose of the exhausted batteries according to the instructions.
- The product shall use electric wires (power wires) recommended by this area, which shall be used within its rated specification.
- Make sure to use a standard power adapter matched with this device. Otherwise, the user shall undertake resulting personnel injuries or device damages.
- Use a power supply that meets SELV (safety extra-low voltage) requirements, and supply power with a rated voltage that conforms to Limited Power Source in IEC60950-1. For specific power supply requirements, please refer to device labels.
- Products with category I structure shall be connected to a grid power output socket, which is equipped with protective grounding.
- The appliance coupler is a disconnecting device. During normal use, please keep an angle that facilitates operation.

Table of Contents

1. Features

1.1 Overview

The IC Realtime NVR series are high-performance network video recorders. The NVRs support local preview, multiple-window display, recorded file local storage, remote control and mouse shortcut menu operation, and remote management and control function. The IC Realtime NVRs supports center storage, front-end storage and client-end storage. The monitor zone in the front-end can be set in anywhere. Working with other front-end devices such as IPC, NVS, this series product can establish a strong surveillance network. In a typical network system, there is only one network cable from the monitor center to the monitor zone in the whole network. This series NVR can be widely used in many areas such as public security, water conservancy, transportation, and educational institutes.

1.2 Features

Feature	Description
P2P Connection	● Fast and easy connection for remote access, can connect using IC Realtime desktop and mobile applications.
Real-time Surveillance	● VGA, HDMI port. Connect a monitor to view real-time surveillance. Some recorders support TV/VGA/HDMI simultaneous output. ● Short-cut menu when preview. ● Supports popular PTZ decoder control protocols. Supports preset, tour, and pattern.
Playback	● Supports each channel's real-time record independently, as well as search, forward play, network monitor, record search, download and etc. ● Supports various playback modes: slow play, fast play, backward play, and frame by frame play. ● Supports time title overlay so that you can view event accurate occurred time ● Supports digital zoom.
User Management	● Each group has different management permissions that can be edited. Every user belongs to an exclusive group.
Storage	● With a corresponding setup (such as alarm setup and schedule setup), you can backup related audio/video data in the network video recorder. ● Supports Web GUI playback and local video storage via Smart ICRSS client.

Feature	Description
Alarm	- Responds to external alarm simultaneously (within 200MS), based on the user's pre-defined relay setup, the NVR can process the alarm input correctly and prompt the user by screen and voice (support pre-recorded audio). - Supports central alarm server setup so that alarm information can remotely notify users automatically. Alarm input can be derived from various connected peripheral devices. - Alert you via email/SMS.
Network Monitor	- Displays audio/video data compressed by IPC or NVS to client-ends through the network. - Supports max 128 connections at the same time. - Transmit audio/video data by HTTP, TCP, UDP, MULTICAST, RTP/RTCP and etc. - Transmit some alarm data or alarm info by SNMP. - Supports Web access in WAN/LAN.
Window Split	- Utilizes video compression and digital processes to show several windows on one monitor. - Supports up to 1/4/8/9/16/25/36-window display when on preview and 1/4/9/16-window display when playback (depending on model).
Record	- Support normal/motion detect/alarm record function. - Saves the recorded files to the HDD, USB device, client-end PC, or network storage server. - You can search or playback the saved files at the local end or via the Web/USB device.
Backup	Supports network backup, USB2.0/3.0 record backup function, the recorded files can be saved in-network storage server, peripheral USB2.0 device, etc.
Network Management	- Supervises NVR via Ethernet. - Supports management via the Web interface.
Peripheral Equipment Management	- Supports peripheral equipment management such as protocol setup and port connection. - Support transparent data transmission such as RS232 (RS-422), RS485 (RS-485).
Auxiliary	- Supports NTSC and PAL. - Supports real-time system resources information and running statistics display. - Supports logging information. - Local GUI output. Shortcut menu operation via mouse. - IR control function (For some series NVR units only). - Playing the video/audio from the network camera or NVS remotely.

2. Front and Rear Panel

2.1 Front Panel

2.1.1 1U POE NVR Series (NVR-MX08POE, NVR-MX16POE, NVR- FX08POE, NVR-FX16POE)

The 1U series front panel is shown as in Figure 2-1.

Figure 2-1

Icon	Name	Function
ICRealtime LED	Power LED	The IC Realtime Logo will light up indicating its power on status. If the unit is not booting all the way up and the LED is turning on and off it could be a power failure or a failed HDD. Power down the unit and try unplugging HDD. Power unit without HDD. If the unit boots HDD has failed. If not, consult IC Realtime Support.
	USB port	Connects to mouse, USB Flash Drive, and etc. Some NVR models are equipped with USB 3.0. External HDDs are not supported.

2.1.2 2U NVR Series (NVR-7516K, NVR-EL32, NVR-EL64)

The NVR-7516K and NVR-6032K front panel is shown as in Figure 2-2. The NVR-6064K front panel is shown as in Figure 2-3

Figure 2-2
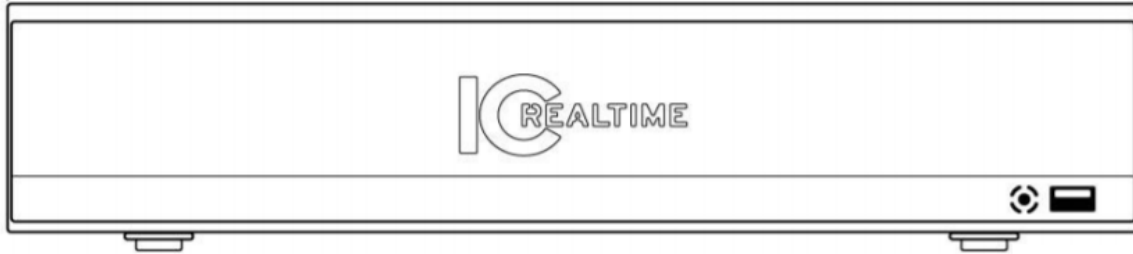
Figure 2-3

Port Name	Connection	Function
⟜⟷	USB 2.0 port	Connects to a mouse, USB Flash Drive, etc. External HDDs are not supported.
Power Button	Power switch	Turns NVR on/ off
POWER / ICRealtime LED	Power LED	The Power Status LED / IC Realtime Logo will light on when powered on. If the unit is not booting all the way up and the LED is turning on and off it could be a power failure or a failed HDD. Power down the unit and try unplugging HDD. Power unit without HDD. If the unit boots HDD has failed. If not, consult IC Realtime Support.
NET	NET LED	Network Status LED
HDD	HDD LED	Hard Drive Status
ALARM	Alarm LED	Alarm Status

Front Panel Lock	HDD Bay panel	Use the provided key to open Hard Drive bay

2.2 Rear Panel

2.2.1 1U POE NVR Series (NVR-MX08POE, NVR-MX16POE, NVR- FX08POE, NVR-FX16POE)

The NVR-FX08POE and NVR-MX08POE front panel is shown in Figure 2-4. The NVR-FX16POE and NVR-MX16POE front panels are shown in Figure 2-5.

Figure 2-4
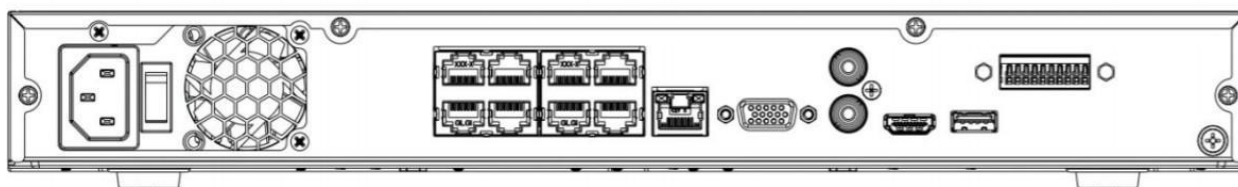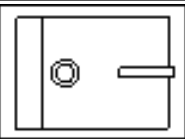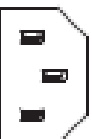
Figure 2-5

Port Name	Connection	Function
	Power switch	Power on/off button.
	Power input port	Power socket. Input AC 100~240V.
	Network port	10M/100Mbps self-adaptive Ethernet port.
	USB 2.0/3.0 port	Connects to mouse, USB Flash Drive, and etc. External HDDs are not supported.
HDMI	High Definition Media Interface	High definition audio and video signal output port. It transmits uncompressed high-definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It connects to a monitor to view the local display.
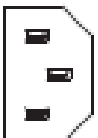
MIC IN	Audio input port	Receives the analog audio signal output from the devices such as a microphone, pickup.
MIC OUT	Audio output port	To output the analog audio signal to devices such as a speaker. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
⏚	GND	Ground end
PoE PORTS	PoE port count will vary depending on the model	Built-in switch. Supports PoE function. IC Realtime cameras are supported. Third-party cameras may not function properly. Port count will vary. Consult product datasheet. Consult datasheets for maximum load.

2.2.2 2U POE NVR Series (NVR-7516K)

The NVR-7516K rear panel is shown in Figure 2-6.

Figure 2-6

Port Name	Connection	Function
Power switch image	Power switch	Power on/off button.
Power input image	Power input port	Power socket. Input AC 100~240V.
Network icon	Network port	10M/100Mbps self-adaptive Ethernet port.
USB icon	USB 2.0/3.0 port	Connects to mouse, USB Flash Drive, and etc. External HDDs are not supported.
HDMI	High Definition Media Interface	High definition audio and video signal output port. It transmits uncompressed high-definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Outputs analog video signal. Connects to a monitor to view local display.

MIC IN	Audio input port	Receives the analog audio signal output from the devices such as a microphone, pickup.
MIC OUT	Audio output port	Outputs the analog audio signal to the devices such as a speaker. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
⏚	GND	Ground end
PoE PORTS	PoE port	Built-in switch. Supports PoE function. IC Realtime cameras are supported. Third-party cameras may not function properly. Port count will vary. Consult product datasheet. Consult datasheets for maximum load.
1–16	Alarm input port 1–16	● The first group is from port 1 to port 4, the second group is from port 5 to port 8, the third group is from 9 to 12, and the fourth group is from 13 to 16. Receives the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	Ground (GND)	Alarm input ground port.
NO1–NO5	Alarm output port 1–5 The number of ports will vary from unit to unit. Consult Datasheet.	● 5 groups of alarm output ports. (Group 1:port NO1–C1,Group 2:port NO2–C2,Group 3:port NO3–C3, Group 4:port NO4–C4, Group 5: port NO5, C5, NC5).Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO: Normal open alarm output port. ● C: Alarm output public end. ● NC: Normal close alarm output port.
C1–C5		
A / B	RS-485 communication port	RS485 Ports connect to the corresponding ports of a PTZ for local PTZ control. Typically not used with modern IP PTZ.

2.2.3 2U NVR Series (NVR-EL16, NVR-EL32, NVR-EL64)

The NVR-EL16, NVR-EL32, NVR-EL64 rear panel is shown on Figure 2-7.

Figure 2-7

Name		Function
Power switch	/	Power on-off button.
Power input port	/	Power socket. Input AC 100~240V
MIC IN	Audio input port	Bidirectional talk input port. Receives the analog audio signal output from the devices such as a microphone or pickup.
MIC OUT	Audio output port	Outputs the analog audio signal to the devices such as a speaker box. ● Bidirectional talk output. ● Audio output on a 1-window video monitor. ● Audio output on 1-window video playback.
Network Port (x2)	Network Ports	NiC1 for local network, NiC2 for IP cam network
1–16	Alarm input port 1–16	● The first group is from port 1 to port 4, the second group is from port 5 to port 8, the third group is from 9 to 12, and the fourth group is from 13 to 16. Receives the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	GND	Alarm input ground port.
NO1–NO5 C1–C5 NC5	Alarm output port 1–5	● 5 groups of alarm output ports. (Group 1:port NO1–C1,Group 2:port NO2–C2,Group 3:port NO3–C3, Group 4:port NO4–C4, Group 5: port NO5, C5, NC5).Output alarm signal to the alarm device. Please make sure there is power to the external alarm device.

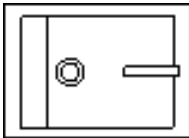|		
		● NO: Normally open alarm output port. ● C: Common, Alarm output public end. ● NC: Normally closed alarm output port.
A	RS-485 communication port	RS485_A port. For cable A. To connect to the control devices such as a PTZ.
B		RS485_B.For cable B. To connect to the control devices such as a PTZ.
⟻⟶	USB port	For connecting to a mouse or a USB storage device.
RS-232	RS-232 COM.	For debug only. No control.
HDMI	High Definition Media Interface	High definition audio and video signal output port. It transmits uncompressed high-definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Outputs analog video signal. Connects to the monitor to view analog video.
CTRL 12V	/	Provides a constant 12vDC/500ma supply. When the last alarm output is triggered, the power turns off for a period of time before resuming when the alarm is cleared.
+12V	/	Constant 12vDC/500ma power source. Can power devices and be used in conjunction with Alarm outputs to trigger the devices powered by it.
⛁	Network port	10M/100M/1000Mbps self-adaptive Ethernet port. Connects to the local network.
eSATA	eSATA port	External SATA port. Contact Technical support for compatible devices.

2.3 Alarm Connection

2.3.1 Alarm Port

The alarm port is shown below. See Figure 2-78. The following figure is for reference only.

- Different models support different numbers of alarm ports. Please refer to the specifications sheet for detailed information.
- Slight differences may be found in the alarm port layout depending on the model.

Figure 2-78
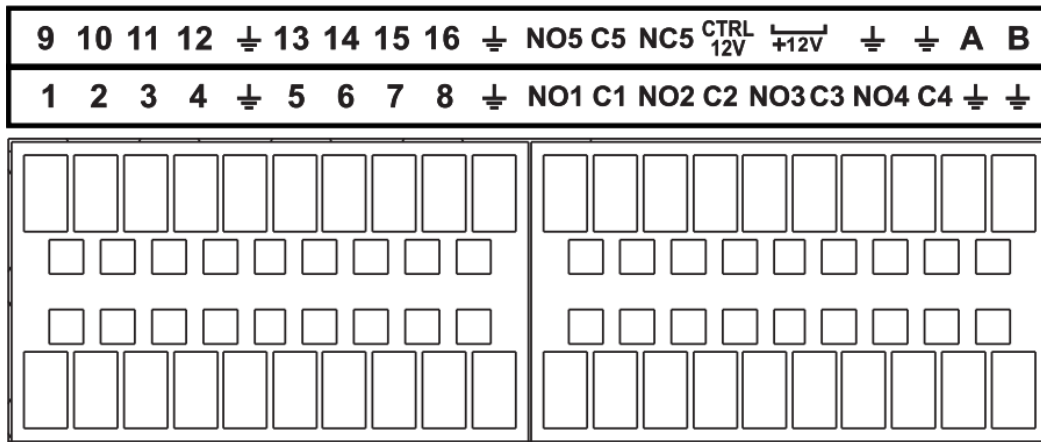
Table 2-34

Icon	Function
1–16	ALARM1–ALARM16. The alarm activates at low level.
NO1 C1, NO2 C2, NO3 C3, NO4 C4	Four NO (Normally open) activation output groups.
NO5 C5 NC5	One NO/NC activation output group.
CTRL 12V	Provides a constant 12vDC/500ma supply. When the last alarm output is triggered, the power turns off for a period of time before resuming when the alarm is cleared.
$+$12V	Constant 12vDC/500ma power source. Can power devices and be used in conjunction with Alarm outputs to trigger the devices powered by it.
$\perp$	GND (Ground)
A/B	RS485 communication port. They are used to control devices such as PTZ. Parallel connect 120TΩ between A/B cables if there are too many PTZ connections.

2.3.2 Alarm Input Port

Connect the positive end (+) of the alarm input device to the alarm input port (ALARM IN 1–16) of the NVR. Connect the negative end (-) of the alarm input device to the ground end (⏚) of the NVR.

Figure 2-79 Alarm input port

📖
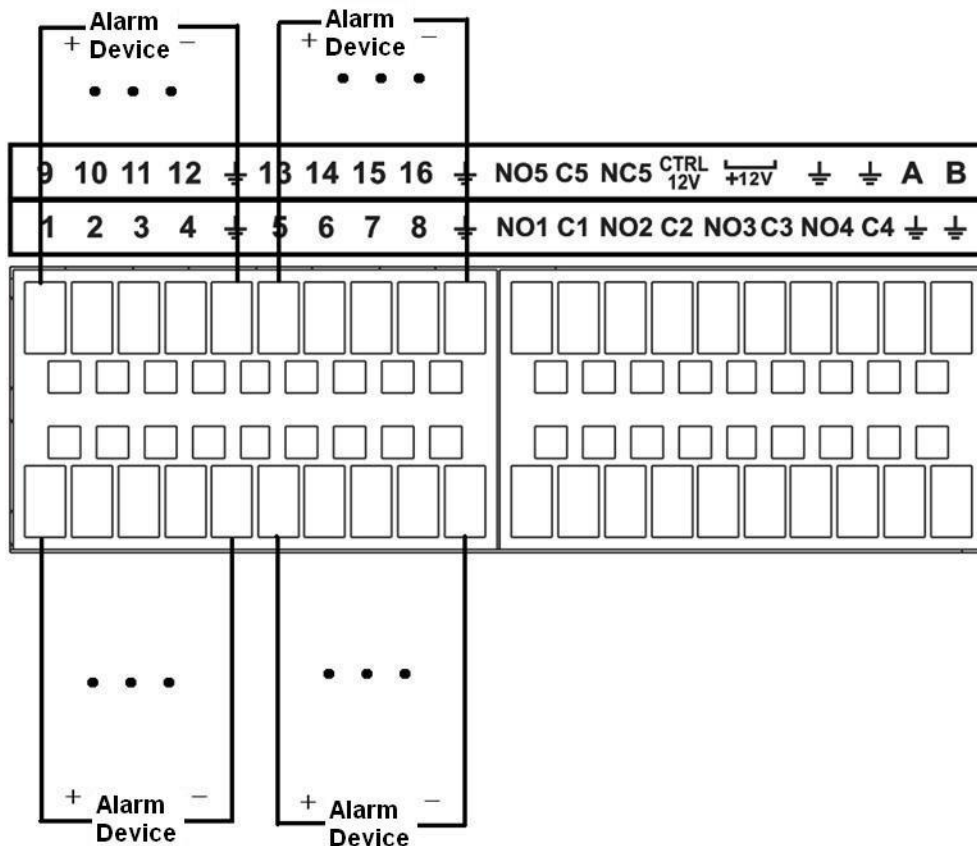
- There are two alarm input types: NO/NC. Alarm input type must be set in the recorder's alarm menu.
- When connecting the ground port of the alarm device to the NVR, use any of the ground ports.
- Connect the NC port of the alarm device to the alarm input port (ALARM) of the NVR.
- When there is peripheral power supplying for the alarm device, please make sure it is grounded with the NVR.

2.3.3 Alarm Output Port

- Peripheral power will be needed to supply the external alarm device. It is recommended not to exceed 1 amps of power.

- The Alarm type for Alarm-out is typically NO (Normally Open).

- Some models will have a CTRL12V+ This can be configured and will show up as the last

alarm output. The ports used will be CTRL 12V and ⏚ (ground) . This port will supply constant 12V+ power until the alarm output is triggered. After some time, the power will resume again.

- A 12v rail is equipped in some models. This supplies constant 12V power. The ports used will be +12V and ⏚ (ground).

- The ports used with NO# and C#. For example, NO1 and C1 for Alarm-Out Channel 1
- An overload may result in NVR damage, please refer to the following relay specifications for detailed information.
- See Figure 2-80 for an example.

Figure 2-80
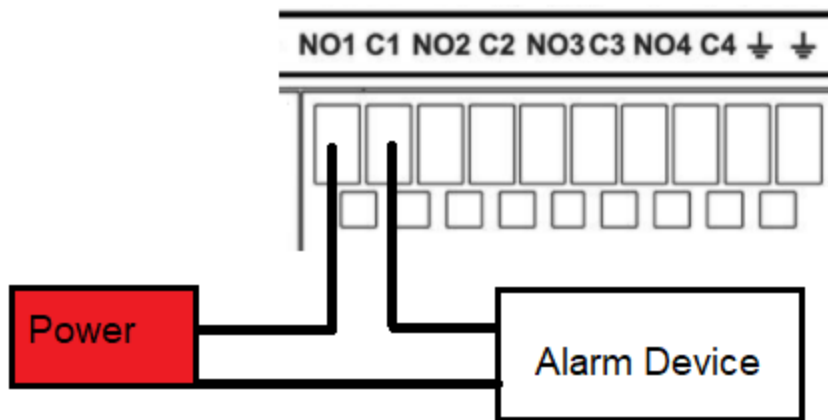
2.3.4 Alarm Relay Specification

Table 2-35

Model: JRC-27F		
Contact Material	Silver	
Rating (Resistance Load)	Rated switch capacity	30VDC 2A, 125VAC 1A
	Maximum switch power	125VA 160W
	Maximum switch voltage	250VAC, 220VDC
	Maximum switch currency	1A
Insulation	Between contact with the same polarity	1000VAC 1minute
	Between contact with different polarity	1000VAC 1minute
	Between contact and winding	1000VAC 1minute
Surge voltage	Between contact with same polarity	1500V (10×160us)

Length of open time	3ms max	
Length of close time	3ms max	
Longevity	Mechanical	50×106 MIN (3Hz)
	Electrical	200×103 MIN (0.5Hz)
Temperature	-40°F to +158°F	

2.4 Two-Way Talk

With a microphone and speaker wired to a recorder and camera it is possible to engage in two way communication. You can engage two-walk talk from the NVR head end to a camera or from a remote PC or application to the NVR or IP camera (IP camera must have an audio input output device connected).

2.4.1 Device-end to Camera

Microphone & Speaker Requirements:

Connect a powered microphone or a pickup to the audio input port, and a speaker to the audio out port on the NVR's rear panel. See Figure 2-80. The camera must have a built-in speaker & microphone or external speaker & microphone connected.

Figure 2-80

Operating Two-Way talk from the recorder to camera

On the local display you can only engage in Two-Way talk with one camera at a time. To enable Two-Way talk to move the mouse to the top center of the desired camera. A small control options menu will appear with a microphone icon. Press it to engage in two-way communication. See figure 2-81.

Figure 2-81

If you wish to simply just listen to the audio of a specific channel without being heard on the other end simply bring the camera full screen (single split). If you have a speaker plugged in and microphone is enabled on the camera you will be able to listen in.

2.4.2 PC-end to the Device-end

Device Connection

Connect a microphone or audio pickup to a PC and then connect a speaker to the audio output port in the device rear panel.

Operating Two-Way talk from PC to Recorder or Camera

Log in to the NVR Web GUI and click "Start Talk" to enable the two-way talk between the PC and Recorder. To enable Two-Way talk with the Camera, open the camera's live view and select the microphone option. See Figure 2-82.

Figure 2-82

Two-way talk to NVR

Two-way talk with IP camera
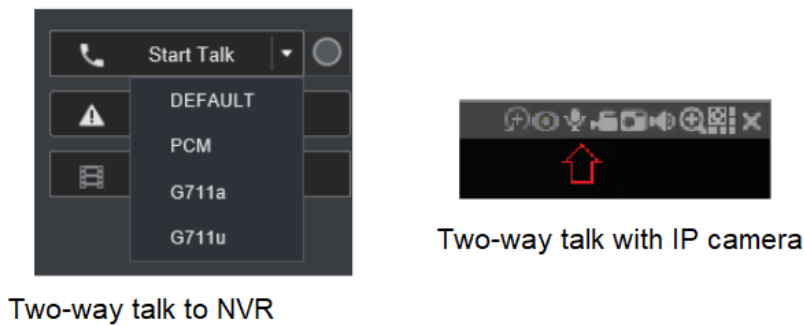
At the PC end, when speaking via the microphone, you will receive the audio to the speakers at the device end. See Figure 2-83.
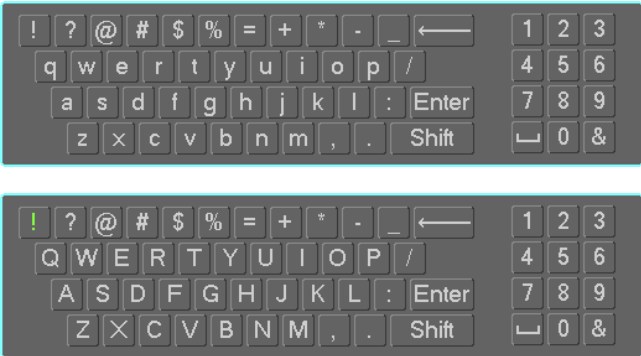
Figure 2-83
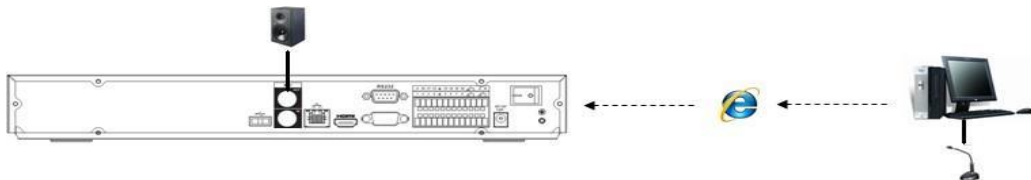
2.5 Mouse Operation

Refer to the following sheet for mouse operation instruction.

Table 2-36

Operation	Description
Left click mouse	- To view menu content, hover the mouse over a menu item, then left-click on the mouse. - Modify checkbox or motion detection status. Click combo box to pop up drop-down list When in an input box, you can select input methods. Left-click the corresponding button on the panel to swap between numeral/English characters (small/capitalized). The icon" ← " is for backspace. The "＿" represents the space button. In Alphabet input mode: _ icon is to input a backspace and ← icon is to delete a previous character. In numeral input mode: the "_" icon is for clear and the "←" icon is for deleting the previous numeral character.
Double left-click mouse	Utilize special control operations such as double-clicking one item in the file list to playback the video.
	In multiple-window mode, double left click selects one channel to view in full-window.
	Double left-click the current video again to go back to the previous multiple-window mode.
Right-click mouse	While in real-time monitor mode, this calls shortcut menu.
	Exit the current menu without saving the modification.
Move mouse	Select current control or motion control.
Drag mouse	Select motion detection zone.
	Select privacy mask zone.

2.6 Remote Control

The remote control interface is shown in Figure 2-84.

Note that remote control may not be a standard accessory on some models and may not be included in the accessory box.

Figure 2-84
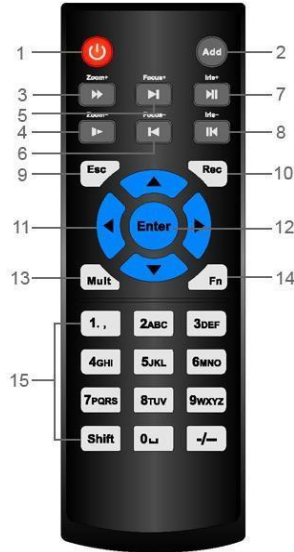
No.	Name	Function
1	Power button	Boots up or turns off the Recorder.
2	Address	Pairs the remote to the Recorder. Press this button and input the NVR device number. (Default is 8)
3	Forward	Multi-step forward speed and normal speed playback.
4	Slow motion	Multi-step slow motion speed on playback mode.
5	Next record	Plays the next video file while in playback mode
6	Previous record	Plays the previous video file while in playback mode
7	Play/Pause	● In playback mode, this toggles the video to pause if playing or play if paused ● Goes to video search mode if in Live view mode.
8	Reverse/pause	Pause while in the reverse playback mode
8	Reverse/pause	If paused in reverse playback mode, this will resume the reverse playback.
9	Esc	Go back to the previous menu or cancel the current operation.

No.	Name	Function
10	Record	- Start or stop record manually. - In the record interface, use the direction buttons to select the channel that you want to record. - Press this button for at least 1.5 seconds, to display the manual record interface.
11	Direction keys	Switch between current activated controls by pressing left or right. Aux function (such as operating the PTZ menu).
12	Enter/menu key	- Confirms an operation. - Navigate to the OK button. - Navigate to the menu.
13	Split view	Switch between multiple and single-split views.
14	FN	- Display the PTZ control and color setting functions if in single-channel monitoring mode. - In the motion detection interface, press this button with direction keys to finish the setup. - In-text mode, Deletes the last character. Long press this button for 1.5 seconds to clear.
15	Alphanumeric keys	- Input password, numbers. - Switch channel. - Press Shift to switch the input method.

3. Device Installation

All the installation and operations here should conform to your local electric safety rules.

3.1 Inspecting NVR box contents

After you receive the NVR in its original package, please verify whether there is any visible damage or missing items. The protective materials used for the package of the NVR can protect against most accidental damages during transportation. Before installation, open the included accessories box to verify the contents included with the NVR. When finished, you can remove the protective film off the NVR.

If your unit was purchased with a preinstalled HDD verify cables are still connected correctly. See the HDD Installation section below for reference.

3.2 Product Label

The model and Serial number located on the sticker on the bottom or on the rear side of the NVR is important. Make sure the product label is protected from damage.

Verify according to your purchase order you have received the correct product.

If the label is damaged this could result in your warranty getting void.

3.3 HDD Installation

For first-time installation, make sure the unit is powered down and you are properly grounded. We recommend using enterprise-level or surveillance level Hard Drives. **It is not recommended to use PC HDD or SSD.**

3.3.1 1U Series

Step 1 Loosen the screws of the rear panel and side panel.

Figure 3-12

Step 2 Place the HDD in relation to the four holes in the bottom.

Figure 3-13

Step 3 Turn the device upside down and then tighten the screws firmly. This will secure the HDD on the chassis.

Figure 3-14

Step 4 Connect the HDD cable and power cable.

Figure 3-15

Step 5 Replace the cover in line with the clips and then install the screws on the rear panel and side panel.

Figure 3-16

3.3.2 1.5U Series

Step 1 Use the screwdriver to remove the screws of the rear panel and then remove the front cover.

Figure 3-17

Step 2 Place the HDD to the HDD bracket in the chassis and then line up the four screws to the four holes in the HDD. Use the screwdriver to install the screws to secure the HDD on the HDD bracket.

Figure 3-18

Step 3 Connect the HDD SATA cable to the mainboard and the HDD port respectively. Locate the power cable for the HDD and connect the cable to the HDD.

Figure 3-19

Step 4 After connecting the cables, replace the front cover to the NVR and then install screws on the rear panel.

Figure 3-20

3.3.3 General 2U Series

Step 1 Use the screwdriver to remove the screws of the rear panel and then remove the front
cover.

Figure 3-21

Step 2 Place the HDD to the HDD bracket in the chassis and then line up the four screws to the
four holes in the HDD. Use the screwdriver to install the screws firmly to secure the HDD
on the HDD bracket.

Figure 3-22

Step 3 Connect the HDD data cable to the mainboard and the HDD port respectively.
Find the power cable for the HDD and connect another end of the power cable to the
HDD port.

Figure 3-23

Step 4 After connecting the cable, replace the top cover back on the NVR and then install screws on the rear panel.

Figure 3-24

3.4 Connection Examples

3.4.1 NVR-MX, NVR-FX and NVR-7516K Series

Figure 3-1
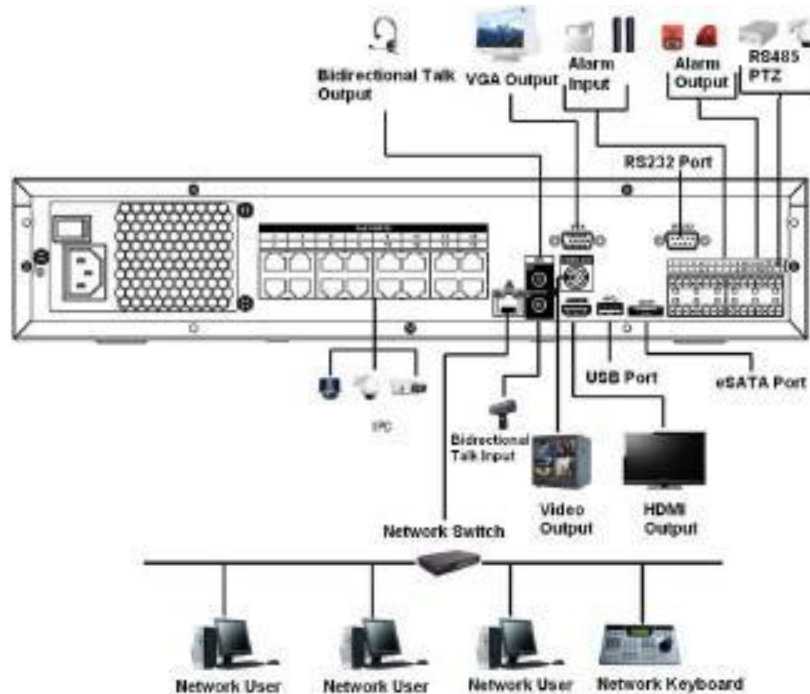
Note:
- Cameras plugged into NVR built-in Poe should only be set to DHCP. The NVR POE will mac bind and address these cameras automatically to a 10.1.1.x by default.
- Only one camera per POE port. **Do not use an external switch on the built-in POE**.
- Cameras using external switches are to be set on static IP, matching the local network IP scheme.

- Multidirectional cameras with multiple independent lenses are not supported on the built-in POE.

3.4.2 NVR-EL Series

Figure 3-2
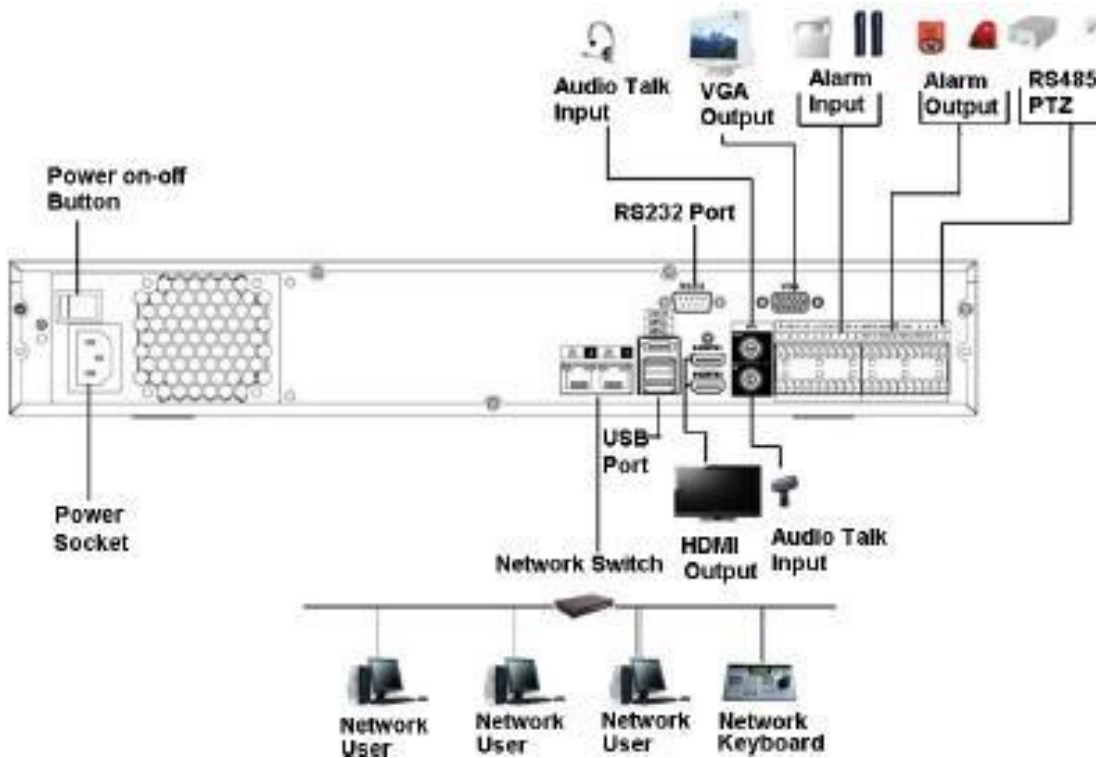
Note:
- The NVR EL series comes equipped with dual network ports.
- Network port 1 (default network port) is typically plugged into a local network with a local IP scheme.
- Network port 2 can be set to a different IP scheme than network port 1. IP cameras are recommended to be set on static to the same IP scheme as network port 2 and plugged into a switch that is connected to network port 2 to isolate cameras.

4 Local Basic Operation

Slight differences may be found on the user interface. The following figures are for reference only.

4.1 Getting Started

This chapter introduces device initial settings such as boot-up, device initialization, reset the password, and Startup Wizard.

4.1.1 Booting up

⚠️

- For device safety, connect the NVR to the power adapter first and then connect the device to the power socket.
- Make sure the supplied rated input voltage matches the device power specifications.
- Make sure the power wire cable and source are in good condition.
- Always use a stable current, if necessary a UPS is a good alternative measure.

    <u>Step 1</u>   Connect the device to the monitor and then connect a mouse.

    <u>Step 2</u>   Connect the power cable.

    <u>Step 3</u>   Click the power button at the front or rear panel and then boot up the device.

After the device has booted up, the system will display multiple-channel mode by default.

4.1.2 Device Initialization

If it is your first time using the device, set a login password for **admin** (system main administrator user). You can select to use unlock pattern to log in or not at your own choosing.

📖

For your device security, properly secure your login password of **admin** steps, and change the password regularly.

<u>Step 1</u>   Power on your NVR. The **Device Initialization** interface will be displayed upon first time boot up. See Figure 4-2

Figure 4-2
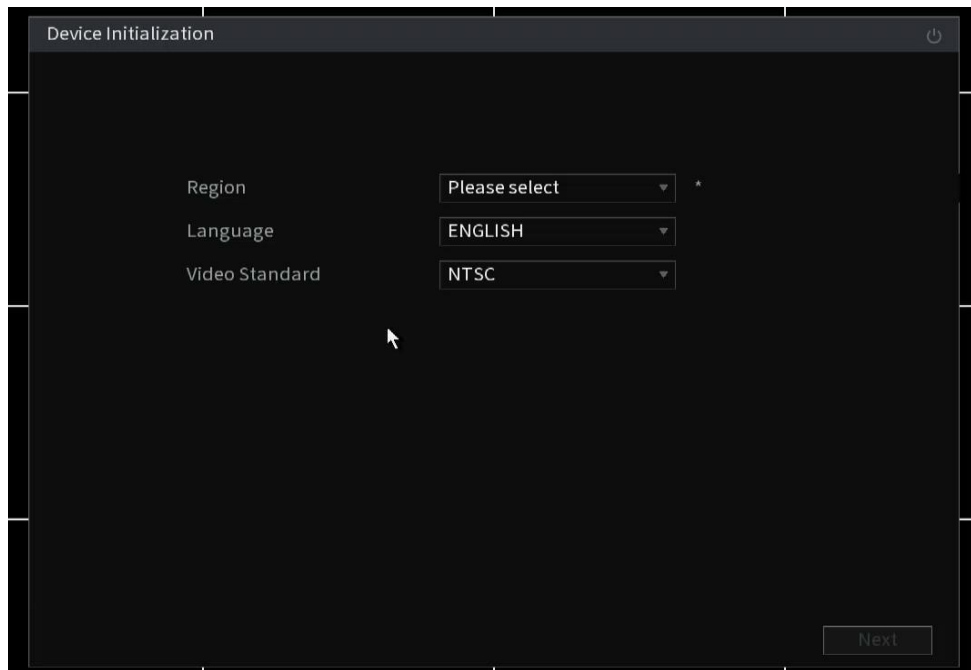
<u>Step 2</u>　Set Region, Language and Video Standard (NTSC for North America).

If you click in the region field, an on-screen keyboard will be displayed. You can type your region instead of looking through the list.

<u>Step 3</u>　Set login password for **admin**. Select Next when done. See Table 4-1 for parameters.

Figure 4-3
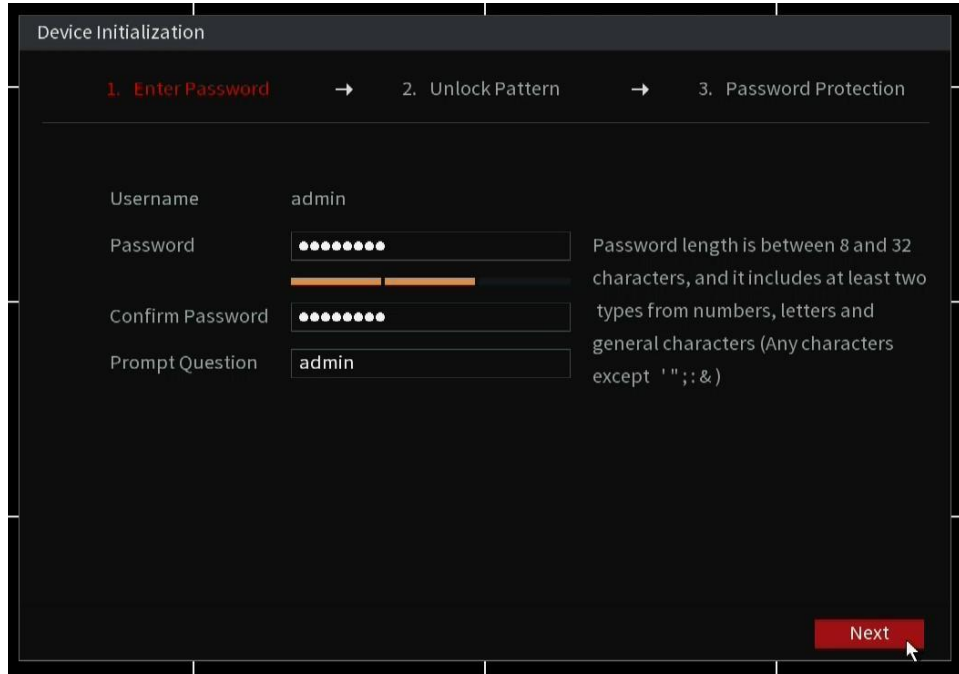
Table 4-1

Parameter	Description
User	By default, the user is admin.
Password	In the **Password** box, enter the password for admin.
Confirm Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding"'", """, ";", ":" and "&").
Prompt Question	In the **Prompt Question** box, is a hint to the admin password. Not recommended to put the actual password. On the login screen, click the lock icon next to the password field to display the password hint

⚠️

For your device's own safety, create a strong password of your own choosing. We also recommend you change your password periodically especially in a high-security environment.

Step 4   Set Unlock Pattern as desired or skip. See notes below Figure 4-4 for details.

Figure 4-4

📖

- To set the unlock pattern by left click the starting point and hold as you draw the pattern. Let go when Done. It will ask you to confirm the pattern by drawing it again.

- The created pattern must cross at least four grids.
- The unlock pattern is only usable at the unit's head end. You will still need the written password for remote methods.
- If you do not want to configure the unlock pattern, click **Skip**.
- Once you have configured the unlock pattern, the system will require the unlock pattern as the default login method. If you skip this setting, enter the password for login.

Figure 4-5
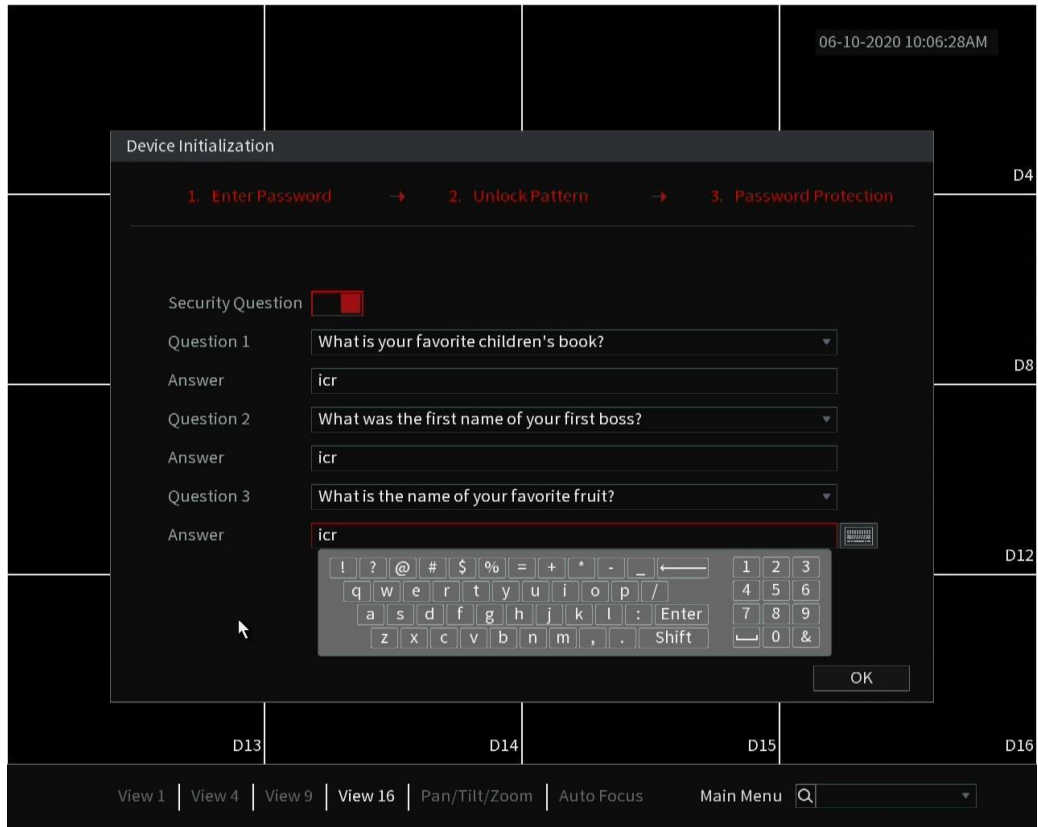
Step 7   Set **Password Recovery** questions. See Table 4-2.

📖

- After configuration, if you forgot the password for the admin user, you can reset the password through the security questions. For details about resetting the password, see "4.1.3 Resetting Password".

- If you do not want to configure the settings, disable the security questions function on the interface. If this is skipped and your password is lost in the future you will need to submit a "Forget My Password" form or contact IC Realtime customer support.

Table 4-2

Password Protection Mode	Description
Security Questions	Configure the security questions and answers. The answers can be the same. ie: Name of company If you forget the password, enter the answers to the questions can allow you reset the password. Refer to "4.15.3 Reset Password" for detailed information.
Customer Support	Contact your original installers or submit a "Forgot My Password (FMP)" Request to IC Realtime. **FMP Instructions:** Go to: https://icrealtime.com/support and click on Password Reset. You will recieve a temporary access code that is only usable directly on the local machine. The code will **NOT** work via a web browser or remote software. Once you enter the temporary access code using the username "**admin**" you will be prompted to create a new password.

Step 8   Click **Save** to complete the device initialization setup.

Step 9   Configure via the startup wizard. Refer to "4.1.4 Startup Wizard" for

detailed information.

4.1.3 Resetting Password

You can reset the password by the following methods when you forgot the password for the **"admin"** account.

- If the password is lost or forgotten, you have two options:
    - ◇ If you configured security questions, you can reset the password by filling the answers for the security questions. You will be prompted to set the new password upon entering the correct answers.
    - ◇ If you did not configure the security questions, you will need to fill out a password reset request form.
        - • Go to: https://icrealtime.com/fmp and click on Password Reset.
        - • You will be provided with a code to be used at the headend of the unit.
            - • This code will not work via the web browser or other remote connections.
            - • The code is only valid for the given calendar day.
        - • On the local monitor of your unit Right click on the screen and select Main Menu. Upon Log in select the username "**admin**".
        - • Enter the 6 digit code provided.
        - • You will be prompted to set your new password and confirm your desired password.
    - ◇ Some units will have a hard reset button. See section 4.1.3.3.

4.1.3.1 Enabling Password Reset Function (If Available)

After enabling the password reset function, you can use the forgot password function on the local menu to reset the password by answering the security questions.

Step 1   Select **Main Menu** > **Advanced Settings** > **Users** > **Password Reset**.
             The **Password Reset** interface will be displayed. See Figure 4-6.

Figure 4-6
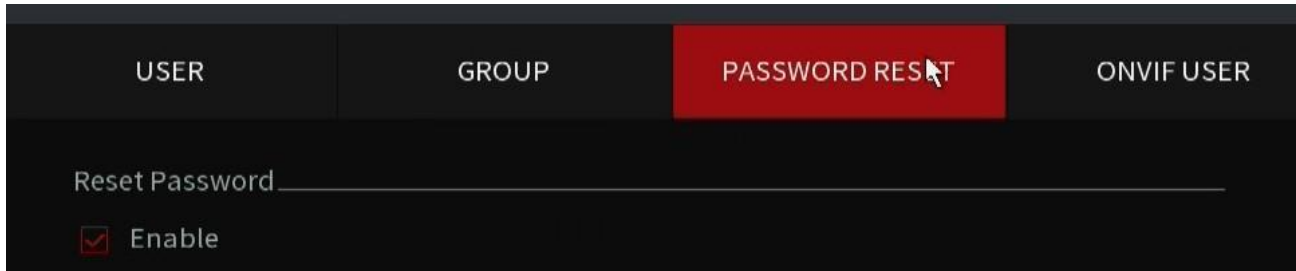
Step 2   Fill in the answers to the security questions.
Step 3   Click **Apply** to set settings.

4.1.3.2 Resetting Password on Local Interface with Security Questions

Step 1   Enter the **Login** interface.
- If you have configured the **unlock pattern**, the unlock pattern login interface will be displayed. Click **Forgot Pattern**, the password login interface will be displayed. See Figure 4-7.
- If you did not configure unlock pattern, the **Login** interface will be displayed. See Figure 4-7.

📖

To login using another user account, on the unlock pattern login interface, click **Switch User**, or on the password login interface, in the **Switch User** list, select another user to login.

Figure 4-7
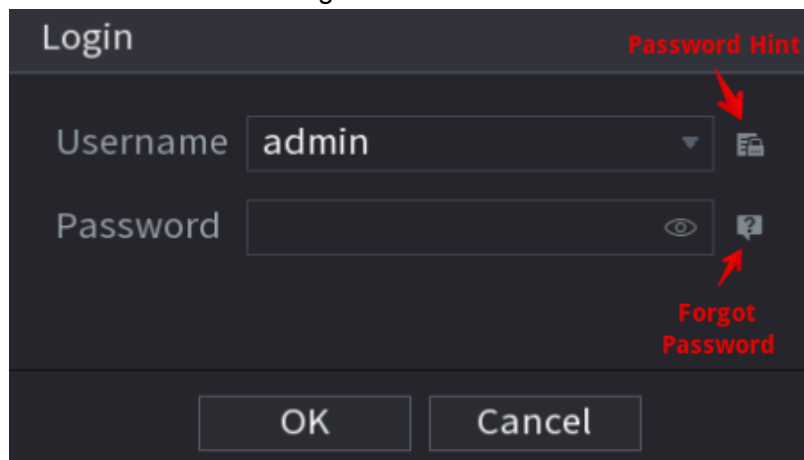
Step 2   Click on Forgot Password. See Figure 4-7
Step 3   Fill in the answers to the Security Questions that was previously set.
Step 4   Click **Next**.

The **Reset Password** interface will be displayed. See Figure 4-13.

Figure 4-13

Step 6   In the **New Password** box, enter the new password and enter it again in the

Confirm Password box.

Step 7   Click **OK** to save your new password
Step 8   A pop-up window appears asking if you want to sync the password with the remote
devices. See Figure 4-14.

⚠ The synchronize function only works on IC Realtime cameras with 2018 firmware or
newer. Third party cameras or older cameras passwords will not update correctly. Use
with caution.

Click **OK** to synchronize the password to the IP Cameras or click **Cancel** to not

update cameras to new password set.

Figure 4-14

4.1.3.3 Factory Reset Button (If Applicable)

Some units may have the reset button located on the motherboard to reset the Device to the factory default settings. This function should only be done by qualified technicians.

Step 1   Disconnect the Device from the power source, and then remove the cover panel. For details about removing the cover panel, see "3.4 HDD Installation".

Step 2   Find the reset button on the mainboard, and then connect the Device to the power source again.

Step 3   Press and hold the reset button for 30 seconds. See Figure 4-15 for the location of the reset button.

Figure 4-15
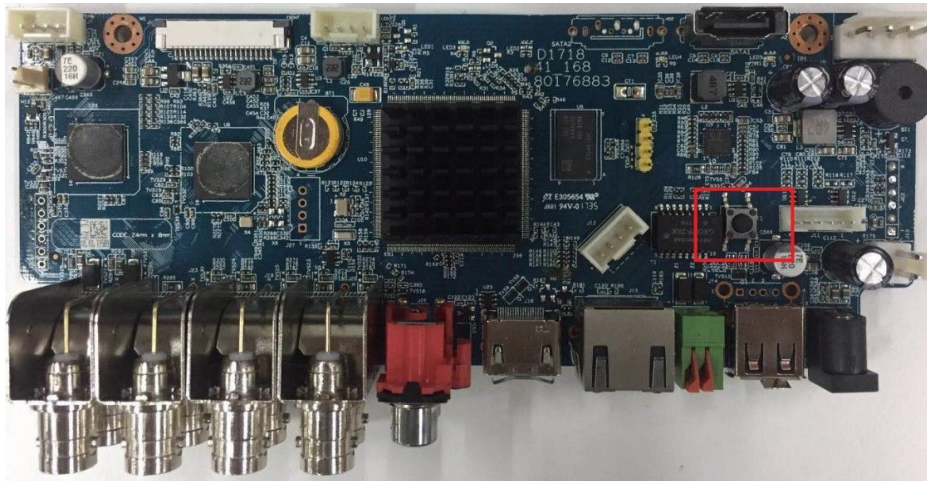
Step 4   The Device will reboot and all settings will be erased and set back to factory default.

4.1.4 Startup Wizard

After you have successfully initialized the device, the startup wizard will appear. Here you can quickly configure your device. Click **Next**, to navigate to the **General** interface.

The startup wizard interface only displays after you first login the device and setup the admin password. See Figure 4-16.

Figure 4-16 Startup wizard
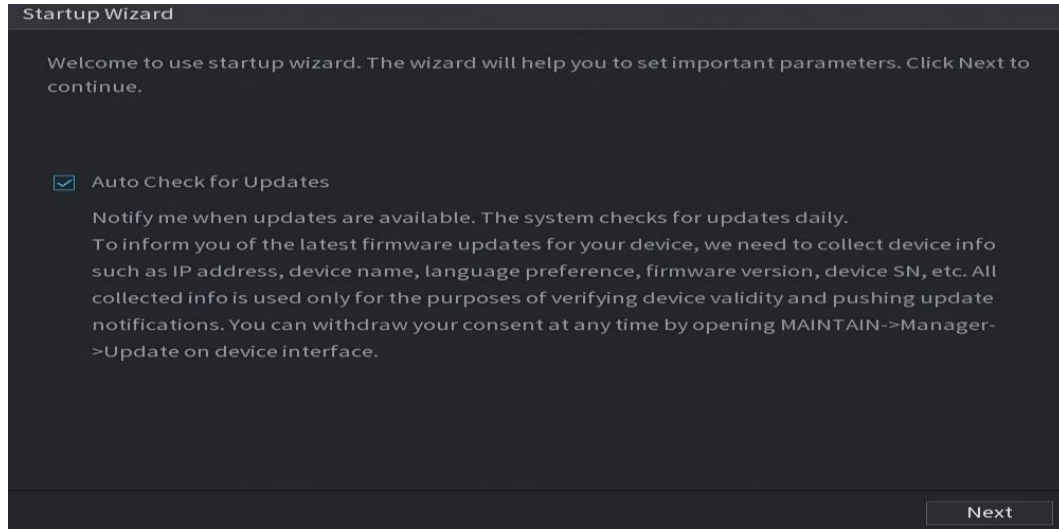
○
- ● If you select the **Auto Check for Updates** check box, the system will notify you automatically when updates are available.
- ● After the auto-check function is enabled, the system will collect information such as IP address, device name, firmware version, and device serial number. The collected information is only used to verify the legality of the Device and push upgrade notices.
- ● If you cancel the **Auto Check for Updates** check box, the system will not perform automatic checks.

4.1.4.1 General Settings

Configures the NVR basic information such as system date, holiday and etc. You can also configure general settings by selecting:

Main Menu > **Advanced Settings** > **System Operation**> **General**.

4.1.4.1.1 General

Configures the device's basic information such as device name, language, etc.

The **Basic** interface will be displayed. See Figure 4-17.

Figure 4-17: Basic settings

Step 1   Set parameters. See Table 4-3.

Table 4-3 Basic parameters

Parameter	Description
Device Name	In the **Device Name** box, enter the Device Name.
Device No.	This number will correspond to IR remote control addressing.
Language	In the **Language** list, select a language for the Device system.
Video Standard	In the **Video Standard** list, select **PAL** or **NTSC** according to your actual situation.
Sync Remote Device	Enable this function; the NVR can synchronize information with the remote devices such as Language, video standard, time zone.
Instant Playback	In the **Instant Play** box, enter the time length for playing back the recorded video. The value ranges from 5 to 60. This feature may not be available in some units.

Parameter	Description
Logout Time	In the **Auto Logout** box, enter the idle time for the Device. The Device automatically logs out when it is not been operated for the given time period. You will need to log in to the Device again. The value ranges from 0 to 60. If set to "0" the system will not log out once logged in automatically unless the unit power cycles. **Monitor Channel(s) when logout**. You can select the channels that you want to continue monitoring when users are logged out.
IPC Time Sync	Syncs the Device time with IP camera.
IPC Time Sync Interval	In the **Interval** box, enter the interval for time sync.
Navigation Bar	Enable the navigation bar. When you click on the live view screen, the navigation bar will be displayed.
Mouse Sensitivity	Adjust the speed of double-click by moving the slider. The greater the value is, the faster the speed will be.

Step 2   Click **Apply** button to save settings.

4.1.4.1.2 Date and Time
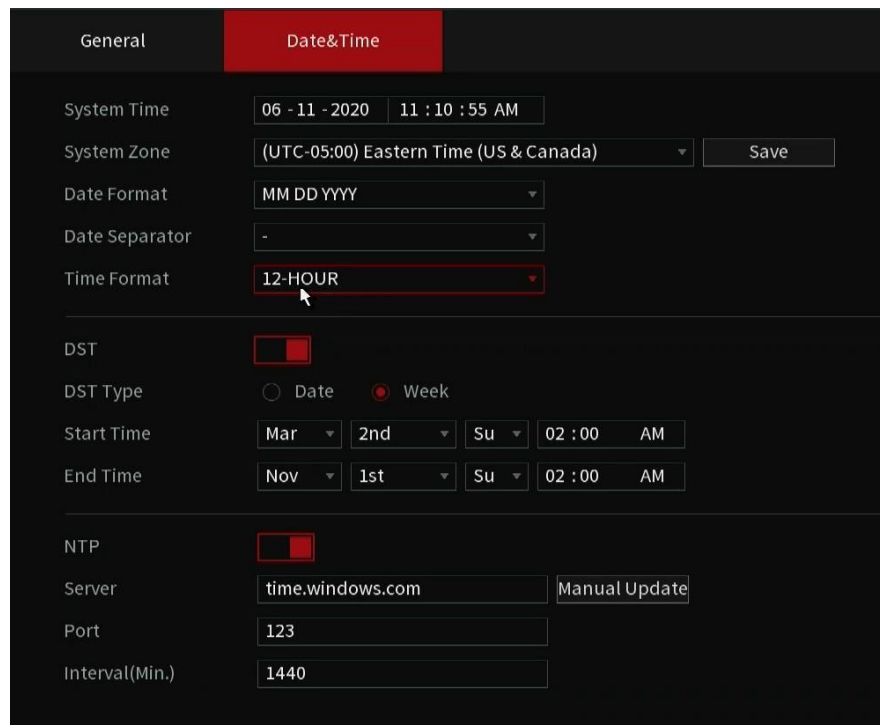
Configures system's time. You can enable NTP (Network Time Protocol) function so that the device can sync time with the NTP server. NTP is enabled by default.
You can also configure date and time settings at a later time by selecting
Main Menu > A**dvanced Settings > System Operation> General** > **Date&Time**.

Step 1   Click the **Date & Time** tab. See Figure 4-18.

Figure 4-18

Step 2   Configure the settings for date and time parameters. See Table 4-4.

Table 4-4 Data and time parameters

Parameter	Description
System Time	In the **System Time** box, enter time for the system. Click the time zone list, you can select a time zone for the system, and the time in adjusts automatically. ⚠ Do not change the system time randomly; otherwise, the recorded video cannot be searched properly. It is recommended to avoid the recording period or stop recording first before you change the system time.
Time Zone	In the **Time Zone** list, select a time zone for the system.
Date Format	In the **Date Format** list, select a date format for the system.
Date Separator	In the **Date Separator** list, select a separator style for the date.
Time Format	In the **Time Format** list, select **12-HOUR** or **24-HOUR** for the time display style.
DST	Enable the Daylight Saving Time function if you are in an area that observes DST. Click **Week** or click **Date** for DST type. ⚠ It is **recommended** to use **Week** as the actual date of DST changes each year. The systems are programmed with the correct DST week settings by default simply just select enable.
Start Time	Configure the start time and end time for the DST.
End Time	
NTP	Enable the NTP function to sync the Device time with the NTP server. ⚠ If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the **Server Address** box, enter the IP address or domain name of the corresponding NTP server. Click **Manual Update**, the Device will sync with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the **Interval** box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

4.1.4.2 Basic Networking Settings

Configure the device's IP address, DNS (Domain Name System) information. You can also configure basic network settings by selecting **Main Menu** > **Basic Settings> NETWORK** > **TCP/IP**.

Make sure the device is properly connected to a network.
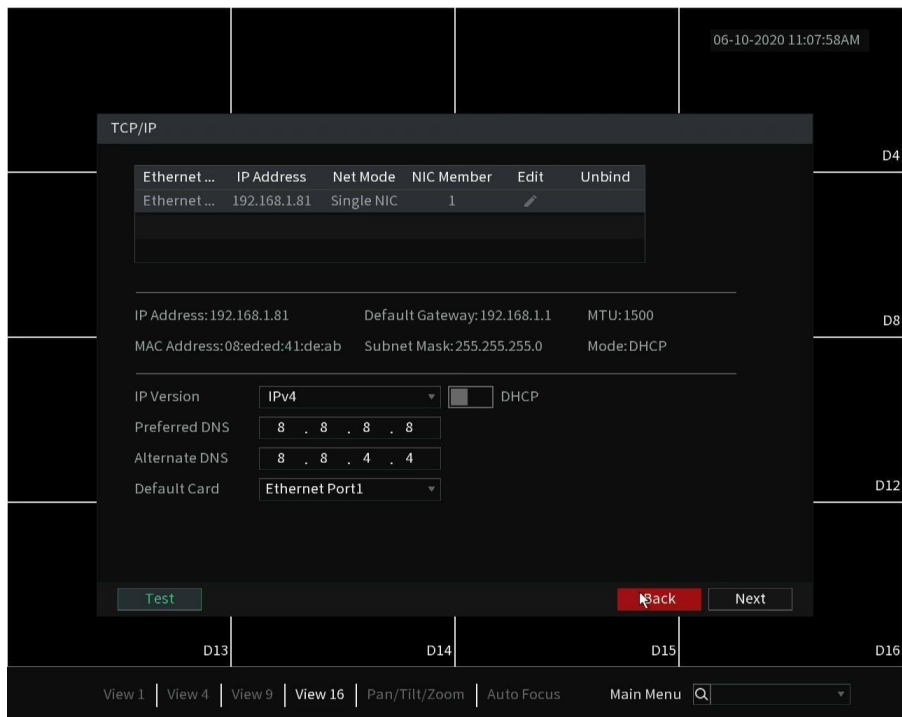It is recommended to use DHCP allowing the system to pull automatically.

The **TCP/IP** interface will be displayed. See Figure 4-21.

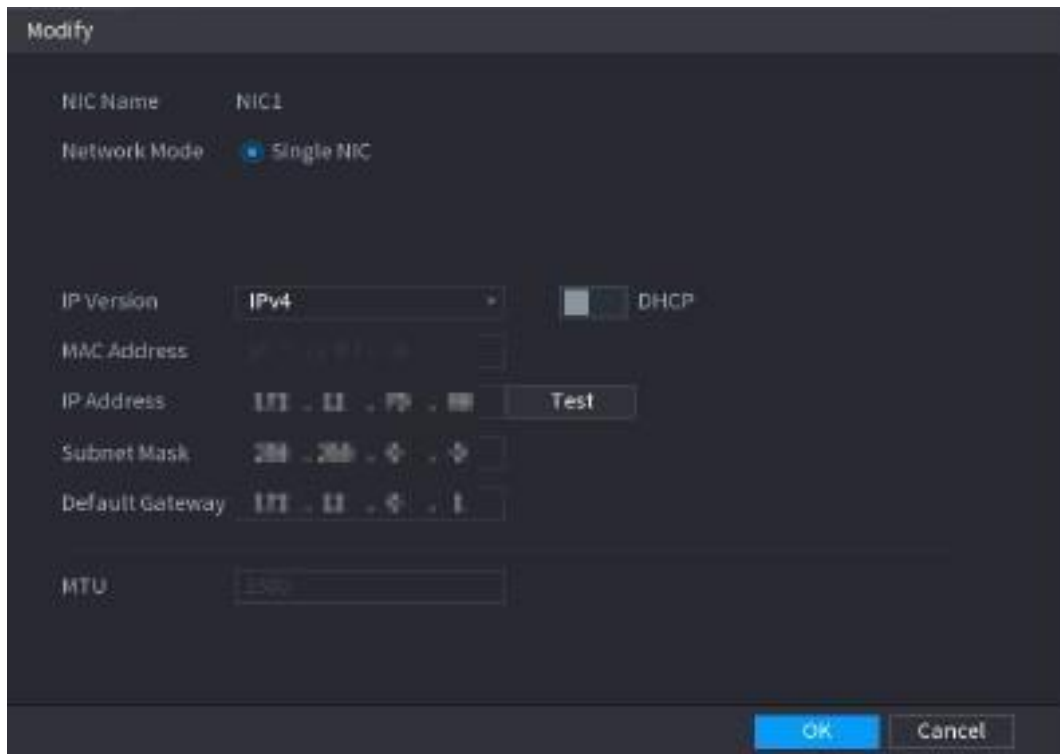Different model NVRs have different Ethernet adapter amounts and types.
Refer to the actual datasheet.

Figure 4-21

Step 1   Click 📝 to modify network settings. The **Modify** interface will be displayed.

Figure 4-22

Step 3   Set parameters. See Table 4-5

Table 4-5

Parameter	Description
Network Mode	● **Multi-address**: Two Ethernet ports work separately through either of which you can request the Device to provide the services such as HTTP and RTSP. you will need to configure a default Ethernet port (usually the Ethernet port 1 by default) to request the services from the device end such as DHCP, Email, and FTP. 📖 If one of the two Ethernet ports is disconnected as detected by networking testing, the system network status is regarded as offline. ● **Fault Tolerance**: Two Ethernet ports share one IP address. Normally only one Ethernet port is working and when this port fails, the other port will start working automatically to ensure the network connection. 📖 When testing the network status, the network is regarded as offline only when both of the two Ethernet ports are disconnected. The two Ethernet ports are used under the same LAN. ● **Load Balance**: Two network ports share one IP address and they are working at the same time to share the network load. If one of them fails, the other can continue working. 📖 When testing the network status, the network is regarded as offline only when both of the two Ethernet ports are disconnected. The two Ethernet ports are used under the same LAN.
Default Ethernet Port	In the **Ethernet Card** list, select an Ethernet port as a default port. This is typically the **port going to the local network.** This setting is available only when the **Multi-address** is selected in the **Net Mode** list.
IP Version	In the **IP Version** list, you can select **IPv4** or **IPv6**. Both versions are supported for access.
MAC Address	Displays the MAC address of the Device.

Parameter	Description
DHCP	Enable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. ● If DHCP is valid, the obtained information will display in the **IP Address** box, **Subnet Mask** box, and **Default Gateway** box. If not, all values show 0.0.0.0. ● If you want manually configure the IP information (static), disable the DHCP function. ● If the PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway.
Subnet Mask	
Default Gateway	IP address and default gateway must be in the same network segment.
DNS DHCP	Enabling DHCP function to get the DNS address from the router.
Preferred DNS	In the **Preferred DNS** box, enter the IP address of DNS.
Alternate DNS	In the **Alternate DNS** box, enter the IP address of the alternate DNS.
Test	Click **Test** to test if the entered IP address and gateway are interworking.

Step 4   Click **OK** to go to NIC settings. Navigate to the **TCP/IP** interface.

Step 5   Set network parameters. See Table 4-6.

Table 4-6

Parameter	Description
IP Version	There are two options: IPv4 and IPv6. The system supports these two IP address formats
Preferred DNS server	DNS server IP address.
Alternate DNS server	DNS server alternate address.
MAC Address	Displays the MAC address of the Device.
DHCP	Enable/disable the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. ● If DHCP is valid, the obtained information will display in the **IP Address** box, **Subnet Mask** box and **Default Gateway** box. If not, all values show 0.0.0.0. ● If you want manually configure the IP information, disable the DHCP function first. ● If PPPoE is enabled and is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.

4.1.4.3 P2P

P2P is used for easily viewing your system remotely. It can be used with our Desktop Software called SmartICRSS or it can be used on our mobile apps called IC View or ICRSS Pro.

To use this feature simply make sure it is enabled and the unit has an internet connection.

On your remote device (Cellphone or Computer) open our application. Go to the Device menu and register a new device via the P2P method. Either manually type in the SN (Serial Number) of your unit or scan the generated QR code from the menu. Enter your systems credentials and you are done.

Before using the P2P function, make sure that the NVR has connected to the internet.
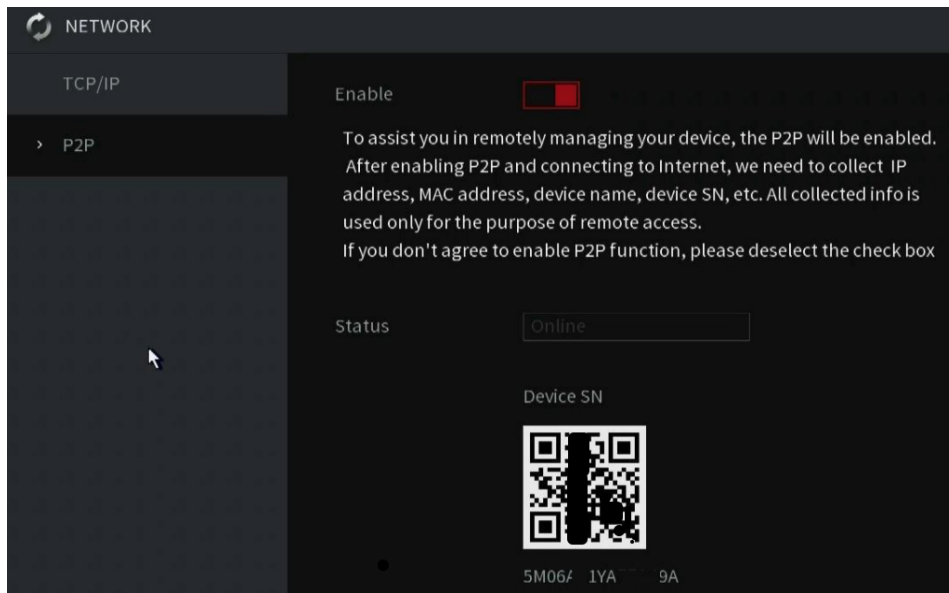
4.1.4.3.1 Local Operation

The **P2P** interface will be displayed in the wizard after the Network IP settings. Or you can manually navigate to the menu. See Figure 4-23 for P2P interface.

Select **Main Menu** > **Network** > **P2P**, to navigate to the **P2P** interface.

Figure 4-23

Step 1   Check the box to enable P2P function.

After the P2P function is enabled and connected to the Internet, the system will collect your information for remote access, and the information includes but not limited to email address, MAC address, and device serial number.

Step 2   Click the **Apply** or **Next** button to complete setup.

The status is online if the P2P registration is successful and has internet connectivity.

4.1.4.3.2 Mobile App Registration

You can find these same steps in a video on our YouTube channel or on our support center.

YouTube Link: https://www.youtube.com/c/ICRealtimeOfficial

Help Center: https://www.icrealtime.com/support

Step 1   On your mobile device, go to the app store and download IC View or ICRSS Pro.

Step 2   On your cell phone, open the application and then tap the **Home** icon at the top left.

Step 3   The home menu will be displayed. Follow the steps below to add your unit.

1) Tap the **Device Manager** at the bottom of the screen.
   The **Device Manager** interface will be displayed. See Figure 4-24.

Figure 4-24 Device manager
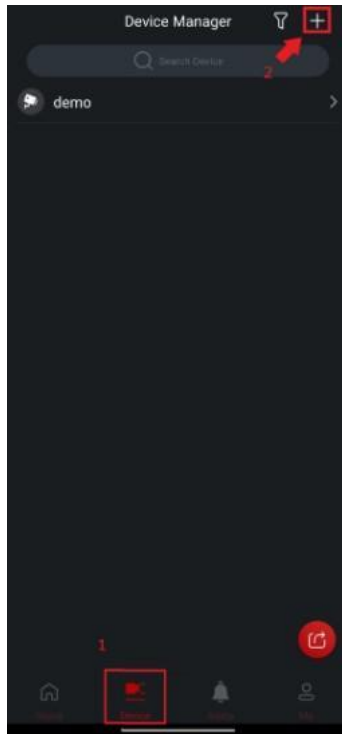
2) Tap (+) icon in the top right corner.

3) Tap **P2P/SN** from the drop-down list.
   You will need to allow permissions to allow the phone app to use the phone camera. Use the camera to scan the QR Code.

4) Scan the QR code from your unit's interface or select **Manually Enter SN** which will allow you to manually type out the SN of the unit. See Figure 4-25.

Figure 4-25
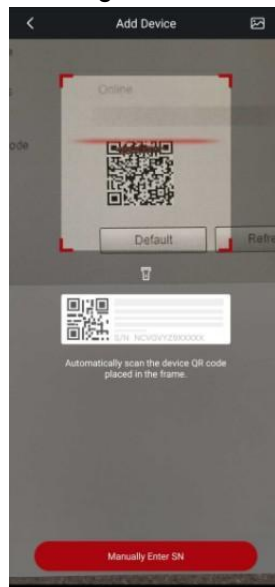
5) Fill in Device Information

Scanning the QR Code will fill out the SN. Enter a name (anything) and then enter the correct username and password for the NVR. See Figure 4-26.

Figure 4-26

6) Tap **Start Live Preview** or **Save** at the bottom.

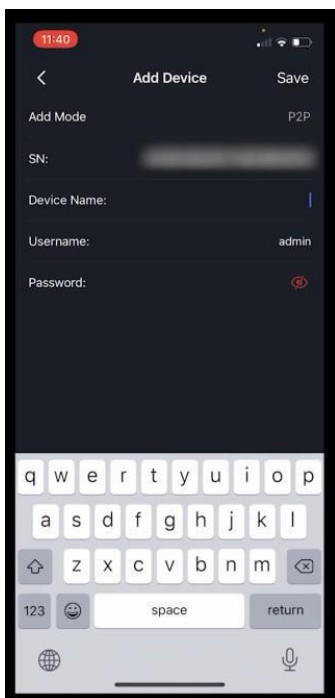The Device is added and displayed on the live view interface of the cell phone.

See Figure 4-27.

Figure 4-27

4.1.4.4 Adding Camera

After adding a remote camera, the NVR can receive, store, and manage the video streams of the remote device. You can view, browse, playback, and manage several remote devices at the same time.

IC Realtime cameras plugged into a recorder with a built-it POE have autoregistration. It will automatically add the cameras to the recorder. If the camera hasn't been activated previously it will set the camera's admin password to the same as the system's admin password.

Step 1 If on the **P2P** interface of the Wizard, click **Next**. Otherwise, go to **Main Menu > Advanced Settings> Camera Configuration> Add/Remove Device.**

The **Add/ Remove Device** interface will be displayed. See Figure 4-28

Figure 4-28

Step 2 Register remote device. IC Realtime cameras plugged into the built-in POE of a recorder will automatically register to the system.

Search and then add

1. Click **Search**.

   The devices found are displayed at the upper pane. You may need to initialize new cameras.

2. Double-click a remote device, or select a remote device and then click **Add** to register it to the **Added Device** list. ***This will add the camera using the NVR credentials**. See Figure 4-29.

3. Set parameters. See Table 4-7.

Figure 4-29

Table 4-7

Parameter	Description
Uninitialized	Enable/disable the **Uninitialized** filter. When searching for devices the list will filter all activated/initialized devices from the list.
Initialize	Used to activate/initialize new cameras that have yet to be activated and set with an admin password. Cameras need to be activated before being able to use them like a recorder. **Usage:** Select the uninitialized device from the device search list (use the uninitialized filter to simplify the list), and then click **Initialize** to start initializing the device.
Filter	In the **Show Filter** list, select the remote device type that you want to display in the searched device list. ● **None**: Display all types of devices. Recommended filter. ● IPC: Display the front-end devices such as IPCs. ● DVR: Display all storage devices such as NVR, DVR, and HCVR. ● OTHER: Display the devices that do not have the IPC or DVR device type. Specialty cameras like thermal cameras or 3rd party cameras will be set to Other for type. In some cases, some IC Realtime cameras will show up as Other as well.
Searched Device List	Displays the searched devices. You can view the device information such as status, IP address.
Search	Click **Search**, the searched devices display in the searched device list. To adjust the display sequence, in the title line, you can click the IP address, Manufacturer, Type, MAC Address, Port, or Device Name text. For example, click the IP address text, the sequence icon IP Address ▲ will be displayed.
Add	In the Searched Device List area, select the device that you want to add.

Manual Add	Add the device by manually configuring settings such as IP address, credentials and channel selection.
Added Device List	Displays the added devices. You can edit and delete the device, and view the device information.
Delete	Select the check box of the added device, and then click **Delete** to delete the added device.
Import	Select the searched devices and then click **Import** to import the devices from a USB storage device.
Export	Select the added devices and then click **Export**. The exported devices information is saved into the USB storage device.

- Manual Add is used to manually configure connection information. This should be used when the admin password is different from the recorder's admin password.
  1. Click **Manual Add**.
     The **Manual Add** interface will be displayed. See Figure 4-30.

Figure 4-30

  2. Configure parameters. See Table 4-8.

Table 4-8

| Parameter	Description
Channel	In the **Channel** section, select the channel that you want to remote device to occupy on the NVR. It will register the device to the next available channel.
Manufacturer	In the **Manufacturer** list, select the manufacturer of the remote device. Select "**Private**" for IC Realtime devices. Select **Onvif** for 3rd party cameras. Select **Custom** or General to add device via **RTSP** stream. RTSP URLs will differ between manufacturers. Consult 3rd party manufacturers for proper RTSP strings.
IP Address	In the **IP Address** box, enter the IP address of the remote device. 📖 The default is 192.168.0.0 which the system cannot connect to as it is not a valid address.
TCP Port	The default value is 37777 (TCP port for private protocol). You can enter the value depending on the IPC manufacturer.
User Name	Enter the user name of the remote device.
Password	Enter the password of the user for the remote device.
Remote CH No.	Enter the remote channel number of the remote device that you want to add (extra channels on camera or recorder)
Decoder Strategy	In the **Decoder Strategy** list, select **Default**, **Realtime**, or **Fluent**.
Protocol Type	● If the remote device is added through the private protocol, the default type is **TCP**. ● If the remote device is added through ONVIF protocol, the system supports **Auto**, **TCP**, **UDP**, or **MULTICAST**. ● If the remote device is added through other manufacturers, the system supports **TCP** and **UDP**.
Encrypt	If the remote device is added through Onvif protocol, selecting the **Encrypt** check box will provide encryption protection to the data being transmitted. 📖 To use this function, the HTTPS function should be enabled for the IP camera.

3. Click **OK**.

The remote device information will be displayed on the **Added Device** list.

