User Manual

Network Video Recorder

Version 1.0 - March 2026

TABLE OF CONTENT

TABLE OF CONTENT **2**
1. Overview of the NVR **5**
1.1. Front Panel & Rear Panel 5
1.2 IR Remote Control Operations 11
1.3 HDD Installation 13
1.4 SSD Installation 14
1.5 IP Camera and Monitor Connection 15
1.6 Power Supply Connection 16
1.7 Input Method Description 17
2. Startup **19**
2.1 Starting Up and Shutting Down the NVR 19
2.2 Using the Startup Wizard 21
2.2.1 Log in via Password 25
2.2.2 User Logout 25
2.3 Adding the Online IP Cameras 26
2.4 Editing the Connected IP Cameras and Configuring Customized Protocols 28
2.5 Editing IP Cameras Connected to the PoE Interfaces 29
3. Live View **33**
3.1 Introduction of Live View 33
3.2 Operations in Live View Mode 34
3.3 Quick Setting Toolbar in Live View Mode 34
3.4 Desktop Shortcut Menu 36
4. Playback **39**
4.1 GUI Introduction 39
4.2 Normal Playback 40
4.3 Event Playback 44
4.4 Back up Clip 45
5. Backup **47**
6. Configuration (Common Mode) **48**
6.1 System Configuration 48
6.1.1 System - Base 48
6.1.2 User 49
6.1.3 Alarm Events & Trigger Process 50
6.2 Network Configuration 52
6.2.1 General - TCP/IP 52
6.2.2 LEGEND-P2P 53
6.2.3 Email 55
6.3 Camera Management 57
6.3.1 Network Camera 57
6.3.2 OSD Settings 62
6.3.3 Event 63
6.3.4 Configure Arming Schedule 70

6.3.5 Configure Alarm Trigger Process....70
6.3.6 Configure Advanced Setting....72
6.4 Recording Management....73
6.4.1 Storage....73
6.4.2 Configure Recording Schedule....75
6.4.3 Configuring Video Encoding....79
7. Maintenance....82
7.1 Restore Default....82
7.2 Search Log....83
7.3 Upgrade....84
7.3.1 Local Upgrade....84
7.3.2 Online Upgrade & The Version....85
8. Alarm Status & Show Message....87
8.1 Alarm Log....87
8.2 View Alarm in Show Message....87
9. Web Operation....89
9.1 Introduction....89
9.2 Login....89
9.3 Preview....90
9.4 Playback....90
9.5 Set....91
9.6 Log....91
10. Configuration (Advanced Mode)....92
10.1 System Configuration....92
10.1.1 Basic Settings....92
10.1.2 Security....95
10.1.3 Maintenance....98
10.1.4 Display setting....99
10.1.5 Reminder....102
10.1.6 Config....103
10.1.7 Hot Standby....105
10.2 Network Configuration....108
10.2.1 TCP/IP....108
10.2.2 NTP....109
10.2.3 Email & P2P....110
10.2.4 Network State....111
10.2.5 Advanced....112
10.2.6 Transfer....118
10.2.7 Wireless....120
10.3 Camera Management....122
10.3.1 IP Channel....122
10.3.2 Encode....125
10.3.3 Color....128
10.3.4 OSD....132

10.3.5 PTZ..... 135
10.4 Event Configuration..... 137
10.4.1 Normal Event..... 137
10.4.2 Alarm Port..... 139
10.4.3 Intelligent Detection..... 144
10.4.4 System Alert..... 150
10.4.5 RAID..... 152
10.4.6 Exception Alarm..... 157
10.4.7 Alarm Log..... 159
10.5 Storage Management..... 160
10.5.1 Base - Storage Device..... 160
10.5.2 Storage Mode..... 160
10.5.3 Configure Recording Schedule..... 165
10.5.4 Record Status..... 165
10.5.5 Advanced Settings..... 165
10.5.6 S.M.A.R.T..... 166
10.6 Smart Search..... 168
10.6.1 Smart Search..... 168
10.7 Playback..... 172
10.7.1 Normal Playback & Event Playback..... 172
10.7.2 Label Play..... 172
10.7.3 Smart Play..... 174
10.7.4 Time Division Playback..... 181
10.7.5 Normal Play (Picture)..... 182
11. Appendix..... 184
11.1 Glossary..... 184
Legal Information..... 186
About This Manual..... 186
Trademarks..... 186
Disclaimer..... 186
FCC Information..... 187
FCC Compliance..... 187
FCC Conditions..... 187
Safety Instructions..... 188
Preventive and Safety Guidelines..... 188

1. Overview of the NVR

1.1. Front Panel & Rear Panel

The NVR front panel is shown in Figure 1-1 to Figure 1-5.

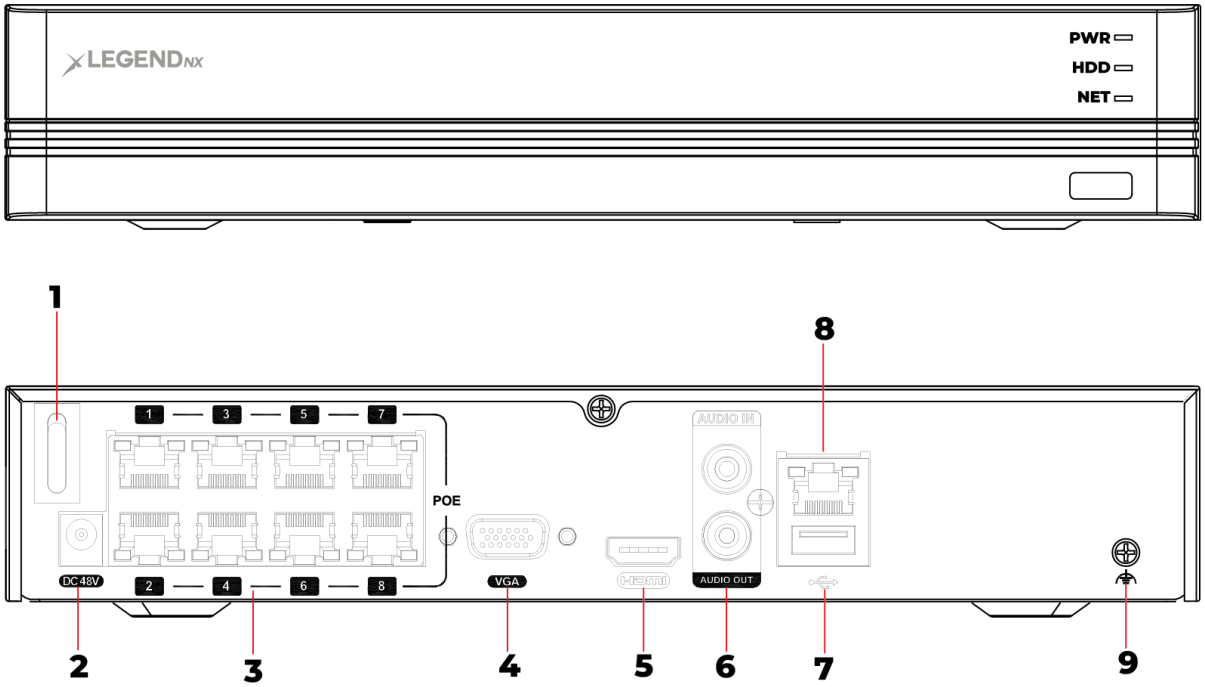


Figure 1-1 Front & Rear panel of the LGNX884KN & LGNX884KLN

Table 1-1 Description of the rear panel

No.	Function Description
1	Power Switch
2	Power Input
3	PoE Network Port
4	VGA Port
5	HDMI Port
6	Audio IN/OUT RCA
7	USB Port
8	Network Port
9	Ground

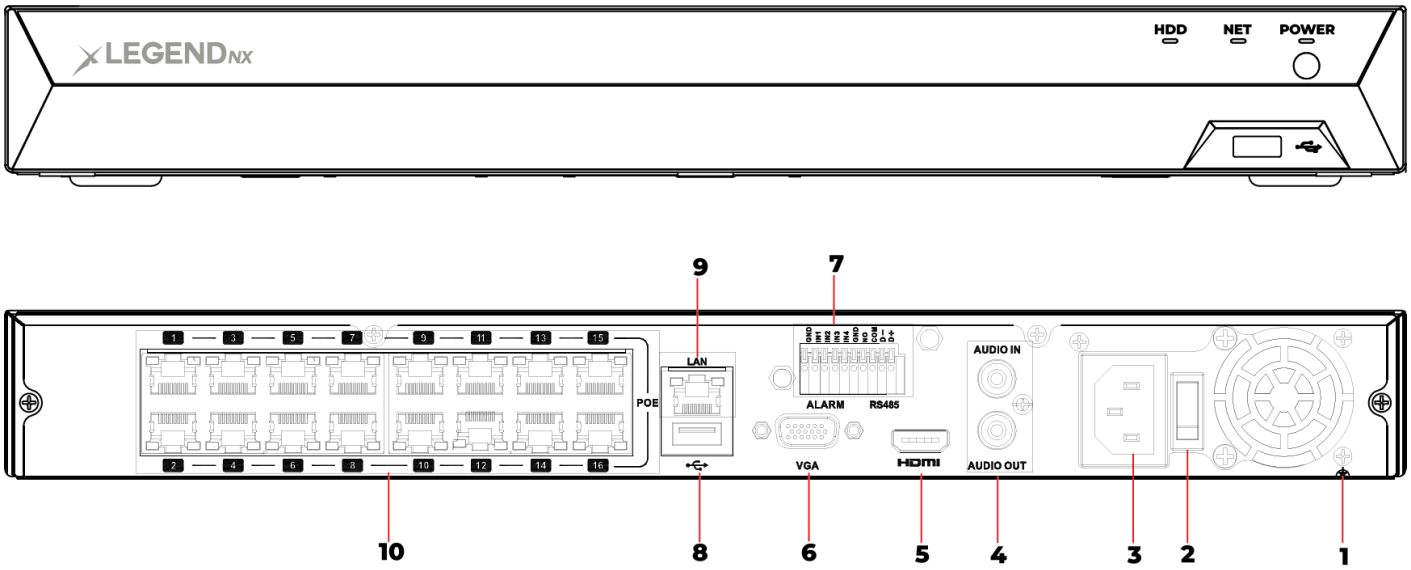


Figure 1-2 Front & Rear panel of LGNX16164KN

Table 1-2 Description of the rear panel

No.	Function Description
1	Ground
2	Power Switch
3	Power Input
4	Audio Input/Output RCA
5	HDMI Port
6	VGA Port
7	Alarm Input
8	USB Port
9	Network Port
10	PoE Network Port

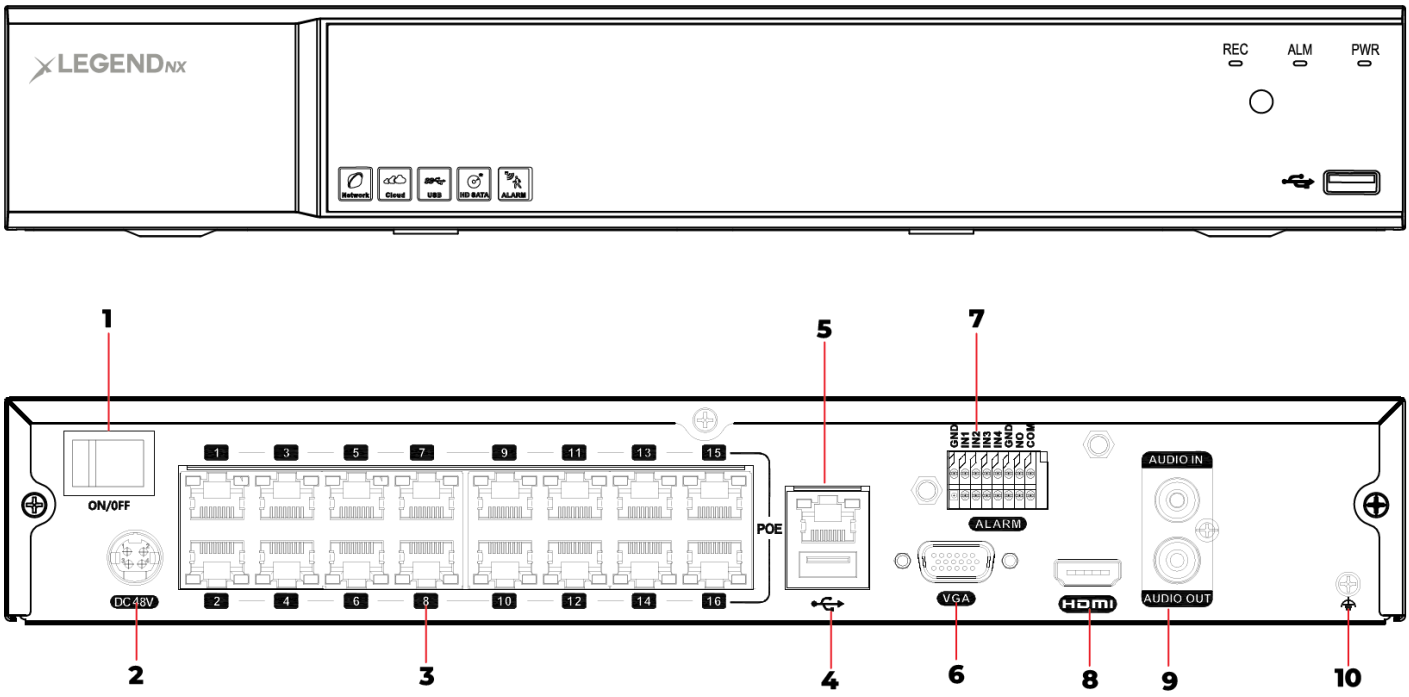


Figure 1-3 Front & Rear panel of LGNX16164KLN

Table 1-3 Description of the rear panel

No.	Function Description
1	Power Switch
2	Power Input
3	PoE Network Port
4	USB Port
5	Network Port
6	VGA Port
7	Alarm Input
8	HDMI Port
9	Audio Input/Output RCA
10	Ground

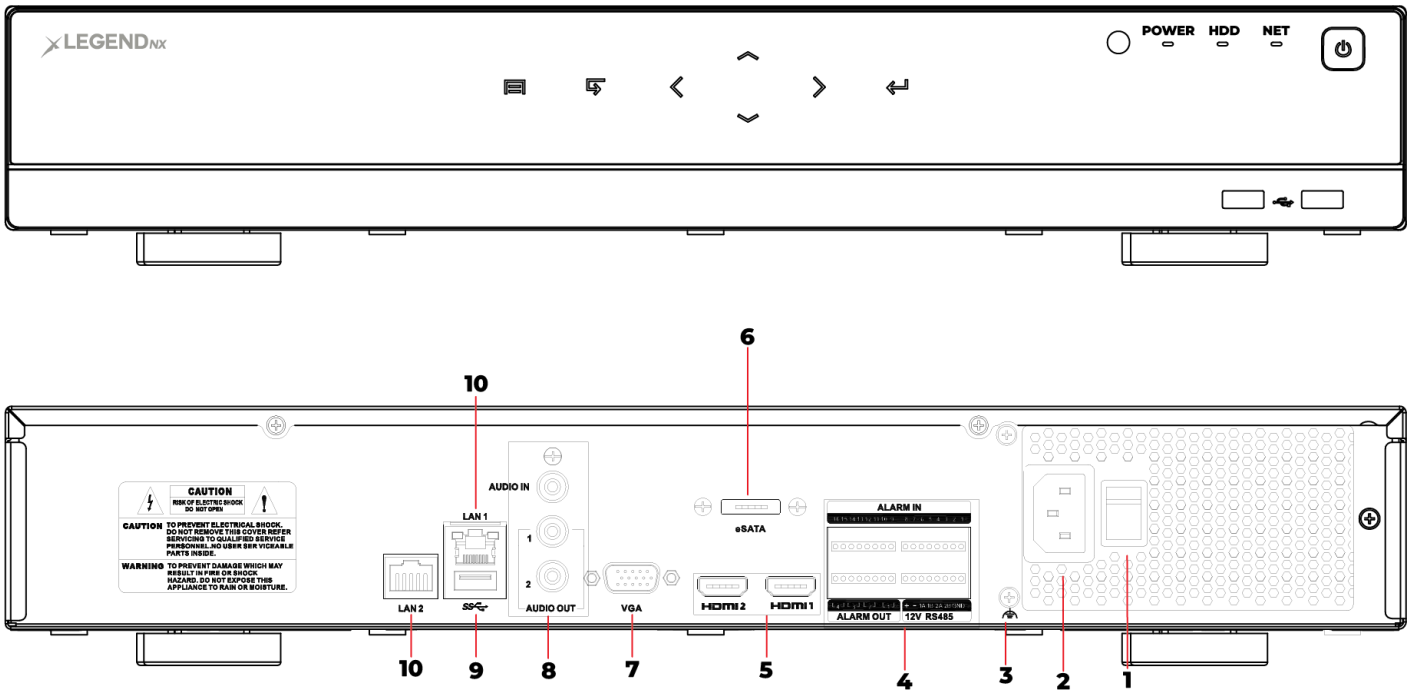


Figure 1-4 Front & Rear panel of LGNX324KN

Table 1-4 Description of the rear panel

No.	Function Description
1	Power Switch
2	Power Input
3	Ground
4	Alarm Input
5	HDMI Port
6	eSATA Port
7	VGA Port
8	Audio Input/Output RCA
9	USB Port
10	Network Port

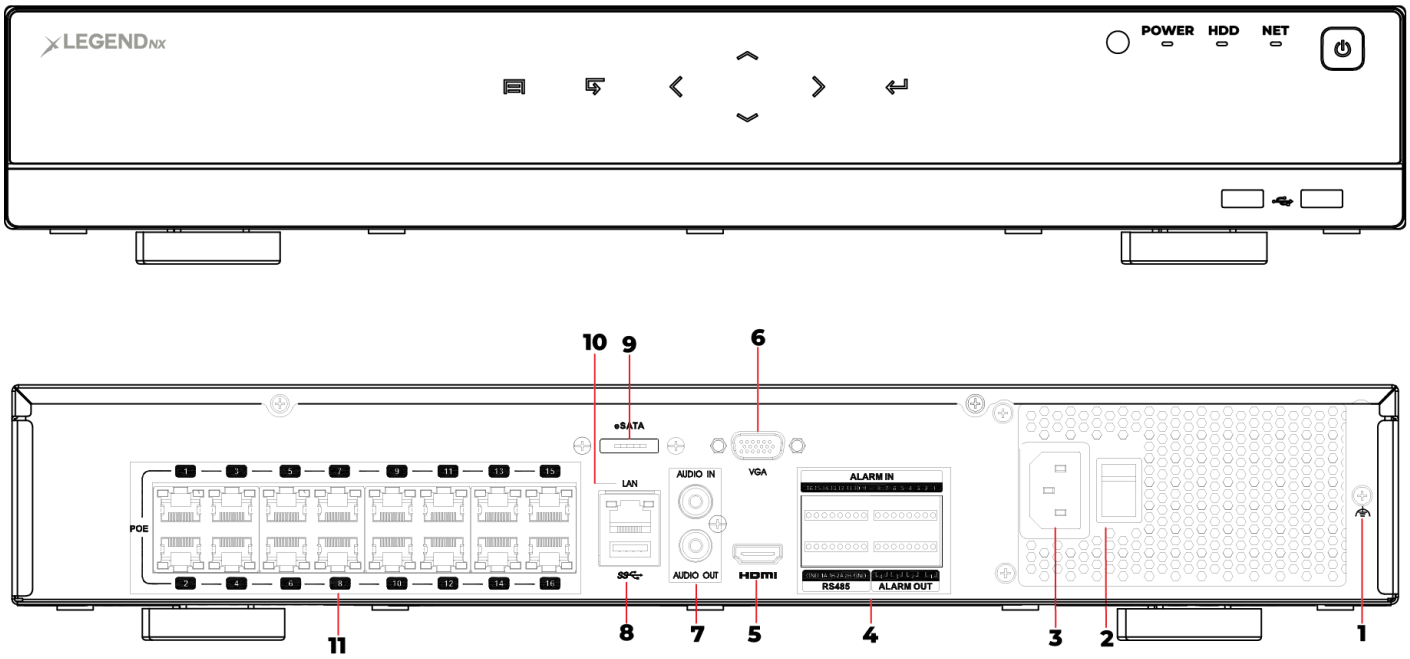


Figure 1-5 Front & Rear panel of LGNX32164KN

Table 1-5 Description of the rear panel

No.	Function Description
1	Ground
2	Power Switch
3	Power Input
4	Alarm Input
5	HDMI Port
6	VGA Port
7	Audio Input/Output RCA
8	USB Port
9	eSATA Port
10	Network Port
11	PoE Network Port

Figure 1-6 Front & Rear panel of LGNX644KN.

Table 1-6 Description of the rear panel

No.	Function Description
1	Power Switch
2	Power Input
3	Ground
4	Alarm Input
5	HDMI Port
6	eSATA Port
7	VGA Port
8	Audio Input/Output
9	USB Port
10	Network Port

Note

All drawings shown above are for reference purposes only

1.2 IR Remote Control Operations

The NVR can also be controlled using the included IR remote control, as shown below. Batteries (2 × AAA) must be installed before operation. The IR remote control is factory-configured to operate the NVR (using the default Device No.) without any additional setup.

Steps

The Device No. is the default universal device identification number shared by the NVRs.

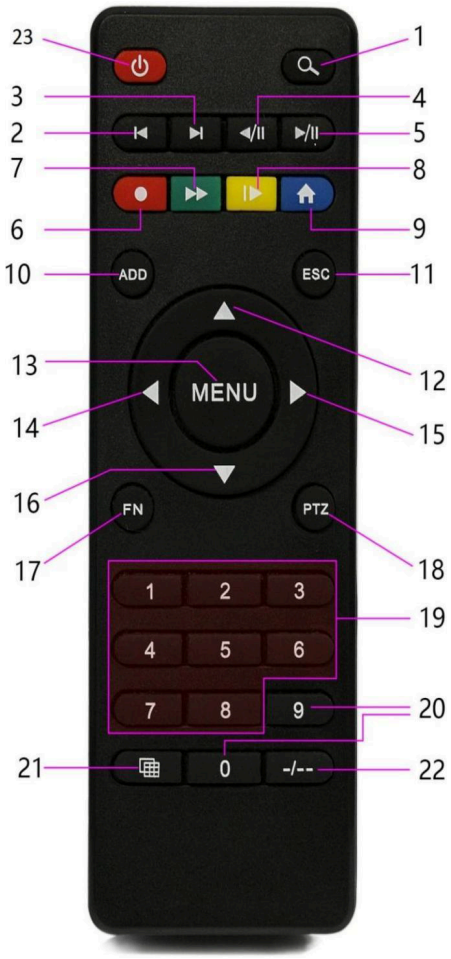


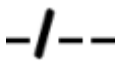
Figure 1-7 Remote Controller

Note

The remote control is only compatible with 6-series NVRs.

Table 1-7 Description of IR Remote Control

No.	Item	Description
1		Enter the Playback Interface
2		Backward One Frame

3		Control Step Frame
4		Backward Playback Control Button
5		Control Playback Status
6		Quick Control of All Channels Record Type
7		Control Playback Speed
8		Slow Down Playback
9		Back to Preview
10	ADD	Set Address to Match the NVR
11	ESC	Back to Preview
12/16		Select Function Area in the Menu / Switch Preview Channels
14/15		Select Function Area in the Menu / Switch Preview Channels
13	MENU	Enter the Main Menu
17	FN	Switch Control Area
18	PTZ	Quick Access to PTZ Control
19/20	Number Area	Enter Numbers / Switch Preview Channels
21		Switch Preview Channel Number
22		Enter Number Digits Sequentially
23	Shutdown	Shutdown / Restart / Logout / Switch User

1.3 HDD Installation

Before installing the hard disk (HDD), ensure that the NVR is powered off and disconnected from the power supply. Refer to the NVR specifications for supported HDD capacities. An NVR without an installed HDD can still support live monitoring, but recording and playback functions will not be available. If the HDD is installed correctly, the HDD indicator will blink regularly when the NVR is operating.

Turn off the power before starting the HDD installation. The installation images are for reference only.

1 or 2 HDD(s) NVRs

Figure 1-8 Remove the cover

Figure 1-9 Install the HDD

Figure 1-10 Connect the power and data cables

Figure 1-11 Install the cover and screws

4 or 8 HDD(s) NVRs

Figure 1-12 Remove the cover

Figure 1-13 Connect the power and data cables

Figure 1-14 Install the HDD

Figure 1-15 Install the cover and screws

1.4 SSD Installation

Before installing the solid-state drive (SSD), ensure that the NVR is powered off and disconnected from the power supply. Refer to the NVR specifications for supported SSD capacities. An NVR without an installed storage device can still support live monitoring, but recording and playback functions will not be available. If the SSD is installed correctly, the SSD indicator will blink regularly when the NVR is operating.

Turn off the power before starting the SSD installation. The installation images are for reference only.

Figure 1-16 Remove the cove

Figure 1-17 Install the SSD

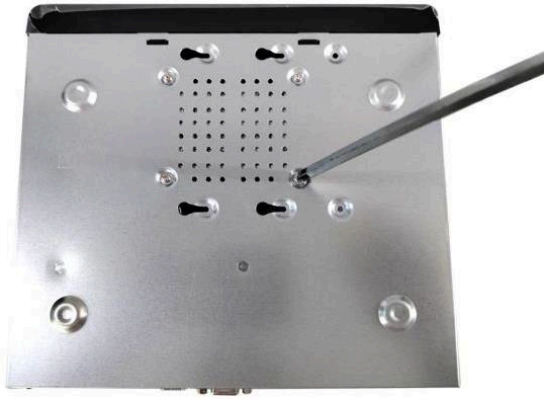


Figure 1-18 Connect the power and data cables

Figure 1-19 Install the cover and screws

Note

• If higher HDD performance is required, it is strongly recommended to use a dedicated surveillance-grade hard drive.

• Do not remove the hard drive while the NVR is operating.

1.5 IP Camera and Monitor Connection

Transmit the IP camera signal to the NVR using a network cable, and connect the VGA port and HDMI port for video output.

Note

This may not be applicable to all installation environments.

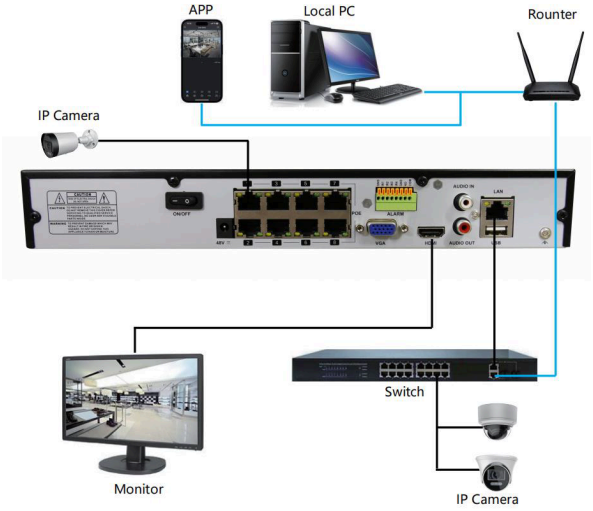


Figure 1-20 Device connection

1.6 Power Supply Connection

Use the supplied power adapter to connect the NVR. Before powering on, ensure that the cables connected to the audio I/O ports and the network port are securely connected.

Figure 1-21 Power Supply Connection

Table 1-8 Key Functions of USB Mouse Operation

Items	Action	Description
Left-Click	Single-Click	Live view: Select a channel and display the quick settings menu. Menu: Select and confirm.
	Double-Click	Live view: Switch between single-screen and multi-screen display.
	Click and Drag	Live view: Drag channel/time bar. Alarm: Select target area. Digital zoom: Drag to select the target area.
Right-Click	Single-Click	Live view: Display the main menu. Menu: Exit the current menu and return to the previous level.

Left & Right Click	Simultaneous Click	Press and hold for 5 seconds to switch the device resolution to the lowest setting.
Scroll Wheel	Scroll Up	Menu: Increase the setting value.
	Scroll Down	Menu: Decrease the setting value.

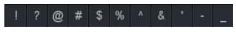
1.7 Input Method Description

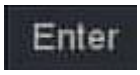
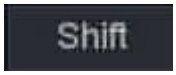
Figure 1-22 Soft keyboard (1)

Figure 1-23 Soft keyboard (2)

Figure 1-24 Soft keyboard (3)

Table 1-9 Description of the Soft Keyboard Icons

Icon	Description
	Symbols
	Number

	Enter
	
	English letters
	Backspace
	Switch between lowercase and uppercase

2. Startup

2.1 Starting Up and Shutting Down the NVR

Purpose

Proper startup and shutdown procedures are essential for extending the service life of the NVR.

Before you start

Ensure that the voltage of the external power supply matches the NVR requirements and that the grounding connection is functioning properly.

Starting up the NVR

Steps:

1. Verify that the power supply is connected to an electrical outlet. It is highly recommended to use an Uninterruptible Power Supply (UPS) with the device. The power indicator LED on the front panel should be on, indicating that the device is receiving power.
2. Turn on the power switch on the rear panel if this is the first startup, or press the power button on the front panel (if applicable). The power indicator LED will blink or remain steadily on, indicating that the unit is starting up.
3. After startup, a beep will be heard and the power indicator LED will remain on. A startup screen displaying HDD status will appear on the monitor. The row of icons at the bottom of the screen indicates HDD status. An “X” indicates that the HDD is not installed or cannot be detected.

Shutting down the NVR

Steps:

1. Right-click and open the **Shutdown** menu.
2. Navigate to **Quick Menu** → **Shutdown**

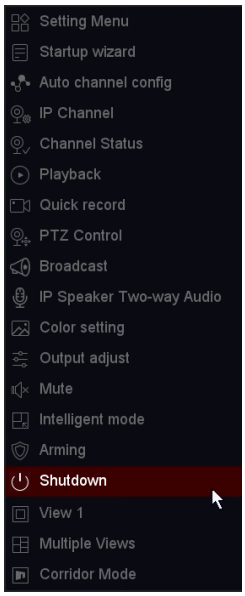


Figure 2-1 Quick Menu

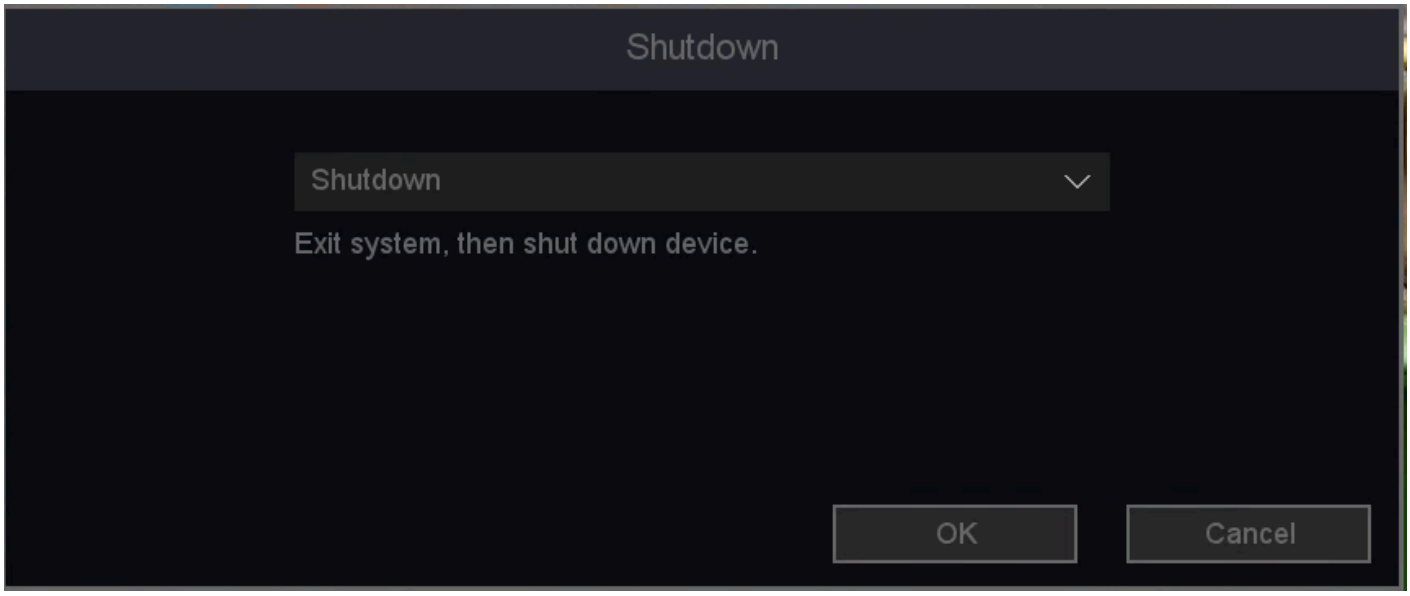


Figure 2-2 Shutdown Menu

3. Select **Shutdown** from the drop-down list.
4. Click the **OK** button.

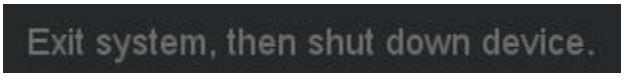


Figure 2-3 Shutdown Notice

Rebooting the NVR

In the Shutdown menu, you can also reboot the NVR.

Steps:

1. Right-click and open the Shutdown menu by selecting **Menu → Shutdown**.
2. In the drop-down list, select **Logout** to lock the NVR or **Reboot** to restart the NVR.

2.2 Using the Startup Wizard

Steps:

1. By default, the **Startup Wizard** launches automatically after the NVR has started, as shown below.

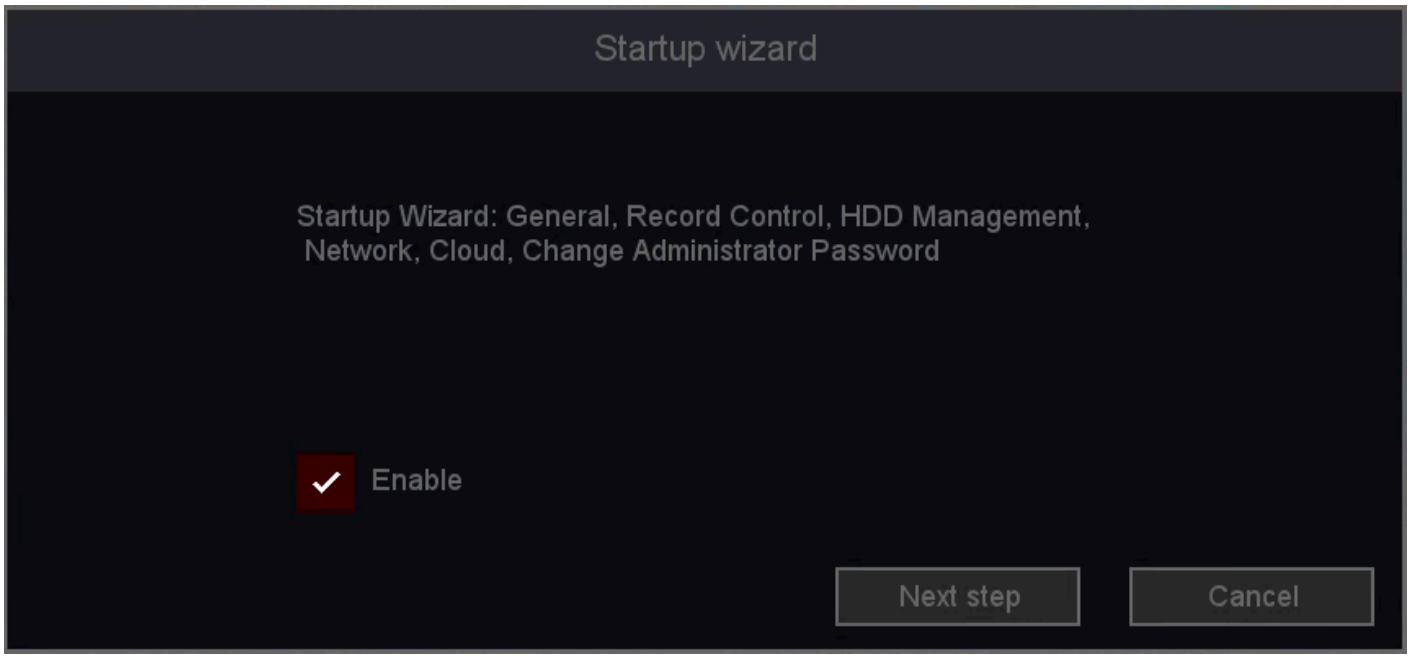


Figure 2-4 Startup Wizard

Note
The Startup Wizard guides you through key NVR settings. If you do not wish to use it at this time, click **Exit**. You can enable it for the next startup by keeping the **Enable** checkbox selected.

2. Click **Next Step** to open the **Set Administrator Password** window.

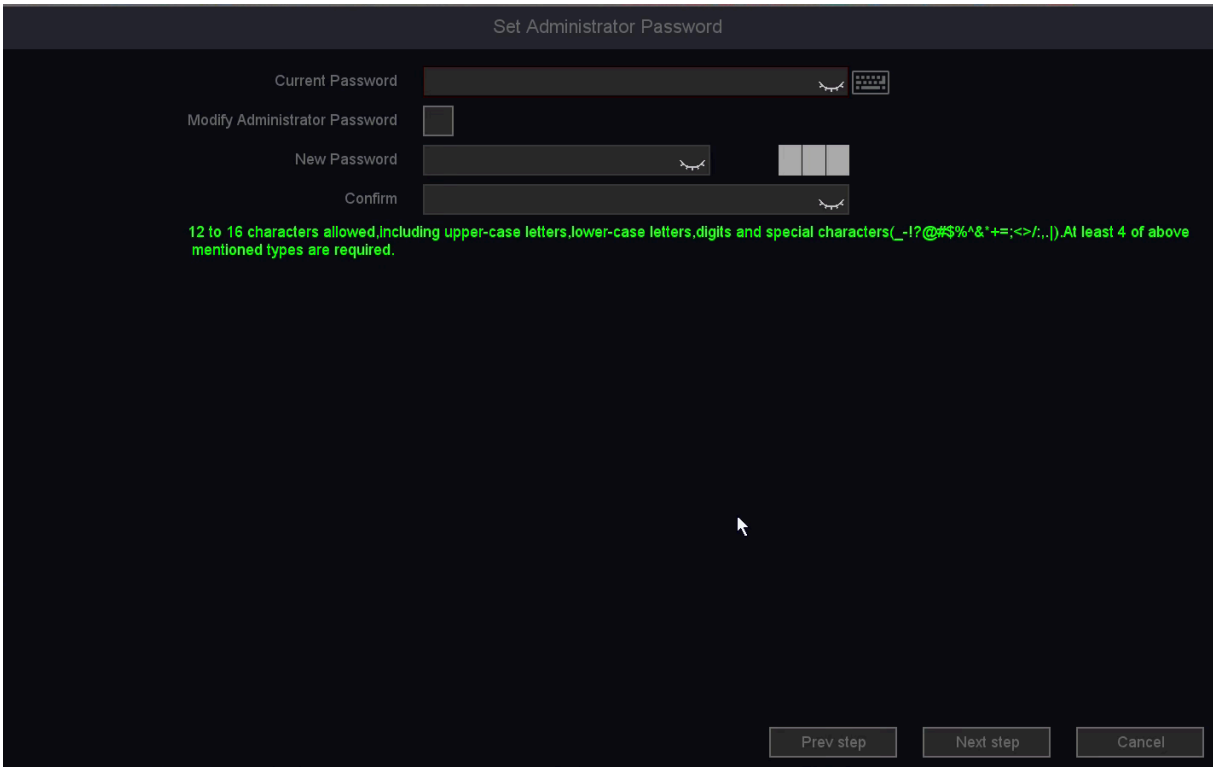


Figure 2-5 Set Administrator Password

3. Click **Next Step** to enter the general settings window, as shown below.

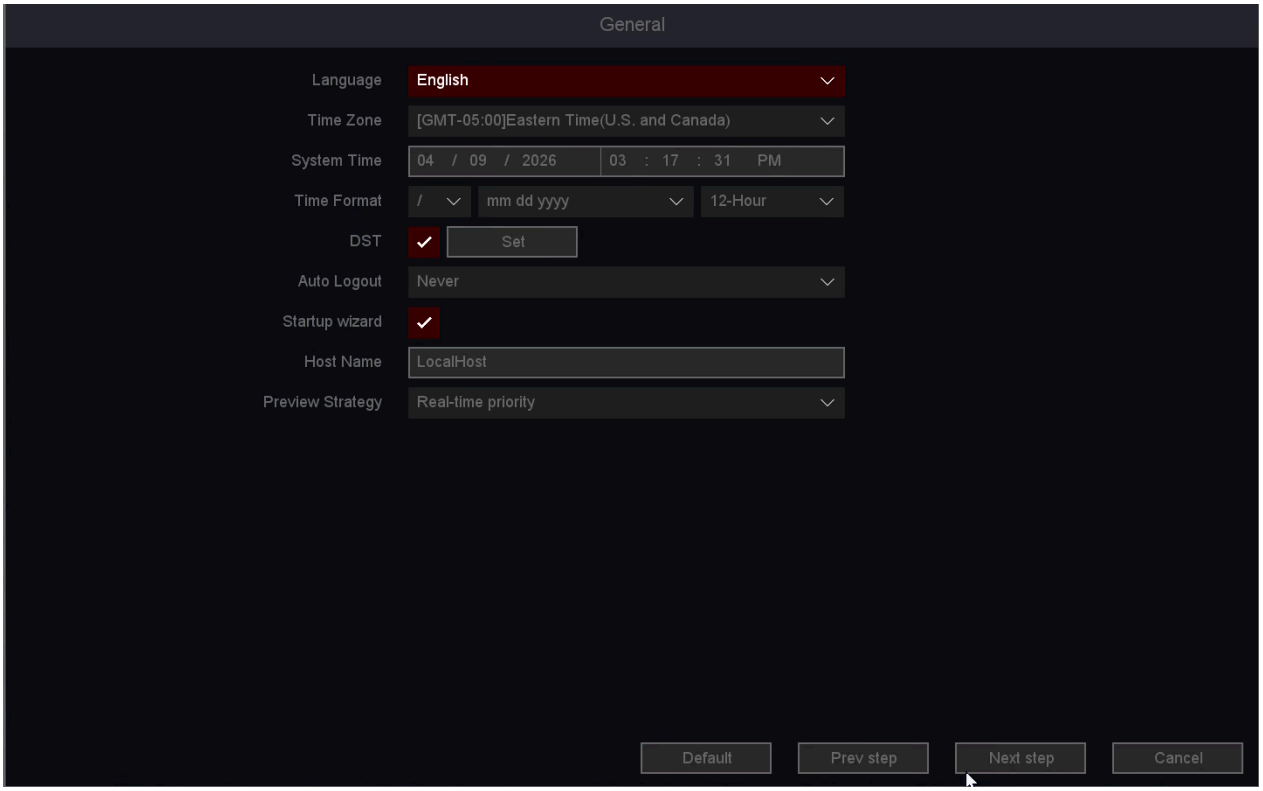


Figure 2-6 General

4. After configuring the general settings, click **Next Step** to proceed to the **Record Control Setup Wizard** window, as shown below.

Figure 2-7 Record

5. After configuring the record control settings, click **Next Step** to proceed to the **HDD Management Setup Wizard** window, as shown below.

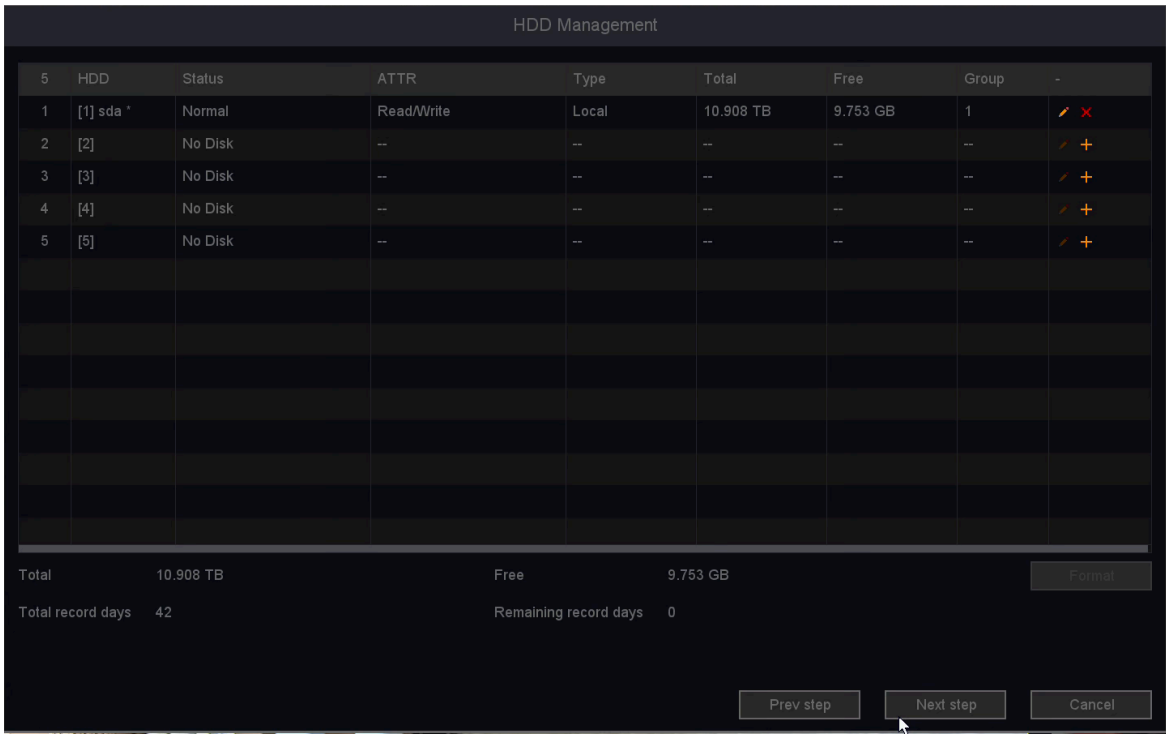


Figure 2-8 HDD Manage

6. Click **Next Step** to enter the **Network Setup Wizard** window, as shown below.

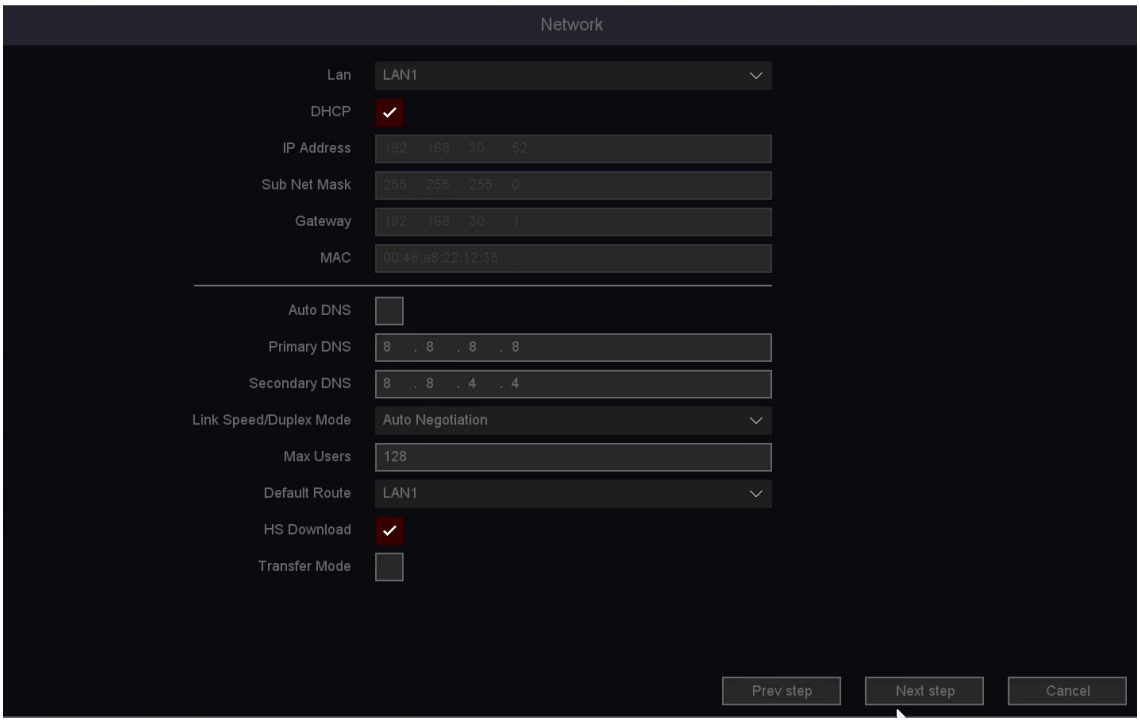


Figure 2-9 Network

7. After configuring the network parameters, click **Next Step** to enter the **Cloud Service Setup Wizard** window, as shown below.

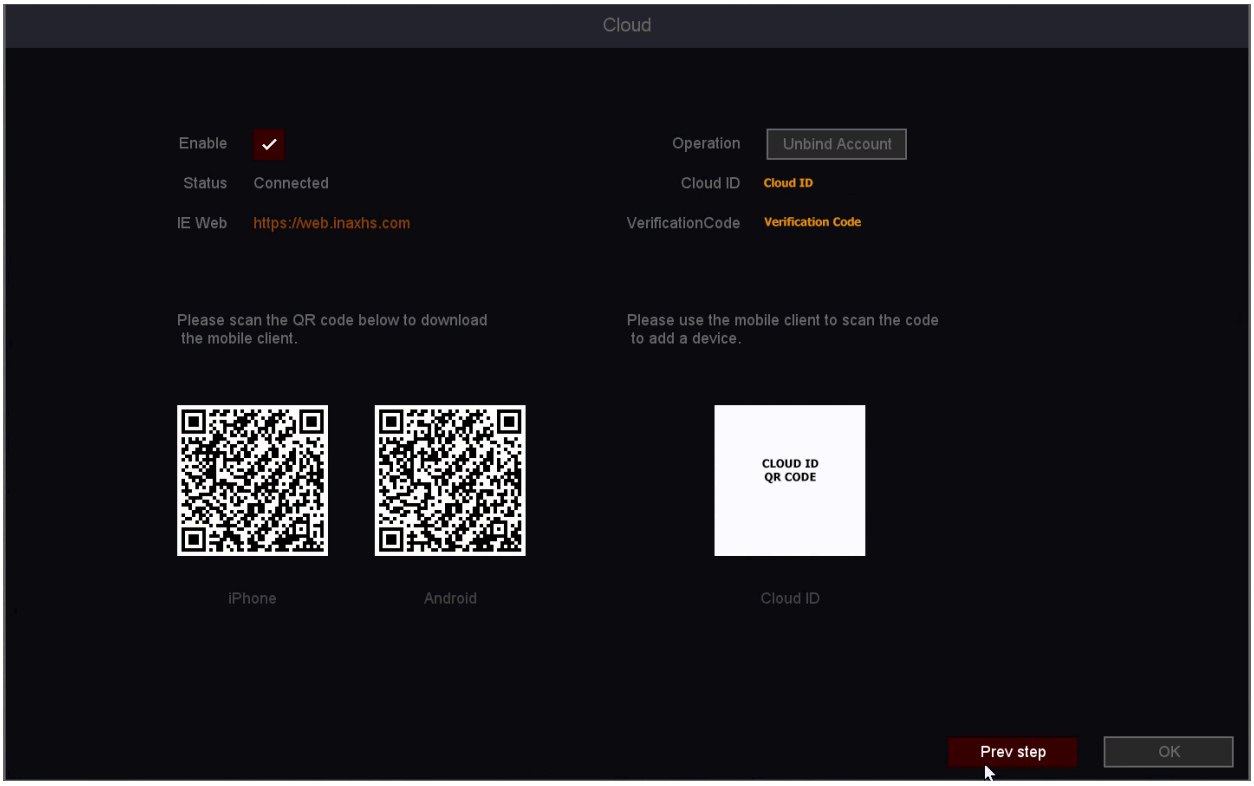


Figure 2-10 Cloud

8. Click **Finish** to complete the Startup Setup Wizard.

2.2.1 Log in via Password

If the video recorder is logged out, you must log in before accessing the menu and other functions.

Steps:

1. Select **User Name**.

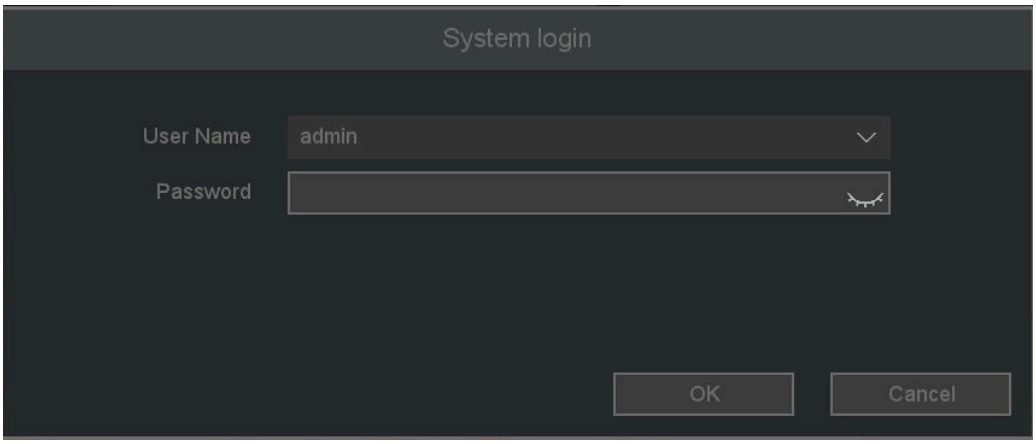


Figure 2-11 Login Interface

2. Enter the password.
3. Click **OK**.

Note

• The default username and password are **admin / 123456**.
• If you forget the administrator password, contact your installer to reset it.
• If an incorrect password is entered six consecutive times, the user account will be locked for 15 minutes.

2.2.2 User Logout

After logging out, the monitor returns to live view mode. To perform any operations, you must log in again using your username and password.

Steps:

1. Right-click on the live view screen and open the **Shutdown** menu, or click the **Shutdown** option in the upper-right corner of the settings interface.
2. Select **Logout** from the drop-down list.
3. Click **OK**.

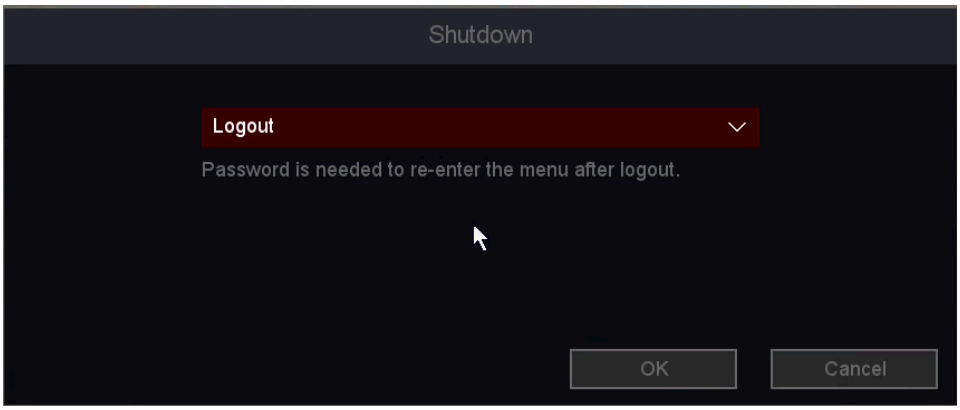


Figure 2-12 Logout

Note

• After logging out, all menu operations are disabled. You must enter a valid username and password to unlock the system.

2.3 Adding the Online IP Cameras

The primary function of the NVR is to connect to network cameras and record their video streams. Before viewing live video or playback, you must add the network cameras to the device's connection list.

Before you start:

Ensure that the network connection is properly configured and functioning. For detailed instructions, refer to the chapters on network checking and network configuration.

Adding the IP Cameras

OPTION 1:

Steps:

1. Select **IP Channel** from the right-click menu, or click the **+** icon in live view mode to open the IP camera management interface.
2. Click the **Search** button. Cameras within the same network segment will be detected and displayed in the camera list.

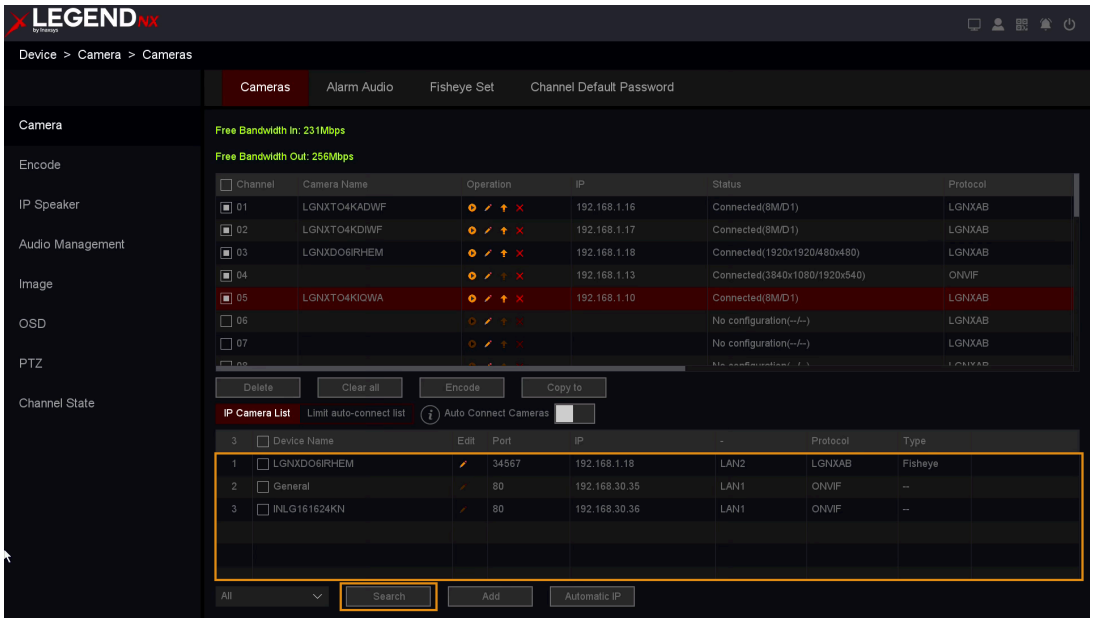


Figure 2-13 IP Camera Management

3. Select the desired IP camera from the list and click **Add** to add the camera.

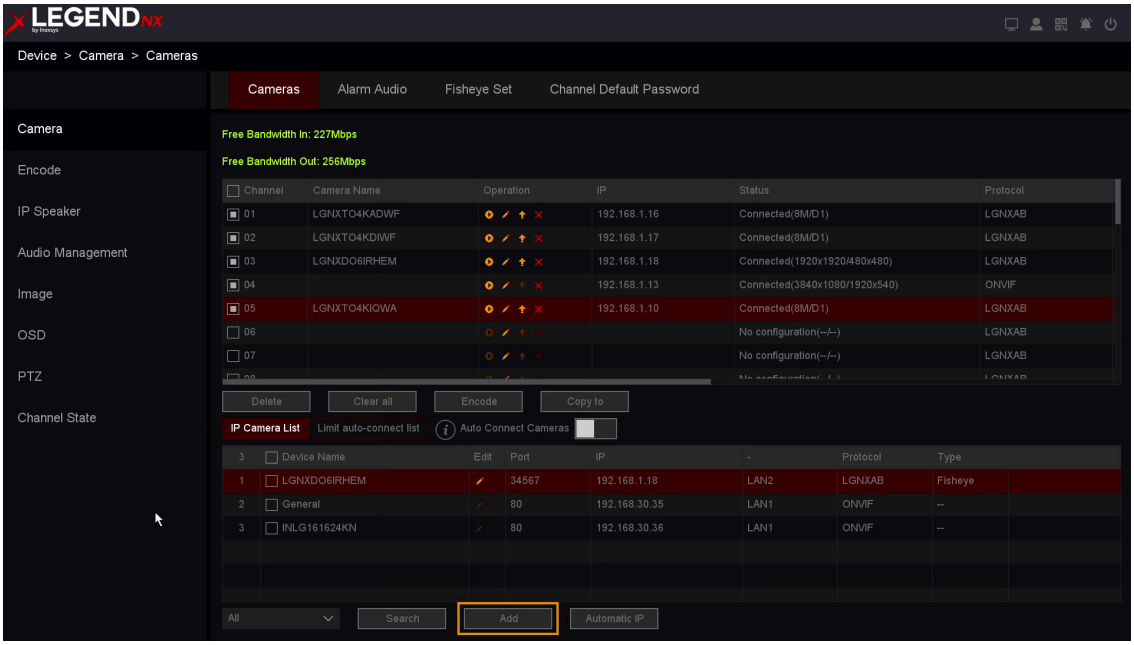


Figure 2-14 Add Camera

4. Check the camera status:

- **Connected**: The camera is successfully connected.
- **Connecting**: The connection is in progress.
- **Authentication Error**: The password is incorrect.

If the status is not **Connected**, verify the connection settings to ensure the camera can connect properly.

Note

• If the camera does not display in the selected position after double-clicking, delete the connection by clicking the red **"X"**, then double-click the IP address to add it again.

View live video from the camera	Edit basic camera parameters	Upgrade the camera firmware	Delete the IP camera

OPTION 2:

Steps:

1. In the IP Camera Management interface, click the **Edit** icon to open the **Edit IP Camera (Custom)** window.
2. If the password is incorrect, enter the correct username and password. If the status shows **Connecting**, adjust the port or protocol settings.

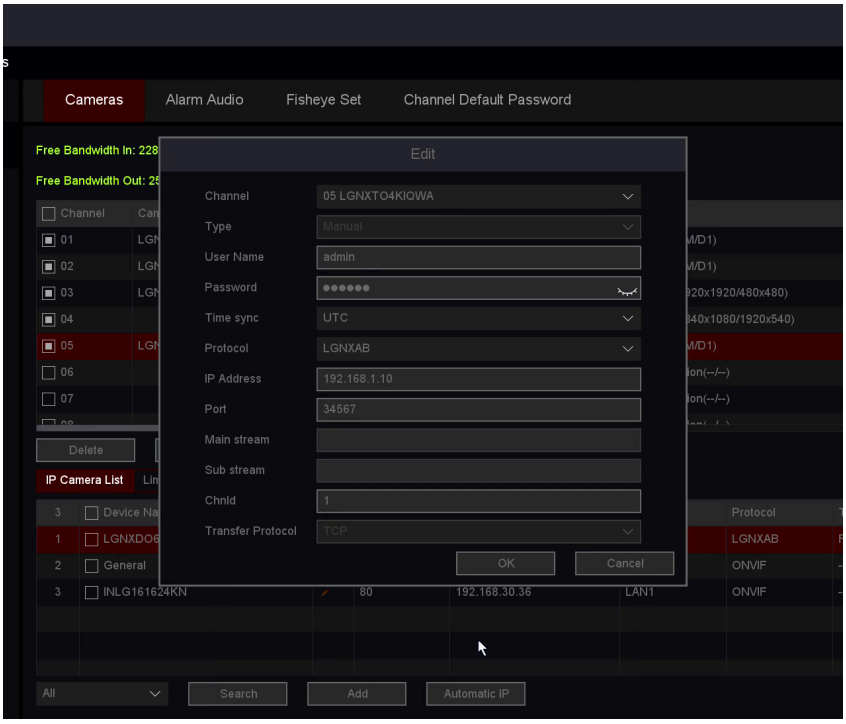


Figure 2-15 Edit

2.4 Editing the Connected IP Cameras and Configuring Customized Protocols

After adding the IP cameras, the basic information of the cameras is displayed on the page. You can configure the basic settings of the IP cameras.

Steps:

1. Click the **Edit** icon  to modify parameters such as IP address, username, password, port, and other settings.

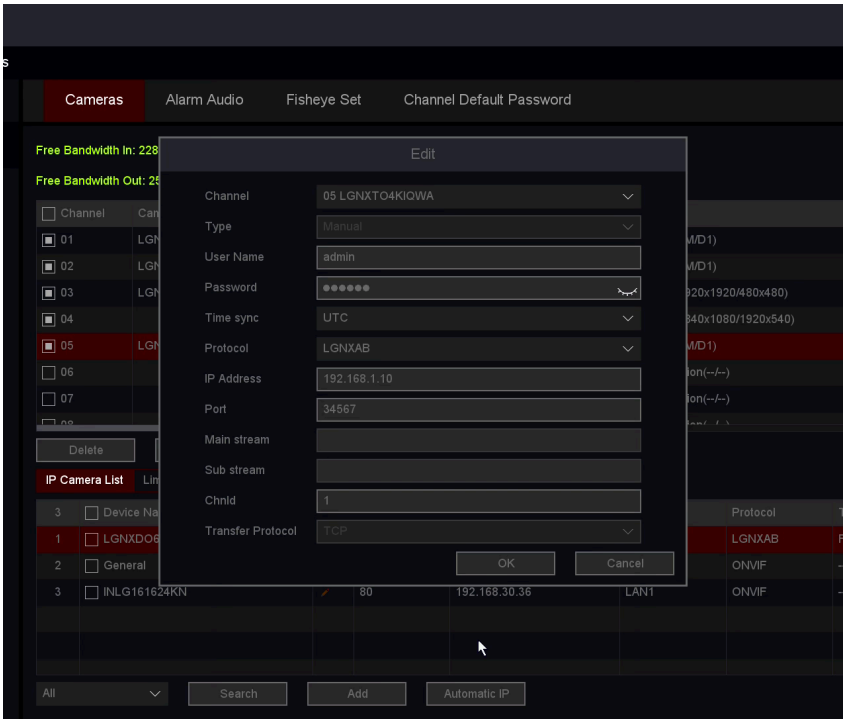


Figure 2-16 Edit

2. Click the **Protocol** drop-down list. You can select from three protocols: **LGNXAB**, **Onvif**, and **RTSP**. **LGNXAB** is a private protocol, while **Onvif** and **RTSP** are mainly used for connecting third-party cameras.
3. Click **OK** to save the settings and exit the editing interface.

2.5 Editing IP Cameras Connected to the PoE Interfaces

The PoE interfaces allow the NVR to supply power and transmit data to connected IP cameras through Ethernet cables. Up to 8 IP cameras can be connected to 8P models, and up to 16 IP cameras to 16P models. If the PoE interface is disabled, the NVR can still connect to cameras over the network. The PoE interface also supports plug-and-play functionality.

To add cameras for NVRs supporting PoE:

Before you start: Connect the network cable from the IP camera to the PoE port of the NVR.

Steps:

1. Go to **Main Menu** → **Camera** → **IP Camera** → **Camera Setting**.

Note
You can also select **IP Channel** from the right-click menu or click the **+** icon in live view mode to access the IP camera management interface.

2. Click the **Edit** icon  for the selected channel.

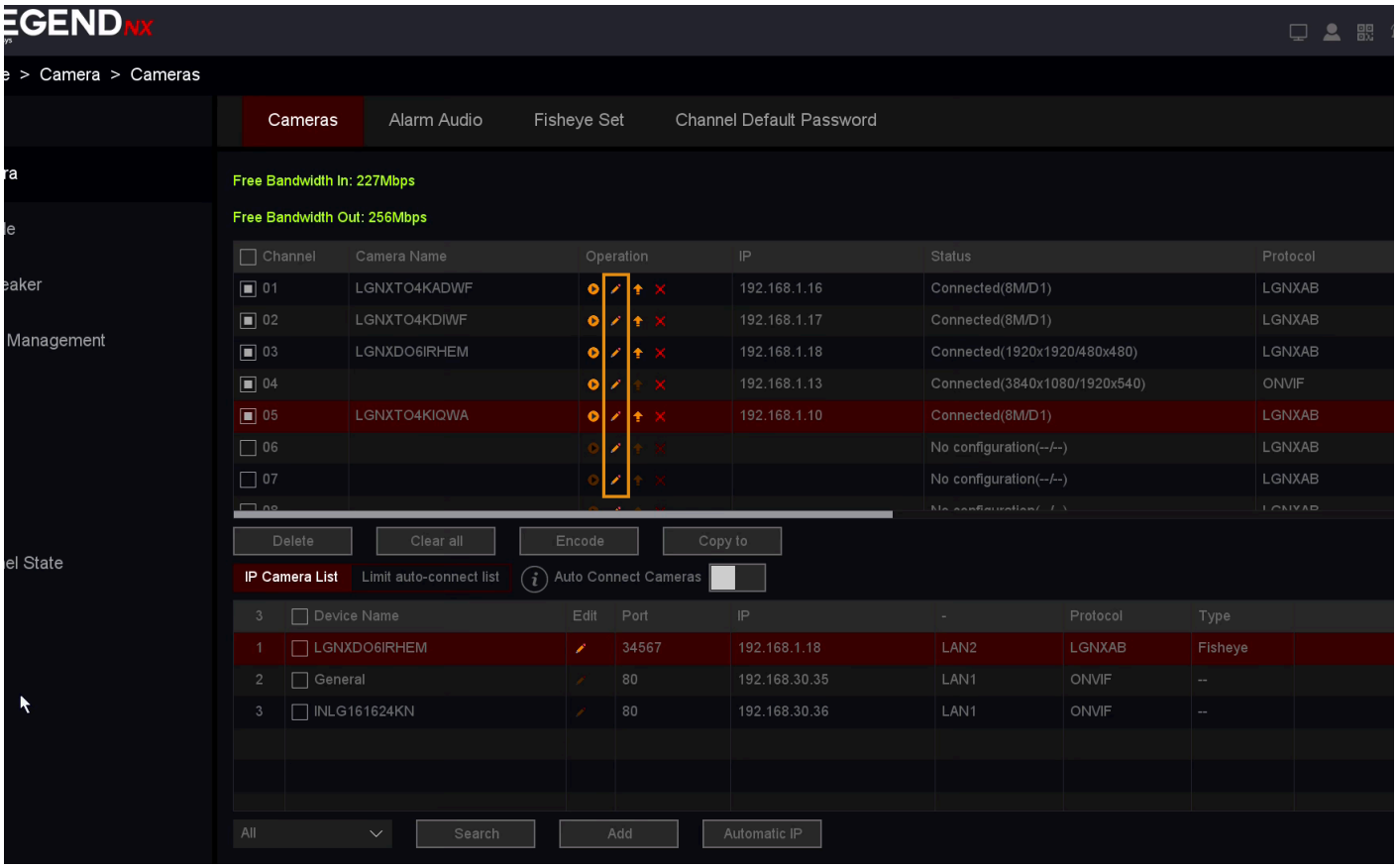


Figure 2-17 Edit

3. In the **Type** drop-down list, select **UPNP**, then click **OK**.

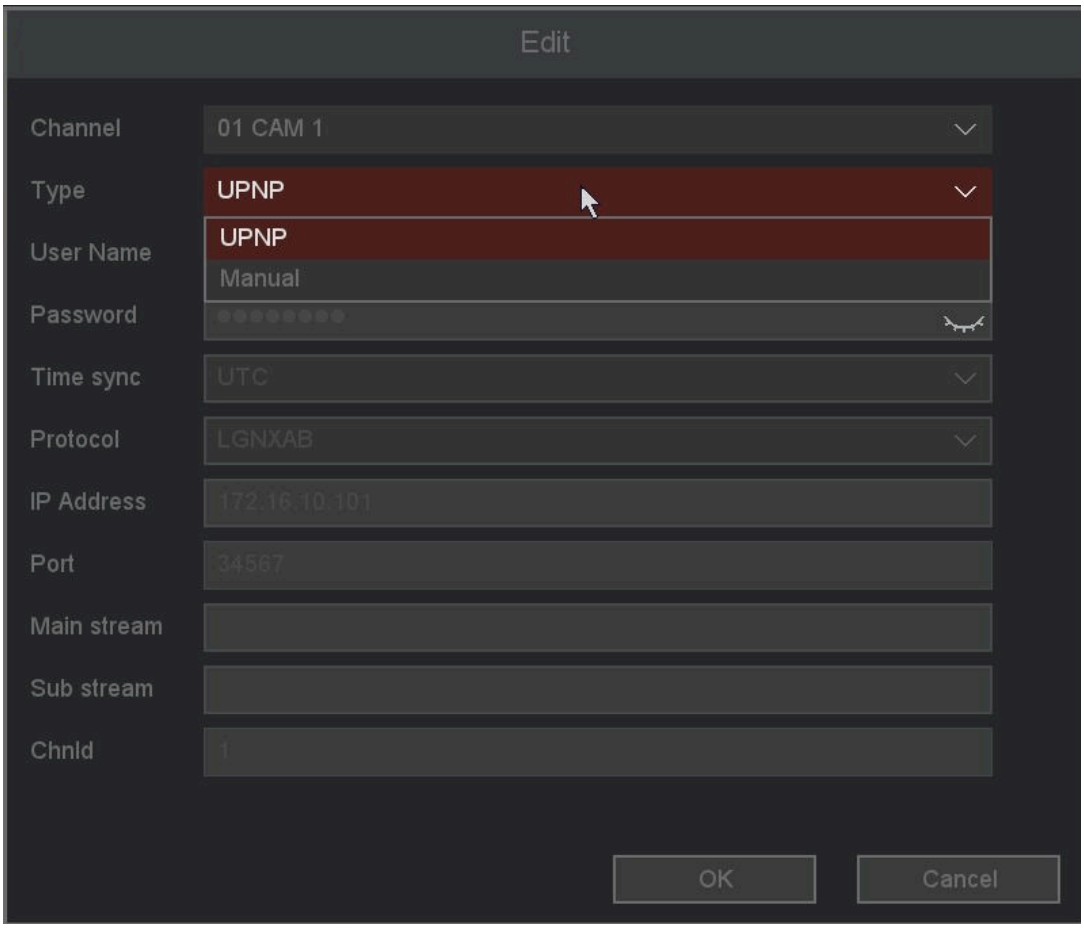


Figure 2-18 UPNP

Note

• The default setting is **UPNP**. If not, follow the steps above to modify it. To quickly apply settings to multiple channels, use the **Copy To** function.

• **Manual**: Disables the PoE interface for the selected channel, allowing it to function as a standard channel. You can manually enter parameters such as IP address, username, and password, then click **OK** to add the IP camera. Refer to **2.4 Adding the Online IP Cameras (Option 2)**.

4. Check the camera status. **Connected** indicates the camera is successfully connected.
5. Click the **PoE Power** tab to view the connection and power status of each PoE port.

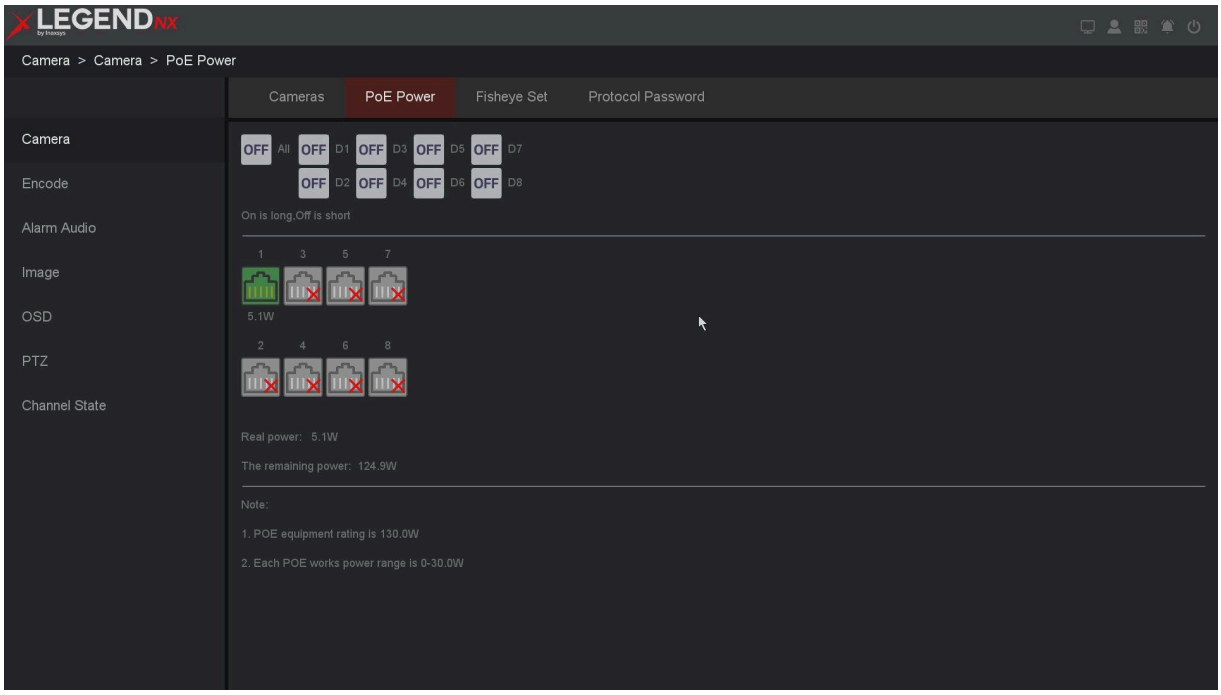


Figure 2-19 Edit the Parameters

Note

• This page displays the power and connection status of all PoE channels.

• **EPoE (Extended Power over Ethernet)** extends the standard PoE transmission distance from 100 m to up to 250 m, enabling installations over longer distances without additional power infrastructure.

• It is recommended to enable EPoE only for cameras using cable lengths greater than 100 m, as it may introduce slight video delay due to data processing over longer distances.

• Switch between PoE and EPoE by toggling the **ON/OFF** button for individual channels or using the **All** option.

3. Live View

3.1 Introduction of Live View

Live view displays real-time video from each connected camera. The NVR automatically enters Live View mode when powered on. It is also located at the top level of the menu hierarchy. Pressing the right mouse button multiple times (depending on the current menu) will return you to Live View mode, as shown below.

