V1.0.0

Network Video Recorder

User's Manual

Foreword

General

This manual introduces the functions and operations of the network video recorder (hereinafter referred to as "the Device"). Read carefully before using the device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related

jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, and comply with the guidelines when using it.

Transportation Requirements

Transport the Device under allowed humidity and temperature conditions.

Storage Requirements

Store the Device under allowed humidity and temperature conditions.

Operation Requirements

- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Operate the Device within the rated range of power input and output.
- Do not disassemble the Device.
- Use the Device under allowed humidity and temperature conditions.
- Replace unwanted batteries with new batteries of the same type and model.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the device.
- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited to throw the battery into a fire or furnace, and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.

- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Install the Device on a stable surface to prevent it from falling.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- The device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the power requirements of the Device.
- When installing the Device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the Device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the Device casing.

Maintenance Requirements

The appliance coupler is a disconnection device. Keep it at a convenient angle when using it.

Table of Contents

1 Introduction

1.1 Overview

The Device is a high-performance network video recorder. It supports local live view, multichannel display, local storage of recorded files, and remote management and control function.

The Device works with network cameras, network video servers and other devices to form a strong surveillance network through the central management software. In the network system, data are transmitted through the network cable between the monitoring center and the monitored zone. You do not need to connect audio or video cables from the monitoring center to the monitored zone and can enjoy the benefits of simple connection and low maintenance costs.

The Device can be widely used in areas such as public security, water conservancy, transportation, and education.

1.2 Features

The actual functions might vary depending on the software and hardware version and the model you are using.

Real-time Surveillance

- Connects to monitor through VGA or HDMI port for real-time surveillance.
- Supports HDMI and VGA output at the same time.

Recording and Playback

- Supports recording and playing back videos of each channel.
- Supports slow play, fast play, backward play and frame by frame play for playback.

Smart Detection

- Supports face detection, VCA and intelligent motion detection.
- Supports search and playback of the smart detection records.

Alarm Linkage

Supports multiple alarm linkage actions in response to an alarm event, such as email, beep.

Online Update

Supports updating the program online.

Backup

Supports backup of logs, system configurations, recorded videos and snapshots, and more.

Network Surveillance

Supports network-based remote monitoring, remote playback and remote PTZ control

2 Unpacking

After receiving the Device, refer to the following table to verify nothing is missing or broken. If any issue occurs, contact our customer support.

Table 2-1 Checking list

No.	Item	Requirements
1	Package	• No visible damage. • Not distorted or broken. • Nothing missing.
2	Label	Not torn up. Keep the label well. You might need to provide the serial number on the label when calling the after-sales service.
3	Casing	• No visible damage. • No loose connection of the cables and mainboard. If cables are loose, contact our customer support.

3 Structure

This chapter introduces the front panel and rear panel of the Device.

3.1 Compact 1U

3.1.1 Front Panel

Figure 3-1 Front panel

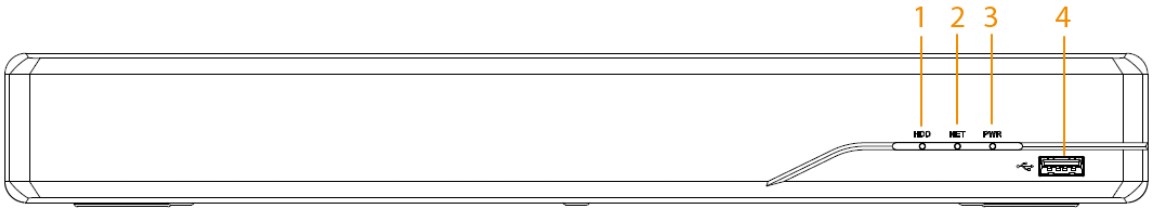


Table 3-1 Front panel description

No.	Name	Description
1	HDD indicator light	The light is solid blue when the HDD is abnormal.
2	Network indicator light	The light is solid blue when the network is abnormal.
3	Power indicator light	The light is solid blue when the power is connected properly.
4	USB port	Connects to peripheral devices such as USB storage device, keyboard, and mouse.

3.1.2 Rear Panel

Figure 3-2 Rear panel (4-PoE port)

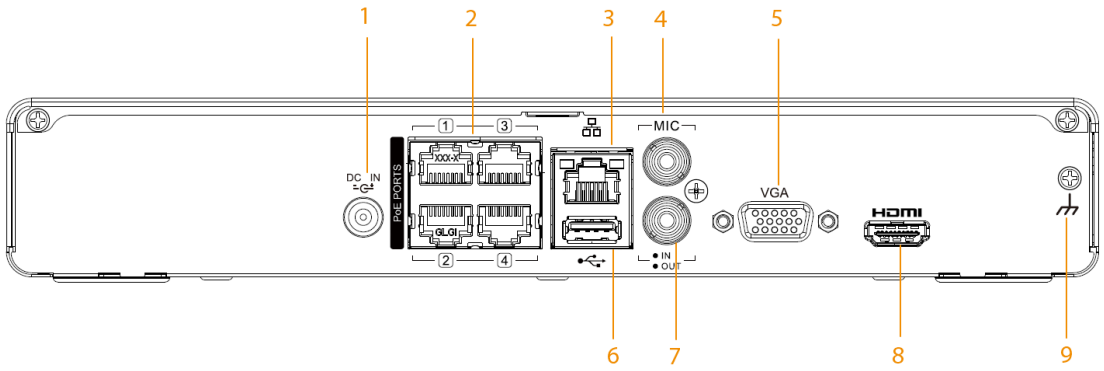


Figure 3-3 Rear panel (8-PoE port)

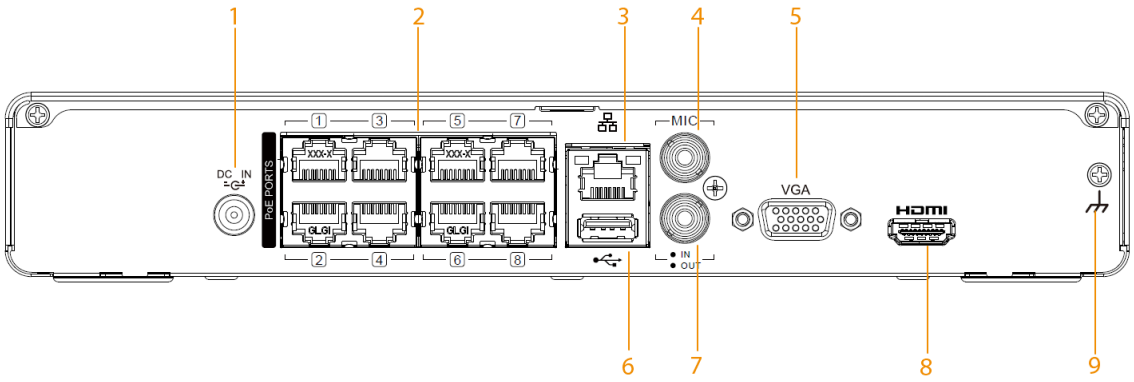


Table 3-2 Rear panel description

No.	Name	Description
1	Power input port	Inputs power.
2	PoE ports	Built-in switch. Support PoE function. You can use this port to provide power to the network camera.
3	Network port	Connects to the network cable.
4	Audio input port	Two-way talk input port which receives the audio signals from the devices such as microphone and pickup.
5	VGA port	Outputs analog video data to the connected display with VGA port.
6	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
7	Audio output port	Outputs the audio signals to the devices such as the sound box.
8	HDMI port	High Definition Media Interface. Transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device.

No.	Name	Description
9	Ground	—

3.2 Big 1U

3.2.1 Front Panel

Figure 3-4 Front panel

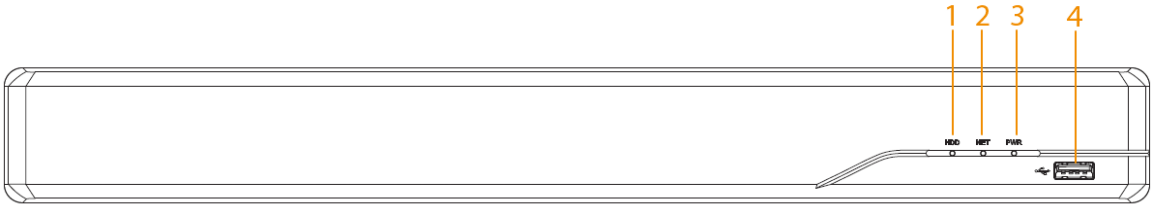


Table 3-3 Front panel description

No.	Name	Description
1	HDD indicator light	The light is solid blue when the HDD is abnormal.
2	Network indicator light	The light is solid blue when the network is abnormal.
3	Power indicator light	The light is solid blue when the power is connected properly.
4	USB port	Connects to peripheral devices such as USB storage device, keyboard, and mouse.

3.2.2 Rear Panel

Figure 3-5 Rear panel (8-PoE port)

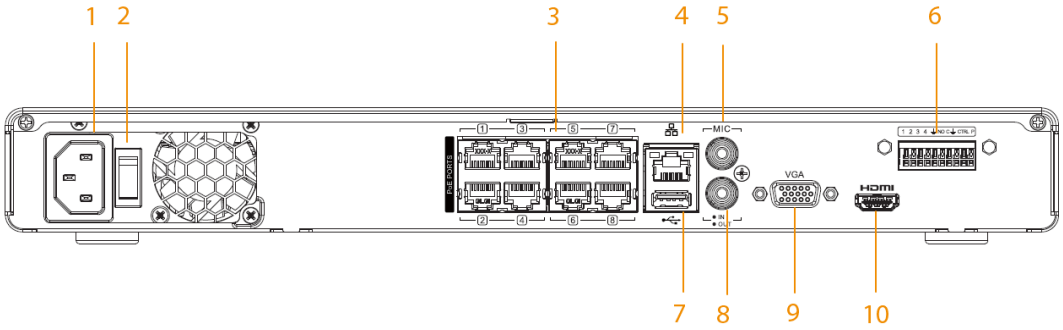


Figure 3-6 Rear panel (16-PoE port)

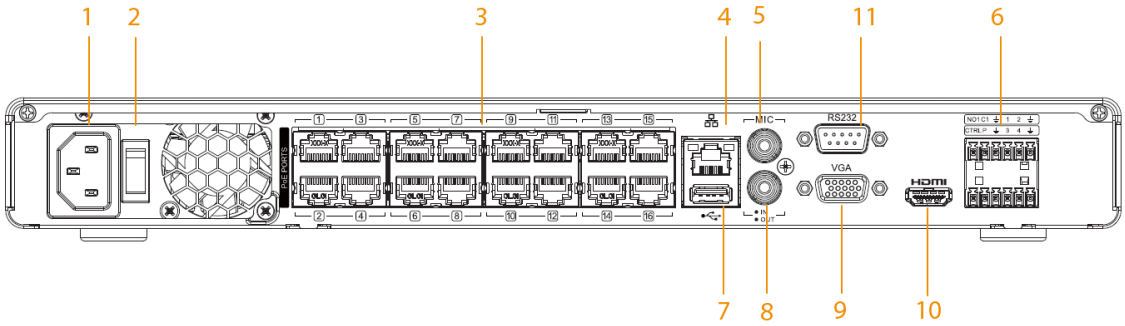


Table 3-4 Rear panel description

No.	Name	Description
1	Power input port	Inputs power.
2	Power switch	Turns on or off the Device.
3	PoE ports	Built-in switch. Support PoE function. You can use this port to provide power to the network camera.
4	Network port	Connects to the network cable.
5	Audio input port	Two-way talk input port which receives the audio signals from the devices such as microphone and pickup.
6	Alarm output ports	Output alarm signals to the alarm device. • NO: Normally open alarm output port. • C: Common alarm output port.
	CTRL (controllable 12 V power supply output)	Controls the output of the on-off button alarm relay. It controls the alarm device with the presence or absence of voltage. It can also be used as power input for some alarm devices such as alarm detectors.
	P (12 V power output port)	Provides power to some peripheral devices such as camera and alarm devices. Make sure the power supply of peripheral device is below 1 A.
	Alarm input ports 1–4	Receive signals from the external alarm source. When your alarm input device is using external power, make sure the device and the NVR have the same ground.
7	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
8	Audio output port	Outputs the audio signals to the devices such as the sound box.

No.	Name	Description
9	VGA port	Outputs analog video data to the connected display with VGA port.
10	HDMI port	High Definition Media Interface. Transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device.
11	RS-232 port	Use the port for general COM debugging to configure IP address or transfer transparent COM data.

4 Installation

This chapter introduces the installation and connection of the Device.

WARNING

Make sure to conform to your local safety rules while performing the operations.

4.1 Installing HDD

Before using the Device, check whether the HDD is already installed the Device. To install HDD, use the surveillance SATA hard drive recommended by the manufacturer.

WARNING

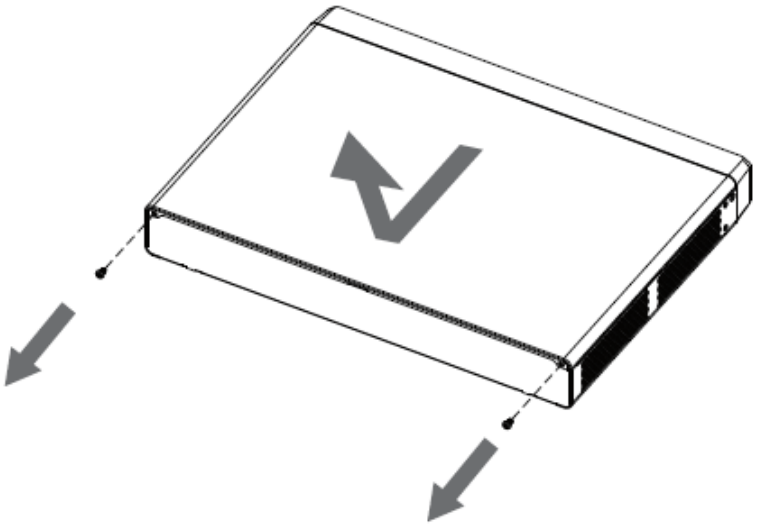
Before installing HDD, make sure to unplug the power cord and put on anti-static gloves.

4.1.1 Compact 1U

Procedure

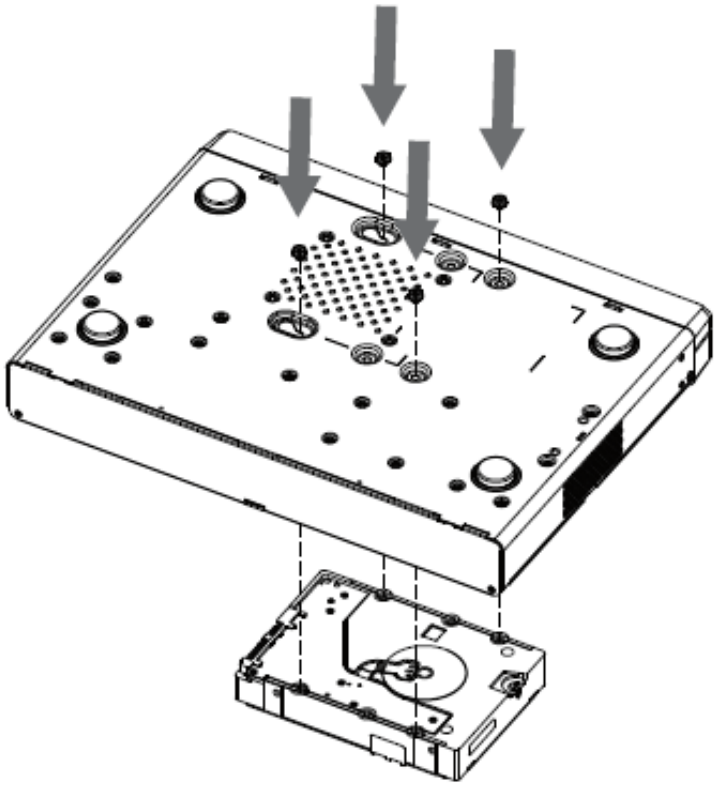
Step 1 Loosen the screws to remove the cover.

Figure 4-1 Remove cover



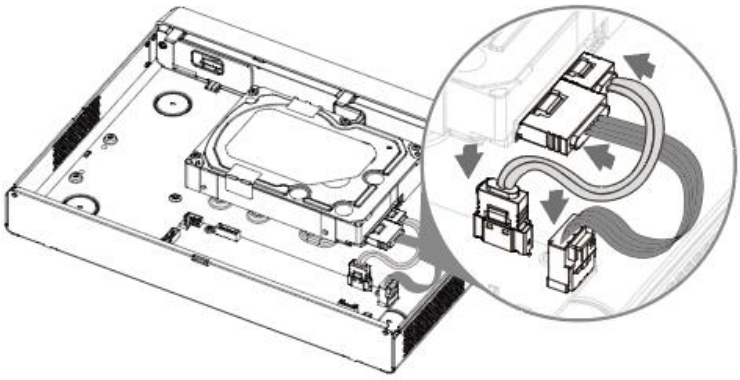
Step 2 Align 4 screw holes on the HDD with 4 holes on the Device and then tighten the screws.

Figure 4-2 Affix HDD



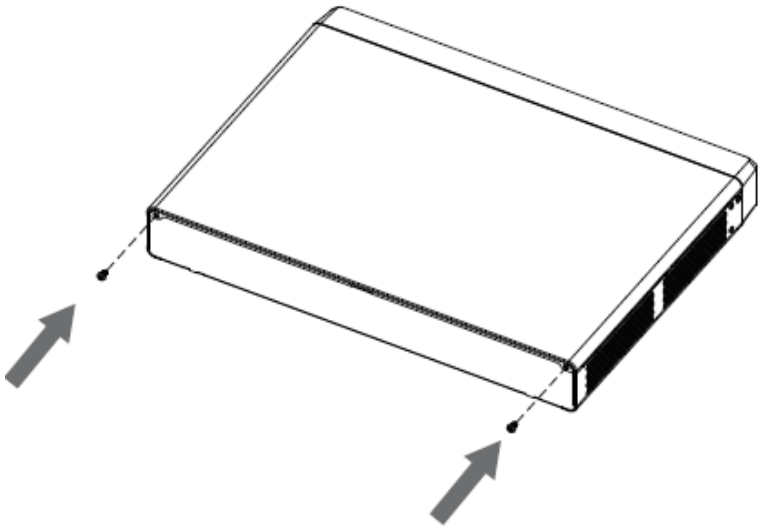
Step 3 Connect the data cable and power cord of the HDD to the Device.

Figure 4-3 Connect cables



Step 4 Put back the cover and then fasten the screws to re-attach the cover.

Figure 4-4 Re-attach the cover

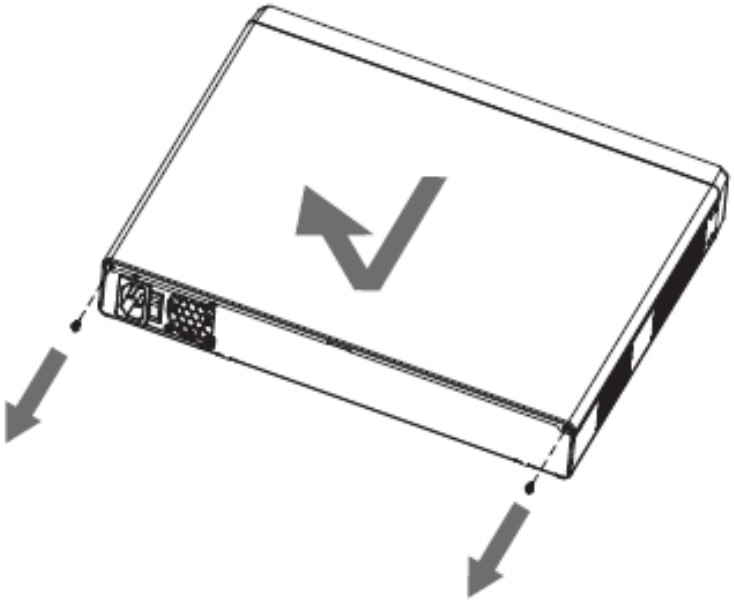


4.1.2 Big 1U

Procedure

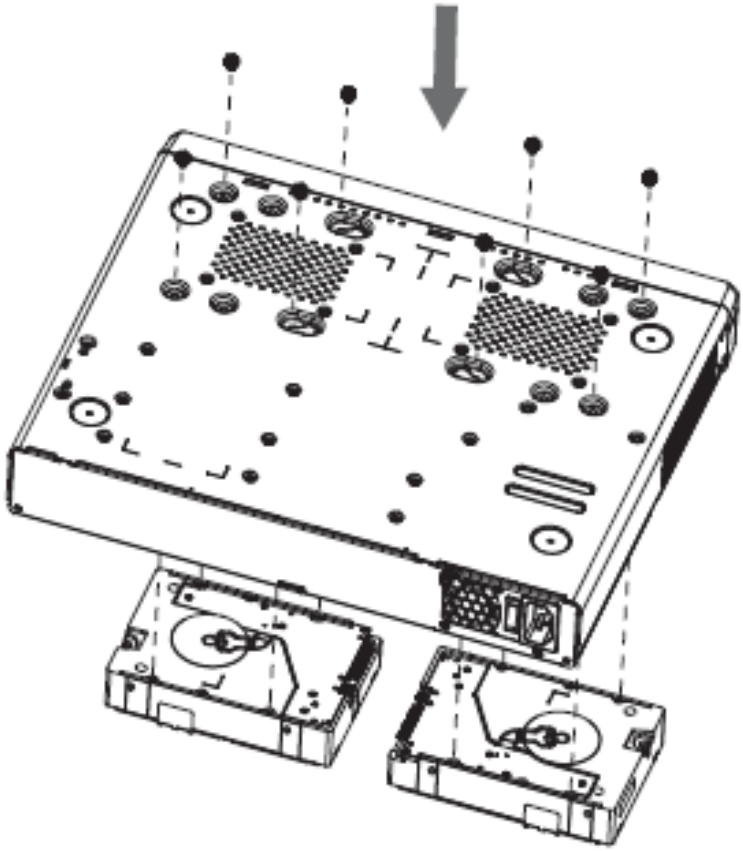
Step 1 Loosen the screws to take off the cover.

Figure 4-5 Take off cover



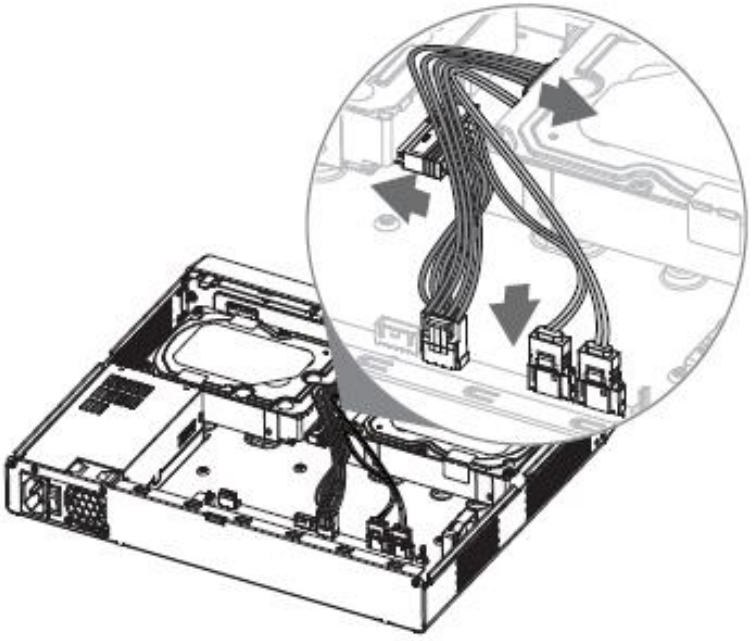
Step 2 Align the screw holes on the HDDs with the holes on the Device and then tighten the screws.

Figure 4-6 Affix HDD



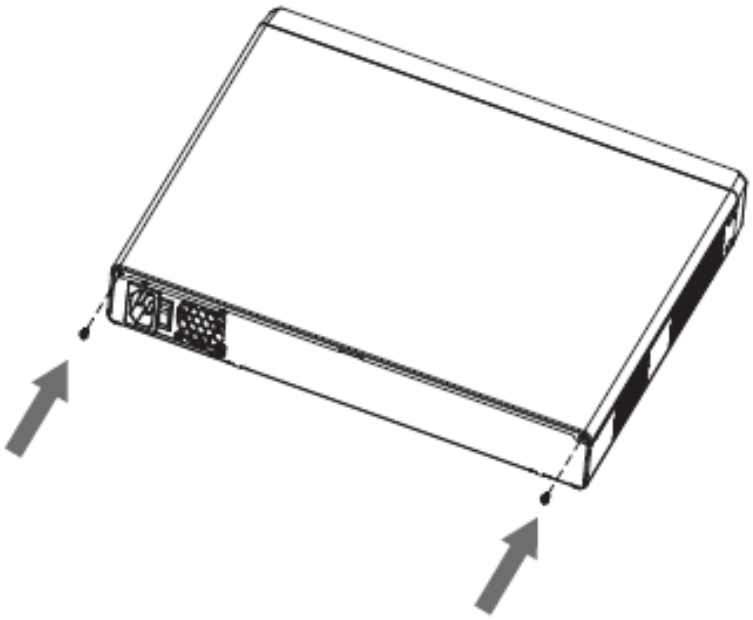
Step 3 Connect the data cable and power cord of the HDDs to the Device.

Figure 4-7 Connect cables



Step 4 Put back the cover and then fasten the screws to re-attach the cover.

Figure 4-8 Re-attach the cover



4.2 Connecting to Alarm Input and Output

4.2.1 Alarm Port Description

The following figure is for reference only. The number of alarm ports might differ depending on the model you are using.

Figure 4-9 Alarm ports

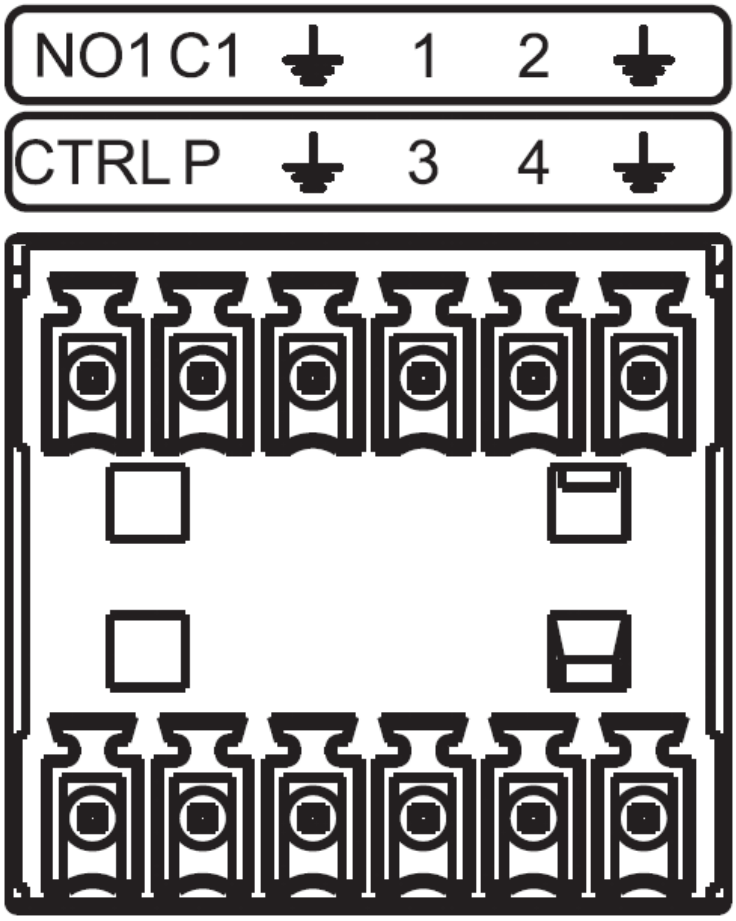


Table 4-1 Alarm port description

Icon	Description
1–4	Alarm input ports. The alarm becomes active in low level.
NO1 C1	Alarm output ports. • NO: Normally open port. • C: Common alarm output port.
⏚	Ground.
CTRL	Controllable 12 V power supply output. Disable power output when alarm is canceled.
P	Provides power to some peripheral devices such as camera and alarm devices. Make sure the power supply of peripheral device is below 1 A.

4.2.2 Alarm Input

- Connect the positive end (+) of the alarm input device to the alarm input port (ALARM IN 1–4) of the NVR.
- Connect the negative end (-) of the alarm input device to the ground end (⏚) of the NVR.

  ◇ When connecting the ground port of the alarm device to the NVR, you can use any of

the GND ports (⏚).

- ◇ Connect the NC port of the alarm device to the alarm input port (ALARM) of the NVR.
- ◇ When there is peripheral power supplying for the alarm device, please make sure it is earthed with the NVR.

4.2.3 Alarm Output

- Provide external power to external alarm device.
- To avoid overloading, read the following relay parameters carefully.
- RS-485 A/B cable is for the A/B cable of the PTZ decoder.

The parameters are for reference only.

Table 4-2 Alarm relay specifications

Model	**Model**	**HFD23/005-1ZS**	**HRB1-S-DC5V**
Material of the touch		AgNi + gold-plating	AuAg10/AgNi10/CuNi30
Rating (Resistance Load)	Rated switch capacity	30 VDC, 1 A/125 VAC, 0.5 A	24 VDC, 1 A/125 VAC, 2 A
	Maximum switch power	62.5 VAC/30 W	250 VAC/48 W
	Maximum switch voltage	125 VAC/60 VDC	125 VAC/60 VDC
	Maximum switch currency	2 A	2 A
Insulation	Between touches	400 VAC, 1 minute	500 VAC, 1 minute
	Between touch and winding	1000 VAC, 1 minute	1000 VAC, 1 minute
Turn-on Time		5 ms maximum	5 ms maximum
Turn-off Time		5 ms maximum	5 ms maximum
Longevity	Mechanical	1 × 107 times (300 times/minute)	5 × 106 times (300 times/minute)
	Electrical	1 × 105 times (30 times/minute)	2.5 × 104 times (30 times/minute)
Working Temperature		-30 °C to +70 °C	-40 °C to +70 °C

5 Local Operations

The figures are for reference only and might differ from the actual interface.

5.1 Starting the Device

Prerequisites

- Make sure that the input voltage complies with the power requirements of the Device.
- To ensure the stable work of the Device and prolong the HDD life, follow related standards to use a power source that provides stable voltage with less interference from ripples. UPS power source is recommended.
- Make sure to connect the Device with the power adapter first, and then connect it to the power supply.

Procedure

Step 1 Connect the Device to the monitor, and then connect a mouse.

Step 2 Connect the power cord, and then turn on the power switch.

5.2 Initialization

Background Information

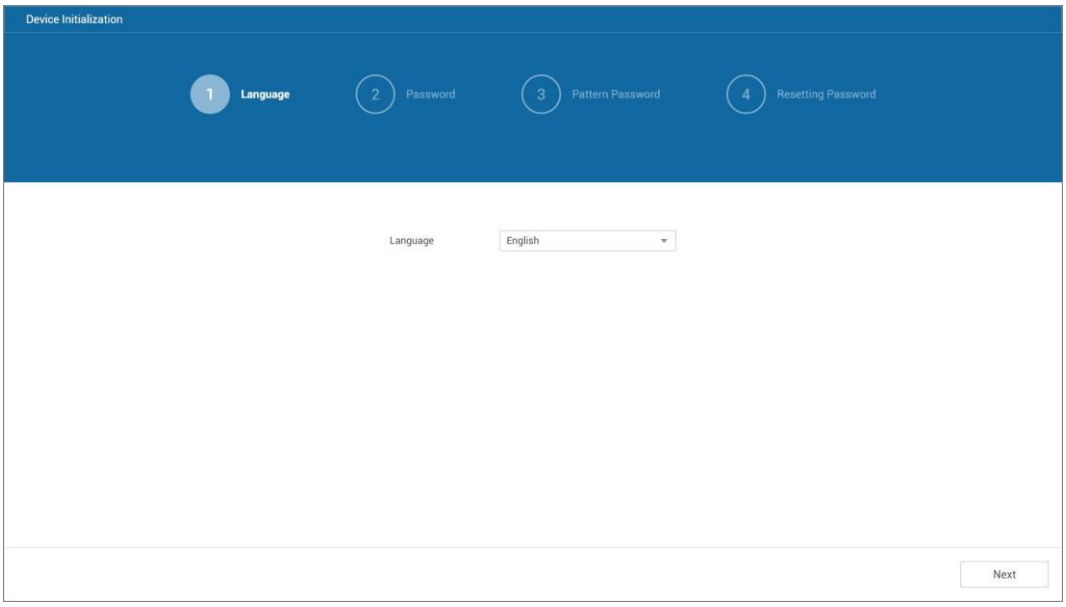
For first-time use, you need to configure the password and related protection for the default admin account.

For device security, we strongly recommend you properly keep the admin password and change it regularly.

Procedure

Step 1 Turn on the Device, select the language, and then click **Next**.

Figure 5-1 Select language



Step 2 Configure the password for admin, and then click **Next**.

Figure 5-2 Password setting

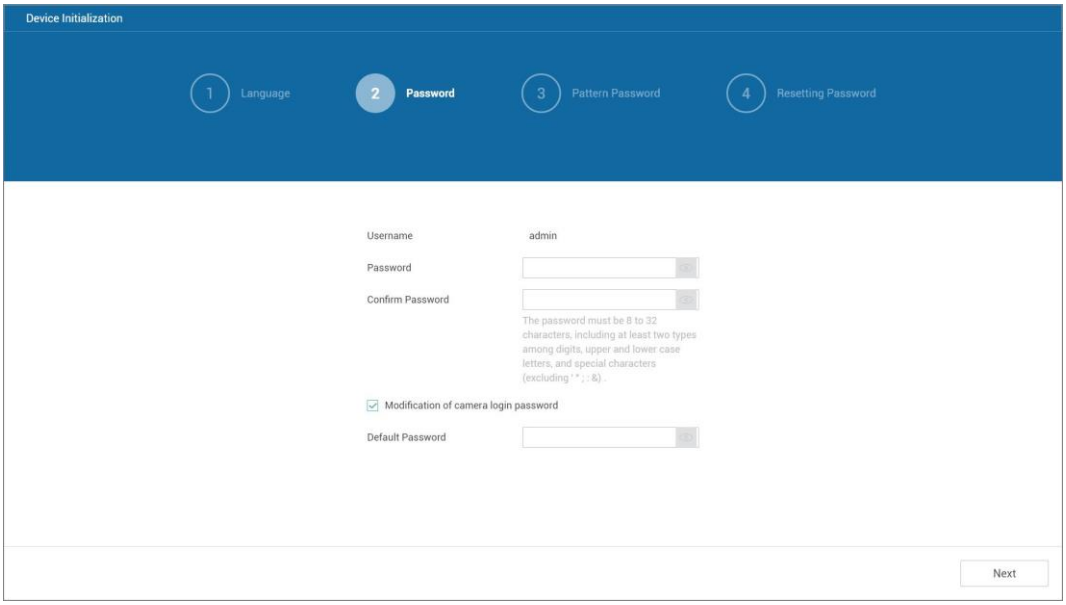


Table 5-1 Password parameters

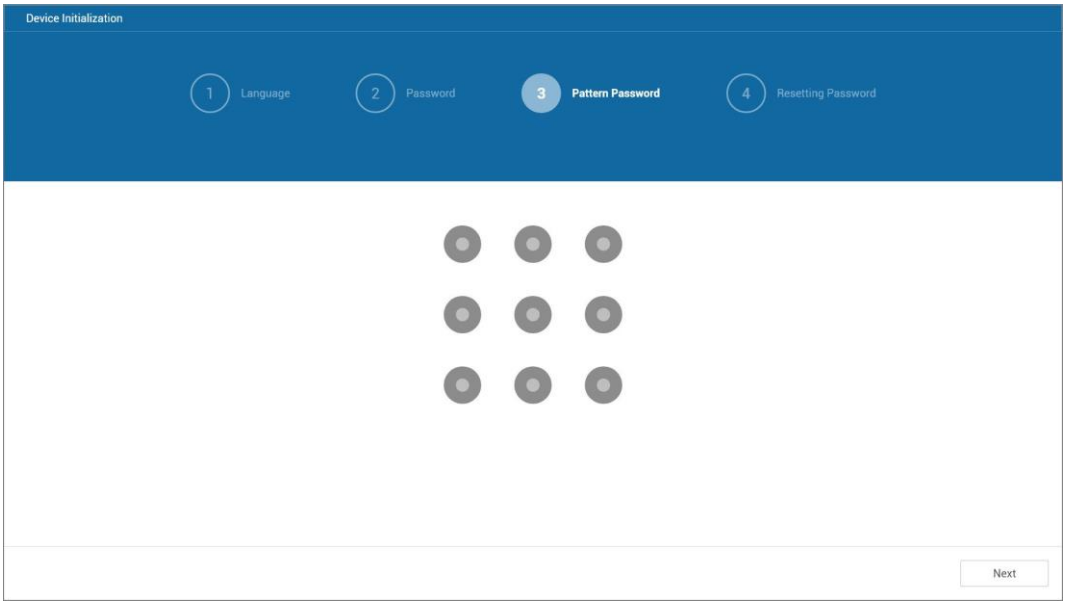
Parameter	Description
Username	The username is admin by default.
Password	Enter and then confirm the password.
Confirm Password	
Default Password	Click **Modification of camera login password** to configure the default password for adding the camera.
Modification of camera login password	

Step 3 Set unlock pattern.

- The pattern that you want to set must cross at least four points.
- If you do not want to configure the unlock pattern, click **Next**.

- Once you have configured the unlock pattern, the system will require the unlock pattern as the default login method. If you did not configure the unlock pattern, you need to enter password for login.

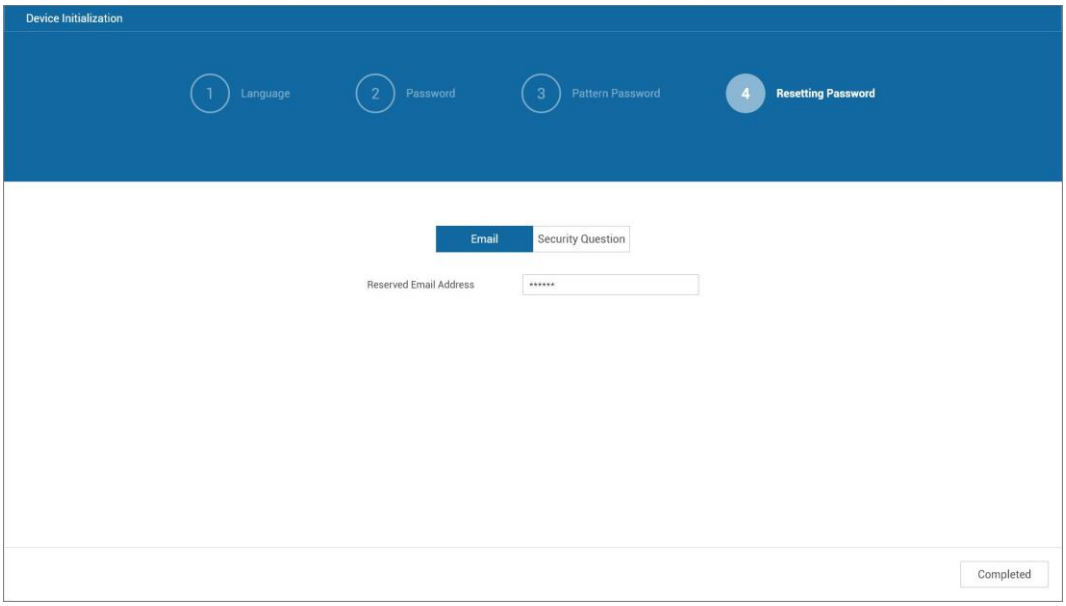
Figure 5-3 Draw unlock pattern



Step 4 Configure the password protection information.

- Reserved email address.
  In the **Reserved Email Address** box, enter your email address. If you forget the password, you can use the email address to get the security code needed for password resetting.
- Security questions.
  Select security questions and enter the corresponding answers. If you forget the password, enter the correct answers to the questions and then you can reset the password.

Figure 5-4 Password protection



Step 5 Click **Completed**.

The **Setup Wizard** window appears.

5.3 Setup Wizard

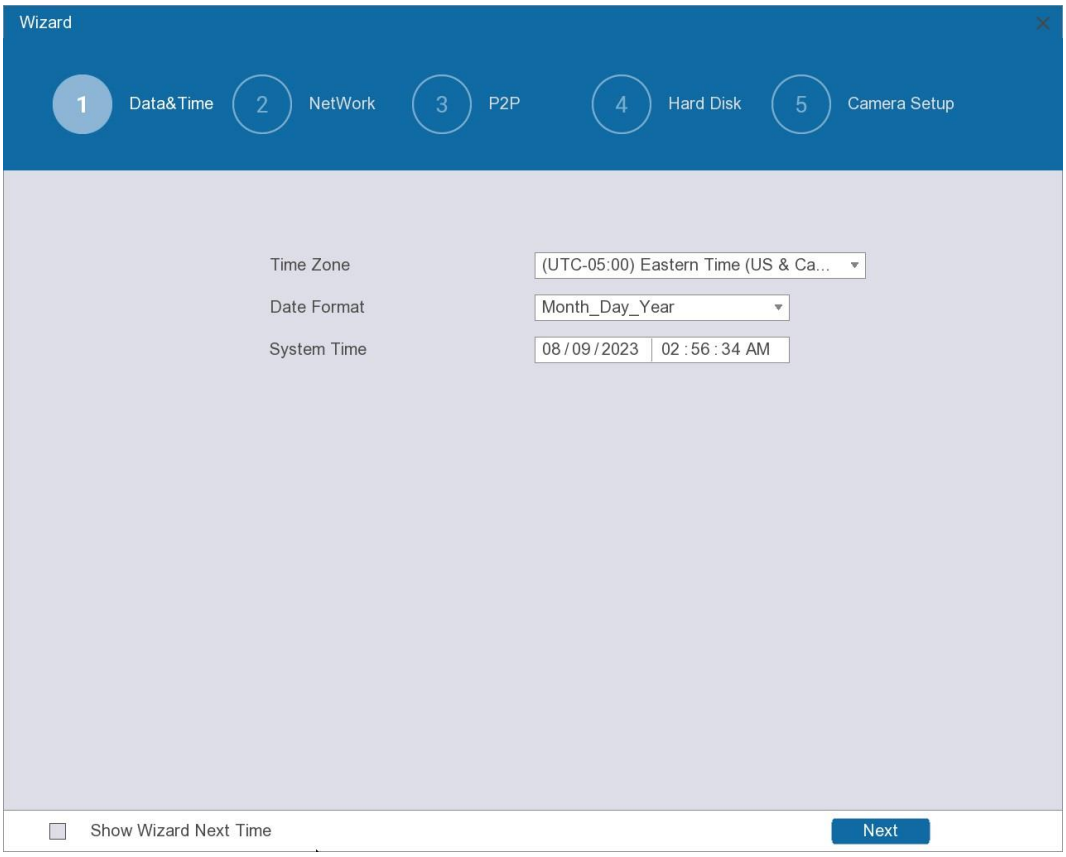
Follow the setup wizard to complete basic settings.

Procedure

Step 1 Configure data and time, and then click **Next**.

You can select the time zone and data format, and set the system time.

Figure 5-5 Data and time



When you click the checkbox next to **Show Wizard Next Time**, the wizard page will appear again when the Device restarts.

Step 2 Configure network settings, and then click **Next**.