Step 3   Click **Next** to complete the remote device registration. See Figure 4-31

Figure 4-31.
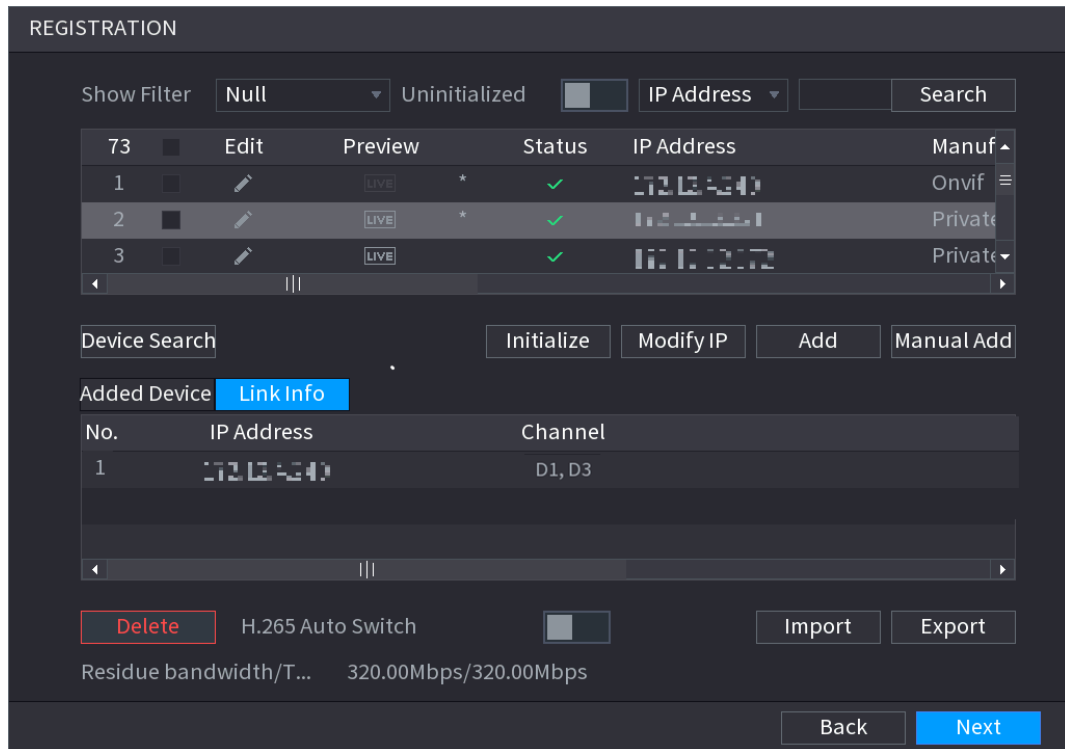
4.1.4.5 RAID Manager

RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for the purposes of data redundancy, performance improvement, or both. Not all NVRs have this feature.

RAID function is for some series products only. A slight difference may be found in the user interface.

When setting HDDs in a RAID array make sure to set a hotspare.

All data on the HDDs will be deleted when creating or removing a RAID group.

It is recommended to have your HDDs placed into multiple RAIDs instead of one large RAID. In the table below the number without "()" represents the disk number of the RAID group. The number with () represents the number of global hot spare disks. For example, for 24 HDD, the setup strategy is 7+7+9+(1). It means three RAID 5 and one hot spare, and each RAID 5 respectively contains 7 disks, 7 disks, and 9 disks.

It is recommended that you have 1 hot spare per RAID group. In the event, the 1 hot spare is being used for another RAID group that had a drive fail if a drive fails in the 2nd or 3rd RAID group but no hot-spare that group will be rendered inactive until issues are resolved.

HDD No.	Creation Strategy	HDD No.	Creation Strategy
3	Not recommended	14	6+7+(1)
4	Not recommended	15	7+7+(1)
5	5	16	5+5+5+(1)
6	5+(1)	17	5+5+6+(1)
7	6+(1)	18	5+6+6+(1)
8	7+(1)	19	6+6+6+(1)
9	8+(1)	20	6+6+7+(1)
10	9+(1)	21	6+7+7+(1)
11	5+5+(1)	22	7+7+7+(1)
12	5+6+(1)	23	7+7+8+(1)
13	6+6+(1)	24	7+7+9+(1)

RAID is no substitute for scheduled backup!

All RAID levels except RAID 0 offer protection from a single drive failure. A RAID 6 system even survives 2 disks dying simultaneously. For complete data security, you still need to back up the data from a RAID system.

Step 1 Select the desired HDDs for the array in the **RAID** interface. See Figure 4-32.

Figure 4-32
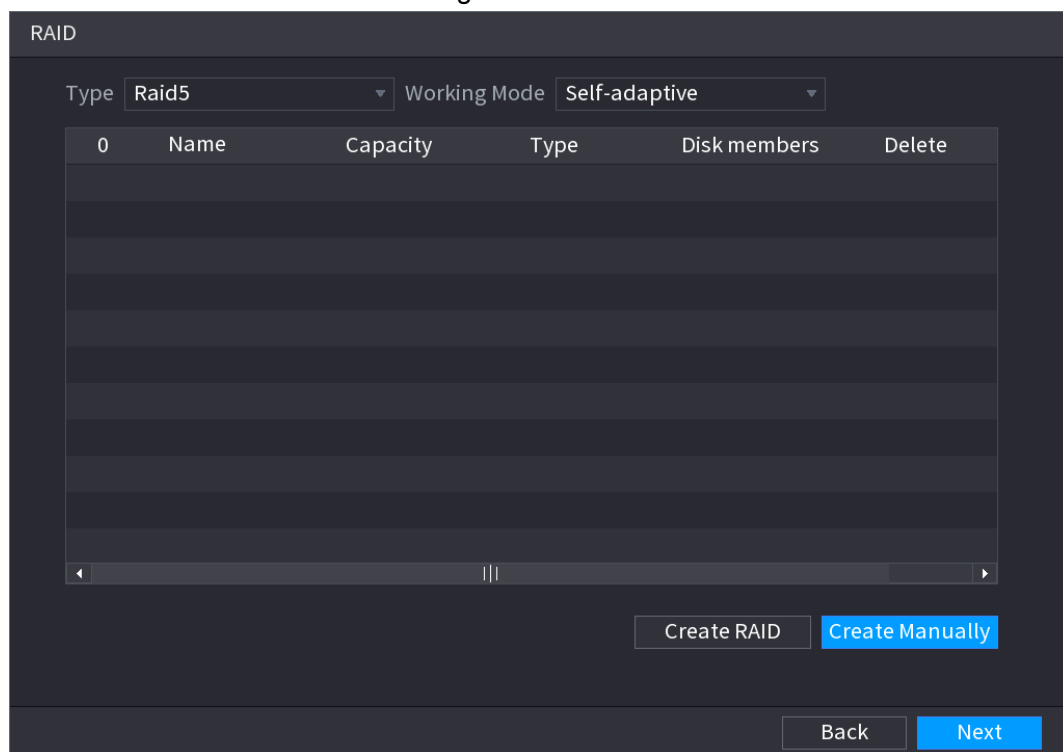
Step 3   You can click **Create RAID** or **Create Manually***, and all the disks involved will be formatted.

- Click **Create RAID**, the system will create RAID automatically.
  - ◇ If there is no existing RAID and no hot spare disk, the system will create RAID5 and a hot spare disk automatically.
  - ◇ If there is no existing RAID, but an existing global hot spare disk, the system will only create RAID5 and use the existing hot spare disk automatically.

    If there is an existing RAID and an existing hot spare disk, the system will delete the original RAID and create RAID5 with all the disks and use the existing hot spare disk automatically.
- Click **Create Manually***.

⚠ Creating a RAID manually may result in an illegal RAID group. This should only be used by advanced users. ICRealtime is not liable for any data loss or issues caused by illegal RAID sizes.

  1. Select RAID type and disks as the system instructed.
  2. Click **Create Manually**, and then the format disk notice will be displayed.
  3. Click **OK**.

Step 4   After creating RAID, the disks need to sync with each other to finish the process. For RAID5 and RAID6, you can select different working modes.

- Self-Adaptive: Automatically adjust the RAID sync speed according to the business status.
- Sync First: Resource priority is assigned to RAID sync.
- Business First: Resource priority is assigned to business operations.
- Balance: Resource is evenly distributed to RAID sync and business operations.

4.1.4.6 Schedule

After setting the record schedule and snapshot schedule, the device can automatically record video and snapshot images based on a specific schedule for each channel.

By default, the NVR records 24/7 regular continuous recordings. To record motion or IVS you will need to edit the schedule for each channel.

To navigate to the menu outside of the Wizard Select **Main Menu** > **Basic Settings** > **Record Schedule**, to enter the **Schedule**

4.1.4.6.1 Recording Schedule

After setting a schedule record, the device can record video files according to the period you set here. For example, the alarm record period is from 6:00–18:00 Monday, the NVR can record alarm video files during the 6:00–18:00 (6 AM to 6 PM).
All channels are recorded continuously by default. Configure customized record period and record type.

Step 1　The **Rec** interface will be displayed. See Figure 4-33.

Figure 4-33
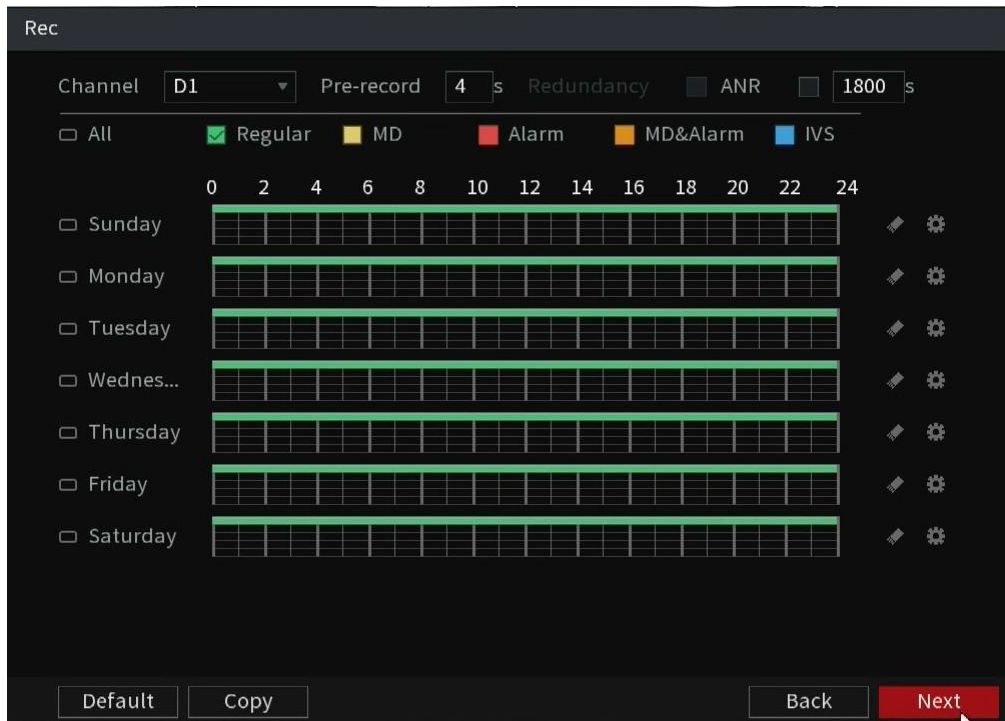
Step 2　Select a channel from the drop-down list, configure different record plans for different channels as necessary. Select All if you want to set for all channels. See Table 4-9 for parameters.

Table 4-9

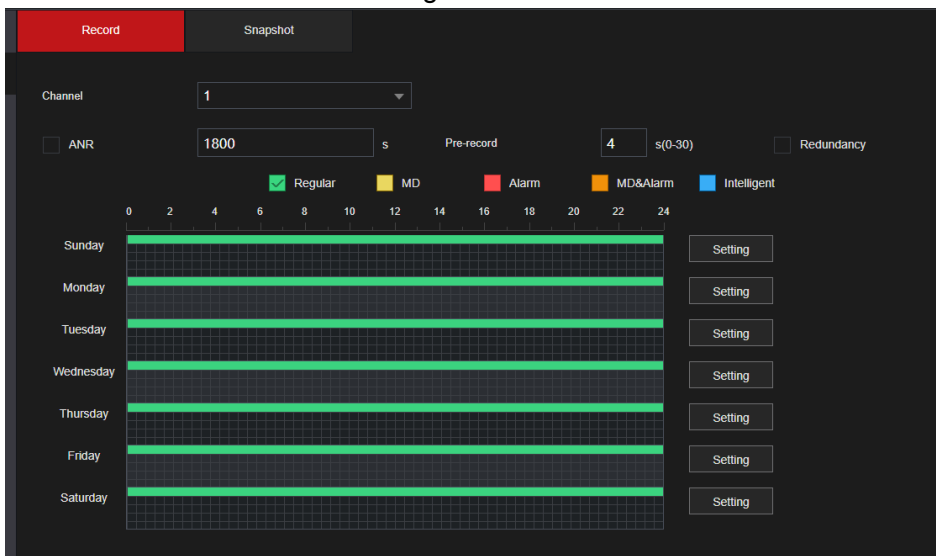| Parameter	Description
Channel	In the drop-down **Channel** list, select a channel to configure.
Pre-record	Enter the amount of time that you want to start the recording in advance. For example, if you set it to 4 seconds the system will record 4 seconds before the motion event was triggered.

Redundancy	If there are several HDDs installed on the NVR, you can set one of the HDDs as the redundant HDD to save the recorded files into different HDDs. In case one of the HDDs is damaged, you can find the backup in the other HDD. Setting a redundant HDD will affect the maximum amount of days you can store footage.
	
	● Select **Main Menu** > **Advanced Settings> Storage Settings> Disk Manager**, then set an HDD as a redundant HDD.
	● Select **Main Menu** > **Advanced Settings> Storage Settings> Record**, and then select the **Redundancy** check box.
	  ◇ If the selected channel is not recording, the redundancy function takes effect next time you record no matter you select the check box or not.
	  ◇ If the selected channel is recording, the current recorded files will be packed, and then start recording according to the new schedule.
	
	📖
	
	● This function is not available in all NVR models.
	● The redundant HDD only back up the recorded videos but not snapshots.

ANR	Configures ANR (auto network resume) function. ● In the event of network failure, the IPC will continue to record if it has a microSD card installed for edge storage adn the camera remains powered on. The NVR can download recorded files from the IPC during the offline period from the IPC. This will guarantee there is no record loss on the current connected IPC channel during network downtime. ● Set the max record upload period. If the offline period is longer than the period you set here, the IPC will only upload the record file during the specified time period. For example, if the network is disrupted for 1 hour (3600s) but the ANR is set to only 30mins (1800s) only the last 30 mins will be retrieved. Adjust settings as desired. 📖 This function is for IPC with an installed microSD card and record functions are enabled.
Period	Define a period during which the configured recording setting is active. See Figure 4-34. 📖 The NVR will only activate the alarm within the defined period.
Copy to	Click **Copy to** to copy the settings to other channels.

Figure 4-34

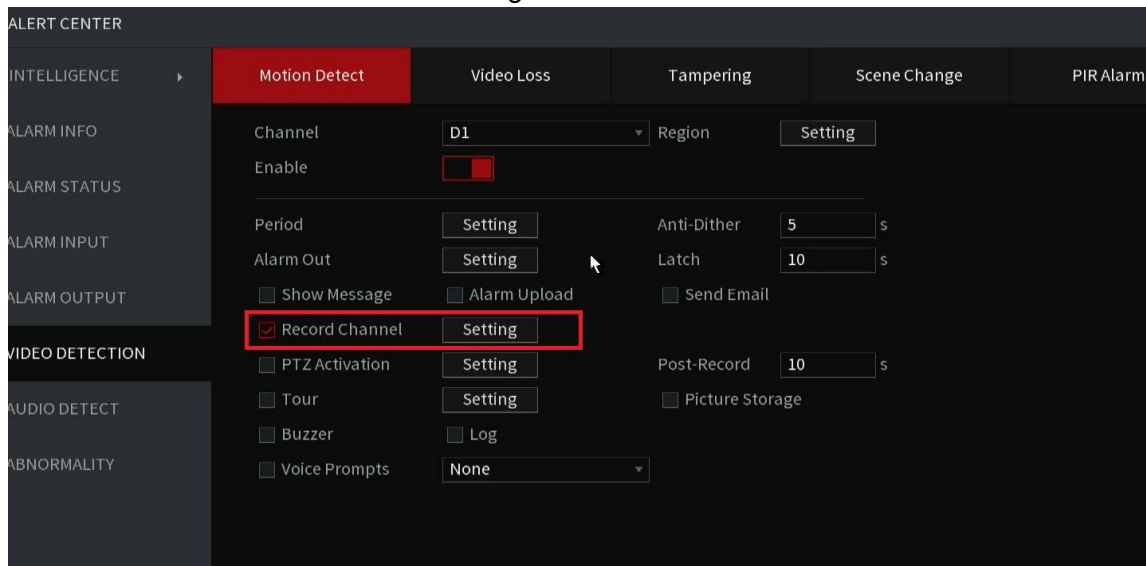Step 3 Set record type then select the times in the table. See Figure 4-35. Or select the **Setting** button to the right of the dates and then set the parameters.

Figure 4-35
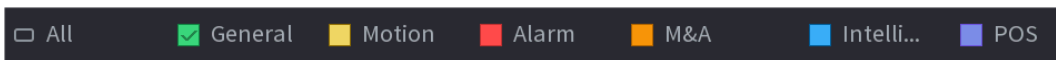
📖

● When the record type is Motion (motion detection), alarm, M&A, and IVS refer to "4.8.5 Video Detection", "4.8.3 Alarm Input", "4.7.1.3 and IVS" for detailed information on setting up the functions to trigger.
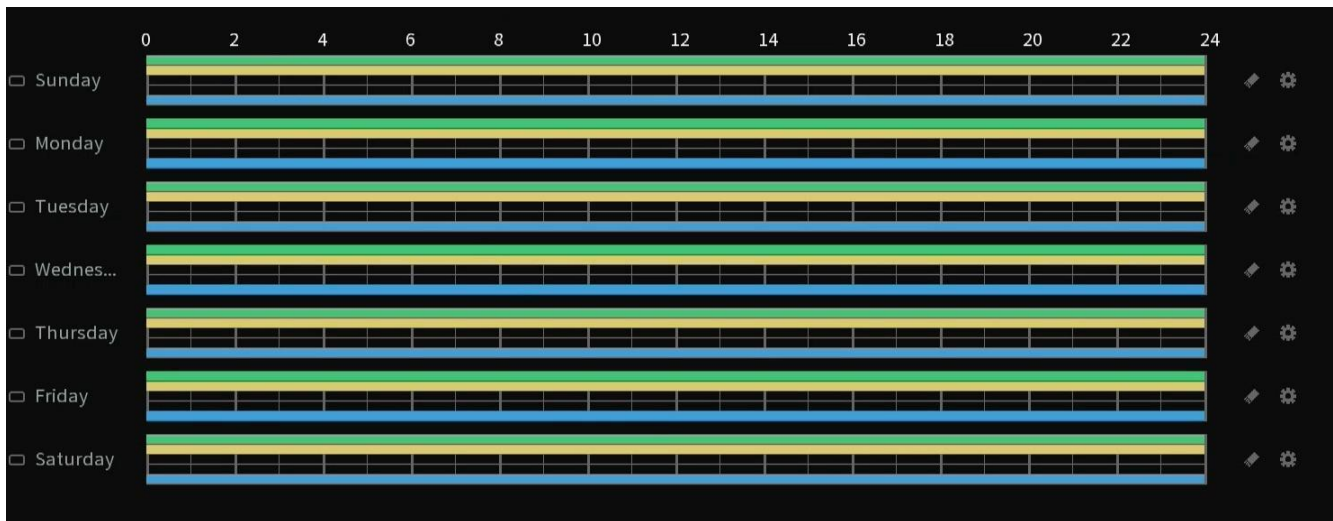
Figure 4-36

Step 4   Set record period. It includes edit mode and draw mode. See Figure 4-39.

📖

Figure 4-37

Define the period by left-clicking and dragging the mouse over the squares or selecting the settings (gear wheel) icon to the right of the calendar.

1. Select a corresponding date to set.
    ◇ Define for the whole week: Click 🔲 next to **All**, all the icons switch to 🔗, you can define the period for all the days simultaneously.
    ◇ Define for several days of a week: Click 🔲 before selecting each day, the icon will change to 🔗. You can define the period for the selected days simultaneously.
2. On the timeline, left click mouse and then drag to define a period.
    There are six periods in one day, the Device starts recoding the selected event type in the defined period. In Figure 4-39, the different color bars stand for different record types.
    ◇ Green represents the general constant recording.
    ◇ Yellow represents for MD (motion detection) record.
    ◇ Red represents alarm triggers (alarm contacts) recordings.
    ◇ Blue represents recoding intelligent events such as iMD or IVS.
    ◇ Orange represents the MD&Alarm record. This requires both event types to be triggered to record the event. If 1 trigger but not the other the video will not be stored. The MD record and alarm record function are both disabled if you enabled the MD&Alarm function
    ◇ Select a record type and then click the ◆ of the corresponding date to clear the corresponding period.

Figure 4-38

- Define the period by editing.
  1. Select a date and then click ⚙. The **Period** interface will be displayed.

Figure 4-39
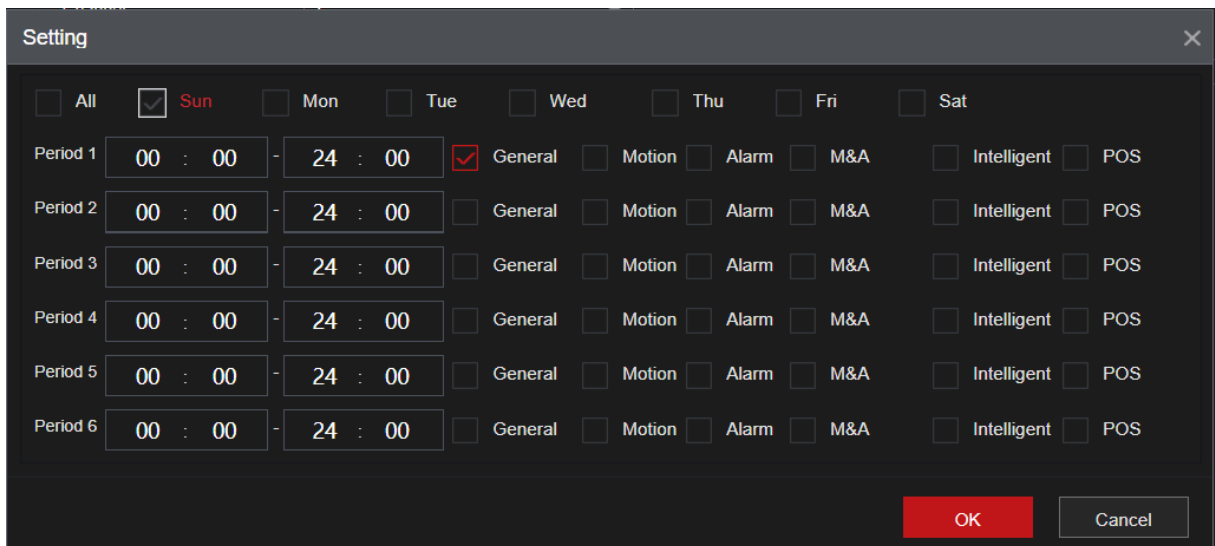
  2. Set record type for each period.
     ◇ There are up to six periods you can set for each day. For example, if you want to record during the night but not during the day you would set Period 1 from 00:00 ~ 08:00 and Period 2 from 18:00 ~ 24:00.
     ◇ Under **Copy to**, select **All** to apply the settings to all the days of a week, or select a specific day(s) that you want to apply the settings to.
     ◇ Click **OK** to save the settings.
  3. Click **Apply** to complete the settings. Refer to "4.1.4.6.3 Record Control" for detailed information.

4.1.4.6.2 Snapshot Schedule

Configure schedule snapshot period.

After setting a schedule for snapshots, the device can store a snapshot image according to the period you set here. For example, if the alarm snapshot period is from 6:00–18:00 Monday, the device will take snapshots during the 6:00–18:00 when an alarm event occurs. It requires the alarm trigger to parameters to have the snapshot checkbox selected. See Figure 4-42

Step 1 Click **Snapshot**, the device goes to the following interface. See Figure 4-40.

Select **Main Menu** > Basic **Settings** > **Record Schedule** > **Snapshot**, to navigate to the snapshot interface.

Figure 4-40

Step 2 Select a channel to set a scheduled snapshot.

Step 3 Set snapshot type as scheduled. Refer to "4.2.6.2 Snapshot" for detailed information.

Step 4 Check the box to set the alarm type. See Figure 4-41.

Figure 4-41

- When the record type is Motion (motion detection), alarm, MD&A, and IVS, enable the channel record function when the corresponding event/ alarm occurs. Fof example, when the alarm type is MD, select **Main Menu** > **ALARM** > **Video Detection** > **Motion Detection**, select the record channel and enable the record function. See Figure 4-42.
- When the record type is Motion (motion detection), alarm, M&A, and IVS, refer to "4.8.5 Video Detection", "4.8.3 Alarm Input", "4.7.1.3 IVS" for detailed information.

Figure 4-42
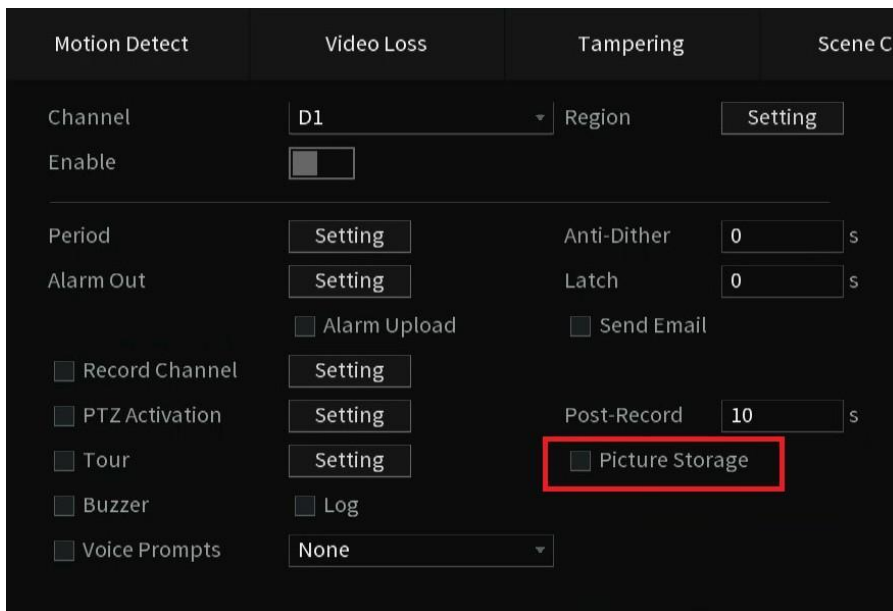
Step 5　Refer to "4.1.4.6.1 Recording Schedule" to set snapshot period.

Step 6　Click **Apply** button to save the snapshot plan.

Enable auto snapshot function so that the snapshot plan can become activated. Refer to "4.1.4.6.3 Record Control" for detailed information.

4.1.4.6.3 Record Control

After setting the schedule record or schedule snapshot, you will need to enable auto record and snapshot function so that system can automatically record or snapshot.
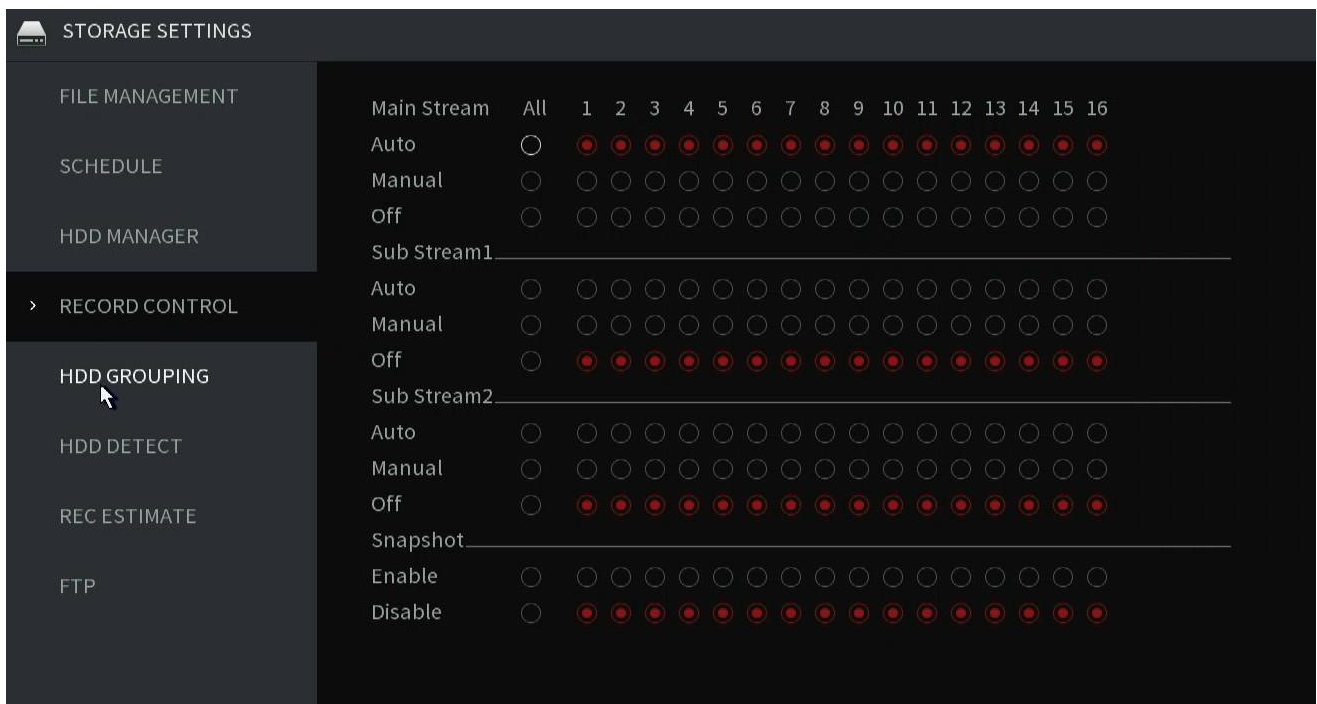
- Auto: (Default setting for main stream) The system will automatically record video based on the type and record period you set in the Schedule interface.
- Manual: The system records general footage constantly unless switched off.
- Off: The system will not record any footage for the specified channel.

📖

You will need to have storage authorities to implement the Manual record operation. Make sure the HDD has been properly installed.

Step 1   Right-click on the mouse and then select **Manual Control** > **Record Mode** or select **Main Menu** > **Advanced Settings** > **Storage Settings >Record Control.** See Figure 4-43.

Figure 4-43

Step 2   Configure parameters.

Table 4-10

Parameter	Description
Streams	Are the different sources from the cameras. ● Main Stream: High Resolution stream of the camera. ● Sub Stream 1: Low Resolution typically D1 Standard Definition. ● Sub Stream 2: Secondary substream can typically handle 720P or 1080P dependent on the camera capabilities.

Channel	Displays all the connected digital channels. You can select a single channel or select All.
Record status	- Auto: Automatically record according to the record type and recording time as configured in the recording schedule. - Manual: Stores general recording for 24 hours for the selected channel. - Off: Does not record.
Snapshot status	Enable or disable the scheduled snapshot for the corresponding channels.

Step 3   Click **Apply** to complete settings.

4.2 Camera

4.2.1 Connection

Select **Main Menu** > **Advanced Settings > Camera Configuration > Add/ Remove Device** to add remote devices. See Figure 4-44.

After adding remote devices to the NVR, you can view the video on the NVR, and manage and store the video file. The maximum amount of cameras that can be added is dependent on the NVR series.

Figure 4-44

4.2.1.1 Changing Camera IP address

Changing IP of a camera can only be done to devices found in the search list on the registration page. Modifying the IP address for cameras registered in the bottom section changes the connection information.
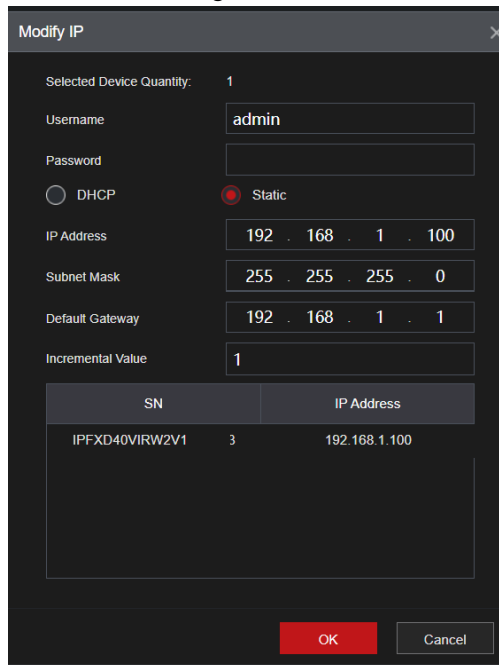
Step 1   Select **Main Menu > Advanced Settings > Camera Configuration** > **Add/Remove Device**, check the box before the left of the camera and then click **Modify IP** or click the ✎ to edit. The **Modify IP** interface will be displayed. See Figure 4-45.

📖

Check the box before several cameras, change the IP addresses of several cameras at the same time.

Figure 4-45

Step 2   Select IP mode.
- **DHCP**: There is no need to input IP address, subnet mask, and default gateway the unit will auto retrieve the network parameters.
- **Static**: Manually input IP address, subnet mask, default gateway, and incremental value.

📖
- To change several devices' IP addresses at the same time, input an incremental value. The device can add the incremental value set to the fourth octet of the IP address one by one to automatically allocate the IP addresses to multiple devices.
- If there is an IP conflict when changing the IP address, an IP conflict dialogue box will appear. If using batch change IP address, the device automatically skips the conflicted IP and begins the allocation according to the incremental value.

Step 3   Input remote device user name and password.

📖

When changing IP addresses of multiple devices at the same time, make sure the cameras' usernames and passwords are the same.

Step 4 Click OK button to save settings. After the modification, click on Device search again, device will display the new IP address.

4.2.1.2 Auto Changing Compression to H.265

This function can automatically set the encode format as H.265 if the H.265 Auto switch function is enabled. The resolution will not be adjusted, and the stream value will be cut in half while keeping the same quality as H.264. H265 may not be ideal for all scenarios user discretion is advised. This is only supported with IC Realtime cameras with H.265 encoding available.

Click to toggle the **H.265 Auto Switch** at the bottom of the interface. See Figure 4-46.

Figure 4-46
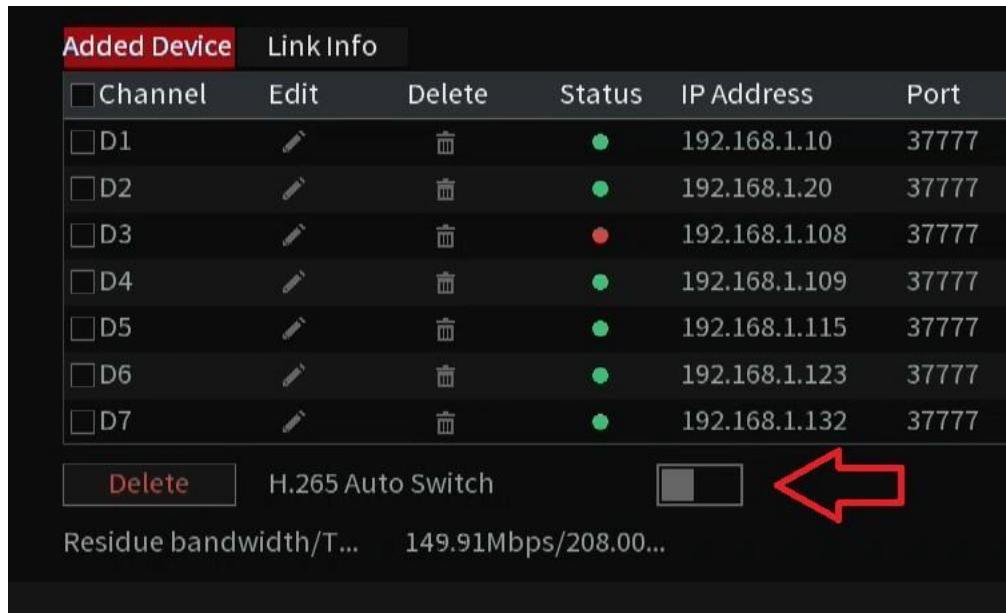
4.2.1.3 IP Camera Export (Exporting Remote Devices)

The list of added IP devices to your NVR can be exported to your local USB device.
This feature may not be available in all NVR models.

Step 1   Select **Main Menu > Advanced Settings > Camera Configuration** > **Add/Remove Device.** Insert a USB flash drive device and then click the **Export** option in the bottom right of the **Add/Remove Device** interface.

The **Backup Browse** interface will be displayed. See Figure 4-47.

Figure 4-47
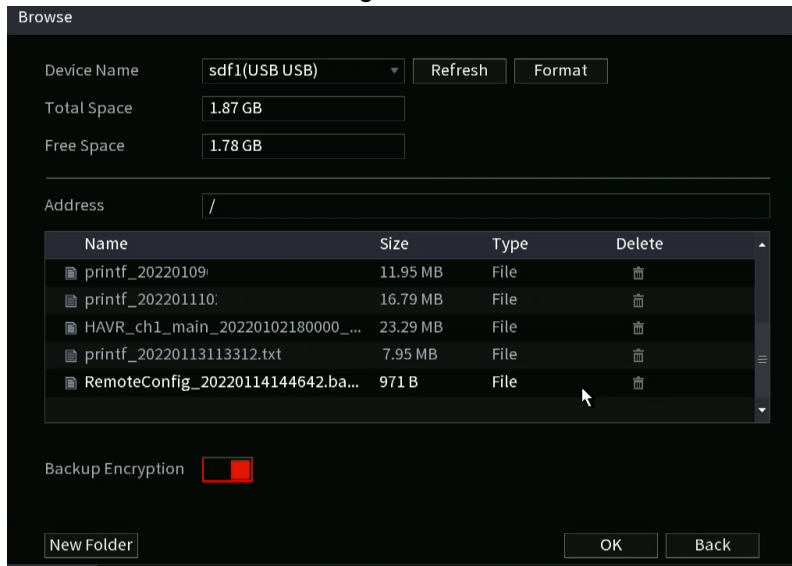
Step 2   Select **Location** to save the device list file.

Step 3   Click **OK**.

Step 4   The NVR will display a dialogue box to indicate successful export.

📖

When exporting remote devices, the **Backup Encryption** check box is enabled by default. The file information includes IP address, port, channel number, manufacturer, username, and password.
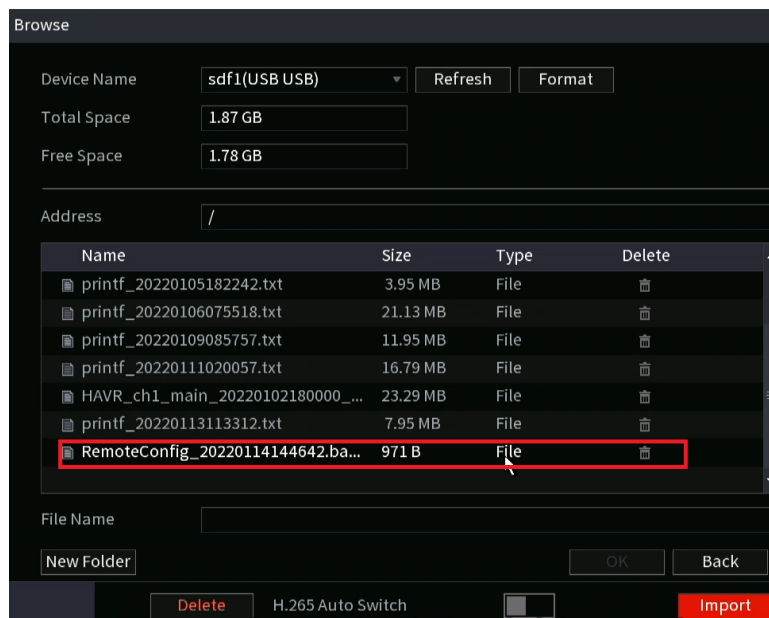
● If you select the File Backup Encryption check box, the file format is ".backup".

● If you un-check the File Backup Encryption box, the file format is ".csv". In this case, there might be a security risk for exported data.

4.2.1.4 IP Camera Import (Importing Remote Devices)

Step 1   Click **Import**.

The **Import Browse** interface will be displayed. See Figure 4-48.

Figure 4-48

Step 2   Navigate the USB's folders to the location of the backup file and select the file.

Step 3   Click Import at the bottom right. A dialogue box will appear if successfully imported.

📖

If the imported IP has conflicted with the currently registered devices, the system will display a dialogue box warning.

4.2.2 Remote Device Initialization

The Remote device initialization will change the remote device login password and possibly the IP address.

📖

- When connecting a new IC Realtime camera to the back of an NVR via the built-in PoE ports, the NVR will automatically initialize the camera. The camera password will be set to the same admin password as the NVR.
- When connecting an older IP camera to the NVR via the built in PoE ports of the NVR, the NVR may fail to initialize the camera. Go to the Registration interface to initialize the camera or Initialize the camera by logging into the camera web GUI using its IP address with a Computer. In other cases older cameras do not initialize as they are set with a default password of admin following the old protocols.

Step 1   Select **Main Menu** > **Advanced Settings** > **Camera Configuration> Add/ Remove Device**

Step 2   Click **Search Device** and then enable **Uninitialized filter**. This will display camera(s) to be initialized.

Step 3   Select a camera to be initialized and then click **Initialize**. An interface prompting to use the NVRs password for the IP camera will be displayed. Selecting the checkbox will allow you to set a different custom password. See Figure 4-49.

Figure 4-49
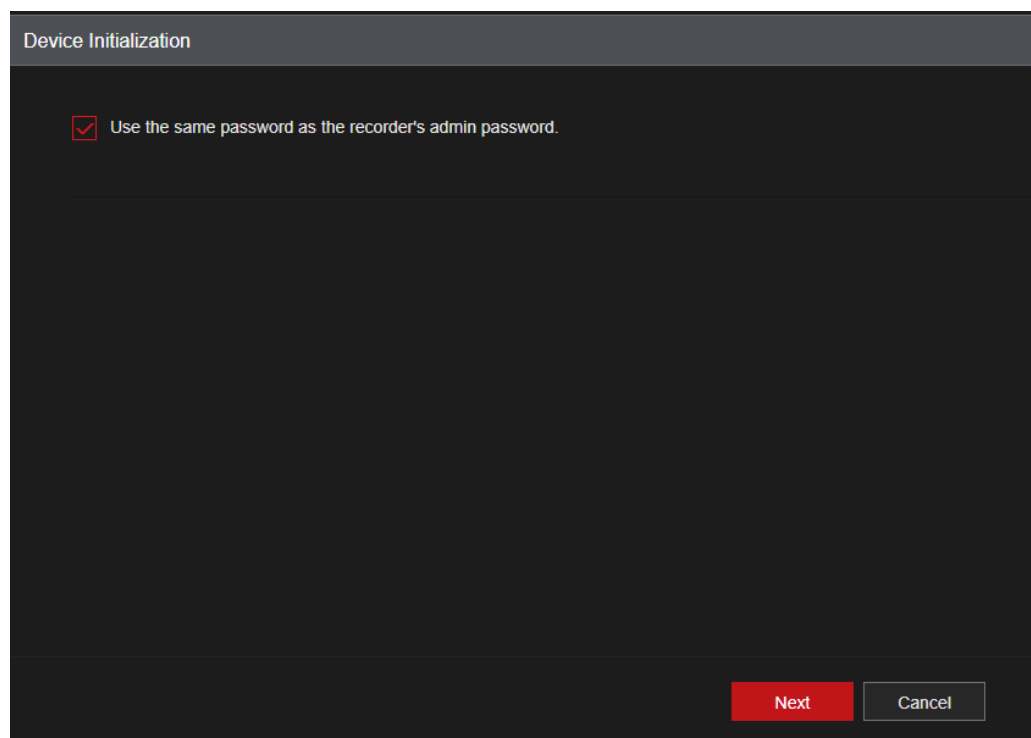
Step 4   If you un-check the "Using same password as the NVR" and clicked Next, the Enter
          Password interface will be displayed so you can set your desired password. See Figure
          4-50.
              1) Set a password. See Table 4-12 for more information.

Figure 4-50

              2) Set password under "Confirm Password" then click Next.

Table 4-12

Parameter	Description
User	The default is **admin.**
Password	The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter and special characters (excluding"", "'", ";", ":" and "&").
Confirm Password	Enter a strong password according to the password strength bar indication.

For your device's security, create a complex password of your own choosing. We
also recommend you change your password periodically, especially in a
high-security environment.

Step 5   Click **Next**.

Step 6.   The **Network** interface will be displayed. See Figure 4-52.

Figure 4-52


Step 7 Set camera IP address to DHCP or Static.

DHCP is recommended for IP cameras connected to the recorder's built-in POE ports. For cameras on a local network, it is recommended to set a static IP address so cameras stay connected.

- **DHCP**: There is no need to input IP address, subnet mask, and default gateway. The NVR automatically allocates the IP address to the camera. *Note that if the IPC is plugged into NVR PoE, IPC should be set only to DHCP.
- **Static**: Manually input IP address, subnet mask, default gateway and incremental value.

- To change several devices' IP addresses at the same time, input incremental value. The device can add the fourth octet address of the IP address one by one to automatically allocate the IP addresses.
- If there is an IP conflict when changing to a static IP address, the device will display the IP conflict dialogue box. If batch changing the IP address, the NVR automatically skips the conflicted IP and begins the allocation according to the incremental value.

<u>Step 8</u>   Click **Next**.

The **Device Initialization** interface will be displayed showing the results. See Figure 4-53.
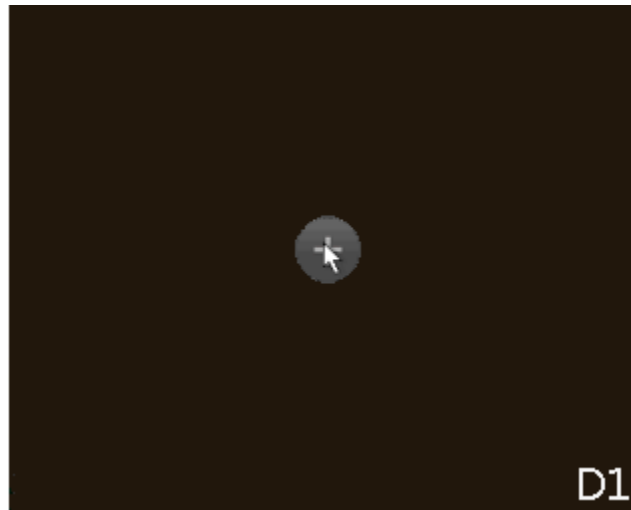
Figure 4-53
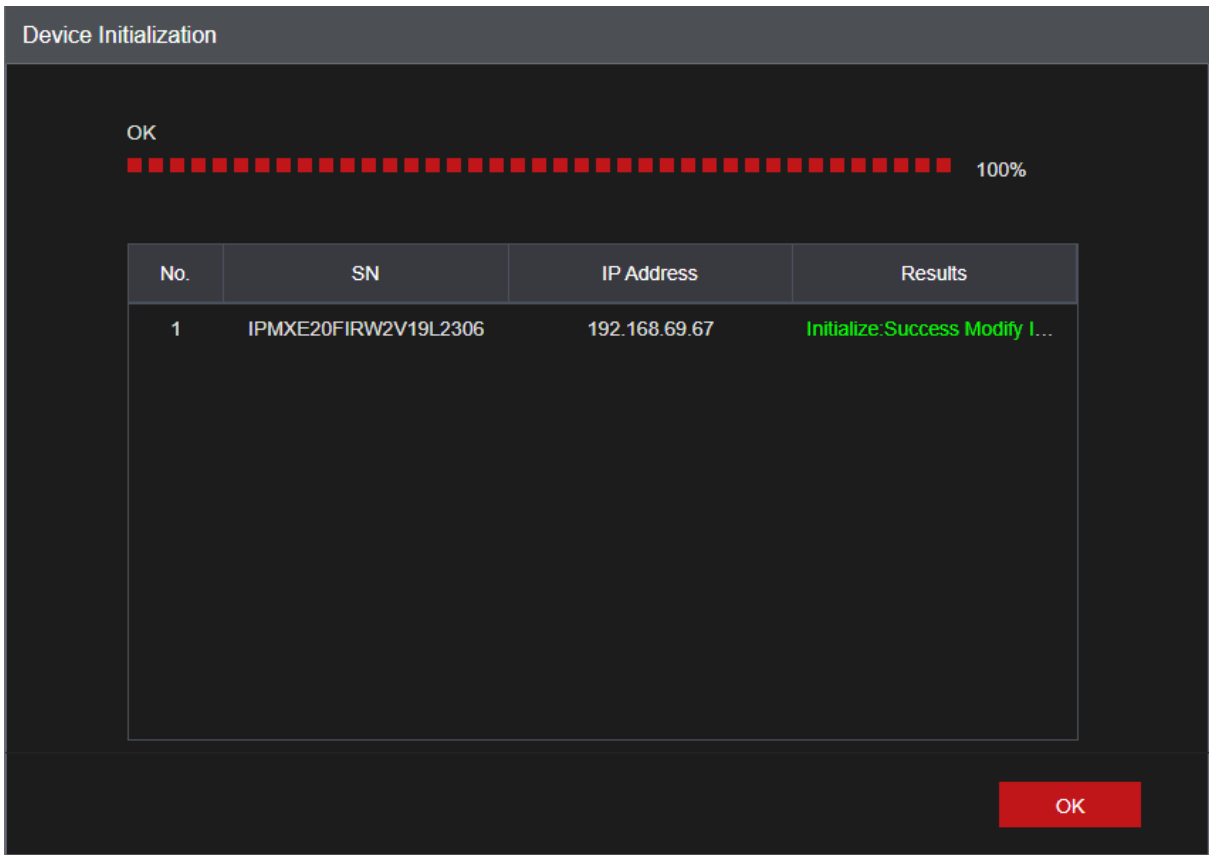
<u>Step 9</u> Click **OK** to complete the setup.

4.2.3 Shortcut Menu to Add Camera

You can register a camera directly on the live view screen using the "+" icon.

<u>Step 1</u>   On the live view interface, move your mouse to the window.
There will be an icon + on the channel window. See Figure 4-54.

<u>66</u>

Figure 4-54

Step 2   Click "+", the device will display the interface to add an IP camera. Refer to "4.1.4.4 Adding Camera" for detailed information.

4.2.4 Image

To achieve the best video appearance, configure the IP camera image parameters as desired.
In most cases, the default settings will display a proper image.

Step 1   Select **Main Menu** > **Advanced** > **Camera Configuration** > **Image**.
The **Image** interface will be displayed. See Figure 4-55.

Figure 4-55
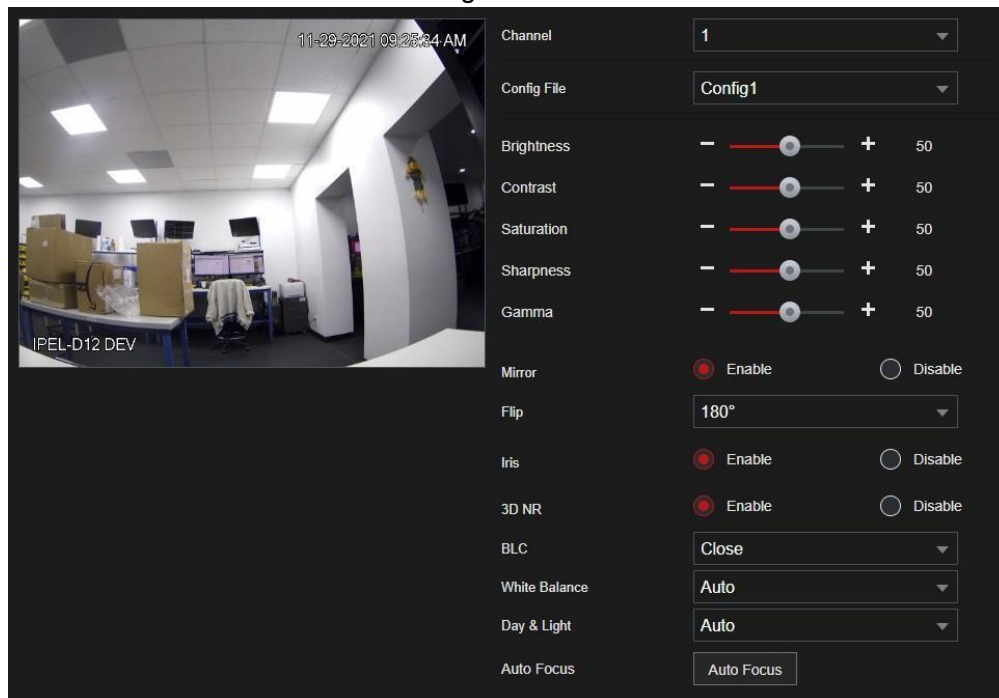
Step 2 Select Camera Channel and Configure parameters as desired. See Table 4-13.

Different series network camera displays different parameters. Actual models may slightly differ. Some options will not be available through the recorder. You will need to log into the camera's web interface to modify those parameters.

Table 4-13

Parameter	Description
Channel	In the Channel list, select the channel that you want to configure.
Profile	There are three config files (saved presets) available. The system has configured the corresponding parameters for each file, you can select one according to your actual situation.
Brightness	Adjusts the image brightness. The greater the value, the brighter the image will become. Adjusts the brightness according to the actual environment. Raising it too high will cause image to be washed out.
Contrast	Adjusts the image contrast. The greater the value, the more obvious the contrast between the light area and dark area will become. Adjusts the contrast according to the environment.
Saturation	Adjusts the color shades. The greater the value, the lighter the color will become. Adjusts the saturation according to the actual environment.
Sharpness	Adjusts the sharpness of the image edge. The greater the value is, the more obvious the image edges will be. Adjusts the sharpness according to the actual environment.
Gamma	This function adjusts image brightness and enhances the image dynamic display range. The greater the value, the bright the video will be.
Mirror	When enabling this function, the left and right sides of the video image will be switched. It is disabled by default. Not all NVR models support this feature.
Flip	Sets the camera video display rotation. It can include Normal, 180°, 90°, 270° depending on camera model
Auto Iris	● For the cameras with auto iris only. ● When enabled, the iris will automatically zoom in/zoom out according to the brightness of the environment, and the image brightness changes as well. ● If disable the auto iris function, the iris does not automatically zoom in/zoom out according to the brightness of the environment when the iris is at the biggest value.
3D NR	This function applies to the image if the frame rate is a minimum of 2fps. Reduces the noise by making use of the information between two frames. The greater the value, the better the effect.

Parameter	Description

Backlight Mode	This is best set when the camera is already installed on location.
	● SSA: In the backlight environment, the system can automatically adjust image brightness to clearly display the object.
	● BLC:
	  ◇ Default: The device auto exposure is set according to the environment so that the darkest area of the video is cleared.
	  ◇ Customize: After selecting the specified area, the system can brighten the specific area to reach the proper brightness
	● WDR: In dynamically lit environments, this lowers the highly lit areas and enhance the brightness of the low bright section., thus enabling you to view these two sections clearly at the same time.
	● HLC: In a backlight environment, it can lower the brightness of the brightest section and reduce the area of the halo and lower the brightness of the whole video.(Cars at night)
	● Stop: Disables the BLC function.

WB Mode	Configures the camera White Balance mode. This affects the image hue so that the image can accurately display the environment. Different cameras support different WB modes such as auto, manual ,natural light, outdoor and etc.
Day/Night Mode	Configure the color and black&white mode of the image. This setting is not affected by the configuration files. The default setting is Auto. ● Color: The camera outputs color image only. ● Auto: Depends on the camera, such as overall brightness and whether there is an IR light, either color image or black&white image is output. ● B/W: The camera outputs Black and white image only. ● Sensor: This will be set when there is a peripheral device connected IR light. The Sensor option is available on some non-IR devices only.

Step 3　Click **Apply** when done.

4.2.5 Video Overlay

Configures the values for overlay such as camera name (channel title) and privacy masking.

4.2.5.1 Overlay

You can add the time and channel information in the live view interface.

 Step 1   Select **Main Menu** > **Advanced> Camera Configuration**> **Video Stream> Overlay**

Step 2   Configure parameters.

Table 4-14

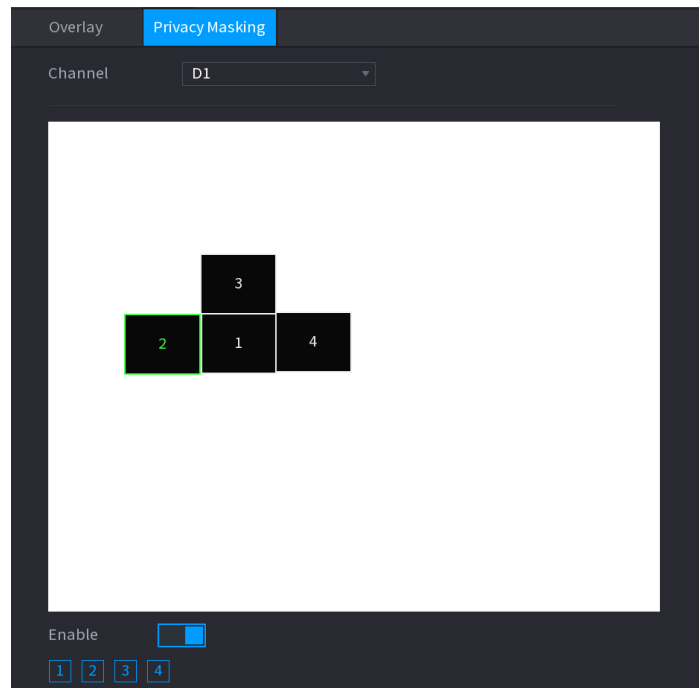| Parameter	Description
Channel	Select a channel.
Time Title	Select **Time Title** and the time will be displayed in the live view and playback.
	Drag the time title to the desired area and click **Apply**.
Channel Title	Select **Channel Title** and the channel name will be displayed in the live view and playback.
	Drag channel title to the desired area and click **Apply**.
Custom Title	You can custom title to be overlaid on the screen. Click **Setting** to set the information such as font size, title content and text alignment, and then click **OK**.
Default	Set the device default configuration.
Copy to	Click **Copy to** to copy the settings to other channels.

Step 3   Click **Apply**.

4.2.5.2 Privacy Masking

Configures the privacy masking area on the screen for the privacy of the area.

Step 1 Select **Main Menu > Advanced Settings > Camera Configuration Configuration**> **Video Stream> Overlay** > **Privacy Masking**.

Figure 4-56

Step 2   Configure parameters.

Table 4-15

Parameter	Description
Channel	Select a channel.
1, 2, 3, 4	Select **Enable** to enable privacy masking. The number represents the number of masking areas. Select a number and drag masking areas to the screen, and you can also change the size of areas or drag an area to another location. 📖 You can drag up to 4 masking areas to one channel.
Default	Set the device default configuration.

Step 3   Click **Apply**.

4.2.6 Encode

Configures the video bit stream and image parameters.

4.2.6.1 Encode

Configures the video bit stream parameters such as bitstream type, compression, resolution. Recommended to keep the NVR maximum bandwidth throughput in mind when adjusting these settings.

Some NVR series may support three streams: main stream, sub stream 1, sub stream 2.

Step 1   Select **Main Menu** > **Advanced> Camera Configuration** > **Encode**.
The **Encode** interface will be displayed. See Figure 4-57.

Figure 4-57

Step 2 Configure parameters. See Table 4-16.

Table 4-16

Parameter	Description
Channel	In the **Channel** list, select the channel that you want to configure the settings for.
Intelli Streaming	Enable the smart codec function. This function can reduce the video bitstream for unimportant recorded video to maximize the storage space. ● [toggle]: Enabled. ● [toggle]: Disabled. Enabling this function will disable some smart functions on specific cameras. Should you have issues with smart functions it is advised to turn this off.
Type	● Main Stream: In the **Type** list, select **General**, **MD** (Motion Detect), or **Alarm**. ● Sub Stream: This setting is not configurable.
Compression	Allows the selection mode (based on camera and NVR model) ● H.265: Main profile encoding. This setting is recommended. ● H.264H: High profile encoding. Low bitstream with high definition. ● H.264: Main profile encoding. ● H.264B: Baseline profile encoding. This requires a higher bitstream compared with other settings for the same definition.
Resolution	In the Resolution list, select resolution for the video. The maximum video resolution might be different depending on your NVR and camera model.
Frame Rate (FPS)	Configures the frames per second for the video. The higher the value is, the clearer and smoother the image will become. Frame rate changes along with the resolution. With NTSC format, the selectable values range from 1 through 30, in PAL format, the selectable values range from 1 through 25. The actual frame rate range varies depending on camera model specifications.
Bit Rate Type	In the **Bit Rate Type** list, select **CBR** (Constant Bit Rate) or **VBR** (Variable Bit Rate). If you select **CBR**, the image quality cannot be configured; if you select **VBR**, the image quality can be configured.
Quality	This function is available if you select **VBR** in the **Bit Rate** List. The bigger the value is, the better the image will become.
I-Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	In the **Bit Rate** list, select a value or enter a customized value to change the image quality. The greater the value, the better the image quality.

Step 3   Click **More**. The **More** interface will be displayed. See Figure 4-58.

Figure 4-58
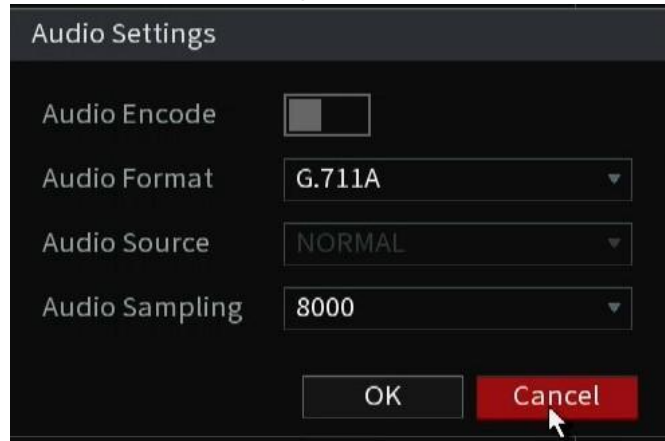
Step 4   Configure Audio parameters. See Table 4-17.

Table 4-17

Parameter	Description
Audio	This function is enabled by default for the main stream. It will need to be manually enabled for the sub stream. If enabled, the recorded video file will be a composite audio and video stream.
Compression	In the **Compression** list, select a format such as G711a, G711u, PCM, AAC. (Varies depending on IPC, NVR)
Sampling Frequency	In the **Sampling Frequency** list, you can select the audio sampling rate.

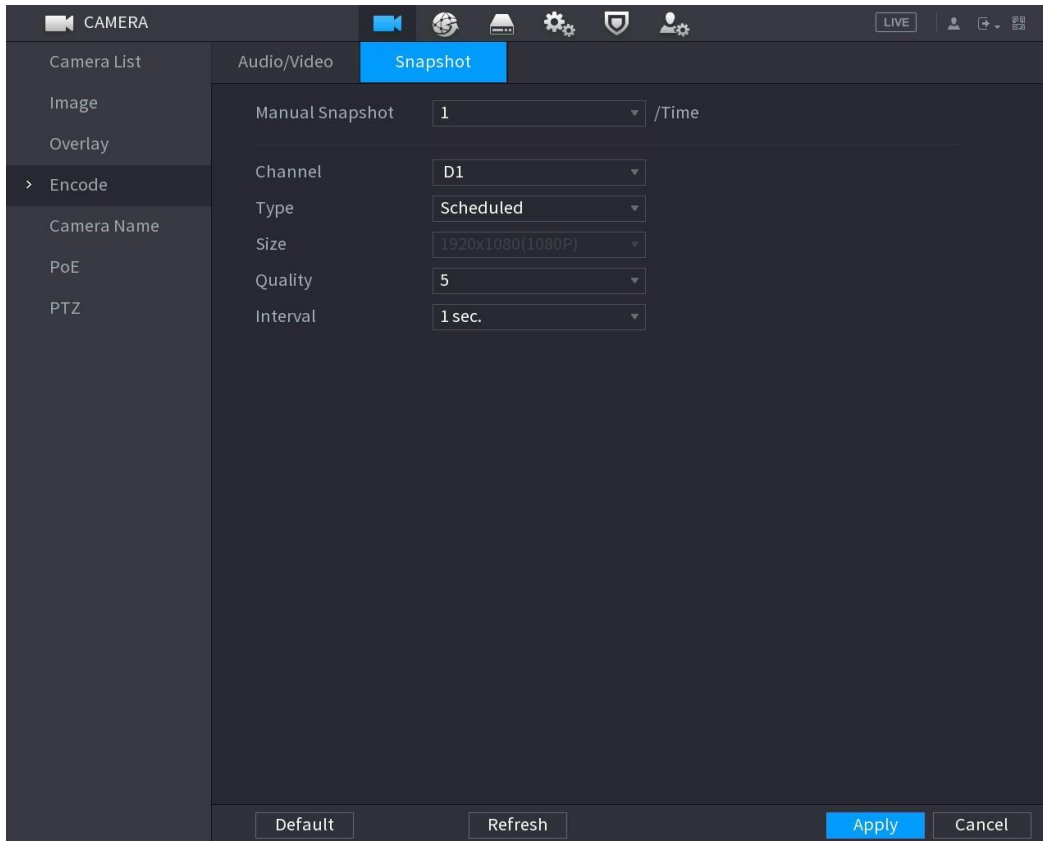Step 5   Click **OK**.
Step 6   Click **Apply**.

4.2.6.2 Snapshot

Configures the snapshot mode, image size, quality and interval.

Step 1   Select **Main Menu > Advanced Settings > Camera Configuration** > **Encode** > **Snapshot**

The **Snapshot** interface will be displayed. See Figure 4-59.

Figure 4-59

Step 2 Configure parameters. See Table 4-18.

Table 4-18

Parameter	Description
Manual Snapshot	In the **Manual Snapshot** list, select how many snapshots to take with each trigger.
Channel	In the **Channel** list, select the channel that you want to configure the settings for.
Type	In the **Type** list, you can select **Scheduled**, or **Event**. ● Scheduled: The snapshot is taken during the scheduled period. ● Event: The snapshot is taken when there is an alarm event occurs, such as motion detection event, video loss, and local alarms.
Size	In the **Size** list, select a value for the image. The greater the value, the better the image quality.
Quality	Configure the image quality by 6 levels. The higher the level is, the better the image quality.

Interval	Configure or customize the snapshot frequency. Supports 3600 seconds/image max.

Click **Apply**.

4.2.7 Channel Name

You can customize the channel name.

Step 1   Select **Main Menu** > **Advanced> Camera Configuration** > **Camera Name**.
The **Camera Name** interface will be displayed. See Figure 4-60.

Figure 4-60

Step 2   Modify the desired channel names.

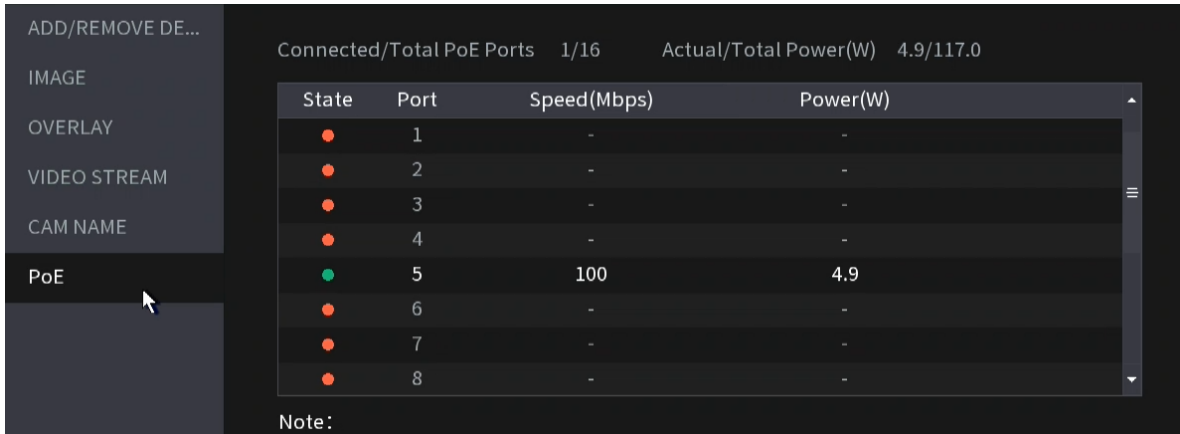- Only IC Realtime cameras support the name change function.
- The channel name supports a max of 63 English characters.

Step 3   Click **Apply**.

4.2.8 Checking PoE Status

This allows you to monitor PoE ports status or enable enhancement mode for each individual PoE port.

Step 1   Select **Main Menu** > **Advanced> Camera Configuration > PoE**.

Figure 4-61

Step 2   (If Available) Set **Enhancement Mode** to **On** or **Off**.

When **On** is selected, the transmission distance of PoE port will be extended. This is only for ePOE supported IP cameras. Extended transmission of cables longer than network cable standards will have a reduced max transmission rate of 10mbps.

4.2.9 Remote Update

This function allows you to upgrade the connected IP camera firmware using a local file. (IC Realtime cameras only)
You will need to have the firmware available on a USB to complete this step. Log into your dealer portal and go to the product page to get the latest firmware. If unavaailable you can contact support via email tech@icrealtime.com.

Step 1   Select **Main Menu** >**Advanced> Camera Configuration** > **Add/Remove Device** > **Upgrade**
The **Update** interface will be displayed. See Figure 4-62.

Figure 4-62
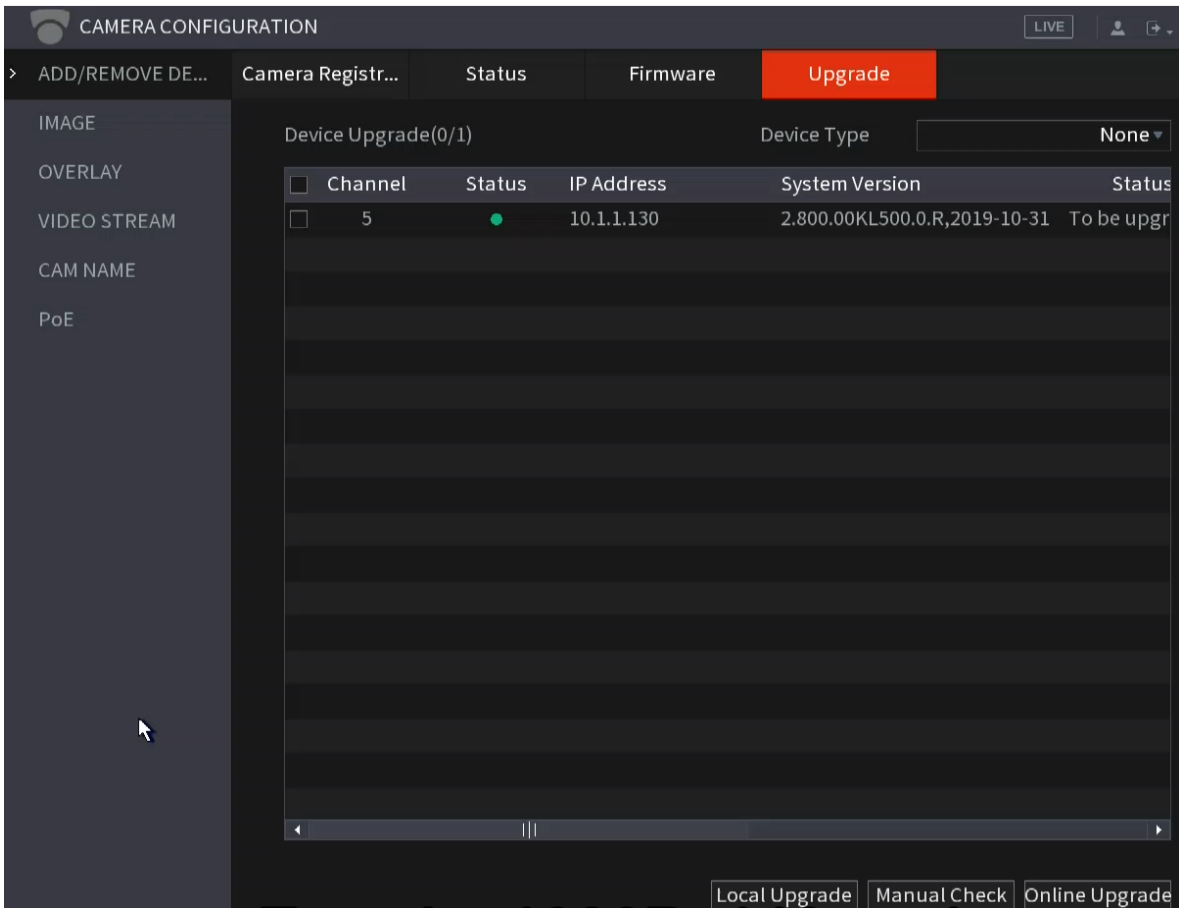
Step 2   Update the firmware of the connected remote device.

● File upgrade

1. Select a channel and then click **File Update / Local Upgrade**.
2. Navigate your USB Flashdrive and Select the update file.
3. Once selected, click **OK**.

4.2.10 Remote Device Info

This function allows you to view the connection and alarm status of the corresponding channel. Select **Main Menu** > **Advanced** > **Camera Configuration** > **Add/ Remove Device> Linked Device Info**, the **Linked Device Info** interface will be displayed. See Figure 4-63.

Refer to Table 4-19 for detailed information.
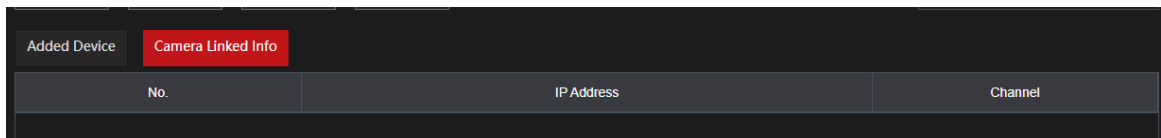
Figure 4-63

Table 4-19

Icon	Description	Icon	Description
●	IPC works properly.	▬	IPC is not supported.
⚠	Alarm Event.	■	Video loss event.

4.3 Live View

The local display of the system will display your camera feeds live. This display menu is called Live View. It has multiple different variations of split views and control options. By default, all active cameras in the live feed are viewable but can be displayed requiring a user to log in to view them for sensitive areas.
The max window split and viewable cameras will vary depending on the NVR model.

4.3.1 Live View

On the live view interface, This function allows you to view the monitor video of each channel. The corresponding channel displays the date, time, and channel name after you overlay the corresponding information. Refer to the following table for detailed information. See Table 4-20.

Table 4-20

SN	Icon	Description
1		The current channel is recording
2		Motion detection has been triggered
3		Video loss status
4		The current channel is in monitor lock status (current owner has no viewing permission). You will need to log in with a user that has rights such as "admin".

4.3.2 Navigation bar

The navigation bar features shortcut configuration icons.

- Different series products may display different navigation bar icons. Refer to the actual product for detailed information.
- Select **Main Menu** > **Advanced** > **System Operation**> **General** > **Basic** to enable navigation bar function and then click **Apply**; to enable the Navigation Bar. Note: This function is enabled by default.

While on the live view interface. You can view the navigation bar. See Figure 4-65. Refer to Table 4-21 to view detailed information. Note that not all icons shown here may not appear in your actual NVR model.
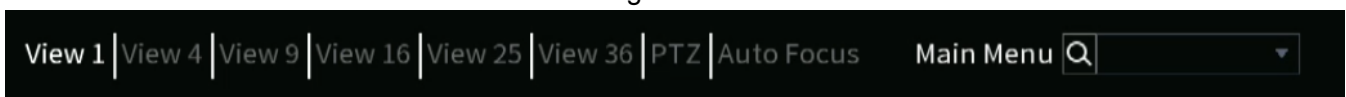
Figure 4-65

View 1 | View 4 | View 9 | View 16 | View 25 | View 36 | PTZ | Auto Focus   Main Menu Q
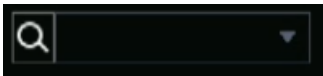
Table 4-21

Icon	Function
Main Menu	Open **Main Menu**.
◀	Expand or minimize the navigation bar.
View 1 | View 36	Select split-view layout.
◀▦	Go to the previous screen.
▦▶	Go to the next screen.
PTZ	Opens the PTZ control panel. For details, see "4.4.2 PTZ Control".
🔍 ▼	Menu Shortcut selection. Clicking the dropdown arrow tab allows you to view the different Sections from the Main Menu. Selecting in the empty filed will bring up a on screen keyboard to search for a menu such as "P2P" for quick selection. Select the desired menu option then click on the 🔍 icon to navigate to that menu section.

4.3.3 Live View Control Interface

To enable the live view control interface, hover the mouse to the top center of the video of the current channel. See Figure 4-68.
If the mouse stays idle for more than 6 seconds, the control bar will automatically hide.

📖

- Disable the navigation bar if it will be displayed on the interface before using this function.
- Note that not all icons shown here may not appear in your actual NVR model.

Figure 4-68

Icon	Function
🕐	Open **Instant Replay** to play back the most recent video. See section 4.3.3.1
🔍	Enables **Digital Zoom** for the desired channel. Digital zoom allows you zoom in on the pixels of the image. The higher the resolution the video the better the quality of the image when using digital zoom. See Section 4.3.3.2

|	
![Instant Backup icon]	**Instant Backup** function. Allows you to save live footage to a usb. See Section 4.3.3.3
![Manual Snapshot icon]	**Manual Snapshot**. Takes a snapshot of the selected channel. See Section 4.3.3.4
![Two Way Talk icon]	**Two Way Talk**. Enables or Disables Two Way Talk with selected channel. Requires microphone and speaker. See Section 4.3.3.5
![Stream Switch icon]	Video **Stream Switch** Control. Allows you to manually change the video stream being displayed. See Section 4.3.3.6

4.3.3.1 Instant Replay

The Instant Replay function allows you to play back the previous (5-60 minutes) recordings of the current channel. Click ![icon] to go to the instant replay interface. See Figure 4-69.

Figure 4-69
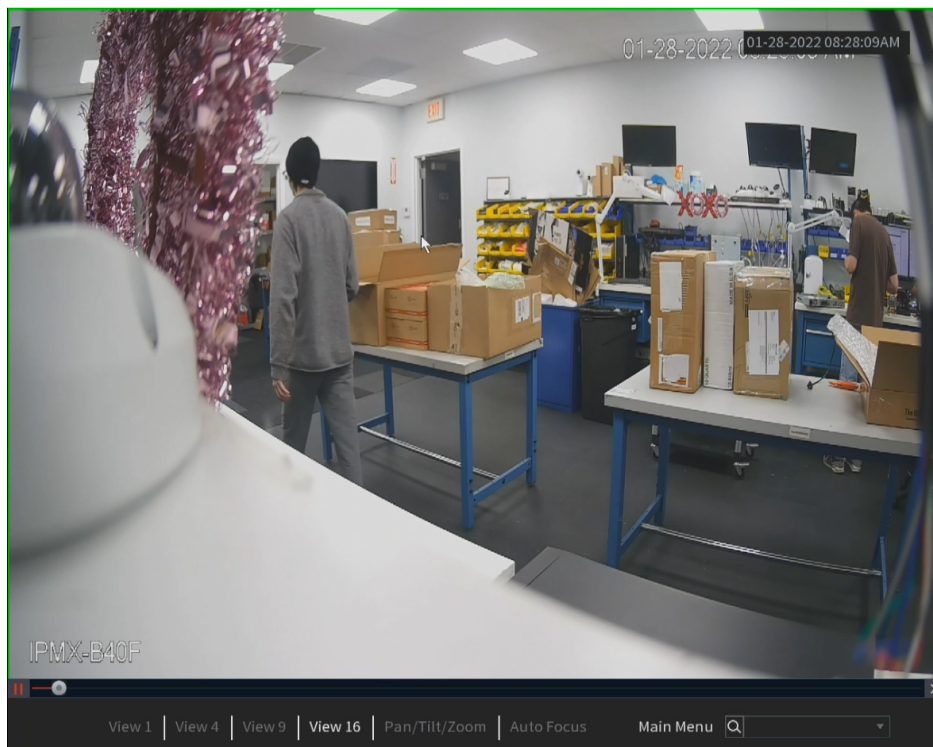
Instant replay allows playback recordings of the last 5 minutes to 60 minutes of the current channel.

- Go to the **Main Menu** > **Advanced> System** > **General** > **Basic** to set Instant Replay time.