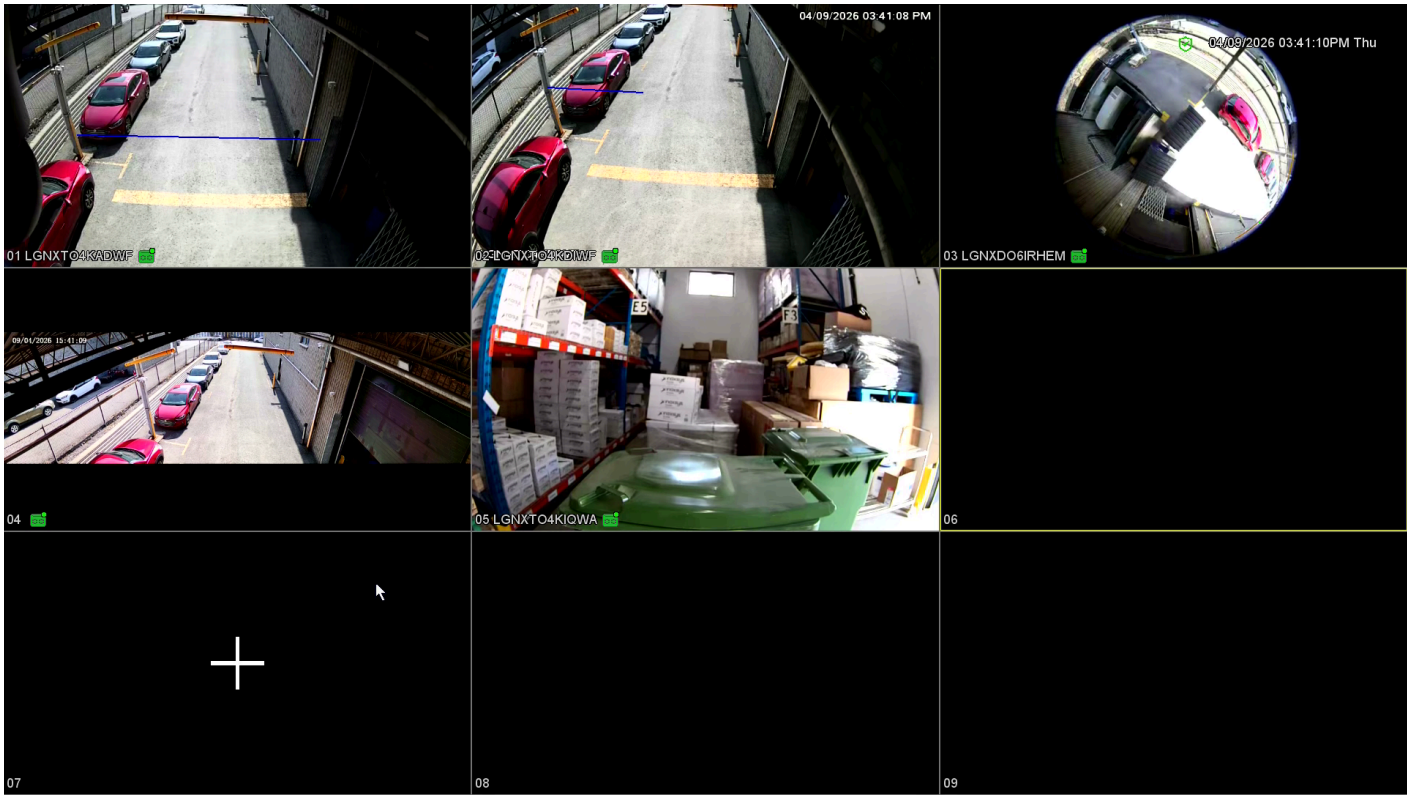


Figure 3-1 Live View

In Live View mode, status icons appear in the upper-right corner of each channel, indicating recording and alarm status. This allows you to quickly determine whether a channel is recording or if an alarm has been triggered.

Table 3-1 Live View Icons

Icon	Items	Description
	Recording Status	Displayed on the channel preview when recording is active.
	Alarm Detection	Displayed on the channel preview when an alarm is triggered.

	Video Loss	Displayed on the channel preview when video signal is lost.
	Camera Lock	No preview permission.

Note

• In Live View mode, click the **"+"** icon on a channel to access the channel management interface. The NVR will automatically search for IP cameras on the same network segment. Select the desired camera and click **Add**. Refer to **2.4 Adding the Online IP Cameras**.

• The number of available IP camera channels may vary depending on the device model.

3.2 Operations in Live View Mode

In Live View mode, multiple functions are available, as listed below:

• **Single Screen**: Displays a single channel on the monitor.
• **Multi-screen**: Displays multiple channels simultaneously on the monitor.
• **Tour**: Automatically switches between channels. The dwell time for each screen must be configured in advance in the settings menu.
• **Start Recording**: Supports continuous recording and motion detection recording.
• **Add IP Camera**: Shortcut to access the IP camera management interface.
• **Playback**: Plays back recorded video for the current day.

3.3 Quick Setting Toolbar in Live View Mode

Each channel includes a quick settings toolbar that appears when you move the mouse cursor to the top of the image.

Figure 3-2 Quick Setting Toolbar in Channel Image

Table 3-2 Quick Setting Toolbar

Items	Description	Icons
Instant Replay	Plays back video from the last 10 minutes in the preview window.	
Zoom	Displays the selected channel in full screen. Use the mouse wheel to zoom in on the selected area.	

Manual Record	Quickly switch the recording mode for the channel (manual/stop).	
Audio Preview	Enables audio monitoring for the selected channel.	
Manual Snapshot	Captures images in real time based on the current display resolution.	
Voice Intercom	Enables two-way audio communication via IP Camera, web, or mobile client.	
Channel Settings	Quickly access the channel management interface.	
Bitrate	Switch stream type and view the bitrate of the current channel.	
Red and Blue Lights	Manually enable or disable the red and blue warning lights.	
Siren	Manually enable or disable the siren.	
PTZ	Quickly access the PTZ control interface.	
Image Stitching	Adjust the stitching length for dual-lens cameras using the scroll bar.	

In preview mode, right-click to open the desktop shortcut menu, as shown below.

Table 3-3 Desktop Shortcut Menu

Items	**Description**	**Icons**
Main Menu	Provides access to playback, settings, maintenance, backup, and shutdown functions.	
Startup Wizard	Refer to Section 2.2 Using the Startup Wizard for details.	
Auto Channel Config	Automatically detects and adds IP cameras on the same LAN when selected from the right-click menu.	
IP Channel	Shortcut to the IP channel management interface.	
Channel Status	Shortcut to the IP channel status interface.	
Playback	Shortcut to the playback interface.	

Quick Record	Displays current channel selection status: “○” indicates not selected, “●” indicates selected.	
PTZ Control	Includes PTZ direction control, speed adjustment, zoom, focus, iris, preset setup, patrol, pattern, border, and tour functions.	
Color Setting	Shortcut to Settings → Channel Management → Image Color Settings.	
Output Adjust	Shortcut to System → Display → Display Settings.	
Mute	Toggles speaker output  . The icon indicates whether audio is enabled or disabled.	
Intelligent Mode	Displays captured face images at the bottom of the preview interface (requires camera face detection to be enabled).	
Guard / Disarm	Quickly enable or disable all alarm and event triggers.	
Shutdown	Provides options for shutdown, restart, logout, and user switching.	
View 1	Displays a single-channel preview.	
Multiple Views	Displays multiple channels (e.g., 4, 6, 8, 9, or 16 views).	
Corridor Mode	Displays multiple channel layouts optimized for corridor viewing (e.g., 3, 4, 5, 7, 9, 10, 12, or 16 views).	

3.4 Desktop Shortcut Menu

Note

• The right-click menu may vary depending on the model. Refer to the actual GUI of the device.

Supplementary function description

• **Quick Record:** Displays the current channel status: “○” indicates not selected, “●” indicates selected.

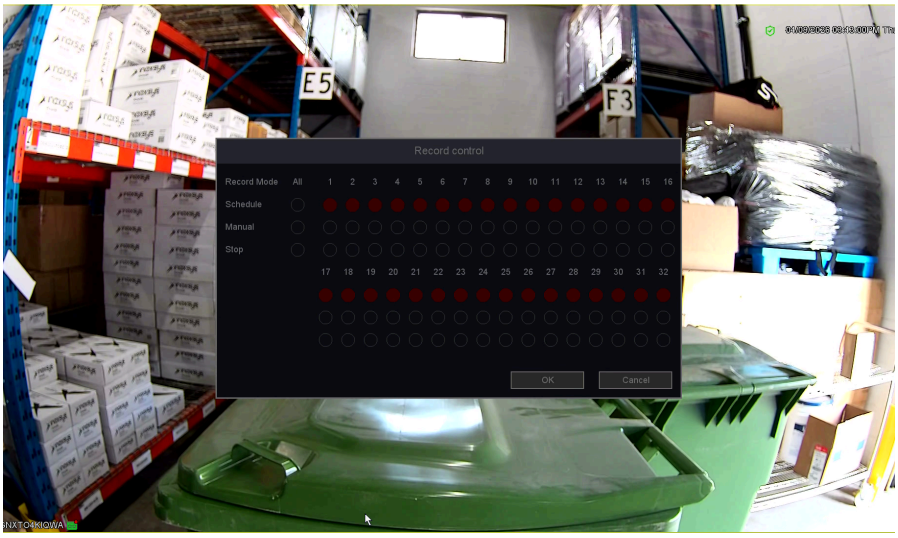


Figure 3-3 Record Control

Table 3-4 Record

Items	Description
Schedule	Records according to the configured schedule.
Manual	Click the button to start recording immediately on the selected channel, regardless of the current state.
Stop	Click the stop button to stop recording on the selected channel, regardless of the current state.

• **PTZ Control:** The operation interface is shown below. Functions include PTZ direction control, speed adjustment, zoom, focus, iris, preset setup, patrol, pattern, border, and tour.

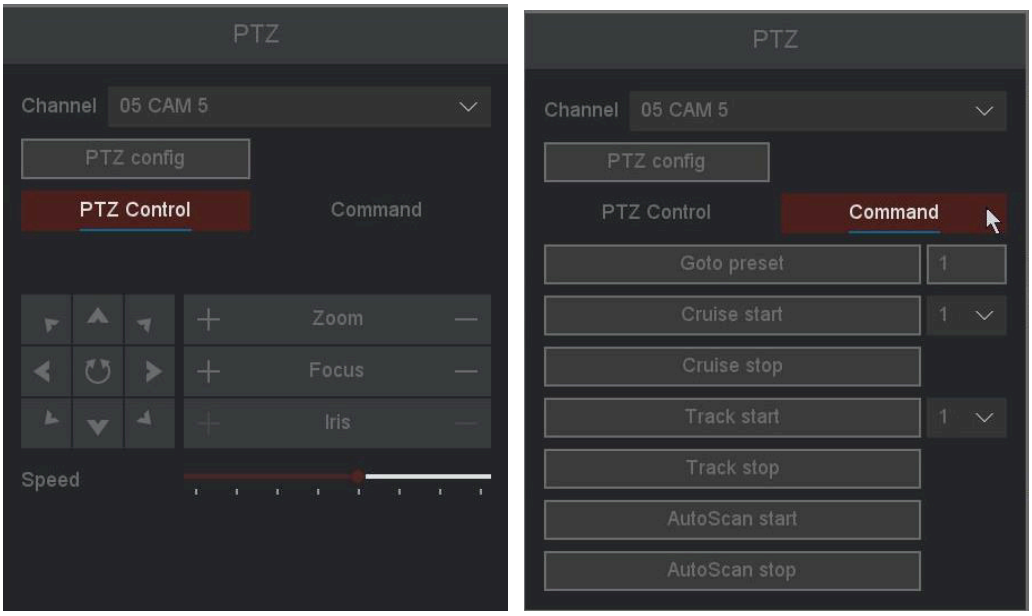


Figure 3-4 PTZ

• **Intelligent Mode:** After enabling this mode, the NVR displays captured face images at the bottom of the preview interface, as shown below (the IP camera's face detection function must be enabled first).

Figure 3-5 Intelligent

4. Playback

4.1 GUI Introduction

Go to **Playback**.

• Right-click and select **Record Playback** to enter the playback interface. You can also click the playback button in the main menu to access the playback interface, as shown in the figure below.

Figure 4-1 Playback

• The functions of each block in the above figure are described as follows.

Table 4-1 Area Functions Introduction of Playback

No.	Items	Function
1	Playback Type	The NVR supports multiple playback modes: Normal Play, Event Play, Label Play, Smart Play, Time Division Play, and Normal Play (Picture).
2	Display	Displays video playback.
3	Camera List	Allows you to select channels for playback.
4	Date	Displays dates that contain video files (highlighted in blue).

5	Time of File	Displays the start and end times of files on the HDD.
6	Timeline	Displays the playback progress of files in this area.

• The video playback timeline is shown below.

Figure 4-2 Timeline

1. Position the cursor on the timeline and drag it to a specific time.
2. Periods marked with a blue bar contain video. Red bars indicate event recordings. Scroll the mouse wheel up/down to fast-forward or rewind.
3. Click the buttons at the bottom-right of the timeline to zoom in or out.

Note

• The second line displays all files from the selected channels. The first line shows files for the channel currently selected in the display area. Event files are marked in red, and normal files are marked in blue.

Table 4-2 Tool Menu Description

No.	Key Title	Key Function
1		Switch playback channel audio on/off
2		Clip the currently playing video
3		Capture a snapshot of the current playback
4		Lock the file to prevent it from being overwritten on the HDD
5		Add a label to the file
6		File manager: manage clipped, locked, and labeled files
7		Zoom the playback channel

4.2 Normal Playback

Play back standard video recordings.

Steps:

1. Go to **Playback**.
2. Select a camera from the camera list.

3. Select a date on the calendar.

Note

The blue square on a calendar date indicates that recordings are available. For example, 

indicates that video is available, while 

indicates that no video is available.

4. Click the timeline to start playback.

Figure 4-3 Timeline

5. Video playback is controlled using the following buttons. The functions of common playback controls are described in the table below.

Table 4-3 Playback Interface Description

Operation	Button	Operation	Button
30 s reverse		30 s forward	
Full screen		Start playback	
Slow down		Speed up	
Speed		Stop playback	
Flip vertically		Switch between synchronous and asynchronous playback	
Switch between main stream and sub stream			

6. To play back a specific time period, select the recording start time and end time under the calendar, as shown below.

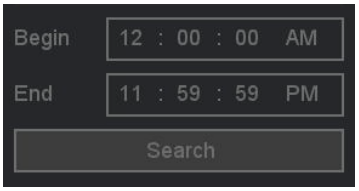


Figure 4-4 Time Period

Note

To locate recordings for a specific time period, set the desired start time and end time under the calendar, as shown above.

7. Video playback can also be controlled using the buttons described above.

Table 4-4 Playback Icon

Description	Button	Description	Button
Cut the selected portion of the currently playing video		Capture a snapshot of the current playback	
Lock the file to prevent it from being overwritten on the HDD		Add a default label to the file	
File manager: manage clipped, locked, and labeled files		Zoom the playback channel	
Toggle audio for the playback channel			

8. For all playback control operations, refer to the previous table.

• The **Cut** button clips the video from the currently playing channel. You can view clipped files in **File Manager**.

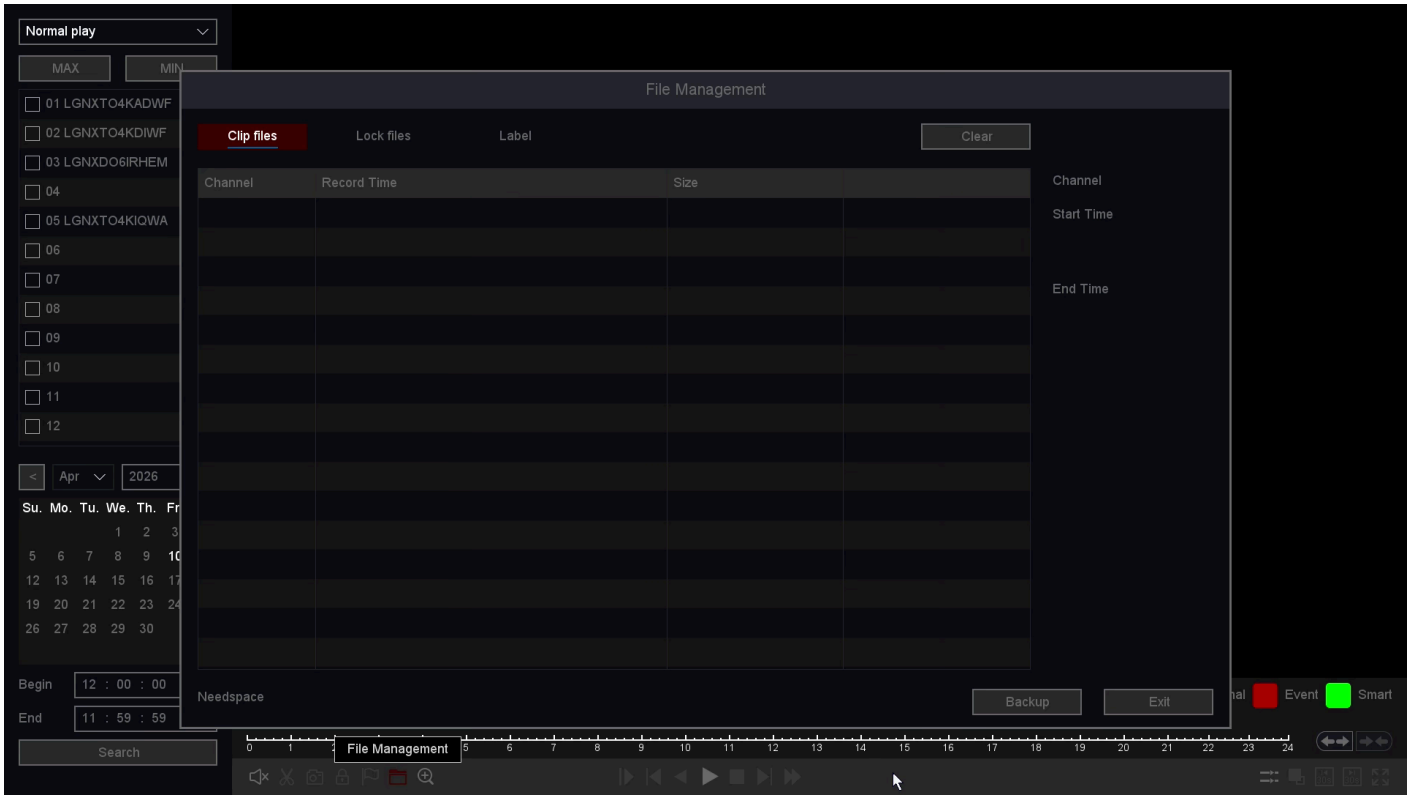


Figure 4-5 File Management

• The **Lock Record** button locks the file to prevent it from being overwritten by new recordings. You can view and back up locked files in **File Manager**, and also unlock them within this interface.

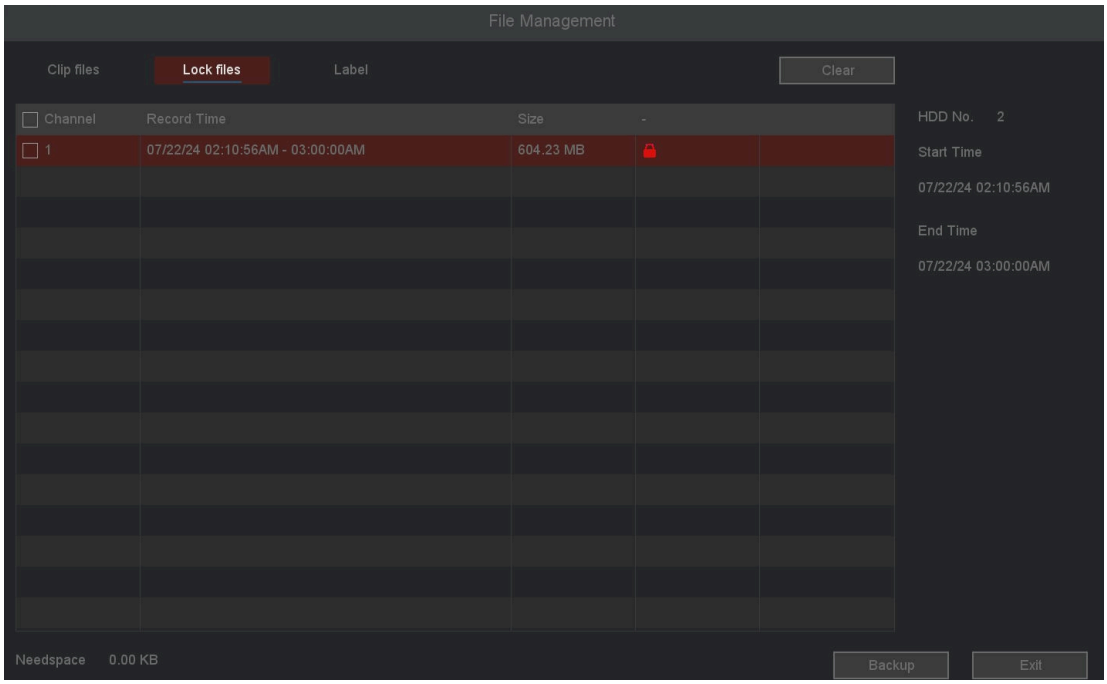


Figure 4-6 Lock File

• Click the **Default Label** button to mark the video with a label. You can edit and review labels in **File Manager**.

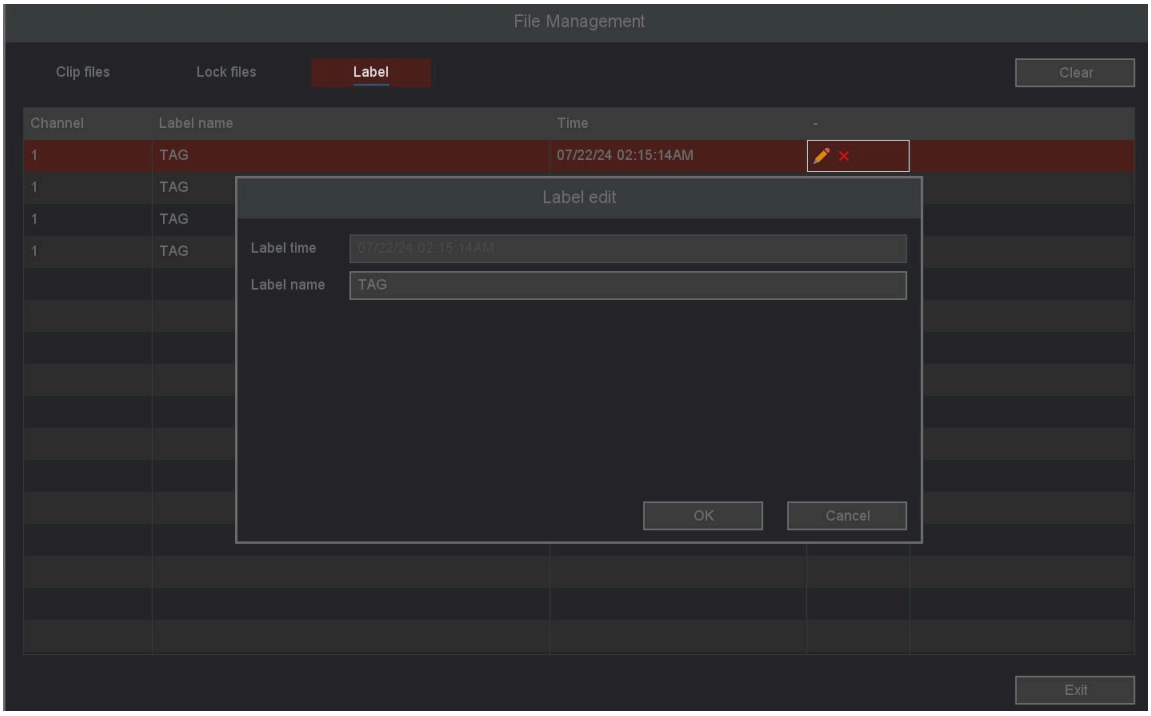


Figure 4-7 File Management

4.3 Event Playback

When **Event Playback** mode is selected, the system analyzes and marks video segments containing motion detection, line crossing detection, or intrusion detection events.

Before You Start

• Ensure that the camera has **Motion Detection**, **Intelligent Detection**, or **Diagnosis** enabled. You can configure this via **Main Menu** → **Event** → **Detect** or **Intelligent Detection**.

• Ensure that **Record Channel** is enabled in the **Trigger Process** settings of the recorder. You can configure this via **Main Menu** → **Event** → **Detect / Intelligent Detection / VQD** → **Trigger Process**.

Steps:

1. Go to **Playback**.
2. Click **Event Play**.
3. Select a camera.
4. Set the time period, then click **Search**.

Figure 4-8 Event Playback

5. The search results are shown as in the figure:
   - **Source** indicates the alarm channel.
   - **Chan** indicates the recording channel triggered by the event.
   - **Time** indicates when the alarm occurred.
6. The results area displays all alarm events. You can change pages to locate the desired event and set playback time before or after the alarm.

7. You can modify alarm types and channels by clicking **Return** to go back to the previous interface. For button operations, refer to the table below. Note that **Sync/Async**, **Main/Sub Stream**, and **Frame Control** functions are not available in Event Playback mode.

The Buttons of Event Search Results:

Table 4-5 Button Description

Descritption	Button	Descritption	Button
Go to the first page of event search results		Go to the last page of event search results	
Go to the previous page of event search results		Go to the last page of event search results	
Go to the next page of event search results		Turn audio on/off	

4.4 Back up Clip

You can clip video during playback. Video clips can be exported to a backup device (USB flash drive, etc.).

Before You Start:

Connect a backup device to the video recorder.

Steps:

1. Start playback. Refer to **Chapter 4 Playback** for details.
2. Click the **clip** button at the desired start time.
3. Click the **clip** button again at the desired end time.
4. You can view the clipped files in **File Management**.
5. Select the videos to back up.
6. Click **Backup** to enter the record backup interface.
7. Select the backup device and folder.
8. Click **Start** to export the clips to the backup device.

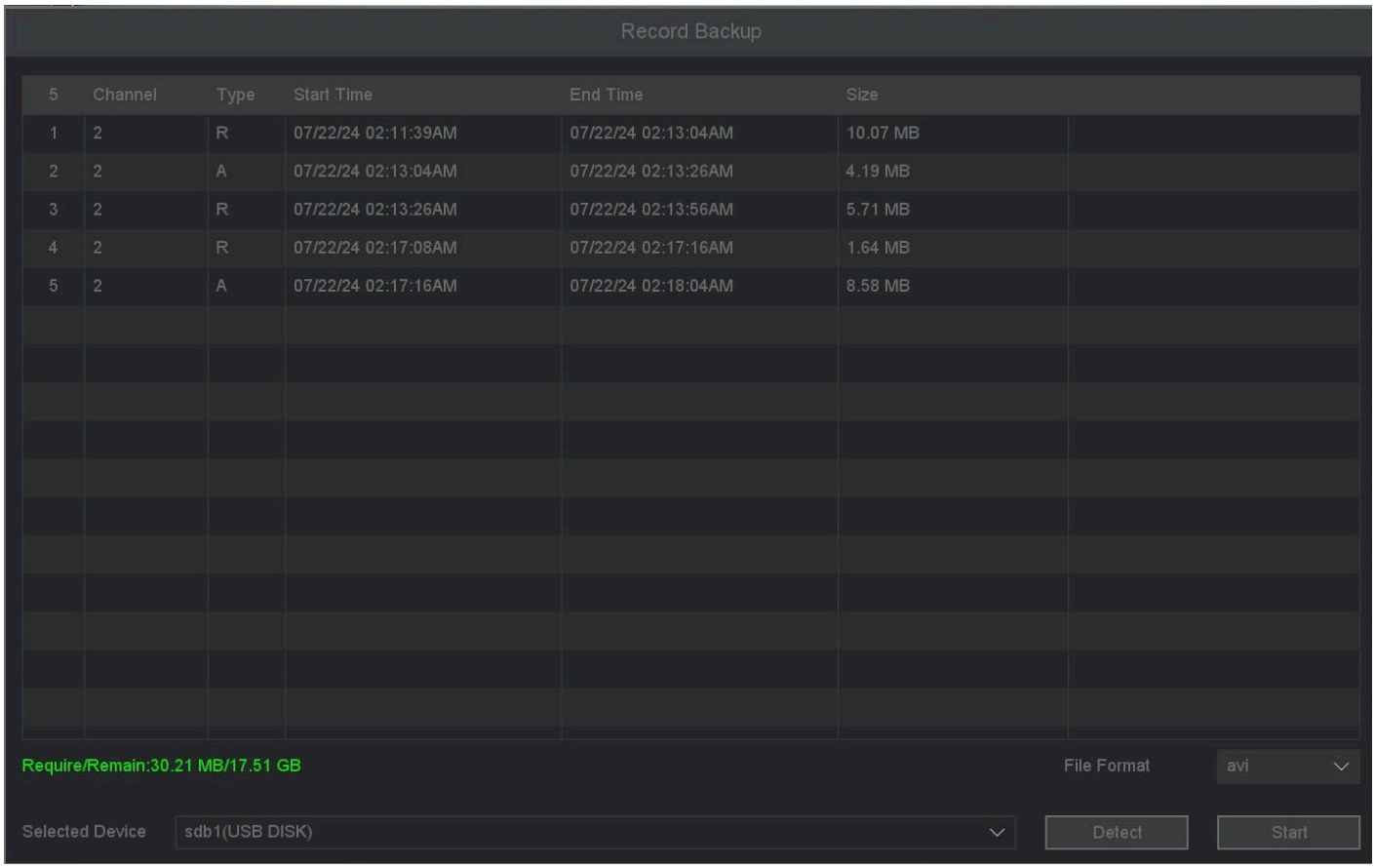


Figure 4-9 Record Backup

5. Backup

You can back up video recordings. Files can be exported to a backup device (USB flash drive, etc.).

Before You Start:
Connect a backup device to your video recorder.

Steps:

1. Go to **Main Menu → Backup → General → Video/Picture/Event**.

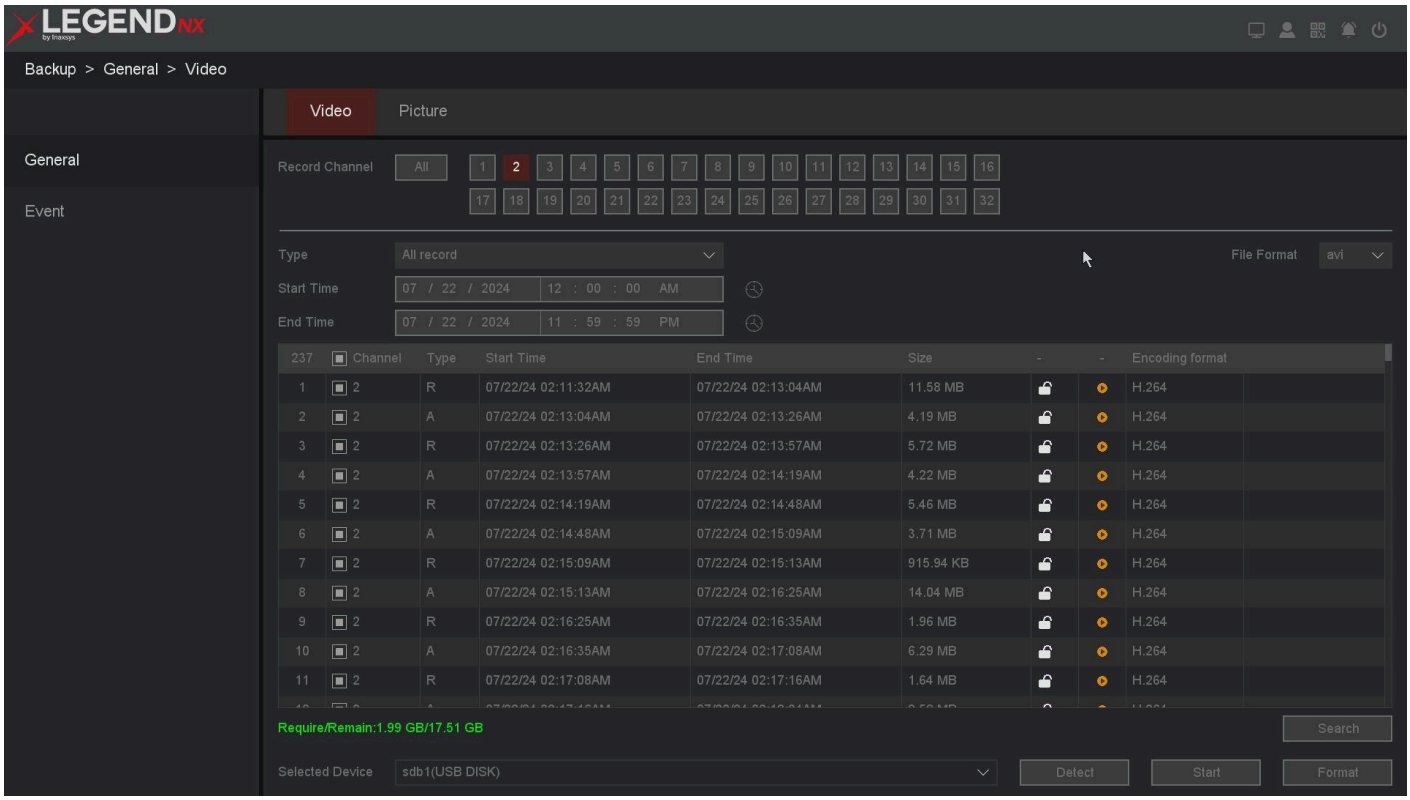


Figure 5-1 Search

2. Select a search type (video or picture).
3. Set the search conditions.
4. Click **Search**.
5. Click the **Play** icon to play the video.
6. Click the **Lock** icon to lock the file. Locked files will not be overwritten.
7. Select the file(s).
8. Select the backup device and folder.
9. Click **Start** to export the file(s) to the backup device.

Note
If the backup device is not detected, unplug and reconnect it. If the backup fails, click the Format button to format the device first.

6. Configuration (Common Mode)

6.1 System Configuration

6.1.1 System - Base

You can configure the language, time zone, system time, device number, host name, etc.

Steps:

1. Go to **Main Menu → System → Base**.

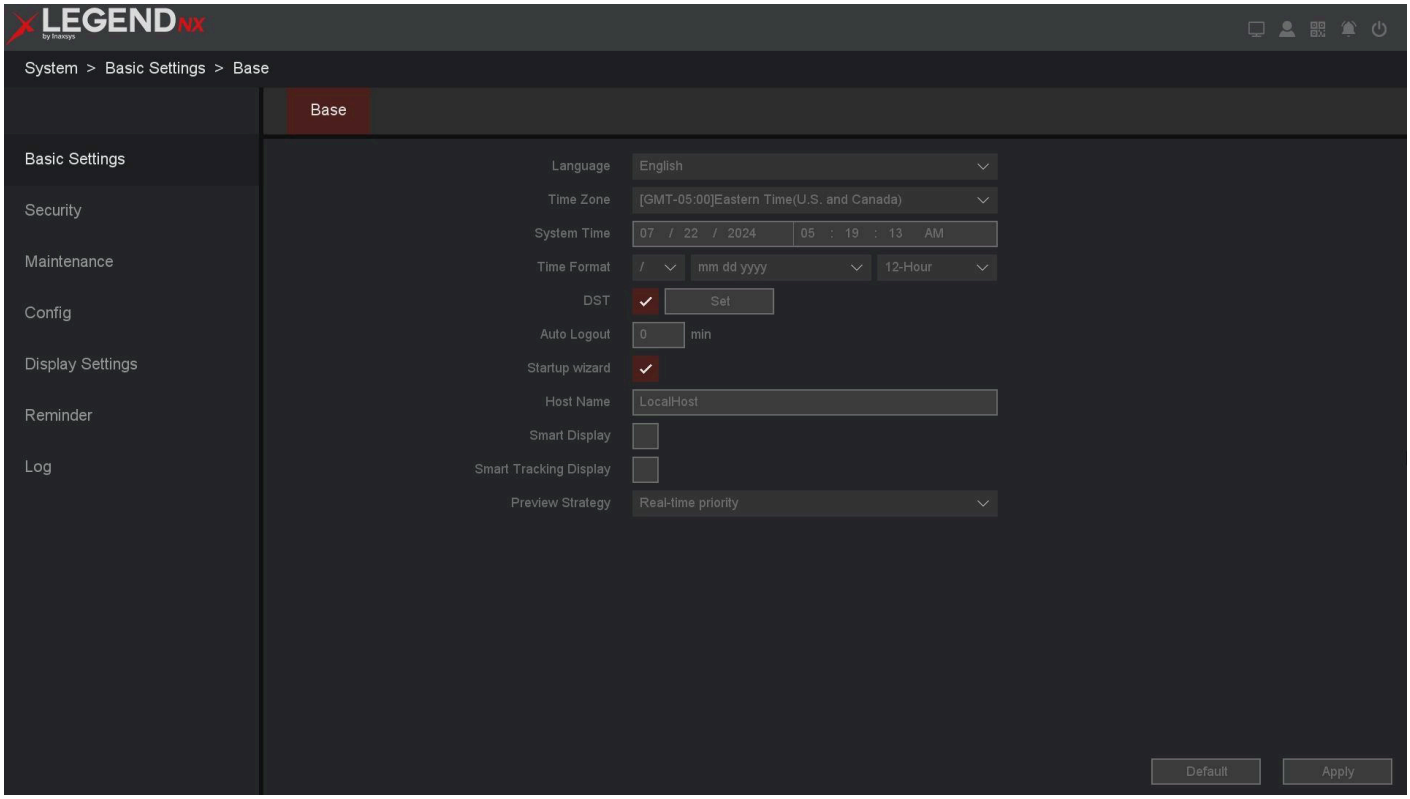


Figure 6-1 Basic Settings

2. Configure the parameters as required.

Time format: The format used for time display.

DST: Daylight Saving Time.

Auto logout: Specifies the automatic logout time. The maximum value is 60 minutes.

Startup Wizard: The wizard will pop up after the device starts.

Smart display: Displays smart rule boxes. Refer to the corresponding section for details.

Smart tracking display: Displays smart tracking boxes. Refer to the corresponding section for details.

3. Click **Apply**.

6.1.2 User

Add User: There is a default account: **admin**. The administrator username is **admin**. The administrator has permission to add, delete, and edit users. The guest user only has permissions for live view, playback, and download.

Steps:

1. Go to **Main Menu** → **System** → **Security** → **Account**.
2. Click **Add**, and confirm the administrator password if prompted.

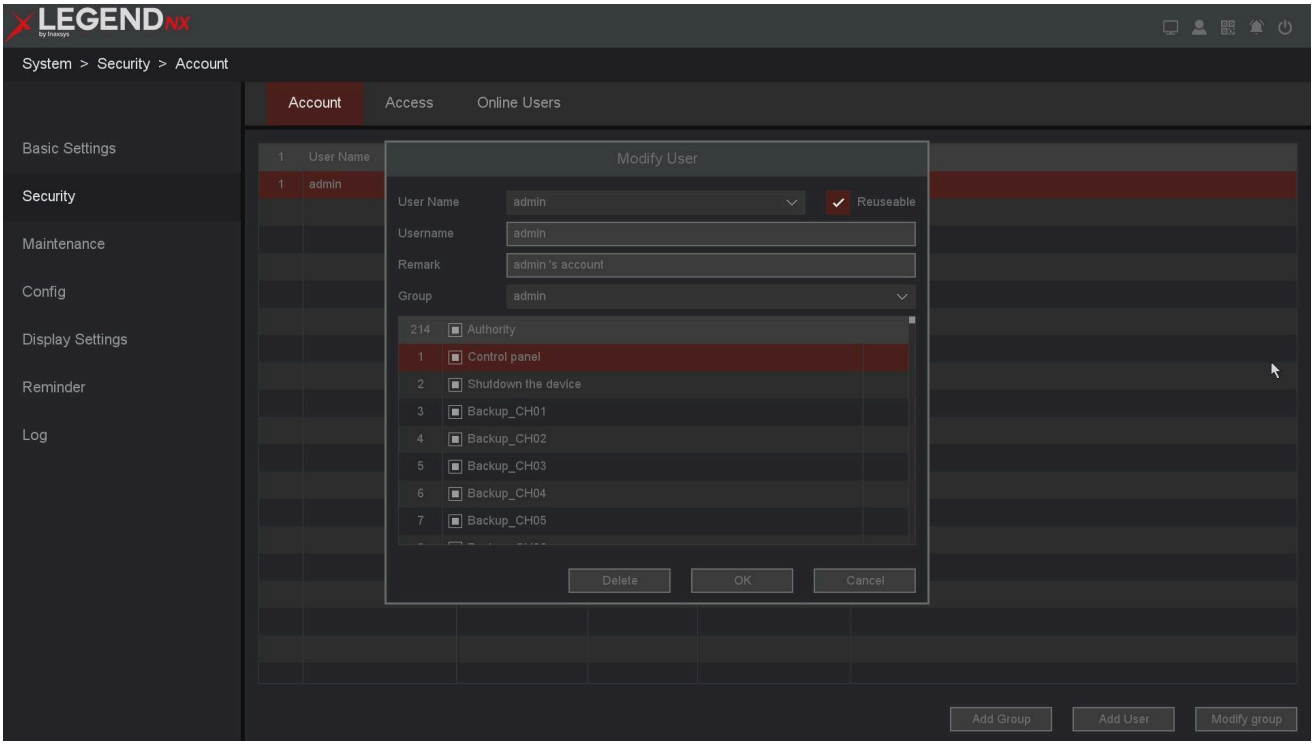


Figure 6-2 Add User

3. Enter the user name.
4. Enter the same password in **Password** and **Confirm**.

Warning
A strong password is recommended. Use at least 8 characters, including at least three of the following categories: uppercase letters, lowercase letters, numbers, and special characters, to enhance system security. It is recommended to change the password regularly. For high-security environments, consider changing the password monthly or weekly.

5. Click **OK**.

Click the **Edit**  **/Delete**  icons to modify or remove a user.

Modify Password

You can change your password if it has been compromised.

Steps:

1. Click the  **Modify Password** icon in the Account interface.

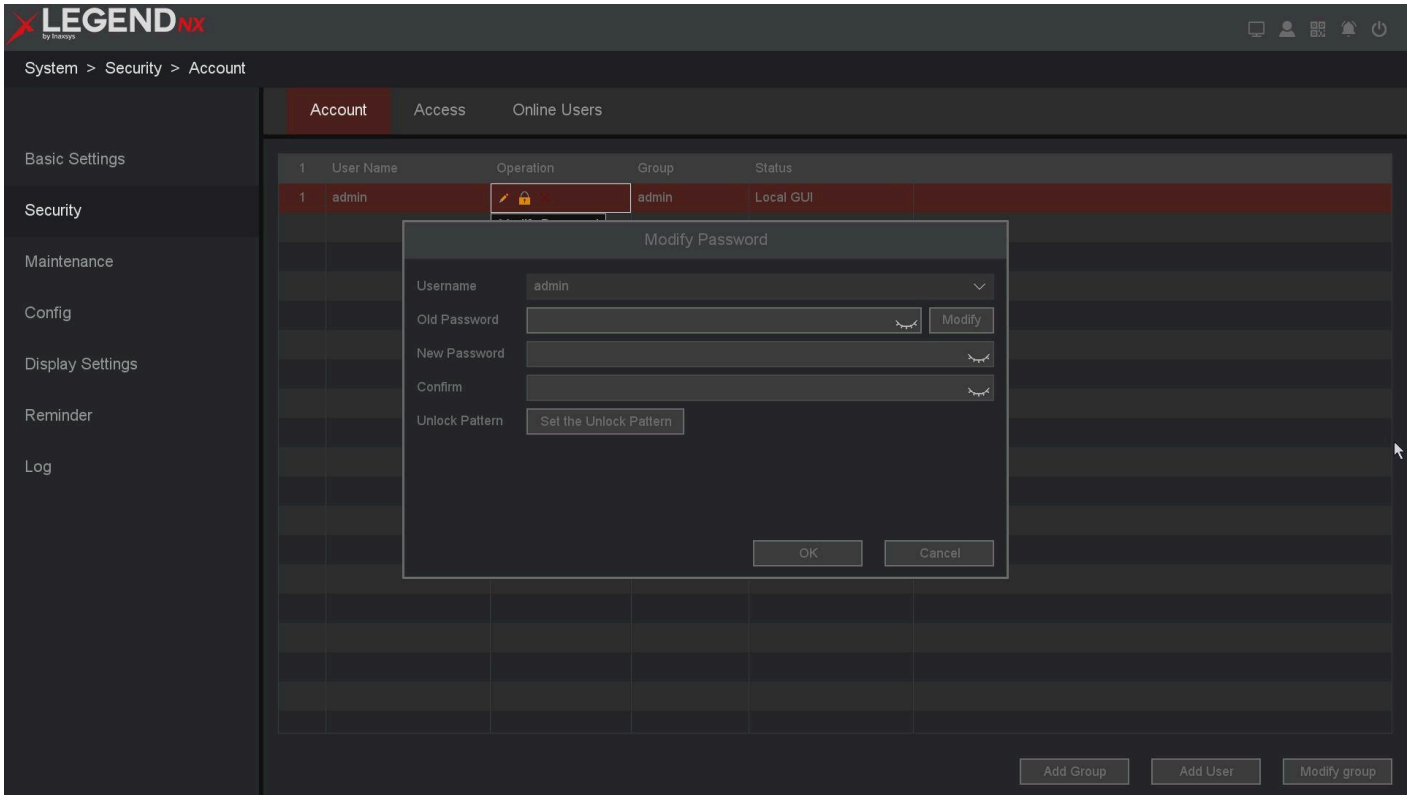


Figure 6-3 Modify Password

2. Enter the **Old Password**.
3. Enter the new password in **New Password** and **Confirm**.
4. Click **OK**.
5. Optional: You can also set a pattern lock by selecting **Set Pattern Lock**.

6.1.3 Alarm Events & Trigger Process

You can receive alarm event notifications in **Alarm Status** and configure exception linkage actions in the **Trigger Process** settings.

Step 1: Alarm Information

1. Go to **Main Menu → Event → Alarm Status → Alarm Information**.

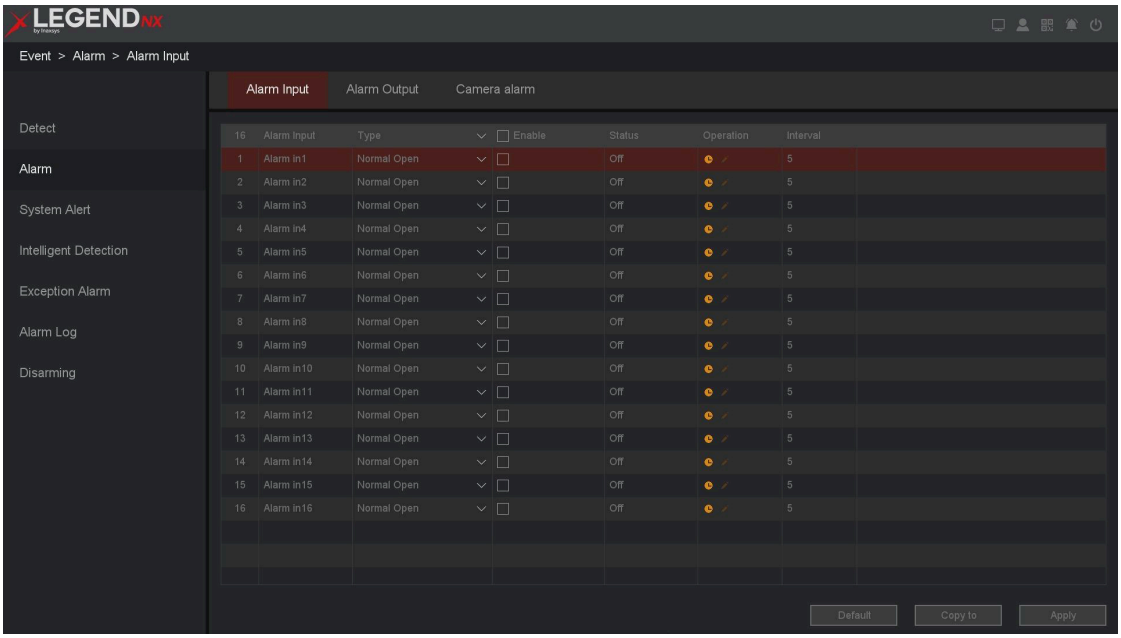


Figure 6-4 Alarm Information

2. When configured events occur, notifications will appear in **Alarm Status**.

Note
You can also click the **Play** icon to view video associated with the alarm event.

Step 2: Enable the Trigger Process

1. Go to **Main Menu → Event → Detect, Intelligent Detection, or VQD → Trigger Process**.

Figure 6-5 Event Process

Show message: Displays a popup video preview when an event occurs.

Buzzer: Triggers an audible alert. You can configure the buzzer duration.

Send email: Sends an email notification when an alarm occurs, if email settings are configured.

Record Channel: Enables recording on the selected channel when an alarm event occurs.

Snapshot: Captures images when an alarm event occurs. You can also set the snapshot interval.

2. Select the linkage actions required when an alarm event occurs.
3. Click **OK**.

6.2 Network Configuration

6.2.1 General - TCP/IP

Properly configure the network settings before operating the device over the network.

Steps:

1. Go to **Main Menu** → **Network** → **Base** → **TCP/IP**.

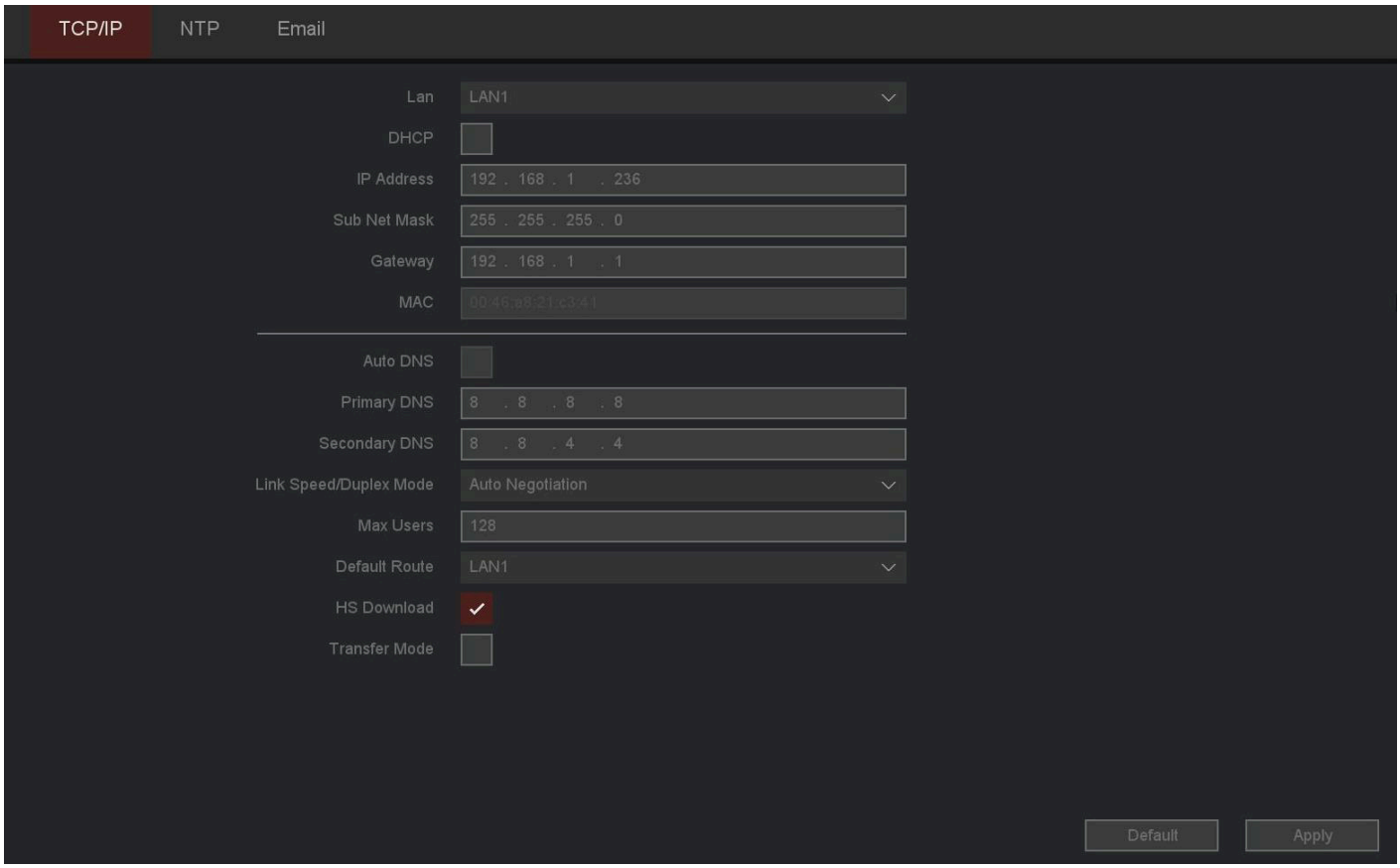


Figure 6-6 Network

Note
Only NVRs with dual Ethernet ports have **LAN** parameters. Refer to the actual interface.

2. Set the network parameters.

DHCP
If a DHCP server is available, enable DHCP to automatically obtain an IP address and other network settings from the server.

Auto Obtain DNS
If DHCP is enabled, you can enable **Auto Obtain DNS** to automatically obtain the **Preferred DNS Server** and **Alternate DNS Server**.

Note
The available options for automatic DNS acquisition may vary depending on the model. Refer to the specific device.

Manual
Manually configure the IP address, for example:

IP Address: 192.168.1.100
Sub Net Mask: 255.255.255.0
Gateway: 192.168.1.1

Make sure that the IP address of the device and the camera are in the same LAN.

3. Click **Apply**.

6.2.2 LEGEND-P2P

We provide mobile applications and cloud services to access and manage your connected devices, allowing you to conveniently monitor your surveillance system remotely.

Steps:

1. Go to **Main Menu → Network → P2P → P2P**.
2. Enable the function. The device will automatically establish a connection and register with the P2P cloud.

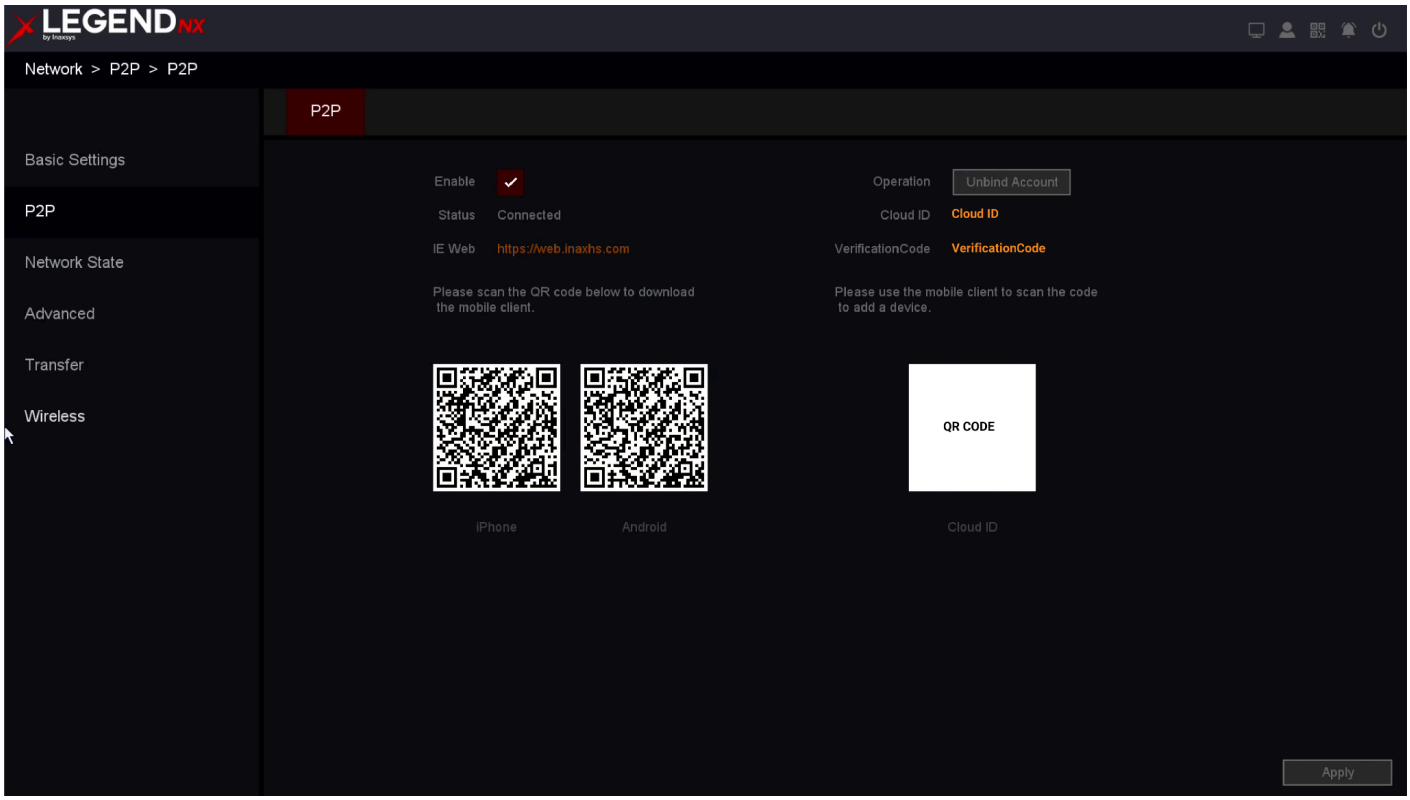


Figure 6-7 P2P

3. The device status will change to **Connected**, indicating that it has been successfully registered with the P2P cloud.
4. Bind the device to a cloud account.

1. Scan the QR code with your smartphone to download the **Legend NX APP**. You can also download it from the apple store or Google Play or by using the QR code below.

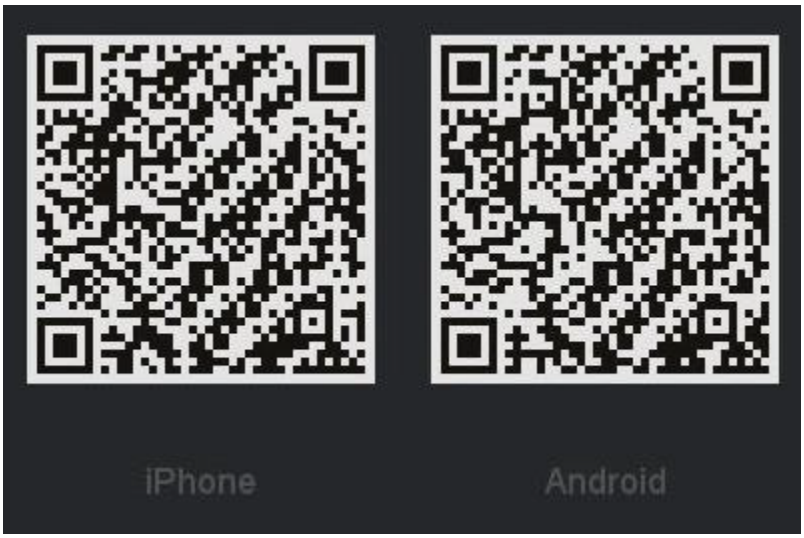


Figure 6-8 QR Code

2. Use the **Legend NX APP** to scan the device QR code and bind the device.

Steps:

1. Open the **Legend NX** application on your smartphone.
2. Tap **Register** in the lower-left corner of the login screen, create your account, and then log in. Creating an account allows you to manage multiple sites.
3. Open the **Menu** by tapping the icon in the top-left corner.
4. Tap **Devices**, then tap the **+** icon in the top-right corner to add a device.
5. Allow the app to access your phone's camera, then scan the QR code. From the startup wizard labeled **Cloud ID**, the device information will be automatically added to the app.
6. Assign a name to the device so it can be easily identified in the list. Using the installation location is a common naming method.
7. Tap **Save**, then you can select **Start Live View**.
8. Locate the device in the device list, tap the play icon, and the system will open the real-time preview (sub-stream by default). Using the sub-stream instead of the main stream improves playback smoothness and reduces mobile data usage.

Note

• You can also download the app directly from your phone's app store.
• If the device is already bound to an account, click **Unbind** to remove it from the current account.
• If your device does not support manual unbinding, contact technical support.

6.2.3 Email

Set up an email account to receive event notifications.

Before You Start

• Ensure that the SMTP service is enabled for your email account.
• Configure the network parameters. Refer to **6.2.1 General - TCP/IP** for details.

Steps:

1. Go to **Main Menu** → **Network** → **Basic Settings** → **Email**.

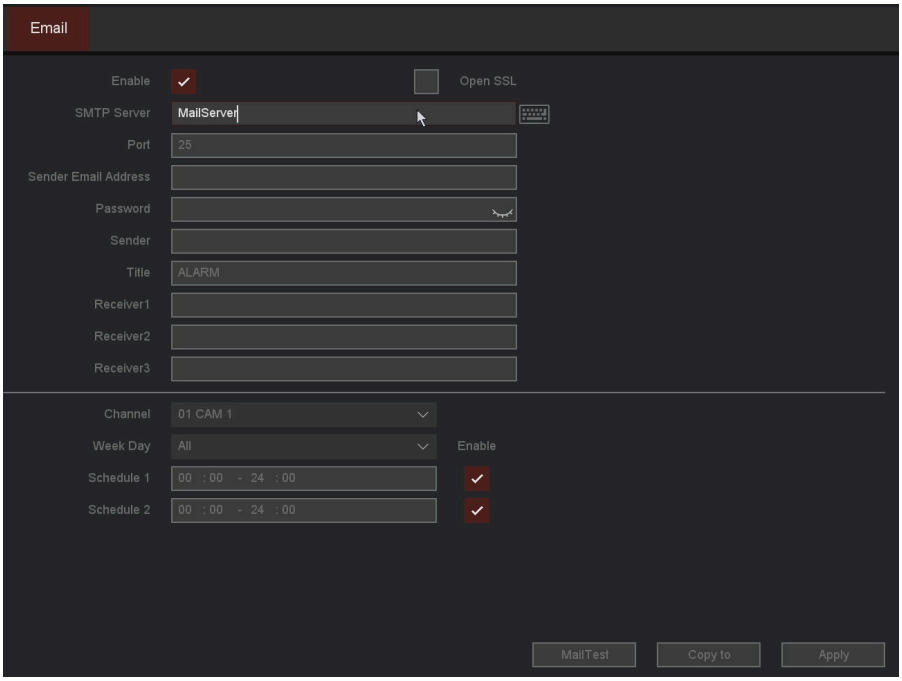


Figure 6-9 Email

2. Configure the email parameters.

Enable
Select this option to enable SMTP server authentication.

SMTP Server
Enter the address of the SMTP server (for example: smtp.163.com).

Port
Enter the SMTP server port number, provided by your email service provider.

User Name
Enter the email account used for SMTP authentication.

Password
Enter the password for the email account used for SMTP authentication.

Sender
Enter the sender name or the sender's email address.

Title
Enter the subject line of the email notification.

SSL/TLS
(Optional) Enable SSL/TLS if required by the SMTP server.

Receiver 1–3
Enter the recipient email addresses. Up to three recipients are supported.

Channel
Select the channel for which email alarm notifications will be sent.

Week Day
Select the days on which email notifications will be sent.

Schedule
Select the time schedule during which email notifications will be sent.

3. Click **MailTest** to send a test email. A confirmation message will appear if the email is sent successfully.

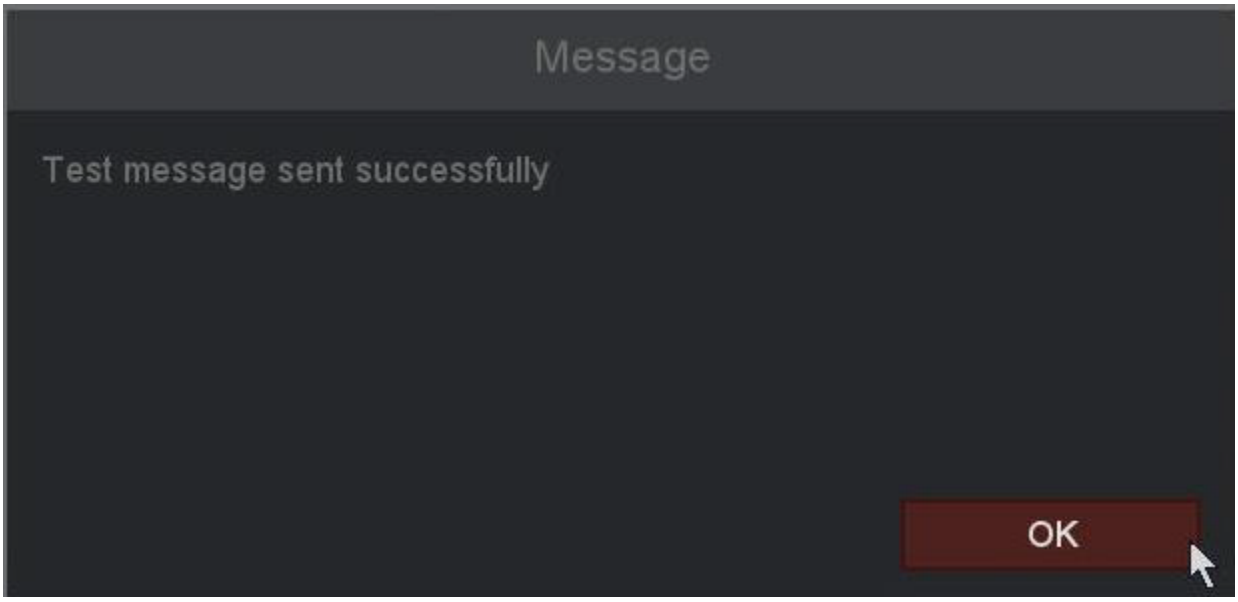


Figure 6-10 Test

Note
• For network cameras, event images are sent as email attachments. Typically, each event includes three images, depending on the actual situation.
• If email sending fails, check whether the DNS service is configured correctly.

4. Click **Apply**.

6.3 Camera Management

6.3.1 Network Camera

Add Network Camera by Quick Set

Add a LEGEND IP camera using the default password or a bundled camera for this device.

Before You Start
• Ensure the network camera is on the same network segment as your video recorder.
• Ensure the network connection is valid and correctly configured. Refer to **6.2.1 General - TCP/IP** for

details.

• Make sure the IP camera password has not been manually changed.

Steps:

1. Go to **Main Menu** → **Camera**.
2. Click the **Search** button.
3. Cameras on the same network segment as the video recorder will be displayed in the **Online Device List**.
4. Select the cameras you want to add, or select all cameras.
5. Click **Quick Set** to add the selected cameras (using the default login password) from the list.

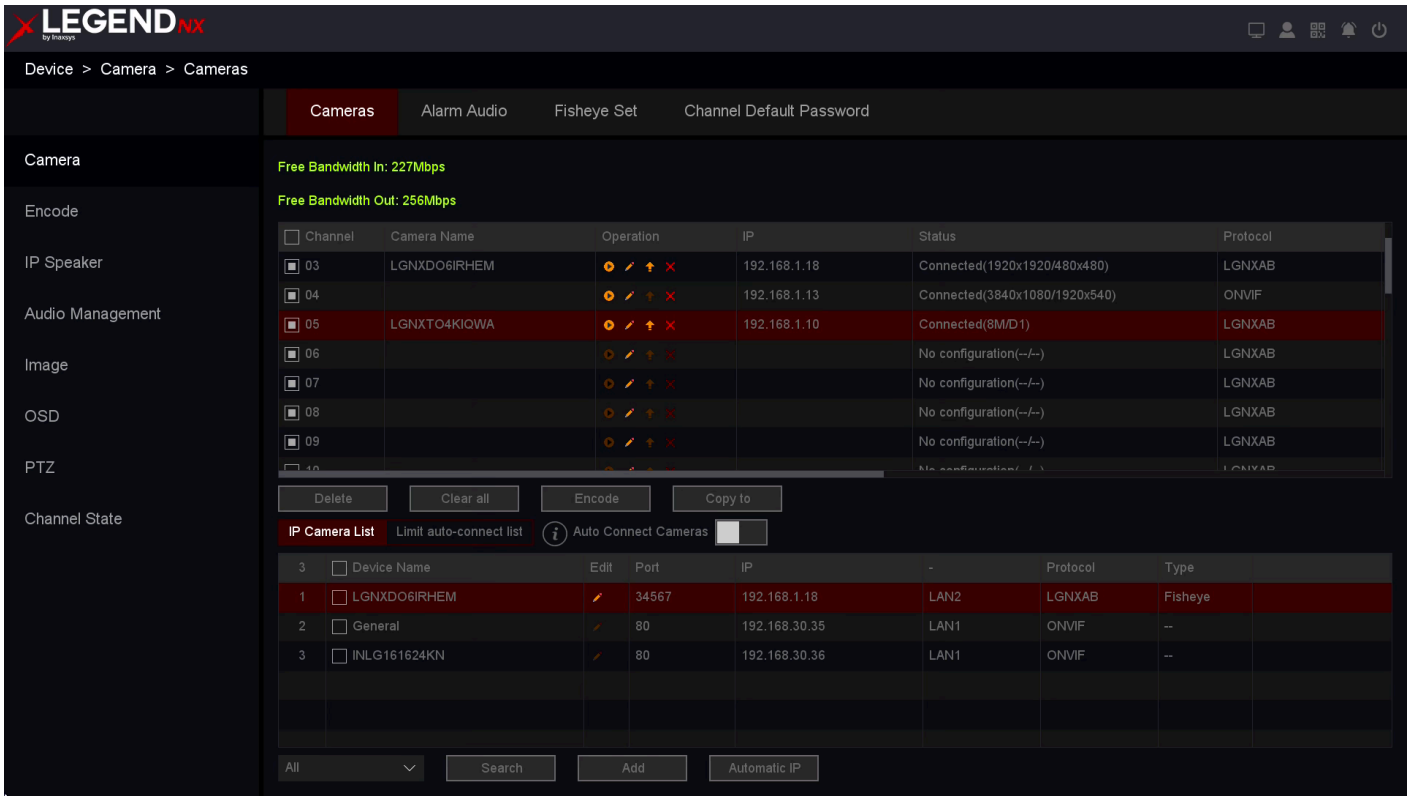


Figure 6-11 IP Camera Management Interface

6. The selected devices will be added quickly.

Note

If a camera cannot be added successfully, you can manually modify the user name, password, port, protocol, or other parameters.

Add Network Camera Manually

Before You Start

• Ensure the network camera is on the same network segment as your video recorder.

• Ensure the network connection is valid and correct.

• Ensure the network camera is activated.

Steps:

1. Go to **Main Menu** → **Camera**.
2. Select the channel you want to configure manually.
3. Click the edit icon  for that channel.
4. Edit the IP address, user name, password, port, and other parameters.

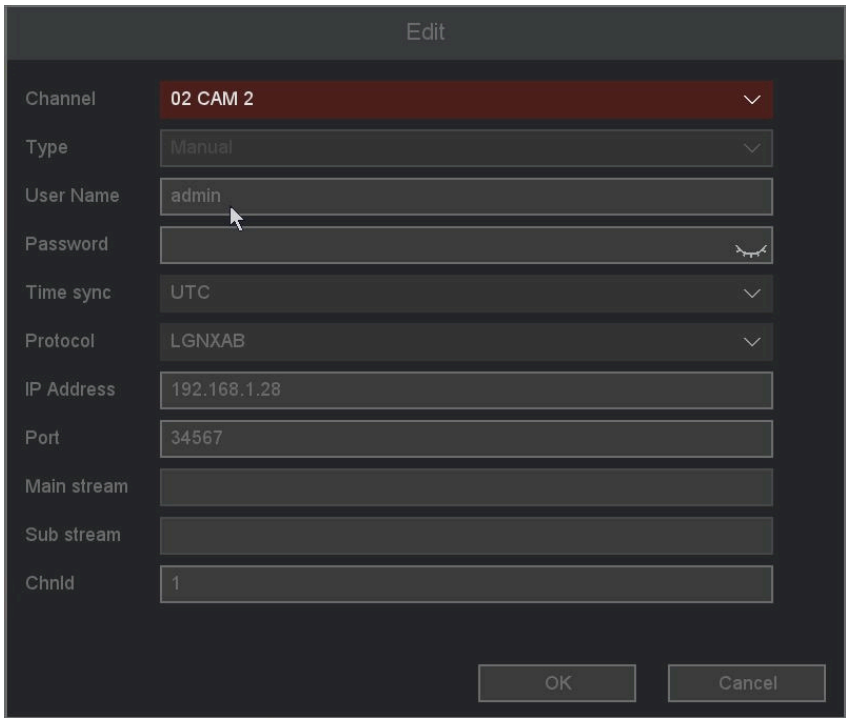


Figure 6-12 Edit the Parameters

5. In the **Protocol** drop-down list, you can select one of the following protocols: **LGNXAB**, ONVIF, or RTSP. **LGNXAB** is a private protocol, while ONVIF and RTSP are mainly used for third-party cameras.
6. Edit the **ChnId** (default is 1).
7. Click **OK** to save and exit the editing interface.
8. Optional: Click **Add More** to add another network camera.

Time sync

Time synchronization is set to UTC by default. You can also disable it if needed.

Port

Device connection ports: **LGNXAB** uses port 34567, ONVIF uses port 80, and RTSP uses port 554. Other ports may be specified by the device manufacturer.

ChnId

Channel number of the device. If the connected device has multiple channels, enter the channel number you want to use.

Previewing Video

The camera can be previewed directly using the preview function.

Before You Start

• Ensure the network camera is on the same network segment as your video recorder.
• Ensure the network connection is valid and correctly configured.
• Ensure the camera status shows **Connected** (e.g., [1080P/720P]), not [-/-].

Steps:

1. Go to **Main Menu** → **Camera**.
2. Click the preview icon .
3. The preview window will appear as shown below.

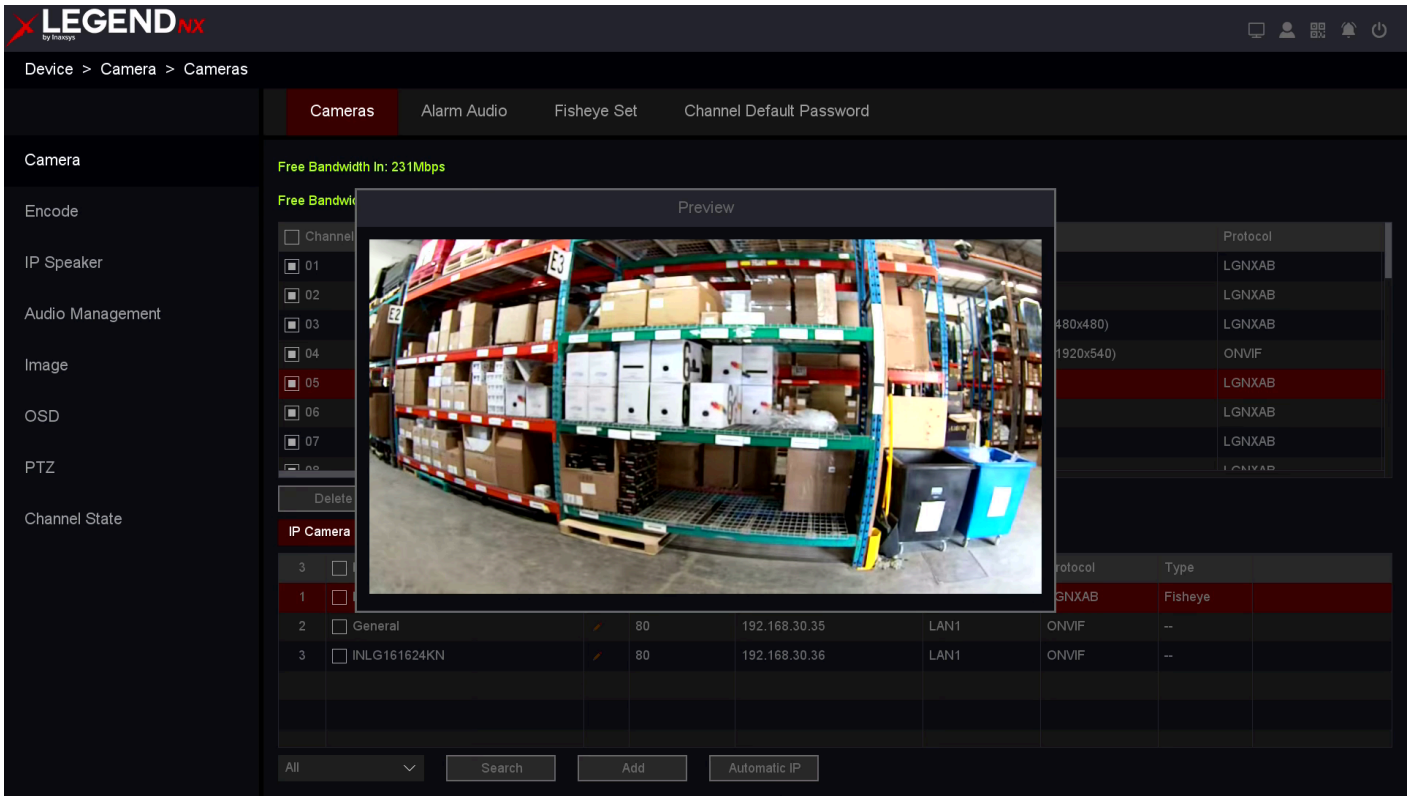


Figure 6-13 Preview

Upgrade Network Camera

The network camera can be upgraded remotely through the device.

Before You Start

• Ensure that a USB flash drive containing the network camera upgrade firmware is inserted into the device.
• Ensure the network camera is on the same network segment as your video recorder.
• Ensure the network connection is valid and correctly configured.

Steps:

1. Go to **Main Menu** → **Camera**.
2. Select the camera you want to upgrade.

3. Click the upgrade icon.
4. Select your USB flash drive from the drop-down list.
5. Select the upgrade file and click **Upgrade**.
6. Click **OK** to start the upgrade. The camera will automatically restart once the upgrade is complete.

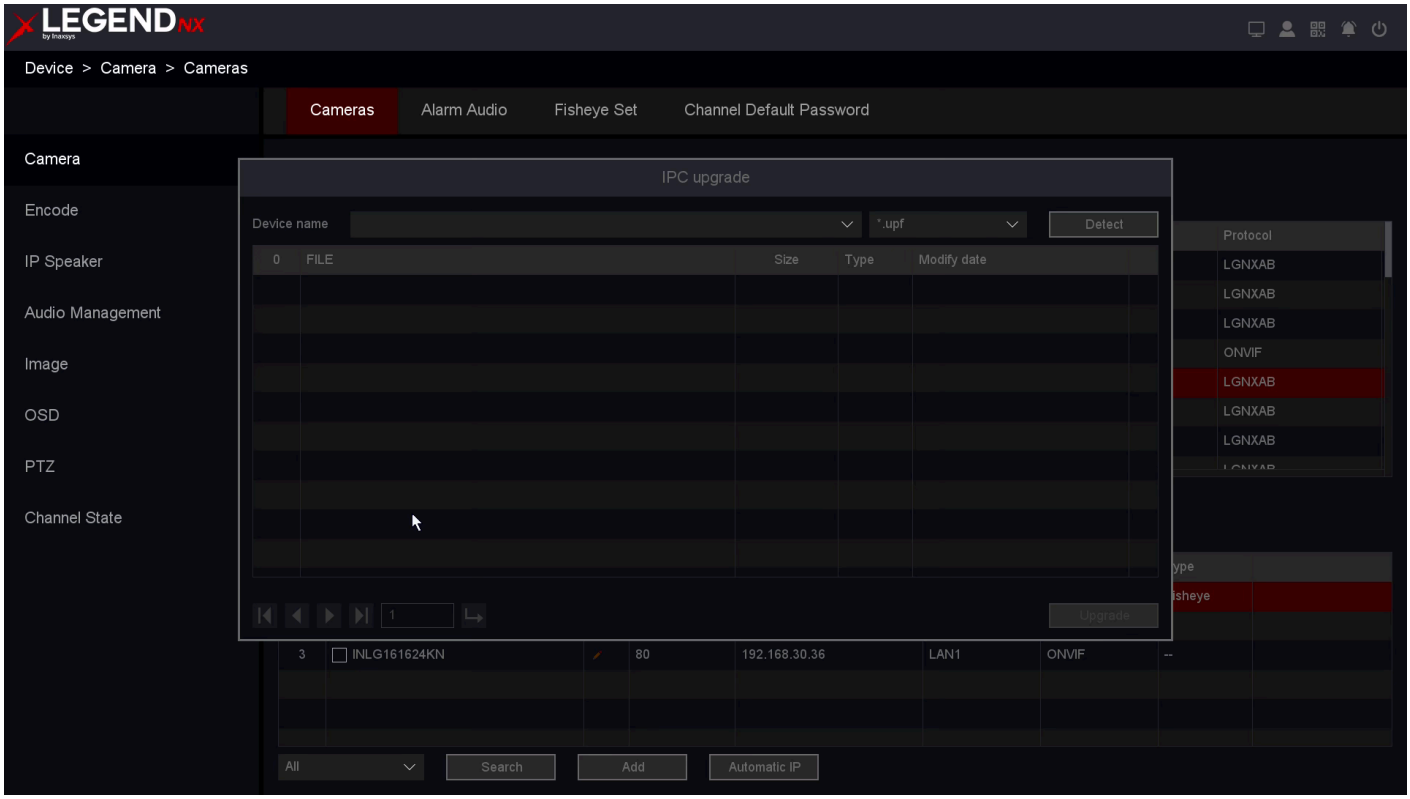


Figure 6-14 IP Camera Upgrade

Delete Camera

The camera can be removed using the delete function.