Figure 5-6 Network settings

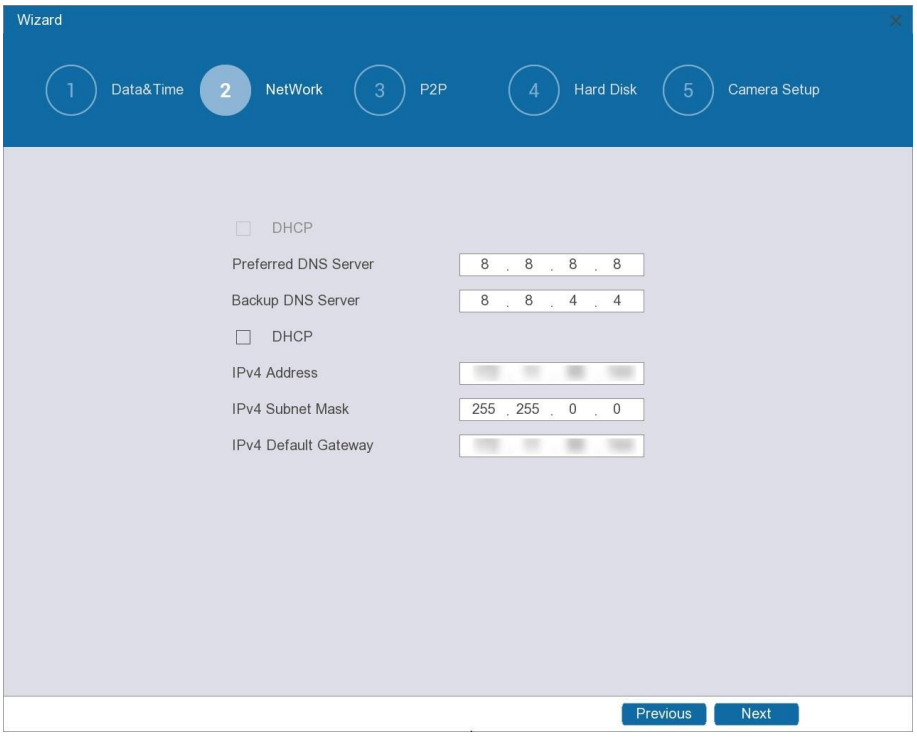


Table 5-2 Network parameters

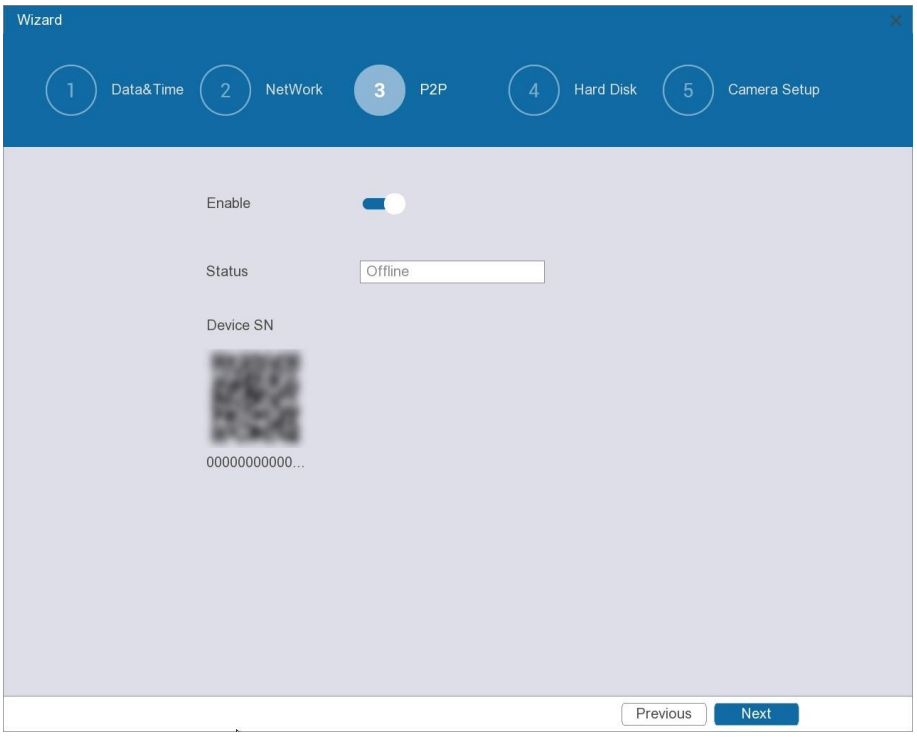
Parameter	Description
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to set IP address manually. • The first DHCP is for the DNS server. • The second DHCP is for the Device. Select the checkbox next to **DHCP** for IPv4, and then you can choose to enable or disable **DHCP** for DNS server.
Preferred DNS Server	Set preferred and backup DNS server address.
Backup DNS Server	
IPv4 Address	Enter the IPv4 address and configure the corresponding subnet mask and default gateway. The IPv4 address and the IPv4 default gateway must be on the same network segment.
IPv4 Subnet Mask	
IPv4 Default Gateway	

Step 3 Enable the P2P function, and then click **Next**.

You can use the mobile client to scan the QR code under **Device SN** to add the Device for remote management.

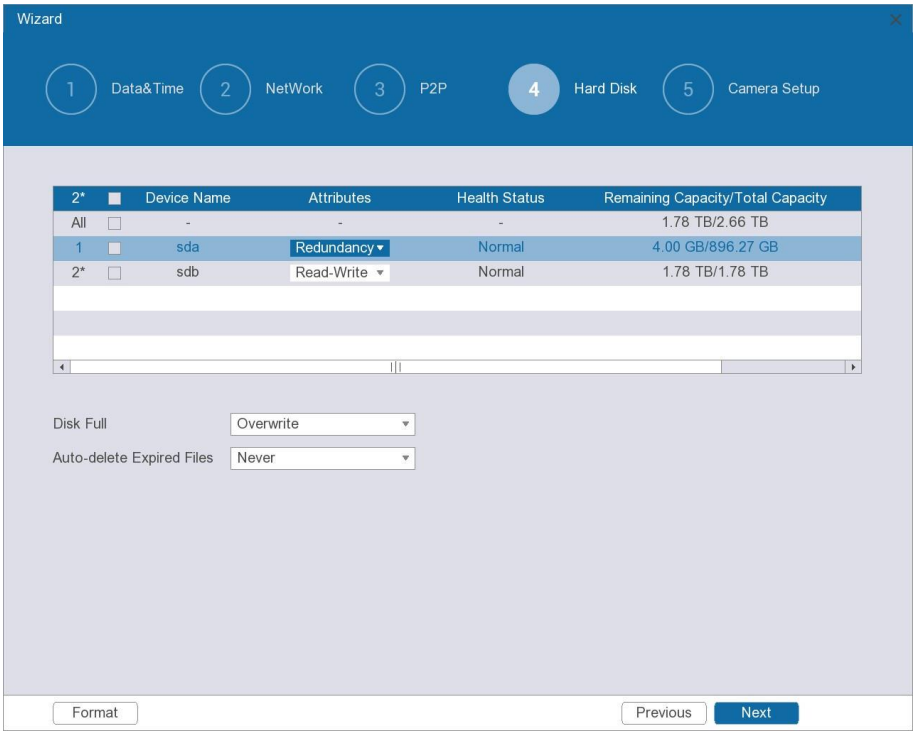
After you enable the P2P function and connect to the Internet, the system will collect the information such as email address and MAC address for remote access.

Figure 5-7 P2P



Step 4 On the disk list, view the HDD information and configure the HDD type, configure the storage strategy, and then click **Next**.

Figure 5-8 Hard disk



- Set HDD type.
  In the **Attributes** column, select **Read-Write**, **Read-only** or **Redundancy** to set the HDD type.
- Format HDD.
  Select an HDD, click **Format**, and then follow the on-screen prompt to format the HDD.

Formatting will erase all data on the HDD. Proceed with caution.

- Configure **Disk Full** and **Auto-delete Expired Files**.

Table 5-3 Disk management parameters

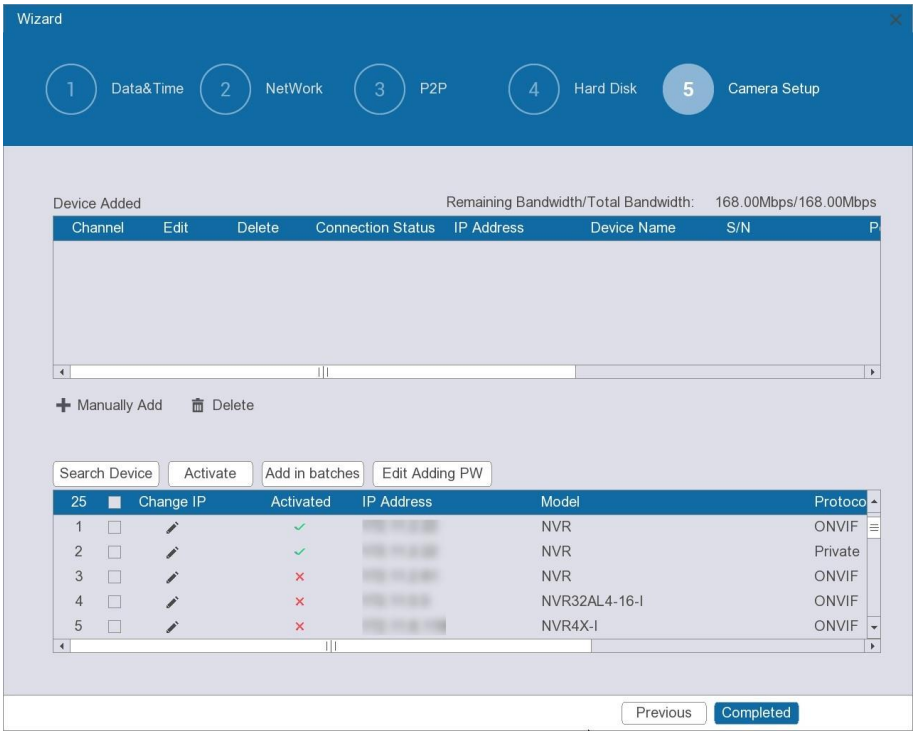
Parameter	Description
Disk Full	Configure the storage strategy to be used when no more storage space is available. • Stop: Stop Recording. • Overwrite: The newest files overwrite the oldest ones.
Auto-delete Expired Files	Configure whether to allow the Device to delete expired automatically. • Select **Never** if you do not want to use the function. • Select **Custom** and then configure how long you want to keep the old files.

Step 5 Connect remote devices.

You can add remote devices from search or add remote devices manually. This section uses adding from search as an example.

1) Click **Search Device**.
2) Select one or more remote devices from the search results, and then click **Add in batches**.
   You can view the added devices on the page.

Figure 5-9 Remote device



Step 6 Click **Completed**.

5.4 Login

Log in to the Device for more operations.

Procedure

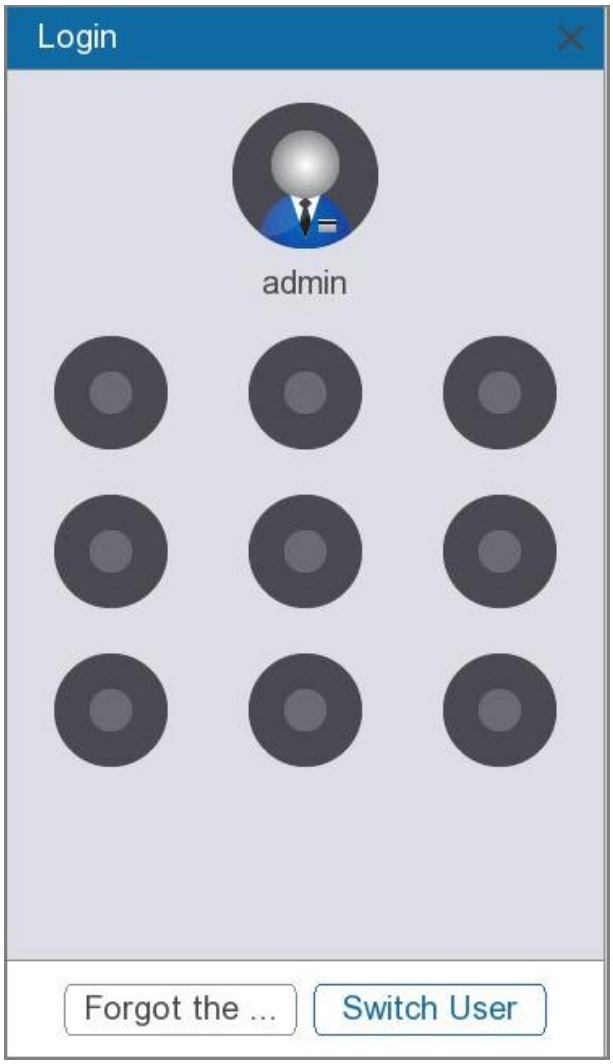
Step 1 Click the live page.

- If you have configured unlock pattern, the unlock pattern login window is displayed. Click **Forgot the Pattern** to switch to password login.
- If you did not configure unlock pattern, the password login window is displayed.
- You can click **Switch User** to enter the password login window.

Step 2 Log in to the Device.

- Draw the unlock pattern.

Figure 5-10 Unlock pattern login



- Enter the password, and then Click **OK**.

Figure 5-11 Password login

If you forget your password, click to reset the password.

5.5 Live View

On the live view page, you can view the video images of different channels.

Select a window, double-click a channel in the channel list, and then the channel will be displayed in the selected window.

The number of channels might vary depending on the model you are using.

5.5.1 Live View Control Bar

Point to the bottom middle of a channel window, and then the live control bar appears. Through the control bar, you can perform the operations such as instant playback, local zoom, manual snapshot, intercom, stream switching, and PTZ control.

Figure 5-12 Live view control bar

Table 5-4 Live view control bar description

Icon	Function	Description
	Instant playback	You can play back the previous five minutes to sixty minutes of the recorded video. Go to **System** > **General** > **Basic Configuration** to configure the length of time for instant playback.

Icon	Function	Description
	Local zoom	• Click the icon, and then select an area. The area is enlarged after you release the mouse button. • Point to the area that you want to enlarge or shrink and then scroll the mouse to zoom in or zoom out. Right-click the channel window to return to the original status.
	Manual snapshot	Take snapshots of the current video channel. The snapshots are automatically saved to the connected USB storage device.
	Intercom	Enables voice interaction between the Device and remote devices. This function is available only when the remote device supports bidirectional talk.
	Stream switching	Switch between the main stream and sub stream. • M: Main stream. Suitable for local recording and storage to achieve high-definition surveillance. • S: Sub stream. Suitable for network transmission when network bandwidth is limited.
	PTZ Control	Open the PTZ Settings window.

5.5.2 Navigation Bar

At the bottom right side of the live page, you can access the functions to perform operations through the function icons on the navigation bar.

Figure 5-13 Navigation bar

Table 5-5 Navigation bar description

Icon	Description
>	Go to the next screen.
<	Go to the previous screen.
	Select view split mode.
	Enable or disable auto switch.
	Click the icon, and you can enter the full screen mode.

Icon	Description
	Click the icon, and you can restore the sequence of channel windows.

5.5.3 Shortcut Menu

Right-click the live page, and then the shortcut menu appears. You can enter into the full screen mode, and then select a view split mode.

Figure 5-14 Shortcut menu

5.5.4 PTZ

PTZ is a mechanical platform that carries a camera and a protective cover and performs overall control remotely. A PTZ can move horizontally and vertically to provide all-around view to the camera.

5.5.4.1 Operating PTZ Control Panel

You can click  on the live view control bar, and the PTZ control panel appears.

Figure 5-15 PTZ control panel

Table 5-6 PTZ control panel description

Parameter	Description
Step	The bigger the value, the faster the PTZ movement speed.
Zoom	•  : Zoom out. •  : Zoom in.

Parameter	Description
Focus	• : Focus far. • : Focus near.
Iris	• : Image darker. • : Image brighter.
	Fast positioning button. • Positioning: Click the icon, and the click any point on the live page. The PTZ will turn to this point and locate this point in the center. • Zooming: Click the icon, and then drag to draw a square on the view. The square supports zooming. ◇ Dragging upward is to zoom out, and dragging downward is to zoom in. ◇ The smaller the square, the larger the zoom effect. This function is available on select models.
	Enable direction control through mouse operation.
	Enable the preset point.
	Enable the patrol group.
	Click the icon, and you can set parameters of **Preset Point** and **Patrol Group**.

5.5.4.2 Configuring PTZ Functions

5.5.4.2.1 Configuring Presets

Procedure

Step 1 On the PTZ control panel, click , and then select **Preset Point**.

Figure 5-16 Preset

Step 2 Click the direction arrows to rotate the camera to a desired position.

Step 3 Enter a number to represent the preset point.

Step 4 Click **Set** to complete settings.

5.5.4.2.2 Configuring Patrol Group

Procedure

Step 1 On the PTZ control panel, click , and then select **Patrol Group**.

Step 2 Click the direction arrows to rotate the camera to a desired position.

Step 3 Enter a patrol number.

Step 4 Enter a number for the preset point, and then click **Set**.

A preset point is set for this patrol. You can continue to set more presets.

Click **Delete Preset** to delete the preset. Some protocols do not support deleting.

5.5.4.3 Using PTZ Functions

After you have configured the PTZ settings, you can use the PTZ functions from the PTZ control panel.

5.5.4.3.1 Using Presets

Procedure

Step 1 On the PTZ control panel, in the **Execute** box, enter the preset number.

Step 2 Click to call the preset.

Step 3 Click again to stop calling.

5.5.4.3.2 Using Patrol Groups

Procedure

Step 1 On the PTZ control panel, in the **Execute** box, enter the patrol number.

Step 2 Click to call the patrol group.

Step 3 Click again to stop calling.

5.6 Main Menu

After logging in, you can directly see the **Live** page, and you can select tiles in the top middle of the **Live** page as required to enter the corresponding configuration pages.

Figure 5-17 Main menu

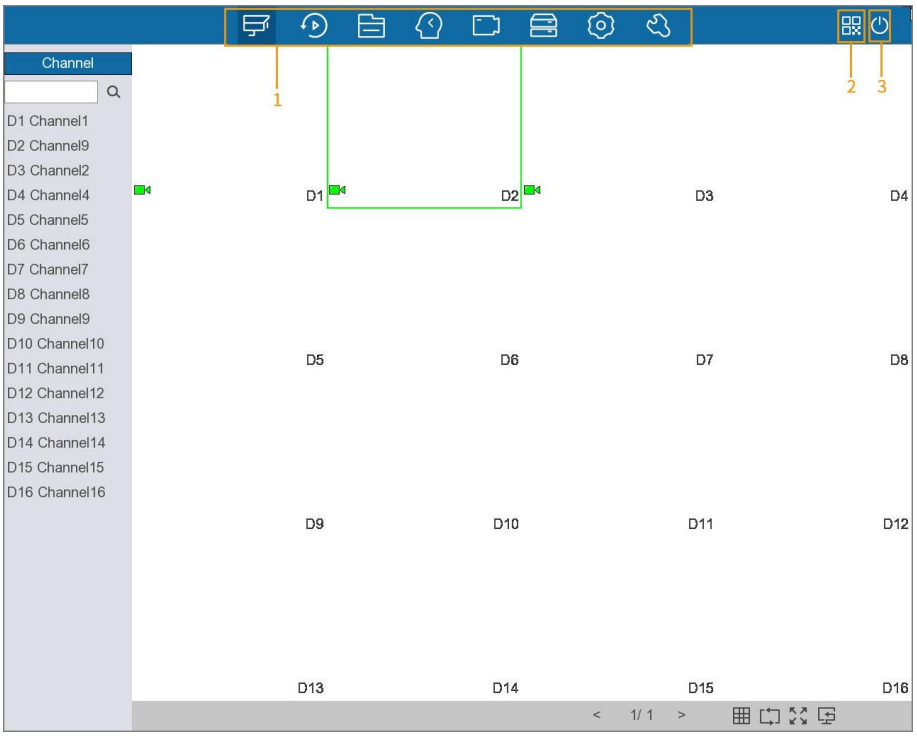


Table 5-7 Main menu description

No.	Name	Description
1	Function tiles	Click the selected tile to open the corresponding configuration page.
2	QR code	Scan the QR code under to add the Device for remote management.
3	Shutdown	Log out of the current account, restart or shut down the Device.

5.7 Playback

5.7.1 Instant Playback

You can quickly view the recorded video of previous 5 to 60 minutes from the live view control bar. For details on instant playback, see "5.5.1 Live View Control Bar".

5.7.2 Playback Page

Click **Playback**. The **Playback** page is displayed.

The following figure is for reference only.

Figure 5-18 Playback

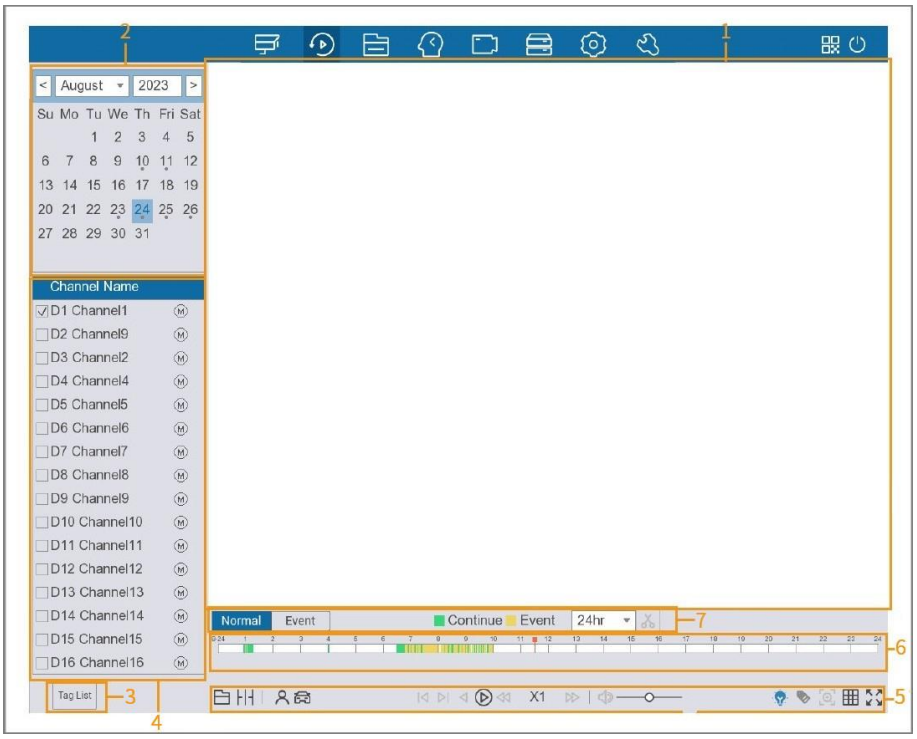


Table 5-8 Playback page description

No.	Function	Description
1	Display window	Displays the recorded video. It supports playing in single-channel or multi-channel mode. • The display window defaults to displaying in the single-channel mode. • Click to split the display window as required. • When playing back in the single-channel mode, click and hold to select an area that you want to enlarge, and then release to enlarge the selected area. To exit the enlarged status, right-click on the image.
2	Calendar	Select the search time. The selected date is highlighted. appears below the date with the recorded video.
3	Tag list	View and manage the tagged videos found after search.

No.	Function	Description
4	Channel list	On the channel list, select one or more channels to play back. • The window split is decided by the number of selected channels. If you select one channel, the playback is displayed in the single-channel view; if you select two to four channels, the playback is displayed in the four-channel view. • Click Ⓜ or Ⓢ switch the streams. ◇ Ⓜ: Main stream. ◇ Ⓢ: Sub stream.
5	Playback controls bar	Playback control buttons. See "5.7.3 Playback Controls" for detailed information.
6	Time Bar	Displays the type and time period of the current recorded video. • In the 4-channel layout, four time bars are displayed; in the other view layouts, only one time bar is displayed. • Click the colored area to start playback from a certain time. • Scroll on the time bar, and then the time bar zooms in. • Click and hold the time bar. When the mouse pointer changes to a hand icon, you can drag to view the playback of the target time. • You can drag the vertical line on the time bar to rapidly view the playback in I-frame format. • When playing back video in the single-channel mode, you can point to time bar to display thumbnail images for the current video.
7	Record type	Select the recording type to search for. • Normal displays all recordings. Green represents general recordings on the time bar. • Event displays motion recordings, alarm recordings, and smart recordings. Yellow represents event recordings on the time bar.
	Time bar unit	Select **24hr**, **2hr**, **1hr**, or **30min** as the unit of time bar.
	Clip	Click ✂ to clip the recorded recording and then save specified footages.

5.7.3 Playback Controls

You can search for and play back videos, images or video clips. The operations are similar. This section uses video playback as an example.

Procedure

Step 1 Select **Playback**, and then click to play the recording from the external device.

Step 2 Select the **Normal** or **Event** as the search type.

Step 3 Select the date, channel.

Step 4 Click or any position on the time bar.

The system starts playback. You can operate the playback controls to control the playback process.

Figure 5-19 Playback controls

Table 5-9 Playback controls description

Icon	Function
	Click the icon to play the recording from the external device. Click to exit the current playback mode.
	Click the icon to split the recordings of one day as required, and then display them on the display window. Click to exit the current playback mode.
	Select a target type for smart playback. You can select **Human** or **Vehicle**.
	Displays previous frame/next frame. • When the playback is paused, click or to play back the video frame by frame. • In frame by frame playback mode, click to resume normal playback mode.
	Rewind. • In normal play mode, click the icon the rewind the video. • In rewinding mode, click to resume normal playback mode.
	Click the icon the play the video. Click again to stop.
	Stop the current playback process.
	Slow playback. • In normal playback mode, click the icon to set the speed of slow playback. • In fast playback mode, click the icon to slow down the speed of fast playback.

Icon	Function
	Fast playback. • In normal playback mode, click the icon to set the speed of fast playback. • In slow playback mode, click the icon to speed up slow playback.
	Adjust the volume of playback video.
	Click the icon to display or hide AI rules.
	Click the icon to tag the video.
	Click the icon to enable smart playback.
	Click the icon to display 1, 4, 9 or 16 videos on the display window.
	Click the icon to enter the full screen mode.

5.7.4 Quick Search

When playing back videos, the Device can detect motion event in the defined region on the video image. The system will display the video footages with motion events.

Prerequisites

Go to **System** > **Video Detection** > **Motion Detection** to enable motion detection.

Procedure

Step 1 Select **Playback**.

Step 2 Set the search conditions and play back the video of a channel. For details, see "5.7.3 Playback Controls".

Smart playback is available only in the single-channel mode. If you select multiple channels, double-click the channel window to display this channel only on the screen.

Step 3 Click 

Step 4 Set the detection area.

Step 5 Click  to view the video footages with motion detected.

Step 6 Click  again to display all recordings.

- The motion detection area must not be the full screen.
- You cannot change the time bar unit, play backward, or play frame by frame are null when the Device is playing motion detection footages.

5.7.5 Clip

During playback, you can clip sections of videos and save to the USB storage device.

Procedure

Step 1 Select **Playback**.

Step 2 Set the search criteria and play back video. For details, see "5.7.3 Playback Controls".

Step 3 Click the time bar to select the start time, and then click .

Step 4 Click the time bar to select the end time, and then click .

Step 5 Click to save the file.

5.7.6 Tag Playback

When you are playing back a video, you can add a tag to mark an important point in time of the video. After playback, you can use time or the tag keywords to search for the corresponding video and then play.

Adding Tag

When system is playing back, click , and then configure the tag name.

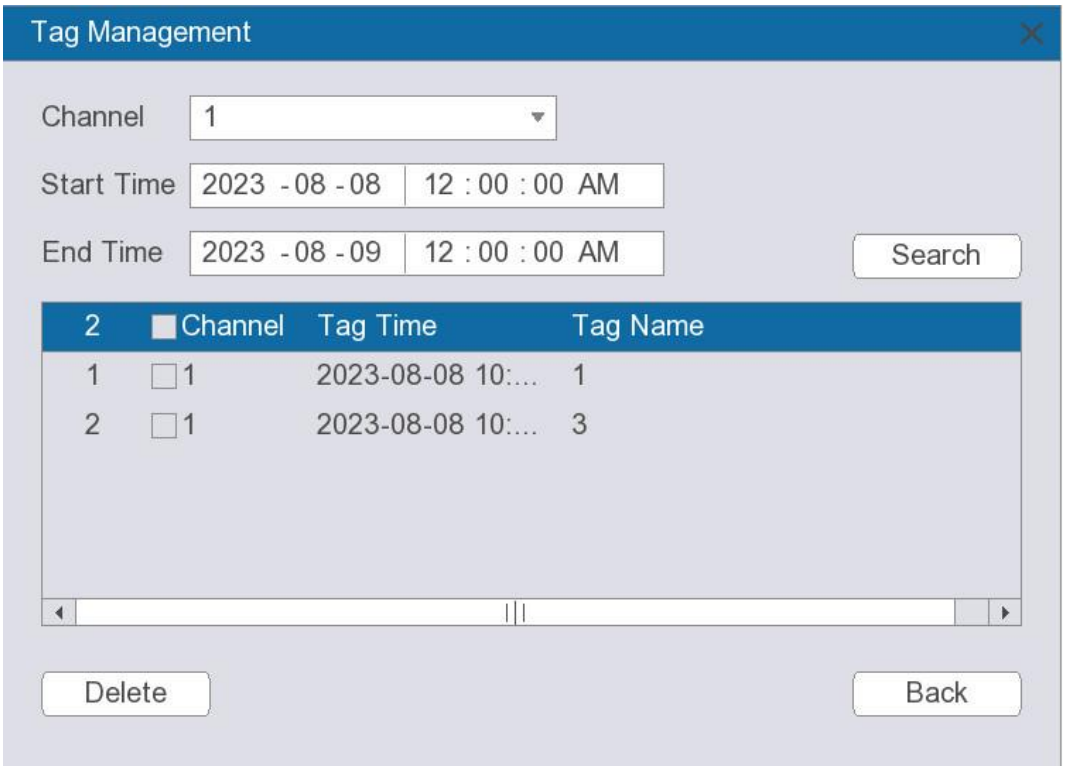
Playing back Tag

During single-channel playback, click Tag List, and then on the tag list, double-click a file to play back.

Managing Tags

On the tag list, click .

Figure 5-20 Tag management



- To search for the tagged video, select channel number, start time and end time, and then click **Search**.
- To change the tag name, double-click a tagged video, and then enter the new name.
- To delete tags, select one or more tagged videos, and then click **Delete**.

5.8 File Search

You can search videos, pictures, and smart events.

5.8.1 Searching for Video

Procedure

Step 1 Select **File Search** > **Video**, and then select **Search by Time** or **Search by Event** as required.

Step 2 Set parameters, and then click **Search**.

You can click **Clear** to clear the completed information.

The search results are displayed on the bottom of the page, and you can back up them.

Figure 5-21 Search by event

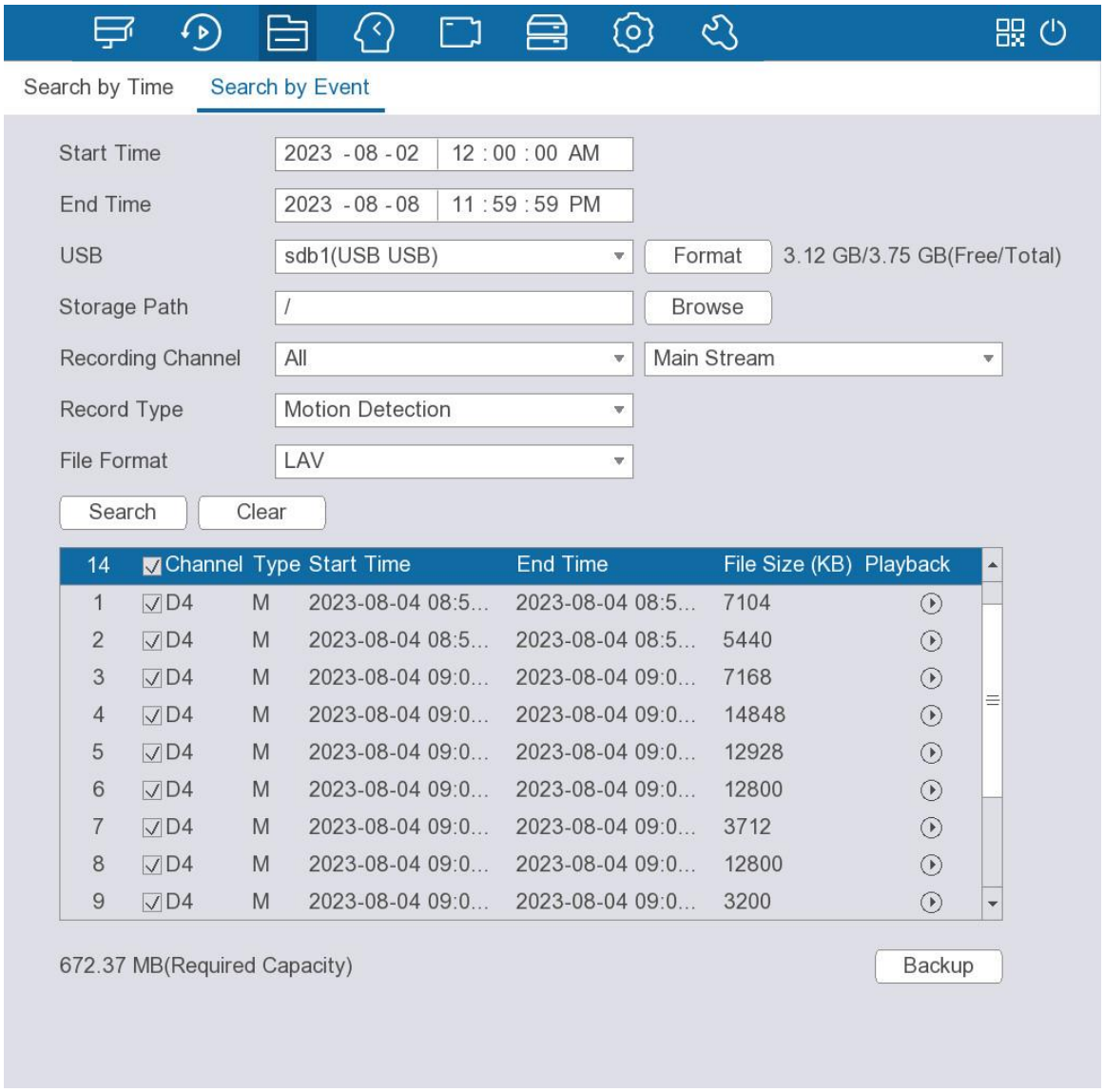


Table 5-10 Video search parameters

Parameter	Description
Start Time	Configure the start time and end time for the video search.
End Time	
USB	Select a USB from the drop-down list. Click **Format** to format the USB.
Storage Path	Click **Browse** to select the storage path.
Recording Channel	Select the recording channel, and then select **Main Stream** or **Sub Stream** as required.
Record Type	Select the record type as required. Supports selecting **All**, **External Alarms**, **Motion Detection**, **Continues Recording**, or **VCA**.

Parameter	Description
File Format	Select the file format as required. Supports selecting **LAV** or **MP4**.

5.8.2 Searching for Picture

Procedure

Step 1 Select **File Search** > **Picture**.

Step 2 Set parameters, and then click **Search**.

You can click **Clear** to clear the completed information.

The search results are displayed on the bottom of the page, and you can back up them.

Figure 5-22 Search for picture

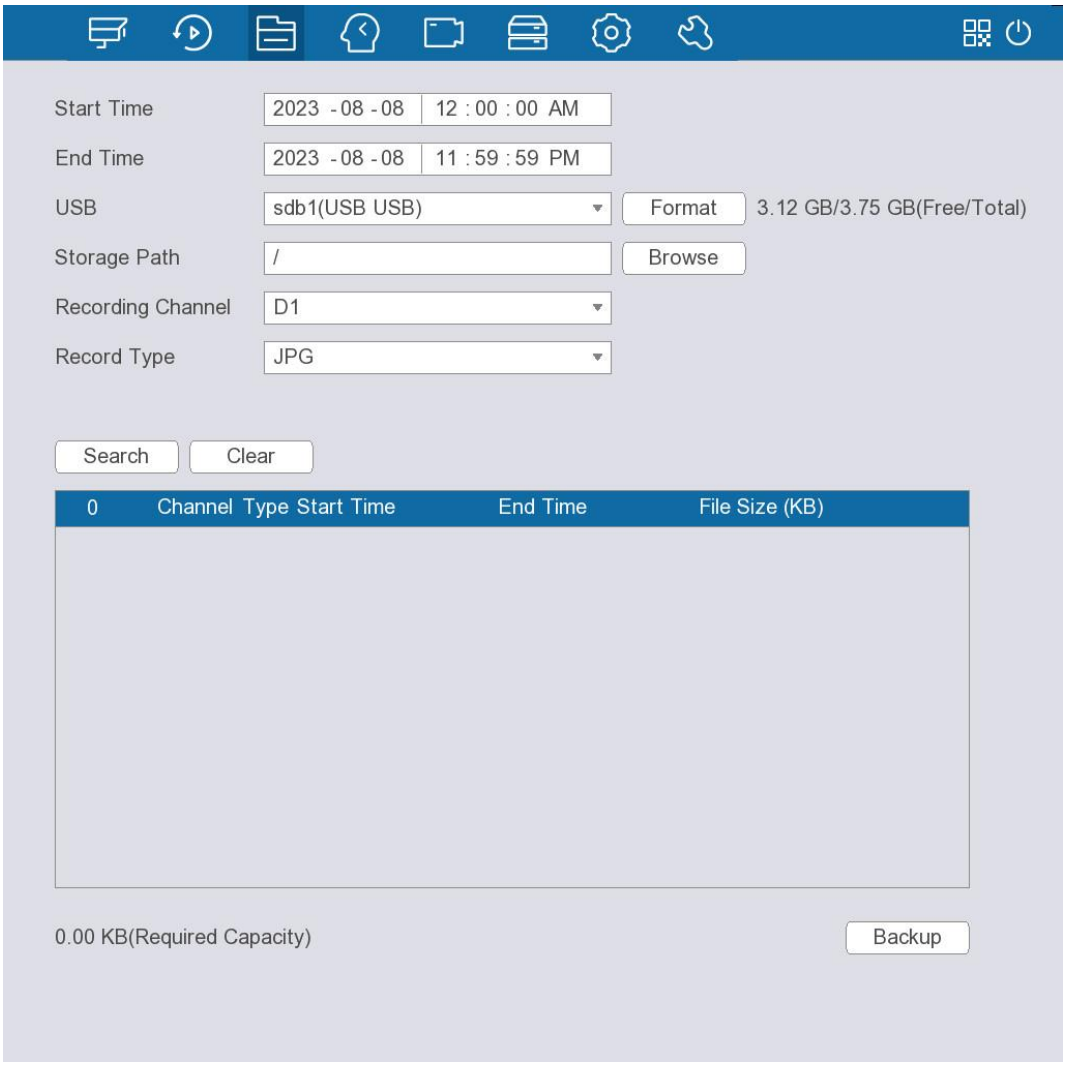


Table 5-11 Video search parameters

Parameter	Description
Start Time	Configure the start time and end time for the picture

Parameter	Description
End Time	search.
USB	Select a USB from the drop-down list. Click **Format** to format the USB.
Storage Path	Click **Browse** to select the storage path.
Recording Channel	Select the recording channel.
Record Type	Select the record type as required. Only supports selecting **JPG**.

5.8.3 Smart Search

Supports face search, VCA search, LPR search, and MD2.0 search.

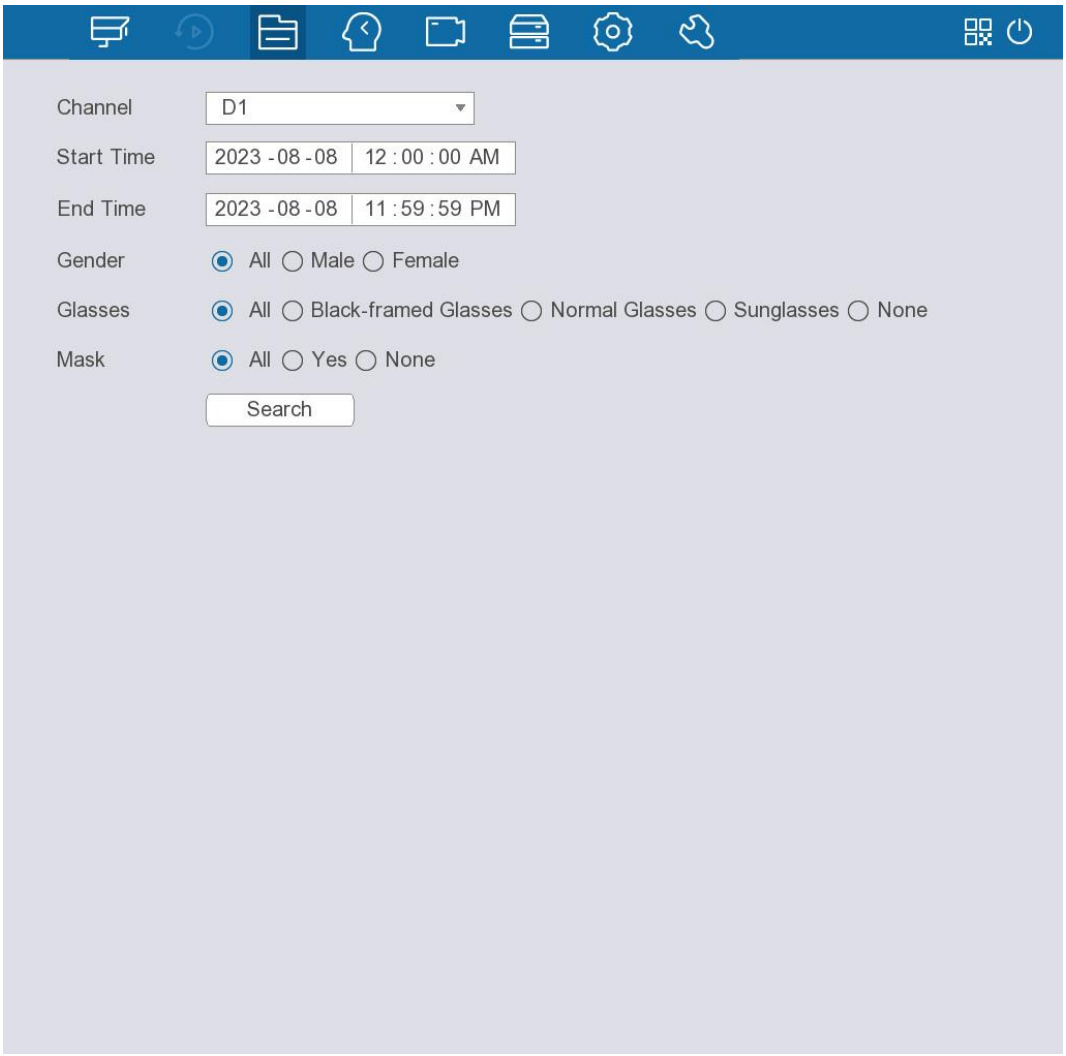
5.8.3.1 Face Search

You can search for and play back detected faces.

Procedure

Step 1 Select **File Search** > **Smart Search** > **Face Search**.

Figure 5-23 Face search



Step 2 Select a channel, set the search period, and then select the attributes.

You can select one or more channels, or select **All**.

Step 3 Click **Search**.

The results are displayed.

Related Operations

- Play.

  Select an image and then click to play back.