- Move the slider to select the time you want to start playing.

- Play, pause and close the instant replay window.

- The information such as channel name and recording status icon is hidden during instant playback and will not display until exited.

- During playback, a screen split layout switch is not allowed.

- If a Tour is enabled, it will take higher system priority than the instant playback. The instant playback will not function when a tour is in process. Stop or disable the tour if this is an issue.

Figure 4-70
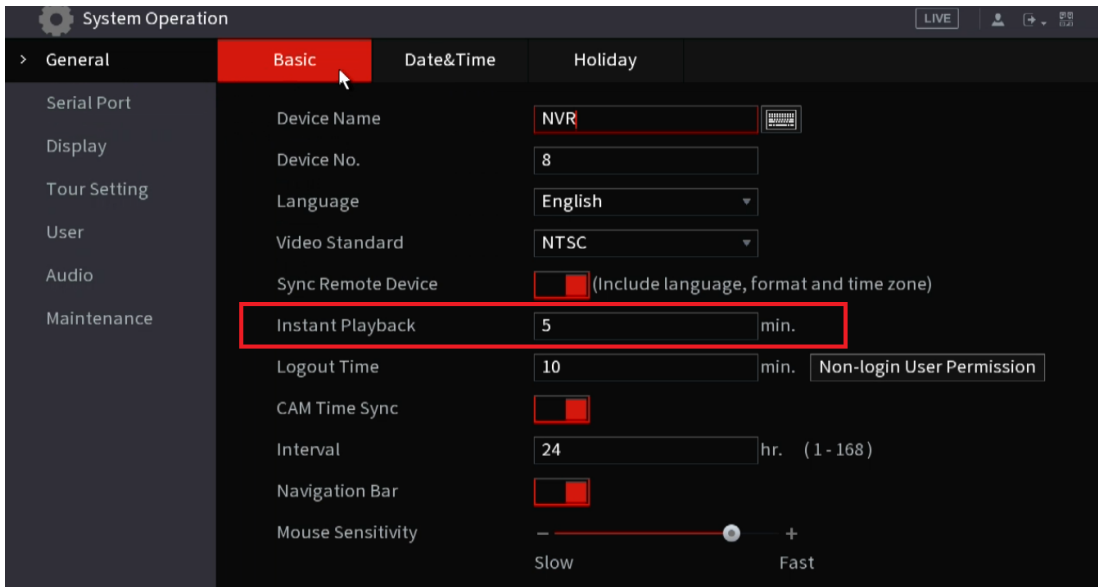
4.3.3.2 Digital Zoom

This function allows you to digitally zoom in a specified zone of the current channel to view the details. There are two ways to achieve this:

- Clicking the ⊕ icon enables digital zoom mode, confirmed when the icon changes to ☑. Click and hold down the left mouse button and draw a box to select the area you want to enlarge. The area will be zoomed in after the left mouse button is released.
- To zoom in or out further while in zoom mode, move the mouse wheel up or down.

The digital zoom interface is shown as in Figure 4-71. When the image is in the zoomed-in status, you can drag the image toward any direction to view the other zoomed-in areas. Right-click the mouse to cancel zoom and return to the original interface.

The higher the camera resolution the better the image quality will be when using digital zoom feature. This is because you are zooming in / blowing up the pixels. Higher resolution video has increased pixel per inch count resulting in a sharper image.

Figure 4-71

4.3.3.3 Instant Backup

This function allows you to record and backup live footage from the NVR into a USB storage device. The recording will start by clicking the ⊞ icon. To stop recording, click this icon again. The clip will be automatically saved into the connected USB storage device

4.3.3.4 Manual Snapshot

This function allows you to take one to five snapshots of a live video and save them into a USB storage device. By clicking the ⬜ icon, you can take snapshots. The snapshots are automatically saved into the connected USB storage device. You can view the snapshots using a PC.

📖

To change the number of snapshots, select **Main Menu** >**Advanced Settings**> **Camera Configuration** > **Video Stream**> **Snapshot**, in the **Manual Snapshot** list, select the desired snapshot quantity.

4.3.3.5 Two-way Talk

This function allows you to perform the voice interaction between the NVR and the remote device (if it has audio output with speakers).

<u>Step 1</u>   Click ▮   to start the two-way talk function the icon now is shown as 🎤.

<u>Step 2</u>   Click 🎤   again, to end the two-way talk.

4.3.3.6 Switch Bit Streams

This function allows you to switch the channel main stream/sub stream according to current network bandwidth.
● M: Main stream. This is typically a high-bitrate, high-resolution stream. It occupies large network bandwidth and is the recording stream by default.
● S: Sub stream. Its definition is low but occupies small network bandwidth. It is suitable for general surveillance, remote connection, etc.

Click 🅜   to switch the bit stream type of the main stream and sub stream.
● M: Main stream.
● S: Sub stream. Some IP cameras support two or more sub streams (S1, S2). Refer to "4.2.6.1 Encode" for detailed information.

4.3.3.7 Shortcut Menu

By right-clicking on the live view interface, you can quickly access the corresponding functional interface and perform relevant operations, including entering the main menu, searching recordings, and selecting screen split mode.
Right-click on the live interface and the shortcut menu will be displayed. Refer to Table 4-22 for detailed information.

⌂ Main Menu		⌂ Main Menu			
🔍 Search		🔍 Search		⌂ Main Menu	
🎥 PTZ Control		🎥 PTZ Control		🔍 Search	
▪ View 1	▶	▪ View 1	▶	🎥 PTZ	
▦ View 4	▶	▦ View 4	▶	▪ View 1	▶
▦ View 8	▶	▦ View 8	▶	▦ View 4	▶
▦ View 9	▶	▦ View 9	▶	▦ View 8	
▦ View 16	▶	▦ View 16	▶	▦ View 9	
▦ View 25	▶	▦ View 25	▶	🎥 Add Camera	
▦ View 36		▦ View 36	▶	◈ Wireless Pairing	
≡ Sequence		≡ Sequence		🎥 Manual	▶
◉ Smart Tracking		◉ Smart Tracking		⊡ Auto Focus	
▦ Live Layout	▶	▦ Live Layout	▶	🎨 Image	
🎥 Add Camera		🎥 Add Camera			
◉ Fisheye		◉ Fisheye			
🎥 Manual Control	▶	▦ Split Track			
🖥 Live Mode	▶	🎥 Manual Control	▶		
📊 Crowd Distribution	▶	🖥 Live Mode	▶		
⊡ Auto Focus		⊡ Auto Focus			
🎨 Image		🎨 Image			
		≡ Sub Port			
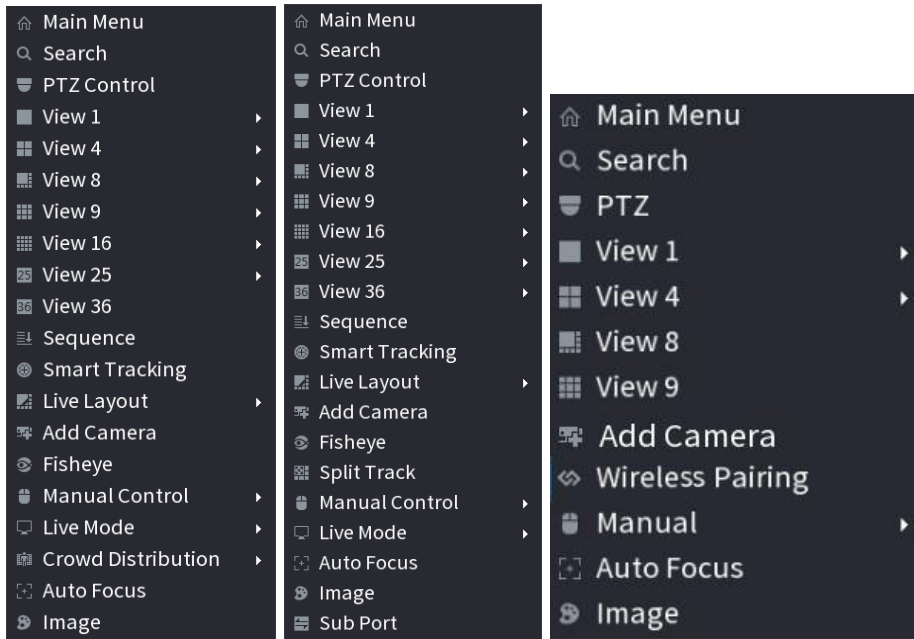
Table 4-22

| Function	Description
Main Menu	Open **Main Menu** interface.
Search	Opens the **SEARCH** interface to search and play back recorded files. For details, see "4.6 Playback and Search".
PTZ Control	Opens the PTZ interface. For details, see "4.4 PTZ".
View 1/4/8/9/16/25/36	Configures the live view screen as a single-channel layout or multi-channel layout.
Sequence	Set customized screen split mode and channels. For details, see "4.3.5 Sequence".
Add Camera	Open the **Add/ Remove Camera** interface. For details, see "4.1.4.4 Adding Camera".
Manual Control	● Selecting **Record Mode**, allows you to configure the recording mode as **Auto** or **Manual**, or stop the recording. You can also enable or disable the snapshot function ● Selecting **Alarm Mode**, allows you to configure alarm output settings.
Live Mode	There are two modes: General/AI mode.
Crowd Distribution	Select enable/disable to start/stop crowd distribution function.
Auto Focus	Click to enable auto focus function. This function is only for IP cameras with an autofocus function.
Image	Click to modify the camera properties. For details, see "4.2.4 Image".
Sub Port	Click **Sub Port**, to control the sub screen/ second monitor.

4.3.3.8 Picture Search

This function is for AI recorders with Face Recognition enabled IP cameras. The Picture search allows searching records for specific faces selected within the current live view. This feature may not be available in all NVR models.

Step 1   Click [image] to pause the live view.

Step 2   Draw a searching range as instructed by the on-screen prompt, and then click **OK**.
- If there are less than 30 faces in the selected range, the searching starts immediately.
- If there are more than 30 faces (or targets) in the selected range, a prompt will display indicating that there are too many targets and the searching range should be reduced. The image stays paused so you can start modifying the range.
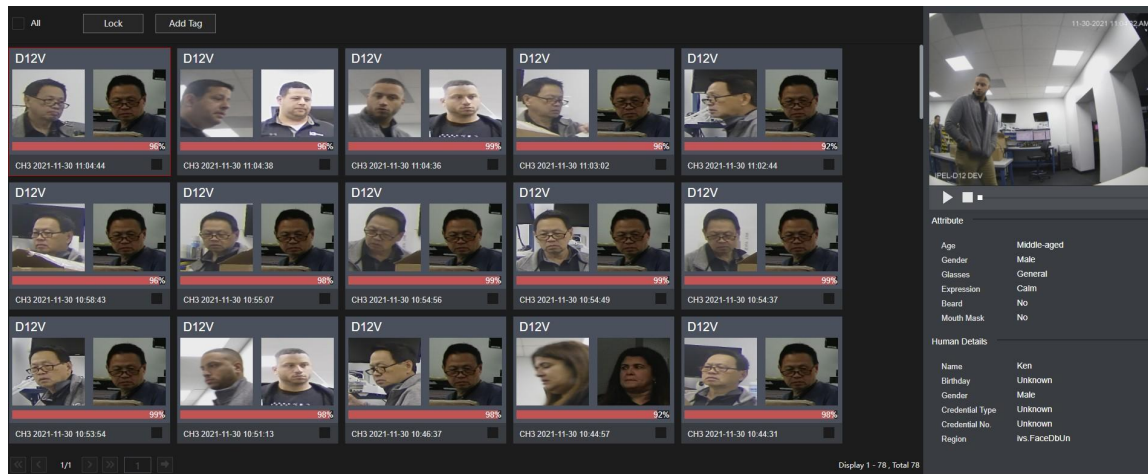
Figure 4-75 Draw a search range
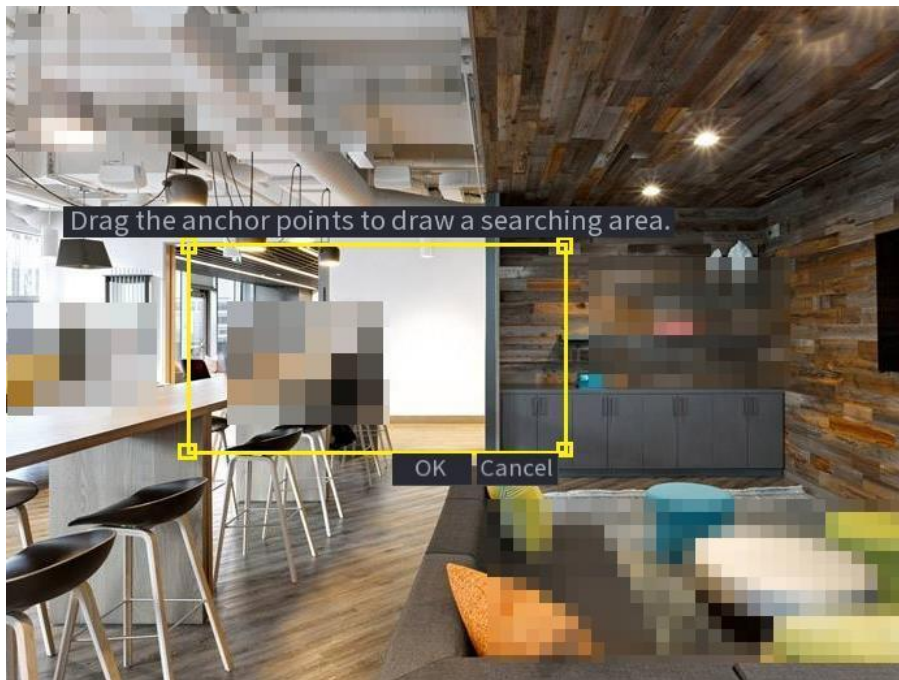
Step 3   Select the target face that you want to search for related videos and configure parameters. You can select maximum 8 target faces.

Step 4   Click **Search**. The search results are displayed.

Figure 4-76 Picture search results

- Play video: Select the picture and then click ▶ to play back the video within 10 seconds before and after the snapshot. During playback, you can click ⏸ to pause, click ◻ to stop, and click to display or hide the intelligent rules (means displaying and means hidden).
- Add tag: Select the picture and then click **Add Tag** to add a tag to the recorded video to find the target recorded video faster. For details, see "4.6.5 Tag Playback".
- Lock recorded video: To keep the recorded video permanently, select the picture, and then click **Lock** to lock video so that it cannot be overwritten and deleted.
- Back up recorded video or picture: Select the picture, and then click **Backup**.
- The **Backup** interface will be displayed. Then you can set the save path, backup type, and file type, and then export to the external storage device.

4.3.4 Adding IC Home Devices

IC Home devices can be added to IC Realtime recorders. After connecting anIC Home device to your local WiFi, You will need a PC with the ICIP DVR/ NVR Finder Utility tool (ConfigTool) installed. Open Configtool to find the IP address of the IC Home Device.

Important: It is recommended that you set an IP reservation on the Router for the IC Home device as a static IP option is not available.

Step 1   Go to **Main Menu > Advanced Settings > Camera Configuration> Add/ Remove Device.**

Step 2   Click on **"Manual Add."**
Note: The Device Search function on the Recorder can also scan the local network for the IC Home Device IP address.

Step 3   Input the IP address, Port (37777 by default), the username (admin), and the password that was set up for the device. Click **OK** to save. See Figure 4-77.

Figure 4-77

	Channel	Edit	Delete	Status	IP Address	Port	Device Name..	Remote Chanr	Manufacturer..	CAM Name	WEB Browse..	Type
☐	1	✏	🗑	●	192.168.1.195	80		1	Onvif	IPC	e	IPFX-D40...
☐	2	✏	🗑	●	192.168.1.9	37777	ORB-OUT...	1	Private	IPC	e	ORB-OUT...
☐	3	✏	🗑	●	192.168.1.178	37777	Orbit-0009	1	Private	CAM 3	e	Orbit

4.3.5 Sequence

Configures a customized view layout.

⚠

The preview layout restores the default channel layout after the Default operation.

Step 1   On the preview interface, right-click mouse and then click **Sequence**.
The **Sequence** interface will be displayed. See Figure 4-78.
📖

● When entering the edit view interface, the device will automatically switch to the max split view mode.
● The channel list on the edit view interface displays the added camera channel number and channel name.
● If the channel amount has exceeded the device max split amount, the edit view interface will display the max screen number amount and current screen number.
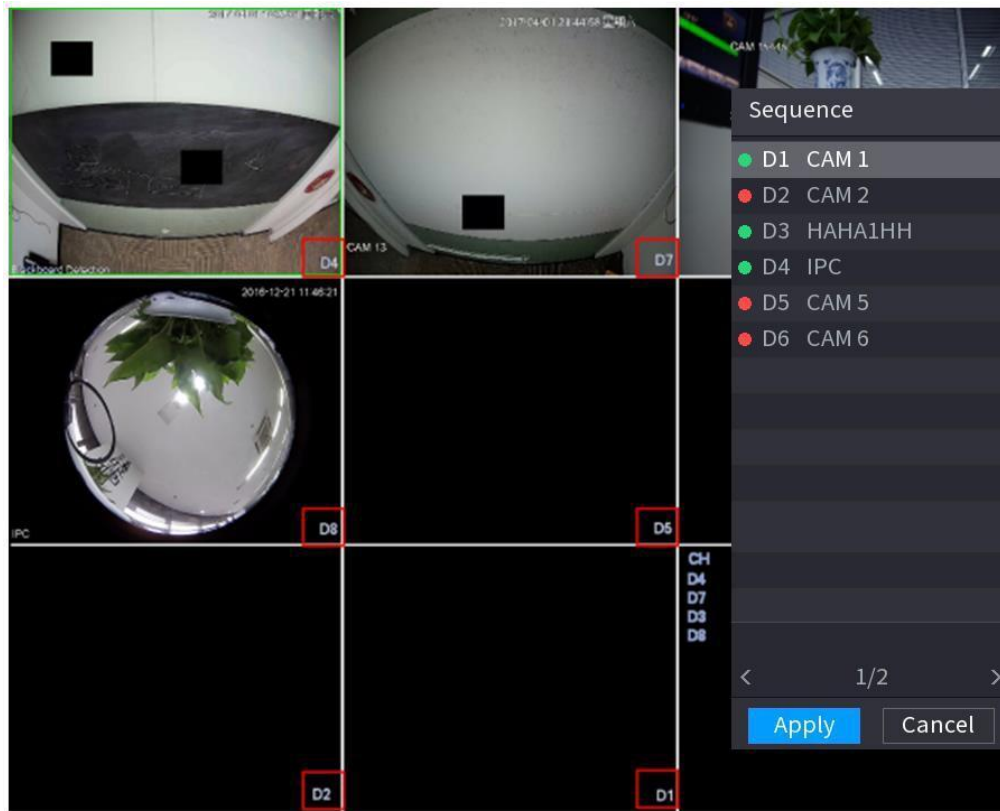
Figure 4-78

Step 2　On the edit view interface, drag the channel to the desired window or left click and drag on the preview window to switch the positions.

Check the channel number at the right bottom corner to view the current channel sequence. See Figure 4-79.

Figure 4-79

Step 3　Click **Apply** to save the current channel sequence.
　　　　After you change the channel sequence, click **Cancel** or right-click the live view interface, the NVR will display the dialogue box.
● Click **OK** to save current settings.
● Click **No** to exit without saving the settings.

4.3.6 Fisheye (Optional)

Some NVR models support native de-warping of IC Realtime cameras with a 360 degree Fisheye lens.

4.3.6.1 Fisheye de-warp during preview interface

The fisheye cameras (panoramic camera) feature a wide video of angle but the video is distorted. The de-warp function can present the proper and vivid video suitable for human eyes. On the preview interface, select channel with the Fisheye camera, then right-click the mouse and select fish eye. See Figure 4-81. Configures the fisheye installation mode and display mode.

📖

- For the non-fish eye channel, the system will display the dialogue box to notify you that the channel is not a fisheye supported and does not support the de-warp function.
- If system resources are insufficient, the system will display the corresponding dialogue box.

Figure 4-81
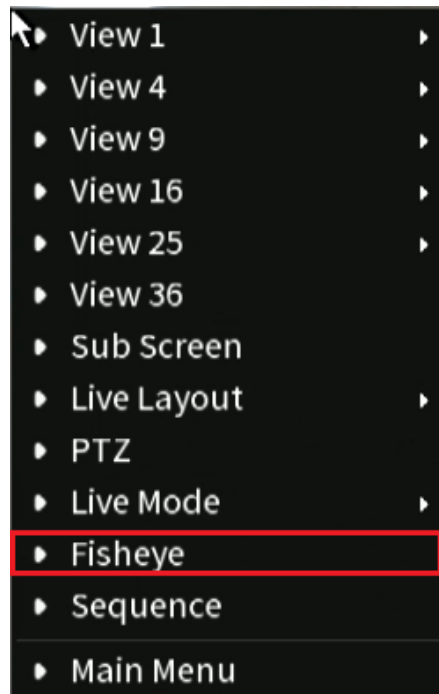
Now you can see an interface shown as in Figure 4-82. Configure the fish eye installation mode and display mode. There are three installation modes: ceiling mount/wall mount/ground mount.

📖

- Different installations modes will have different de-warp modes.
- Some series products support 180°de-warp. 180°de-warp fisheye supports wall mount de-warp only. The actual product shall prevail.
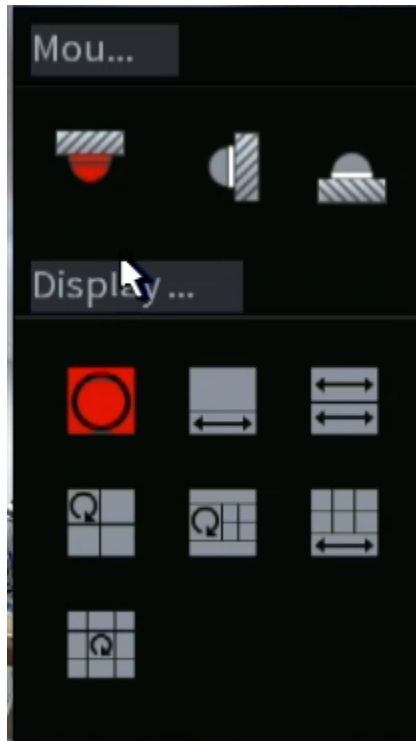
Figure 4-82

Table 4-23

Installation modes	Icon	Note
▣(Ceiling mount) ▣(Ground mount)	◯	360°panorama original view
	▭	1 de-warp window+1 panorama stretching
	▤	2 panorama stretching view
	▦	1 360° panorama view+3 de-warp windows
	▦	1 360°panorama view+4 de-warp windows
	▦	4 de-warp windows+1 panorama stretching
	▦	1 360° panorama view+8 de-warp windows
▣ （Wall mount）	◯	360°panorama original view
	⊠	Panorama stretching
	⊠	1 panorama unfolding view+3 de-warp windows
	⊠	1 panorama unfolding view +4 de warp windows
	▦	1 panorama unfolding view +8 de warp windows

Figure 4-83
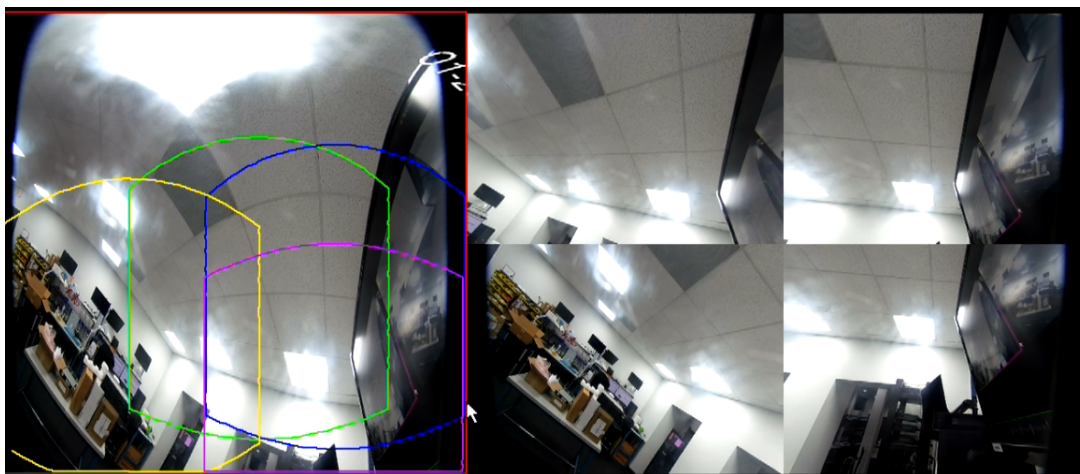
In Figure 4-83, you can adjust the color pane on the left pane or use your mouse to change the position of the small images on the right pane to realize fish eye de-warp.

Operation: Use mouse to zoom in/zoom out, move, and rotate the image (Not for wall mount mode.)

4.3.6.2 Fisheye de-warp during playback

When playing back the fisheye record file, you can use de-warp function to enable different view options with the fisheyecamera.

Step 1   On the main menu, click **Playback,** then select **Playback**.

Step 2   Select 1-window playback mode and corresponding fish eye channel, click ▶ to play.

Step 3   Right-click the 👁 icon, to navigate to the de-warp playback interface. For detailed information, refer to Figure 4-83.

4.3.7 AI Live View Mode

IC Realtime AI-enabled NVRs feature a Live- View AI Mode. When enabled, the NVR will display real-time information for Face recognition, vehicle and non-motor vehicle enabled cameras on the right side of the preview interface. The AI mode supports instant playback and displays feature attributes.

Face detection/ recognition, vehicle detection, and non-motor vehicle detection must be set up and enabled to support this function. For details, see "Video Metadata".

Step 1   Right-click to select **Live Mode** > **AI Mode**.
          The AI preview interface will be displayed. See Figure 4-85.

Figure 4-85
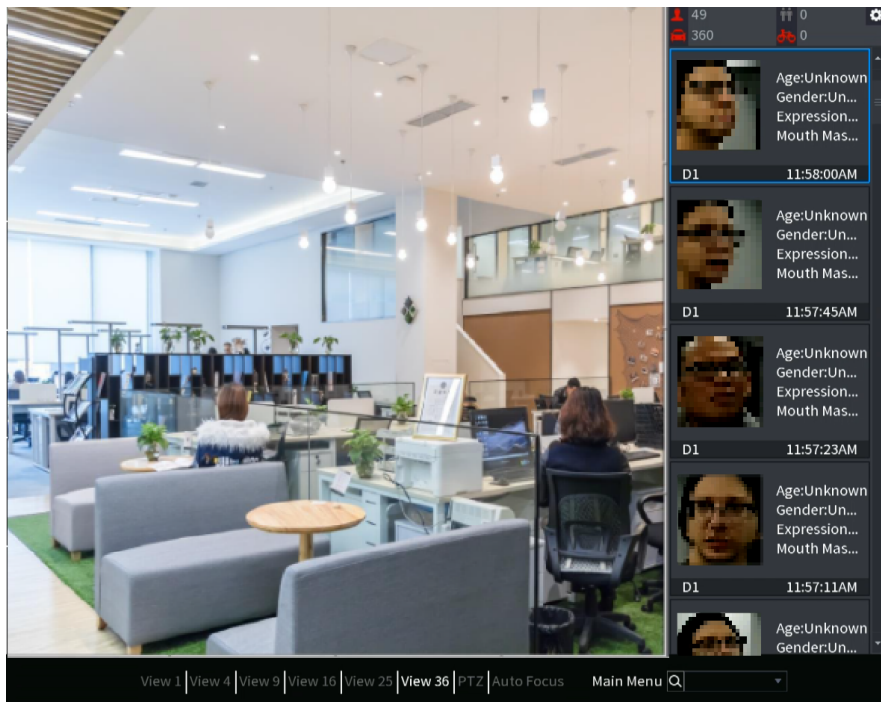
Step 2   (Optional) Double-click the image on the right to play the corresponding video.
Step 3   Click ⚙.
          The Properties interface will be displayed. See Figure 4-86.

Figure 4-86
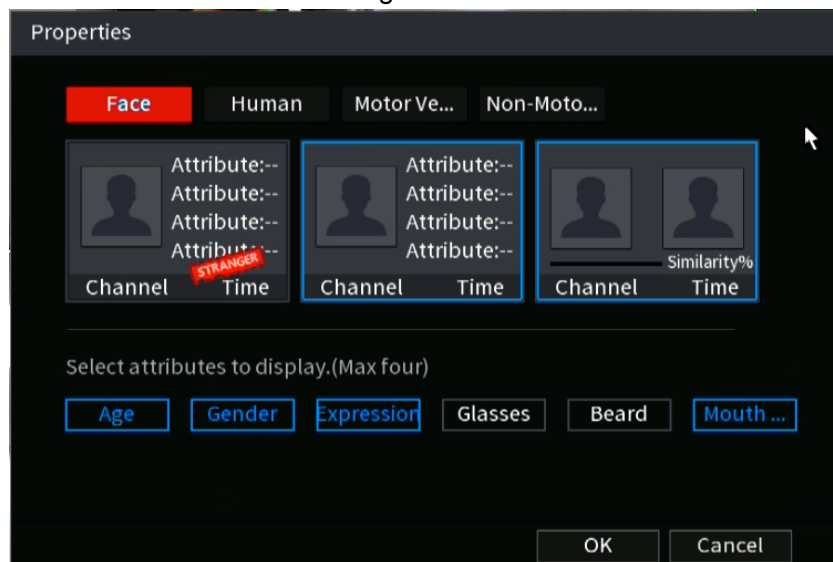
Step 4 (Optional) Click the **Face** tab to select attributes to display, including age, gender, expression, glasses, beard and mask.

Step 5   (Optional) Click the **Human** tab to select attributes to display, including top, pants, hat, bag, bag style, umbrella, age and gender. See Figure 4-87.

Figure 4-87
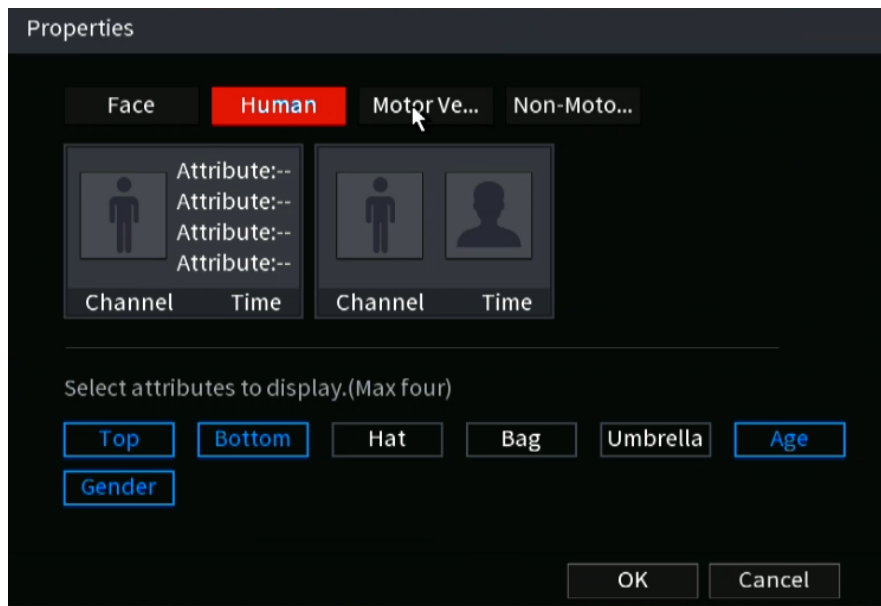
Step 6 (Optional) Click the **Vehicle** tab to select attributes to display, including vehicle logo, vehicle color, vehicle model, plate recognition, plate color, seatbelt, call, vehicle decorations and countries & regions. See Figure 4-88.

Figure 4-88
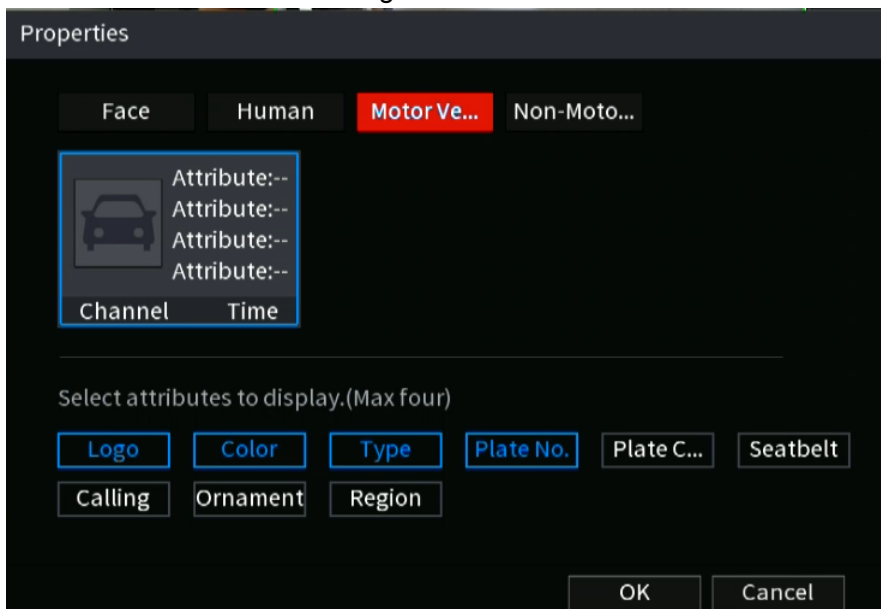
Step 7 (Optional) Click **Non-Motor** and select attributes to display, including color, type and people number. See Figure 4-89.

Figure 4-89

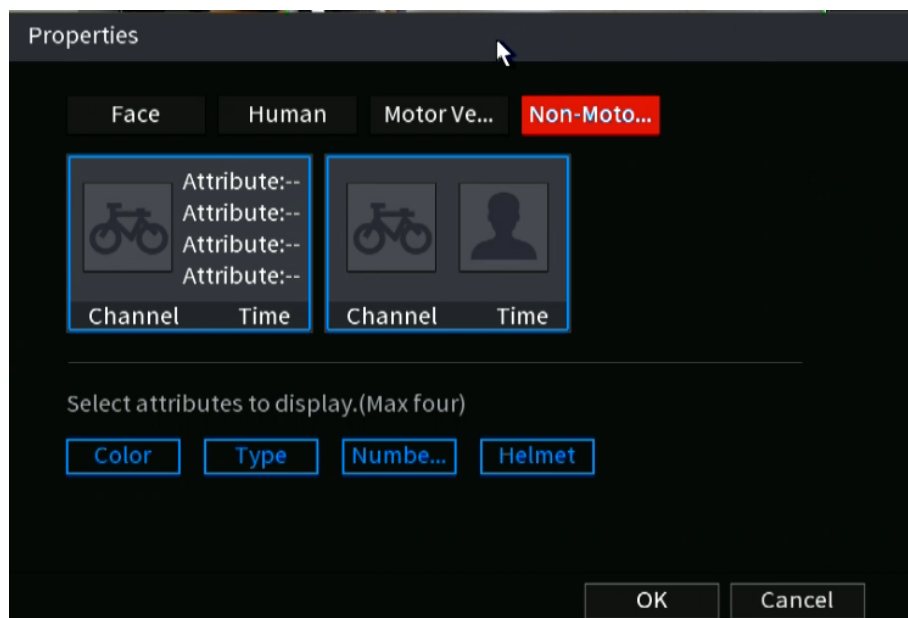

Step 8   Click **OK** to complete the setting.

The system can display four attributes at most.

4.4 PTZ

PTZ (Pan, Tilt and Zoom) IP Cameras that are added to the NVR can be controlled by the NVR.

Before you control a coaxial PTZ, make sure the PTZ decoder is connected to the NVR and the RS-845 wires are connected to the recorders rear panel (A/B inputs).

4.4.1 PTZ Settings

This section configures the different PTZ parameters for local or remote type. Before you use a coaxial PTZ, make sure you have set PTZ protocol. Otherwise, you cannot control the PTZ.

● **Local:** For PTZ control when NVR is connected to PTZ via RS-485.
● **Remote:** (recommended) For IP PTZ devices. NVR sends commands over network to PTZ.

Step 1   Select **Main menu** > **Advanced Settings > Camera Configuration** > **PTZ**.

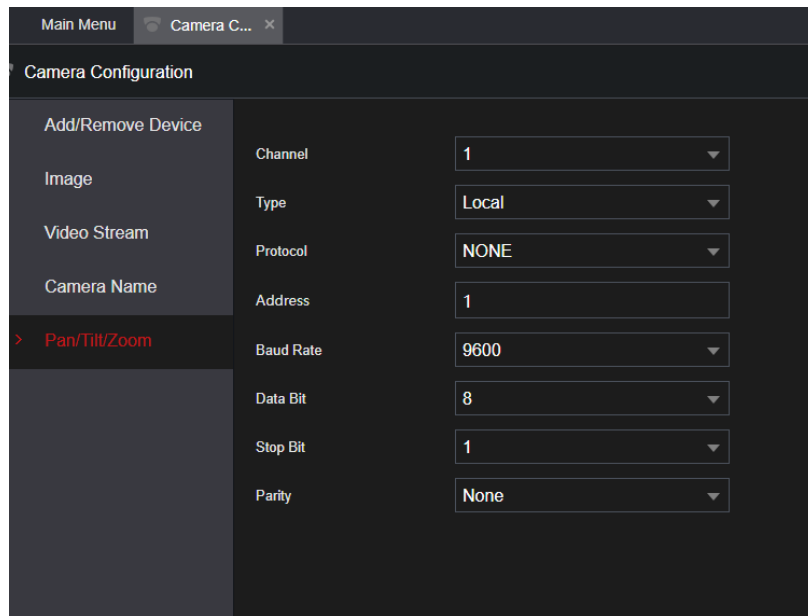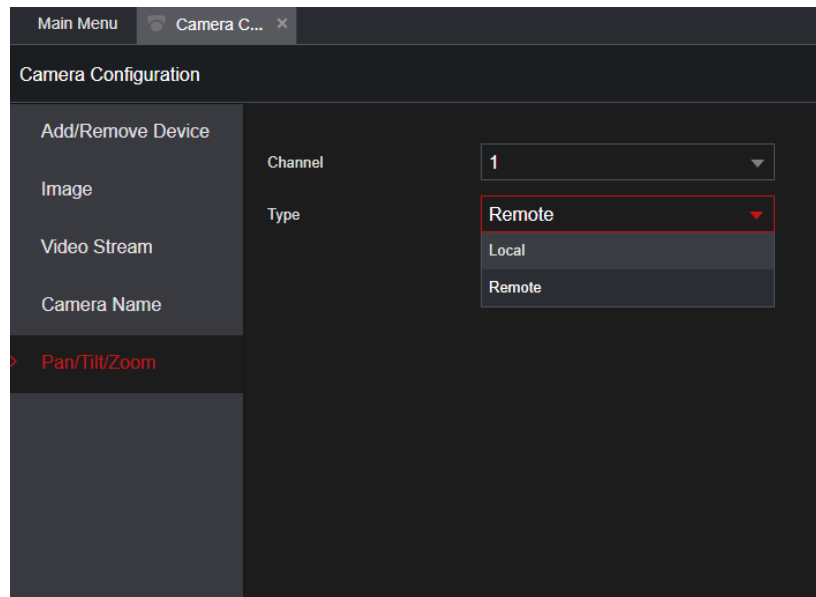The **PTZ** interface will be displayed. See Figure 4-92 or Figure 4-93.

Figure 4-92

Figure 4-93

Step 2   Configure parameters. See Table 4-26.

Table 4-26

Parameter	Description
Channel	In the Channel list, select the channel of the PTZ you want to configure.
Type	● Local: Connect PTZ via serial cable to RS-485 port. ● Remote: Connect through the network by adding the IP address of the PTZ camera to the NVR.
Protocol	In the Protocol list, select the protocol for the PTZ camera such as PELCOD.
Address	In the Address box, enter the address for the PTZ camera. The default is 1. The entered address must be the same as the address configured on the PTZ camera, otherwise, the system cannot control the PTZ camera. Some PTZs will show this information upon bootup initialization.
Baud rate	In the Baud rate list, select the baud rate for the PTZ camera. The default is 9600. The Baud rate must match the PTZ settings.
Data Bit	The default value is 8.
Stop Bit	The default value is 1.
Parity	The default is value NONE.

Step 3   Click **Apply**.

4.4.2 PTZ Control

PTZ control panel allows operations such as moving the camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

4.4.2.1 Basic PTZ Control Panel

Right-click on the live view screen and then select PTZ. The PTZ control panel will be displayed.

Figure 4-94
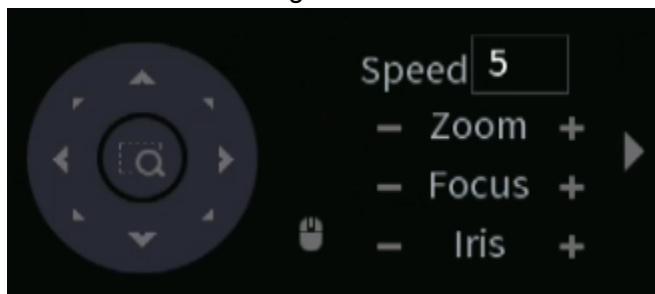
● The gray button indicates that the NVR does not support the current function.
● For some series products, the PTZ function is only active in one-window mode.

Table 4-27

Parameter	Description
Speed	Controls the movement speed. The greater the value, the faster the movement of the PTZ will be.
Zoom	▬ : Zoom out. ✚ : Zoom in.
Focus	▬ : Focus far. ✚ : Focus near.
Iris	▬ : Iris close: Causes image to become darker. ✚ : Iris open: Causes image to become brighter.
PTZ movement	Controls the movement of the PTZ in eight directions.
⊙	Fast positioning button. ● Positioning: Click ⊙ to enter the fast positioning mode, and then click anywhere on the live view screen, the PTZ will turn to this point and zoom to the middle of the screen. ● Zooming: On the fast positioning screen, drag to draw a square on the live view. The PTZ will zoom in on the square. ● Dragging upward will to zoom out, and dragging downward will zoom in. ● The smaller the square is drawn, the greater the zoom effect. 📖 This function is for some products only and can only be controlled through mouse operations.
🖱	Click 🖱, to control the four directions (left, right, up, and down) PTZ movement through mouse operation.
▶	Click ▶ to open the expanded option PTZ control panel.

4.4.2.2 Expanded PTZ Control Panel

On the basic PTZ control panel, click ▶ to open the expanded PTZ control panel to find more options. See Figure 4-95.

Figure 4-95
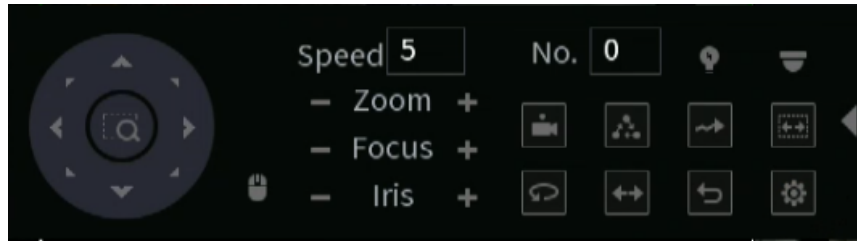
- ● The functions that are grayed out are not supported by the system.
- ● Right-click once to return to the interface of the PTZ basic control panel.

Icon	Function	Icon	Function
🎥	Preset: a pre-set static position	↺	Pan: Moves left and right
⛭	Tour: Moves between presets	↔	Flip: Flips image
→	Pattern: Recorded set of movements that the PTZ will follow	↩	Reset: Resets PTZ
↔	Scan: PTZ moves left-right with set limits.	⚙	**AUX Config** icon: Opens the PTZ functions setting interface.
💡	AUX Switch: For Auxiliary features such as Wiper.	▽	**Enter Menu** icon: Opens the **PTZ Menu** interface.

4.4.3 Configuring PTZ Functions

4.4.3.1 Configuring Presets

<u>Step 1</u>   On the expanded PTZ control panel, click ⚙.
The **Preset** interface will be displayed. See Figure 4-96.

Figure 4-96
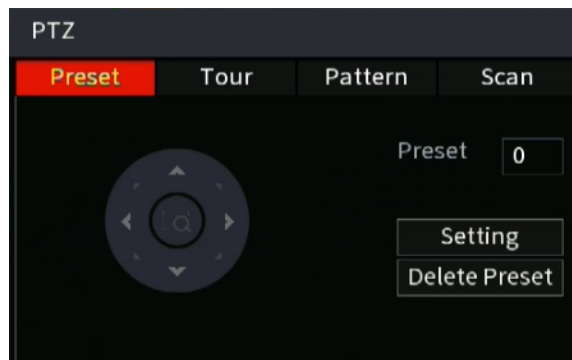
Step 2   Click on the directional arrows to move the PTZ to the required position.

Step 3   In the **Preset** box, enter the value to represent the required position.

Step 4   Click **Setting** to save and complete the preset settings.

4.4.3.2 Configuring Tours

Step 1   On the expanded PTZ control panel, click ⚙.

The **PTZ** interface will be displayed.

Step 2   Click the **Tour** tab.

The **Tour** tab will be displayed. See Figure 4-97.

Figure 4-97
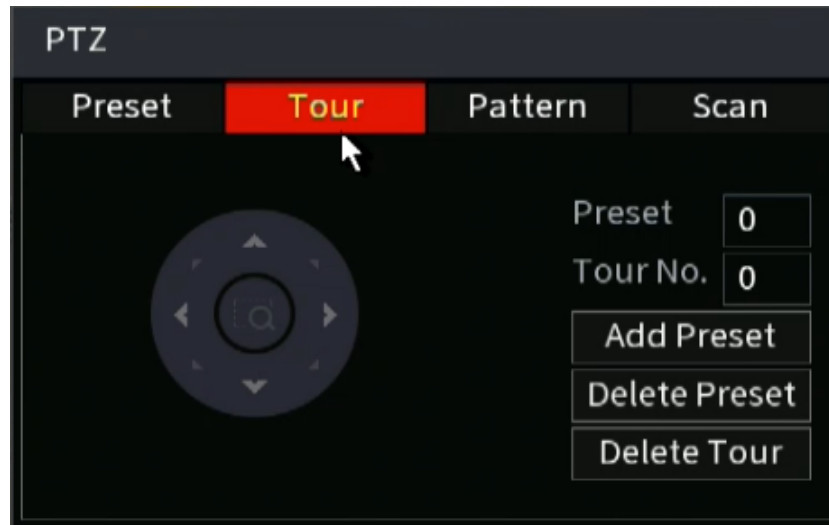
Step 3   In the **Tour No.** box, enter the value for the tour route.

Step 4   In the **Preset** box, enter the preset value.

Step 5   Click **Add Preset**.

A preset will be added for this tour.

📖

- You can repeat adding more presets.
- Click **Delete Preset** to delete the preset for this tour. This operation can be repeated to delete more presets. Some protocols do not support deleting.

4.4.3.3 Configuring Patterns

Step 1   On the expanded PTZ control panel, click ⚙.

The **PTZ** interface will be displayed.

Step 2   Click the **Pattern** tab.

The **Pattern** interface will be displayed. See Figure 4-98.

Figure 4-98
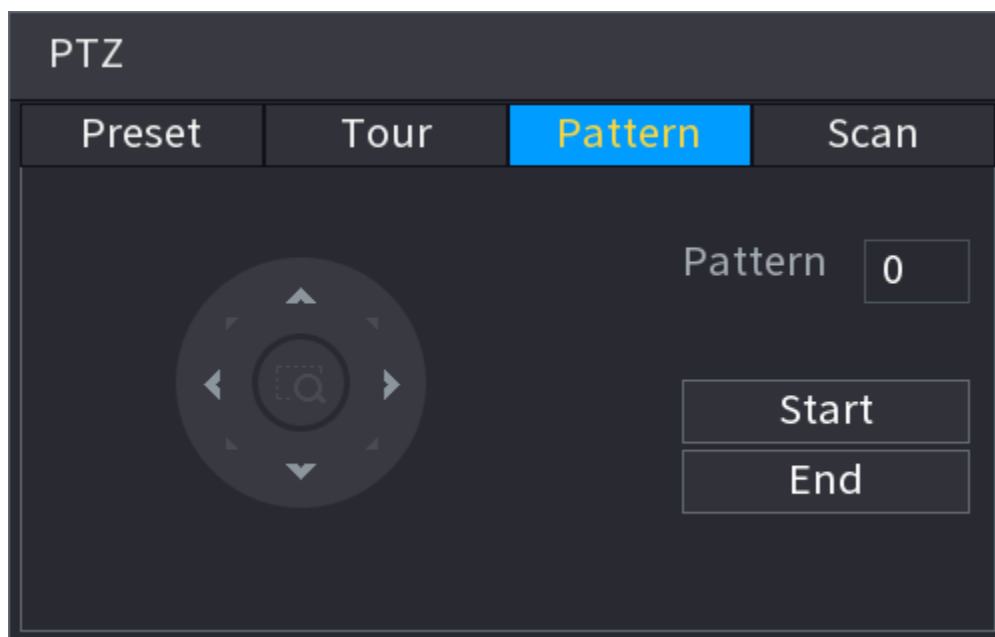
Step 3   In the **Pattern** box, enter the value for the pattern.

Step 4   Click **Start** to and move the PTZ accordingly. You can also go to the PTZ Control Panel to perform the operations of adjusting zoom, focus, iris, and directions.

Step 5   On the **PTZ** interface, click **End** to save and complete the setting.

4.4.3.4 Configuring AutoScan

Step 1   On the expanded PTZ control panel, click [icon].

The **PTZ** interface will be displayed.

Step 2   Click the **Scan** tab.

The **Scan** interface will be displayed. See Figure 4-99.

Figure 4-99
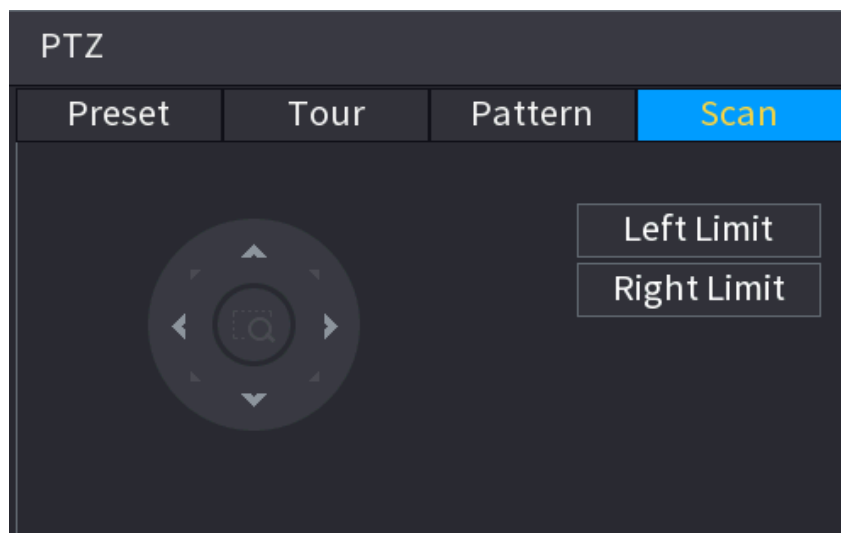
Step 3   Click the direction arrows to position the left and right limits.

4.4.4 Calling PTZ Functions

After you have configured the PTZ settings, you can call the PTZ functions from the Expanded PTZ Control Panel. See Figure 4-100.

Figure 4-100
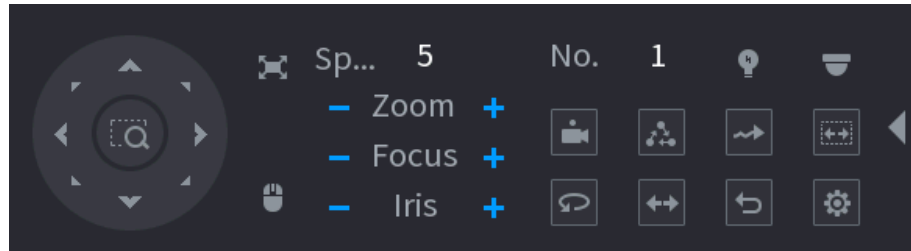
4.4.4.1 Calling Presets

Step 1   On the expanded PTZ control panel, in the **No.** box, enter the value of the preset that you want to call.

Step 2   Click [icon] to call the preset.

Step 3   Click [icon] again to stop calling the preset.

4.4.4.2 Calling Tours

Step 1   On the expanded PTZ control panel, in the **No.** box, enter the value of the tour that you want to call.

Step 2   Click [icon] to call the tour.

Step 3   Click [icon] again to stop the tour.

4.4.4.3 Calling Patterns

Step 1   On the expanded PTZ control panel, in the **No.** box, enter the value of the pattern that you want to call.

Step 2   Call [icon] to call the pattern.

Step 3   The PTZ camera moves according to the configured pattern repeatedly.

Step 4   Click [icon] again to stop performing the pattern.

4.4.4.4 Calling AutoScan

Step 1   On the expanded PTZ control panel, in the **No.** box, enter the value of the border that you want to call.

Step 2   Click [icon].

Step 3   The PTZ camera will perform scanning according to the configured borders.

Step 4   Click [icon] again to stop auto scanning.

4.4.4.5 Calling AutoPan

Step 1   On the expanded PTZ control panel, click ⟳ to start moving in a horizontal direction.

Step 2   Click ⟳ again to stop moving.

4.4.4.6 Using Auxiliary Button

On the expanded PTZ control panel, click 🔘, the AUX setting interface will be displayed. See Figure 4-100.

In the **Shortcut Aux** list, select the option that corresponds to the applied protocol.

In the **Aux No.** box, enter the number that corresponds to the AUX switch on the decoder.

Figure 4-101
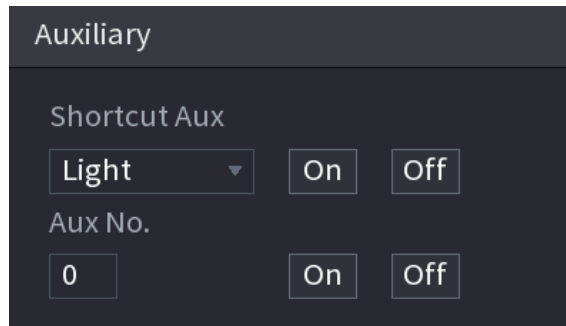
4.5 Record File

The NVR is set for 24-hour continuous record by default. It supports customized record period and record types. Refer to "4.1.4.6 Schedule" for detailed information.

4.6 Playback and Search

4.6.1 Instant Playback

This allows a quick view of the previous 5 to 60 minutes of recordings on a channel. Refer to "4.3.2 Navigation bar" for instant playback information.

4.6.2 Search Interface

You can search and playback the recorded files on the NVR.

Select **Main Menu** > **Playback**, or right-click on the live view interface and then select **Playback**, the search and playback interface will be displayed. See Figure 4-102.

📖

The following figure is for reference only. The actual NVR GUI may have slight changes.

Figure 4-102
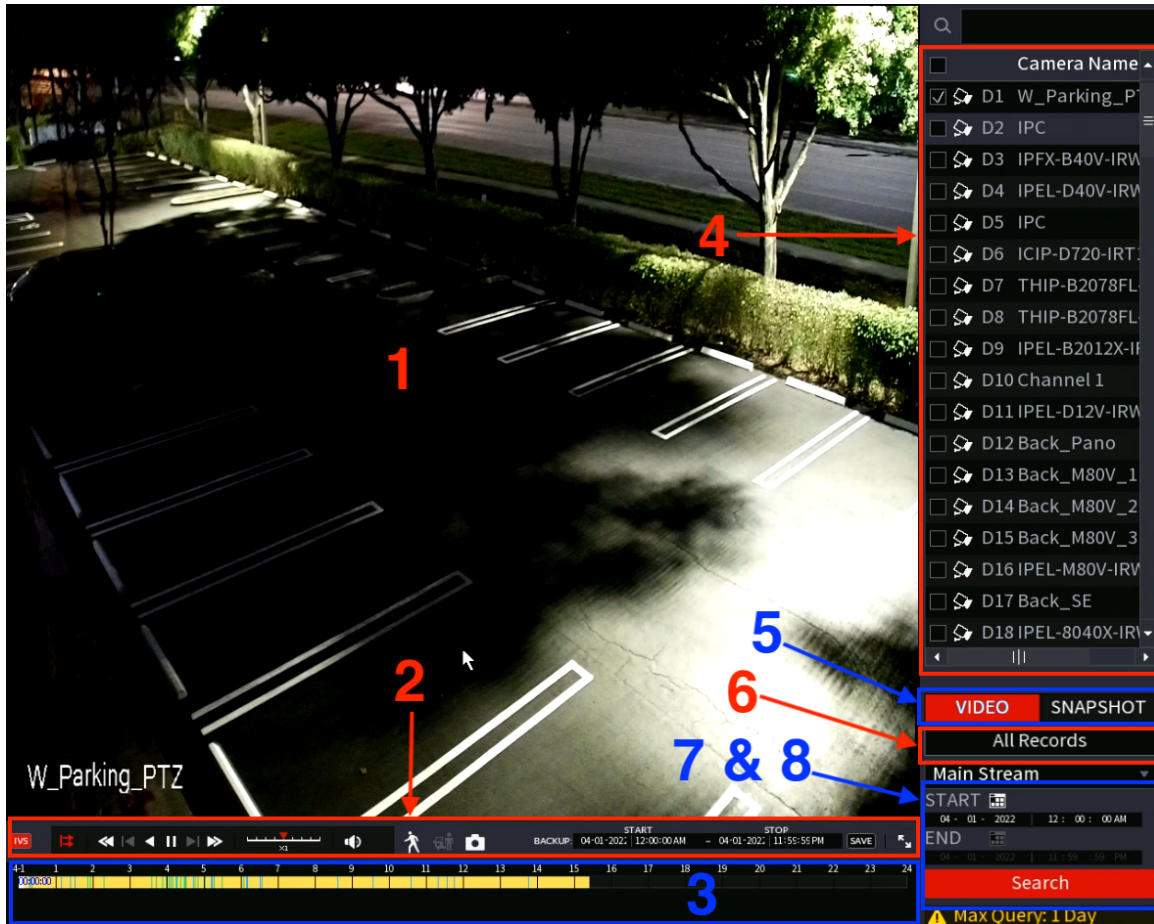
Table 4-28

No.	Function	Description
1	Display Window	Displays the searched recorded video or picture. Depending on the mode, the NVR can support playing in single-channel, 4-channel, 9-channel, and 16-channel simultaneously. 📖 Digital Zoom: When playing back in a single channel mode, hold down the left mouse button to select the area that you want to enlarge. The area will be enlarged after the left mouse button is released. To exit the enlarged status, right-click on the image.
2	Playback Controls Bar	Playback control buttons. Refer to "4.6.2.1 Playback Control" for detailed information.
	Backup (Start & Stop)	Used to specify desired time period you wish to export / save to a USB. Refer to "4.6.2.3 Download Video of Specified time" for detailed information.
	Save	Click "Save" to backup the specified clip. Refer to "4.6.2.4 Video Backup" for detailed information.

3	Time Bar	Displays the record type and time period during playback.
		• Up to 4 channels can be displayed with an independent time bar. Viewing over 4 channels will show only a single time bar.
		• Click on the colored area to start playback from a desired time.
		• To zoom in on the time bar, hover the mouse over the time bar while a recorded file is playing and scroll the mouse wheel down. Scroll down to zoom out.
		• Time bar colors: Green indicates constant recording; Red indicates external alarm events; Yellow indicates motion detection; Blue indicates intelligent events; Purple indicates POS events.
		• To view footage along the time bar, click and hold the time bar, and the mouse pointer will change to a hand icon, and then you can drag the time bar to the desired point.
		• Drag the vertical orange line on the time bar to view the playback in iframe format.
		• For some models, If you are clicking on the blank area in the time bar, the system will automatically move to the next time point where there is a recorded video located.
4	View Layout and Channel Selection	• In the **Camera Name** list, select the channel(s) that you want to play back. • The window split is decided by how many channel(s) you selected. • For example, if you select one channel, the playback will be displayed in the single-channel view; if you select two to four channels, the playback will be displayed in the four-channel view. The maximum is eight channels.
5	Search type	Select the content to play back: **VIDEO** or **SNAPSHOT**. For details about the selecting search type, refer to "4.6.2.2 Search Type" for detailed information.
6	Record type	Select to define the recording type to search for. By default it will search for all events but can be changed to IVS or Motion for example.
7	Date & Time	Enter the date that you want to search, the time bar displays the corresponding record. Selecting the calendar icon will open the calender to choose a date. Dates with a solid circle under the date have footage saved. It does not guarantee all channels have footage.

8	Search List Display	After setting desired time and selecting "Search" the File List will display. ● **File List**: Displays the available stored events / files in order based on time stamp.

📖

All the operations above (such as playback speed, channel, time and progress) are dependent on hardware of the NVR model. Some of the functions may not be present depending on the NVR model.

4.6.2.1 Playback Control

The playback control interface is shown as below. See Figure 4-103.

Figure 4-103

Refer to the following sheet for more information. See Table 4-29.

Table 4-29

Icon	Function
▶, ⏸	Play/Pause In slow play mode, click to switch between play/pause.
⏹	Stop When playing back, click to stop the current playback process.
◀	Backwards play In normal play mode, left-click the button, and the file will play backward. Click again to pause the current play. In backward play mode, click ▶ or ⏸ to restore normal play.
◀▮▶	Display previous frame/next frame. When pausing the normal playback file, click ◀▮ or ▮▶ to play back frame by frame. In frame by frame playback mode, click ▶ or ⏸ to resume normal playback mode.
▶▮	Slow play In playback mode, click it to realize various slow play modes such as slow play 1, slow play 2, and etc.
▶▶	Fast forward In playback mode, click to enable various fast play modes such as fast play 1, fast play 2 and etc.

🔊	Adjust the volume of the playback.
🚶	Smart search. Used to search for movement/pixel change in a defined area. Refer to "4.6.3 Smart Search Playback" for detailed information.
👥	Intelligent Motion detection. Click the icon to select a human or motor vehicle, and the NVR will play only videos if a person or motor vehicle was detected. 📖 Human and motor vehicle can be selected at the same time.
📷	To take a Snapshot, click the snapshot button in the full-screen mode. The NVR supports custom snap picture saved path. Connect the peripheral device (USB), click snap button on the full-screen mode, then select or create path. Click Start button to save to the specified path.

4.6.2.2 Search Type

This allows you to search the recorded videos, splice, or take snapshots from Disk or an external storage device.

- From R/W Disk: Recorded videos or snapshots playback from HDD of the Device. See Figure 4-104.

Figure 4-104

From R/W Disk ▼
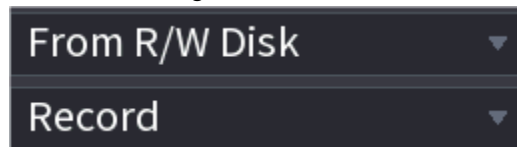
Record ▼

- From I/O Device: Recorded videos playback from an external storage device (such as a USB). See Figure 4-105.
  Click **Browse**, select the file path of the recorded video file that you want to play.
  Double-click the video file or click ▶ to start playing.

Figure 4-105

From I/O Device ▼

sda4 ▼ Refresh

/ Browse
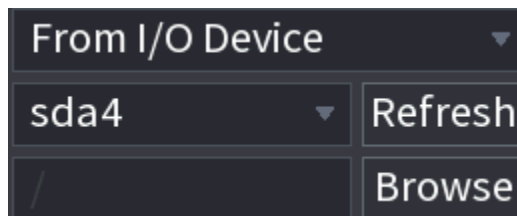
4.6.2.3 Download Video of Specific Time

📖
This function allows you to download and save a specific time of a recorded video to a USB device. See Figure 4-106.

- Clip function is for one-channel/multiple-channel.
- You are able to save a maximum of 1024 files at the same time.

Step 1   Select a recording and then click ▶ to play back.
Step 2   Input the desired starting date and time in the **START** field.
See Figure 4-106.

Step 3   Input the desired ending date and time in the **STOP** field

Step 4   Click the SAVE icon to save the clip file.

Figure 4-106
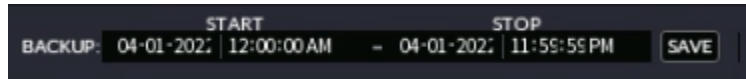
4.6.2.4 Video Backup

This function is to backup files checked in the file list, or the file that was just clipped.
Step 1   Select the recorded video file that you want to back up. You can select the following two types of files:

- Recorded video file: Click ▤ , the File List area will be displayed. Select the file(s) that you want to back up.
- Saves the clip footages as a recorded file.

Step 2   Click 💾 , to display the BACKUP interface. See Figure 4-107.

Figure 4-107
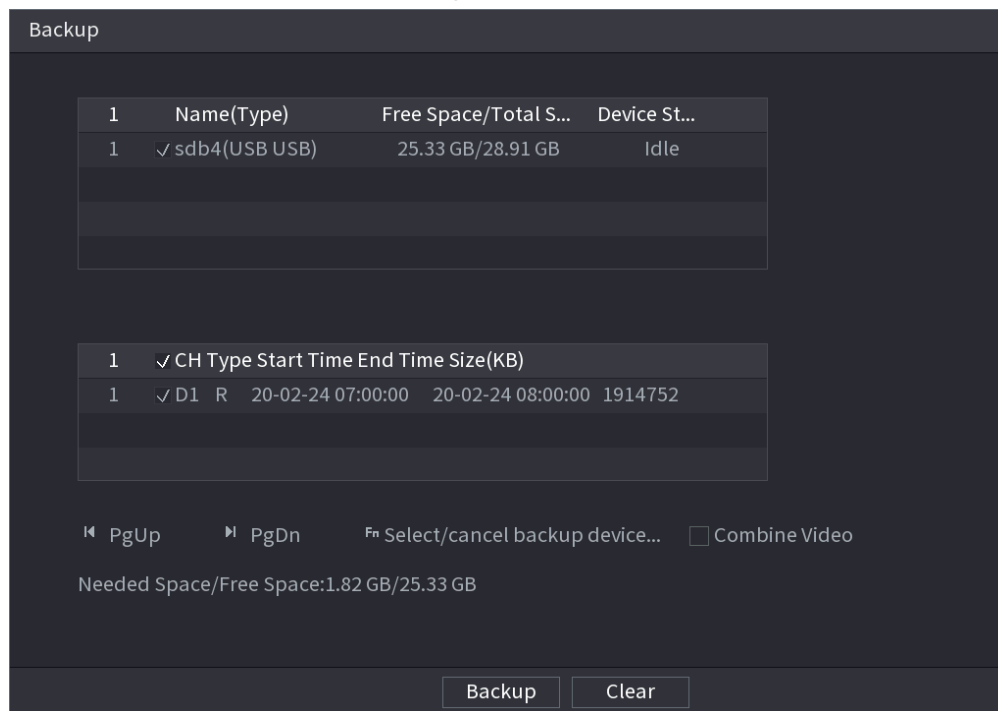
Step 3   Click **Backup** to begin the process.

4.6.3 Smart Search Playback

During the playback process, Smart Search will analyze the motion detect zone in the scene and return results that had triggered motion within the specified zone.

This function is for channels motion detect function enabled (**Main Menu** >

Basic Settings > **Motion Detection**).

Step 1   Select a channel to play back video and then click ⼈. A 22x15 area grid will populate on the played video.

● This function is only supported with one-channel playback mode.
● If you are in multiple-channel playback mode, double-click a channel to switch to one-channel playback mode.

Step 2   Left click mouse and then drag to select smart search zones.

Step 3   Click ⼈   to enable Smart Search to analyze. The results on the time line will display any motion within the specified zones.

Step 4   Click ⼈   again to exit the Smart Search function.

● The motion detect zone created cannot be the entire full screen area.
● The motion detect region will display the current single play pane by default.
● If selecting another file on the list, the NVR will play the motion detect footage of the other file.
● The time bar unit switch, backward play, frame by frame are disabled when the NVR is playing the motion detect file.

4.6.4 Picture Search Playback

This function allows you to select an image of the target person on the playback interface and then search by image for all the related videos with the target person.

Right-click on the live view interface and then select **Search** to show the search interface.

Select a channel to play back video and then click 🔍   to pause the playback.

For more details, see "4.3.3.8 Picture Search".

This feature is not available on all units. Only available on select special units or is still in development.

Figure 4-108 Picture search playback
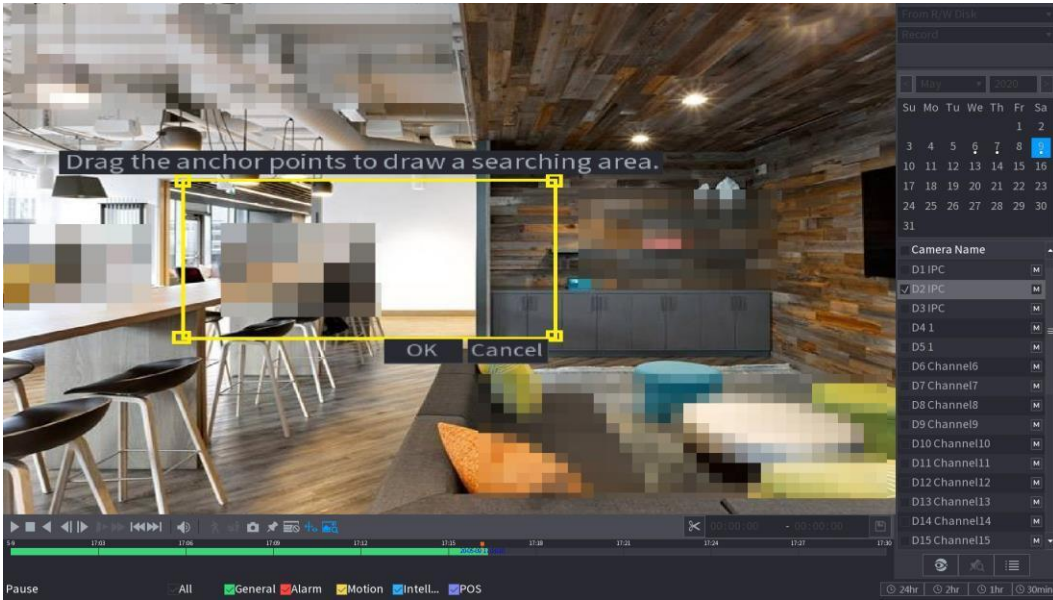
4.6.5 Tag Playback

When playing back a video record, you can tag the record as necessary. After playback, you can use time or the tag keywords to search the corresponding record to play. This allows quick and easy search indexing.

📖 **This feature is not available on all units. Only available on select special units or is still in development.**

4.6.5.1 Add Tag

When the NVR is playing back, click the 📌 icon to view the following interface. Input the Tag under **Tag Name** then click **OK**. See Figure 4-109.

Figure 4-109
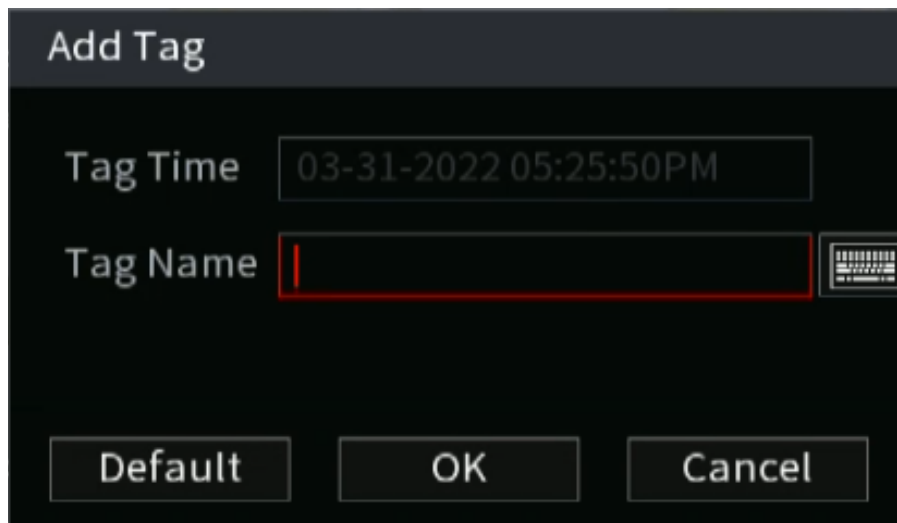
4.6.5.2 Play back Tagged files

During 1-window playback mode, click 🔧 in Figure 4-102, to toggle the tag file list interface. Double-click one tagged file to begin playback from the tagged time.

4.6.5.3 Tag Manager
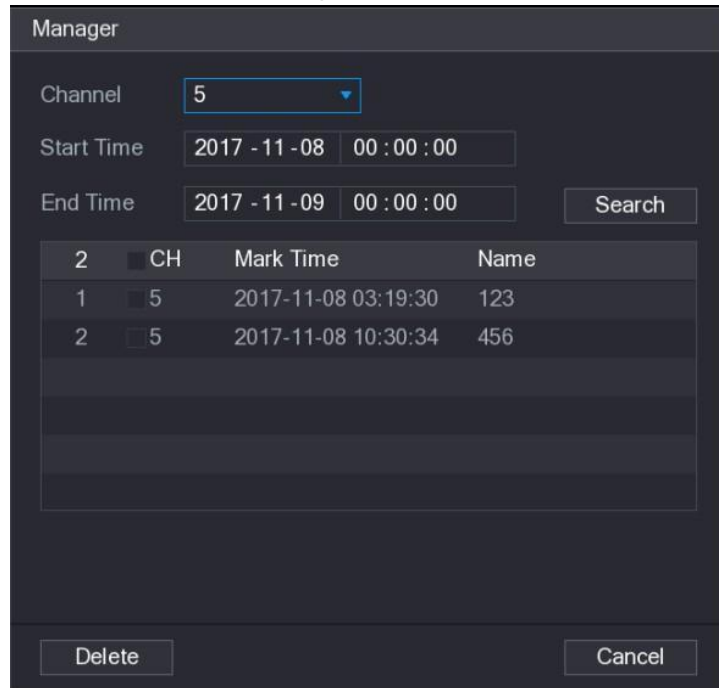
Click the mark manager button ![icon] on the Search interface (Figure 492); to navigate to the Tag Manager interface. See Figure 4-110. The NVR can manage all the record-tagged information of the current channel by default. You can view tagged information of the current channel by time.

Figure 4-110

4.6.5.4 Modify

Double-click a tag information item to populate a dialogue box to change tag information. You can only change the tag name here.

4.6.5.5 Delete

Here you can check in the tag information item you want to delete and then click **Delete** to remove one tag item.

📖

After you go to the tag management interface, the NVR will pause the current playback. It will resume playback after you exit the tag management interface.
If the tag file you want to playback has been removed, system will playback the first file in the list.

4.6.6 Playback Image

This function allows to search and view snapshots. Follow the steps listed below.

Step 1   Select **Main Menu** > **Playback**, or right-click on the live view window and select **Playback** to view the **Playback** interface.

Step 2   At the upper-right corner, select image and then input playback interval.

Step 3   Select date and channel, click ▶ to play.

4.6.7 Subperiod Playback

This function allows you to clip recorded video files into splices and then play back at the same time.

📖 **This feature is not available on all units.**

Step 1   Select **Main Menu** > **Playback > Playback**.
The **SEARCH** interface will be displayed.
Step 2   In the Search Type list, select **Subperiod**; In the Split Mode list, select 4, 8, or 16.
See Figure 4-111.

Figure 4-111
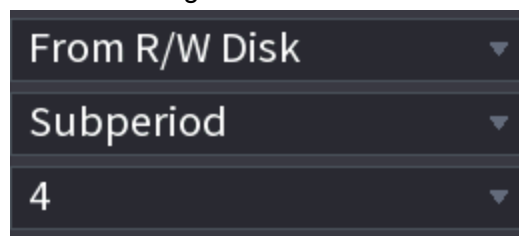
Step 3   In the **Calendar** area, select a date.
Step 4   In the **Camera Name** list, select a channel.

Step 5   Start playing back splices. See Figure 4-112.
Click ▶, the playback starts from the beginning.
Double-click anywhere on the time bar, the playback starts from where you click.

Figure 4-112

4.6.8 File List

Click 📱, the NVR will display the file list. It displays the first channel of the record. See Figure 4-113.

Figure 4-113
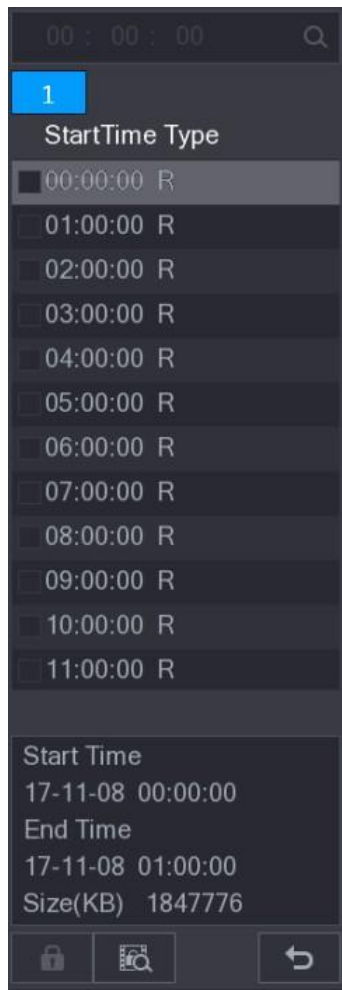
- To play a file, check a file name, then double-click the file or click ▶.
- To search records of current day, input the desired time at the top column.
- The NVR will display a maximum of 128 record files in one list.
- To go back to the calendar/channel selection interface, click ↩

Lock or Unlock File

- To lock the recorded video on the **File List** interface, select the check box of the recorded video, and then click the 🔒 icon. The locked video will not be overwritten.
- To view the locked information, click 🔍, the **File Lock** interface will be displayed.

> Any recorded video that is under writing or overwriting process cannot be locked.

- To unlock the recorded video, in the **File Lock** interface, select the video, and then click **Unlock**. See Figure 4-114.

Figure 4-114

File Lock					
3	☐ Cha...	Type	Start Time	End Time	Size(KB)
1	☐ D1	R	2019-12-01 08:00:00	2019-12-01 09:00:00	35072
2	☐ D1	R	2020-01-04 06:00:00	2020-01-04 07:00:00	35712
3	☐ D1	R	2020-02-24 14:00:00	2020-02-24 15:00:00	1914816

Unlock   Cancel

4.6.9 Other Aux Functions

4.6.9.1 Digital Zoom

In 1-window playback mode, left click mouse to select any zone on the screen, you can zoom in the current zone. Right click the mouse to exit.

4.6.9.2 Switch Channel

- During playback mode, select from the drop-down list to switch playback channel.
- The smart search channel does not support this function either.

4.7 AI

4.7.1 AI Search

The AI Search allows specific search results based on Intelligent Events such as IVS rules, Face, human and vehicle recognition, and Heat Map.

📖

Typically the AI events are camera based, meaning the IP camera must support the necessary AI or IVS events to properly work with the NVR..

4.7.1.1 Face Detection

You can search the detected faces and play back recordings.

Step 1   Select **Main Menu** > **Playback** > **Advanced Search** >

Face Detection.

The **Face Detection** interface will be displayed. See Figure 4-115.

Figure 4-115
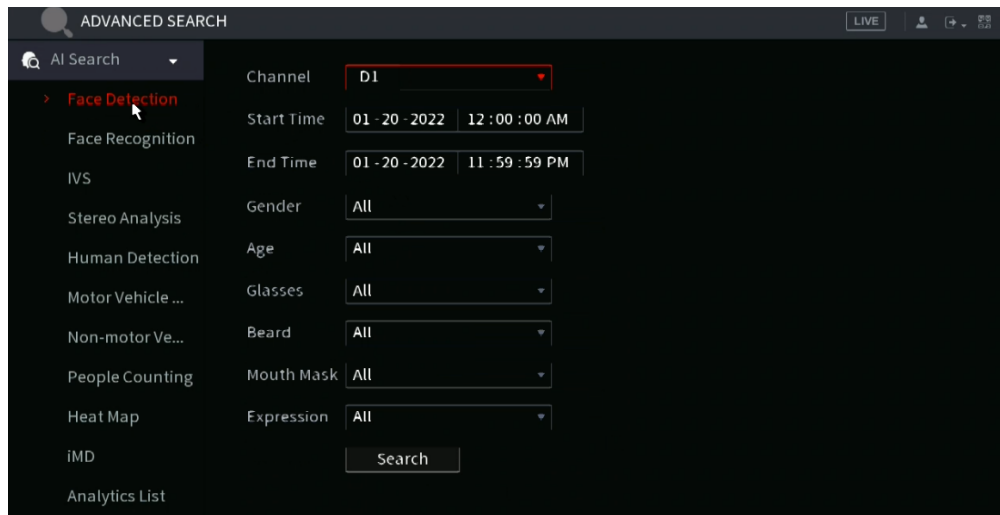
Step 2   Select the channel, then enter the start time and end time. Select the desired values for the gender, age, glasses, beard, and mask. Click **Search** to display the results. See Figure 4-116.