Before You Start

Ensure that the network camera you want to delete is selected.

Steps:

1. Go to **Main Menu** → **Channel** → **IP Channel** → **Channel Setting**.
2. Click the delete icon , or select the camera and click **Delete**.
3. Optional 1: Select the device(s) to be deleted and click **Delete**.
4. Optional 2: Click **Clear All** to remove all selected channels.
5. As shown in the figure below, click **OK** to confirm.

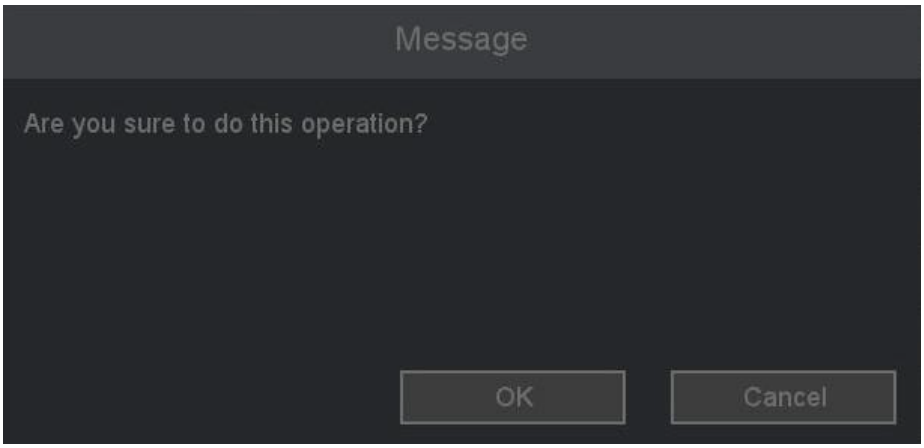


Figure 6-15 Delete

6.3.2 OSD Settings

Configure OSD (On-Screen Display) settings for the camera, including date format, camera name, and other display options.

Steps:

1. Go to **Main Menu** → **Camera** → **OSD**.
2. Select a camera.

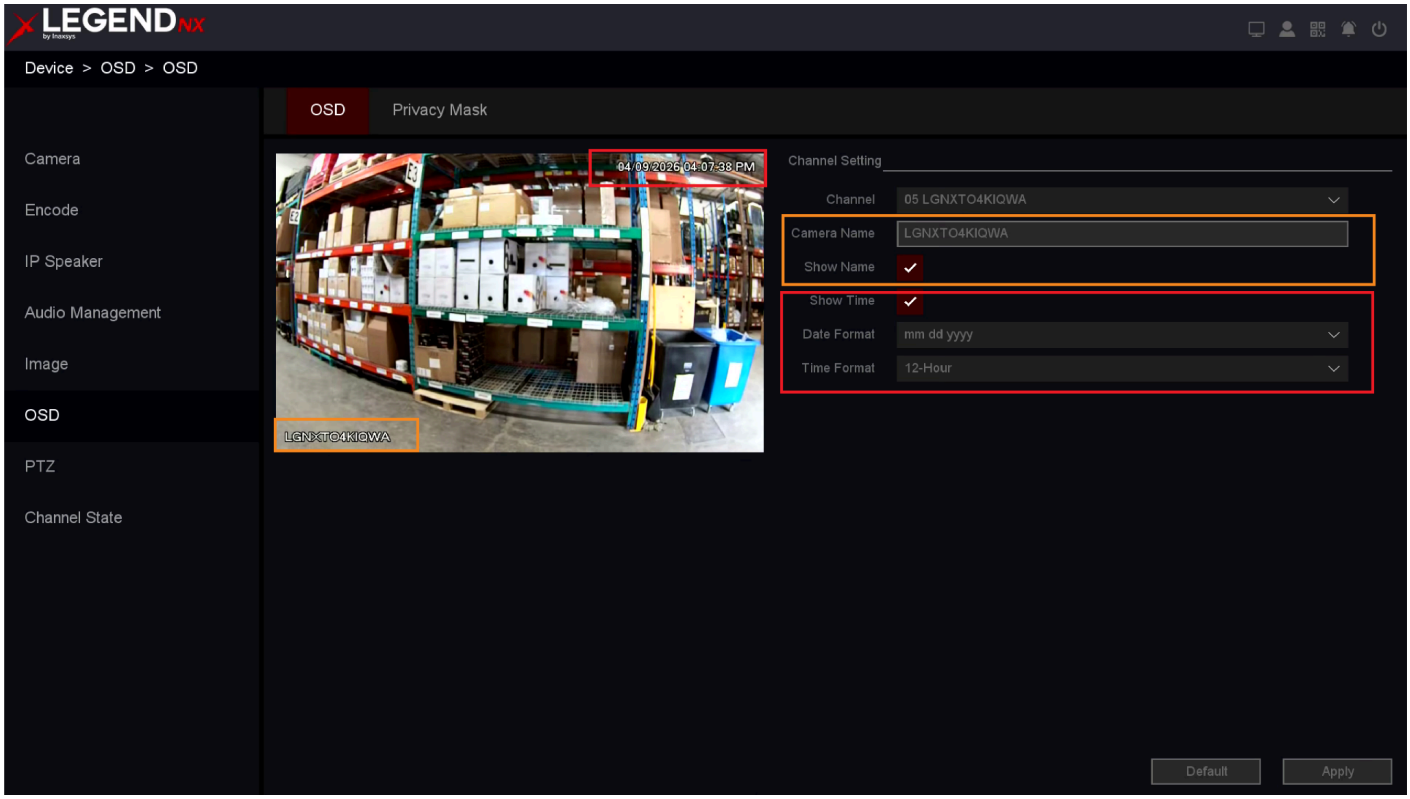


Figure 6-16 OSD

3. Configure the parameters as needed.
4. You can choose whether to display the camera name and time, and customize these settings as required.
5. Click **Apply**.

6.3.3 Event

Motion Detection

Motion detection allows the video recorder to detect moving objects within the monitored area and trigger alarms.

Steps:

1. Go to **Main Menu → Event → Detect → Motion**.

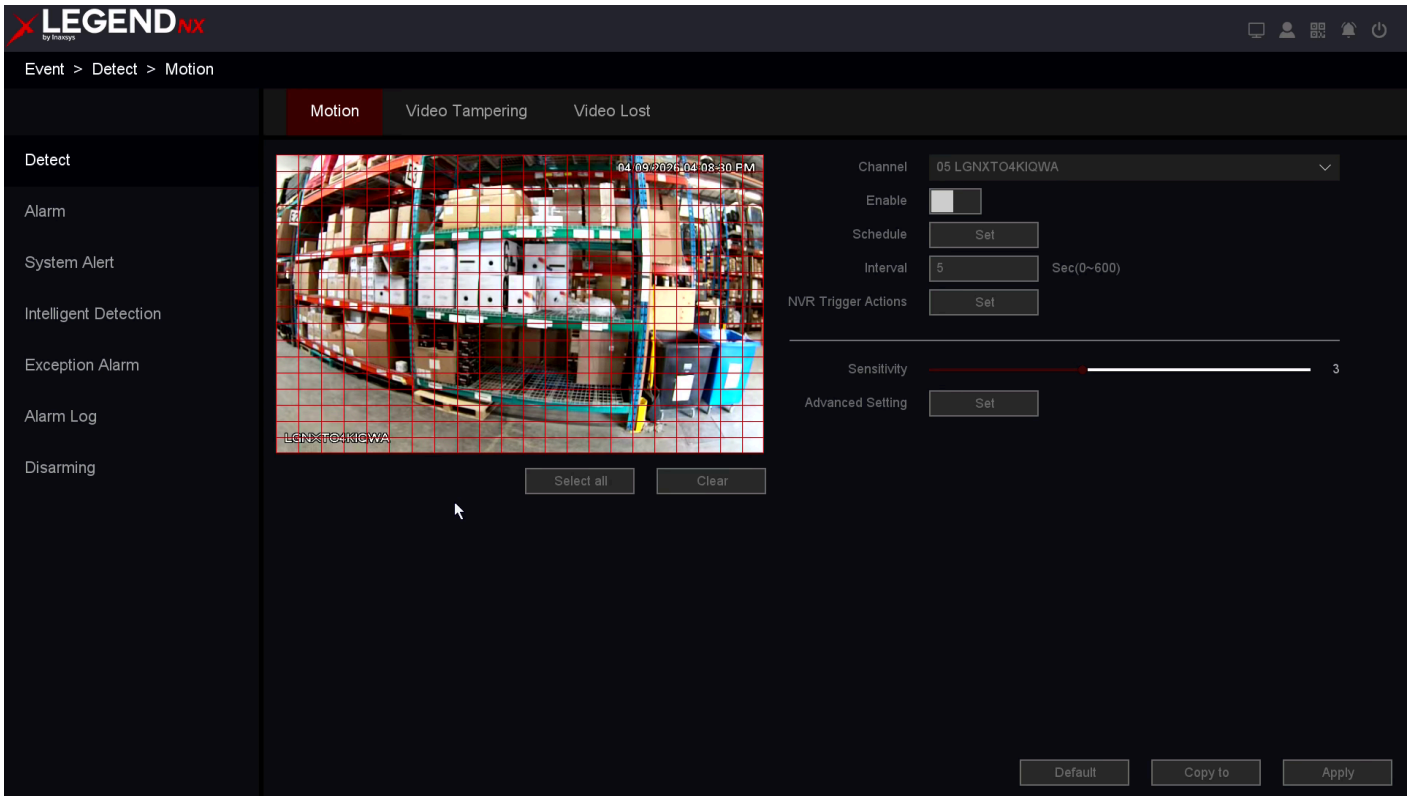


Figure 6-17 Motion Detection

2. Select a camera.
3. Enable the function by turning on **Enable**.
4. Configure the motion detection area.
   Click **Clear** or press and hold the left mouse button to clear or draw detection areas. By default, the first area covers the full screen.
   Click **Select All** to set the detection area to full screen. You can also drag within the preview window to define specific detection zones.
5. Set the arming schedule. Refer to **6.3.4 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.

7. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
8. Set the **Sensitivity** (1–100). The value represents how sensitive the system is to movement within the detection area. A value of 0 means the alarm is triggered only when the target fully enters the area, while 100 means the alarm is triggered as soon as the target begins to enter the area.
9. Configure **Advanced Setting**. Refer to **6.3.6 Configure Advanced Setting** for details.
10. Click **Apply**.

Line Crossing

Line crossing is a virtual boundary drawn on the live video. When a target crosses this line in a specified direction, the system triggers an alarm and performs configured linkage actions.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Perimeter Protection → Line Crossing**.
2. Enable **Line Crossing** by selecting the checkbox.
3. Click the settings icon to open the configuration window.

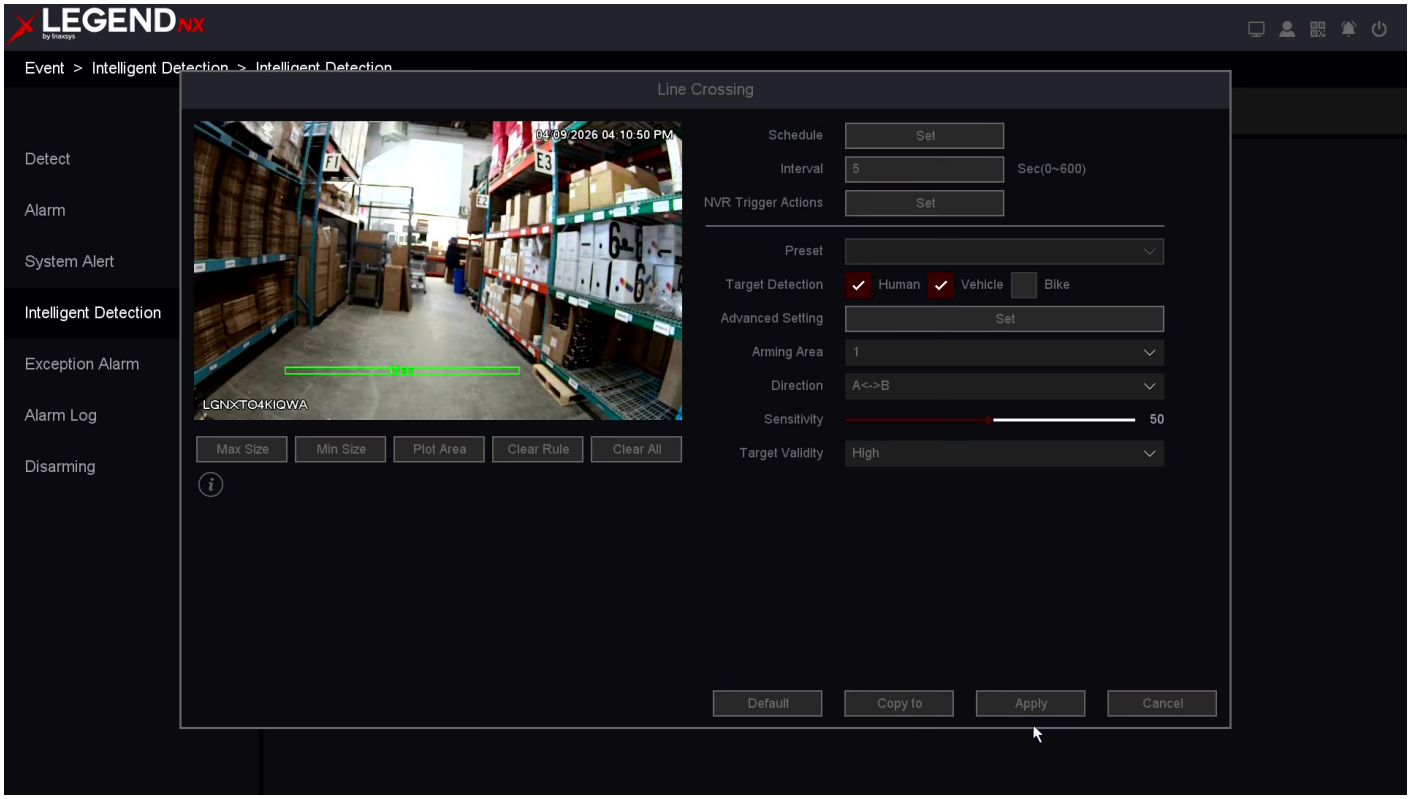


Figure 6-18 Line Crossing

4. Configure the line crossing rules and detection line. You can adjust the warning line by dragging the anchor points at both ends of the default line directly on the screen.

Max Size

If the detected object size exceeds the configured maximum size, no alarm will be triggered.

Min Size

If the detected object size is smaller than the configured minimum size, no alarm will be triggered.

Clear Area
Removes the currently defined detection area.

Clear All
Removes all defined detection areas.

5. Set the arming schedule. Refer to **6.3.4 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
8. Enable the **Human/Vehicle/Bike** filters if needed. When enabled, alarms are triggered only for the selected target types.
9. Configure **Advanced Setting**. Refer to **6.3.6 Configure Advanced Setting** for details.
10. Select the **Arming Area**. Up to four detection lines can be configured.
11. Select the **Direction**: **A↔B**, **A→B**, or **B→A**.

A↔B
Objects crossing the line in either direction will trigger an alarm.

A→B
Only objects crossing from side A to side B will trigger an alarm.

B→A
Only objects crossing from side B to side A will trigger an alarm.

12. Set the **Sensitivity** (1–100). This value represents how sensitive the system is to targets crossing the line. A value of 0 means the alarm is triggered only when the target fully crosses the line, while 100 means the alarm is triggered as soon as the target begins to cross.
13. Select **Target Validity** for the event. The default is **Higher**. Higher values improve detection accuracy for human and vehicle targets.
14. Click Apply.

Area Intrusion

Area intrusion allows you to define one or more detection zones within the monitoring area. When an object enters the defined area and meets the configured size and duration conditions, an alarm is triggered and the configured actions are executed.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Perimeter Protection → Area Intrusion**.
2. Enable **Area Intrusion** by selecting the checkbox.
3. Click the settings icon to open the configuration window.

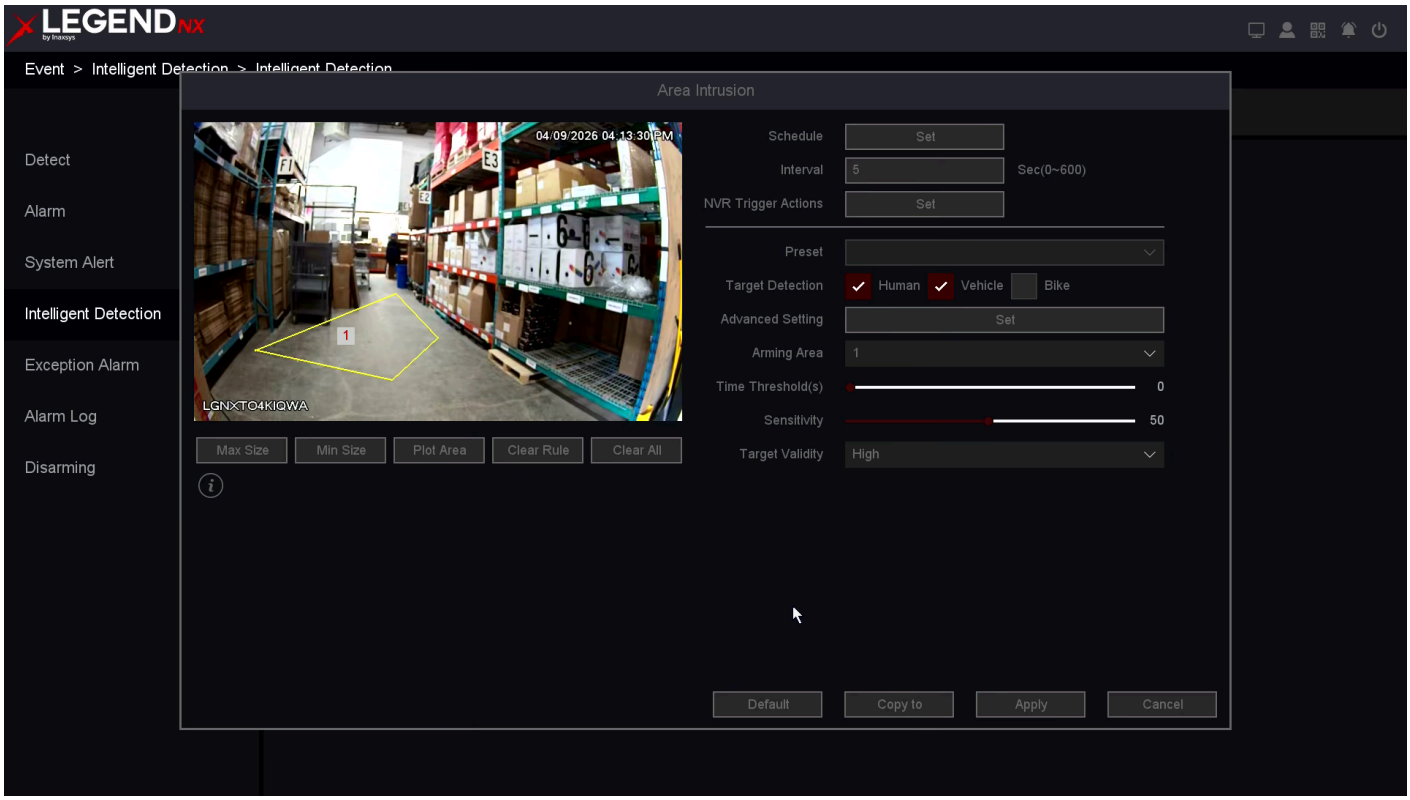


Figure 6-19 Intrusion Detection

4. Click **Plot Area**, then click four points in the video window using the left mouse button to draw the detection area.

Max Size

If the detected object size exceeds the configured maximum size, no alarm will be triggered.

Min Size

If the detected object size is smaller than the configured minimum size, no alarm will be triggered.

Clear Area

Removes the currently defined detection area.

Clear All

Removes all defined detection areas.

5. Set the arming schedule. Refer to **6.3.3 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.4 Configure Alarm Trigger Process** for details.
8. Enable the **Human/Vehicle/Bike** filters if needed. When enabled, alarms are triggered only for the selected target types.
9. Configure **Advanced Setting**. Refer to **6.3.5 Configure Advanced Setting** for details.
10. Select the **Arming Area**. Up to four areas can be configured.
11. Set the **Threshold**. An alarm is triggered when a target enters the defined area and remains there longer than the configured time (0–10 seconds adjustable).

12. Set the **Sensitivity** (1–100). This value represents how sensitive the system is to intrusion. A value of 0 means the alarm is triggered only when the target fully enters the area, while 100 means the alarm is triggered as soon as the target begins to enter the area.
13. Select **Target Validity** for the event. The default is **Higher**. Higher values improve detection accuracy for human and vehicle targets.
14. Click **Apply**.

Region Entrance

Region Entrance allows you to define one or more detection areas within the monitoring scene. When an object enters a defined area, an alarm is triggered and the configured actions are executed.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Perimeter Protection → Region Entrance**.
2. Enable **Region Entrance** by selecting the checkbox.
3. Click the settings icon to open the configuration window.

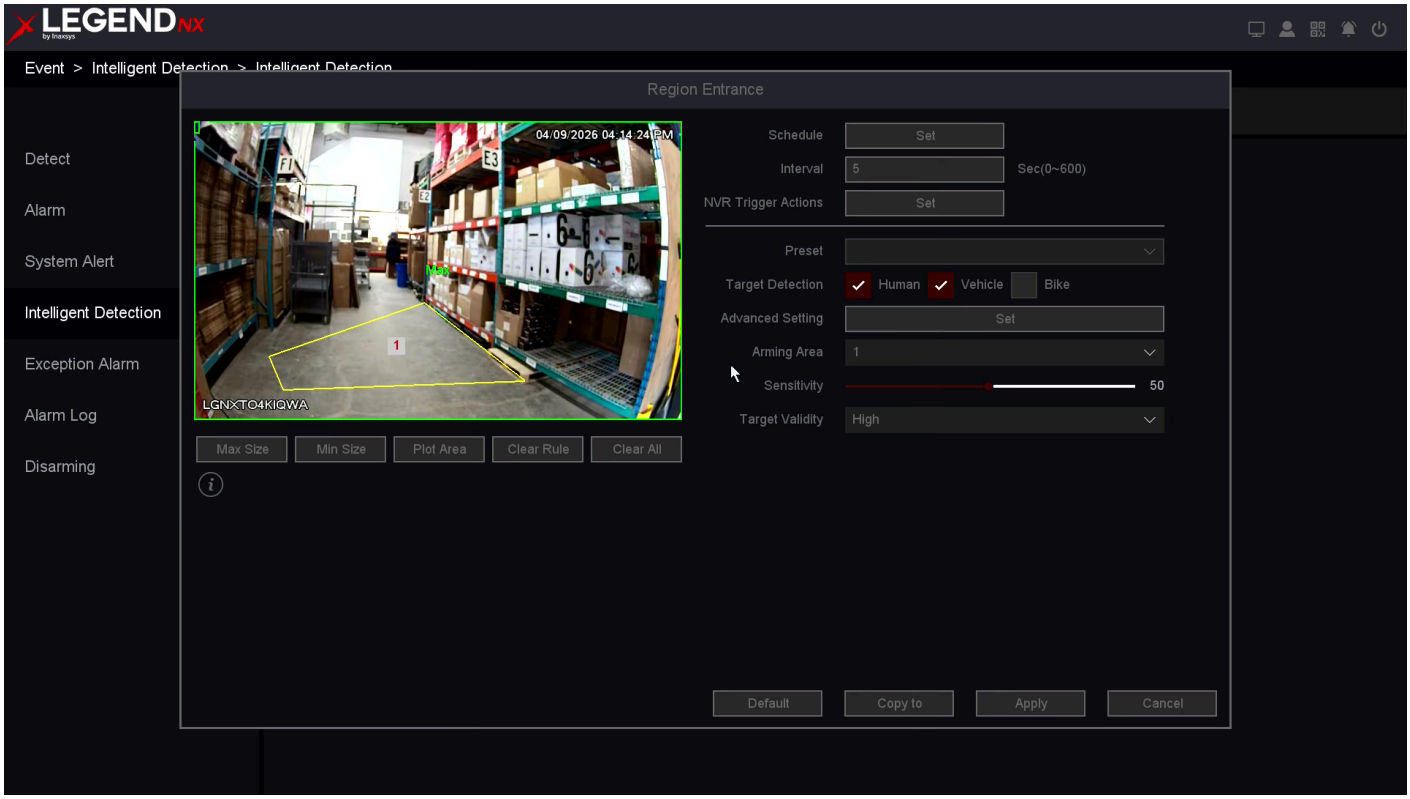


Figure 6-20 Region Entrance Detection

4. Click **Plot Area**, then click four points in the video window using the left mouse button to draw the detection area.

Max Size

If the detected object size exceeds the configured maximum size, no alarm will be triggered.

Min Size

If the detected object size is smaller than the configured minimum size, no alarm will be triggered.

Clear Area
Removes the currently defined detection area.

Clear All
Removes all defined detection areas.

5. Set the arming schedule. Refer to **6.3.3 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.4 Configure Alarm Trigger Process** for details.
8. Enable the **Human/Vehicle/Bike** filters if required. When enabled, alarms are triggered only for the selected target types.
9. Configure **Advanced Setting**. Refer to **6.3.5 Configure Advanced Setting** for details.
10. Select the **Arming Area**. Up to four areas can be configured.
11. Set the **Sensitivity** (1–100). This value represents how sensitive the system is to targets entering the area. A value of 0 means the alarm is triggered only when the target fully enters the area, while 100 means the alarm is triggered as soon as the target begins to enter the area.
12. Select **Target Validity** for the event. The default is **Higher**. Higher values improve detection accuracy for human and vehicle targets.
13. Click **Apply**.

Region Exiting

Region Exiting is used to detect whether a target leaves a defined monitoring area. When the system detects a target exiting the specified area, configured alarm actions are triggered.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Perimeter Protection → Region Exiting**.
2. Enable **Region Exiting** by selecting the checkbox.
3. Click the settings icon to open the configuration window.

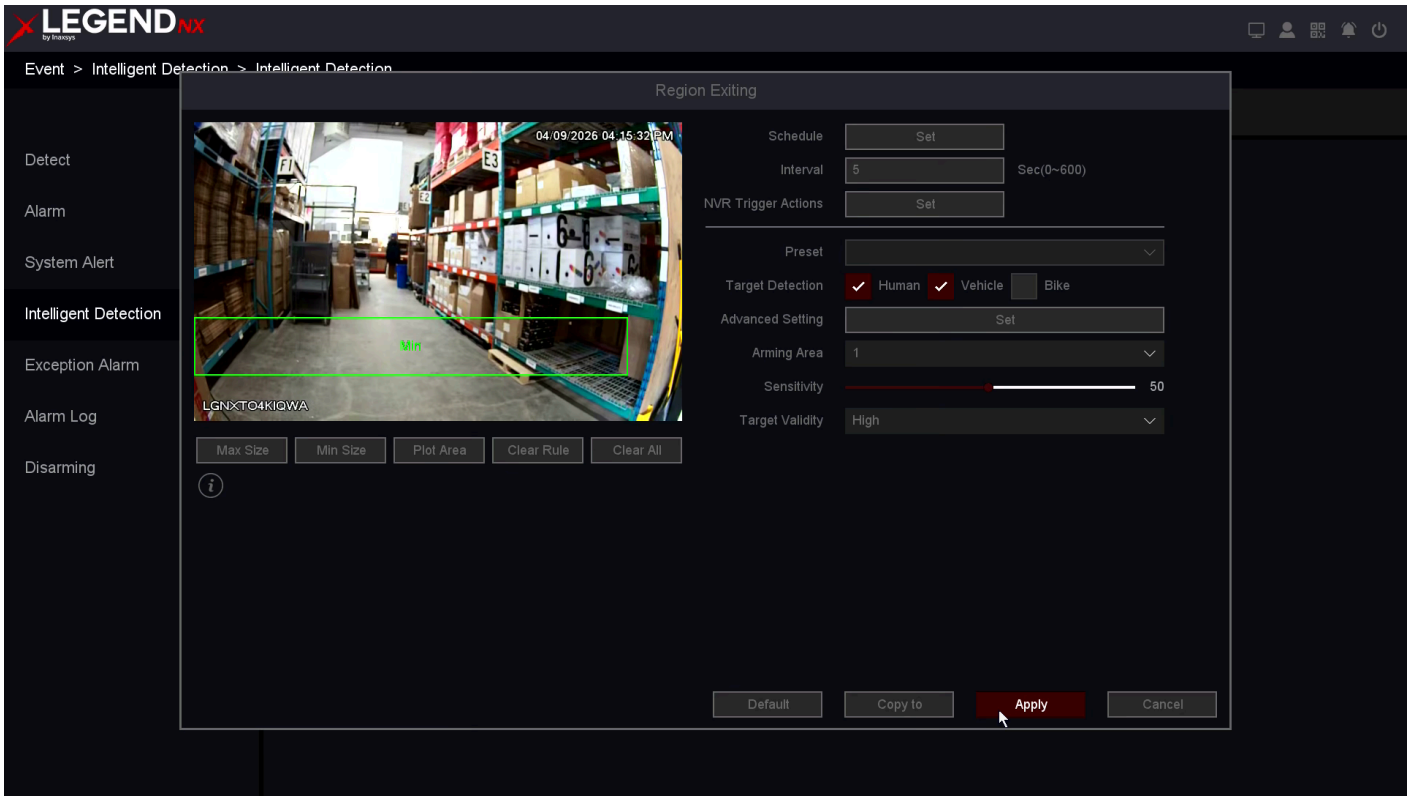


Figure 6-21 Region Exiting Detection

4. Click **Plot Area**, then click four points in the video window using the left mouse button to draw the detection area.

Max Size

If the detected object size exceeds the configured maximum size, no alarm will be triggered.

Min Size

If the detected object size is smaller than the configured minimum size, no alarm will be triggered.

Clear Area

Removes the currently defined detection area.

Clear All

Removes all defined detection areas.

5. Set the arming schedule. Refer to **6.3.4 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
8. Enable the **Human/Vehicle/Bike** filters if required. When enabled, alarms are triggered only for the selected target types.
9. Configure **Advanced Setting**. Refer to **6.3.6 Configure Advanced Setting** for details.
10. Select the **Arming Area**. Up to four areas can be configured.
11. Set the **Sensitivity** (1–100). This value represents how sensitive the system is to targets exiting the area. A value of 0 means the alarm is triggered only when the target has fully exited the area, while 100 means the alarm is triggered as soon as the target begins to exit the area.

12. Select **Target Validity** for the event. The default is **Higher**. Higher values improve detection accuracy for human and vehicle targets.
13. Click **Apply**.

6.3.4 Configure Arming Schedule

Steps:

1. Click **Arming Schedule**.
2. Select a day of the week and configure the time periods. Up to six time periods can be set for each day.

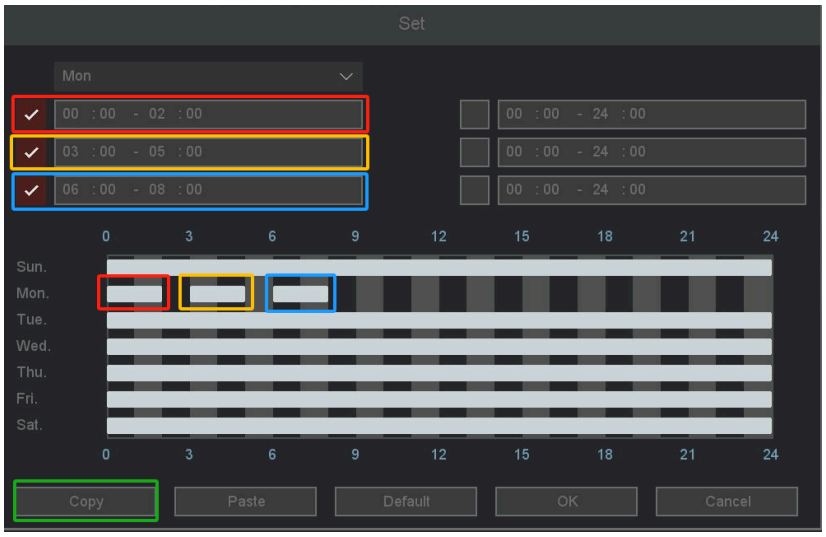


Figure 6-22 Set Arming Schedule

Note
Time periods must not overlap or repeat.

3. Edit the time periods (1–6) during which alarms should be triggered, and enable the corresponding checkboxes as shown in the figure.
4. Click **OK**.

Note
Configure the required time periods (1–6) and enable them as needed.

6.3.5 Configure Alarm Trigger Process

The alarm trigger process is activated when an alarm or exception occurs.

Steps:

1. Click **Trigger Process**.

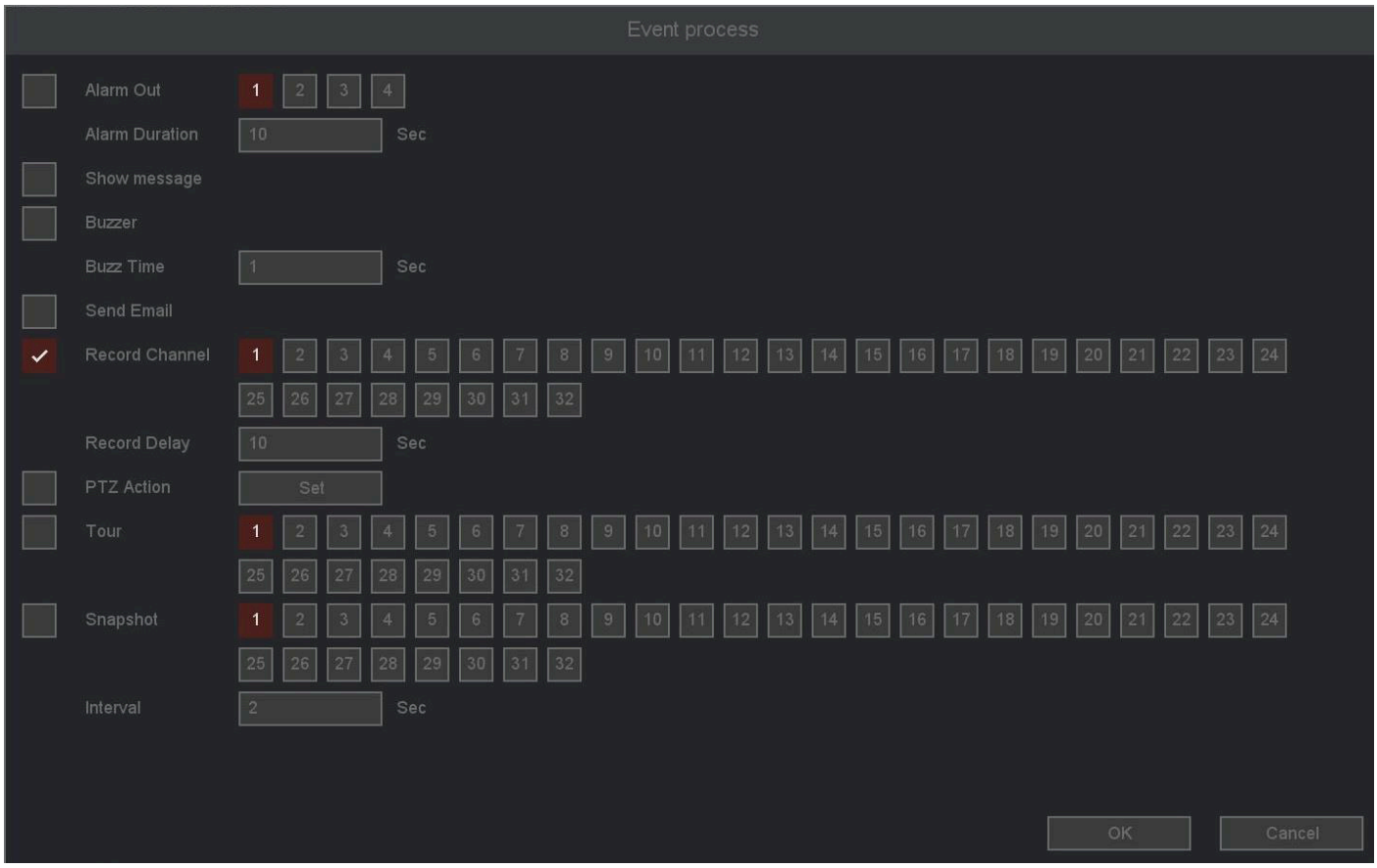


Figure 6-23 Set Trigger Process

2. Configure the trigger actions, including normal trigger process, alarm output, and linked channels.

Alarm Out

Displays the alarm channel on the local monitor when an alarm is triggered. You must select the corresponding channel(s) in **Trigger Channel**.

Show Message

Displays a popup message with the alarm channel on the local monitor. You must select the corresponding channel(s) in **Trigger Channel**.

Buzzer & Buzz Time

Triggers an audible buzzer when an alarm occurs. The duration can be configured.

Send Email

Sends an email notification containing alarm information when an alarm is triggered.

Record Channel

Starts recording on the selected channel(s) when an alarm is triggered, and links the recording for playback.

Record Delay

Defines how long recording continues after the alarm has ended.

PTZ Action
Triggers PTZ actions (such as preset, patrol, or pattern) when an event occurs.

Tour
Automatically cycles through selected channels on the screen when an alarm is triggered.

Snapshot
Captures images for the selected channel(s) when an alarm is triggered.

Interval
Defines the interval between snapshots while the alarm is active.

3. Click **OK**.

Note
- For some network cameras, alarm linkage can include audio or light alerts.
- Ensure your camera supports audio and light alarm linkage.
- Verify that audio output and volume are properly configured.
- To configure audio and light parameters, log in to the network camera via a web browser.

6.3.6 Configure Advanced Setting

Advanced settings are activated when an alarm or exception occurs. These settings include configurations for red and blue lights, sirens, and white lights.

Red and Blue Lights
You can configure the red and blue lights to flash when an event is triggered.

Schedule
Set the time schedule during which the lighting will be active.

Flash Rate
Set the flashing frequency of the red and blue lights.

Stay Time
Set the duration for which the red and blue lights remain active.

File
Select the siren sound to be played when an event is triggered.

Play Count
Set the number of times the siren will sound.

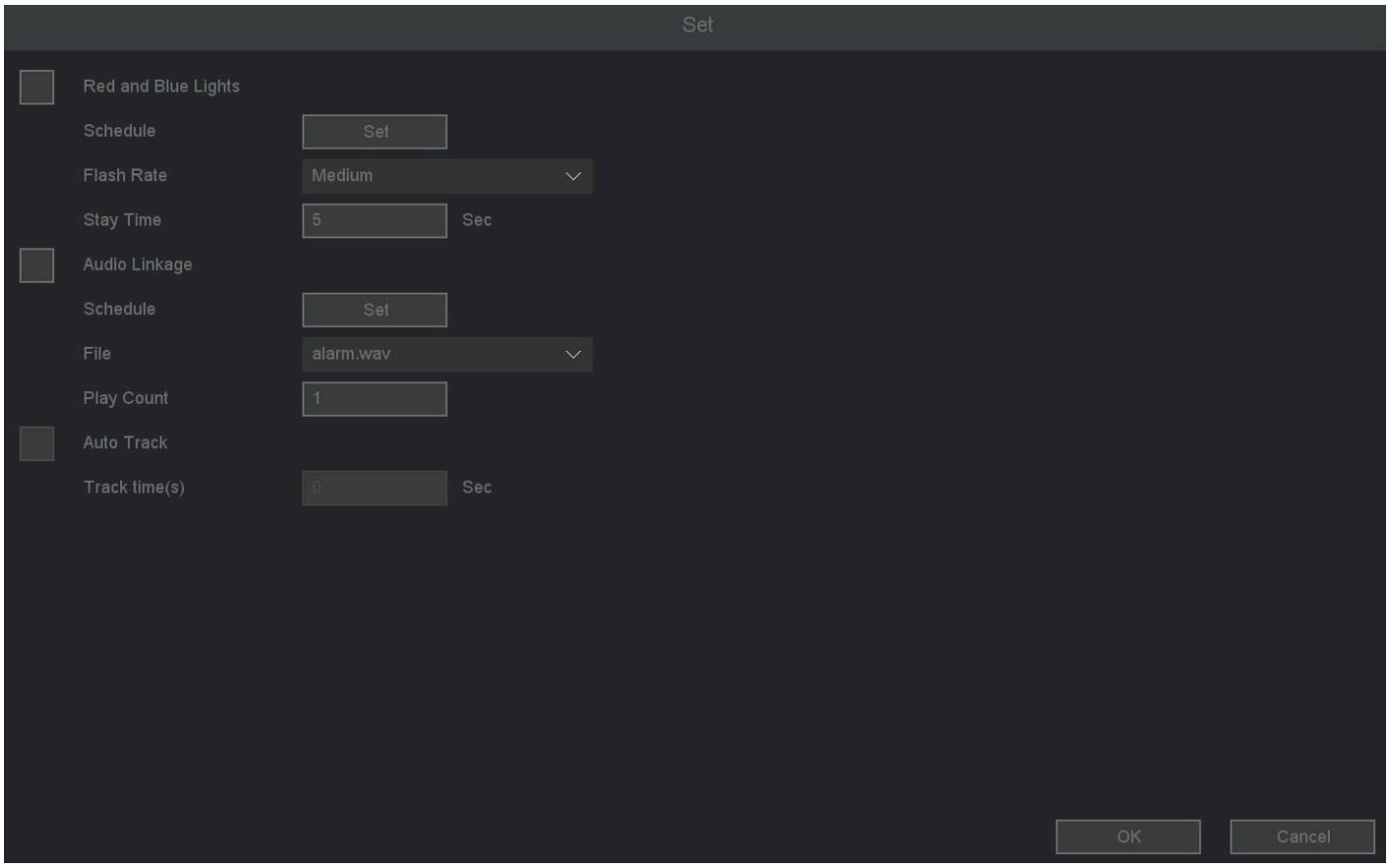


Figure 6-24 Advanced Setting

6.4 Recording Management

6.4.1 Storage

Initialize HDD

A newly installed hard disk drive (HDD) must be initialized before it can be used to store video and data.

Before You Start

Install at least one HDD in the video recorder. For detailed instructions, refer to **1.4 HDD Installation**.

Steps:

1. Go to **Main Menu** → **Storage** → **Base**.

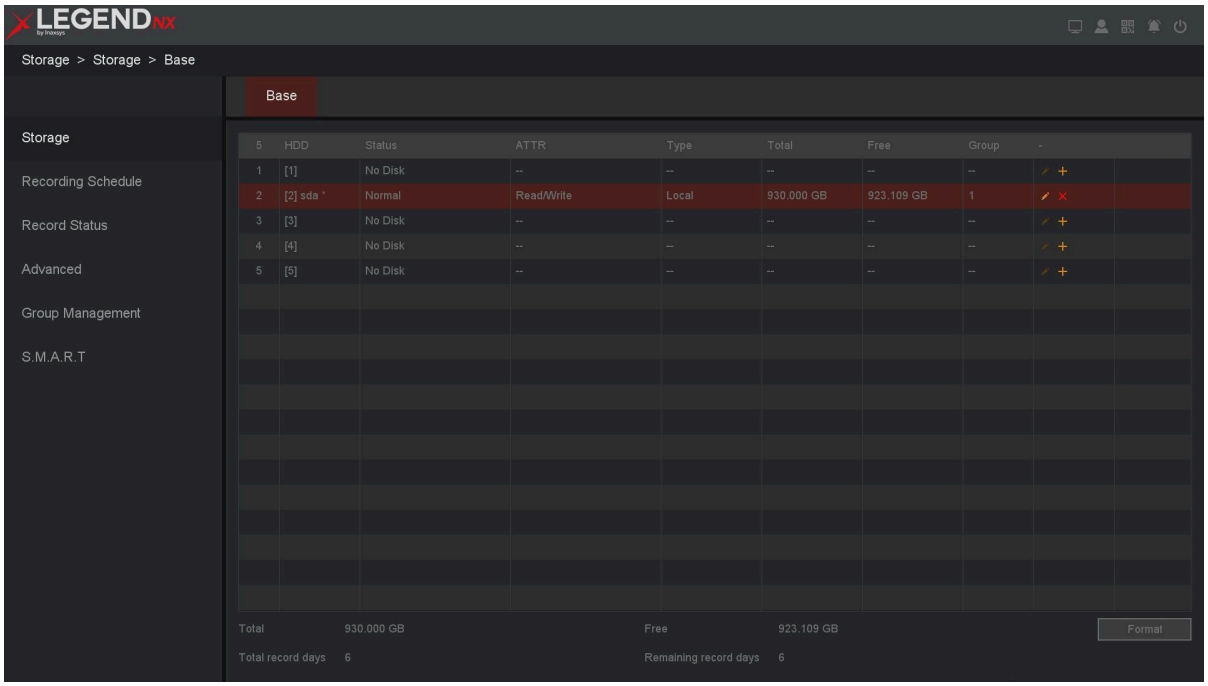


Figure 6-25 Base

2. Select an HDD.
3. Click **Format**.
4. Click **OK** to continue.

Note

If the HDD has database errors, contact professional technical support for repair.

HDD Setting

This section displays information about the installed hard drives, including status, serial number, name, attributes, type, total capacity, remaining capacity, group assignment, as well as options for editing and uninstalling/loading.

HDD

Displays the HDD identifier, such as “[1] sda” or “[2] sdb”.

Status

Displays the HDD status, such as “Unformatted,” “Normal,” or “No Disk”.

ATTR

Three modes are available: **Read/Write**, **Read Only**, and **Redundant**.

• **Read/Write**: Supports both reading and writing. Data can be stored and playback is supported.
• **Read Only**: Supports read operations only. Playback is available, but data cannot be written.
• **Redundant**: Uses two hard drives—one for read/write and one as a backup. Video data is written simultaneously to both drives to ensure data security.

Type

Displays the HDD connection type.

Total
Displays the total storage capacity of the HDD.

Free
Displays the remaining available storage capacity.

Group
Assigns the HDD to a specific group. Video from selected channels can be recorded to a designated HDD group. Refer to HDD group configuration for details.

Uninstall
Removes the HDD from the system.

Add
Adds an HDD that is currently in an uninstalled state.

Format
Formats the HDD manually.

Total Record Days
Displays the total number of days the HDD can store recordings without overwriting.

Remaining Record Days
Displays how many days of recording can still be stored without overwriting.

Steps:

1. Click **HDD Set**. The configuration window will open as shown above.
2. Configure the parameters as required.
3. Click **OK**

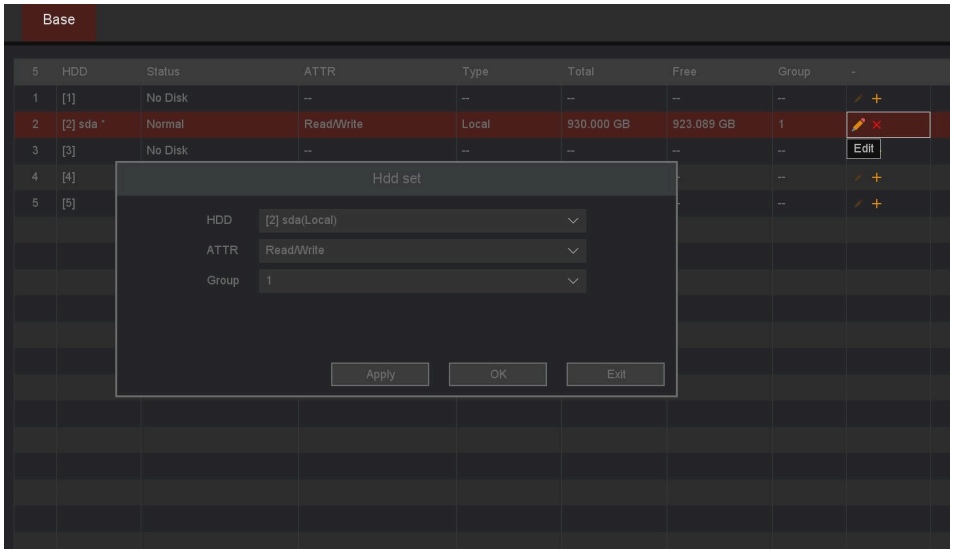


Figure 6-26 Edit

6.4.2 Configure Recording Schedule

Configure the recording schedule by setting the relevant parameters. The video recorder will automatically start and stop recording according to the configured schedule. Before performing these operations, ensure that the HDD has been installed and formatted. If not, install and initialize the HDD first. For detailed information, refer to **6.4.1 Storage / Initialize HDD**.

Configure Recording

Steps:

1. Go to **Main Menu → Storage → Schedule**.

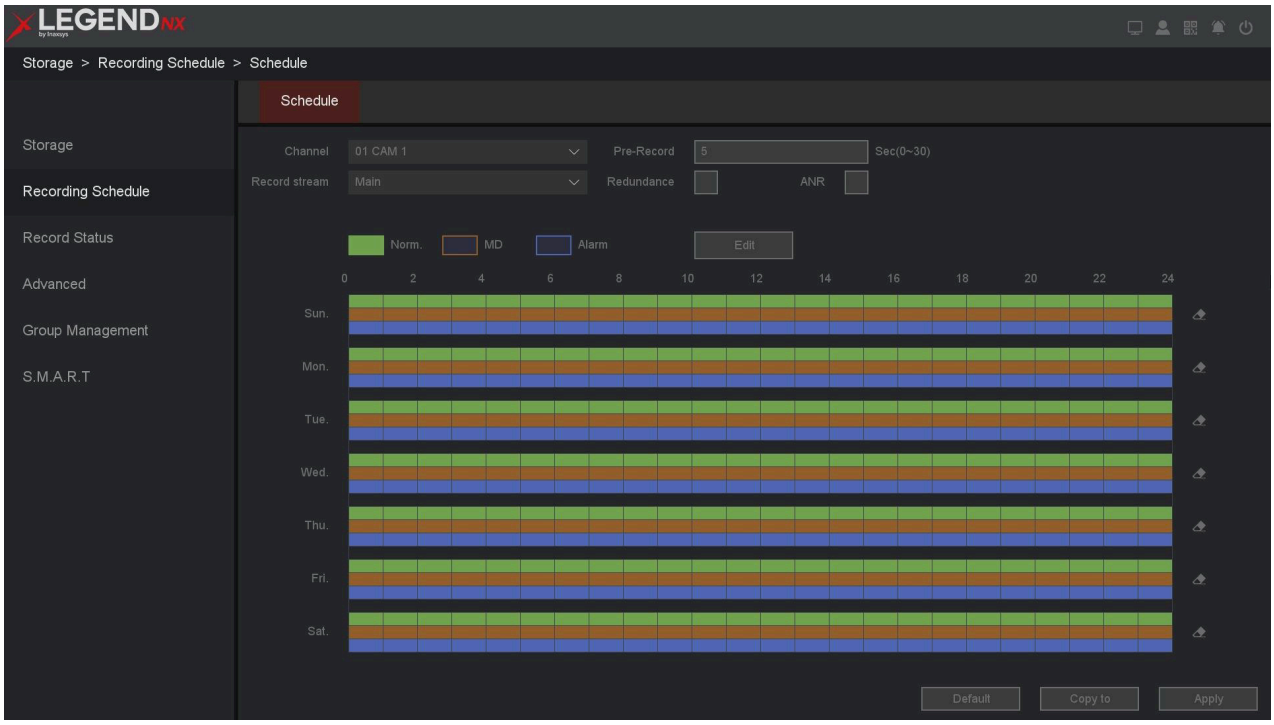


Figure 6-27 Schedule

2. Select the channel.
3. Set **Pre-Record** (the time for pre-recording event video, ranging from 0 to 30 seconds).
4. Select **Main Stream** recording or **Sub Stream** recording (some devices with fewer than 16 channels support dual-stream recording).
5. Configure the recording schedule. Refer to **Edit Schedule** below for details.
6. Click **Apply**.

Note

• ANR: When the IP Camera is disconnected from the NVR and records locally to its TF card, the NVR will retrieve and supplement the recordings from the IP Camera's TF card once the connection is restored.

• Redundancy: If a redundant HDD is installed, recordings will be backed up to the redundant HDD. Refer to Chapter 4.4.3 for details.

• If multiple channels are configured with the pre-record function, the pre-record time may be less than 30 seconds (maximum value), as this function consumes system resources and automatically adjusts to support multiple channels simultaneously.

Edit Schedule

OPTION 1:

You can click the **Edit** button to enter the editing interface and configure the recording schedule.

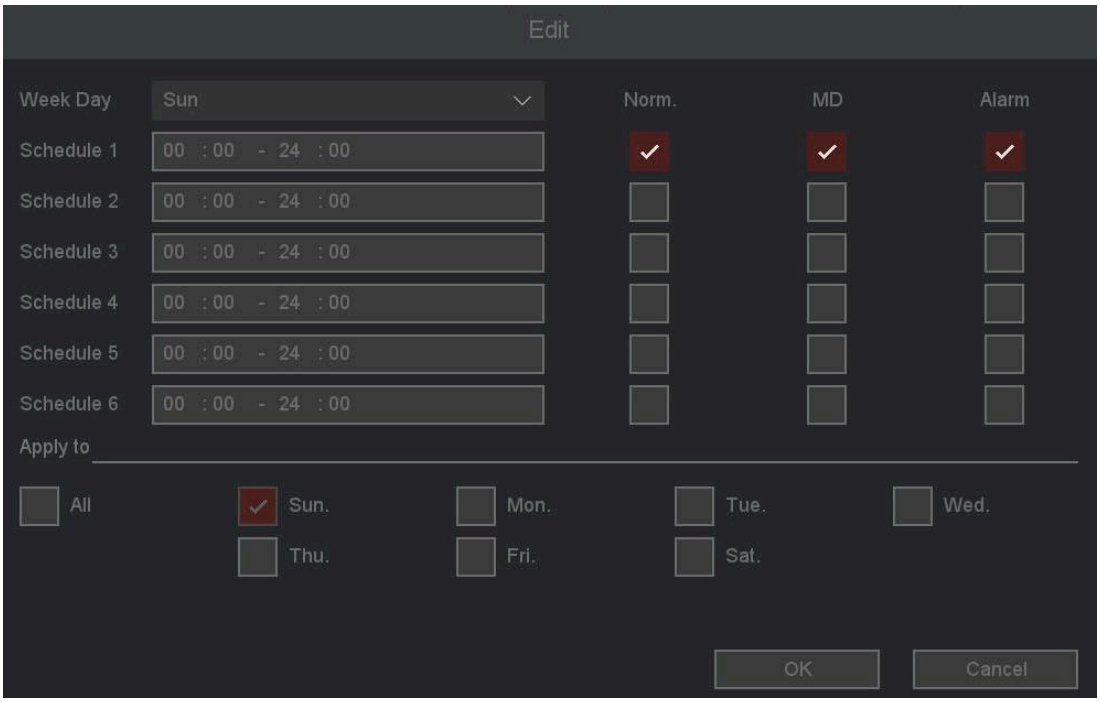


Figure 6-28 Edit

Week Day
The day for which the schedule is set, from Sunday to Saturday.

Schedule 1–6
The recording time periods. Up to six time periods can be configured per day.

Norm
The recording type for normal video.

MD
The recording type for motion detection video.

Alarm
The recording type for alarm-triggered video.

Steps:

1. Click the **Edit** button to enter the editing interface.
2. Select the **Week Day** (Sunday to Saturday).
3. Set the time periods for recording.
4. Select **Alarm**, **MD**, or **Norm** as the recording type.
5. Click **OK**.

Note
You can select **All** to apply the schedule to all weekdays at once, or select multiple days as needed. If

Norm, **MD**, and **Alarm** are selected simultaneously, the recording priority is: **Alarm > MD > Norm**. If multiple event types occur at the same time, the recording will be saved as **Alarm** video.

OPTION 2:

You can also edit the schedule directly on the graphical configuration screen, as shown below.

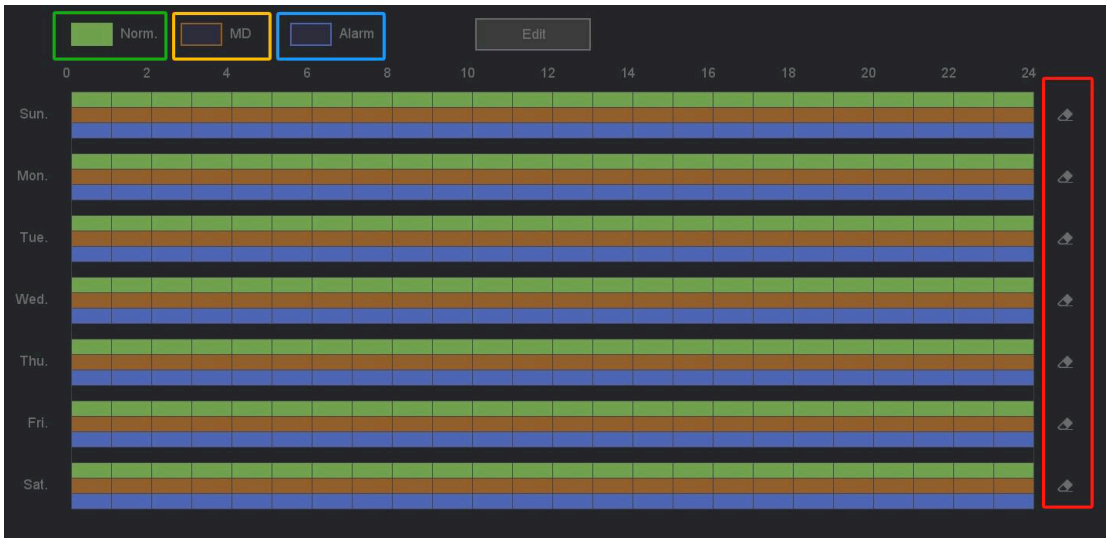


Figure 6-29 Schedule

Steps:

1. Select **Norm**, **MD**, or **Alarm** in the upper-left corner.
2. Press and hold the left mouse button, then drag across the corresponding time bar.
3. If **Norm** is selected, dragging the mouse will modify the green section of the bar. The first drag selects an area; dragging again deselects it, and so on.
4. Click the **eraser icon** to clear the entire bar at once.
5. After completing all settings, click **Apply** to activate them.
6. Optional: Click **Copy To** to apply the current channel settings to other channels.

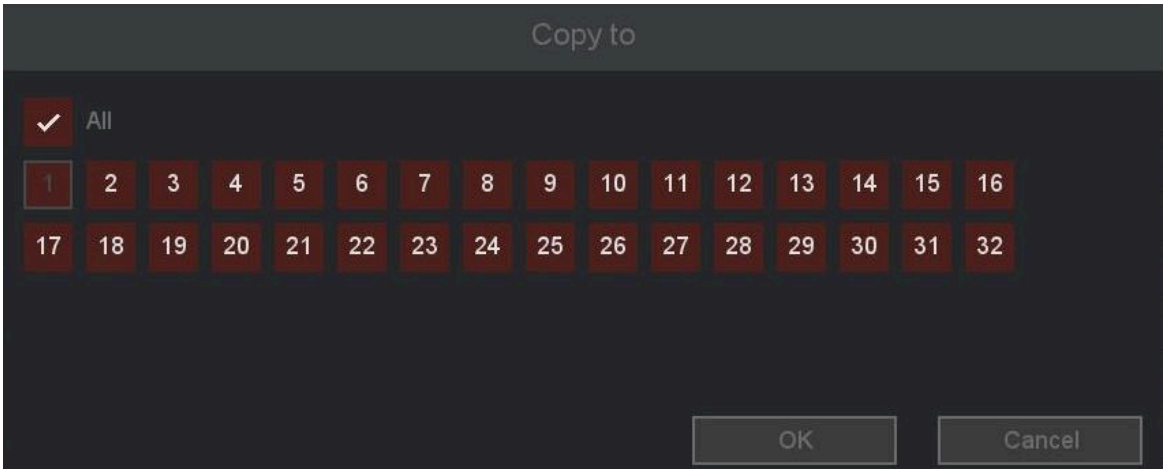


Figure 6-30 Copy to

Note
Click **Default** to reset all settings.

Configure MD Recording

You can configure recording triggered by motion detection.

Steps:

1. Select **MD** in the upper-left corner.
2. Press and hold the left mouse button, then drag across the corresponding yellow bar to select or clear time periods.
3. Optional: Click the **eraser icon**  to clear the entire bar at once.
4. After completing all settings, click **Apply** to activate them.
5. Optional: Click **Copy To** to apply the current channel settings to other channels.

Configure Alarm Recording

You can configure recording triggered by **Line Crossing Detection**, **Intrusion Detection**, **Region Entrance**, and similar events.

Steps:

1. Select **Alarm** in the upper-left corner.
2. Press and hold the left mouse button, then drag across the corresponding blue bar to select or clear time periods.
3. Optional: Click the **eraser icon**  to clear the entire bar at once.
4. After completing all settings, click **Apply** to activate them.
5. Optional: Click **Copy To** to apply the current channel settings to other channels.

6.4.3 Configuring Video Encoding

By configuring encoding parameters, you can define the settings that affect image quality, such as compression type, resolution, frame rate, bit rate type, and quality.

The NVR supports dual-stream encoding. You can configure both the main stream and sub-stream encoding on this screen.

Steps:

1. Go to **Main Menu** → **Channel** → **Encode**.
2. Configure the video encoding parameters as required.

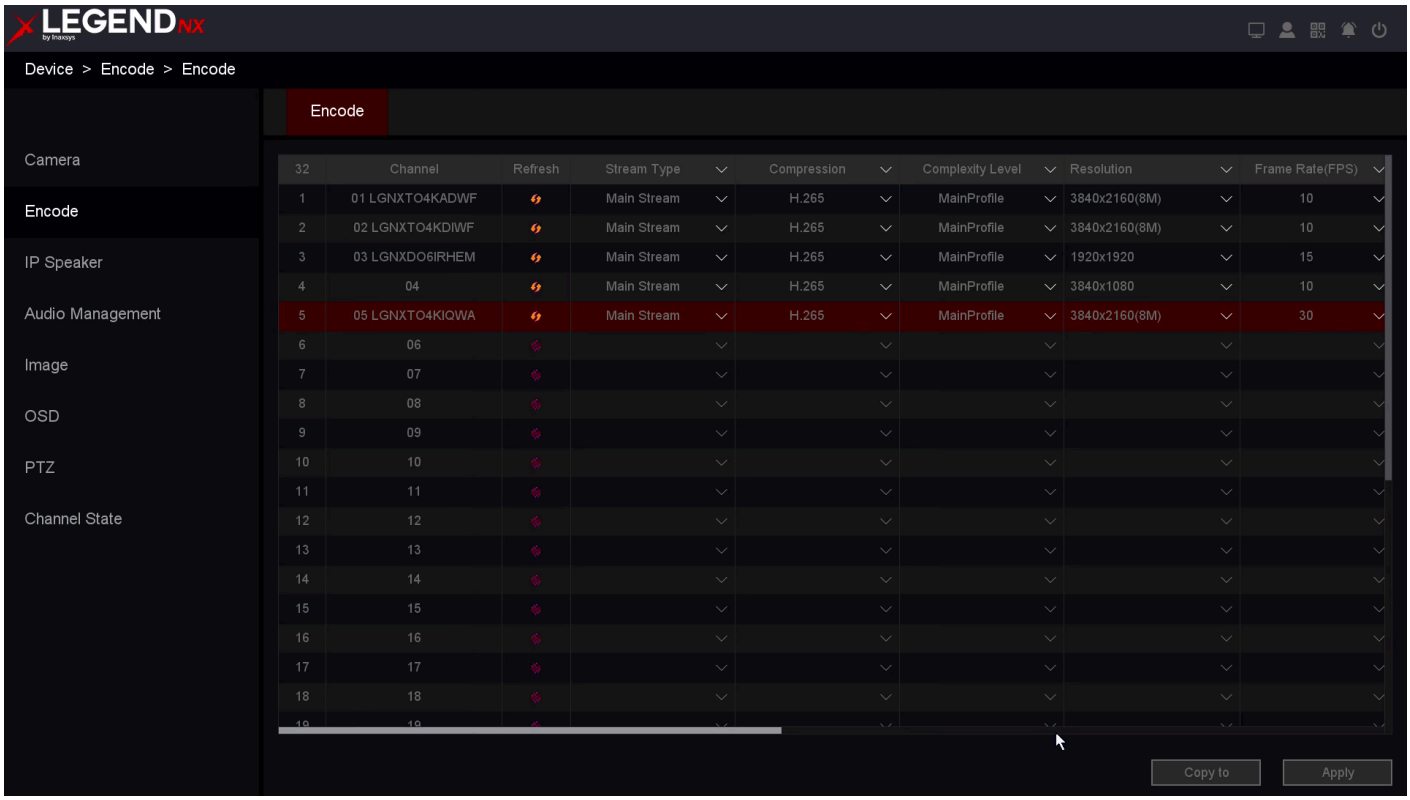


Figure 6-31 Encode

Channel

Select the channel to configure.

Refresh

Click to refresh the encoding parameters of the IP channel.

Main Stream

The main stream is the primary stream used for recording to the hard disk drive. It directly determines video quality and image size. Compared with the sub-stream, it provides higher quality video with higher resolution and frame rate.

Sub Stream

The sub-stream is a secondary stream that runs alongside the main stream. It helps reduce outgoing bandwidth usage without affecting the main recording quality. It is typically used for remote viewing, such as on mobile applications, and is especially useful when network bandwidth is limited.

Compression

H.265 is the encoding compression protocol. The system also supports H.264 IP cameras.

Resolution

Resolution indicates the level of detail in an image. The higher the resolution, the greater the detail. It is defined by the number of pixels in width × height (e.g., 1024 × 768).

Frame Rate

Frame rate refers to the number of frames captured per second. A higher frame rate provides smoother video, especially in scenes with movement.

Bitrate

Bitrate (in Kbit/s or Mbit/s) defines the amount of data transmitted per unit of time.

H.264+ / H.265+

Enable smart encoding technology to reduce HDD storage usage by up to 80%–90% in static scenes.

Audio

Configure the audio encoding parameters for the selected channel as shown below.

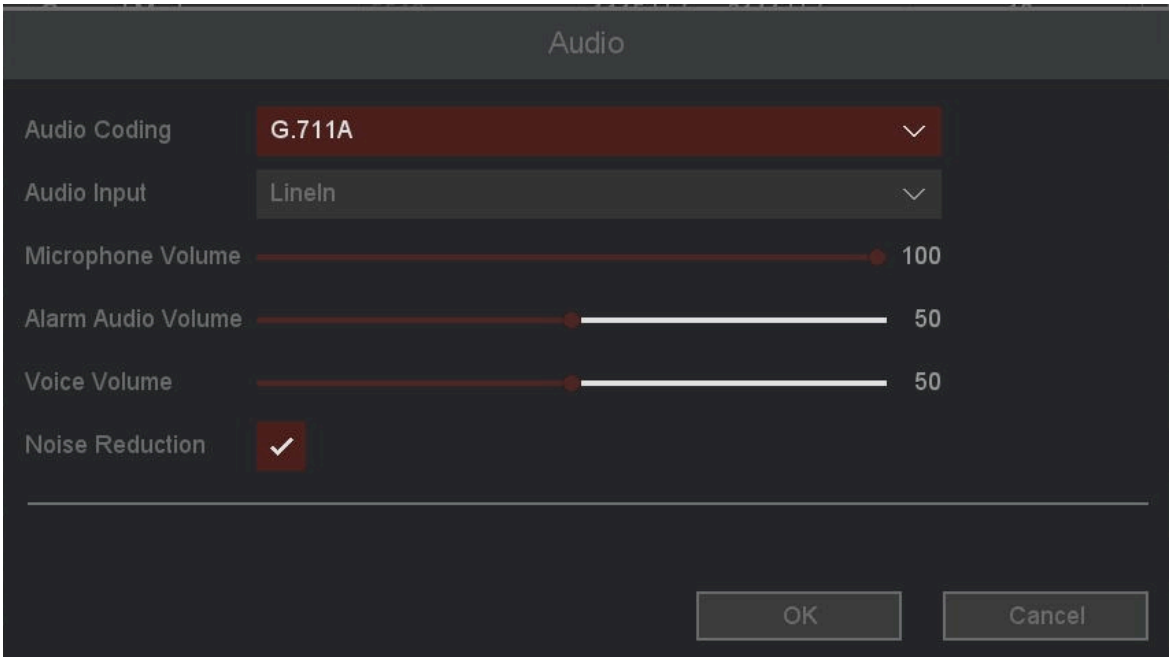


Figure 6-32 Audio

Note

Higher resolution, frame rate, and bitrate improve video quality but also require more bandwidth and consume more storage space on the hard disk drive.

3. Click **Apply**.
4. Optional: You can copy the configuration of selected channels to other channels by clicking **Copy To**. Select the target channels and save the settings.

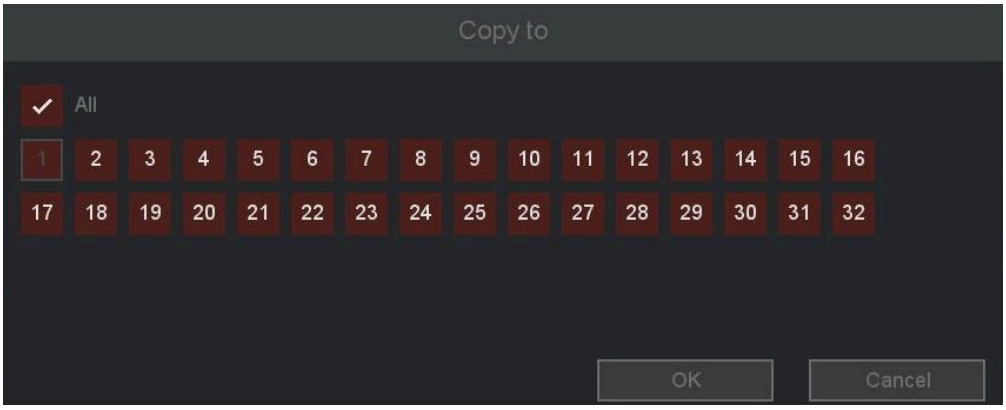


Figure 6-33 Copy

7. Maintenance

7.1 Restore Default

Steps:

1. Go to **Main Menu → System → Config → Default**.

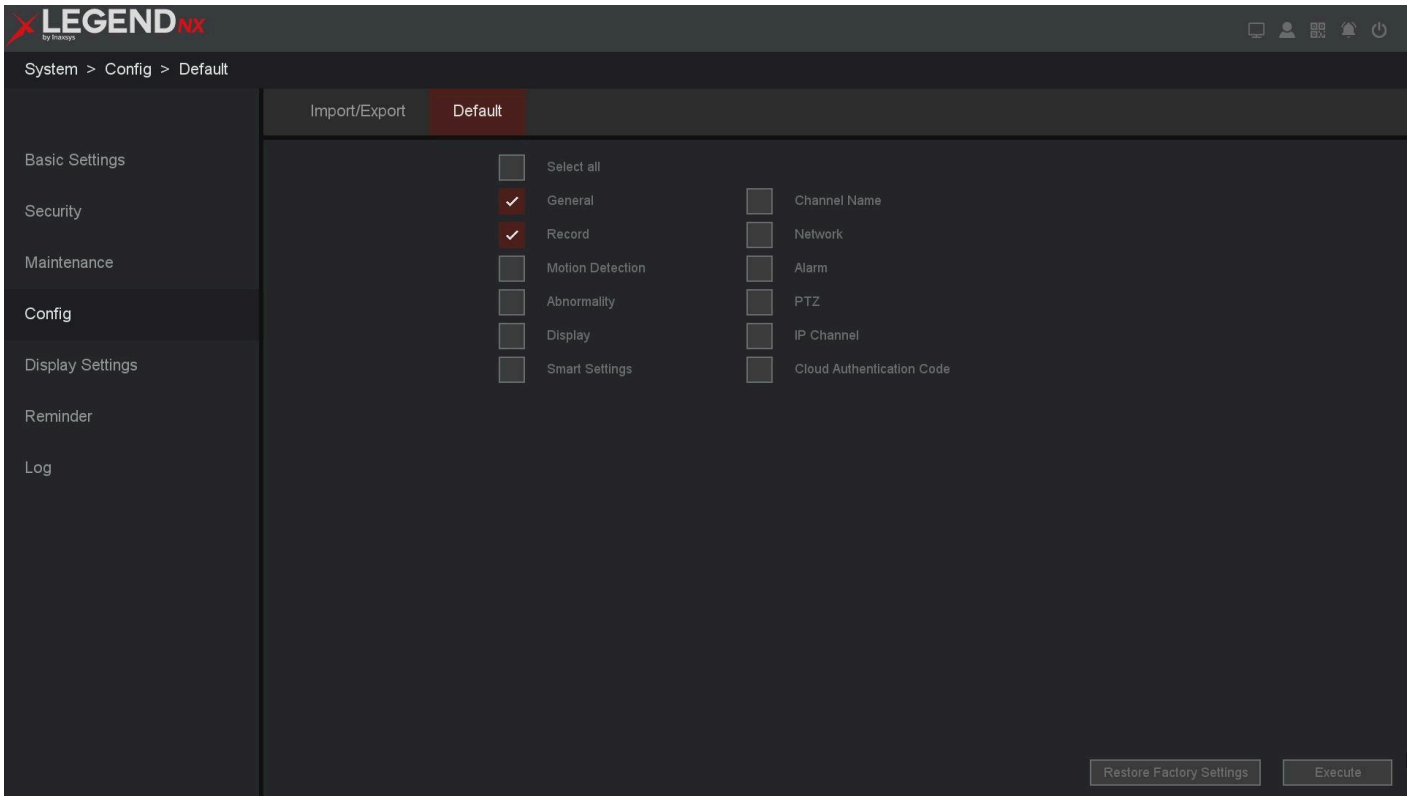


Figure 7-1 Default

2. Select the restore type.

Simple Restore

• Select the function items: General / Channel Name / Control / Network / Motion Detection / Alarm / Abnormality / PTZ / Display / IP Channel / Smart Settings / Cloud Authentication Code.
• Click the **Execute** button. The selected items will be restored to default settings.
• Optional: You can also select **Select All** to restore all items to default.

Factory Defaults

Click **Restore Factory Settings** to reset all parameters to factory default values.

3. After the restore is completed, the device will reboot automatically.

7.2 Search Log

The operation, alarm, exception, and information of the video recorder are stored in logs, which can be viewed and exported at any time.

Steps:

1. Go to **Main Menu** → **System** → **Log** → **Log**.

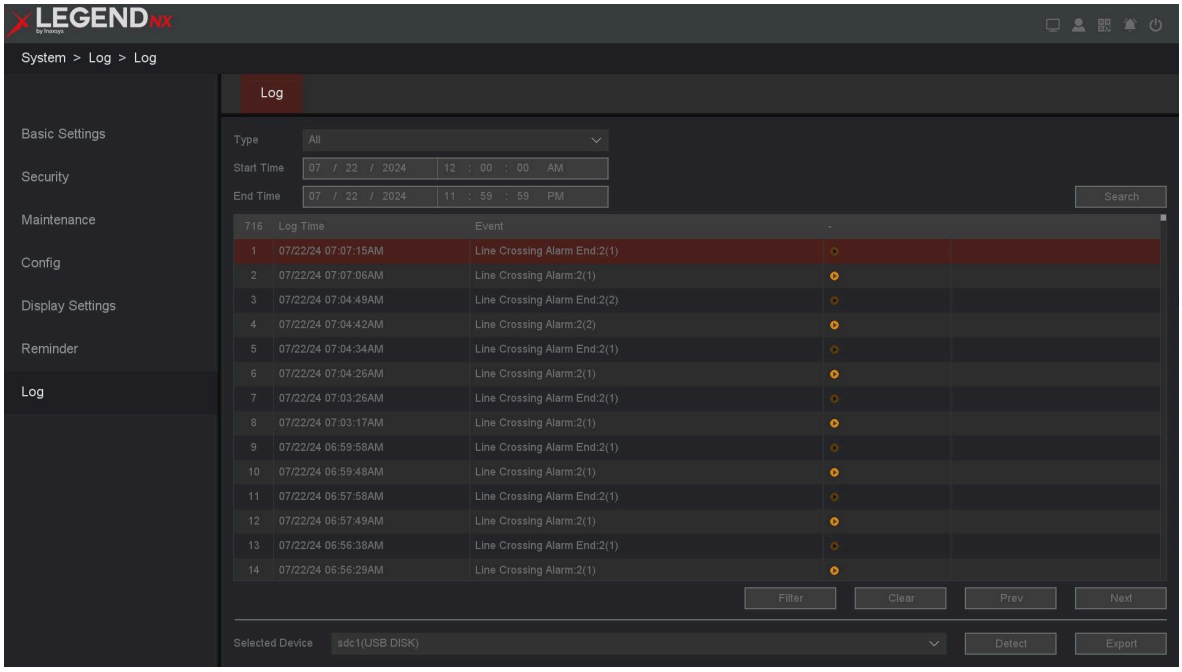


Figure 7-2 Log

2. Select the **Type** of log.
3. Select the time period of the log you want.
4. Click **Search**.

Type

Search types include **System**, **Config**, **Storage**, **Alarm**, **Record**, **Account**, **Clear**, and **Playback**.

Start Time / End Time

Set the time range for the search.

Search

After setting the time range and log type, click the search button. The device can store up to 4096 logs.

Prev / Next

Up to 1000 logs can be displayed per page. Use **Prev**/**Next** to navigate through additional pages.

Filter

On this page, you can choose whether to overwrite logs when storage is full and select which types of operation logs to save.

Detect
Detect the USB device.

Export
Export operation logs to a USB flash drive.

7.3 Upgrade

Warning
Do not shut down or power off the device during the upgrade process.

7.3.1 Local Upgrade

Before You Start
Store the upgrade firmware on a backup device (USB flash drive), and connect it to your device.