  Double-click the playing image to switch between full-screen playing and thumbnail playing.

- Sort.

  Click to sort the images by time.

- Export.

  Click to export the search results in an Excel document.

- Back up.

  Select one or more images, click , and then select the storage path.

- Add tag.

Select one or more images, and then click .

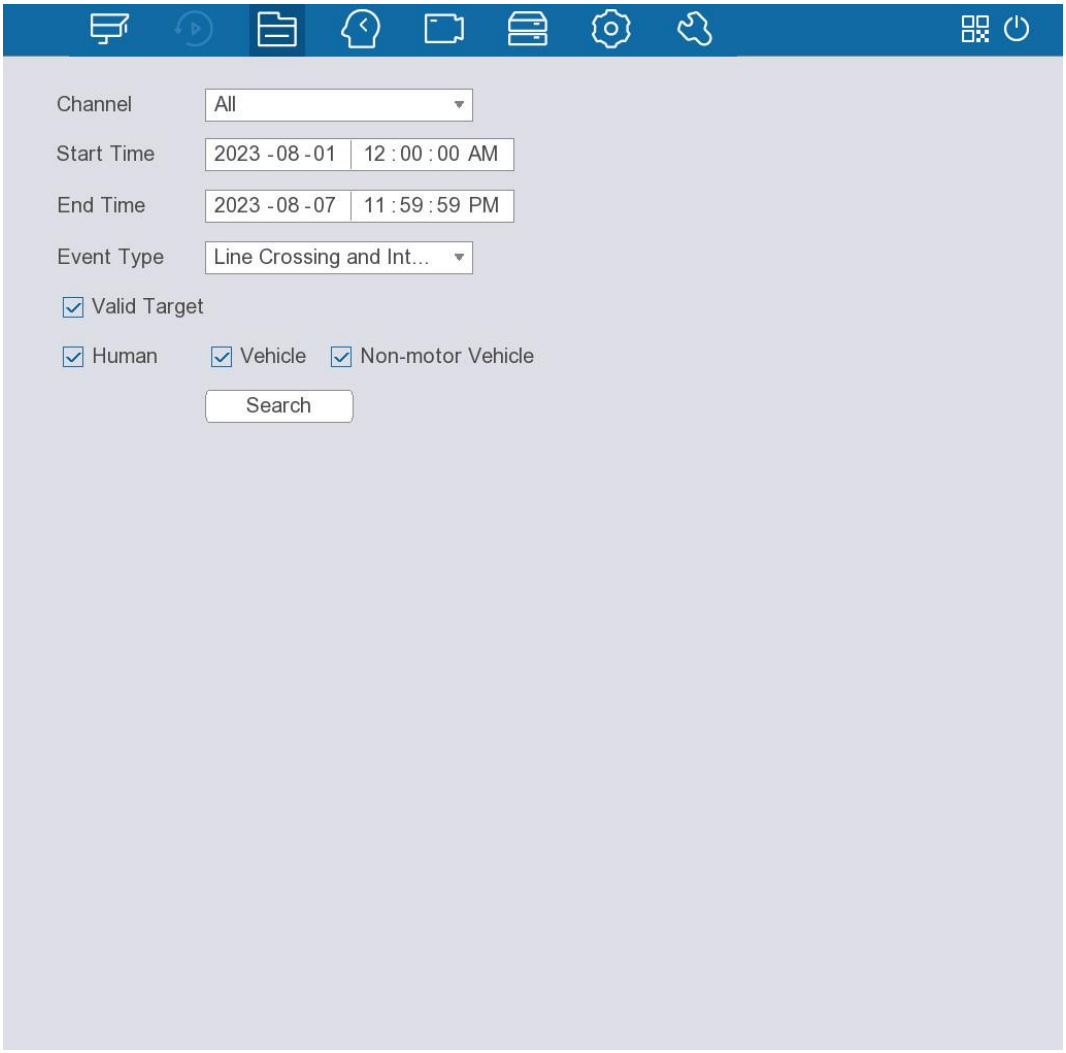
5.8.3.2 VCA Search

You can search for the VCA detection results.

Procedure

Step 1 Select **File Search** > **Smart Search** > **VCA Search**.

Figure 5-24 VCA search



Step 2 Select a channel, and then set the start time and end time.

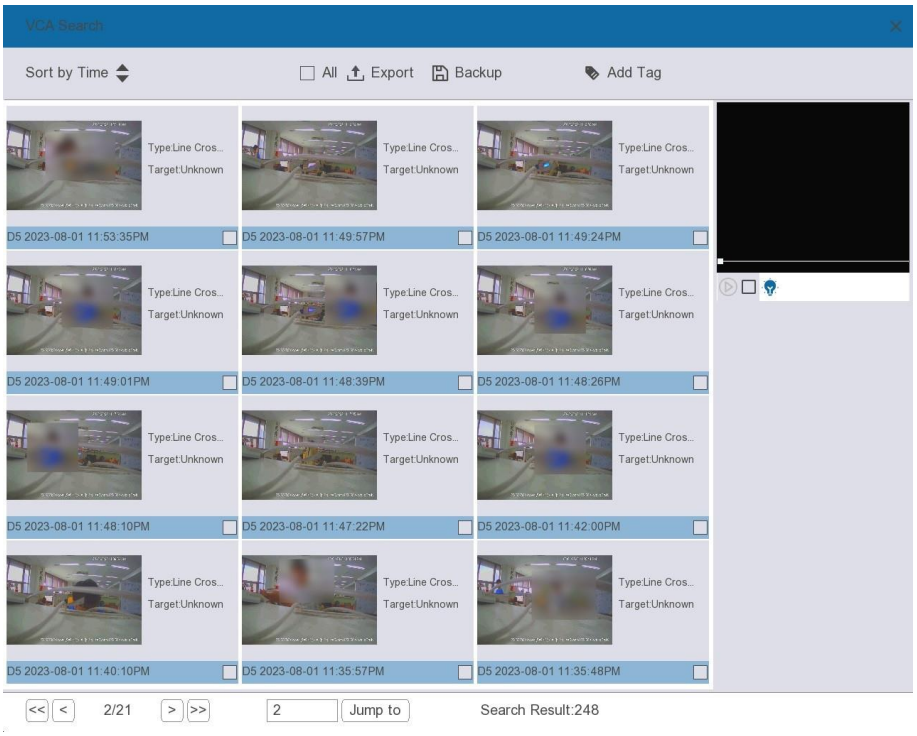
You can select one or more channels, or select **All**.

Step 3 Select an event type.

Step 4 Click **Search**.

The results are displayed.

Figure 5-25 Search results



Related Operations

- Play.

  Select an image and then click to play back.

- Sort.

  Click to sort the images by time.

- Export.

  Click to export the search results in an Excel document.

- Back up.

  Select one or more images, click , and then select the storage path.

- Add tag.

  Select one or more images, and then click .

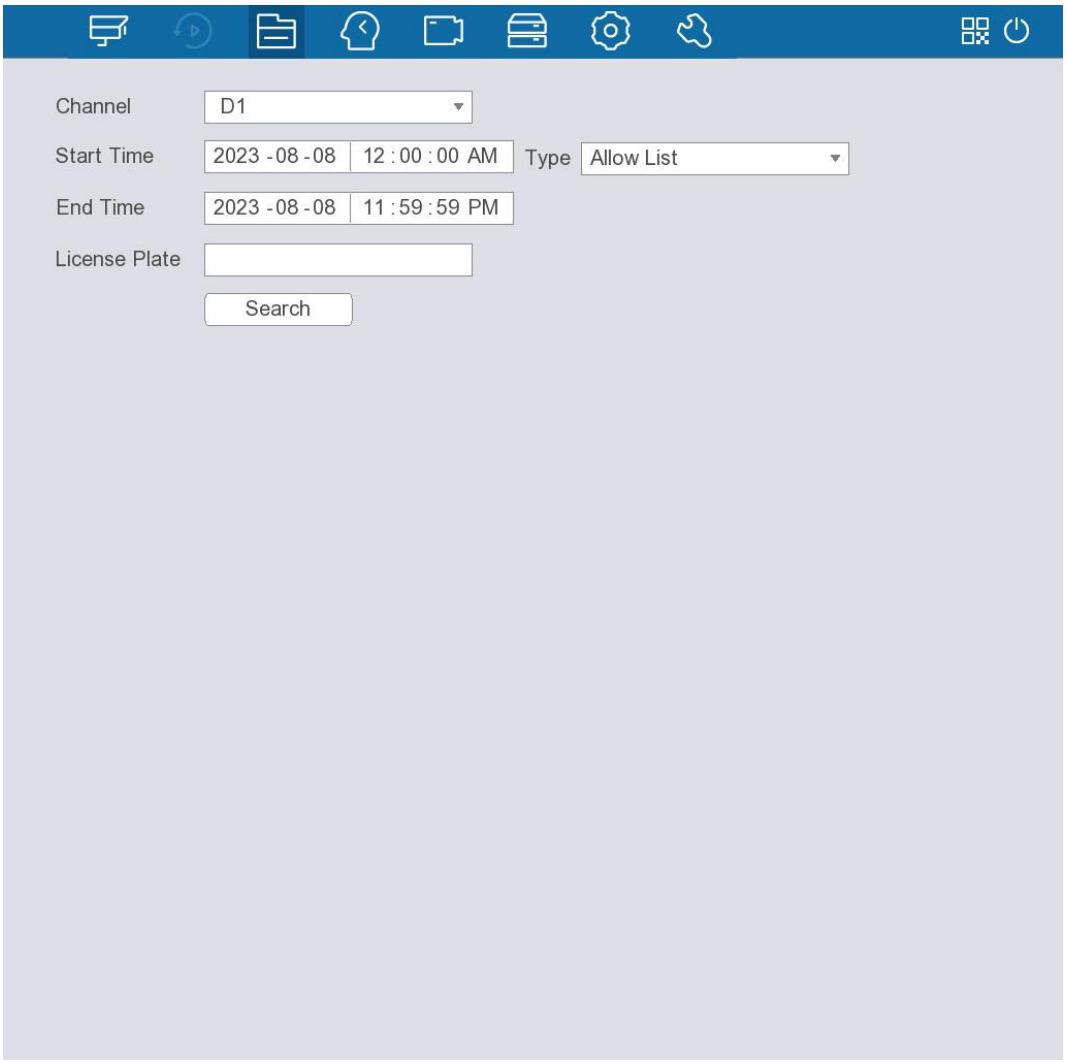
5.8.3.3 LPR Search

You can search for the license plate results.

Procedure

Step 1 Select **File Search** > **Smart Search** > **LPR Search**.

Figure 5-26 LPR search



Step 2 Select a channel, and then select the target type from **Allow List**, **Block List**, **Standard**, or **All**.

You can select one or more channels, or select **All**.

Step 3 Set the start time and end time.

Step 4 Click **Search**.

The results are displayed.

Related Operations

- Play.

  Select an image and then click to play back.

- Sort.

  Click to sort the images by time.

- Export.

  Click to export the search results in an Excel document.

- Back up.

  Select one or more images, click , and then select the storage path.

- Add tag.

  Select one or more images, and then click .

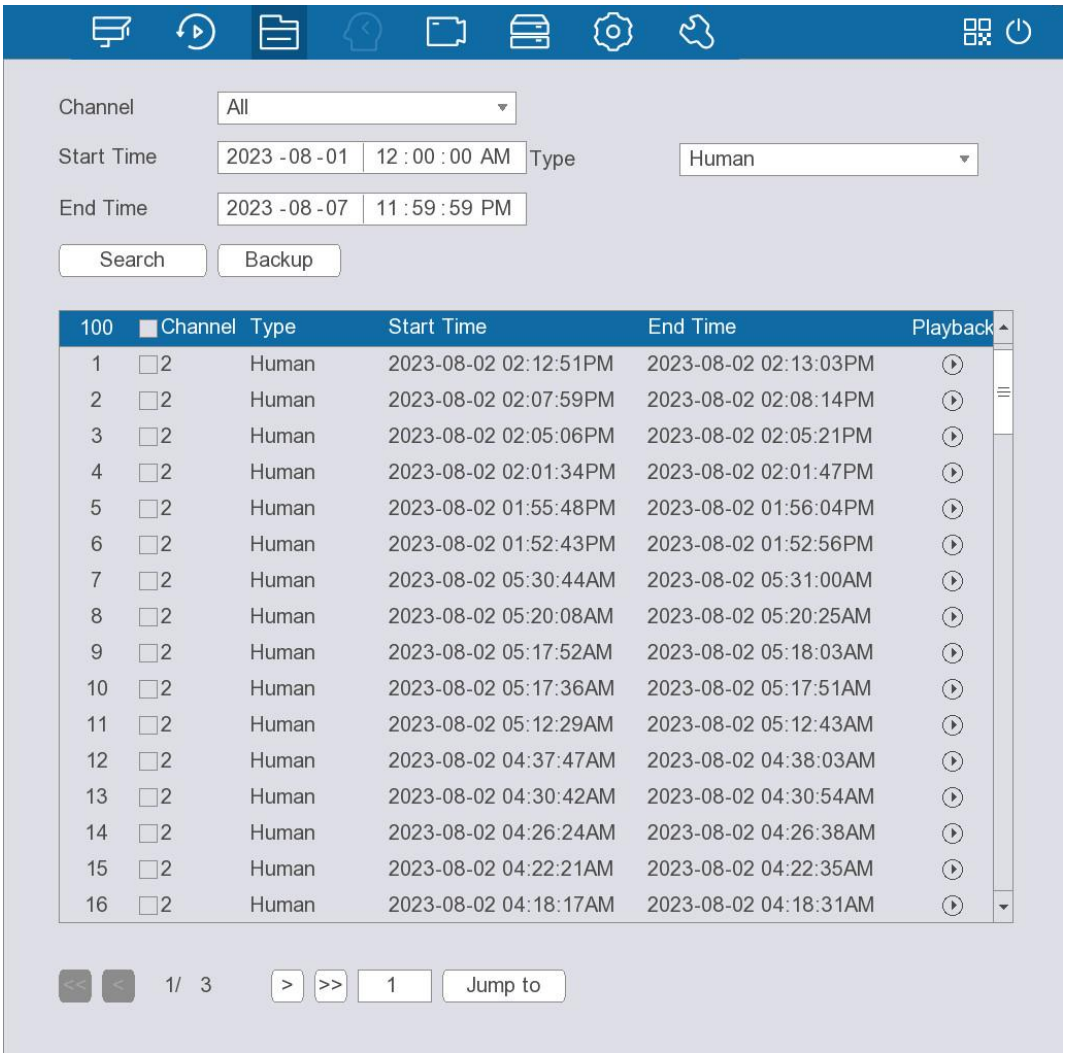
5.8.3.4 MD2.0 Search

You can search for the motion detection results.

Procedure

Step 1 Select **File Search** > **Smart Search** > **MD2.0 Search**.

Figure 5-27 MD2.0 search



Step 2 Select a channel, and then select the target type from **All**, **Human** and **Vehicle**.

You can select one or more channels, or select **All**.

Step 3 Set the start time and end time.

Step 4 Click **Search**.

The results are displayed.

Related Operations

- Play.

  Select an event, and then click to play back.

- Back up.

  Select one or more events, click **Backup**, and then select the storage path to back up the search result.

5.9 Smart Analysis

5.9.1 VCA Settings

5.9.1.1 VCA Option

To use face detection, VCA and other smart functions supported by the smart network cameras, you need to enable the corresponding smart plan.

Procedure

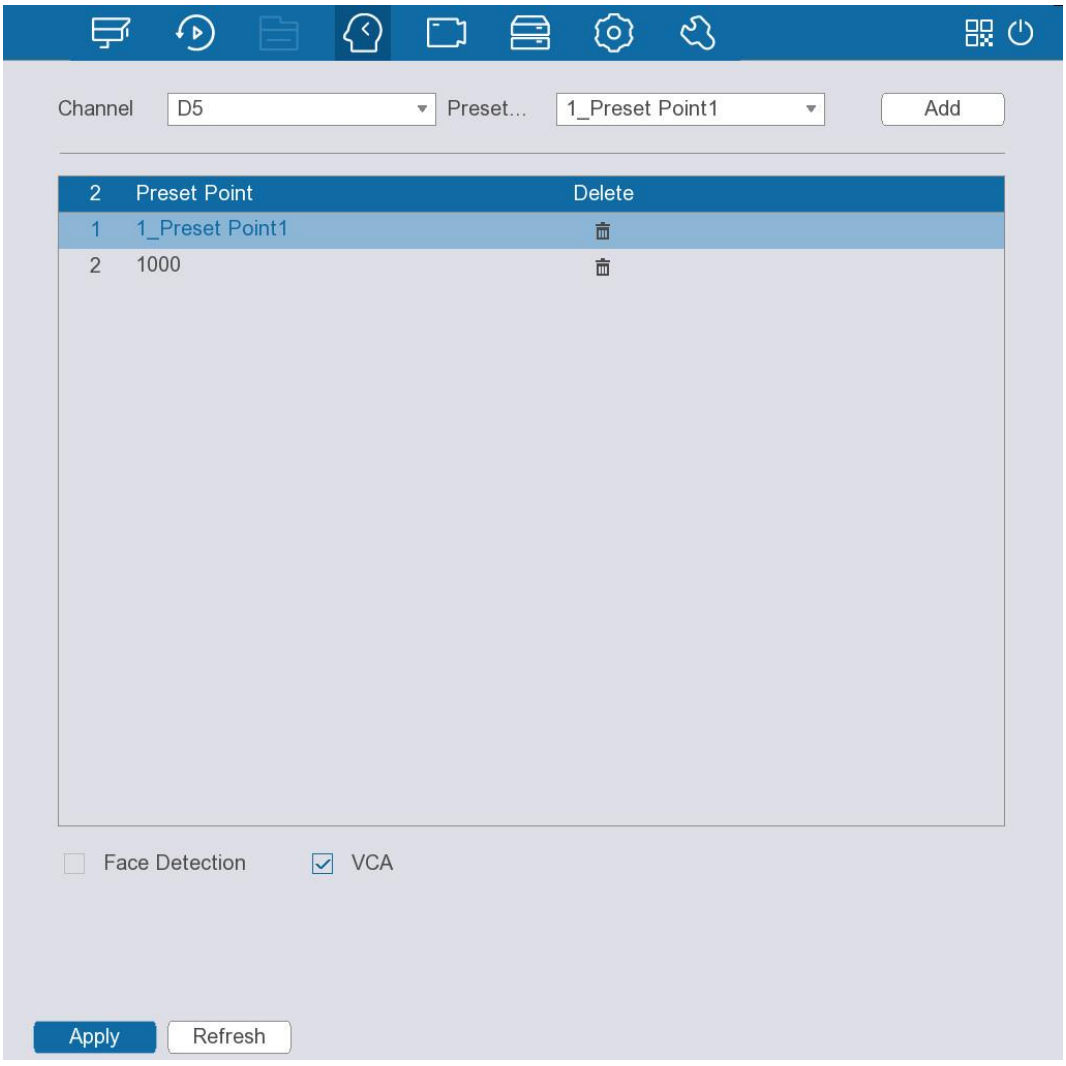
Step 1 Select **Smart Analysis** > **VCA Settings** > **VCA Option**.

Step 2 Select a channel.

The system displays the smart functions available on the connected camera.

The smart functions available are different depending on the camera.

Figure 5-28 VCA option



Step 3 Click the checkbox next to the corresponding the smart plan to enable it.

If the channel is connected to a PTZ camera, you can set smart functions separately for each preset point.

Step 4 Click **Apply**.

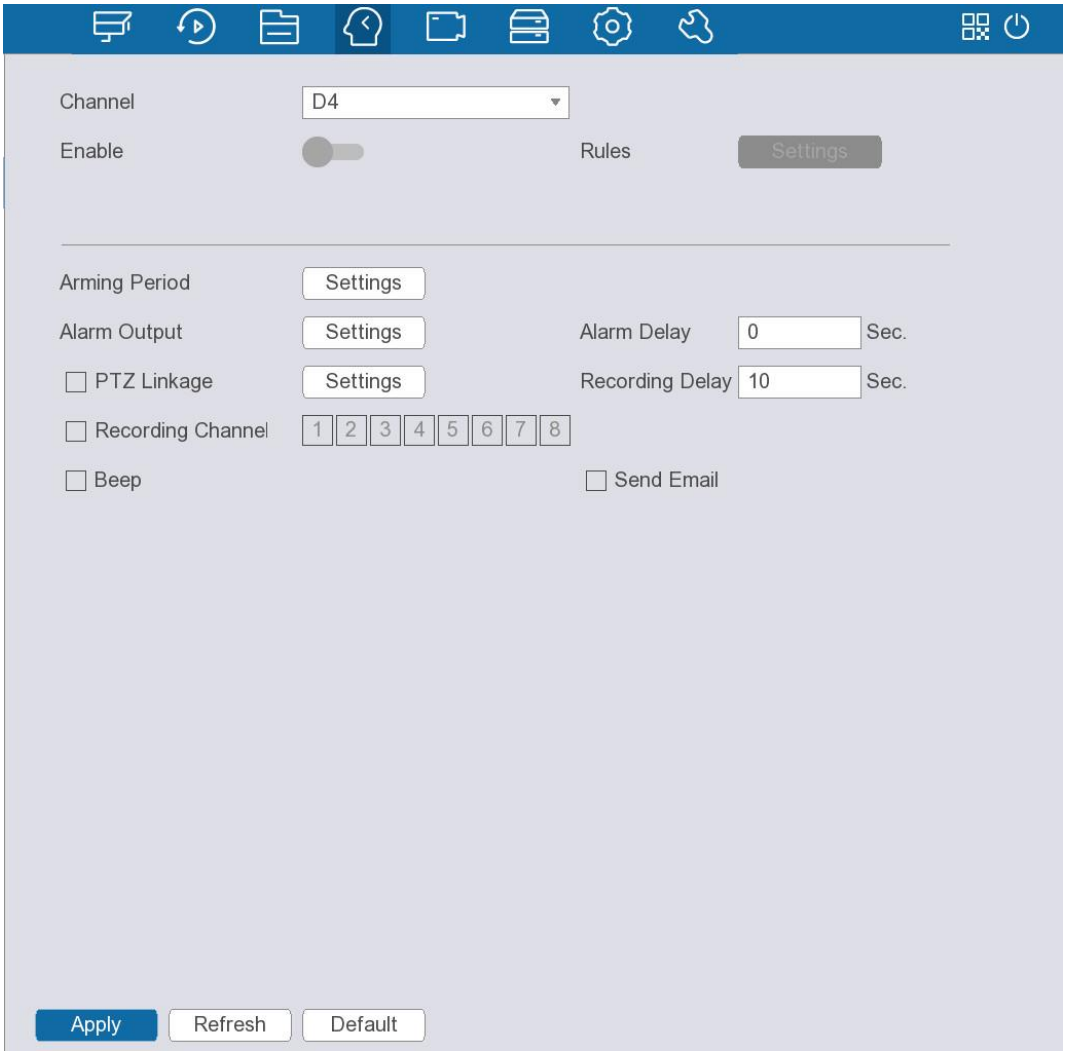
5.9.1.2 Configuring Face Detection

Configure alarm rule of face detection. An alarm is triggered when human faces are detected in the detection area.

Procedure

Step 1 Select **Smart Analysis** > **VCA Settings** > **Face Detection**.

Figure 5-29 Face detection



Step 2 Select a channel, and then click to enable the face detection.

Step 3 Click **Settings** next to **Rules** to draw the minimum size or maximum size to filter the target.

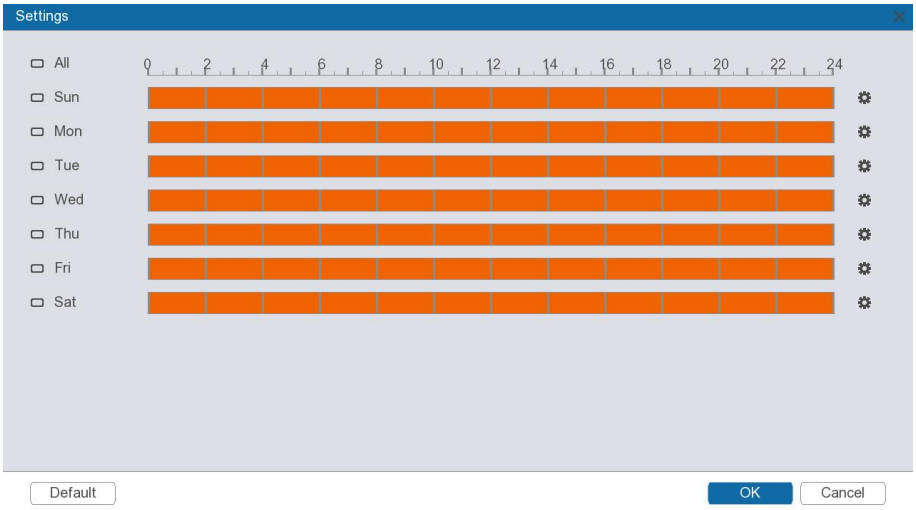
The system triggers an alarm when the size of detected target is between the maximum size and the minimum size.

Step 4 Click **Settings** next to **Arming Period** to configure the arming period.

The arming period is highlighted. There are two ways to configure the period.

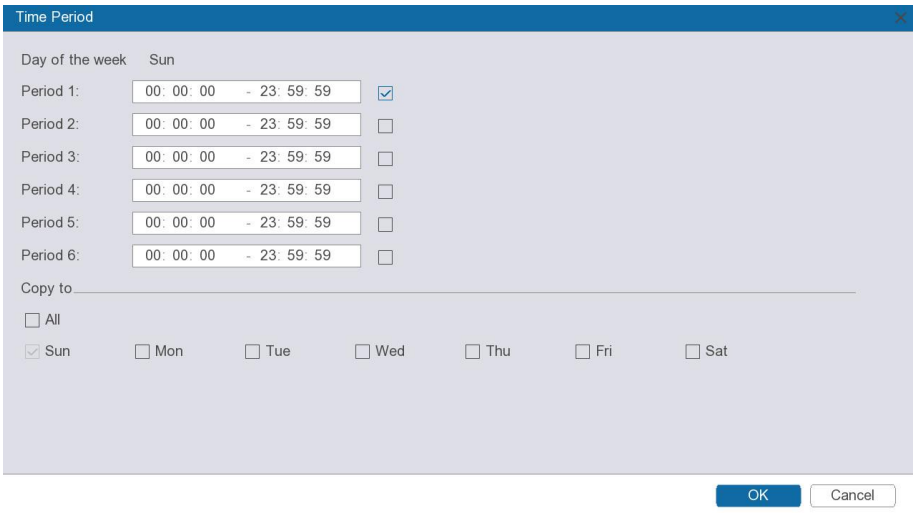
- Drag on the time line to define the period. You can click the orange part to disarm the period.

Figure 5-30 Arming period (1)



- Click ⚙ to define the arming period for each day in a week.
  - There are six periods for you to set for each day.
  - Under **Copy to**, select **All** to apply the settings to all the days of the week, or select specific days that you want to apply the settings to.

Figure 5-31 Arming period (2)



Step 5 Configure the alarm linkage.

Table 5-12 Alarm linkage

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as required. Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".
PTZ Linkage	Select the checkbox, and then click **Settings** to configure PTZ linkage. Make sure that the PTZ control has been configured. For details, see "5.5.4 PTZ".
Recording Channel	Select the checkbox, and then select one or more channels for recording. Make sure that the recording plan and recording mode has been configured in **Storage** > **Recording Plan** > **Video Recording**.
Beep	Select the checkbox to enable the device to make a beep noise when an alarm occurs.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends.
Recording Delay	Configure the length of time for the device to continue recording after the alarm ends.
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.

Step 6 Click **Apply**.

5.9.1.3 Configuring VCA

Background Information

Configure VCA alarm rules. An alarm is triggered when the system detects a certain behavior.

Table 5-13 VCA functions

Function	Description	Scene
Cross Fence	When the target crosses the warning line toward the defined direction, an alarm is triggered and then the system performs configured alarm linkages.	Scenes with median strips such as roads, and airports.
Line crossing and intrusion	When the target crosses the tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Abandoned Object	When an object is abandoned in the detection area longer than the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. • Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. • In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Missing Object	When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs configured alarm linkages.	
Parking Detection	When the vehicle stays in the detection area longer than the configured duration, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.
People Gathering	When people gather and stay in the detection area longer than the defined duration, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. It is not suitable for short-distance view analysis.
Fast Moving	When the target moves fast in the detection area, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and less occlusion. The camera should be installed right above the monitoring area. The light direction should be vertical to the motion direction.

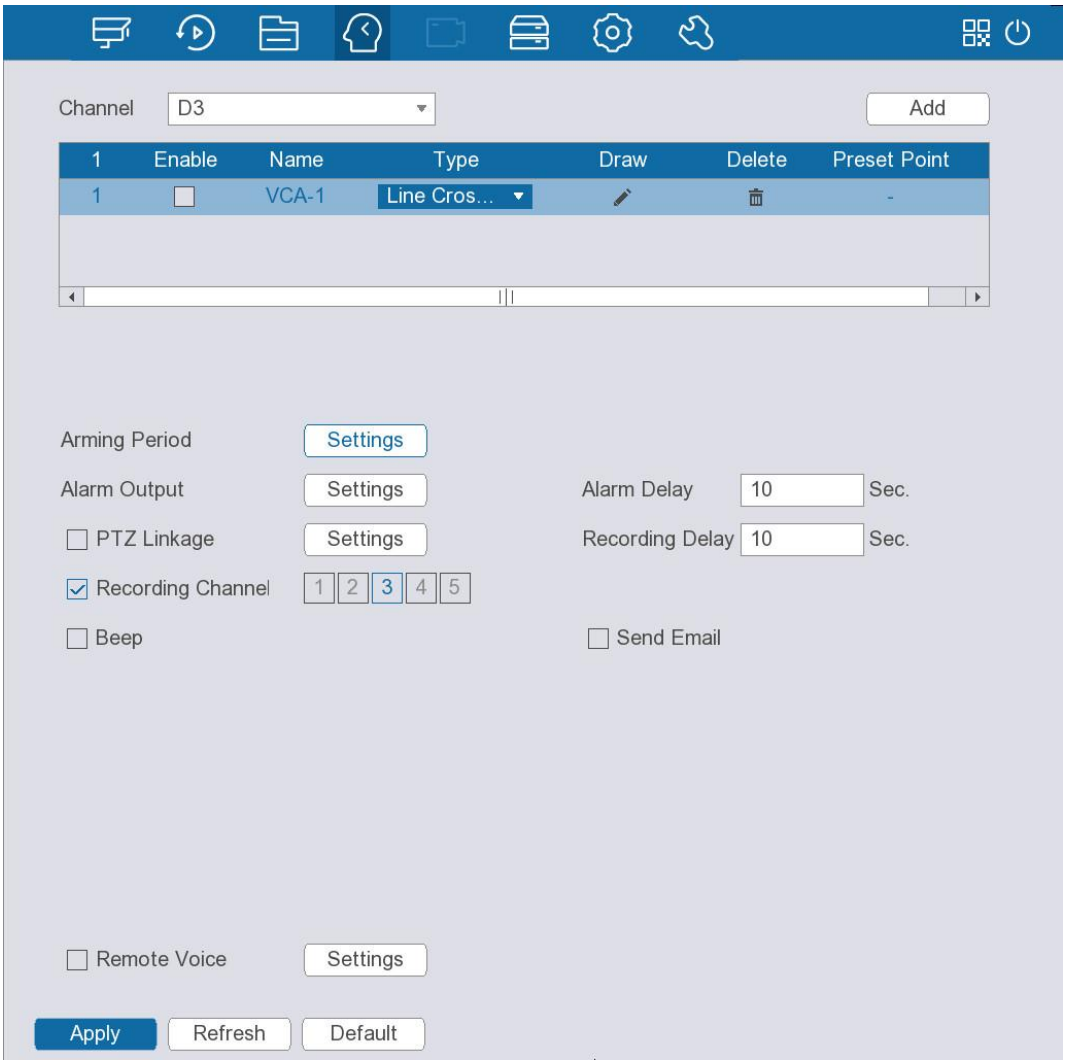
Function	Description	Scene
Loitering Detection	When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes such as park and hall.

In this section, line crossing and intrusion acts as an example of how to configure the VCA rules.

Procedure

Step 1 Select **Smart Analysis** > **VCA Settings** > **VCA**.

Figure 5-32 VCA

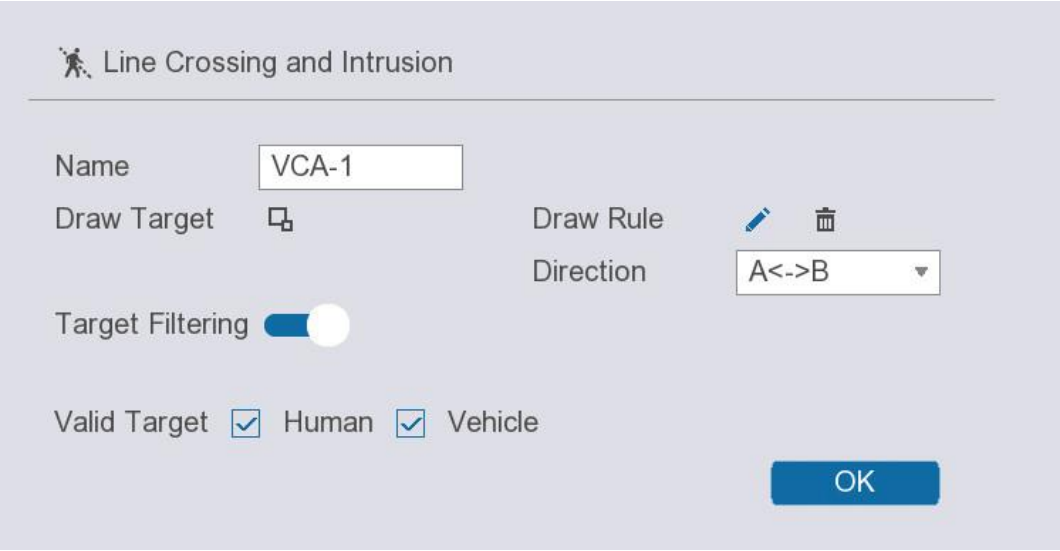


Step 2 Select a channel, and then click **Add** to add a rule.

Step 3 Configure the rule.

1. In the **Type** column, select **Line crossing and intrusion**.
2. Click .

Figure 5-33 Line crossing and intrusion



3. Configure the parameters.

Table 5-14 Line crossing and intrusion parameters

Parameter	Description
Name	Enter the rule name.
Draw Target	Click to draw the minimum size or maximum size to filter the target. The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
Draw Rule	Drag to draw a line. The line can be a straight line, broken line or polygon.
Direction	Select a line direction, including A→B, B→A and A↔B.
Target Filtering	Click and then select valid target.
Valid Target	**Human** and **Vehicle** are selected by default.

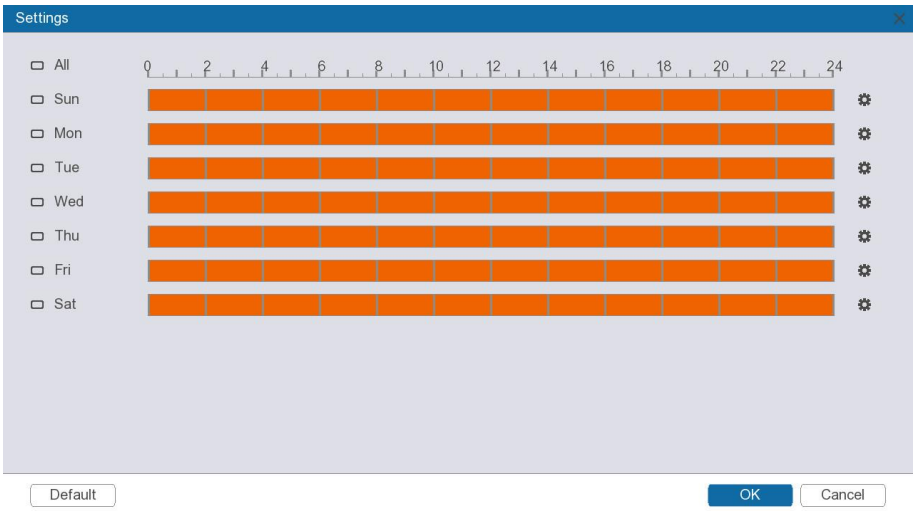
4. Click **OK**.

Step 4 Click **Settings** next to **Arming Period** to configure the arming period.

The arming period is highlighted. There are two ways to configure the period.

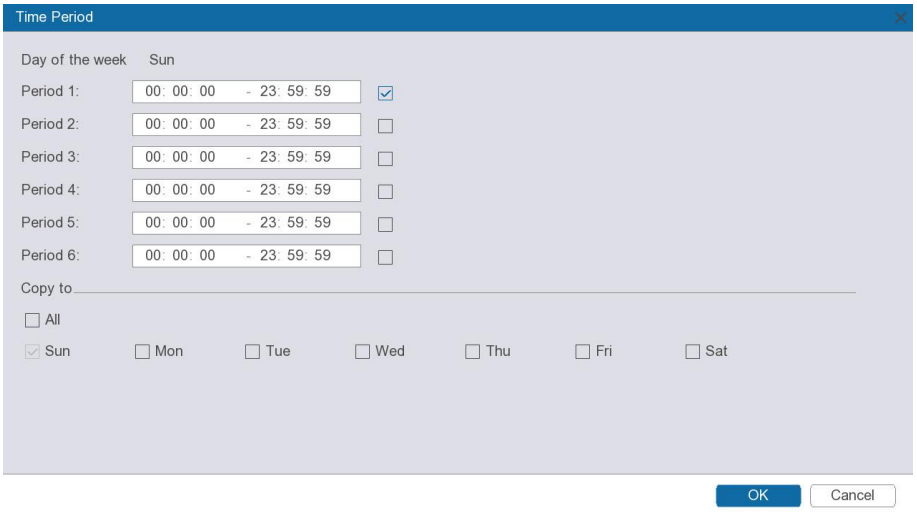
- Drag on the time line to define the period. You can click the blue part to disarm the period.

Figure 5-34 Arming period (1)



- Click ⚙ to define the arming period for each day in a week.
  - There are six periods for you to set for each day.
  - Under **Copy to**, select **All** to apply the settings to all the days of the week, or select specific days that you want to apply the settings to.

Figure 5-35 Arming period (2)



Step 5 Configure the alarm linkage.

Table 5-15 Alarm linkage

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click ⬬ to enable the local alarm, and then select alarm output port as required. 📖 Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".

Parameter	Description
PTZ Linkage	Select the checkbox and then click **Settings** to configure PTZ linkage. Make sure that the PTZ control has been configured. For details, see "5.5.4 PTZ".
Recording Channel	Select the checkbox, and then select one or more channels for recording. Make sure that the recording plan and recording mode has been configured in **Storage** > **Recording Plan** > **Video Recording**.
Beep	Select the checkbox to enable the device to make a beep noise when an alarm occurs.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends.
Recording Delay	Configure the length of time for the device to continue recording after the alarm ends.
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.

Step 6 Click **Apply**.

5.9.1.4 Configuring LPR

Configure LPR alarm rules. An alarm is triggered when the system detects a certain license plate.

Procedure

Step 1 Select **Smart Analysis** > **VCA Settings** > **LPR**.

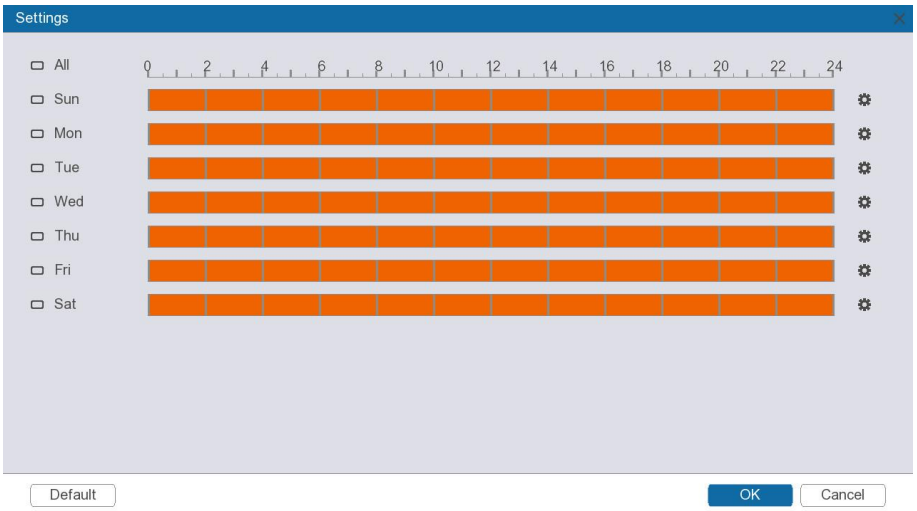
Step 2 Select a channel, click to enable LPR, and then select the target type from **Allow List**, **Block List**, **Standard**, or **All**.

Step 3 Click **Settings** next to **Arming Period** to configure the arming period.

The arming period is highlighted. There are two ways to configure the period.

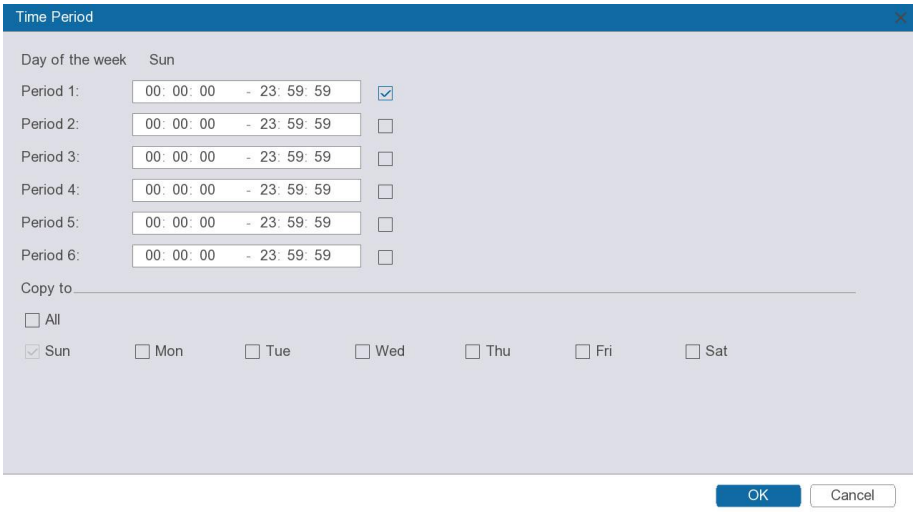
- Drag on the time line to define the period. You can click the blue part to disarm the period.

Figure 5-36 Arming period (1)



- Click ⚙ to define the arming period for each day in a week.
  - There are six periods for you to set for each day.
  - Under **Copy to**, select **All** to apply the settings to all the days of the week, or select specific days that you want to apply the settings to.

Figure 5-37 Arming period (2)



Step 4 Configure the alarm linkage.

Table 5-16 Alarm linkage

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click ⬭ to enable the local alarm, and then select alarm output port as required. 📖 Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".

Parameter	Description
PTZ Linkage	Select the checkbox and then click **Settings** to configure PTZ linkage. Make sure that the PTZ control has been configured. For details, see "5.5.4 PTZ".
Recording Channel	Select the checkbox, and then select one or more channels for recording. Make sure that the recording plan and recording mode has been configured in **Storage** > **Recording Plan** > **Video Recording**.
Beep	Select the checkbox to enable the device to make a beep noise when an alarm occurs.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends.
Recording Delay	Configure the length of time for the device to continue recording after the alarm ends.
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.

