Network Video Recorder

User Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.2.0

Foreword

General

This user manual introduces the installation, functions and operations of the Network Video Recorder (NVR) (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.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
	Provides methods to help you solve a problem or save you time.
	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.2.0	Added smart calibration.	November 2025
V1.1.0	• Added Wizseek, text rule and text-defined alarms. • Updated mode and AcuPick settings.	September 2025
V1.0.0	First release.	May 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, 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 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.

Installation Requirements

Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- Before extending the rack to the installation position, read the installation instructions.
- When the Device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the Device is installed on it.

- Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.
- Before installation, disconnect all the power cords.
- 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.
- Use the power adapter and cables provided with the Device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.

- Reliably ground the grounding terminal of the Device to improve safety. The grounding terminal differs depending on the device, and some devices do not have grounding terminals. Process the situation according to the device model.

- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- 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.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- 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 server power requirement.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the controller securely to the building before use.

Operation Requirements

DANGER

- The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - Keep new and used batteries out of reach of children.
  - If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  - Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  - Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  - Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

Place the Device in a location that children cannot easily access.

- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

- 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 without professional instruction.
- Transport, use and store the Device under allowed humidity and temperature conditions.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword I
Important Safeguards and Warnings III
1 Product Introduction 1
1.1 Overview 1
1.2 Features 1
2 Initialization 4
2.1 Initializing the Device 4
2.2 Startup Wizard 6
2.3 Login 12
3 Device 15
3.1 Remote Device Initialization 15
3.2 Main Menu 15
3.3 Adding Remote Devices 17
3.3.1 Adding Cameras from Search 17
3.3.2 Adding Cameras Manually 19
3.3.3 Importing Cameras 21
3.4 Adding IoT Devices 23
3.5 Group Management 24
3.6 Camera Settings 25
3.6.1 Image 25
3.6.2 Overlay 29
3.6.3 Encode 30
3.6.4 Camera Name 33
3.7 Camera Update 34
4 Live View 36
4.1 Live View Overview 36
4.2 Live View Page 36
4.3 Live View Control Bar 38
4.4 Shortcut Menu 42
4.5 PTZ 43
4.5.1 PTZ Settings 43
4.5.2 PTZ Control 45
4.5.3 Configuring PTZ Functions 47
4.5.4 EPTZ 48
4.6 Fisheye De-Warp on Live View 51
4.7 Shortcut Menu to Modify Camera 53

4.8 Smart Tracking....53
5 Playback....54
5.1 General Video....54
5.1.1 Smart Search....57
5.1.2 AcuPick....57
5.1.3 Region of Interest....59
5.1.4 Video Clip....60
5.1.5 Tag Playback....60
5.1.6 EPTZ Linkage....61
5.1.7 Fisheye De-Warp during Playback....63
5.2 Target Video....63
5.3 Event Video....64
5.4 Video Clip....66
6 Events....68
6.1 Local Events....68
6.1.1 AI Function Overview....69
6.1.2 Mode Setting....70
6.1.3 AcuPick....71
6.1.4 Text Rule....72
6.1.5 Alarm Settings....73
6.1.6 Database....83
6.2 Events of Remote Devices....91
6.2.1 Alarm Event Settings....91
6.2.2 AI Settings....98
7 Searching Events and Reports....145
7.1 Event Center....145
7.1.1 Searching Real-Time Events....145
7.1.2 Searching Event History....146
7.2 Report Search....147
7.2.1 Face Statistics....147
7.2.2 People Counting....148
7.2.3 Crowd Density....148
7.2.4 Vehicle Density....149
7.2.5 Video Metadata....149
7.2.6 Heat Map....150
8 Backup....151
8.1 Video Backup....151
8.2 Picture Backup....151
8.3 Tag Backup....152

9 Maintenance 153
9.1 Log 153
9.2 System Information 154
9.2.1 Version 154
9.2.2 Intelligent Algorithm 154
9.2.3 Disk 154
9.2.4 Record 154
9.2.5 BPS 155
9.2.6 Device Status 155
9.2.7 Online User 156
9.3 Maintenance Management 156
9.3.1 Update 156
9.3.2 Device Maintenance 157
9.3.3 Import/Export 157
9.3.4 Default 158
9.3.5 Advanced Maintenance 159
9.3.6 Network Detection 159
10 Vehicle Entrance and Exit 162
11 Wizseek 165
12 Local Settings 168
12.1 Network Settings 168
12.1.1 TCP/IP 168
12.1.2 Port 171
12.1.3 External Wi-Fi 172
12.1.4 3G/4G 173
12.1.5 PPPoE 175
12.1.6 DDNS 176
12.1.7 UPnP 177
12.1.8 Email 178
12.1.9 SNMP 180
12.1.10 Multicast 182
12.1.11 Alarm Center 182
12.1.12 Auto Registration 183
12.1.13 P2P 184
12.1.14 Cluster IP 185
12.2 Storage Settings 185
12.2.1 Configuring Basic Parameters 185
12.2.2 Schedule 186
12.2.3 Disk Management 193

12.2.4 Disk Group 194
12.2.5 Disk Quota 195
12.2.6 Disk Check 196
12.2.7 Record Estimate 199
12.2.8 FTP 201
12.2.9 iSCSI 203
12.3 POS Settings 205
12.3.1 Privacy Setup 206
12.3.2 Connection Mode 207
12.4 System Settings 207
12.4.1 General Settings 207
12.4.2 Time 210
12.4.3 Output and Display 213
12.4.4 Account 216
12.4.5 Audio 224
12.4.6 Security 227
13 Web Operation 239
13.1 Network Connection 239
13.2 Web Login 239
13.3 Web Main Menu 239
14 Glossary 242
Appendix 1 HDD Capacity Calculation 243
Appendix 2 Mouse Operation 244
Appendix 3 Compatible Network Camera List 245
Appendix 4 Security Commitment and Recommendation 251

1 Product Introduction

1.1 Overview

The NVR is a high performance network video recorder. It supports local live view, multiple-window display, recorded file local storage, remote control and mouse shortcut menu operation, and remote management and control function.

This product supports central storage, front-end storage and client-end storage. The front-end monitoring points can be located anywhere in the network, without geographical restrictions. When networked with other front-end devices such as IP cameras and network video servers, along with specialized video surveillance system software, the system with a powerful security monitoring network can be established. In the network deployment system of this product, the central point and monitoring points can be connected with just a single network cable, eliminating the need for video and audio cables.

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

1.2 Features

Real-Time Surveillance

- Connects the NVR to a monitor through the VGA or HDMI port. Some series support TV/VGA/HDMI output at the same time.
- Shortcut menu for preview.
- Supports multiple popular PTZ decoder control protocols. Supports preset, tour and pattern.

Playback

- Supports independent real-time recording for each channel. At the same time, it supports functions such as smart search, forward play, network monitor, record search and download.
- Supports various playback modes: slow play, fast play, backward play and frame-by-frame play.
- Supports time title overlay so that you can view the accurate event time.
- Supports specified zone enlargement.

Smart Playback

This function is available on select models.

- IVS playback. It can screen out and replay the records meeting the set rules.
- Face detection playback. It can screen out and replay the records with human faces.
- Face recognition playback. It can compare the face information in the video with the information in the database and replay the corresponding records.
- ANPR playback. It can screen out the records with a specific vehicle plate number or all the records with car plate numbers.
- Human body detection playback. It can screen out and replay the records with specific human bodies.

- Smart search. It includes smart functions such as searching by attribute and searching by image to enable users to get target records quickly.

Alarm

- Responds to external alarm simultaneously (within 200 ms). Based on your pre-defined relay settings, the system can process the alarm input correctly and sends user screen or voice prompts (supporting pre-recorded audios).
- Supports settings of the central alarm server, so that the system can automatically notify users of the alarm information. Alarm input can be derived from various connected peripheral devices.
- Alerts you of alarm information via email.

AI Functions

AI functions are available on select models and vary with models.

- Face detection. The system can detect the faces that are on the video image.
- Face recognition. The system can compare the detected faces with the images in the face database in real time.
- Human body detection. The system activates alarm actions once human body is detected.
- People counting. The system can effectively count the number of people and flow direction.
- Heat map. The system can monitor the active objects in a specific area.
- Automatic number plate recognition (ANPR). The system can effectively monitor the passing vehicles.

Cloud Upgrade

For the NVR connected to the Internet, it supports online application upgrade.

User Management

Users can be added to user groups for management. Each group has a set of permissions that can be individually edited.

Storage

- With corresponding settings (such as alarm settings and schedule settings), you can back up related audio/video data in the network video recorder.
- You can take records via the web and the record files are saved on the computer in which the client locates.

Network Surveillance

- Sends audio/video data compressed by IPC or NVS to client-ends through the network, and then the data will be decompressed and displayed.
- Supports max 128 connections at the same time.
- Transmits audio/video data by protocols such as HTTP, TCP, UDP, MULTICAST and RTP/RTCP.

- Transmits some alarm data or alarm information by SNMP.
- Supports web access in WAN/LAN.

Window Split

Adopts video compression and digital processing to display several windows in one monitor. Supports 1, 4, 8, 9, 16, 25, and 36 window splits in live view and 1, 4, 9 and 16 window splits in playback.

Record

Supports regular record, motion record, alarm record and smart record. Save the recorded files in the HDD, USB device, client-end PC or network storage server and you can search or playback the saved files at the local-end or via the Web/USB devices.

Backup

Supports network backup and USB record backup. You can back up the recorded files in devices such as network storage server, peripheral USB 2.0 device and DVD.

Network Management

- Supervises NVR configuration and control power via Ethernet.
- Supports web management.

Peripheral Device Management

- Supports peripheral device control and you can freely set the control protocol and connection port.
- Supports transparent data transmission through RS-232 and RS-485.

Auxiliary

- Supports switch between NTSC and PAL.
- Supports real-time display of system resources information and running status.
- Supports log record.
- Local GUI output. Shortcut menu operation with the mouse.
- IR control function (for some series only). Shortcut menu operation with remote control.
- Supports playing the video/audio files from remote IPC or NVS.

2 Initialization

2.1 Initializing the Device

Background Information

- For first-time use, set a login password for the admin account (default user).
- We recommend setting password protection so that you can reset password in case you forgot.

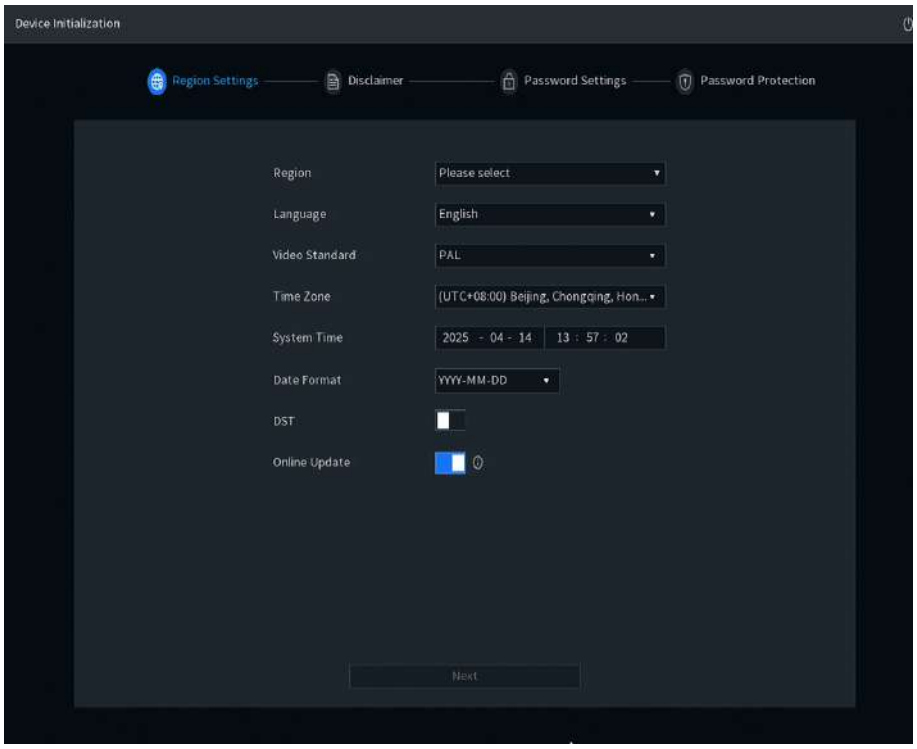
- For your device safety, keep your login password well, and change the password regularly.
- The IP address of the Device is 192.168.1.108 by default.

Procedure

Step 1 Start the NVR.

Step 2 Set region, time zone, and time according to the actual situation, and then click **Next**.

Figure 2-1 Region settings



Click to shut down the device. The system integrator or the user can shut down the Device directly after setting the time zone.

Step 3 Read the disclaimer, select **I have read and agree to the terms of the Software License Agreement and Privacy Policy** , and then click **Next**.

Step 4 Set the login password for the admin account, set the login password for trying to log in IPC, and then click **Next**.

You can click to enable the pattern password.

The camera will share the same password with the Device in the case that you select the checkbox next to **Same as the Local Password**.

Figure 2-2 Set password

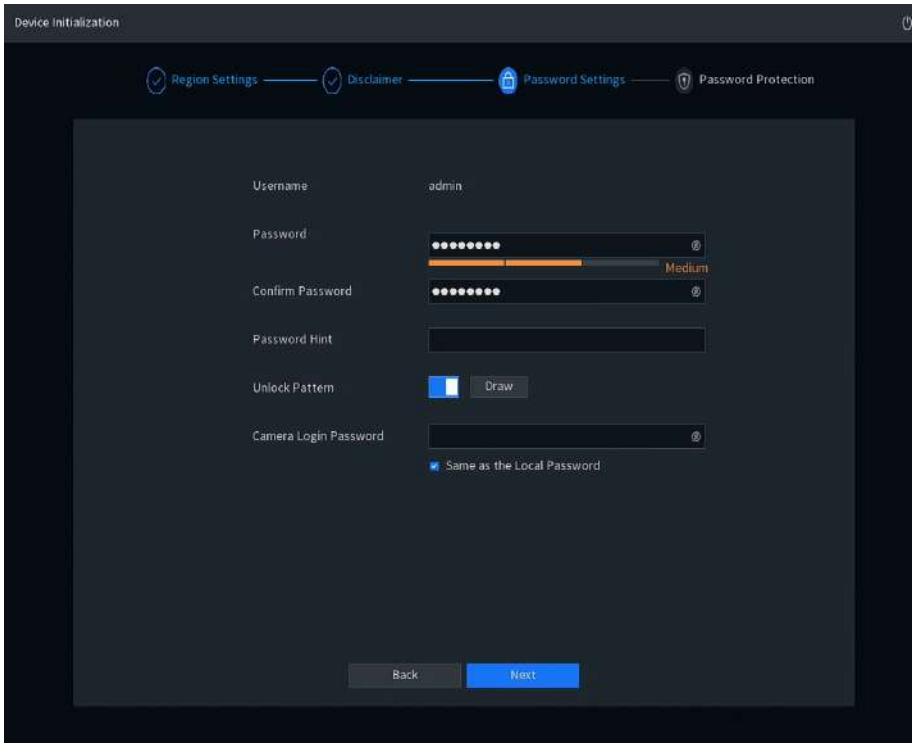


Table 2-1 Password parameters

Parameter	Description
Username	By default, the user is admin.
Password	Enter the password for admin and then confirm the password.
Confirm Password	
Password Hint	Enter the information that can remind you of the password. On the login window, click to display the password hint.
Unlock Pattern	Enable the pattern unlocking method. Click **Draw** to draw the unlock pattern.