📖

For privacy reasons, the faces in the sample images are pixelated. The actual image will be clear.

Figure 4-116
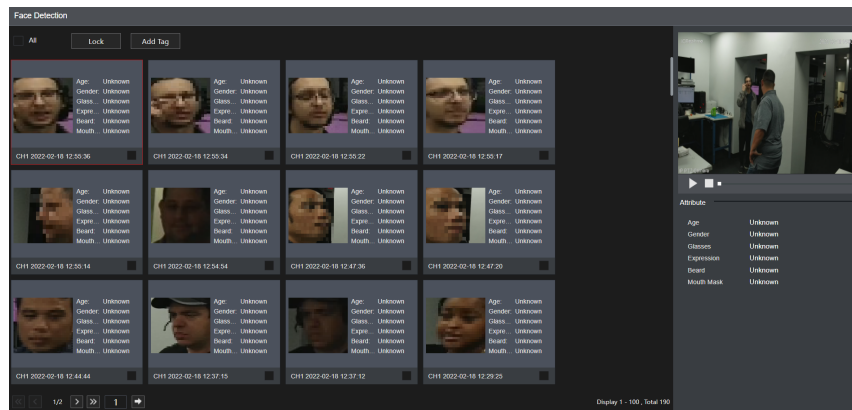
Step 3   Select the face that you want to view the play back for.
The picture with registered information will be displayed.
Other functions here include:
● Click **Export** to export results in Excel format.
● To back up the recorded files to the external storage device, select the files, click **Backup**, select the save path and file type, and then click **Start**. See Figure 4-117.

Figure 4-117
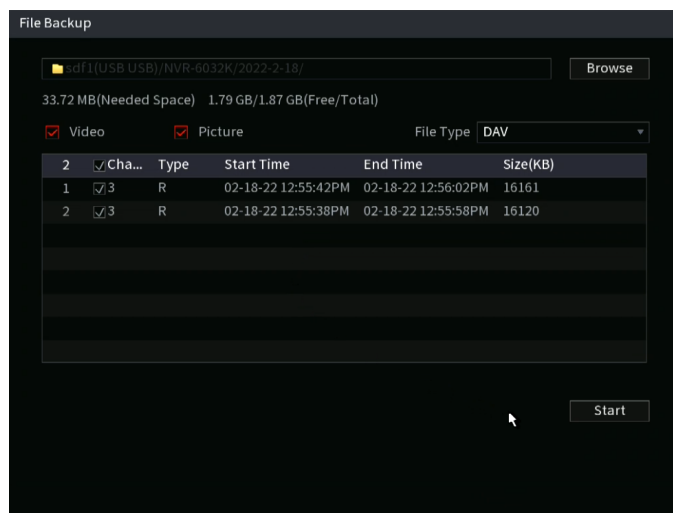
- To make the files unable to be overwritten, select the files, and then click **Lock**.
- To add a tag to the file, select the files and then click **Add Tag**.
- Click **Add to Face Database** and enter corresponding information in the displayed interface, and then add the picture to the face database.

Figure 4-118 Add face pictures to database
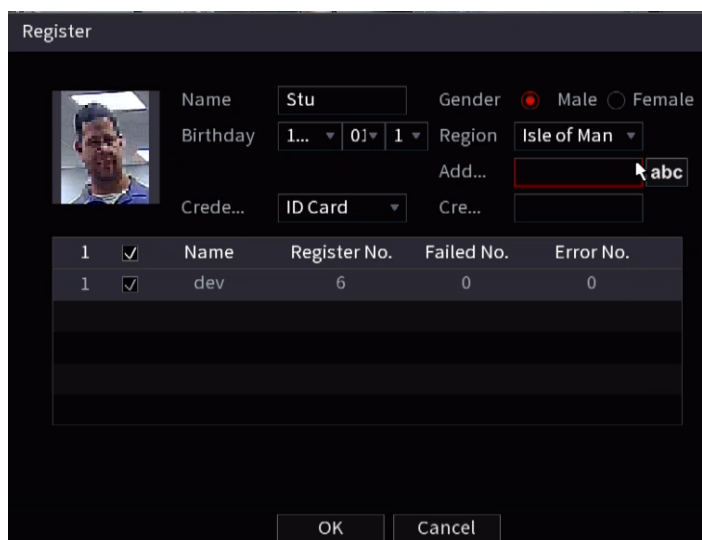
4.7.1.2 Face Recognition

The Face recognition function allows the search and comparison of recorded human faces with the face image on the database, and playback the corresponding record file.

The AI search allows two search parameters: Search by attributes and search by image.

This function is only supported by EL series NVRs and the NVR-FX24POE.

4.7.1.2.1 Searching by Attributes

Step 1   Select **Main Menu** > **Playback** > **Advanced Search** > **Face Recognition** > **Search by Attributes**.

The **Search by Attributes** interface will be displayed. See Figure 4-119.

Figure 4-119
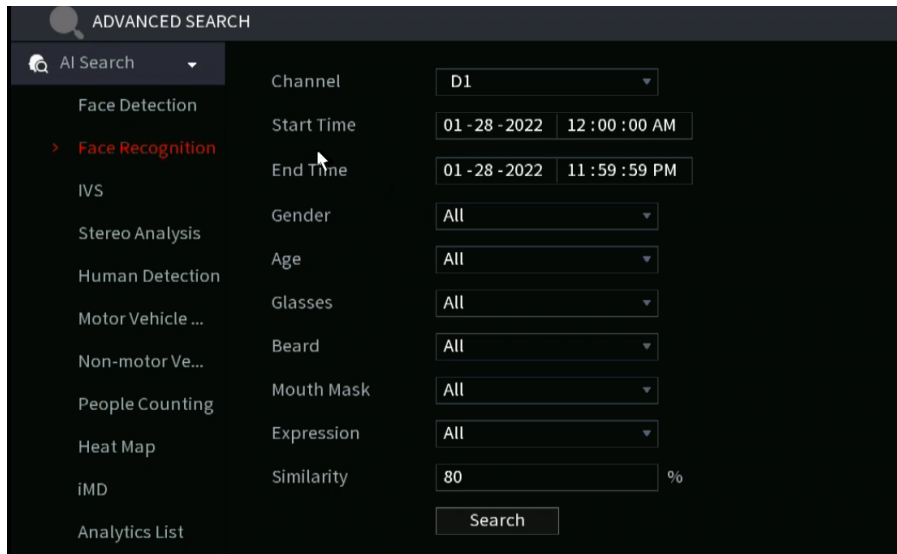
Step 2   Select the channel and set the parameters such as start time, end time, gender, age, glasses, beard, mask, and similarity according to your requirement.

Step 3   Click **Search**.

The search result will be displayed. See Figure 4-120.

Figure 4-120
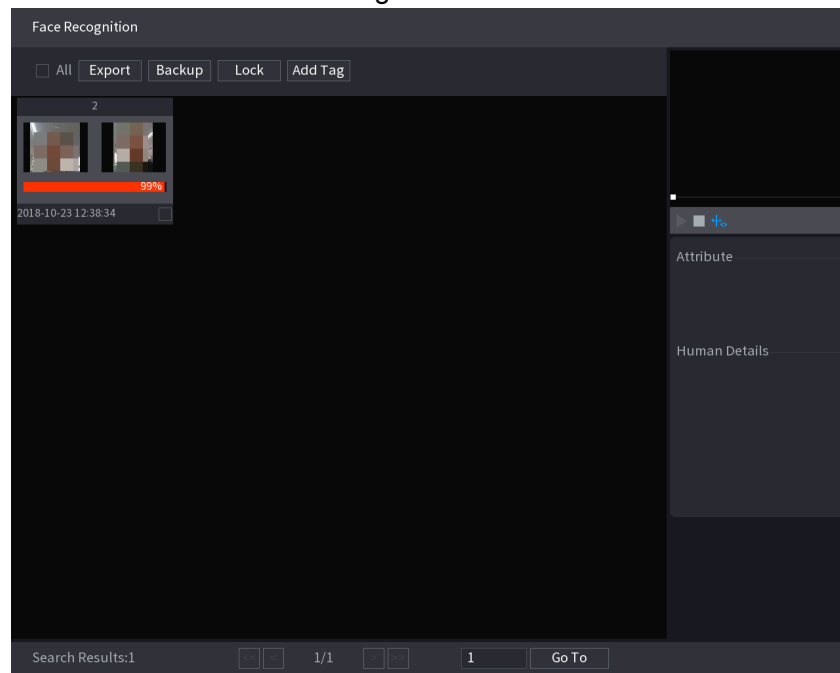
Step 4   Click the picture that you want to play back.

The picture with registered information will be displayed.

You can also do the following operations to the recorded files.

● To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

- To make the files unable to be overwritten, select the files, and then click **Lock**.
- To add a tag to the files, select the files and then click **Add Tag**.
- Navigate to the **Attributes** and **Human Details** to view detailed information.

4.7.1.2.2 Search by Image

Step 1   Select **Main Menu** > **Playback** > **Advanced Search** > **Face Recognition** > **Search by Image**. The **Search by Image** interface will be displayed. See Figure 4-121.

Figure 4-121
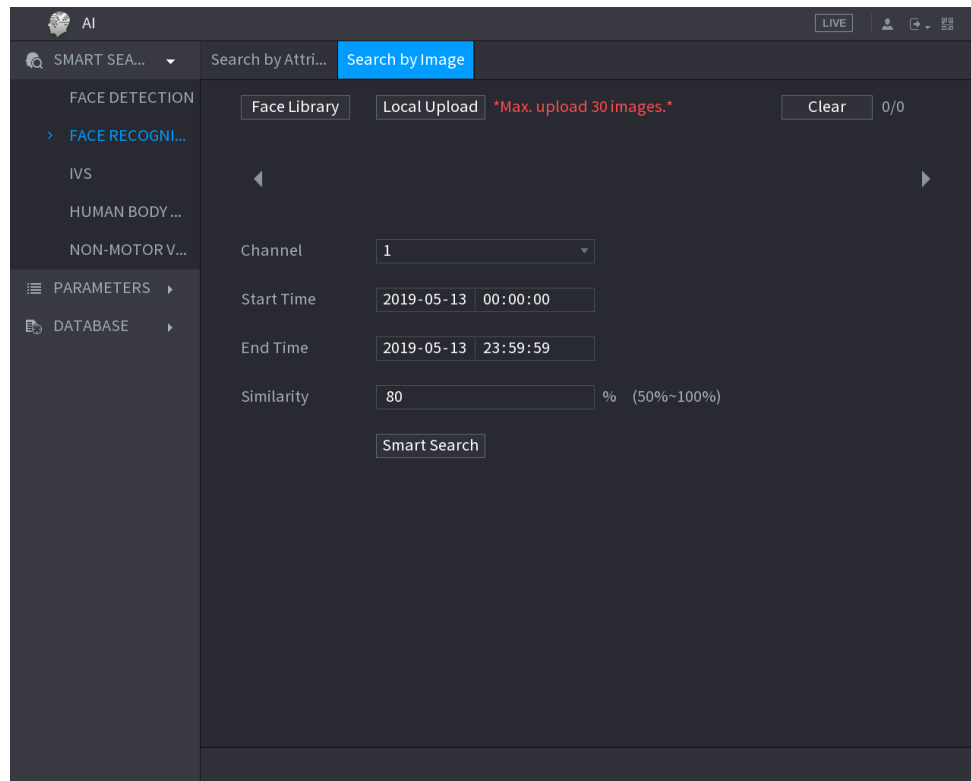
Step 2   Select the channel and set the parameters such as start time, end time, gender, age, glasses, beard, mask, and similarity according to your requirements.

Step 3   Click **Search**. The search result will be displayed. See Figure 4-122.

Figure 4-122
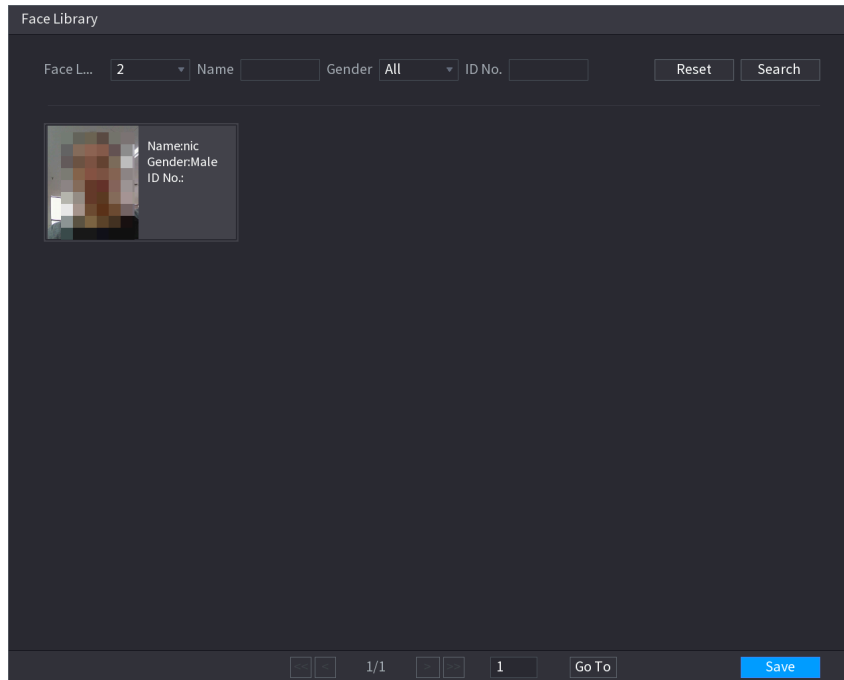
For privacy reasons, the face in the sample image are pixelated. The actual image will be clear.

Step 4   Click the picture that you want to view the play back on.

The picture with registered information will be displayed.

Other functions here include:

- To back up the recorded files to an external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.
- To make the files unable to be overwritten, select the files, and then click **Lock**.
- To add a tag to the file, select the files and then click **Add Tag**.
- Go to the **Face Properties** and **Person Details** to view detailed information.

4.7.1.3 IVS

This function allows you to view IVS based events, such as tripwire or intrusion

Step 1   Select **Main Menu** > **Playback** > **Advanced Search** > **IVS**.

The **IVS** interface will be displayed. See Figure 4-123.

Figure 4-123
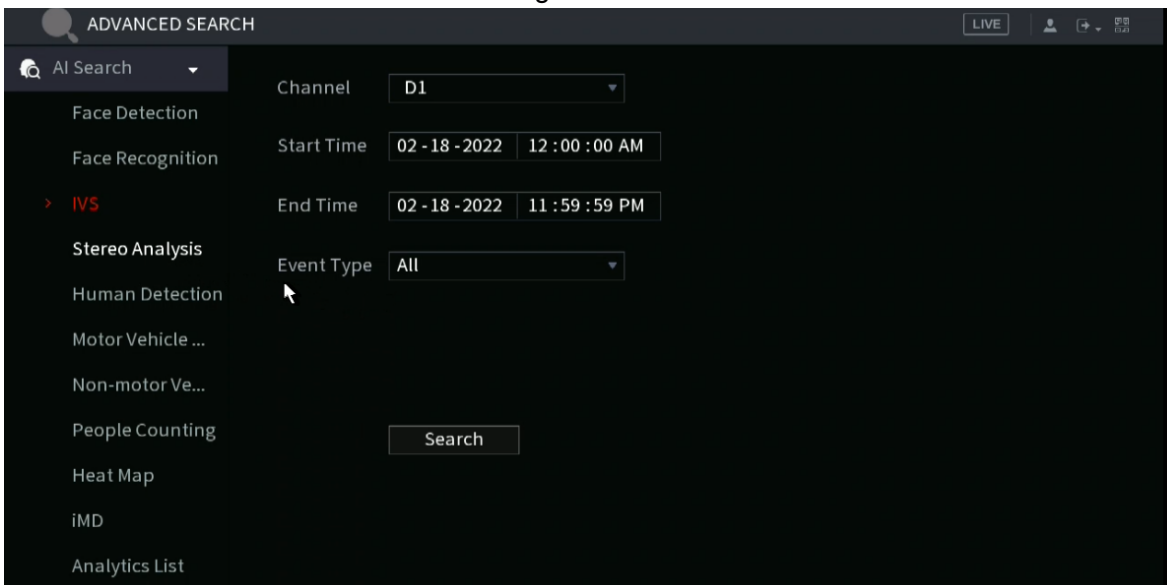
Step 2 Select a channel, start time, end time, event type, and then click **Search**.
The search result will be displayed.

Step 3 Click the picture that you want to play back.
You can also do the following operations to the recorded files:

● To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

● To make the files unable to be overwritten, select the files, and then click **Lock**.

● To add a tag to the file, select the files and then click **Add Tag**.

● Go to the **Attributes** and **Human Details** to view detailed information.

4.7.1.4 3D Analysis

This function allows you to create rules and zones for different event types as well as trigger alarm linkage. Types of events include Approaching Human detection, fall detection, violence detection, and Loitering detection.

📖
● Cameras are required to be mounted up high looking down at objects with preferably 45 degree angle for optimal performance.
● This feature requires IP camera equipped with 3D behavior analysis.
● 3D analysis and IVS are mutually exclusive, and you will need to configure the smart plan in advance.

4.7.1.4.1 People Approach Detection

When two or more people loiter in the detection area for a minimum duration or when the distance between the people reaches the parameter setting, an event will be triggered.

Step 1 Select **Main Menu** > **Advanced**> **Events**> **Parameter** >**3D Analysis**.

Step 2 Select a channel and click **Add**.

Step 3 Select **Enable** and set **Type** to **People Approach Detection**.

Step 4   Click ![icon], and then click and hold the left mouse button to draw an area on the screen.

Step 5   Configure the parameters.

Table 4-30

Parameter	Description
Sensitivity	Configure alarm sensitivity.
Duration	Configure the minimum time of triggering an alarm when people approach.
Repeat Alarm Time	Configures the repeat alarm time. If the alarm status continues, an alarm will be triggered again when the set threshold is reached.
Interval Threshold	When the interval between people in the area is greater than or less than the set interval threshold, an alarm will be triggered.

Step 6   Click **OK**.

4.7.1.4.2 Fall Detection

This event is triggered when a person falls from a height in the detection area and the duration of the action is greater than the minimum duration set by the parameter, an alarm will be triggered.

Step 1   Select **Main Menu** > **Advanced** > **Event > Parameters** > **3D Analysis**.

Step 2   Select a channel and click **Add**.

Step 3   Select **Enable** and set **Type** to **Fall Detection**.

Step 4   Click ![icon], and then click and hold the left mouse button to draw an area on the screen.

Step 5   Configure parameters.

Table 4-31

Parameter	Description
Sensitivity	Configure the alarm sensitivity.
Duration	Sets the minimum time to trigger an event when a fall is detected.
Repeat Alarm Time	Configures the repeat alarm time. If the alarm status continues, an alarm will be triggered again when the set threshold is reached.

Step 6   Click **OK**.

4.7.1.4.3 People Exception Detection

When the number of people based on the alarm type are reached in the same detection area, an event will be triggered.

Step 1   Select **Main Menu** > **Advanced** > **Event > Parameters** > **3D Analysis**. Step

2   Select a channel and click **Add**.

Step 3   Select **Enable** and set **Type** to **People Exception Detection**.

Step 4   Click ![icon], and then click and hold the left mouse button to draw an area on the screen.

Step 5   Configure parameters.

Table 4-32

Parameter	Description
Sensitivity	Configures the alarm sensitivity.
Duration	Set the minimum time of triggering an alarm when the number of people reaches the threshold.
Repeat Alarm Time	Configures the repeat alarm time. If the alarm status continues, an alarm will be triggered again when the set threshold is reached.
Alarm People No.	When the interval between people in the area is greater than or equal to or less than the set interval threshold, an alarm will be triggered.

<u>Step 6</u>   Click **OK**.

4.7.1.4.4 People Retention Detection

When the target stays beyond the set retention time threshold in the detection area, an alarm will be triggered.

<u>Step 1</u>   Select **Main Menu** > **Advanced** > **Event** > **Parameters** > **3D Analysis**.

<u>Step 2</u>   Select a channel and click **Add**.

<u>Step 3</u>   Select **Enable** and set **Type** to **People Retention Detection**.

<u>Step 4</u>   Click ✎ , and then click and hold the left mouse button to draw an area on the screen.

<u>Step 5</u>   Configure the parameters.

Table 4-33

Parameter	Description
Sensitivity	Configures the event sensitivity.
Duration	Set the minimum time of triggering an alarm when people stay in the detection area.
Repeat Alarm Time	Configures the repeat alarm time. If the alarm status continues, an event will be triggered again when the set threshold is reached.
Alarm People No.	When the interval between people in the area is greater than or equal to or less than the set interval threshold, an event will be triggered.

<u>Step 6</u>   Click **OK**.

4.7.1.5 Human Body Detection

This function allows for human body search within the recorded footage based on attributes such as shirt, pants or hat color.

<u>Step 1</u>   Select **Main Menu** > **Playback** > **Advanced Search** > **Human Detection**.

The **Human Detection** interface will be displayed. See Figure 4-124.

Figure 4-124
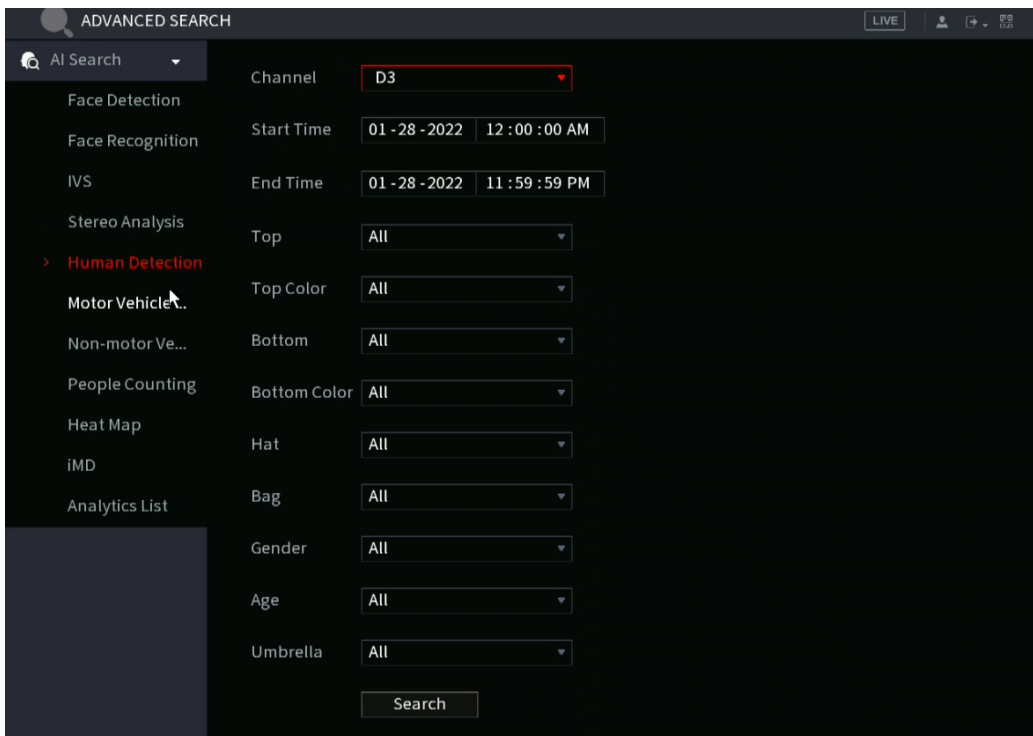
Step 2 Select a channel, start time, end time, and set the corresponding parameters.

Step 3 Click **Search**.

The search result will be displayed. See Figure 4-125.

For privacy reasons, the faces in the sample image are pixelated.

The actual image will be clear.

Figure 4-125
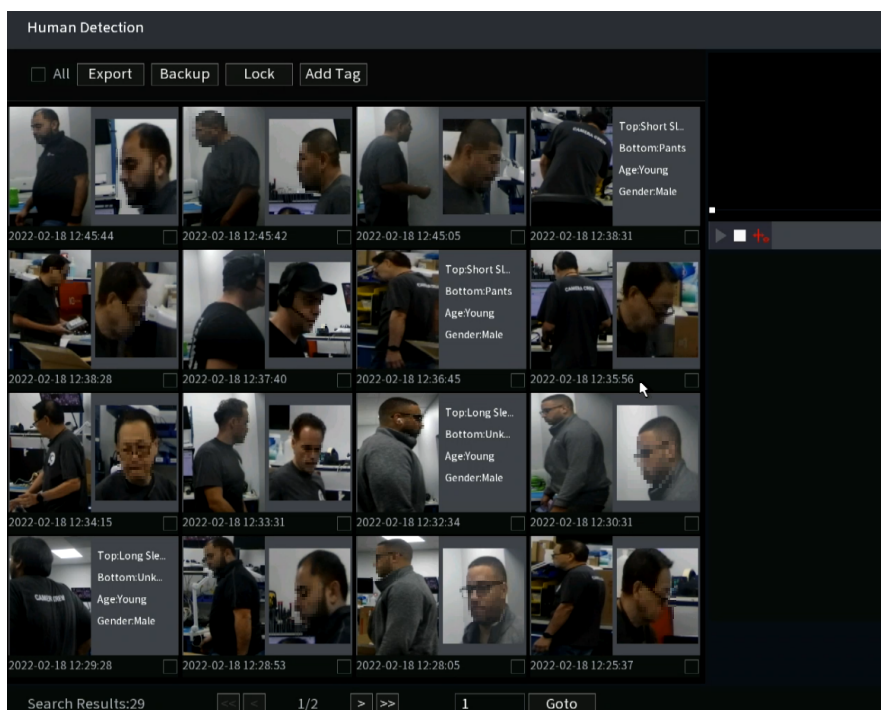
Step 4 Select one or multiple results, to perform the following operations as needed.
- Click **Export** to export results in Excel format.
- To back up the recorded files to an external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.
- To make the files unable to be overwritten, select the files, and then click **Lock**.
- To add a tag to the file, select the files and then click **Add Tag**.
- Click **Add to Face Database** to add the picture to a face database.

4.7.1.6 Vehicle Detection

This allows you to search for vehicles with parameters such as plate number and color.

📖

This function is only supported on select NVR models.

Step 1 Select **Main Menu** > **Playback**> **Advanced Search** > **Motor Vehicle Detection**.
The **Motor Vehicle Detection** interface will be displayed. See Figure 4-126.

Figure 4-126
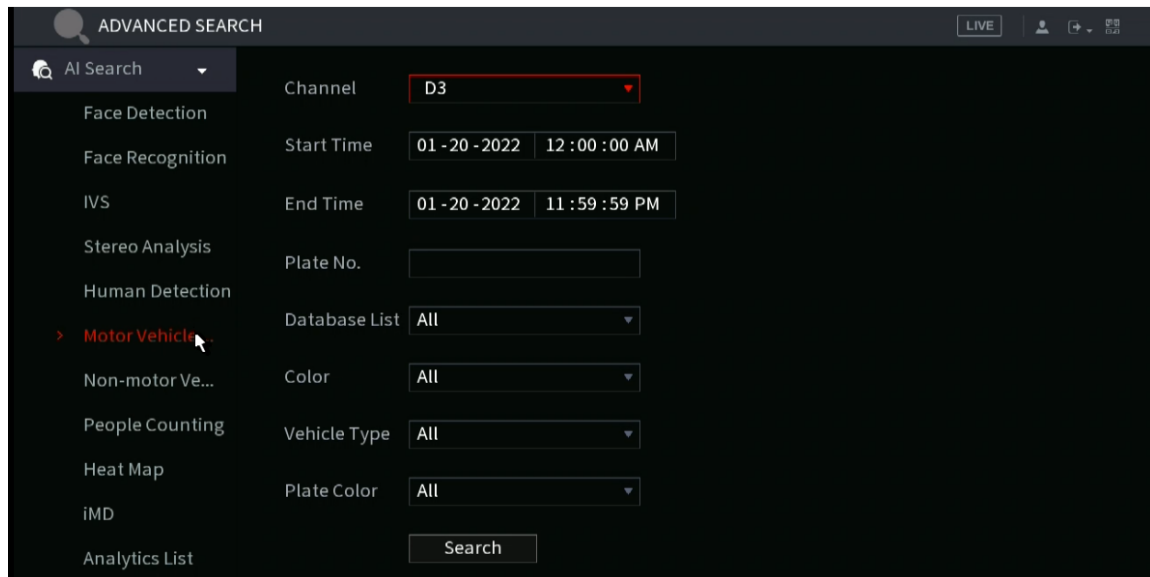
Step 2 Select a channel and set parameters.

📖

- The NVR searches all plate numbers by default if you have not set a plate number.
- The NVR supports plate resemble search.

Step 3 Click **Search**.
The search result will be displayed.

📖

When black list or white list is selected as **Type**, the black list or white list information will be displayed in search results.

Step 4 Select one or multiple results, and then you can do the following operations as needed.
1) To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.

2) To lock the files to make it unable to be overwritten, select the files, then click **Lock**.

3) To add a mark to the file, select the files and then click **Add Tag**.

4.7.1.7 Non-motor Vehicle Detection

This allows search for objects, such as motorcycles and other two-wheeled vehicles.

📖

Not all NVRs support this function.

Step 1 Select **Main Menu** > **Playback** > **Advanced Search** > **Non-Motor Vehicle Detection** .
The **Non-Motor Vehicle Detection** interface will be displayed. See Figure 4-127.

Figure 4-127
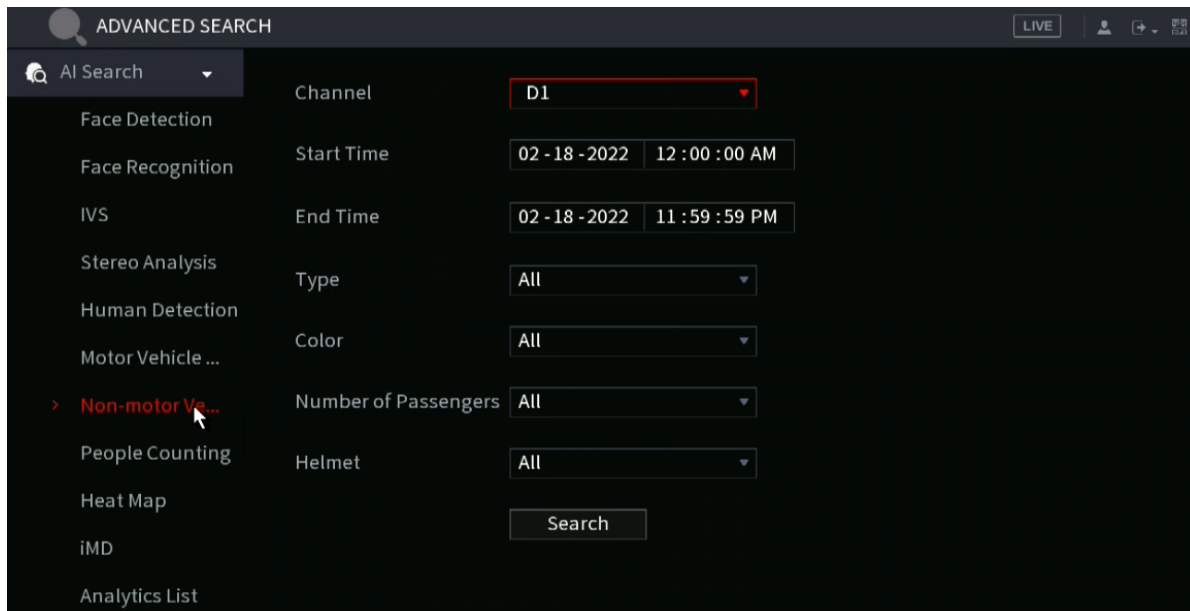
Step 2 Select the channel and the time, then select one or multiple parameters from **Type**, **Color**, **Occupancy**, or **Helmet**.

Step 3 Click **Search**.
The search result will be displayed. See Figure 4-128.

Figure 4-128
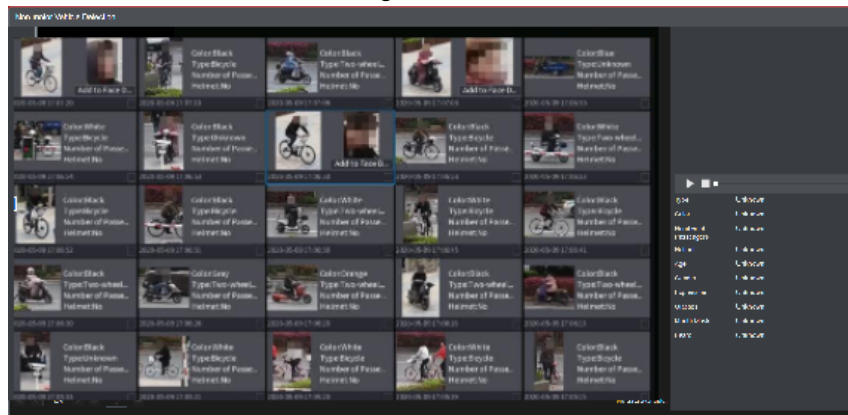
Step 4 Select one or multiple results, and then you can do the following operations as needed.

● Click **Export** to export results in Excel format.

124

- To back up the recorded files to the external storage device, select files, click **Backup**, select the save path and file type, and then click **Start**.
- To lock the files to make it unable to be overwritten, select the files, and then click **Lock**.
- To add a tag to the file, select the files and then click **Add Tag**.
- Click **Add to Face Database** to add the detected face picture to a face database.

4.7.1.8 People Counting

This feature allows you search for people counting statistics

. Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **AI Search** > **People Counting**.

The **People Counting** interface will be displayed. See Figure 4-129.

Figure 4-129
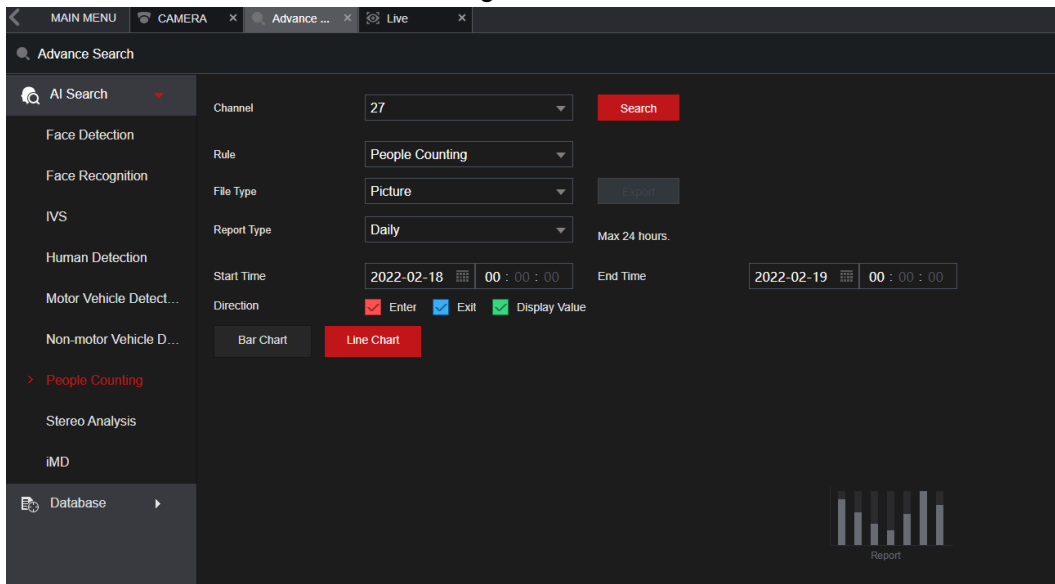
Step 2   Set parameters such as channel, report type, start time, end time, etc. See Table 4-34.

Table 4-34

Parameter	Description
Channel	Select the channel you want to search people amount.
Rule	Select the rule from the drop-down list.
Report Type	Select report type from the drop-down list: daily report, monthly report, yearly report.
Start time/End time	Set search start time and end time.
Type	Select from the drop-down list.

4.7.1.9 Heat map

Heat Map allows you to detect the distribution of active objects within the monitor zone during the specified period, and use different colors to display on the heat map report.

4.7.1.9.1 General

Step 1 Select **Main Menu > Advanced Settings > Alert Center** > **AI Search** > **Heat Map** > **General**.
The **General** interface will be displayed. See Figure 4-130

Figure 4-130
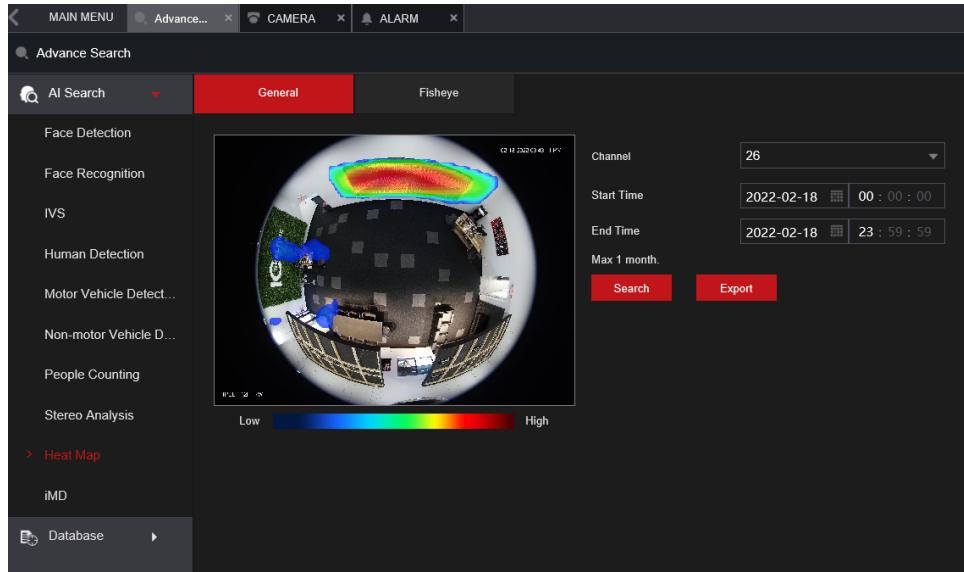
Step 2 Select channel, start time, end time.
Step 3 Click **Search**.
Step 4 System display heat map report.

📖
Click **Export**, and then select path. Click **Save** to save the current report to the USB device.

4.7.1.9.2 Fisheye

Step 1 Select **Main Menu > Advanced Settings > Alert Center** > **AI Search** > **Heat Map** > **Fisheye**.
The **Fisheye** interface will be displayed. See Figure 4-131

Figure 4-131
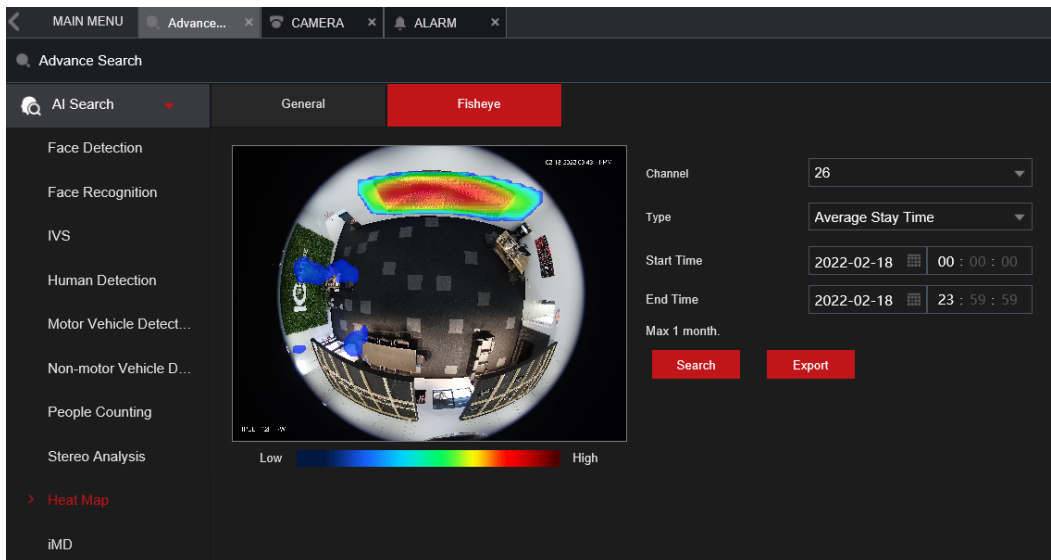
Step 2   Set **Channel**, **Type**, **Start Time**, **End time**.

Step 3   Click **Search**.

Step 4   The Heat map report will be displayed..

📖

Click **Export** and then select saved path, click **Save** to save the heat map report to the USB device.

4.7.1.10 iMD (Intelligent Motion Detect)

You can search and play back videos that triggered iMD events.

Step 1   Select **Main Menu > Advanced Settings > Alert Center**

> **AI Search** > **iMD**.

Step 2   Select channel, type, start time and end time, and then click **Search**.

- Click ⏺ to play back the video.
- Select a video and click **Export** to export video file to a USB flash drive.

4.7.2 AI Parameters / Configuration

In the following sections we will be covering how to set up the AI settings. The AI events are mutually exclusive meaning each individual channel can only use one of the following functions at a time. This is due to the resources allocated to do these functions being one and the same, just processed differently. Each channel can have a different type of event. In the case of none AI recorders, the cameras will have to have the feature built in to support it.

Third-party cameras will not be able to take advantage of these features unless you are using one of IC Realtime's AI NVRs such as the NVR916NS which has a dedicated onboard AI processor.

4.7.2.1 Smart Plan

The Smart Plan is used to specify the type of advanced IVS or AI functions that will be used for each specific channel. The selection options will vary depending on the capabilities of NVR and IP Cameras.

Options: IVS, human face detection, human face recognition, human body detection, people counting, and heat map.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Smart Plan**.
The **Smart Plan** interface will be displayed. See Figure 4-132.

Figure 4-132
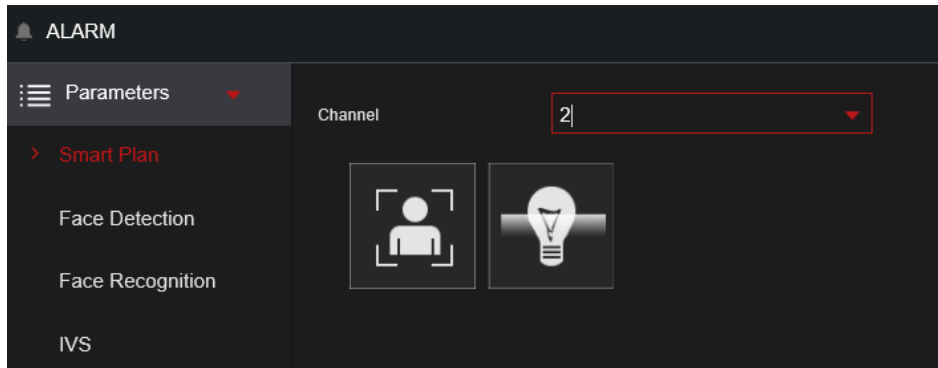
Step 2　Select a channel number.

System will display different smart plan options depending on what IVS or AI functions the IP camera is equipped with.

- If the remote device is a PTZ, the interface will be shown in Figure 4-13.
- For PTZ you will need to save presets before doing this step. You will need to enable the IVS or AI functions for each individual preset.

Figure 4-133
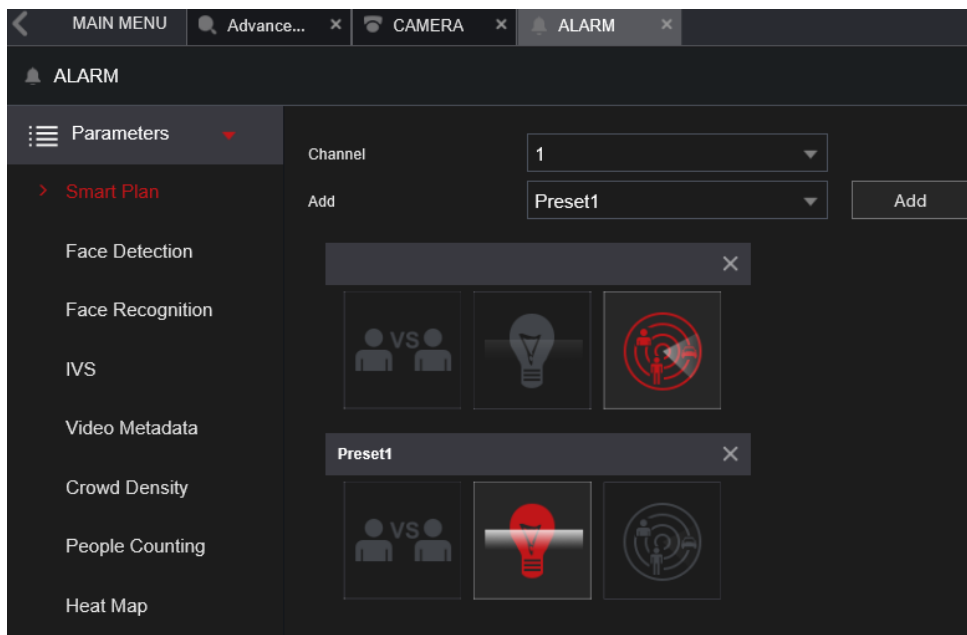
1. Select a channel.
2. Select a preset.
3. Click the smart plan icon at the bottom left. The icon will become highlighted.
4. Click **Apply**.

- If the remote device does not support a preset function, the interface is shown as in Figure 4-134.

Figure 4-134
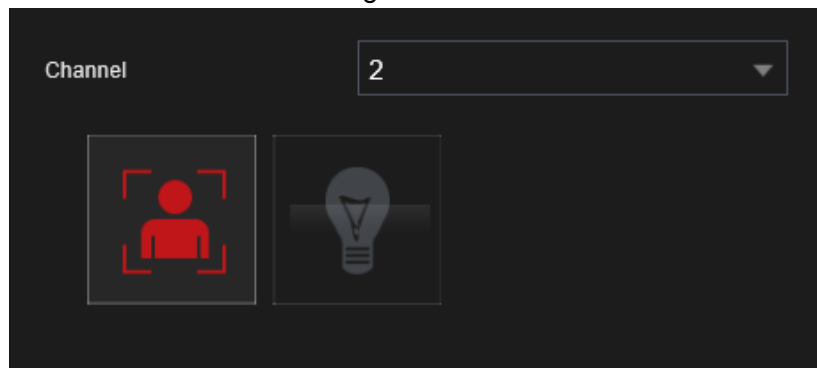
1. Select a channel.
2. Click the smart plan icon. The icon will be highlighted in red.
3. Click **Apply**.

4.7.2.2 Face Detection

The Device can analyze the pictures captured by the camera to detect whether the faces are on the video stream. You can search and filter the recorded videos the faces and playback.
This feature only with IC Realtime Face Detect equipped cameras.

Setup

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Face Detection**.
The **Face Detection** interface will be displayed. See Figure 4-135.

Figure 4-135
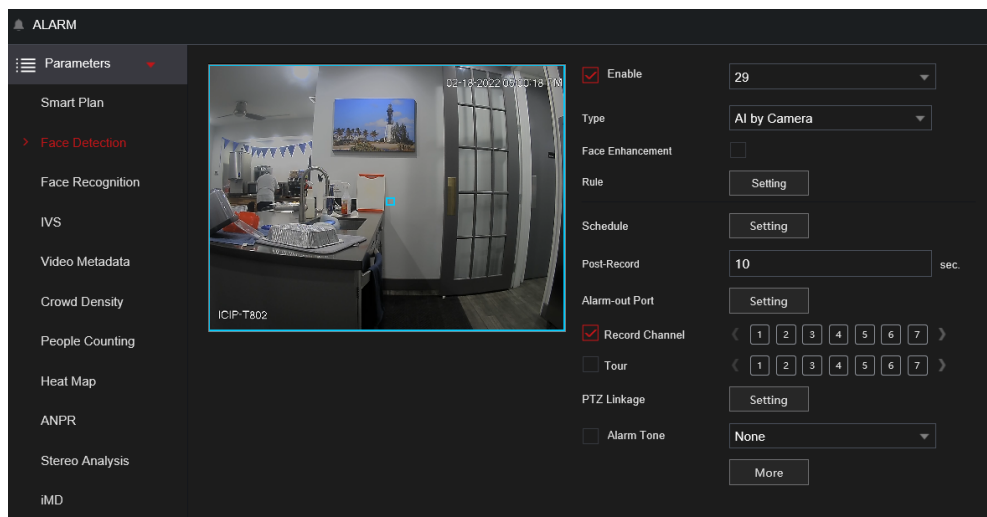
Step 2   In the **Channel** list, select a channel that you want to configure the face detection function.
Step 3   In the **Type** list, select **AI by Recorder** or **AI by Camera**.

When **AI by Camera** is selected, you can enable **Face Enhancement** function to improve face detection efficiency.

Step 4   Configure the parameters. See Table 4-35.

Table 4-35

Parameter	Description
Enable	Click to enable or disable the face detection.
Rule	Click **Setting** to draw areas to filter the target. Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size
Schedule	Configure the period and in the set time range, the corresponding configuration item will be linked to start the alarm.
Alarm-out Port	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Post-Alarm	When the alarm ends, the alarm extended for a period of time. The time range is from 0 seconds to 300 seconds.
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● This function not available in all NVR models. ● Alarm Center must be configured prior. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. 📖 You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".

Parameter	Description
Post-Record	At the end of the event, the recording extends for a period of time. The time range is from 10 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.
More	Click **More** to configure remote alarm output. When alarm event is triggered, the Device links the alarm output ports on camera to trigger an action, such as triggering an access controller to unlock door. ● Enable: Select the check box to enable the remote alarm output. ● Alarm Output: Select the alarm output port as needed. The displayed ports are obtained by Device capability set. ● Post-Alarm: When the alarm ends, the camera alarm output setting returns to the previous status after a period of time. The range is from 0 seconds to 300 seconds, and it is 10 seconds by default.

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

4.7.2.3 Face Recognition

The system will compare the detected faces with the faces in the database to compare the similarity. If the detected face similarity meets the specified requirements (ie: 80% similar) then it will trigger a "Recognized" event based on the grouping settings of the database. The comparison result will be displayed on the AI mode live view screen and smart search interface.

4.7.2.3.1 Configuring AI by Recorder

Step 1   Select **Main Menu > Advanced Settings > Alert Center >**
Parameters > **Face Recognition**.

Step 2   Select the channel, enable the function, and select **AI by Recorder** in the **Type** list.

Figure 4-136
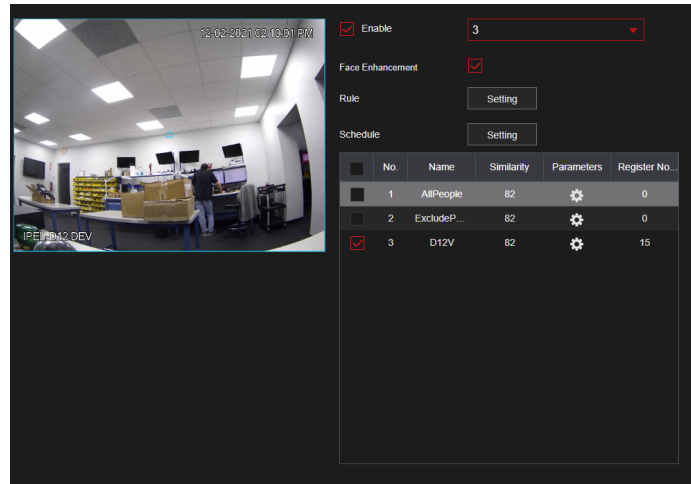
Step 3   Click **Setting** next to **Schedule** to configure arming periods. The corresponding alarm actions are linked by the alarm events triggered during armed period.

Step 4   Arm target face database.

- **General Alarm**: The alarm is triggered when the detected face matches a face in the database within the similarity threshold.
  Select **General Alarm** in **AI Mode**, click **Setting** next to **Target Face Database**, select the face database that you want to arm, and then click **OK**.

  📖

  Click ✏ to modify similarity, and click ⚙ to configure alarm links.

- **Stranger Alarm**: The alarm is triggered when the detected face does not meet the similarity threshold with a face in the database.
  Select **Stranger Alarm** in **AI Mode**, click **Setting** next to **Target Face Database**, enable the function, and then set alarm linages.

Figure 4-137 Stranger alarm (AI by recorder)
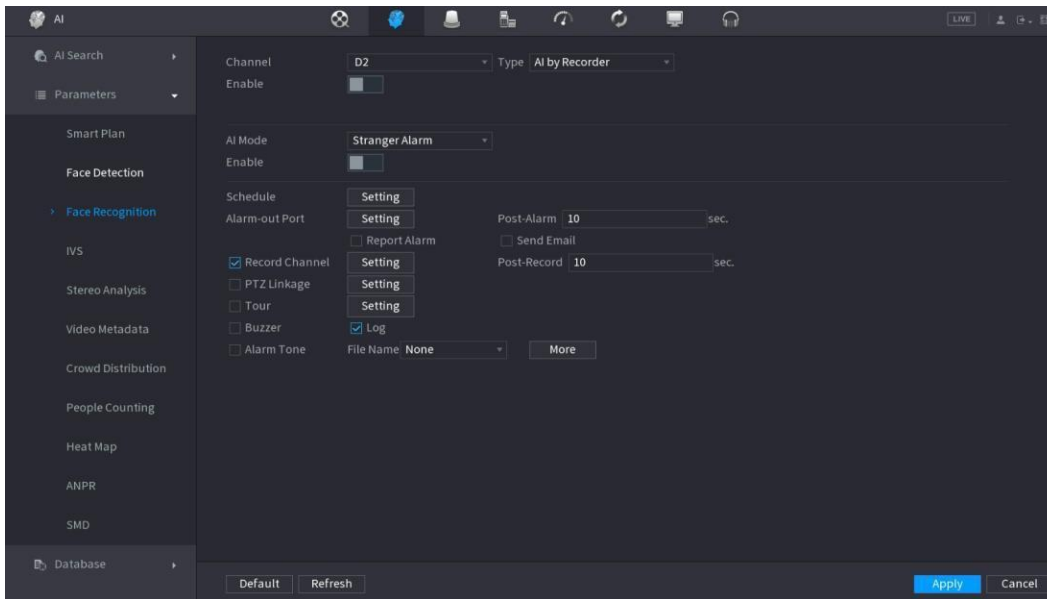
Step 5 Click **Apply**.

4.7.2.3.2 Configuring AI by Camera

This setup is for IC Realtime IP cameras with built-in Face Recognition function and database.
The NVR will use the camera's face database to compare faces.

Step 1 Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Face Recognition**.

Step 2 Select the channel, enable the function, and select **AI by Camera** in the **Type** list.

Figure 4-138 AI by camera
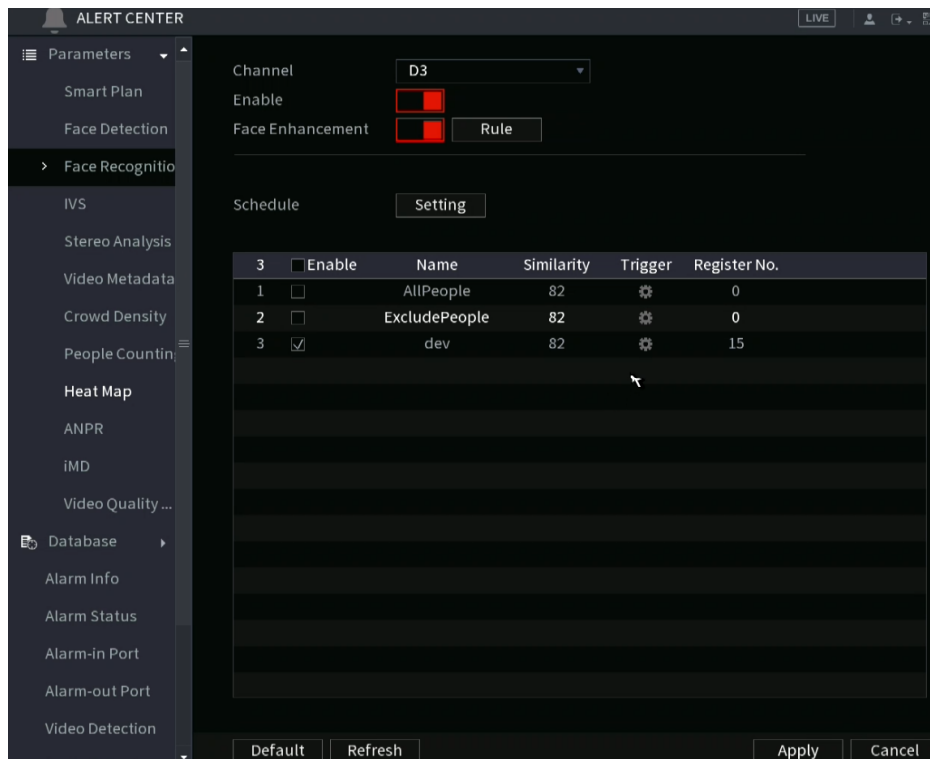
Step 3 Enable **Face Enhancement**. This allows more refined face capture results.

133

Step 4   Click **Rule** to draw areas to filter the target.

Configure the target filtering rules. Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size

Step 5   Select target face database in the table list, and click ⚙ to configure alarm linkage.

Step 6   Click **Apply**.

4.7.2.4 IVS (General Behavior Analytics)

The IVS function processes and analyzes the images to extract the key information to match the specified rules. When the rule is triggered, an event will be created.

📖

- Not all NVR models support this feature.
- A single channel cannot have both IVS function and human face detection functions enabled.

To achieve the best results, the IVS environment should meet the following **requirements**:
- The object's total size shall not be more than 10% of the whole video.
- The object size on the video shall not be more than 10 pixels by 10 pixels. The abandoned object size shall be more than 15 pixels by 15 pixels (CIF resolution). The object width shall not be more than 1/3 of the video height and width. The recommended height is 10% of the video.
- The object and the background brightness different should not exceed more than 10 grey levels.
- The object should remain on the video for more than 2 seconds. The moving distance is larger than its own width and should not be smaller than 15pixels (CIF resolution).
- Avoid complicated environments. The IVS function is not suitable for the environment of too many objects or the rapidly changing (or flashing) lighting conditions.
- The surveillance environment shall not contain reflective objects such as glass, mirrors and water. Avoid creating rules within tree branches, shadow, or around flying mosquitoes and bugs. Do not use the IVS function in a backlit environment and avoid direct sunlight.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **IVS**.

The **IVS** interface will be displayed. See Figure 4-139.

Figure 4-139
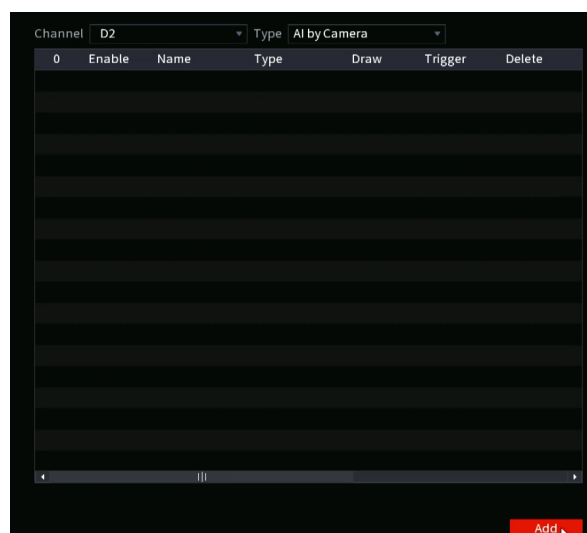
Step 2   Select a channel from the dropdown list at the top.
Step 3   Click **Add** and then set the corresponding rule. See Figure 4-140.

Click the trash icon 🗑 to delete the selected rule.

Figure 4-140

Step 4   Set corresponding parameters.
Step 5   Click **Apply**.

4.7.2.4.1 Tripwire

The tripwire IVS rule allows you to draw a virtual "tripwire" in the image. If an object crosses the rule within the defined directions, the NVR will create an IVS event trigger.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **IVS**.
          In the **Type** drop-down list, select **Tripwire**. See Figure 4-141.

Figure 4-141
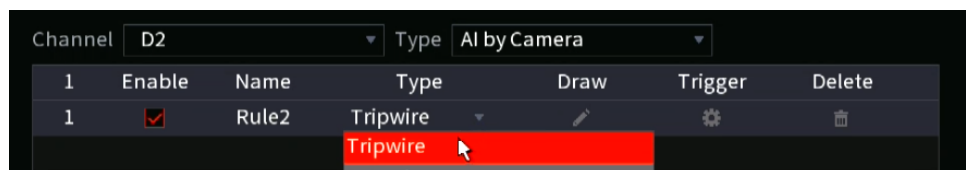
Step 2   Draw the detection rule.
          1) Click ✎ to draw the rule on the current channel, as shown in Figure 4-142.

Figure 4-142

2) Configure the parameters. See Table 4-36.

Table 4-36

Parameter	Description
Name	Customizes the rule name.
Direction	Set the tripwire direction, including A→B, B→A and A↔B.
Min/ Max Size	Click ⊡ to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.
Target Filter (Perimeter protection)	Click the enable to display the selectable target types (Human and/ or Vehicle) This allows the NVR AI to filter only the object types selected. 📖 On available NVR models and IP Cameras with Perimeter Protection support

3) Press and hold down the left button on the monitor screen to draw the line. The line can be a straight or curved.
4) Click **OK** to complete the rule setting.

Step 3 Click ⚙.

The **Parameters** interface will be displayed. See Figure 4-143.

Figure 4-143
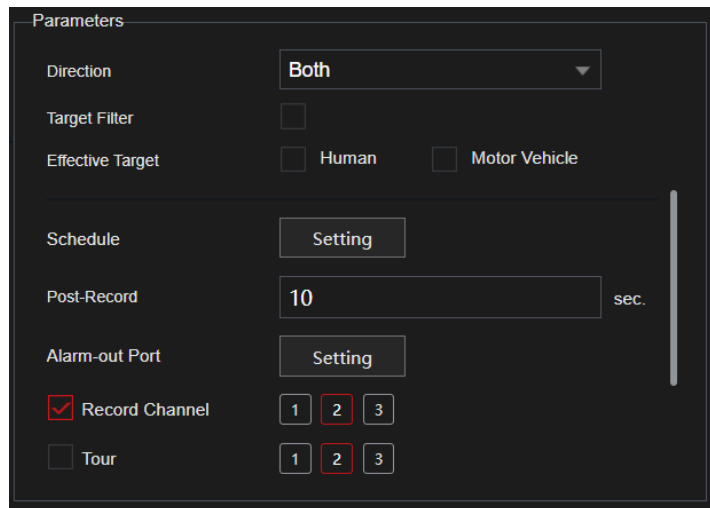
Step 4 Configure the parameters.

Table 4-37

Parameter	Description
Enable	Click to set the rules as active or inactive.
Rule	Click **Setting** to draw areas to apply the target filter. Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.
Schedule	This configures the days of the week and time when the rules will be active.
Alarm-out Port	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Post-Alarm	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.

Parameter	Description
Report Alarm	Select the check box. When an alarm occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● Not all NVR models support this feature. ● The alarm center must be configured first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".

Record Channel	Select the check box and select the desired recording channel (supports multiple choices). when an event occurs, the NVR will record the channels selected. 📖 Alarm recording should be enabled in Storage Schedule. For details, see "4.1.4.6 Schedule".
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Post-Record	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour".". ● After the tour ends, the previous screen split mode will resume.
Log	When enabled, the triggered IVS events will be recorded into the NVR system log.

Parameter	Description
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 5   Click **OK** to save the alarm setting.

System displays the **IVS** interface.

Step 6   Select the **Enable** check box and click **Apply** to complete the tripwire setting.

4.7.2.4.2 Intrusion

The Intrusion rule allows you to draw a custom area within the image. Any objects that appear or cross into the area (depending on the configuration) will create an IVS event trigger.

Step 1 　In the **Type** drop-down list, select **Intrusion**. See Figure 4-144.

Figure 4-144
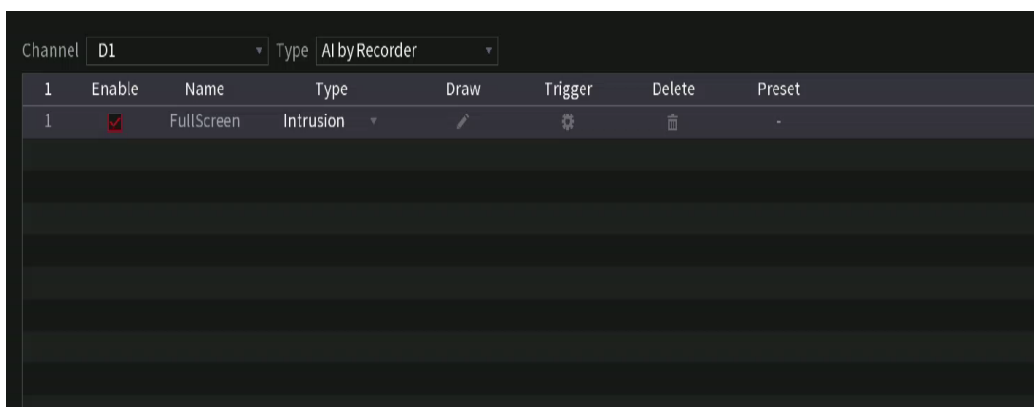
Step 2 　Draw the detection rule.
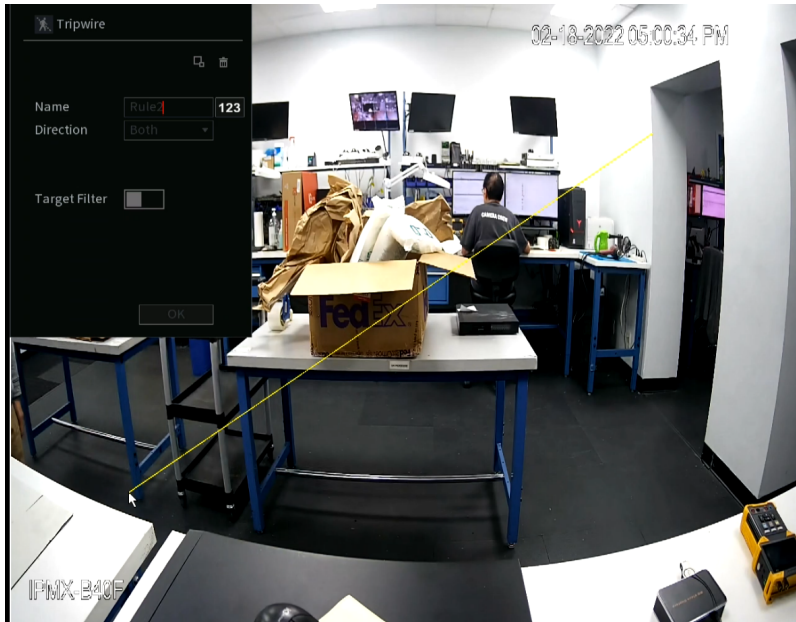
    1) Click 　 to draw the rule on the live view, the system displays as Figure 4-145.

Figure 4-145
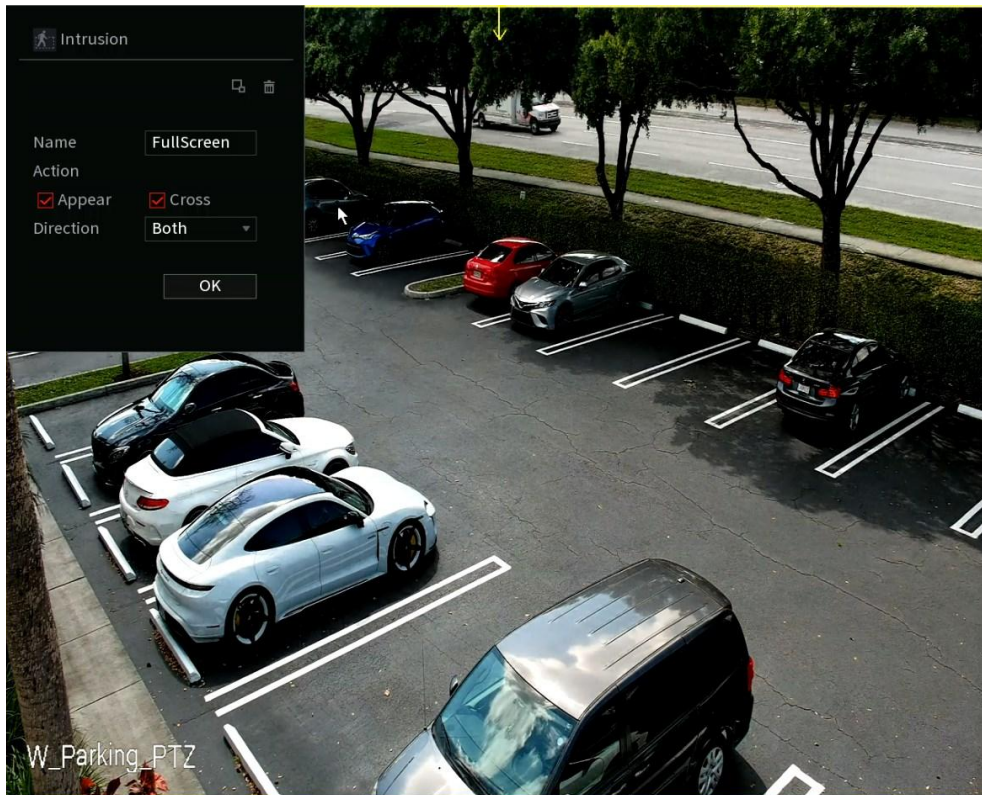
2) Configure the parameters. See Table 4-36.

Table 4-38

Parameter	Description
Name	Customizes the rule name.
Action	Sets the intrusion action trigger for the target object, such as appearing and crossing.
Direction	Set the direction to cross the area, including enter, exit and both.
Filter target	Click ⬚ to set the target filter. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.
AI recognition	On available models with Perimeter Protection support, this allows the NVR AI to filter only the object types selected (Human and/ or Vehicle).

3) Click and hold down the left button on the monitoring screen to draw the monitoring area. This will be the area in which the IVS rule is active.

4) Click **OK** to complete the rule setting.

Step 3   Click ⚙, you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Select **Enable** check box and click **Apply** to complete the intrusion

setting.

4.7.2.4.3 Abandoned Object Detection

This IVS rule generates an IVS event when there is an abandoned object within the specified zone.

Step 1   In the **Type** drop-down list, select **Abandoned Object**.

The interface is shown in Figure 4-146.

Figure 4-146
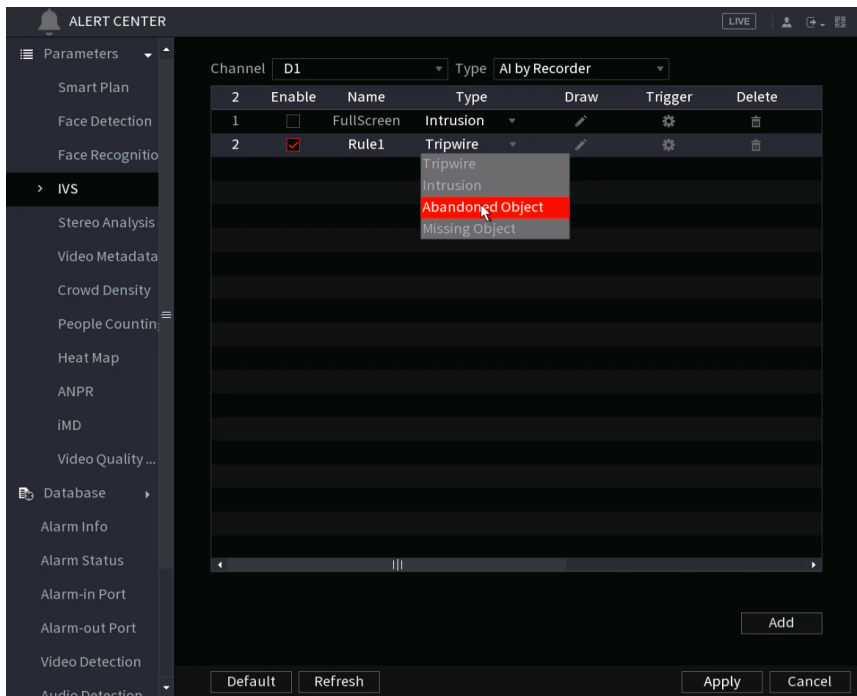
Step 2   Draw the detection rule.

1) Click [pencil icon]   to draw the rule on the live video. See Figure 4-147.

Figure 4-147
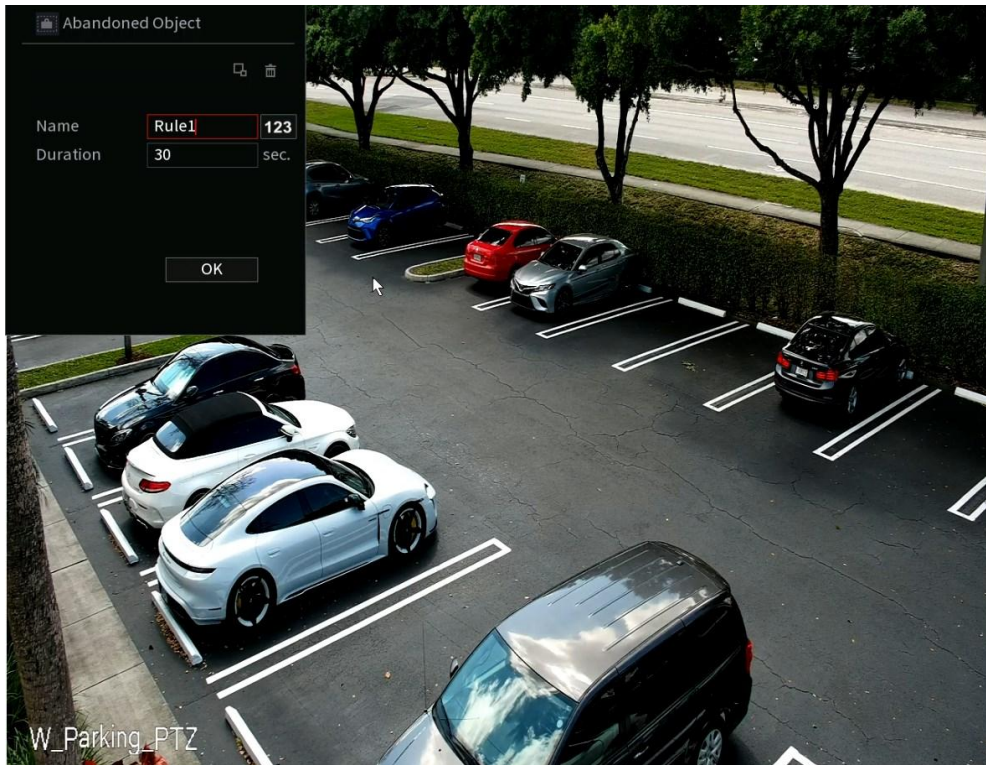
2) Set parameters. See Table 4-39.

Table 4-39

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.
Name	Input customized rule name
Duration	System can generate an alarm once the object is in the zone for the specified duration period.
Filter target	Click ⬚ to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.

3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right click the mouse when finished.

4) Click **OK** to save the rule setting.

Step 3   Click ⚙, you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Click **Apply** to save and complete the setup.

4.7.2.4.4 Fast Moving

This IVS rule will create and alarm event when fast moving objects have been detected on the live video.

Step 1 In the **Type** drop-down list, select **Fast Moving**.
The interface is shown as below. See Figure 4-148.

Figure 4-148
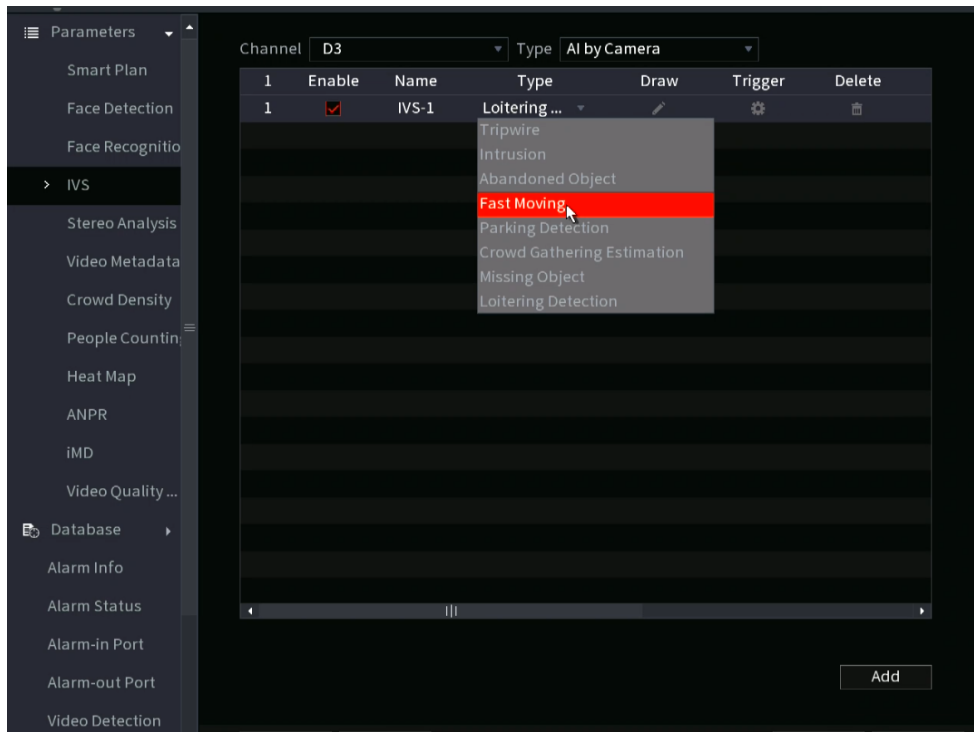
Step 2 Draw the detection rule.

1) Click [pencil icon] to draw the rule on the live video. See Figure 4-149.

Figure 4-149

2) Set parameters. See Table 4-40.

Table 4-40

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.
Name	Input customized rule name
Sensitivity	Configures the event sensitivity. The value ranges from 1 to 10.The default setup is 5.
Filter target	Click ▣ to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.

3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right-click the mouse when finished.
4) Click **OK** to complete the rule setting.

Step 3   Click ⚙, you can refer to "4.7.2.4.1 Tripwire" to set other parameters.
Step 4   Click **Apply** to complete the setup.

4.7.2.4.5 Crowd Gathering

The NVR can generate an alarm once the people amount gathering in the specified zone is larger than the threshold.

Step 1   In the **Type** drop-down list, select **Crowd Gathering Estimation**.
The interface is shown as below. See Figure 4-150.

Figure 4-150
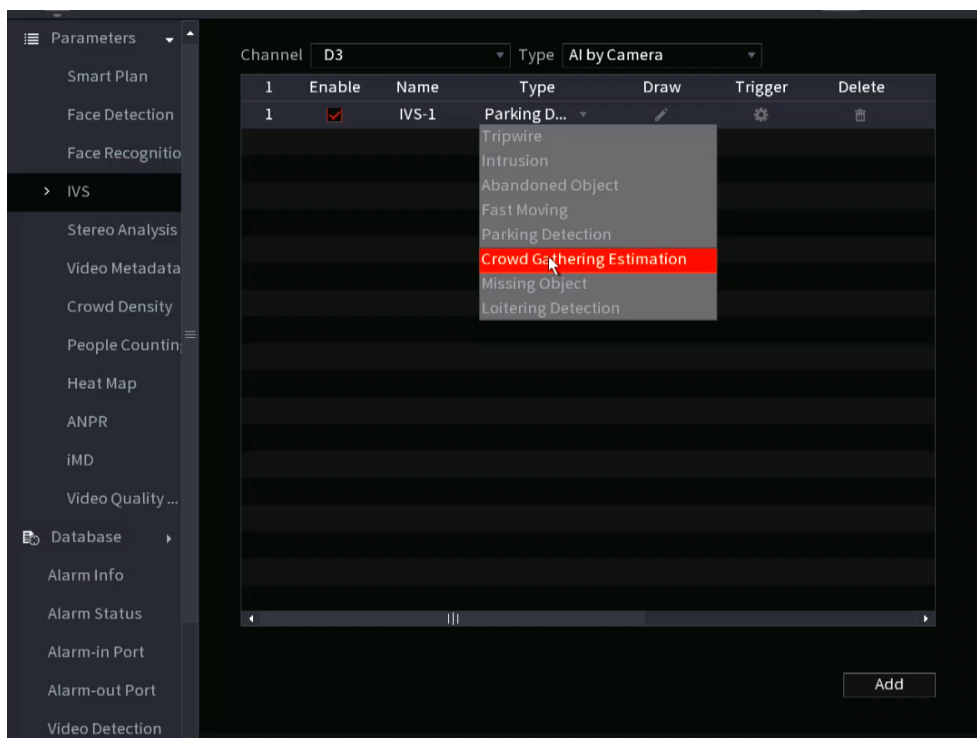
Step 2   Draw the detection rule.