Step 5 Click **Apply**.

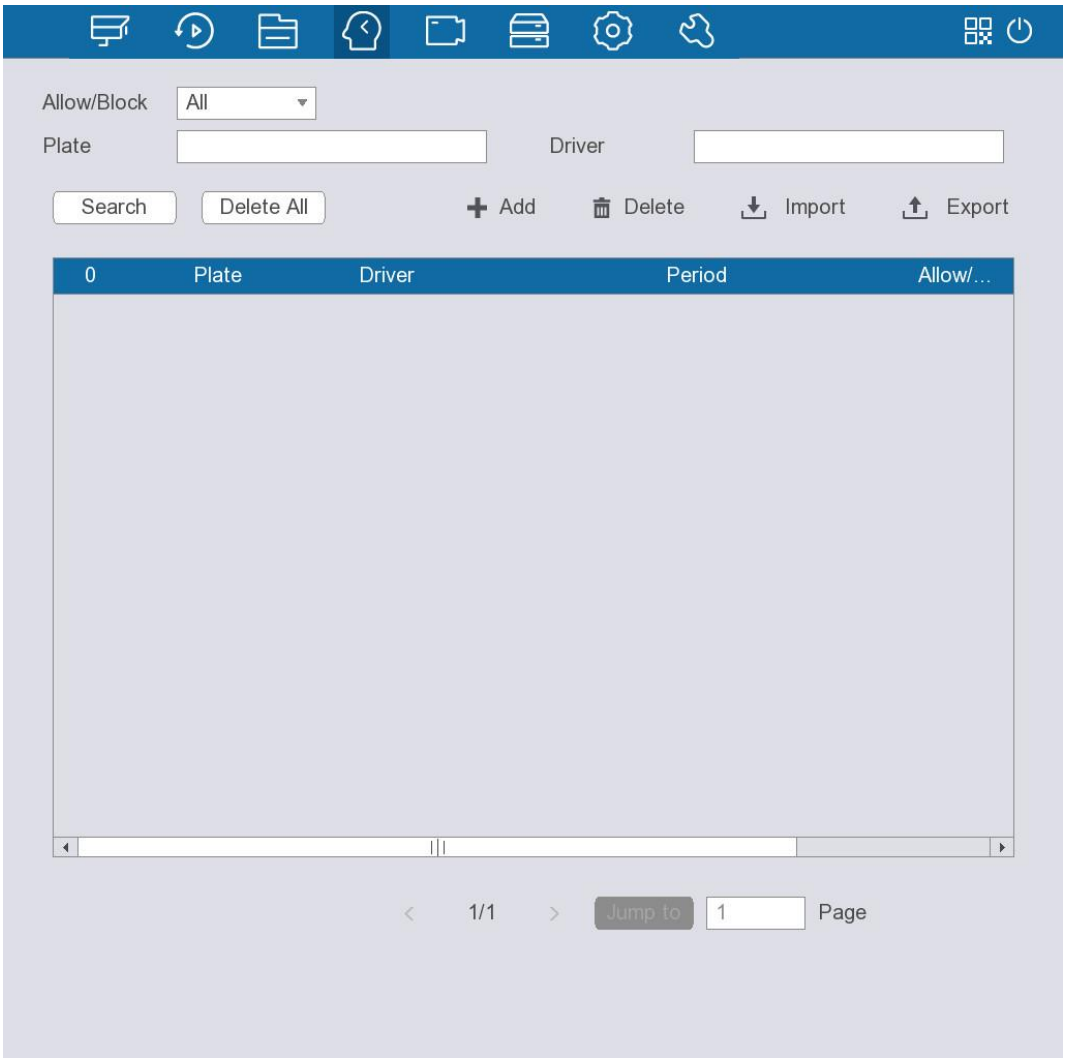
5.9.2 Database Settings

To facilitate vehicle management, you can add the plate numbers to the blocklist or allowlist. The system can compare the detected plate information with the plate on the blocklist and allowlist and then trigger the corresponding alarm linkage.

Procedure

Step 1 Select **Smart Analysis** > **Database** > **Blocklist and Allowlist**.

Figure 5-38 Blocklist and allowlist



Step 2 Click ➕ to manually add.

Step 3 Set plate information such as plate number, driver name, select **Block List** or **Allow List**, and then set validity period.

Step 4 Click **OK**.

Related Operations

- Search.

  Enter keywords for **Plate** and **Driver**, select type and then click **Search**.
- Import and export plate information.
  - Import: Click ⬇ to import, select the corresponding file, and then click **Browse** to import the file.
  - Export: Click ⬆ to export, select the file storage path and then click **Save**.
- Delete plate information.
  - Delete one by one: Select the plate number to be deleted, and then click 🗑.
  - Delete in batches: Select the plate numbers to be deleted, and then click **Delete All**.

5.10 Camera

You can configure camera registration, image attributes, overlay information, video parameters and other settings of the cameras connected to the device.

5.10.1 Configuring Remote Devices

5.10.1.1 Adding Remote Devices

Add remote devices to the NVR to receive, store, and manage the video streams of the remote device.

Before adding the remote devices, make sure that the devices have been initialized.

5.10.1.1.1 Adding Remote Devices from Search

Background Information

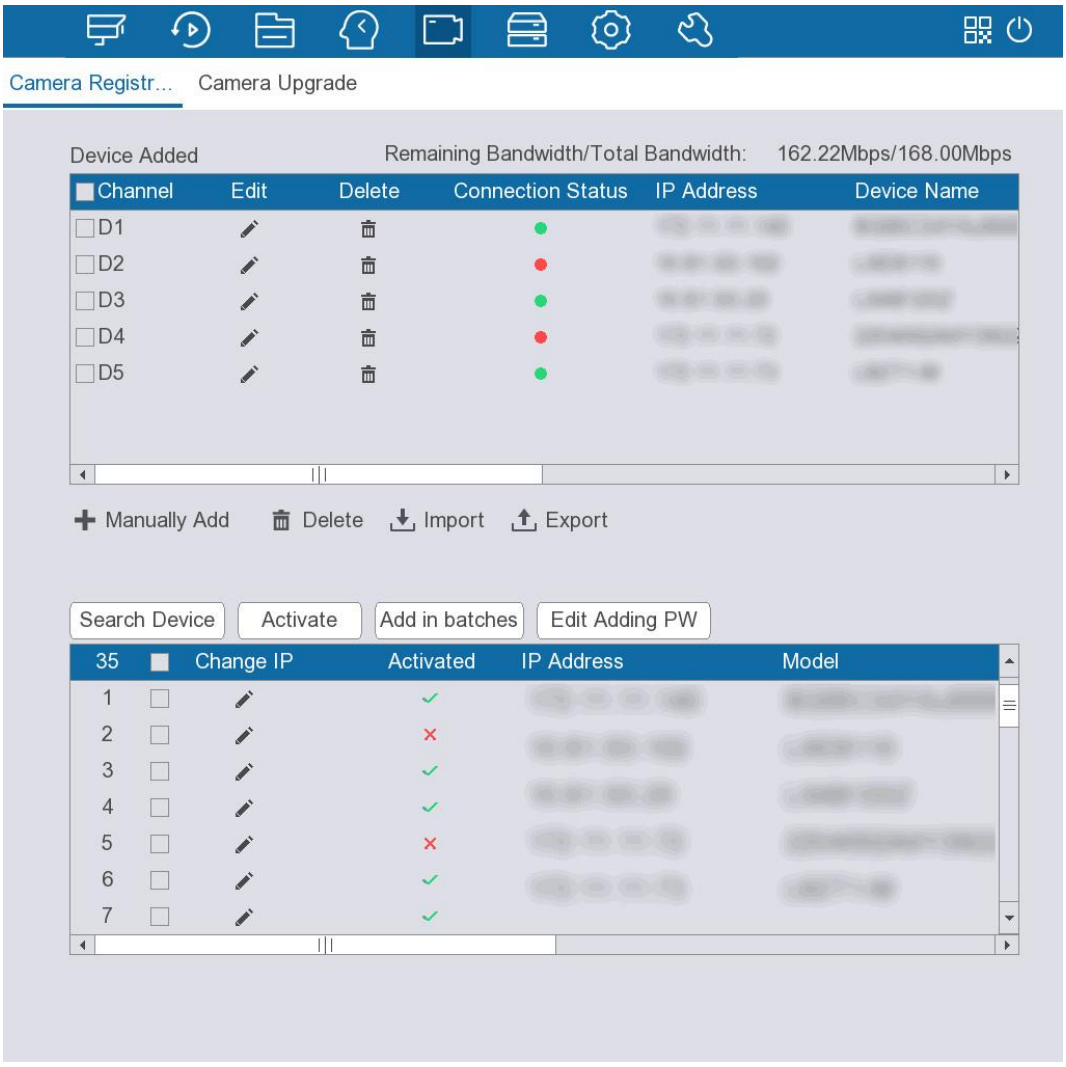
Search for the remote devices on the same network with the NVR, and then add the remote devices from the search results.

We recommend this method when you do not know the specific IP address of the remote device.

Procedure

Step 1 Select **Camera** > **Camera Registration** > **Camera Registration**.

Figure 5-39 Remote device



Step 2 Click **Search Device**.

Step 3 Select one or more remote devices from the search results and then click **Add in batches**.

You can view the added devices on the list under **Device Added**.

Related Operations

You can click under **Change IP** to change IP addresses.

- **DHCP**: There is no need to enter IP address, subnet mask, and default gateway. Device automatically allocates the IP address to the camera.
- **Static**: You need to enter IP address, subnet mask, and default gateway.

When you are changing IP addresses of several devices at the same time, enter incremental value. The system can add the fourth decimal digit of the IP address one by one to automatically allocate the IP addresses.

If an IP conflict occurs when you change static IP address, the system will notify you of the issue. If you change IP addresses in batches, the system automatically skips the conflicted IP and begins the allocation according to the incremental value.

5.10.1.1.2 Adding Remote Devices Manually

Background Information

Configure the IP address, username, password and other information of the remote device manually to add the Device.

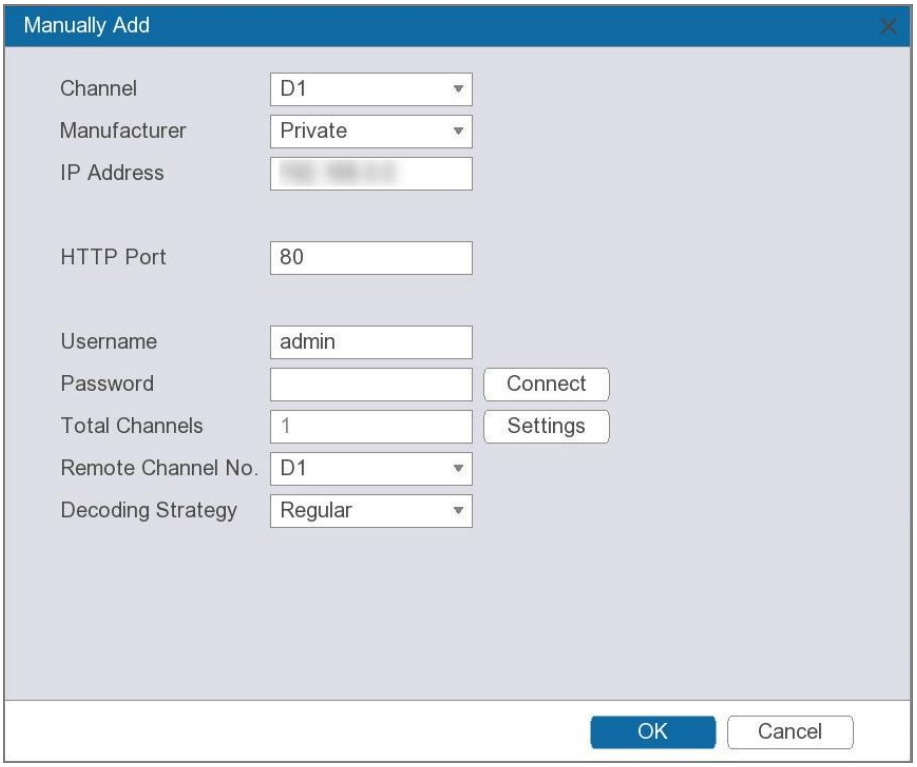
We recommend this method when you want to add only a few remote devices and know their IP addresses, usernames and passwords.

Procedure

Step 1 Select **Camera** > **Camera Registration** > **Camera Registration**.

Step 2 Click ➕ to manually add.

Figure 5-40 Manually add



Step 3 Configure the parameters.

Table 5-17 Parameters of manual add

Parameter	Description
Channel	Designate a channel for the remote device.
Manufacturer	Select the manufacturer of the remote device.
IP Address	Enter the IP address of the remote device.
HTTP Port	Enter the HTTP port of the remote device.
Username	Enter the username and password used to log in to the remote device.
Password	
Total Channels	Click **Connect** to get the total number of channels of the remote device.

Parameter	Description
Remote Channel No.	Select one or more remote channels that you want to connect to.
Decoding strategy	Select a decoding strategy from **Real-time**, **Regular**, and **Smooth**.
Encrypt	Select an encrypting strategy from **Automatic**, **TCP**, **UDP**, and **MULTICAST.**

Step 4 Click **OK**.

Related Operations

- Click under **Edit** to modify information of the added device.
- Click to delete the added device.
- Click **Edit Adding PW** to change the camera login password.

5.10.1.1.3 Importing Remote Devices

Prerequisites

Connect a USB storage device to the Device.

Background Information

You can import remote devices in batches.

We recommend this method when you want to add lots of remote devices whose IP addresses, usernames and passwords are not the same.

Procedure

Step 1 Select **Camera** > **Camera Registration** > **Camera Registration**.

Step 2 Click to export the template.

You need to disable backup encryption when exporting the template.

Step 3 Fill in the template.

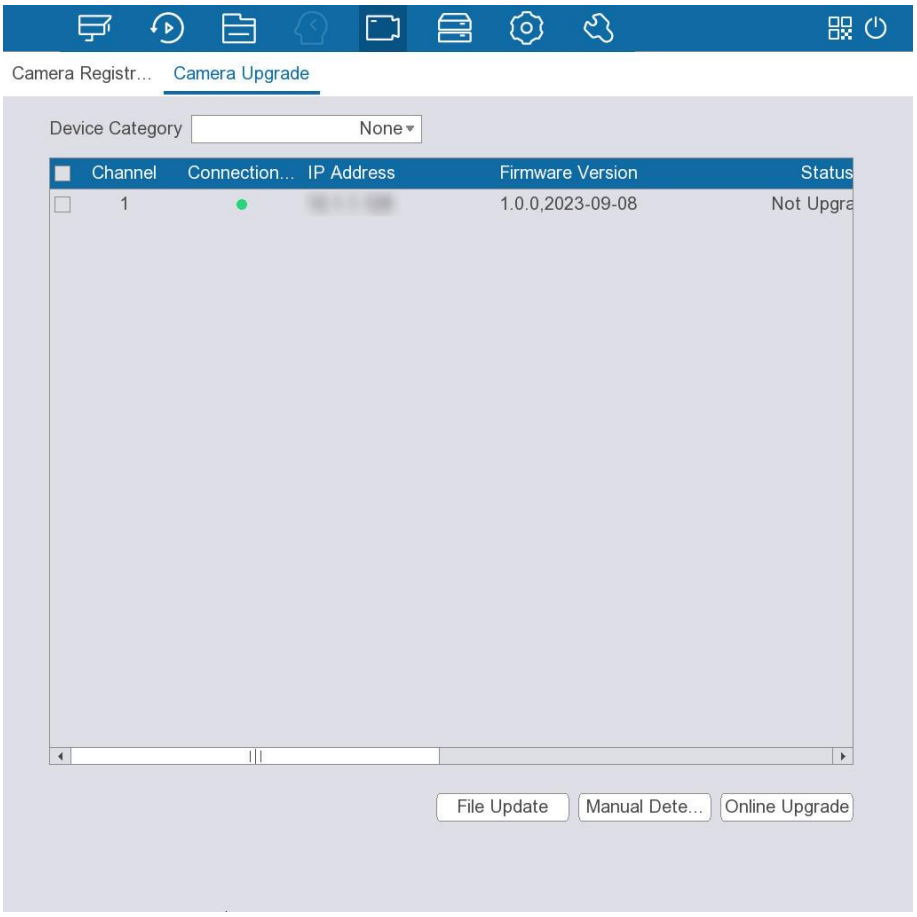
Step 4 Click to import the template.

Step 5 Click **OK**.

5.10.1.2 Upgrading Remote Devices

Select **Camera** > **Camera Registration** > **Camera Update** to update the remote devices.

Figure 5-41 Camera upgrade



- File update.
  1. Connect a USB storage device containing the update file to the Device.
  2. Select one or more remote devices.
  3. Click **File Update**.
  4. Select the update file to update.
- Online update.
  1. Select one or more remote devices and then click **Manual Detection**.
     The system starts detecting whether there is a new version available.
  2. Select the remote devices with a new version available, and then click **Online Upgrade**.

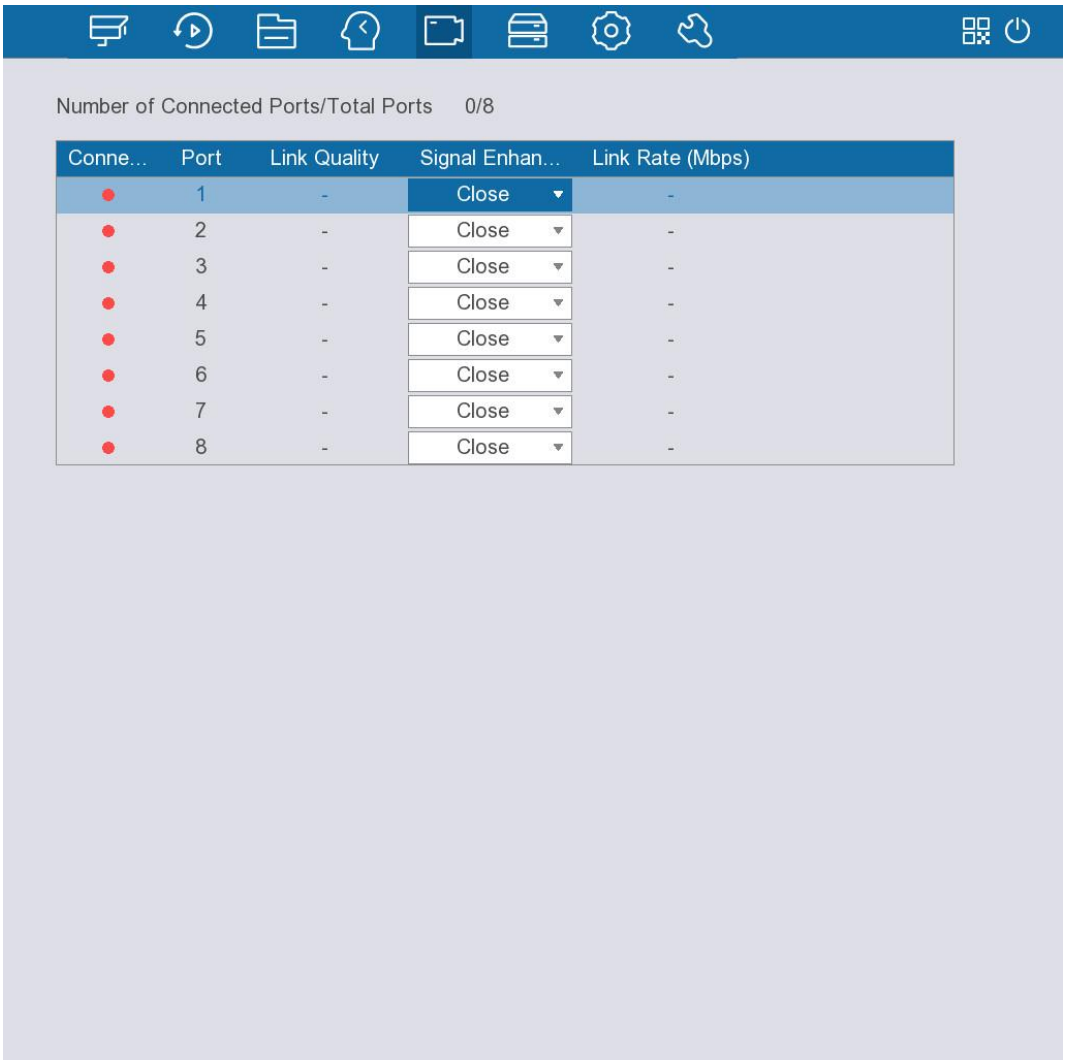
     You can filter the remote devices through the **Device Category** list.

5.10.2 Checking PoE Status

Select **Camera** > **PoE** to check the status of the PoE ports.

You can select **Signal Enhancement Mode** from **On** or **Close**.

Figure 5-42 PoE



5.10.3 Configuring Image Attributes

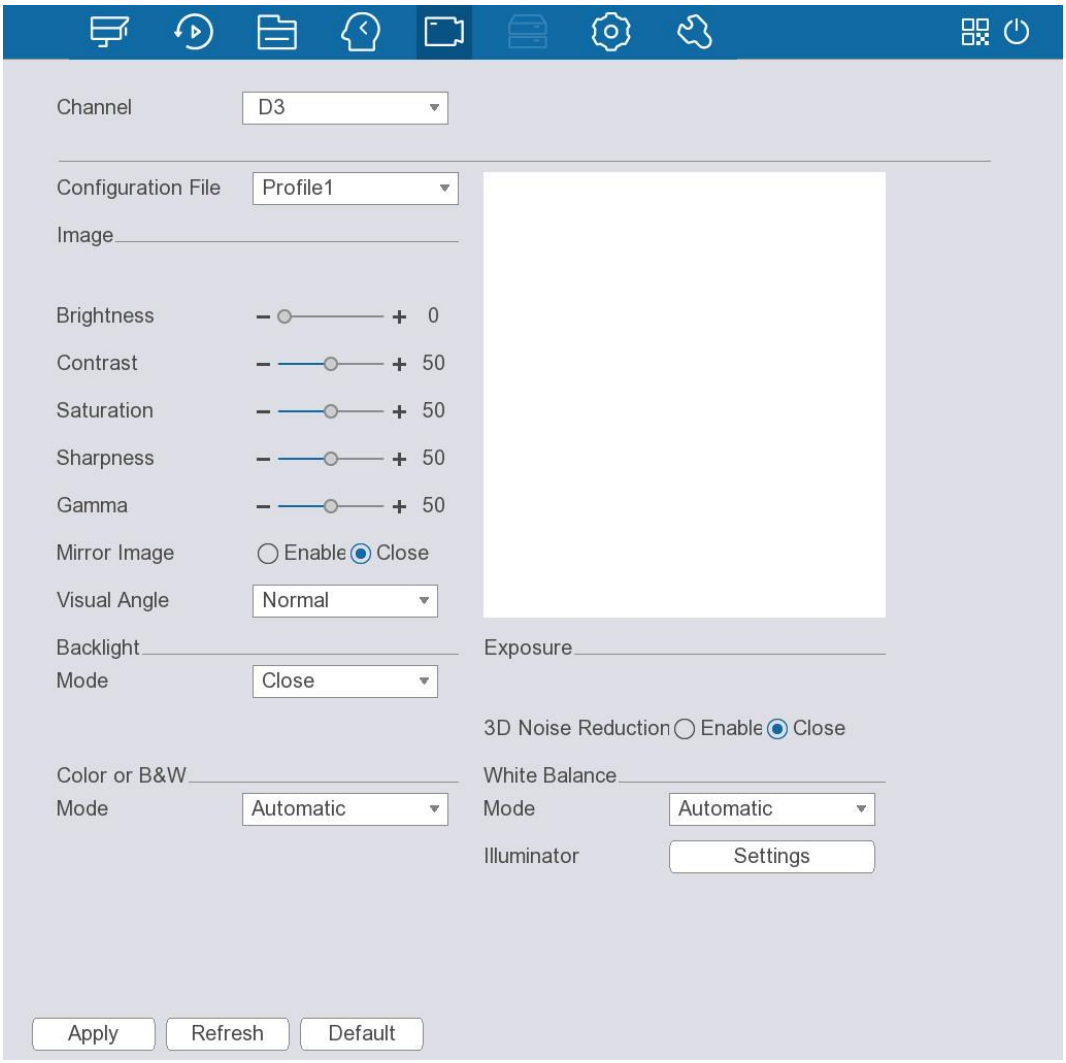
Background Information

Configure the image attributes, such as saturation, brightness, contrast, and chromaticity.

Procedure

Step 1 Select **Camera** > **Image Attributes**.

Figure 5-43 Image attributes



Step 2 Select a channel and then configure the parameters.

Table 5-18 Parameters of image attributes

Parameter	Description
Configuration File	Select a configuration file from **Profile1** or **Profile2**. The image attributes vary with the configuration files.
Brightness	The bigger the value, the brighter the image.
Contrast	The bigger the value, the more obvious the contrast between the light area and dark area.
Saturation	The bigger the value, the more intense the color.
Sharpness	The bigger the value, the more obvious the image edge.
Gamma	Adjust the image brightness and enhance the image dynamic display range. The bigger the value is, the brighter the image.
Mirror Image	Select **Enable** to switch the left and right side of the video image. This function is available on select models.
Visual Angle	Set the video display direction.

Parameter	Description
Backlight Mode	• **Close**: Disable backlight mode. • **Backlight Compensation**: Enable the camera to get a clearer image of the dark areas on the target when shooting against light. • **Wide Dynamic Range**: The system dims bright areas and enhances the brightness of the dark areas to ensure the overall clarity of the image. • **Highlight Compensation**: Select this mode when extremely strong light exists in the environment. The system lowers the brightness of the brightest section and reduces the area of the halo to lower the brightness of the whole image.
3D Noise Reduction	Reduces the noise of multiple-frame images by using inter-frame information between two adjacent frames in a video.
White Balance Mode	Enable white balance to make the image color display precisely as it is. This function changes the overall hue of the image. The white balance modes might differ depending on the camera.
Day and Night Modes	Switches the video image between the color mode and the black & white mode. • **Automatic**: The camera outputs color images or black and white images according to ambient conditions. • **Full Color**: The camera outputs color images only. • **Black & White**: The camera outputs black and white images only.
Illuminator	The illuminator ensures the brightness and definition of video images in a dark environment. • **Automatic**: The system adjusts the illuminator brightness automatically. • **Manual**: Set the illuminator brightness manually. • **Close**: Turn off the illuminator.

Step 3 Click **Apply**.

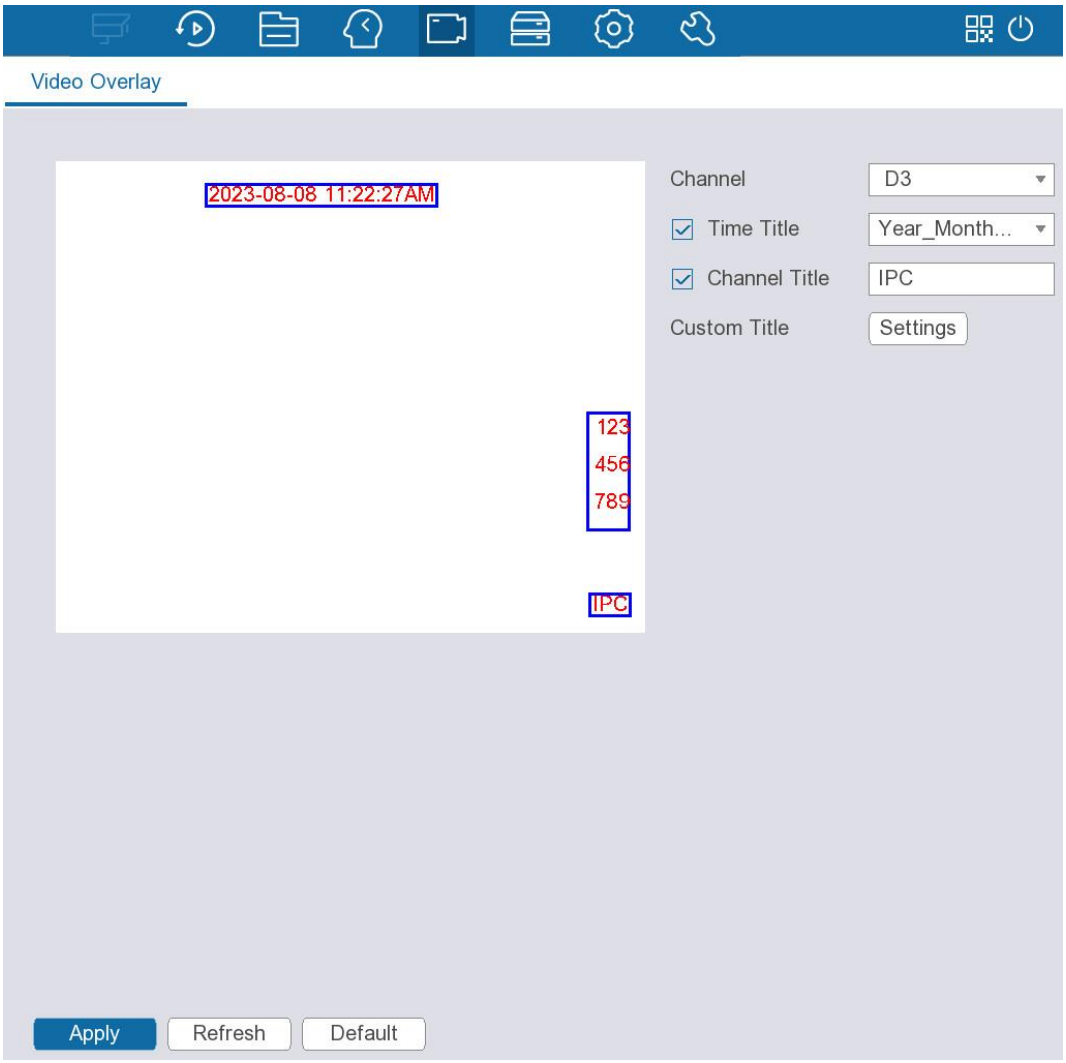
5.10.4 Configuring Overlay Settings

Configure the overlay information on the live page.

Procedure

Step 1 Select **Camera** > **Video Overlay**.

Figure 5-44 Overlay



Step 2 Select a channel and then configure the overlay information.

- **Time Title**: Select the checkbox, and then configure the time format.
- **Channel Title**: Select the checkbox, and then configure the channel name.

Click **Settings** next to **Custom Title** to add custom titles for the channel.

Step 3 Click **Apply**.

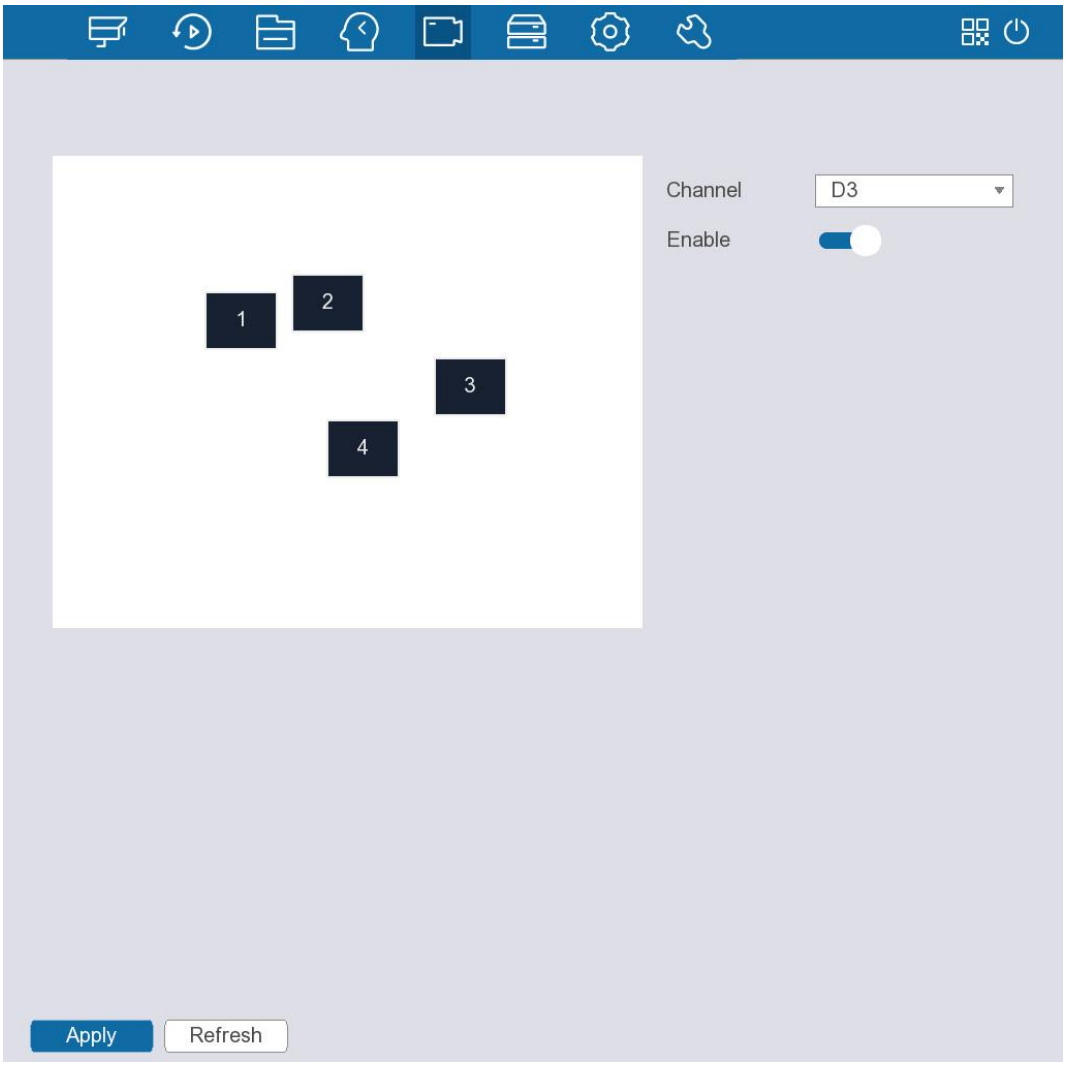
5.10.5 Configuring Privacy Masking

You can mask part of the image for privacy protection.

Procedure

Step 1 Select **Camera** > **Privacy Masking**.

Figure 5-45 Privacy masking



Step 2 Select a channel, and then configure the masking.

1. Click to enable privacy masking.
2. Click **1**, **2**, **3** or **4** to add a masking block to the image.

   You can add up to four masking blocks for each channel.
3. Adjust the size and position of the masking block.

Step 3 Click **Apply**.

5.10.6 Configuring Video Settings

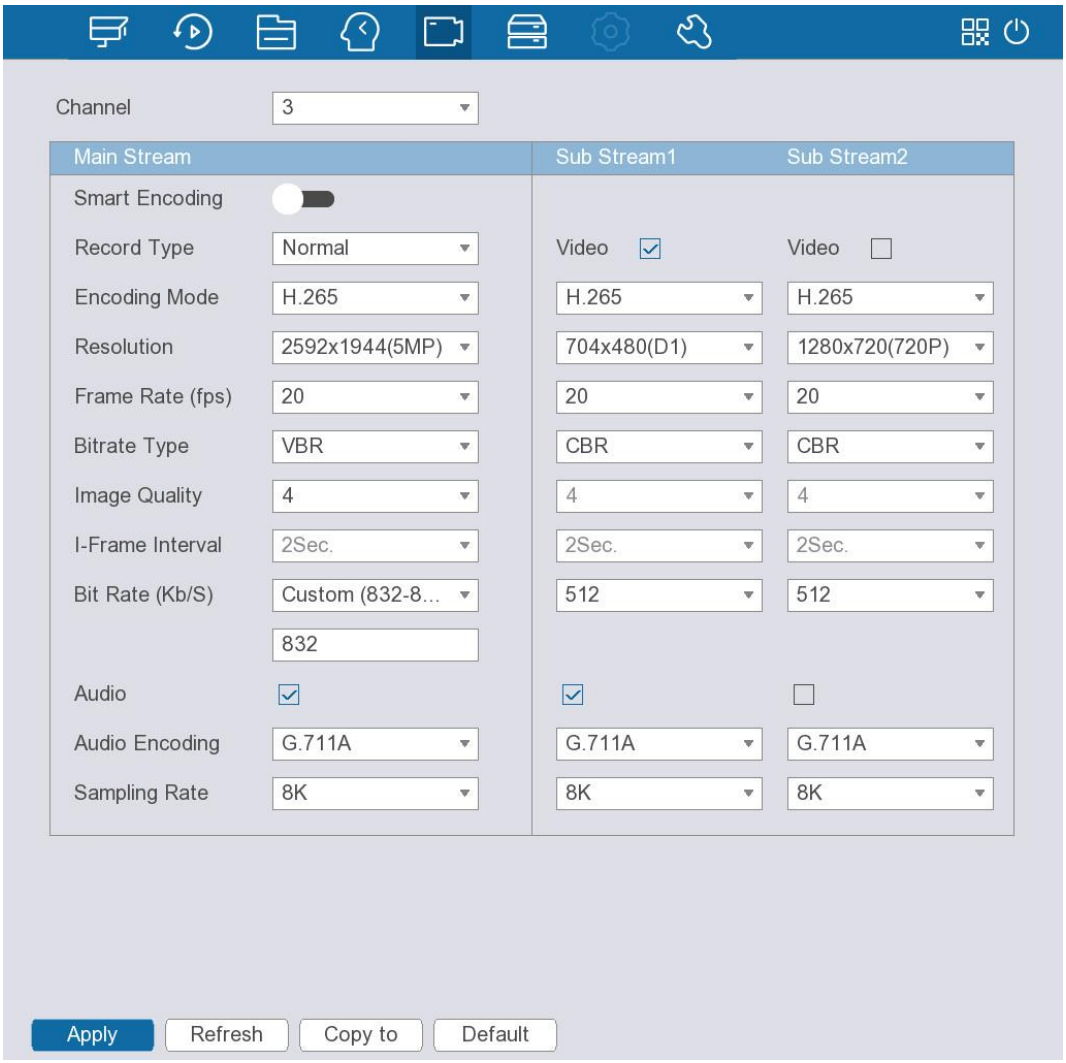
Background Information

Configure the video encoding setting according to the actual bandwidth.

Procedure

Step 1 Select **Camera** > **Video Parameters**.

Figure 5-46 Video parameters



Step 2 Configure the parameters.

Table 5-19 Video settings

Parameter	Description
Channel	Select a channel for which you want to configure the settings.
Smart Encoding	Enable this function to reduce the bit stream for non-important recorded video to maximize the storage space.
Record Type	Select **Normal**, **Motion detection** or **Alarm** for main stream.
Encoding Mode	• H.265 (recommended): Main profile encoding. This format is recommended. • H.264H: High profile encoding. Low bit stream with high definition. • H.264: General profile encoding. • H.264B: Baseline profile encoding. • MJPEG: In this format, the image requires big bit rate value to ensure clarity.

Parameter	Description
Resolution	Select a resolution for the video.  The maximum resolution available might vary with the models.
Frame Rate (FPS)	Configure the frames per second for the video. The bigger the value, the clearer and smoother the image. Frame rate changes along with the resolution.
Bitrate Type	• **CBR** (Constant Bitrate): The bit rate changes slightly around the defined value. We recommended selecting constant stream when there might be only small changes in the monitoring environment. • **VBR** (Variable Bitrate): The bit rate changes with monitoring scenes. Select variable stream when there might be big changes in the monitoring environment.
Image Quality	The bigger the value, the better the image quality.  This parameter is available when the **Bitrate Type** is **VBR**.
I-Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	• Main stream: The higher the bitrate, the better the image quality. • Sub stream: For constant stream, the bitrate changes near the defined value; for variable stream, the bitrate changes along with the image but the maximum value still stays near the defined value.
Audio Encoding	Select an audio encoding format.
Sampling Rate	Set how many times per second a sound is sampled. The bigger the value, the more natural the sound.

Step 3 Click **Apply**.

5.11 Storage

You can configure the recording plan, recording mode, storage strategy, and more.

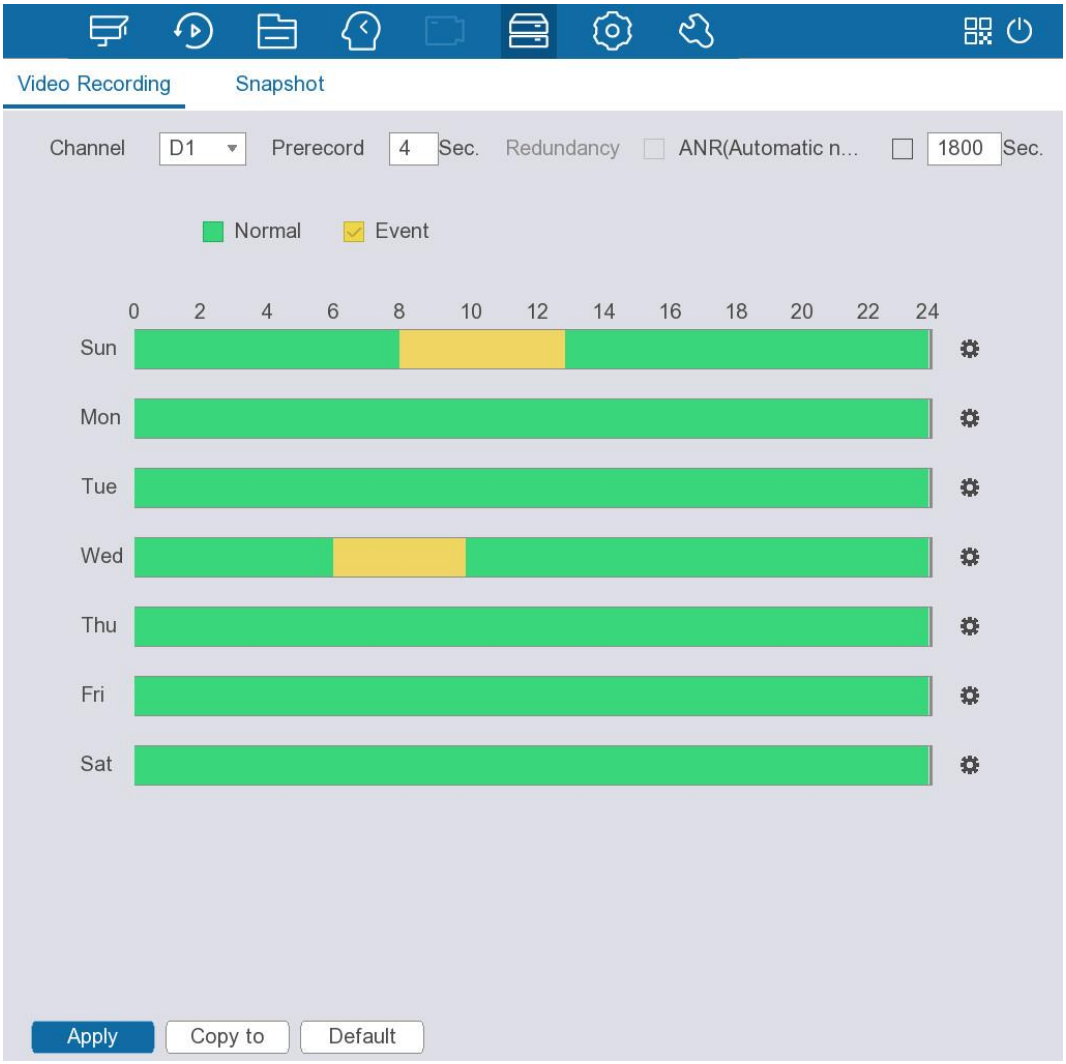
5.11.1 Configuring Recording Plan

Configure the recording plans for videos and snapshots. This section uses video recording as an example. The configuration of snapshot plan is similar.