Step 5 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 **Skip**.
- 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.

Step 6 Set password protection.

- After configuration, if you forgot the password for admin user, you can reset the password through the linked email address or security questions. For details on resetting the password, see "12.4.4.4 Password Reset".
- If you do not need password protection, disable **Reserved Email** and **Security Question**.

Figure 2-3 Set password protection

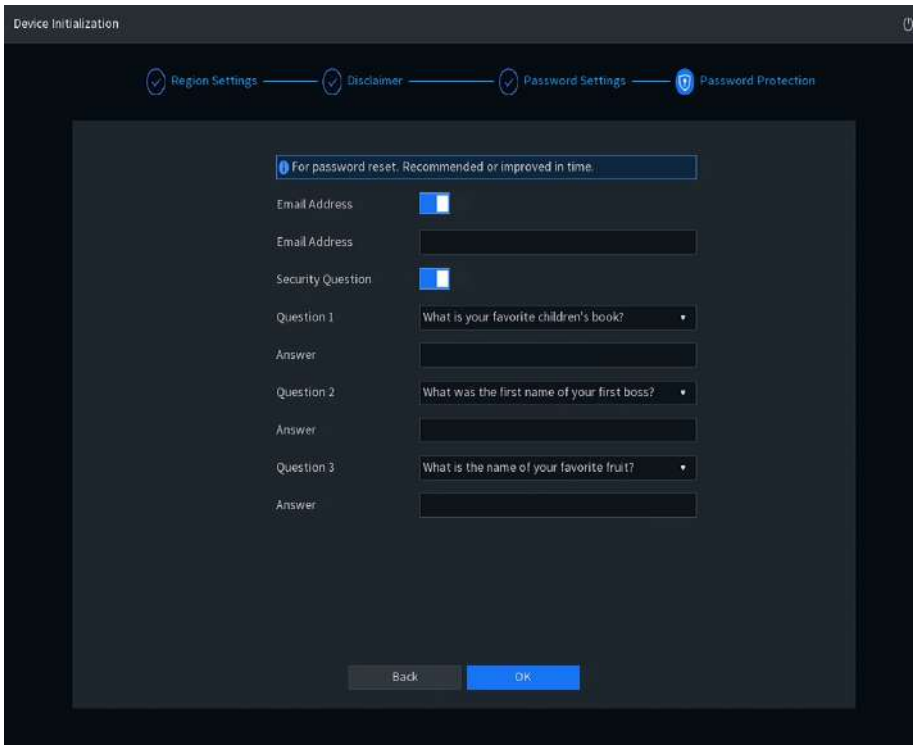


Table 2-2 Security question parameters

Password Protection Mode	Description
Email Address	Enable the **Email Address**. Enter an email address for password reset. If you forgot the password, enter the security code that you will get from this linked email address to reset the password of admin.
Security Questions	Configure the security questions and answers. If you forgot the password, you can reset the password after entering the answers to the questions.

Step 7 Click **OK**.

2.2 Startup Wizard

Background Information

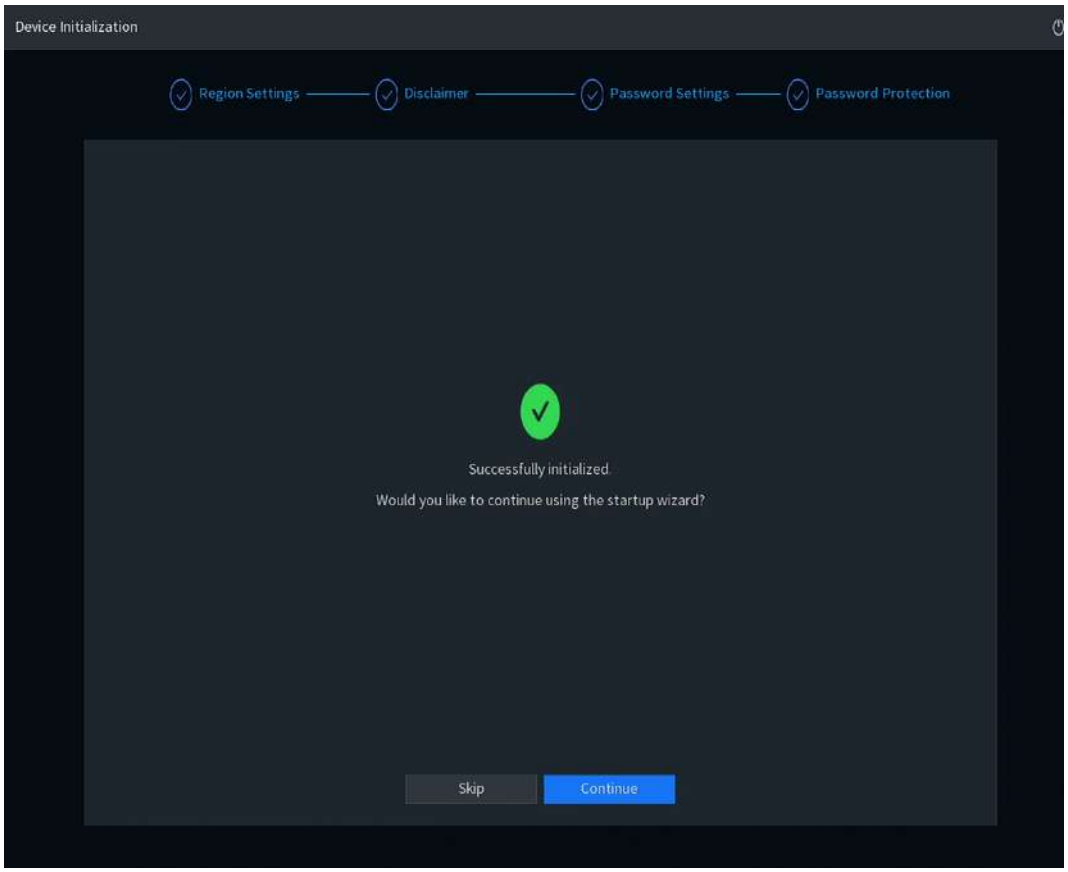
After initialization, the system goes to **Startup Wizard**. You can quickly configure your device.

Startup Wizard is displayed only when you log in to the Device for the first time or have restored the Device to factory settings.

Procedure

Step 1 After the initialization is successful, Click **Continue** to continue using the startup wizard.

Figure 2-4 Startup wizard

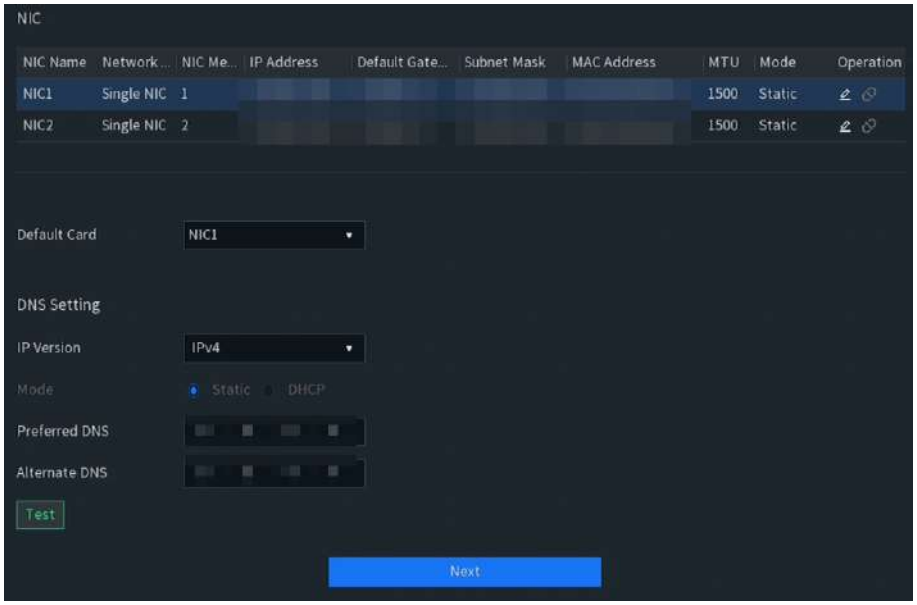


Step 2 Configure IP address, and then click **Next**.

The number of network adapters might vary with models. Configure the IP address of the network adapter according to the actual connection situation.

1. Click .

Figure 2-5 Edit network adapter



2. Configure parameters.

Table 2-3 Network parameters

Parameter	Description
Network Mode	• **Single NIC** : The current NIC card works independently. If the current NIC card is disconnected, the Device becomes offline. • **Fault Tolerance**: 2 NIC cards share one IP address. Normally only one NIC card is working. When this card fails, the other NIC card will start working automatically to ensure the network connection. The Device is regarded as offline only when both NIC cards are disconnected. When you select **Fault Tolerance** , you need to select the other NIC in **NIC Member**. • **Load Balance**: 2 NIC cards share one IP address and work at the same time to share the network load averagely. When one NIC card fails, the other card continues to work normally. The Device is regarded as offline only when both NIC cards are disconnected. When you select **Load Balance** , you need to at least select 2 binding NICs in **NIC Member**. • **Link Aggregation**: Multiple network cards share a single IP address to increase bandwidth or achieve redundancy through aggregation. When one network card fails, the other can still function normally. During network monitoring, the device's network connection is only lost when both network cards are disconnected. In environments with poor network conditions, the bandwidth of the network cards is more stable under dynamic aggregation. When you select **Link Aggregation** , you need to at least select 2 NICs in **NIC Member**. The Device with single Ethernet port does not support this function.
Default Ethernet Port	
IP Version	Select **IPv4** or **IPv6**. Both versions are supported for access.
DHCP	Enable the system to automatically obtain a dynamic IP address.
MAC Address	Displays the MAC address of the Device.
IP Address	• Enter the IP address and then configure the corresponding subnet mask and default gateway. • After configuration, click **Test** to check whether there is conflict in IP address. IP address and default gateway must be on the same network segment.
Subnet Mask	
Default Gateway	

To unbind NIC, on the **TCP/IP** page, click . The unbinding will take effect after the Device restarts.

3. On the **TCP/IP** page, configure DNS server. This step should be performed when you enable the domain name service.

You can get DNS server address or manually enter it.

- Automatically get DNS server address: When there is a DHCP server in the network, you can enable **DHCP**, and then the Device gets a dynamic IP address.
- Enter DNS server address: Select **IP Version**, and then configure the preferred DNS server and alternate DNS server.

4. On the **Default Card** drop-down list, select the default NIC.
5. Click **Next**.

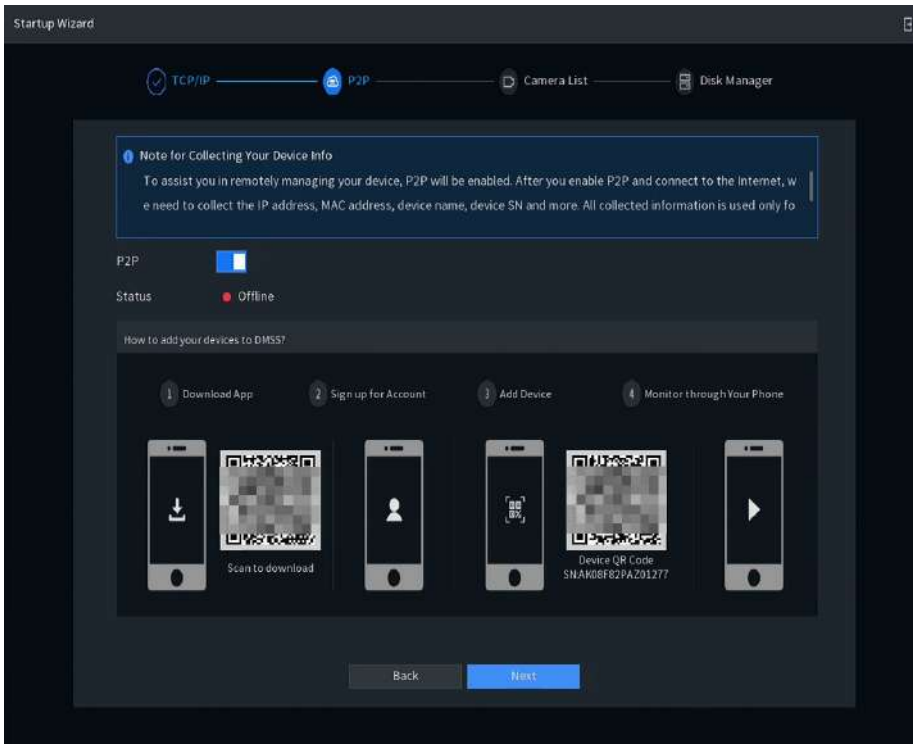
Step 3 Enable **P2P**, and then click **Next**.

Scan the QR code on the actual page to download the app. Register an account and then you can add the Device to the app.

Before using the P2P function, make sure that the NVR has connected to the WAN.

The **Status** becomes **Online** after you successfully configure P2P.

Figure 2-6 P2P



Step 4 Add cameras according to the actual situation.