1) Click ![pencil icon] to draw the rule on the live view. See Figure 4-151.

Figure 4-151
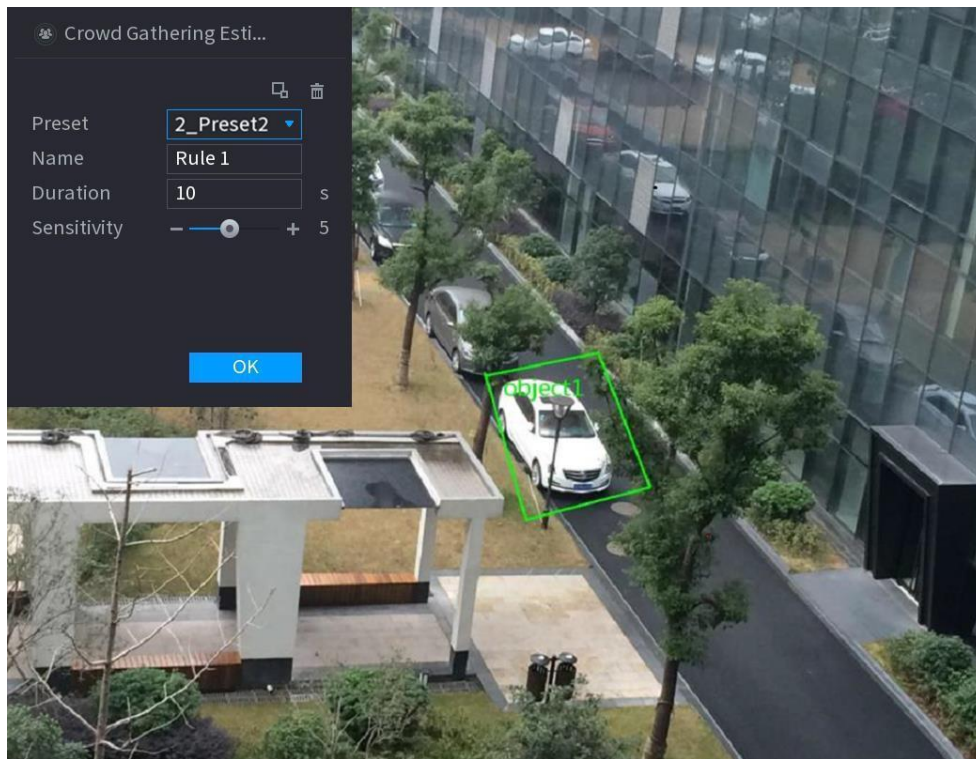
2) Set parameters. See Table 4-41.

Table 4-41

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.
Name	Input customized rule name
Duration	Set the minimum time that the object stays until the alarm is triggered.
Filter target	Click ![icon] to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size), that is, when the passing target is smaller than the minimum target or larger than the maximum target, no alarm will be generated. The maximum size should not be smaller than the minimum size.

3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right click the mouse when finished.

4) Click **OK** to complete the rule setting.

Step 3   Click ![gear icon], you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Click **Apply** to complete the setup.

4.7.2.4.6 Parking

The Parking IVS rule triggers when a detection target stays in the defined monitoring area

for more than the set duration.

Step 1   In the **Type** drop-down list, select **Parking**.

The interface is shown as below. See Figure 4-152.

Figure 4-152
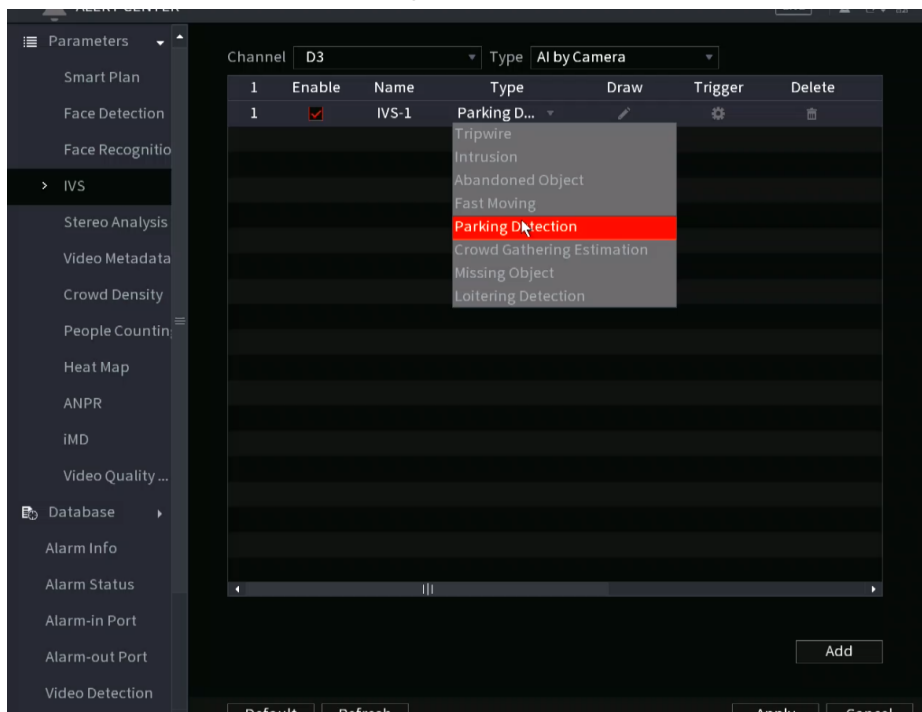
Step 2   Draw the detection rule.

1) Click [icon] to draw the rule on the channel live video. See Figure 4-153.

Figure 4-153
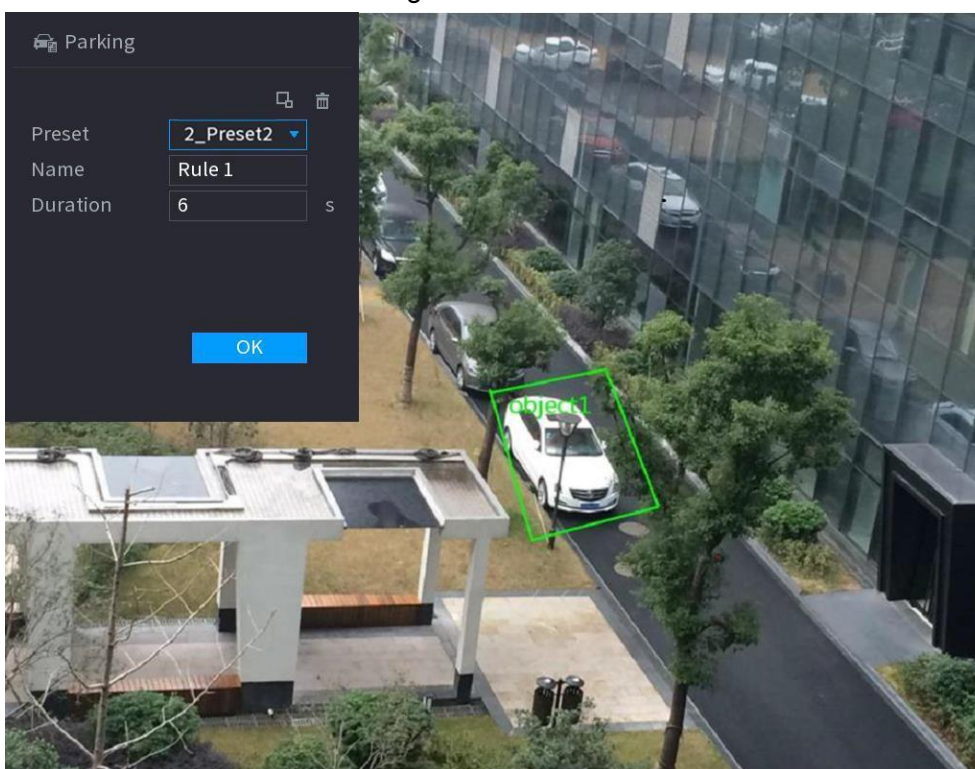
2) Set the desired parameters. See Table 4-42.

Table 4-42

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.
Name	Customize the rule name.
Duration	Set the minimum time that the object stays until an alarm event is triggered.
Filter target	Click ⊡ to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.

3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right-click the mouse when finished.

4) Click **OK** to complete the rule setting.

Step 3   Click ⚙, you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Click **Apply** to complete the setup.

4.7.2.4.7 Missing Object Detection

This IVS rule generates an event alarm when an object becomes missing ot disappears in the specified zone.

Step 1   In the **Type** drop-down list, select **Missing Object**.

The interface is shown as below. See Figure 4-154.

Figure 4-154
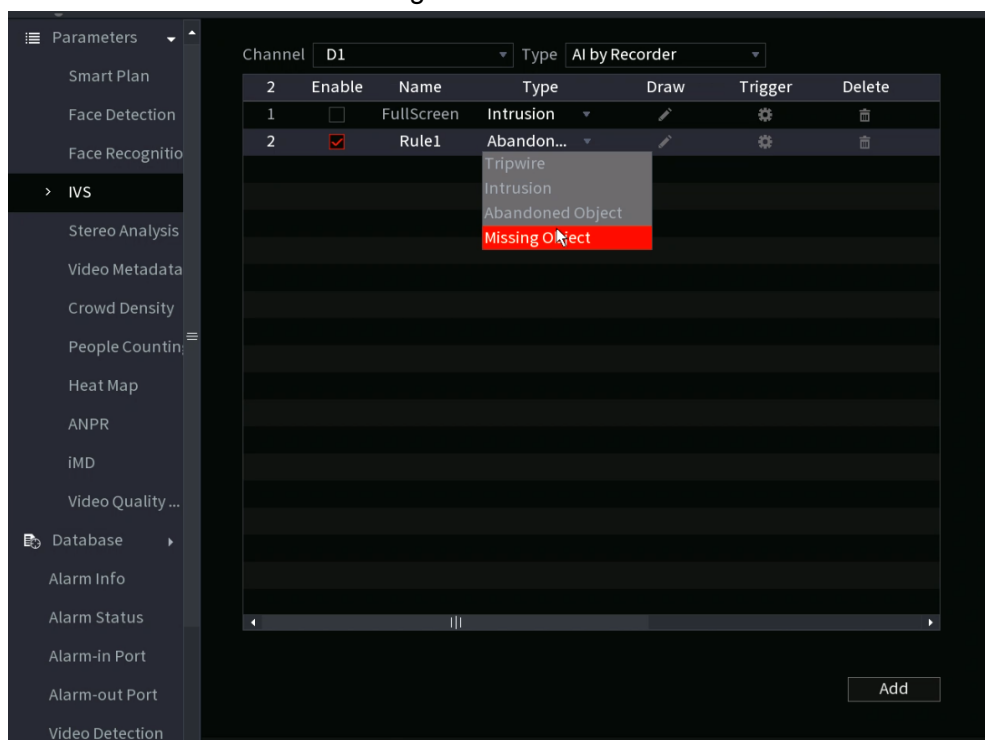
Step 2   Draw the detection rule.

1) Click ![pencil icon] to draw the rule on the live view. See Figure 4-155.

Figure 4-155
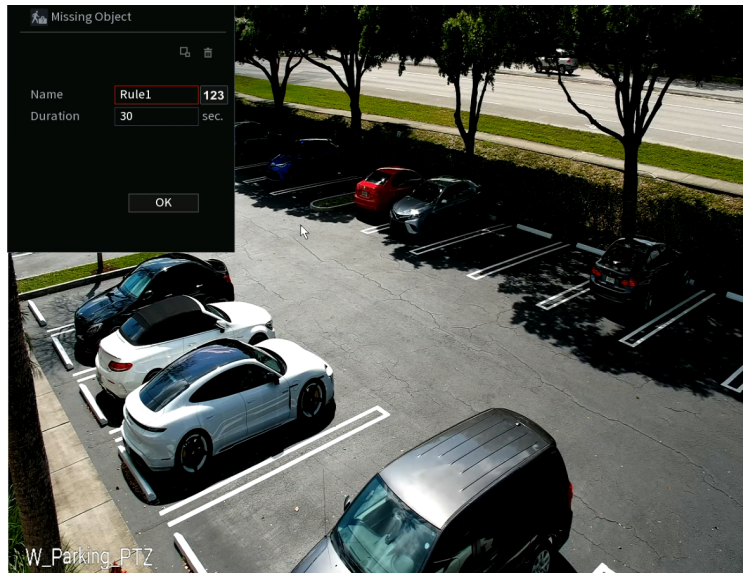
2) Set parameters. See Table 4-43.

Table 4-43

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.
Name	Customize the rule name.
Duration	Set the minimum time that the object stays until the event alarm is triggered.
Filter target	Click ![icon] to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size), that is, when the passing target is smaller than the minimum target or larger than the maximum target, no alarm will be generated. The maximum size should not be smaller than the minimum size.

3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right-click the mouse when finished.

4) Click **OK** to complete the rule configuration.

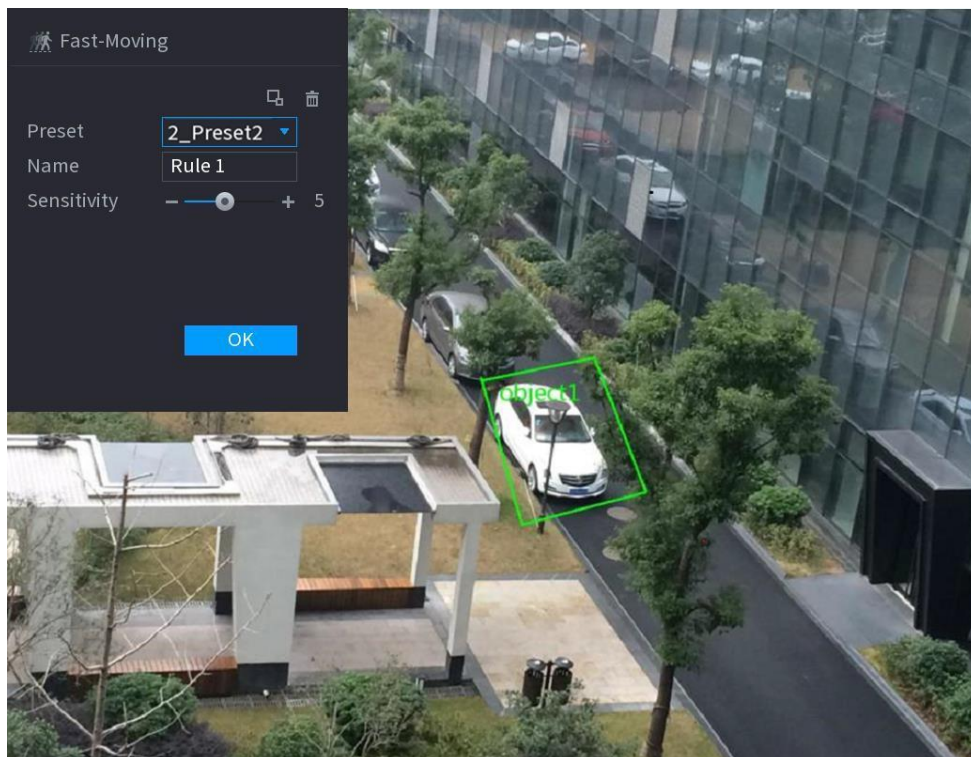Step 3   Click ![gear icon], you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Click **Apply** to complete the setup.

4.7.2.4.8 Loitering Detection

This IVS rule generates an event alarm when a target appears and stays in the specified zone longer than the set threshold.

Step 1   In the **Type** drop-down list, select **Loitering Detection**.

The interface is shown as below. See Figure 4-156.

Figure 4-156
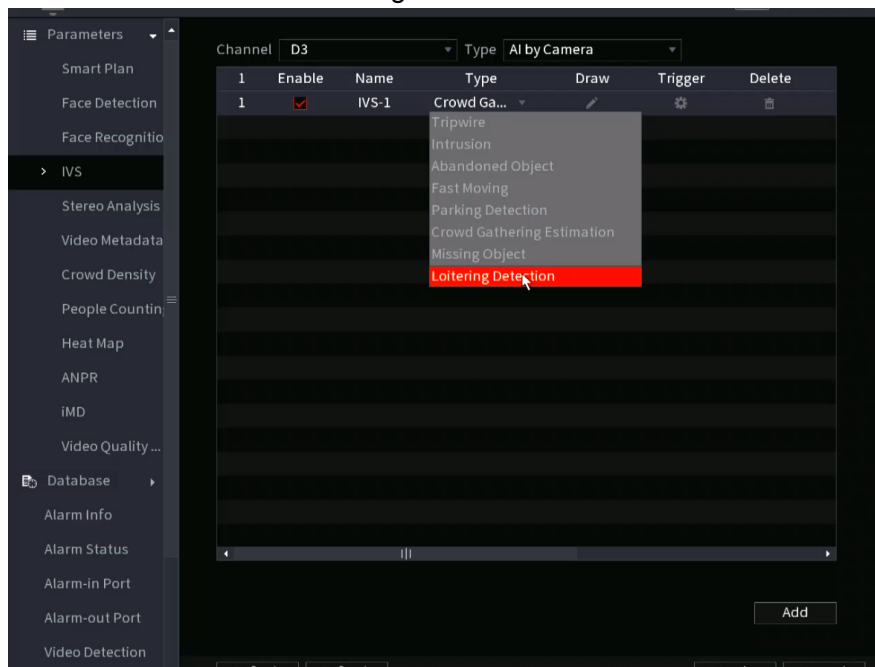
Step 2   Draw the detection rule.

1) Click ![pencil icon] to draw the rule on the current channel live view. See Figure 4-157.

Figure 4-157
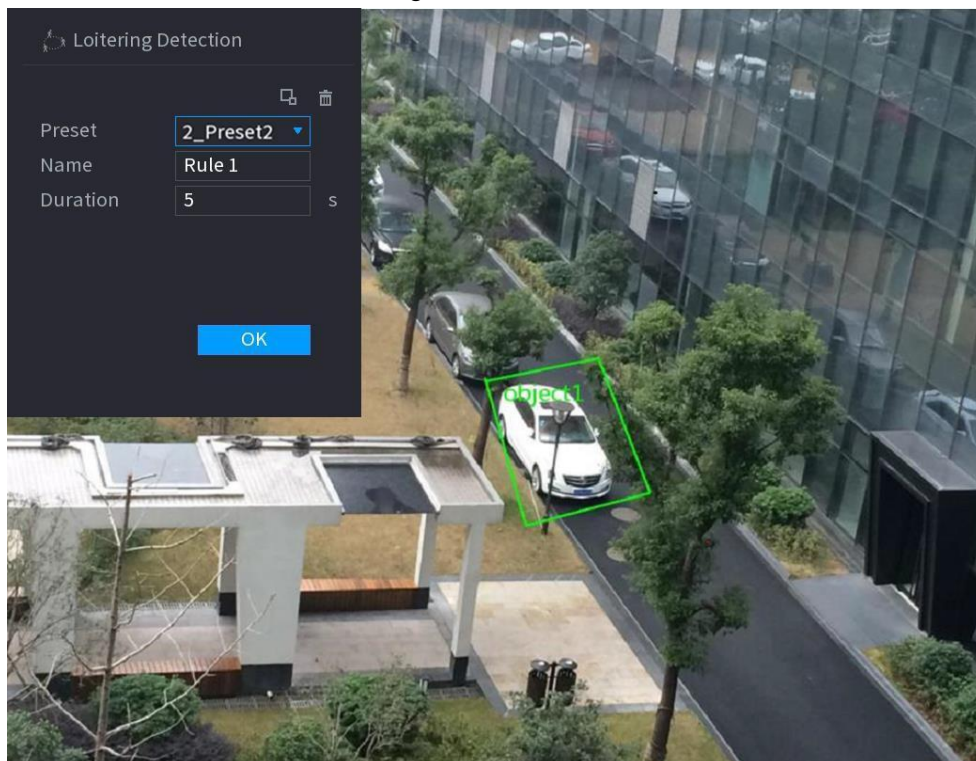
2) Set parameters. See Table 4-44.

Table 4-44

Parameter	Description
Preset	For a PTZ camera, select the preset to set up the IVS rule on.

Parameter	Description
Name	Customize the rule name.
Duration	Set the minimum time that the object stays until the event alarm is triggered.
Filter target	Click ⧉ to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size), that is, when the passing target is smaller than the minimum target or larger than the maximum target, no alarm will be generated. The maximum size should not be smaller than the minimum size.

      3) Draw a rule. Left-click mouse to draw a zone until you draw a rectangle. Right click the mouse when finished.

      4) Click **OK** to complete the rule setting.

Step 3   Click ⚙, you can refer to "4.7.2.4.1 Tripwire" to set other parameters.

Step 4   Click **Apply** to complete the setup.

4.7.2.5 Video Metadata

This feature allows the detection and extraction of key features from the human body, motor vehicle, and non-motor vehicles from the live video. These features can then be usde in search queries.

When enabling the video Metadata Function, the NVR will set the corresponding smart plan as active.

📖

The connected IC Realtime camera must support the video Metadata function.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Video Metadata**.

      The **Video Metadata** interface will be displayed. See Figure 4-158

Figure 4-158
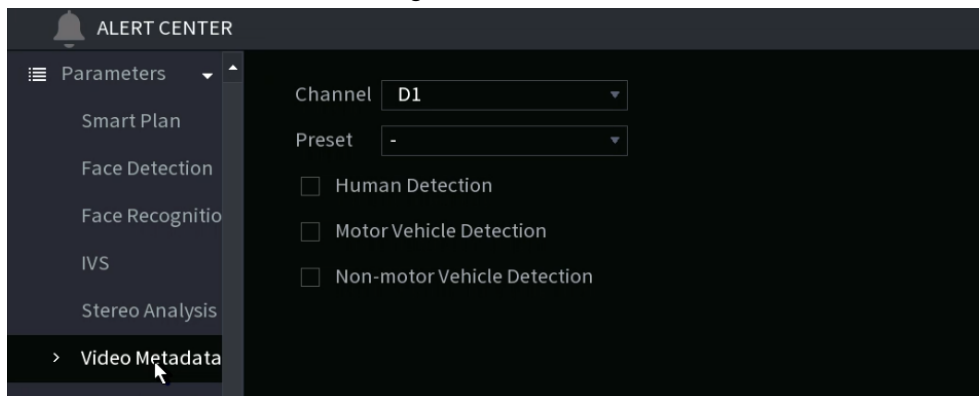
Step 2   In the **Channel** list, select a channel that you want to configure video MetaData function, and then select the Metadata type. See Table 4-45

Table 4-45

Parameter	Description
Human Detection	Selecting this check box allows the NVR to extract Human-based metadata such as shirt and pants color, gender, and age.

Parameter	Description
Face Detection	Selecting this check box allows the NVR to extract human face-based metadata such as expression, gender, and age.
Motor Vehicle Detection	Selecting this check box allows the NVR to extract Motor vehicle-based metadata such as plate number, color, and vehicle type.
Non-motor Vehicle Detection	Selecting this check box allows the NVR to extract Non-motor vehicle-based (2 wheeled vehicles) metadata such as type and color.

Step 3   Click **Apply**.

4.7.2.6 Crowd Distribution

The Crowd Distribution function detects the number of people in the monitored areas, and sends alarm events if it exceeds the configured threshold. It can also automatically generate crowd reports for analysis.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Crowd Density**. The **Crowd Density** interface will be displayed. See Figure 4-159.

Figure 4-159
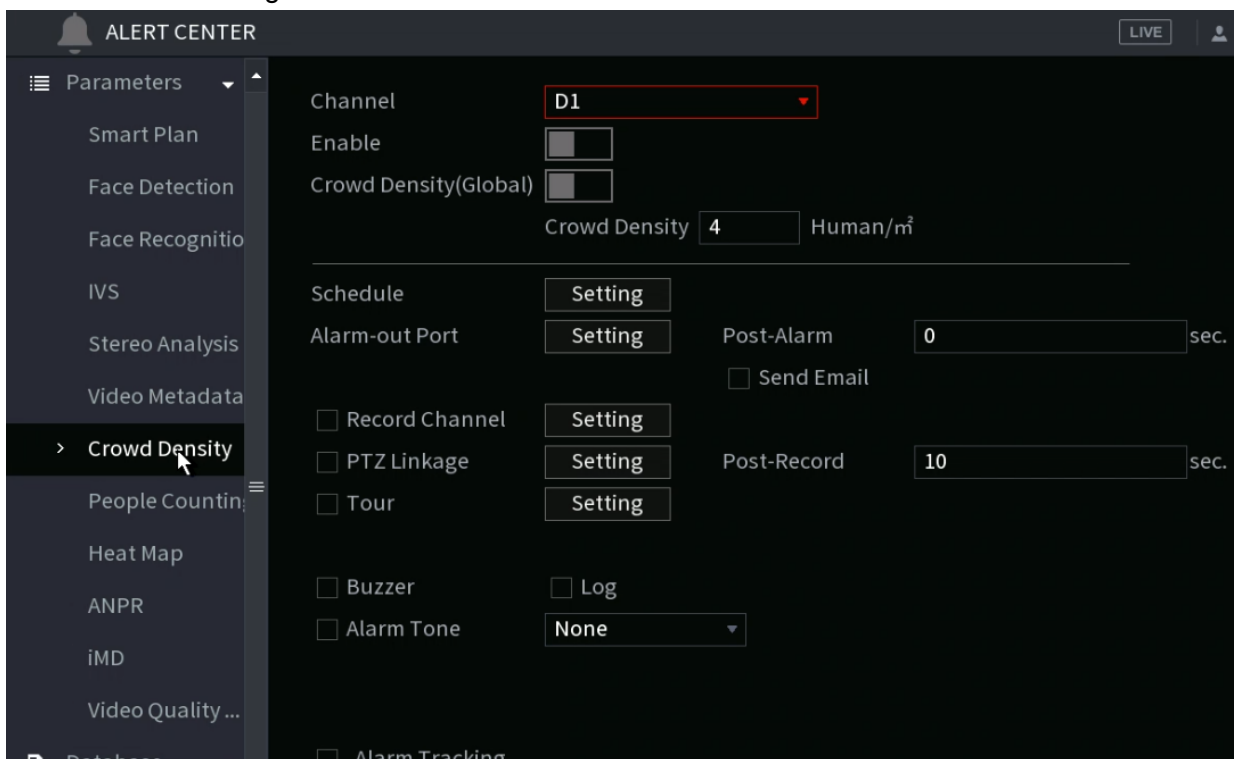
Step 2   Configure parameters. See Table 4-46.

Table 4-46

Parameter	Description
Channel	Select a channel from the dropdown list.
Enable	Check the box to enable the function.
Global	Check the box to enable the global crowd distribution alarm.
Crowd Density	Configure the alarm threshold. The default setup is 4 persons per square meter. The value ranges from 2 to 10.
Period	Configures the date/time schedule when the function will be active.
Alarm Out	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Latch	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Alarm Upload	If the check box is selected, when an event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● Not all NVR models support this feature. ● you will need to set the alarm center prior. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. 📖 You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Activation	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the event, the recording will extend for a period of the specified time. The time range is from 10 seconds to 300 seconds.

Parameter	Description
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● you will need to set the time interval and mode for tour prior, see "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Log	Select the check box, the NVR device records the alarm information in the log when an event occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. The NVR will play the audio file when the event occurs. 📖 Refer to "4.18.1 File Management" to add the audio file first.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 3   Click **Apply** to complete the setup.

4.7.2.7 People Counting

When using a People Counting supported camera with a supported NVR, the video analysis technology can calculate the number of people exiting or entering the specified zone on the video. The NVR can then generate an event when the amount has exceeded the threshold.

4.7.2.7.1 People Counting

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **People Counting** > **People Counting**.
The **People Counting** interface will be displayed. See Figure 4-160.

Figure 4-160
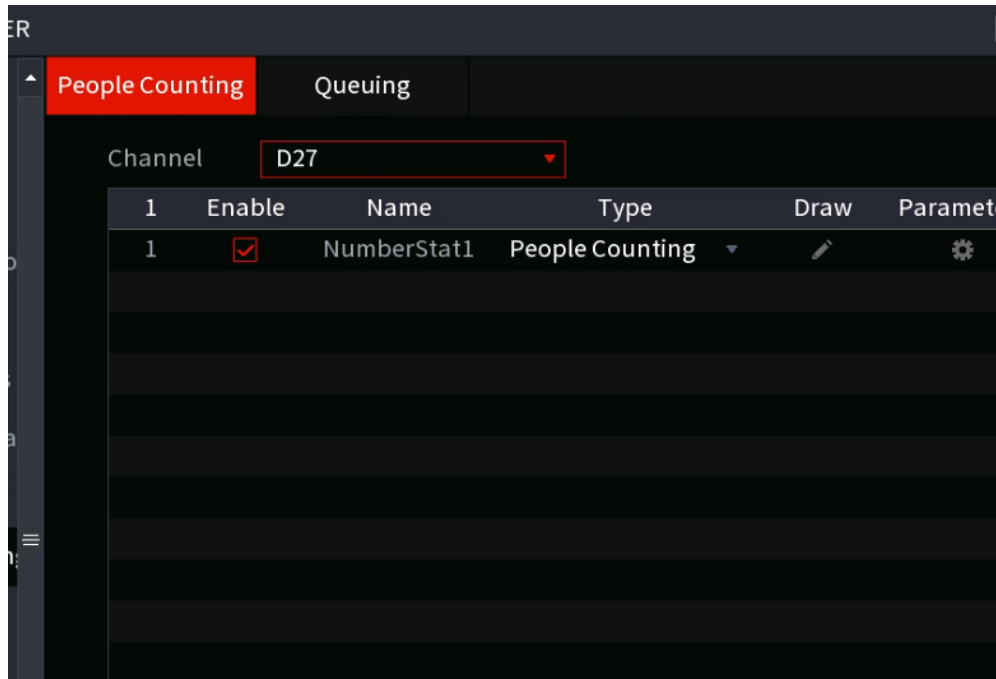
Step 2   Draw the people counting rule.

1) Click ✎   to draw the people counting rule.

2) Configure parameters.

Table 4-47

Parameter	Description
Name	Customize the rule name.
Duration	Set the minimum time that the object stays until the alarm is triggered.
Filter target	Click 🔲 to filter the target. Click and hold the blue wireframe and drag to adjust the size of the area with the mouse. 📖 Each rule can set 2 target filters (maximum size and minimum size). Targets smaller than the minimum target or larger than the maximum target will be ignored. The maximum size should not be smaller than the minimum size.

3) Click and hold the left mouse key to draw an area for people counting.

4) Click **OK** when finished.

Step 3   Click 🔧 to configure parameters in both the **Parameters** and **Trigger** columns.

Table 4-48

Parameter	Description
Channel	Select a channel from the dropdown list.
Enable	Check the box to enable the function.
Rule Type	Select a people counting rule type.
Rule	Click **RULE** to set statistics region, name, direction.
Alarm	Click **Setting** to set alarm parameters. OSD Overlay: Toggles a people counter on the OSD. Entry No.: Configures the people entry amount. The NVR can generate an event once the amount has exceeded the threshold. Exit No.: Configures the people exit amount. The NVR can generate an event once the amount has exceeded the threshold. Remaining No.: Configures the number of people allowed to loiter within the zone. The NVR can generate an event once the amount has exceeded the threshold.
Period	Configures the date/time schedule when the function will be active.
Alarm Out	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Latch	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Alarm Upload	When an event occurs, the NVR uploads an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	Select the check box and select the needed recording channel (support multiple choices). when an event occurs, the NVR device activates the channel for recording. you will need to enable intelligent recording and auto recording first. For details, see"4.1.4.6 Schedule".

Parameter	Description
PTZ Activation	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the event, the recording will extend for a period of the specified time. The time range is from 10 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● you will need to set the time interval and mode for tour first, see "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. The NVR plays the audio file when the alarm occurs. 📖 Refer to "4.18.1 File Management" to add audio file first.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 4   Click **Apply**.

4.7.2.7.2 Queuing

If using an AI fisheye camera that supports the queuing function, A supported NVR can connect the corresponding linkage actions once the people amount in the queue or the waiting time has triggered an alarm. Select a region first to set the corresponding actions. For the same line, the queue people number alarm and queue time alarm have the same linkage actions.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **People Counting** > **Queuing**.

Step 2   The **Queuing** interface will be displayed. See Figure 4-161.

Figure 4-161
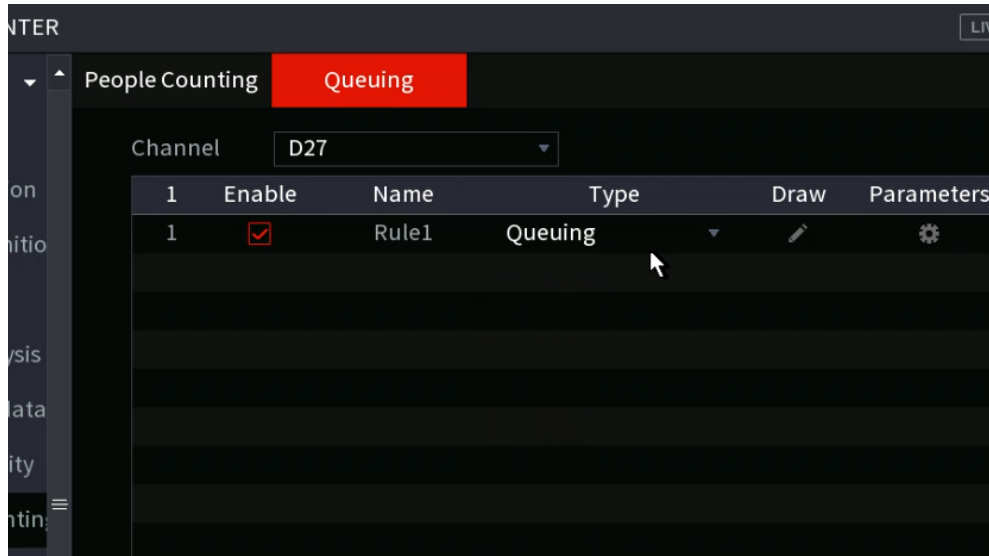
Step 3   Select Channel and then click **Add**.

Step 4   Select the **Enable** check box.

Step 5   Click ![pencil] to draw queuing rule and area.

Step 6   Click ![gear] under the **Parameters** column, and then select alarm type to **Queue People No. Alarm** or **Queue Time Alarm**.

Step 7   Click ![gear] under the **Trigger** column and configure alarm linkages.

Table 4-49

Parameter	Description
Period	Configures the date/time schedule when the function will be active.
Alarm Out	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Latch	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Alarm Upload	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".

Parameter	Description
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. 📖 You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Activation	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the alarm, the recording extends for a period of time. The time range is from 10 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● you will need to set the time interval and mode for tour first, see "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. The NVR plays the audio file when the alarm occurs. 📖 Refer to "4.18.1 File Management" to add audio file first.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 8   Click **Apply**.

4.7.2.8 Heat map

Heat map technology monitors the human traffic distribution in the specified zone during a period of time and uses different colors to display on a heat map report.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameters** > **Heat Map**. The **Heat Map** interface will be displayed. See Figure 4-162.

Figure 4-162
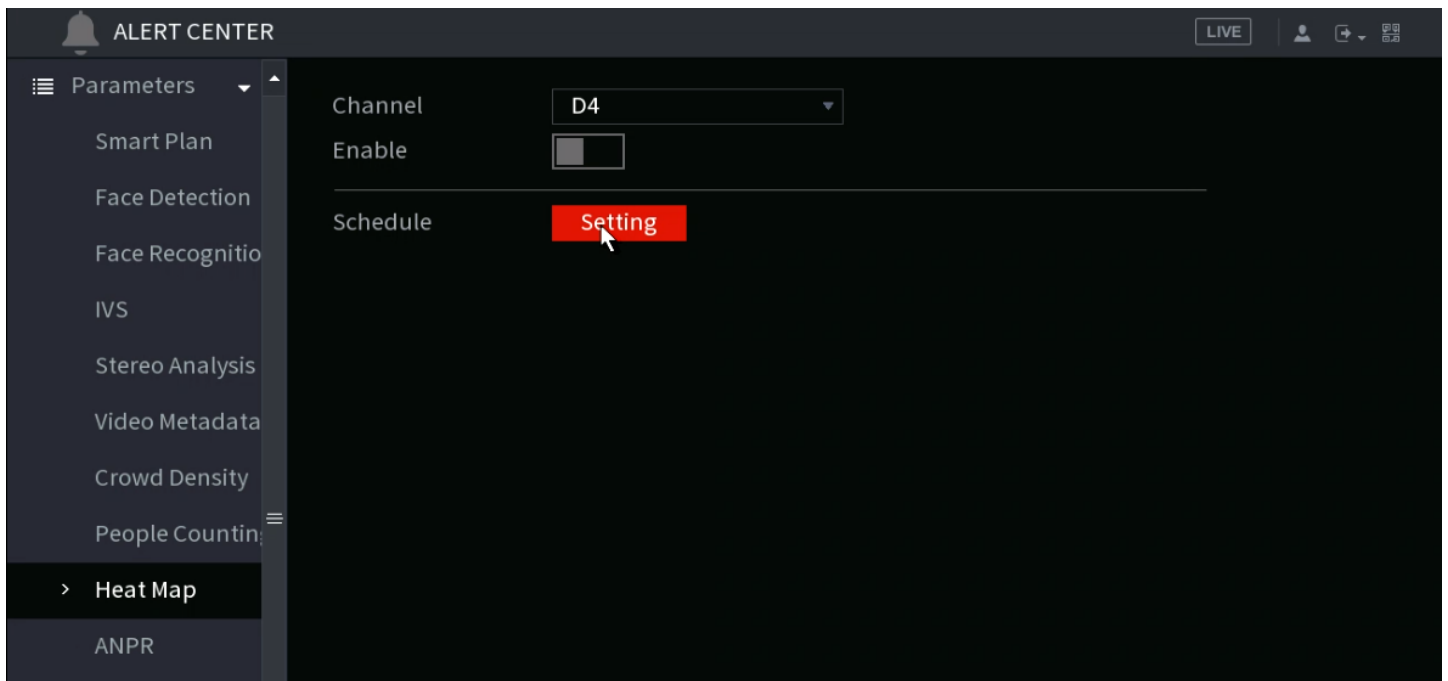
Step 2   Select a channel number and then check the box to enable the function.

Step 3   Click **Setting**.

The **Setting** interface will be displayed. See Figure 4-163.

Figure 4-163
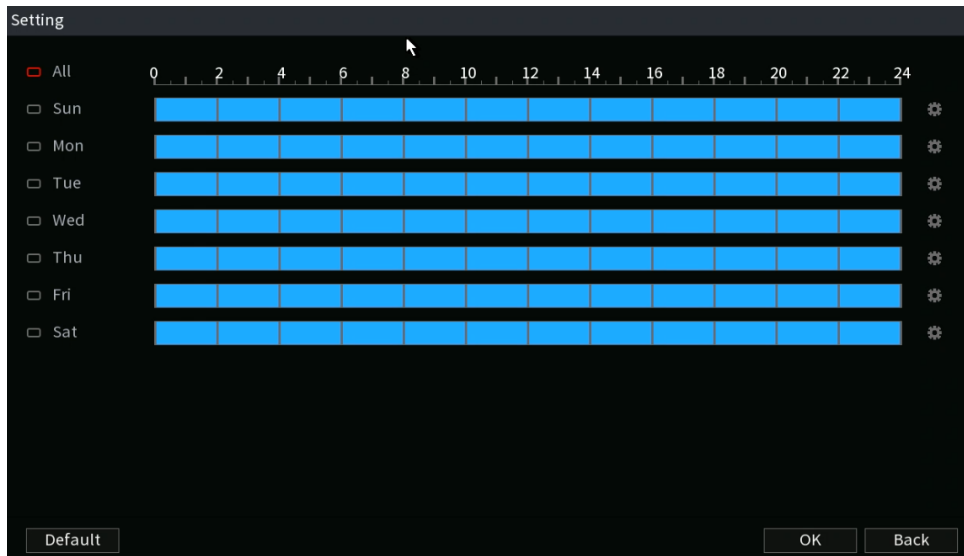
Step 4   Set the arm/disarm period. There are two ways to set the period when the rule will be active.

- Configure the period by drawing.

  Select the corresponding date and then use mouse to drag the bar to set the period.

  ◇ Configure for the whole week: Click ☐ next to **All**, (the all the icon will change to ∞) you can then define the period for all the days simultaneously.

  ◇ Configure for several days of a week: Click ☐ on each day, and the, the icon will change to ∞. You can define the period for the selected days simultaneously.

- Configure the period by editing.

1. Click ⚙ of the corresponding date, and then set the period on the pop-up interface. Click **OK** to save.

◇ Up to six periods can be configured for each day.

◇ Under **Copy**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.

2. Click **Apply** to save the settings.

Step 5 Click **Apply** button to complete setup.

4.7.2.9 ANPR

The Automatic number-plate recognition (ANPR) function uses optical character recognition on images to read vehicle registration plates. Note that this function is for IC Realtime ANPR-equipped cameras connected to IC realtime ANPR-supported NVRs.

This section configures the different plate recognition rules, alarm linkage actions depending on set conditions (blacklist, whitelist and regular).

Step 1 Select **Main Menu > Advanced Settings > Alert Center > Parameters > ANPR**. The **ANPR** interface will be displayed. See Figure 4-164.

Figure 4-164
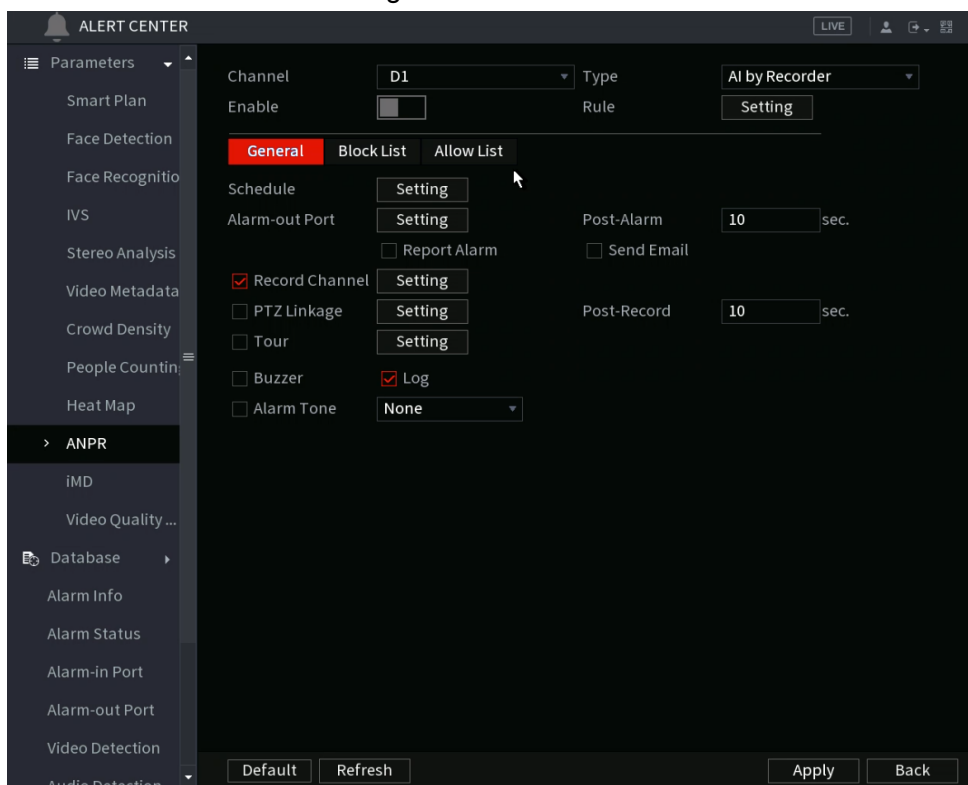
Step 2 Select the **Enable** check box to enable ANPR.

Step 3 Click **General** (default), **Blacklist** or **Whitelist** tab to configure the respective options..

📖

Before enabling the blacklist or whitelist alarm, you will need to add the corresponding plate information to the database. Refer to "4.7.3.3 Black/whitelist" for detailed information.

- Regular: The NVR will trigger an event alarm when it detects any plate number.
- Blacklist: The NVR will trigger an event alarm when it detects a plate number in the blacklist.

● Whitelist: The NVR triggers an alarm when it detects a plate number in the whitelist.

Step 4 Set parameters. See Table 4-50.

Table 4-50

Parameter	Description
Period	Configures the date/time schedule when the function will be active.
Alarm Out	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Latch	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Alarm Upload	When an alarm event occurs, the NVR device will upload an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● Alarm center will need to be set the prior. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. You will need to enable intelligent recording and auto recording first. For details, see "4.1.4.6 Schedule".
PTZ Activation	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the event, the recording will extend for a period of the specified time. The time range is from 10 seconds to 300 seconds.

Parameter	Description
Tour	Click to select the check box and then select the channel(s) for tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● you will need to set the time interval and mode for tour first, see "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Log	If selected, the NVR device will record the information in the log when an alarm event occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. The NVR plays the audio file when the alarm occurs. 📖 Refer to "4.18.1 File Management" to add audio file first.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 5   Click **Apply**.

4.7.2.10 iMD

Intelligent Motion Detect allows the AI algorithm to detect and human or vehicle objects in the live video.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Parameter** > **iMD**.

Figure 4-165
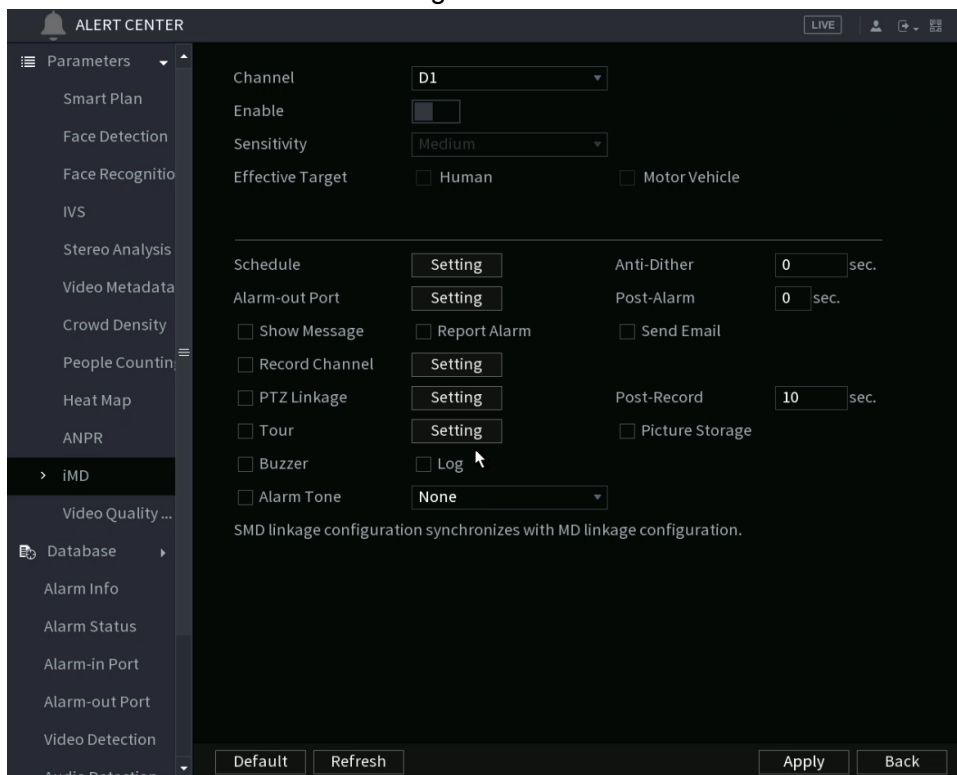
Step 2   Select and enable a channel, and then configure parameters.

Table 4-51

Parameter	Description
Sensitivity	The higher the value is, the easier it is to trigger an alarm. But at the same time, a false alarm may occur. The default value is recommended.
Effective Target	Select human or vehicle or both.
Schedule	Configures the date/time schedule when the function will be active.
Anti-Dither	When an event occurs, there will be a specified time delay before another event can trigger The range is 0 to 600 seconds.
Alarm-out Port	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Post-Alarm	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. you will need to enable intelligent recording and auto recording first. For details, see "4.1.4.6 Schedule".
Post-Record	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.

Parameter	Description
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only supports PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Tour	Click to select the check box and then select the channel(s) for tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **Encode** > **Snapshot**, select **Event** in **Type** list.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.

Step 3   Click **Apply**.

4.7.3 Database

📖

Creating a Face database allows the Face Recognition algorithm to compare faces detected in the live video to the faces stored in the database. Compared faces can be set with a similarity threshold and can trigger an event if the faces detected meet (or do not meet) the similarity threshold or are not in the database.

For privacy reason, the sample images are pixelated.

4.7.3.1 Creating Face Database

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Face Database Config**.
The **Face Database Config** interface will be displayed. See Figure 4-166.

Figure 4-166
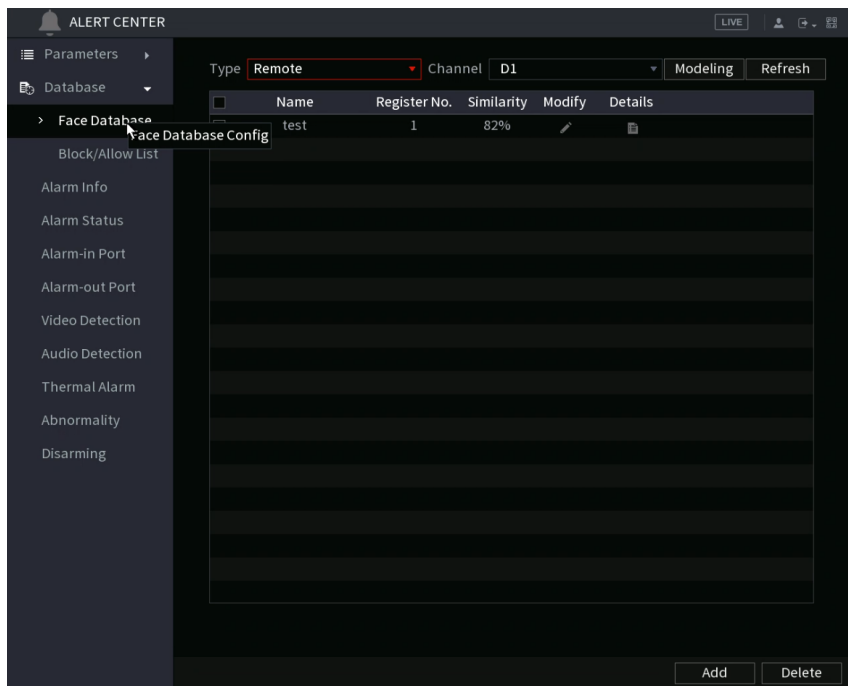
Step 2   Select a channel and then click **Add**.

Figure 4-167
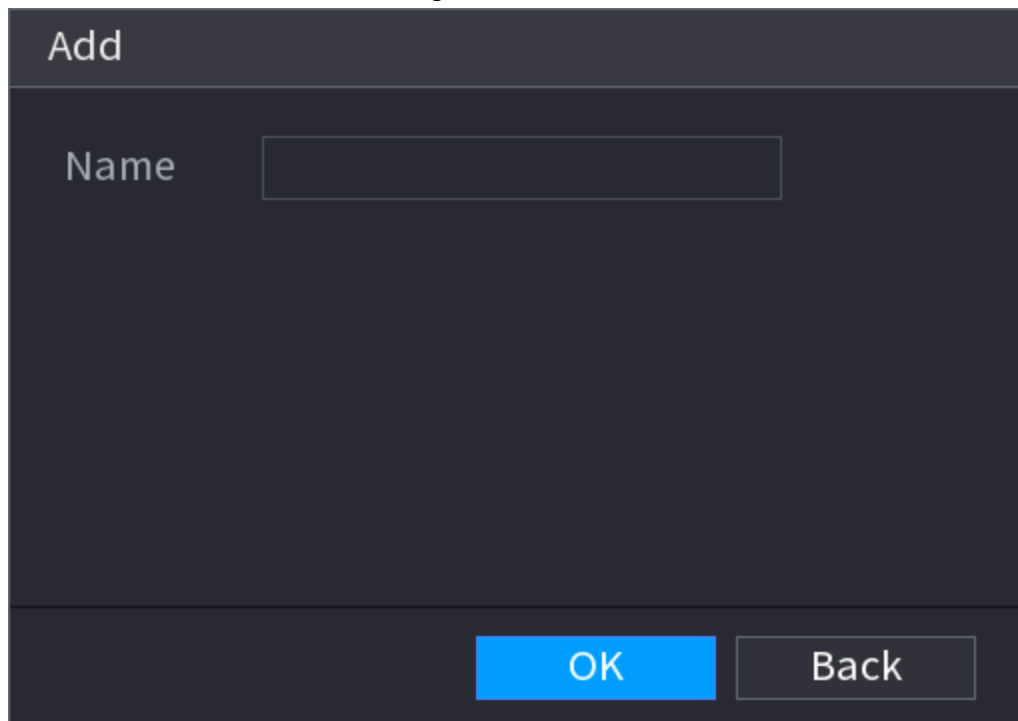
Step 3   Enter the human face database name and then click
OK. The NVR will save the face library.

4.7.3.1.1 Adding Face Pictures

The NVR allows options to add face pictures to the existing libraries one at a time or by batch, or add from the detected faces in an advanced search query.

📖

To import single face pictures or by batch, the pictures will need to be stored in a USB storage device. The picture size should be smaller than 256K with a resolution between 200×200–6000×5000.

4.7.3.1.2 Adding a Single Face Picture

Follow the instructions to add a single face picture to the database.

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Face Database Config**
The **Face Database Config** interface will be displayed.
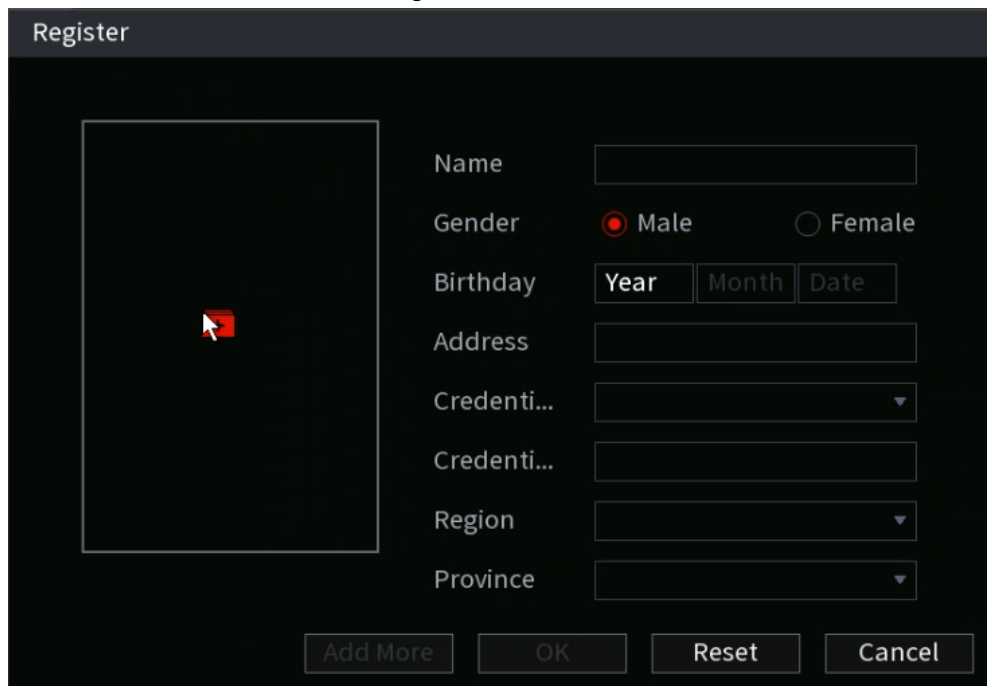
Step 2   Click the 📄 icon next to the library that you want to configure.
The **Details** interface will be displayed. See Figure 4-168.

Figure 4-168
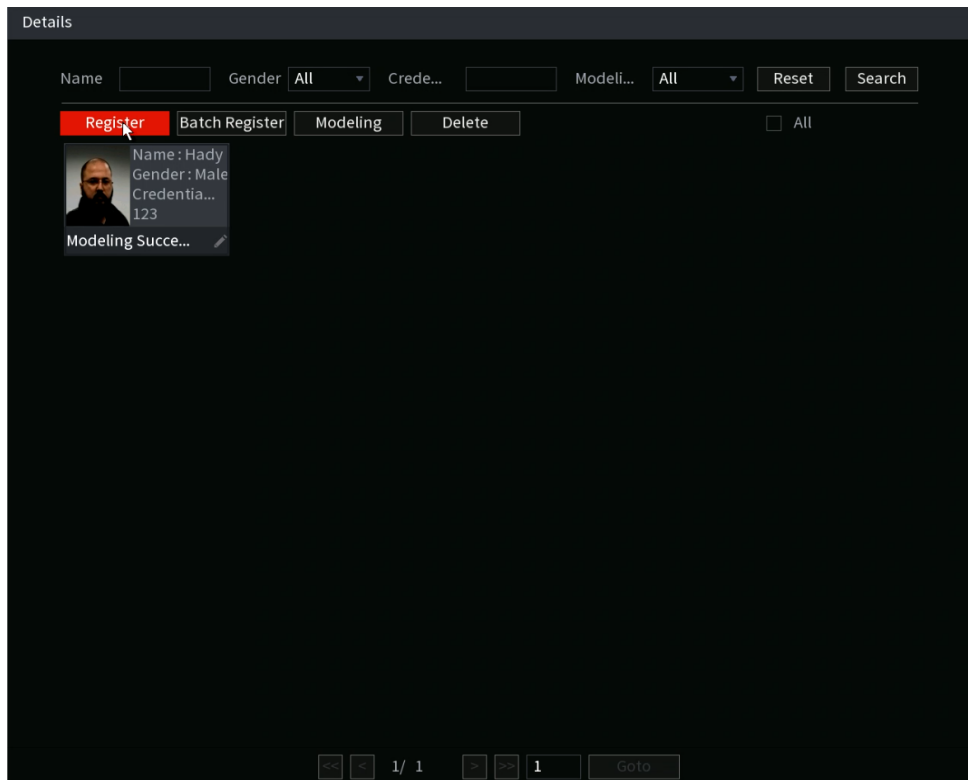
Step 3   Click **Register**.
The **Register** interface will be displayed. See Figure 4-169.

Figure 4-169
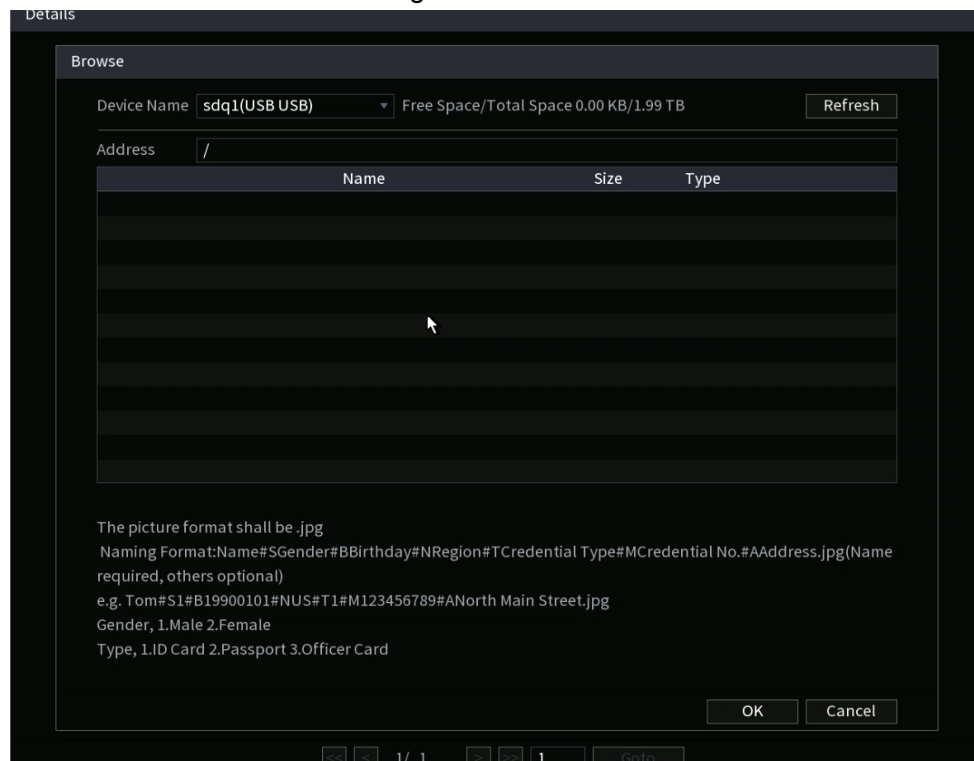
Step 4   Click ⊞ to add a face picture.
The Browse interface will be displayed. See Figure 4-170.

Figure 4-170

Step 5   Select a face picture and enter the registration information. See Figure 4-171.

Figure 4-171

Step 6   Click **OK**.

The NVR will notify with a prompt if the registration is successful.

Step 7 On the **Details** interface, click **Search**.

The NVR will notify with a prompt if modeling is successful. See Figure 4-172.

📖

If the NVR prompts a message indicating modeling is in process, wait for a few moments before clicking Search again as the system is currently processing.

If modeling has failed, the registered face picture cannot be used for face recognition.

Figure 4-172

4.7.3.1.3 Adding Face Pictures in Batches

The NVR supports a batch add system if you want to import several human face images at a time.

Step 1   You can name the individual pictures in the following format to include information when registering the faces to the database. The format and information are shown below in Table 4-52.

Table 4-52

Name#SGender#BBirthday#NRegion#PProvince#CCity#TCredentialType#MCredential No.#AAddress#RRemarks

Naming format	Description
Name	Input the name.
Gender	Input 1 or 2. (1 represents male, and 2 represents female)
Birthday	Input the numbers in the format of yyyy-mm-dd.
Country	Enter the abbreviation of country. For example, CN for China.
ID Type	Input 1, 2 or 3. (1 represents ID card; 2 represents passport; 3 represents military officer password.
ID No.	Input the ID number (if applicable)
Address	Input the address.(if applicable)

Step 2   Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Face Database Config**.

The **Face Database Config** interface will be displayed.

Step 3   Click on the 🗊 icon next to the library that you want to configure.

The **Details** interface will be displayed. See Figure 4-168.

Step 4   On the **Details** interface, click **Batch Register**.

The Batch register interface will be displayed. See Figure 4-173.

Figure 4-173
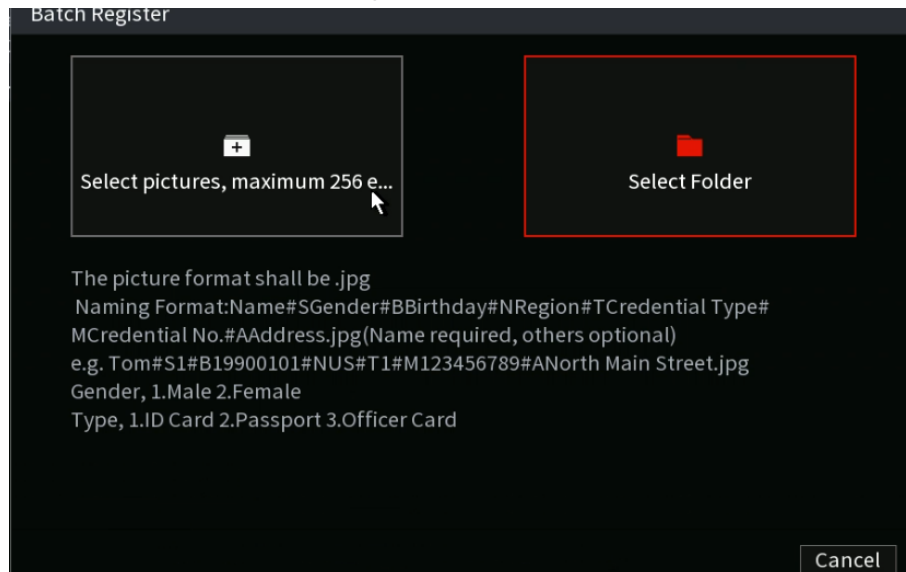
Step 5 Click **Select pictures, maximum 256 per batch** or **Select a Folder** to import face
pictures.
Step 6 Click **OK** to complete batch registration.

4.7.3.2 Exporting/Importing Face Database

You can export and import a local face database.

4.7.3.2.1 Exporting Face Database

Step 1 Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Face
Database Config**.

Step 2 Select one or several face databases, and then click **Export**.
Step 3 Configure the address (file path) and password.
📖

- A password is required; otherwise, the imported database cannot be saved.
- The address will change to /NVR/Facelib/ automatically if this directory is not
changed.

Figure 4-174
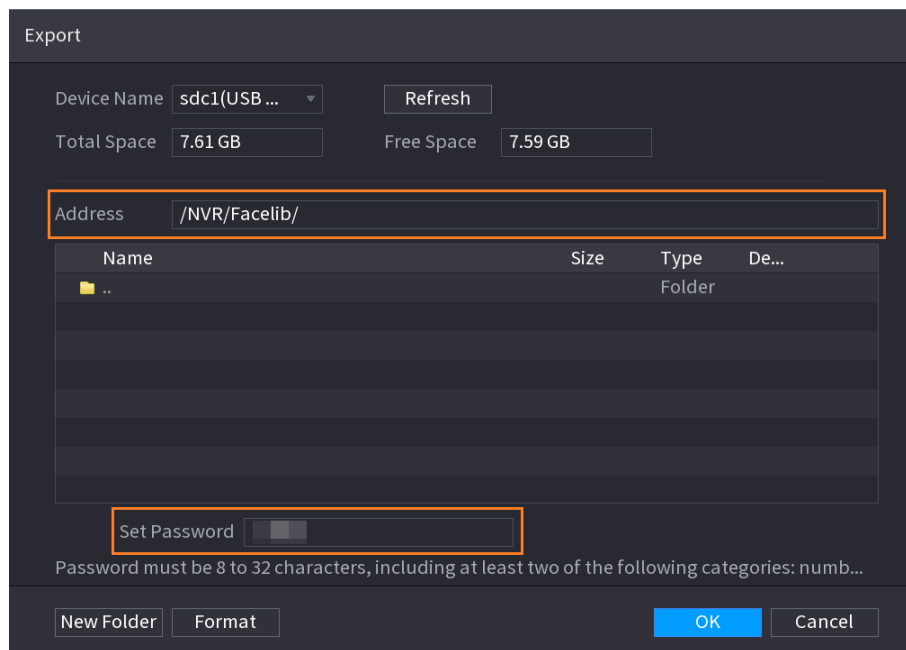
Step 4 Click **OK** to start exporting the face database. You can view the progress on the
exporting interface.

Figure 4-175 Export progress
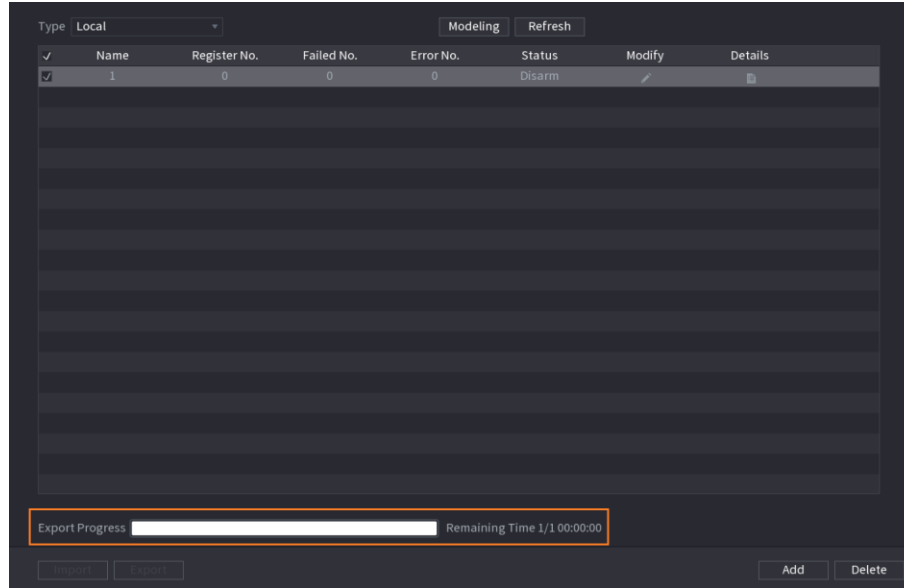
4.7.3.2.2 Importing Face Database

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Face Database Config**

Step 2   Click **Import**.

Step 3   Set address and password.

📖

- Password is required. This is the same password created when the database was exported. Without a correct password, the import will not be saved..
- The address will change to /NVR/Facelib/ automatically if this directory is not changed.

Step 4   Click **OK** to start importing the face database, and you can view the progress on the importing interface.

4.7.3.3 Black/whitelist

The Blacklist/ White list database is used in conjunction with an ANPR camera. The NVR can compare the detected plate information with the plate on the blacklist/whitelist and then trigger the corresponding alarm linkage.

After creating and enabling the black/whitelist, the plate in the blacklist will be indicated on the preview interface with a red outline on the plate list, while the plate in the whitelist will be indicated as green on the plate list. For the plate not in the black/whitelist, the plate will be indicated as white.

4.7.3.3.1 Adding B/W List

Step 1   Select **Main Menu > Advanced Settings > Alert Center** > **Database** > **Block/Allow List**. The **Block/Allow List** interface will be displayed. See Figure 4-176.

Figure 4-176
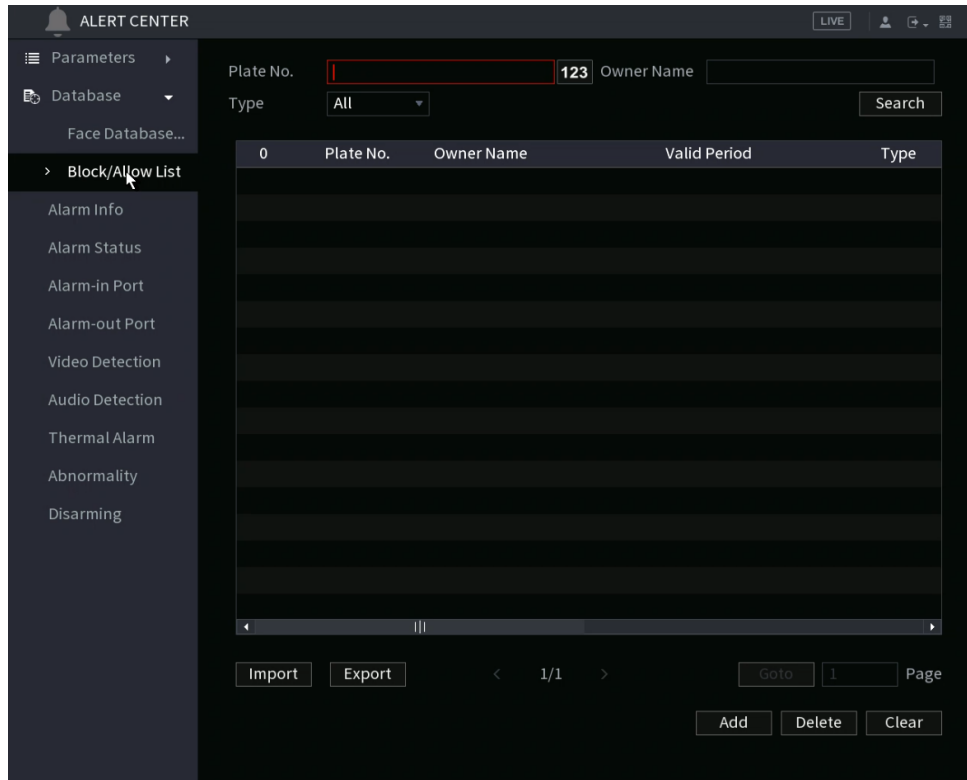
Step 2 Input the plate information such as plate number, car owner name, and then select
Black List or **White List** as needed.

Step 3 Click **Add**.

Changes to black list/white list configurations on the NVR will be synchronized to the
ANPR-supported camera with black list/white list support.

4.7.3.3.2 Deleting Black/White List

Set type as **White List**, **Black List**, or **All**, and then click **Search**. The NVR will
display the black/whitelist information. See Figure 4-177.

● On the searched results list, check the box before the plate number and then click **Delete**, or
click the 🗑 of the corresponding plate number, you can then delete the plate information on
the black/white list.

● Click **Clear** to delete all plate information on the black/white list.

Changes to black list/white list configurations on the NVR will be synchronized to the
ANPR-supported camera with black list/white list support.

Figure 4-177
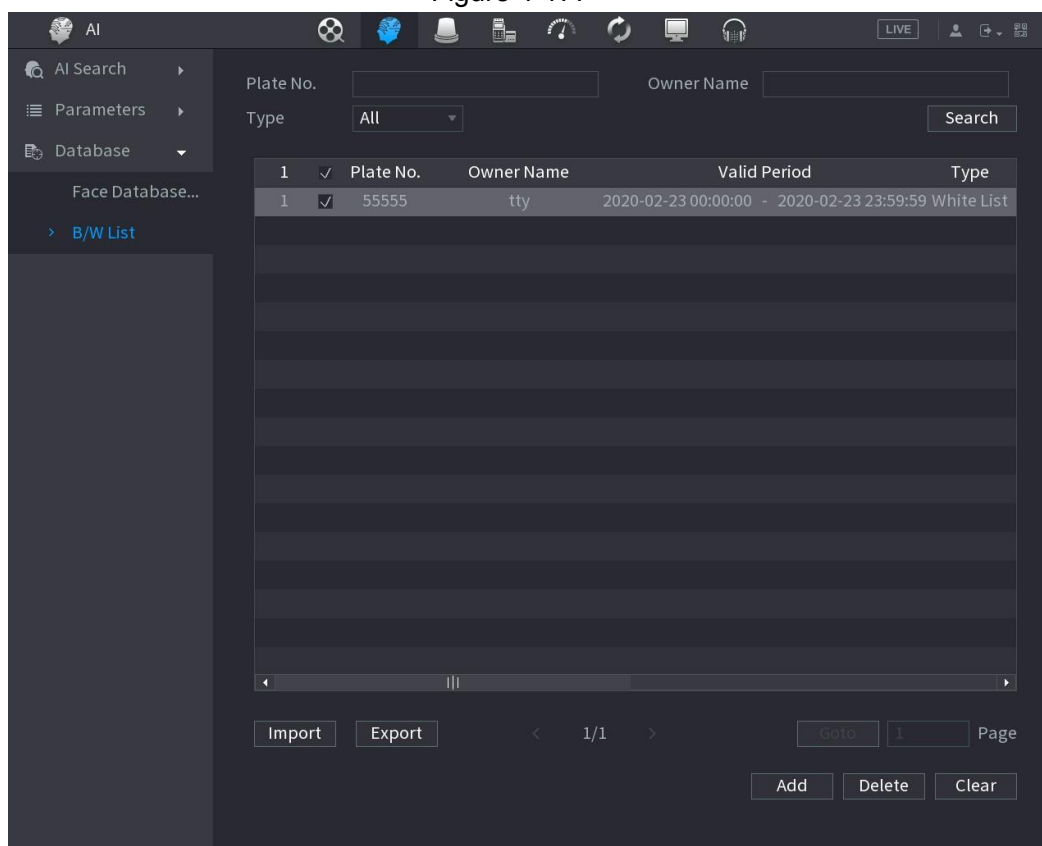
4.7.3.3.3 Import/Export Black/whitelist

The NVR supports the exporting black/whitelist to the USB device, or importing black/whitelist from a USB device. The NVR supports .csv or .xlsx file. The export file format is .csv.

● To import black/whitelist: Click **Import** and then select the corresponding file, click **Browse** to select and import the file.
● To export black/whitelist: Click **Export** and then select the file storage path and then click **Save**.

4.8 Event Manager

4.8.1 Alarm Info

You can search, view and back up the alarm information.

Step 1　Select **Main Menu > Advanced Settings > Alert Center > Alarm Info**.
　　　　The **Alarm Info** interface will be displayed. See Figure 4-178.

Figure 4-178
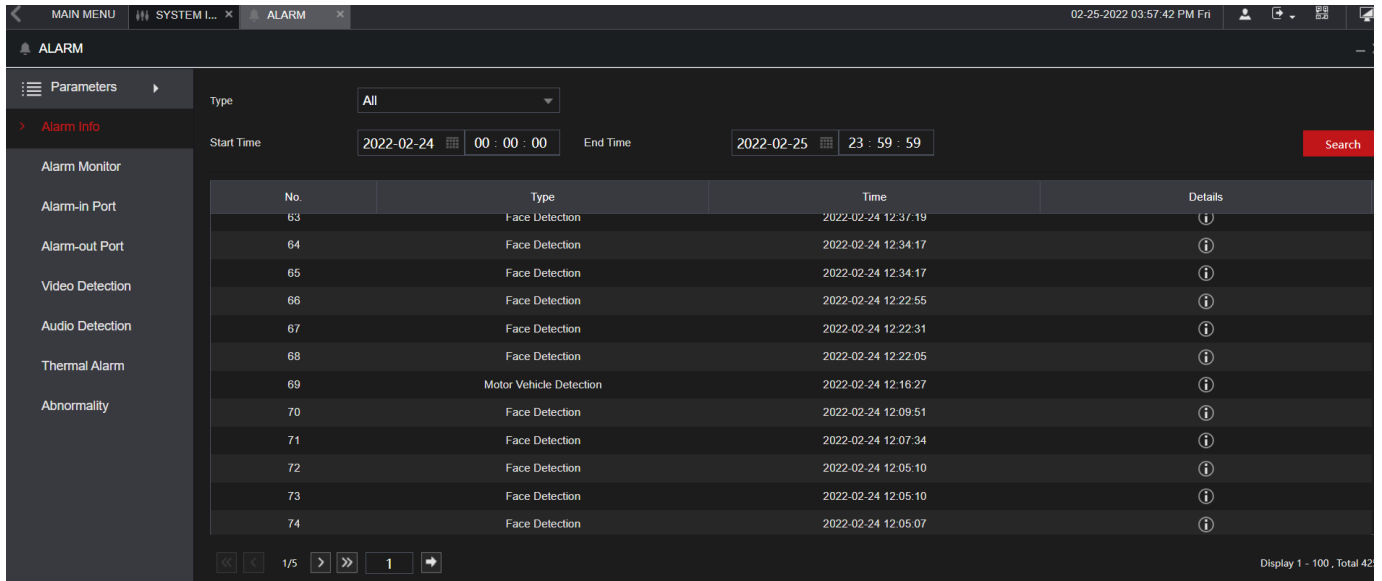
Step 2   In the **Type** list, select the event type; In the **Start Time** box and **End Time** box, enter the desired time.

Step 3   Click **Search**.

The search results will be displayed.

Step 4   Click **Backup** to back up the search results into an external storage device.

- Click to play the recorded video of the alarm event.
- Double-click a log or click Details to view the detailed information of the event.

4.8.2 Alarm Monitor

This section allows you to live view NVR and remote camera alarm events.

Select **Main Menu > Advanced Settings > Alert Center >Alarm Monitor.** The interface will be displayed. See Figure 4-179.

Here, you select the event types you want to monitor. When the selected event type occurs, it will appear in the events list on the right side.