Procedure

Step 1 Select **Storage** > **Recording Plan**.

Figure 5-47 Video recording



Step 2 Configure recording settings.

Table 5-20 Video recording parameters

Parameter	Description
Channel	Select a channel to record videos.
Prerecord	Set how long the device records before an event.

Parameter	Description
Redundancy	Enable redundancy for the channel. If there are two or more HDDs installed on the Device, you can set one of the HDDs as the redundant HDD to back up the recorded files. • If the selected channel is not recording, the redundancy function takes effect next time you record no matter you select the checkbox or not. • If the selected channel is recording, the current recorded files will be packed, and then the Device starts recording according to the new schedule. 📖 • This function is available on select models. • The redundant HDD only backs up videos but not snapshots.
Automatic network replenishment (ANR)	You can set the ANR (auto network resume) function. • The IPC continues recording once the NVR and IPC connection fails. After the network becomes normal, the NVR can download recording files while it is disconnected from the IPC. This is to help protect against data loss from the current IPD channel that is connected. • Set the maximum recording upload period. If the offline period is longer than the period you set, IPC will only upload the recording file during the specified period. 📖 Make sure that SD card is installed and the recording function is enabled on the IPC.
Event type	Select **Normal** or **Event**, and the default is **Normal**.
Time Period	Set a period during which the configured recording settings are active. • On the time line, drag to set the period. • You can also click ⚙ to set the period.
Default	Restore the recording plan to default settings.
Copy to	Copy the recording plan to other channels.

Step 3 Click **Apply**.

5.11.2 Configuring Storage Strategy

Configure storage strategy and manage the HDDs.

Procedure

Step 1 Select **Storage** > **Disk Management**.

Step 2 Configure the storage strategy.

Figure 5-48 Disk management

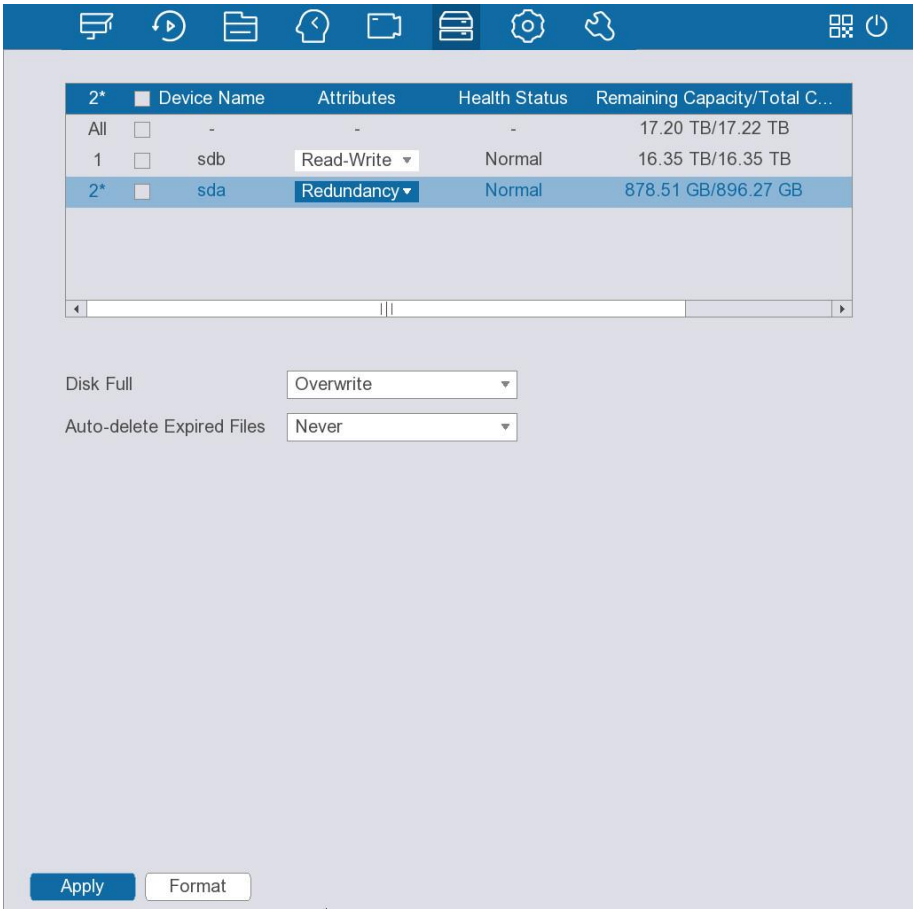


Table 5-21 Disk management parameters

Parameter	Description
Disk Full	Configure the storage strategy to be used when no more storage space is available. • Stop: Stop recording. • Overwrite: The newest files overwrite the oldest ones.
Auto-delete expired files	Configure whether to allow the Device to delete expired automatically. • Select **Never** if you do not want to use the function. • Select **Custom** and then configure how long you want to keep the old files.

Step 3 On the disk list, view the HDD information and configure the HDD type.

- Set HDD type.

  In the **Attributes** column, select **Read-Write**, **Read-only** or **Redundancy** to set the HDD type.
- Format HDD.

  Select an HDD and then click **Format**, and then follow the on-screen prompt to format the HDD.

⚠

Formatting will erase all data on the HDD. Please be advised.

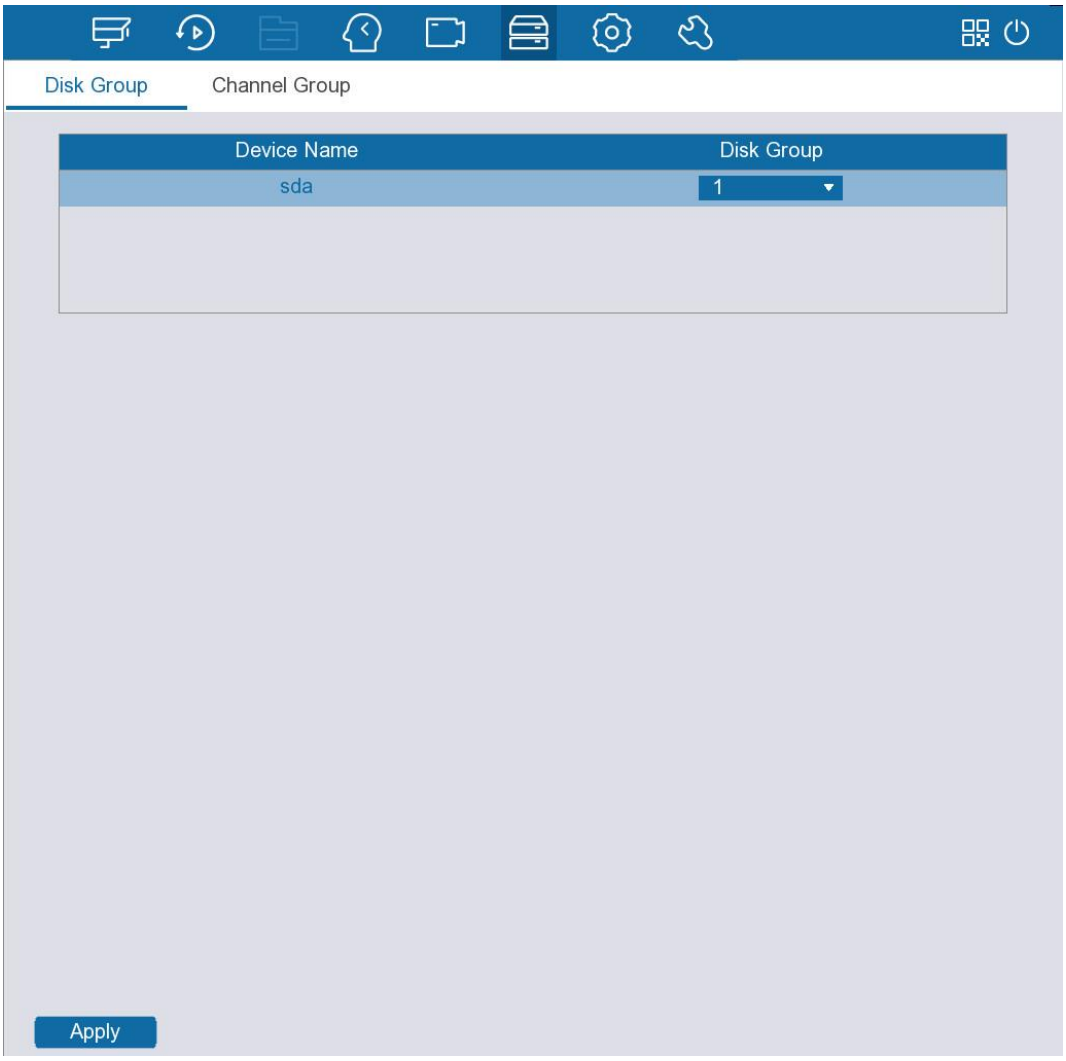
5.11.3 Configuring Disk Group

By default, the installed HDD and created RAID are in Disk Group 1. You can set HDD group, and HDD group setup for main stream, sub stream and snapshot operation.

Procedure

Step 1 Select **Storage** > **Disk Group** > **Disk Group**.

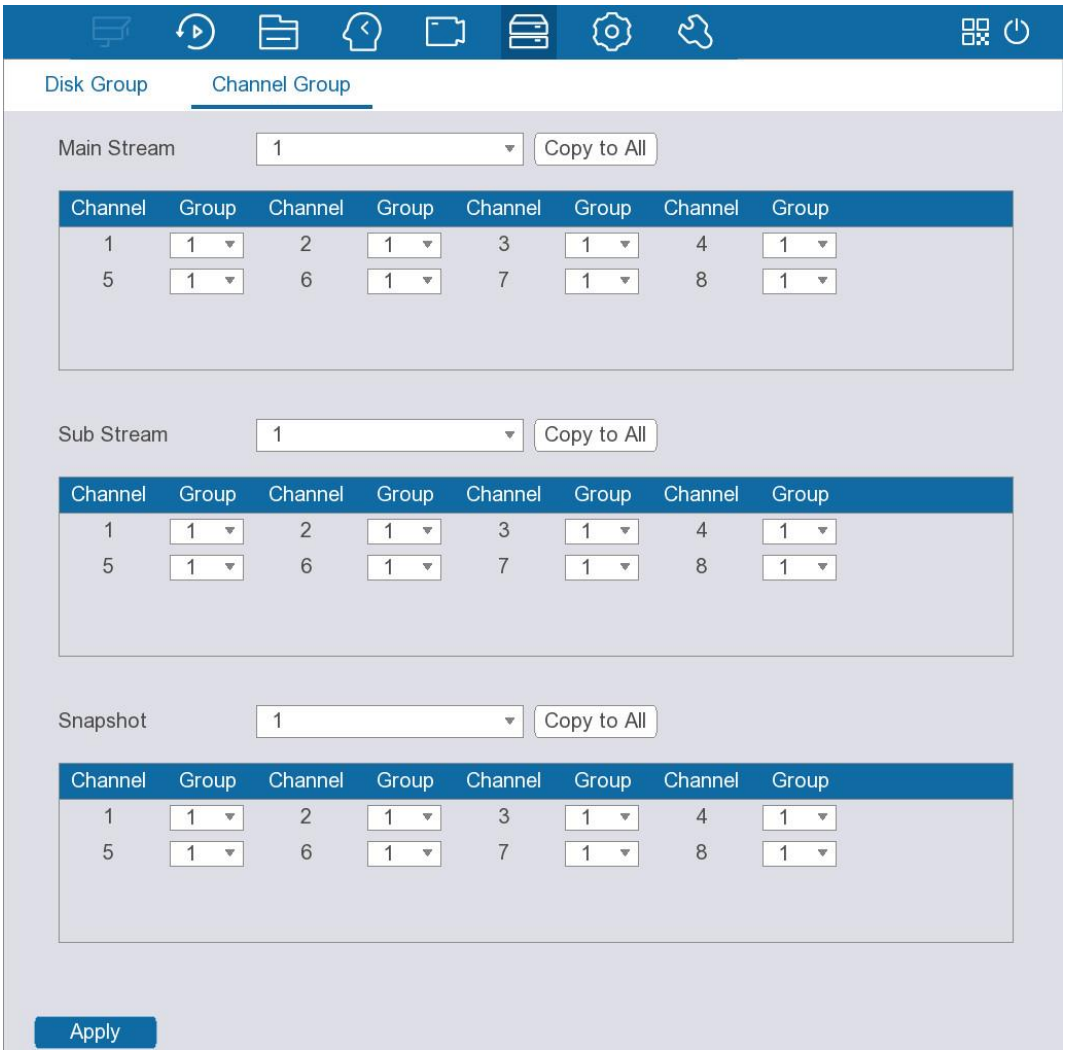
Figure 5-49 Disk group



Step 2 Select the group for each HDD, and then click **Apply**.

After configuring HDD group, under the **Channel Group** tab, configure settings to save the main stream, sub stream and snapshot to different disk groups, and then click **Apply**.

Figure 5-50 Channel Group



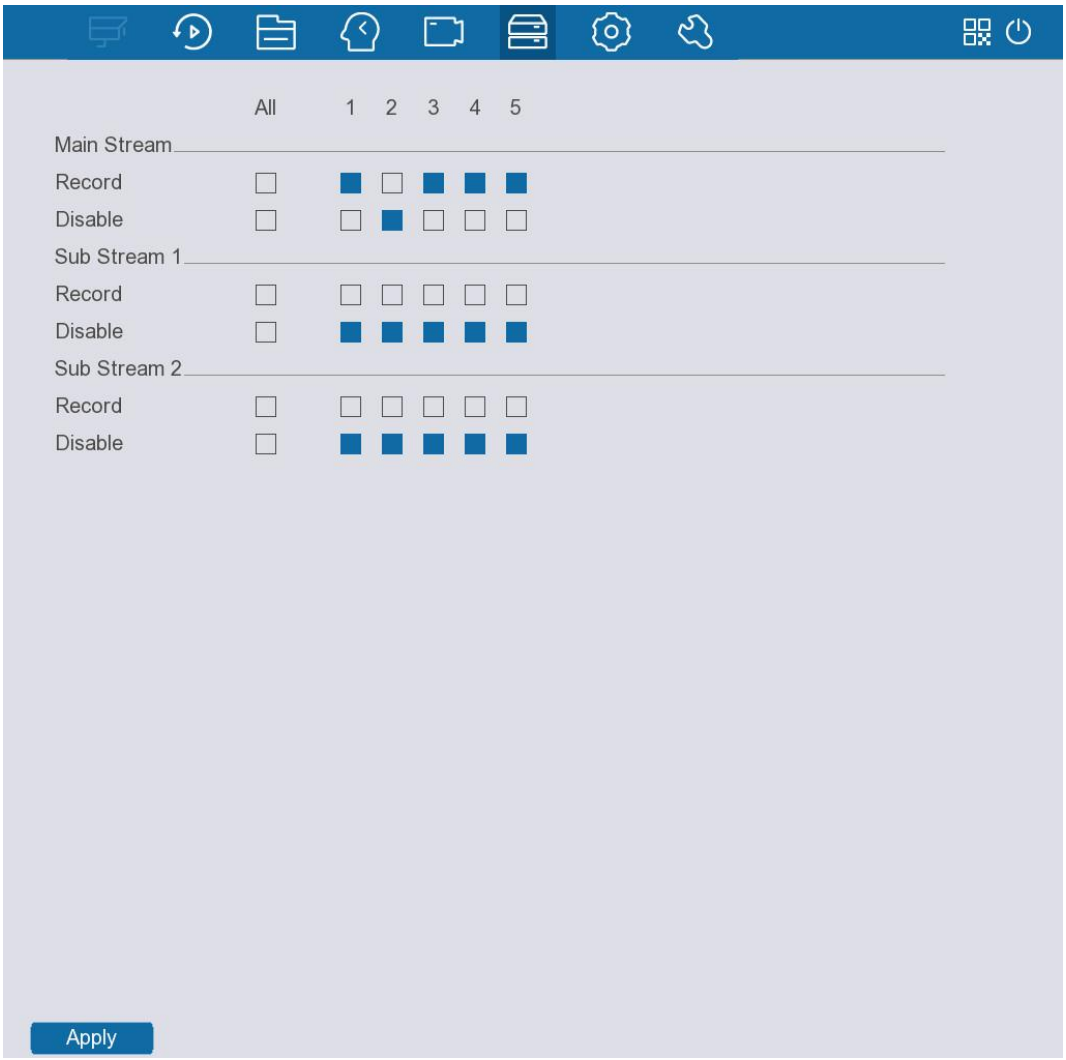
5.11.4 Configuring Recording Mode

Enable or disable the video recording for each channel. The device keeps recording all the time.

Procedure

Step 1 Select **Storage** > **Recording Mode**.

Figure 5-51 Recording mode



Step 2 Enable recording for each channel.

You can select **All** if you want to configure the same recording mode for all channels.

Step 3 Click **Apply**.

5.12 System

You can configure the system settings, including date, accounts, display output and more.

5.12.1 Configuring General System Settings

Configure general system settings, such as device name, date and holiday.

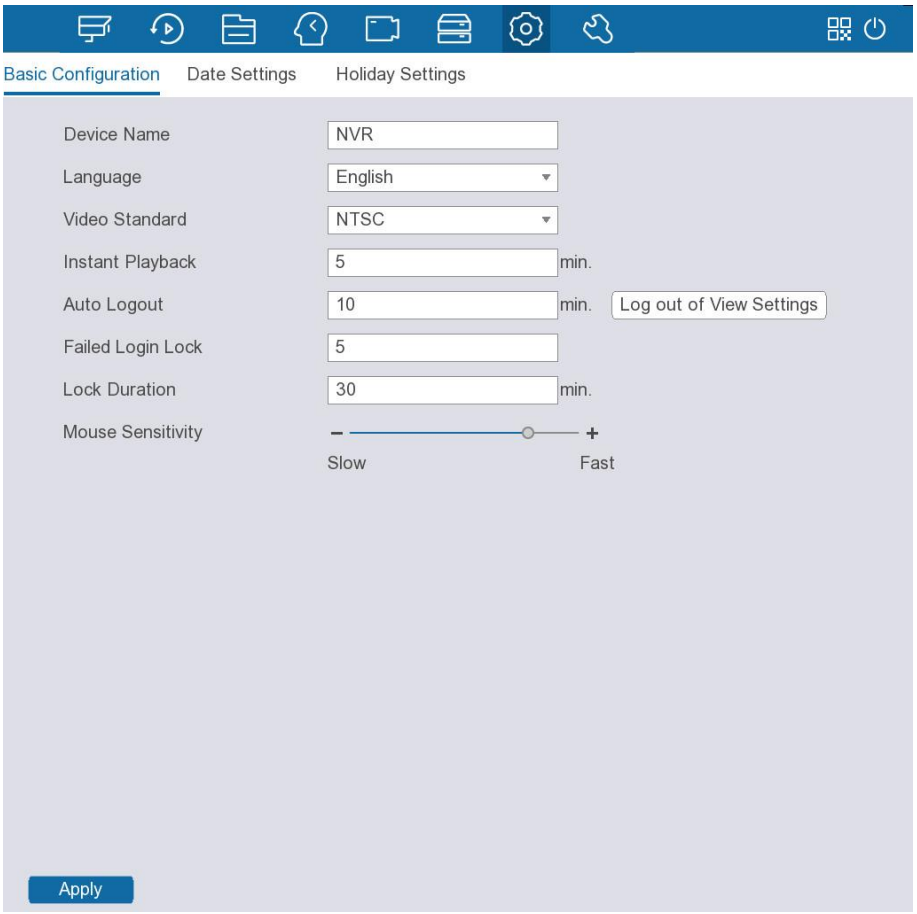
5.12.1.1 Configuring Basic Configuration

Configure basic configurations such as video standard, logout time, and mouse sensitivity.

Procedure

Step 1 Select **System** > **General** > **Basic Configuration**.

Figure 5-52 Basic configuration



Step 2 Configure the parameters.

Table 5-22 Parameters of basic configuration

Parameter	Description
Device Name	Configure the device name.
Language	Displays the system language.
Video Standard	Select **PAL** or **NTSC** as needed.
Instant Playback	Configure the length of time for instant playback. On the live page, you can click to play back recorded file of previous 5 to 60 minutes.
Auto Logout	Enter the time of inactivity before logout. The Device logs out automatically after the period of inactivity. Click **Log out of View Settings** to select the channels that you want to continue monitoring after logout.
Failed Login Lock	Configure the number of allowed failed login attempts before the account is locked for a defined period.
Duration	Configure the duration, and if the number of failed login attempts reaches the defined threshold, the account will be locked for the defined duration.

Parameter	Description
Mouse Sensitivity	Adjust the speed of double-clicking.

Step 3 Click **Apply**.

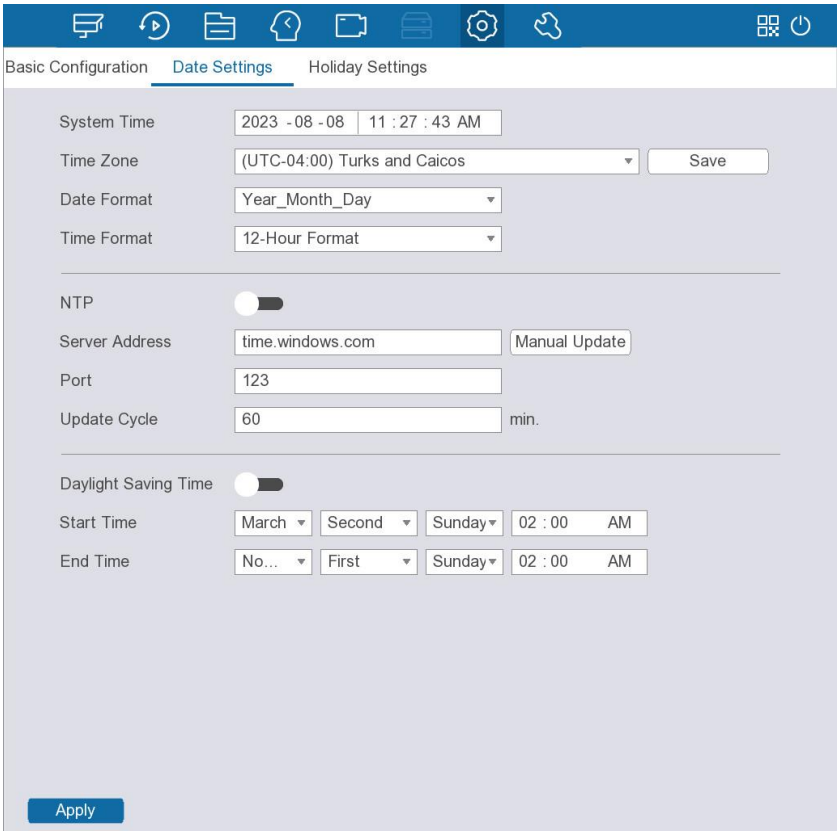
5.12.1.2 Configuring Date Settings

Configure date and time settings.

Procedure

Step 1 Select **System** > **General** > **Date Settings**.

Figure 5-53 Date settings



Step 2 Configure the parameters.

Table 5-23 Parameters of date and time

Parameter	Description
System Time	In the **System Time box**, enter time for the system. Click the time zone list, you can select a time zone for the system, and the time in adjust automatically. ⚠ Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.

Parameter	Description
Time Zone	Select a time zone and then click **Save**.
Date Format	Select a date format.
Time Format	Select **12-Hour Format** or **24-Hour Format**.
NTP	After enabling the NTP function, the system time will be automatically synchronized with the NTP server. 1. Click to enable the function. 2. Configure the address and port of the NTP server. 3. Set the update cycle.
Daylight Saving Time	If your country or region adopts the practice of daylight saving time, you can enable the function to ensure that the system time is correct. 1. Click to enable the function. 2. Set the start time and end time.

Step 3 Click **Apply**.

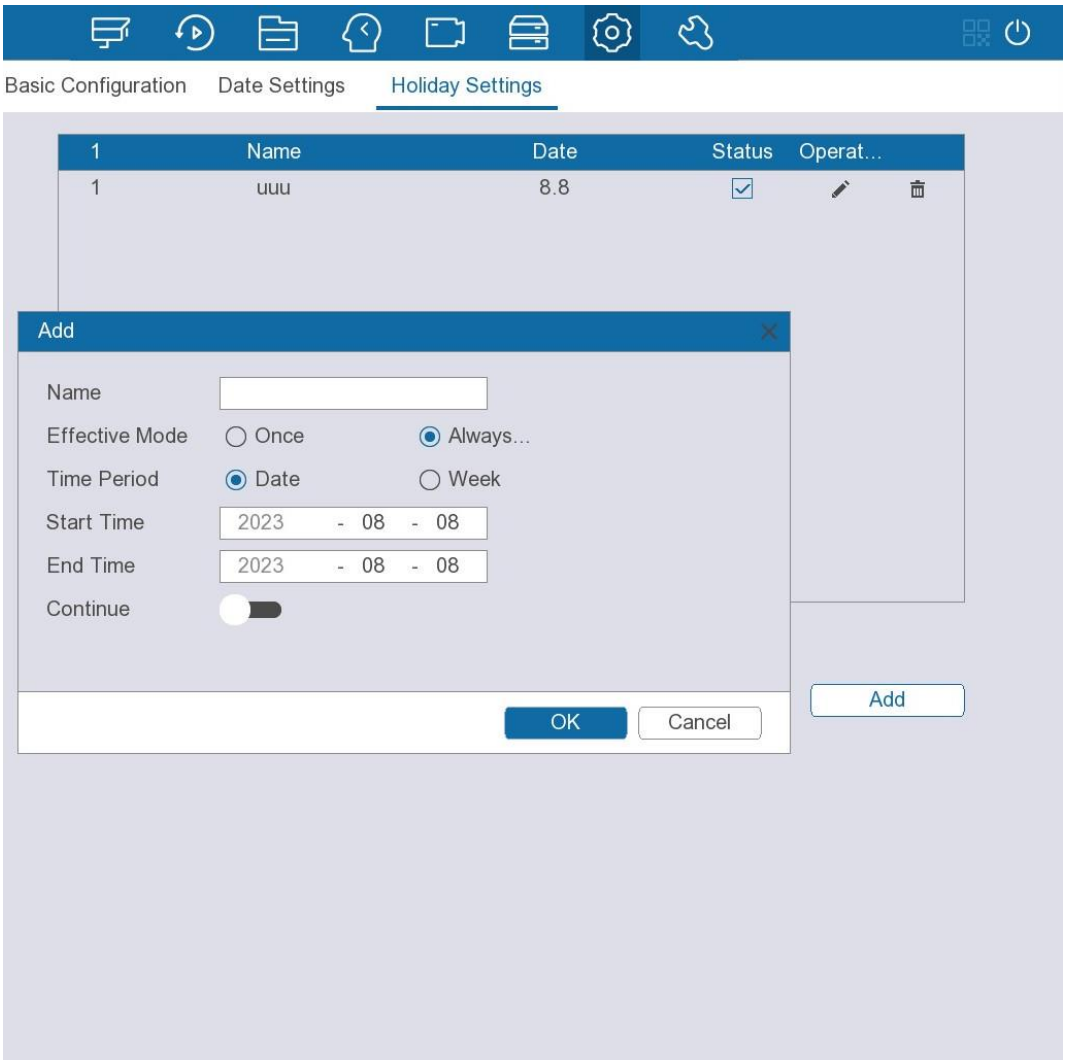
5.12.1.3 Configuring Holiday Settings

You can add holidays for which you can configure recording plan separately.

Procedure

Step 1 Select **System** > **General** > **Holiday Settings**, and then click **Add**.

Figure 5-54 Add holidays



Step 2 Configure the holiday name, effective mode, and time period.

Step 3 (Optional) Enable **Continue** to add more holidays.

Step 4 Click **OK**, you can add current holiday to the list.

Click to change the holiday information. Click to delete current date.

Related Operations

Go to **Storage** > **Recording Plan** to configure the recording plan for the holiday. For details, see "5.11.1 Configuring Recording Plan".

5.12.2 Configuring Account Settings

You can add and manage users, ONVIF users, and user groups and set information for password reset.

5.12.2.1 Adding Users

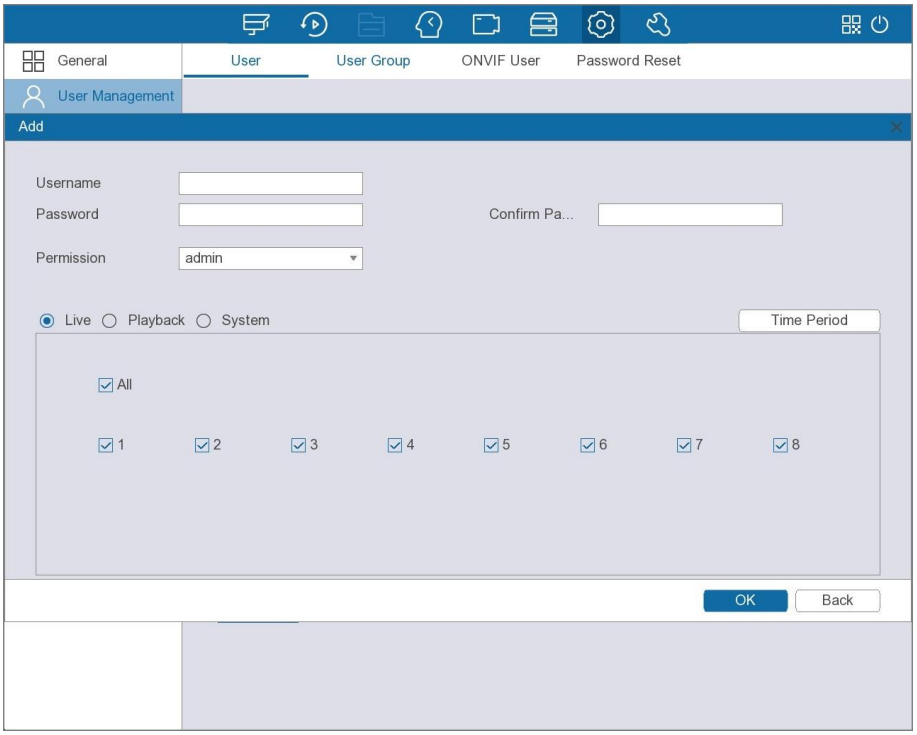
A user can access and manage the Device. The default administrator of the Device is admin, which cannot be modified or deleted. You can add more users and grant the users permissions within the permission range of the corresponding user group.

Procedure

Step 1 Select **System** > **User Management** > **User**.

Step 2 Click **Add**.

Figure 5-55 Add user



Step 3 Configure the parameters.

Table 5-24 Parameters of adding user

Parameter	Description
Username	Enter a name for the user.
Password	Enter the password, and then enter the password again to confirm it.
Confirm Password	
Time Period	Click **Time Period** to set a period during which the new user can log in to the device. The user cannot access the device in other periods.
Permission	Select a group for the user. The permissions of the user must not exceed the permissions of the user group.

Step 4 Select the checkbox under the **Live** tab, **Playback** tab, and **System** tab as required respectively.

Step 5 Click **OK**.

5.12.2.2 Adding User Groups

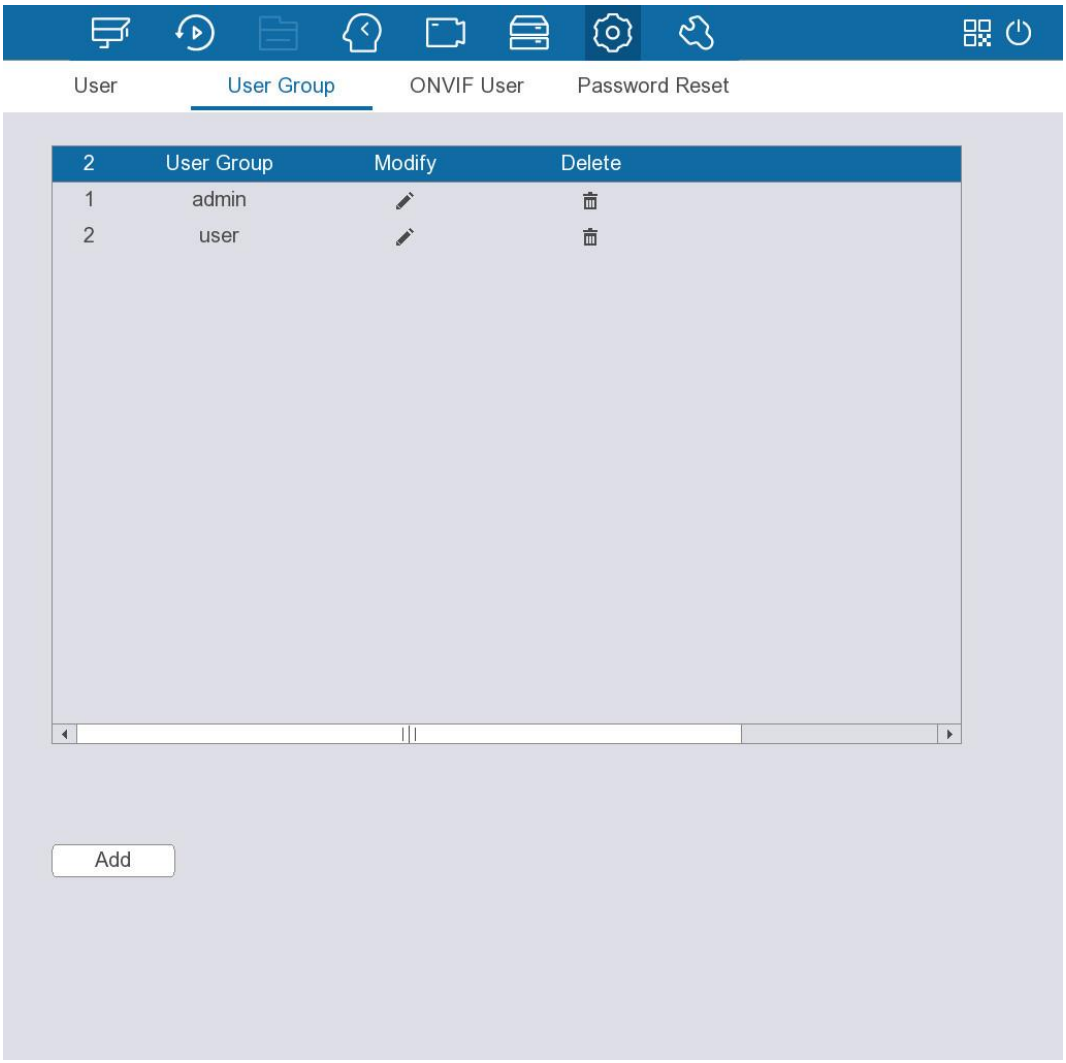
The accounts of the device adopt two-level management mode: user and user group. Every

user must belong to a group, and one user only belongs to one group. The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

Procedure

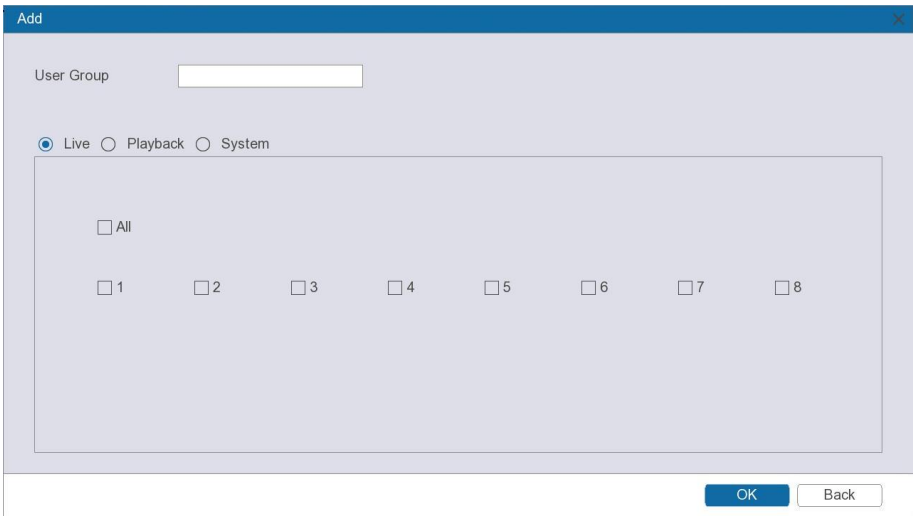
Step 1 Select **System** > **User Management** > **User Group**.

Figure 5-56 User group



Step 2 Click **Add**.

Figure 5-57 Add user group



Step 3 Enter group name.

Step 4 Select the checkbox under the **Live** tab, **Playback** tab, and **System** tab as required respectively.

Step 5 Click **OK**.

5.12.2.3 Adding ONVIF Users

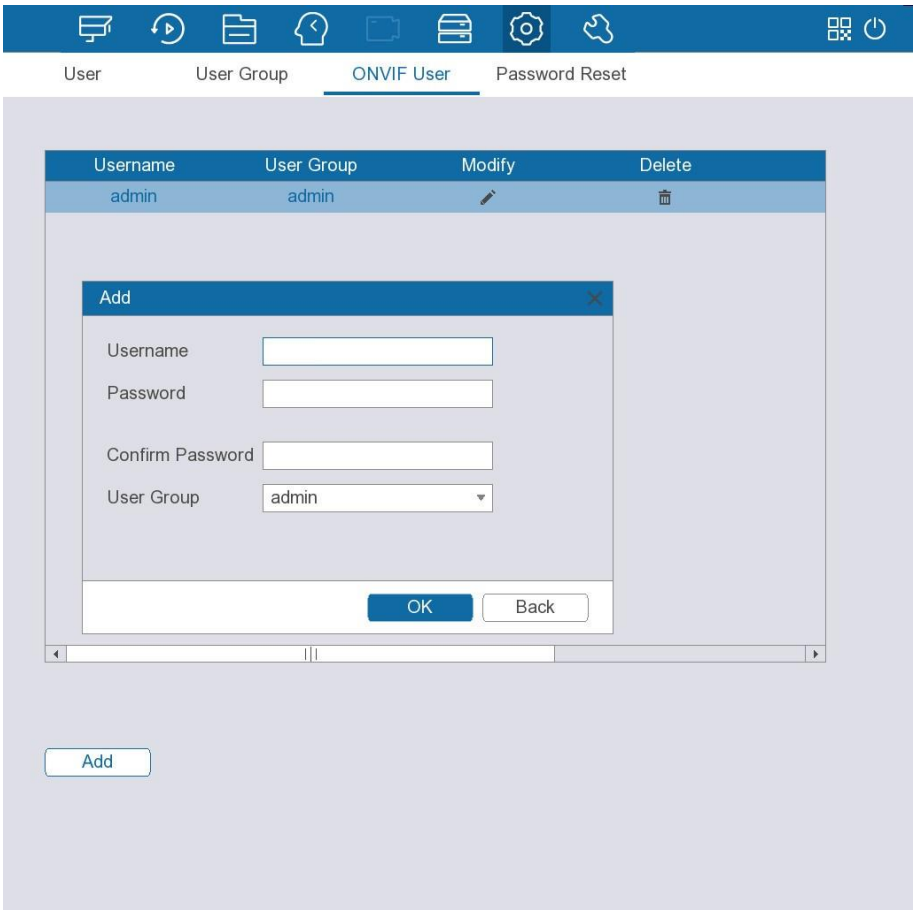
The devices from other manufacturers can connect with the device through ONVIF protocol by using a verified ONVIF account.

Procedure

Step 1 Select **System** > **User Management** > **ONVIF User**.

Step 2 Click **Add**.

Figure 5-58 Add ONVIF user



Step 3 Configure username, password and user group.

There are three ONVIF user groups by default: admin, operator and user. You cannot add ONVIF user group manually.

Step 4 Click **OK**.

5.12.2.4 Resetting Password

You can use email address or answer the security questions to reset password if you forgot it.

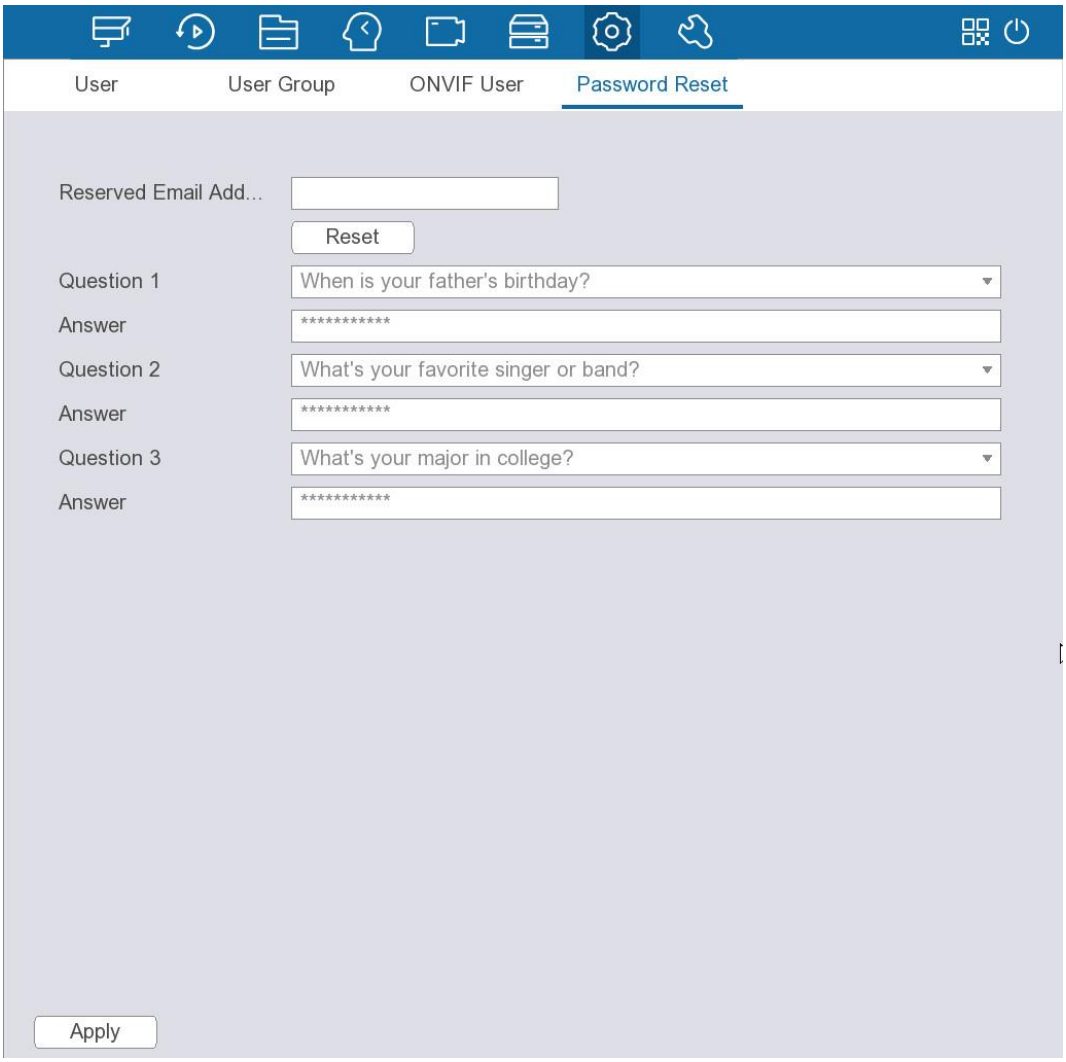
5.12.2.4.1 Configuring Password Reset

Configure the linked email address and security questions that are used to reset the password.