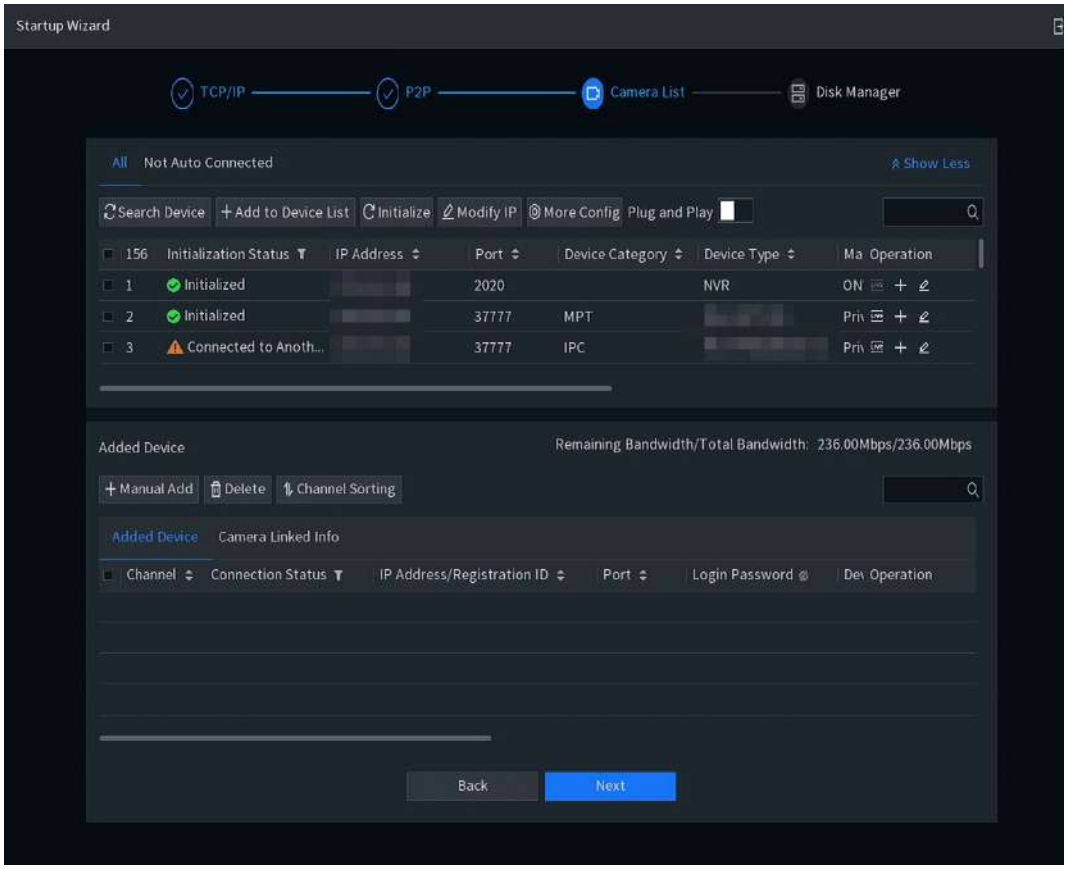
After adding cameras, you can view the video images transmitted from the cameras, and change camera configuration.

- The number of cameras that can be added to the NVR varies with models.
- The system supports adding camera through searching, manual add and batch add. This section uses adding by searching as an example.
- Initialize the camera before adding to the Device.

1. Click **Search Device**.

   The devices found are displayed at the upper pane, excluding devices already added.

Figure 2-7 Search device



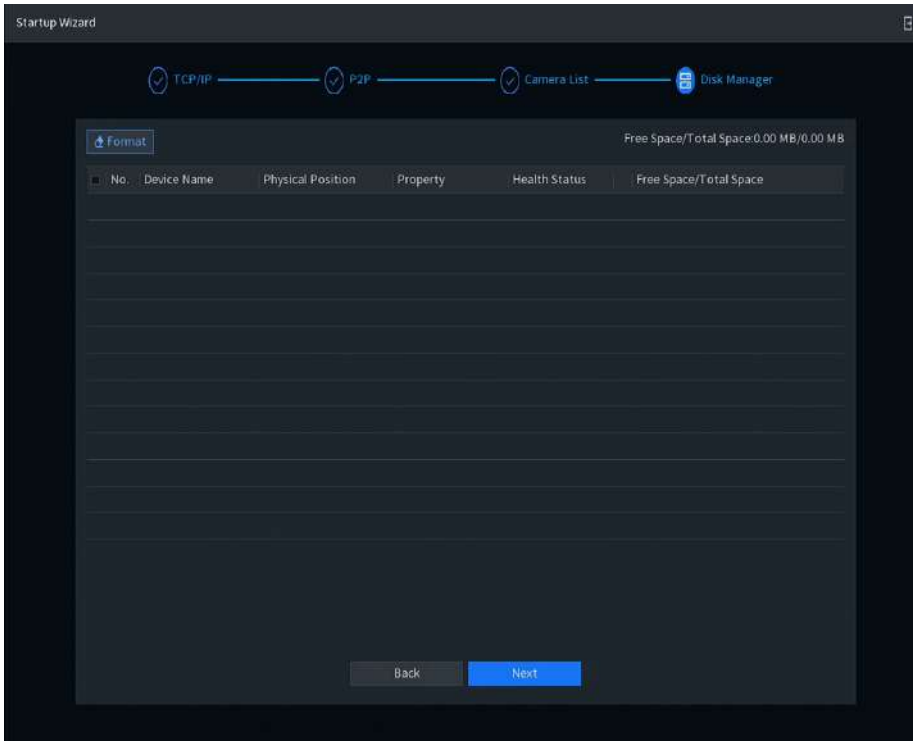
- To view the live image of a camera, click **LIVE** and then enter the username and password. You can only view live images of cameras accessed through private protocol.
- To filter the remote devices, select device name from the filter drop-down list.
- To view all remote devices added through plug and play, click the **Not Auto Connected** tab. You can remove devices added through plug and play, and they can be automatically added again after plug and play is enabled.

For more details about adding cameras, see "3.3 Adding Remote Devices".

Step 5 Manage HDD. You can view HDD name, physical position, health status, capacity, and more.

- To configure read/write property, select an option from the **Properties** drop-down list.
- To format an HDD, select the HDD, and then click **Format**.

Figure 2-8 Manage HDD



Step 6 Click **OK**.

When the Device prompts whether to restart, click **OK**. The configurations through startup wizard take effect after the Device restarts.

2.3 Login

Log in to the Device to perform local operations.

Procedure

Step 1 Right-click the live view, and then click the shortcut menu.

- If you have configured unlock pattern, the unlock pattern login window is displayed. Click **Forgot Pattern** to switch to password login.
- If you have not configured the unlock pattern, the password login window is displayed.

Figure 2-9 Unlock pattern login

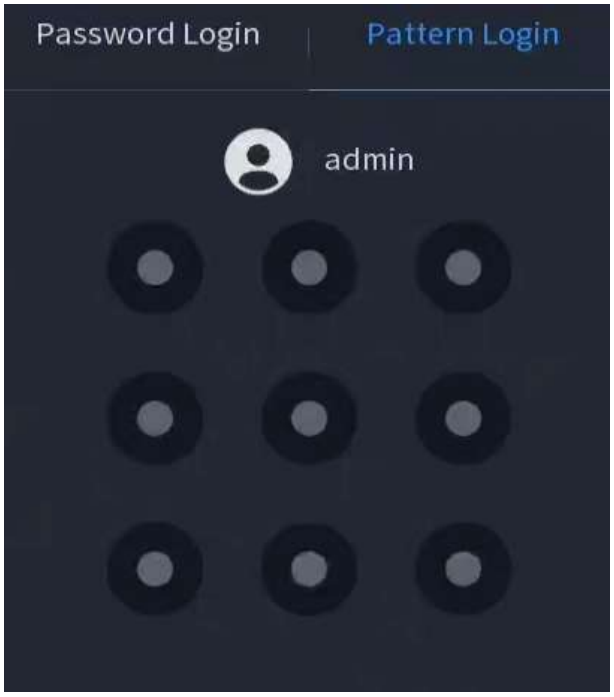
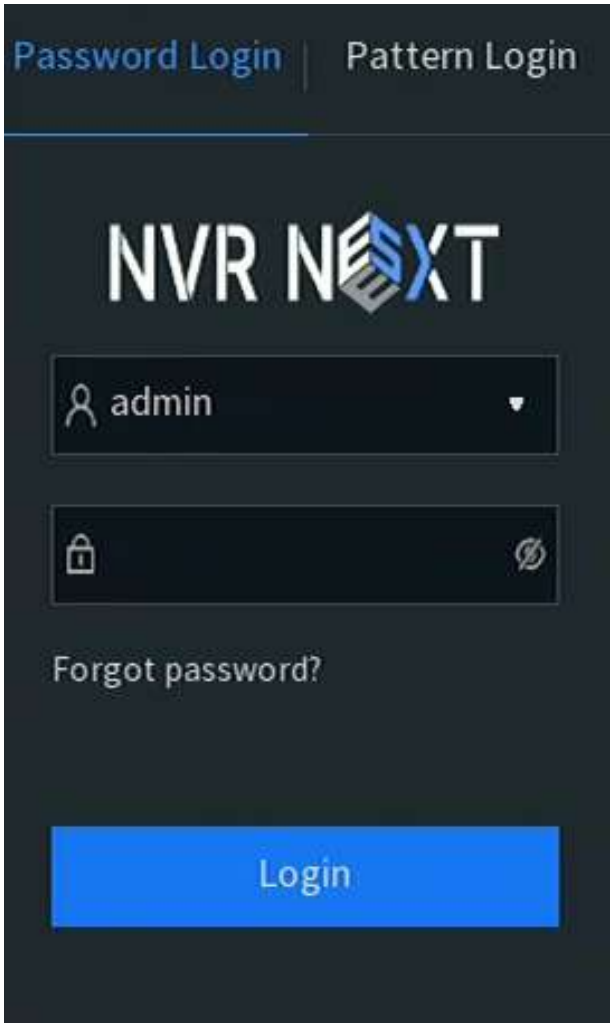


Figure 2-10 Password login



Step 2 Draw unlock pattern, or enter password, and then click **Login**.

3 Device

3.1 Remote Device Initialization

After initializing the remote device, you can view the camera video and modify the camera's login password and IP address.

Background Information

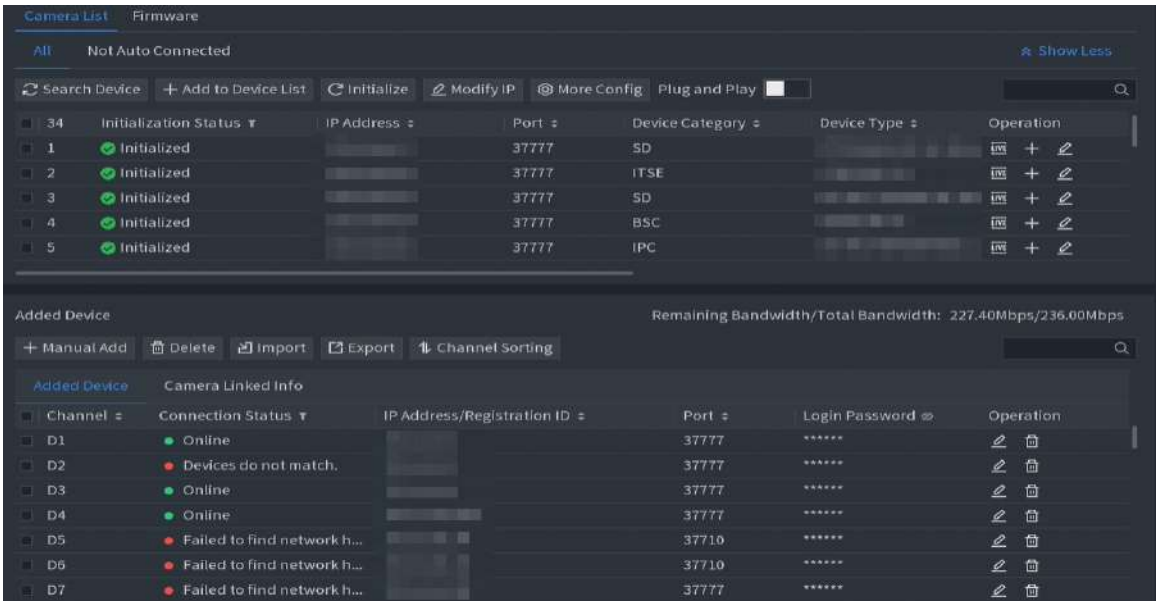
- When the IPC is connected to the device via the PoE interface, the system automatically initializes the IPC, inheriting the device's password and mobile information by default.
- If the device has just been upgraded to a new system version, the IPC may fail to initialize upon connection through the PoE interface. In this case, you can perform the initialization operation for the IPC on the remote device's PoE devices in **REMOTE DEVICE** > **PoE Devices**.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **Video Device**.

Step 2 Click **Search Device**.

Figure 3-1 Search device



Step 3 Select the uninitialized remote devices and click **Initialize**.

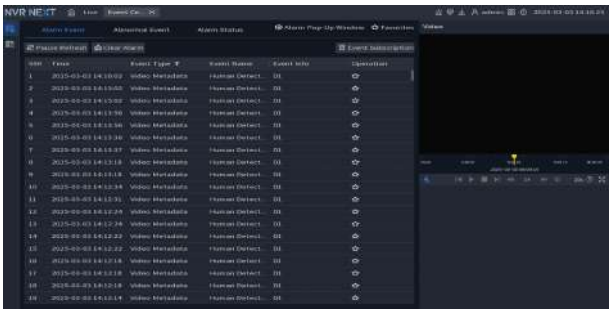
Step 4 Configure the password and click **OK**.

3.2 Main Menu

After login, right-click the live view, and then click **Main Menu**.

Figure 3-2 Main menu

Table 3-1 Main menu description

No.	Description
1	Click each part to open the corresponding configuration page.
2	Click the icon to go back to the main menu.
3	Go back to live view.
4	Click the icon to view the alarm information about **Alarm Event** , **Abnormal Event** and **Alarm Status**. 
5	Click the icon to enable or disable the arming function.
6	Click the icon to view the downloading information.
7	Log out of, restart, or shut down the Device.
8	Click the icon to get the QR codes of mobile client, device SN and product material. You can add the Device to the mobile client for remote management.
9	Click the icon to view the device information.

No.	Description
10	Displays the date and time.
11	Configure the applications of live view, playback, AI report, maintenance, backup, event center and vehicle entrance and exit.
12	Configure the settings of remote device, network, storage, event, POS and system.

You can click the icons on the main menu to go to the corresponding configuration page. After that, you can go to other function parts or setting items through the quick operation bar.