Figure 4-179
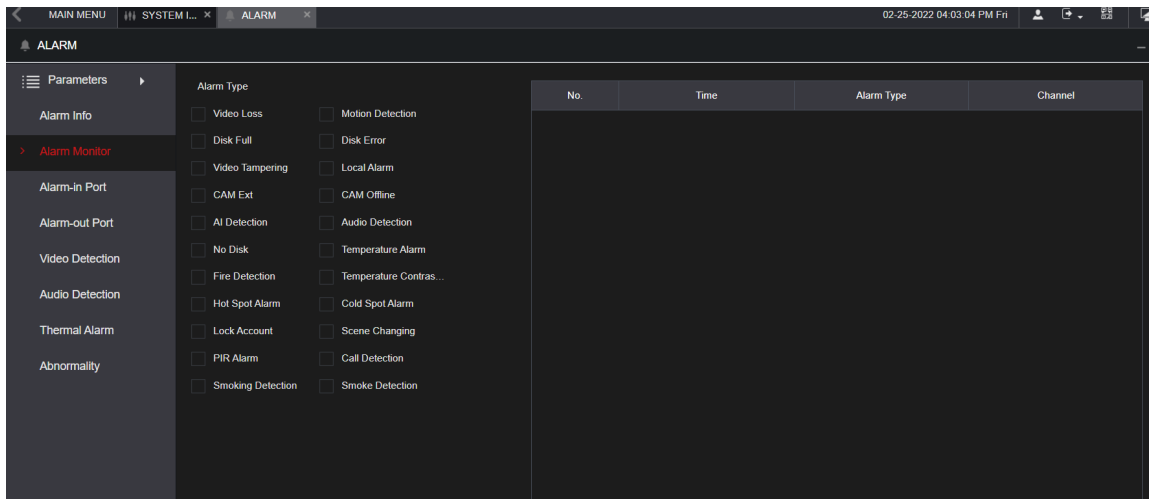
4.8.3 Alarm Input

Step 1   Select **Main Menu > Advanced Settings > Alert Center > Alarm-in Port**.
The **Alarm-in Port** interface will be displayed. See Figure 4-180.

Step 2   There are four alarm input types:

- Local alarm: After connecting an alarm device to the NVR alarm input port, The NVR can trigger the corresponding alarm operations when there is alarm signal from the alarm input port to the NVR.
- Network alarm: NVR triggers corresponding alarm operations when it receives the alarm signal via the network transmission.
- IPC external alarm: When a network camera with a connected peripheral device has triggered an alarm, it can upload the alarm signal to the NVR via the network transmission. The NVR can trigger the corresponding alarm operations.
- IPC offline alarm: When the network connection between the NVR and the network camera is off, the NVR can trigger the corresponding alarm operations.

Figure 4-180
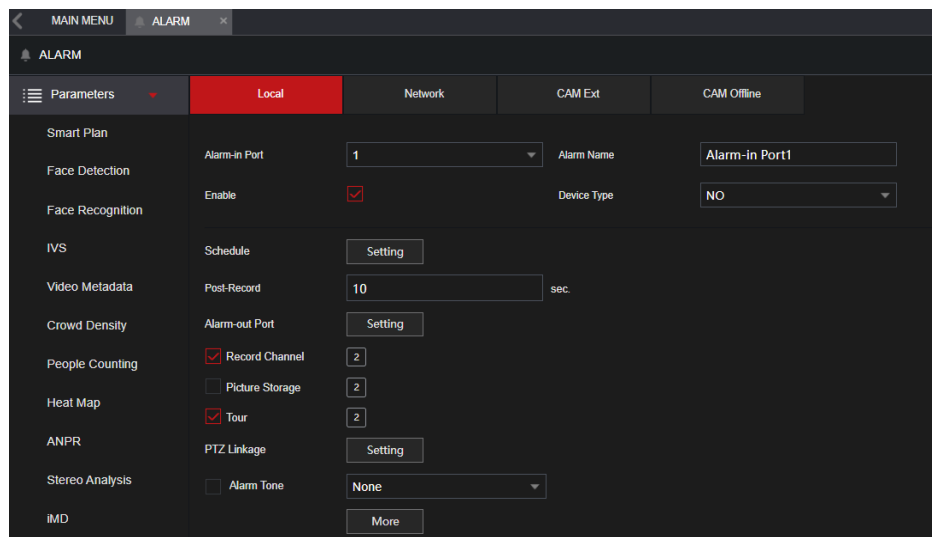
Step 3   Set **Alarm-in Port** channel number and then select the Enable check box to enable the function.

Table 4-53

Parameter	Description
Alarm-in Port	Select a channel to set alarm.
Enable	Check the box [✓] to enable the function.
Alarm Name	Enter an alarm name.
Device Type	NO (normally open) or NC (normally closed).
Schedule	Define a period during which the alarm is active. For details, see "4.8.5.1 Motion Detection".
Alarm-out Port	This will trigger an alarm device (such as lights, sirens, etc.) if one is connected to the NVR alarm output port.
Post-Alarm	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule"..
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. ● Tripwire events only support PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".

Parameter	Description
Post Record	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour ends, the previous screen split mode will resume.
Picture Storage	Select the **Picture Storage** check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **Encode** > **Snapshot**, and then select **Event (Trigger)** in **Type** list.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Buzzer	Select the check box to activate the buzzer when an alarm event occurs.

Step 5   Click **Apply**.

4.8.4 Alarm Control

This allows you to configure the alarm output operation (Auto/manual/off). The normal operating mode should be "Auto". See below for options:

● Auto: Once an event occurs, the NVR can generate an alarm.
● Manual: This manually triggers the device connected to the alarm output.
● Off: Disables the alarm output function.

    Step 1   Select **Main menu** > **Advanced Settings > Alert Center** > **Alarm-out Port**.
        The **Alarm-out Port** interface will be displayed. See Figure 4-181.

Figure 4-181
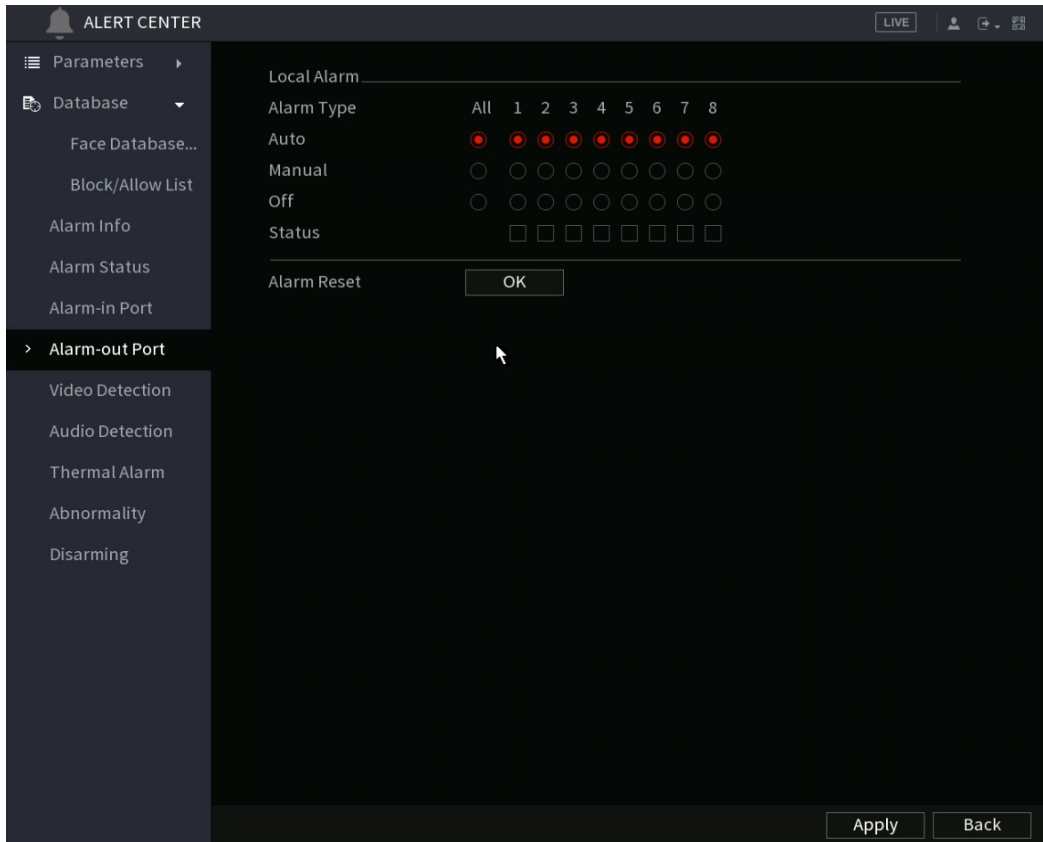
Step 2   Select the alarm mode of the alarm output channel.
● To clear all alarm output statuses, click **OK** in the **Alarm Reset** section.
● View the alarm output status, click on the **Status** column.

Step 3 Click **Apply**.

4.8.5 Video Detection

The Video Detection function (motion detection) detects pixelation change. If the live video has changed considerably (such as moving objects, or if the video is distorted), the NVR can trigger the corresponding event activation operations.

Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** > **Motion Detection**, here you can view the Video detect interface. There are five detection types: motion detection, video loss, tampering, scene changing, and PIR alarm.

4.8.5.1 Motion Detection

If a moving object appears or moves fast enough to reach the preset sensitivity value, the NVR will trigger an event.

Select **Main menu > Basic Settings> Motion Detection**.

The **Motion Detection** interface will be displayed. See Figure 4-182.

Figure 4-182
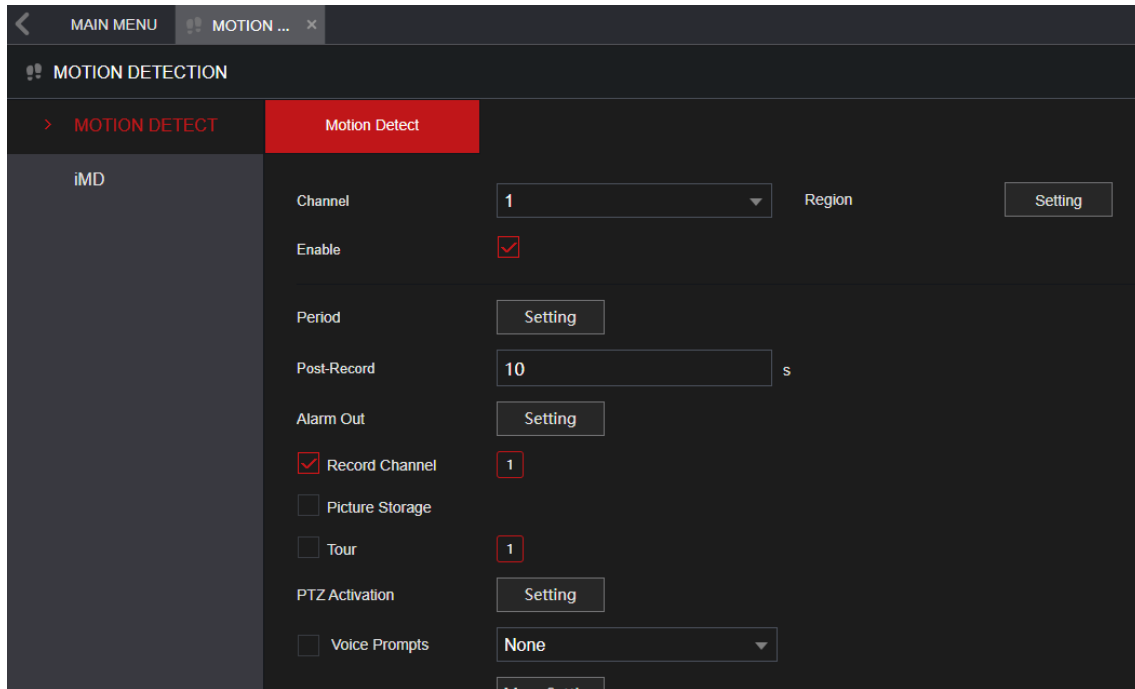
Configure the settings for the motion detection parameters. See Table 4-54.

Table 4-54

Parameter	Description
Channel	In the Channel list, select a channel to set the motion detection.
Region	Click Setting to define the motion detection region.
Enable	Enable or disable the motion detection function. Check the box to enable the function.
Sensitivity	The higher the value is, the easier it is to trigger an alarm. But at the same time, a false alarm may occur. The default value is recommended.
Schedule	Define a period during which the motion detection is active.
Anti-Dither	When an event occurs, there will be a specified time delay before another event can trigger The range is 0 to 600 seconds.
Alarm-out Port	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Post-Alarm	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.

Parameter	Description
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. 📖 You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
Post-Record	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. when an alarm event occurs, the NVR device associates the channel to perform the corresponding PTZ action. For example, activates the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire alarm supports to activate PTZ preset point only. ● you will need to set the corresponding PTZ actions first, see "4.4.4 Calling PTZ Functions".
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour is over, the preview interface is restored to the screen split mode before the tour.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **Encode** > **Snapshot**, select **Event** in **Type** list.

Parameter	Description
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.

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

📖

- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, then select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply. Note:** This is not recommended as typically each camera (if looking at a different view), may require its own specific settings.

4.8.5.1.1 Setting the Motion Detection Region

The NVR and supported IP cameras allow up to four different regions per channel. These regions can be configured with their own Sensitivity and Threshold settings.

Step 1   Next to **Region**, click **Setting**.
The region setting screen will be displayed.
Step 2   Point to the middle top of the interface.
The setting interface will be displayed. See Figure 4-183.

Figure 4-183
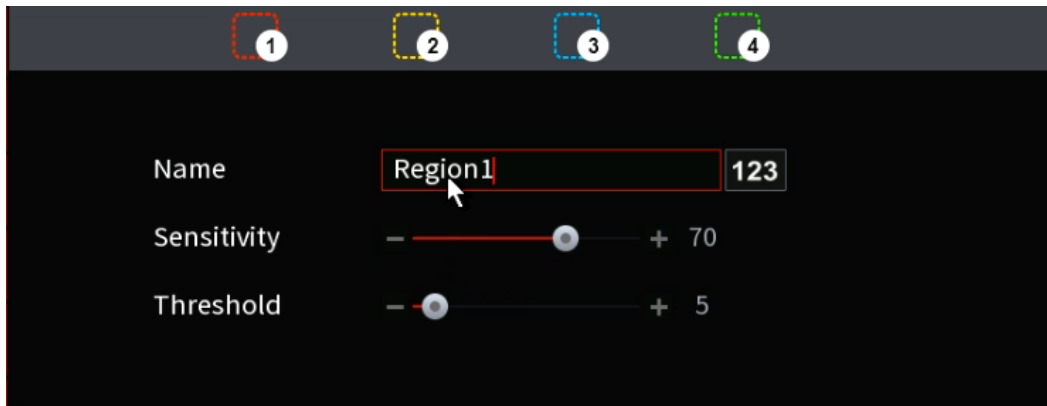
Step 3   Configure the regions settings. You can configure totally four regions.

- Select one region, for example, click 🔘.
- Drag on the screen to select the region that you want to detect.
- The selected area shows the color that represents the region.
- Configure the parameters. See Table 4-55.

Table 4-55

Parameter	Description
Name	Enter a name for the region.
Sensitivity	Every region of every channel has an individual sensitivity value. The greater the value is, the easier the event will be triggered.
Threshold	The threshold for motion detect. Every region of every channel will have an individual threshold.

When any one of the four regions triggers a motion detect event, the channel where this region belongs will trigger a motion detect event.

Step 4 Right-click on the screen to exit the region setting interface.

Step 5 On the **Motion Detection** interface, click **Apply** to complete the settings.

4.8.5.1.2 Setting Schedule

Motion Detect events will only occur within the defined time period.

Step 1 Next to **Schedule**, click **Setting**.

The Setting interface will be displayed. See Figure 4-184.

Figure 4-184
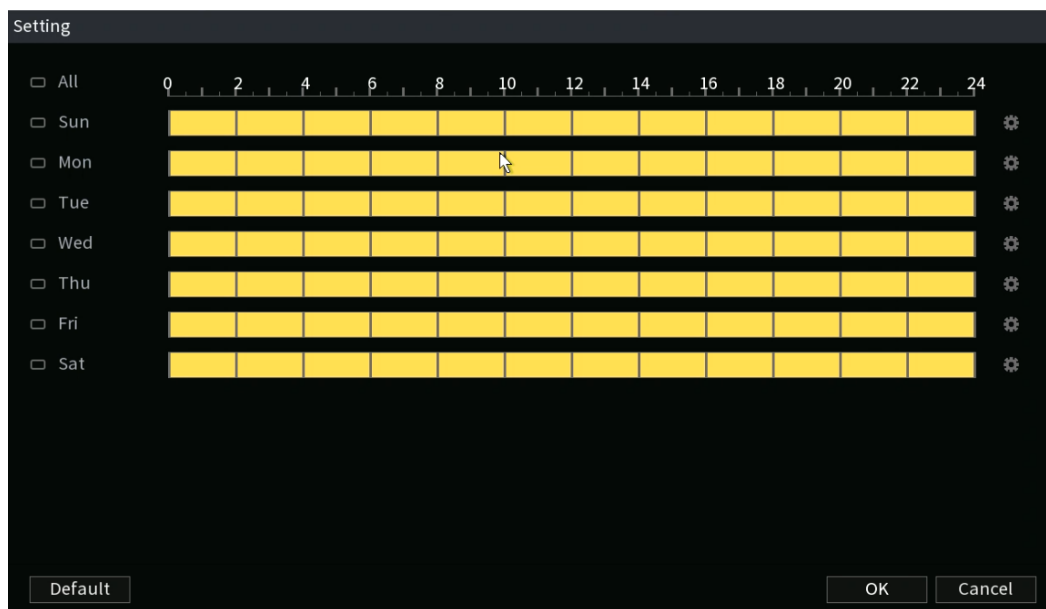
Step 2 Define the motion detection period. By default, it is active all the time.

- Define the period by drawing.
  - ◇ Define for a specified day of a week: On the timeline, click the half-hour blocks to select the active period.
  - ◇ Define for several days of a week: Click ▢ before each day, the icon will change to ∞. On the timeline of any selected day, click the half-hour blocks to select the active periods, all the days with the ∞ icon will take the same settings.

◇ Define for all days of a week: Click **All**, all ⬛ icons will change to 🔗. On the timeline of any day, click the half-hour blocks to select the active periods, and all the days will take the same settings.

● Define the period by editing. For the example, Sunday will be configured..
  1. Click ⚙.
     The **Period** interface will be displayed. See Figure 4-185.

Figure 4-185
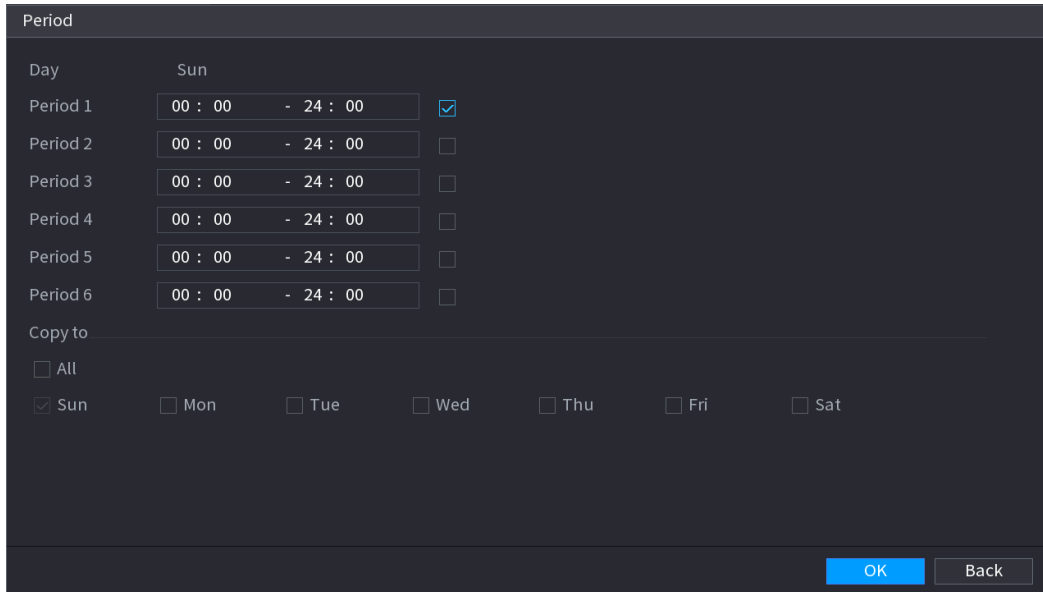
2. Enter the time frame for the period, and then select the check box to enable the settings.
   ◇ There are six periods for you to set for each day.
   ◇ Under **Copy to**, select **All** to apply the settings to all the days of a week, or select specific day(s) that you want to apply the settings to.
3. Click **OK** to save the settings.

Step 3   On the **Motion Detection** interface, click **Apply** to complete the settings.

4.8.5.2 Video Tampering

If a camera lens is covered, or if the video displays in a single color due to sunlight conditions, the NVR can detect and create an event for these situations.

Step 1   Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** > **Video Tampering**.
         The **Video Tampering** interface will be displayed. See Figure 4-186.

Figure 4-186
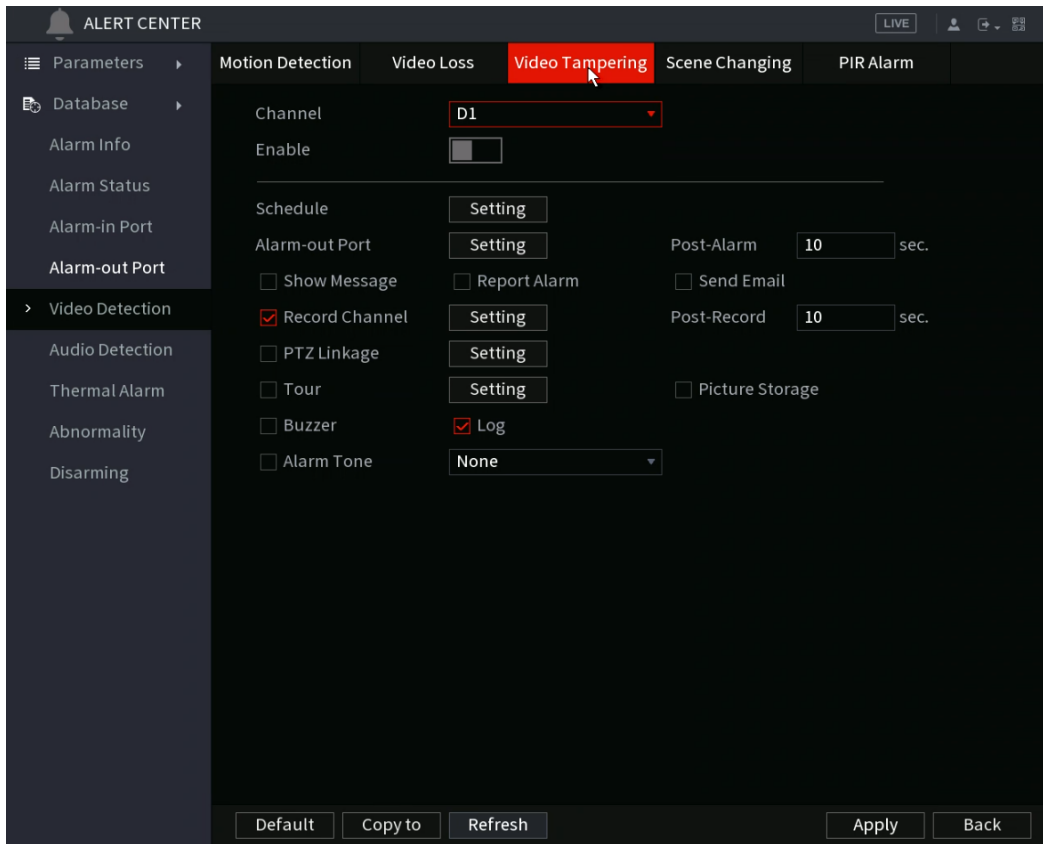
Step 2   To configure the settings for the tampering detection parameters, see "4.8.5.1 Motion Detection".

The Tampering function does not have region and sensitivity options.

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

- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the settings to, and then click **Apply**.

4.8.5.3 Video Loss

If the video loss occurs with a connected camera, the NVR can create an alarm event.

Step 1   Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** > **Video Loss**.
The **Video Loss** interface will be displayed. See Figure 4-187.

Figure 4-187
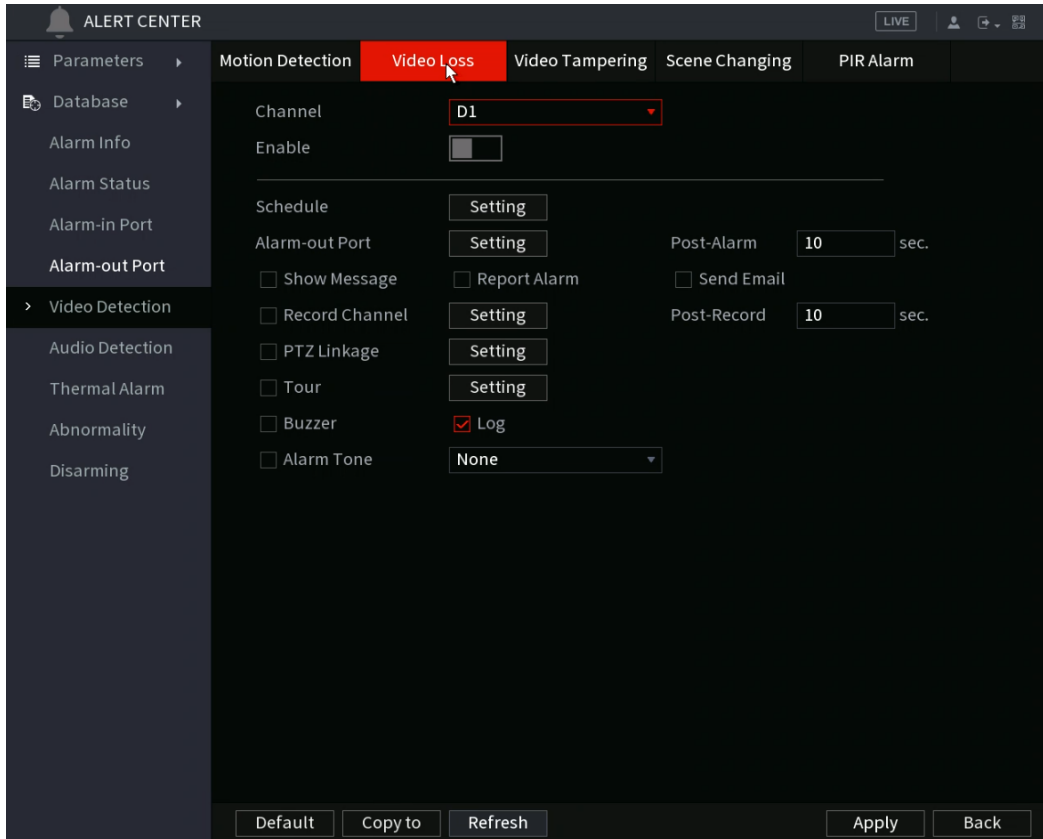
Step 2   To configure the settings for the video loss detection parameters, see "4.8.5.1 Motion Detection".

The video loss function does not have region and sensitivity options.

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

- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply**.

4.8.5.4 Scene Change

This function is for static cameras. If the image scene had changed (for example, if the camera is moved or disturbed the camera without permission), the NVR can generate an alarm event.

Step 1   Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** > **Scene Changing**.

The **Scene Changing** interface will be displayed. See Figure 4-188.

Figure 4-188
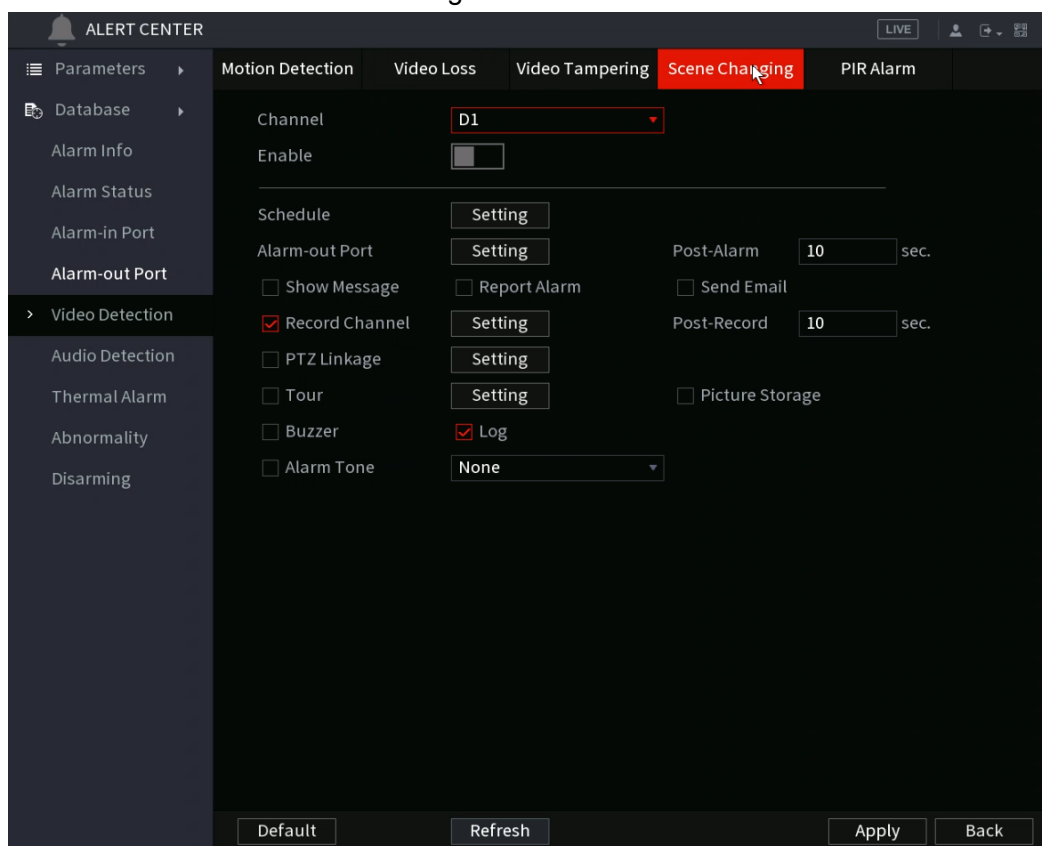
Step 2   To configure the settings for the scene change parameters, see "4.8.5.1 Motion Detection".

Step 3   The scene change function does not have region and sensitivity options.

Step 4   Click Apply to complete the settings.

📖

- Click **Default** to restore the default setting.
- Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you want to copy the motion detection settings to, and then click **Apply**.

4.8.5.5 PIR Alarm

Supported IC Realtime cameras with PIR sensors can communicate with the NVR if the PIR sensor was triggered. PIR sensors are typically more accurate than pixel based motion alarms.

Step 1   Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** > **PIR Alarm**. The PIR Alarm interface will be displayed. See Figure 4-189.

Figure 4-189
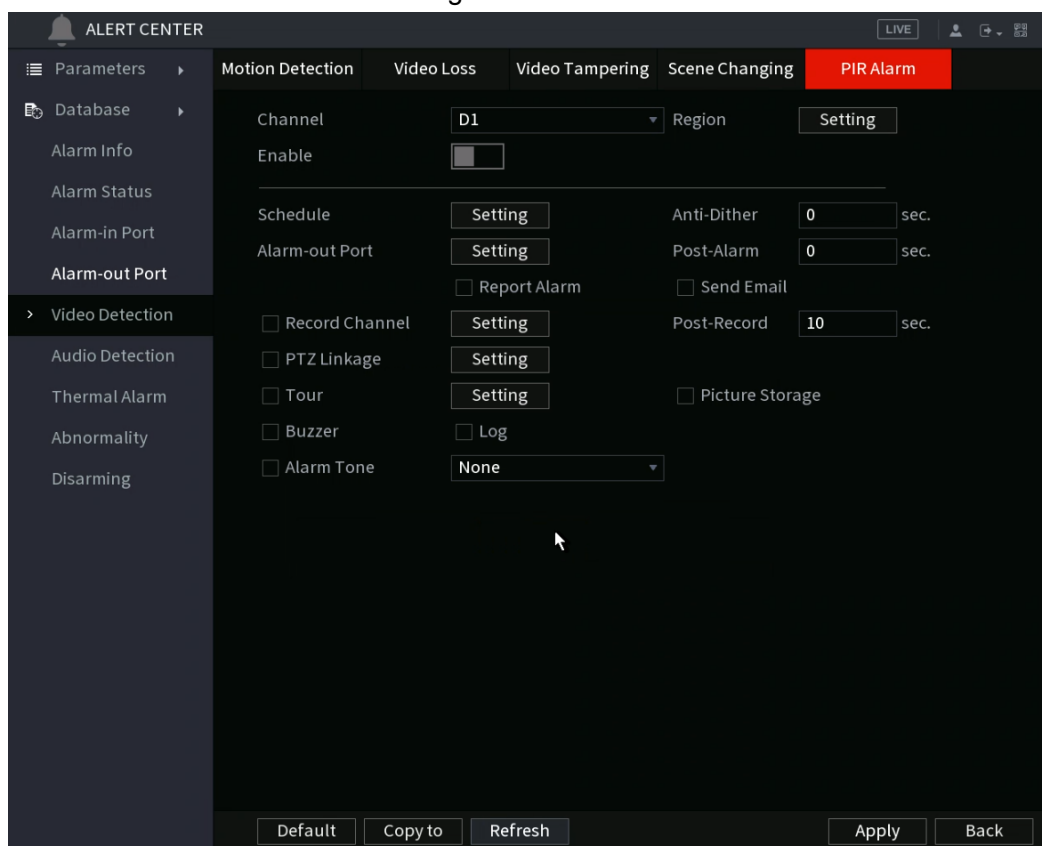
Step 2   To configure the settings for the PIR alarm parameters, see "4.8.5.1 Motion
Detection".

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

📖
● Click **Default** to restore the default setting.
● Click **Copy to**, in the **Copy to** dialog box, select the additional channel(s) that you
want to copy the motion detection settings to, and then click **Apply**.

4.8.6 Audio Detection

The NVR can generate an alarm if it detects abnormal or audio volume changes.

Step 1   Select **Main Menu** > **Advanced Settings**> **Alert Center** > **Video Detection** >
Audio Detection.

Step 2   Configure parameters. See Table 4-56.

Table 4-56

Parameter	Description
Channel	In the Channel list, select a channel to set.
Audio Exception	Check the box here, the NVR can generate an alarm once the audio input is abnormal.
Intensity change	Check the box here, the NVR can generate an alarm once the audio volume becomes strong.
Period	Define a period during which the function is active.

Parameter	Description
Sensitivity	The higher the value is, the easier it is to trigger an alarm. But at the same time, a false alarm may occur. The default value is recommended.
Threshold	You can set the intensity change threshold. The smaller the value is, the higher the sensitivity is.
Period	Configures the date/time schedule when the function will be active.
Alarm Out	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Latch	When the event ends, the alarm will extend for the specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Alarm Upload	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Activation	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. ● Tripwire events only support PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the event, the recording will extend for a period of the specified time. The time range is from 10 seconds to 300 seconds.

Parameter	Description
Tour	Click to select the check box and then select the channel(s) for tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour is over, the preview interface is restored to the screen split mode before the tour.
Snapshot	Select the Snapshot check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **ENCODE** > **Snapshot**, in the Mode list, select **Event (Trigger)**.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.
Voice Prompts	Check the box and then select the corresponding audio file from the dropdown list. The NVR plays the audio file when the alarm occurs. 📖 Refer to "4.18.1 File Management" to add audio file first.
Buzzer	Select the check box to activate the buzzer when an alarm event occurs.

<u>Step 3</u>   Click **Apply** to complete the settings.

4.8.7 Thermal Alarm

The NVR supports IC Realtime thermal IP devices and receives the alarm signal from them. It can recognize the alarm type, and then trigger the corresponding event actions. Depending on the model, the NVR can support fire alarm, temperature (temperature difference), and cold/hot alarm.

● Fire alarm: NVR generates an alarm once it detects there is a fire. The alarm mode includes Preset and Excluded zone.
● Temperature (temperature difference): The NVR triggers an alarm once the temperature difference between two specified area is higher or below the specified threshold.
● Cold/hot alarm: The NVR triggers an alarm once the detected position temperature is higher or below the specified threshold.

📖
● Check device specifications if the IP channel and connected camera support the temperature functions.

<u>Step 1</u>   Select **Main Menu** > **ALARM** > **Thermal Alarm**.
The **Thermal Alarm** interface will be displayed. See Figure 4-190.

Figure 4-190
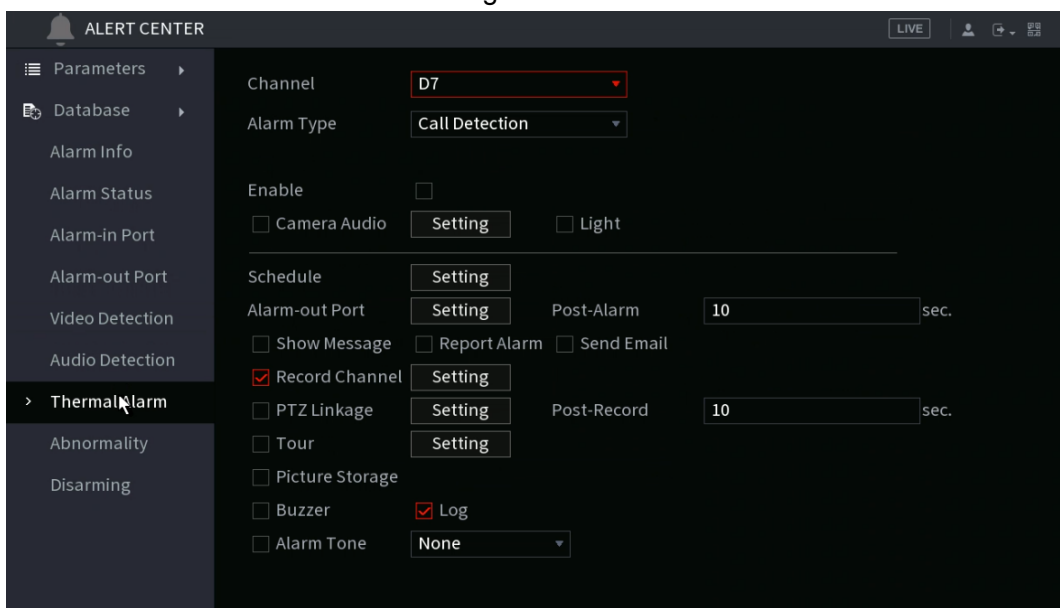
Step 2   Select a channel and alarm type, enable the thermal alarm function.

Step 3   Select fire mode and then enable this function (If the alarm type is **Fire Alarm**).

The NVR supports preset mode and zone excluded mode.

- **Preset**: Select a preset and then enable the function. The NVR generates an alarm once it detect there is a fire.
- **Global**: The NVR filters a specified high temperature zone. The NVR generates an alarm once it has detected the specified zone has fire.

Step 4   Set parameters. See Table 448.

Table 4-57

Parameter	Description
Alarm-out Port	This will trigger an alarm device (such as lights, sirens, etc.) if one is connected to the NVR alarm output port.
Post-Alarm	When the alarm ends, the alarm extends for a period of specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). 📖 ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".

Parameter	Description

Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. 📖 You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Linkage	Select the check box and click Setting to select the channel and PTZ action. When an event occurs, the NVR will have the selected channel perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. 📖 ● Tripwire events only support PTZ preset point activation. ● Corresponding PTZ actions must be configured prior, see "4.4.4 Calling PTZ Functions".
Delay	At the end of the event, the recording will extend for a period of the specified time. The time range is from 10 seconds to 300 seconds.
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. 📖 ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour is over, the preview interface is restored to the screen split mode before the tour.
Snapshot	Select the Snapshot check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **ENCODE** > **Snapshot**, in the Mode list, select **Event (Trigger)**.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.

Parameter	Description

	The NVR will play a specified audio file when the event occurs.
Alarm Tone	To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.

Step 5   Click **Apply**.

4.8.8 Abnormality

Step 1   Select **Main Menu** > **Advanced Settings** > **Alert Center > Abnormality**.

The **Abnormality** interface will be displayed. See Figure 4-191.

Figure 4-191
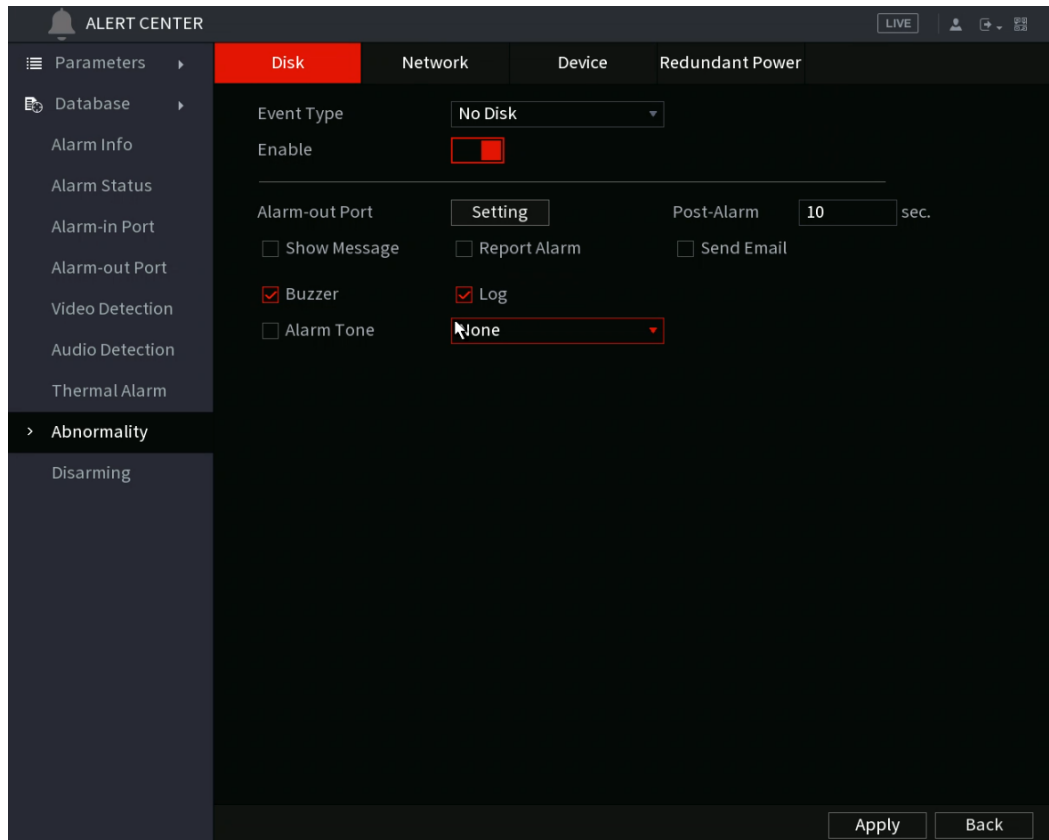
Figure 4-192

Figure 4-193

Step 2   Configure parameters. See Table 4-58.

Table 4-58

Parameter	Description
Event Type	- Disk: Configures a linkage when there is a HDD event such as HDD error, no HDD, no space. - Network: Configures a linkage when there is a network event such as disconnection, IP conflict, MAC conflict. - Device: Configures a linkage when there is a device event such as fan speed exception. 📖 Different series NVRs support different event types. Please see device specifications.
Less than	The NVR generates an alarm once the HDD space is less than the threshold. 📖 For **HDD No Space** selection only.

Parameter	Description
Alarm-out Port	This will trigger an alarm device (such as lights, sirens, etc.) if one is connected to the NVR alarm output port. .
Post-Alarm	When the alarm ends, the alarm will extend for a period of the specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Report Alarm	Select the check box. when an alarm event occurs, the NVR device uploads an alarm signal to the network (including the alarm center). ● Not all NVR models support this feature. ● you will need to set the alarm center first. For details, see "4.12.13 Alarm Center".
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".
Record Channel	This allows channels to record when the event occurs. Select the check box and then select the channel(s) to be recorded. You will need to set up the appropriate record schedule prior. For details, see "4.1.4.6 Schedule".
PTZ Linkage	● Select the check box and click **Setting** to select the channel and PTZ action. When an event occurs, the NVR will trigger the selected PTZ action on the channel. For example, activate the PTZ in channel one to turn to the preset point X. ● Tripwire events only support PTZ preset point activation. ● Configure the corresponding PTZ actions prior, see "4.4.4 Calling PTZ Functions".
Tour	Click to select the check box and then select the channel(s) for the tour. When the event is triggered, the local interface of the NVR device will display the selected channel(s) on the screen. ● It is recommended to set the interval and tour mode beforehand. See "4.17.2 Tour". ● After the tour is over, the preview interface is restored to the screen split mode before the tour.

Parameter	Description
Snapshot	Select the Snapshot check box to take a snapshot of the selected channel. 📖 To use this function, select **Main Menu > Advanced Settings > Camera Configuration** > **ENCODE** > **Snapshot**, in the Mode list, select **Event (Trigger)**.
Log	Select the check box, the NVR device records the alarm information in the log when an alarm event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Buzzer	● Activates the onboard buzzer when an event occurs.

Step 3　Click **Apply**.

4.8.9 Disarming

This section allows you to disarm all alarm linkage actions as needed.

Step 1　Select **Main Menu** > **Advanced Settings** > **Alert Center** > **Disarming**.

Step 2　Click ▮▮ to enable disarming.

Figure 4-194
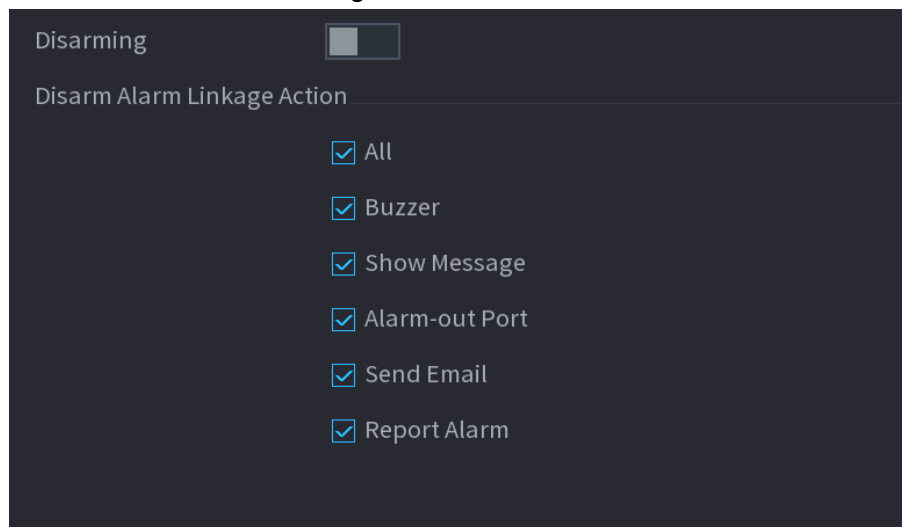
Step 3　Select alarm linkage actions to disarm.

📖

All alarm linkage actions will be disarmed when you select **All**.

Step 4　Click **Apply**.

4.9 Operation and Maintenance

4.9.1 Log

You can view and search the log information, or backup log to the USB device.

Step 1   Select **Main Menu** > **Info** > **Log**.

The **Log** interface will be displayed. See Figure 4-199.

Figure 4-199
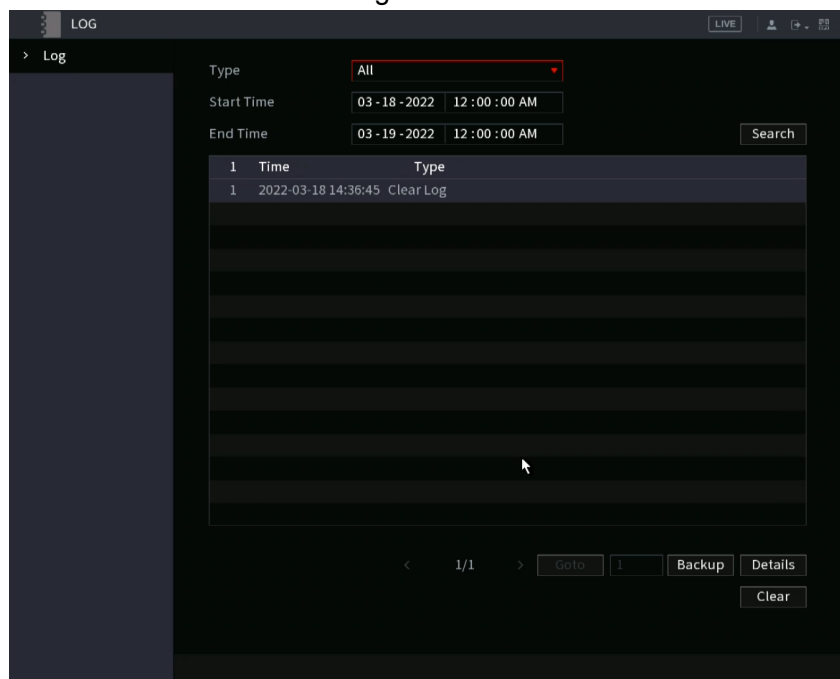
Step 2   In the **Type** list, select the log type that you want to view (**System**, **Config**, **Storage**, **Record**, **Account**, **Clear Log**, **Playback**, and **Connection**) or select **All** to view all logs.

Step 3   In the **Start Time** box and **End Time** box, enter the time period to search, and then click **Search**.

The search results will be displayed.

- Click **Details** or double-click the log that you want to view, the **Detailed Information** interface will be displayed. Click **Next** or **Previous** to view more log information.

Figure 4-200
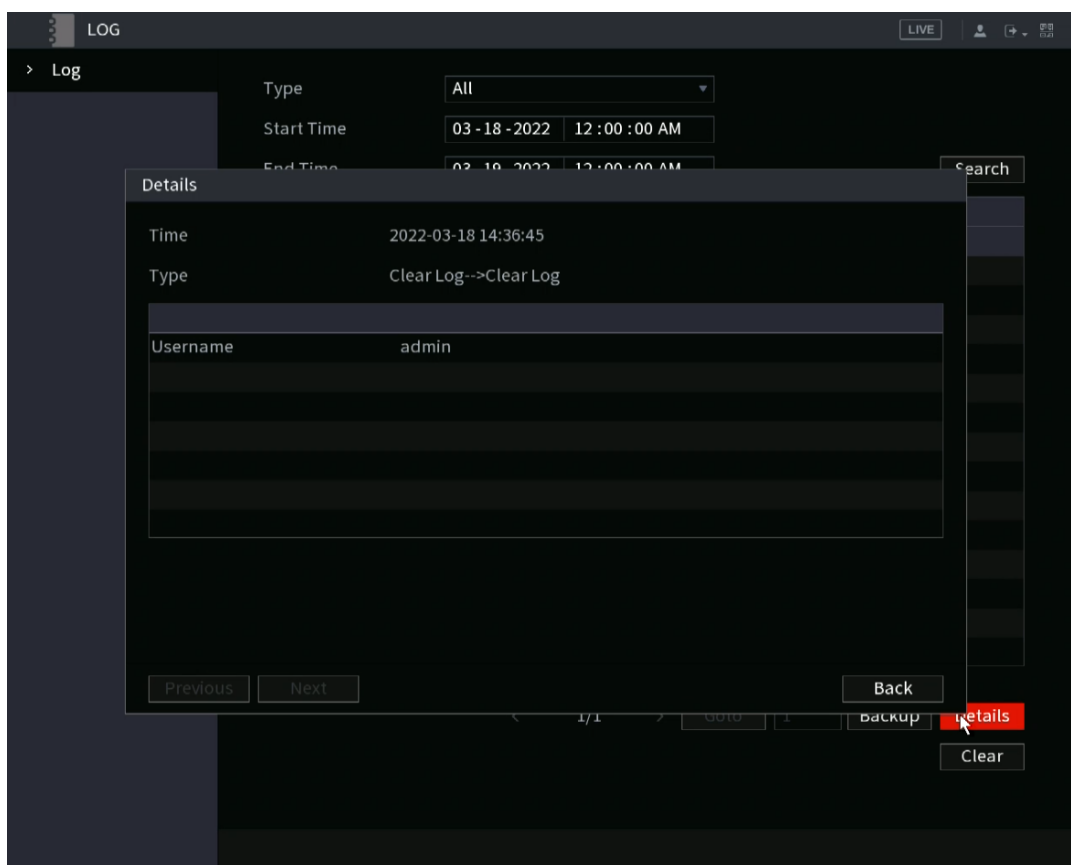
- Click **Backup** to back up the logs into the USB storage device.
- Click **Clear** to remove all logs.

4.9.2 System
4.9.2.1 System Version

Select **Main Menu** > **Info** > **System Info** > **Version**.

You can view the NVR version information such as Serial number and firmware version. Slight differences may be found in the actual user interface.

4.9.2.2 HDD Info

The HDD Info section allows you to view the HDD quantity, HDD type, total space, free space, status, and S.M.A.R.T information.

Select **Main Menu** > **Info** > **System Info** > **Disk**, the **Disk** interface will be displayed. See Figure 4-201. Refer to Table 4-60 for detailed information.

Figure 4-201
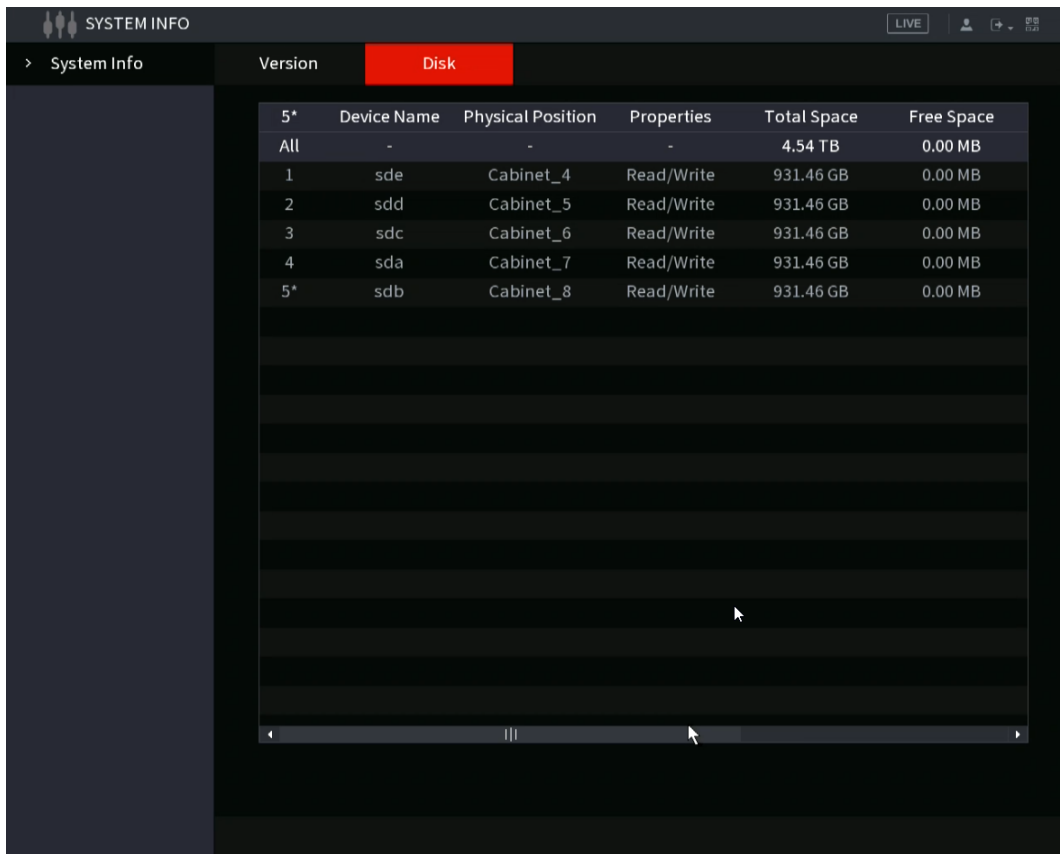
Table 4-60

Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) indicates the current working HDD.
Device Name	Name of HDD.
Physical Position	Installation position of HDD on the motherboard.
Properties	HDD type.
Total Space	Total capacity of HDD.
Free Space	Usable capacity of HDD.
Health Status	Health status of the HDD.
S.M.A.R.T	View the HDD S.M.A.R.T reports.
Status	Status of the HDD to show if it is working normally.

4.9.2.3 BPS

The BPS section allows you to view the current video bit rate (kb/s) and resolution of the connected devices.
Select **Main Menu** > **Info** > **BPS**, the BPS interface will be displayed. See Figure 4-202.

Figure 4-202

4.9.3 Network

4.9.3.1 Online User

You can view the online user information or block any online user for a period of time. To block
an online user, click ![icon] and then enter the time that you want to block this user. The maximum
value you can set is 65535.
The NVR checks every 5 seconds to check whether there is any user added or deleted, and
update the user list accordingly.
Select **Main Menu** > **Info**> **Network** > **Online User**, the **Online User** interface will be
displayed. See Figure 4-205.

Figure 4-205
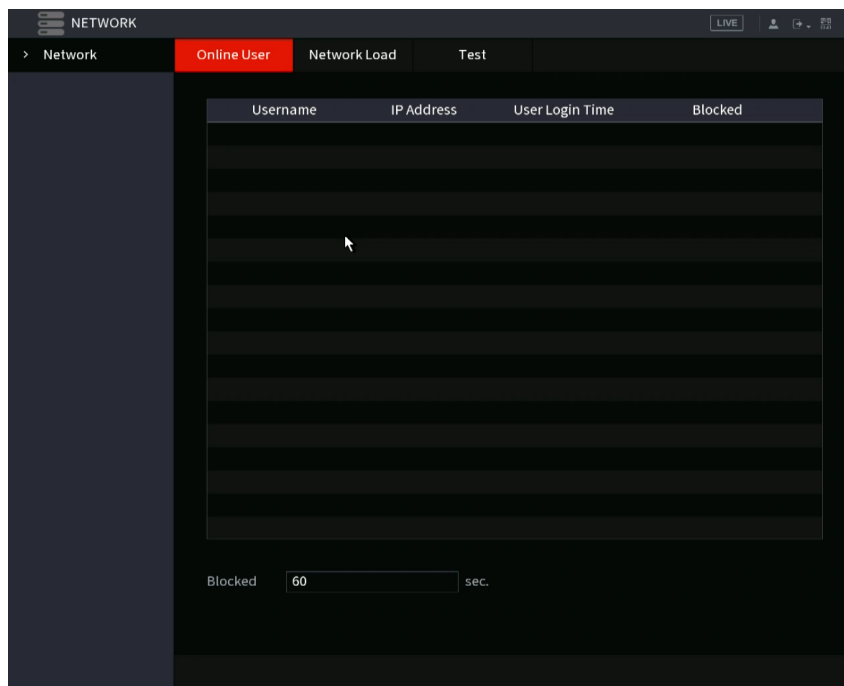
4.9.3.2 Network Load

This section allows you to view the data flow such as data receiving speed and sending speed.
Viewing this information will help you to measure the transmission capability of your system.

Step 1　Select **Main Menu** > **Info** > **Network** > **Network Load**. The
　　　　Network Load interface will be displayed. See Figure 4-206.

Figure 4-206
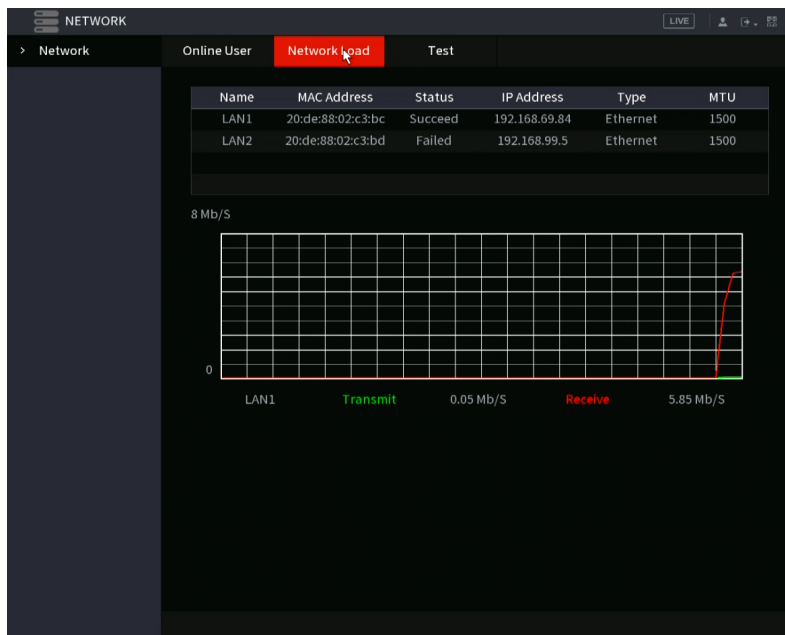
Step 2　Click the LAN (Network port) name that you want to view, for example, **LAN1**.
　　　　The NVR will display the data sending speed and receiving speed information.

　　　　● NVR will display LAN1 load by default.
　　　　● Only one LAN load can be displayed at one time.

4.9.3.3 Network Test

You can test the network connection status between the NVR and other devices.

Step 1 Select **Main Menu** > **Info** > **Network** > **Test**.
The **Test** interface will be displayed. See Figure 4-207.

Figure 4-207
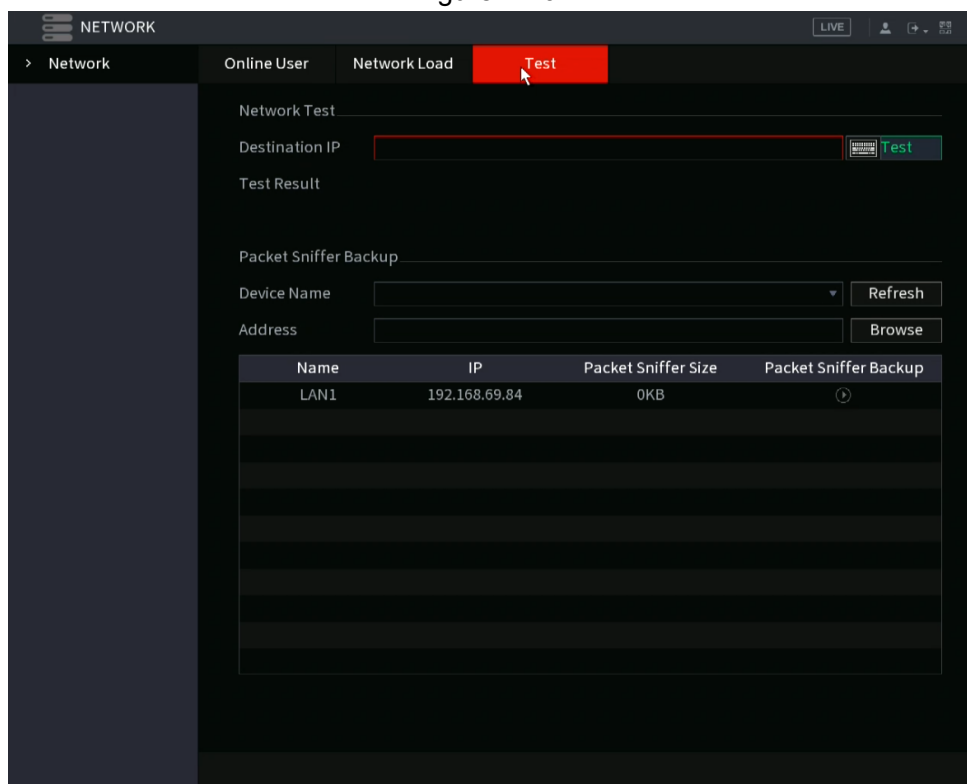
Step 2 In the **Destination IP** box, enter the IP address.
Step 3 Click **Test**.
After testing is completed, the test result will display information for the average delay, packet loss, and network status.

4.9.4 Maintenance and Management

4.9.4.1 Device Maintenance

You can can configure the auto reboot for periodical maintenance of the NVR. It is recommended to reboot at least once a week. You can also configure the case fan mode to reduce noise and extend the service life.

Step 1 Select **Main Menu** > **Advanced Settings** > **System Operation** > **Maintenance** > **Scheduled Maintenance**.
The **Maintenance** interface will be displayed. See Figure 4-208.

Figure 4-208
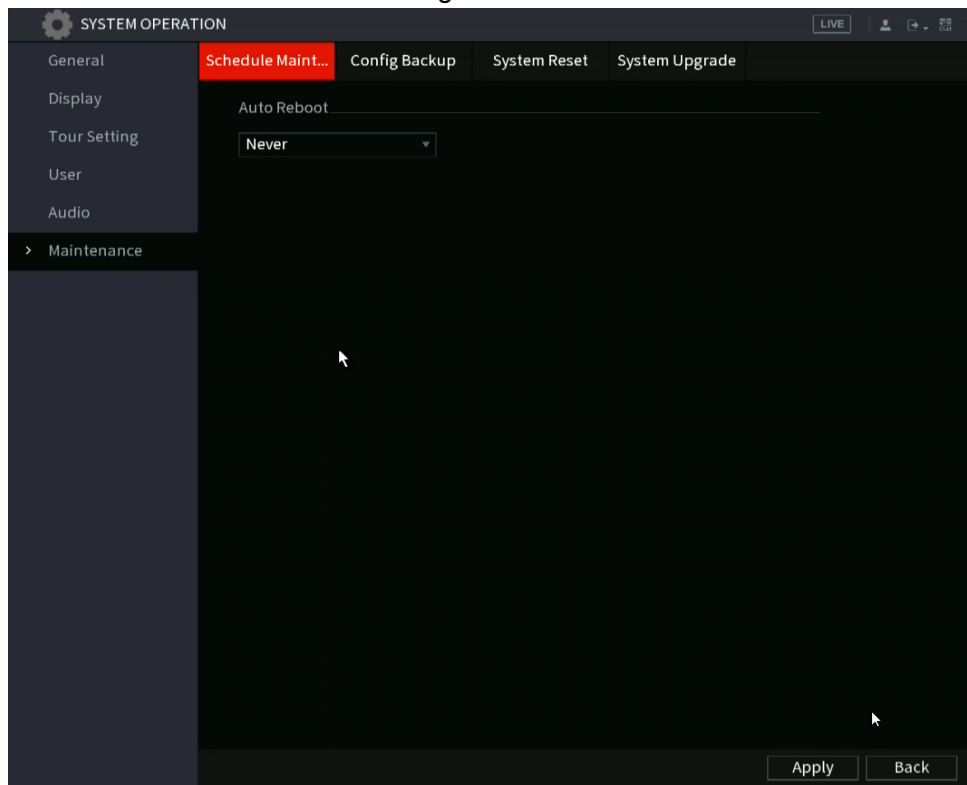
Step 2   Configure the settings for the NVR maintenance parameters. See Table 4-61.

Table 4-61

Parameter	Description
Auto Reboot	Select the reboot options: Never, Every day, or a specified day of the week. You can also select the time for a reboot.
Case Fan Mode	Select fan behavior options. Selections include: **Always run** or **Auto**. If you select **Auto**, the case fan will stop or start according to conditions such as the Device temperature. 📖 Not all NVR models support this feature, and it is only supported on the local configuration interface.

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

4.9.4.2 Exporting System Settings

You can export or import the Device system settings if there are several devices that require the same setup or to create a backup if experimenting with settings.

📖
● The **Import/Export** interface cannot be opened if the backup operation is ongoing on the other interfaces.
● When opening the **Import/Export** interface, the NVR will refresh its device list and set the current directory as the first root directory.
● Click **Format** to format the USB storage device.

Step 1 Select **Main Menu** > **Advanced Settings** > **System Operation** > **Maintenance >
Config Backup**.

The **Import/Export** interface will be displayed. See Figure 4-209.

Figure 4-209
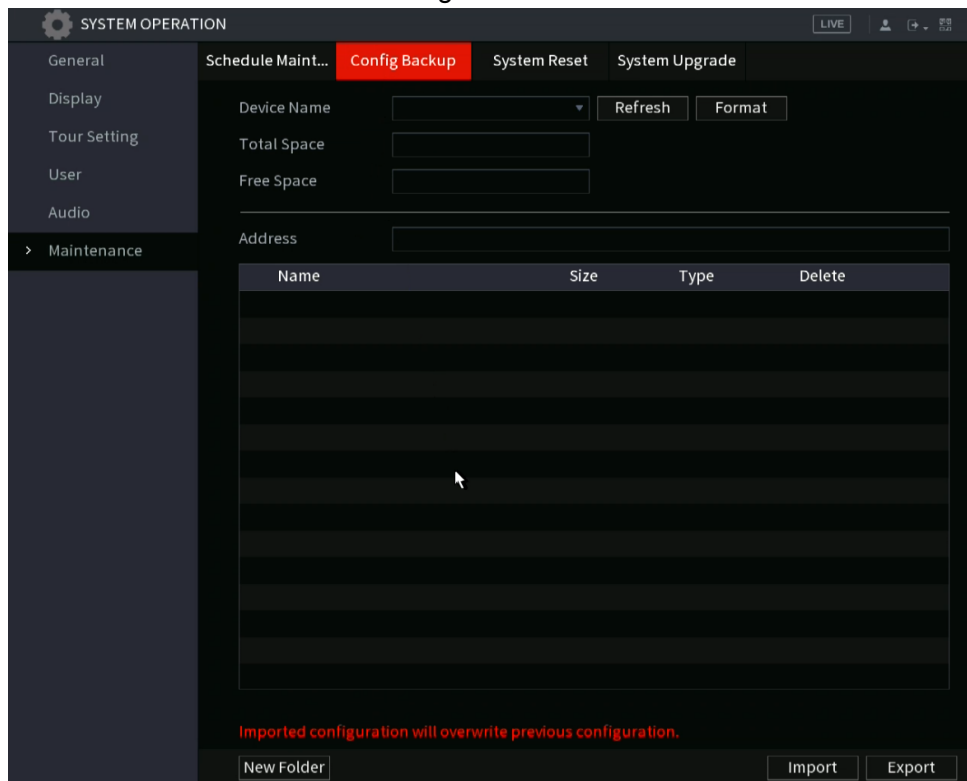
Step 2 Insert a USB storage device into one of the USB ports on the NVR.

Step 3 Click **Refresh** to refresh the interface.

The connected USB storage device information will be displayed. See Figure 4-210.

Figure 4-210
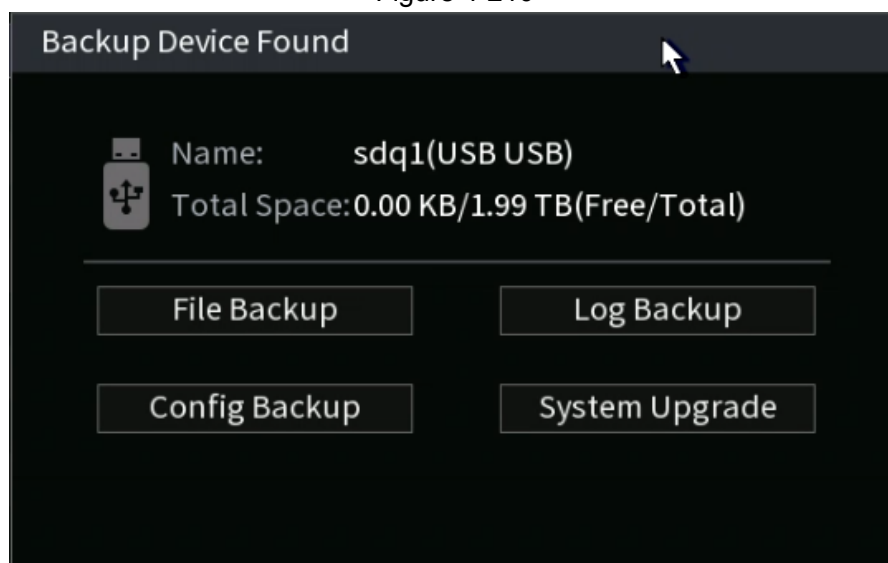
Step 4 Click **Export**.

The backup file will be created under a folder: "Config_[YYYYMMDDhhmmss]".

Double-click this folder to view the backup files.

4.9.4.3 Default

📖

This section allows you to select the settings that you want to restore to the factory default.

Step 1　Select **Main Menu** > **Advanced Settings > System Operation**> **Maintenance** > **System Reset**.

The **Default** interface will be displayed. See Figure 4-211.

Figure 4-211
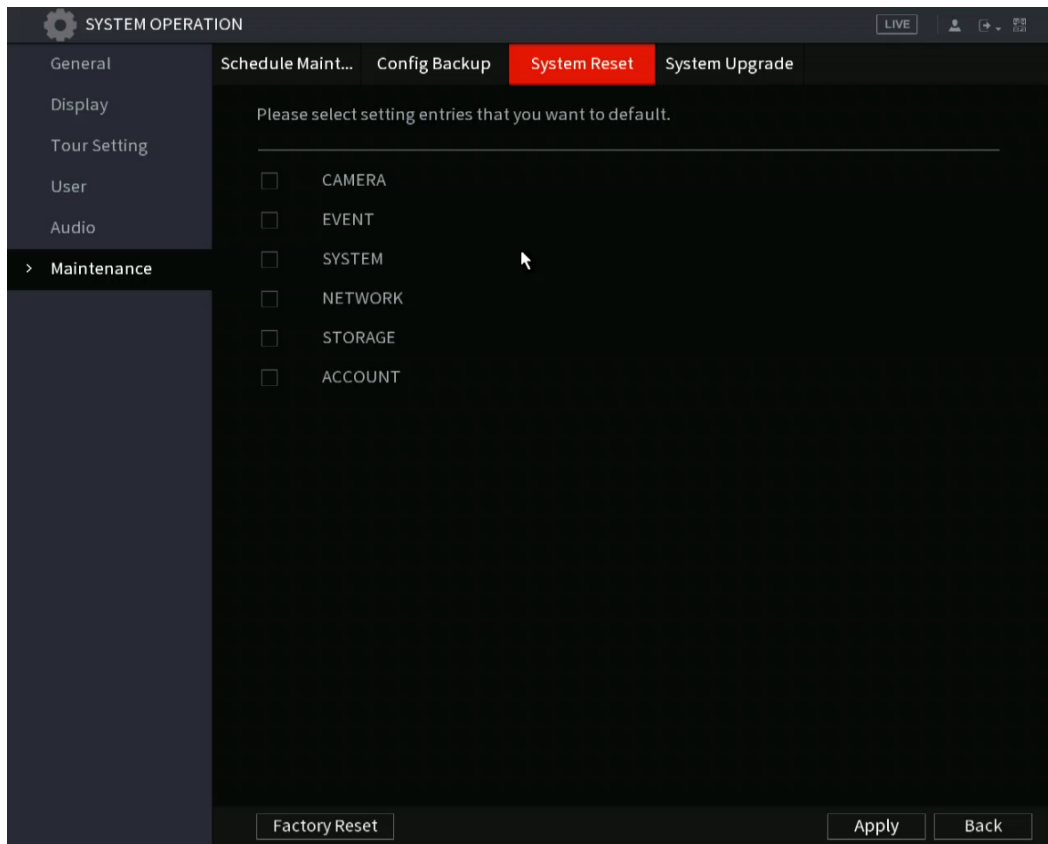
Step 2　Select the sections you want to default.
- Click **Default**, and then click **OK** in the prompted dialog box. The NVR will restore the selected settings.
- Click **Factory Default**, and then click **OK** in the prompted dialog box.
  1. Enter the admin password in the second dialog box.
  2. Click **OK**.
  The NVR will restore the factory settings.

4.9.4.4 System Update

4.9.4.4.1 Upgrading NVR Firmware

Step 1   Insert a USB storage device containing the upgrade files into the USB port of the
Device.

Step 2   Select **Main Menu** > **Advanced** > **System Operation** > **Maintenance** > **System Update**
The **Update** interface will be displayed. See Figure 4-212.

Figure 4-212
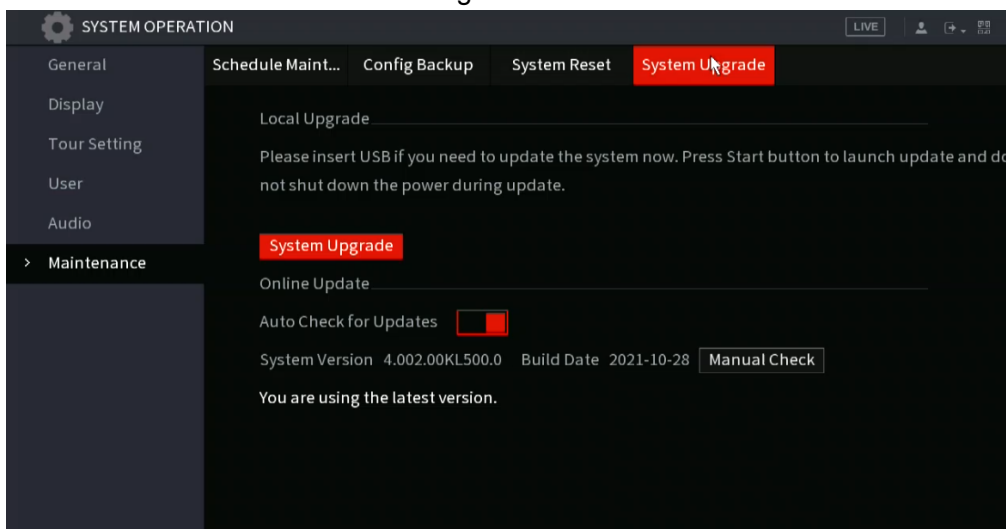
Step 3   Click **Update**.
The **Update** interface will be displayed. See Figure 4-213.

Figure 4-213
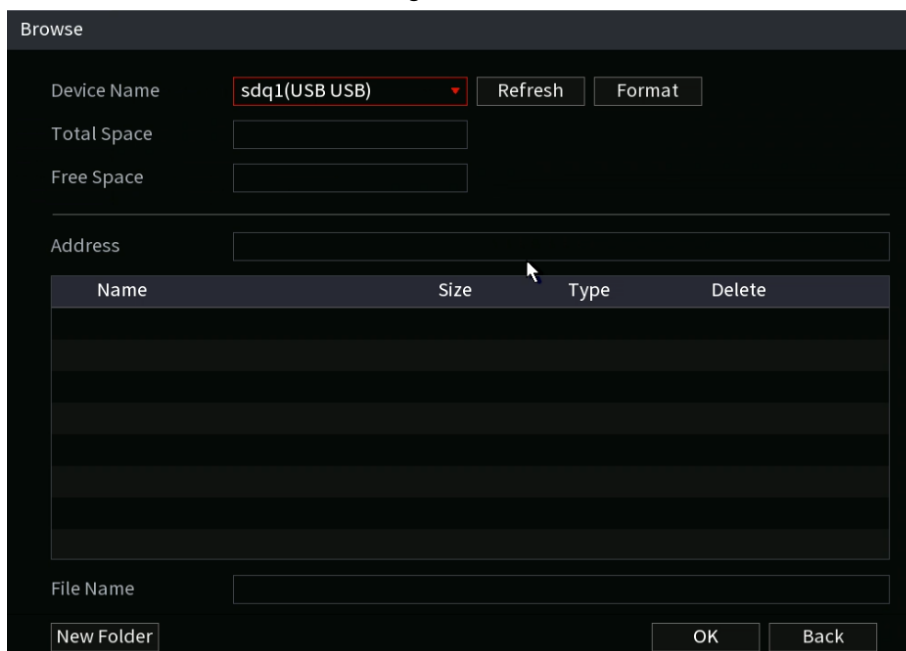
Step 4   Click the appropriate upgrade file.

Step 5   The selected file will be displayed in the **File Name** field.

Step 6   Click **Update**.

4.10 File Backup

This section allows you to backup recorded files to a USB device connected to the NVR.

Step 1   Connect a USB storage device to the NVR. (Flash drives are recommended)

Step 2   Select **Main Menu** > **Playback > BACKUP**, the **Backup** interface will be displayed.