Steps:

1. Go to **Main Menu** → **System** → **Maintain** → **Upgrade**.

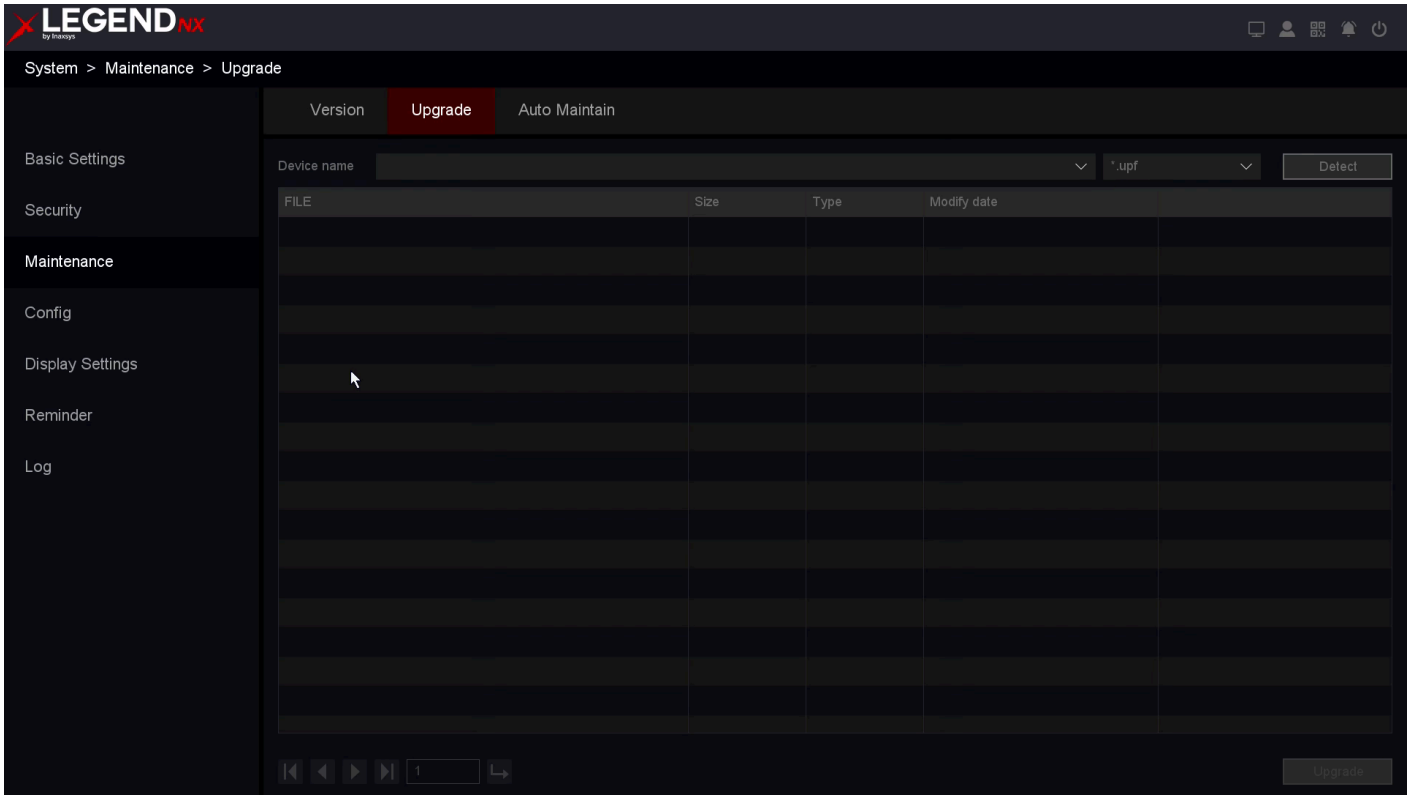


Figure 7-3 Upgrade

2. Select your USB flash drive from the **Device Name** drop-down list.
3. Select the correct upgrade firmware.
4. Click **Upgrade**.
5. Click **OK**. The device will automatically reboot after the upgrade is complete.

7.3.2 Online Upgrade & The Version

Upgrade the device using the latest online firmware.

Before You Start

Ensure that **P2P** is enabled and properly configured. Refer to **6.2.2 LEGEND-P2P** for details.

Steps:

1. Go to **Main Menu** → **System** → **Maintain** → **Version**.

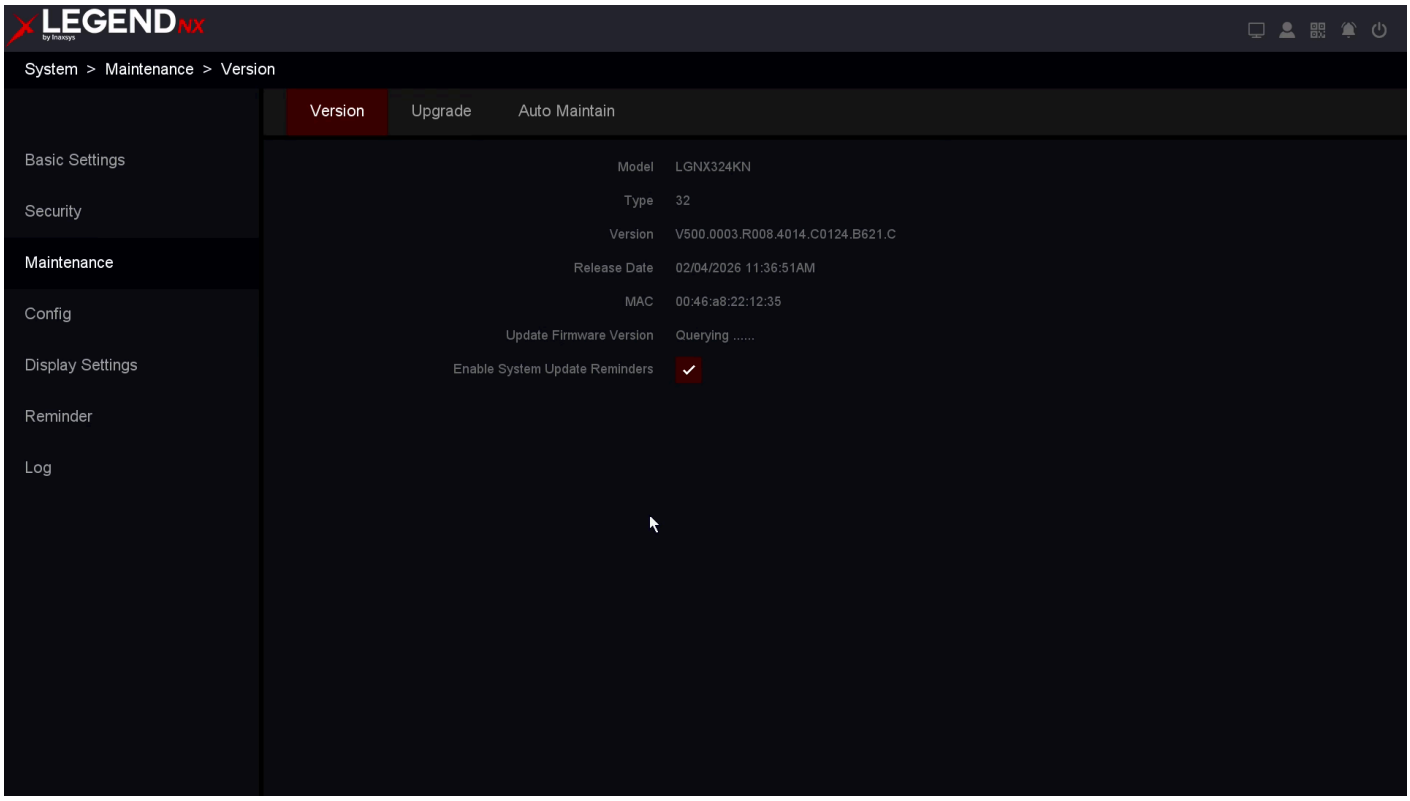


Figure 7-4 Version

2. The system will automatically detect whether the latest firmware is available.
3. If a new firmware version is available, click **Upgrade**.
4. Click **OK**. The device will automatically reboot after the upgrade is complete.
5. Optional: On this page, you can view the device version information.

Type

Number of channels supported by the device.

Version

Firmware version information.

Release Date

The firmware release date.

MAC
The MAC address of the device.

Update Firmware Version
Information about the available firmware update.

8. Alarm Status & Show Message

When events occur, you can view their details in **Alarm Status**.

8.1 Alarm Log

All alarm events are displayed here.

Steps:

1. Click the **Alarm** icon in the upper-right corner, or go to **Main Menu → Event → Alarm Log → Alarm Information**.

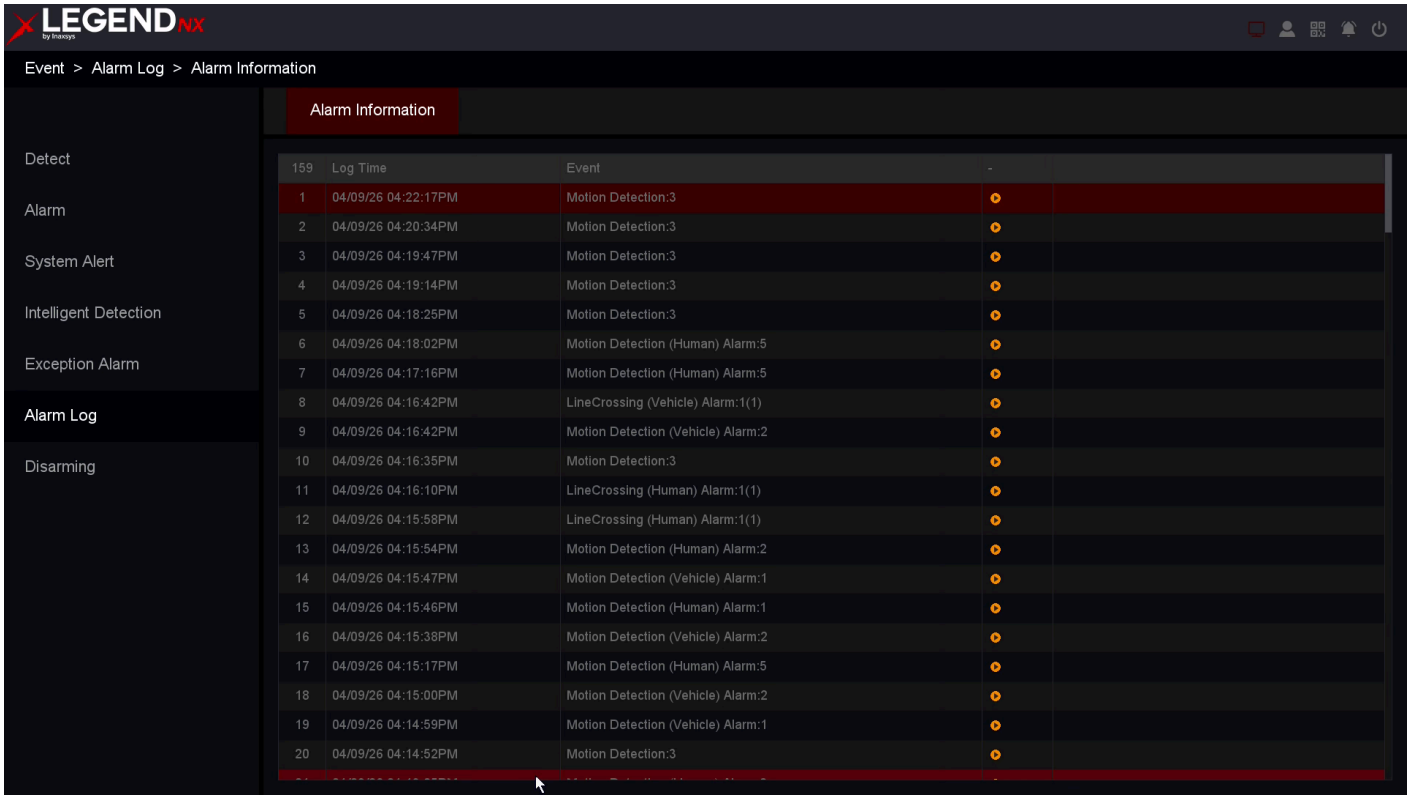


Figure 8-1 Alarm Center

2. You can also click the **Play** button to view the video associated with the alarm event.

8.2 View Alarm in Show Message

If **Show Message** is configured in the **Trigger process**, refer to **6.1.3 Alarm events & Trigger process** for configuration details.

Steps:

1. Go to **Main Menu → Event → Detect, Intelligent Detection or VQD → Trigger process**.
2. Enable **Show Message** as shown below.

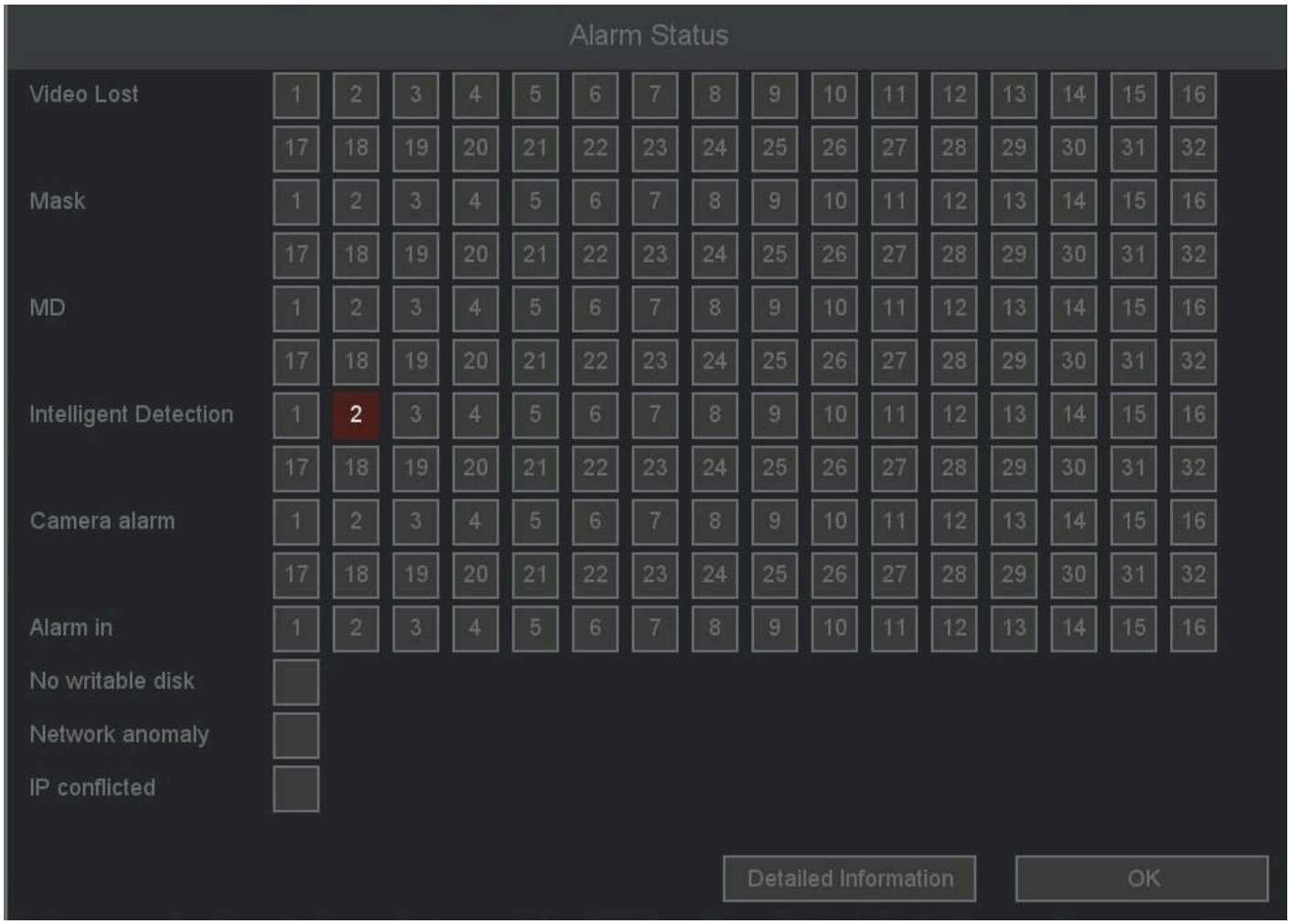


Figure 8-2 Alarm Status

9. Web Operation

9.1 Introduction

You can access the video recorder through a web browser.
Supported web browsers include Internet Explorer 6.0 to 11.0, Apple Safari, Mozilla Firefox, and Google Chrome. The supported resolution is 1024 × 768 or higher.

9.2 Login

Be aware that using the product with Internet access may expose it to network security risks. To prevent network attacks and information leakage, strengthen your security settings. If the product does not function properly, contact your dealer or the nearest service center.

Steps:

1. Open a web browser, enter the IP address of the video recorder, and press **Enter**.

Note
If you have changed the HTTP port, enter **http://IP address:HTTP port** in the address bar.
Example: **http://192.168.1.10:81**

2. The first time you log in, you will be prompted to install the plugin.
3. Allow the prompt and download the plugin to complete the installation.
4. Close the browser and reopen it.
5. Select the language in the interface.
6. Enter the username and password on the login page (the default username is **admin**, and the password is empty).
7. Click **Login**.

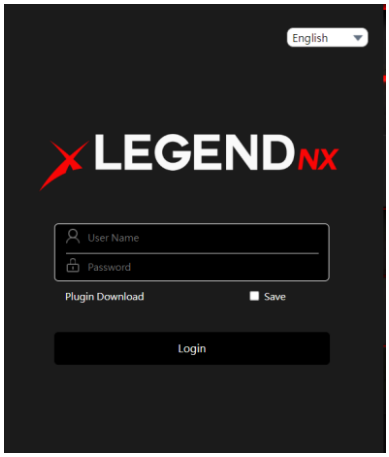


Figure 9-1 Login

Note
• If you log in without installing the plugin, you will still be prompted to install it. Follow the installation prompts; otherwise, the system may not function properly.
• You may need to close the web browser to complete the plugin installation.

9.3 Preview

After successfully logging in, you will enter the preview interface, as shown below.

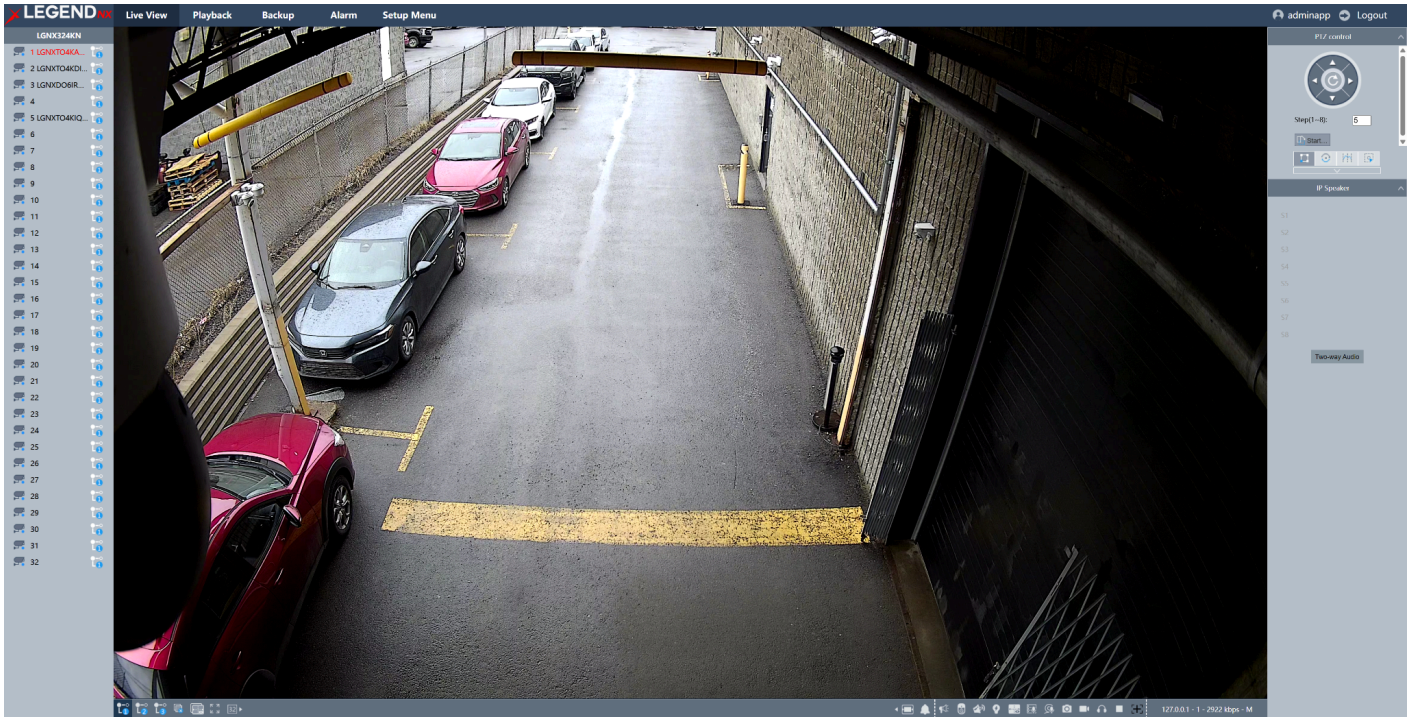


Figure 9-2 Live View

9.4 Playback

Click **Playback** to enter the playback interface, as shown below.

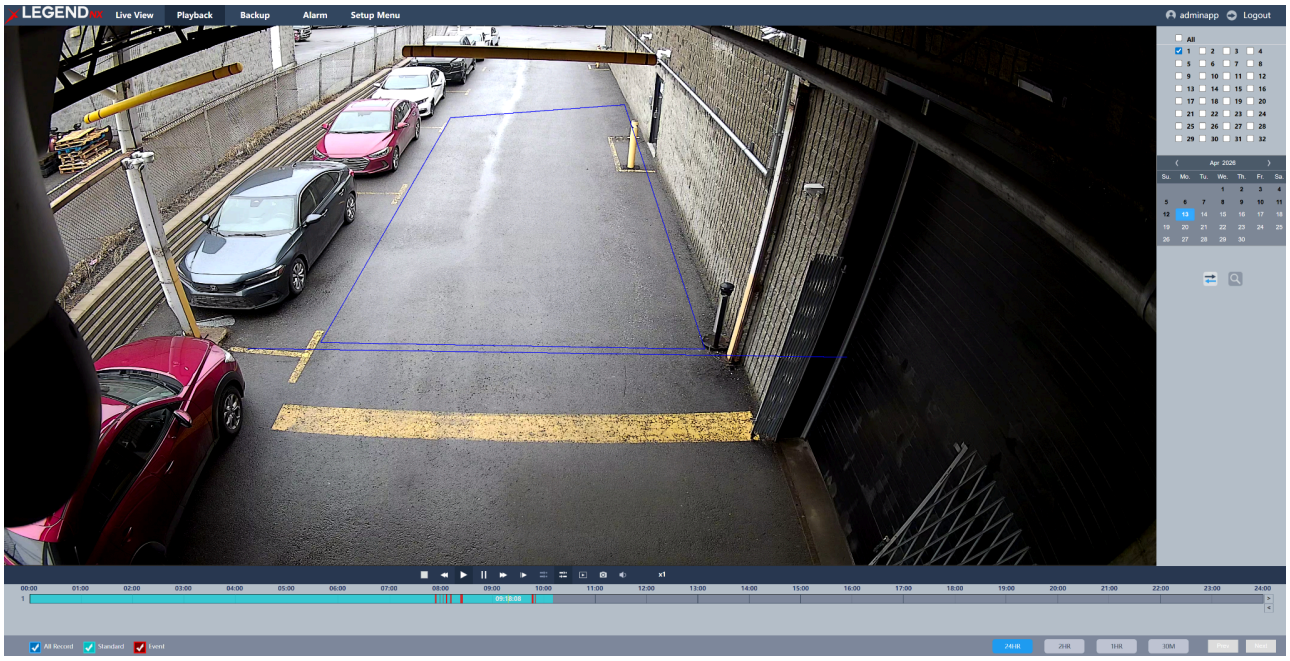


Figure 9-3 Playback

9.5 Set

Click **Set** to enter the configuration interface.

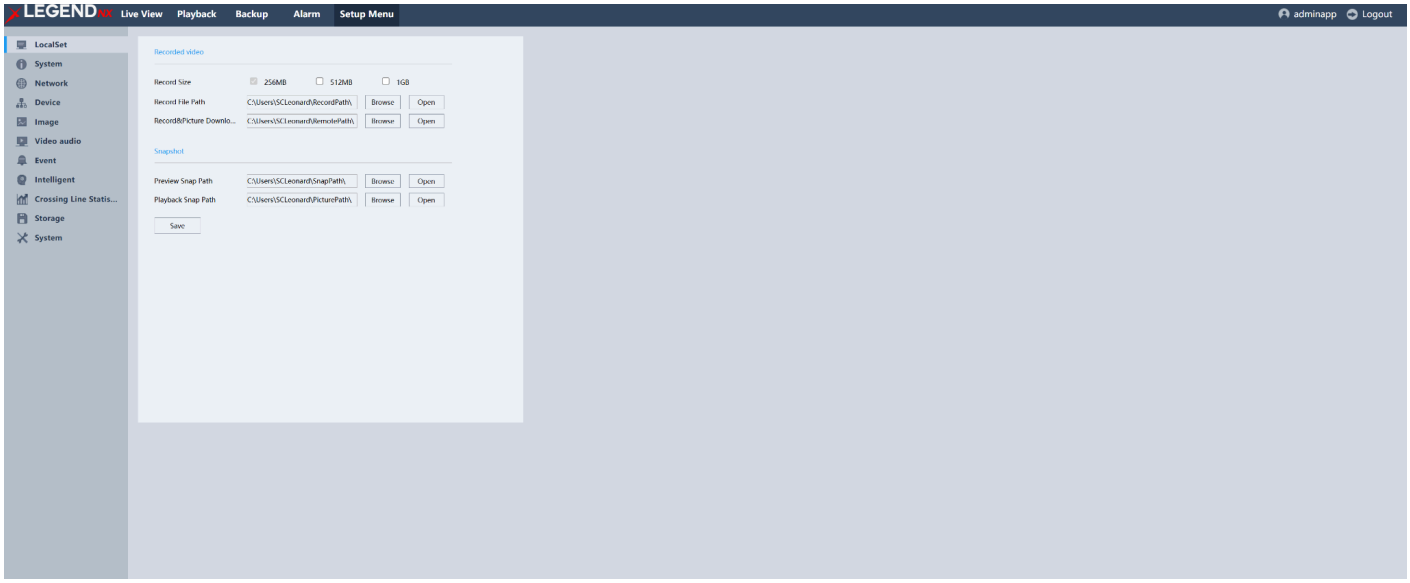


Figure 9-4 Configuration

9.6 Log

Steps:

1. Go to **Set** → **System** → **Log**.
2. Set the search conditions.
3. Click **Search**.

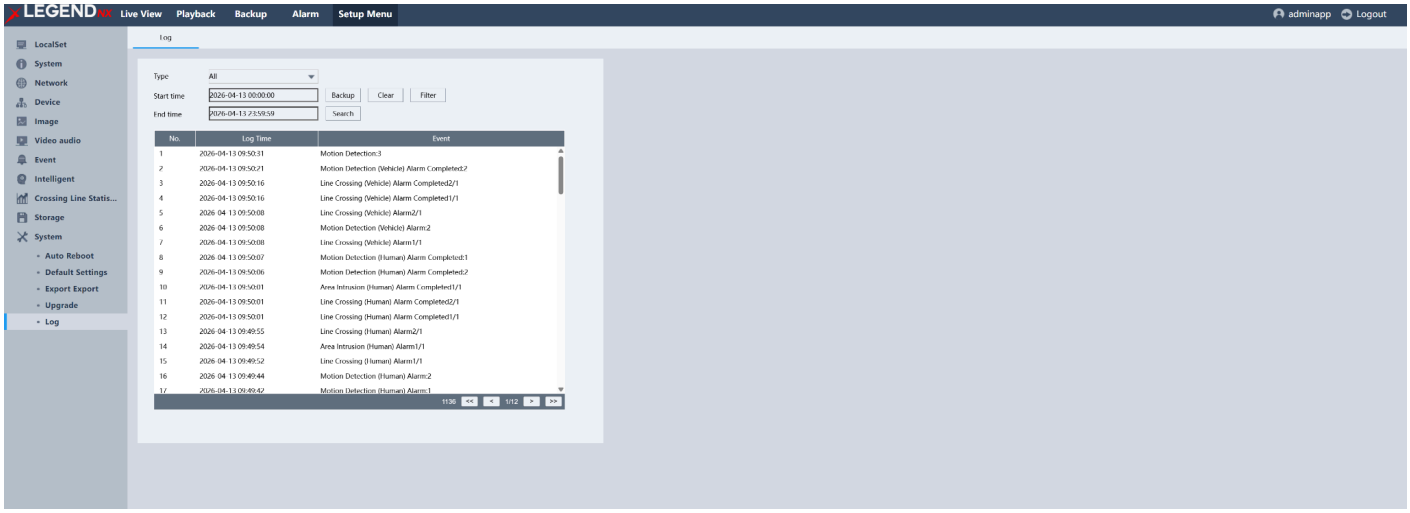


Figure 9-5 Log

10. Configuration (Advanced Mode)

10.1 System Configuration

10.1.1 Basic Settings

Configure Basic Settings

You can configure the Language, Time zone, System time, Time format, DST, Auto logout, Startup Wizard, Smart display, Smart tracking display, and Preview strategy.

Steps:

1. Go to **Main Menu → System → Basic Settings**.
2. Configure the parameters as required.

DST
DST (Daylight Saving Time) refers to the period of the year when clocks are set forward by one hour. In some regions, this results in longer daylight hours in the evening during warmer months.

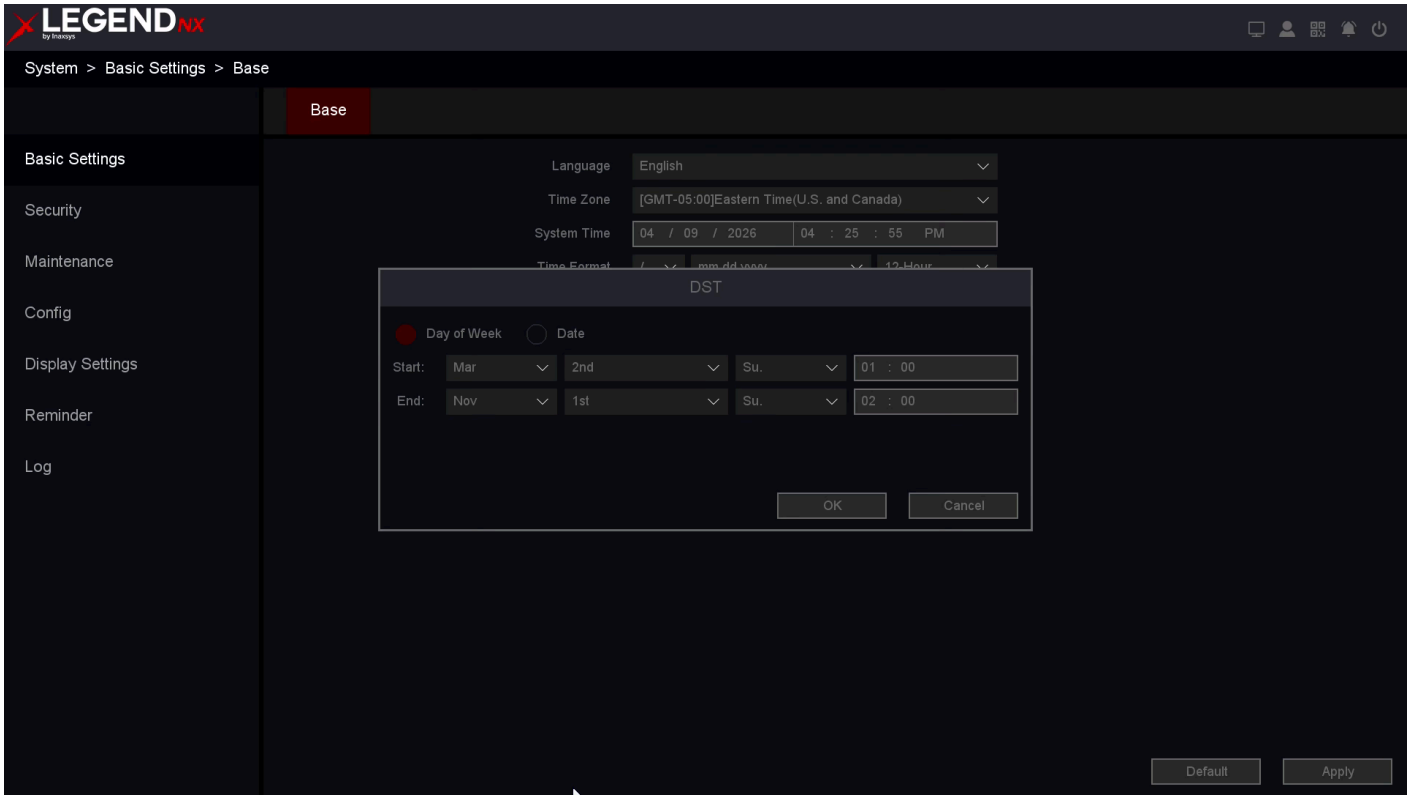


Figure 10-1 DST Settings

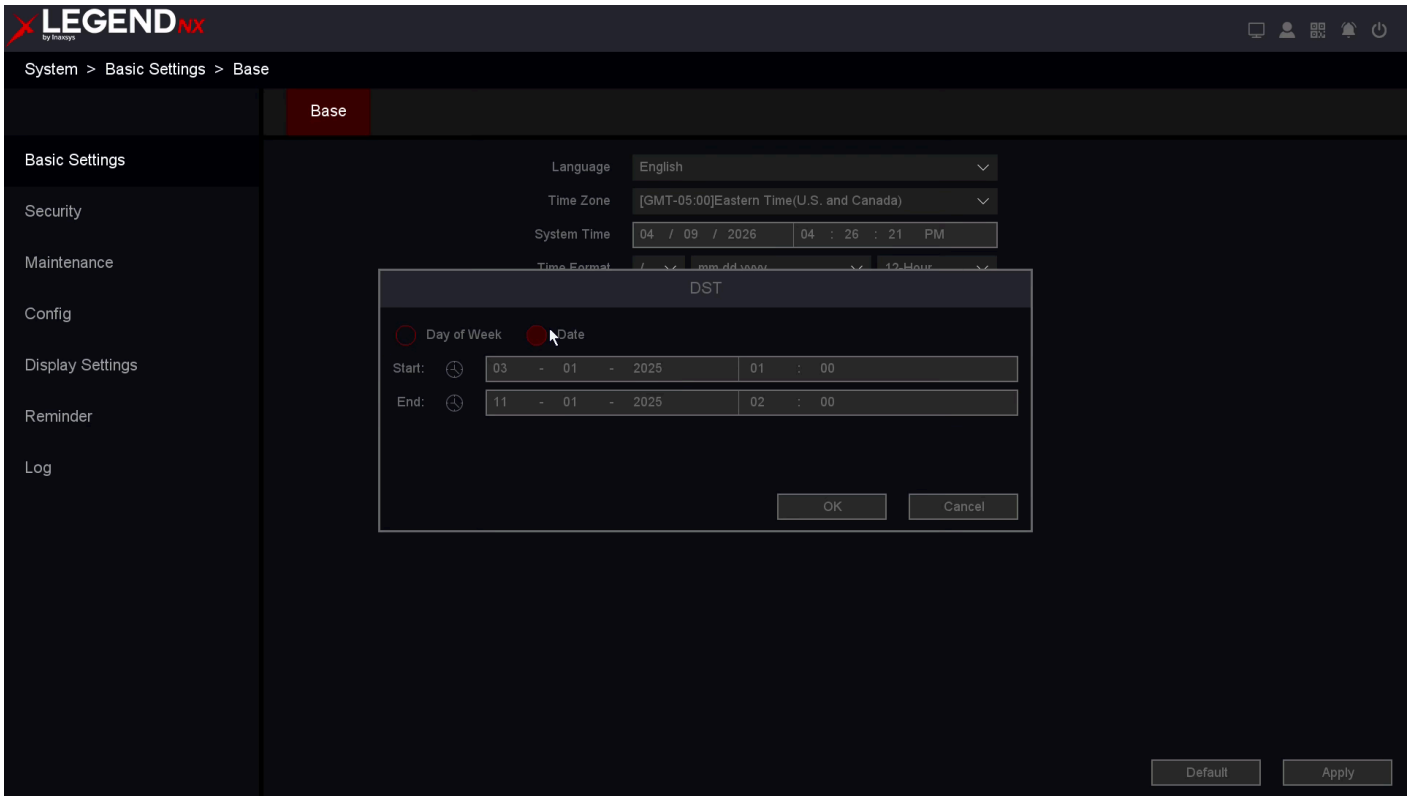


Figure 10-2 DST Settings

Time format

The format used for time display.

Device No

When using one remote control to manage multiple NVRs, you can assign a number to each NVR for identification.

Host Name

The name of the NVR.

Smart display

After enabling this function, smart alarm lines or areas will be displayed. The blue boxes shown in the figure below indicate these areas.

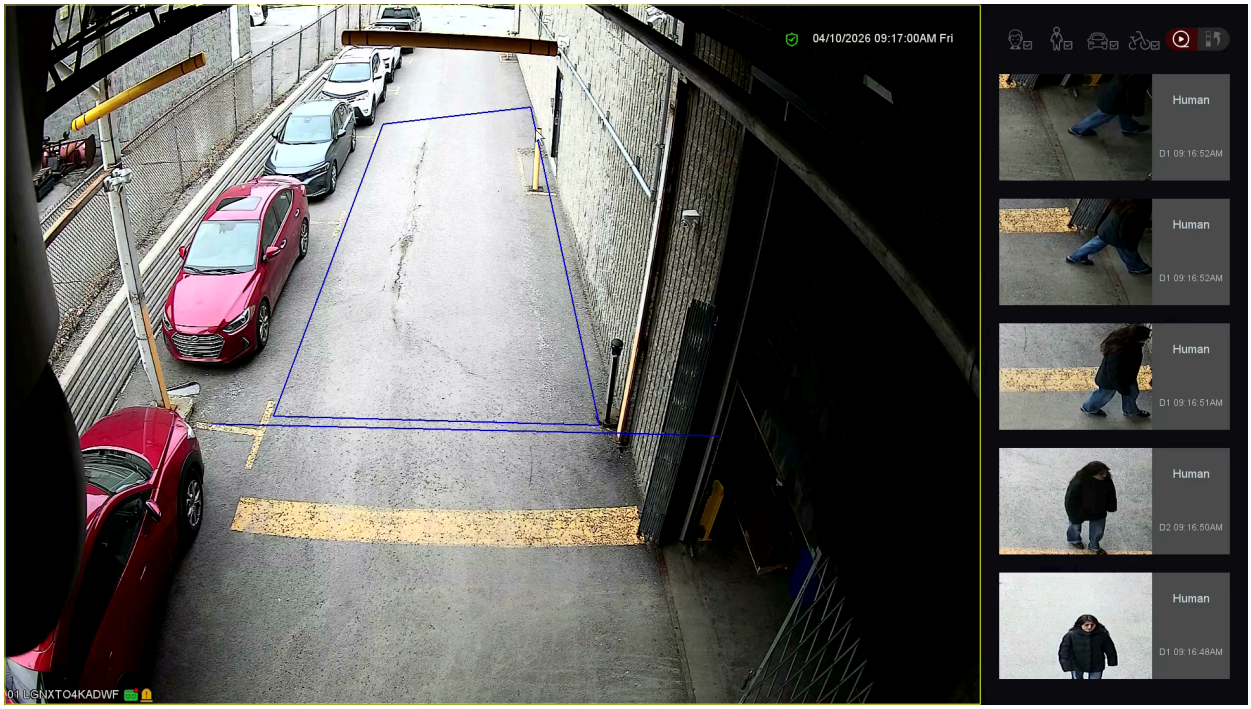


Figure 10-3 Smart Display

Smart tracking display

Tracks moving objects based on the selected intelligent alarm type. The blue tracking box will be displayed as shown below.

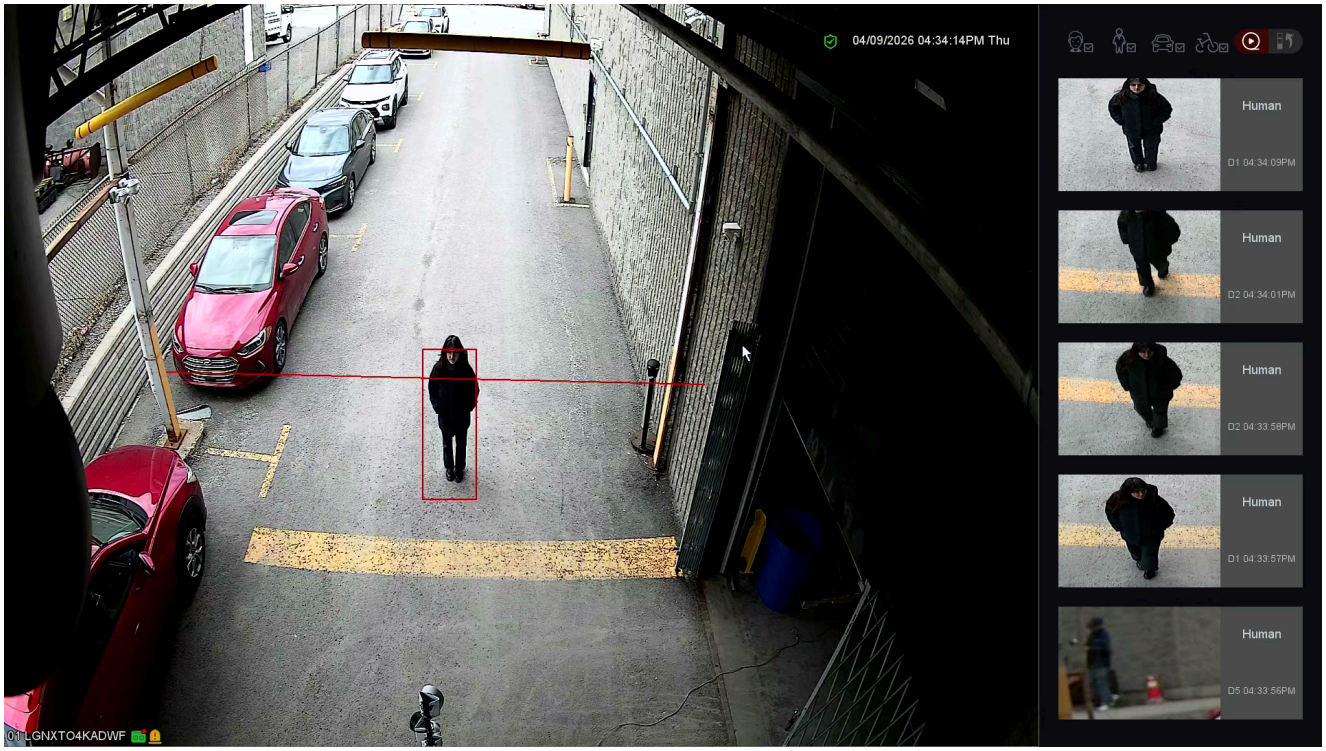


Figure 10-4 Smart Tracking Display

Preview strategy

Select either real-time priority or fluency priority for preview.

3. Click **Apply**.

10.1.2 Security

Account

There are three default accounts in the NVR: **admin / guest / default**, and their default passwords are empty. The **admin** account has administrator privileges, allowing it to add and delete users and configure user parameters. The **default** account is used when logged out and has preview-only permissions. This account can also be used to determine which channel preview is displayed when logged out.

Steps:

1. Go to **Main Menu → System → Security → Account**.

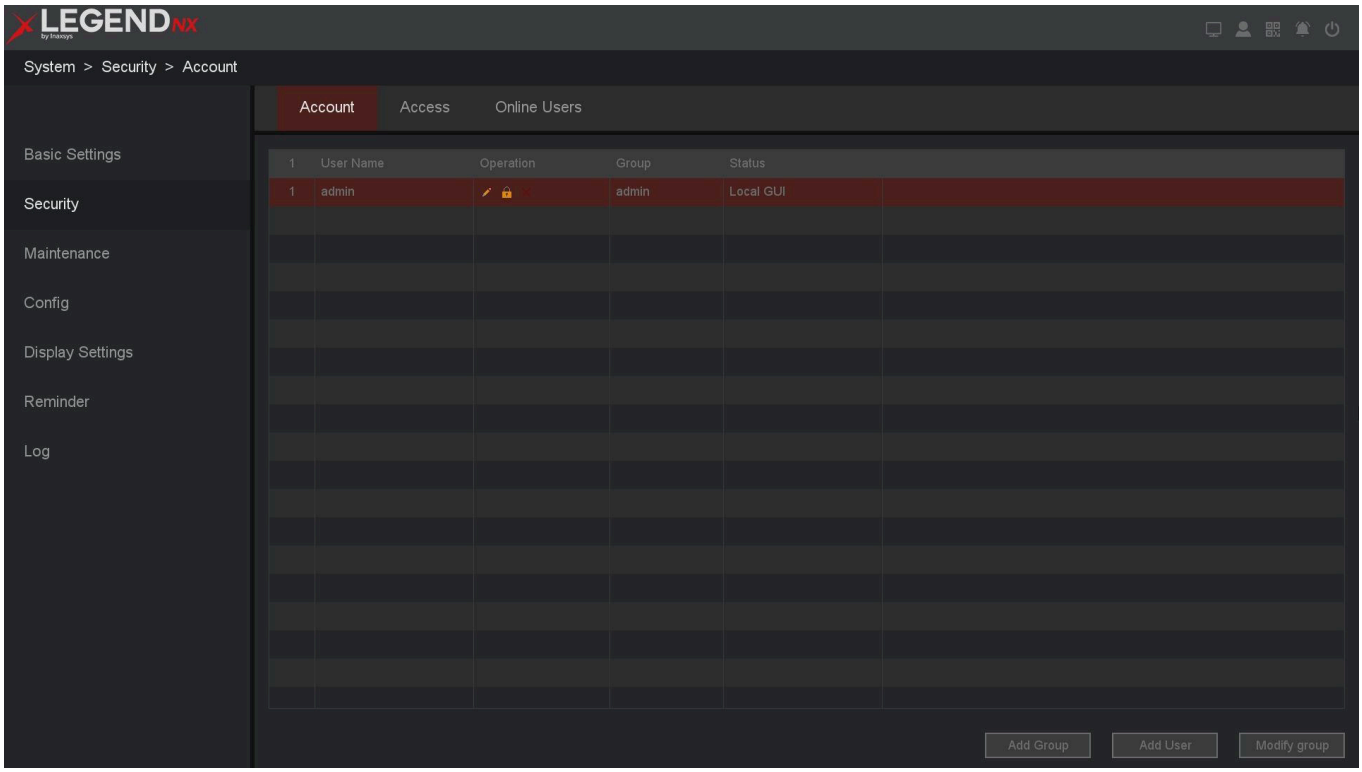


Figure 10-5 Account

Add Group

Add a user group and assign permissions. Available permissions include control panel access, real-time surveillance, playback, recording setup, video file backup, and more.

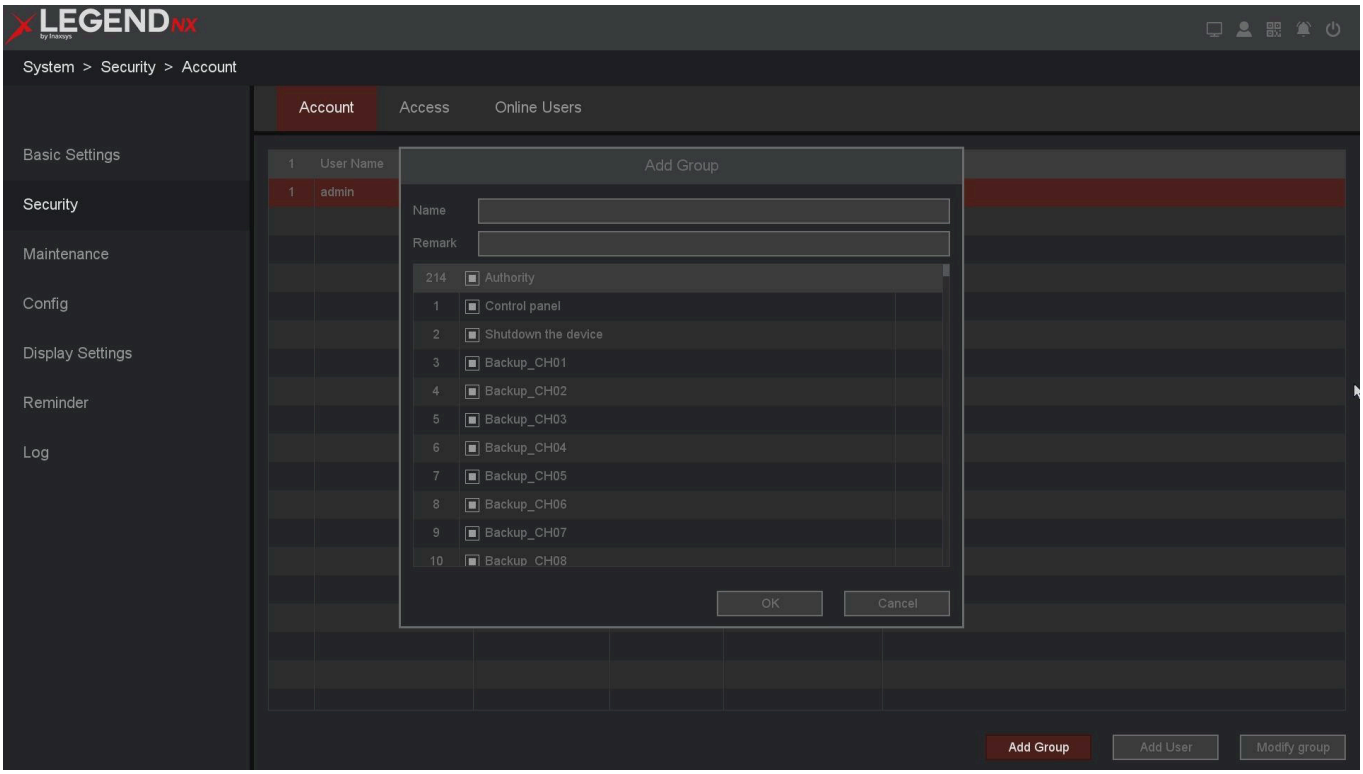


Figure 10-6 Add Group

Modify Group

Modify the attributes of existing groups and configure the parameters as required, as shown below.

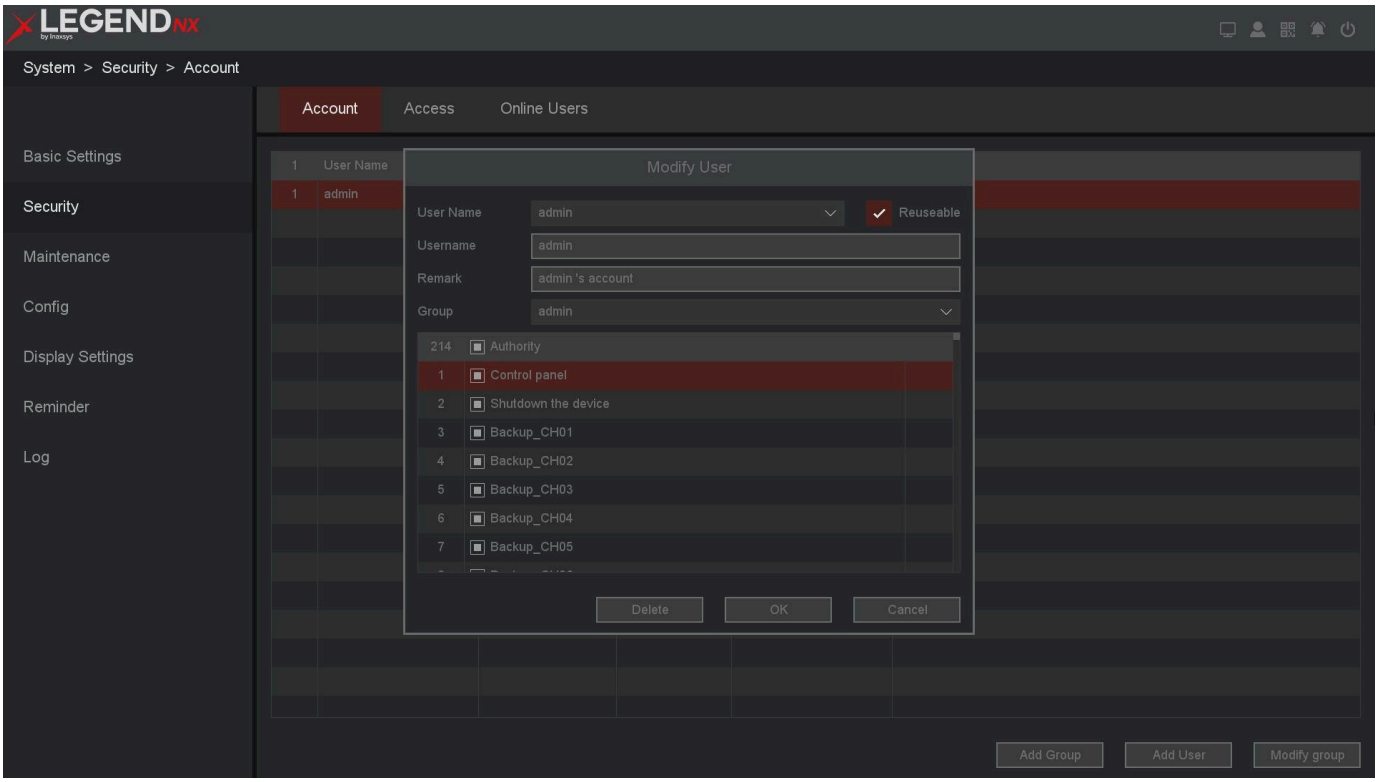


Figure 10-7 Modify Group

Add user & Modify User & Modify password

Please refer to **6.1.2 User**.

Note

- The maximum length of a name is 64 bytes for both users and user groups. Allowed characters include letters and numbers; other characters are not supported.
- User management includes groups and users. Each user must belong to one group.

Access

In this section, you can configure blocked and trusted IP addresses. This allows you to block specific IP addresses or permit access only from trusted IPs.

Steps:

1. Go to **Main Menu → System → Security → Access**.

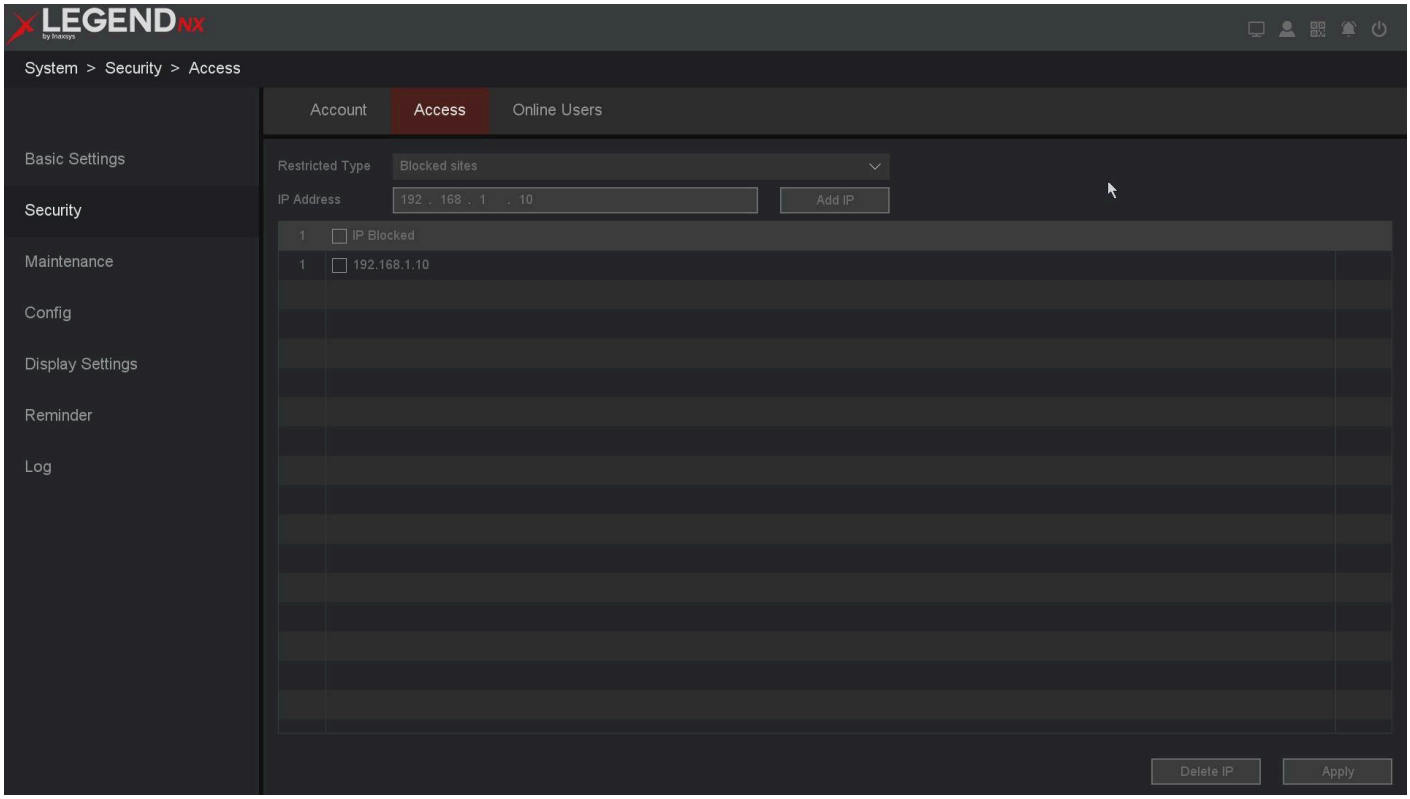


Figure 10-8 Access

Blocked Sites

IP addresses added to the blocked sites list are not allowed to log in to the NVR.

Trusted Sites

Only IP addresses added to the trusted sites list are allowed to log in to the NVR.

1. Add or delete IP addresses by clicking **Add IP** or **Delete IP**.
2. Click **Apply**.

Online Users

On the Online Users interface, you can view all currently connected users. If there are unknown users, you can disconnect them or block the connection for a specified duration.

1. Go to **Main Menu → System → Security → Online Users**.

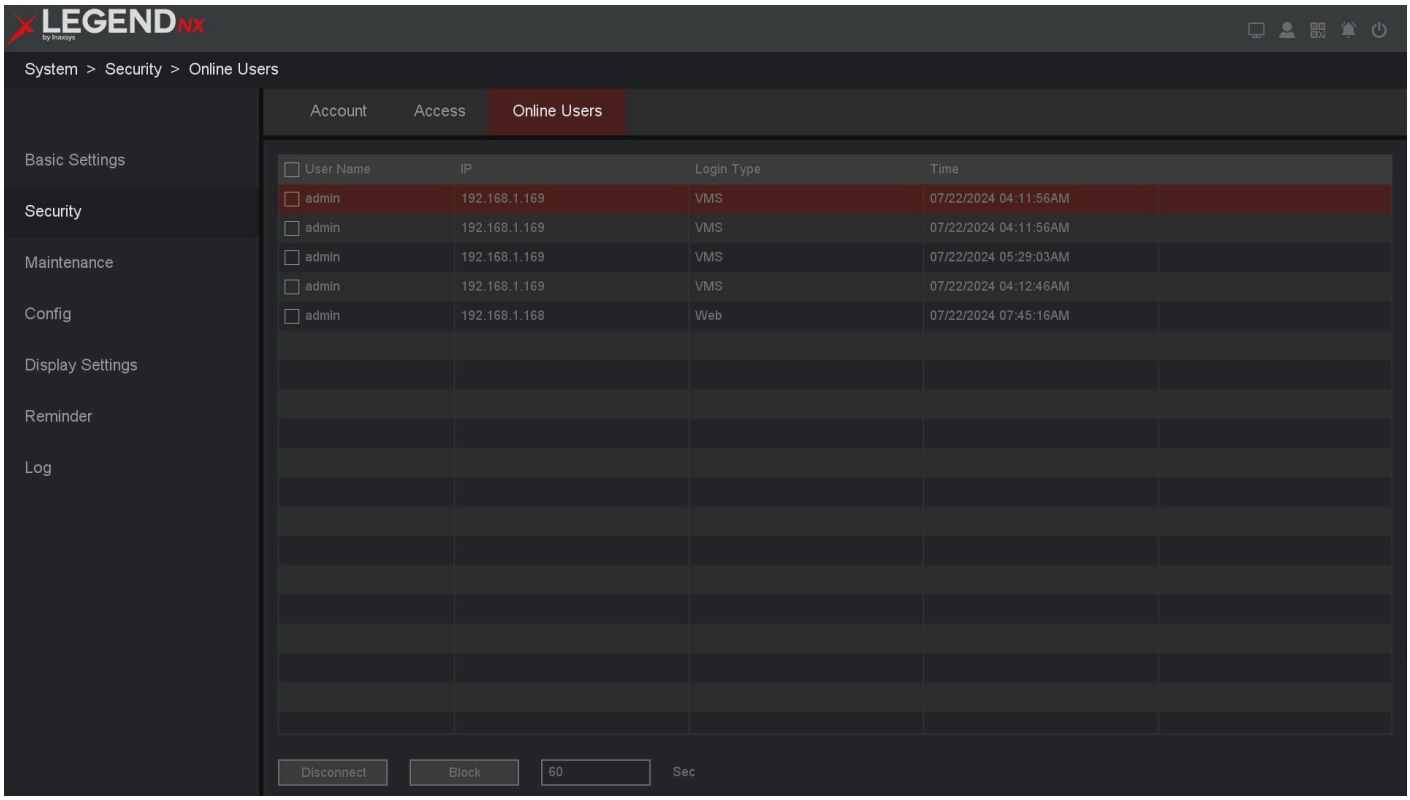


Figure 10-9 Online Users

User Name

The account used by the remote device to log in to this NVR.

IP

The IP address of the remote device accessing the system.

Login Type

The type of remote connection.

Disconnect

Disconnect the selected user. Disconnected users may reconnect automatically after a short period.

Block

Block the selected user for a specified duration. The user will be unable to reconnect during this period.

10.1.3 Maintenance

The Version & The Upgrade

Please refer to **7.3.1 Local Upgrade & 7.3.2 Online Upgrade & The Version**.

Auto maintain

In this interface, you can configure the automatic maintenance schedule of the device. Scheduled automatic maintenance can clear unnecessary cache and improve device performance.

1. Go to **Main Menu** → **System** → **Maintenance** → **Auto maintain**.

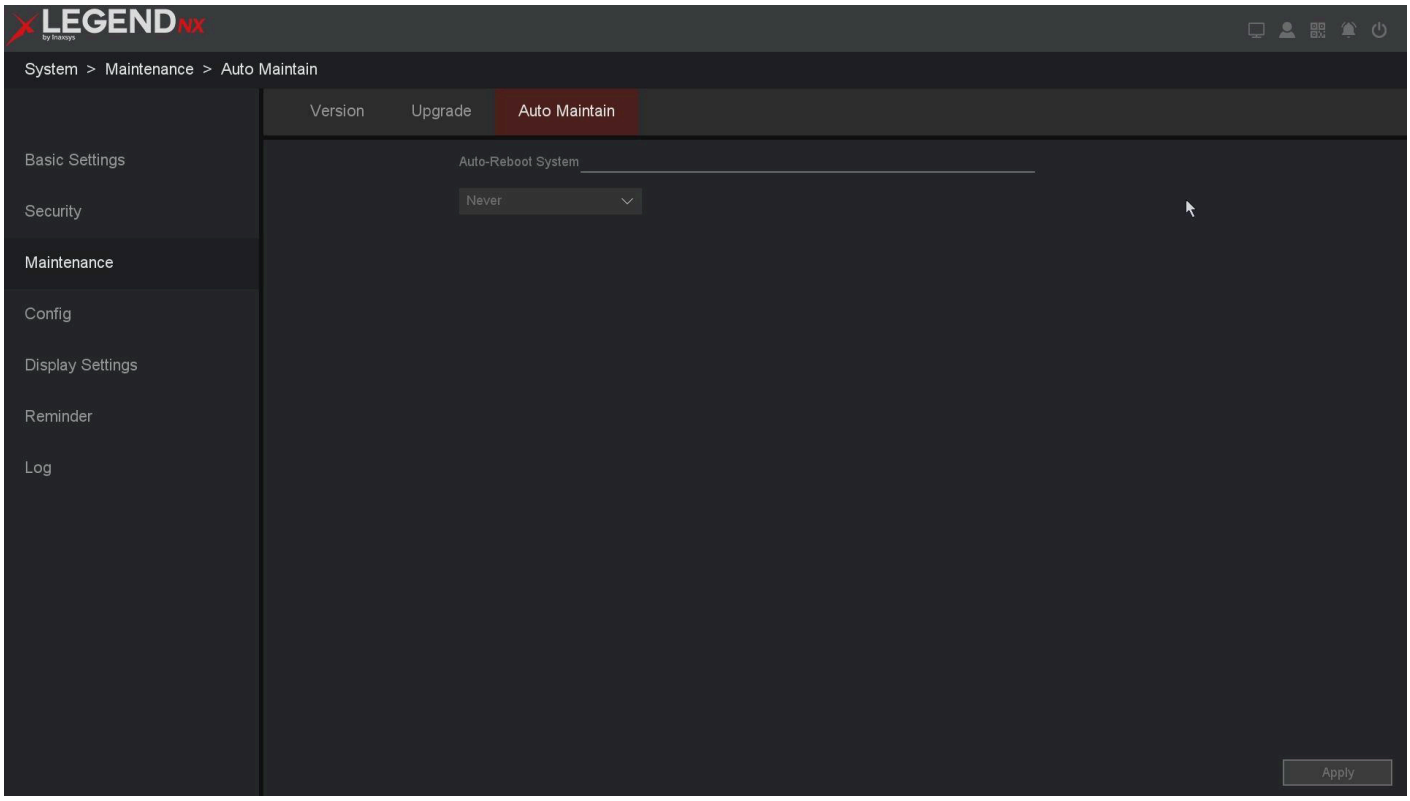


Figure 10-10 Auto Maintain

10.1.4 Display setting

Display

In this section, you can adjust the video output parameters.

1. Go to **Main Menu** → **System** → **Display settings** → **Display**.
2. Click **Apply** after completing the configuration.

Resolution
Select the appropriate resolution for the menu output.

Hue
Adjust the color tone of the display.

Brightness
Adjust the brightness of the display.

Contrast
Adjust the contrast of the display.

Saturation
Adjust the saturation of the display.

Top & Bottom & Left & Right
Adjust the margins between the top, bottom, left, and right edges of the display.

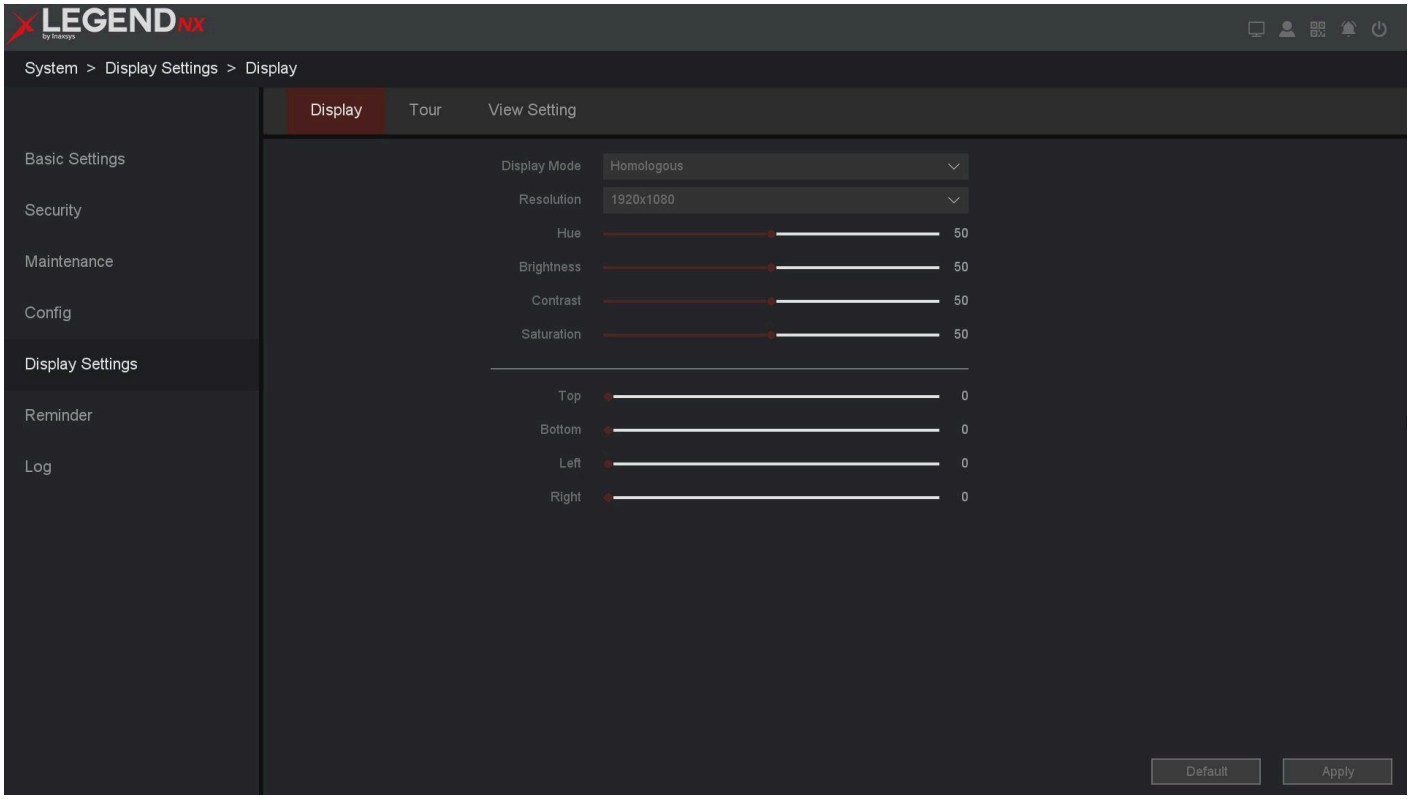


Figure 10-11 Display

Tour

In this section, you can configure the patrol (auto-switch) display on the monitor.

1. Go to **Main Menu → System → Display settings → Tour**.
2. Click **Apply** after completing the configuration.

Layout
Configure the number of channels and channel groups for preview. For example, on a 64-channel NVR, selecting **View 16–1** displays channels 1–16 in the preview interface; selecting **View 16–2** displays channels 17–32, and so on.

Dwell Time
Set the interval (in seconds) between automatic channel switches when auto-switch is enabled in Live View.

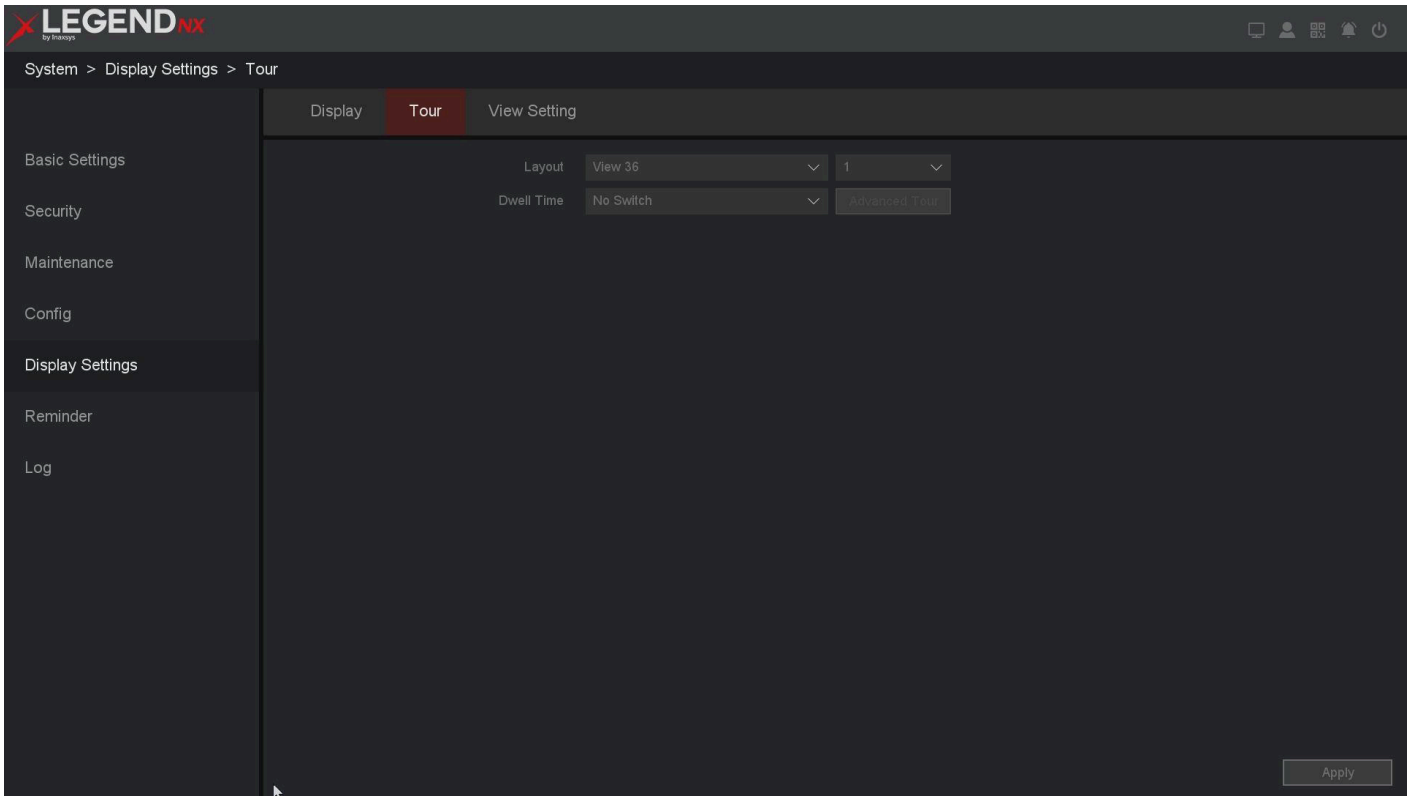


Figure 10-12 Dwell Time

3. If you select **Advanced Tour** under **Dwell Time**, configure the settings as shown in the figure below.

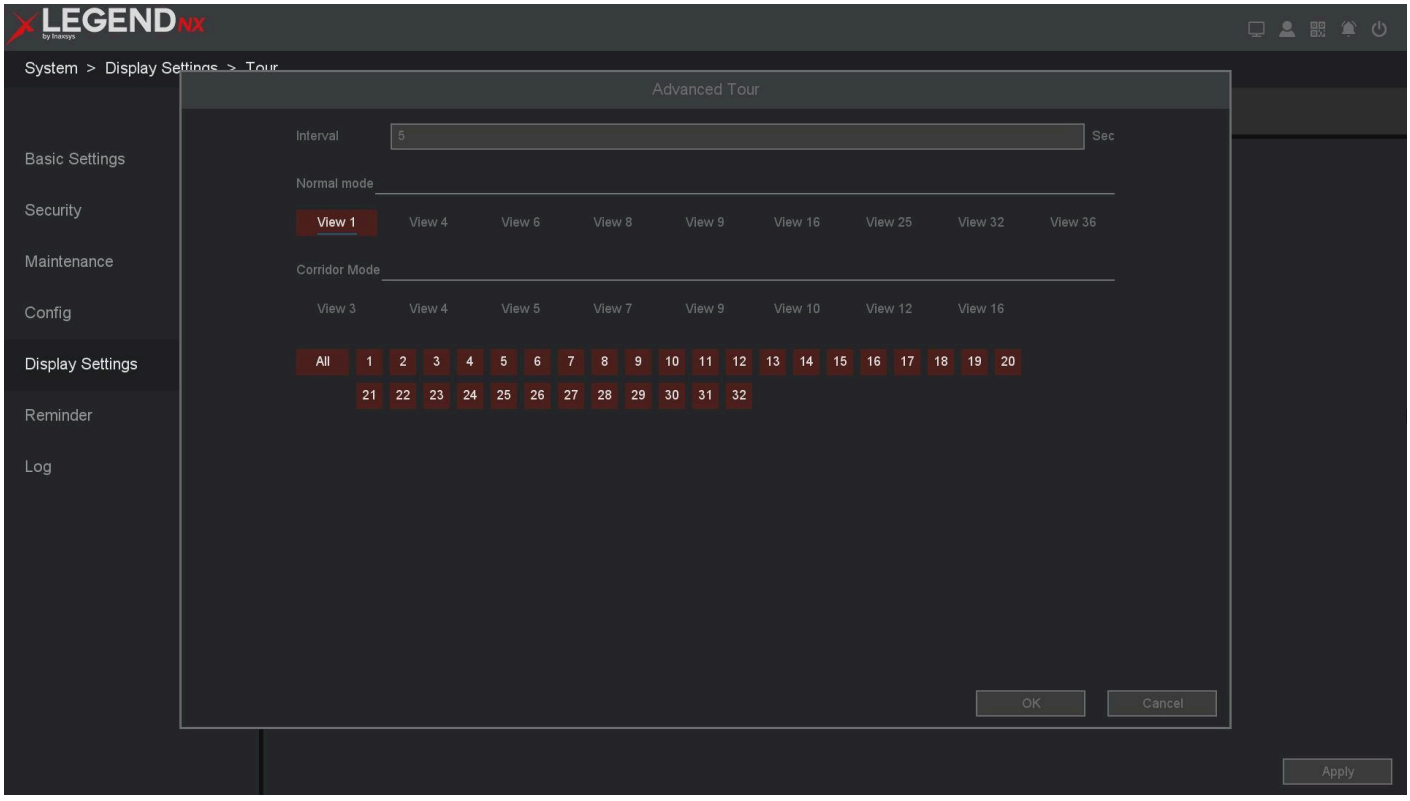


Figure 10-13 Advanced Tour

Interval

Set the interval time. The adjustable range is from 5 s to 120 s. This determines how long each screen is displayed before switching to the next one during the tour.

View

Select the views to be included in the tour sequence.

View setting

In this section, you can configure the patrol (auto-switch) display of the monitor.

1. Go to **Main Menu → System → Display settings → View setting**.
2. Select the **Channel** from the drop-down list.
3. Click a window to select it, then double-click a camera name in the channel list to assign it to the selected window.
4. You can also click the  to display the configured channels for each screen, and click the cancel icon  to remove configured channels from the screen. Click the previous or next page icons to navigate between pages.
5. Click **Apply** after completing the configuration.