3.3 Adding Remote Devices

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

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

3.3.1 Adding Cameras from Search

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

Background Information

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

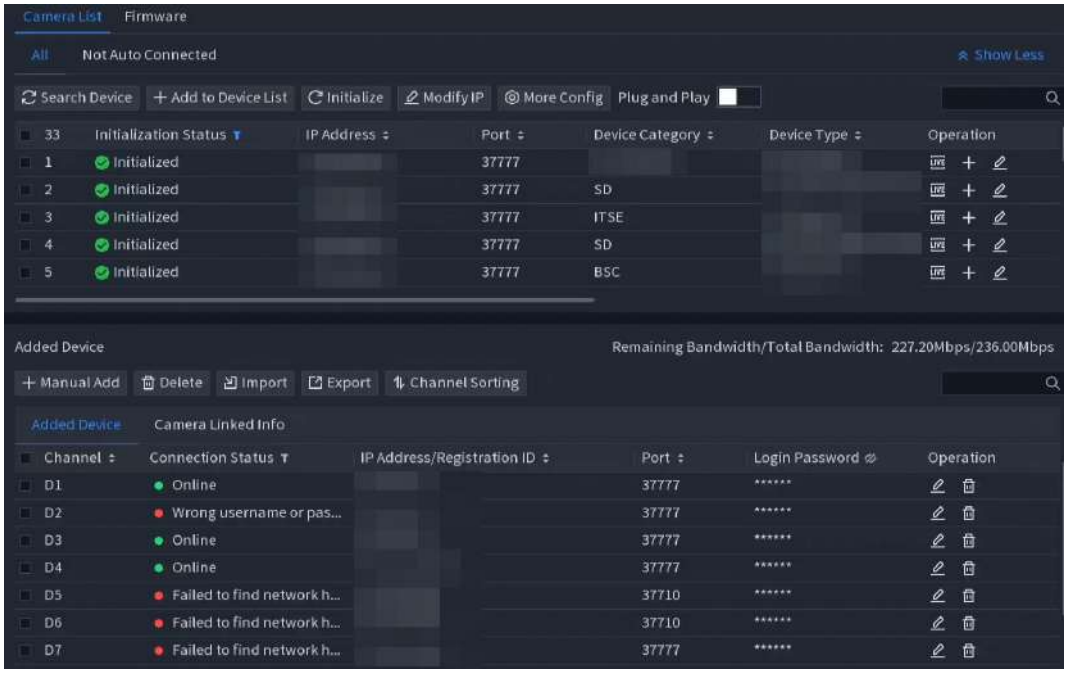
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **Video Device** > **Camera List**.

Step 2 Click **Search Device**.

The remote devices found are displayed at the upper pane. Devices already added are not included in the searched results.

Figure 3-3 Search device



- For cameras accessed through private protocol, you can click **LIVE** and then enter the username and password to play live video.
- To filter the remote devices, you can enter all or part of device name in the filter box.
- To view all remote devices added through plug and play, you can click the **Not Auto Connected** tab. You can remove devices added through plug and play, and they can be automatically added again after plug and play is enabled.

Step 3 (Optional) Enable **Plug and Play**.

When **Plug and Play** is enabled, the NVR automatically adds remote devices on the same subnet.

- For uninitialized remote devices, the NVR automatically initializes them before adding them.
- You can click **More Config** to select **Plug and Play Validity Period**. For example, when you set the validity period as 1 hour, the plug and play will be automatically turned off after 1 hour.

Figure 3-4 Validity period

Step 4 (Optional) Click **More Config** to select **H.265 Auto Switch**.

When **H.265 Auto Switch** is enabled, the video compression standard of added remote devices is switched to H.265 automatically.

Step 5 Double-click a remote device, or select a remote device and then click **Add** to register it to the **Added Device** list.

Related Operations

- Change device login password.

  Click **More Config** to select **Change Device Login Password** to change the password.
- Show camera login password.

  Select an added camera, and then click **Show Device Password** to show the password.
- Edit camera information.

  On the **Added Device** list, click to change the IP address, username, password and other information.
- Import and export cameras.

  You can export the information of the connected cameras and import camera information to the system to add cameras in batches. For details, see "3.3.3 Importing Cameras".
- Sort channel

  Click **Channel Sorting**, and then you can directly drag the channel to rearrange channels.
- View linked information.

  If the camera has multiple channels, you can click the **Camera Linked Info** to view linked information of the remote device.
- Delete cameras.
  - Delete one by one.

    Click to delete the corresponding camera.
  - Delete in batches.

    Select one or more cameras, and then click **Delete**.

3.3.2 Adding Cameras Manually

Background Information

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

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 **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **Video Device** > **Camera List**.

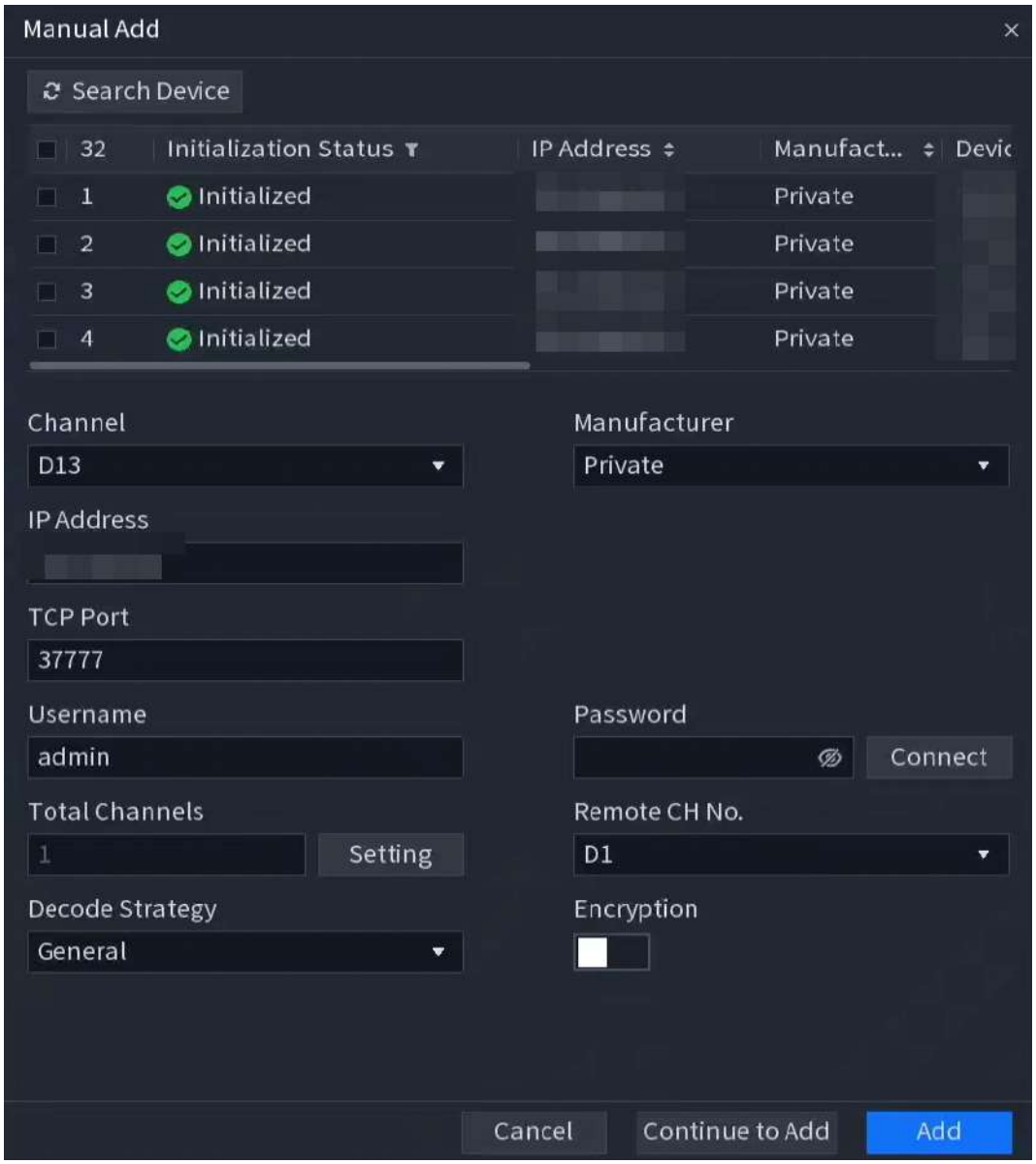
Step 2 (Optional) Click **More Config** to select **H.265 Auto Switch**.

When **H.265 Auto Switch** is enabled, the video compression standard of added remote devices is switched to H.265 automatically.

Step 3 Click **+ Manual Add**.

On this page, you can also search devices and select them to add.

Figure 3-5 Manual add



Step 4 Configure the parameters.

The parameters might vary depending on the manufacturer that you select.

Table 3-2 Remote channel parameters

Parameter	Description
Channel	Select the channel that you want use on the Device to connect the remote device.

Parameter	Description
Manufacturer	Select the manufacturer of the remote device. Connect the Imou camera to the Device through the ONVIF protocol, otherwise the Imou camera added through private protocols cannot be connected.
Registration ID	Enter the registration ID of the remote device.
IP Address	Enter the IP address of the remote device.
RTSP Port	Enter the RTSP port number. The default value is 554.
HTTP Port	Enter the HTTP port number. The default value is 80.
TCP Port	The default value is 37777. You can enter the value as needed.
Username	Enter the username of the remote device.
Password	Enter the password of the user for the remote device.
Total Channels	Click **Connect** to get the total number of channels of the remote device. For the remote device with multiple channels, you can choose the connected number of channels as needed.
Remote CH No.	Enter the remote channel number of the remote device.
Decode Strategy	Set up the decoding cache, including **Default** , **Realtime**, or **Fluent**.
Protocol Type	• If the remote device is added through private protocol, the default type is **TCP**. • If the remote device is added through ONVIF protocol, the system supports **Auto** , **TCP**, **UDP**, or **MULTICAST**. • If the remote device is added through other manufacturers, the system supports **TCP** and **UDP**.
Encryption	If the remote device is added through ONVIF protocol, select the **Encrypt** checkbox and then the system will provide encryption protection to the data being transmitted. To use this function, make sure that the HTTPS function is enabled for the remote IP camera.

Step 5 Click **OK**.

3.3.3 Importing Cameras

You can import remote devices in batches.

Background Information

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

Procedure

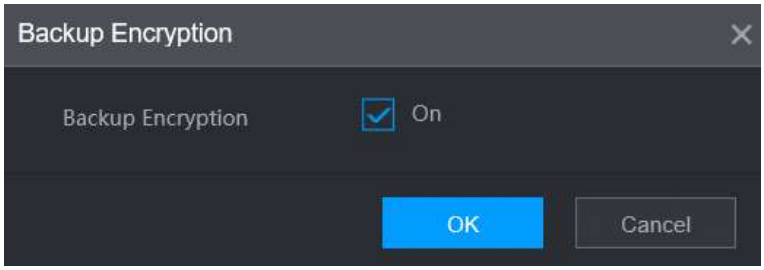
Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **Video Device** > **Camera List**.

Step 2 Export the template.

The exported template includes the information of the added remote device. Pay attention to your data security.

1. Click **Export**.

Figure 3-6 Backup encryption



2. Enable or disable the backup encryption, and then click **OK**.

- If **Backup Encryption** is enabled, the file format is .backup.
- If **Backup Encryption** is disabled, the file format is .csv. Keep unencrypted files well to avoid data leakage.

3. Select the storage path and then click **Save**.

- The template file is named RemoteConfig_*20220222191255*.csv. *20220222191255* represents the export time.

  Please open the file using the latest version of Excel.
- The template includes the IP address or registration ID, port, remote channel No., manufacturer, username, password and other information.

Step 3 Fill in the template and then save the file.

Do not change the file extension of the template. Otherwise, the template cannot be imported.

Step 4 Click **Import**, select the template file and then open it.

The remote devices in the template are added to the NVR. If the remote device in the template has been added, the system will prompt you whether to replace the existing one on the device list.

- If you select **Yes**, the system deletes the existing one and import the device again.
- If you select **No**, the system retains the existing one and add the device to another unoccupied channel.

3.4 Adding IoT Devices

Search and add IoT remote devices in the same network.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **IoT**.

Step 2 Add devices.

- Add devices through search.

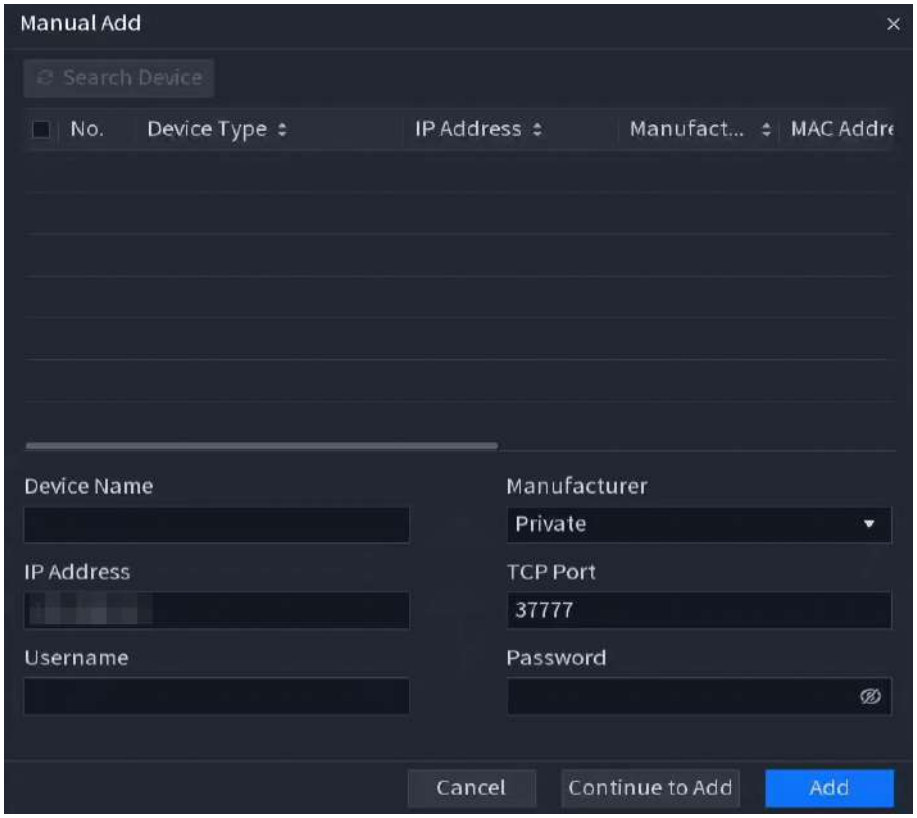
1. Click **Search Device** and all remote devices are displayed except for already-added remote devices.
2. Select the icon next to the remote device and click **Add**. The added remote devices will be displayed in the list. Icon indicates a successful connection.
3. Double-click the remote device information, or select the checkbox in front of the remote device and click **+ Add to Device List**.

Figure 3-7 All devices

- Manual add.