Procedure

Step 1 Select **System** > **User Management** > **Password Reset**.

Figure 5-59 Password reset



Step 2 Enter an email address to receive the security code used to reset the password.

Step 3 Set security questions.

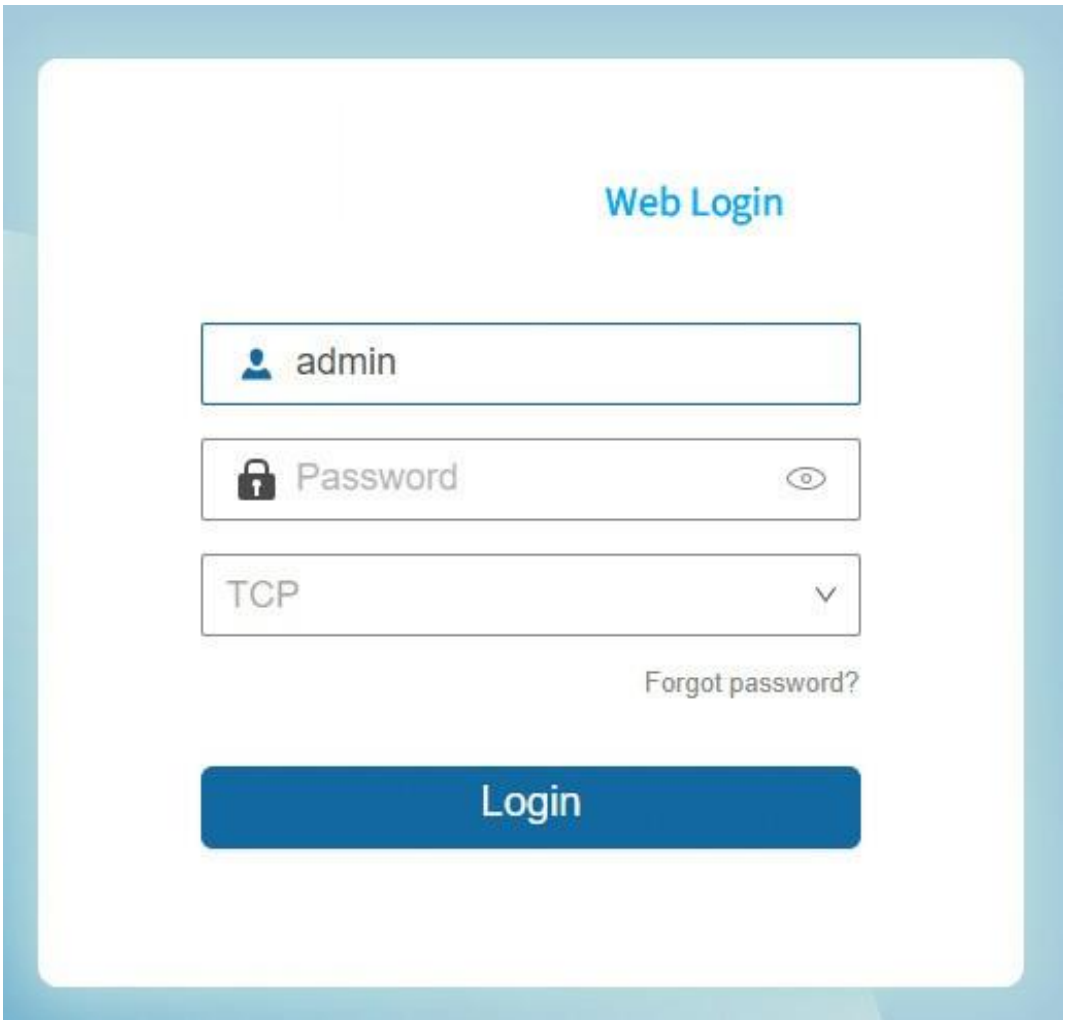
Step 4 Click **Apply**.

5.12.2.4.2 Resetting Password on Local Interface

Procedure

Step 1 After the Device starts, click the live page.

Figure 5-60 Login

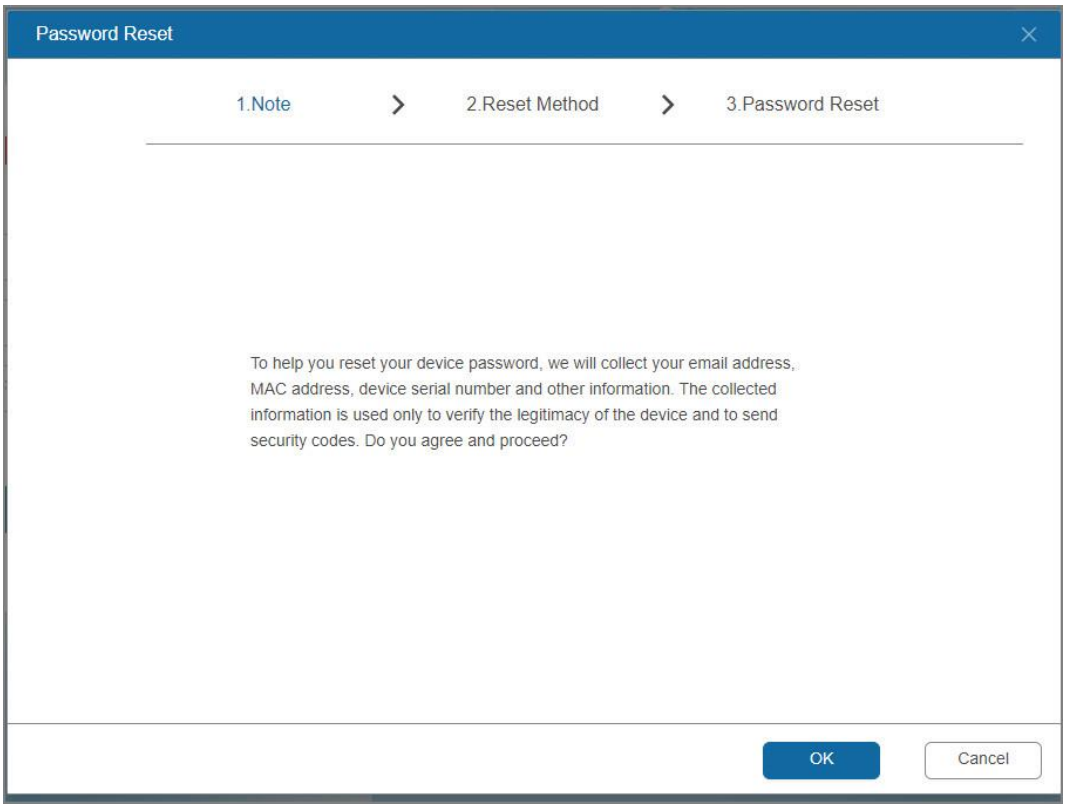


Step 2 Click **Forgot password?**.

- If you have configured the linked email address, the system will notify you of data collection required for resetting password.
- If you have not configured the linked email address, the system prompts you to enter an email address. Enter the email address and then click **Next**. Then the system will notify you of data collection required for resetting password.

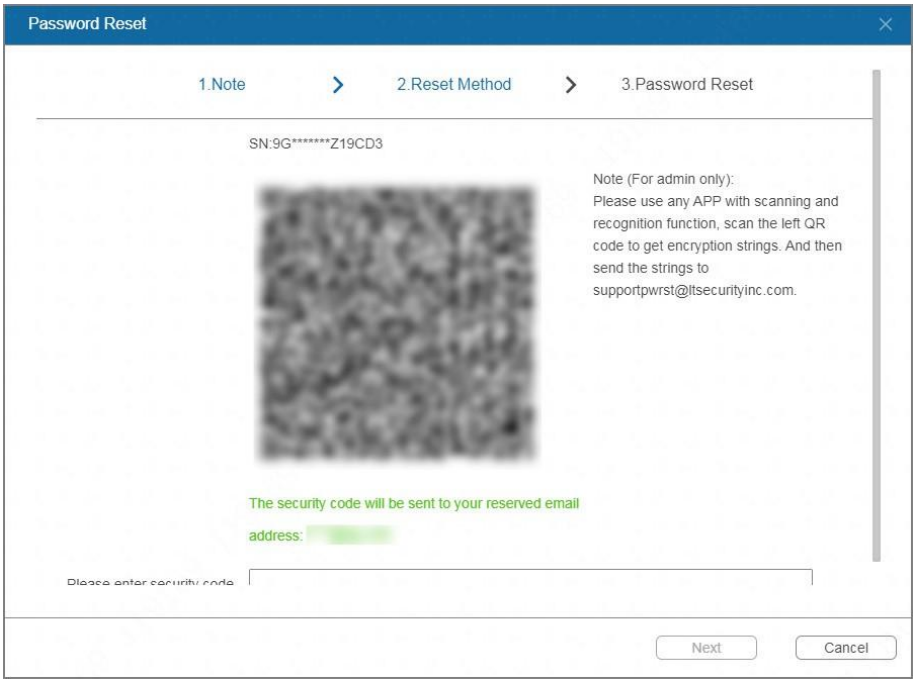
Step 3 Read the prompt, and then click **OK**.

Figure 5-61 Prompt



Step 4 Reset the password by means of mail recovery.

Figure 5-62 Reset password



Follow the on-screen instructions to obtain the security code in your linked email address, and then enter the security code.

- You can get the security code twice by scanning the same QR code. After that, you need refresh the page and then scan the QR code to get the security code.
- The security code sent to your email box is valid within 24 hours. Check your email box in time.

Step 5 Click **Next**.

Step 6 Enter the new password, and then enter the password again to confirm it.

Step 7 Click **OK**.

5.12.3 Configuring Network Settings

Configure the network settings to ensure the Device can communicate with other devices.

5.12.3.1 Configuring Basic Settings

5.12.3.1.1 Configuring TCP/IP Settings

You can configure the settings for the device such as IP address, DNS according to the networking plan.

Procedure

Step 1 Select **System** > **Network** > **Basic** > **TCP/IP**.

Figure 5-63 TCP/IP

Step 2 Configure the network adapter.

Table 5-25 Network adapter parameters

Parameter	Description
IP Version	Both IPv4 and IPv6 are available.
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to set IP address manually.
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. • The IP address and the default gateway must be on the same network segment. • Click **Test** to test whether the IP address is available.
Subnet Mask	
Default Gateway	
MAC Address	Displays the MAC address of the Device.
MTU	Displays the MTU value of the network adapter.

Step 3 Configure the DNS server information, including IP version, and the IP addresses of the preferred DNS server, and backup DNS server.

Step 4 Click **Apply**.

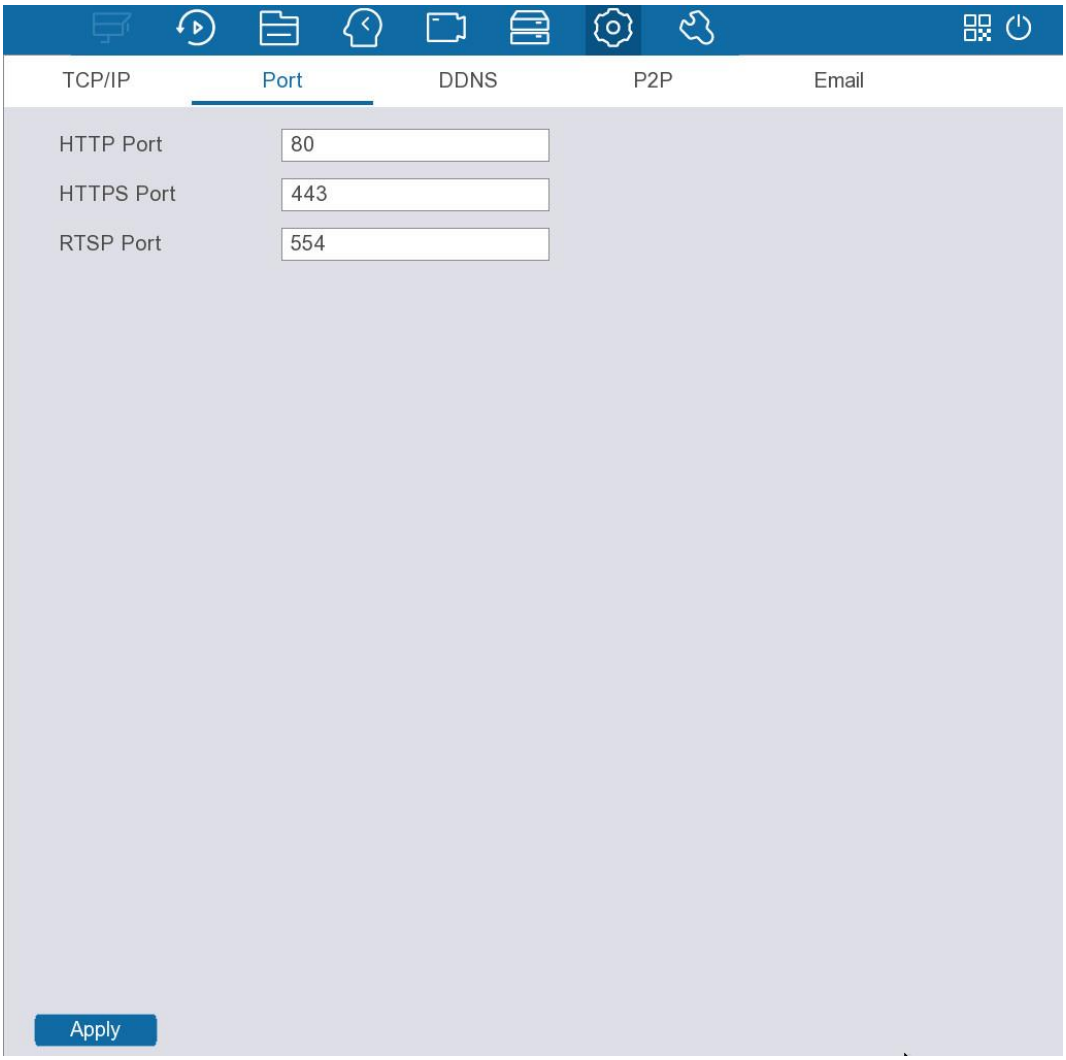
5.12.3.1.2 Configuring Port Settings

You can configure the maximum connection for accessing the device from web, platform, mobile phone or other clients at the same time, and configure each port settings.

Procedure

Step 1 Select **System** > **Network** > **Basic** > **Port**.

Figure 5-64 Port



Step 2 Configure the parameters.

Table 5-26 Port parameters

Parameter	Description
HTTP Port	The default value setting is 80. If you change the port number, for example, 90, then you should enter 90 after the IP address when logging in to the web interface of the Device.
HTTPS Port	HTTPS communication port. The default value is 443. You can enter the value according to your actual situation.
RTSP Port	The default value setting is 554. You can enter the value according to your actual situation.

Step 3 Click **Apply**.

5.12.3.1.3 Configuring DDNS Settings

After you enable DDNS, when the IP address of the Device changes frequently, the system dynamically updates the relation between domain name and IP address on DNS server. You can use domain name to remotely access the Device.

Prerequisites

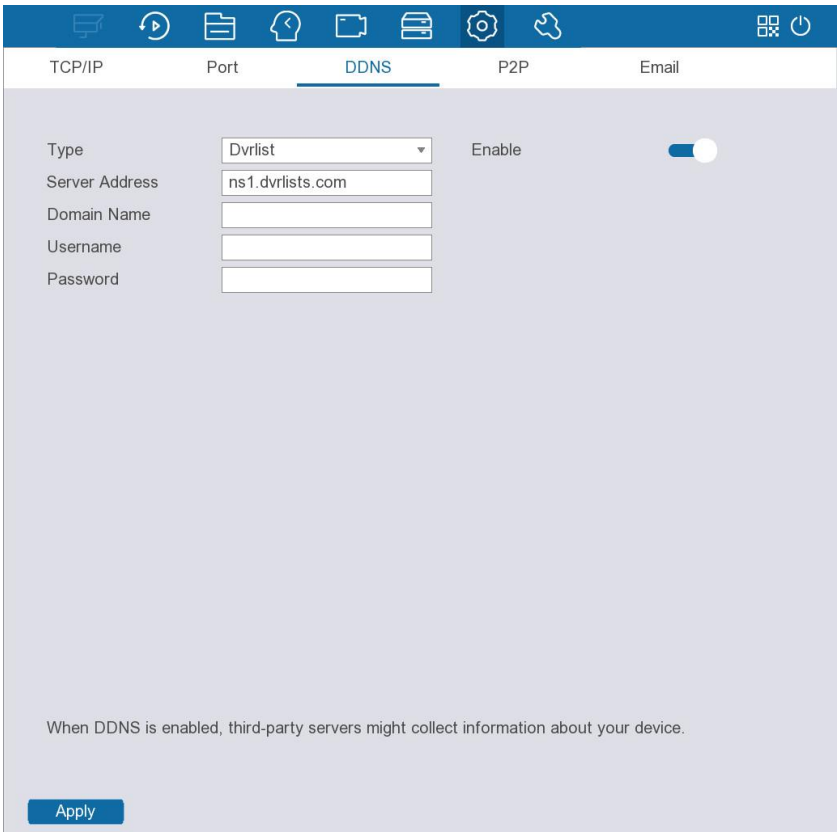
Check the type of DDNS that the Device supports and then log in to the website provided by the DDNS service provider to register domain and other information.

After registration, you can log in to the DDNS website to view the information of all the connected devices under the registered account.

Procedure

Step 1 Select **System** > **Network** > **Basic** > **DDNS**.

Figure 5-65 DDNS



Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 5-27 DDNS parameters

Parameter	Description
Type	Displays the type and address of the DDNS service provider. • For **Dvrlist**, the default address is nsl.dvrlists.com. • For **NO-IP DDNS**, the default address is dynupdate.no-ip.com. • For **CN99 DDNS**, the default address is members.3322.org.
Server Address	
Domain Name	Enter the domain name that you have registered on the DDNS website.
Username	Enter the username and password provided from DDNS service provider.
Password	

Step 4 Click **Apply**.

If the configuration is successful, you can access the web interface of the device by using the domain name.

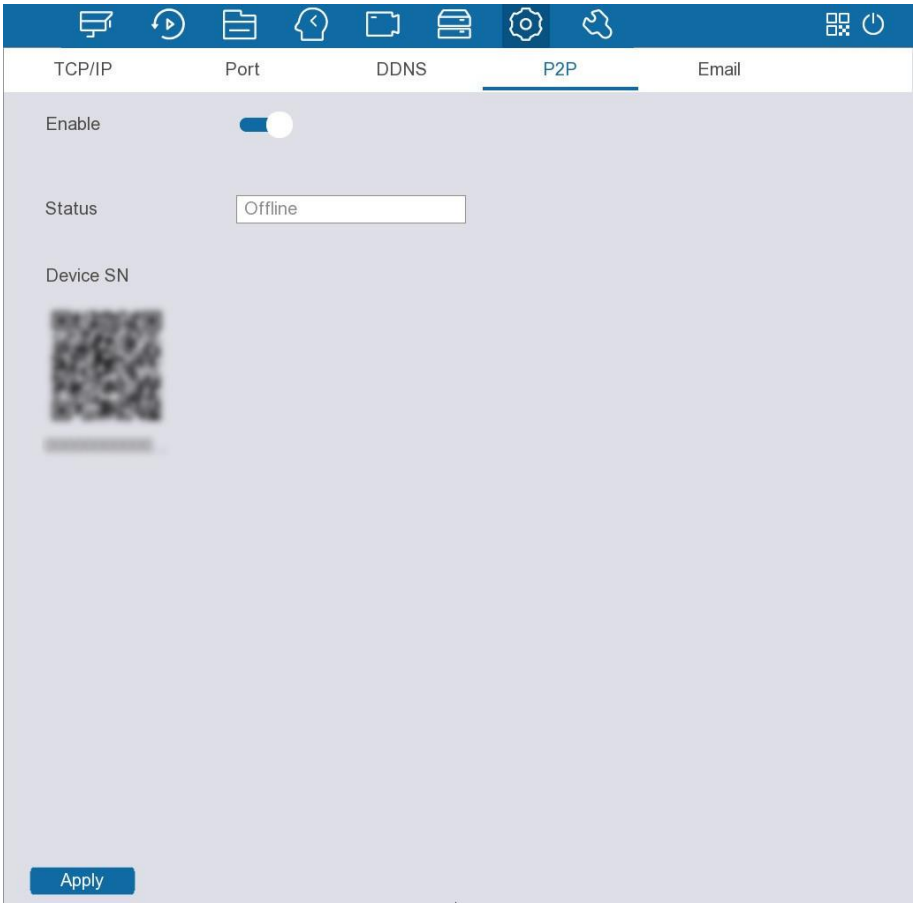
5.12.3.1.4 Configuring P2P Settings

P2P is a peer to peer technology. After downloading mobile app and registering the Device to the app, you can manage the Device remotely on the phone.

Procedure

Step 1 Select **System** > **Network** > **Basic** > **P2P**.

Figure 5-66 P2P



Step 2 Click to enable the function.

Step 3 Click **Apply**.

The P2P function is enabled. After downloading and installing the mobile client, you can use the mobile client to scan the SN QR code to add the Device for remote management.

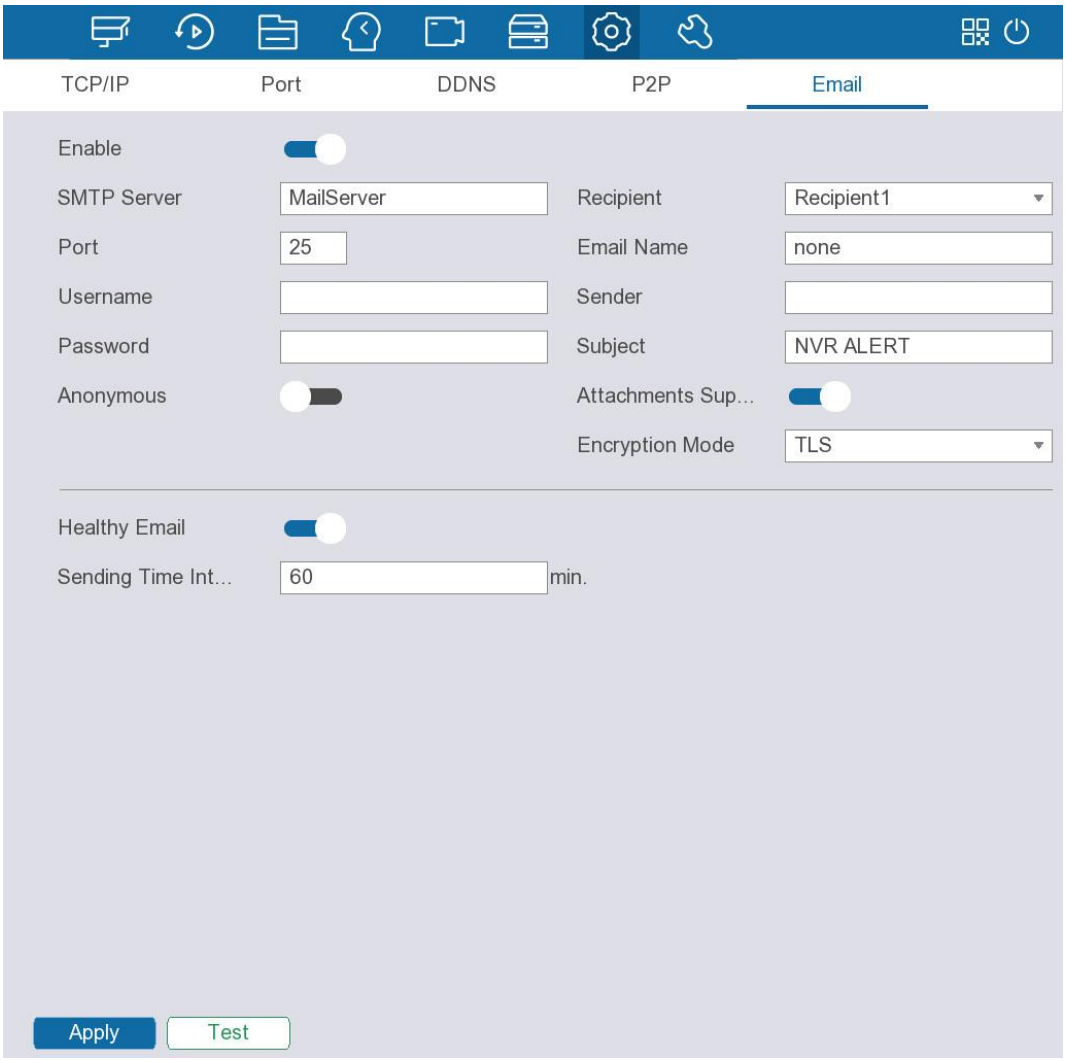
5.12.3.1.5 Configuring Email Settings

Configure the email settings to enable the system to send the email as a notification when an alarm event occurs.

Procedure

Step 1 Select **System** > **Network** > **Basic** > **Email**.

Figure 5-67 Email



Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 5-28 Email parameters

Parameter	Description
SMTP Server	Enter the SMTP server address of the sender's email account.
Port	Enter the port of SMTP server. The default value is 25.
Username	Enter the username and password of sender's email account.
Password	
Anonymous	Enable anonymous login.
Recipient	Select the number of recipient to receive the notification. The Device supports up to three mail recipients.
Email Name	Enter the email address of mail recipient.
Sender	Enter the email address of the sender. You can enter up to three senders separated by comma.
Subject	Enter the email subject.

Parameter	Description
Attachments supported	After enabling the attachment function, when an alarm event occurs, the system attaches snapshots as an attachment to the email.
Encryption Mode	Select **None**, **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.
Healthy Mail	Enable the system to send a test email to check the connection.
Sending Time Interval	Set the interval at which the system send the health test email.

Step 4 Click **Apply**.

Step 5 (Optional) Click **Test** to test the email sending function. If the configuration is correct, the recipient will receive the email.

5.12.3.2 Configuring Security Settings

You can configure the basic services, HTTPS function, and firewall for the Device.

5.12.3.2.1 Configuring Basic Services

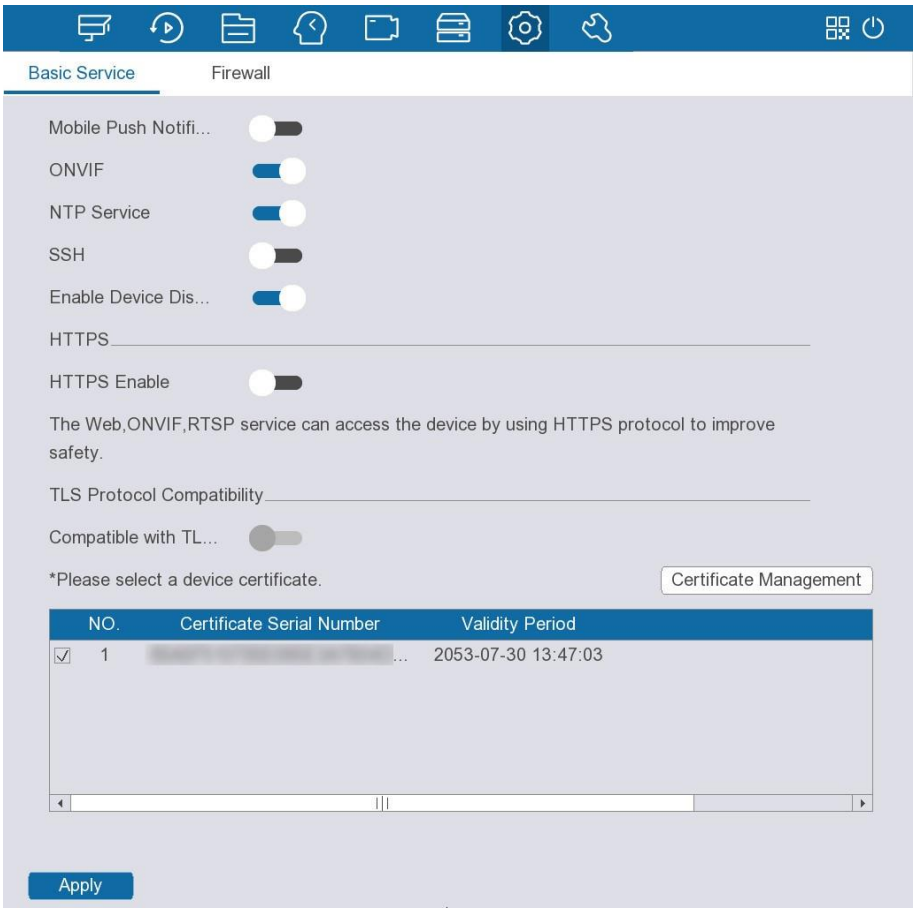
Enable basic services such as mobile push notification, ONVIF, NTP and SSH. HTTPS helps to protect user information and ensure device security and data security. We recommend enabling this function.

Procedure

Step 1 Configure basic services.

1) Select **System** > **Network** > **Security** > **Basic Service**.

Figure 5-68 Basic service



2) Click to enable the system services.

Table 5-29 Basic system services

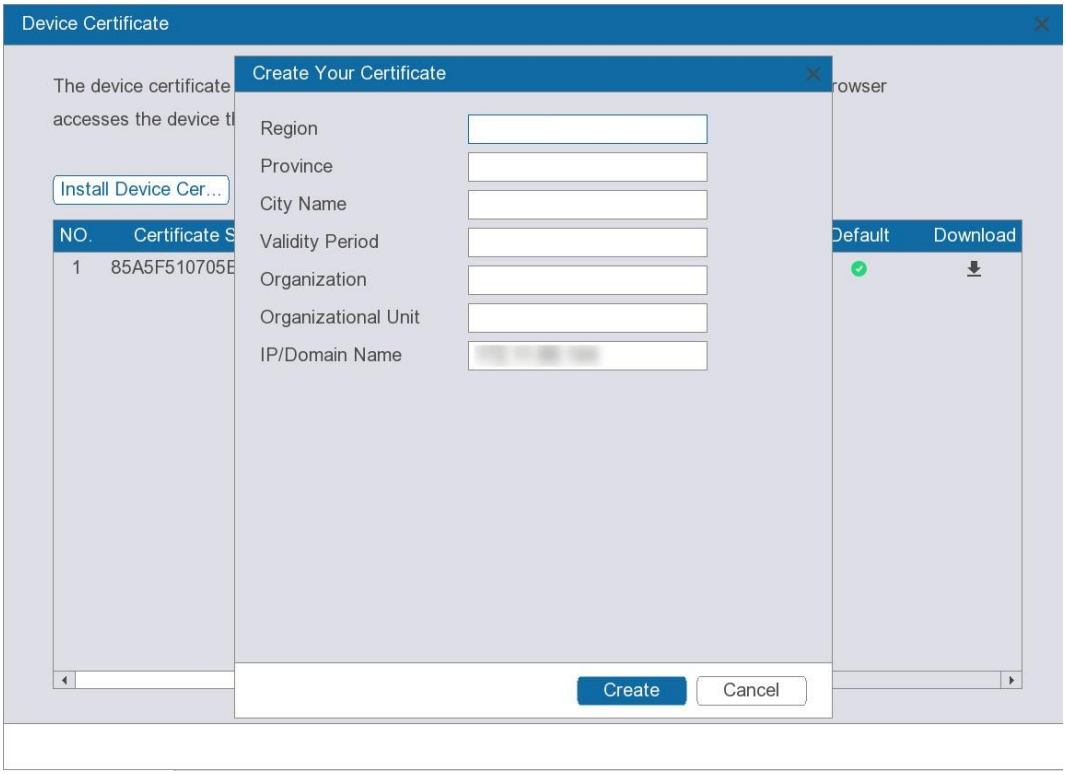
Parameter	Description
Mobile Push Notification	After enabling this function, you can receive alarm information from the Device on the mobile client. To reduce security risks, disable this function when it is not needed.
ONVIF	After the function is enabled, remote devices can connect to the device through the ONVIF protocol. To reduce security risks, disable this function when it is not needed.
NTP Service	After enabling this function, you can use the NTP server for time synchronization.

Parameter	Description
SSH	After enabling this function, you can access the device through the SSH protocol for system debugging and IP configuration. To reduce security risks, disable this function when it is not needed.
Enable Device Discovery	Enable the device to be found by other devices through search.

3) Click to enable the HTTPS function.
4) Click to enable compatibility with the TLS protocol.

   TLS (Transport Layer Security) provides privacy and data integrity between 2 communications applications.
5) Click **Certificate Management** to create an HTTPS certificate.
   a. Click **Install Device Certificate**.
   b. Configure the parameters.
   c. Click **Create**.

Figure 5-69 Create certificate



Step 2 Click **Apply**.

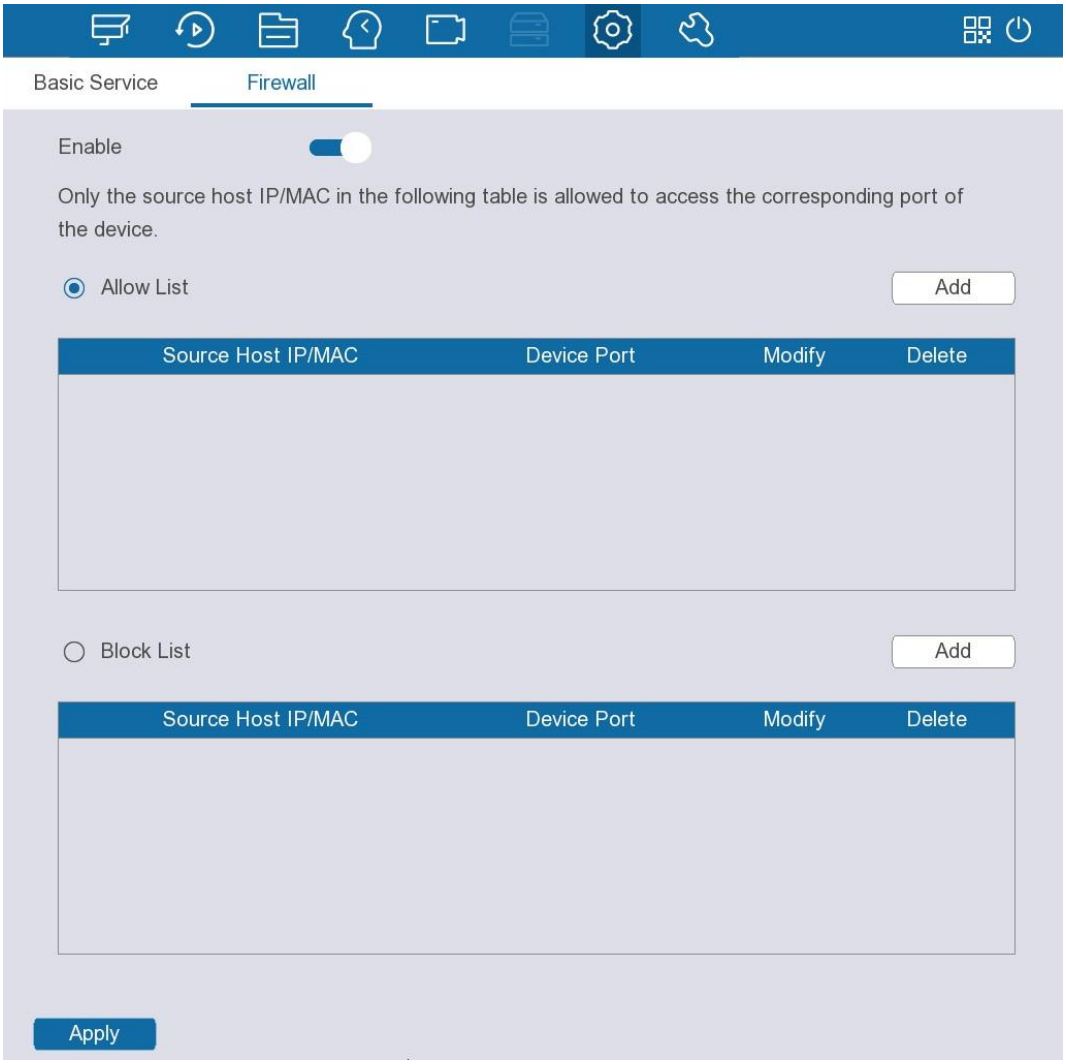
5.12.3.2.2 Configuring Firewall

You can configure the hosts that are allowed or prohibited to access the device.

Procedure

Step 1 Select **System** > **Network** > **Security** > **Firewall**.

Figure 5-70 Firewall



Step 2 Click to enable the firewall.

Step 3 Select a firewall mode.

- Allow list: The hosts on the allowlist can access the device.
- Block list: The hosts on the blocklist are prohibited to access the device.

Step 4 Click **Add** and then select a type for the allowlist or blocklist.

You can allow or prohibit a specific IP address, IP addresses on a specific network segment, or a specific MAC address to access the Device.

- IP address.

  Enter the IP address, starting port and ending port, and then click **OK**.
- IP segment.

  Enter the start address and end address, starting port and ending port, and then click **OK**.
- MAC address.

  Enter the MAC address, and then click **OK**.

Step 5 Click **Apply**.

5.12.4 Configuring Events

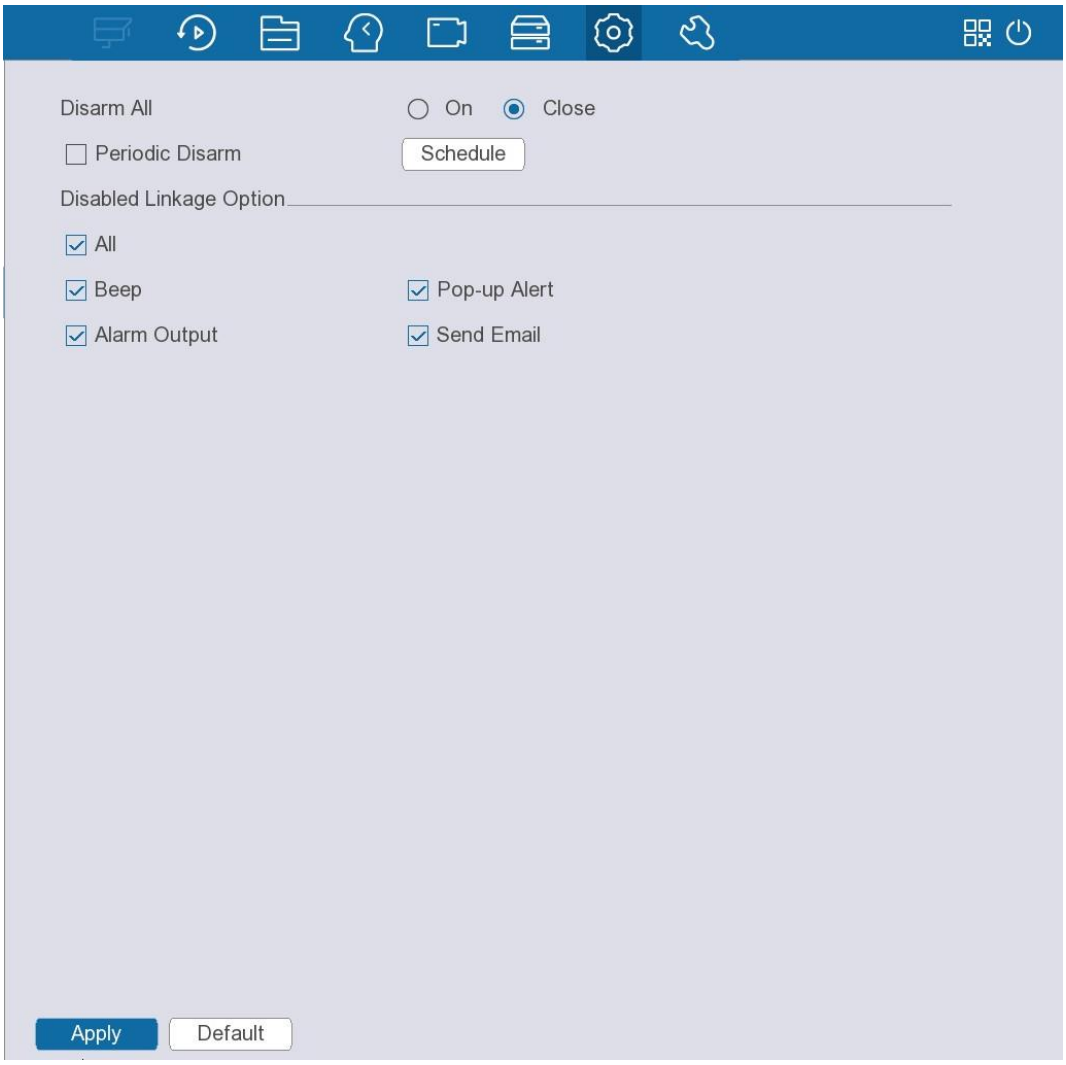
5.12.4.1 Disarming All

You can disarm all alarm linkage actions with one click.

Procedure

Step 1 Select **System** > **Events** > **Disarm All**.

Figure 5-71 Disarming all



Step 2 Enable disarm all or periodic disarm.

- Disarm all: Select **On** to enable this function.
  The alarm will take effect at all times.
- Periodic disarm: Select **Close** for **Disarm All**, and then click **Schedule** to set the disarm period.
  The alarm will take effect at a specific time.

Periodic disarm is available only when disarm all is disabled.

Step 3 Select the alarm linkage actions that you want to disarm.

Table 5-30 Alarm linkage actions

Parameters	Description
Beep	Enable the Device to make a beep noise when an alarm occurs.
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as required. Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".
Pop-up Alert	Enable on-screen prompt of detected motion.
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.

Step 4 Click **Apply**.

5.12.4.2 Configuring Video Detection Alarms

You can configure alarms for events such as motion detection, scene changing, and video tampering.