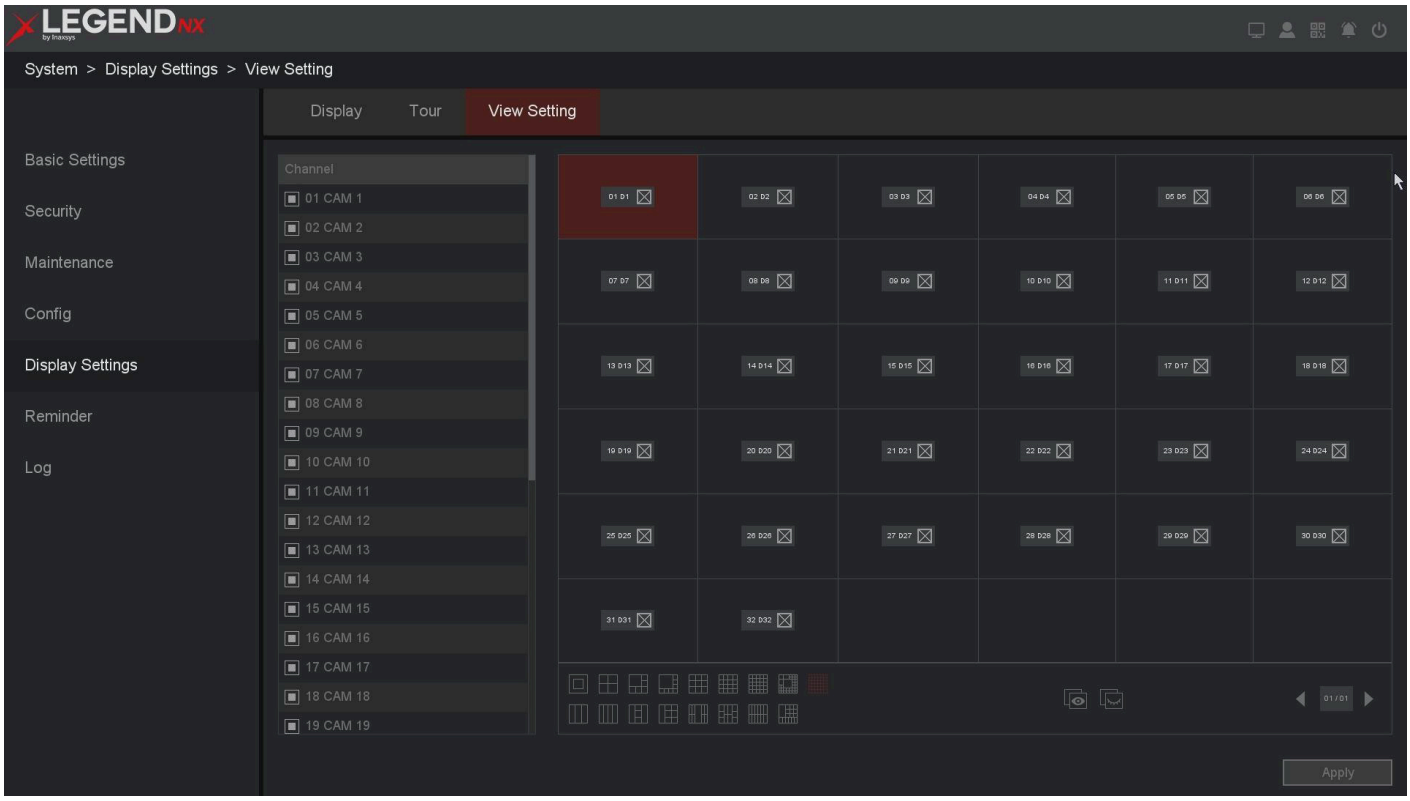


Figure 10-14 View Setting

10.1.5 Reminder

When this function is enabled, the user must manually confirm the “on-duty” prompt displayed on the GUI. The prompt interval can be configured as required. Each confirmation is recorded in the log.

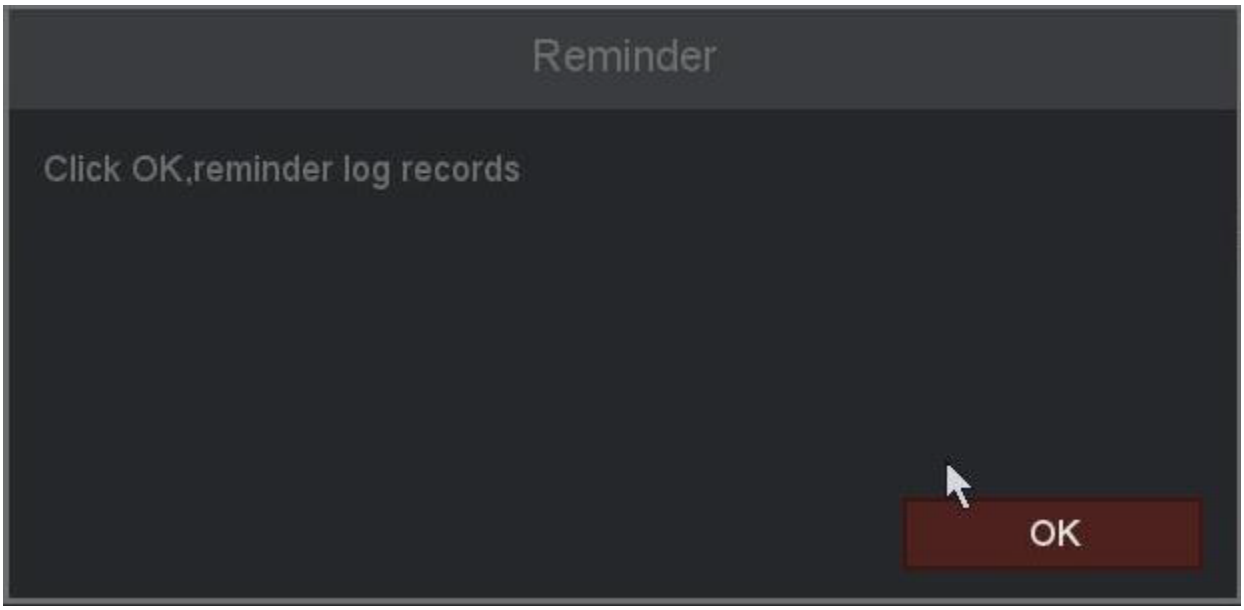


Figure 10-15 System-Reminder

1. Go to **Main Menu** → **System** → **Reminder**.
2. Set the time interval between patrol checks and the duration for cloth removal.
3. Click **Apply** after completing the configuration.

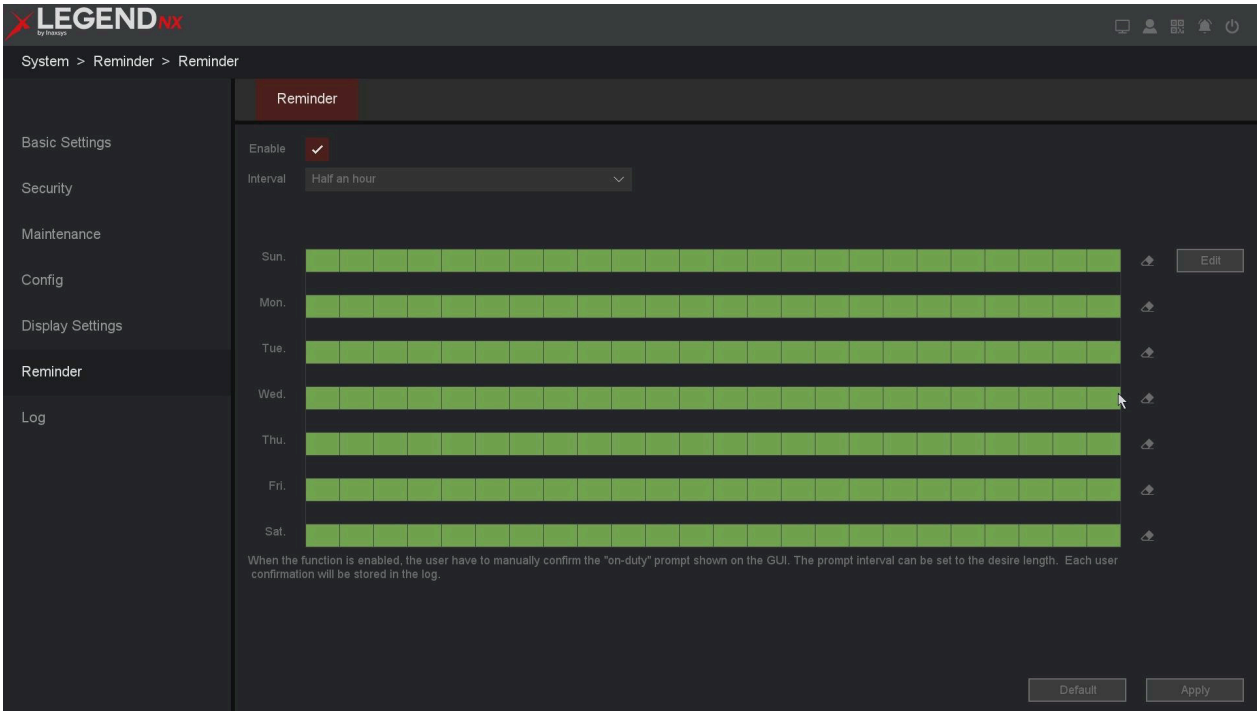


Figure 10-16 Reminder

10.1.6 Config

Import/Export

On this page, you can back up device parameters to a USB flash drive. You can also import previously backed-up parameters.

1. Go to **Main Menu → System → Config → Import/Export**.
2. Click **Detect**.
3. Click **Import** or **Export**.

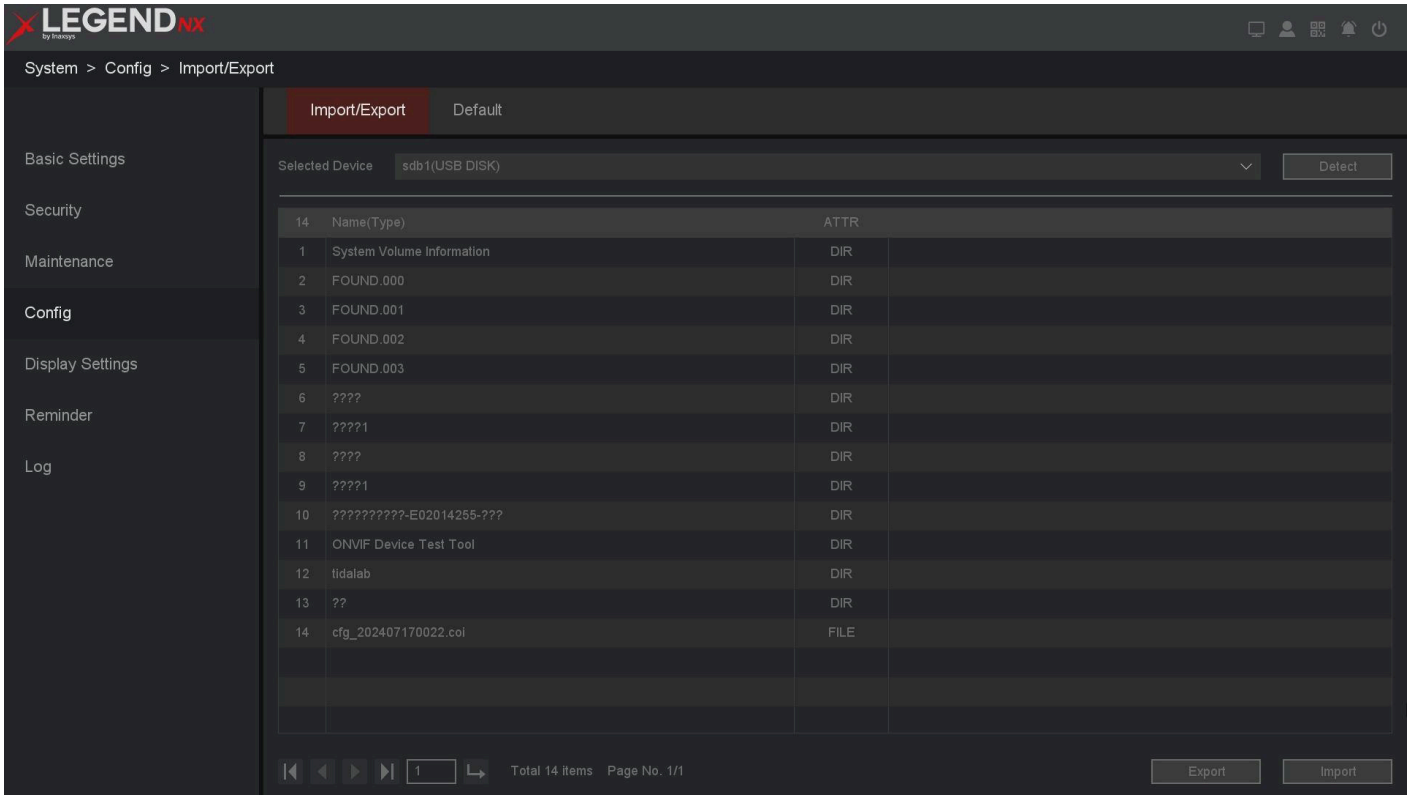


Figure 10-17 Import/Export

Detect

Detect the USB device.

Name (type)

Displays the file name and file type. The backup file uses the ".coi" format.

ATTR

Displays the file type.

Export

Export the parameter backup file to a USB disk.

Import

Select a backup file and click **Import**. The device parameters will be updated with the selected file.

Default

On this page, you can select function items such as General/Channel Name/Control/Network/Motion Detection/Alarm/Abnormality/PTZ/Display/IP Channel/Smart Settings/Cloud Authentication Code. After clicking the **Execute** button, the selected items will be restored to their default settings. You can also select **Select all** to restore all items to their default values.

1. Go to **Main Menu → System → Config → Import/Export**.
2. Select the function items for which you want to restore default parameters, or select **Select all**.
3. Click **Execute**.

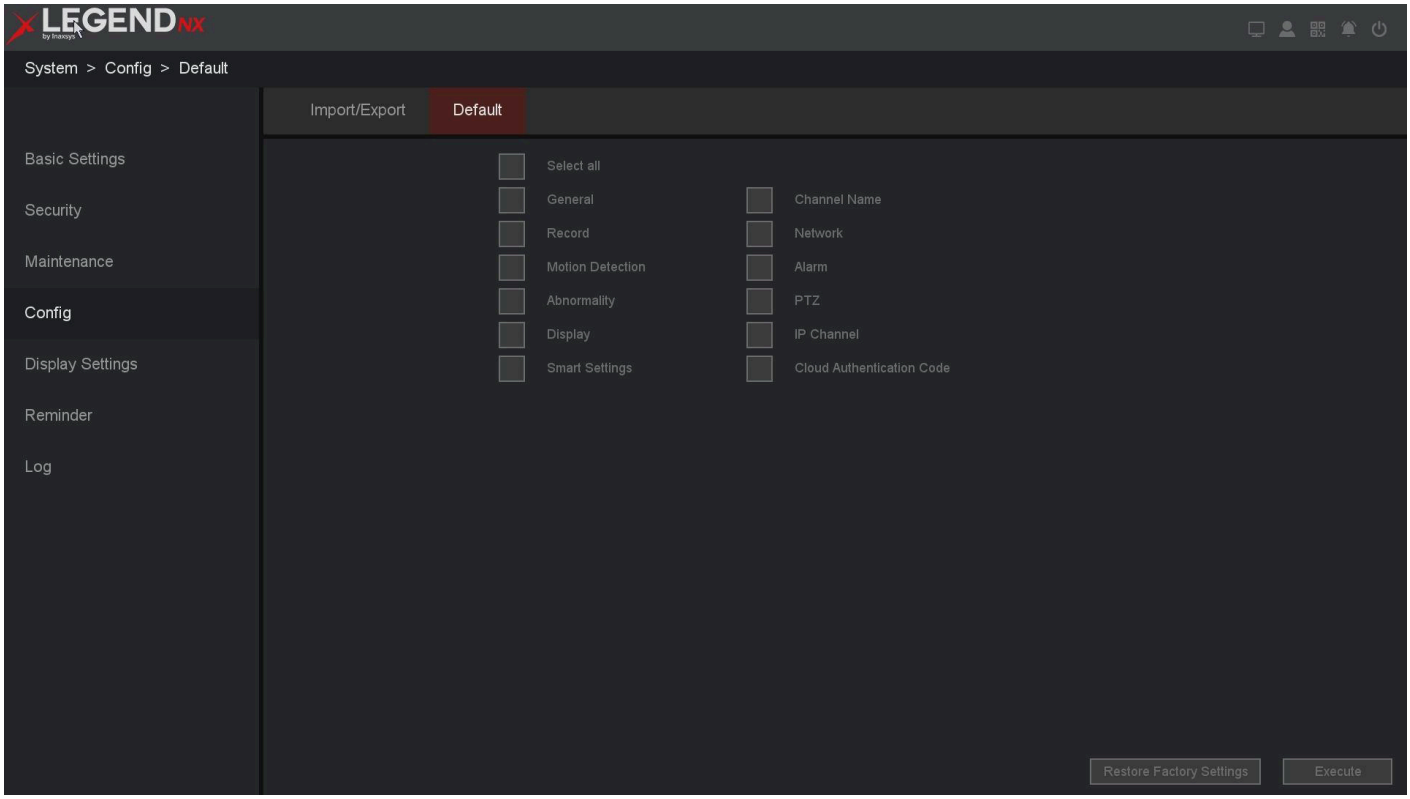


Figure 10-18 Default

Note

You can also click **Restore factory settings** to quickly restore factory defaults. Use this function with caution. It is recommended to back up your data before performing this operation.

10.1.7 Hot Standby

Enable the hot standby function. When the active NVR in the system fails, the system automatically switches to the standby NVR to continue recording. When the active NVR returns to normal operation, the system automatically switches back. This helps reduce video loss and ensures continuity of recording.

Note

All active and standby devices must be of the same model.

Config working machine

The working machine is the primary NVR used for daily operation. If it fails, the system automatically switches to the standby NVR to continue recording. The hot standby function takes effect only after the standby device has been configured and the working NVR has been added.

Steps:

1. Go to **Setting menu → System → Hot Standby**.

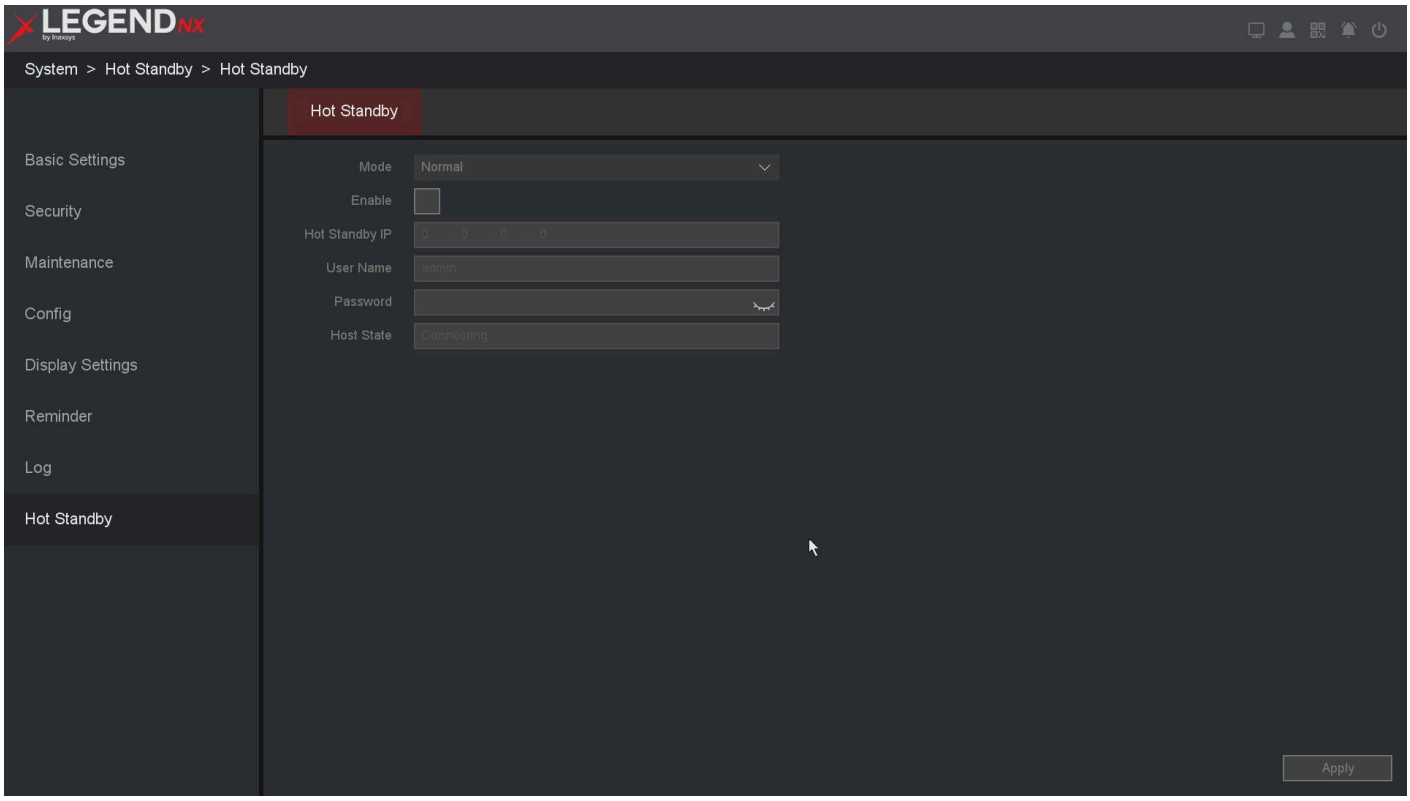


Figure 10-19 Normal Mode

2. Set **Mode** to **Normal**. The device will be configured as the working machine.
3. Enable **Enable**.
4. Enter the IP address of the standby device.
5. Enter the password of the standby device.
6. Click **Apply**.

Config hot standby machine

The standby NVR does not operate continuously. When the corresponding working NVR fails, it automatically takes over and continues recording.

Steps:

1. Go to **Main menu → System → Hot Standby**.
2. Set **Mode** to **Standby**.
3. Click **Apply**.
4. Click **OK**, then wait for the device to reboot successfully.

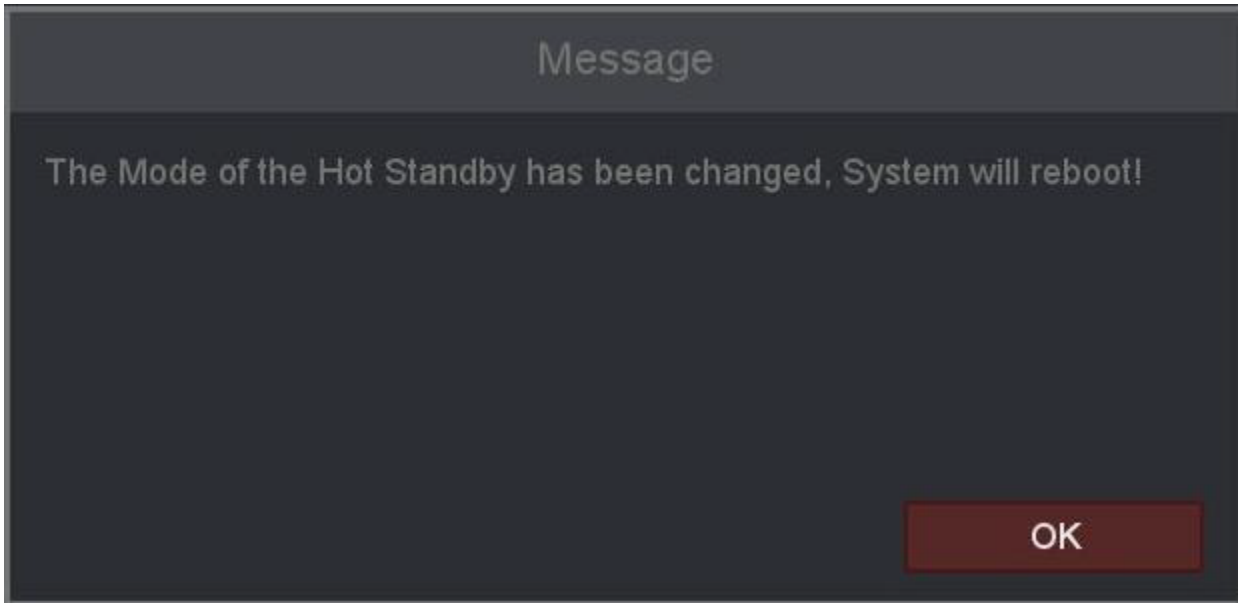


Figure 10-20 Prompt to Reboot

Note

After hot standby mode takes effect, some device parameters will change. For example, all IP channels will be deleted (preview configuration will also be cleared).

5. After restarting, go to **Setting menu → Storage → Hot Standby**.

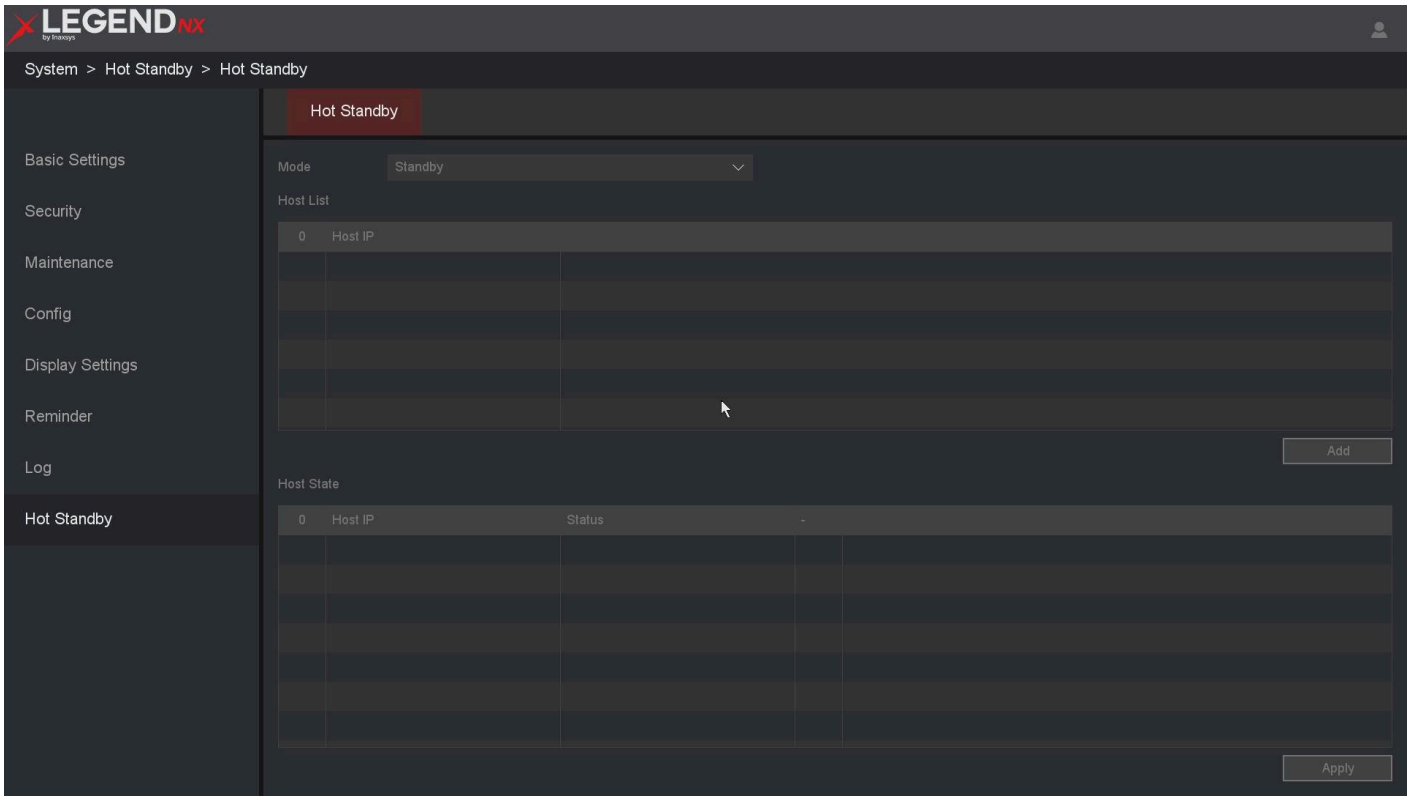


Figure 10-21 Hot Standby Mode

6. Add working NVRs.

Note

• If no working machine is added to the hot standby system, or if the working machine is removed, video backup or synchronization will not be available.

• If the hot standby is switched to normal operating mode, it can be switched back to the working machine for use.

10.2 Network Configuration

10.2.1 TCP/IP

TCP/IP must be properly configured before operating the video recorder over the network. On this page, you can set the device IP address, gateway, DNS, and view the MAC address. If the NVR has two Ethernet ports, it can be connected to two network segments, and one can be set as the default route.

Steps:

1. Go to **Main Menu** → **Network** → **Basic Settings** → **TCP/IP**.
2. For general settings, refer to **6.2.1 General - TCP/IP** for details.
3. Configure other network parameters as required.

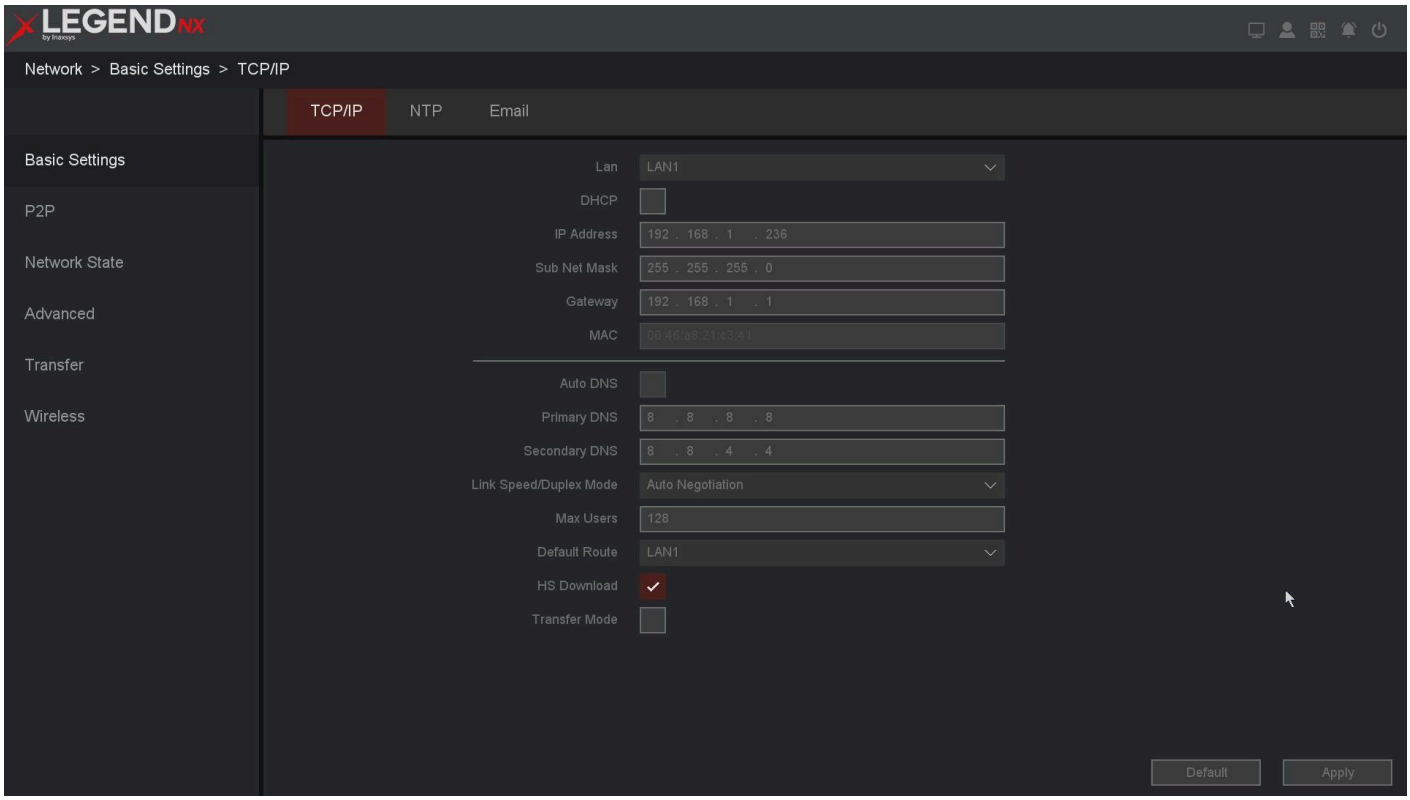


Figure 10-22 TCP/IP

DHCP

If a DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from the server.

MAC
The physical address of the NVR.

DNS setup
The Domain Name Server (DNS) translates domain names into IP addresses. It includes a primary DNS and a secondary DNS.

Link Speed/Duplex Mode
Sets the operating mode of the network interface card. It is recommended to use **Auto Negotiation**.

Internal IP
Sets the starting IP address for IP cameras connected to the PoE interface. The default is 192.168.3.10. Ensure that this address is not in the same subnet as the NVR's IP address.

Max Users
The maximum number of users who can access the NVR simultaneously. This includes APP, Web, VMS, and other client software logins. The default value is 32.

HS Download
Enables high-speed download over the network.

Transfer Mode
Three modes are available: **Quality Preferred**, **Fluency Preferred**, and **Adaptive**. The stream will adjust according to the selected mode. **Adaptive** balances image quality and fluency. *Fluency Preferred* and *Adaptive* are effective only when the sub-stream is enabled; otherwise, only *Quality Preferred* is applied.

4. Click **Apply**.

Note
The internal IP address cannot be configured if the NVR does not support the PoE function. Please verify whether your NVR supports PoE.

10.2.2 NTP

Your device can connect to a Network Time Protocol (NTP) server to ensure that the system time remains accurate.

Steps:

1. Go to **Main Menu** → **Network** → **Base** → **NTP**.
2. Enable the **Enable** option.
3. Enter the required parameters.

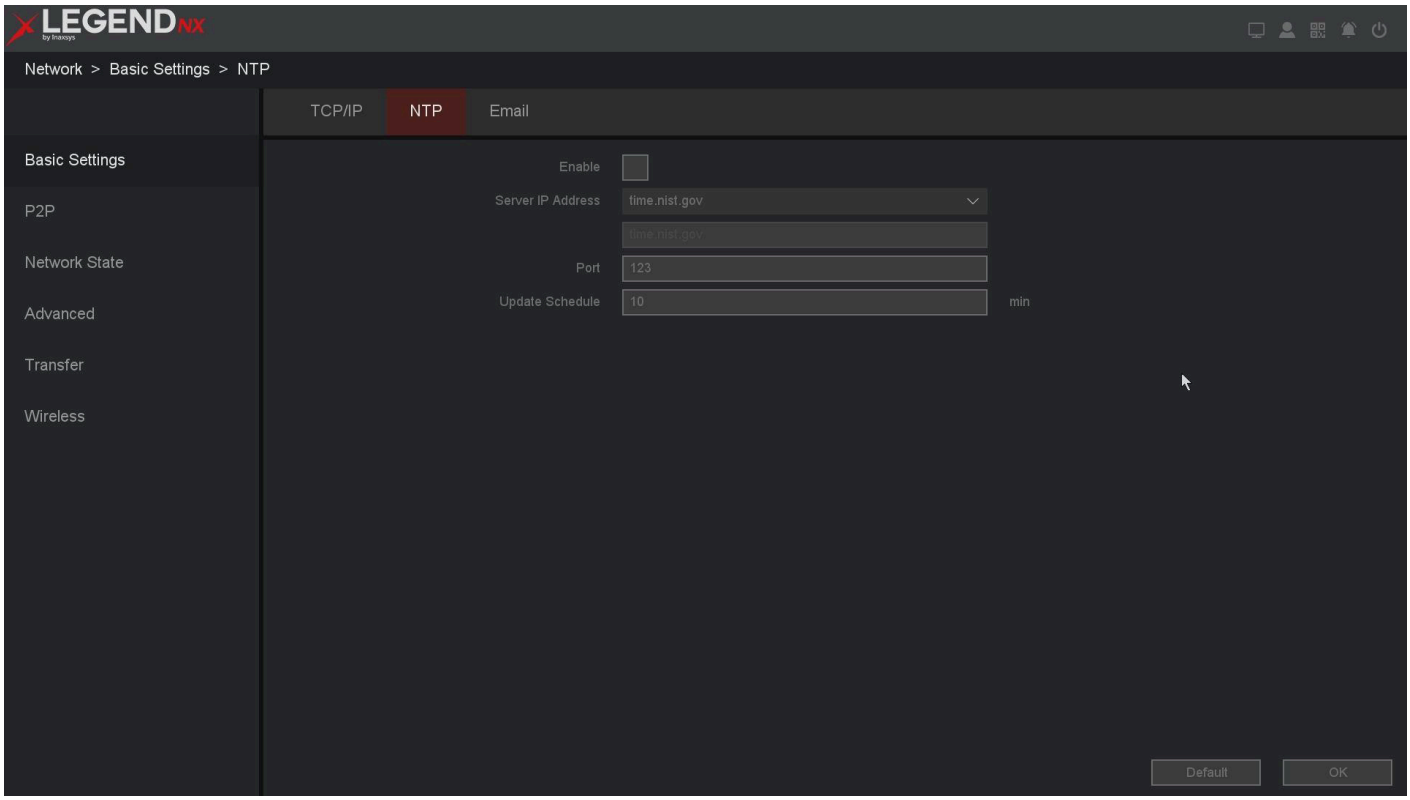


Figure 10-23 NTP

Server IP

The IP address or hostname of the NTP server. Two built-in server addresses are supported, as well as custom configuration.

Port

The port used by the NTP server.

Update Schedule

The time interval between synchronization operations with the NTP server, in minutes.

4. Click **OK**.

Note

The synchronization interval can be set from 1 to 65,535 minutes, with a default value of 10 minutes. If the NVR is connected to a public network, it is recommended to use a reliable NTP server that supports time synchronization, such as a national time service server.

10.2.3 Email & P2P

1. Go to **Main Menu → Network → Basic Settings → Email**. Refer to **6.2.3 Email** for details.
2. Go to **Main Menu → Network → P2P → P2P**. Refer to **6.2.2 LEGEND-P2P** for details.

10.2.4 Network State

Base

In this interface, you can view the network parameters and DHCP status of the device.

3. Go to **Main Menu → Network → Network State → Base**.

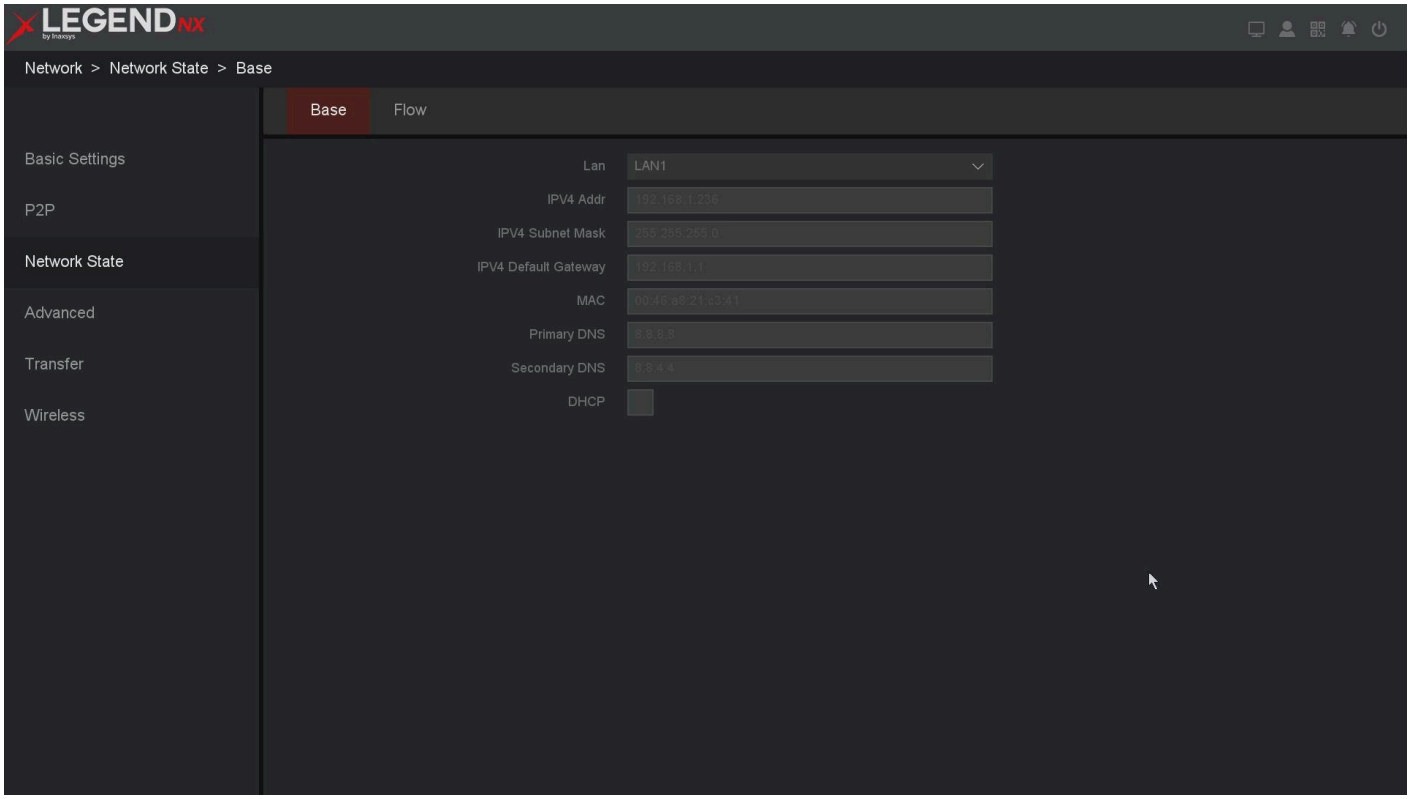


Figure 10-24 Base

Flow

In this interface, you can check the transmission and receiving status of each LAN port.

1. Go to **Main Menu → Network → Network State → Flow**.

Figure 10-25 Flow

Receive

Displays the real-time data rate received by the NVR device.

Transmit

Displays the real-time data rate transmitted by the NVR device.

10.2.5 Advanced

FTP

You can upload recorded files to an FTP server by configuring the FTP settings. This feature allows uploads based on recording type and recording time.

Before You Start

Ensure that the FTP server is running properly and is able to receive uploaded files.

Steps:

1. Go to **Main Menu → Network → Advanced → FTP**.
2. Configure the parameters of the FTP service.

FTP setting

The FTP configuration is divided into video FTP and picture FTP. You can configure the server IP, port, username, password, directory, and file length. An **Anonymous** option is also available, and you can test whether the FTP configuration is successful.

Channel setting

You can select the channel for transmission and configure the schedule by weekday and time period.

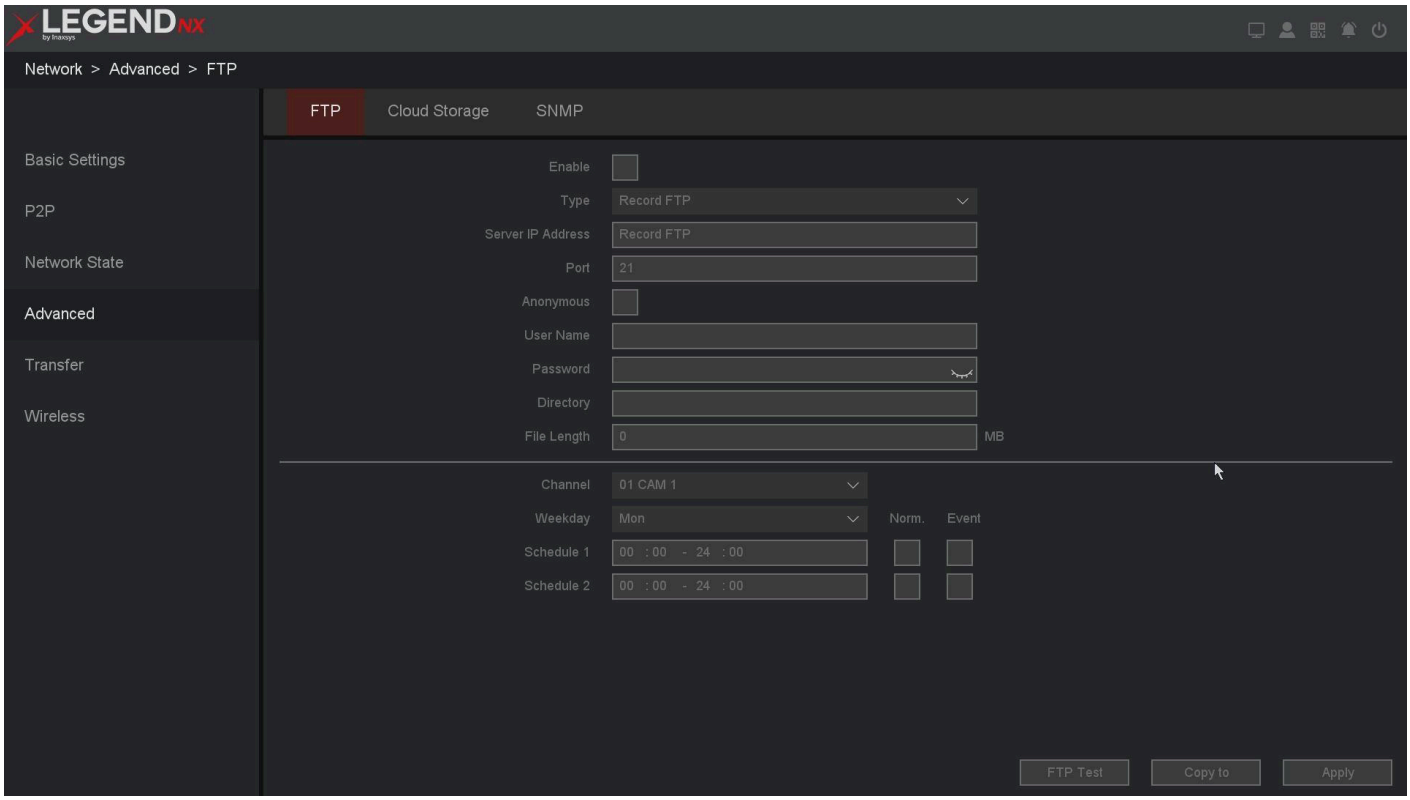


Figure 10-26 FTP

Note

• After completing the configuration, click **FTP Test** to verify that the FTP service is available. The **Copy To** button allows you to copy the current channel configuration to other channels. Click **Apply** to activate the settings.

• Some mail servers require a special authorization code instead of a password. Please follow the requirements of your mail service provider.

Cloud Storage

This feature allows the device to upload video and images to cloud storage. The system supports uploading files stored on the local hard drive to cloud platforms such as Google Drive or Dropbox. Storage costs depend on the pricing policies of the selected cloud service provider.

A hard drive must be installed in the DVR/NVR for cloud storage to function. Once configured correctly, video and image files will be uploaded automatically to the cloud.

Before You Start

Ensure that you have registered accounts for Google Drive and Dropbox.

Steps:

1. Go to **Main Menu → Network → Advanced → Cloud Storage**.

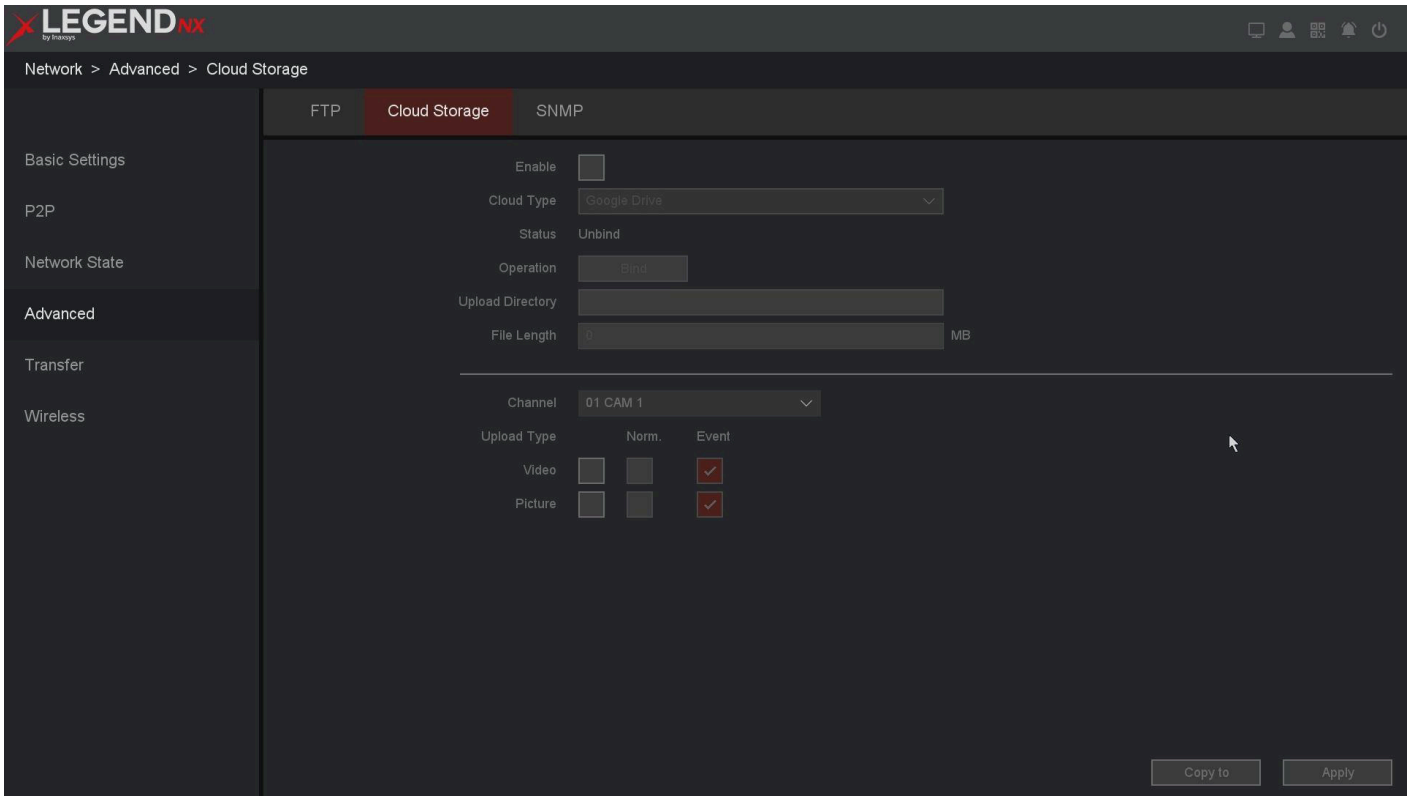


Figure 10-27 Cloud Storage

2. Enable the feature.
3. Select the cloud type.
4. Click the **Bind** button.
5. A window will open displaying a verification code and a QR code.

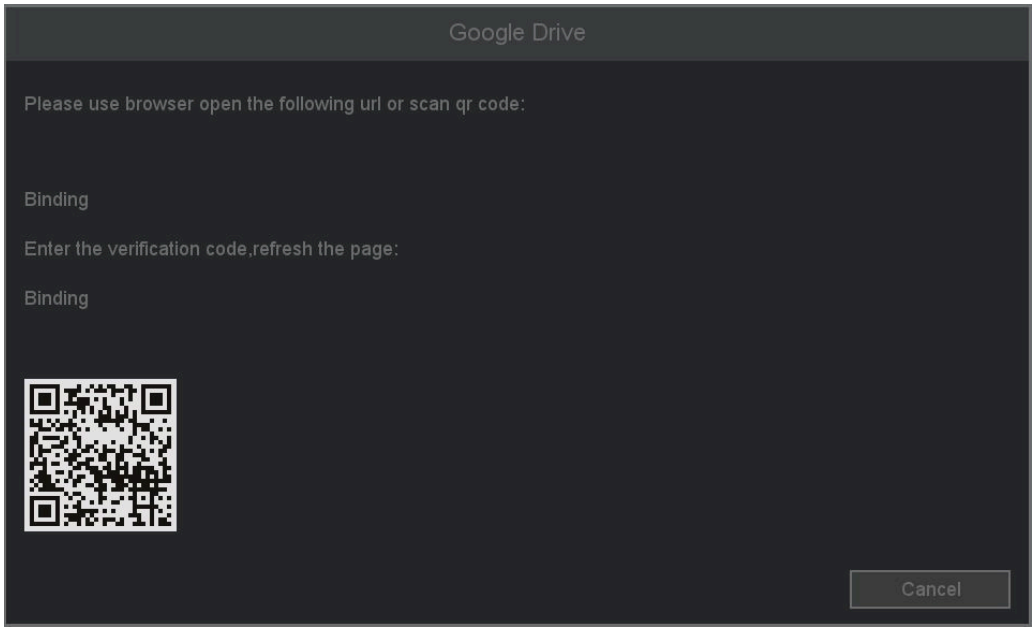


Figure 10-28 Bind

6. Use your mobile phone to scan the QR code, or use a computer to open the URL shown in the prompt.

7. Follow the instructions to enter the verification code, sign in to your account, and click **Allow**.

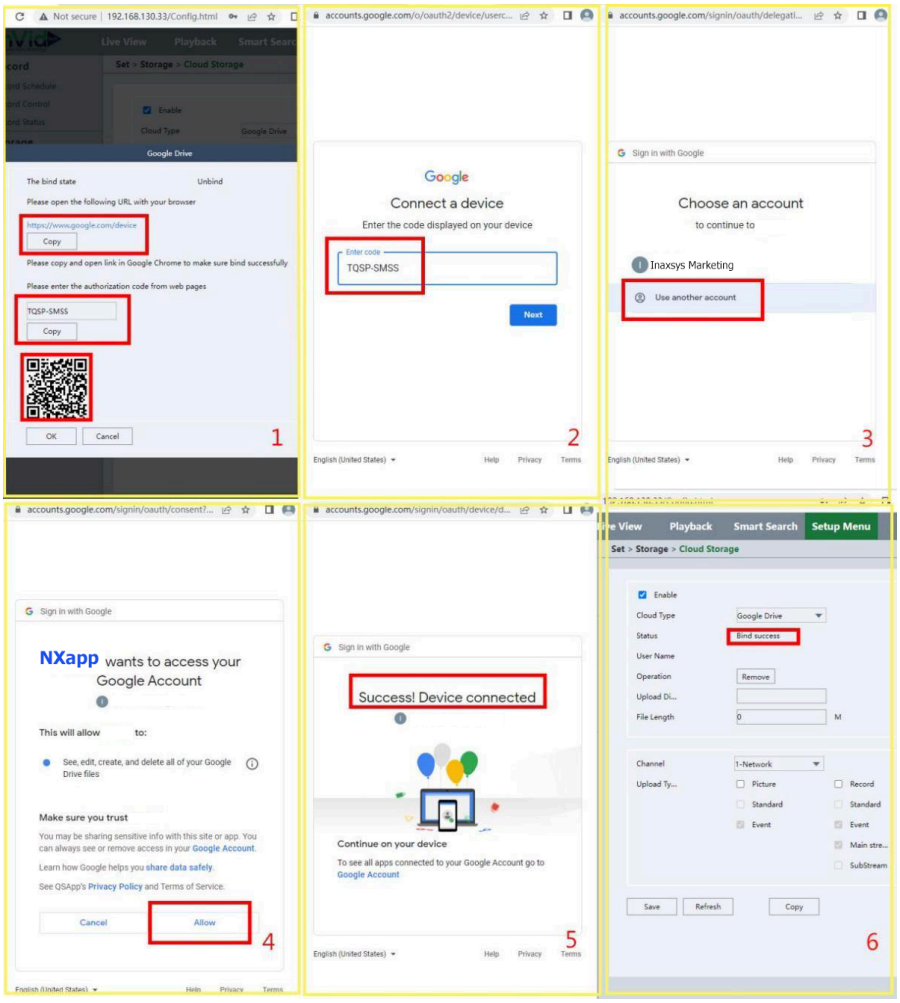


Figure 10-29 Configuration steps

8. After you enter your information and click **Allow** for Google Drive or Dropbox, the status will show **Bind Success**. At this point, you can click **Logout** to close the window.
9. The **Status** field will then display your bound login name.

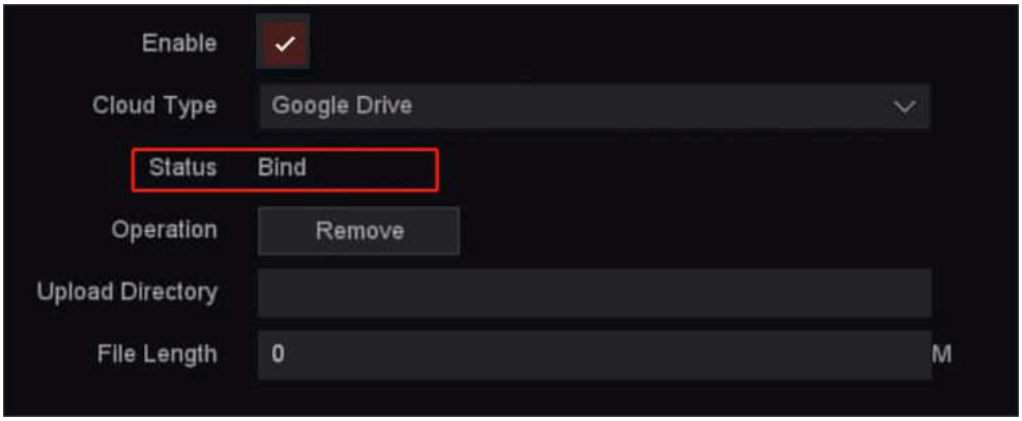


Figure 10-30 Status

10. Under **Upload Directory**, enter a folder name of your choice. This path will automatically appear in the Google Drive or Dropbox directory.
11. Click **Apply** to save the settings.

Cloud Type

The system supports two cloud storage types: **Google Drive** and **Dropbox**.

Upload Directory

Set the folder path for your account on the device.

File Length

Set the duration of video files to be uploaded to the cloud.

Other Setting Items

These settings define how cloud storage works and allow you to specify which types of files will be uploaded.

Channel

Select the channel for which you want to upload files. Different channels can use different upload plans.

Upload Type

Four upload types are available: **Normal**, **Event**, **Main Stream**, and **Sub Stream**.

Video

In **Normal** mode, the device continuously uploads video files while recording is in progress. In **Event** mode, the device uploads video files only according to the plan configured in the alarm trigger process. **Main Stream** and **Sub Stream** allow you to choose which recording stream type will be uploaded.

Picture

The picture upload settings are similar to the video settings. **Normal** and **Event** upload modes are supported.

SNMP

Simple Network Management Protocol (**SNMP**) is an Internet-standard protocol used for collecting and organizing information about managed devices on IP networks, as well as modifying that information to change device behavior.

Steps:

1. Go to **Main Menu** → **Network** → **Advanced** → **SNMP**.
2. Three SNMP versions are supported. **V1/V2** are shown below.

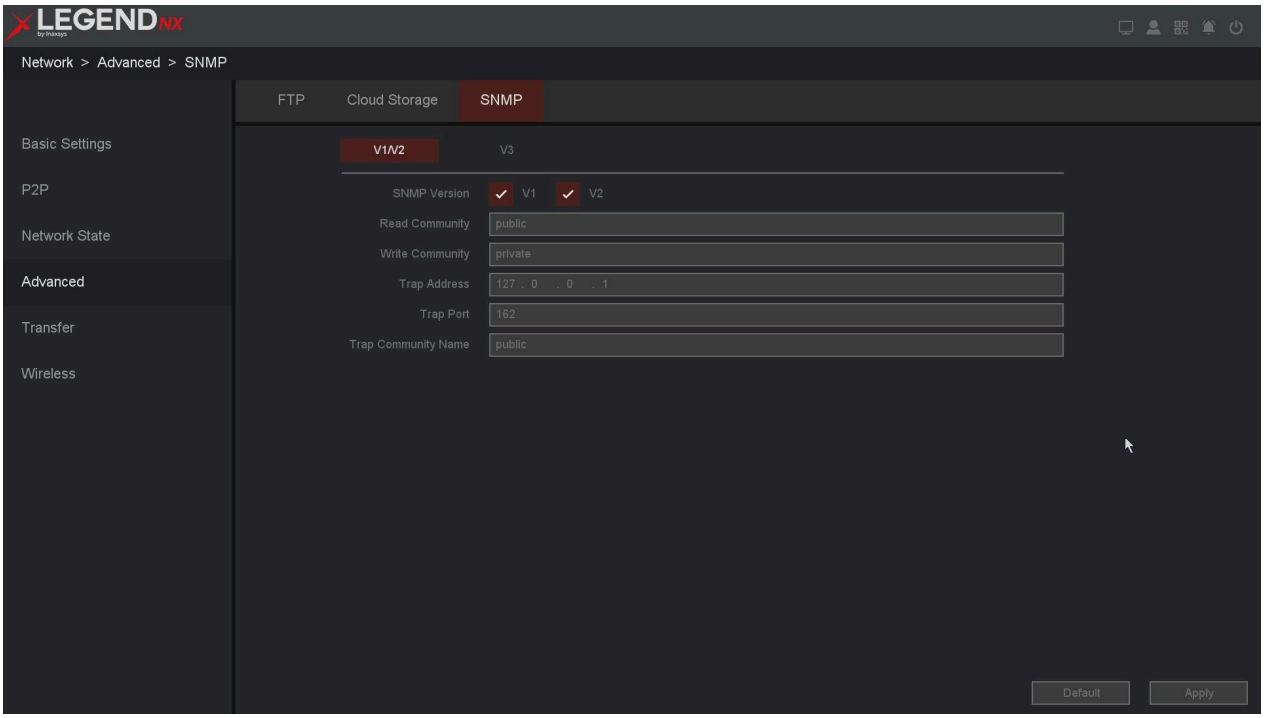


Figure 10-31 V1/V2

3. **V3** is shown below.

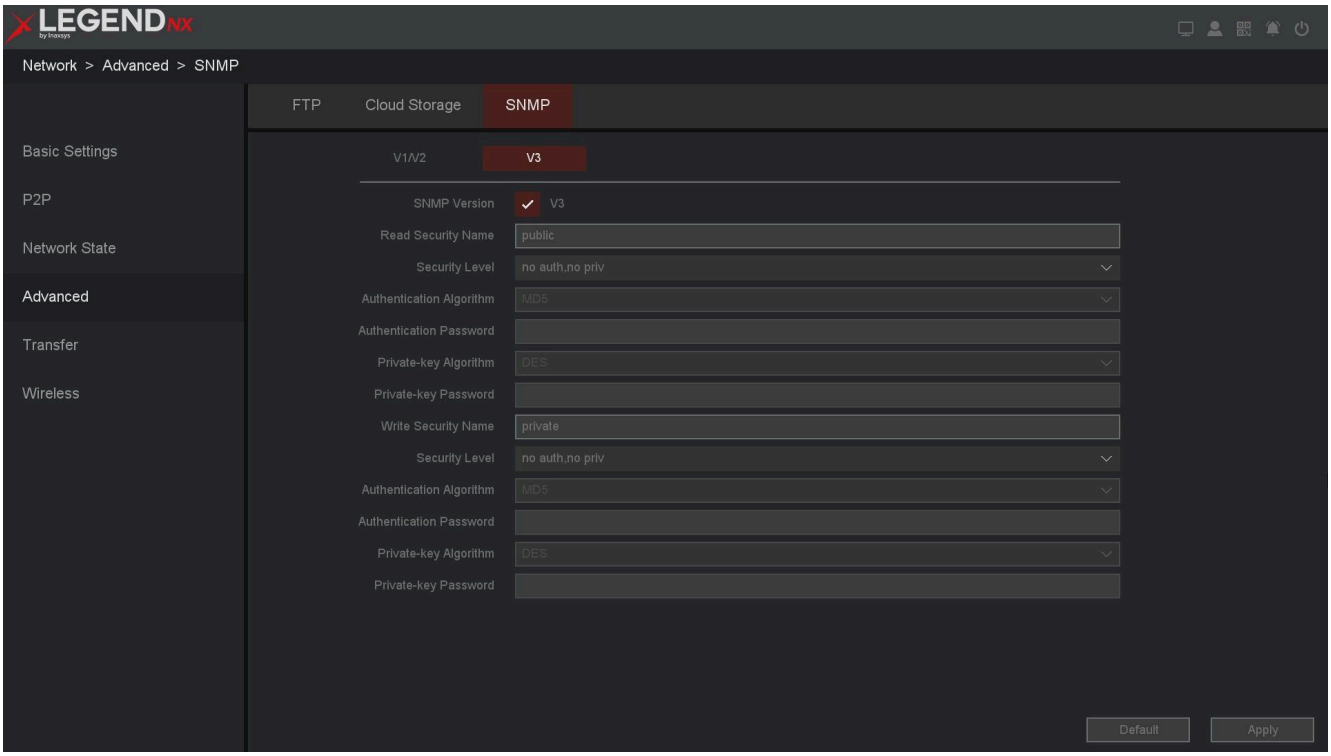


Figure 10-32 V3

4. Select the protocol version according to your requirements.
5. Click **Apply** to save the settings.

10.2.6 Transfer

UPNP

Universal Plug and Play (**UPnP**) is a networking standard that uses Internet protocols to allow devices on a network to automatically detect and identify each other. It also supports automatic port forwarding.

Before You Start

To use the UPnP function, enable UPnP on your router. When the device operates in multi-address mode, ensure that the default route of the device is on the same network segment as the router's LAN IP address.

Steps:

1. Go to **Main Menu** → **Network** → **Transfer** → **UPNP**.
2. Enable **UPNP**.
3. Configure the **Media Port**, **HTTP Port**, **Handset Port**, **HTTPS**, and **SNMP** as required.
   (If you are unsure, do not modify these values, as they may conflict with other system ports.)
4. Click **Apply**.

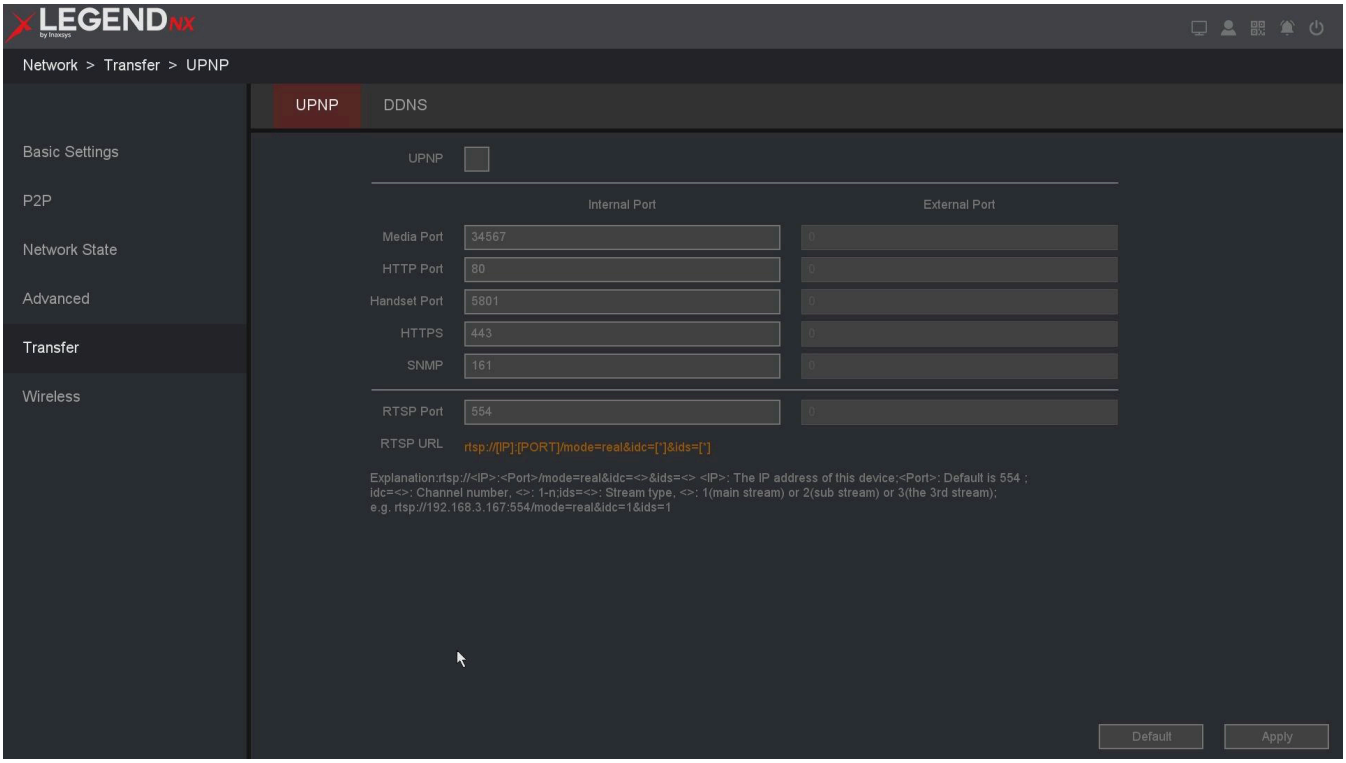


Figure 10-33 UPNP

Note

- **RTSP Port**: RTSP (Real-Time Streaming Protocol) is a network control protocol used in streaming media systems. Enter the RTSP port in the corresponding field. The default port is **554**, but it can be modified as needed.

- The RTSP port value should be **554** or within the range **1024–65535**. Other port values must be between **1–65535**, and each port must be unique. If multiple devices are configured with UPnP under the same router, ensure that each device uses a different port number.
- As shown in the figure above, the RTSP address can be used for RTSP streaming.

DDNS

Dynamic Domain Name System (**DDNS**) is a service that automatically updates DNS records when a client device obtains its IP address from a DHCP server. When DDNS is enabled on the NVR, you can access the device using a domain name provided by your Internet Service Provider (ISP).

Before You Start

Register a DDNS service such as **Oray DDNS**, **CN99 DDNS**, **DynDNS**, or **NO-IP** with your ISP.

Steps:

1. Go to **Main Menu** → **Network** → **Transfer** → **DDNS**.
2. Enable the function.
3. Select a DDNS type.
4. Enter the required parameters, including **domain name**, **user name**, and **password**.
5. Click **Apply**.

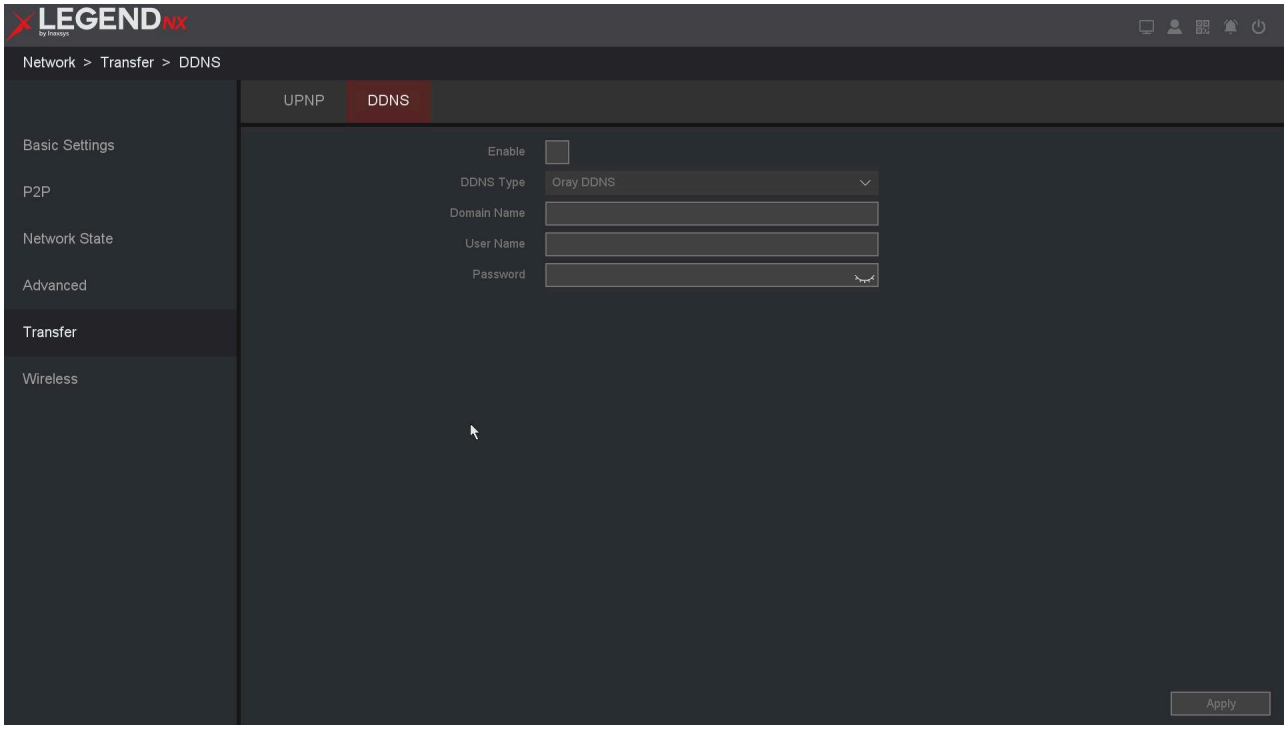


Figure 10-34 DDNS

DDNS Type
Select the DDNS service provider, such as **Oray DDNS**, **CN99 DDNS**, **DynDNS**, or **NO-IP**. This option can be customized based on user requirements.

Domain Name
Enter the domain name provided by your ISP.

User Name/Password
Enter the username and password associated with the domain name.

10.2.7 Wireless

Use the **Wireless** function to enable your device to connect to the network wirelessly.

3G/4G
This feature allows the device to connect via a **3G/4G mobile network**.

Before You Start

Ensure that your device model supports wireless functionality. Prepare a **3G/4G data card** and connect it to the USB port of the NVR. The **username** and **password** must be provided by your ISP.

Steps:

1. Go to **Main Menu → Network → Wireless → 3G/4G**.
2. Check the **Status**. (If it displays “Device does not exist,” the function is not available.)
3. Enable the function.
4. Configure the **3G/4G signal type**, **Access Point**, **Dial Number**, **User Name**, **Password**, and **IP Address**.

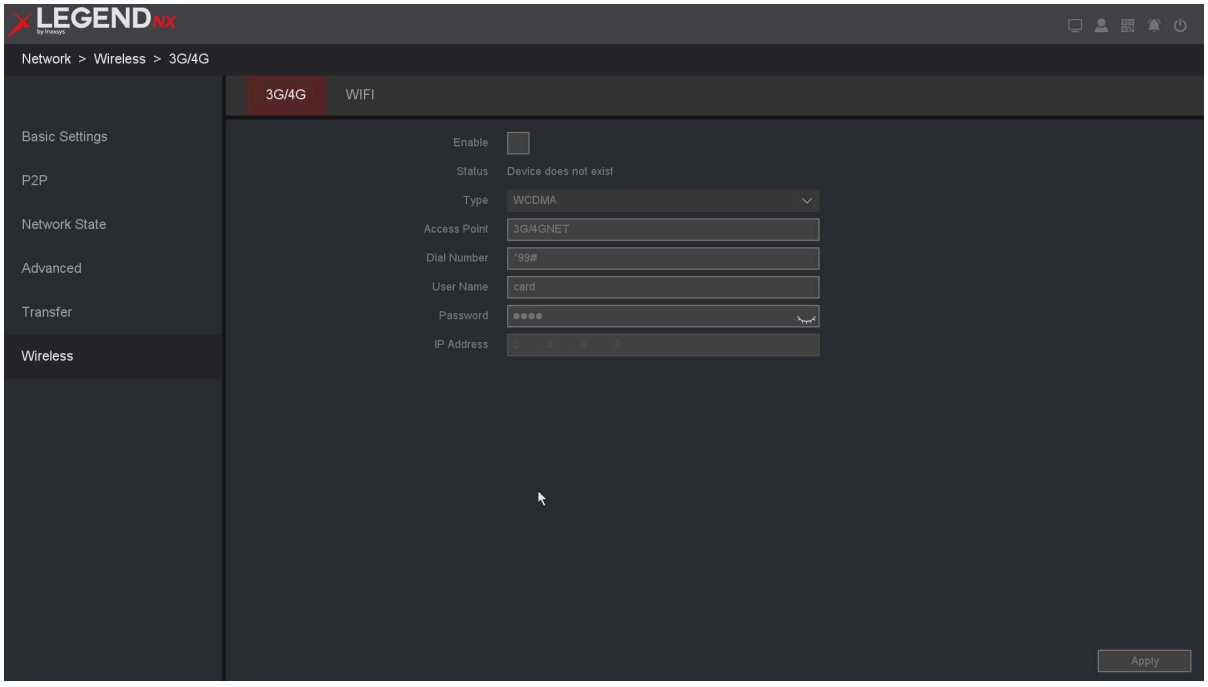


Figure 10-35 3G/4G

5. Click **Apply**.

WIFI

This feature allows your device to connect to a Wi-Fi network.

Before You Start

Ensure that your device model supports wireless functionality, and confirm that your Wi-Fi network can access the Internet properly.

Steps:

1. Go to **Main Menu → Network → Wireless → WIFI**.

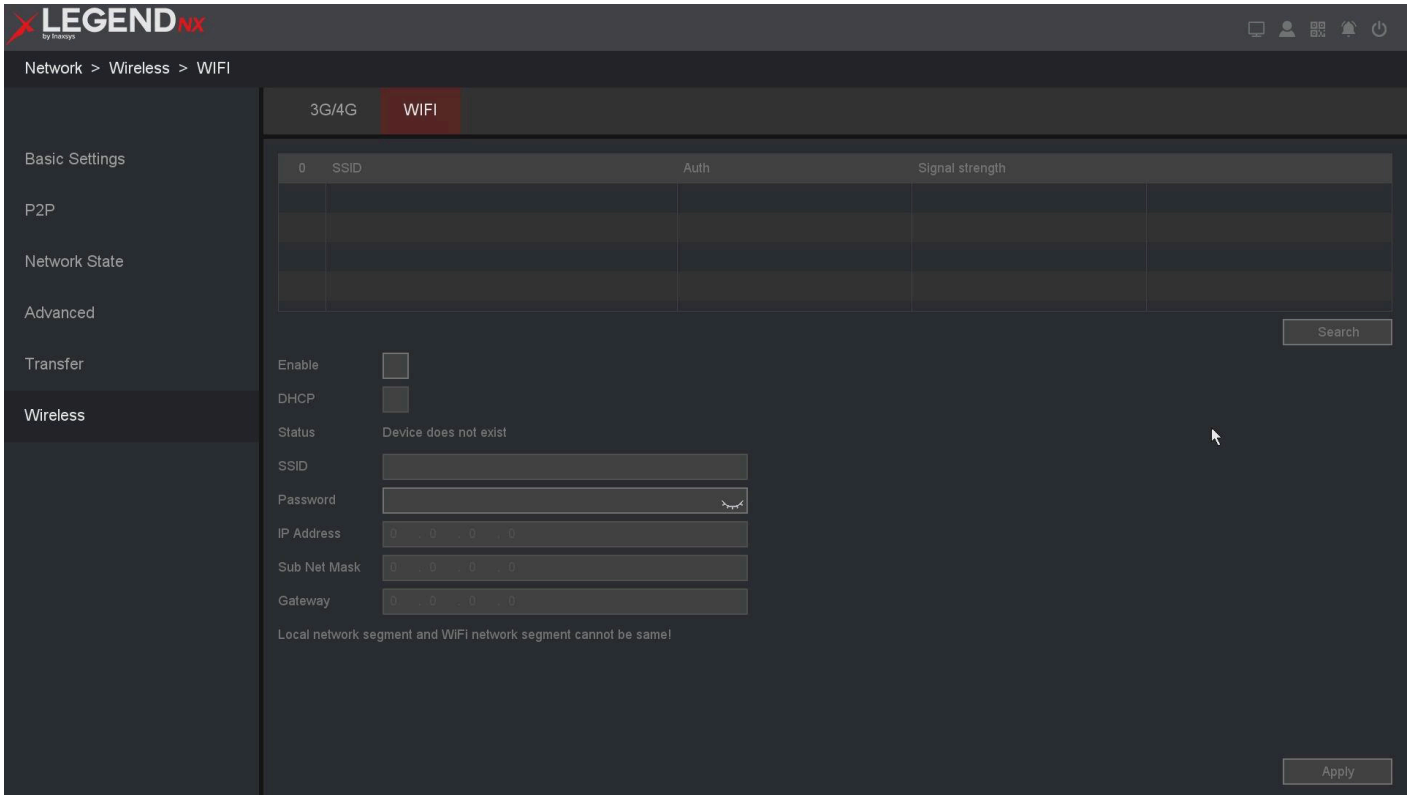


Figure 10-36 WIFI

2. Click **Search** to find available Wi-Fi networks.
3. Select the desired Wi-Fi network.
4. Enable the function.
5. Enable **DHCP**.
6. Check the **Status**. If it shows “Connected,” the wireless Wi-Fi connection has been successfully established.