1. Click **Manual Add**.

Figure 3-8 Manual add



2. Set the information and the added remote devices will be displayed in the list. Icon indicates a successful connection.
3. Configure the parameters.

   If you want to add more devices, click **Continue to Add**.
4. Click **Add**.

3.5 Group Management

Create groups and add cameras, IoT devices to construct the arming schedule.

Procedure

Step 1 Select **Main Manu** > **SETTINGS** > **REMOTE DEVICE** > **Add Device** > **Group Management**

Step 2 Click to create a group list. You can set group names and add devices.

Figure 3-9 Group management

You can click **Add** to add devices or click **Delete** to delete devices within a group list.

3.6 Camera Settings

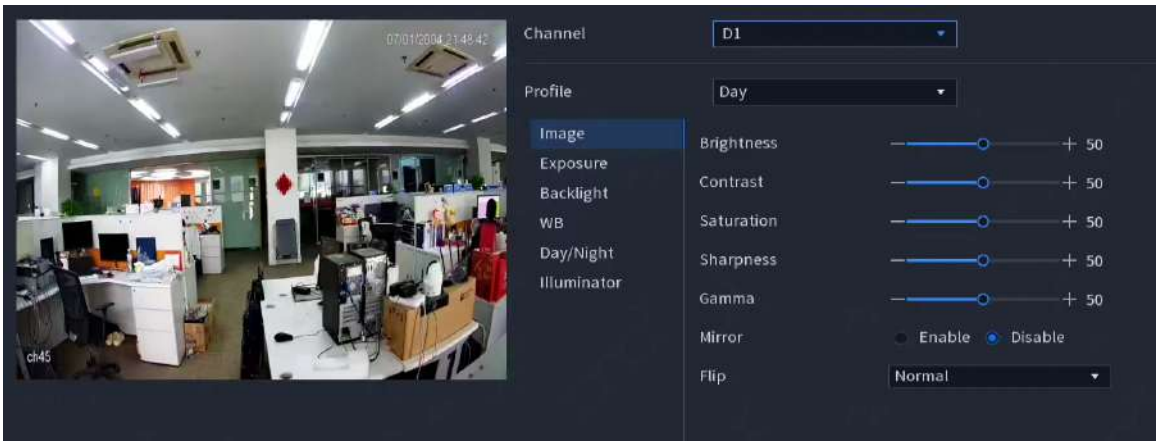
3.6.1 Image

You can set network camera parameters according to different contexts to get the desirable video effect.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Image**.

Figure 3-10 Image



Step 2 Select a channel, and then configure parameters.

The parameters might vary depending on the camera model.

Table 3-3 Image parameters

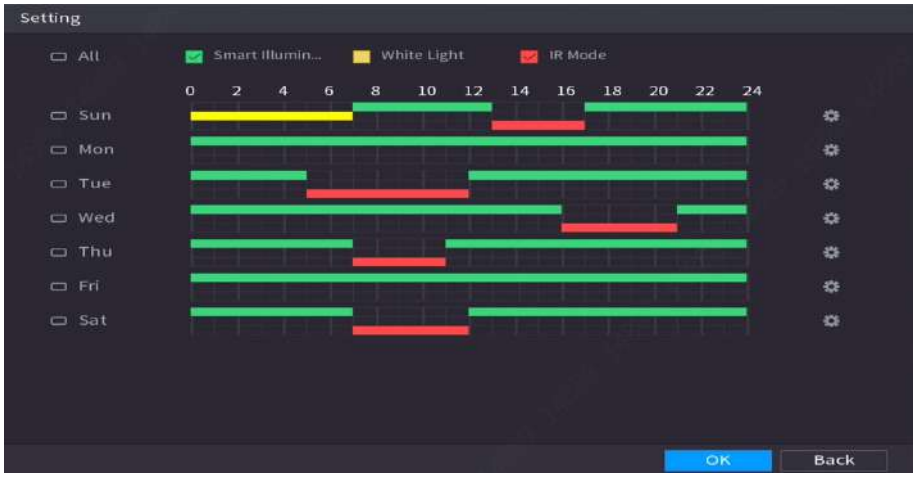
Parameter	Description
Profile	There are three configuration files. The system has configured the corresponding parameters for each file. You can select according to your actual situation.
Brightness	Adjust the image brightness. The bigger the value is, the brighter the image will become.
Contrast	Adjust the image contrast. The bigger the value is, the more obvious the contrast between the light area and dark area will become.
Saturation	Adjust the color shades. The bigger the value, the lighter the color will become.
Sharpness	Adjust the sharpness of image edge. The bigger the value is, the more obvious the image edge is.
Gamma	Adjust image brightness and enhance the image dynamic display range. The bigger the value is, the brighter the video is.

Parameter	Description	
Mirror	Switch the left and right sides of the video image. It is disabled by default. This function is available on selected models.	
Flip	Set video display direction. It includes normal, 180°, 90°, and 270°.	
AI SSA	After you enable AI SSA (AI Scene Self-adaptation), the camera can detect environmental conditions, such as rain, fog, backlight, low light and flicker, to adjust the parameters of the image to suit the conditions, ensuring that clear images are always produced. ● When AI SSA is enabled, some image parameters such as exposure and backlight mode will become unavailable. ● This function is only available on select models.	
Exposure	Auto Iris	● This function is available when the camera is equipped with the auto iris lens. ● After you enable auto iris function, the iris can automatically zoom in and zoom out according to the brightness of the environment and the image brightness changes accordingly. ● If you disable the auto iris function, the iris is at the biggest value. The iris does not automatically zoom in or zoom out according to the brightness of the environment.
	3D NR	This function specially applies to the image whose frame rate is configured as 2 at least. It reduces the noise by using the information between two frames. The bigger the value is, the better the effect.
Backlight Mode	You can set camera backlight mode. ● SSA: In the backlight environment, the system can automatically adjust image brightness to clearly display the object. ● BLC: ◇ Default: The device performs automatic exposures according to the environment situation to make the darkest area of the video clear. ◇ Customize: After you select the specified zone, the system can expose the specific zone so that the zone can reach the proper brightness. ● WDR: In backlight environment, the system lowers the high bright section and enhances the brightness of the low bright section, so that you can view these two sections clearly at the same time. ● HLC: In the backlight environment, the system lowers the brightness of the brightest section, reduces the area of the halo and lowers the brightness of the whole video. ● Close: Disable the BLC function.	

Parameter	Description
WB Mode	You can set camera white balance mode. The system adjusts the overall image hue to make the image color display precisely as it is. Different cameras support different white balance modes, such as auto, manual, natural light, and outdoor.
Day/Night Mode	Configure the color and black & white mode of the image. This parameter is not affected by the configuration files. • **Color** : The camera outputs color image only. • **Auto** : The camera outputs color images or black and white images according to ambient brightness • **B/W** : The camera outputs black and white image only. • **Sensor** : Use this mode when there is peripheral IR light connected. The **Sensor** mode is available on select non-IR models.

Parameter	Description
Illuminator	When the camera comes with an illuminator, you can configure the illuminator solution. 1. Click **Settings** next to **Illuminator** to configure the illuminator. 2. Select an illuminator solution from the **Fill Light** drop-down list. • **IR Mode**: Enable the IR illuminator, and the white light is disabled. You can only capture black and white images after enabling this function. • **White Light**: Enable the white light, and the IR illuminator is disabled. You can capture clear scene image after enabling this function. • **Smart Illumination**: This function is mainly used at night. Smart illumination applies IR mode in most situations. When an event occurs (such as perimeter, motion detection and human detection), the camera automatically switches to white light mode to link image capturing and video recording under the full color mode. The white light turns off when the event stops, and then the mode switches to IR mode according to the ambient brightness. The status of the illuminator mainly depends on time and environment. If the smart illumination is triggered at night and the event continues during the day, the illuminator configured for the daytime will be turned off. • **By Time**: Set the illumination solution according to the time period and use different solutions at different time periods. 3. Configure the time plan. a. Click **Settings** next to **Time Plan**. b. Select an illumination solution, and then drag on the timeline to select the time period of the illumination solution. Different colors represent different illumination solutions on the timeline, as shown in the following figure. • Click the selected time period, and then set an accurate start and end time. • Click **Copy**, select weeks, and then click **Apply**. Time plans for the current week can be quickly copied to other weeks. 4. Click **OK**.

Figure 3-11 Set the time plan



Step 3 Click **Apply**.

3.6.2 Overlay

You can set parameters for overlay and private masking.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Overlay**.

Step 2 Select a channel and then configure parameters.

Table 3-4 Video overlay parameters

Parameter	Description
Channel title	Displays the channel title on the video image in live view and playback. 1. Select **Channel Title** and then edit the channel title. 2. Drag the channel title to a desired place. 3. Click **Apply**.
Time title	Displays the time title on the video image in live view and playback. 1. Select **Time Title**. 2. Drag the time title to a desired place. 3. Click **Apply**.
Location	Displays geographic location on real-time live view page and video playback page. 1. Enable the location function and enter the geographic location. 2. Click **+** to expand geographic location overlay, supporting up to an additional 13 rows.
Custom title	You can customize title to be overlaid on the video image. Click **Setting** to set the information such as font size, title content and text alignment, and then click **OK**.

Parameter	Description
Font Properties	• Set font size: Supports adaptive, 16 * 16, 32 * 32, 48 * 48, and 64 * 64. • Set font color: Customizes color.
Privacy Masking	Displays concealment color blocks on the real-time live view page and the recorded video playback page. 1. Enable **Privacy Masking** to enter the customized title. 2. Enable the function, move and resize the color blocks, with a maximum of 4 blocks supported.
Default	Restore the overlay settings to default configuration.
Copy to	Copy the overlay settings to other channels.

Step 3 Click **Apply**.

3.6.3 Encode

You can set video bit stream and image parameters.

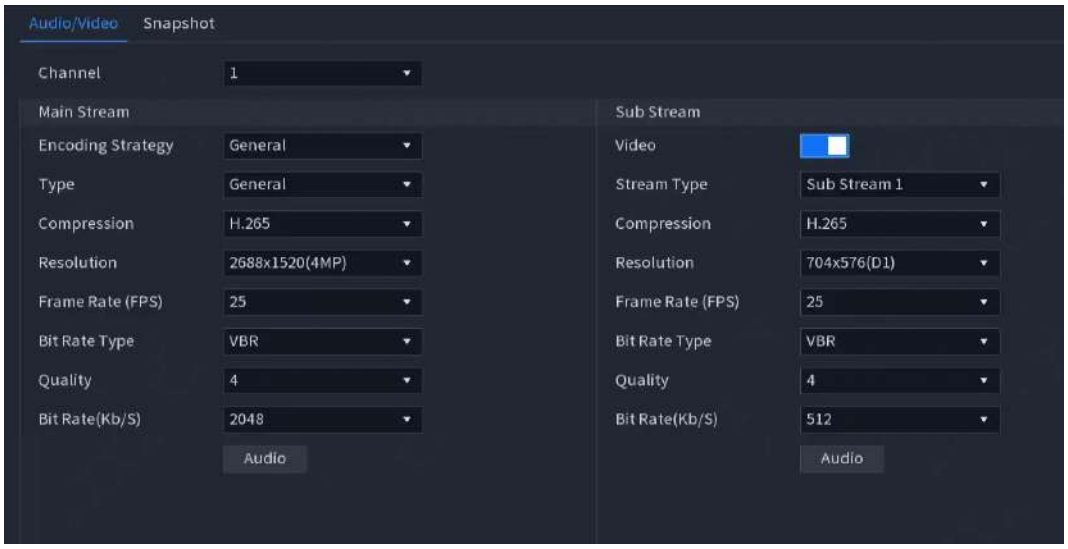
3.6.3.1 Configuring Audio and Video Encoding Settings

You can set audio and video encoding parameters such as bit stream type, compression, and resolution.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Encode** > **Audio/Video**.

Figure 3-12 Audio/video



Step 2 Select a channel and then configure parameters.

The parameters for main stream and sub stream are different. Some models support three streams: main stream, sub stream 1, sub stream 2.

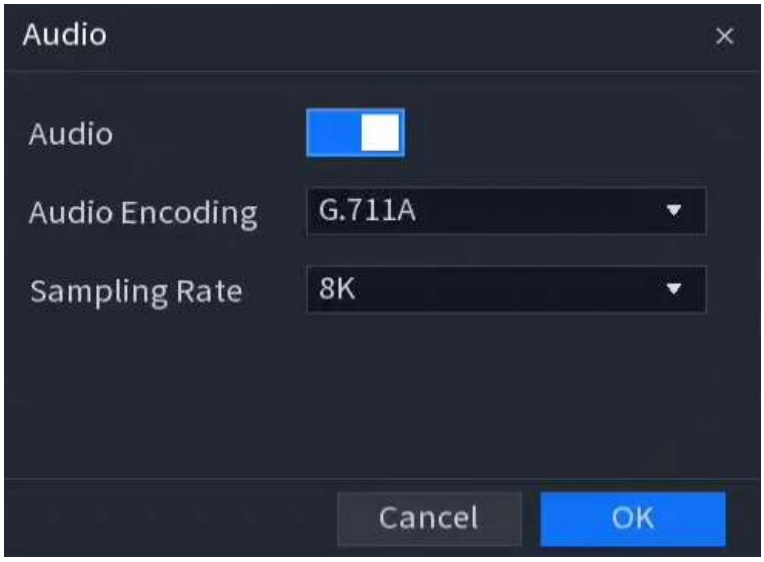
Table 3-5 Audio/video parameters

Parameter	Description
Coding Strategy	• **General** : Use general coding strategy. • **Smart Coding** : Enable the smart coding function. This function can reduce the video bit stream for non-important recorded video to maximize the storage space. • **AI Coding** : Enable the AI coding function. This function can reduce the camera code stream, network transmission pressure, and hard drive storage space without affecting the image quality.
Type	Select the recording type for main stream from **General** , **Motion** (motion detection), or **Alarm**.
Compression	Select the encoding mode. • H.265: Main profile encoding. This setting is recommended. • H.264H: High profile encoding. Low bit stream with high definition. • H.264: Main profile encoding. • H.264B: Baseline profile encoding. This mode requires higher bit stream compared with other modes for the same definition.
Resolution	Select resolution for the video. The maximum video resolution might be different depending on your device model.
Frame Rate (FPS)	Configure the frames per second for the video. The higher the value is, the clearer and smoother the image will become. Frame rate changes along with the resolution. Generally, in PAL format, you can select the value from 1 through 25; in NTSC format, you can select the value from 1 through 30. However, the actual range of frame rate that you can select depends on the capability of the Device.
Bit Rate Type	• **CBR** (constant bit rate): The bit rate changes slightly around the defined value. We recommended selecting **CBR** when there might be only small changes in the monitoring environment. • **VBR** (variable bit rate): The bit rate changes with monitoring scenes. Select variable stream when there might be big changes in the monitoring environment. • **ABR** (average bit rate): When selecting **ABR**, you need to configure **Max Bit Rate** and **ABR**. The connected camera needs to support the average bit rare.
Quality	The bigger the value is, the better the image will become. This parameter is available if you select **VBR** as **Bit Rate Type**.