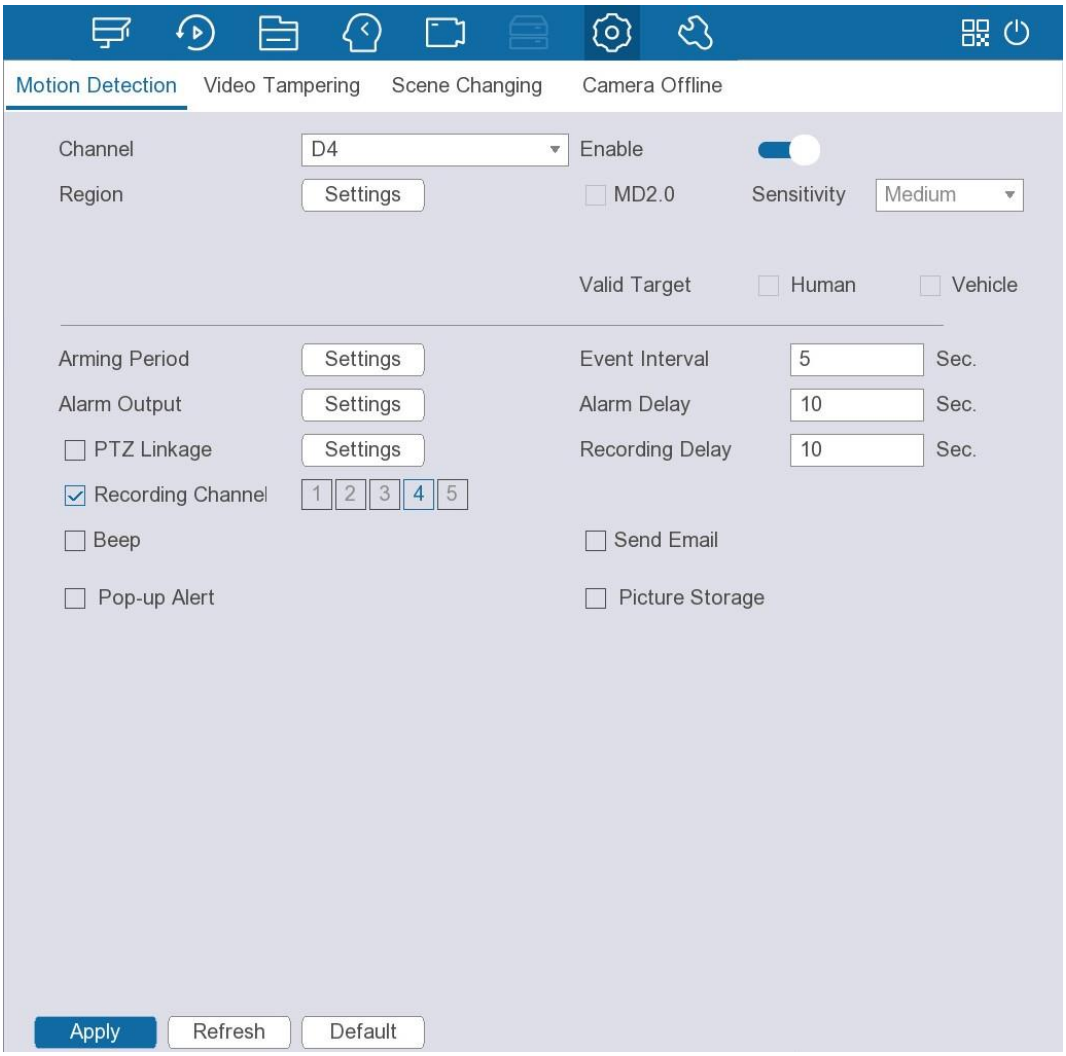
5.12.4.2.1 Configuring Motion Detection Alarms

When a moving object appears and moves fast enough to reach the defined sensitivity threshold, an alarm is triggered.

Procedure

Step 1 Select **System** > **Events** > **Video Detection** > **Motion Detection**.

Figure 5-72 Motion detection

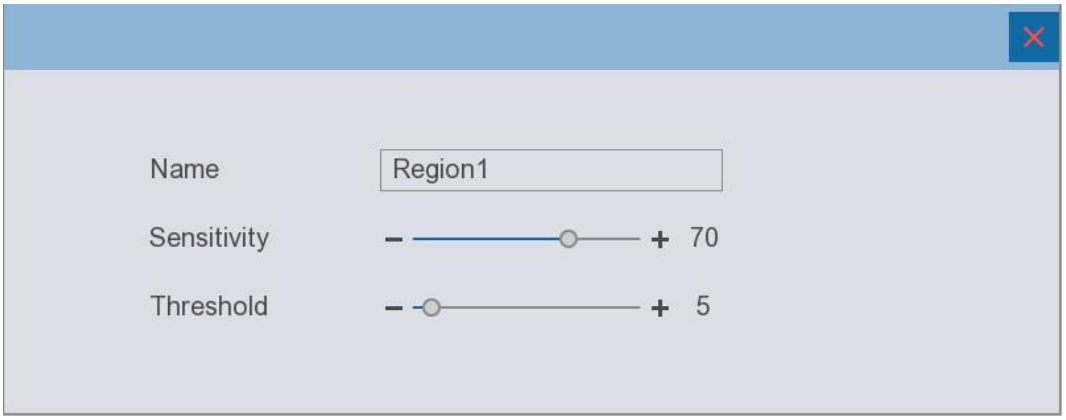


Step 2 Select a channel, and then click next to **Enable** to enable motion detection.

Step 3 Click **Settings** next to **Region** to configure the detection region.

1. Point to the middle top of the page.

Figure 5-73 Detection region



2. Configure the parameters.
   - **Name**: Enter a name to identify the region.
   - **Sensitivity**: Configure the sensitivity for motion detection. The higher the value, the easier to trigger alarm but meanwhile the higher the false alarm rate. We recommend using the default setting.
   - **Threshold**: An alarm is triggered when the percentage of the detected target

to the detection region reaches or exceeds the defined threshold.

You can set up to 4 detection regions. When motion is detected in any one of the 4 regions, the corresponding channel will trigger an alarm.

Step 4 Select the checkbox next to **MD2.0**, select the sensitivity, and then select the valid target from **Human** or **Vehicle**.

The higher the sensitivity, the easier to trigger an alarm.

When the MD2.0 function is enabled, only huamn or vehicle can be detected, and then the alarm is trigged.

Step 5 Configure other parameters.

Table 5-31 Alarm settings

Parameter	Description
Arming Period	Click **Settings** to set the arming period for motion detection.
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as required. Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".
PTZ Linkage	Select the checkbox and then click **Settings** to configure PTZ linkage. Make sure that the PTZ control has been configured. For details, see "5.5.4 PTZ".
Recording Channel	Select one or more channels for recording. Make sure that the recording plan and recording mode has been configured in **Storage** > **Recording Plan**.
Beep	Enable the Device to make a beep noise when an alarm occurs.
Pop-up Alert	Enable on-screen prompt of detected motion.
Event Interval	Configure the period from the end of motion detection to the end of alarm linkage action.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends.
Recording Delay	Configure the length of time for the Device to continue recording after the alarm ends.

Parameter	Description
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.
Picture Storage	When an alarm occurs, the system takes snapshots of the selected channel and stores them on the device. Make sure that snapshot schedule and snapshot mode have been configured. For details, see "5.11.1 Configuring Recording Plan".

Step 6 Click **Apply**.

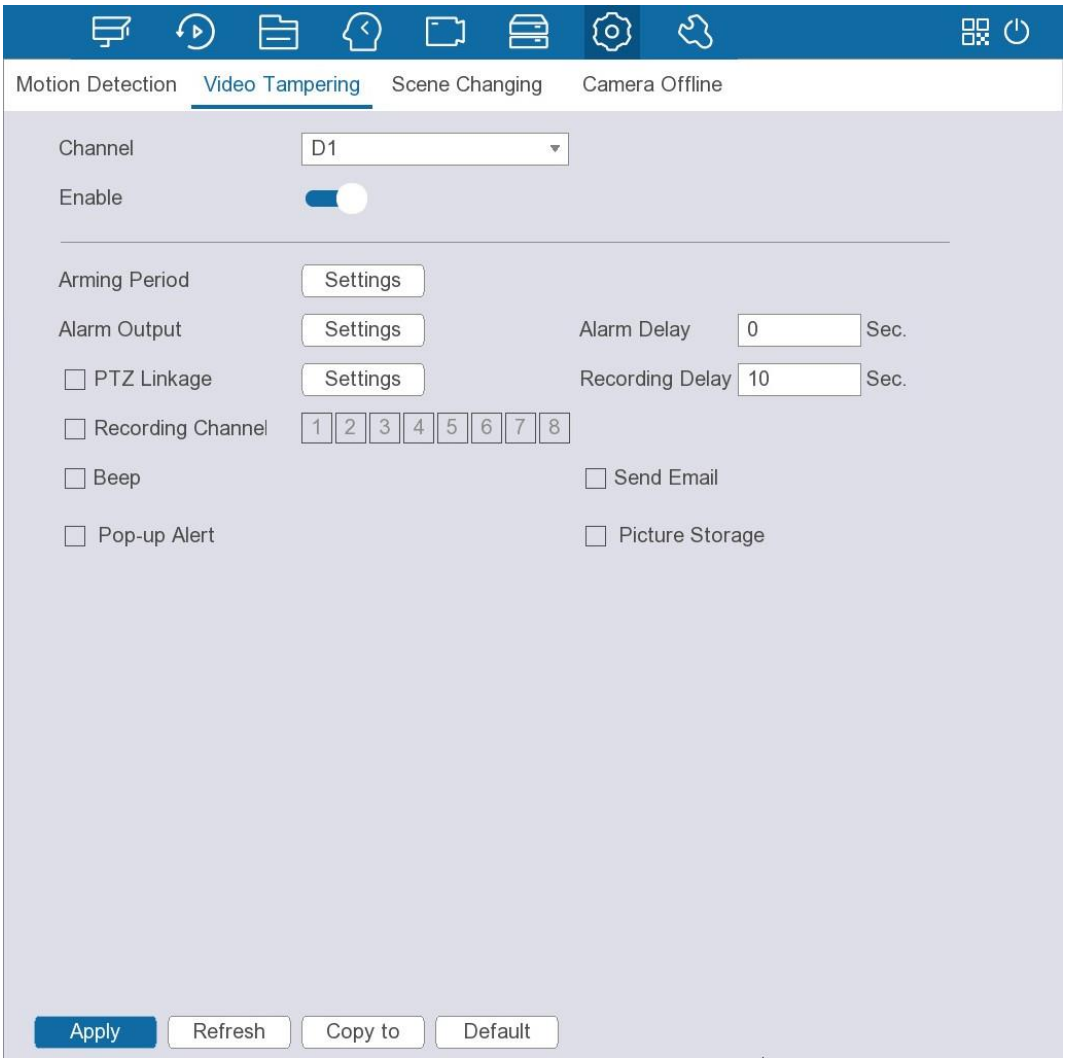
5.12.4.2.2 Configuring Video Tampering Alarms

Video tampering occurs when the camera lens is covered, or the video is displayed in a single color because of sunlight status or other reasons. You can configure alarms for such situations.

Procedure

Step 1 Select **System** > **Events** > **Video Detection** > **Video Tampering**.

Figure 5-74 Video tampering



Step 2 Select a channel and then click to enable alarm against video tampering.

Step 3 Configure other parameters. For details, see Table 5-31.

Step 4 Click **Apply**.

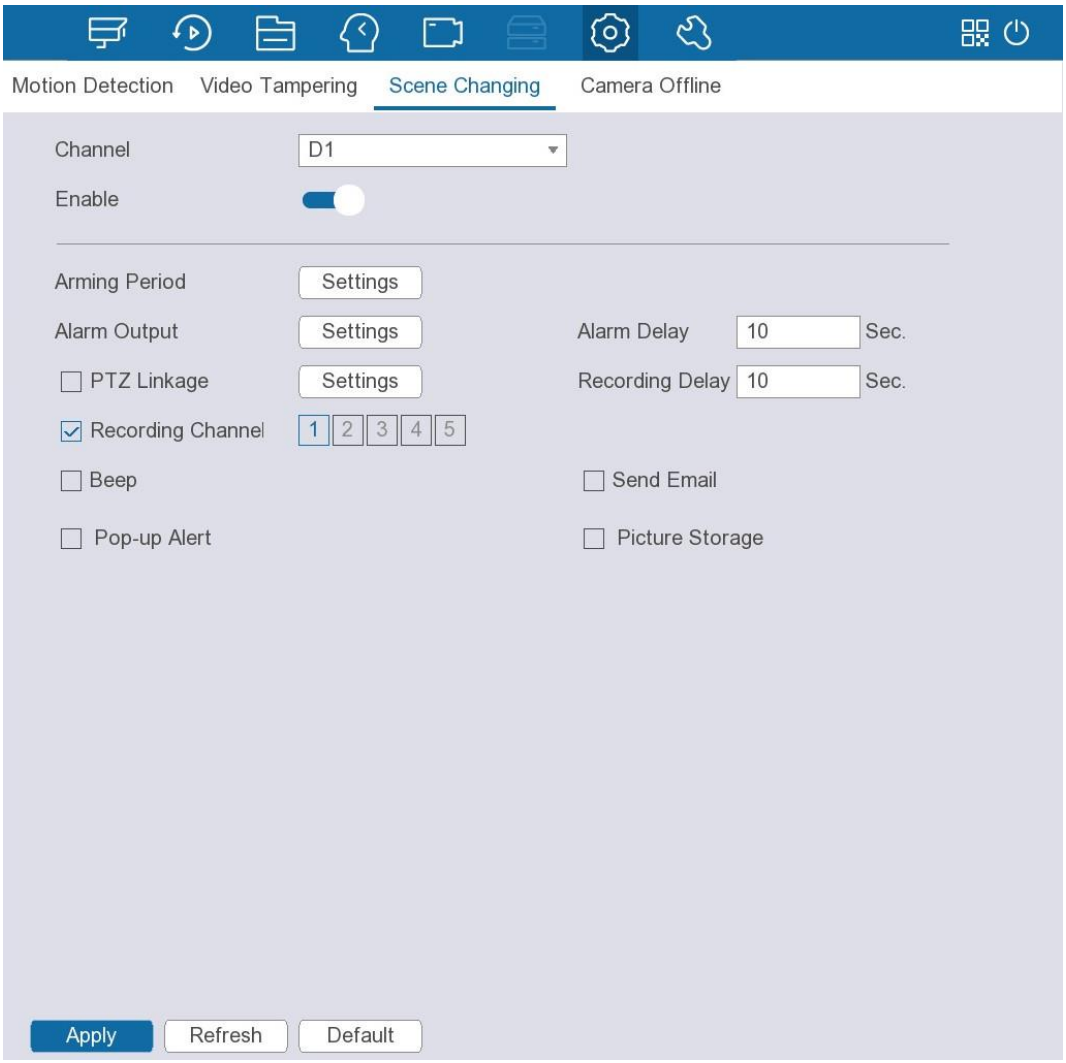
5.12.4.2.3 Configuring Scene Changing Alarms

An alarm is triggered when the system detects scene change.

Procedure

Step 1 Select **System** > **Events** > **Video Detection** > **Scene Changing**.

Figure 5-75 Scene changing



Step 2 Select a channel and then click to enable alarm against scene change.

Step 3 Configure other parameters. For details, see Table 5-31.

Step 4 Click **Apply**.

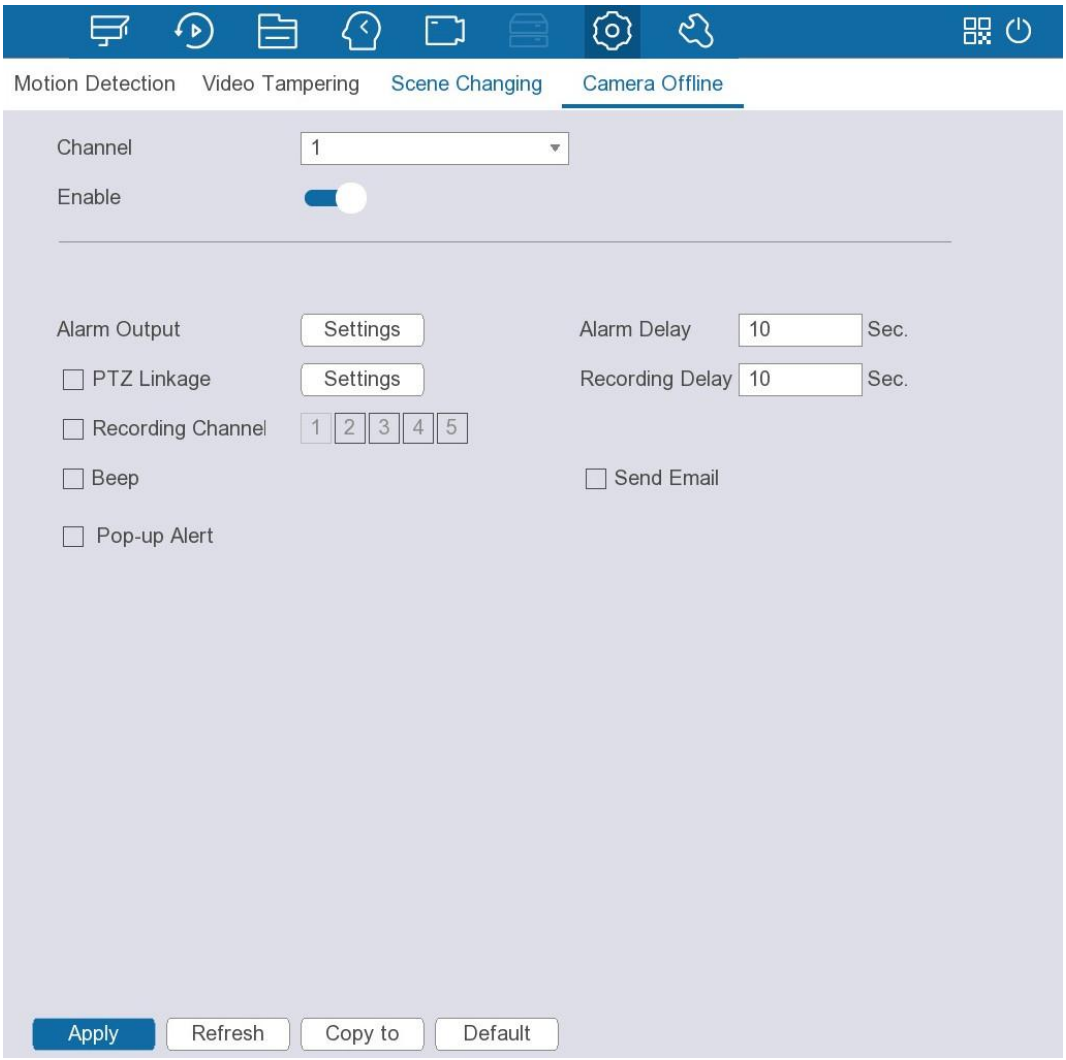
5.12.4.2.4 Configuring Camera Offline

An alarm is triggered when the camera is offline.

Procedure

Step 1 Select **System** > **Events** > **Video Detection** > **Camera Offline**.

Figure 5-76 Camera Offline



Step 2 Select a channel, and then click to enable alarm against video loss.

Step 3 Configure other parameters. For details, see Table 5-31.

Step 4 Click **Apply**.

5.12.4.3 Configuring Alarm Settings

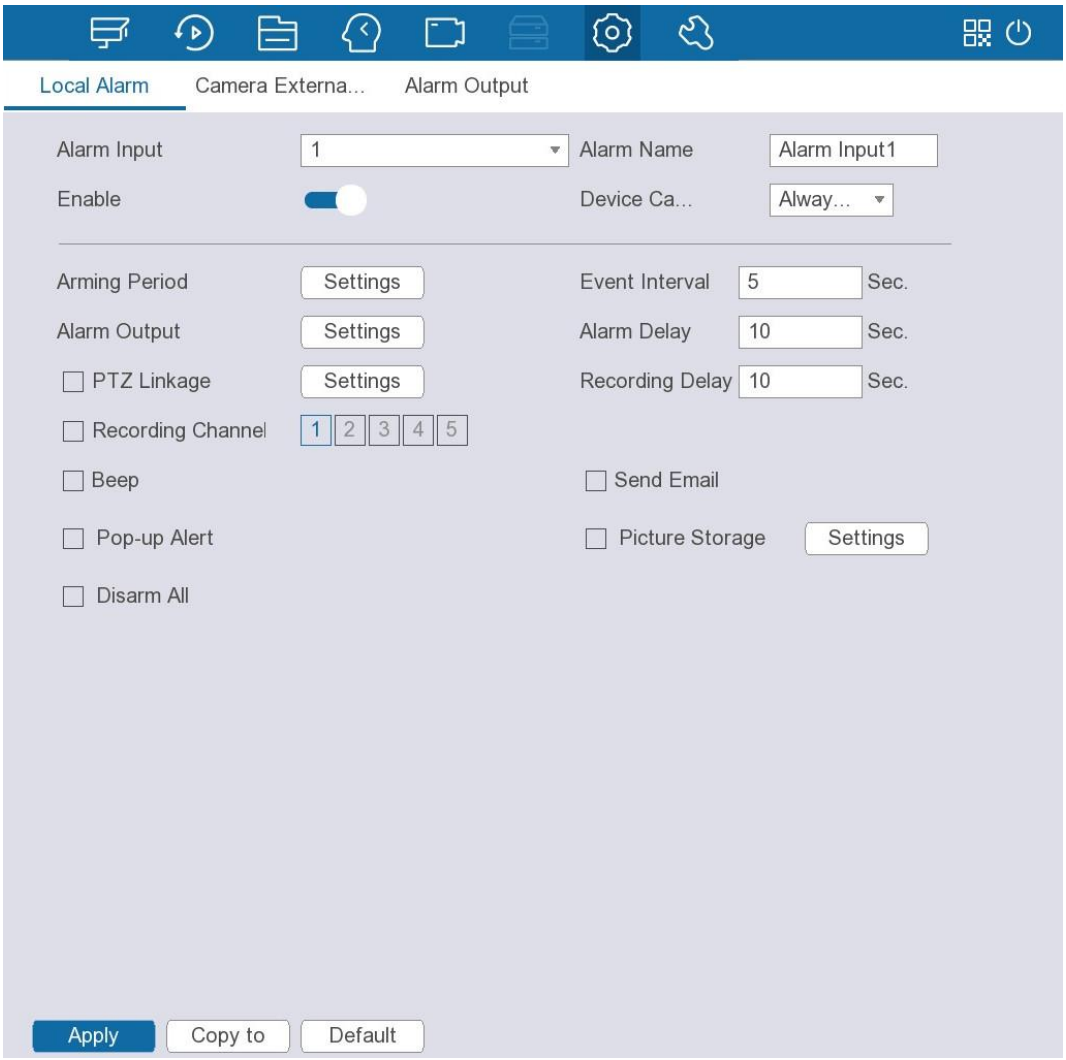
5.12.4.3.1 Configuring Local Alarms

After connecting the alarm device to the NVR alarm input port, the system performs alarm linkage actions when there is an alarm signal from the alarm input port to the NVR.

Procedure

Step 1 Select **System** > **Events** > **Alarm Settings** > **Local Alarm**.

Figure 5-77 Local Alarm



Step 2 Select an alarm input, and then set the alarm name.

Step 3 Click to enable the alarm.

Step 4 Select the device category from **Always Closed** and **Always Open**.

Step 5 Configure other parameters. For details, see Table 5-31.

Step 6 Click **Apply**.

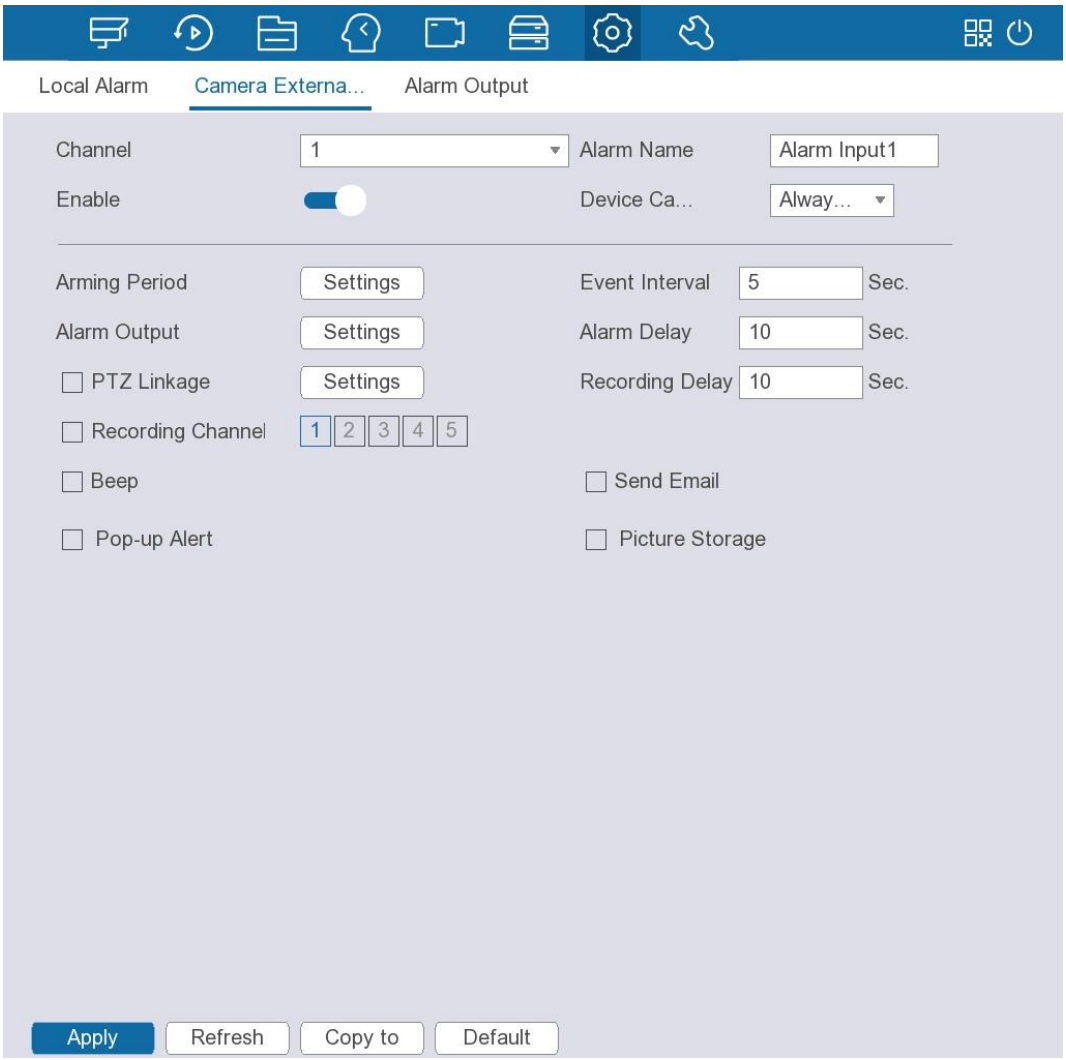
5.12.4.3.2 Configuring Alarms from External Cameras

When the external alarm device of the camera triggers an alarm, the alarm signal is transmitted to the Device and then the system performs alarm linkage actions.

Procedure

Step 1 Select **System** > **Events** > **Alarm Settings** > **Camera External Alarm**.

Figure 5-78 Camera external alarm



Step 2 Select a channel, and then set the alarm name.

Step 3 Click to enable the alarm.

Step 4 Select the device category from **Always Closed** and **Always Open**.

Step 5 Configure other parameters. For details, see Table 5-31.

Step 6 Click **Apply**.

5.12.4.3.3 Configuring Alarm Output

You can set proper alarm output mode to automatic, manual or close. After you connect the alarm device to the alarm output port of NVR, and set the mode to automatic, the system performs alarm linkage actions when an alarm occurs.

Background Information

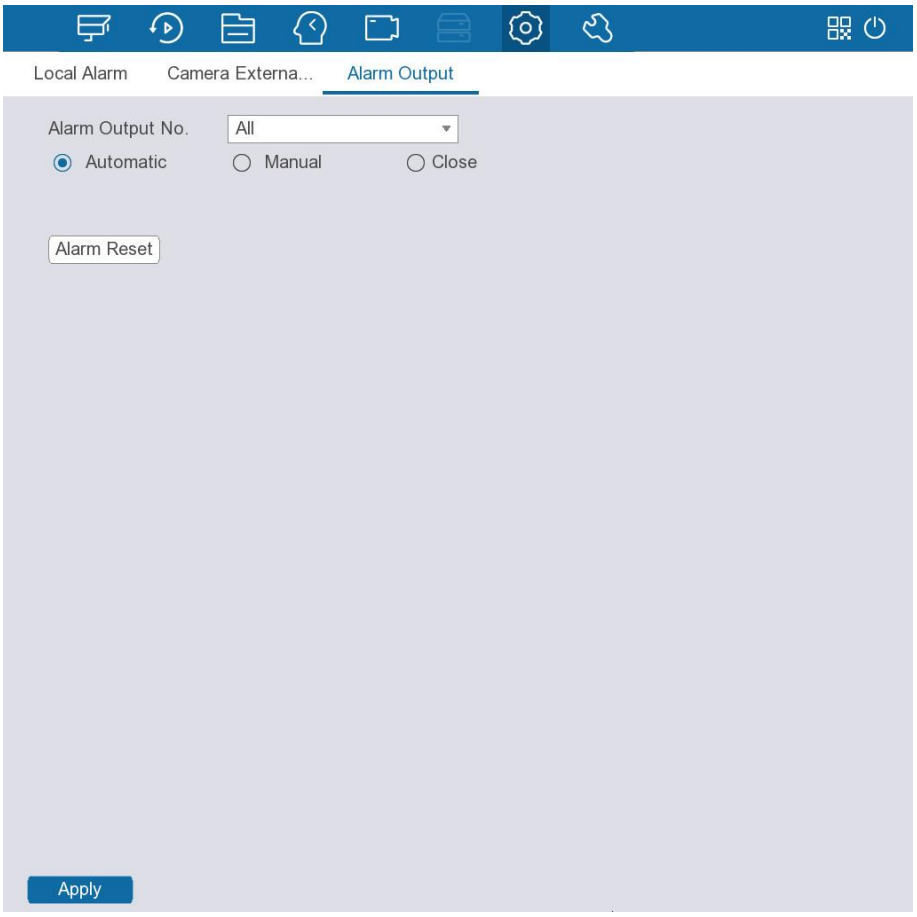
- Automatic: Once an alarm event occurs, the system generates an alarm.
- Manual: Alarm device is always on the alarming mode.
- Close: Disable the alarm output function.

Procedure

Step 1 Select **System** > **Events** > **Alarm Settings** > **Alarm Output**.

Step 2 Select the alarm mode of the alarm output channel.

Figure 5-79 Alarm output



Step 3 Click **Apply**.

- Click **Alarm Reset** to clear all alarm output statuses.
- View the alarm output status on the **Status** column.

5.12.4.4 Configuring Error Alarms

You can configure alarms for system errors.

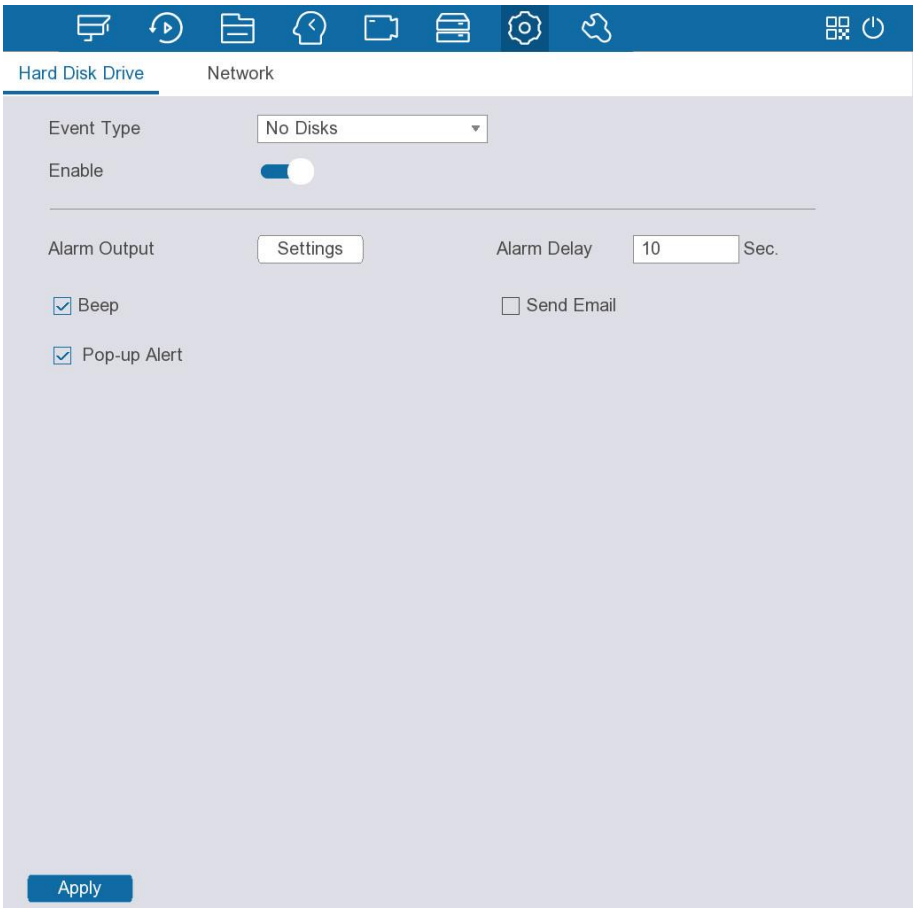
5.12.4.4.1 Configuring Storage Error Alarms

An alarm is triggered when a storage error occurs.

Procedure

Step 1 Select **System** > **Events** > **Exception** > **Hard Disk Drive**.

Figure 5-80 HDD alarm



Step 2 Select an event type from **No disks**, **Hard Disk Error** and **Insufficient storage capacity**.

Step 3 Click to enable the alarm.

Step 4 Configure other parameters.

Table 5-32 Alarm settings

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as required. Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".
Beep	Select the checkbox to enable the Device to make a beep noise when an alarm occurs.
Pop-up Alert	Enable on-screen prompt of an alarm event.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends.

Parameter	Description
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **Main Menu** > **Network Settings** > **Email**.

Step 5 Click **Apply**.

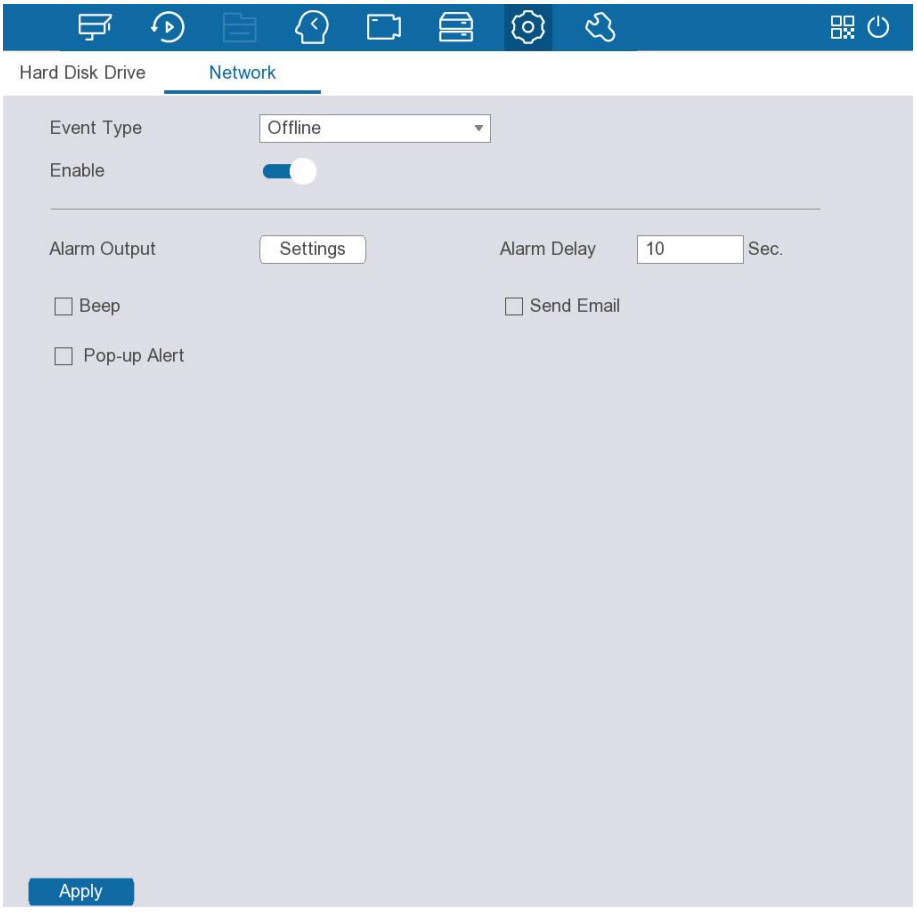
5.12.4.4.2 Configuring Network Error Alarms

An alarm is triggered when a network error occurs.

Procedure

Step 1 Select **System** > **Events** > **Exception** > **Network**.

Figure 5-81 Network alarm



Step 2 Select an event type from **Offline**, **IP Conflict** and **MAC conflict**.

Step 3 Click to enable the alarm.

Step 4 Configure other parameters.

Table 5-33 Alarm settings

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as required. Make sure that the alarm state of the alarm output port has been configured. For details, see "5.12.4.3.3 Configuring Alarm Output".
Beep	Select the checkbox to enable the Device to make a beep noise when an alarm occurs.
Pop-up Alert	Enable on-screen prompt of an alarm event.
Alarm Delay	When alarm delay is configured, alarm continues for an extended period after the alarm ends
Send Email	Enable the system to send an email to notify you of an alarm event. • This function is available on select models. • Make sure that the email function has been configured in **Main Menu** > **Network Settings** > **Email**.

Step 5 Click **Apply**.

5.12.4.5 Searching for Alarm Information

You can search for, view and back up the alarm information.

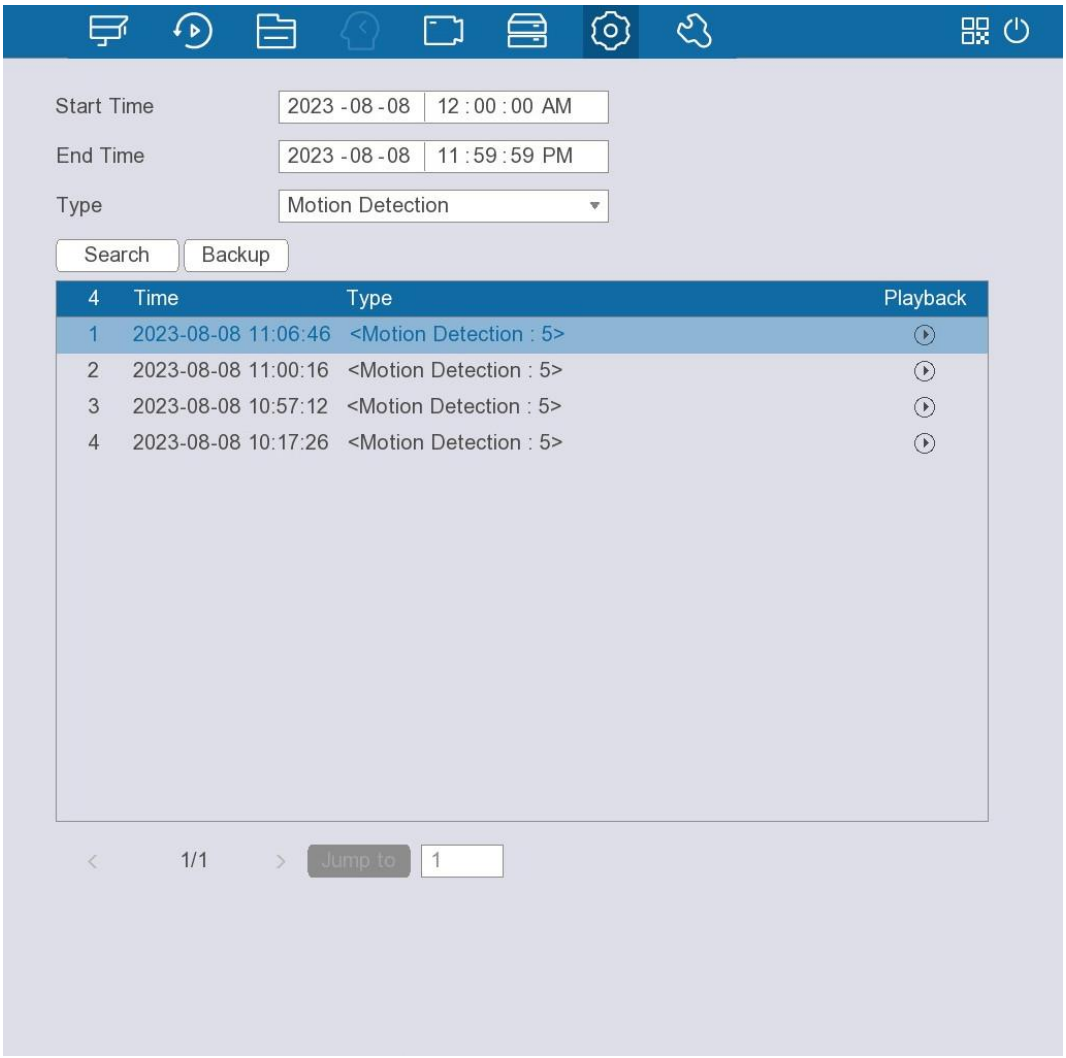
Procedure

Step 1 Select **System** > **Events** > **Event Search**.

Step 2 Set the search period, and then select an event type.

Step 3 Click **Search**.

Figure 5-82 Search results



Related Operations

- View details.

  Select a record, and then double-click an alarm record to view details.
- Back up.

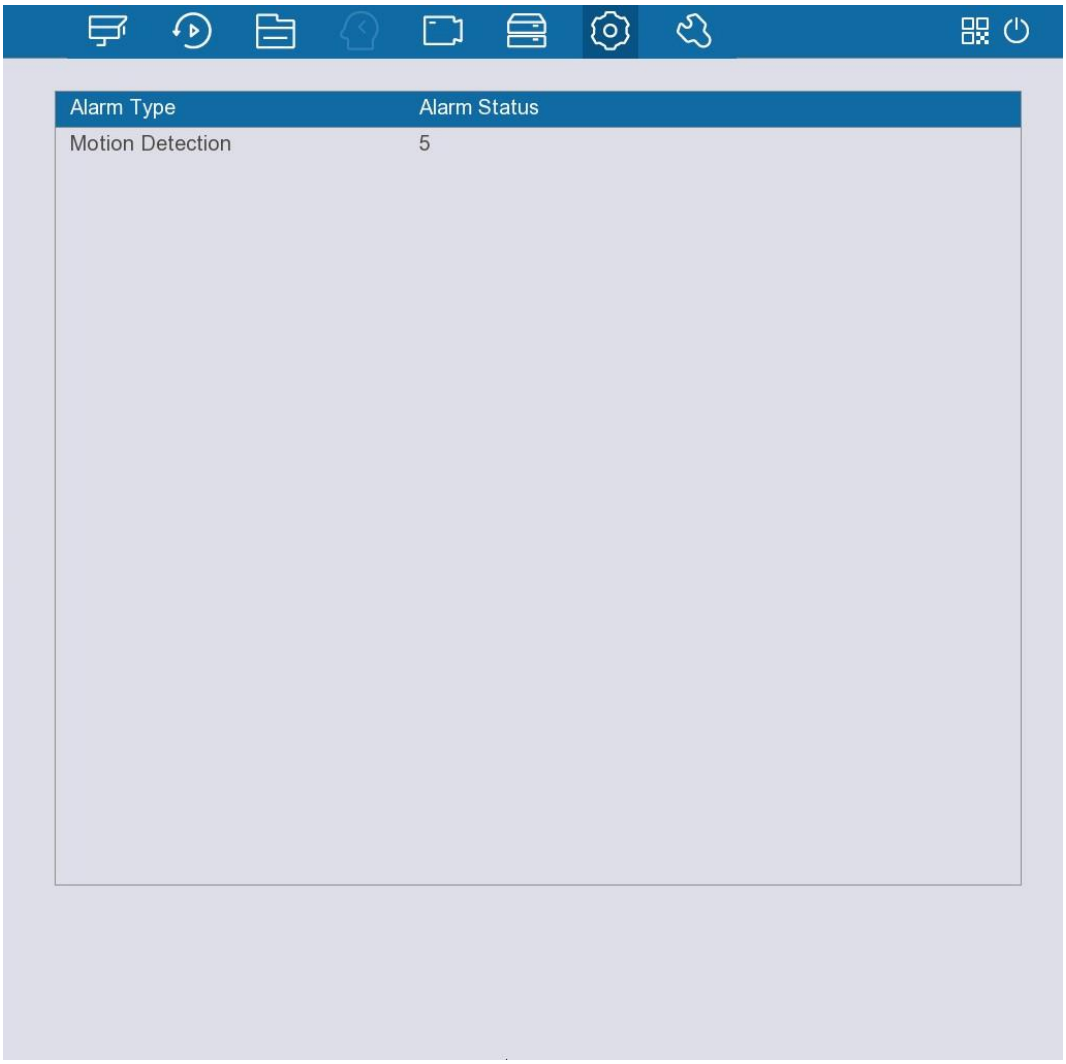
  Click **Backup** to save the alarm information to a USB storage device.
- Play recorded video.