10.3 Camera Management

10.3.1 IP Channel

Channel Setting
To automatically add detected online network cameras or to add network cameras manually, refer to **2.5 Adding the Online IP Cameras**, **2.6 Editing the Connected IP Cameras and Configuring**, **2.7 Editing IP Cameras Connected to the PoE Interfaces**, and **6.3.1 Network Camera**.

Fisheye Set
In this interface, you can configure the mounting mode and preview mode for fisheye cameras.

Before You Start

Ensure that a fisheye camera is connected to your network.

Steps:

1. Go to **Main Menu** → **Camera** → **Fisheye Set**.

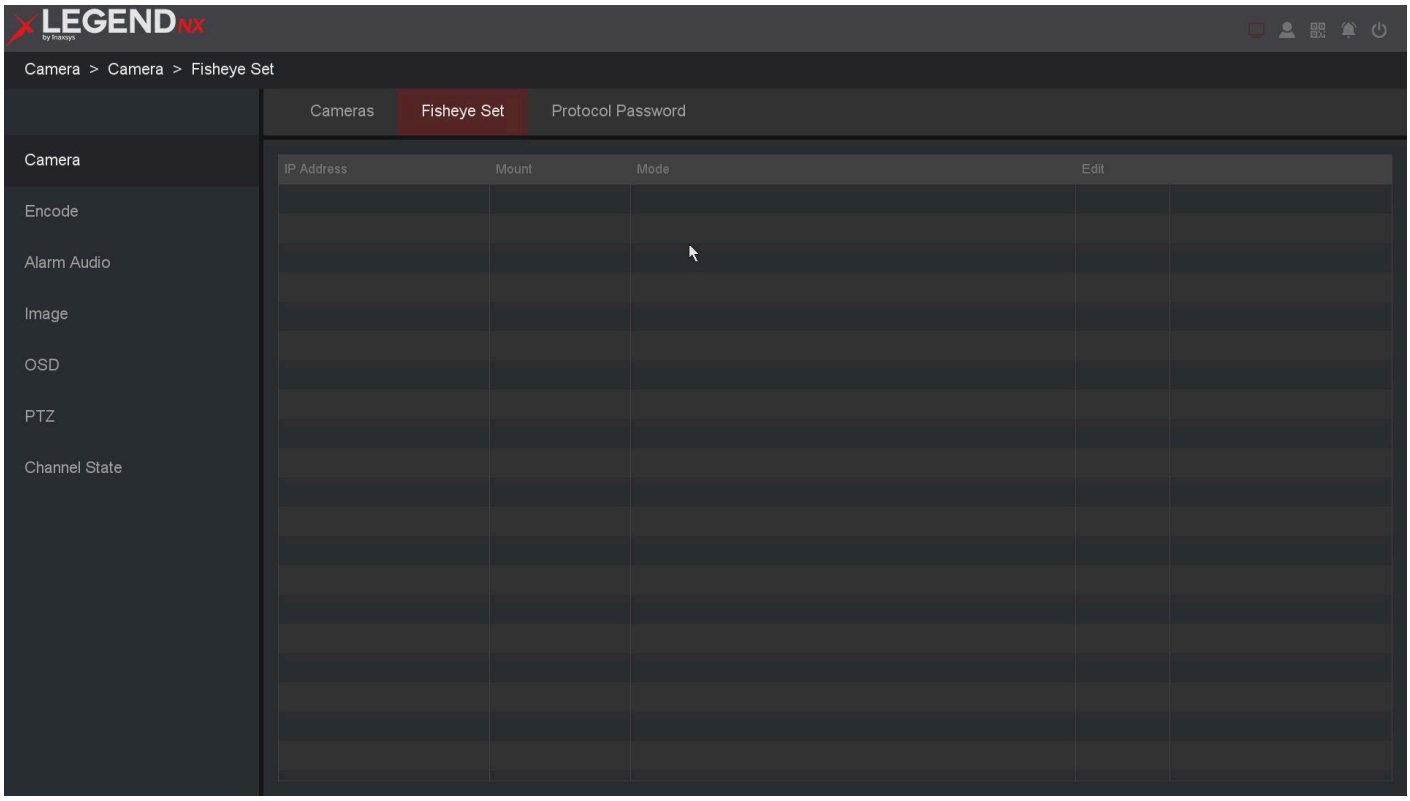


Figure 10-37 Fisheye Set

2. Click **Edit**.
3. Configure the parameters as required.
4. Three mounting modes are available: Desktop, Ceiling, and Wall.
5. Six preview modes are available:

Fisheye
Displays only the fisheye image.

Panoramic
Displays only a panoramic image.

PTZ 1 + PTZ 2 + PTZ 3 + PTZ 4
Displays four PTZ views simultaneously.

Fisheye + Panoramic + PTZ 1 + PTZ 2 + PTZ 3
Displays one fisheye view, one panoramic view, and three PTZ views simultaneously.

Fisheye + PTZ 1 + PTZ 2 + PTZ 3 + PTZ 4
Displays one fisheye view and four PTZ views simultaneously.

Panoramic + PTZ 1 + PTZ 2 + PTZ 3 + PTZ 4
Displays one panoramic view and four PTZ views simultaneously.

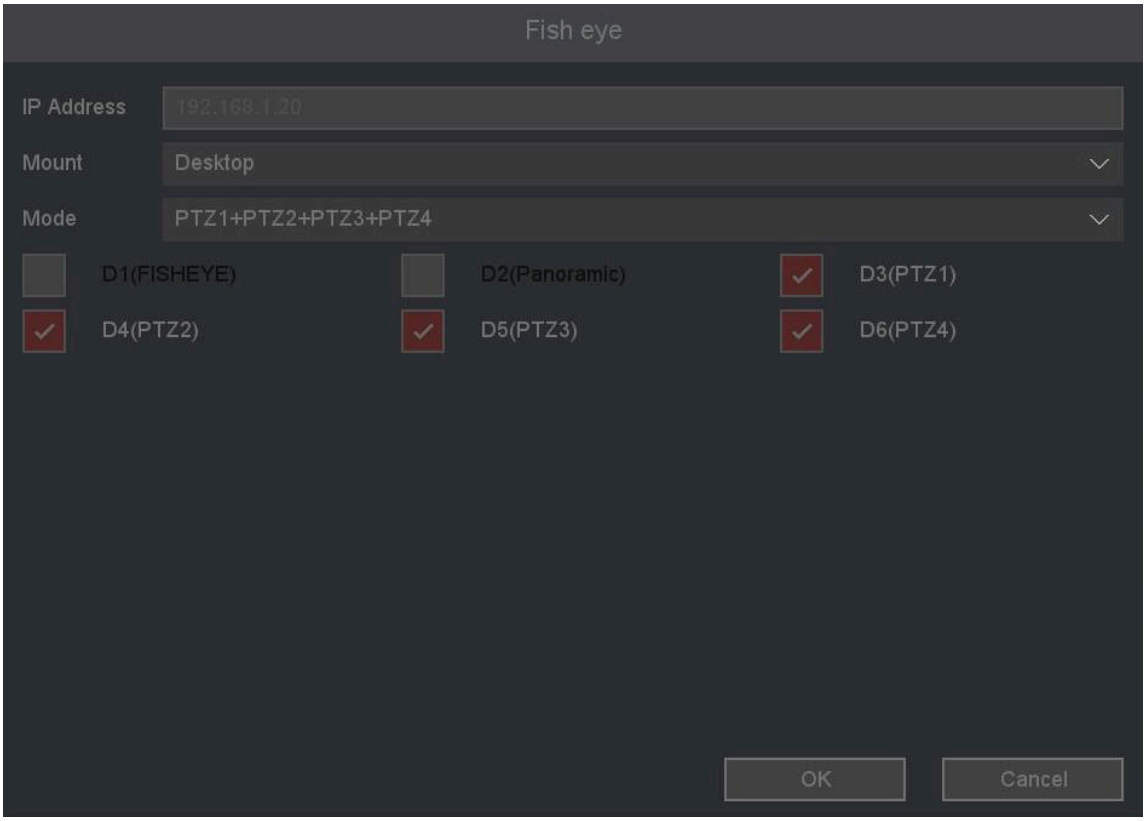


Figure 10-38 Fisheye Modes

Note
Each time the preview mode is changed, the fisheye camera will reboot.

Protocol Password

When adding IP cameras detected by the NVR, the system will prioritize using the specified password.

Before You Start

Ensure that you know the protocol and the corresponding password required to connect to the camera.

Steps:

1. Go to **Main Menu** → **Camera** → **Protocol Password**.

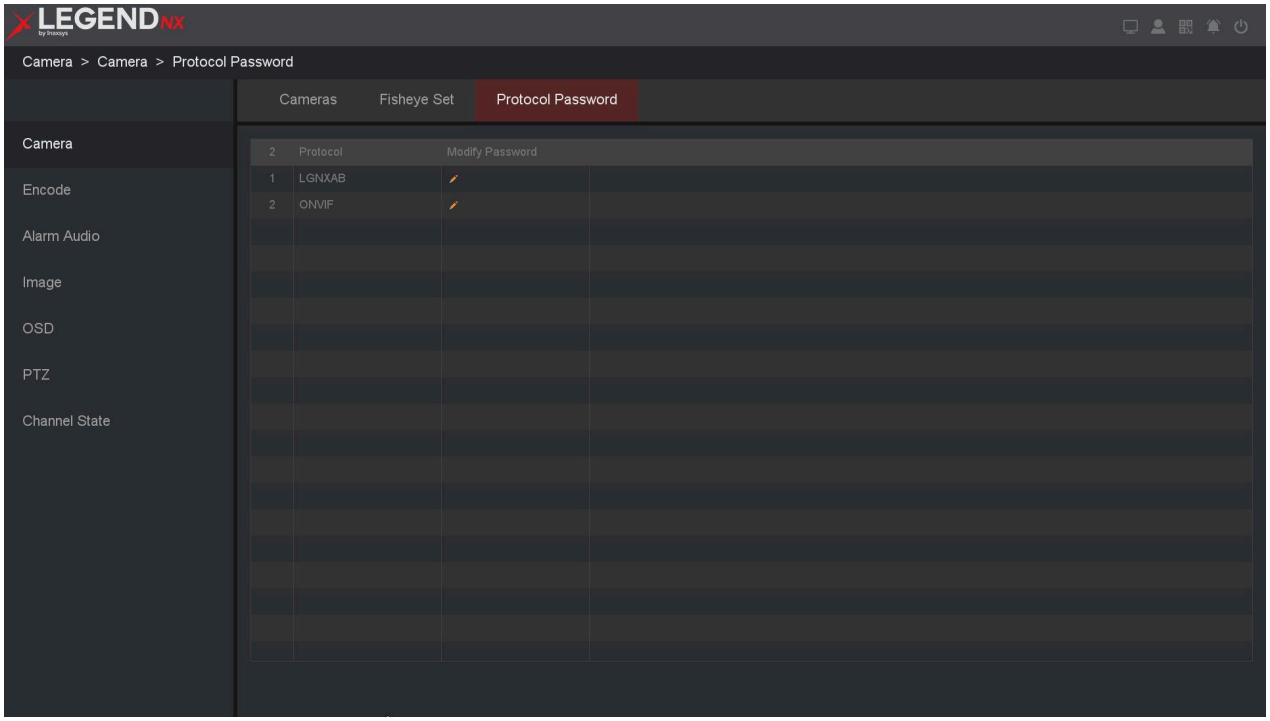


Figure 10-39 Protocol Password

2. Click **Edit**.

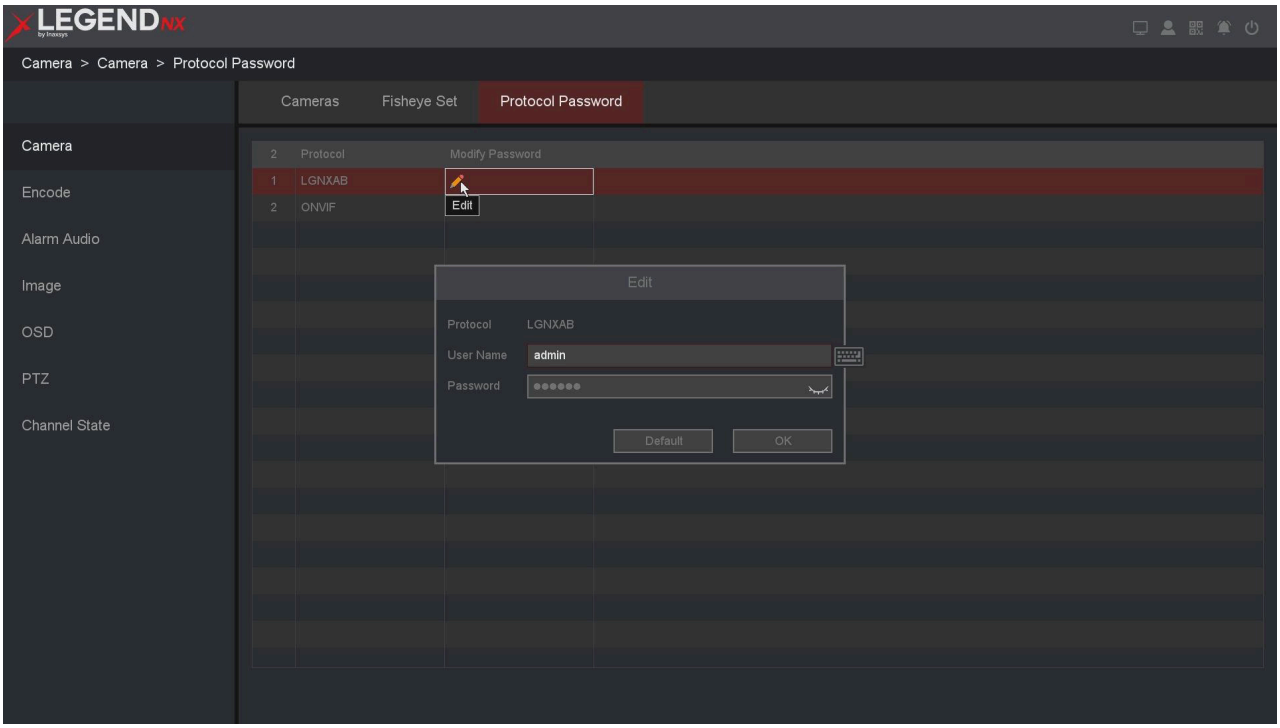


Figure 10-40 Edit Protocol Password

3. Select the **protocol** you want to modify.
4. Set the common password.
5. Click **OK**.
6. Click **Apply**.

Note
If the camera connection status shows an identification error, you must manually change the password again. For details, refer to **2.6 Editing the Connected IP Cameras and Configuring**.

10.3.2 Encode

By configuring the encoding parameters, you can define settings that affect image quality, such as compression type, resolution, frame rate, bit rate type, and quality.

The NVR supports dual-stream encoding, allowing you to configure both the main stream and sub stream on this screen.

Before You Start

Ensure that at least one IP Camera is connected and its status is **Connected**.

Steps:

1. Go to **Main Menu → Camera → Encode**.

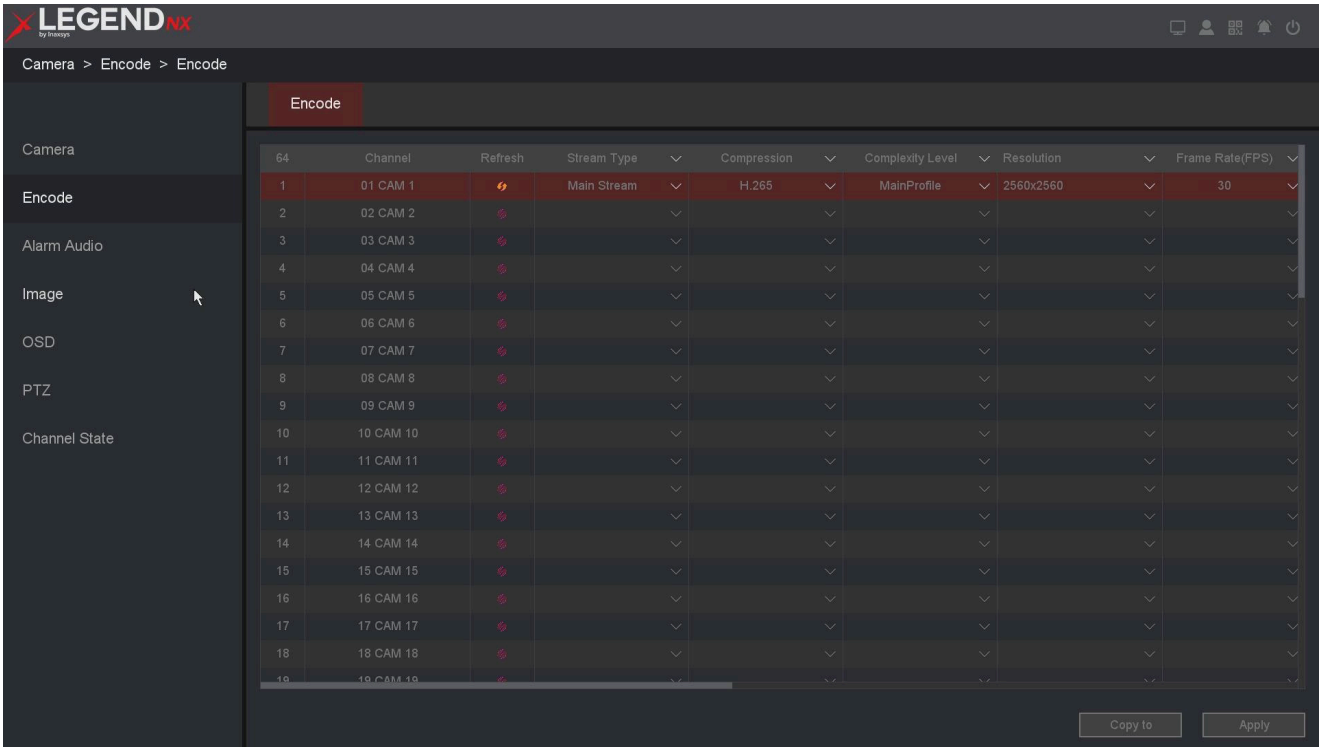


Figure 10-41 Encode

2. You can also access this page via **Main Menu → Camera → Encode**.

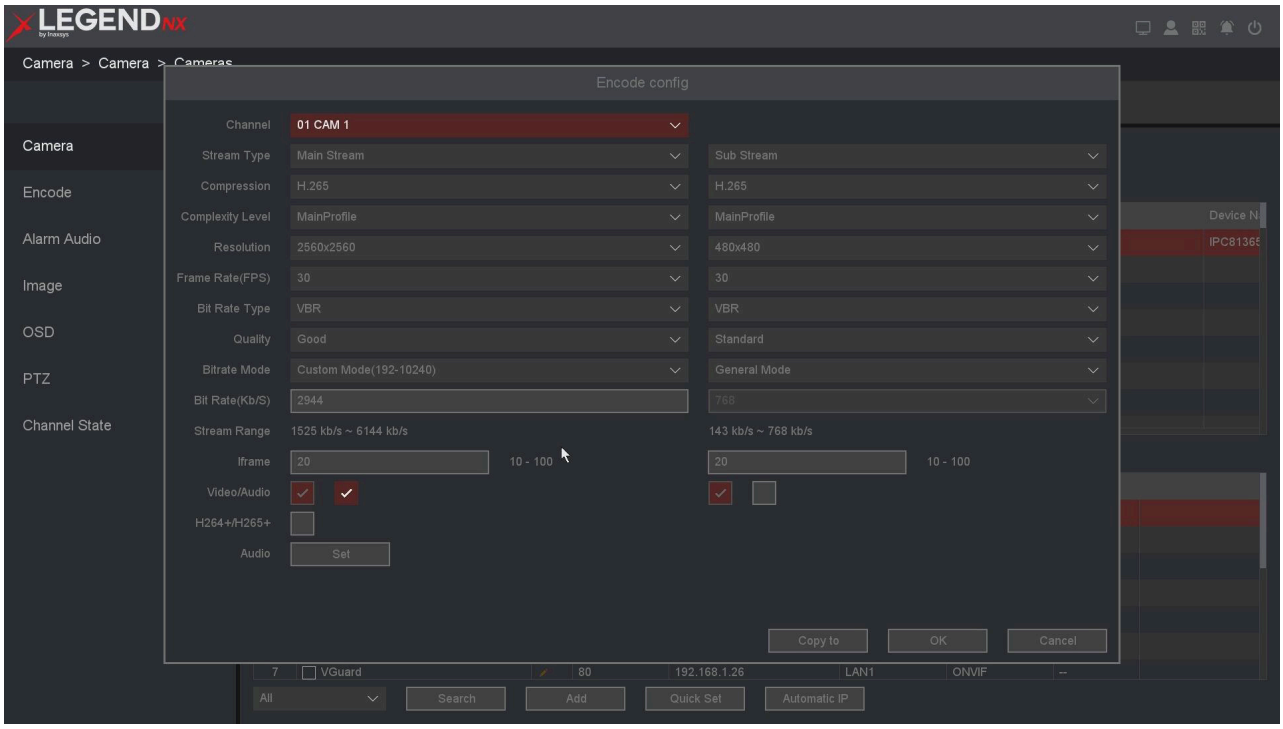


Figure 10-42 Encode Config

3. Configure the parameters as required.

Channel
Select the channel to configure.

Refresh
Click to refresh the encoding parameters of the IP channel.

Stream Type
Main Stream / Sub Stream / Event Stream / Mobile Stream.

Compression
H.265 is used for encoding. H.264 IP cameras are also supported.

Complexity Level
Base Profile / Main Profile / High Profile.

Resolution
The resolution of the recorded video.

Frame Rate (FPS)
The number of frames per second in the video stream.

Bit Rate Type
CBR / VBR.

Image Quality
Lowest / Low / Standard / Good / Better / Best.

Bit Rate Mode
General Mode / Custom Mode.

Bit Rate (Kb/s)
Defines the bandwidth value.

Stream Range
The bitrate range for this channel.

I-Frame GOP
I-frame interval setting, range: 10–100.

Video/Audio
Enables video and audio encoding for recorded files. Video for the main stream is always enabled.

H.264+ / H.265+
Enables smart encoding technology, which can reduce HDD storage usage by up to 80%–90% in static scenes.

Audio
Configure the audio encoding settings for this channel as shown below.

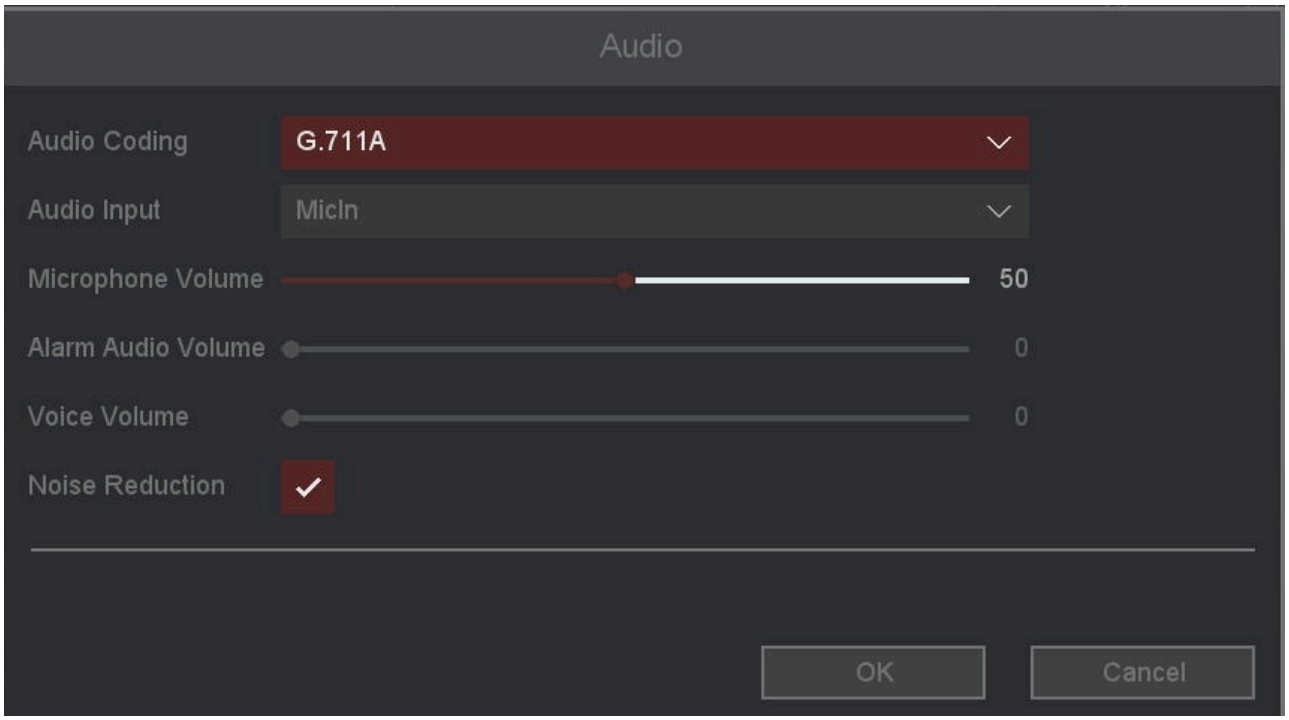


Figure 10-43 Audio

1. Optional: You can use the **Copy to** function to quickly apply the same parameters to multiple channels.
2. Click **OK**, then click **Apply**.

Note
When using the **Copy to** function, it is recommended to apply it to cameras of the same model.

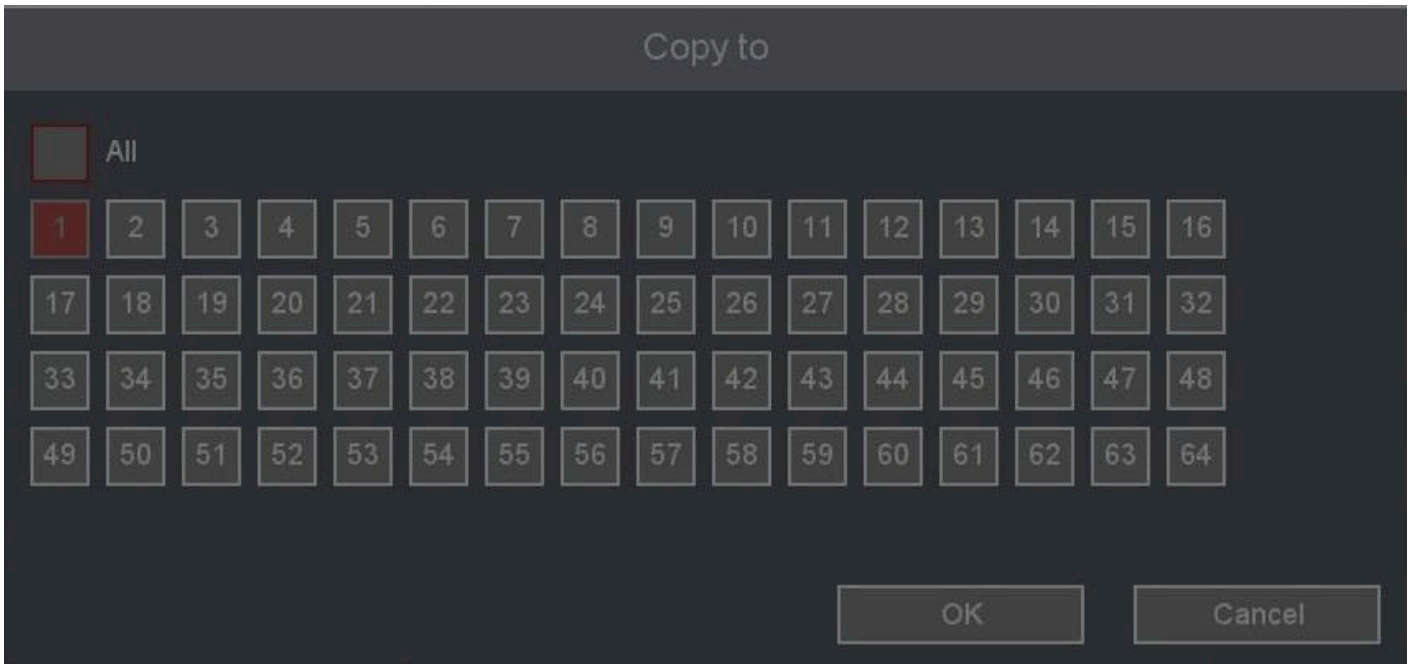


Figure 10-44 Copy to

10.3.3 Color

The camera is preconfigured with default settings before leaving the factory, which meet most standard application requirements. If higher image quality is required, IP cameras support image adjustments such as brightness, contrast, saturation, hue, and sharpness. Some advanced IP cameras also support additional settings, including image adjustment, exposure, backlight, white balance, and day/night configuration. In this section, you can configure these parameters to optimize image quality and improve the viewing experience.

Before You Start

Ensure that at least one IP Camera is connected and its status is **Connected**.

Steps:

1. Go to **Main Menu** → **Channel** → **Color**.
2. Configure the parameters as required.

Channel
Select the channel to configure.

Image Mode
Defines the image mode for specific time periods. Available options are Auto and Manual.
Auto mode applies the same image settings 24 hours a day.
Manual mode allows separate configurations for two periods: Day and Night.
You can configure different image parameters for each period.

Start-End
When **Image Mode** is set to Manual, specify the start and end times for the Day or Night period.

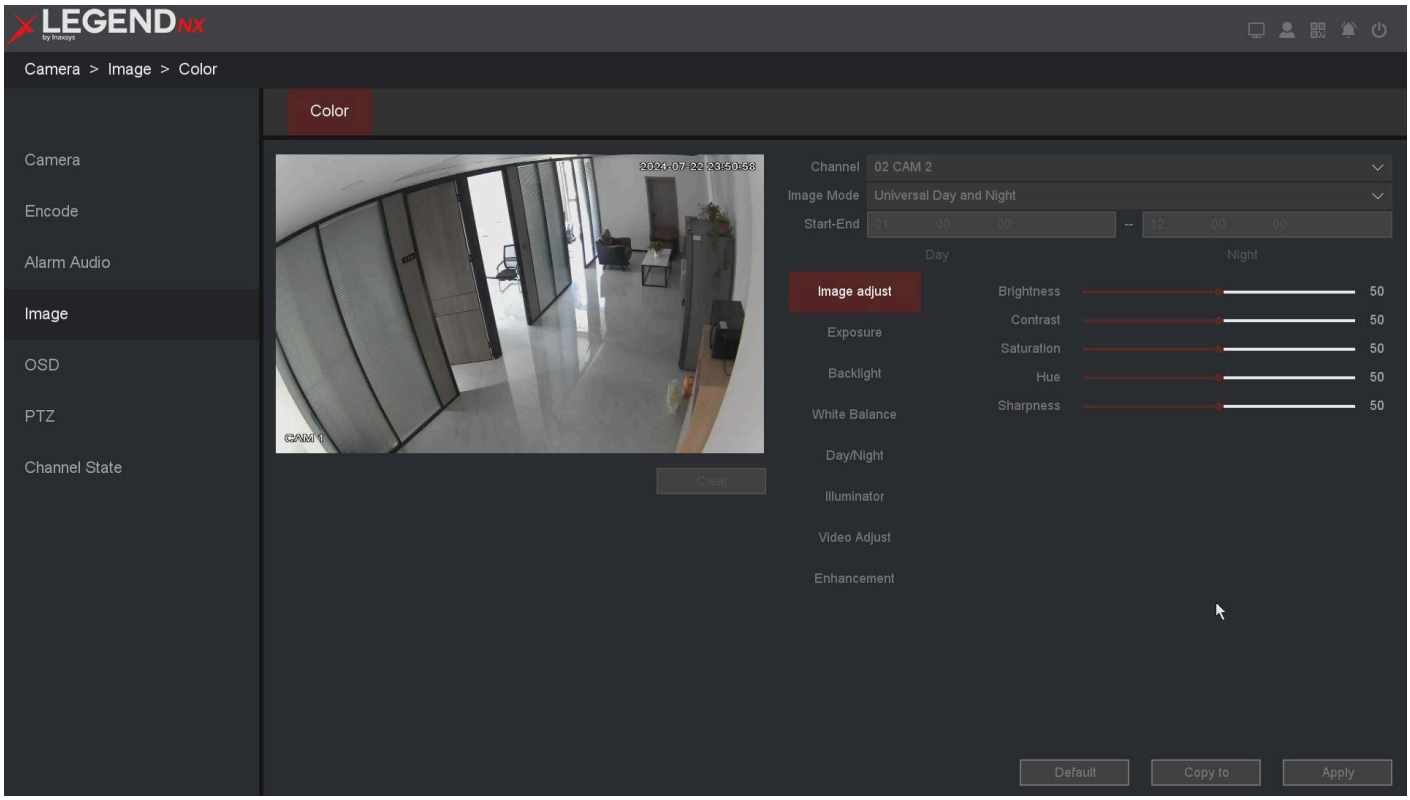


Figure 10-45 Color

3. Set the IP camera parameters on this screen if the camera is compatible with the NVR.

Table 10-1 Function Description

Functions	Description	Functions	Description
Image adjust	Brightness: 0–100 Contrast: 0–100 Saturation: 0–100 Hue: 0–100 Sharpness: 0–100	Video adjust	Image: Close / Up / Down / Left / Right / Center Rotate: Off / 90 / 180 / 270
Exposure	Auto: Automatically sets exposure time Manual: Set exposure time manually	Defog	Only supported on certain models Close: Disable Auto: Automatic defog Manual: Adjust manually
Backlight	DWDR: Close / DWDR / WDR (if supported) Limit: Adjust DWDR/WDR level Backlight Comp: Off / HLC / BLC (when DWDR is disabled)	Illuminator	Only supported on certain models IR Setting: Controls infrared light Warm Light Setting: Controls warm light

White balance	Auto: Automatic adjustment Manual: Set Red Gain and Blue Gain manually	Enhancement	Only supported on certain models NR Level: 0–6 Defog: Close / Auto / Manual Smart Light: Close / Manual / Auto
Day/Night	Auto: Switches based on sensitivity Daytime: Always color Night: Always black & white Switch Type: IR synchronous Filter Time: 1–120 s adjustable Fill Light: Configure when supported		

Image adjust
Customize image parameters such as brightness, contrast, and saturation for live view and recording.

Exposure
Set the camera exposure time (1/10000 to 1 second). A higher exposure value results in a brighter image.

Backlight
Adjust the camera's wide dynamic range (0–100). When there is a significant difference in brightness between the subject and the background, configure the WDR value accordingly.

Day/Night
The camera can be set to Day mode, Night mode, or Auto switching mode based on ambient lighting conditions.

Illuminator

Note
This function is only supported on certain device models.

Fill Light
Four options are available: IR Mode, Warm Light Mode, Smart Illumination, and Schedule.
The **Schedule** and **Setting** buttons are displayed only when Schedule mode is selected. Click **Setting** to open the Lighting Plan configuration, as shown below.

In this interface, you can define lighting schedules for different illumination modes. The color indicators represent:

- Green: Smart mode
- Orange: Warm Light mode
- Blue: Infrared Lamp

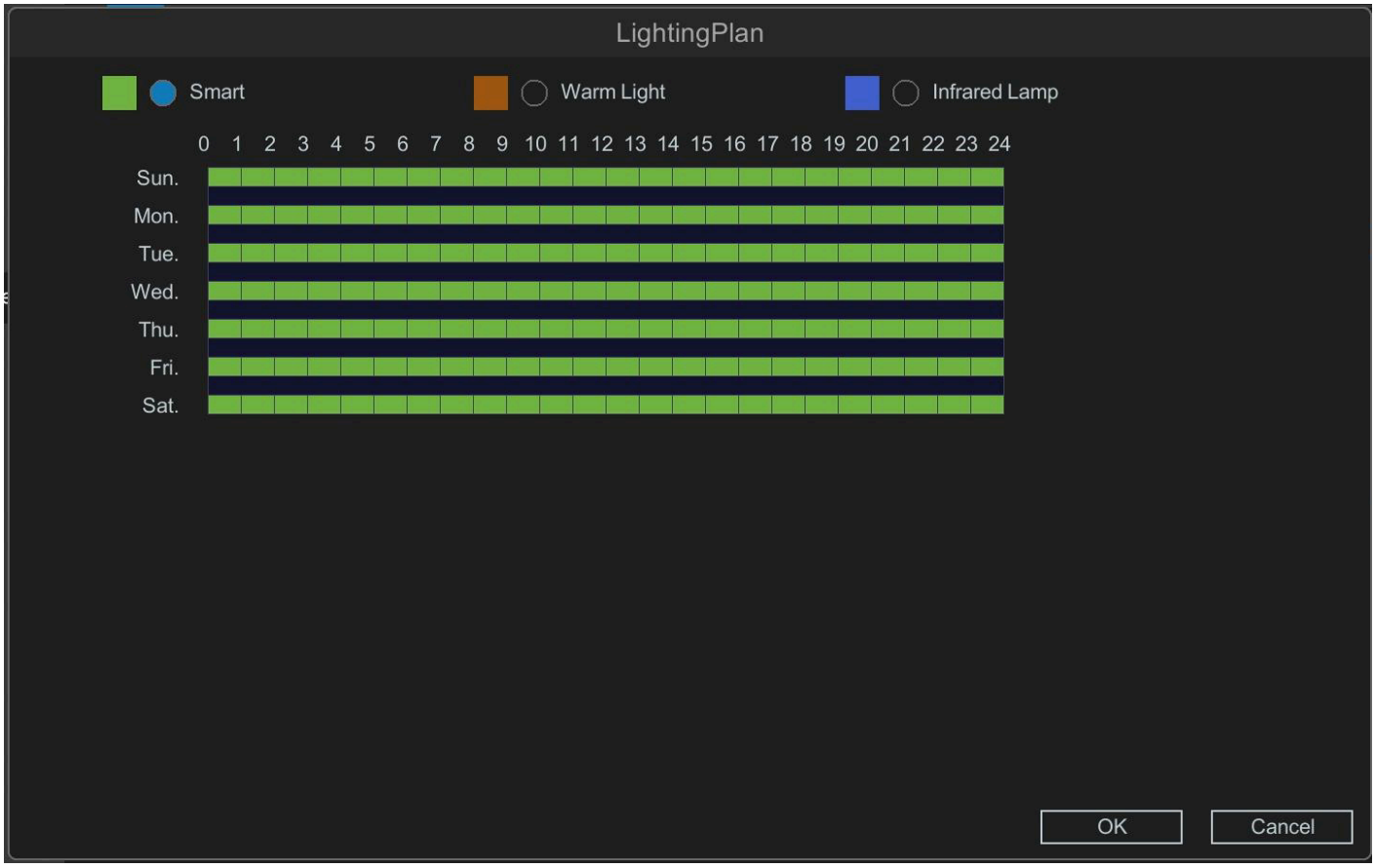


Figure 10-46 Illumination Plan

IR Light Setting

Fill Light Mode

Controls the camera's infrared lighting hardware switch, independent of the Fill Light selection.

Available options: Close, Manual, and Auto. Default is Manual.

Close

Disables the camera's infrared light.

Note

If you need to use the infrared lighting function, do not set **Fill Light Mode** to Close.

Manual

In this mode, the infrared light operates at maximum brightness.

Auto

Automatically adjusts infrared brightness. When Auto mode is enabled, Smart IR is activated.

Smart IR dynamically adjusts infrared intensity based on scene brightness. When an object is very close to the camera, excessive IR illumination may cause overexposure (white-out). Smart IR reduces the IR output to preserve image details.

Warm Light Setting

Fill Light Mode
Controls the camera's warm light hardware switch, independent of the Fill Light selection.
Available options: Close, Manual, and Auto. Default is Auto.

Close
Disables the camera's warm light.

Note
If you need to use the warm light function, do not set **Fill Light Mode** to Close.

Manual
When enabled, the **Brightness Upper Limit** parameter becomes available, with an adjustable range of 0–100 (default: 50).

Auto
When enabled, the **Brightness Upper Limit** parameter becomes available, with an adjustable range of 1–100 (default: 100).

Illuminator Delay
Adjustable from 10 to 300 seconds. Default: 30 seconds.

Video Adjust
Adjust the image orientation and rotation angle.

Enhancement
Used to enhance image contrast and overall visual quality.

10.3.4 OSD

OSD
You can configure the OSD (On-Screen Display) settings for the camera, including channel name, date/time format, recording status, and alarm status. For additional details, refer to **6.3.2 OSD Settings**.

Before You Start
Ensure that at least one IP Camera is connected and its status is **Connected**.

Steps:

1. Go to **Main Menu** → **Channel** → **IP Channel** → **OSD**.
2. Select a camera.

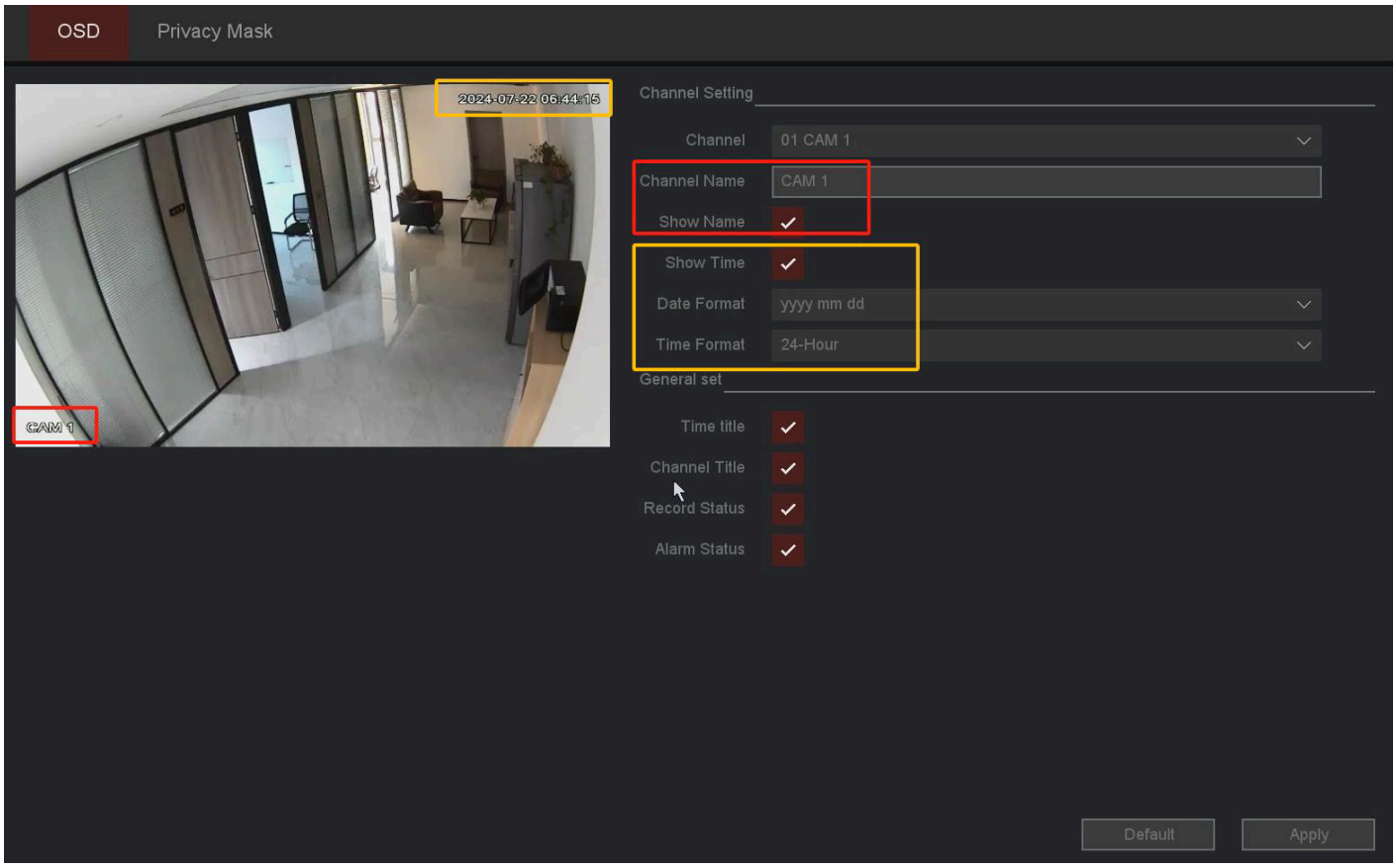


Figure 10-47 OSD

3. Configure the parameters as required.
4. Choose whether to display the channel name and time, and customize them as needed.
5. Click **Apply**.

The settings are divided into two sections: **Channel Settings** and **General Settings**.
Channel settings configure the IP Camera, while general settings control the NVR's local display.

For Channel Settings:

Channel
Select the channel to configure.

Channel Name
Set the name of the channel.

Show Name, Show Time
Enable or disable the display of the channel name and time on the screen.

Date Format, Time Format
Set the display format for date and time.

For General Settings:
Time Title, Channel Title
Enable or disable the display of the time title and channel title on the monitor.

Record Status, Alarm Status

Enable or disable the display of recording status and alarm status on the screen.

Privacy Mask

The Privacy Mask function allows you to block sensitive areas in the monitoring view. Up to four areas can be masked simultaneously.

Before You Start

Confirm in advance the areas that need to be masked.

Steps:

1. Go to **Main Menu** → **Camera** → **OSD** → **Privacy Mask**.
2. Select the camera for which you want to configure masking.
3. In the preview window, define a masking area by selecting two opposite corners to form a rectangular region (Region 1).
4. Repeat the same operation to configure Regions 2–4.
5. Enable the **Enable** option.
6. Click **Apply**.

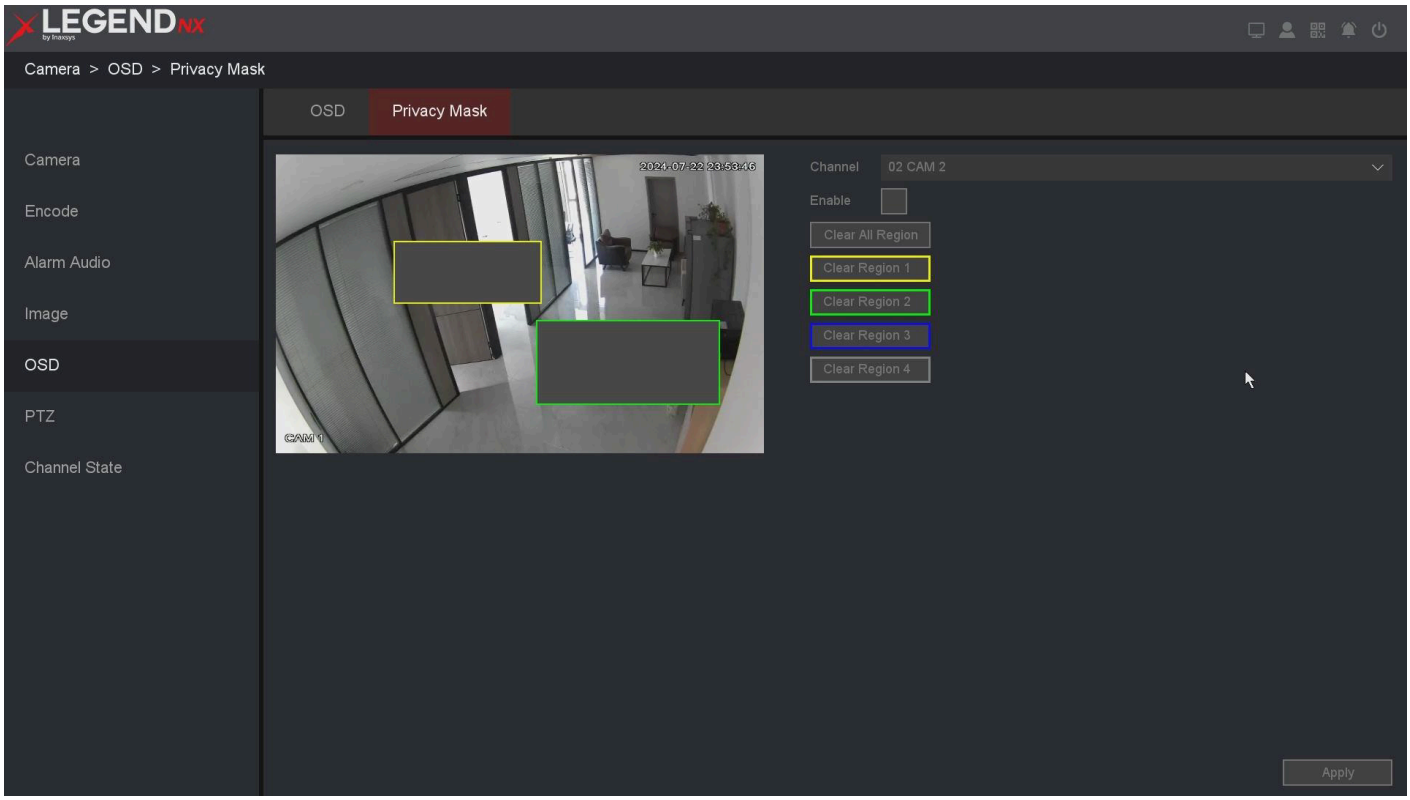


Figure 10-48 Cover

Note

Up to four privacy mask areas can be configured. The size of each area can be adjusted.

10.3.5 PTZ

This section explains how to configure the actions that the PTZ camera will perform when a corresponding alarm is triggered.

Before You Start

Ensure that presets, patrols, and patterns are supported by the PTZ protocol.

Steps:

1. Go to **Main Menu** → **Camera** → **PTZ**.
2. Select the channel to configure.
3. Configure the parameters as required.

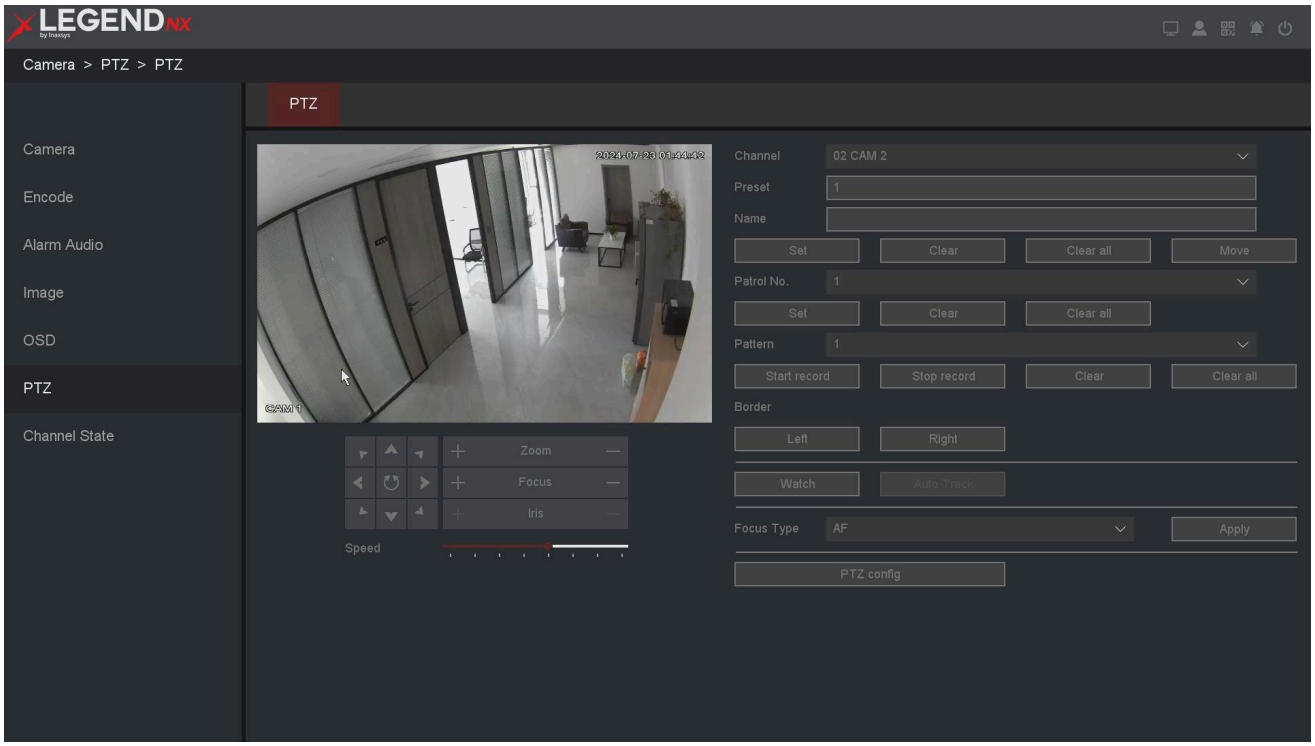


Figure 10-49 PTZ

Preset

This function allows the camera to move to a predefined position (for example, a specific area or object) when an event occurs.
Up to 255 preset points can be configured.

Patrol

Patrols allow the PTZ camera to automatically move between multiple preset points, remaining at each position for a specified duration before moving to the next.

The preset points serve as key positions in the patrol sequence. You can configure up to 4 patrol routes. Each route includes preset points, dwell time at each preset, and movement speed.

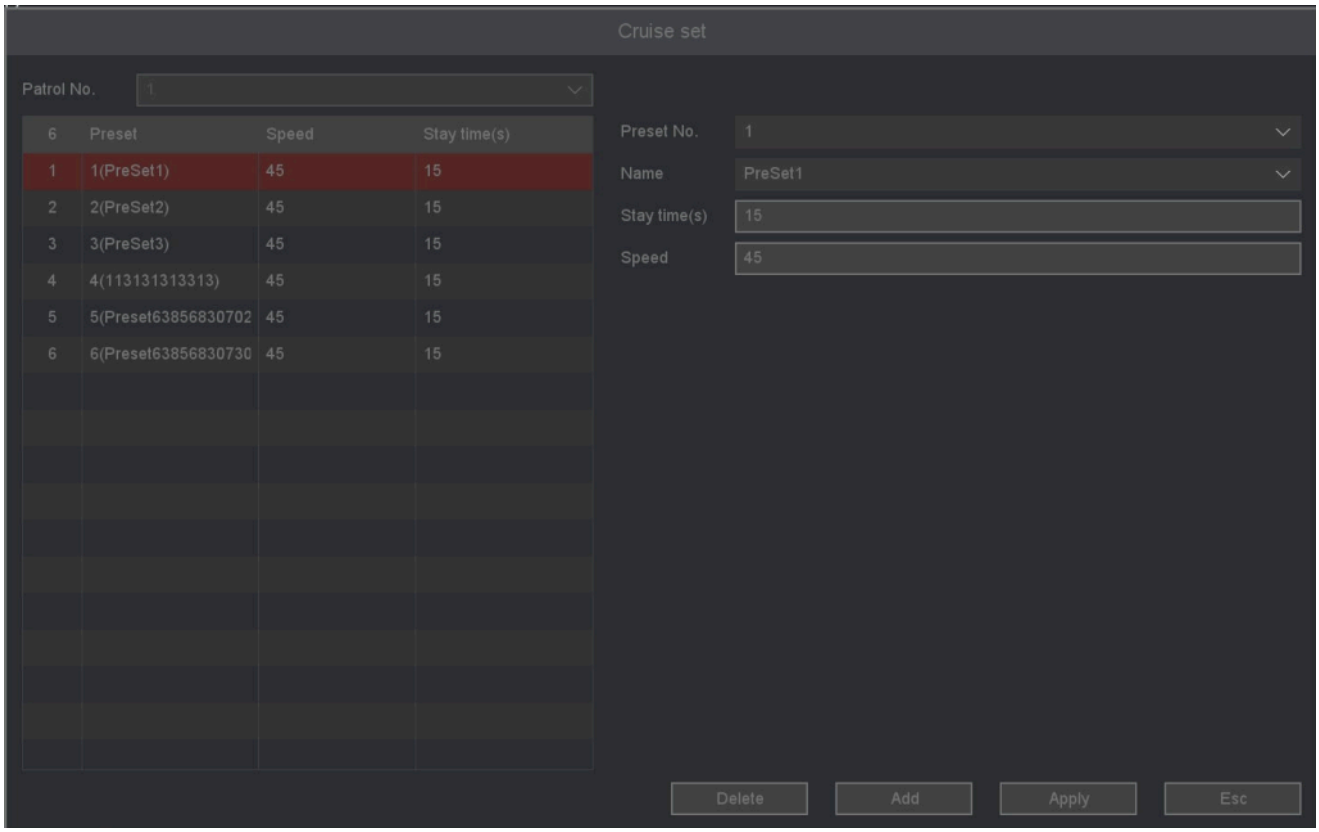


Figure 10-50 Patrol

Pattern

Patterns can be created by recording the movement of the PTZ camera. Once recorded, the pattern can be called to make the PTZ follow the predefined movement path.

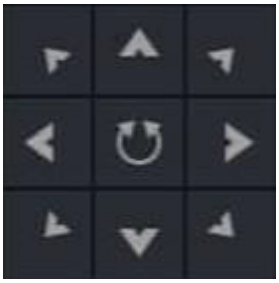
Border

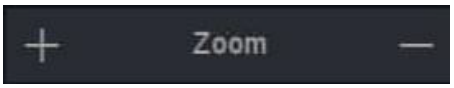
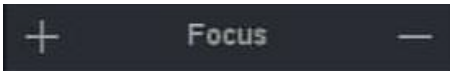
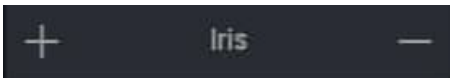
Defines the movement boundaries, including left and right limits.

Speed

Sets the movement speed of the PTZ camera.

Table 10-2 PTZ Function Description

Items	Function Description
	Controls PTZ movement direction and enables automatic cycling

	Zoom in (+) / Zoom out (−)
	Focus in (+) / Focus out (−)
	Iris open (+) / Iris close (−)
	Adjusts the PTZ movement speed

10.4 Event Configuration

10.4.1 Normal Event

Motion Detection

Motion detection enables the video recorder to detect moving objects within the monitored area and trigger alarms. For more information, refer to **6.3.3 Motion Detection**.

Video Tampering

Triggers an alarm when the camera lens is covered and executes the configured alarm response actions.

Before You Start

Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu** → **Event** → **Detect** → **Video Tampering**.

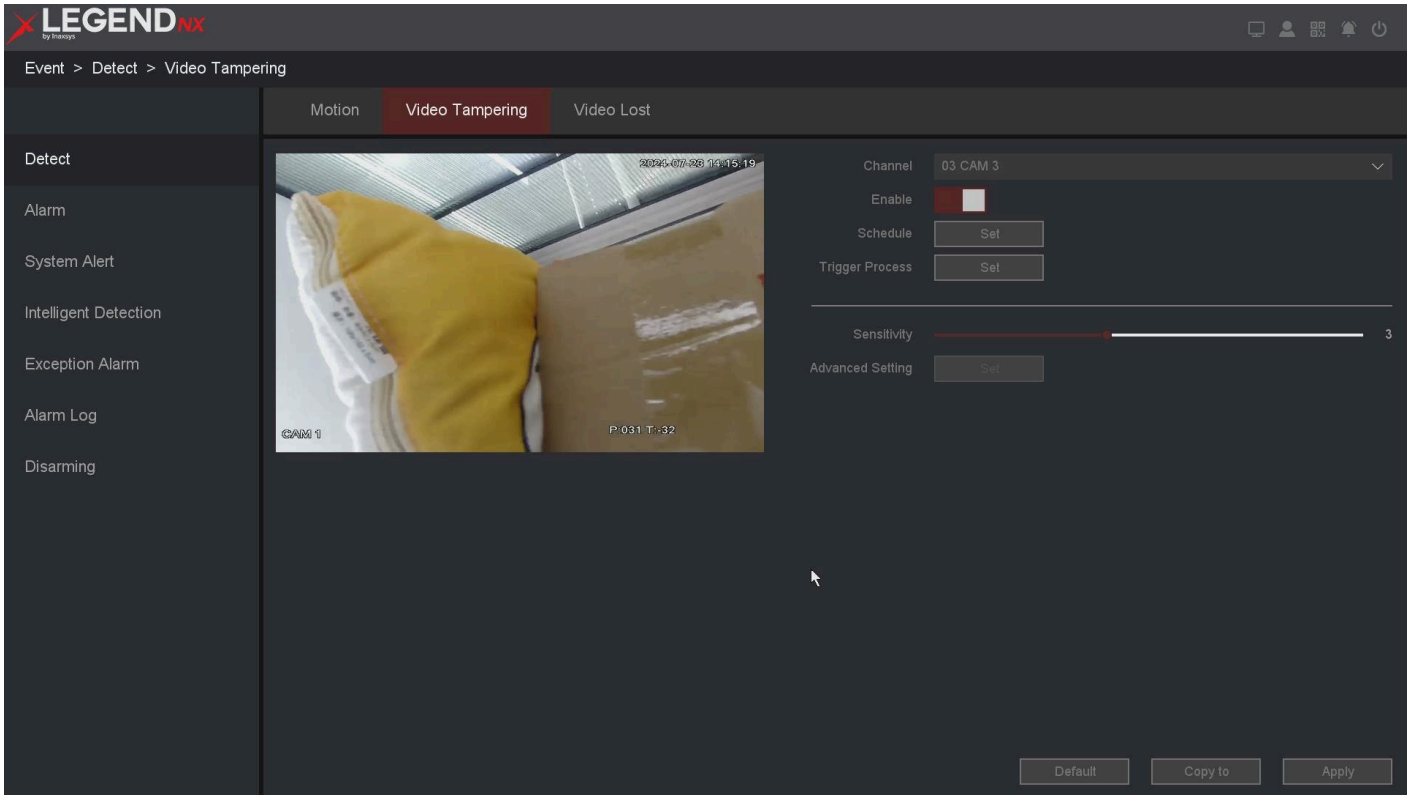


Figure 10-51 Masking

2. Set the **Channel**.
3. Enable the **Enable** option.
4. Adjust **Sensitivity** as required. A higher value makes video tampering detection more sensitive.
5. Configure the arming schedule. For details, refer to **6.3.4 Configure Arming Schedule**.
6. Configure the trigger actions. For details, refer to **6.3.5 Configure Alarm Trigger Process**.
7. Click **Apply**.

Video Loss

Detects video signal loss from a camera and triggers alarm response actions.

Before You Start

Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu → Event → Detect → Video Lost**.

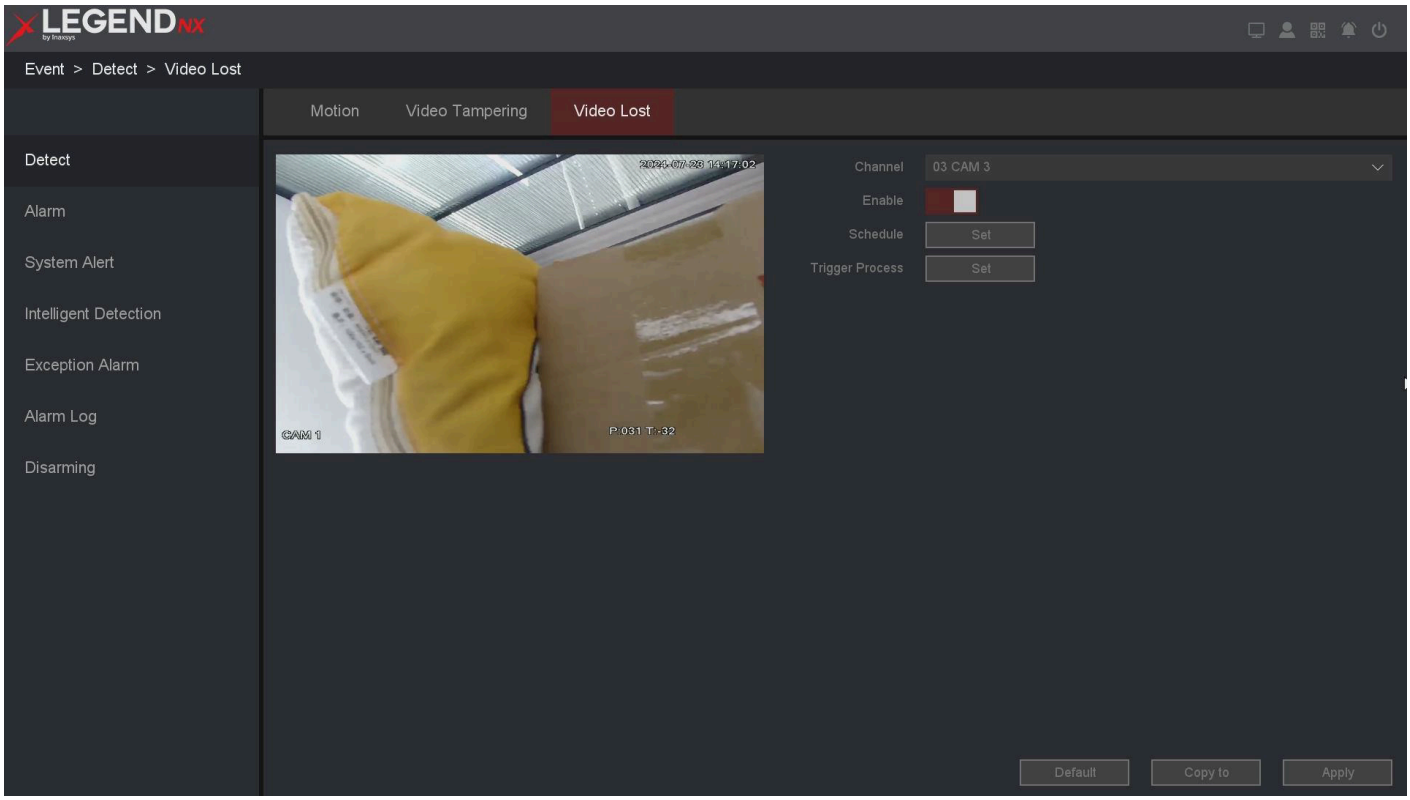


Figure 10-52 Video Lost

2. Set the **Channel**.
3. Enable the **Enable** option.
4. Configure the arming **Schedule**. For details, refer to **6.3.4 Configure Arming Schedule**.
5. Configure the **Trigger Process**. For details, refer to **6.3.5 Configure Alarm Trigger Process**.
6. Click **Apply**.

10.4.2 Alarm Port

Alarm Input

Configure linkage actions for external sensor alarms.

Steps:

1. Go to **Main Menu → Event → Detect → Alarm**.

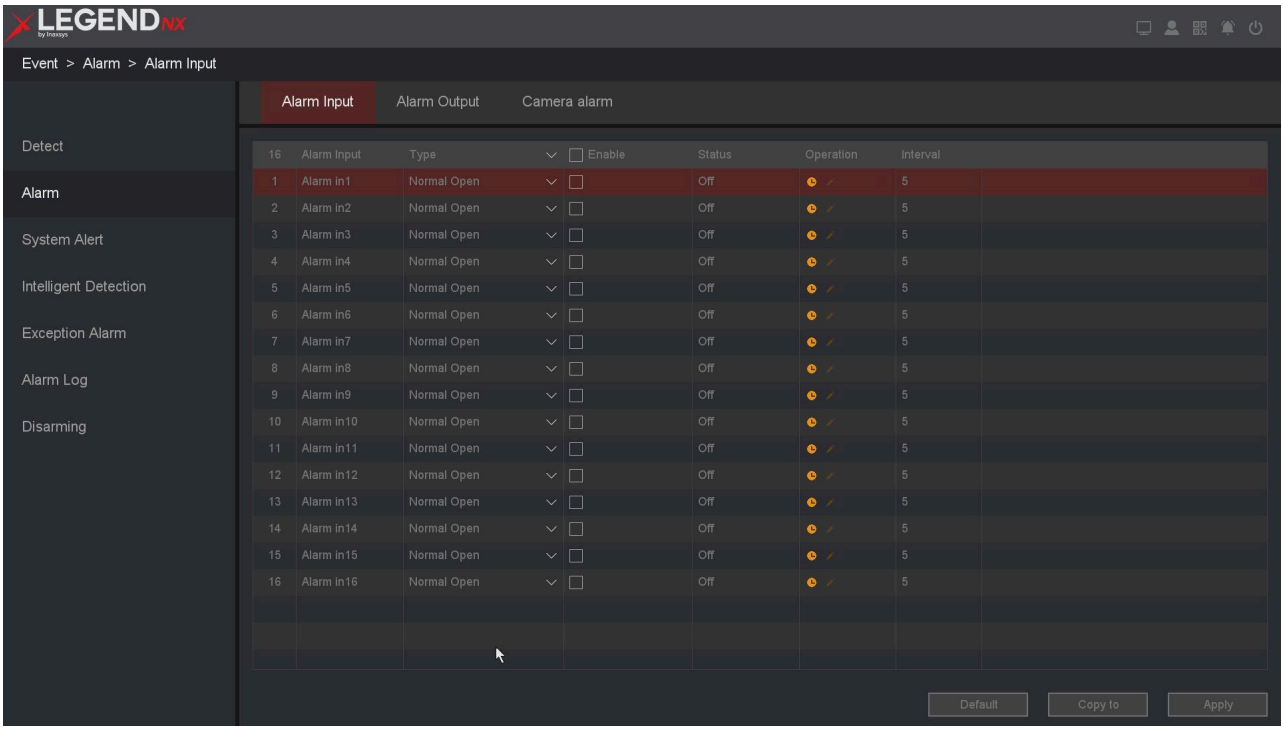


Figure 10-53 Alarm Input

Note

Local alarm input is triggered by external devices connected to the recorder's terminal block. It can detect changes in the monitored environment through sensors such as infrared or temperature sensors. When environmental changes occur, the sensor detects the change and updates its status.

2. Click the alarm input name to edit it as required.

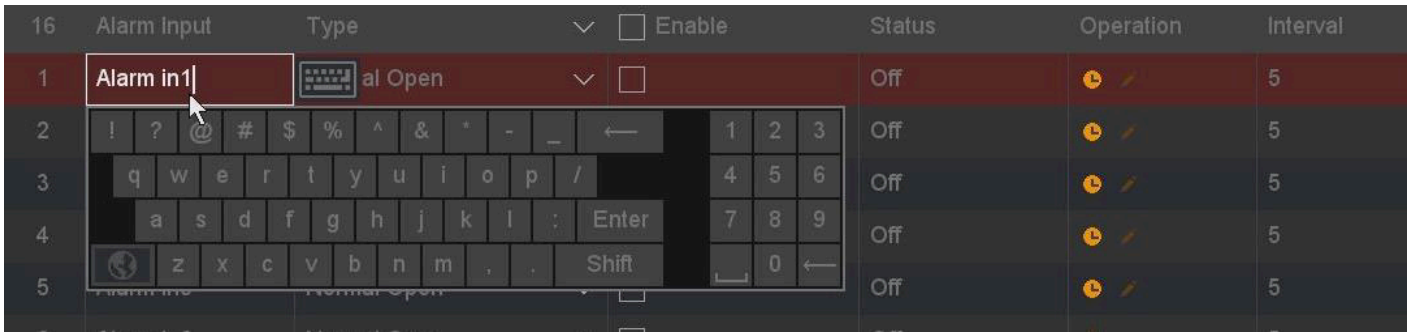


Figure 10-54 Edit Alarm Input

3. Set the alarm type to **Normally Open** or **Normally Closed**.
4. Select the **Enable** checkbox to activate the alarm input.
5. Configure the remaining parameters as required.

Note

If **Settings** is set to **Nonuse**, the alarm input will be disabled.

If **Settings** is set to **One-Key Disarming**, the selected linkage actions for the alarm input will be disabled.

6. Click the clock icon to configure the arming **Schedule**. For details, refer to **6.3.4 Configure Arming Schedule**.
7. Click the edit icon to configure the **Trigger Process**. For details, refer to **6.3.5 Configure Alarm Trigger Process**.
8. Click **Apply**.

Type of Alarm Ouput

Select **Normally Open** or **Normally Closed**. This defines how the system interprets the external sensor status.
The sensor has two states: Open and Closed. An alarm is triggered when the status changes (from Open to Closed or from Closed to Open).

Enable
Enables or disables the alarm input.

Status
Displays the current trigger status of the alarm input port.

Interval
Sets the interval between alarm triggers.

Alarm Output
Triggers an alarm output when an alarm event occurs.

Steps:

1. Go to **Main Menu** → **Event** → **Alarm** → **Alarm Output**.

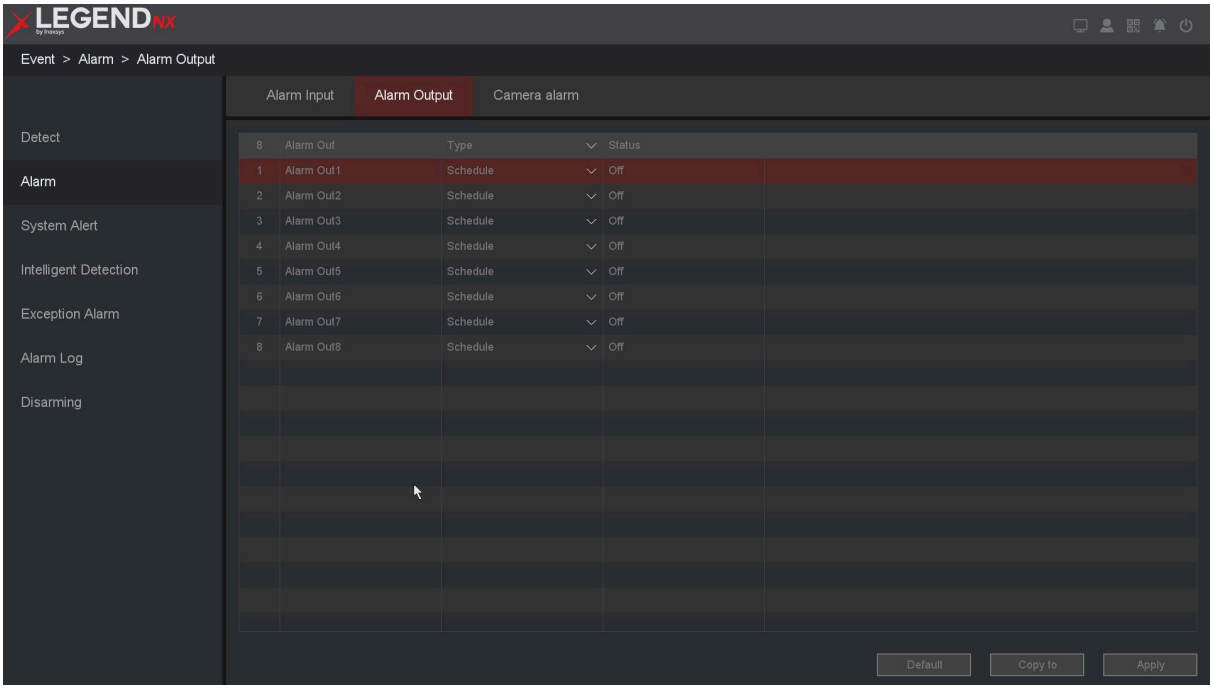


Figure 10-55 Alarm Output

2. Click the alarm output name to edit it as required.
3. Set the alarm type to **Schedule**, **Manual**, or **Stop**.
4. Configure the remaining parameters as required.
5. Click **Apply**.

Type of Camera Alarm

Three types are available: **Schedule**, **Manual**, and **Stop**.

- **Schedule**: The alarm output device is activated automatically when the NVR detects an alarm, based on the configured schedule.
- **Manual**: The alarm output device is activated manually after selecting this option and clicking **Apply**.
- **Stop**: The alarm output device is disabled and will not respond to alarms.

Status
Displays the current trigger status of the alarm output port.

Network Alarm
This function receives alarm signals from the IP Camera's alarm input port and triggers corresponding actions on the NVR.

Before You Start
Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu → Event → Alarm → Camera Alarm**.

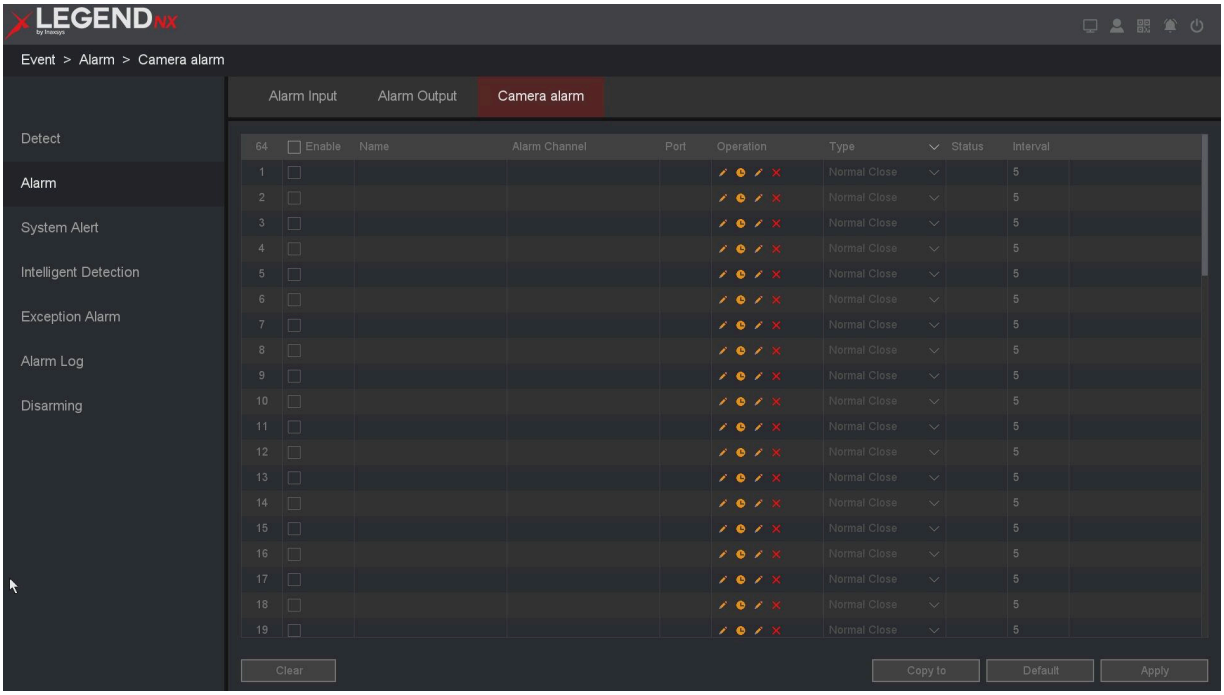


Figure 10-56 Network Alarm

2. Click the edit icon to configure the **Name**, **Alarm Channel**, and **Port**.

3. Click the clock icon  to configure the arming **Schedule**. For details, refer to **6.3.4 Configure Arming Schedule**.
4. Click the edit icon  to configure the **Trigger Process**. For details, refer to **6.3.5 Configure Alarm Trigger Process**.
5. Configure the remaining parameters as required.
6. Select the **Enable** checkbox to activate the function.
7. Click **Apply**.

Enable
Enables or disables the alarm input for the IP channel.

Name
Specifies the name of the alarm input device.

Alarm Channels
Displays which IP channel the alarm input belongs to.

Port
Displays the alarm input port of the IP channel.

Operations
Includes the following actions: **Edit**, **Schedule**, **Trigger Process**, and **Delete**.

Type
Select **Normally Open** or **Normally Closed**. The system supports external sensors with two states: Open and Closed. An alarm is triggered when the state changes (Open → Closed or Closed → Open).

Status
Displays the trigger status of the alarm input port.

Interval
Sets the interval between alarm triggers.