Parameter	Description
I Frame Interval	The interval between two reference frames.
Bit Rate (Kb/S)	• Main stream: The higher the value, the better the image quality. • Sub stream: For constant stream, the bit rate changes near the defined value; for variable stream, the bit rate changes along with the image but the maximum value still stays near the defined value.

Step 3 Click **Audio**.

Figure 3-13 Audio settings



Step 4 Configure audio compression parameters.

Table 3-6 Audio compression parameters

Parameter	Description
Audio	This function is enabled by default for main stream. You need to manually enable it for sub stream. Once this function is enabled, the recorded video file is composite audio and video stream.
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 5 Click **OK**.

Step 6 Click **Apply**.

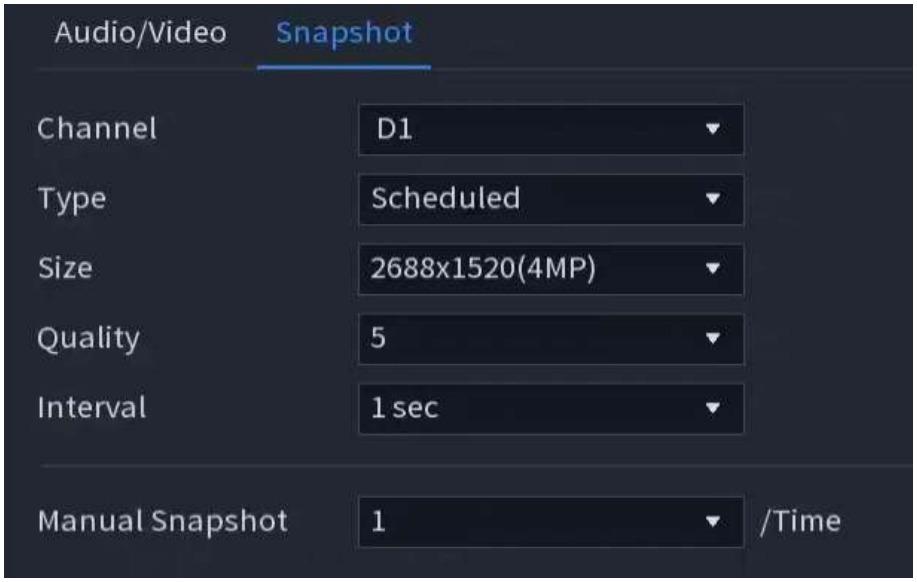
3.6.3.2 Snapshot

You can set snapshot mode, image size, quality and interval.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Encode** > **Snapshot**.

Figure 3-14 Snapshot



Step 2 Configure parameters.

Table 3-7 Snapshot parameters

Parameter	Description
Channel	Select the channel that you want to configure the settings for.
Type	• **Scheduled** : The snapshot is taken during the scheduled period. • **Event** : The snapshot is taken for motion detection, video loss, local alarms and other events.
Size	The size is determined by the resolution of the main stream or sub stream of the channel.
Quality	Configure the image quality. The higher the level is, the better the image will become. Level 6 represents the best quality.
Interval	Select or customize how frequently snapshots are to be taken.
Manual Snapshot	Select the number of snapshots that you want to take each time.

Step 3 Click **Apply**.

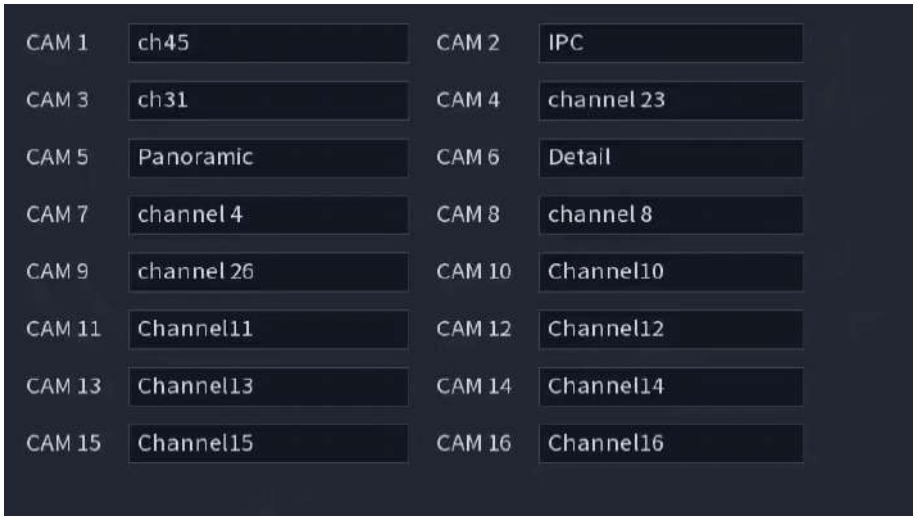
3.6.4 Camera Name

You can customize channel name.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Camera Name**.

Figure 3-15 Camera name



Step 2 Modify a channel name.

- You can only change the name of the camera connected via the private protocol.
- You can enter up to 63 English characters for a channel name.
- When the system is in Chinese or English, the content in the text input box (excluding password input box) can be copied and pasted.

Step 3 Click **Apply**.

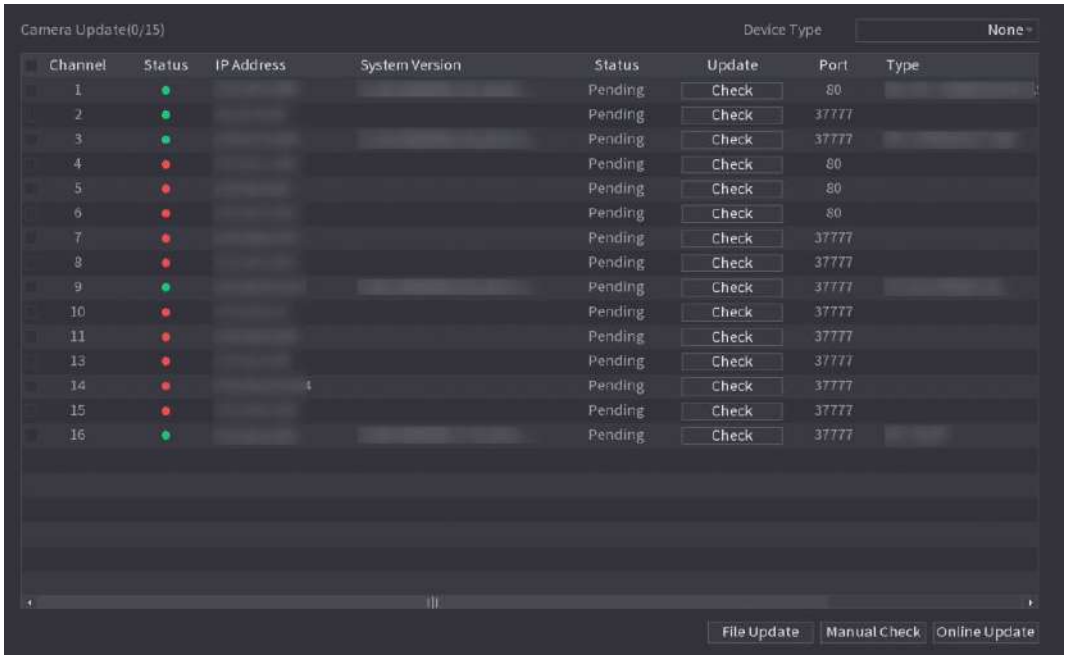
3.7 Camera Update

You can update the firmware of the connected network camera through online update or file update.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Remote Maintenance** > **Update**.

Figure 3-16 Update



Step 2 Update the firmware of the connected remote device.

If the upgrade fails, you can check the update log.

- Online update.
  1. Select a remote device and then click **Manual Check**.

     The system checks for available updates.
  2. Select a remote device that has an update available for it, and then click **Online Update**.
- File update.
  1. Select a channel and then click **File Update**.
  2. Select an update file.
  3. Click **OK**.

     If there are too many remote devices, you can filter them on the **Device Type** list.

4 Live View

4.1 Live View Overview

After you logged in, the system goes to multiple-channel live view mode by default. You can view the live video of each channel.

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

4.2 Live View Page

Click **LIVE** on the main menu, and you can view the live video of each channel and configure the channel layout, display settings, and PTZ settings.

Figure 4-1 Live view page

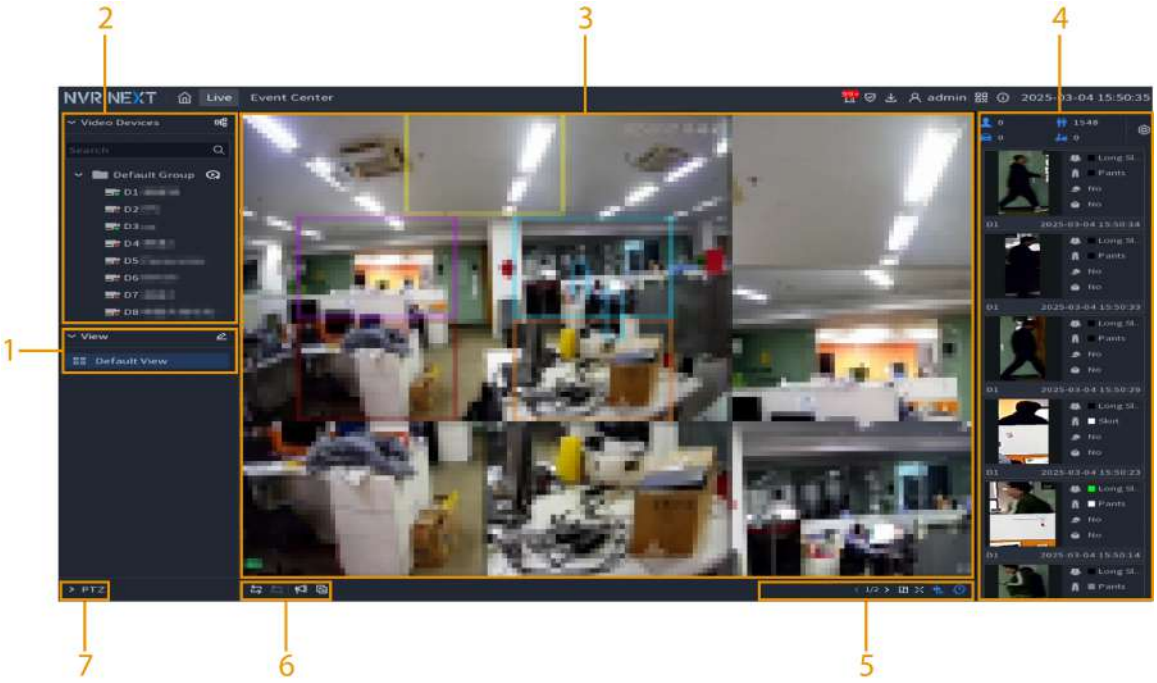


Table 4-1 Page description

No.	Module	Description
1	View layout	Edit the layout of the channel live view section, supporting the pre-configuration of view layouts.
2	Video devices	Configure the grouping of video devices. For details, see "3.5 Group Management".
3	Live view of channels	Modify the channel layout and display or interact with the channels using the function buttons for channel display, channel switching, and the broadcast section.

No.	Module	Description
4	AI live page	Enable the AcuPick function to analyze the characteristics of targets, including faces, human bodies, motor vehicles, and non-motor vehicles.
5	Channel display and layout	• is used to switch the channel display. • is used to modify the content shown in the display.
6	Channel switching and broadcasting	• Click to start tour and click to pause or proceed with tour. • Click to enable the voice broadcast function. • Click to switch channels to display on the main or secondary screen.
7	PTZ settings	Adjust the PTZ settings of devices. For details, see "4.5 PTZ".

View

1. Click to edit the view layout.
2. Click to add the custom layout and change the layout.

   You can drag the channel to the live view by long-pressing the left mouse button.
3. Click to delete the view layout.

Channel Display and Layout

- : Go to or go back to the layout page.
- : Switch the default view layout scheme, supporting 1, 4, 8, 9, 16, 25 and 36 splits.
- : Display the live view of channels in full screen. Right-click to select **Exit Full Screen** to exit the full screen.
- : Enable **AI Display** , including **AI Rule** and **AI Area**.
- : Enable **AI Live**, and the AI live results are displayed on the right side of the live page.

  Click to modify the channel, panel style and attribute settings.

Figure 4-2 AI live view

Figure 4-3 AI display settings

4.3 Live View Control Bar

Point to the top center of the video of current channel; and then the live view control bar appears.

If your mouse stays in this area for more than 6 seconds and has no operation, the control bar automatically hides.

- Disable the navigation bar before using this function.
- The live view control bar is different depending on the model.

Figure 4-4 Live view control bar

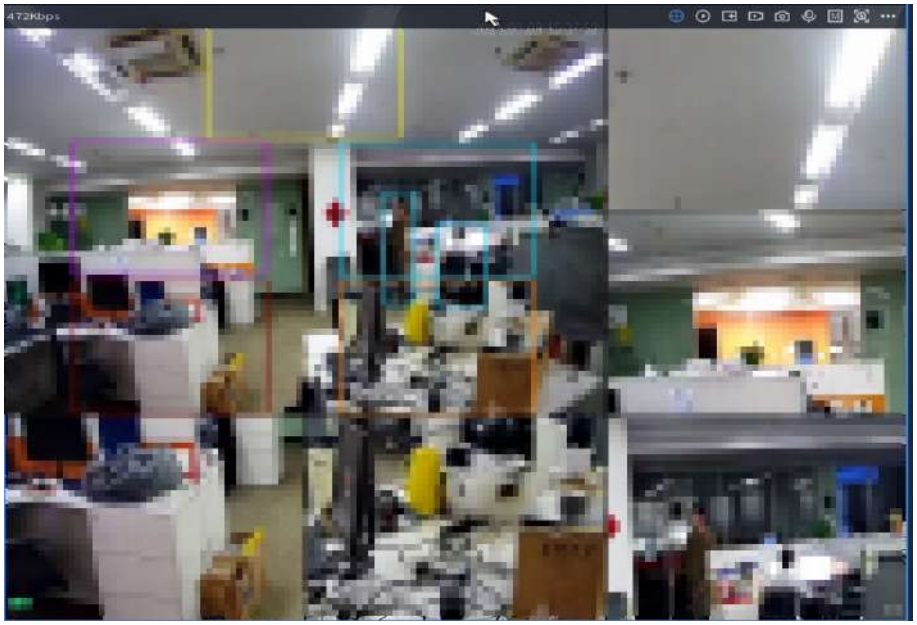


Table 4-2 Live view control bar description

Icon	Name
	EPTZ function. For details, see "4.5.4 EPTZ".