  Click ⊙ to play the recorded video of the alarm event.

5.12.4.6 Viewing Alarm Status

Select **System** > **Events** > **Event Search** to view alarm status.

Figure 5-83 Alarm status



5.12.5 Configuring Display Settings

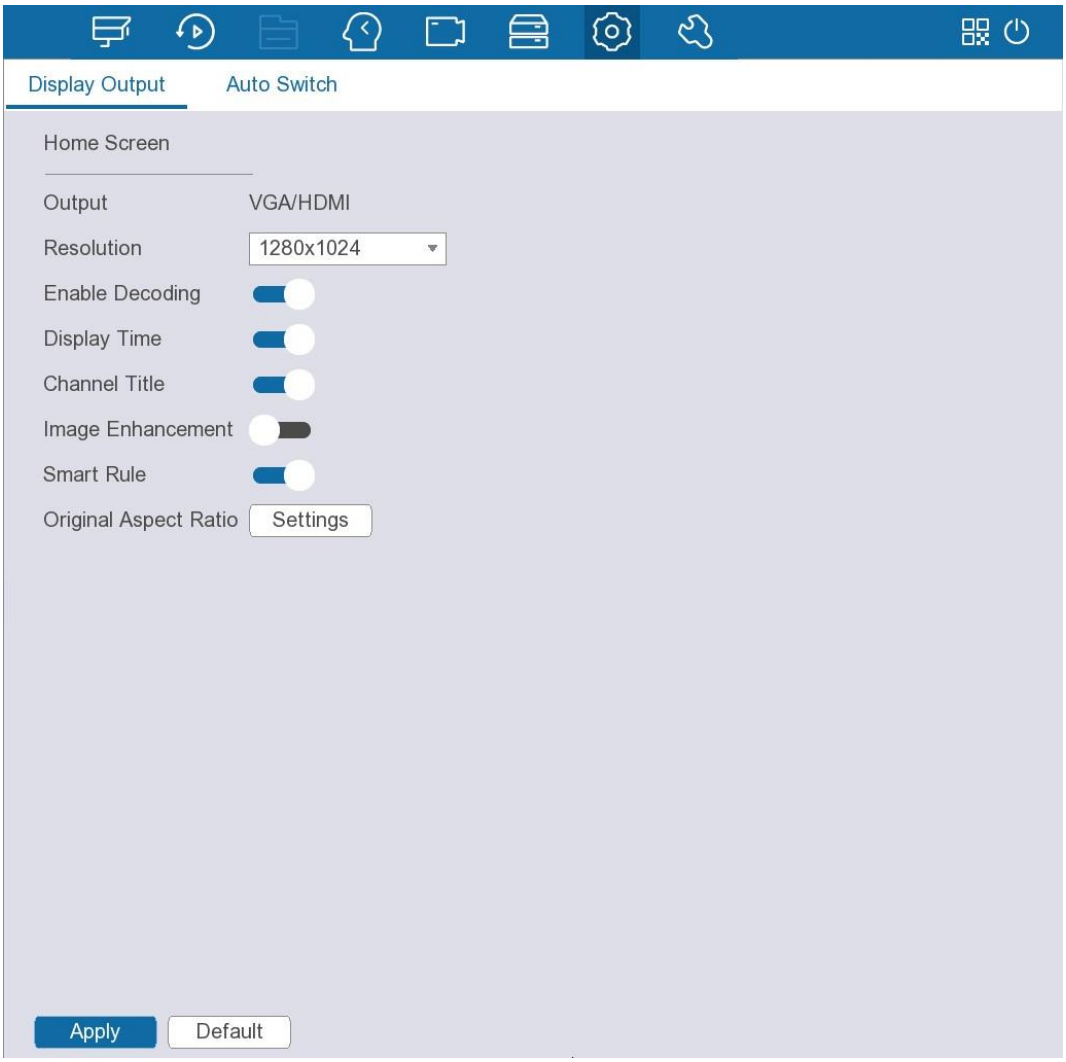
5.12.5.1 Configuring Display Output

You can configure whether to display time title and channel, adjust image transparency, set the resolution and more.

Procedure

Step 1 Select **System** > **Display Output**.

Figure 5-84 Display output



Step 2 Configure the display parameters.

Table 5-34 Display parameters

Parameter	Description
Resolution	Select a resolution for the video image. The default value is 1280 × 1024.
Enable Decoding	Enable the decoding function.
Display Time	Displays time information in each live channel window.
Channel Title	Displays channel name, channel number and recording status in each live channel window.
Image Enhancement	After the function is enabled, the system optimizes the live images.
Smart Rule	Displays smart rule in each live channel window.
Original Aspect Ratio	Click **Settings**, and then select one or more channels to restore the channel image to the original scale.

Step 3 Click **Apply**.

5.12.5.2 Configuring Auto Switch

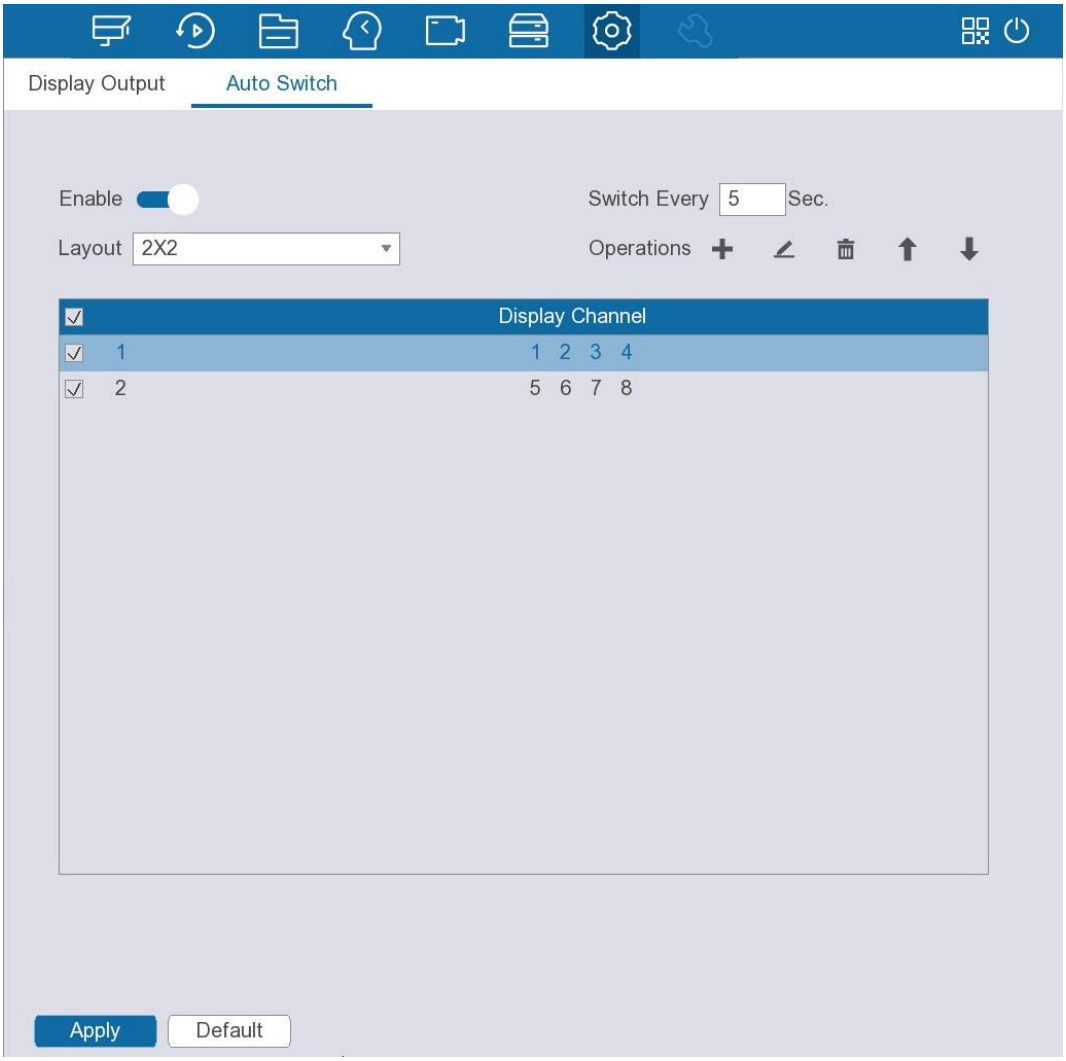
You can configure a tour of selected channels to repeat playing videos. The videos are displayed in turn according to the channel group configured in tour settings. The system displays one channel group for a certain period and then automatically changes to the next channel group.

Procedure

Step 1 Select **System** > **Display** > **Auto Switch**.

Step 2 Click to enable this function.

Figure 5-85 Auto Switch



Step 3 Configure the tour parameters.

Table 5-35 Tour parameters

Parameter	Description
Switch Every	The duration for which each channel group is displayed. The default value is 5 seconds.
Layout	Select a layout of the live view.
Operations	You can add, modify, delete, or change the sequence of the channel groups.

Step 4 Click **Apply**.

Related Operations

On the navigation bar on the live page, click  to enable or disable tour.

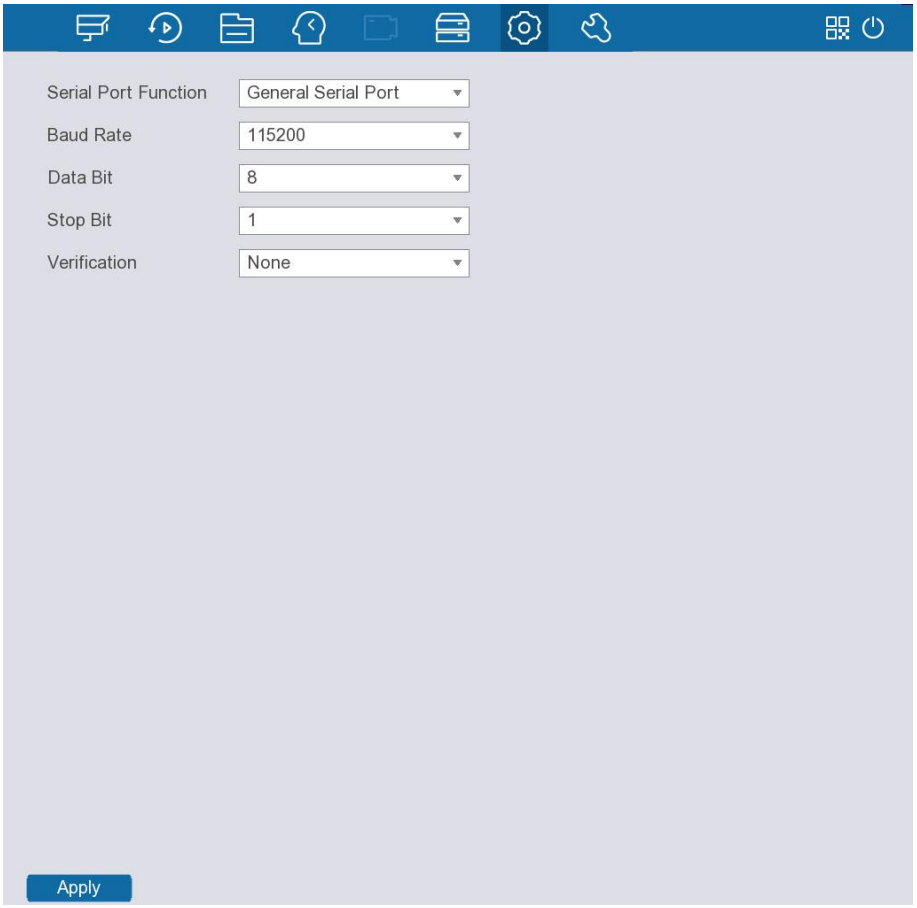
5.12.6 Configuring Serial Port

After setting RS-232 parameters, the NVR can use the COM port to connect to other device to debug and operate.

Procedure

Step 1 Select **System** > **Serial Port**.

Figure 5-86 Serial port



Step 2 Configure parameters.

Table 5-36 Serial port parameters

Parameter	Description
Function	Select serial port control protocol. • General Serial Port: Upgrade the program and debug with the console and mini terminal software. • Control Keyboard: Control this Device with special keyboard. • Transparent Serial Port: Connect with the computer directly for transparent transmission of data. • Protocol Serial Port: Configure the function to protocol COM, in order to overlay card number. • PTZ Matrix: Connect matrix control Different series products support different RS-232 functions.
Baud Rate	Select baud rate, which is 115200 by default.
Data Bits	It ranges from 5 to 8, which is 8 by default.
Stop Bits	It includes 1, 1.5 and 2.
Verification	It includes none, odd, even, flag and empty.

Step 3 Click **Apply**.

5.13 Maintenance

Select **Maintain**, and then you can view system information and logs, update the system, restore the device to factory defaults, and more.

5.13.1 Viewing System Information

Select **Maintain** > **Device Info** to view the version information, disk information, stream information, and more.

- Version information: The device model, alarm input, alarm output, firmware version, system version, ONVIF server version, and more.
- Disk information: The device name, physical position, attributes, total capacity, health status and other information on each HDD.
- Stream information: The resolution and stream rate of each channel.
  You can click **Waveform** to view the stream fluctuation chart.
- Network information: The DHCP, IPv4 address, IPV4 subnet mask, IPv4 default gateway, MAC address, preferred DNS server, and more.

5.13.2 Searching for Logs

Background Information

You can search for and view logs.

- If there is HDD installed, the logs on system operations are saved in the memory of the Device and other types of logs are saved into the HDD. If there is no HDD installed, the other types of logs are also saved in the memory of the Device.
- If you format the HDD, the logs will not be lost. However, if you take out the HDD from the Device, the logs might be lost.

Procedure

Step 1 Select **Maintain** > **Log Info**.

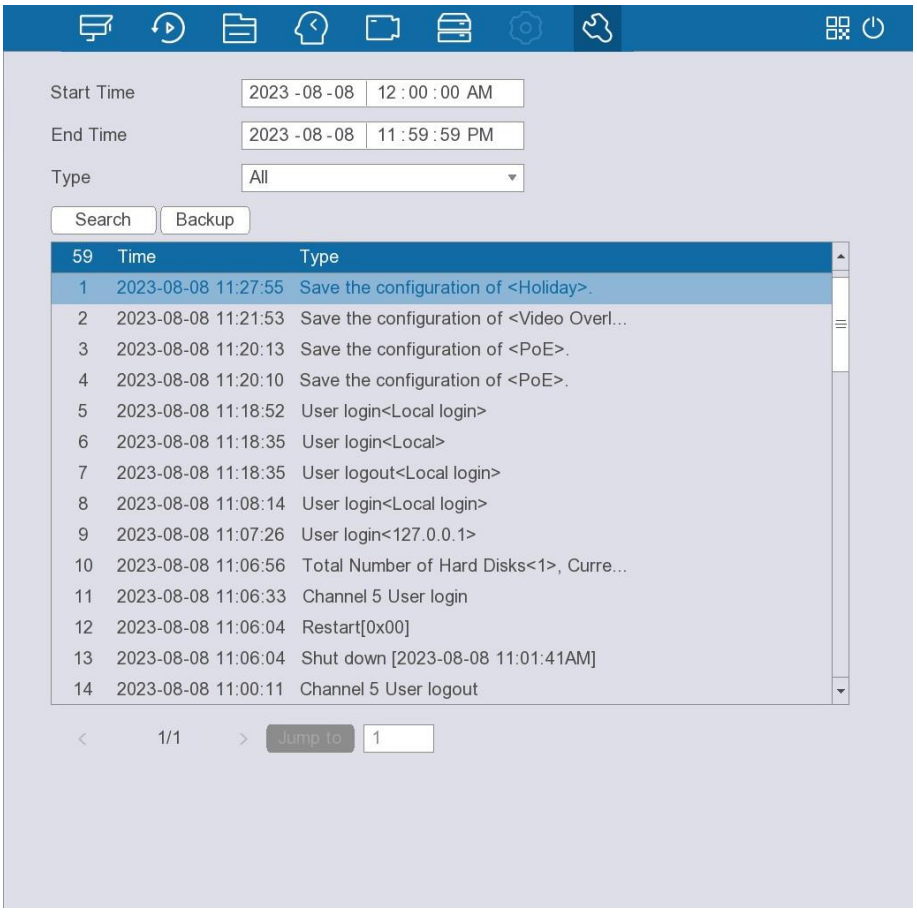
Step 2 Set the search period.

Step 3 Select a log type.

Step 4 Click **Search**.

The search results are displayed.

Figure 5-87 Search results



Related Operations

- View details.

  Select a log, and then double-click a log to view details. Click **Previous** or **Next** to view details of other logs.
- Back up.

Click **Backup** to save the logs to a USB storage device.

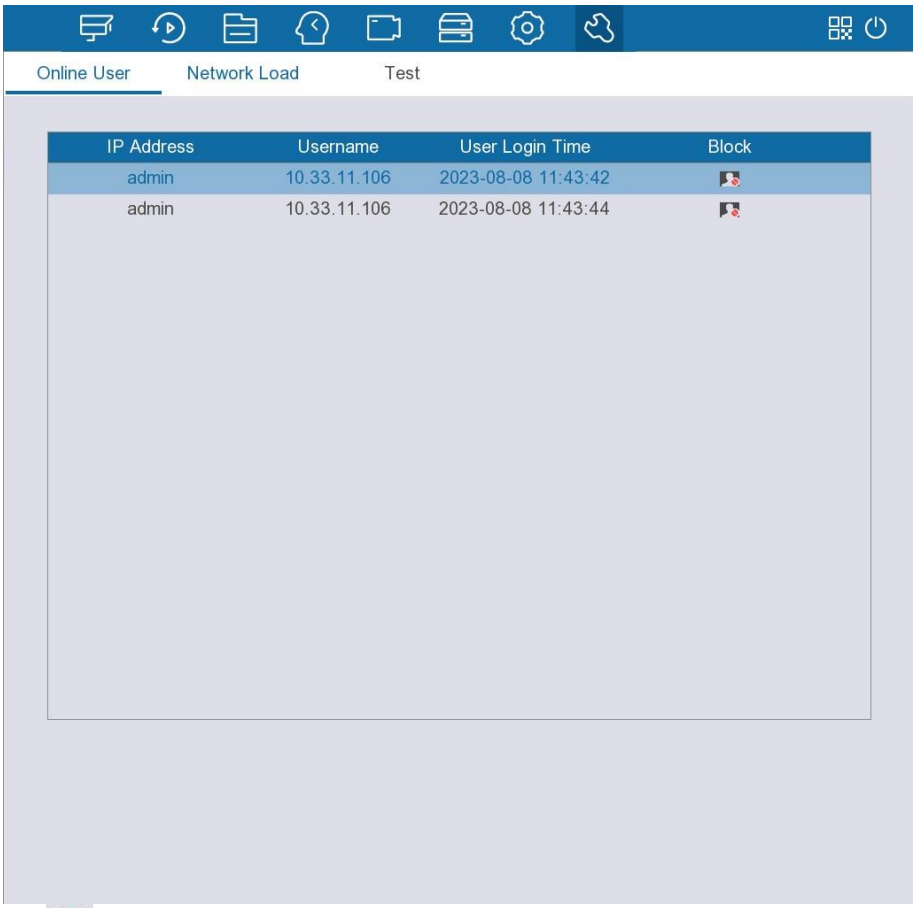
5.13.3 Viewing Network Information

You can view the online users, network load, and test network connection.

5.13.3.1 Viewing Online User

Select **Maintain** > **Network** > **Online User**, and then you can view the information on the online user.

Figure 5-88 Online user



You can click  to block a user from logging in to the device.

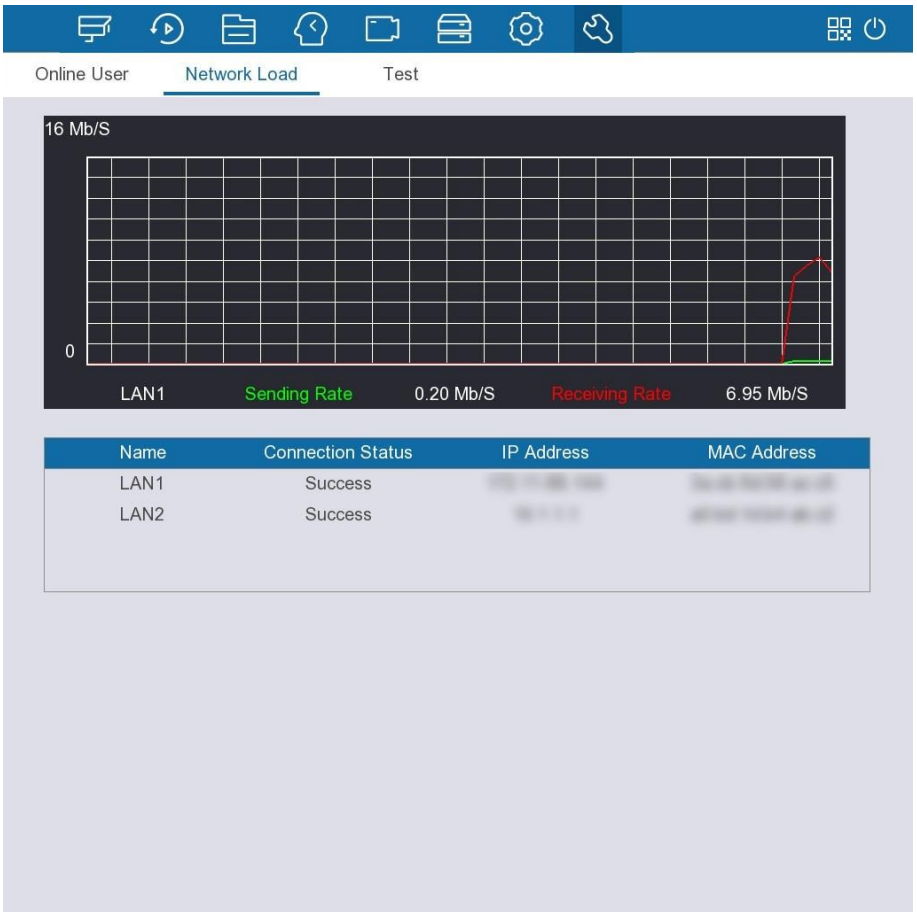
5.13.3.2 Viewing Network Load

Network load refers to the data flow that measures the transmission capability. You can view the data receiving speed and sending speed.

Procedure

Step 1 Select **Maintain** > **Network** > **Network Load**.

Figure 5-89 Network load



Step 2 Click the LAN name to view the corresponding sending and receiving rate.

You can view the network of one LAN at one time.

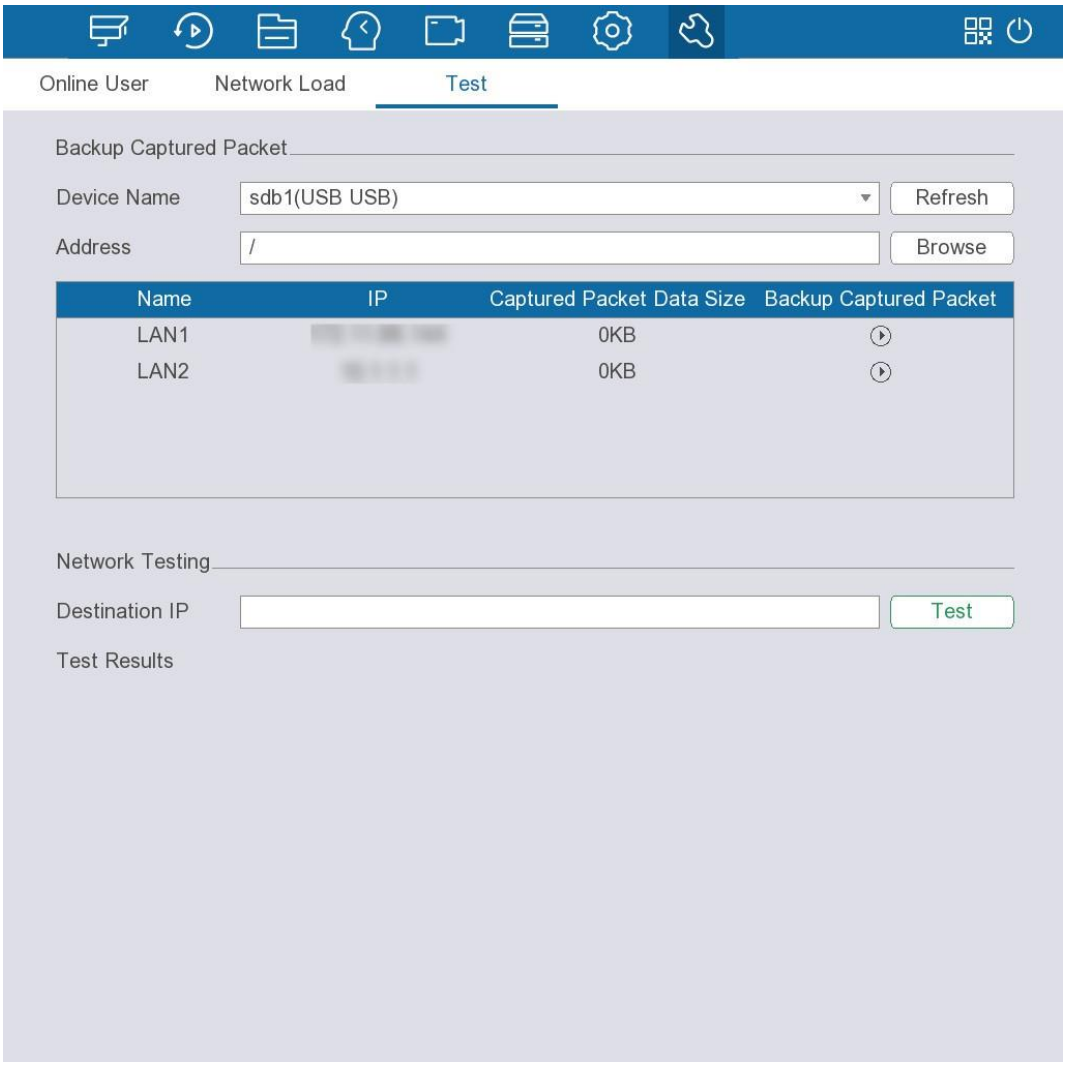
5.13.3.3 Testing Network

You can test the network connection between the Device and other devices and capture the packets when the network of the Device is abnormal. The captured packets can help technical support to diagnose and solve network problems.

Procedure

Step 1 Select **Maintain** > **Network** > **Test**.

Figure 5-90 Test



Step 2 Capture packets.

1) Connect a USB storage device to the Device.
2) Click **Refresh**.

   After the Device detects the connected USB device, the name of the USB device appears in the **Device Name** box.
3) Click **Browse** to select the storage path.
4) Click ⊙ to start packet capturing and backup. Click the icon again to stop.

- You cannot capture the data packets of several network adapters at the same time.
- During packet capturing, you can go to other pages for operation and go back to the **Test** page later to stop packet capturing.

Step 3 Enter the destination IP address, and then click **Test**.

You can view the load of one network adapter at one time.

After testing is complete, view the test results of the average delay, packet loss rate, and network status.

5.13.4 Exporting and Importing System Configurations

You can export the configuration file of the Device for backup. When the Device malfunctions, you can import the backup configuration file to restore.

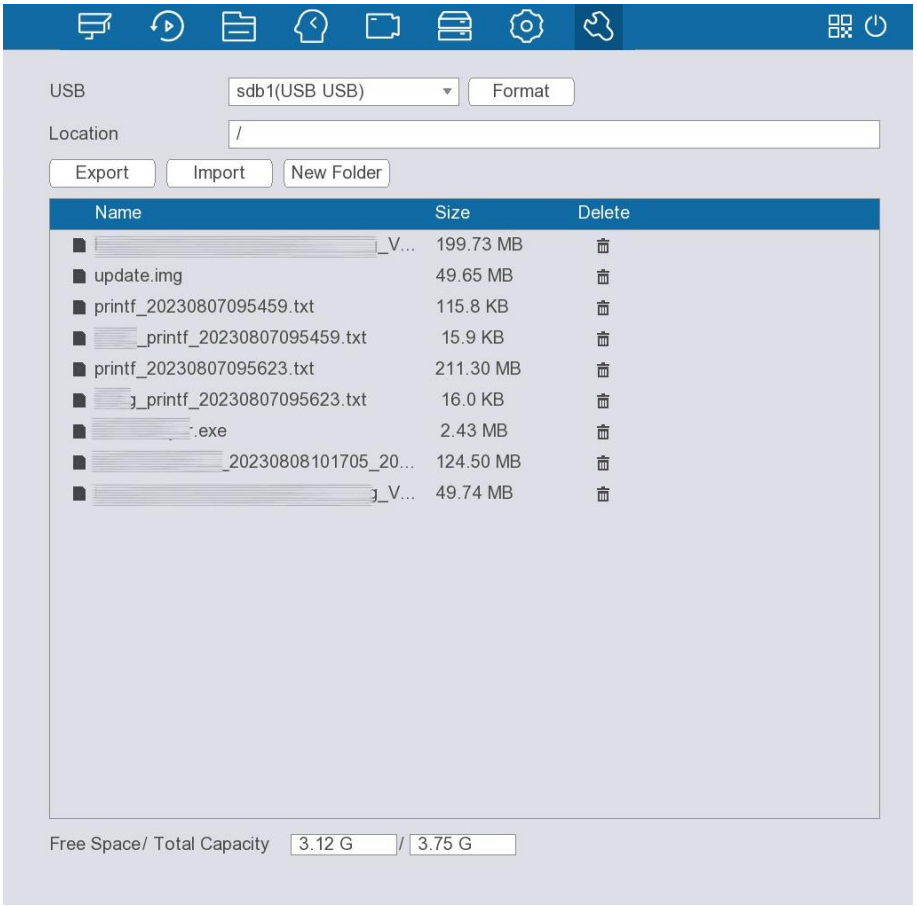
You cannot import or export the system configurations when another backup process is ongoing on other pages.

5.13.4.1 Exporting System Configurations

Procedure

Step 1 Select **Maintain** > **Import/Export**.

Figure 5-91 Configuration maintenance



Step 2 Connect a USB storage device to the Device.

Step 3 Click **Export**.

The configurations are exported to a folder under a name of "Config_[YYYYMMDDhhmmss]".

Double-click this folder to view the backup files.

5.13.4.2 Importing System Configurations

Procedure

Step 1 Connect a USB storage device containing the configuration files to the Device.

Step 2 Select **Maintain** > **Import/Export**.

Step 3 Select the configuration folder (under a name of "Config_XX").

Step 4 Click **Import**.

The Device will restart after the configurations are imported.

The imported configurations will overwrite the original configurations.

5.13.5 Updating the System

You can upgrade the system through file update and online update.

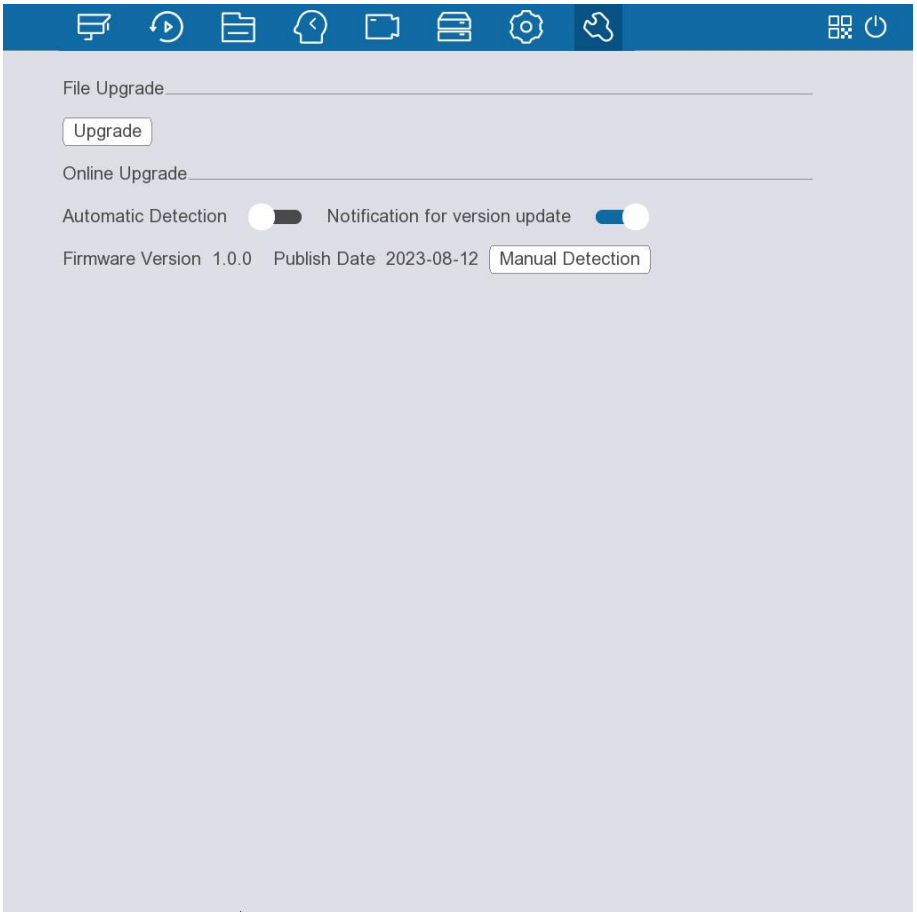
5.13.5.1 File Update

Procedure

Step 1 Connect a USB storage device containing the update file to the Device.

Step 2 Select **Maintain** > **Upgrade**.

Figure 5-92 Update



Step 3 Click **Upgrade**.

Step 4 Select the update file that you want to use.

Step 5 Click **OK**.

5.13.5.2 Online Update

After the Device is connected to the network, you can update the system online.

Procedure

Step 1 Select **Maintain** > **Upgrade**.

Step 2 Check whether there is a new version available.

- Automatic detection: Click to enable automatic detection.
- Manual detection: Click **Manual Detection** to check the version immediately.

If the system prompts **Already the latest version**, you do not need an update. If the system prompts a new version is available, go to the next step.

Step 3 Click **Upgrade now**.

5.13.6 Restoring Defaults

When the system runs slowly and has errors in configuration, you can try to fix such problems by restoring the default settings.

5.13.6.1 Restoring Defaults on the Local Interface

You can restore the Device to default settings on the local interface.

Procedure

Step 1 Select **Maintain** > **Default**.

Step 2 Restore the settings.

- **Restore**: Restore all the configurations except network settings and user management to the default.
- **Factory Default**: Restore all the configurations to the factory default settings.

5.13.6.2 Resetting Device through the Reset Button

Background Information

You can use the reset button on the mainboard to reset the Device to factory default.

This button is available on select models.

Procedure

Step 1 Power off the Device, and then remove the cover. For details on the removal operation, see "4 Installation".

Step 2 Press and hold the reset button  on the mainboard for 5 seconds to 10 seconds.

The position of the reset button might vary depending on the model.

Step 3 Restart the Device.

After restart, the settings are restored to the factory default.

5.13.7 Configuring Automatic Reboot

When the Device has been running for a long time, you can enable the Device to restart automatically at the idle time.

Procedure

Step 1 Select **Maintain** > **Auto Reboot**.

Step 2 Select a time for automatic restart.

Step 3 Click **Apply**.

6 Web Operations

6.1 Logging in to the Web

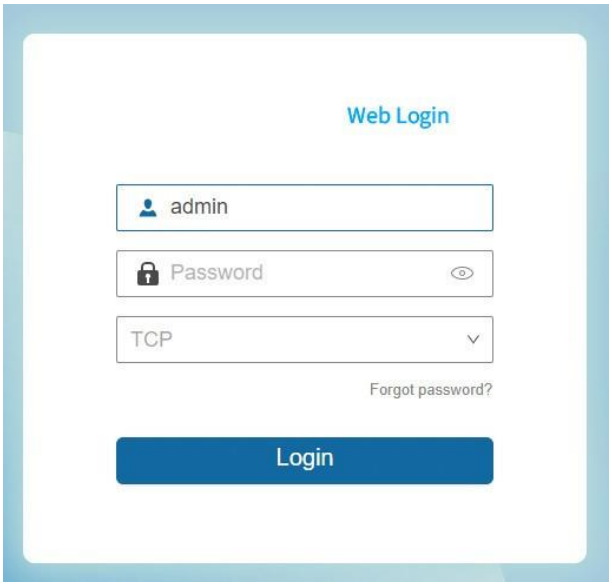
Prerequisites

Make sure that the IP addresses of your computer and the Device are on the same network segment.

Procedure

Step 1 Enter the IP address of the Device in the address bar of the browser, and then press the Enter key.

Figure 6-1 Login



Step 2 Enter username and password.

Step 3 Click **Login**.

6.2 Web Main Menu

After login, the main menu is displayed.

Figure 6-2 Web main menu

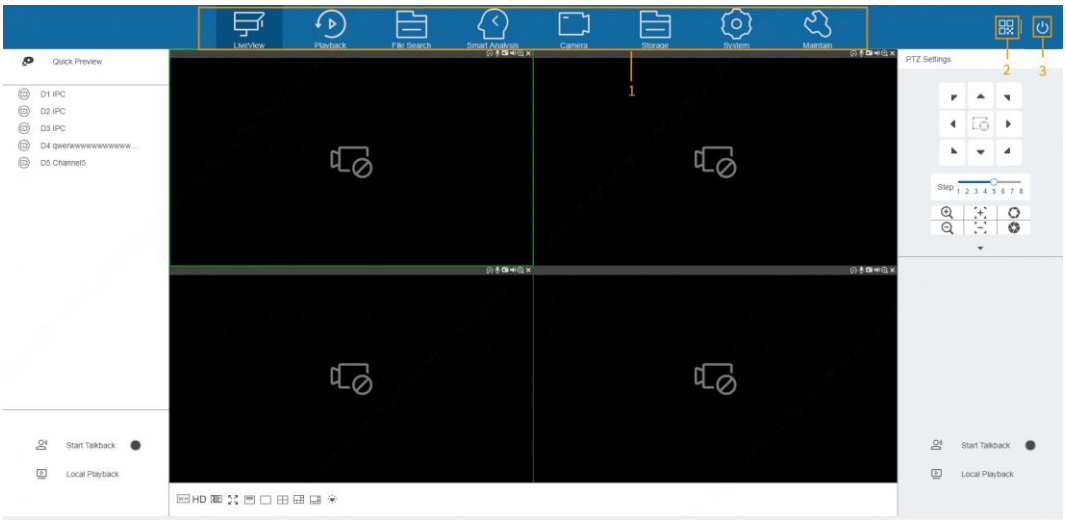


Table 6-1 Main menu description

No.	Name	Description
1	Function tiles	Click each tile to open the corresponding configuration page.
2	QR code	Scan the QR code to add the Device for remote management.
3	Shut down	Log out of the current account, restart or shut down the Device.

Appendix 1 HDD Capacity Calculation

Use the following formula to calculate the HDD capacity:

Total capacity (MB) = Channel number× Demand time length (hour) × HDD capacity occupied per hour (MB/hour)

Based on this formula, the formula to calculate recording time goes as follows:

$$\text{Recording time (hour)} = \frac{\text{Total capacity (M)}}{\text{HDD capacity occupied per hour (M/hour)} \times \text{Channel number}}$$

For example, for single-channel recording, the HDD capacity occupied per hour is 200 MB/hour. If you use 4-channel device to make 24-hour continuous recording in every day of one month (30 days), the required HDD space is: 4 channels× 30 days× 24 hours× 200 MB/hour = 576 G. Therefore, you need five 120 G HDDs or four 160 G HDDs.

According to the formulas, at different stream values, recording file size of 1 channel in 1 hour is shown as follows:

Appendix Table 1-1 HDD capacity

Max. bit stream value	File size	Max. bit stream value	File size
96 Kbps	42 MB	128 Kbps	56 MB
160 Kbps	70 MB	192 Kbps	84 MB
224 Kbps	98 MB	256 Kbps	112 MB
320 Kbps	140 MB	384 Kbps	168 MB
448 Kbps	196 MB	512 Kbps	225 MB
640 Kbps	281 MB	768 Kbps	337 MB
896 Kbps	393 MB	1024 Kbps	450 MB
1280 Kbps	562 MB	1536 Kbps	675 MB
1792 Kbps	787 MB	2048 Kbps	900 MB

The table is for reference only. The data might differ in the actual situation.

Appendix 2 Cybersecurity Recommendations

Compulsory measures to ensure the basic device network security:

- Timely Update Firmware and Client Software
  - Keep the device (such as video recorder and IP camera) firmware up-to-date based on standard procedure in the tech-industry to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the"auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
  - Download and use the latest version of client software.
- Use Complex Passwords with Combination of Characters, Numbers and Symbols
  Please refer to the following suggestions to set passwords:
  - The length should not be less than 8 characters;
  - Combine at least two types of characters in a password among upper and lower case letters, numbers and symbols;
  - Do not contain the account name or the account name in reverse order;
  - Do not use continuous characters, such as abcdefgh and 12345678;
  - Do not use overlapped characters, such as aaaaaaaa and 11111111.

Constructive suggestions on improving device network security:

- Change Passwords Regularly
  We recommend that you change passwords regularly to reduce the risk of being guessed or cracked.
- Configure and Update Password Reset Information in Time
  Password reset function is supported by the device. Please configure related information for password reset in time, including the end user's email address and password protection questions. Please update the information accordingly in time if it changes. Please do not use simple questions whose answers can be easily obtained when setting password protection questions.
- Enable Account Lock
  The account lock is enabled by default. We recommend you keep it on to ensure the account security. A number of failed login attempts will lead the corresponding account and the source IP address to be locked.
- Physical Protection
  Physical protection is recommended on the device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement strict access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware and unauthorized connection of removable device (for example, USB flash drive and serial port).
- Reset Default HTTP and Other Service Ports
  Changing the default HTTP and other service ports is recommended. We recommend you

change them into any set of numbers between 1024–65535 to reduce the risk of exposing ports in use to outsiders.

- Enable HTTPS
  HTTPS is recommended to be enabled so that you can obtain the web service through a secure communication channel.
- Bind IP and MAC Address to Device
  To reduce the risk of ARP spoofing, we recommend you bind the IP and MAC address of the gateway to the device.
- Assign Accounts and Privileges Reasonably
  Based on business requirements and management requirements, prudently add user accounts and assign a minimum set of permissions to them.
- Disable Unnecessary Services and Apply Secure Modes
  If not needed, we recommend you turn off some services such as SNMP, SMTP, and UPnP to reduce risks.
  If necessary, we recommend using security modes, including but not limited to the following services:
  - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
  - SMTP: Choose TLS to access mailbox server.
  - FTP: Choose SFTP, and set up strong passwords.
  - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
- Establish a Secure Network Environment
  The following actions are highly recommended to ensure device security and to reduce potential cyber risks:
  - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
  - Partition and isolate the network according to the actual network needs. If there are no communication requirements between two sub networks, we recommend you adopt network isolation through VLAN, network GAP and other technologies.
  - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
  - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.
- Security Auditing
  - Check online users: Check online users regularly to prevent unauthorized login.
  - Check device log: Obtain the IP addresses that were used to log in to the device and their key operations with help of the logs.
- Network Log
  The stored log is not saved in full due to the limited storage capacity. If you need to save the log for a long time, we recommend you enable the network log function to make sure that the critical logs are synchronized to the network log server for tracing.