10.4.3 Intelligent Detection

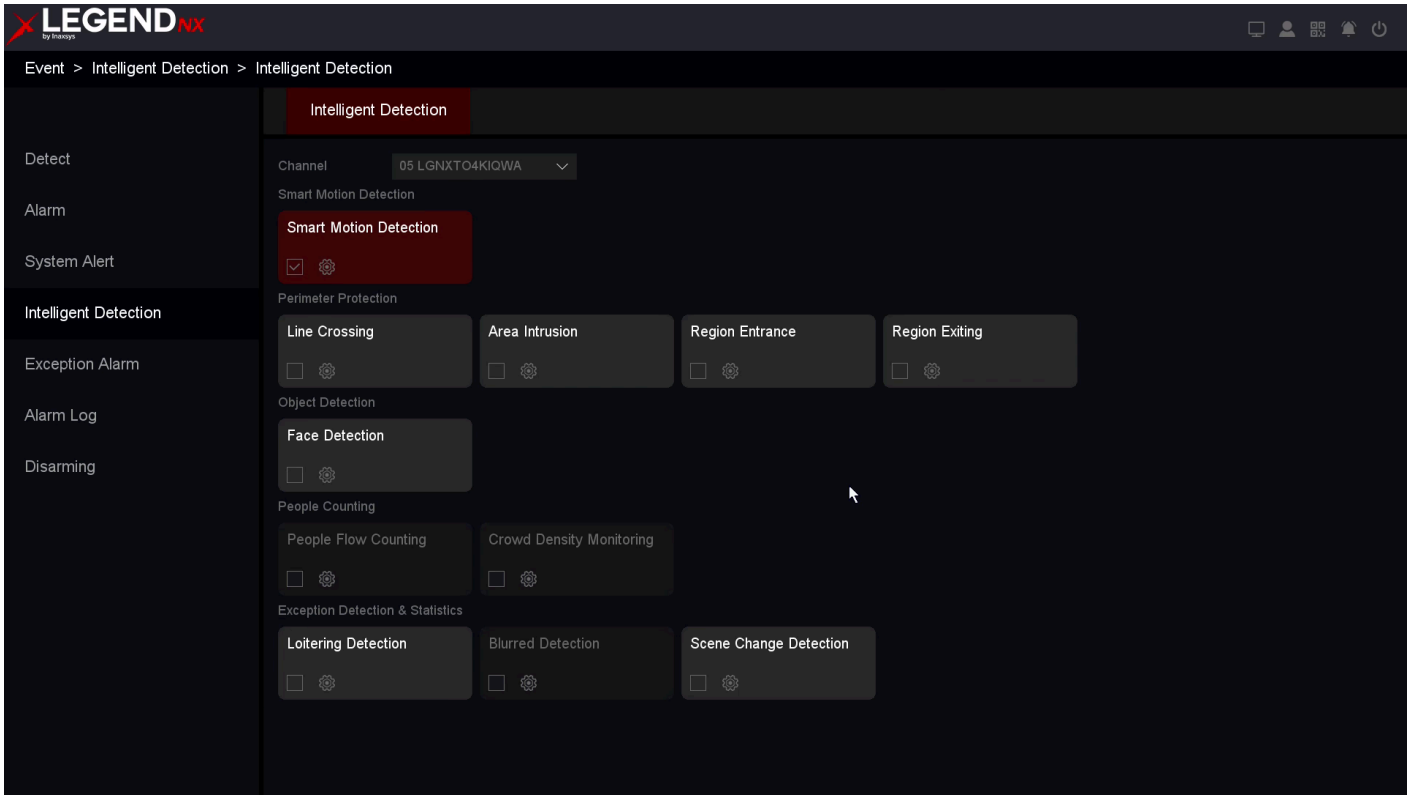


Figure 10-57 Intelligent Detection

Smart Motion Detection

Smart Motion Detection is an advanced motion detection function that supports filtering for humans and vehicles. It effectively reduces false alarms caused by lighting changes, moving shadows, small animals, and similar disturbances.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Smart Motion Detection**.
2. Select the **Smart Motion Detection** checkbox.
3. Click the settings icon to open the configuration window.

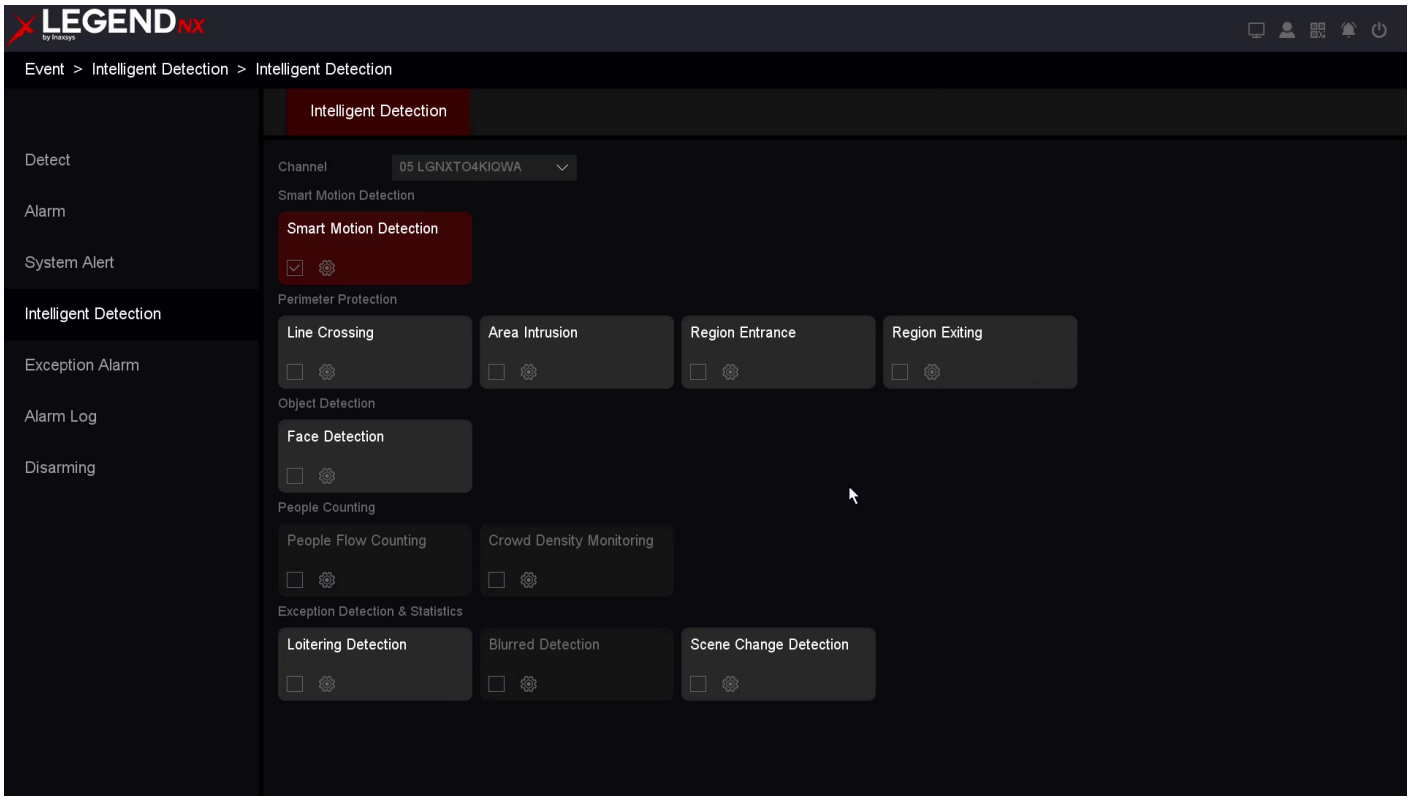


Figure 10-58 Smart Motion Detection

4. Click **Plot Area**, then drag the cursor in the preview window to define the detection area (selected areas are highlighted in red).

Max Size

If the detected object exceeds the defined maximum size, no alarm will be triggered.

Min Size

If the detected object is smaller than the defined minimum size, no alarm will be triggered.

Clear Area

Removes the selected detection area.

Clear All

Removes all defined detection areas.

5. Configure the arming **Schedule**. For details, refer to **6.3.3 Configure Arming Schedule**.
6. Set the **Interval**. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. For details, refer to **6.3.4 Configure Alarm Trigger Process**.
8. Enable the **Human / Vehicle / Bike** filters as needed. When enabled, alarms are triggered only for the selected target types.
9. Configure **Advanced Settings**. For details, refer to **6.3.5 Configure Advanced Setting**.
10. Set **Sensitivity** (1–100). This value represents the percentage of the target entering the detection area required to trigger an alarm.

- A value of 0 means the alarm is triggered only when the target fully enters the area.
- A value of 100 means the alarm is triggered as soon as the target enters the area.

11. Select **Target Validity**. The default is **Higher**. Higher values improve the accuracy of human/vehicle detection.
12. Click **Apply**.

Perimeter Protection

Line Crossing & Area Intrusion & Region Entrance & Region Exiting

These are the four most commonly used intelligent detection functions. When **Target Detection** is set to Human Shape Filter or Vehicle Shape Filter, alarms not triggered by human bodies or vehicles are filtered out. These functions are collectively referred to as **Perimeter Protection (PP)**.

Only certain camera models support these features. Refer to **6.3.3 Event** for details.

Object Detection

Face Detection

Face Detection is an intelligent event detection function that uploads an alarm message after detecting a human face.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Perimeter Protection → Face Detection**.
2. Select the **Face Detection** checkbox.
3. Click the settings icon to open the configuration window.

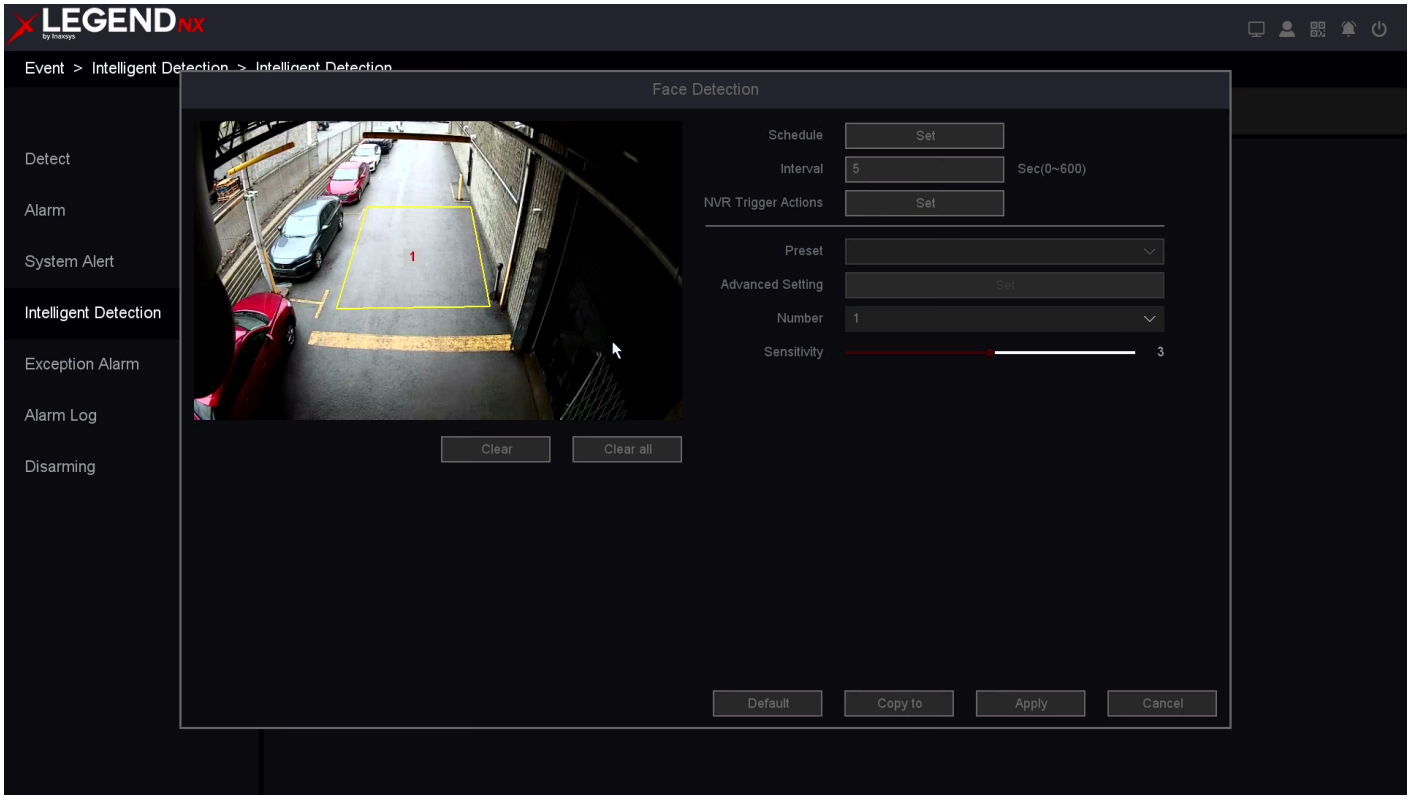


Figure 10-59 Set Disarming Time

4. Click four points with the left mouse button in the video window to draw the detection area.

Clear
Removes the selected area.

Clear All
Removes all defined areas.

5. Configure the arming **Schedule**. Refer to **6.3.4 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
8. Configure **Advanced Settings**. Refer to **6.3.6 Configure Advanced Setting** for details.
9. Set **Sensitivity** (1–5). This value represents the percentage of the target entering the detection area required to trigger an alarm. A higher sensitivity results in a higher face detection rate.
10. Click **Apply**.

Exception Detection & Statistics

Loitering Detection
Loitering Detection can identify a moving person who remains in a predefined area for longer than a specified duration or exhibits an abnormal movement trajectory. When an alarm is triggered, predefined actions can be executed.

Before You Start
Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Exception Detection → Loitering Detection**.
2. Select the **Loitering Detection** checkbox.
3. Click the settings icon  to open the configuration window.

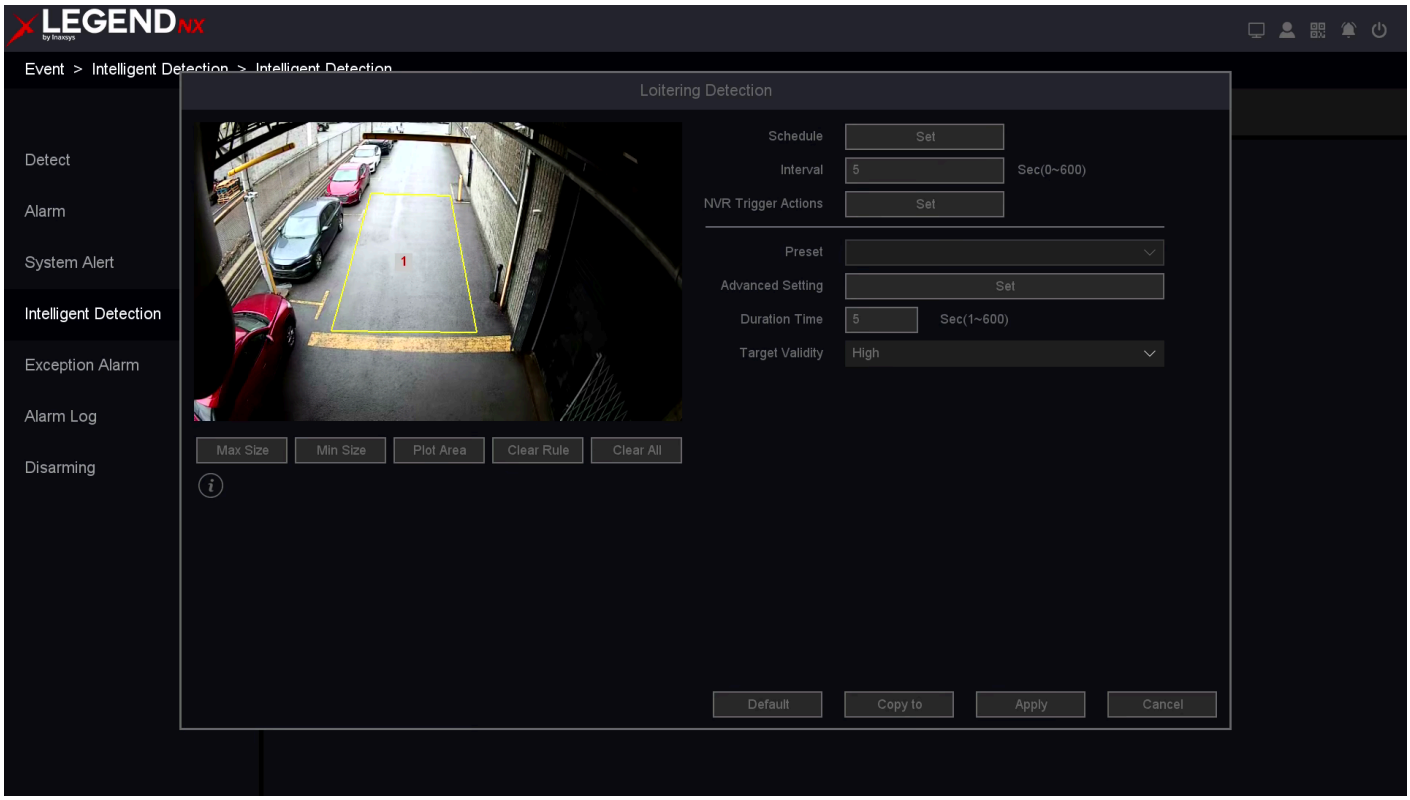


Figure 10-60 Loitering Detection

4. Click **Plot Area**, then use the left mouse button to click four points and draw the detection area directly in the video window.

Clear

Removes the selected area.

Clear All

Removes all defined areas.

Max Size

If the size of an object in the scene exceeds the configured maximum size, the alarm will not be triggered.

Min Size

If the size of an object in the scene is smaller than the configured minimum size, the alarm will not be triggered.

5. Configure the arming **Schedule**. Refer to **6.3.4 Configure Arming Schedule** for details.
6. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
7. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
8. Configure **Advanced Settings**. Refer to **6.3.6 Configure Advanced Setting** for details.
9. **Duration Threshold**: The loitering alarm is triggered when a target enters the armed area and remains there longer than the configured duration (1–600 seconds).
10. Select **Target Validity** for the event. The default is Higher. A higher level increases the likelihood of detecting human/vehicle targets.
11. Click **Apply**.

Blurred Detection

Before You Start

Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Exception Detection → Blurred Detection**.
2. Select the **Blurred Detection** checkbox.
3. Click the settings icon to open the configuration window.

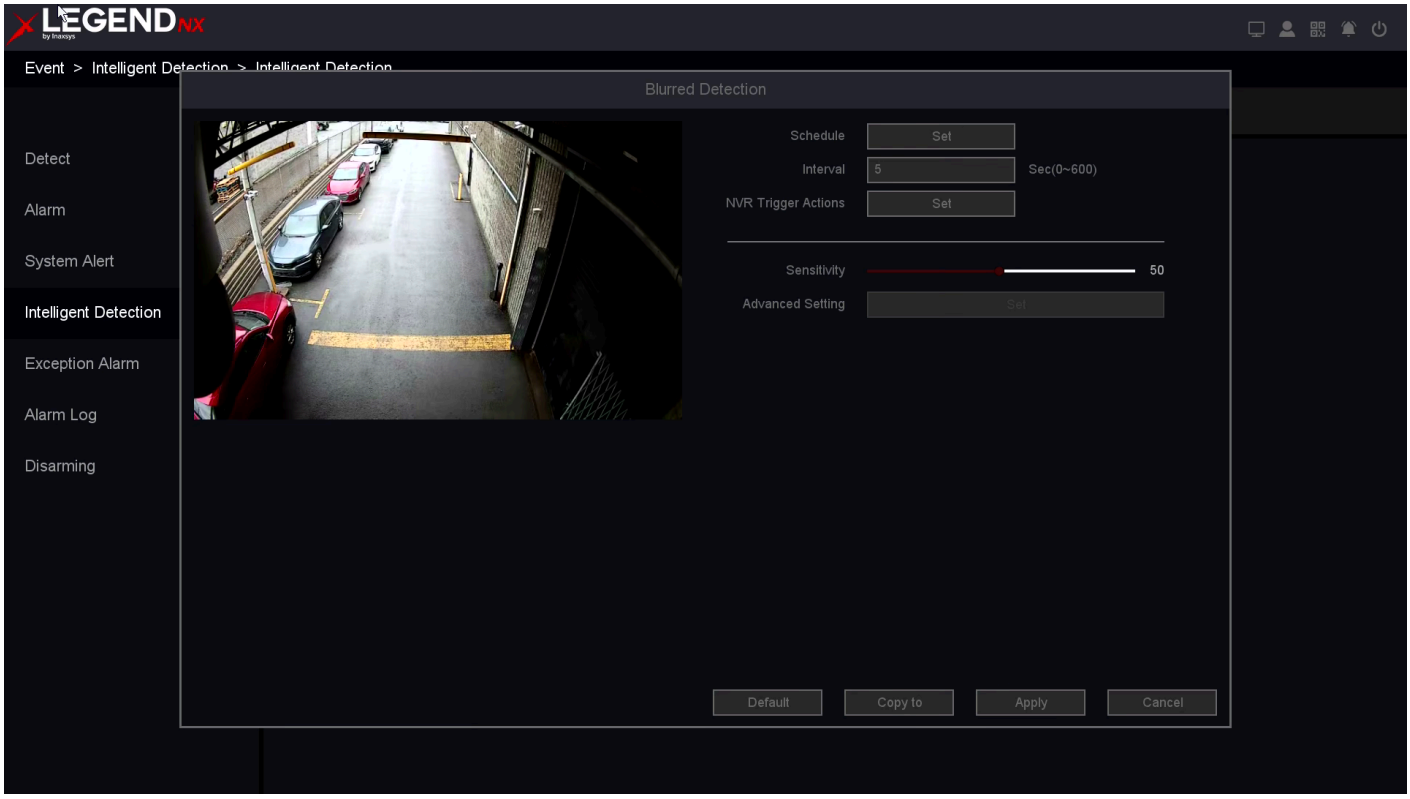


Figure 10-61 Blurred Detection

4. Configure the arming **Schedule**. Refer to **6.3.4 Configure Arming Schedule** for details.
5. Set the **Interval** for the event. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
6. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
7. **Sensitivity** controls the threshold for detecting image blur. A higher sensitivity triggers alarms even for slight blurring, while a lower sensitivity triggers alarms only when the image is significantly blurred.
8. Configure **Advanced Settings**. Refer to **6.3.6 Configure Advanced Setting** for details.
9. Click **Apply**.

Scene Change Detection

When the scene captured by the camera changes due to human activity, environmental factors, or other causes, the camera detects the scene change event and triggers the corresponding alarm linkage actions.

Steps:

1. Go to **Main Menu → Event → Intelligent Detection → Exception Detection → Scene Change Detection**.
2. Select the **Scene Change Detection** checkbox.
3. Click the settings icon to open the configuration window.

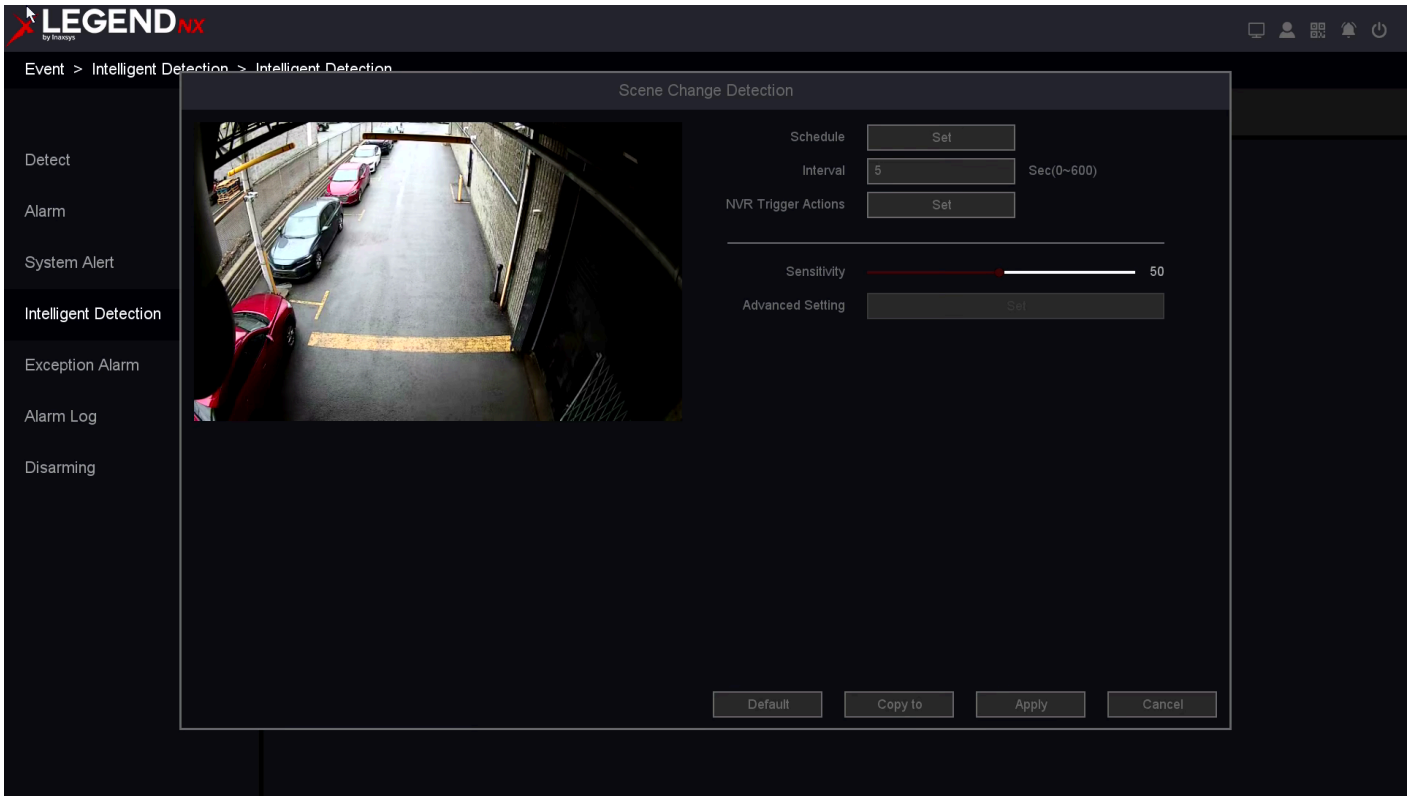


Figure 10-62 Scene Change Detection

4. Configure the arming **Schedule**. Refer to **6.3.4 Configure Arming Schedule** for details.
5. Set the alarm **Interval**. This defines the minimum time between two consecutive alarms. Increase the value to reduce frequent alarms, or decrease it to avoid missing events.
6. Configure the **Trigger Process**. Refer to **6.3.5 Configure Alarm Trigger Process** for details.
7. Adjust the **Sensitivity** (1–100). A higher sensitivity triggers alarms for minor changes in the image, while a lower sensitivity triggers alarms only for significant changes.
8. Configure **Advanced Settings**. Refer to **6.3.6 Configure Advanced Setting** for details.
9. Click **Apply**.

10.4.4 System Alert

Exception settings define how the system handles various abnormal conditions, including no writable disk, disk error, insufficient disk space, network disconnection, and IP conflict.

Steps:

1. Go to **Main Menu → Event → System Alert → System Alert**.

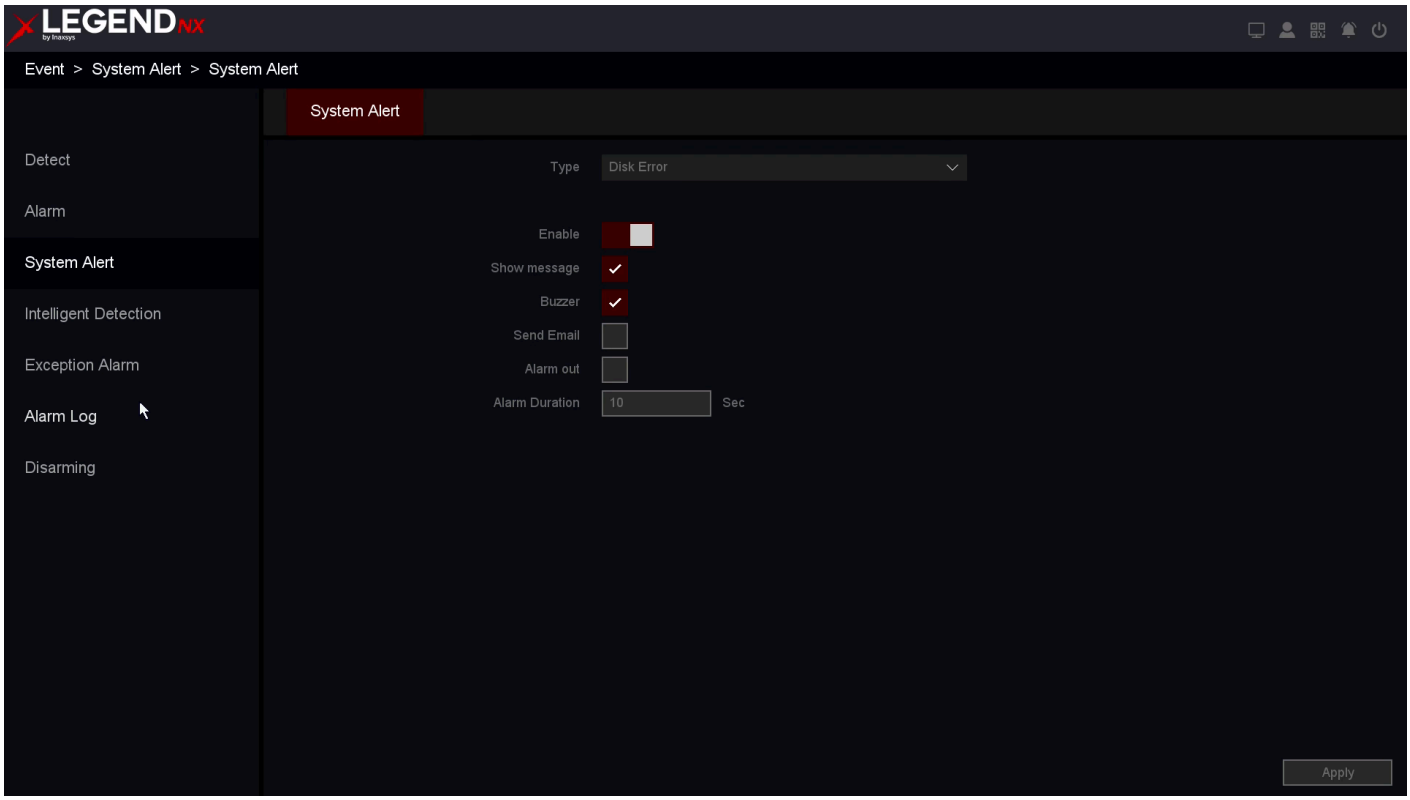


Figure 10-63 System Alert

2. Select the **Exception Type**.
3. Enable the function by turning on **Enable**.
4. Configure the other parameters as required. When the configured event occurs, notifications will be displayed in the **Alarm Status**.
5. Click **Apply**.

No Writable Disk

If all HDDs are set to read-only, this exception will be triggered. The system supports the following notification methods: **Show Message**, **Buzzer**, **Send Email**, and **Alarm Out**.

Disk Error

If a write error occurs on the HDD or the disk is not formatted, this exception will be triggered. The system supports the following notification methods: **Show Message** and **Buzzer**.

Disk No Space

You can configure a minimum remaining disk space threshold. When the available space falls below this value, the exception is triggered. The system supports the following notification methods: **Show Message**, **Buzzer**, **Send Email**, and **Alarm Out**.

Network Disconnection

If the network connection is lost, this exception will be triggered. The system supports the following notification methods: **Show Message**, **Buzzer**, and **Alarm Out**.

IP Conflict

If an IP address conflict occurs with another device on the same network, this exception will be triggered. The system supports the following notification methods: **Show Message**, **Buzzer**, and **Alarm Out**.

10.4.5 RAID

When RAID is enabled on the device, a Redundant Array of Independent Disks (RAID) can be implemented.

Warning

- The array function has high requirements for hard disks. To ensure long-term stable and reliable operation, it is recommended to use enterprise-grade hard drives for array creation and related configurations. The manufacturer is not responsible for data loss or damage caused by using surveillance-grade or desktop-grade hard drives.
- It is recommended to use HDDs of the same model and capacity.
- The capacity of a single disk must not be less than 4 TB.

Enable RAID

The NVR must have RAID enabled before configuring arrays (e.g., creating an array).

Before You Start

Ensure that the device supports the RAID function.

Steps:

1. Go to **Setting Menu** → **Storage** → **Advanced**.
2. Enable **Enable RAID**.

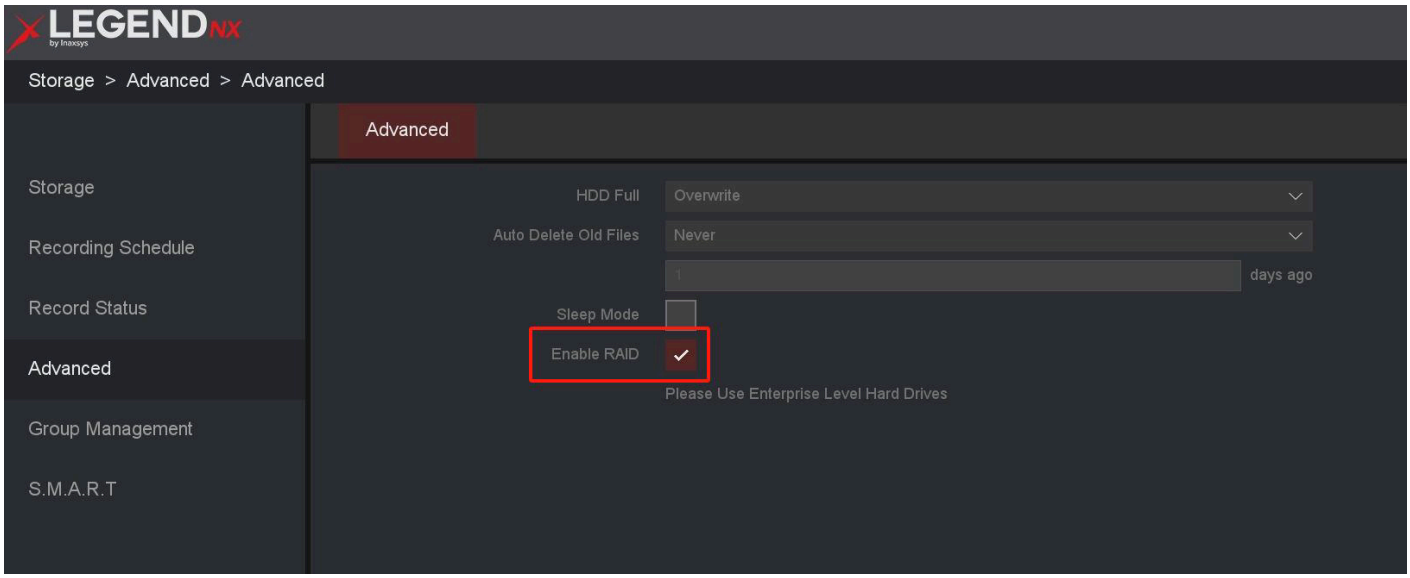


Figure 10-64 Advanced Setting

3. Click **OK** to continue.

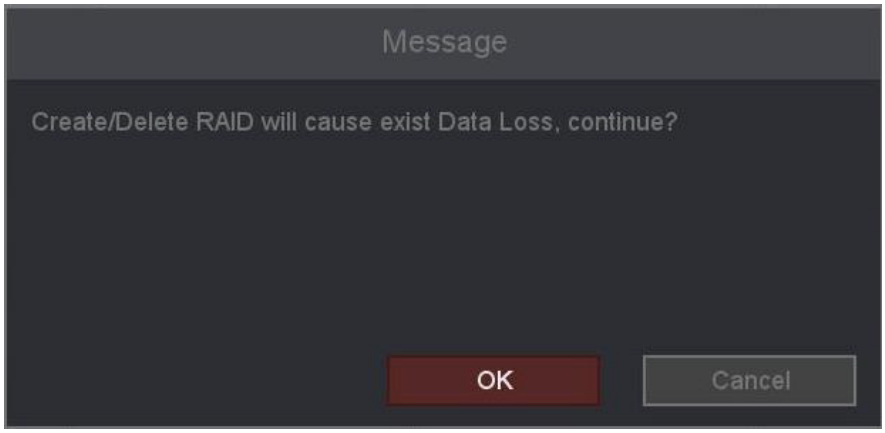


Figure 10-65 Continue

4. Click **OK** and wait for the restart to complete.

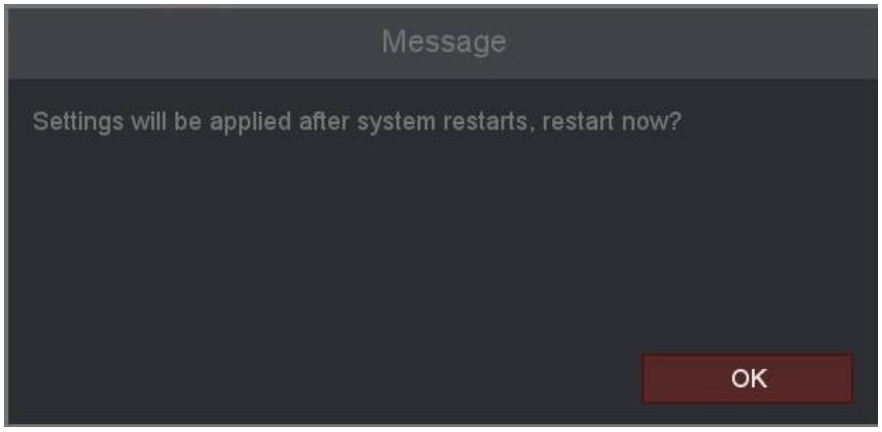


Figure 10-66 Restart

Note
The NVR does not record when RAID is enabled. Please refer to **Create RAID** to configure recording.

Create RAID

There are two ways to create RAID: **Quick Set** configuration and **Manual Create RAID**. Quick Set creates RAID5 by default, while Manual Create RAID supports RAID0, RAID1, RAID5, and RAID10.

Table 10-3 Description of Number of Hard Disk

Type	Number of Hard Disk
RAID0	≥2
RAID1	2
RAID5	≥3
RAID10	4 or 8

Quick Set RAID

With Quick Set, the device can quickly create disk arrays and virtual disks. The default array type is RAID5.

Before You Start

Ensure that the NVR has at least 3 physical disks installed.

Steps:

1. Go to **Setting Menu** → **Storage** → **RAID**.
2. Click **Quick Set**.
3. Click **OK**.

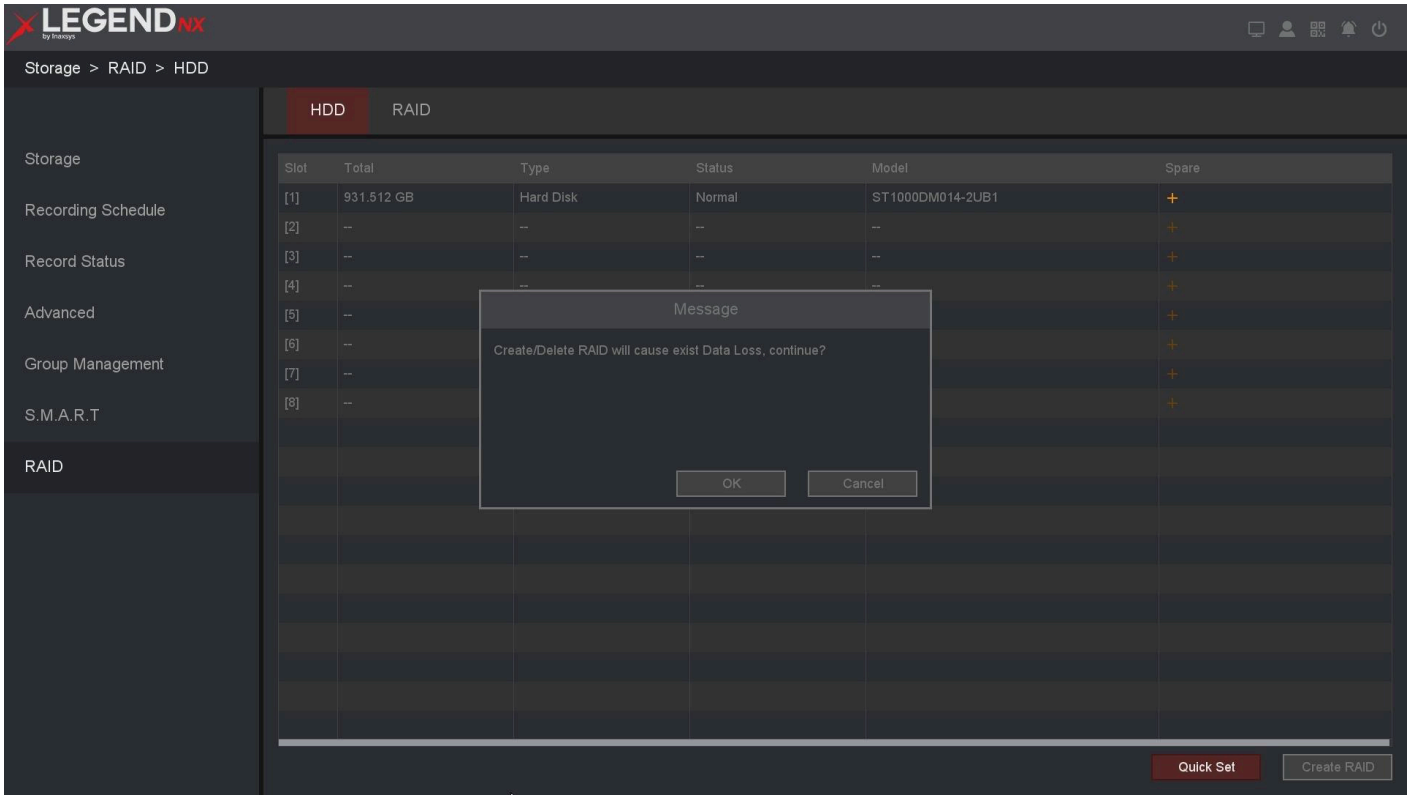


Figure 10-67 Quick Set

4. Go to **Setting Menu** → **Storage** → **RAID** → **RAID** to check the RAID status. When initialization is complete, the status is displayed as normal, and the disk is ready for normal reading and writing.

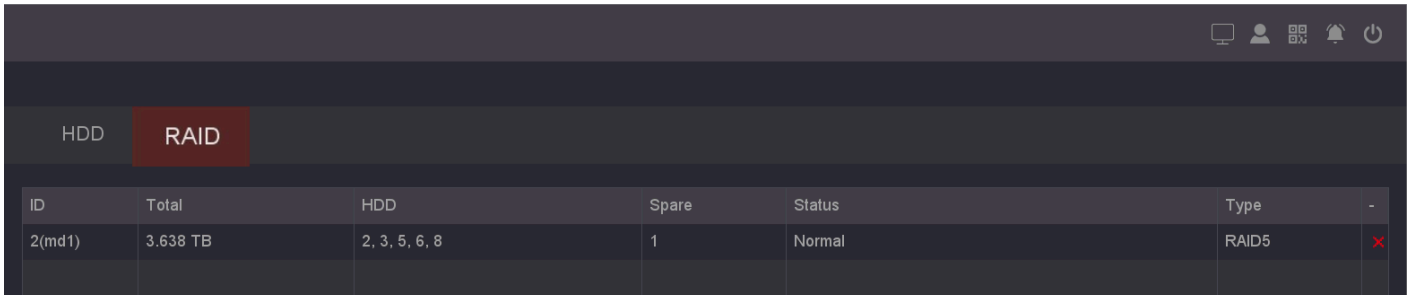


Figure 10-68 Check Status

5. Optional: click  to delete, or click **Quick Delete** to delete all RAID configurations.

6. Go to **Setting Menu** → **Storage** → **Base** to check the array (equivalent to a high-capacity logical disk) recording status information.

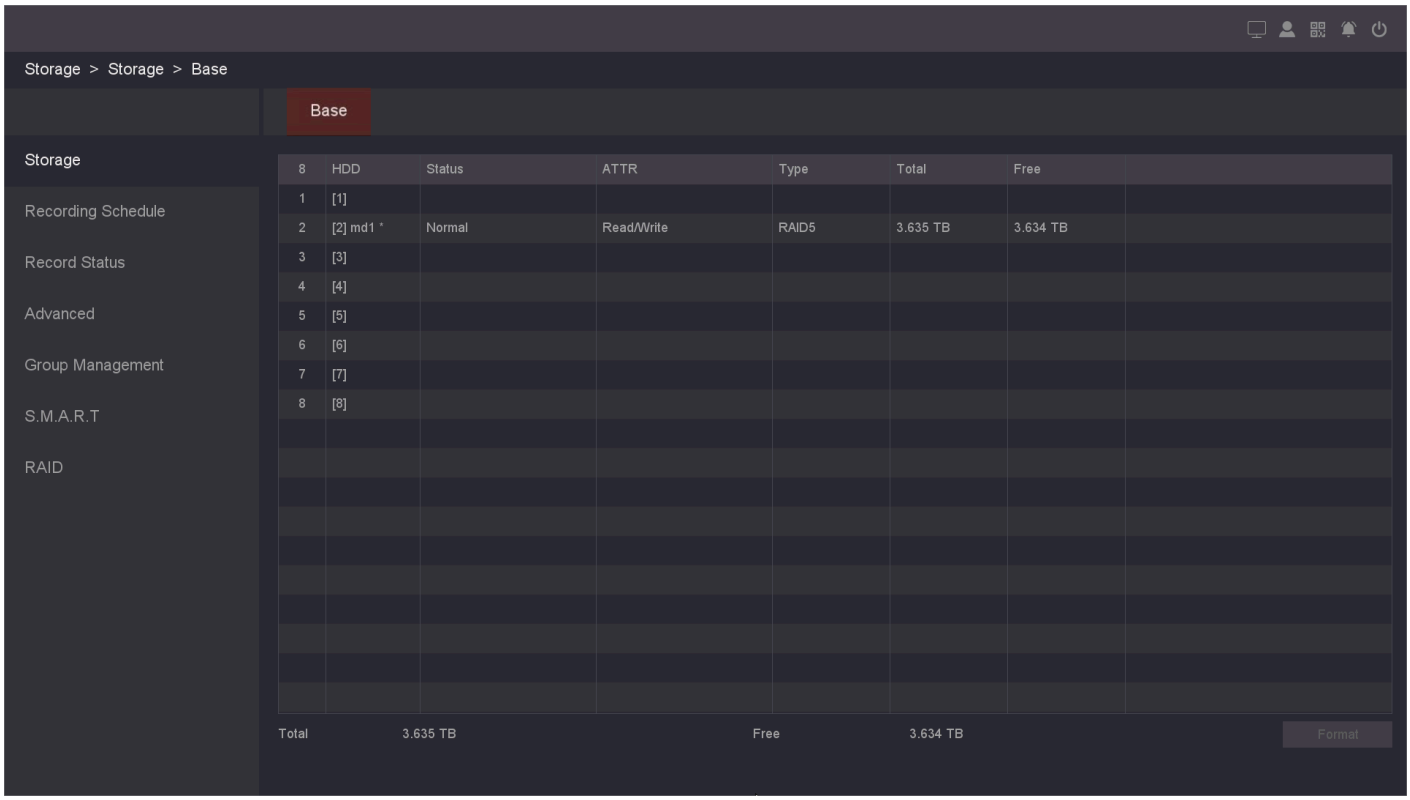


Figure 10-69 Check Recording Status Information

Manual RAID Creation

With manual configuration, users can create different types of RAID arrays based on the number of installed hard disks.

Before You Start

Ensure that the NVR has at least 2 physical disks installed.

Steps:

1. Go to **Setting Menu** → **Storage** → **RAID** → **HDD**.
2. Click **Create RAID**.

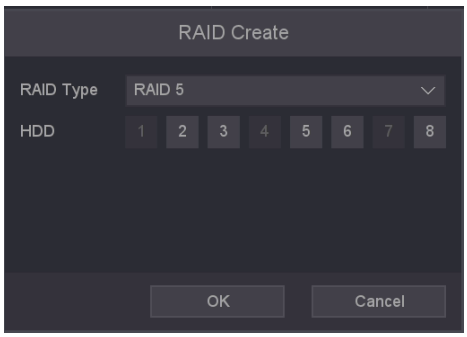


Figure 10-70 Manual RAID Creation

3. Select the physical disks to include in the array, then click **OK** to continue.

Note

If the array creation requirements are not met, a message “Available disks are not enough!” will be displayed.

4. Go to **Setting Menu** → **Storage** → **RAID** → **RAID** to check the RAID status. When initialization is complete, the status will be displayed as **Normal**, and the disk will be ready for standard read and write operations.

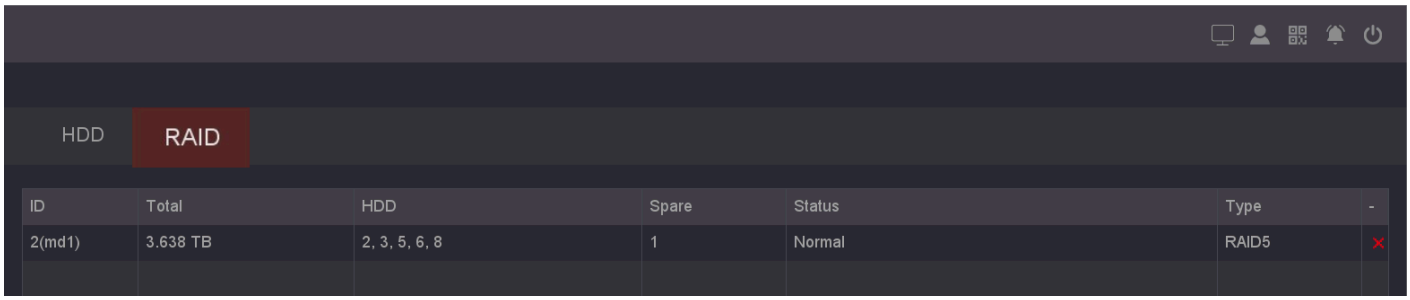


Figure 10-71 Check Status

5. Optional: click  to delete a RAID, or click **Quick Delete** to delete all RAID configurations.
6. Go to **Setting Menu** → **Storage** → **Base** to view the array (equivalent to a high-capacity logical disk) recording status information.

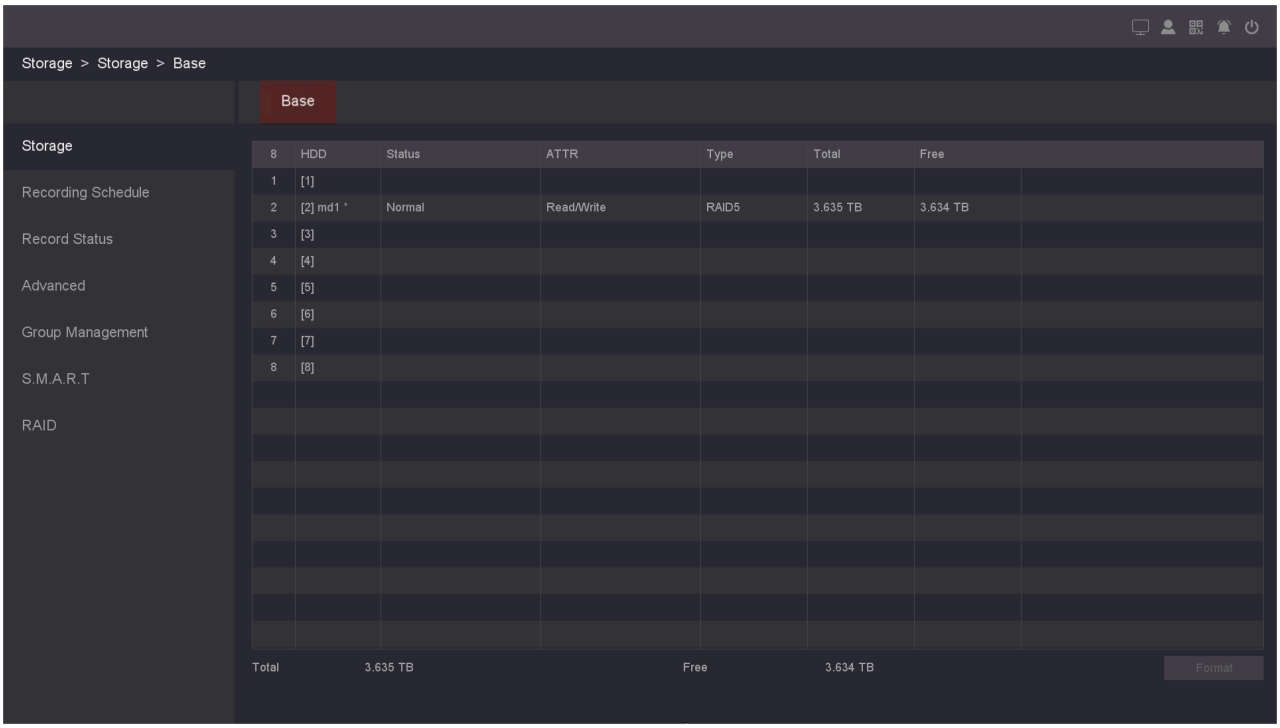


Figure 10-72 HDD Management

7. Optional: configure a hot spare disk.

(1) Go to **Setting Menu** → **Storage** → **RAID** → **HDD**.

(2) Select a disk with **Normal** status, then click **+**.

(3) Click **OK**.
(4) The status will be displayed as **Spare (Global)**.

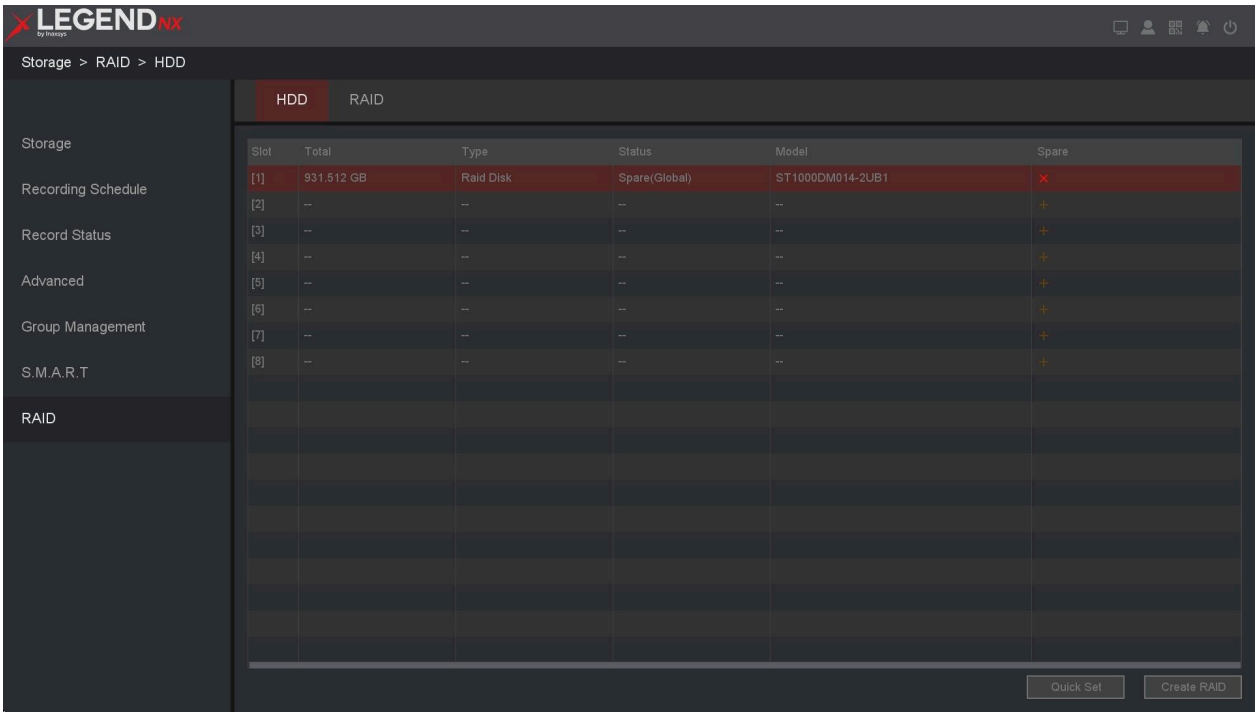


Figure 10-73 Set a Hot Spare Disk

10.4.6 Exception Alarm

An audio detection alarm is triggered when abnormal sound is detected around the camera. When an alarm is triggered, corresponding actions can be executed.

Before You Start
Ensure that your IP Camera supports this function.

Steps:

1. Go to **Main Menu → Event → Exception Alarm → Audio Detection**.

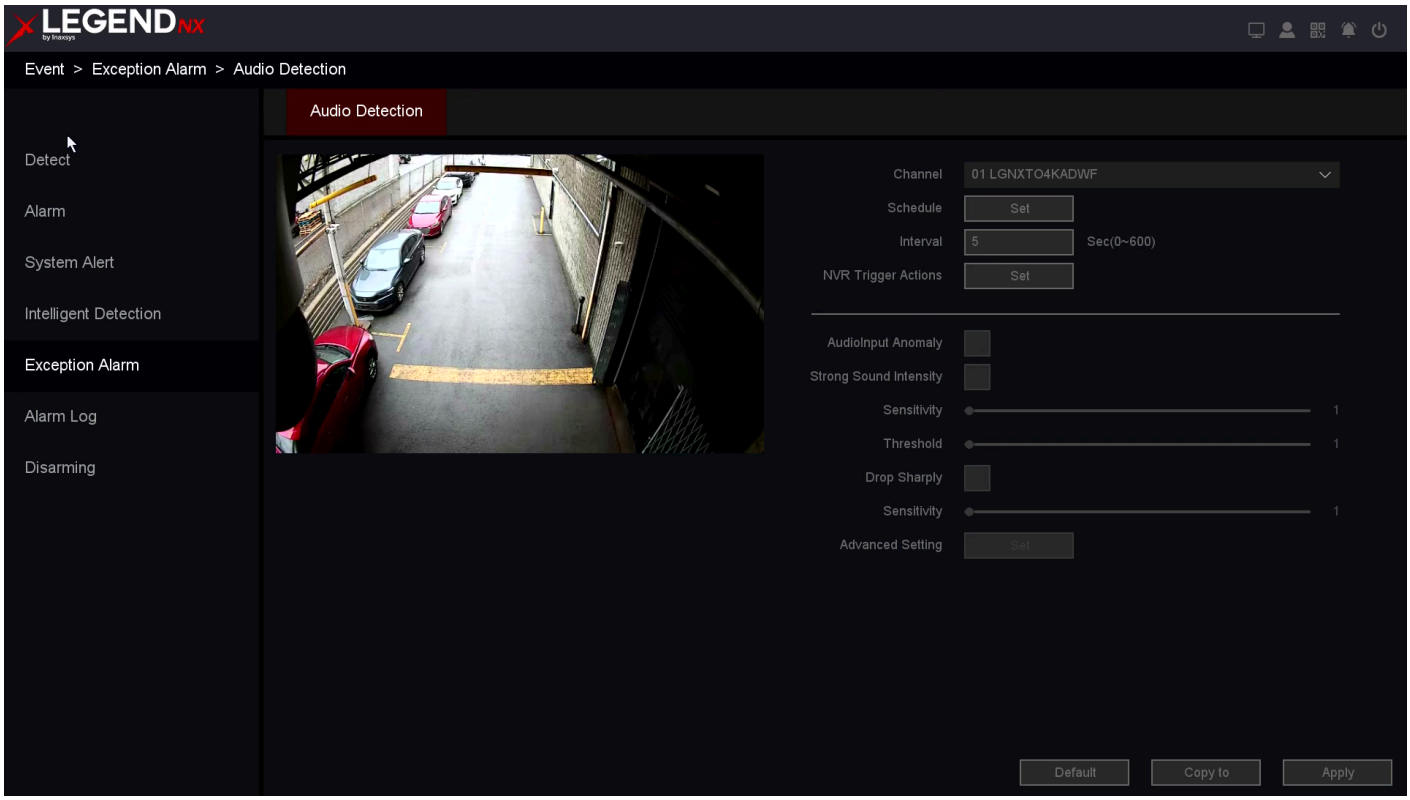


Figure 10-74 Audio Exception Detection

2. Select a camera.
3. Set the arming **Schedule**. Refer to **Configure Arming Schedule** for details.
4. Set the **Trigger Process**. Refer to **Configure Alarm Trigger Process** for details.
5. **Audio Input Anomaly:**
   When **Enable** is checked, the system monitors the current audio input. If the audio volume is lower than 20 dB, an audio input exception alarm will be triggered.
6. **Strong Sound Intensity:**
   After enabling this option, the system detects sudden increases in sound intensity.

Sensitivity:
Controls how easily a sudden increase in volume triggers an alarm. Higher sensitivity means even slight increases will trigger an alarm, while lower sensitivity requires a larger increase.

Sound Intensity Threshold:
An alarm is triggered when the increased volume exceeds the defined threshold.

7. **Drop Sharply:**
   After enabling this option, the system detects sudden decreases in sound intensity.

Sensitivity:
Controls how easily a sudden drop in volume triggers an alarm. Higher sensitivity means even slight decreases will trigger an alarm, while lower sensitivity requires a larger drop.

8. Set the alarm interval time. It is recommended to use the default value.
9. Click **Apply**.

10.4.7 Alarm Log

Alarm Information

All alarm events are displayed in this section. You can also use this interface to play back recorded video associated with each alarm.

1. Go to **Main Menu → Event → Alarm Log → Alarm Information**.

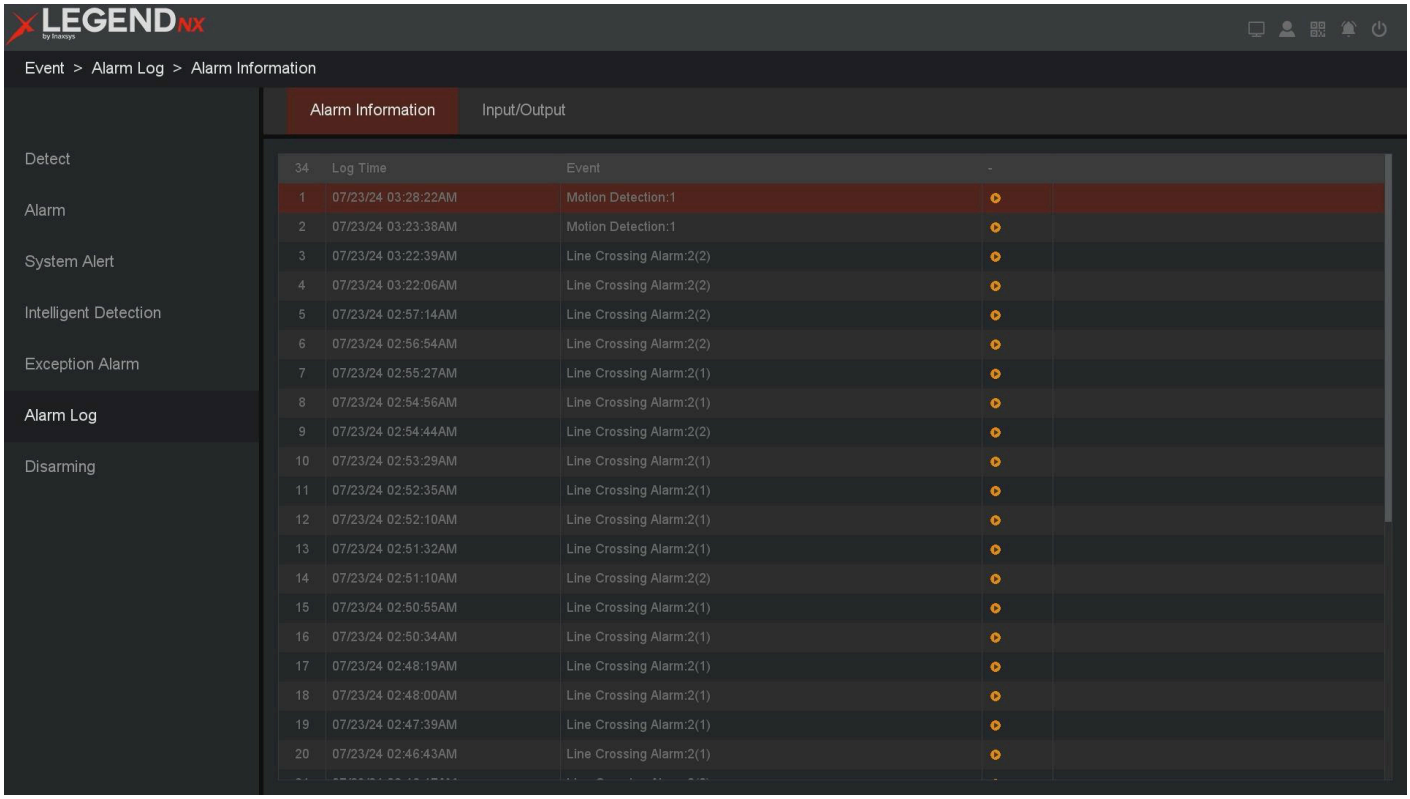


Figure 10-75 Alarm Information

2. You can click the **play** button to view the video corresponding to the alarm event.
3. The maximum number of log entries is 1000. This value may vary depending on the device model.

Input/Output

In this interface, you can view the status of the NVR's alarm input and output ports.

Steps:

1. Go to **Main Menu → Event → Alarm Status → Input/Output**.

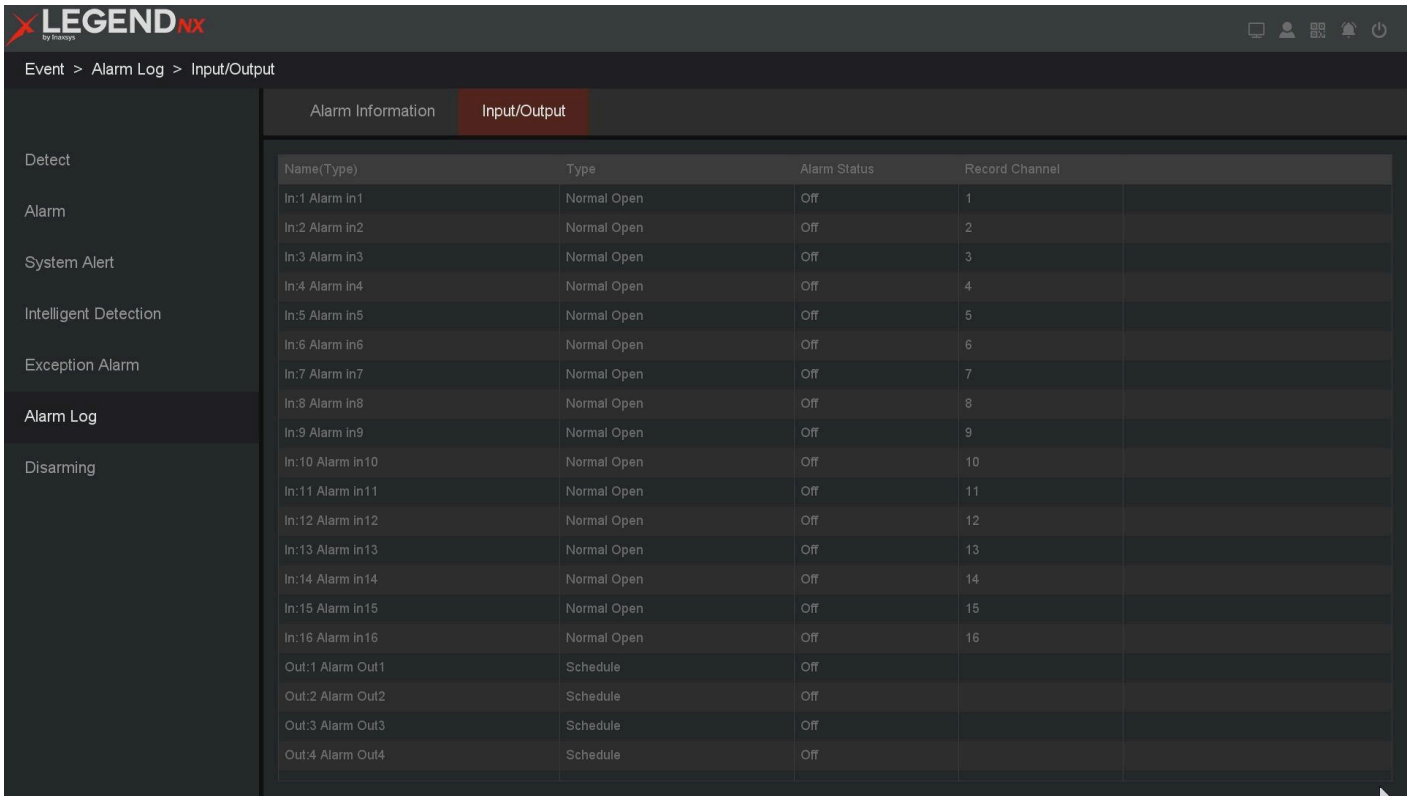


Figure 10-76 Input/Output

Name (Type)
Displays the alarm input/output type and the corresponding alarm name.

Type
For alarm inputs, the types include **Normal Open** and **Normal Close**.
For alarm outputs, the types include **Schedule**, **Manual**, and **Stop**.

Alarm Status
Displays the current alarm status, including **On** and **Off**.

Record Channel
Indicates the video recording channels linked to the alarm input.

10.5 Storage Management

10.5.1 Base - Storage Device

Initialize HDD
If you are using the HDD for the first time, initialize it after installation. Refer to **6.4.1 Storage** for details.

Add Cloud Storage
You can also add network storage. Refer to **10.2.5 Advanced - Cloud Storage** for details.

10.5.2 Storage Mode

Configure HDD Groups

Multiple HDDs can be managed in groups. Video from specified channels can be recorded to a designated HDD group through HDD settings. You can also switch the storage mode of the hard disk, including **Group**, **Quota (Capacity)**, and **Quota (Time)**.

Before You Start

Install at least one HDD in the video recorder.

Steps:

1. Go to **Main Menu** → **Storage** → **Group Management**.
2. Set **Mode** to **Group**.
3. Select a group number.
4. Select the IP channels to be recorded to the HDD group.

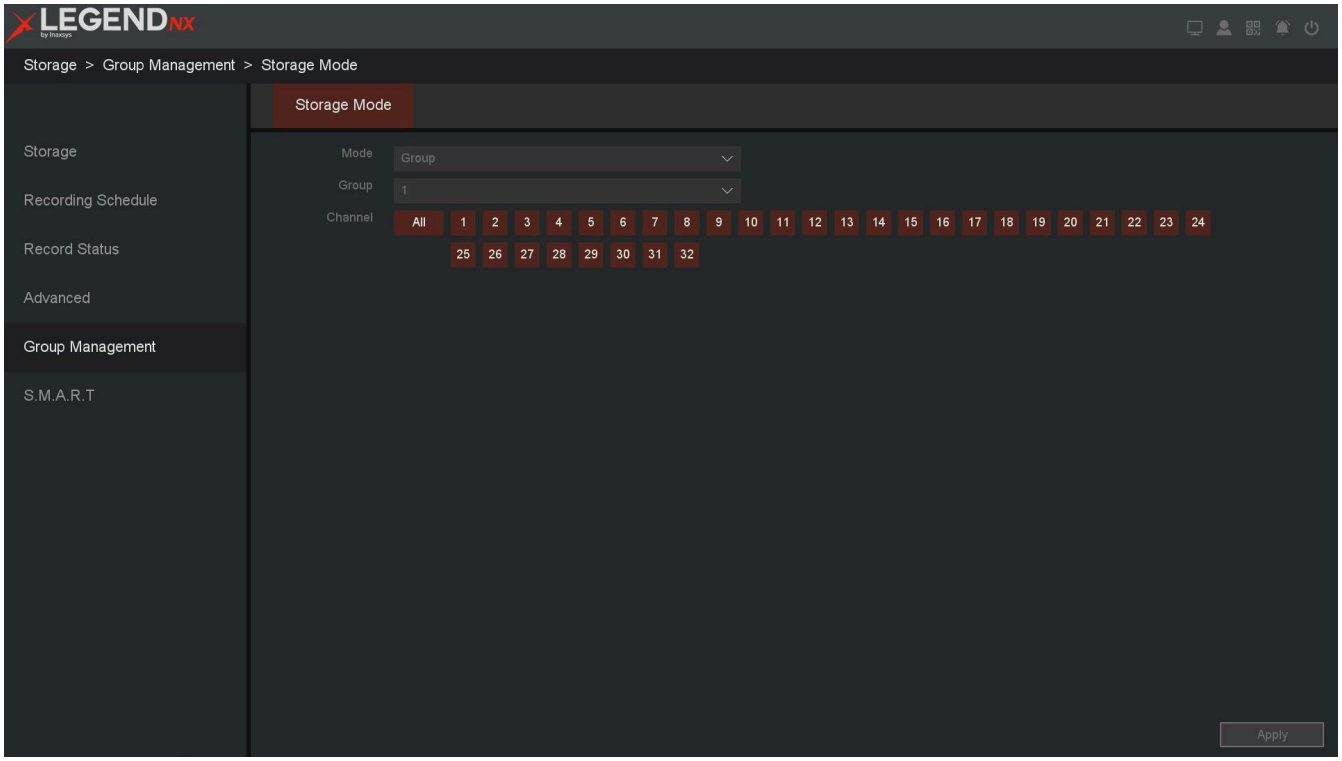


Figure 10-77 Storage Mode

5. Click **Apply**.
6. Restart the video recorder to activate the new storage mode settings.
7. After the restart, go to **Main Menu** → **Storage** → **Storage** → **Base**.
8. Click the **edit** icon of the desired HDD to assign it to a group.
9. Select a group number for the current HDD.

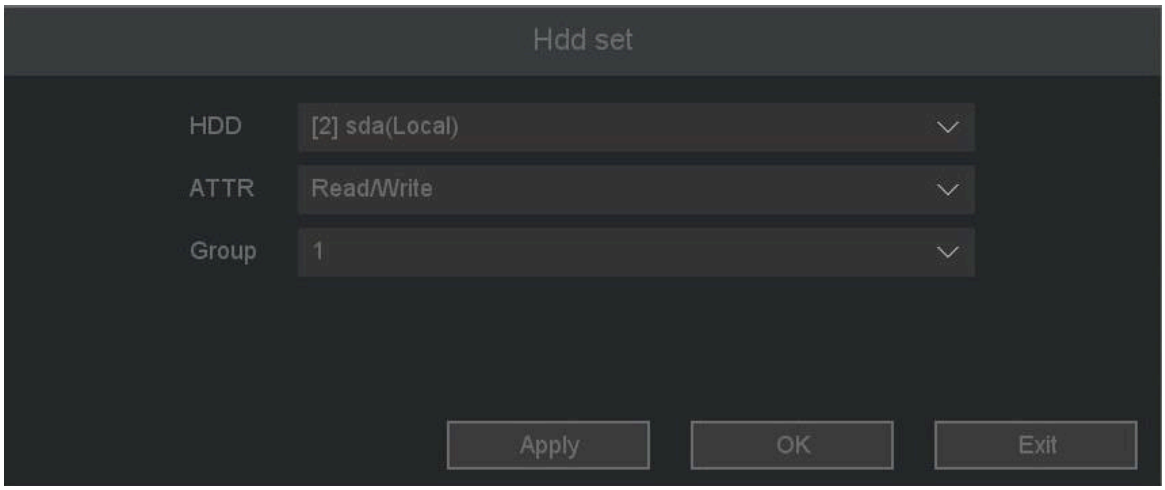


Figure 10-78 Group

10. Click **OK**.

Note
You can configure up to 16 groups in Group mode, and each channel operates independently. If a channel is not assigned to any group, no video will be recorded. If a channel belongs to multiple groups, it will use the storage space of each group sequentially until all groups are full.

Configure HDD Quota (Capacity)

Each camera can be assigned a storage quota (capacity) for video and image storage.

Steps:

1. Go to **Main Menu** → **Storage** → **Storage Mode** → **Storage Mode**.
2. Set **Mode** to **Quota (Capacity)**.
3. Select a camera under **Channel** to configure its quota.
4. Enter the values for **Record Quota (GB)** and **Picture Quota (GB)**.

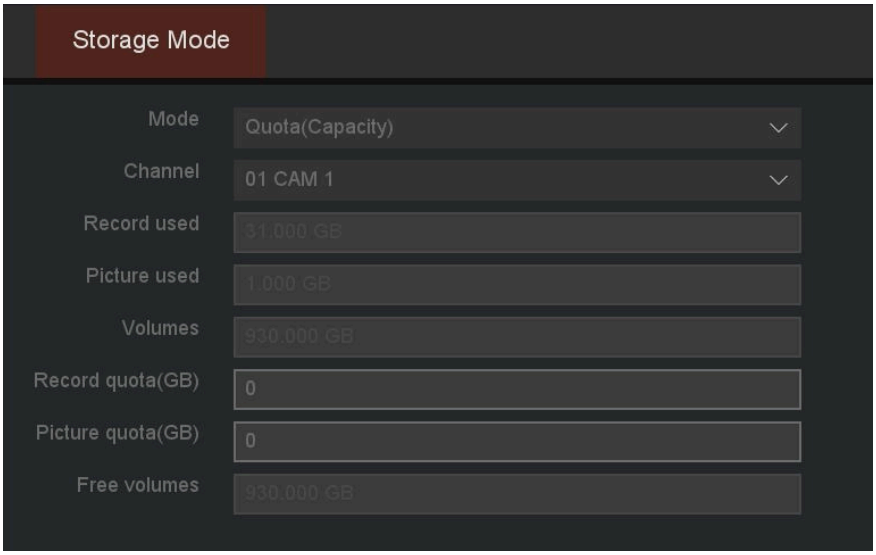


Figure 10-79 Quota

5. Click **Apply**.
6. Click **OK** to activate the new settings.

Note
If the quota is set to 0, all cameras will share the total HDD capacity for storing videos and images. Each time you change the storage mode, the NVR must be restarted.

Record Used
Displays the real-time storage space used by video recordings for the selected channel.

Picture Used
Displays the real-time storage space used by images for the selected channel.

Volumes
Displays the total capacity of all hard drives.

Record Quota
Allows you to manually set the storage quota for video recordings of the selected channel.

Picture Quota
Allows you to manually set the storage quota for images of the selected channel.

Free Volumes
Displays the remaining available storage after quotas have been allocated to other channels.

Note
Regarding the capacity quota mechanism (must be enabled to allow overwriting when the HDD is full; refer to **10.5.5 Advanced Settings/HDD Full** for details):

- Video recording has priority. As long as storage space is available, recording will continue. The system prioritizes retaining as many video files as possible.
- When the storage is full, the system will first overwrite data blocks from the channel with the earliest end time that exceed the allocated quota.
- Once quota allocation is applied, the system overwrites the earliest data blocks within the quota range.

Configure HDD Quota (Time)

Each camera can be assigned a storage quota based on time (number of recording days).

Steps:

1. Go to **Main Menu** → **Storage** → **Storage Mode** → **Storage Mode**.
2. Set **Mode** to **Quota (Time)**.
3. Select a camera under **Channel** to configure its quota.
4. Enter the number of recording days in **Record Quota (Day)**.