Figure 4-215
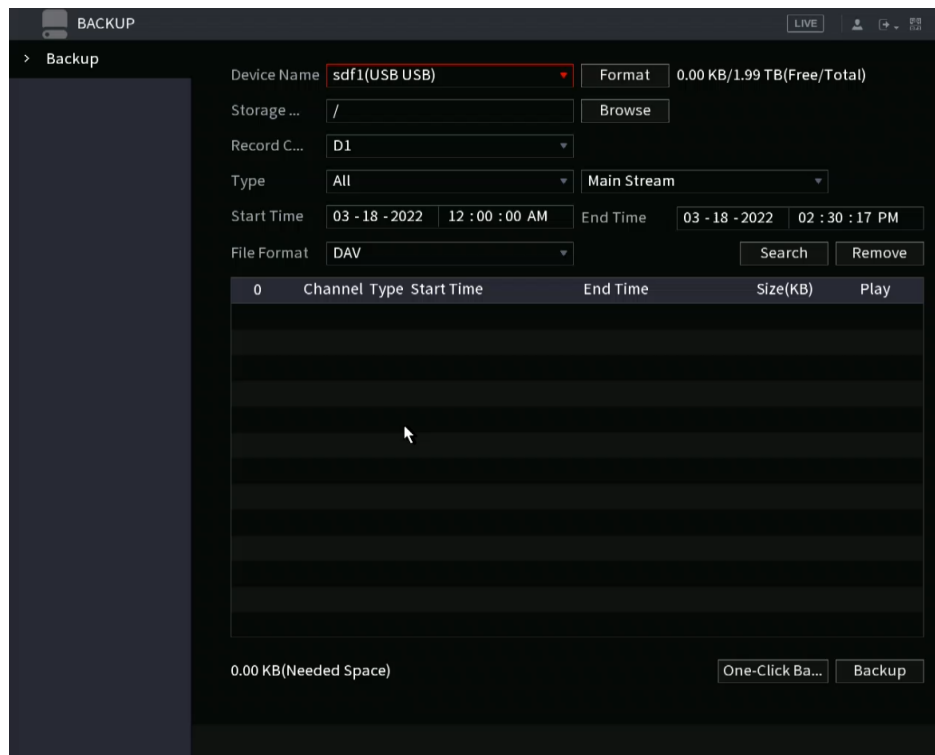
Step 3   Select the backup device and then select the desired channel, file start time, and end time.

Step 4   Click **Search**, the NVR will begin the search. All matched files will be listed below. The NVR will calculate the capacity needed and remaining in the USB.

Step 5   The NVR will backup files with a √ before channel name. You can use Fn or cancel button to remove the √.

Step 6   Click the backup button to backup the selected files. A process bar will populate.

Step 7   When the NVR completes backup, the dialogue box will prompt a successful backup.

📖

● The NVR will populate a corresponding dialogue box if there is no backup device, no backup file, or if an error occurs during the backup process.

- The file name format is typically: Channel number+Record type+Time. In the file name, the YDM format is Y+M+D+H+M+S.
- The default file extension is .dav.
- Click **One-Click Backup** to back up all required files.

4.11 Network

This section covers the network configuration options on the NVR.

4.11.1 TCP/IP

Select **Main Menu** > **Basic Settings** > **NETWORK** > **TCP/IP**, the **TCP/IP** interface will be displayed. See Figure 4-216.

Figure 4-216
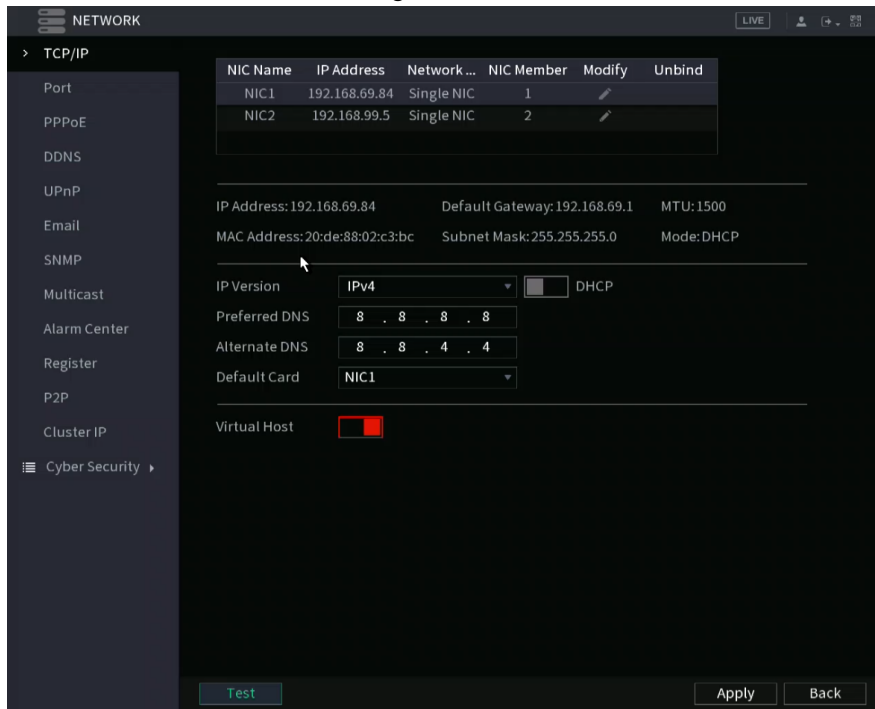
Table 4-62

Parameter	Description
Net Mode	● **Multi-address**: The wwo Ethernet ports work separately through either of which you can request the Device to provide the services such as HTTP and RTSP. You will need to configure a default Ethernet port (usually the Ethernet port 1 by default) to the local network (if this is the case, the second Ethernet port will be configured for the IP camera IP scheme. If one of the two Ethernet ports is disconnected as detected by the NVR network monitor, the system network status is regarded as offline. ● **Fault Tolerance**: The two Ethernet ports share one IP address. Normally, only one Ethernet port is working and when this port fails, the other port will start working automatically to ensure a constant network connection. ● When both of the two Ethernet ports are disconnected, the NVR network monitor will regard this as offline. The two Ethernet ports are used under the same LAN. ● **Load Balance**: The two network cards share one IP address and they are working at the same time to share the average network load. 📖 The Device with a single Ethernet port does not support this function.
Default Ethernet Port	In the **Ethernet Card** list, select an Ethernet port as a default port. This is typically the port going to the local network. This setting is available only when the **Multi-address** is selected in the **Net Mode** list.
IP Version	In the IP Version list, you can select IPv4 or IPv6. Both versions are supported for access.
MAC Address	Displays the MAC address of the Device.

Parameter	Description
DHCP	Enables the DHCP function. The IP address, subnet mask and default gateway are not available for configuration once DHCP is enabled. ● If DHCP is successful, the obtained information will display in the **IP Address** box, **Subnet Mask** box and **Default Gateway** box. If not, all values show 0.0.0.0. ● If you want manually configure the IP information, disable the DHCP function. ● If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway.
Subnet Mask	
Default Gateway	📖 IP address and default gateway must be in the same network segment.
DNS DHCP	Enable the DHCP function to get the DNS address from the router.
Preferred DNS	In the **Preferred DNS** box, enter the IP address of DNS.
Alternate DNS	In the **Alternate DNS** box, enter the IP address of alternate DNS.
MTU	In the **MTU** box, enter a value for network card. The value ranges from 1280 byte through 1500 byte. The default is 1500. The suggested MTU values are as below. ● 1500: The greatest value of the Ethernet information package. This value is typically selected if there is no PPPoE or VPN connection, and it is also the default value of some routers, network adapters, and switches. ● 1492: Optimized value for PPPoE. ● 1468: Optimized value for DHCP. ● 1450: Optimized value for VPN.
Test	Click this button to test if the entered IP address and gateway are valid.

4.11.2 Port

You can configure the maximum connections accessing the Device from Clients such as WEB, Software Platform, or Mobile Phone and configure each port settings.

Step 1   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **Port**.

The **Port** interface will be displayed. See Figure 4-217.

Figure 4-217
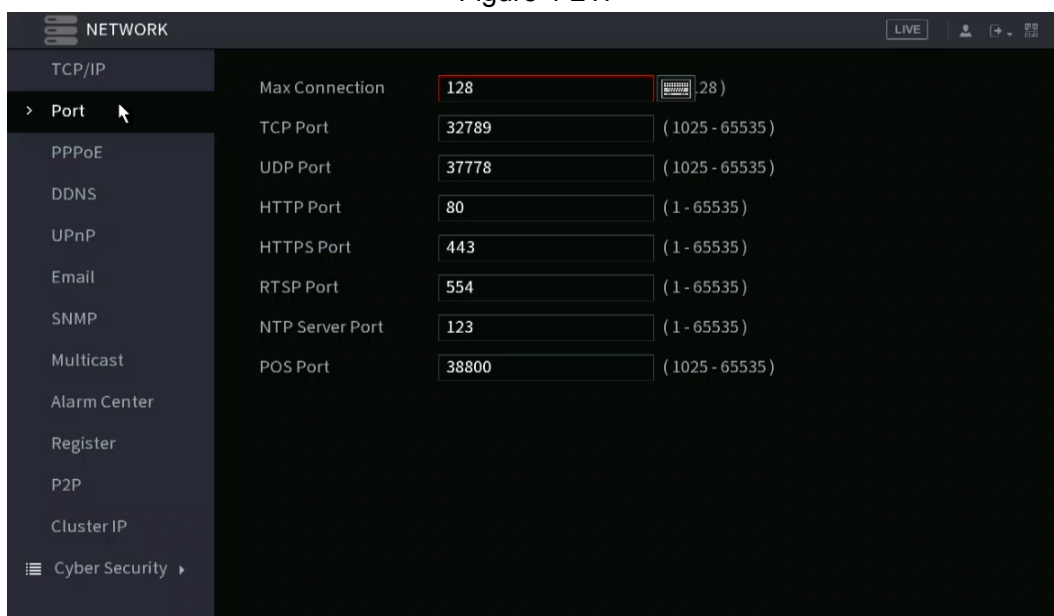
Step 2   Configure the settings for the connection parameters. See Table 4-63.

📖

The connection parameters except Max Connection cannot take effects until the Device has been restarted.

Table 4-63

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time. This includes Web GUI, Desktop Software Platform, and Mobile Devices.
	Select a value between 1 and 128. The default value setting is 128.
TCP Port	The default value setting is 37777. You can enter the value according to your actual situation.
UDP Port	The default value setting is 37778. You can enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation.
	If you enter another value, for example, 70, then you should enter :70 after the IP address when logging in to the Web GUI.
RTSP Port	The default value setting is 554.
HTTPS Enable	Enable **HTTPS**.
HTTPS Port	HTTPS communication port. The default value setting is 443. You can change the value as needed.

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

4.11.3 PPPoE

PPPoE is another way for the Device to access the network. You can establish a network connection by configuring PPPoE settings to give the NVR a dynamic WAN IP address. To use this function, you will need to obtain a user name and password from the Internet Service Provider the NVR will be utilizing.

Step 1   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **PPPoE**.

The **PPPoE** interface will be displayed. See Figure 4-225.

Figure 4-225
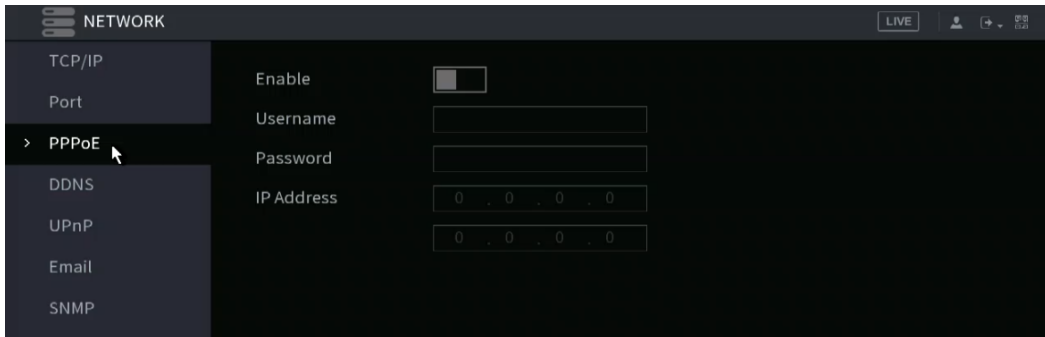
Step 2   Enable the PPPoE function.

Step 3   In the **User Name** box and **Password** box, enter the user name and password provided by the Internet Service Provider.

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

The system will populate a message to indicate the settings have been successfully saved. The IP address will appear on the PPPoE interface. You can use this IP address to access the Device.

If the PPPoE function is enabled, the IP address on the **TCP/IP** interface cannot be modified.

4.11.4 DDNS

If the WAN IP the NVR is utilizing is Dynamic (Frequently changes), the DDNS function can dynamically refresh the correspondence between the domain name on the DNS and the IP address, ensuring remote access to the NVR by using the domain name. This function is typically used when port forwarding for remote access and not P2P.

Background Information

IC Realtime devices come with a built-in ICDDNS registration for your convenience. If you select other DDNS services, you will need to login to the respective web site for the DDNS service for additional configuration.

After you have registered and logged in the DDNS website successfully, you can view the information of all the connected devices under this user name.

Step 1   Select **Main Menu** > **Advanced Settings > NETWORK** > **DDNS**.

The **DDNS** interface will be displayed. See Figure 4-226.

Figure 4-226
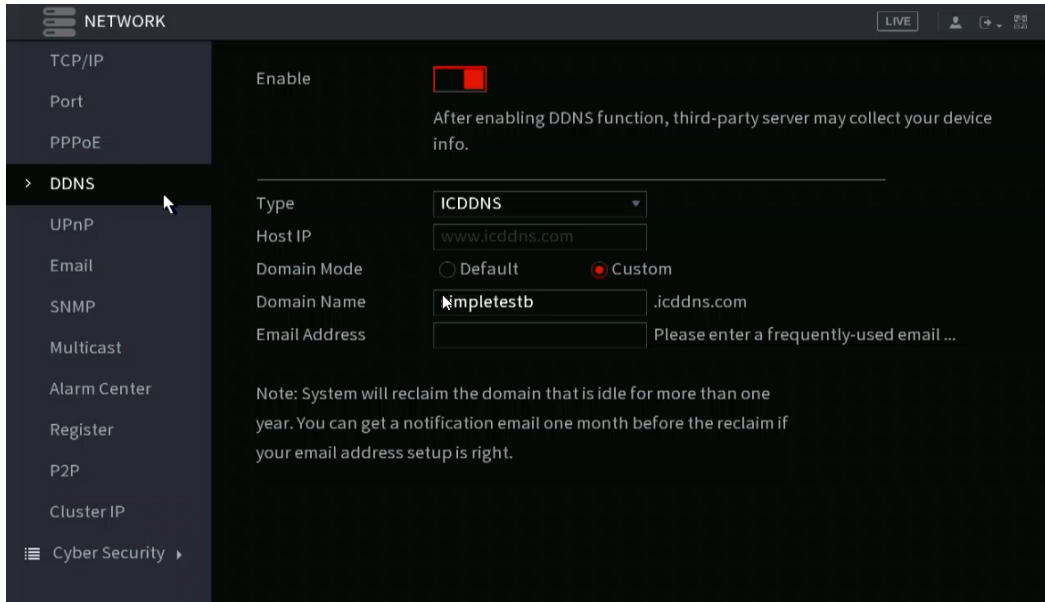
Step 2   Configure the settings for the DDNS parameters. See Table 4-68.

Table 4-68

Parameter	Description
Enable	Enable the DDNS function. 📖 After enabling DDNS function, third-parties may collect your Device information.
Type	Type and address of DDNS service provider.
Server Address	● Type: ICDDNS; address: https://www.icddns.com/ ● Type: NO-IP DDNS; address: dynupdate.no-ip.com ● Type: Dyndns DDNS; address: members.dyndns.org
Domain Name	The domain name for registering on the website of DDNS service provider.
User Name	Enter the user name and password obtained from DDNS service provider. you will need to register (including user name and password) on the website of DDNS service provider.
Password	
Interval	The DDNS service will refresh in the specified time

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

Enter the domain name in the browser on your PC, and then press **Enter**.

If the web interface of the NVR will be displayed, the configuration is successful. If not, the configuration is failed. Note: This will only work if accessing offsite or NAT loopback is enabled on the local network of the NVR.

4.11.5 UPnP

This function allows communication between the NVR and the router to enable port mapping and forwarding. You will need to have a UPnP-enabled router for this configuration.

4.11.5.1 Configuring the Router

You may need to refer to your router's manual or contact the ISP regarding any information on configuring your router.

Step 1   Log in to the router using a web browser. On most residential routers, type in the default gateway IP in the address bar and press enter.

Step 2   Enable the UPnP function on the router.

Step 3   Connect the Device with the LAN port on the router to connect into the LAN.

Step 4   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **TCP/IP**, configure the IP address into the router IP address range, or enable the DHCP function to obtain an IP address automatically.

4.11.5.2 Configuration UPnP

Step 1   Select **Main Menu** > **NETWORK** > **UPnP**.

The **UPnP** interface will be displayed. See Figure 4-227.

Figure 4-227
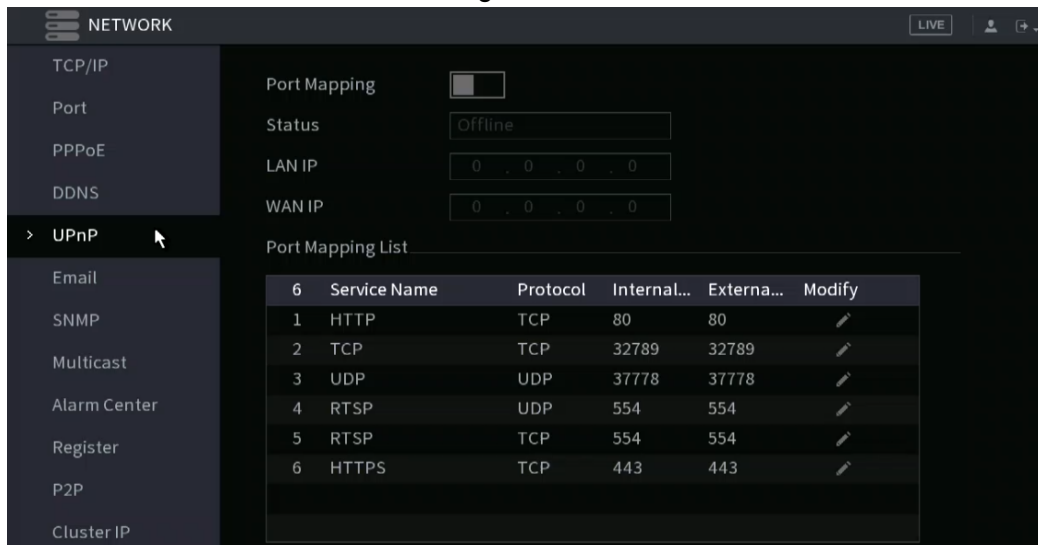
Step 2   Configure the settings for the UPnP parameters. See Table 4-69.

<div align="center">Table 4-69</div>

Parameter	Description
Port Mapping	Enable the UPnP function.
Status	Indicates the status of UPnP function. ● Offline: Failed. ● Online: Succeeded.
LAN IP	Enter the IP address of the router on the LAN. 📖 After mapping has succeeded, the system will obtain the IP address automatically.
WAN IP	Enter IP address of router on the WAN. 📖 After mapping has succeeded, the system obtains IP address automatically
Port Mapping List	The settings in the port mapping list correspond to the UPnP port mapping list on the router. ● Service Name: Name of the network server. ● Protocol: Type of protocol. ● Internal Port: Internal port that is mapped on the Device. ● External Port: External port that is mapped on the router. 📖 ● To avoid port conflict, when setting the external port, try to use the ports from 1024 through 5000 and avoid popular ports from 1 through 255 and system ports from 256 through 1023. ● When establishing a mapping configuration, ensure the mapping ports are not occupied or limited. ● The internal and external ports of TCP and UDP must be the same and cannot be modified. ● Click the pencil icon to modify the external port.

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

4.11.6 Email

This section allows the NVR (Sender) to send emails to a set of defined receivers. This must be set up correctly in order to use "Send Email" functions on events such as iMD, Motion Detection or any other event.

Step 1   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **Email/ SMTP**.
The **Email** interface will be displayed. See Figure 4-229.

Figure 4-229
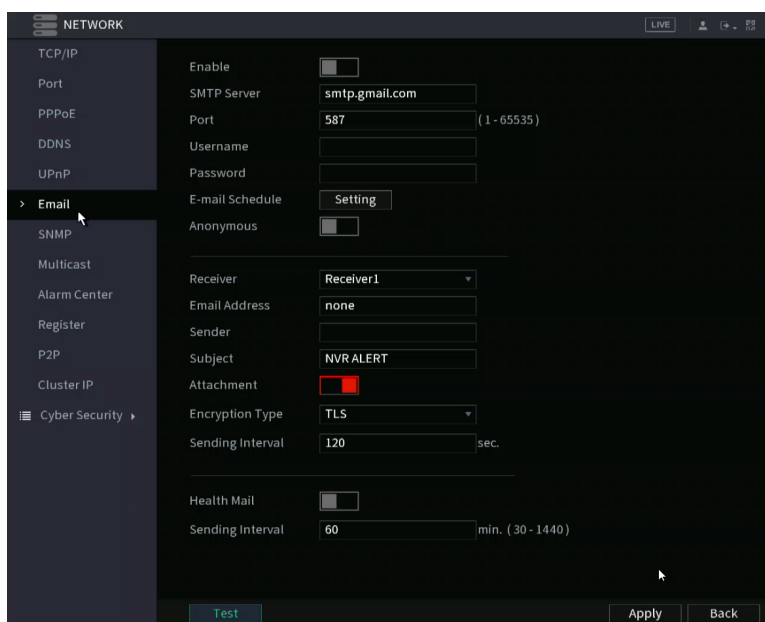
Step 2   Configure the settings for the email parameters. See Table 4-70.

Table 4-70

Parameter	Description
Enable	Enables the email function.
SMTP Server	Enter the SMTP server address of the sender's email account.
Port	Enter the port value of SMTP server. Input 587 for TLS or 425 if using SSL.
Anonymous	Allows anonymous login.
Username	Enter the username and password of the sender's email account.
Password	
Sender	Enter the sender's email address.
Encryption Type	Select the encryption type: **NONE**, **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.
Subject	Enter the subject name for the Email
Receiver	In the **Receiver** list, add the email of a receiver that you want to receive the notification, then press the "+" icon to add. The Device supports up to three receivers. if using Email to SMS, contact the appropriate mobile providers to acquire the Email to SMS format.
Attachment	This will need to be enabled if sending snapshots via email notification.
Encryption Type	Select the encryption type: **NONE**, **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.

Parameter	Description
Interval (Sec.)	The NVR will not send emails caused by frequent alarm events of the same type within the interval time The value ranges from 0 to 3600. Select 0 disable interval.
Health Mail	The NVR can send a test email to check the connection at the specified Inteval.
Sending Interval	This is the interval that the system sends a health test email. The value ranges from 30 to 1440. 0 means that there is no interval.
Test	Click **Test** to test the email sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click **Apply** to save the settings.

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

4.11.7 SNMP

SNAMP allows the NVR to be managed by a database such as a MIB. Once configured, you can utlize software such as MIB Builder and MG-SOFT MIB Browser to manage and control the NVR from the software.

Prerequisites

● Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser

● Obtain the MIB files that correspond to the current version from the technical support.

This function is not supported in all NVR models.

Procedure

Step 1   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **SNMP**.
The SNMP interface will be displayed. See Figure 4-230.

Figure 4-230
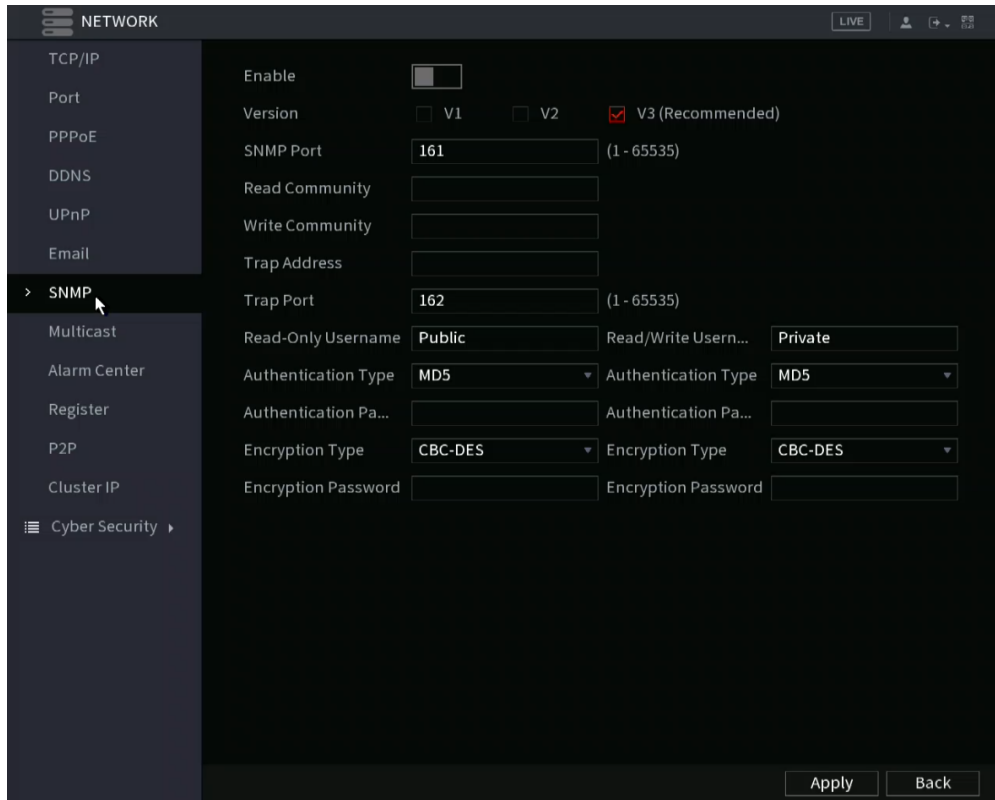
Step 2   Configure the settings for the SNMP parameters. See Table 4-71.

Table 4-71

Parameter	Description
Enable	Enable the SNMP function.
Version	Select the check box of SNMP version(s) that you are using. The default version is **V3**. There may be a security risk if selecting V1 or V2.
SNMP Port	Indicates the monitoring port on the agent program.
Read Community	Indicates the read/write strings supported by the agent program.
Write Community	
Trap Address	Indicates the destination address for the agent program to send the Trap information.
Trap Port	Indicates the destination port for the agent program to send the Trap information.
Read-Only Username	Enter the user name that is allowed to access the Device and has the "Read Only" permission.
Read/Write Username	Enter the user name that is allowed to access the Device and has the "Read and Write" permission.
Authentication Type	Includes MD5 and SHA. The system will recognize automatically.
Authentication Password/ Encryption Password	Enter the password for authentication type and encryption type. The password should be no less than eight characters.

217

Parameter	Description
Encryption Type	In the **Encryption Type** list, select an encryption type. The default setting is CBC-DES.

Step 3　Compile the two MIB files by MIB Builder.

Step 4　Run MG-SOFT MIB Browser to load in the module from the compilation.

Step 5　On the MG-SOFT MIB Browser, enter the Device IP that you want to manage, then select the version number to query.

Step 6　On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

4.11.8 Multicast

This allows you to view the NVR if the connected users have exceeded the limit. Multicast enables information (in this case, video streams and such) to be sent to multiple receivers at the same time.

Step 1　Select **Main Menu** > **Advanced Settings** > **NETWORK** > **Multicast**.
The **MULTICAST** interface will be displayed. See Figure 4-231.

Figure 4-231
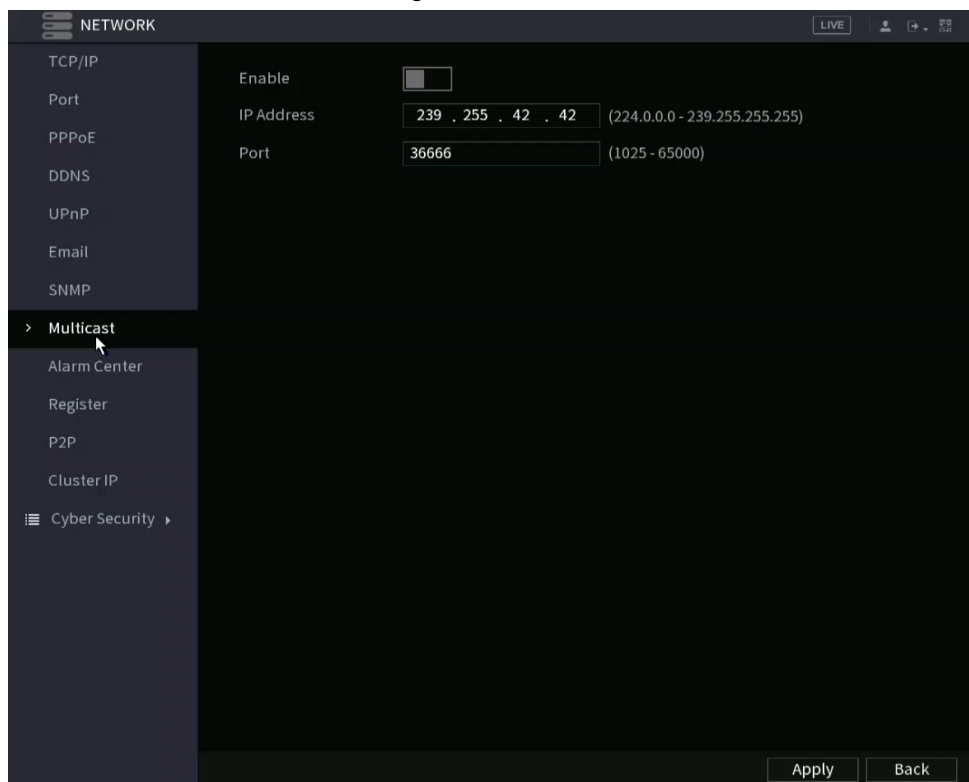
Step 2　Configure the settings for the multicast parameters. See Table 4-72.

Table 4-72

Parameter	Description
Enable	Enables the multicast function.
IP Address	Enter the IP address that you want to use as the multicast IP. The IP address ranges from 224.0.0.0 through 239.255.255.255.
Port	Enter the port for the multicast. The port ranges from 1025 through 65000.

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

You can use the multicast IP address to login to the web GUI.

On the web login dialog box, in the **Type** list, select **MULTICAST**. The web will automatically obtain the multicast IP address and join. You can then view the video through the multicast function.

4.11.9 Alarm Center

You can configure the alarm center server to receive the uploaded alarm information. To use this function, the **Alarm Upload** check box must be selected.

Step 1   Select **Main Menu** > **NETWORK** > **Alarm Center**.

The **Alarm Center** interface will be displayed. See Figure 4-232.

Figure 4-232
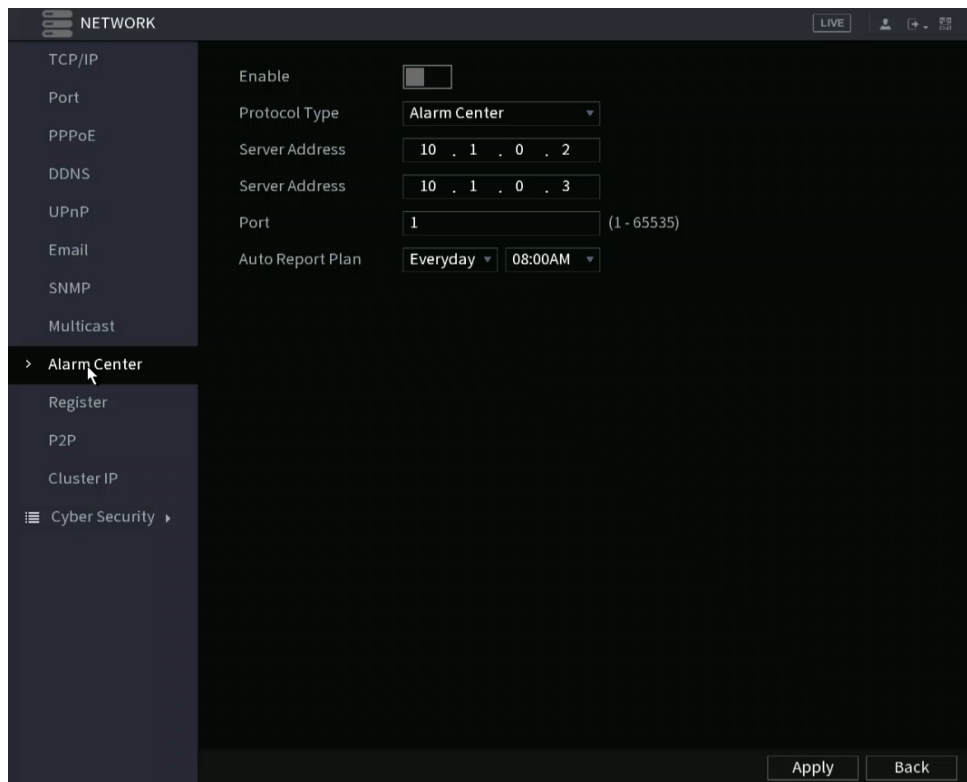
Step 2   Configure the settings for the alarm center parameters. See Table 4-73.

Table 4-73

Parameter	Description
Enable	Enable the alarm center function.
Protocol Type	In the **Protocol Type** list, select protocol type. The default is **Alarm Center**.
Host IP	The IP address and communication port of the PC installed with alarm client.
Port	
Auto Report Plan	In the **Auto Report Plan** list, select time cycle and specific time for uploading alarm.

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

4.12.6 Register

This function allows you to register the NVR into a specified proxy server which acts as the transit to make it easier for the client software to access the NVR.

Step 1   Select **Main Menu** > **Advanced Settings** > **NETWORK** > **Register**.
         The **Register** interface will be displayed. See Figure 4-233.

Figure 4-233
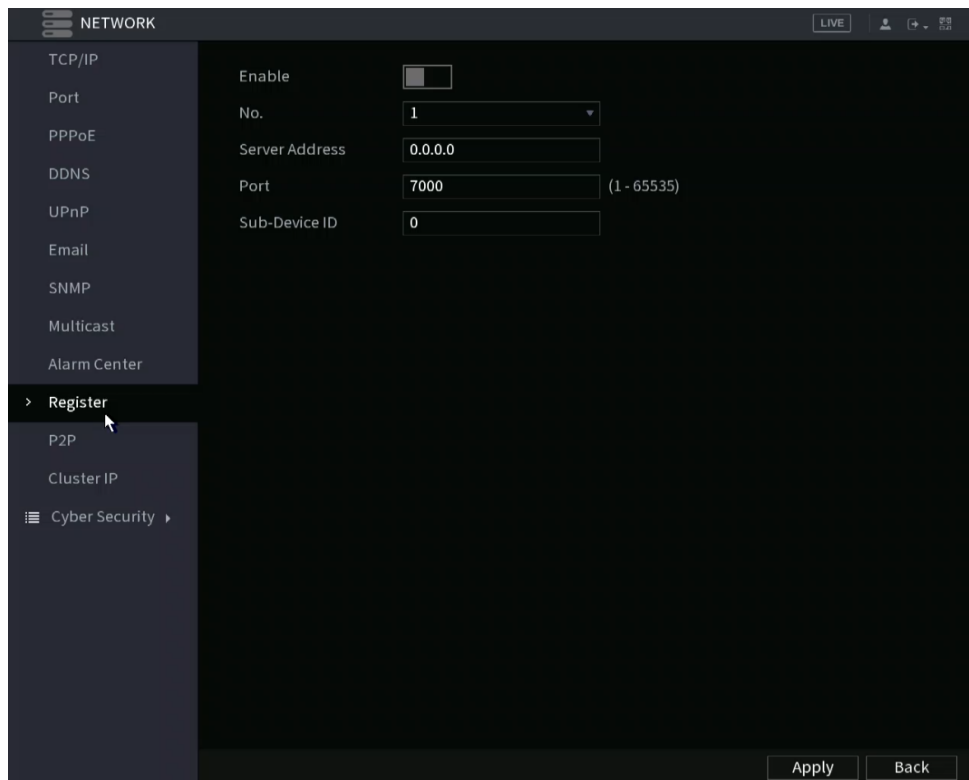
Step 2   Configure the settings for the register parameters. See Table 4-74.

Table 4-74

Function	Description
Enable	Enables the register function.
Server IP Address	Enter the server IP address or the server domain that you want to register to.
Port	Enter the port of the server.
Sub Service ID	This ID is allocated by the server and used for the Device.

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

4.11.11 Switch Setting

This manages the internal switch setting for NVRs with built-in PoE. You can change the IP scheme of the internal switch if necessary. The default IP scheme is 10.1.1.X. IP cameras plugged into the built-in POE will acquire this IP scheme if the cameras are set to DHCP.

- Only models with built-in PoE ports support this function.
- Do not connect the PoE port to a switch, as this can cause connection failures.
- This function is enabled by default, and the IP segment starts from 10.1.1.1, we recommend that you use the default setting.
- Third party IPCs are using the NVR built-in is not a supported configuration. If attempting this, your mileage may vary.

Step 1   Select **Main Menu** > **Advanced Settings** > **Network** > **Switch**.

Figure 4-234

Step 2   Set the values of **IP Address**, **Subnet Mask,** and **Default Gateway**.
Do not set the value of **IP Address** to the same local network segment as the NVR, we recommend that you use the default setting.

PoE Status	Description
Connect to PoE port	When an IPC is connected to the PoE port, the system automatically assigns the IP address to the IPC according to the set IP segment. The NVR will try the method of **arp ping** to assign the IP address. If DHCP is enabled on the NVR, the NVR will use DHCP to assign the IP address. ● When IP address is successfully set, the system will broadcast through the **Switch**. If there is a response from the IPC, it means the connection is successful, and the NVR will log in with the IPC. You can find the corresponding channel being occupied and there is a PoE icon at the upper-left corner. ● You can also view PoE status such as channel number and PoE port number in **Main Menu > Advanced Settings > Camera Configuration** > **Add/ Remove Device**
Disconnect PoE port	When an IPC is disconnected from PoE port, you will find the information of **Failed to find network host** on the **Live View** interface.
PoE connection mapping	The PoE ports are bound to corresponding channels. When an IPC is connected to PoE port 1, the corresponding channel is Channel 1.

4.11.12 P2P

P2P allows for easy remote access without having to configure the router. You will just need an internet connection to the NVR and the mobile app (IC View/ ICRSS Pro) or desktop software (Smart ICRSS) for remote viewing.

📖

Connect the NVR device to the Internet, otherwise, P2P will not function

Step 1 Select **Main Menu** > **Basic Settings** > **NETWORK** > **P2P**.

The **P2P** interface will be displayed. See Figure 4-235.

Figure 4-235
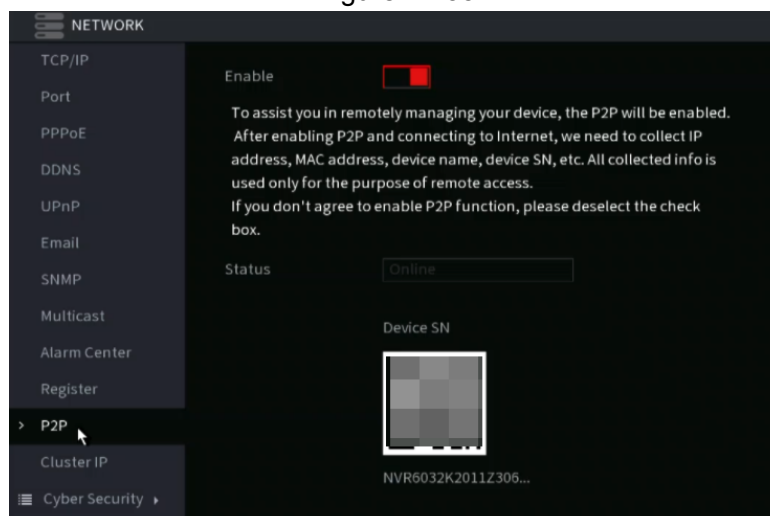
Step 2   Enable the P2P function. The Status section will indicate if the P2P connection is successful.

📖
After the P2P function is enabled and connected to the Internet, the system will collect your information for remote access. The information includes and is not limited to email address, MAC address, and device serial number.
You can now add the device.

- Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Mobile App (IC View/ ICRSS Pro), input the login information access the NVR.
- Desktop Software: Obtain the Device SN by scanning the QR code. Go to the Main Menu, then Devices. Click "+Add" and input the Device SN and login credentials. Click "Add" to save the settings and connect.

4.11.12.1 Adding to Mobile App

The following contents are introduced in the example of the mobile App.

Step 1 Navigate to your mobile device's store section, then download and install the mobile App (ICRSS Pro or IC View).

Step 2 Open the app and have the Serial number and login credential for your NVR ready.

Step 3   Register device in the mobile App:

1) Go to Home, then Devices section in the bottom of the app. See Figure 4-236.

Figure 4-236
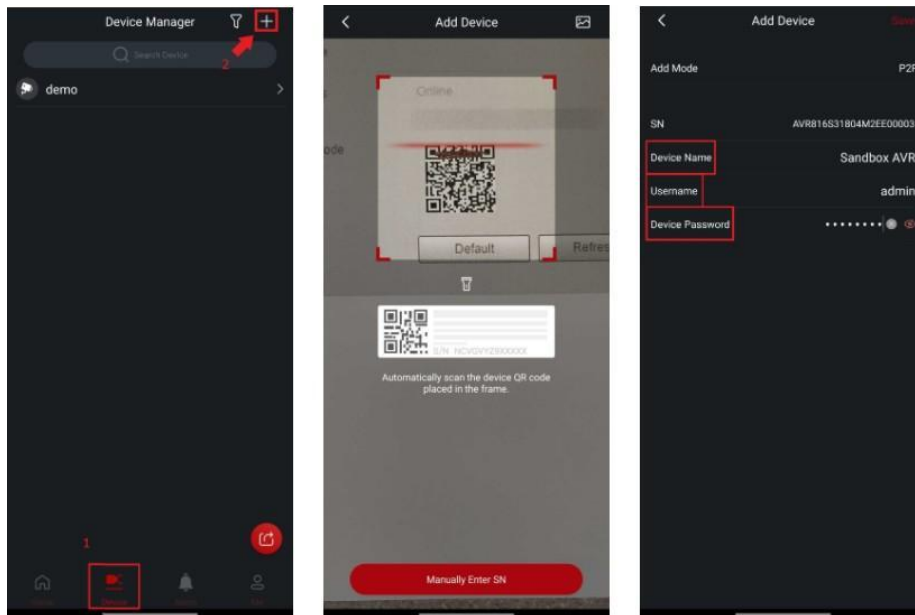
2) Click ➕ to enter the Add Device interface.

3) Select **P2P** to enter the P2P interface.

4) Scan the device label or scan the SN QR code got by selecting **Main Menu** > **Network** > **P2P**. When the scan is successful, the device SN will be displayed in the SN item.

5) Enter the user name and password for the NVR. If successful, you will be taken to the Live View screen and the cameras will display.

4.12 Storage

This section allows you to manage the storage resources (such as recorded files) and storage space.

4.12.1 File Management

You can set basic storage parameters.

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **File Management**. The Basic interface will be displayed. See Figure 4-237.

Figure 4-237

Step 2   Set parameters. See Table 4-76.

Table 4-76

Parameter	Description
Disk Full	This will allow you to select the NVR behavior when the recording disks are full. ● Select **Stop Record** to stop recording ● Select **Overwrite** to overwrite the recorded video files always from the earliest time. (This is the default setting)
Create Video Files	Configure the time length and file length for each recorded video in constant recording mode.
Delete Expired Files	Configures whether to delete the old files. To enable select the drop-down to "Custom" and input the number of days. The NVR will delete any files older than the specified days. The default setting is "Never". Deleted files cannot be recovered!

Step 3   Click **Apply** or **Save** to complete setup.

4.12.2 Schedule

You can set a schedule for recordings and snapshots. For detailed information, refer to "4.1.4.6.1 Recording Schedule" and "4.1.4.6.2 Snapshot Schedule".

4.12.3 Disk Manager

This section allows you to view and configure or format Hard Drives (HDD). You can view the current HDD type, status, capacity, etc. The operation includes format HDD, and change HDD property (read and write/read-only/redundancy).
To prevent files be overwritten in the future, you can set HDD as read-only.

Step 1 Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Manager**.
The **Disk Manager** interface will be displayed. See Figure 4-238.

Figure 4-238
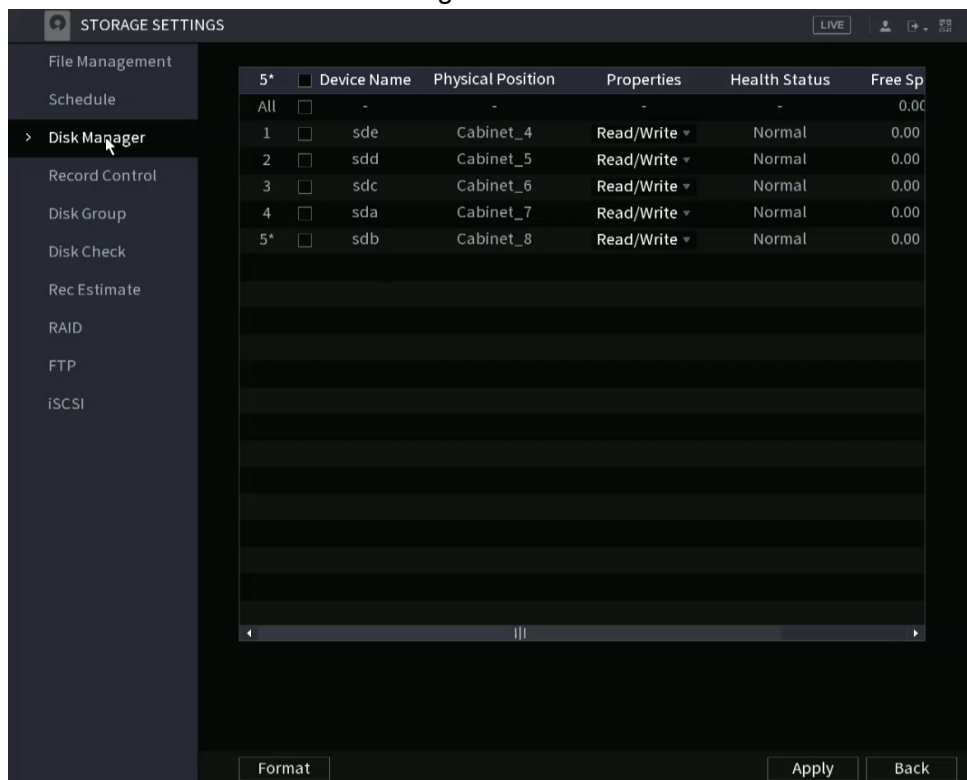
Step 2 Select a Hard Drive (HDD) and then select a time from the drop-down list.

Step 3 (Optional) Formatting a HDD:

  1) Select a HDD and then click **Format**.

  2) Click **OK**.

  3) Enter the admin password and click **OK**.

   📖

   ● This operation will erase all data in the HDD; proceed with caution.

   ● If xxx is selected, the database will also be formatted/ erased.

Step 4 Click **Apply** button to complete the setup. The NVR will restart to activate the current setup formatting a HDD.

4.12.4 Record Control

After setting the schedule for record or snapshot, make sure the recording stream (main by default) or the snapshot function is set to auto. This ensures the NVR will follow the set schedules accordingly. For detailed information, refer to "4.1.4.6.3 Record Control".

4.12.5 Disk Group

The installed HDD and any created RAIDs will default to Disk Group 1. You can set HDD group, and HDD group setup for the main stream, sub stream, and snapshot operation in this section as necessary.

📖
If **Disk Quota is selected** is shown on the interface, click **Switch to Disk Group mode.**

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Group**.
The **Disk Group** interface will be displayed. See Figure 4-239.

Figure 4-239
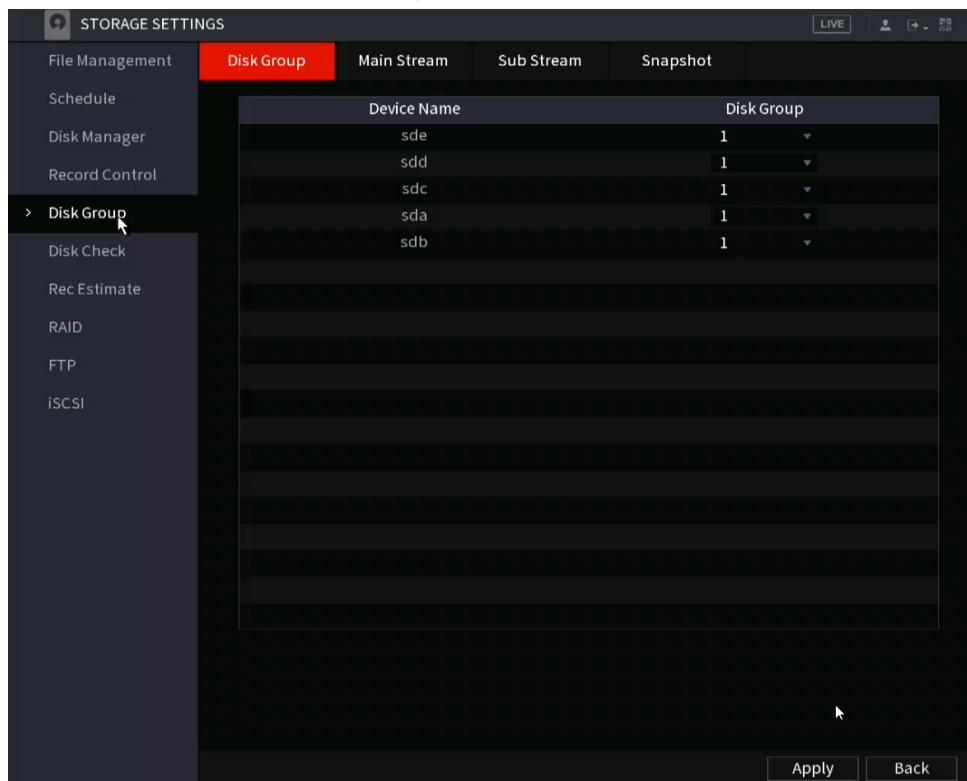
Step 2   Select the group for each HDD group and then click **Apply** to save the settings. After configuring HDD group, under the **Main Stream** tab, **Sub Stream** tab, and **Snapshot** tab, configure settings to save the main stream, sub stream, and snapshot to different HDD groups as necessary.

4.12.6 Disk Quota

The disk quota function helps to allocate a fixed storage capacity for each channel and

allocate the recording storage space for each channel. This feature is not available in all NVRs. This feature may be only accessible via web GUI.

📖

- If **Disk group mode selected.** is shown in the interface, click **Switch to Quota Mode.**
- Disk quota mode and disk group mode can not be selected at the same time.

Step 1　Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Quota**.

Figure 4-240

Step 2　Select a channel and set the values of record duration, bit rate and storage capacity of the pictures.

Step 3　Click **Apply**.

4.12.7 Disk Check

The HDD detect function detects the HDD current status for monitoring and identifies any malfunctioning HDDs to be replaced.

The two detect types are:

- Quick detect:　Detects via universal system files. If you want to use this function, make sure the target HDD currently in use. This allows for a quicker operation.
- Global detect adopts Windows mode to scan. This operation typically takes a long time and may affect the HDD that is recording.

4.13.7.1 Manual Check

Step 1　Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Check** > **Manual Check**. The **Manual Check** interface will be displayed. See Figure 4-241.

Figure 4-241
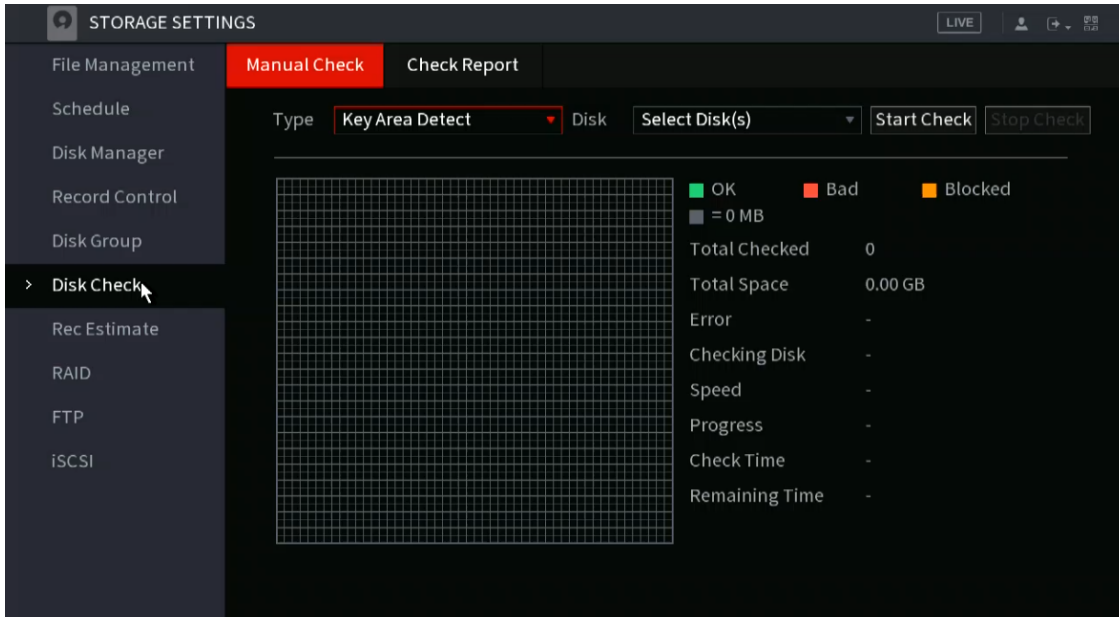
Step 2   In the **Type** list, select **Key Area Detect** or **Global Check**; and in the **Disk** list,
select the HDD that you want to detect.

Step 3   Click **Start Check**.
The system will start detecting the HDD and display the results when completed.

When the system is performing a disk check and you need to pause the
operation, click **Stop Check** to stop current detection. Click
Start Check to detect again.

4.13.7.2 Detect Report

After running a Disk check, you can view the results under the Detect Report section. Any failed
hard drives will be displayed in the reports and should be replaced if malfunctioning or defective.

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Check** > **Check Report**.
The **Check Report** interface will be displayed. See Figure 4-242.

Figure 4-242

1	Disk No.	Check Type	Start Time	Total Space	Er
1	Host-2	Key Area Detect	2020-02-23 18:55:09	2794.52 GB	

Step 2   Click ▣ . The Details interface will be displayed. There, you can view the detected results and S.M.A.R.T reports. See Figure 4-243 and Figure 4-244.

Figure 4-243

Details

Results	S.M.A.R.T

Type   Key Area Detect   Export search results.

■ OK   ■ Bad   ■ Blocked
■ = 1244 MB
Total Checked   1
Total Space   2794.52 GB
Error   0
Disk No.   2
Bad Sector List

No.	Sector No

Figure 4-244
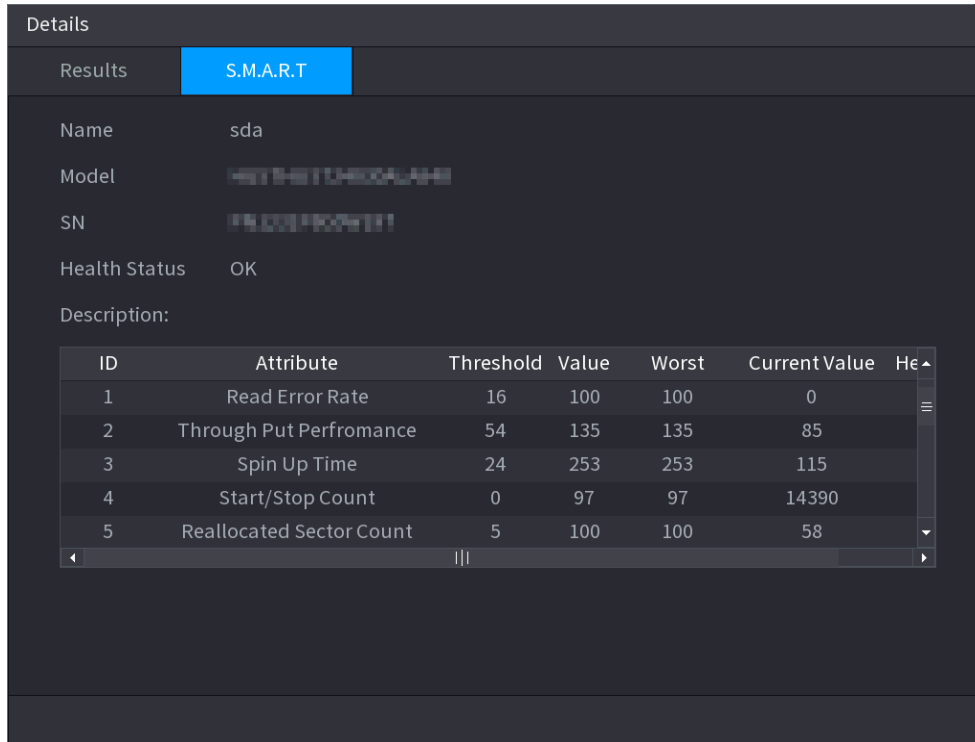
4.13.7.3 Disk Health Monitoring

This section allows you to monitor the health status of disks, and repair if any exceptions are found to avoid data loss. Select **Main Menu > Advanced Settings > Storage Settings** > **Disk Check** > **Health Monitoring**

Click [info icon] to show disk details interface. Then select **Check Type**, set time period, and then click **Search**. The interface shows the details of the disk monitoring status.

Figure 4-245 Disk details
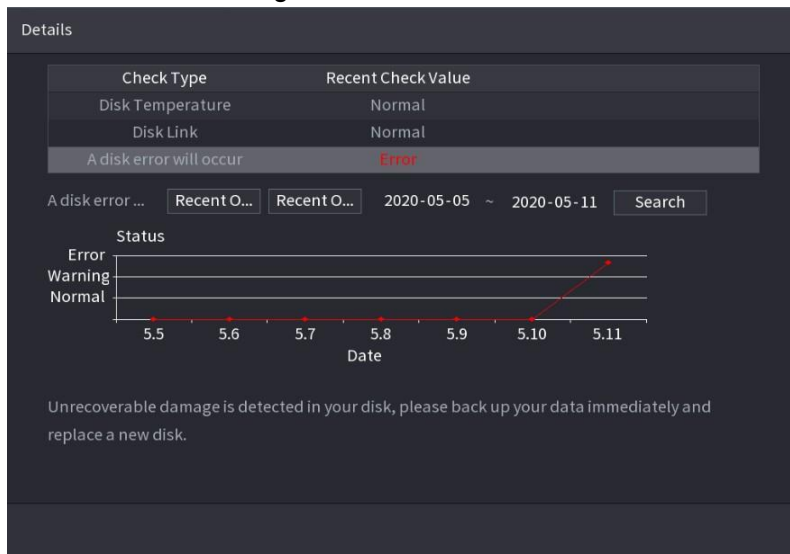
4.12.8 RAID

RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for data redundancy, performance improvement, or both.

📖

- RAID function is not available in all NVR models. See actual product specifications.
- Slight differences may be found in the user interface.
- The NVR supports RAID0, RAID1, RAID5, RAID6, and RAID 10. Local hot spare supports RAID1, RAID5, RAID6, and RAID10.

See below for the disk quantity required for each RAID type. See Table 4-77.

Table 4-77

RAID type	Required disk quantity
RAID0	At least 2.
RAID1	Only 2.
RAID5	At least 3, and using 4 disks to 6 disks is recommended.
RAID6	At least 4.
RAID10 (1+0)	

4.13.8.1 Creation Manager

RAID has different types (such as RAID5, RAID6) which have different data protection, data availability, and performance grades.

See below for RAID creation steps.

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **RAID** > **RAID**.
The RAID interface will be displayed. See Figure 4-246.

Figure 4-246
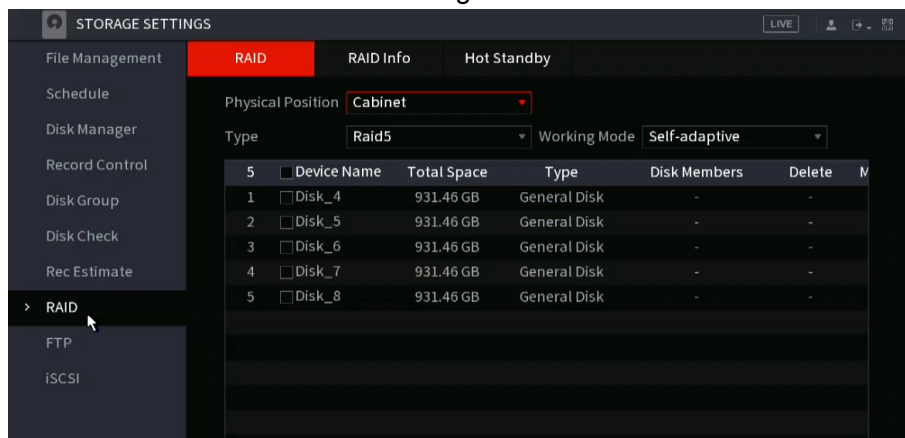
Step 2   You will have options for: **Create RAID** (one-click quick setup) or **Create Manually**, and all the disks involved will be formatted.

- If selecting **Create RAID**, the NVR will create RAID automatically.
  - If there is no existing RAID and no hot spare disk, the system will create RAID5 and a hot spare disk automatically.
  - If there is no existing RAID, but an existing hot spare disk, the system will only create RAID5 and use the existing hot spare disk automatically.
  - If there is an existing RAID and existing hot spare disk, the system will delete the original RAID and create RAID5 with all the disks and use the existing hot spare disk automatically.
- If selecting **Create Manually**:
  1. Select THE RAID type and disks as required.
  2. Click **Create Manually**, and then the format disk notice will be displayed.
  3. Click **OK**.

Step 3   After creating a RAID, the disks need to sync with each other to finish the process. For RAID5 and RAID6, you can select different working mode.
- **Self-Adaptive**: Automatically adjust the RAID sync speed according to the business (process) status.

   When there is no business running, sync is performed at a high speed.

   When there is business running, sync is performed at a low speed.
- **Sync First**: Resource priority is assigned to RAID sync.
- **Business First**: Resource priority is assigned to business operations.
- **Balance**: Resource is evenly distributed to RAID sync and business operations.

4.13.8.2 Raid Info

You can view the existing RAID information, including type, disk space, hot spare, and status.
Select **Main Menu > Advanced Settings > Storage Settings** > **RAID** > **RAID Info**.
The RAID Info interface will be displayed. See Figure 4-247.

Figure 4-247
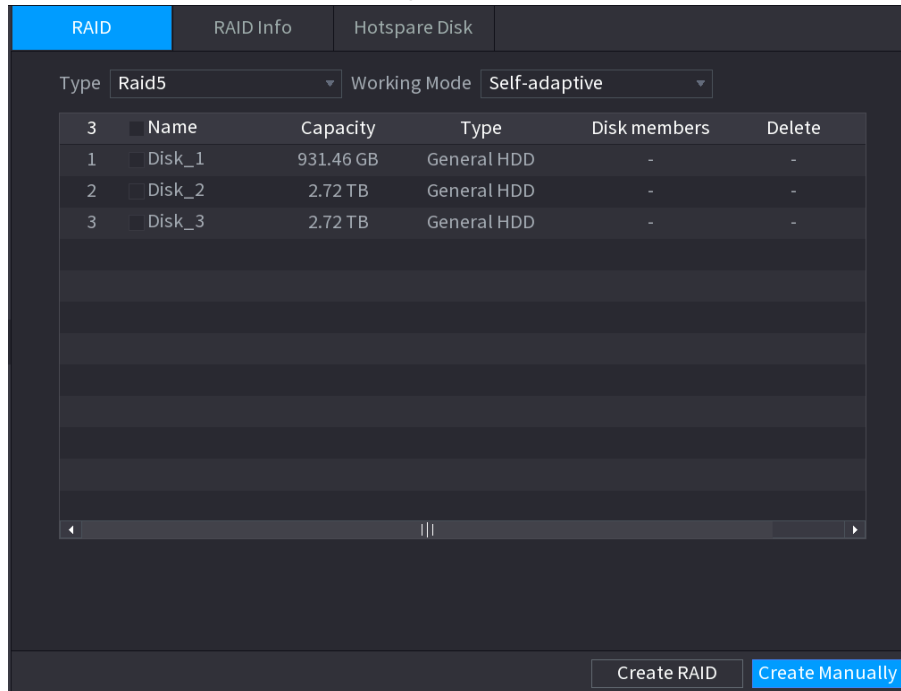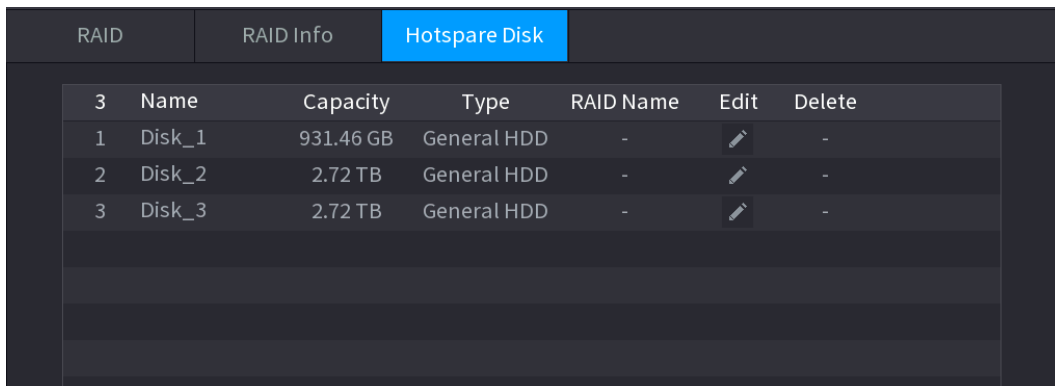
4.13.8.3 Hot Spare Disk

You can add a hot spare disk to a specific disk in the RAID or to the entire RAID. The hot spare disk will switch into operation if any disk fails.

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **RAID** > **Hotspare Disk**. The **Hotspare Disk** interface will be displayed. See Figure 4-248.

Figure 4-248
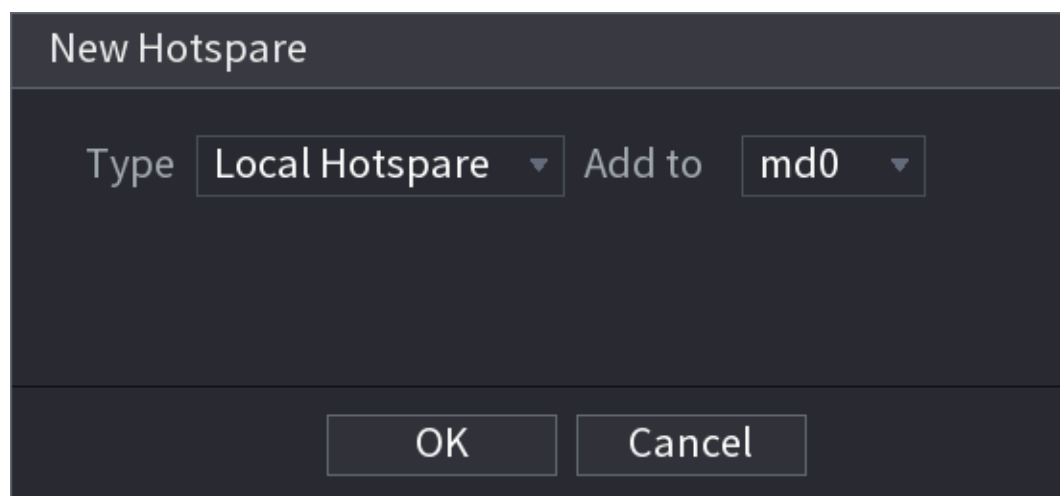
Step 2   Click the ✏ icon behind a disk.

Step 3   The **New Hotspare** interface will be displayed. See Figure 4-249 (New hot spare (local) or Figure 4-250 (New hot spare (global).

Figure 4-249

Figure 4-250

New Hotspare

Type Global Hotspare ▼

OK   Cancel
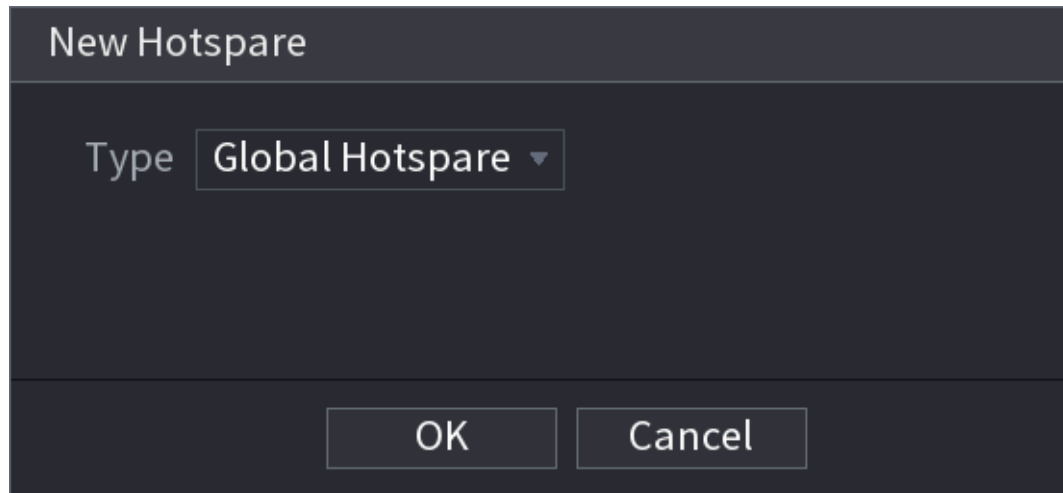
Step 4   You can select **Local Hotspare** or **Global Hotspare**.
- Local Hotspare: Select a target disk, and the new disk will serve as the hot spare disk for the selected disk.
- Global Hotspare: The new disk will serve as the hot spare disk for the entire RAID.

Step 5   Click **OK**.

📖

Click 🗑 behind a hot spare disk to delete it.

4.12.9 Record Estimate

The record estimate function can calculate how long the video can record according to the HDD capacity, and calculate the required HDD capacity according to the recording period. This function may not be available in all model NVRs.

Step 1   **Select Main Menu > Advanced Settings > Storage Settings** > **Rec Estimate**.
The **Rec Estimate** interface will be displayed. See Figure 4-251.

Figure 4-251
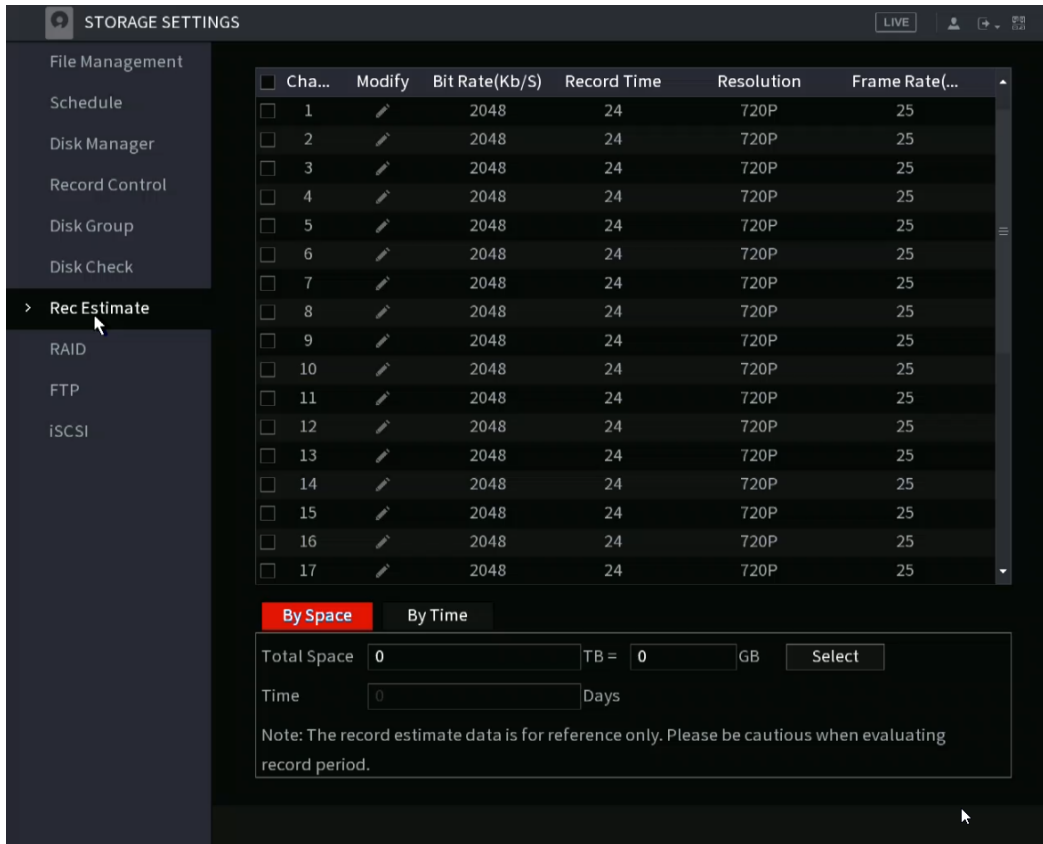
Step 2   Click   .

The **Edit** dialogue box will be displayed. See Figure 4-252. You can configure the **Resolution**, **Frame Rate**, **Bit Rate,** and **Record Time** for the selected channel.

Figure 4-252

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

Then the system will calculate the time period that can be used for storage
according to the channels settings and HDD capacity.

📖
Click **Copy to** to copy the settings to other channels.

4.13.9.1 Calculating Recording Time

Step 1   On the **Rec Estimate** interface, click the **By Space** tab. The **By Space** interface
will be displayed. See Figure 4-253.

Figure 4-253

Step 2   Click **Select**.

The **Select HDD(s)** interface will be displayed.

Step 3   Select the check box of the HDD that you want to calculate.

In the Known Space tab, in the Time field, the recording time will be displayed. See
Figure 4-254.

Figure 4-254

4.13.9.2 Calculating HDD Capacity for Storage

Step 1   On the **Rec Estimate** interface, click the **By Time** tab.
The **By Time** interface will be displayed. See Figure
4-255.

Figure 4-255

Step 2   In the **Time** field, enter the time period that you want to record. The
required HDD capacity will be displayed in the **Total Space** field.

4.12.10   FTP

FTP (File Transfer Protocol) allows you to store and view the recorded videos and
snapshots on a remote FTP server. You will need to download an FTP server software
and install it on your PC prior to configuring the NVR.

For the created FTP user, you will need to set the write permission; otherwise, the upload
of recorded videos and snapshots will fail.

Step 1   Select **Main Menu > Advanced Settings > Storage Settings** > **FTP**.
The **FTP** interface will be displayed. See Figure 4-256.

Figure 4-256

Configure the NVR settings accordingly using the FTP server parameters. See Table 4-78.

Table 4-78

Parameter	Description
Enable	Select to enable the FTP upload function.
FTP type	● Select FTP type. ● FTP: Plaintext transmission. ● SFTP: Encrypted transmission (recommended)
Server Address	IP address of FTP server.
Port	● FTP: The default is 21. ● SFTP: The default is 22.
Anonymous	Enter the user name and password to log in to the FTP server.
User Name	Enable the anonymity function, and then you can login anonymously
Password	without entering the user name and password.

Parameter	Description
Storage Path	Create a folder on FTP server. ● If you do not enter the name of a remote directory, the system automatically creates folders according to the IP and time. ● If you enter the name of the remote directory, the system creates a folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.

File Size	Enter the length of the uploaded recorded video. ● If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. ● If the entered length is more than the recorded video length, the entire recorded video can be uploaded. ● If the entered length is 0, the entire recorded video will be uploaded.
Picture Upload Interval	● If this interval is longer than the IPC snapshot interval, the NVR will upload according to its set interval. For example, if the NVR interval is 5 seconds, and IPC snapshot interval is 2 seconds per snapshot, the NVR will upload the recent snapshot every 5 seconds. ● If this interval is shorter than the IPC snapshot interval, the NVR uploads the snapshot per the IPC snapshot interval. For example, the NVR interval is 5 seconds, and the IPC snapshot interval is 10 seconds per snapshot, the system will upload the snapshot every 10 seconds. ● To configure the snapshot interval, select **Main Menu** > **Advanced Settings > Camera Configuration** > **Encode** > **Snapshot**.
Channel	Select the channel that you want to apply the FTP settings to.
Day	Select the day and set the time period that you want to upload the recorded files. You can set two periods for each day.
Period 1, Period 2	
Record type	Select the record type (Alarm, Intel, MD, and General) that you want to upload. The selected record type will be uploaded during the configured time period.

Step 3   Click **Test**.

The system will populate a message to indicate success or failure. If this fails, check the network connection or configurations for the NVR and FTP server.

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

4.13 System

4.13.1 General

You can set device general information, including device information, system date. Refer to "4.1.4.1 General" for detailed information.

4.13.2 RS232

Once setting RS-232 parameters, the NVR can use the COM port to connect to other devices to debug and operate.

Step 1   Select **Main Menu > Advanced Settings > System Operation** > **RS232**.

Step 2   The **RS232** interface will be displayed. See Figure 4-257.

Figure 4-257

Step 3   Configure the parameters. See Table 4-79.

Table 4-79

Parameter	Description
Function	Select serial port control protocol: ● Console: Upgrade the program and debug with the console and mini terminal software. ● Keyboard: Control this Device with a special keyboard. ● Adapter: Connect with PC directly for transparent transmission of data. ● Protocol COM: Configure the function to protocol COM, in order to overlay the card number. ● PTZ Matrix: Connect matrix control 📖 Not all NVR models support this function. See actual product specificationsl.
Baud Rate	Select Baud rate (115200 by default)
Data Bits	Options include the ranges from 5 to 8 (8 by default)
Stop Bits	Options include 1 and 2.
Parity	Options include none, odd, even, mark, and null.

Step 4   Click **Apply**.

4.14Security

Some NVR models include network security options to strengthen NVR security and prevent unwanted operations.

4.14.1Security Status

Security scanning helps get an overview of the device's current security status. You can scan user, service, and security module status for detailed information about the security status of the device.

Detecting User and Service

📖
The green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

● Login authentication: When there is a risk in the device configuration, the icon will be in orange to warn of the risk. You can click **Details** to see the detailed risk description.
● User Status: If one of the device users or Onvif users uses a weak password, an icon will be in orange to warn of the risk. You can click **Details** to optimize or ignore the risk warning.