Icon	Name
	Instant playback. You can play recordings from the previous 5 seconds to 60 minutes of the current channel. • Move the slider to choose the time you want to start playing. • You can start, pause and close playback. • The information such as channel name and recording status icon are shielded during instant playback and will not display until you exit playback. • During playback, screen split layout switch is not allowed. • Tour has high higher priority than the instant playback. The instant playback function is not available when tour function is in process and the live view control bar automatically hides either. The function becomes available again after tour ends. • Supports AcuPick. For more details, see "5.1.2 AcuPick". Go to the **Main Menu** > **SETTINGS** > **SYSTEM** > **General** > **Basic** to set instant playback time.
	Digital zoom. Click to select an area. The area is enlarged after you release the mouse button. For some models, when the image is enlarged in this way, the selected area is zoomed proportionally according to the window. When the image is in the enlarged status, you can drag the image toward any direction to view the other enlarged areas. Right-click to cancel zoom and go back to the original video image.

Icon	Name
	Instant record. You can record the video of any channel and save the clip to a USB storage device. Click to start the recording. To stop recording, click this icon again. The clip is automatically saved to the connected USB storage device. Make sure that the backup device is connected to the NVR.
	Manual snapshot. You can take one to five snapshots of the video and save to a USB storage device. Click to take snapshots. The snapshots are automatically saved to the connected USB storage device. You can view the snapshots on your computer. To change the quantity of snapshots, select **Main Menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Encode** > **Snapshot**. In the **Manual Snapshot** drop-down list, select the snapshot quantity.
	Talk. You can perform the voice interaction between the NVR and the remote device to improve efficiency of emergency.
	Switch stream. Click to switch the bit stream type of the main stream and sub stream according to current network bandwidth. • M (main stream): Its bit streams are big and definition is high. It occupies large network bandwidth suitable for video wall surveillance, storage and more. • S (sub stream): Its definition is low but occupies small network bandwidth. It is suitable for general surveillance, remote connection and more. Some models support two sub streams (S1, S2).

Icon	Name
	AcuPick function. Make sure that you have set the mode as **AcuPick**. For details, see "6.1.2 Mode Setting". 1. When you want to search the target in the image, click to freeze the live view. The image automatically shows the targets. If the target is not selected by the device, you can also draw an area to search the target. • **Search by Area** : Conduct a search and display search results for all targets within the area based on the drawing area. • **Search by Target** : Conduct a search and display search results for all targets based on the targets within the drawing area. Right-click to exit this page. 2. Point to the target you want, and then click to check the details.
	Click to view the other functions, such as smart tracking and fisheye. • For smart tracking, see "4.8 Smart Tracking". • For fisheye, see "4.6 Fisheye De-Warp on Live View".

4.4 Shortcut Menu

Right-click the live view page to bring up the shortcut menu. You can go to main menu, play back videos or images, configure view split, and configure the settings of PTZ, image, and more.

The shortcut menu is different for different models, please refer to the actual page.

Figure 4-5 Shortcut menu

Table 4-3 Shortcut menu description

Function	Description
Full Screen	Display the live view of channels in full screen. Right-click the mouse to select **Exit Full Screen** to exit the full screen.
Main Menu	Go to main menu.
Playback	Go to the playback page.
Default View	Configure the live view screen as a single-channel layout or multi-channel layout. Click to switch view layouts, supporting the selection of view 1, 4, 8, 9, 16, 25, and 36.
Manual Control	• **Record Mode** : You can configure the recording mode as **Auto** or **Manual**, or stop the recording. You can also enable or disable snapshot function • **Alarm Mode** : You can configure alarm output settings.
Image	Click to modify the camera image parameters. For details, see "3.6.1 Image".

4.5 PTZ

PTZ is a mechanical platform that carries a camera and a protective cover and performs overall control remotely. A PTZ can move in both horizontal and vertical direction to provide all-around view to the camera.

Before you control the PTZ, make sure the PTZ decoder and the NVR network connection is OK.

4.5.1 PTZ Settings

Background Information

You can set different PTZ parameters for local type and remote type. Before you use local PTZ, make sure you have set PTZ protocol; otherwise you cannot control the local PTZ.

- Local: The PTZ device connects to the NVR through the cable.
- Remote: The PTZ device connects to the NVR through the network.

This function is available on select models.

Procedure

Step 1 Select **Main menu** > **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **PTZ**.

Figure 4-6 PTZ (local)

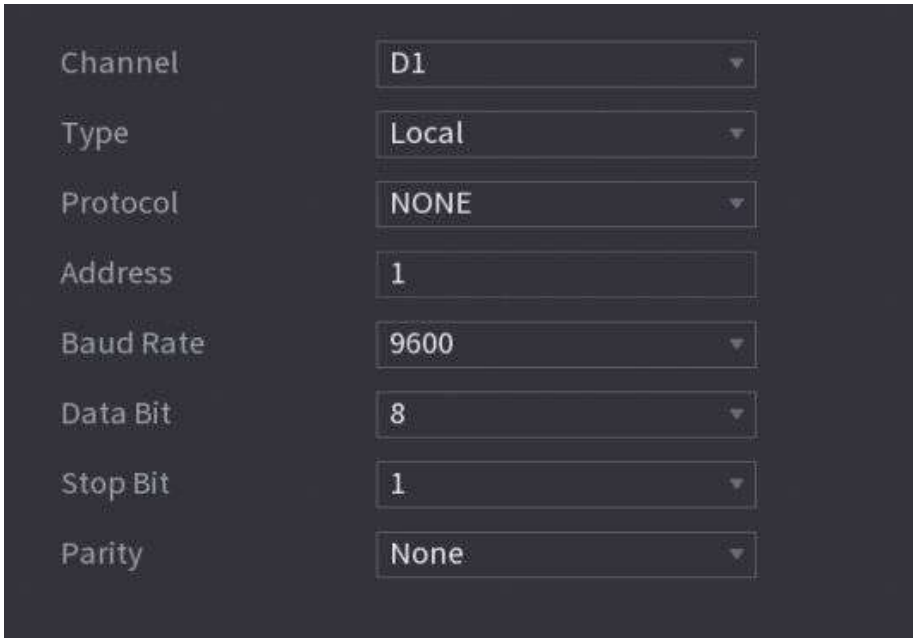
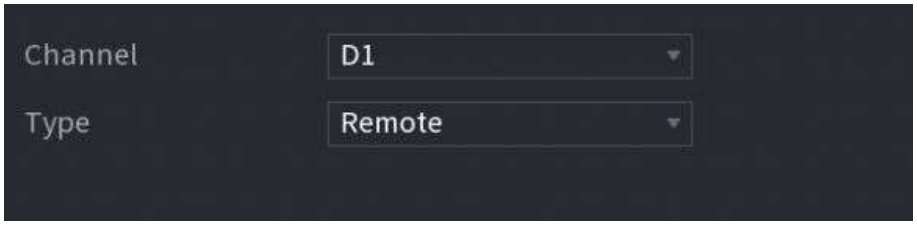


Figure 4-7 PTZ (remote)



Step 2 Configure parameters.

Table 4-4 PTZ parameters

Parameter	Description
Channel	Select the channel that you want to connect the PTZ camera to.
Type	• Local: Connect through RS-485 port. • Remote: Connect through network by adding IP address of PTZ camera to the Device.
Protocol	Select the protocol for the PTZ camera such as PELCOD.
Address	Enter the address for PTZ camera. The default is 1. The entered address must be the same with the address configured on the PTZ camera; otherwise the system cannot control PTZ camera.
Baud rate	Select the baud rate for the PTZ camera. The default is 9600.
Data bit	The default value is 8.
Stop bit	The default value is 1.
Parity	The default value is **None**.

Step 3 Click **Apply**.

4.5.2 PTZ Control

You can use the PTZ control panel to perform the operations such as directing camera in eight directions, adjusting zoom, focus and iris settings, and quick positioning.

Basic PTZ Control Panel

Right-click the live view, and then select **PTZ Control**.

Figure 4-8 PTZ control panel

- The gray button means system does not support current function.
- For some model, the PTZ function is available only in one-window mode.

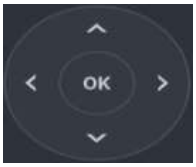
Table 4-5 PTZ control parameters

Function	Description
	Use the arrow keys to adjust the direction of the PTZ control. The PTZ control supports 8 directions, including up, down, left, right, upper left, upper right, lower left, and lower right. Click , and in the live view page, select the area; the PTZ will quickly rotate and zoom to position the specified area.
	Measure the rotation stride; the larger the value, the greater the rotation stride. For example, a step length of 8 results in a significantly larger rotation stride than a step length of 1.

Function	Description
	Zoom, adjusting the magnification of the image.
	Zoom, adjusting the camera's focus level.
	Aperture, adjusting the size of the aperture in the image.
	PTZ menu. Click this icon to enter the PTZ menu.
	Auto focus: Click this icon for the device to perform auto focus.
	Gesture control: Click this icon to control the PTZ movement using gestures in front of the lens.
	Reset: Restore the PTZ settings to default.
	Preset.
	Tour group.
	Pattern.
	Scan.
	 Different devices might display different functions; please refer to the actual page. Click to view more functions of the PTZ control. • Click , and the device rotates continuously 360° horizontally at a certain speed. • Click , and the device rotates horizontally 180 degrees • Click , and the device enables the wiper function. • Click , and the device enables the light function. • Set the auxiliary number and enable the function. The auxiliary number corresponds to the auxiliary switch on the decoder, and once activated, the PTZ can be controlled through the decoder.

Configure the PTZ menu

Click to enter the PTZ menu in the live view page.

Click the directional keys of 

and **OK** to select and enter the menu.

4.5.3 Configuring PTZ Functions

4.5.3.1 Configuring Presets

Click to view the presets.

- Click and the image moves to the preset position.
- Double-click on a blank preset to set the preset name, then click to save the current preset.
- Click to delete the preset.

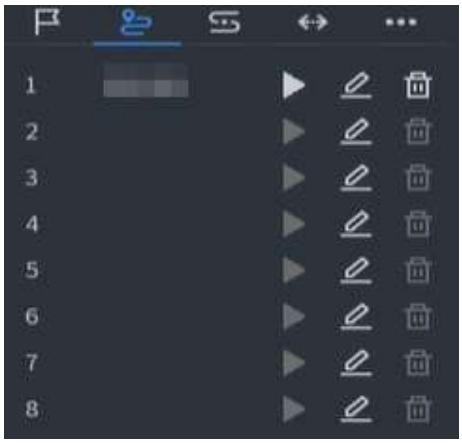
4.5.3.2 Configuring Tour Group

The number of tour groups is determined by the currently connected front-end devices.

Click to view the tour group.

- Click and the image starts to follow the path according to the presets added in the tour group.
- Double-click the blank tour group to configure the name of the tour group.
  1. Click to enter the tour group configuration.
  2. Click **Add Preset** and click the drop-down box for the preset name and select a preset.
  3. Configure the staying time and movement speed.
  4. Click **OK**.
- Click to delete the presets.

Figure 4-10 View the tour group



4.5.3.3 Configuring Patterns

The number of pattern routes is determined by the currently connected front-end devices.

1. Click to view the pattern routes.
   - Click and the image starts to follow the route set for the pattern.

- Double-click the blank pattern to configure the name. Click to use the PTZ direction control keys to control its movement, and after completing the target route movement, click to save the route.
- Click to delete the presets.

4.5.3.4 Configuring Scan

The number of scan routes is determined by the currently connected front-end devices.

Click to view the scan routes.

- Click and the image is set to start scanning along a linear scanning route.
- Double-click the blank scan to set the scan name. Click to use the PTZ direction control keys to control its movement, and after completing the target route movement, click to save the route.
- Click to delete the presets.

4.5.4 EPTZ

4.5.4.1 Configuring EPTZ Linkage

Turn on the EPTZ linkage function on the live page. This function can simultaneously zoom in and track multiple humans and vehicles that trigger alarms. It provides rich details and a panoramic view at the same time.

Prerequisites

AI events have been configured.

Background Information

- The EPTZ is not displayed for more than 4 splits, while it is shown for 4 splits or fewer.
- When you switch between screen splits, live view layouts, or channel sequences, you will exit the EPTZ live view mode. If you right-click to access the main menu, playback, or other functions, exiting those will return them to the EPTZ live view mode.
- The camera side does not support enabling, disabling, or configuring EPTZ linkage operations.

Procedure

Step 1 Select the channel in the live view page, and click in the live view control bar to enable the local EPTZ live view mode.

Step 2 Configure the parameters.

Figure 4-11 EPTZ linkage

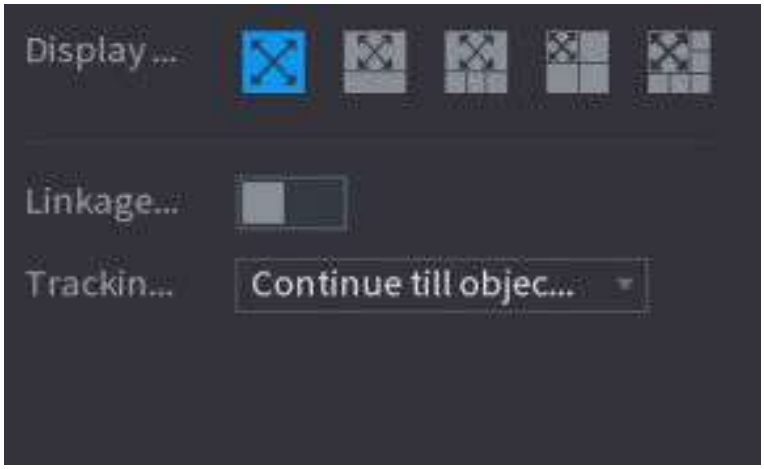


Table 4-6 Parameters description

Parameter	Description
Display Mode	Select the number of tracked channels. Full screen, 1+1, 1+3 and 1+5 modes are available, and full screen is selected by default.
Linkage Track	After **Linkage Track** is enabled, intelligent events will be tracked. It is disabled by default.
Tracking Duration	• Custom: Select the tracking duration time manually. For example, if you set from 30 seconds to 60 seconds, after tracking object A for 30 seconds, if object B appears, the camera will start tracking object B; if no other object appears in the process of tracking A, the camera will stop tracking object A after 60 seconds. • Continue till object disappears: The camera will stop tracking when the detected object disappears in the image.