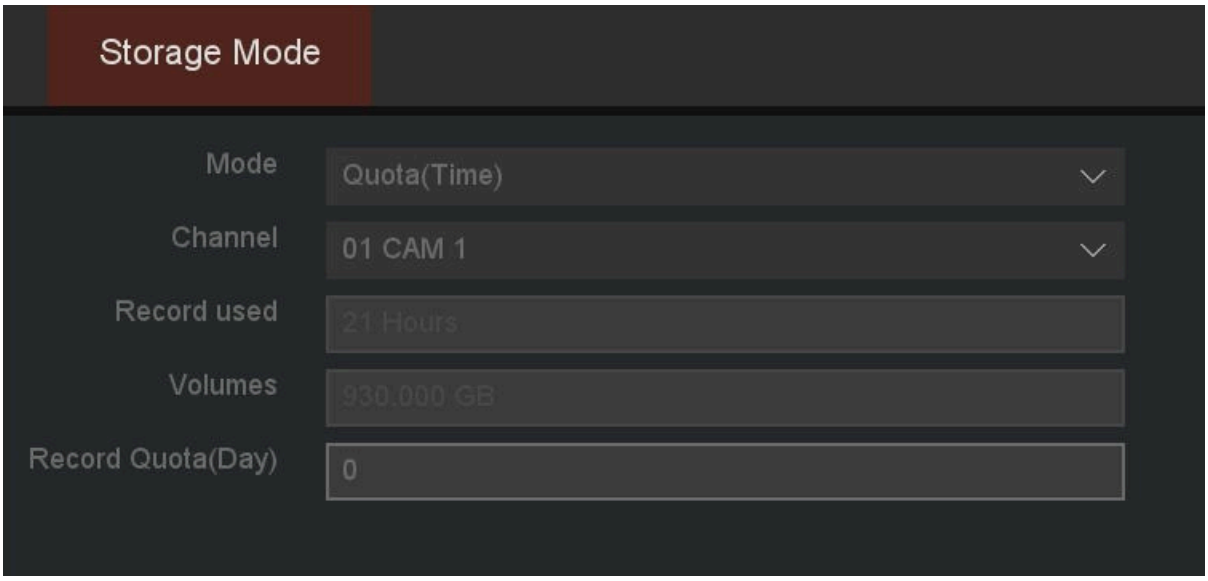


Figure 10-80 Quota

5. Click **Apply**.
6. Click **OK** to activate the new settings.

Note

If **Record Quota (Day)** is set to 0, all cameras will share the total HDD capacity for storing videos and images. Each time you change the storage mode, the NVR must be restarted.

Record Used

Displays the real-time storage usage of video files for the selected channel.

Volumes

Displays the total capacity of all hard drives.

Record Quota (Day)

Defines the retention period for recordings (0–60 days). During this period, newly recorded files will not overwrite existing files.

Note

Regarding the time-based quota mechanism (must be enabled to allow overwriting when the HDD is full; refer to **10.5.5 Advanced Settings/HDD Full** for details):

- Video recording has priority. As long as storage space is available, recording will continue. The system prioritizes retaining as many video files as possible.
- When storage is full, the system first overwrites data blocks from the channel with the earliest end time that exceed the configured time quota.
- The time quota mechanism takes effect only after recordings exceed the defined quota period.
- Because video bitrates vary dynamically, to ensure proper operation of the time quota mechanism, it is recommended to allocate a larger time quota to other channels when necessary.

10.5.3 Configure Recording Schedule

The video recorder automatically starts and stops recording according to the configured schedule. Refer to **6.4.2 Configure Recording Schedule** for details.

10.5.4 Record Status

On this page, you can view the recording status of all channels, including start/stop status, stream type, video or mixed stream (video and audio), frame rate, bit rate, main/sub stream resolution of IP channels, and whether redundancy is enabled.

Before You Start

Ensure that the recording schedule has been configured.

Steps:

1. Go to **Main Menu → Storage → Record Status → Record**.

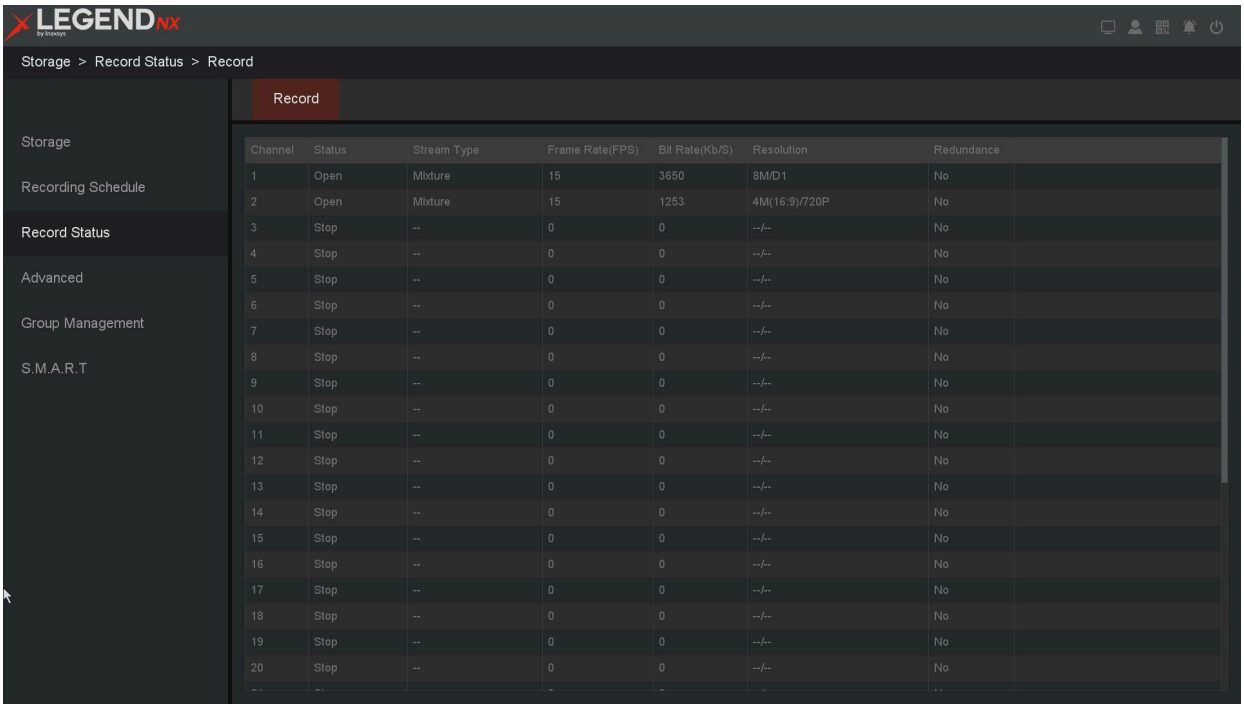


Figure 10-81 Record

10.5.5 Advanced Settings

On this page, you can configure the HDD full handling strategy: **Stop** or **Overwrite**.

Steps:

1. Go to **Main Menu → Storage → Advanced → Advanced**.

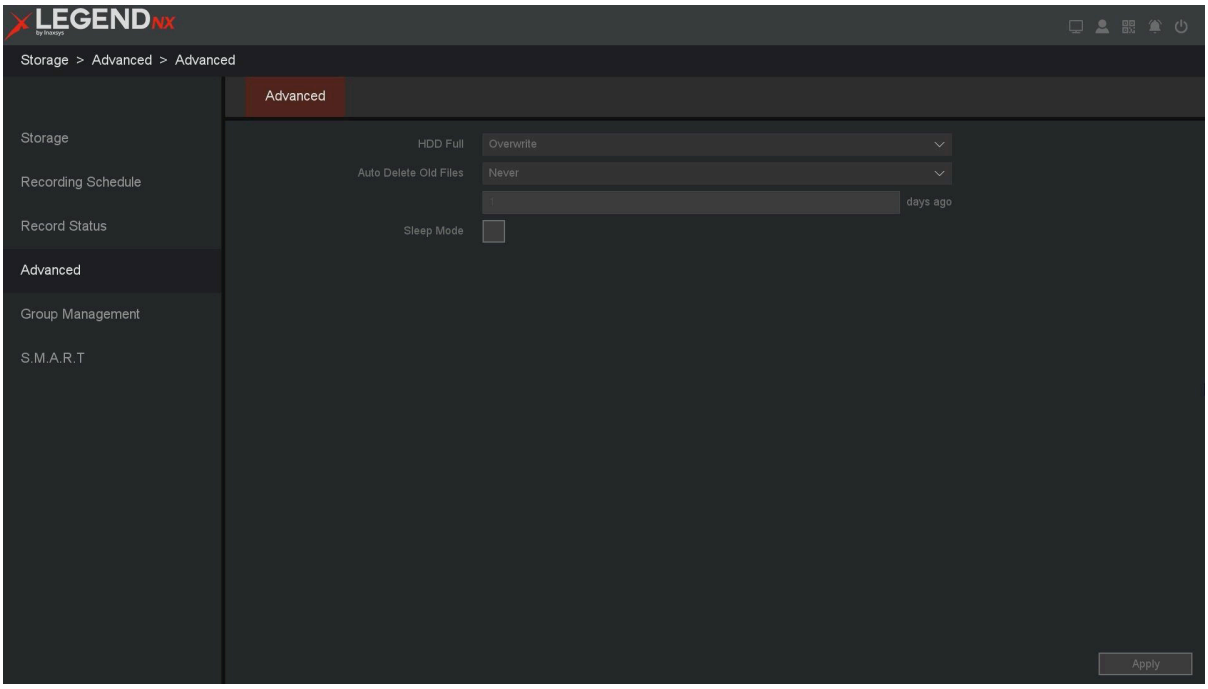


Figure 10-82 Advanced

2. Configure the parameters as required.
3. Click **Apply**.

HDD Full

- **Stop Record**: When the HDD is full, the video recorder stops recording.
- **Overwrite**: When the HDD is full, the video recorder continues recording by overwriting the oldest files.

Auto-Delete Old Files

Supports two modes: **Never** and **Custom**. In **Custom** mode, you can set the auto-delete period from 1 to 30 days.

Sleep Mode

HDDs that remain idle for an extended period will enter sleep mode.

Enable RAID

When RAID is enabled on the device, a Redundant Array of Independent Disks (RAID) can be configured. Refer to **10.4.5 RAID** for details.

Note

This feature is only supported on certain models. Refer to the actual product interface for availability.

10.5.6 S.M.A.R.T

The device provides HDD health detection functions, including S.M.A.R.T. and bad sector detection. S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) is a monitoring system that detects and reports various indicators of HDD reliability to help predict potential failures.

Before You Start

Install at least one HDD in the video recorder.

Steps:

1. Go to **Main Menu** → **Storage** → **S.M.A.R.T** → **S.M.A.R.T**.
2. Select the HDD you want to test.
3. Select the self-test type: **Short Test** or **Extended Test**.

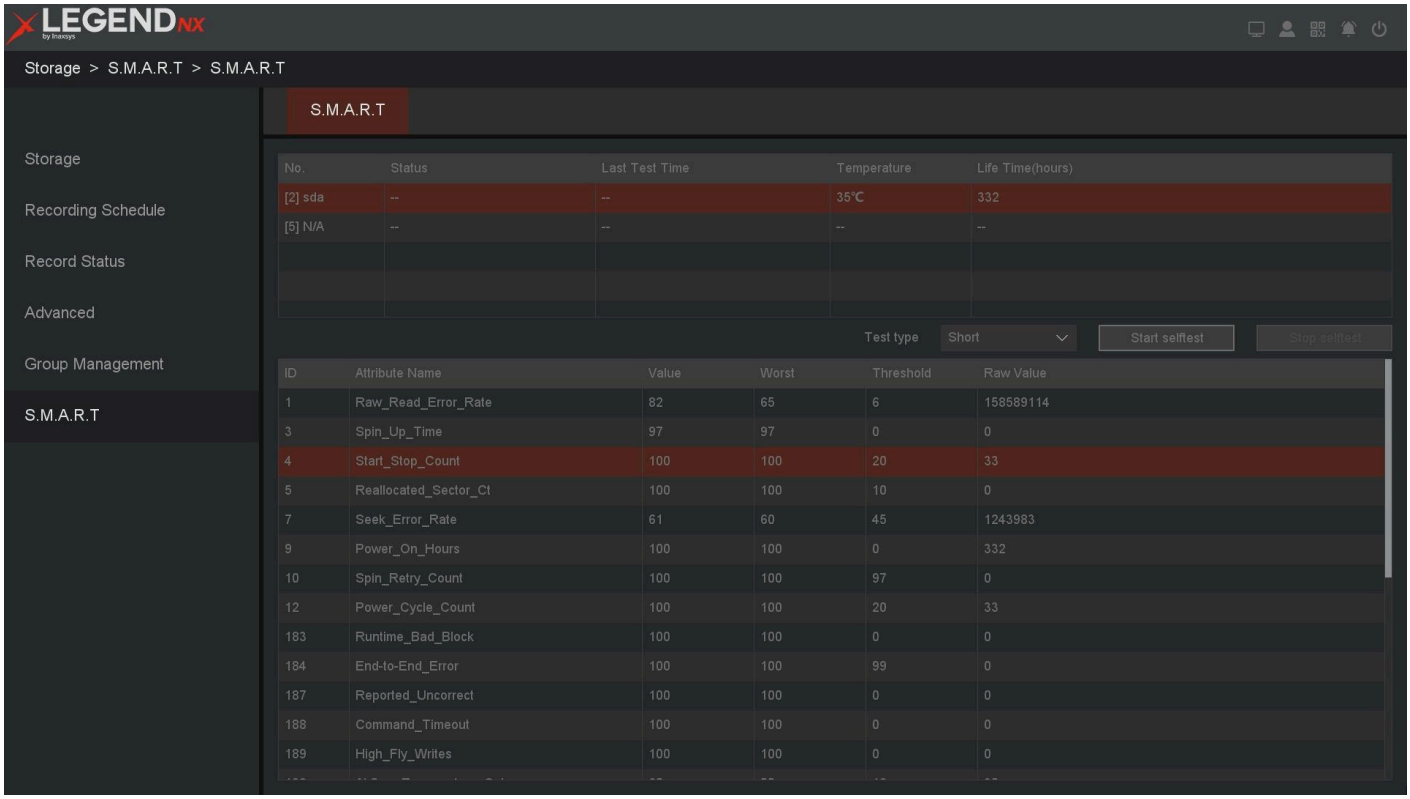


Figure 10-83 S.M.A.R.T

4. Click **Start Self-Test** to begin the S.M.A.R.T HDD self-test.
5. If the HDD is functioning normally, the **Status** will display **Passed**. You can also pause or stop the test if needed.

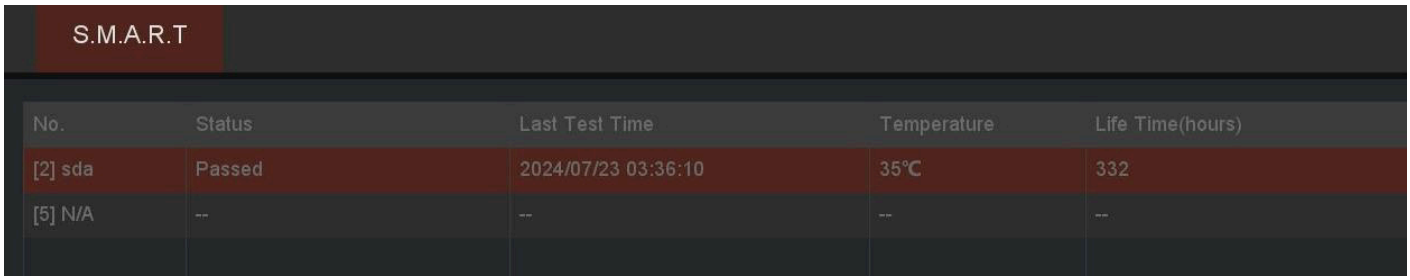


Figure 10-84 Status

10.6 Smart Search

10.6.1 Smart Search

Face Detection
On this page, you can select the recording channel that has triggered face detection and contains recorded files. You can then set the start time and end time.

Before You Start
Ensure that **Face Detection** is enabled on the camera via the NVR. Also ensure that **Record Channel** and **Snapshot** are enabled in the trigger process for face detection, and that **Snapshot** is enabled on the camera. For details, refer to the **IP Camera User Manual**.

Steps:

1. Go to **Main Menu** → **Smart Search** → **Smart Search** → **Face Detection**.
2. Select the **Record Channel** you want to search.
3. Set the **Start Time** and **End Time**.

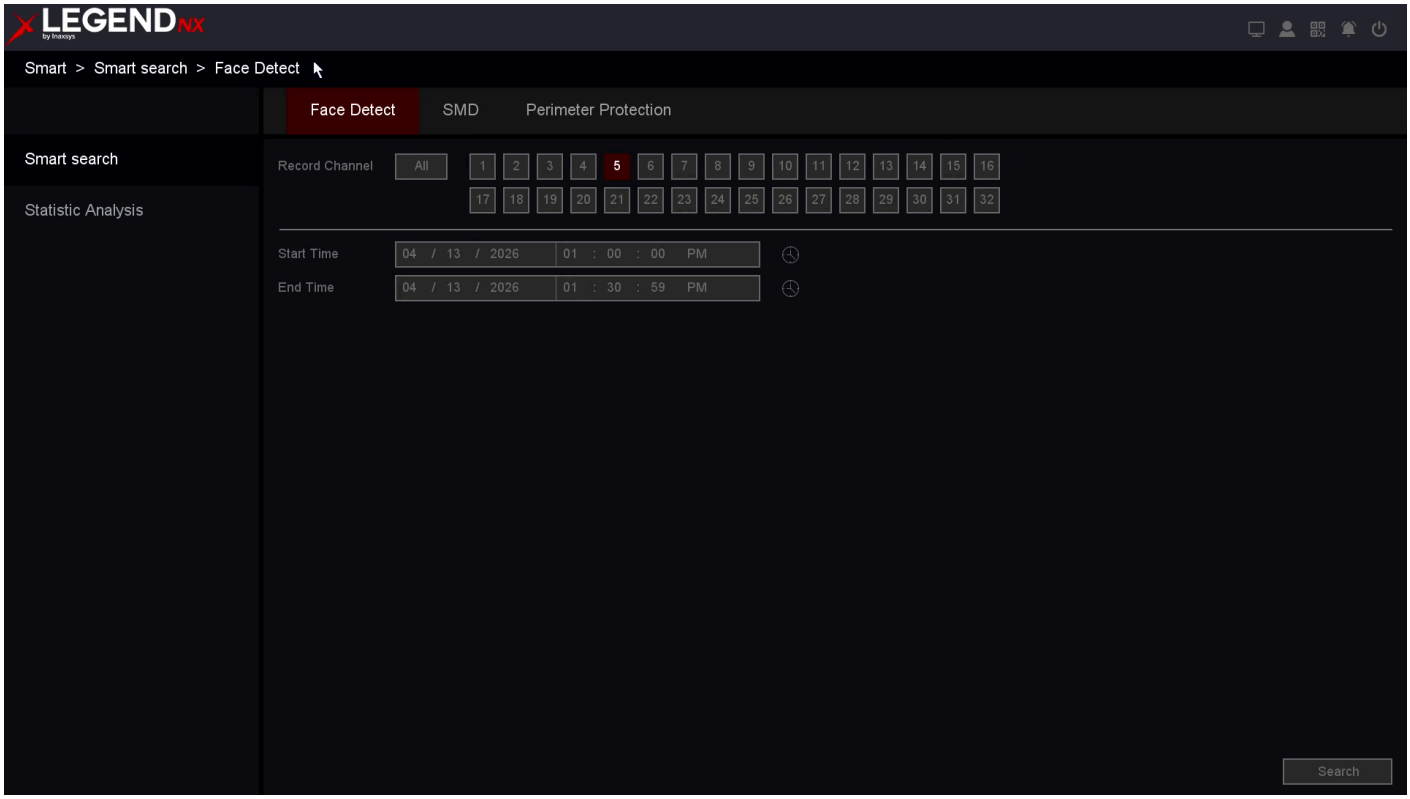


Figure 10-85 Status

4. Click **Search**.
5. The search results will be displayed as shown below.

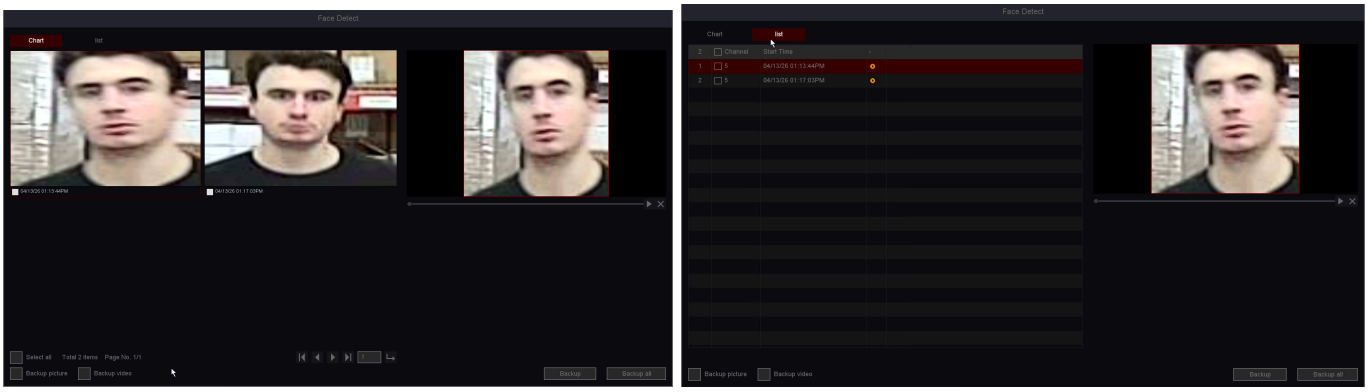


Figure 10-86 Search Result

Note

- On this page, you can choose the display mode for face detection results (**thumbnail view** or **list view**). You can also select recordings and choose to back up images or videos.
- If no images are displayed in thumbnail view, verify that **Snapshot** is enabled on the camera. For camera settings, refer to the **IP Camera User Manual**.

Smart Motion Detection (SMD)

On this page, you can select the recording channel that triggered **Motion Detection** with **Human Shape Filter** or **Vehicle Shape Filter**, and view the associated alarm videos or snapshots. You can then set the start time and end time.

Before You Start

Ensure that **Motion Detection with Human Shape Filter/Vehicle Shape Filter** is enabled on the camera via the NVR. Also ensure that **Record Channel** and **Snapshot** are enabled in the trigger process for motion detection, and that **Snapshot** is enabled on the camera. For details, refer to the **IP Camera User Manual**.

Steps:

1. Go to **Main Menu** → **Smart** → **Smart Search** → **SMD**.
2. Select the event type: **SMD-Human** or **SMD-Vehicle**.
3. Select the **Record Channel** you want to search.
4. Set the **Start Time** and **End Time**.

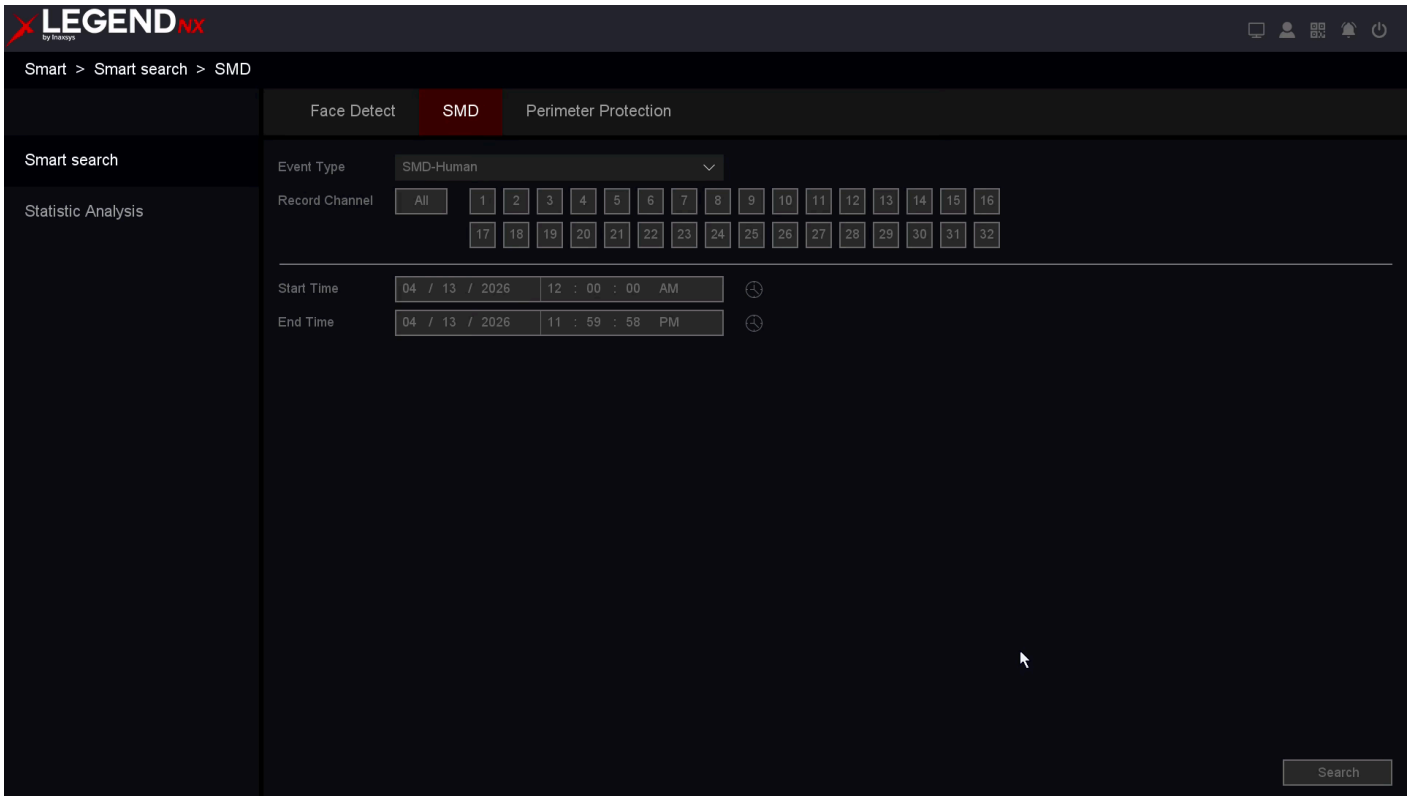


Figure 10-87 SMD

5. Click **Search**.
6. The search results will be displayed as shown below.

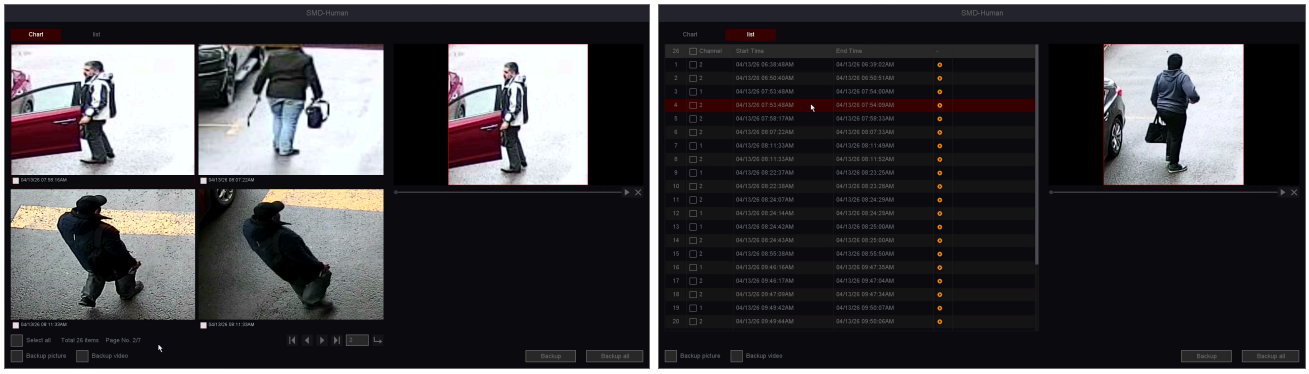


Figure 10-88 Search Result

Note

- On this page, you can choose the display mode for SMD results (**thumbnail view** or **list view**). You can also select recordings and choose to back up images or videos.
- If no images are displayed in thumbnail view, verify that **Snapshot** is enabled on the camera. For camera settings, refer to the **IP Camera User Manual**.

Perimeter Protection (PP)

On this page, you can select the recording channel that triggered **Line Crossing**, **Area Intrusion**, **Region Entrance**, or **Region Exiting** with **Human Shape Filter** or **Vehicle Shape Filter**, and view the associated alarm videos or snapshots. You can then set the start time and end time.

Before You Start

Ensure that **Line Crossing**, **Area Intrusion**, **Region Entrance**, and **Region Exiting** with **Human Shape Filter/Vehicle Shape Filter** are enabled on the camera via the NVR. Also ensure that **Record Channel** and **Snapshot** are enabled in the trigger process, and that **Snapshot** is enabled on the camera. For details, refer to the **IP Camera User Manual**.

Steps:

1. Go to **Main Menu → Smart → Smart Search → PP**.
2. Select the event type: **Line Crossing-Human/Vehicle**, **Area Intrusion-Human/Vehicle**, **Region Entrance-Human/Vehicle**, or **Region Exiting-Human/Vehicle**.
3. Select the **Record Channel** you want to search.
4. Set the **Start Time** and **End Time**.

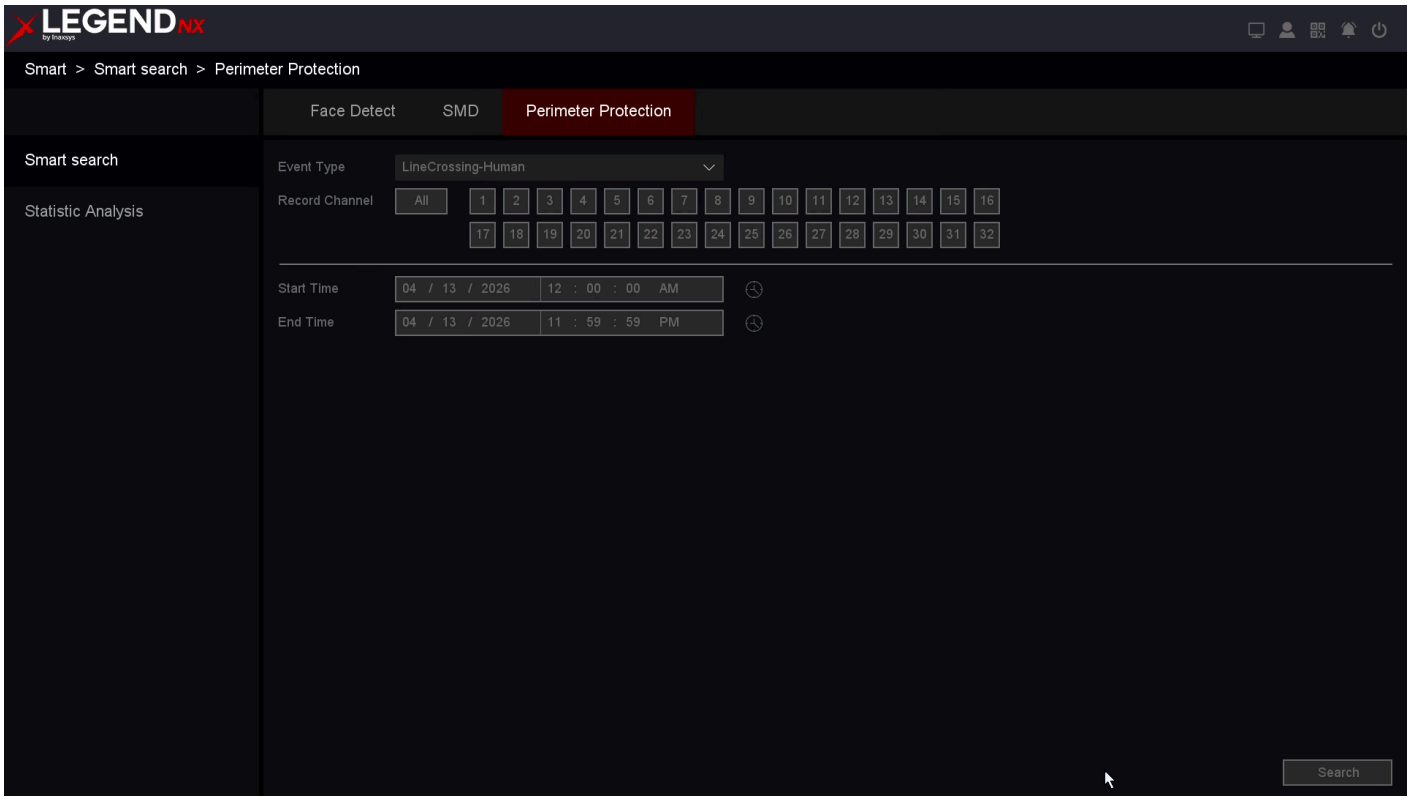


Figure 10-89 PP

5. Click **Search**.
6. The search results will be displayed as shown below.

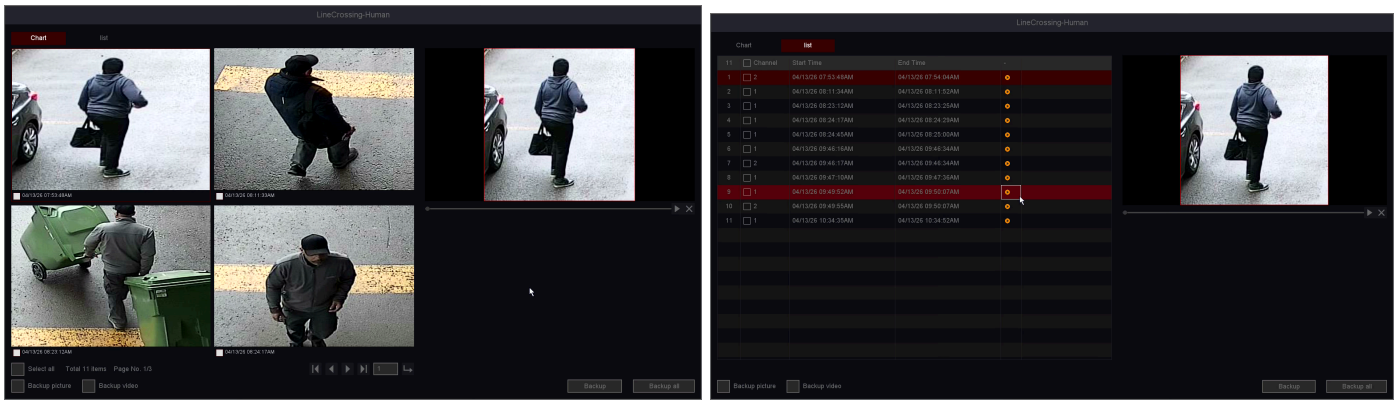


Figure 10-90 Result

Note

- On this page, you can choose the display mode for results (**thumbnail view** or **list view**). You can also select recordings and choose to back up images or videos.
- If no images are displayed in thumbnail view, verify that **Snapshot** is enabled on the camera. For camera settings, refer to the **IP Camera User Manual**.

10.7 Playback

10.7.1 Normal Playback & Event Playback

Right-click and select **Playback** to enter the playback interface. Alternatively, click the playback button in the main menu to access the playback interface.

For **Normal Playback** and **Event Playback**, refer to **4.2 Normal Playback** and **4.3 Event Playback**.

10.7.2 Label Play

Select **Label Play** to enter label playback mode.

Before You Start

Ensure that you have added default labels during normal playback and that the corresponding label records already exist in **File Management**, as shown below. You can also refer to **4.2 Normal Playback**.

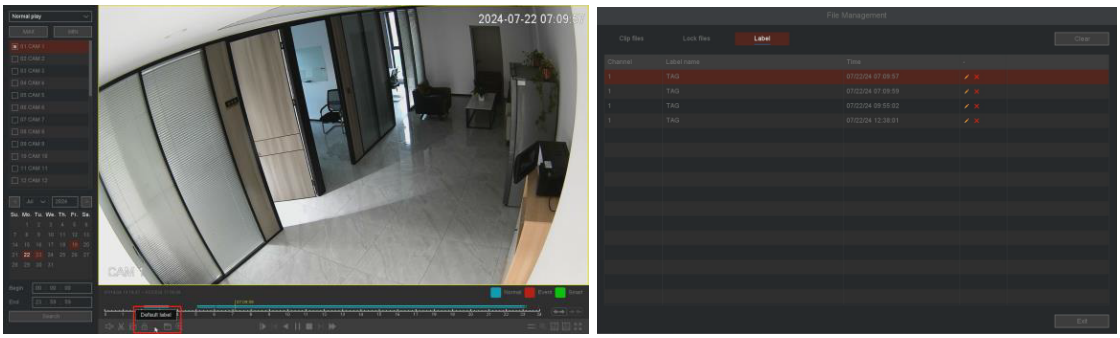


Figure 10-91 Label Play

Steps:

1. Go to **Playback**.
2. Select **Label Play**.
3. Select the desired channels.
4. Set the time period, then click **Search**.

Figure 10-92 Label Play

5. The search results are displayed as shown above.
6. Click a label in the list to start label playback as required.
7. Click **Return** to go back to the previous interface and change the search channels.

Label
The label name, which can be edited in **File Management**.

Chan
The channel associated with the label.

Time
The time at which the label was created during playback.

Left and Right Arrows
Use these to switch pages and locate the desired label entries.

Play Before and Play Delay
Set the playback duration before and after the label time.

Note
For details on these controls, refer to **Table 4-3 Playback Interface Description**. The following functions are not available in label playback mode: **Sync/Async**, **Main/Sub Stream**, and **Frame Control**.

10.7.3 Smart Play

Select **Smart Play** to enter Smart playback mode.

Before You Start
Ensure that intelligent detection features such as Motion Detection, Line Crossing, Area Intrusion, Region Entrance, and Region Exiting are enabled on the device, and that alarm videos have been generated.

Table 10-4 Icon Description

Icon	Description	Icon	Description
	Draw a line for detection rules		Search for faces
	Draw a quadrilateral detection area		Search for human bodies
	Draw a rectangular motion detection area		Search for vehicles
	Enable full-screen motion detection		Search for bicycles

Line Drawing

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Draw Line** icon  to draw a line on the video interface.
6. Click **Setting** to configure playback parameters such as **Skip Non-Focus Video**, and set the playback speed for **Non-Concerned Video** and **Attention Video**. You can also define the playback time before and after events (0 to 600 seconds), as shown below.

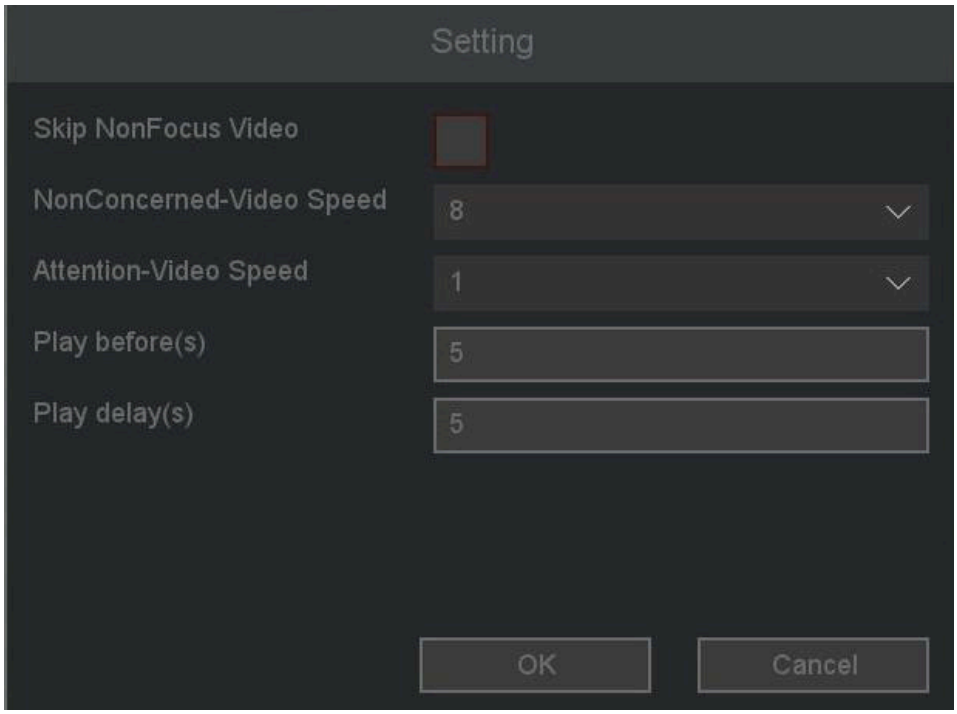


Figure 10-93 Setting

7. Click **Search**. The results will be displayed below. Videos with line-crossing events will be highlighted in green, and playback will follow the settings configured in Step 6.

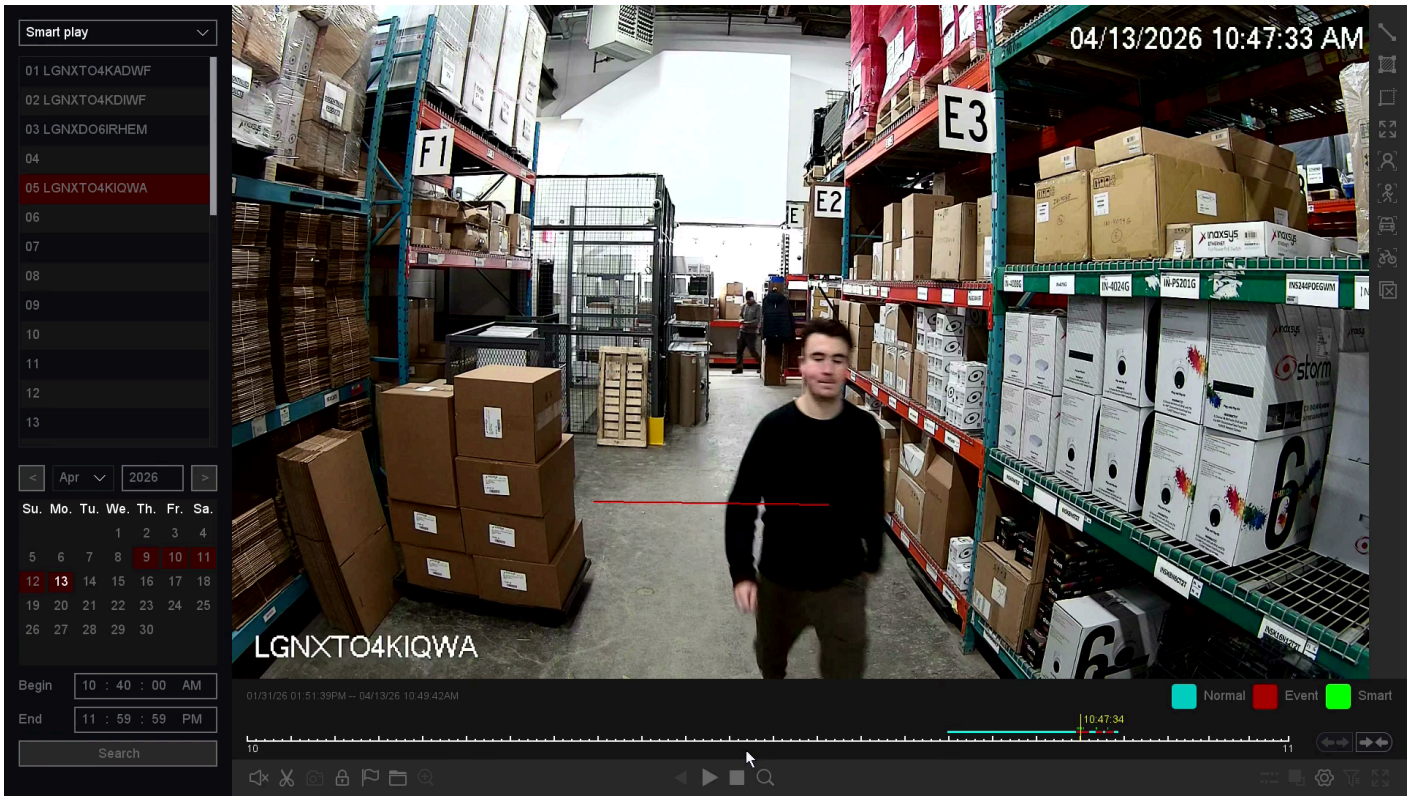


Figure 10-94 Search Result

Square / Rectangle Drawing

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Draw Quadrilateral** icon  to draw a quadrilateral on the video interface.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos with area intrusion events will be highlighted in green, and playback will follow the settings configured in Step 6.

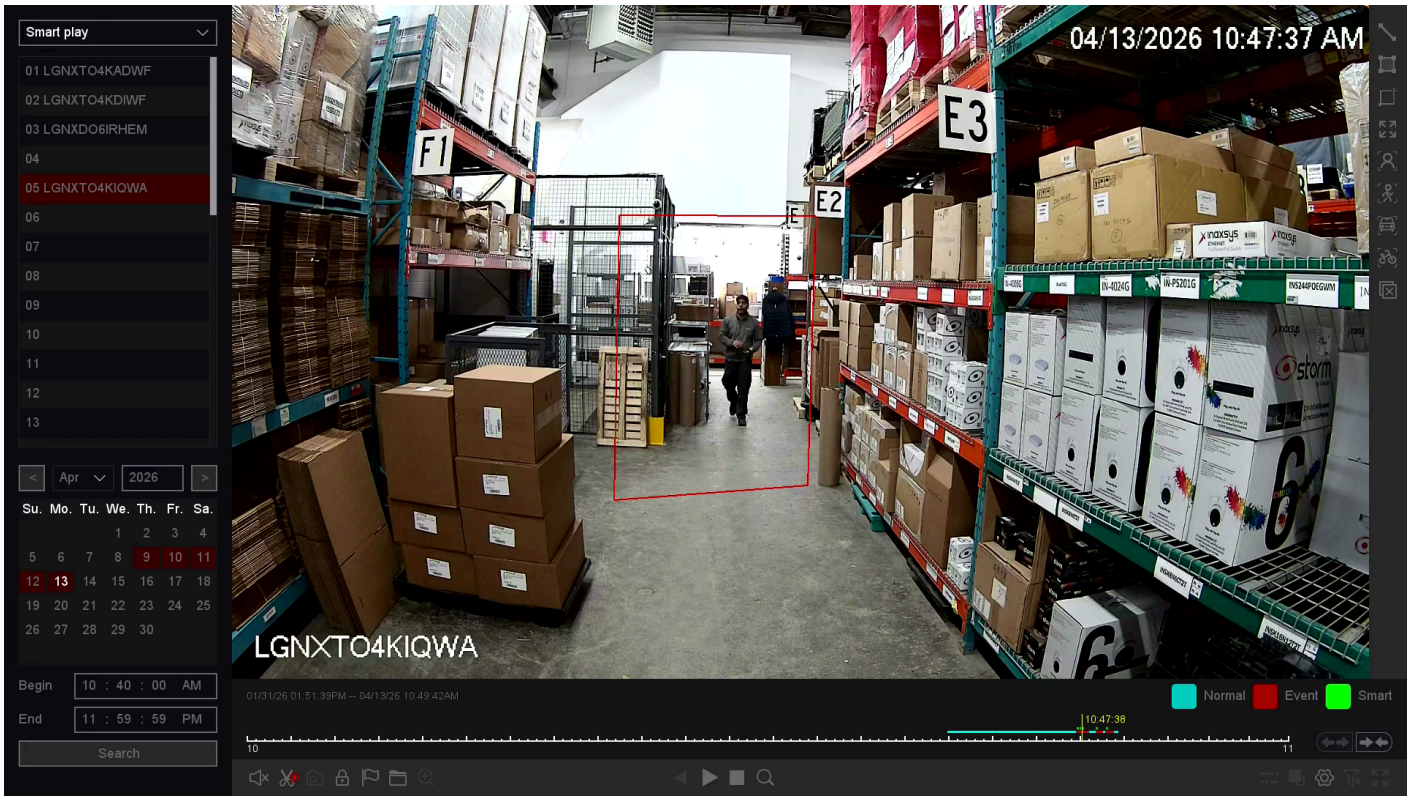


Figure 10-95 Search Result

Motion-Based Area Search

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Motion Draw Rectangle** icon  to define a motion detection area on the video interface.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos with motion events will be highlighted in green, and playback will follow the settings configured in Step 6.

Figure 10-96 Search Result

Full-Screen Motion Search

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Motion Full Screen** icon  to enable full-screen motion detection on the video interface.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos with motion events will be highlighted in green, and playback will follow the settings configured in Step 6.

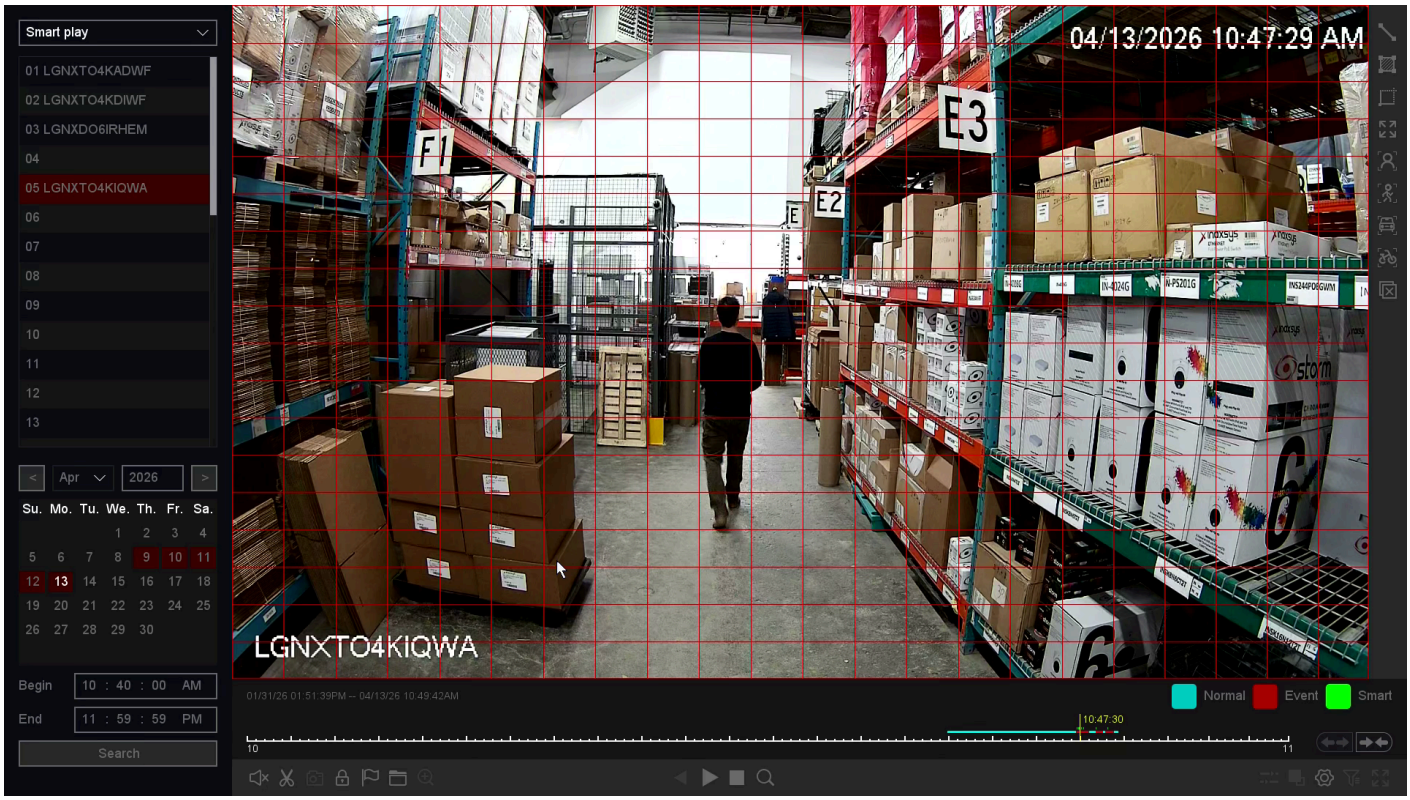


Figure 10-97 Search Result

Face Detection Search

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Face Search** icon  . The system will analyze the entire video frame by default.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos containing detected faces will be highlighted in green, and playback will follow the settings configured in Step 6.

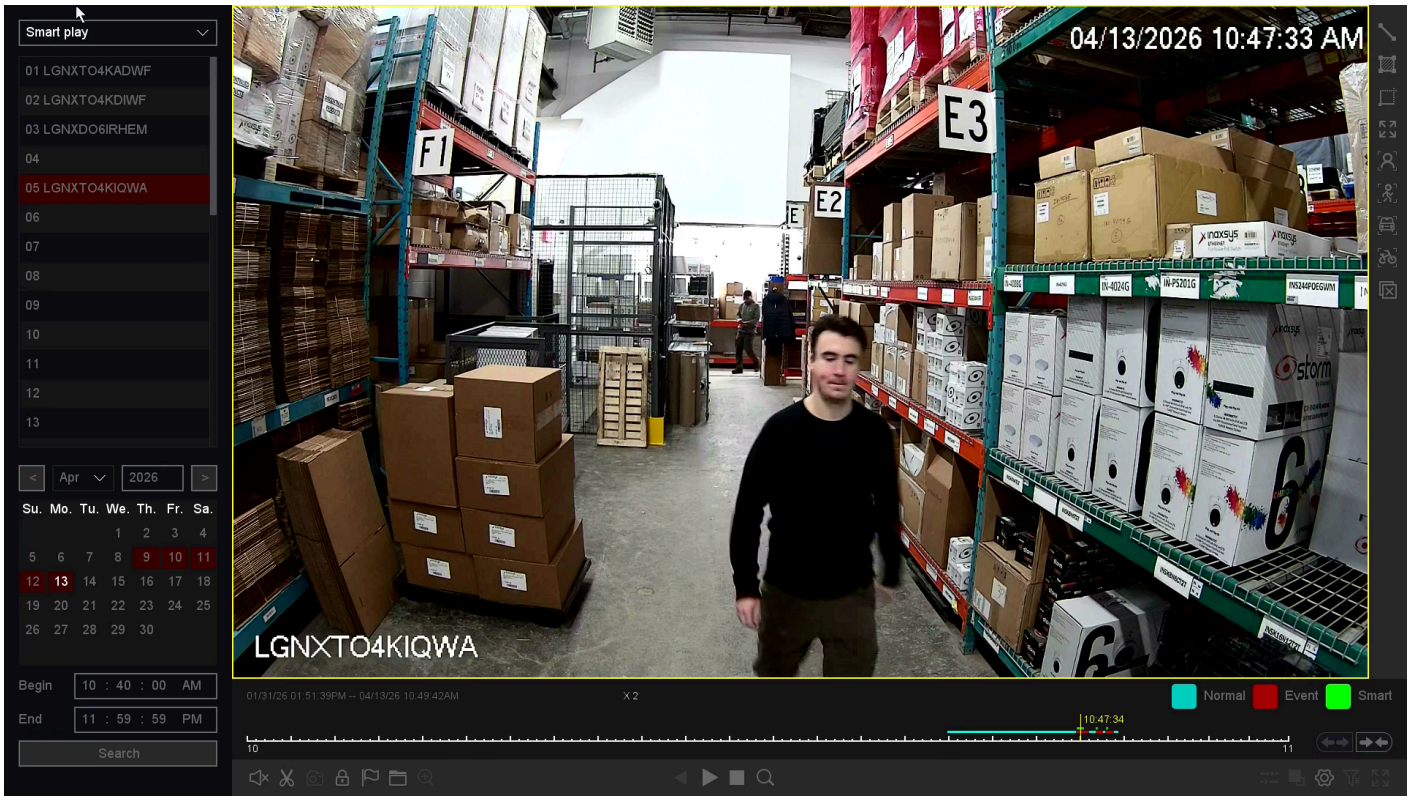


Figure 10-98 Search Result

Note

Smart Play is only supported on LegendNX IP Cameras that provide this functionality.

Human Body Search

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Human Body Search** icon  . The system will analyze the entire video frame by default.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos containing detected human movement will be highlighted in green, and playback will follow the settings configured in Step 6.

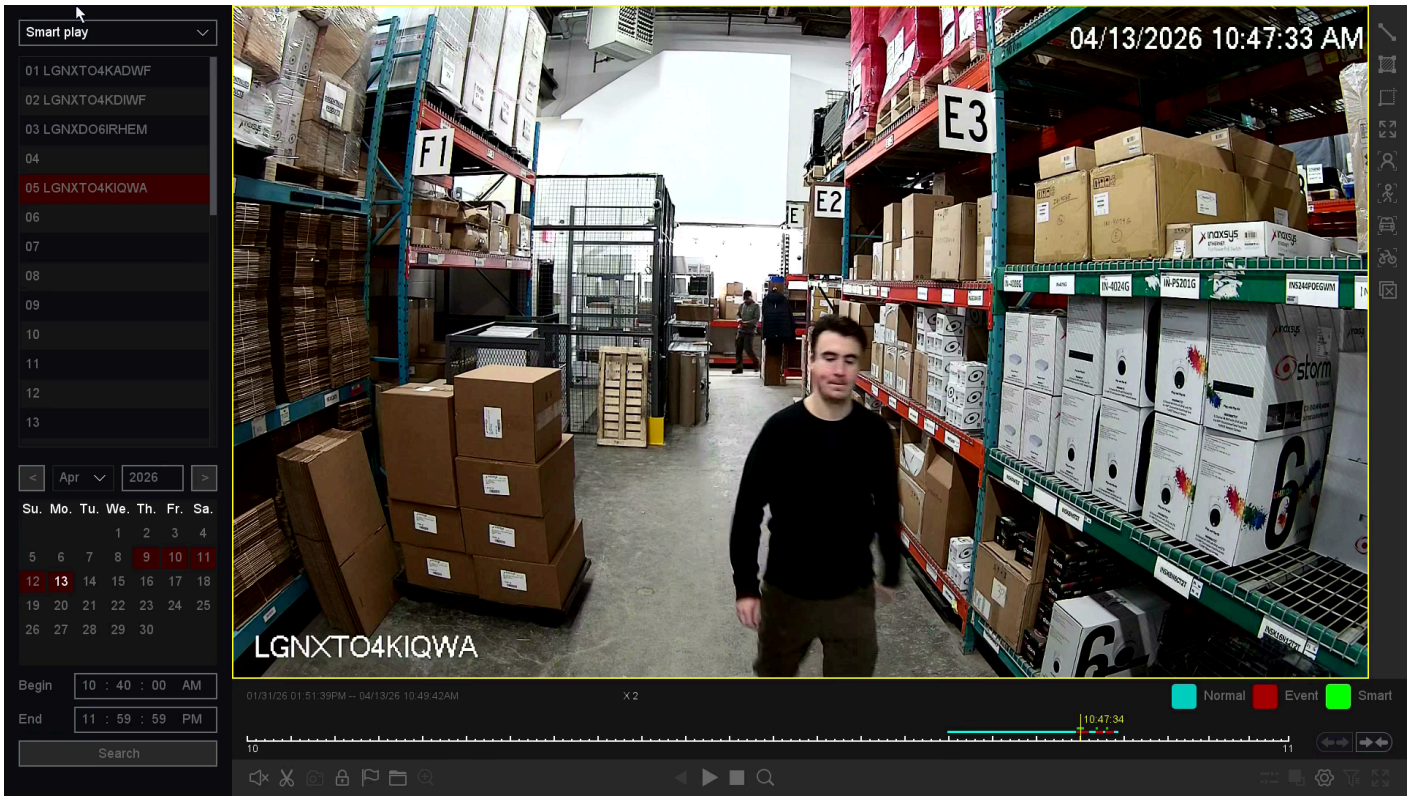


Figure 10-99 Search Result

Vehicle Search

Steps:

1. Go to **Playback**.
2. Select **Smart Play**.
3. Select the channel and set the recording time as required.
4. Click the **Play** button or click the blue timeline.
5. Click the **Vehicle Search** icon  . The system will analyze the entire video frame by default.
6. Click **Setting** to configure the parameters as required.
7. Click **Search**. The results will be displayed below. Videos containing detected vehicles will be highlighted in green, and playback will follow the settings configured in Step 6.

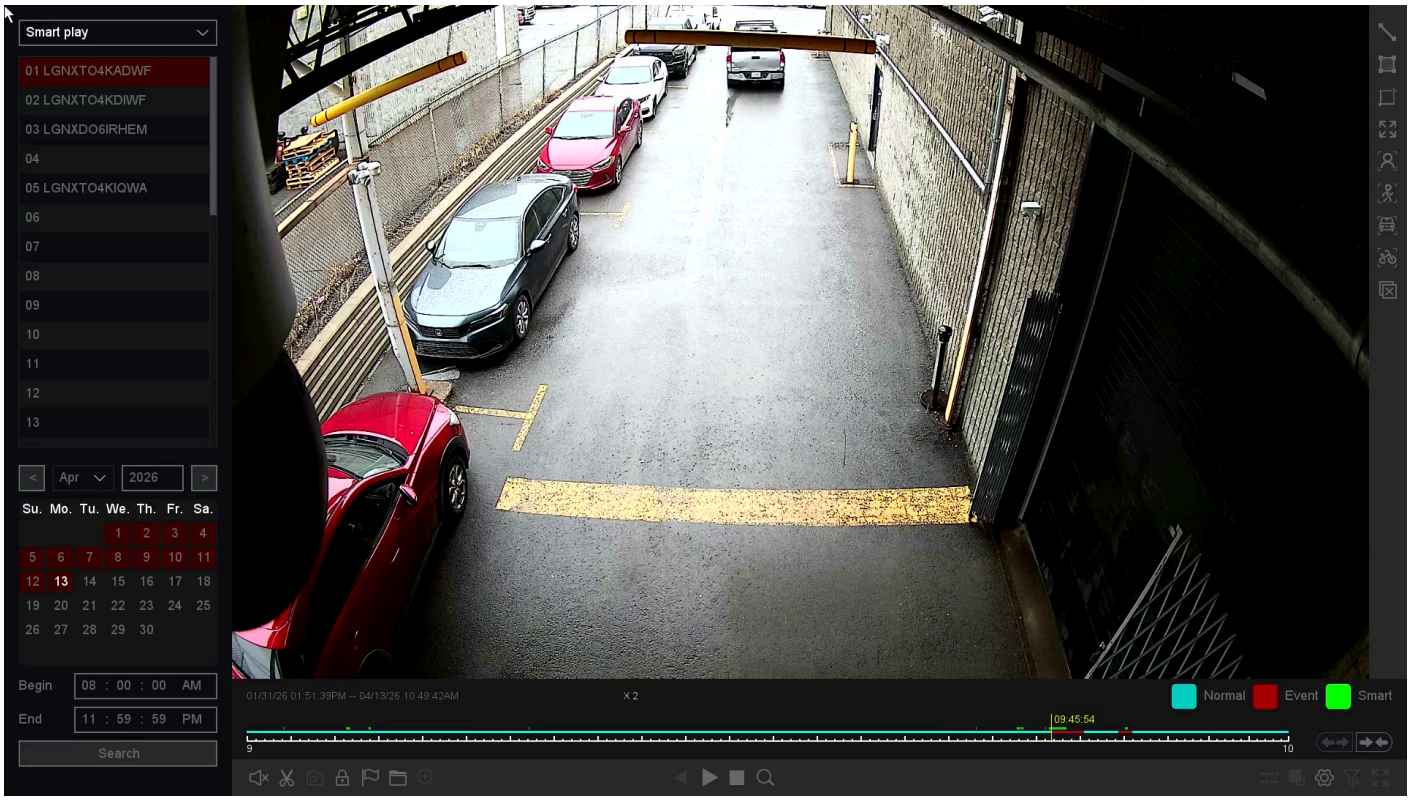


Figure 10-100 Search Result

Note

Clear All: Clicking this button will remove all previously drawn lines and rectangles. You can then draw new lines and define new rules.

10.7.4 Time Division Playback

Selecting **"Time Division Playback"** enters the time-division playback mode. On this page, you can play recordings by time period and distribute 24-hour recordings evenly based on the number of windows selected (from 1 to 16). For example, if you select 4 windows, the recordings for the selected date will be divided into 4 equal segments.

Before You Start

Ensure that the selected camera channel has recorded data.

1. Go to **Playback**.
2. Select **Time Division Playback**.
3. Select the desired channel.
4. Set the number of division windows and the recording time.

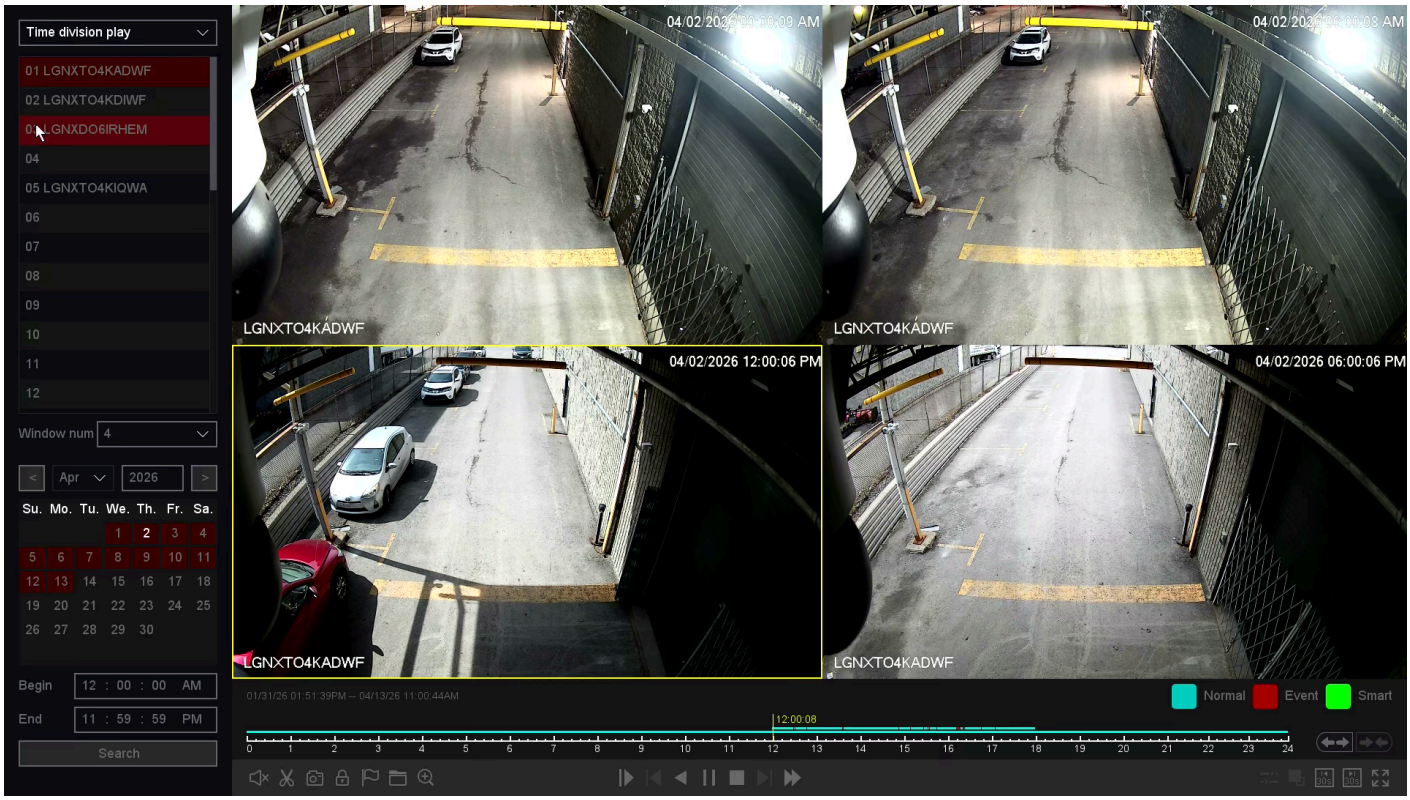


Figure 10-101 Select Windows Number

5. Click **Search**.
6. Select the corresponding window to quickly play the desired video segment.

Note

If the selected number of division windows is too high, the device may not be able to display all windows due to decoding limitations. In this case, reduce the number of windows.

10.7.5 Normal Play (Picture)

On this page, you can play back recordings in picture format.

Before You Start

Ensure that the selected channel already has pictures generated by manual capture or intelligent detection alarms.

1. Go to **Playback**.
2. Select **Normal Play (Picture)**.
3. Select the desired channel.
4. Select the time period you want to play back.
5. Click **Search**.

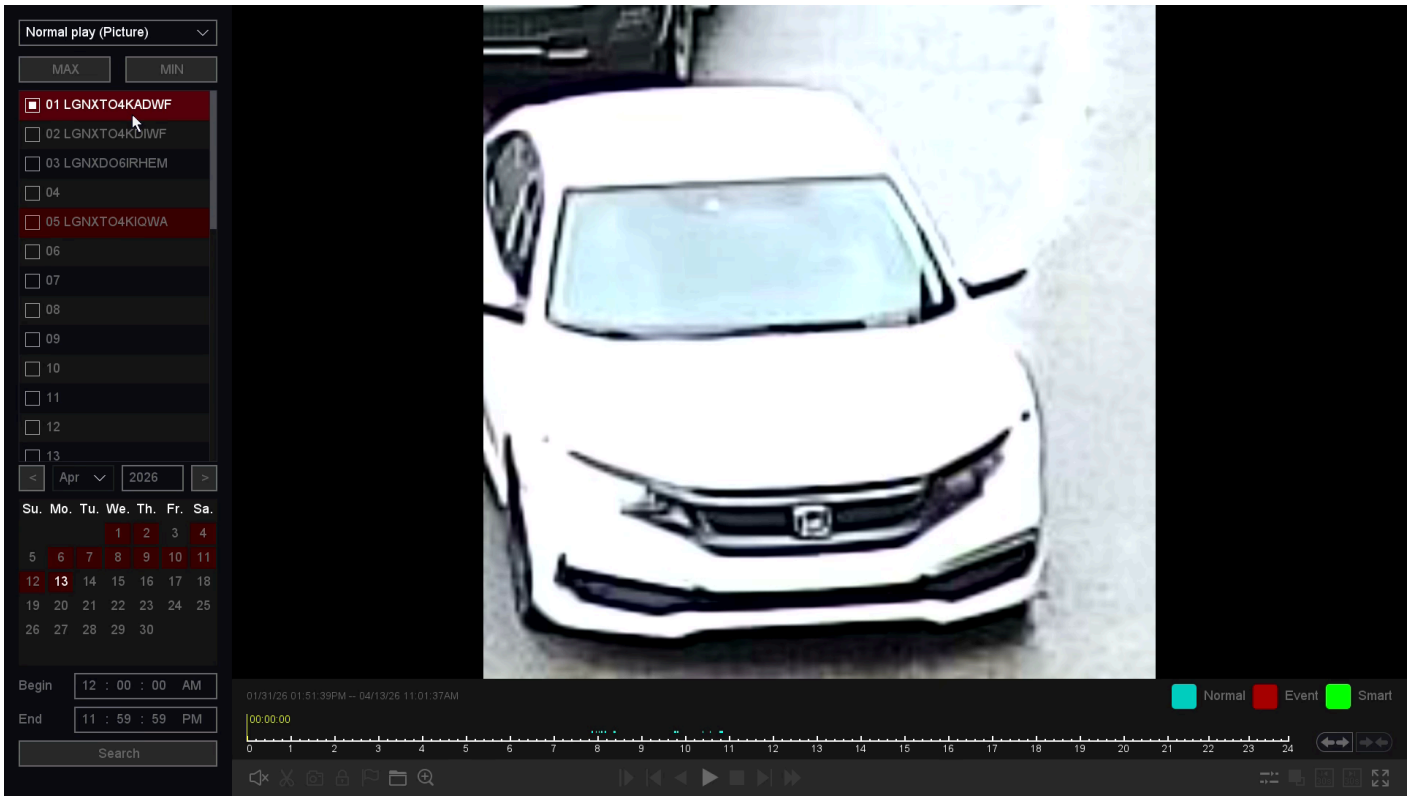


Figure 10-102 Normal Play

6. Playback control buttons include **File Management**, **Sync/Async**, **Start/Pause**, **Backward Play**, **Stop Playing**, **Slow Down**, **Speed Up**, **Timeline Stretch**, and **Timeline Shorten**.

Note

You can stop playback by right-clicking, and exit the playback interface by right-clicking again.

11. Appendix

11.1 Glossary

DVR
Acronym for **Digital Video Recorder**. A DVR is a device that receives video signals from analog cameras, compresses them, and stores them on internal hard drives.

NVR
Acronym for **Network Video Recorder**. An NVR can be a PC-based or embedded system used for centralized management and storage of IP cameras, IP dome cameras, and other DVRs.

Dual-Stream
Dual-stream is a technology that records high-resolution video locally while simultaneously transmitting a lower-resolution stream over the network. The DVR generates both streams: the main stream can reach up to 4K resolution, while the sub-stream typically supports up to 720p.

HDD
Acronym for **Hard Disk Drive**. A storage device that stores digitally encoded data on magnetic platters.

DHCP
Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables devices (DHCP clients) to automatically obtain configuration information for operation within an Internet Protocol (IP) network.

HTTP
Acronym for **Hypertext Transfer Protocol**. A protocol used to transfer hypertext requests and information between servers and web browsers over a network.

P2P
Peer-to-peer (P2P) is a type of network architecture commonly used for distributing digital media files. In a P2P network, each device functions as both a client and a server, sharing bandwidth and processing resources across all participants.

DDNS
Dynamic DNS (DDNS) is a method, protocol, or network service that allows a device (such as a router or computer) to automatically update a domain name server with changes to its IP address or other DNS records in real time.

NTP
Acronym for **Network Time Protocol**. A protocol used to synchronize the clocks of computers over a network.

NTSC
Acronym for **National Television System Committee**. NTSC is an analog television standard used in regions such as the United States and Japan. Each frame consists of 525 scan lines at 60 Hz.

PAL

Acronym for **Phase Alternating Line**. PAL is an analog television standard widely used in many parts of the world. Each frame consists of 625 scan lines at 50 Hz.

PTZ

Acronym for **Pan, Tilt, Zoom**. PTZ cameras are motorized systems that allow the camera to pan (left/right), tilt (up/down), and zoom in or out.

USB

Acronym for **Universal Serial Bus**. A plug-and-play interface standard used to connect devices to a host computer.

Legal Information

About This Manual

This manual provides instructions for the installation, configuration, operation, and maintenance of the product.

All images, diagrams, and illustrations in this manual are provided for reference purposes only and may differ from the actual product. The information contained herein is subject to change without prior notice due to firmware updates or product improvements. For the latest version of this manual, please visit the official Inaxsys website.

This manual is intended for use by qualified professionals. Installation and servicing should be performed by trained personnel only.

Trademarks

Legend NX and all related trademarks, logos, and brand names are the property of **Inaxsys Security Systems Inc.** and may be registered in applicable jurisdictions.

Disclaimer

To the maximum extent permitted by applicable law, this manual and the product described herein, including all hardware, software, and firmware, are provided **“as is”** and **“with all faults.”**

Inaxsys makes no warranties, express or implied, including but not limited to warranties of merchantability, fitness for a particular purpose, or satisfactory quality. Use of the product is at your own risk.

In no event shall Inaxsys be liable for any indirect, incidental, special, or consequential damages, including but not limited to:

- loss of business profits
- business interruption
- loss or corruption of data
- system failure
- loss of documentation

whether arising from breach of contract, tort (including negligence), product liability, or otherwise, even if Inaxsys has been advised of the possibility of such damages.

You acknowledge that internet-based products and systems may be subject to inherent security risks. Inaxsys shall not be held responsible for abnormal operation, privacy breaches, or damages resulting from cyber-attacks, hacking, viruses, or other network-related threats. However, Inaxsys will provide reasonable technical support where applicable.

You agree to use this product in compliance with all applicable laws and regulations. You are solely responsible for ensuring that your use does not infringe upon the rights of third parties, including but not limited to intellectual property rights, privacy rights, and data protection regulations.

This product must not be used for any prohibited purposes, including but not limited to:

- development or production of weapons of mass destruction
- chemical or biological weapons activities
- unsafe nuclear activities or nuclear fuel cycle misuse
- activities that violate human rights

In the event of any conflict between this manual and applicable law, the applicable law shall prevail.

FCC Information

Please note that any changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

FCC Compliance

This equipment has been tested and found to comply with the limits for a **Class A digital device**, pursuant to **Part 15 of the FCC Rules**. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

FCC Conditions

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

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

Safety Instructions

- Proper configuration of all passwords and security settings is the responsibility of the installer and/or end user.
- In the use of this product, you must comply with all applicable electrical safety regulations for your country and region.
- Firmly connect the power plug to the outlet. Do not connect multiple devices to a single power adapter.
  Always power off the device before connecting or disconnecting accessories and peripherals.
- **Danger:** Shock hazard. Disconnect all power sources before performing maintenance.
- The equipment must be connected to a properly grounded (earthed) mains outlet.
- The socket outlet should be installed near the equipment and remain easily accessible.
- ⚡ Indicates hazardous live voltage. External wiring connected to terminals must be installed by a qualified person.
- **Warning:** Do not install the equipment in an unstable location. The device may fall, causing serious injury or death.
- The input voltage must comply with **SELV (Safety Extra Low Voltage)** and **LPS (Limited Power Source)** requirements in accordance with **IEC 62368**.
- High leakage current. Ensure proper grounding before connecting to the power supply.
- If smoke, unusual odor, or abnormal noise is detected, immediately power off the device, unplug it, and contact technical support.
- For optimal performance, use the device with a UPS (Uninterruptible Power Supply) and manufacturer-recommended hard drives.
- This product contains a coin/button cell battery. If swallowed, it can cause severe internal burns within two hours and may result in death.
- This equipment is not suitable for use in locations where children are likely to be present.
- Risk of explosion if the battery is replaced with an incorrect type.
- Improper battery replacement may disable safety protections (especially for certain lithium battery types).
- Do not dispose of the battery in a fire or a hot oven. Do not crush, puncture, or cut the battery, as this may result in explosion.
- Do not expose the battery to extremely high temperatures, which may result in explosion or leakage of flammable substances.
- Do not expose the battery to extremely low air pressure, which may result in explosion or leakage of flammable substances.
- Dispose of used batteries in accordance with local regulations.
- Keep body parts away from moving components such as fan blades and motors. Disconnect the power source before servicing.

Preventive and Safety Guidelines

Before installing and operating this device, please review the following guidelines:

- This device is designed for **indoor use only**. Install it in a well-ventilated, dust-free environment away from liquids.
- Ensure the recorder is securely mounted on a rack or stable surface. Dropping or subjecting the unit to strong impacts may damage internal components.

- Do not expose the equipment to dripping or splashing liquids. Do not place objects filled with liquids (such as vases) on top of the device.
- Do not place open flame sources (such as lit candles) on or near the equipment.
- Do not obstruct ventilation openings. Avoid covering the device with materials such as newspapers, cloths, or curtains.
  Do not place the device on soft surfaces such as beds, sofas, or rugs that may block airflow.
- Maintain a minimum clearance of **200 mm (7.87 inches)** around the device to ensure proper ventilation.
- For applicable models, ensure correct wiring of terminals when connecting to an AC mains power supply.
- Certain models may be designed or configured for connection to an IT power distribution system. Verify compatibility before installation.
- The battery symbol indicates the battery holder and the correct polarity/positioning of the cell(s).
- The “+” and “–” symbols indicate the positive and negative terminals for direct current (DC) connections.
- Use only power supplies specified in this manual or provided by Inaxsys.
- The USB port is intended for connecting a mouse, keyboard, USB flash drive, or Wi-Fi dongle only.
- Avoid contact with sharp edges or corners of the equipment.