Figure 4-258
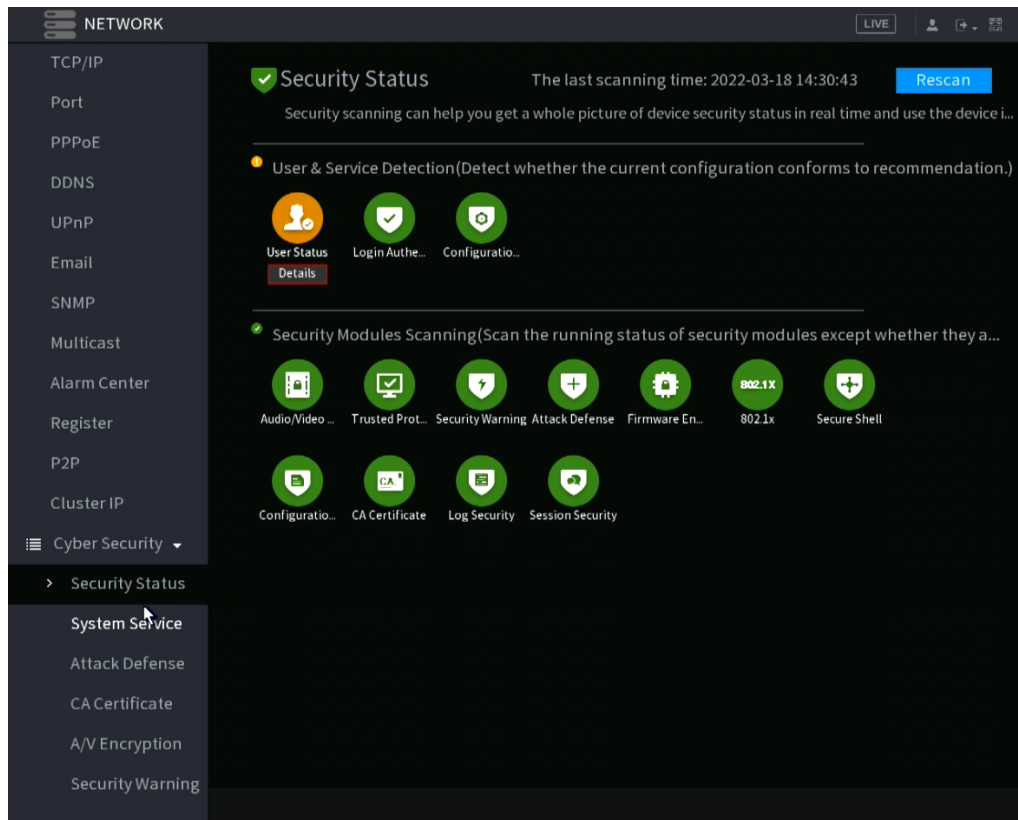
Figure 4-259
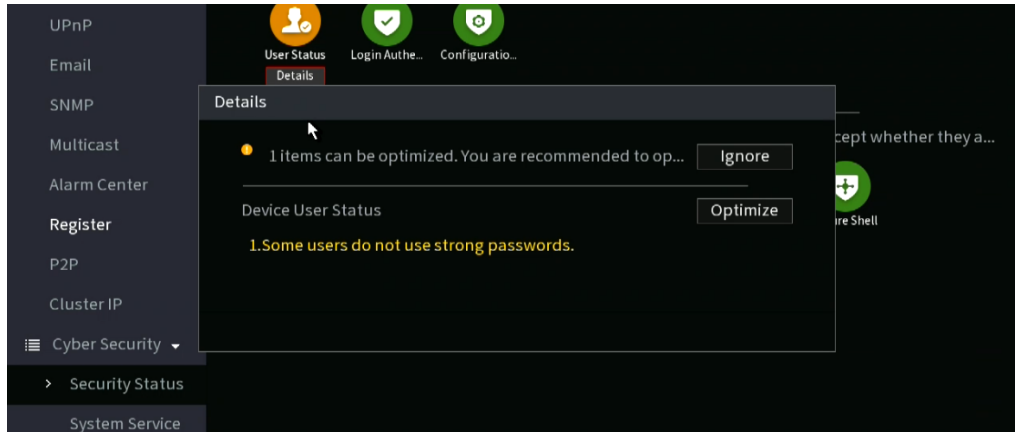
- Configuration Security: When there is a risk detected in the device configuration, the icon will be colored orange to warn of the risk. You can click **Details** to see the detailed risk description. See Figure 4-260.

Figure 4-260
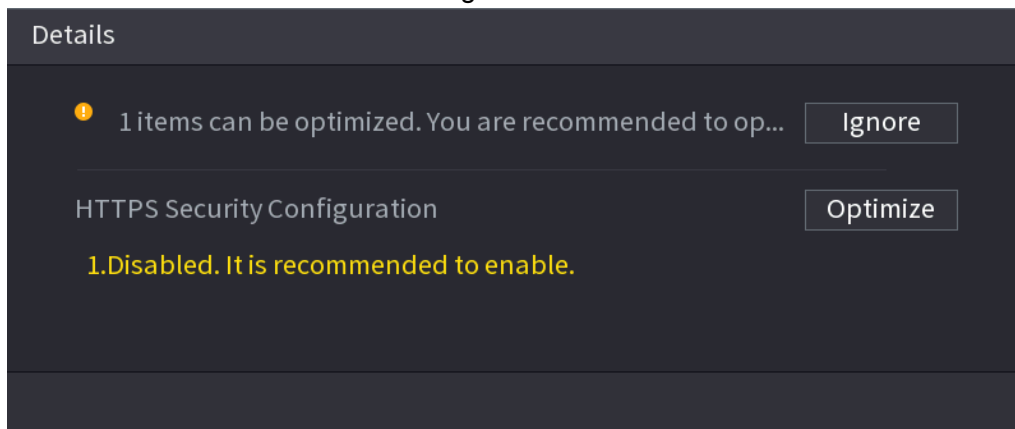
Scanning Security Modules

This area shows the operating status of the security modules. For details about the security modules, move the mouse pointer on the icon to view the on-screen instructions.

Scanning Security Status

To scan security status, click **Rescan** .

4.14.2 System Service

This section allows you to set basic network configurations such as 802.1x and HTTPS.

4.14.2.1 Basic Services

Step 1　　Select **Main Menu > Advanced Settings > Network > Cyber Security > System Services > Basic Services**.

The **Basic Services** interface will be displayed. See Figure 4-261.

Figure 4-261
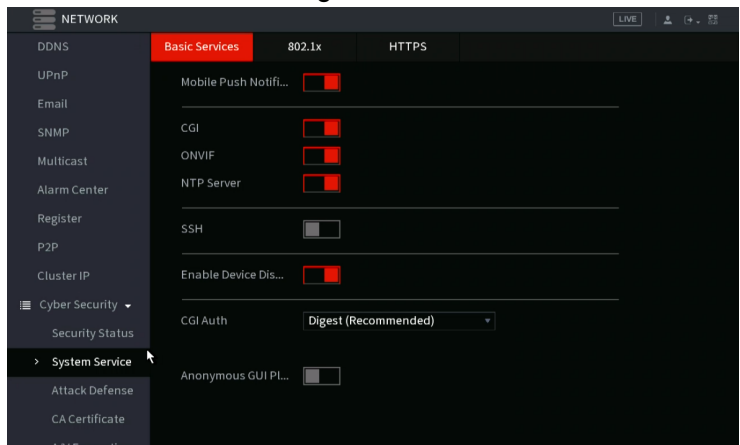
Step 2   Select **Basic Services** and configure parameters.

There may be a security risk if **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** services are enabled.

Table 4-80 Basic service parameters

Parameter	Description
Mobile Push Notifications	When enabling this function, the events triggered by the NVR can be pushed to a mobile phone. This function is enabled by default.
CGI	When this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default.
ONVIF	When this function is enabled, remote devices can be added through the ONVIF protocol. This function is enabled by default.
NTP Server	When enabling this function, an NTP server can be used to synchronize the time of the device. This function is enabled by default.
SSH	After enabling this function, you can use the SSH service. This function is disabled by default.
Enable Device Discovery	After enabling this function, the NVR can be found by other devices through network scanning or searching.
Private Protocol Authentication Mode	● Security Mode (Recommended): Uses Digest access authentication when connecting to NVR. ● Compatible Mode: Select this mode if the client does not support Digest access authentication.

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

4.14.2.2 802.1x

This section is for configuring 802.1x certification to enter a LAN requiring this authentication.

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security > System Services** > **802.1x**.

The **802.1x** interface will be displayed. See Figure 4-262

Figure 4-262
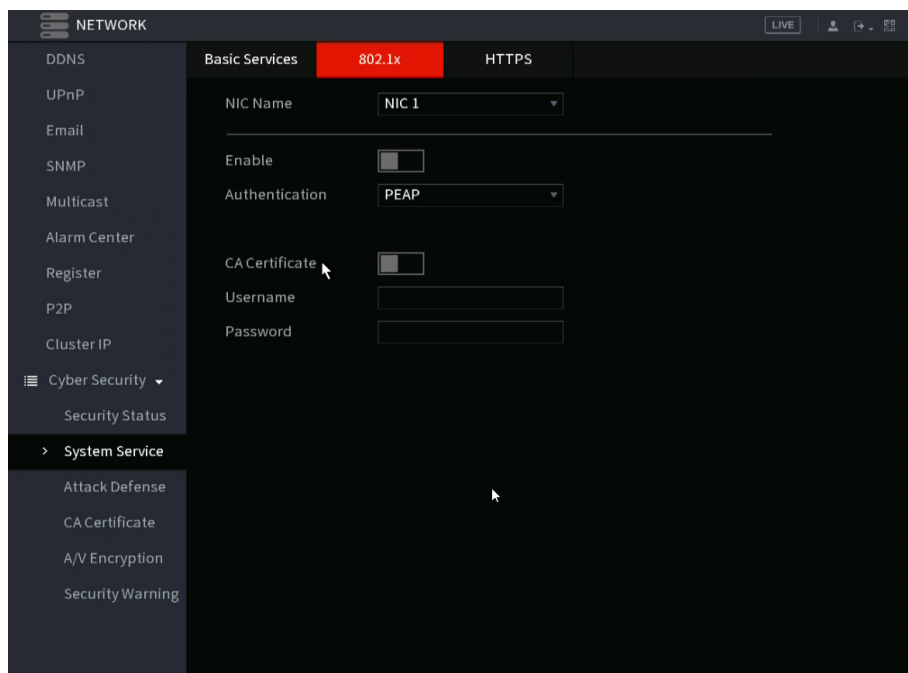
Step 2   Select the Ethernet card you want to certify.

Step 3   Select **Enable** and configure parameters. See Table 4-81.

Table 4-81 802.1x parameters

Parameter	Description
Authentication	● PEAP: protected EAP protocol. ● TLS: Transport Layer Security. Provides privacy and data integrity between two communications application programs.
CA Certificate	If enabled, click **Browse** to import CA certificate from a flash drive. For details about importing and creating a certificate, see "4.15.4 CA Certificate".
Username	The username will be authorized at the server.
Password	The password of the corresponding username.

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

4.14.2.3 HTTPS

HTTPS enables a more secured web interface experience. This is typically recommended.

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security > System Services** > **HTTPS**.

The **HTTPS** interface will be displayed. See Figure 4-263.

Figure 4-263
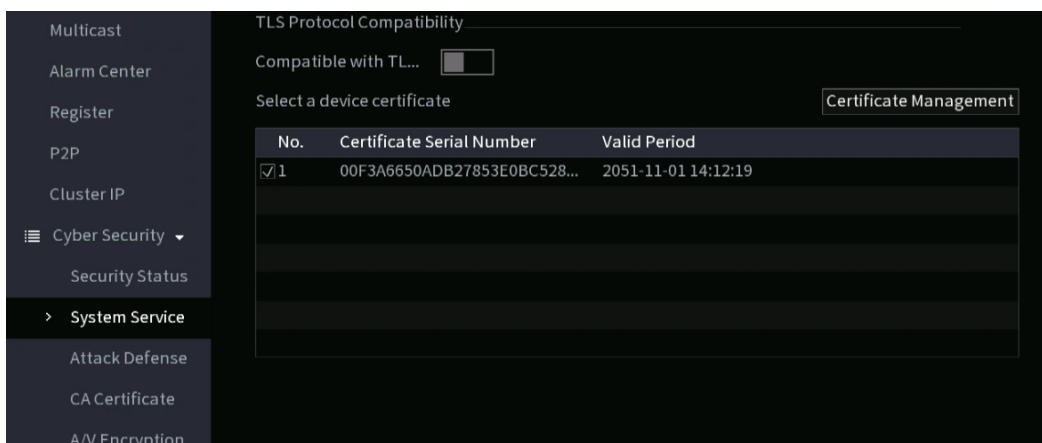
Step 2   Enable the HTTPS function.

Step 3   (Optional) Enable **Compatible with TLSv1.1 and earlier versions** to allow protocol compatibility.

Step 4   Click **Certificate Management** to create or import an HTTPS certificate from a USB drive. For details about importing or creating a CA certificate, see "4.15.4 CA Certificate".

Step 5   Select an HTTPS certificate.

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

4.14.3 Attack Defense

4.14.3.1 Firewall

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >Attack Defense > Firewall**.

The **HTTPS** interface will be displayed. See Figure 4-264.

Figure 4-264 Firewall
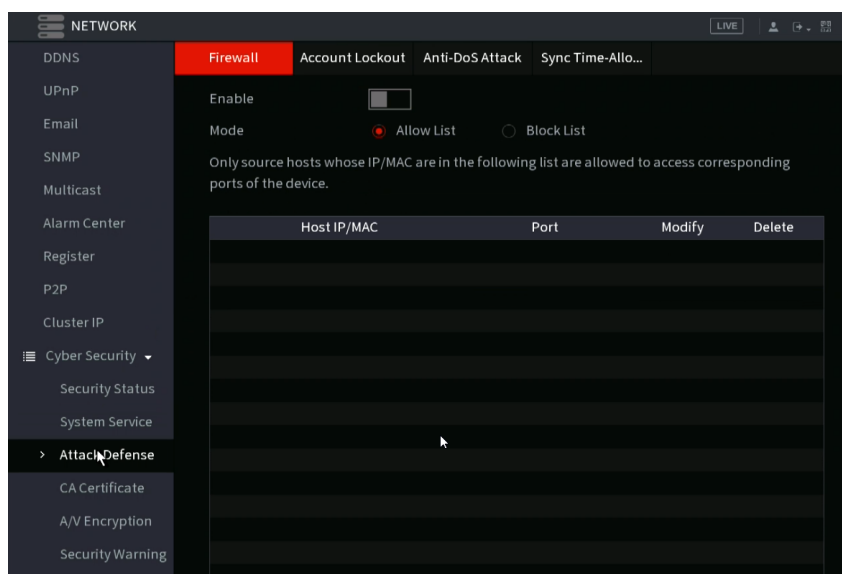
Step 2   Select **Enable** to enable the firewall.

Step 3   Configure the parameters. See Table 4-82.

Table 4-82 Parameters

Parameter	Description
Mode	Mode can be configured if Type is set to Network Access. ● If Trusted Sites is enabled, you can visit the HTTPS port successfully with IP/MAC hosts in Trusted Sites. ● If Blocked Sites is enabled, you cannot visit the HTTPS port with IP/MAC hosts in Blocked Sites.
Add	If the Type is Network Access, you can configure IP Address, IP Segment, and MAC Address.
Type	Options include IP address, IP segment, and MAC address.
IP Address Start Port End Port	Enter IP Address, Start Port, and End Port to be allowed or forbidden. ▭ This can only be configured if the Type is set to IP Address. Start Port and End Port can be configured only in Network Access Type.
Start Address	Enter the Start Address and End Address of IP Segment. ▭ This can only be configured if the Type is set to Segment.

Parameter	Description
MAC Address	Enter MAC Address that is allowed or forbidden ▭ This can only be configured if the Type is set to MAC Address.

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

4.14.3.2 Account Lockout

This section allows you to set the NVR behavior for incorrect password attempts.

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >Attack Defense** > **Account Lockout**.

The **Account Lockout** interface will be displayed. See Figure 4-265.

Figure 4-265 Account lockout
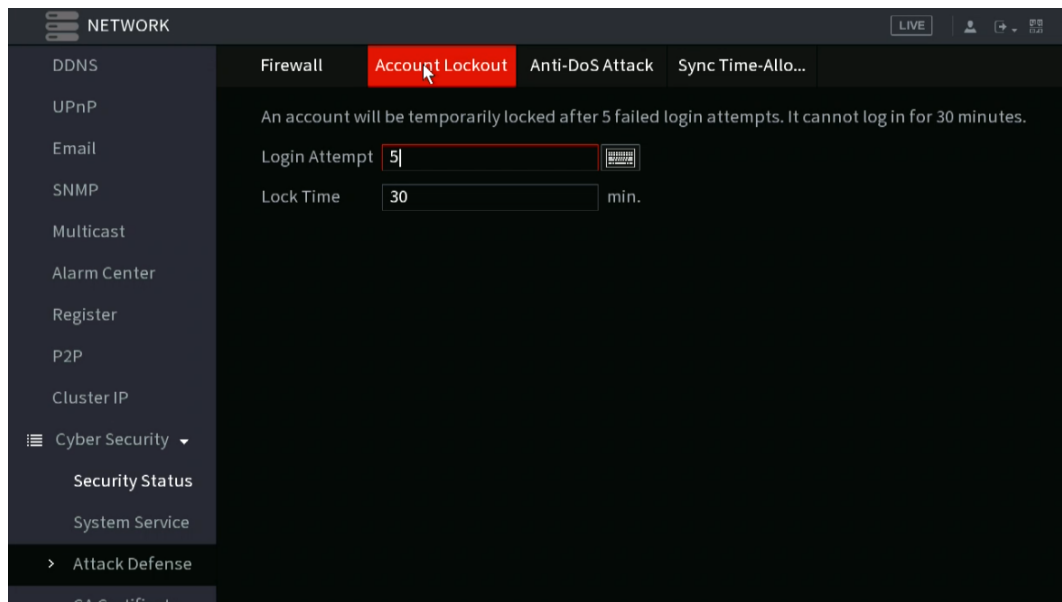
Step 2   Set parameters. See Table 4-83.

Table 4-83 Account lockout parameters

Parameter	Description
Attempt(s)	Configures the maximum number of allowable incorrect password entries. The account will be locked after the entries exceed the maximum number. Value range: 5–30. (Default value is 5)
Lock Time	Configuers the lock out duration Value range: 5–120 minutes. (Default value is 30 minutes)

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

4.14.3.3 Anti-Dos Attack

This section allows you to enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against a Dos attack. See Figure 4-266.

Figure 4-266 Anti-Dos Attack

14.4.4 Sync Time-Whitelist

📖

The synchronization is only allowed with hosts in the trusted list.

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >Attack Defense** > **Sync Time-Whitelist**.

The **Sync Time-Whitelist** interface will be displayed. See Figure 4-267.

Figure 4-267 Sync Time-Whitelist

Step 2   Select **Enable** to enable **Sync Time-Whitelist** function.

Step 3   Configure the parameters. See Table 4-84.

Table 4-84 Sync Time-Whitelist parameters

Parameter	Description
Add	Adds trusted hosts for time synchronization.
Type	Select IP address or IP segment for hosts to be added.
IP Address	Input the IP address of a trusted host. This can only be configured if the Type is IP Address.
Start Address	Input the start IP address of trusted hosts. This can only be configured if the Type is IP Segment.
End Address	Input the end IP address of trusted hosts. This can only be configured if the Type is IP Segment.

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

4.14.4 CA Certificate

4.14.4.1 Device Certificate

Create Certificate

1. Select **Main Menu > Advanced Settings > Network > Cyber Security >CA Certificate > Device Certificate**. The **Device Certificate** interface will be displayed. See Figure 4-268.

2. Configure parameters. See Table 4-85.

Figure 4-268 Device Certificate
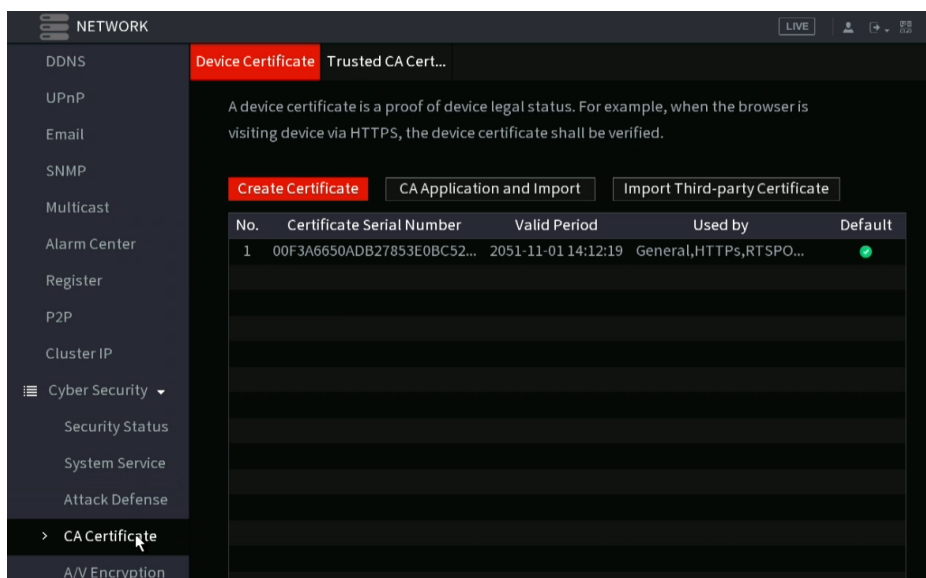
Table 4-85 Creating certificate

Parameter	Description
County	This parameter is user-defined.
State	This parameter is user-defined.

Parameter	Description
City Name	This parameter is user-defined.
Valid Period	Input a valid period for the certificate.
Organization	This parameter is user-defined.
Organization Unit	This parameter is user-defined.
Domain Name	Input the domain name or IP address of the certificate.

3. Click **Create**.

CA Application and Import

Follow the on-screen instructions to finish the CA application and import. See Figure 4-269.

Figure 4-269 CA application and import
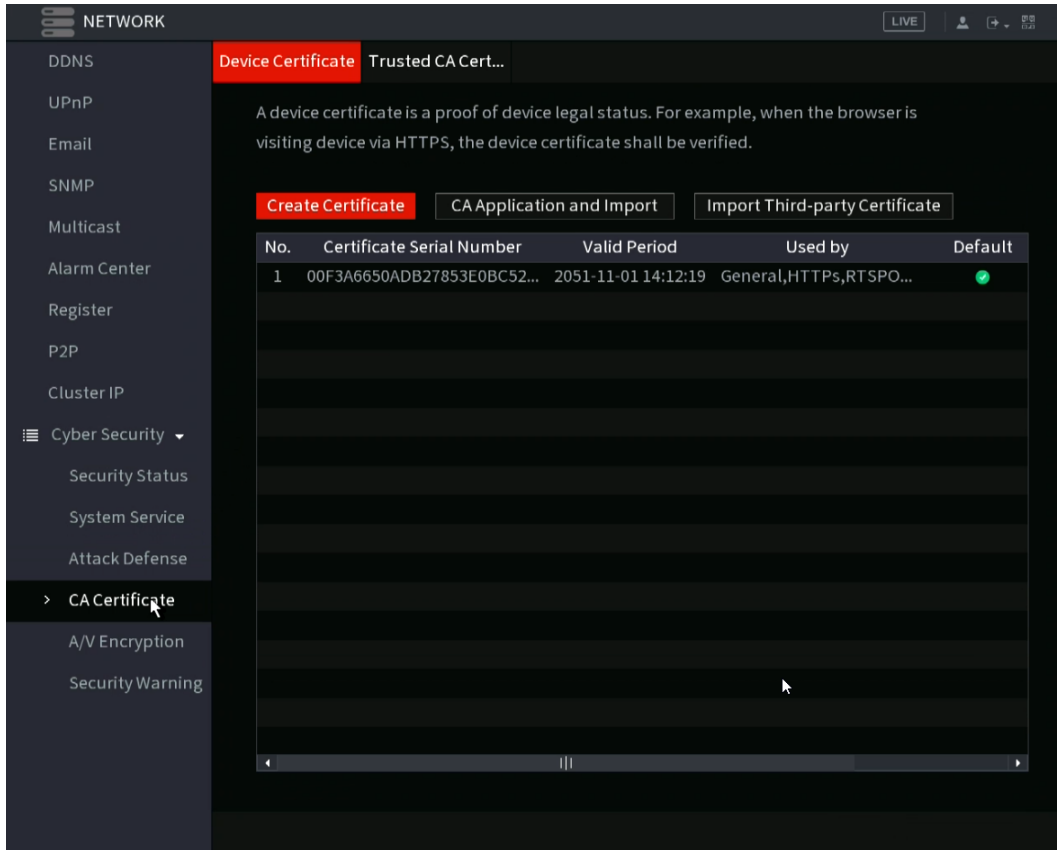
Import Third-Party Certificate

1. Configure Parameters. See Table 4-86.

Table 4-86 Importing third-party certificate

Parameter	Description
Path	Click **Browse** to find the third-party certificate path on the USB drive.
Private Key	Click **Browse** to find the third-party certificate private key on the USB drive.
Private Key Password	Input the private key password.

2. Click **Create**.

4.14.4.2 Trusted CA Certificate

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >CA Certificate** > **Trusted CA Certificate**.

Step 2   Click **Install Trusted Certificate**.
The **Create Certificate** will be displayed. See Figure 4-270.

Figure 4-270 Creating certificate
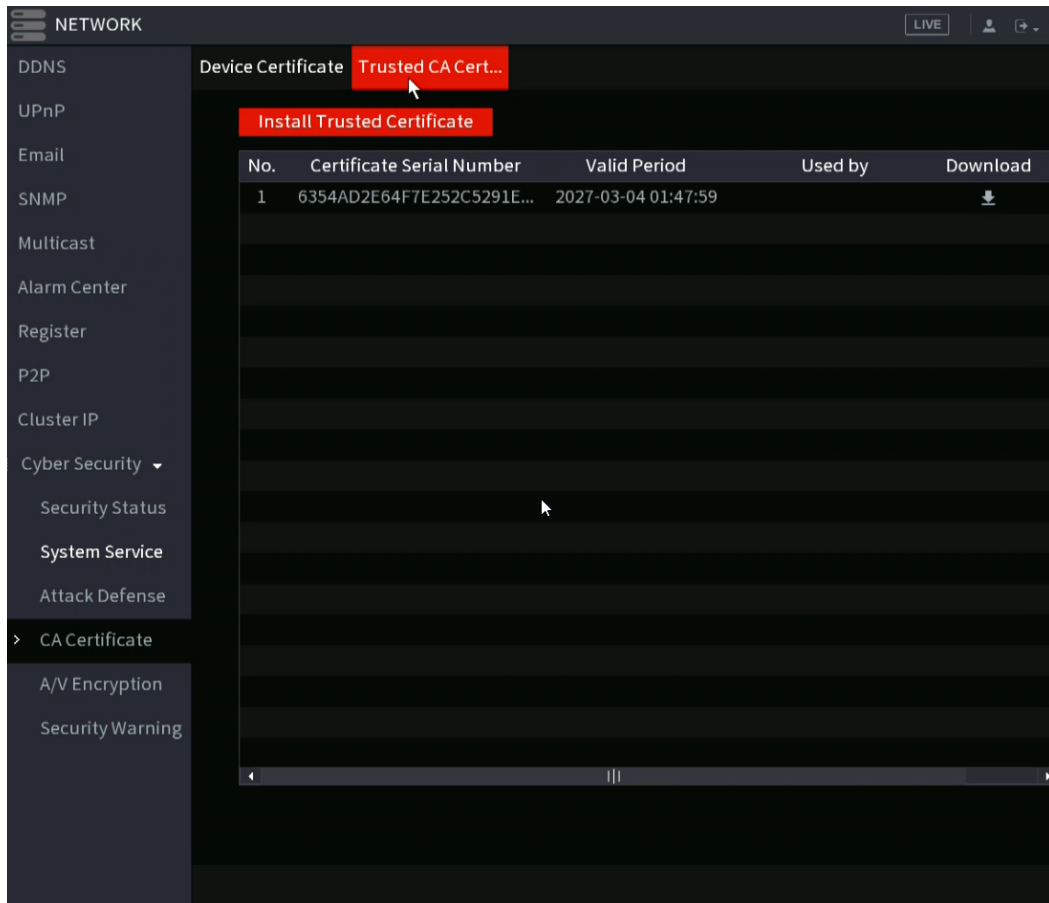
Step 3   Click **Browse** to select the certificate that you want to install.

Step 4   Click **Import**.

4.14.5 Audio/Video Encryption

This section covers the NVR configuration of the audio and video encryption during data transmission.

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >A/V Encryption** > **Audio/Video Transmission**.

The **Audio/Video Transmission** interface will be displayed. See Figure 4-271.

Figure 4-271
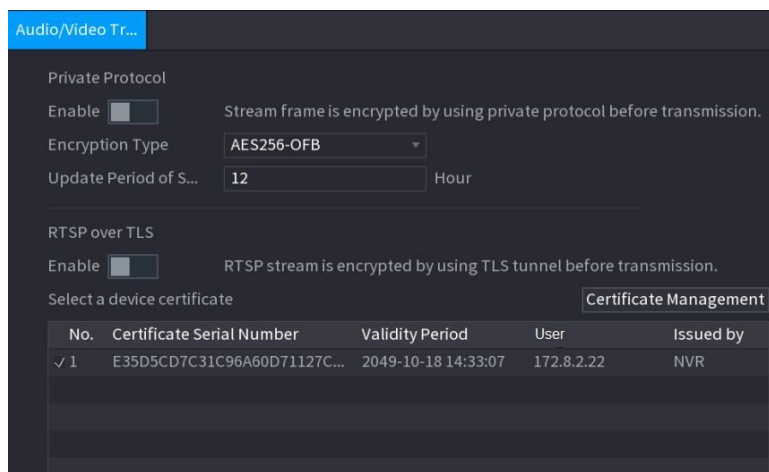
Table 4-87 Audio and video transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using the private protocol. 📖 There may be security risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. Select 0 to never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. 📖 There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "4.15.4.1 Device Certificate".

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

4.14.6 Security Warning

4.14.6.1 Security Exception

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >Security Warning** > **Security Exception**.

The **Security Exception** interface will be displayed. See Figure 4-272.

Figure 4-272 Security Exception
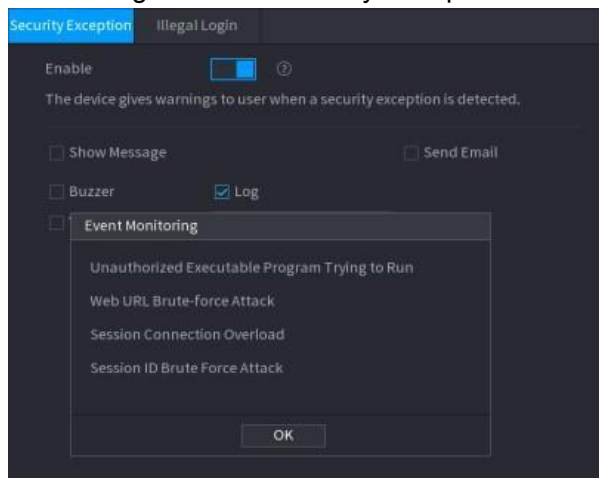
Step 2   Select **Enable** and configure parameters. See Table 4-88.

Table 4-88 Security exception parameters

Parameter	Description
Alarm-out Port	When the event is triggered, this will trigger an alarm device (such as lights, sirens, etc.) connected to the NVR alarm output port.
Post-Alarm	When the event ends, the alarm extends for a period of specified time. The time range is from 0 seconds to 300 seconds.
Show Message	Enablea a pop-up message in a local host PC (software).
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. 📖 Refer to "4.18.1 File Management" to add audio files.
Log	The NVR will record the information in the log when an alarm event occurs.
Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. 📖 Email settings must be configured prior. For details, see "4.12.10 Email".
⑦	Security Event monitoring description. Indicates the type of attacks that can trigger security exceptions. ● Unauthorized executable program attempting to run ● Web URL brute-force attack ● Session connection overload ● Session ID brute-force attack

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

4.14.6.2 Illegal Login

Step 1   Select **Main Menu > Advanced Settings > Network > Cyber Security >Security Warning** > **Illegal Login**.
The **Illegal Login** interface will be displayed. See Figure 4-273.

Figure 4-273 Illegal Login
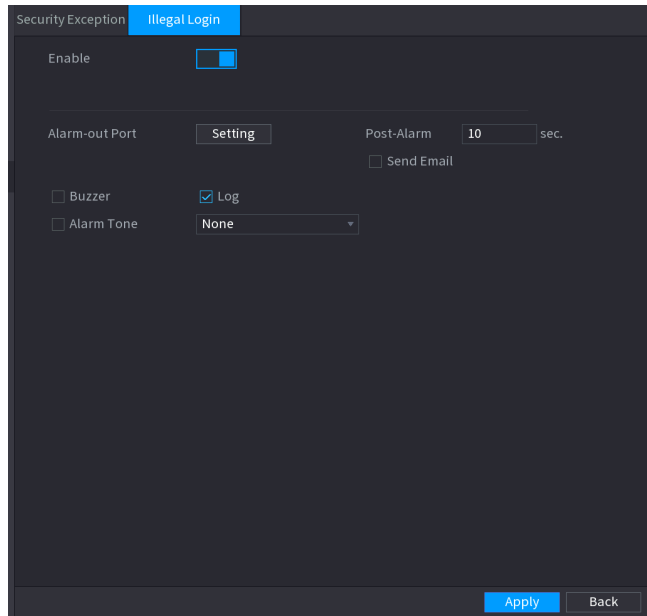
Step 2   Select **Enable** and configure parameters. See Table 4-89.

Table 4-89 Illegal login parameters

Parameter	Description
Alarm-out Port	This will trigger an alarm device (such as lights, sirens, etc.) if one is connected to the NVR alarm output port.
Post Alarm	When the event ends, the alarm extends for the specified time. The time range is from 0 seconds to 300 seconds.
Buzzer	Select the check box to activate the onboard buzzer when an event occurs.
Alarm Tone	The NVR will play a specified audio file when the event occurs. To enable, check the box and then select the corresponding audio file from the drop-down list. Refer to "4.18.1 File Management" to add audio files.
Log	The NVR will record the information in the log when an alarm event occurs.

Send Email	When selected, the NVR sends an Email to the set receivers when the event is triggered. Email settings must be configured prior. For details, see "4.12.10 Email".

4.15 Account

This section allows you to manage the users, user group and ONVIF user, as well as configure the admin (recovery) security questions.

- The max character allowable for a username is 31. The max characters allowable for a group is 15.
- The user name can only contain English letters, numbers and "_", "@", ".".
- The default user amount is 64 and the default group amount is 20. The NVR utilizes two-level management: group and user. The user authorities shall be less than group authorities (The admin user authorities are set by default).
- For group or user management, there are two levels: admin and user. The user name should be unique and a user is allowed to belong to one group only.

4.15.1 User

4.15.1.1 Add User

Step 1   Select **Main Menu > Advanced Settings > System Operation > User** > **User**.
The **User** interface will be displayed. See Figure 4-274.

Figure 4-274
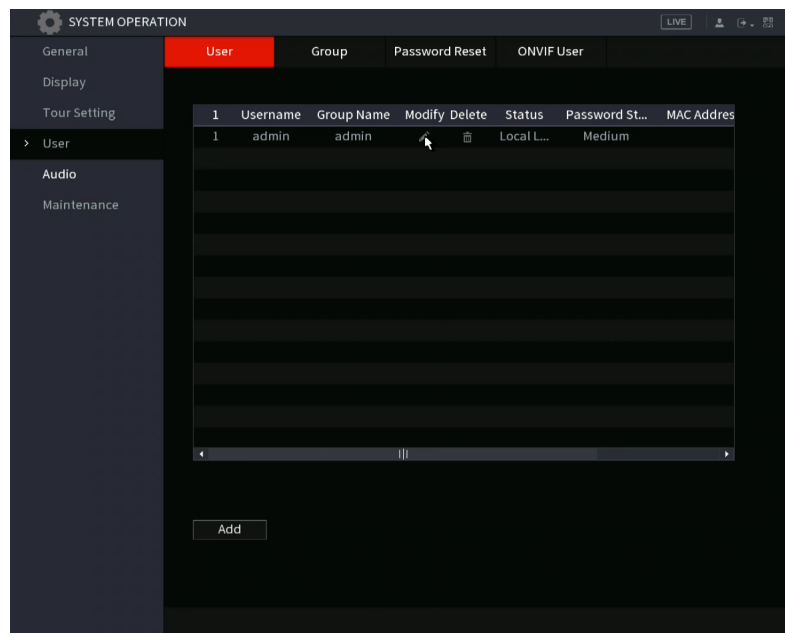
Step 2   Click **Add**.
The **Add** interface will be displayed. See Figure 4-275.

Figure 4-275

Step 3   Input the user name, password, select the group it belongs to from the drop-down list. Then you can check the corresponding rights for current user. See Table 4-90.

Table 4-90

Parameter	Description
Username	Enter a user name and password for the account.
Password	
Confirm Password	Re-enter the password for confirmation.
Remarks	(Optional) Enter a description of the account.
User MAC	(Optional) Enter user MAC address
Group	Select a group for the account to belong to. 📖 The user rights must be within the group permission.
Period	This allows you to create a defined time period during which the account can log in the device. Click **Setting** to display the **Setting** interface and configure the time periods.
Permission	In the **Permission** area, select the checkboxes to give those permissions to the user. There will be different permission types under the **System** tab, **Search** tab, and **Live** tab.

Step 4   Click **OK** button to save.

📖
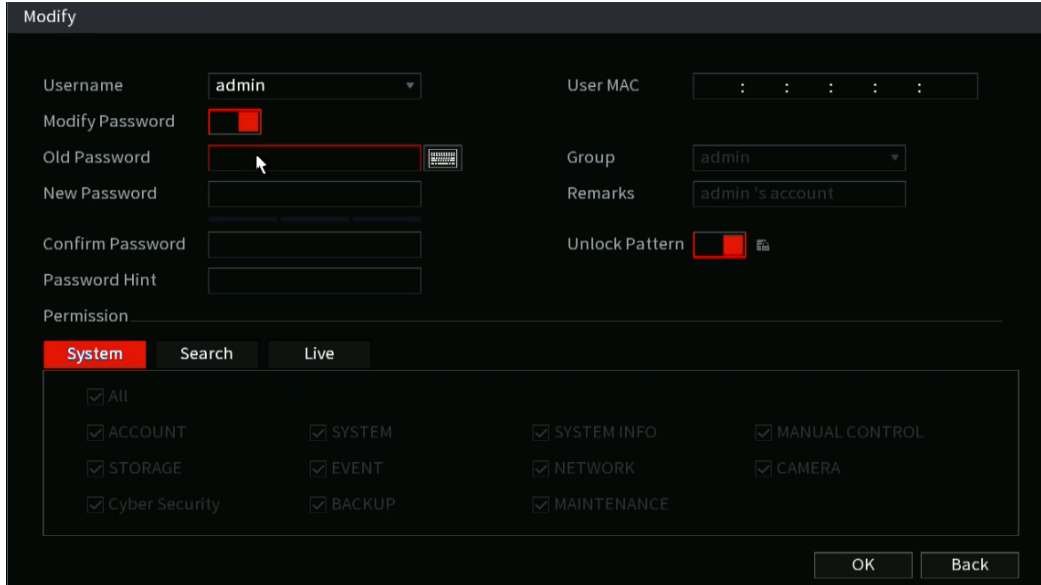
Click 🖉   to modify the corresponding user information, click 🗑   to delete the user.

4.15.1.2 Modify Password

Step 1   Select **Main Menu > Advanced Settings > System Operation > User** > **User**, click ✎ of the corresponding user.

The **Modify User** interface will be displayed. See Figure 4-276.

Figure 4-276

Step 2   Check the box to enable the **Modify Password** function. Enter old password and then enter the new password twice. Proceed to step 3 if creating Unlock pattern.

📖

- Password/confirm password: The password character limit ranges from 8 to 32 characters. The password can contain letters, numbers and special characters (excluding "'", "''", ",", ":", "&"). It is recommended to create a strong password.
- STRONG PASSWORDS ARE HIGHLY RECOMMENDED-For your device own security, create a strong password of your own choosing. We also recommend you change your password periodically especially in the high security system.
- To enable Unlock Pattern function, click 🖼 .

Step 3 Enter the **Unlock Pattern** interface. See Figure 4-277.

Figure 4-277

Step 4   Click **Back** to save.

## 4.15.2 Group

Step 1   Select **Main Menu > Advanced Settings > System Operation > User** > **Group**.
The **Group** interface will be displayed. See Figure 4-278.

Figure 4-278

Step 2   Click **Add**.
The **Add** interface will be displayed. See Figure 4-279.

Step 3   Enter group name and then input some memo information if necessary. Check the appropriate boxes
to select permissions.

Figure 4-279

Step 4   Click **OK** to save.

📖   Click ✏ to modify a group
          Click 🗑 to delete a group.

4.15.3 Reset Password

The NVR allows you to utilize security questions and answers to recover a lost password. After successfully answering the security questions, you can reset admin account password.

📖
This function is for **admin** user only.

Step 1   Select **Main Menu > Advanced Settings > System Operation > User** > **Password Reset**.
          The **Password Reset** interface will be displayed. See Figure 4-280.

Figure 4-280
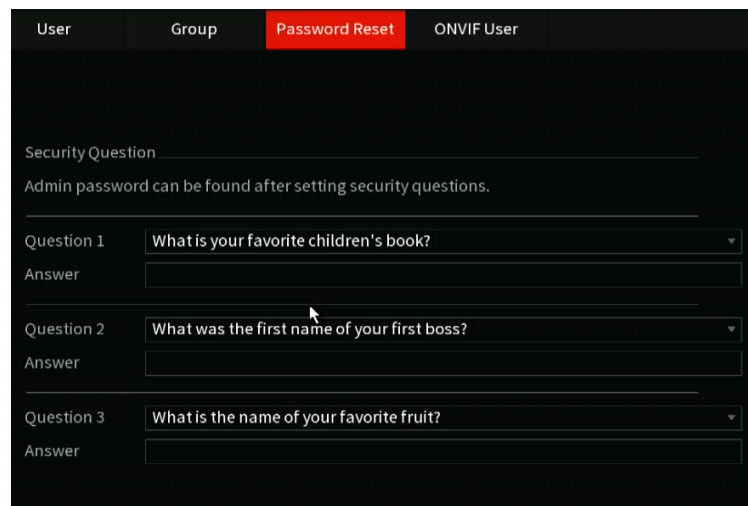
Step 2   Check the box to enable Reset password function.

📖

This function is enabled by default.

Step 3   Input proper security questions and answers.

Step 4   Click **OK**.

After you successfully set security questions, you can answer the security questions to reset the **admin** password.

4.15.4 ONVIF User

This section allows you to create ONVIF users to interact with third-party devices.

📖

The default ONVIF user is **admin**. It is created after initializing the NVR.

For some series NVRs, the ONVIF user password will be modified when initializing the NVR and setting the admin password.

Step 1   Select **Main Menu > Advanced Settings > System Operation > ONVIF User**.

The **ONVIF User** interface will be displayed. See Figure 4-281

Figure 4-281

Username	Group Name	Modify	Delete	Password S...
admin	admin	✎	🗑	Strong

Step 2   Click **Add**.

The **Add** interface will be displayed. See Figure 4-282.

Figure 4-282

Step 3   Set user name, password and then select group from the drop-down list.

Step 4   Click **OK** to complete setup.

Click to modify the corresponding user information, click to delete current
user.

4.16 Output and Display

4.16.1 Display

This section allows you to configure the local interface display settings such as displaying time and channel
title, adjusting image transparency, and selecting the resolution.

Step 1   Select **Main Menu** > **Advanced Settings** > **System Operation**> **Display**.
The **Display** interface will be displayed. See Figure 4-283.

Figure 4-283

<u>Step 2</u>   Configure the settings for the display parameters.

Table 4-91

Parameter	Description
Main Screen/Sub Screen	Configure the output port format of both screens. NVRs with only 1 HDMI and VGA will only support simultaneous output. ● When sub screen is disabled, the format of main screen will be HDMI1/VGA simultaneous output. ● When sub screen is enabled, the format of main screen and sub screen are non-simultaneous outputs. ◇ When output port of sub screen is set to **HDMI**, the output port of main screen is set to **VGA** by the device. ◇ When output port of sub screen is set to **VGA**, the output port of main screen is set to **HDMI** by the device.
Time Title/Channel Title	Select the check box and the date and time of the system will be displayed in the preview screen.

Transparency	Set the transparency of the local menu of the NVR device. The higher the transparency, the more transparent the local menu.
Time Title/Channel Title	Select the check box to display the date and time the preview screen.
Image Enhancement	Select the check box to optimize the edges of the preview image.
iMD Preview	Select the check box to display the iMD previews in the live view interface.
AI Rule	Select the check box to display the AI rules in the live view interface. 📖 Not all NVR models support this feature.
Original Ratio	Click **Setting** and select the channel to restore the corresponding channel image to the original aspect ratio.
Live Audio	Configure audio input on live view. You can select **Audio 1**, **Audio 2**, and **Mixing**. For example, if **Audio 1** for **D1** channel is selected, the sound of audio input port 1 of the camera will play. If **Mixing** is selected, the sound of all audio input ports will play.
Resolution	Sets the resolution for the display. Resolution ranges vary depending on model.

<u>Step 3</u>   Click **Apply**.

4.16.2 Tour

This section allows you to create local display tours. When a tour is enabled, the NVR local display will cycle through different channel split view groups if the NVR is left inactive.

<u>Step 1</u>   Select **Main Menu** >**Advanced Settings** > **System Operation** > **DISPLAY** > **Tour Setting** > **Main Screen** (click sub screen to configure tour properties for that screen).

The **Tour** interface will be displayed. See Figure 4-284.

Figure 4-284
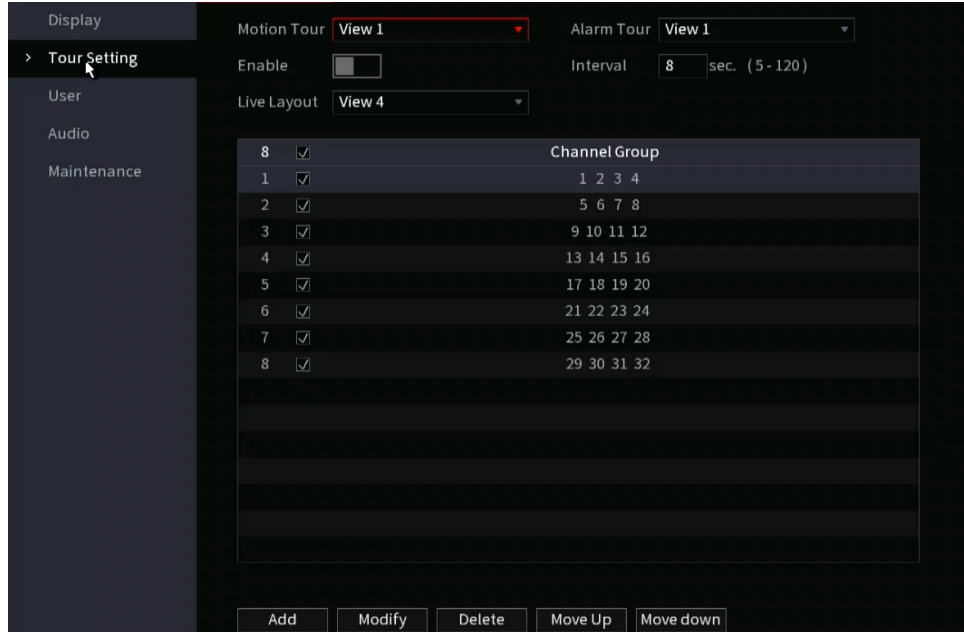
- To toggle image switching, click the left mouse button on the top right of the live view screen or press Shift to switch between the ⊙ icon (image switching is allowed) and 🖼 (image switching is not allowed).
- On the navigation bar, click the ↻ icon to enable the tour and click ⊛ to disable it.

Step 2   Configure the tour setting parameters. See Table 4-92.

Table 4-92

Parameter	Description
Enable Tour	Enables the tour function.
Interval	Enter the amount of time that you want a channel group to display before switching to another group. The value ranges from 5 seconds to 120 seconds, and the default value is 5 seconds.
Motion Tour, Alarm Tour	The tour will be triggered by alarm and motion events. Select the View 1 or View 8 for **Motion Tour** and **Alarm Tour.**
Live Layout	In the **Live Layout** list, select **View 1**, **View 4**, **View 8**, or other modes that are supported by the NVR.
Channel Group	Displays all channel groups under the current Window Split setting. - To Add a channel group: Click **Add**, in the pop-up **Add Group** channel, select the channels to form a group, and then click **Save**. - To Delete a channel group: Select the check box of any channel group, and then click **Delete**. - To Edit a channel group: Select the check box of any channel group and then click **Modify**, or double-click on the group. The **Modify Channel Group** dialog box will be displayed. You can also regroup the channels. - Click **Move up** or **Move down** to adjust the position of the

	channel group. 📖 It is recommended to delete any channel groups you do not want to show on the tour. When enabled, the tour will cycle through all the split views and show any groups under those split views.

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

4.16.3 Customized Display

Some NVR models allow you to create a custom split view.

📖

● This function is for some series NVR models. Refer to the actual product for detailed information.
● The NVR supports a maximum of 5 customized views.

Step 1   Select **Main Menu >Advanced Settings > System Operation > DISPLAY > DISPLAY** > **Custom Split**.

The **Custom Split** interface will be displayed. See Figure 4-285.

Figure 4-285
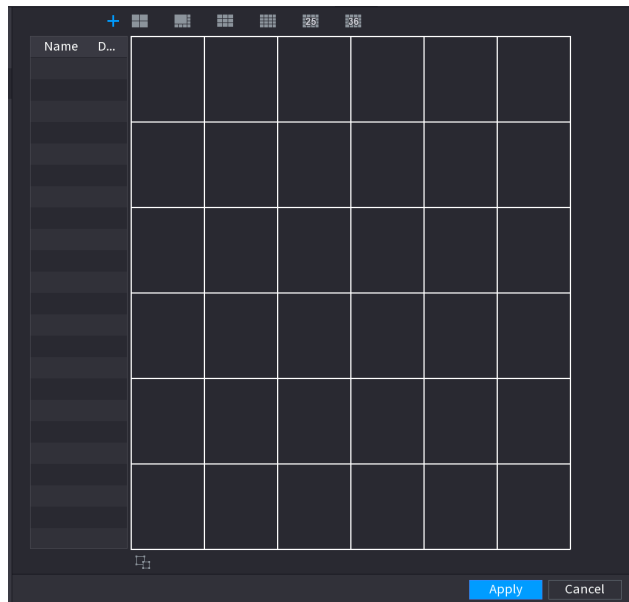
Step 2   Click ➕ and then click ⬛⬛⬛⬛⬛⬛ to select basic mode.

The NVR utilizes the basic window mode as the new window name. For example, if you select the 8 display mode, the default name is Split8.In regular mode, drag the mouse in the preview frame to merge several small windows to one window to get the desired split mode. See Figure 4-286.

📖

● After merge the window, system adopts the remaining window amount as the new name such as Split4.

Figure 4-286
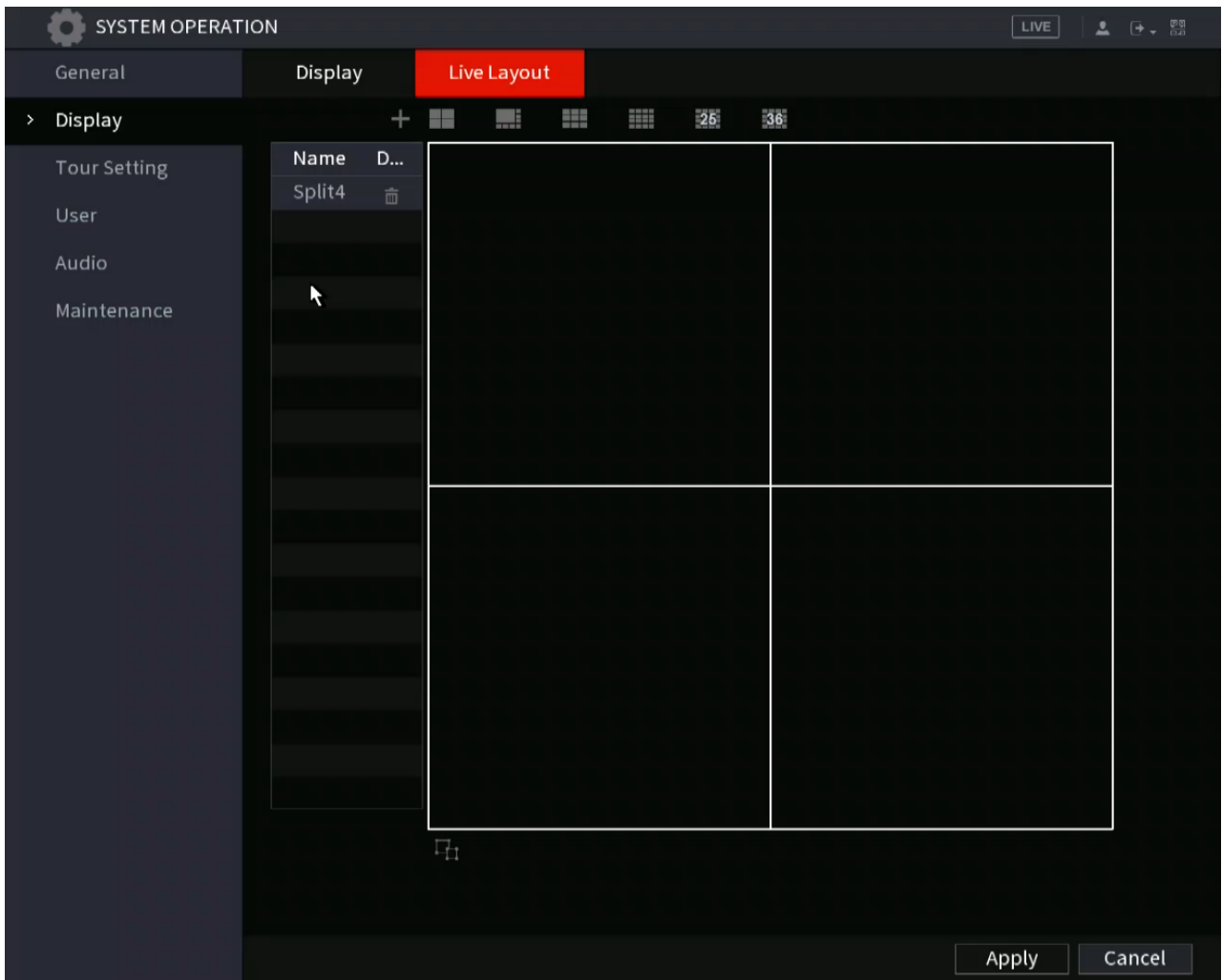
Step 3   Click **Apply** to exit.

After the setup, navigate to the preview window, right click mouse and then select Custom Split.

4.17 Audio

This section manages audio files and configuration for the schedule play function.

Not all NVR models support this feature.

4.17.1 File Management

This section allows you to add audio files, listen to audio files, rename and delete audio files, and configure the audio volume.

Step 1   Select **Main Menu** > **Advanced Settings** > **System Operation** > **File Management**.

The **File Management** interface will be displayed. See Figure 4-288.

Figure 4-288
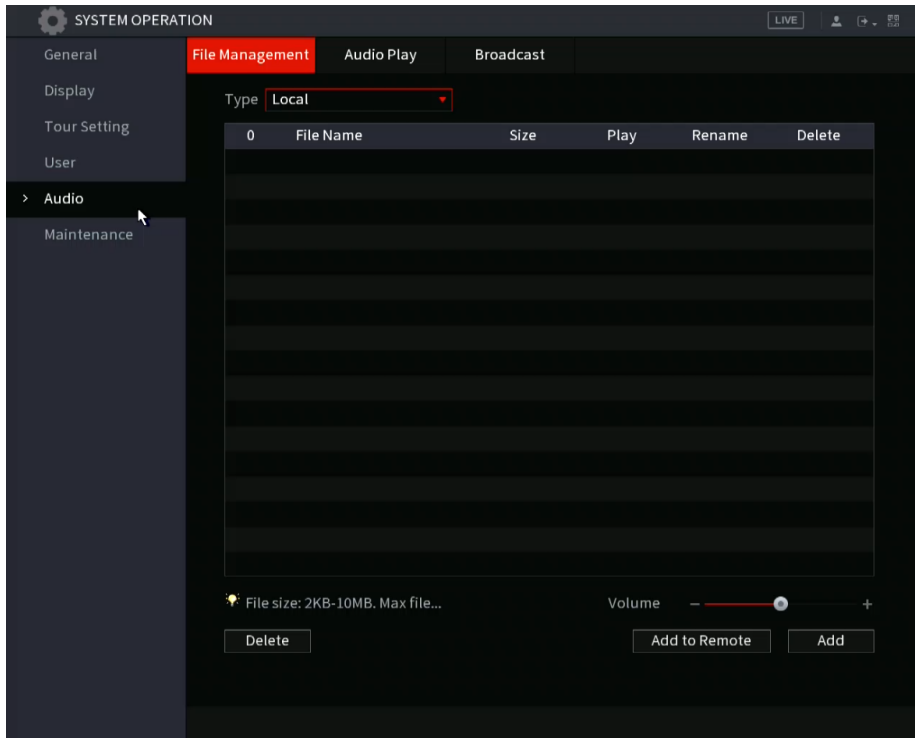
Step 2   Click **Add** to add an audio file.

The **Add** interface will be displayed. See Figure 4-289.

The local NVR interface only supports USB import for audio files.

Figure 4-289
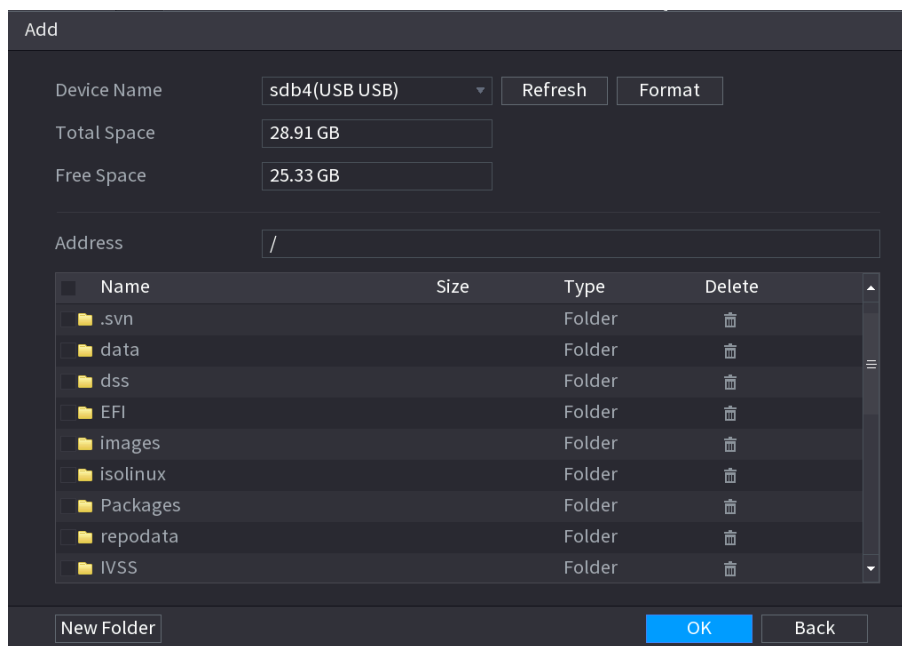
Step 3   Select the audio file and then click **Import**. The NVR supports MP3 and PCM audio format.

Step 4   Click **OK** to start importing audio files from the USB storage device.

If the importing is successful, the audio files will display in the **File Management** interface.

4.17.2 Audio Play

This section allows you to configure the settings to play the audio files during the defined time period.

Step 1   Select **Main Menu** > **Main Menu > Advanced Settings > System Operation > Audio Play**.

The **Schedule** interface will be displayed. See Figure 4-290.

Figure 4-290

Step 2   Configure the settings for the schedule parameters. See Table 4-93.

Table 4-93

Parameter	Description
Period	Select the check box to enable the settings. Enter the desired time. You can configure up to six periods.
File Name	Select the audio file that you want to play for this configured period.
Interval	Enter the time in minutes for how often you want to repeat the audio playing.
Loop	Configure how many times you want to repeat the audio playing in the defined period.
Output	The two options are: MIC and Audio. MIC is set by default. The MIC function shares the same port with talkback function and the latter has the priority. 📖 Some series NVRs do not have an audio port. The actual product shall prevail.

📖
- The finish time for audio playing depends on audio file size and the configured interval.
- Playing priority: Alarm event > Audio talk > Trial listening > Schedule audio file.
- Step 3   Click **Apply** to complete the settings.

4.18 USB Device Auto Pop-up

After you inserted the USB device, the system can auto detect it and pop up the following dialogue box. It allows you to conveniently backup files, log, configure or update the system. See Figure 4-294.
Refer to "4.18.1 File Management", "4.10.1 Log", IMP/EXP, and "4.10.4.4 System Update" for detailed information.

📖

You can add a USB keyboard through USB port, and it can input characters limited to soft keyboard.

Figure 4-294
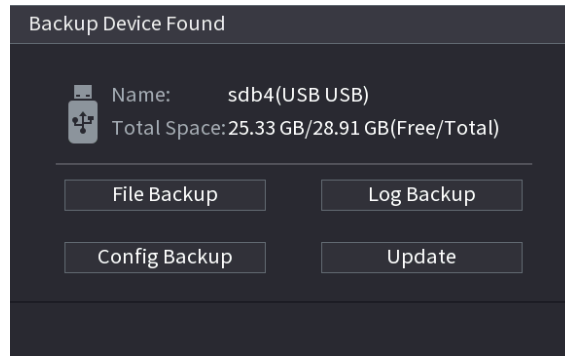
4.19 Shutdown

⚠️
● If a dialogue box appears with: "System is shutting down…" Do not switch the power on-off button.
● Do not unplug the power cable or click the power on-off button to shut down the down the device when it is running (especially when it is recording.)
● Before replace the HDD, shut down the device and then unplug the power cable.

Procedure

● From the main menu (Recommended)
   1. Click 🔼 at the top right corner. See Figure 4-295.

Figure 4-295
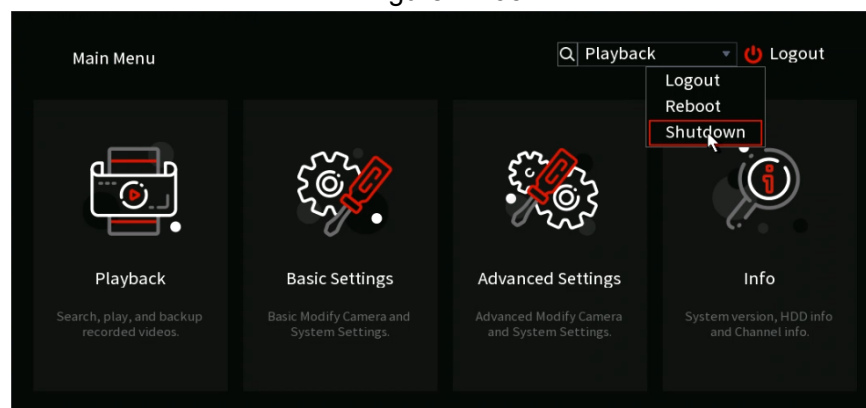
2. Select **Shutdown.**

Draw the unlock pattern or input the password first if you have no authority to shut down.

See Figure 4-296 or Figure 4-297

Figure 4-296
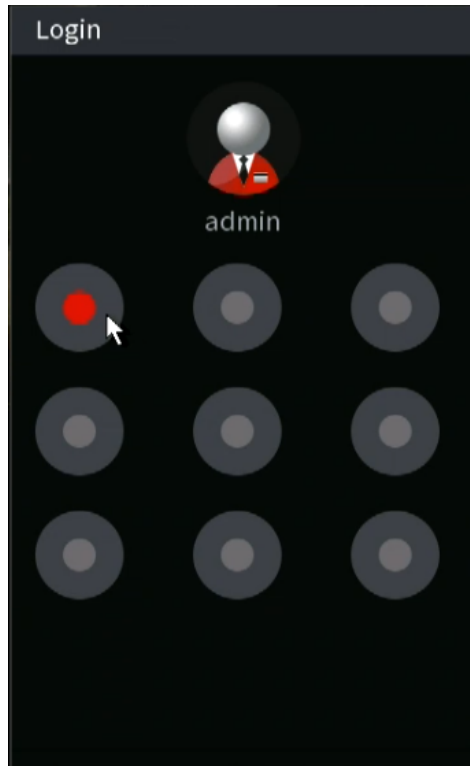
Figure 4-297
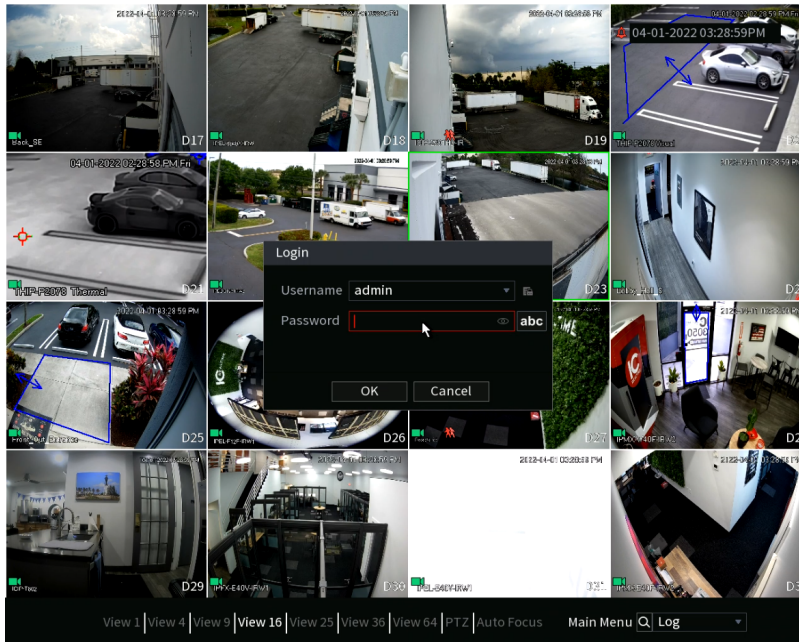
You can also shut the NVR down with these following options:

- Remote Control: Press the power button on the remote for at least 3 seconds.
- Press the power button at the rear panel of the device.

Auto Resume after Power Failure

The system can automatically backup video file and resume previous working status after power failure.

📖

- The interfaces in the Manual are used for introducing the operations and only for reference. The actual interface might be different dependent on the model you purchased. If there is an inconsistency between the Manual and the actual product, the actual product shall govern.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Besides Web, you can use our Smart PSS to login the device. For detailed information, refer to Smart PSS user's manual.

5 Web Operation

5.1 Network Connection

📖

- The NVR is set to DHCP by default. If not on a network with DHCP, the IP of the NVR is 192.168.1.199.
- The NVRs support different browsers such as Safari, Firefox, Google Chrome.

Step 1   Verify the NVR is physically connected to the network via network cable.

Step 2   Configure the IP address, subnet mask, and gateway for the PC and the Device as necessary. For details about the network configuration of the Device, refer to "4.10.3 Network".

Step 3 (Optional) On your PC, open the command prompt to check the network connection of the Device by using "ping IPAddress." (for example, ping 192.168.1.199)

Usually the return value of TTL is 255.

5.2 Web Login

Step 1   Open a web browser, then enter the IP address of the Device (keep in mind to specify the port if the HTTP port has been changed, IE: 192.168.1.199:81 if the HTTP port was changed to 81), and then press Enter.

The Login in the dialog box will be displayed. See Figure 5-1.

Figure 5-1
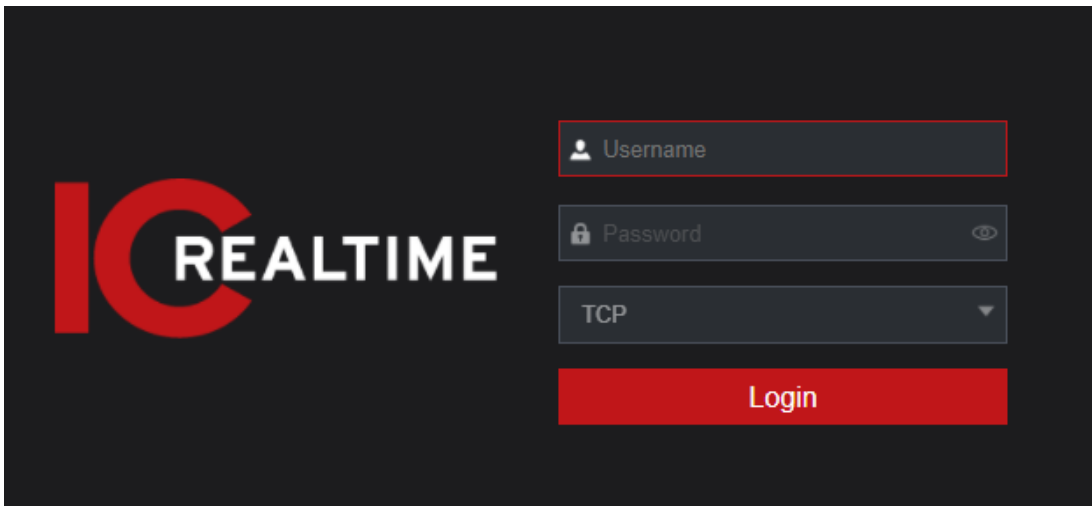
Step 2   Enter the user name and password.

The default administrator account is **admin**. The password is the created when first initializing the NVR. To secure your account, it is recommended to change the password periodically. Click ⊙ to display the password.

Step 3   Click **Login**.

5.3 Web Main Menu

Once logging into the web GUI, the main menu will be displayed. See Figure 5-2. For detailed operations, you can refer to "4 Local Basic Operation".

Figure 5-2
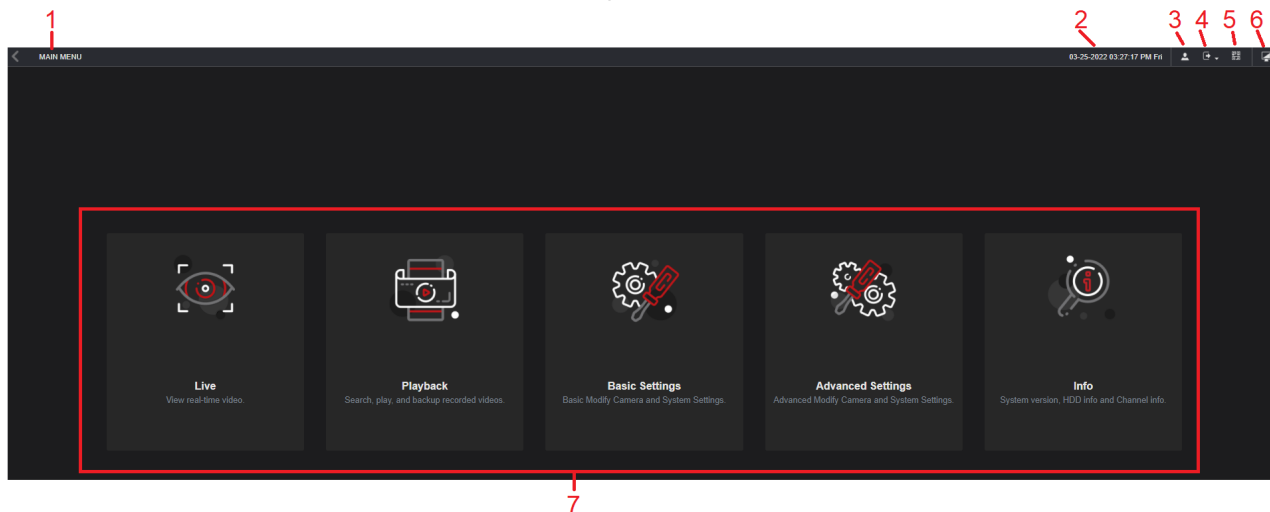
Table 5-1

No.	Icon	Description
1	▦	Opens the configuration menu to configure camera settings, network settings, storage settings, system settings, account settings, and view information.
2	None	Displays system date and time.

3		Displays the current user account being used.
4		Shutdown Menu. Select Logout, Reboot, or Shutdown according to your actual needs.
5		Displays Device SN QR Code. ● Device SN: Obtain the Device SN by scanning the QR code. For details, refer to the P2P operation manual. You can also configure P2P function in the local configurations, refer to "4.12.16 P2P".
6		Displays the web main menu.
7	N/A	Main menu icons: **LIVE, PLAYBACK, BASIC SETTINGS, ADVANCED SETTINGS AND INFO**. Click the respective icon to open the configuration interface. ● **LIVE**: For operations such as viewing real-time video, 2-way talk and, PTZ controls, etc. ● **PLAYBACK**: Search for and play back the recorded videos saved on the NVR. ● **BASIC SETTINGS**: Basic system config, Users, Display, Network, Motion Detect, and Record Schedule settings. ● **ADVANCED SETTINGS:** Camera Configuration (adding and deleting IP cams and remote devices) as well as image and encode settings for the camera, Advanced Network settings, System Operation, Alert Center (For Events such as IVS and Alarm I/O configuration), and Storage Settings. ● **INFO** View system and network information, as well as logs.

Glossary

DHCP: DHCP (Dynamic Host Configuration Protocol) is a network protocol. It is typically used to assign temporary IP addresses to computers and other devices on a network.

DDNS: DDNS (Dynamic Domain Name Server) is a service that maps Internet domain names resolve to IP addresses. This service is useful to anyone who wants to operate a server (web server, mail server, ftp server and etc) connected to the internet with a dynamic IP.

eSATA: eSATA(External Serial AT) is an interface that provides fast data transfer for external storage devices. It is an extension specification of a SATA interface.

GPS: GPS (Global Positioning System) is a satellite system, protected by the US military, safely orbiting thousands of kilometers above the earth.

PPPoE: PPPoE **(**Point to Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site. The current popular mode is ADSL, which utilizes the PPPoE protocol.

Wi-Fi: Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The standard is for wireless local area networks (WLANs). WiFi is like a common language that all the devices use to communicate to each other. It is included in the IEEE802.11, a family of standards, The IEEE (Institute of Electrical and Electronics Engineers Inc.)

3G: 3G is the wireless network standard. It is called 3G because it is the third generation of cellular telecom standards. 3G is a faster network for phone and data transmission and speed Is over several hundred kbps. There are currently four standards: CDMA2000, WCDMA, TD-SCDMA and WiMAX.

Dual-stream: Dual-stream technology utilizes a high-rate bit stream and resolution for local HD storage such as 1080P-4K for the recorded main stream and one low-rate bit sub stream for network transmission such as QCIF/CIF. This enables a balance between quality in local storage and remote network transmission which as mobile devices using 3G/4G network.

On-off value: It is the non-consecutive signal sampling and output. It includes remote sampling and remote output. It has two statuses: 1/0.

FAQ

Cannot search local records.	● HDD ribbon is damaged.
	● HDD is broken.
	● Check the record schedule configuration.
	● The recorded file has been overwritten.
	● Record function has been disabled.
Video is distorted when searching local records.	● Video quality setup is too low.
	● Program read error, data bit is too small if there is mosaic in the full screen. Restart the NVR to solve this problem.
	● Bad or damaged HDD data cable.
	● NVR hardware malfunctions.
Time display is incorrect.	● The setup is incorrect.
	● CMOS Battery contact is incorrect or voltage is too low.
Burn error /USB back error.	● NVR is using too much CPU resources. Stop recording first and then begin the backup.
	● Data amount exceeds backup device capacity. It may result in burner error.

	• Backup device is not compatible.
	• Backup device is damaged.
Network Keyboard cannot control NVR.	• NVR serial port setup is incorrect.
	• Address is incorrect.
	• Net Keyboard and NVR in different network segments.
	• Transmission distance is too far.
The alarm signal cannot be disarmed.	• Alarm setup is incorrect.
	• Alarm output has been open manually.
	• Input device error or connection is incorrect.
	• Some program versions may have this problem. Upgrade your system.
Alarm function is null.	• The alarm setup is incorrect.
	• The alarm cable connection is incorrect.
	• The alarm input signal is incorrect.
	• There are two loops connected to one alarm device.
Record storage period is not enough.	• The camera quality is too low. Lens is dirty. Camera is installed against the light. Camera aperture setup is incorrect.
	• HDD capacity is not enough.
	• HDD is damaged.
Cannot playback the downloaded file.	• There is no media player installed on PC.
	• No DXB8.1 or higher graphic acceleration software.
	• There is no DivX503Bundle.exe control when you play the file converted to AVI via media player.
	• No DivX503Bundle.exe or ffdshow-2004 1012 .exe in Windows OS.
Forgot local menu operation password or network password	Contact your local service engineer or our iCare customer support.
There is no video. The screen is in black.	• IPC IP address is incorrect.
	• IPC port number is incorrect.
	• IPC account (user name/password) is incorrect.
	• IPC is offline.
The displayed video is not full in the monitor.	Check current resolution setup. Make sure the output resolution of the NVR mathes the Monitors resolution capabilities.
There is no HDMI output.	• Display settings is not set for HDMI mode.
	• HDMI cable connection is bad/ damaged.
The video is not fluent when I view it in multiple-channel mode from the client-end.	• The network bandwidth is not sufficient. The multiple-channel monitor operation needs at least 100Mbps or higher.
	• Your PC resources are not sufficient. For 16-ch remote monitor operation, the PC requires: Quad Core, 8GB or higher memory, independent displayer, display card memory 256M or higher.

Questions	Solutions
After I set the NVR resolution as 1080P, my monitor does not display.	Login to the web GUI of the NVR to change the display output to match the monitor.
My admin account has been changed and I cannot log in.	Contact your administrator, local installer, or IC Realtime customer support.

Maintenance

- Use a brush to clean the board, socket connector, and chassis regularly.
- The device should be earthed to minimize audio/video disturbance. Keep the device away from the static voltage or induced voltage.
- Unplug the power cable before you remove the audio/video signal cable, RS232 or RS485 cable.
- Do not connect a TV to the local video output port (VOUT).It may result in a video output circuit.
- Always shut down the device properly. Use the shutdown function in the menu, or you can flip the power switch in the rear pane for at least three seconds to shut down the device. Otherwise, it may result in HDD malfunction.
- Make sure the device is away from direct sunlight or other heating sources. Keep the sound ventilation.
- Check and maintain the device regularly.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic equipment network security

1. **Use Strong Passwords**
   Please refer to the following suggestions to set passwords:
   - The length should not be less than 8 characters;

- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not use the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. **Update Firmware and Client Software in Accordingly**
- According to the standard procedure in Tech-industry, we recommend to keep your equipment (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the NVR is equipped with the latest security patches and fixes.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your equipment network security

1. **Physical Protection**

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from performing physical contacts such as damaging hardware, unauthorized connections of other equipment (such as USB flash disk, serial port), etc.

2. **Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed.

3. **Set and Update Passwords Reset Information Timely**

The NVR supports the password reset function. Set up related information for password reset and password protection questions. If the information changes, please modify accordingly. Do not use password questions that may be easy to guess.

4. **Enable Account Lock**

The account lock feature is enabled by default, we recommend you to keep it enabled to guarantee account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. **Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of unauthorized access

6. **Enable HTTPS**

We suggest you to enable HTTPS, so to allow a more secure web interface connection.

7. **Enable Whitelist**

We suggest you to enable the whitelist function to prevent everyone, except those with specified IP addresses, from accessing the NVR. If doing so, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. **Assign Accounts and Privileges Reasonably**

Add users and assign a minimum set of permissions according to business and management requirements.

10. **Disable Unnecessary Services and Select Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to

reduce risks. If necessary, it is highly recommended to use safe modes, including but not limited to the following services:

- ● SNMP: Select SNMP v3, and set up strong encryption passwords and authentication passwords.
- ● SMTP: Select TLS to access the mailbox server.
- ● FTP: Select SFTP, and set up strong passwords.
- ● AP hotspot: Select WPA2-PSK encryption mode, and set up strong passwords.

11. **Audio and Video Encrypted Transmission**

If your audio and video data contents are important or sensitive, we recommend that you use the encrypted transmission function to reduce the risk of audio and video data being stolen during transmission.

Reminder: Encrypted transmissions will cause some loss in transmission efficiency.

12. **Secure Auditing**

● Check online users: It is suggested to check online users regularly to find any unauthorized logins.

● Check equipment log: By viewing the logs, you can view the IP addresses that were used to log in to your devices and their key operations.

13. **Network Log**

Due to the limited storage capacity of the equipment, the stored log is limited. If it is necessary to saves the logs, enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

14. **Construct a Safe Network Environment**

In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

● Disable the port mapping function of the router to avoid direct access to the intranet devices from the external network.

● The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP, and other technologies to partition the network, so as to achieve the network isolation effect.

● Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

● It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

Appendix 2 HDD Capacity Calculation

Calculate total capacity needed by each device according to video recording needs(video recording type and video file storage time).

1. According to Formula (1) to calculate storage capacity q_i that is the capacity of each channel needed for each hour, unit Mbyte.

$$q_i = d_i \div 8 \times 3600 \div 1024 \qquad (1)$$

   In the formula: d_i means the bit rate, unit Kbit/s

2. After video time requirement is confirmed, according to Formula (2) to calculate the storage capacity m_i, which is storage of each channel needed unit Mbyte.

$$m_i = q_i \times h_i \times D_i \qquad (2)$$

   In the formula:

   h_i means the recording time for each day (hour)

   D_i means number of days for which the video shall be kept

3. According to Formula (3) to calculate total capacity (accumulation) q_T that is needed for all channels in the device during **scheduled video recording**.

$$q_T = \sum_{i=1}^{c} m_i \qquad (3)$$

   In the formula:

   c means total number of channels in one device

4. According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in device during **alarm video recording (including motion detection)**.

$$q_T = \sum_{i=1}^{c} m_i \times a\% \qquad (4)$$

   In the formula: $a\%$ represents alarm occurrence rate