Step 3 Click **Apply**.

Related Operations

When an intelligent event is triggered, the live page will display the linkage track effect.

Check the EPTZ linkage in the live view.

Right-click the live view, and then select **EPTZ**. Enable EPTZ linkage function, and then you can view local EPTZ live videos.

Figure 4-12 EPTZ live view

4.5.4.2 EPTZ Live View

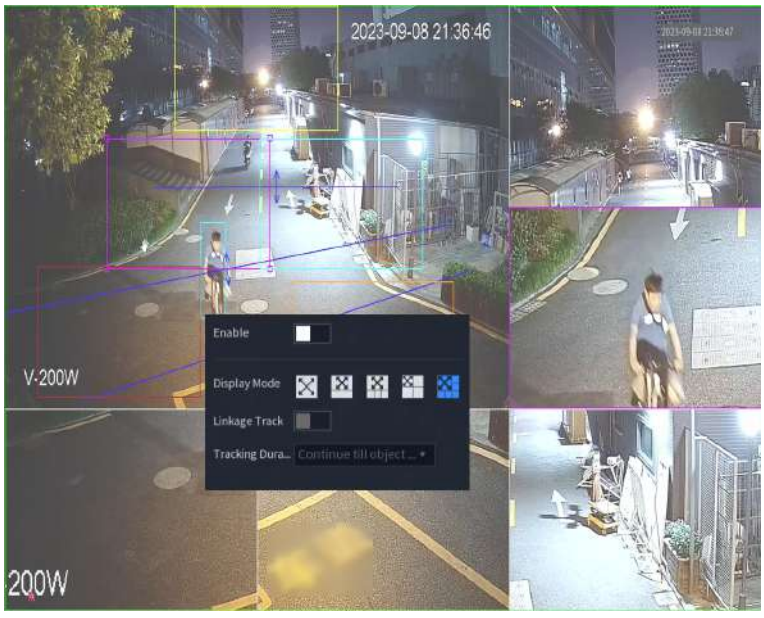
Some models can directly turn on the EPTZ linkage function in the live view.

Right-click the live page, and then configure EPTZ linkages parameters. For details, see "4.5.4.1 Configuring EPTZ Linkage".

According to the EPTZ configuration of the corresponding channel, you can see split image and tracking display effects.

When switching to splitting, live view layout or channel order, the device automatically exits the EPTZ live view mode. When switching to main menu or playback page, the device exits that page, and then returns to EPTZ live view mode.

Figure 4-13 EPTZ live view



4.6 Fisheye De-Warp on Live View

This function is only available on select models.

The fisheye camera (panoramic camera) has wide video of angle but its video is seriously distorted. The de-warp function can present the proper and vivid video suitable for human eyes.

On the live view, right-click the fisheye channel, and then select **Fisheye**. You can set fisheye installation mode and display mode.

- For the non-fish eye channel, the system prompts you it is not a fisheye channel and does not support de-warp function.
- If system resources are insufficient, the system prompts you the de-warp function is not available.

There are three installation modes: Ceiling mount, wall mount, and ground mount.

- The different installations modes have different de-warp modes.
- Some models support de-warp of 180° fisheye camera. The 180° fisheye camera supports de-warp in wall mount mode only.

Figure 4-14 Fisheye settings

Table 4-7 Installation mode

Installation mode	Icon	Description
(Ceiling mount)		360° panorama original view
(Ground mount)		1 de-warp window+1 panorama stretching

Installation mode	Icon	Description
		2 panorama stretching views
		1 360° panorama view+3 de-warp windows
		1 360° panorama view+4 de-warp windows
		6 de-warp windows+1 panorama stretching
		1 360° panorama view+8 de-warp windows
(Wall mount)		360° panorama original view
		Panorama stretching
		1 panorama unfolding view+3 de-warp windows
		1 panorama unfolding view +4 de-warp windows
		1 panorama unfolding view +8 de-warp windows

Figure 4-15 De-warp

You can adjust the color pane on the left pane or use your mouse to change the position of the small images on the right pane to realize fish eye de-warp.

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

4.7 Shortcut Menu to Modify Camera

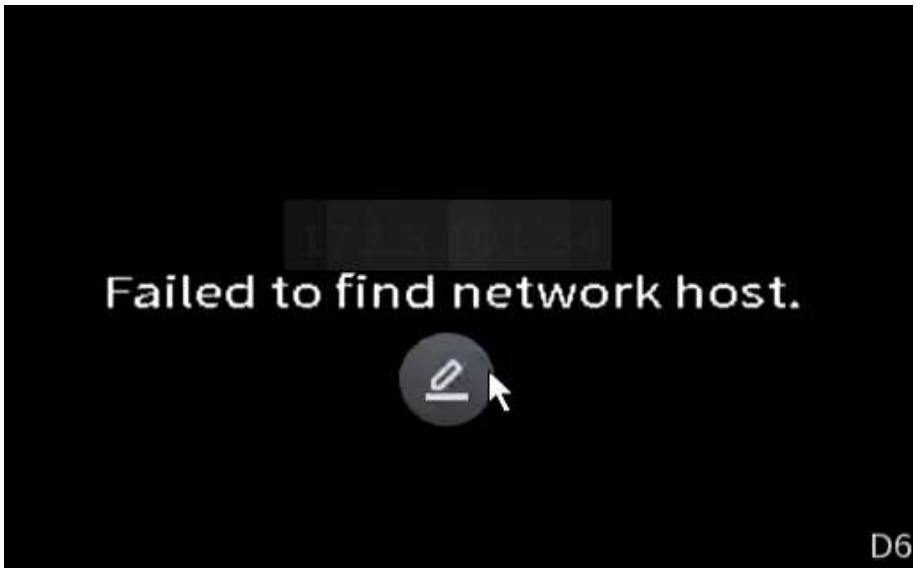
You can modify abnormal cameras on the live view.

Procedure

Step 1 On the live view, point to a channel window that prompts **Failed to find network host**.

There is an icon on the channel window.

Figure 4-16 Modify icon



Step 2 Click the icon, and then configure the parameters to add the remote device. For details, see "3.3 Adding Remote Devices".

4.8 Smart Tracking

Track targets manually or automatically. This function is only available on the multi-sensor panoramic camera and PTZ camera.

Background Information

Make sure that the linked tracking function has been enabled.

Procedure

Step 1 In the live view page, click ··· at the upper-right corner of the video image and select **Smart Tracking**.

Step 2 Select the tracking method.

- Manual positioning: Click a spot or select a zone on the bullet camera video, and then the PTZ camera will automatically rotates there and zoom in.
- Manual tracking: Click or select a target on the bullet camera video, and then the PTZ camera automatically rotates and tracks it.
- Automatic tracking: The tracking action is automatically triggered by tripwire or intrusion alarms according to the pre-defined rules.

5 Playback

5.1 General Video

Log in to the main menu, select **PLAYBACK** or right-click the mouse in the live view page to select **Playback**, and then click to enter the playback page of general video.

Figure 5-1 General video

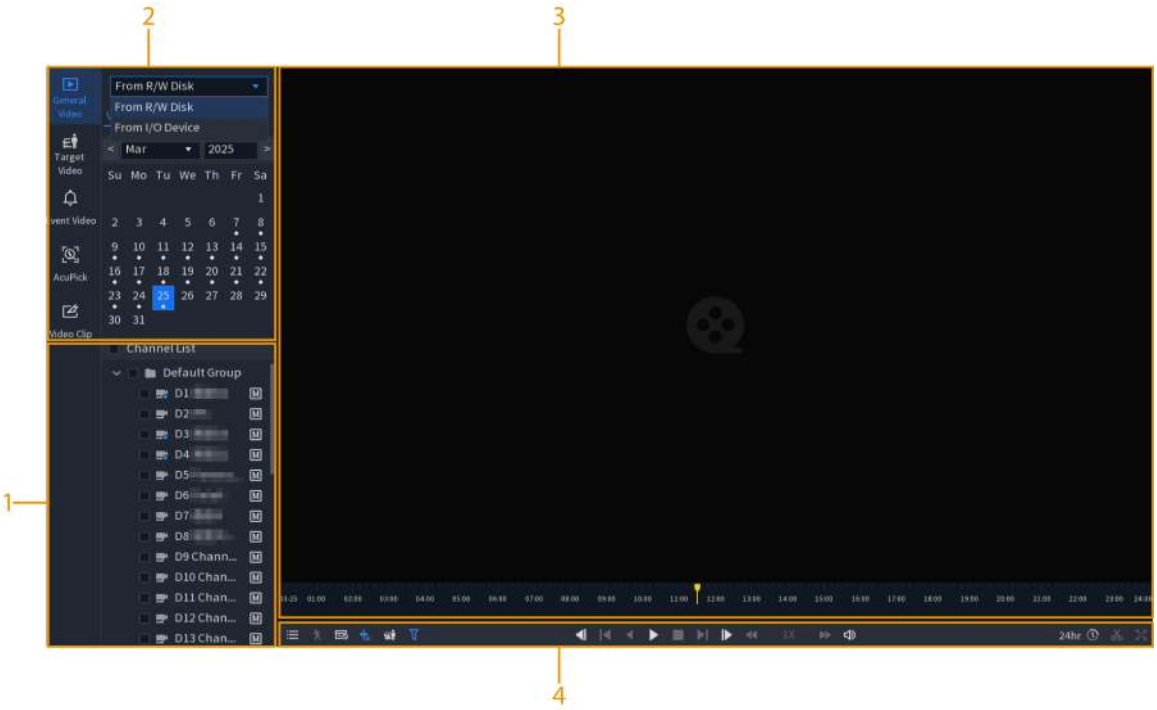


Table 5-1 Description of the general video page

No.	Name	Description
1	Channel list	Displays device tree groups based on device grouping, and shows the playback according to the selected devices when viewing playback. The maximum number of playback channels is limited to 16.
2	Playback source and date	Select the playback source and date, supporting the selection of **From R/W Disk** and **From I/O Device**.
3	Display window	Channel playback shows the type of video or image and the corresponding time period under the current conditions.
4	Playback control bar	Use the function buttons to filter, control, and edit the playback videos. For details, see "Playback control description".

Display Window

- Click to zoom in on a specific area of the screen to view the details of that region.

  The system supports dragging in any direction to view the enlarged image of other areas on the screen. When in the zoomed-in state, right-click to cancel the zoom effect and restore the original image.
- Click to manually capture 1 to 5 images, and the captured images will be stored on the external storage device.

  In the main menu page, select **SETTINGS** > **REMOTE DEVICE** > **Camera Settings** > **Encode** > **Snapshot** to set the number of images to capture in a single manual snapshot.
- Click to add tags for playback. For details, see "5.1.5 Tag Playback".
- Click to configure the EPTZ. For details, see "5.1.6 EPTZ Linkage".
- Click to set the fisheye dewarping. For details, see "5.1.7 Fisheye De-Warp during Playback".
- Click anywhere on the colored area of the timeline to start playback from that point in time.
- When you change the playback mode or select the recording channel, the timeline will update synchronously.
- Scrolling the mouse will zoom in on the timeline within the nearest range of the current playback time.
- Some device models support automatic jumping to the next recorded timestamp for playback when clicking on a blank area of the timeline.
- On the playback timeline, holding down the left mouse button allows you to drag the timeline, changing the mouse cursor to a hand grab icon, and the playback interface will display frames corresponding to the timeline.
- Thumbnail display: When playing a single channel normally, moving the mouse over the timeline will show a thumbnail of the clicked moment along with the four previous and next frames.
- It supports dragging the vertical line on the timeline (I-frame hover); during playback, holding down the (orange) vertical line on the timeline allows for quick browsing of playback (fast jumping playback according to I-frames).

Playback Control

Figure 5-2 Playback control

Table 5-2 Playback control description

Icon	Function
	You can view the file list to display the queried recording files, and perform locking or unlocking operations on the files.
	Smart search. See "5.1.1 Smart Search" for detailed information.
	Display and hide POS information. In 1-channel playback mode, you can click it to display/hide POS information on the video.

Icon	Function
	In 1-channel playback mode, click it to enable or disable display IVS rule information on the video. This function is for some series only.
	Smart motion detection. You can click the icon to select a human, motor vehicle or animal, and the system plays detected videos of the person or motor vehicle. Human and motor vehicle can be selected at the same time.
	Select the recording type. Supports filtering by normal, alarm, motion detection, smart, and POS.
	Play/Pause In slow play mode, click it to switch between play/pause.
	Stop When playing back, click to stop current playback process.
	Rewind In normal play mode, left-click the button, the file begins to rewind. Click it again to pause it. While it is rewinding, click or to restore normal play.
	Display previous frame/next frame. When you pause the normal playback file, click or to play back frame by frame. In frame by frame playback mode, click or to resume normal playback mode.
	Slow play In playback mode, click it to use various slow play modes such as slow play 1, slow play 2, and more.
	Fast forward In playback mode, click to realize various fast play modes such as fast play 1,fast play 2 and more.
	Adjust the volume of the playback.
	View playback by time range, with options for 24 hours, 2 hours, 1 hour, 30 minutes, and 5 minutes.
	Configure the video clip and save it. For details ,see Video Clip.

Icon	Function
	View the videos in full screen.

5.1.1 Smart Search

During the playback process, the system can analyze the motion detection zone in the scene and give the analysis result.

Prerequisites

Smart search is only available in channels that have the motion detection function enabled. In the main menu page, select **APPLICATIONS** > **Event Center** > **Event Subscription** and enable the motion detection function for the corresponding channel.

Procedure

Step 1 Log in to the main menu, select **PLAYBACK** and select the date and time.

Step 2 Click and drag the left mouse button to enable the smart search function.

- This function is for one-channel playback mode.
- In multiple-channel playback mode, double-click a channel to switch to one-channel playback mode.

Step 3 Click to enter the smart search playback page.

The page will display the video with dynamic image within the detected area.

Step 4 Click to exit the smart search.

- The motion detection region cannot be the full screen zone.
- The motion detection region adopts the current whole play pane by default.
- The time bar unit switch, rewinding, frame by frame are not available when the system is playing a motion detection file.

5.1.2 AcuPick

During video playback, conduct AcuPick for detected targets to view the locations and time of their appearances.

Prerequisites

AcuPick is only available in AcuPick mode. For switching the search mode, see "6.1.2 Mode Setting".

Both single-screen playback and multi-screen playback support precise searching. The following section will introduce the process using single-screen playback as an example.

Procedure

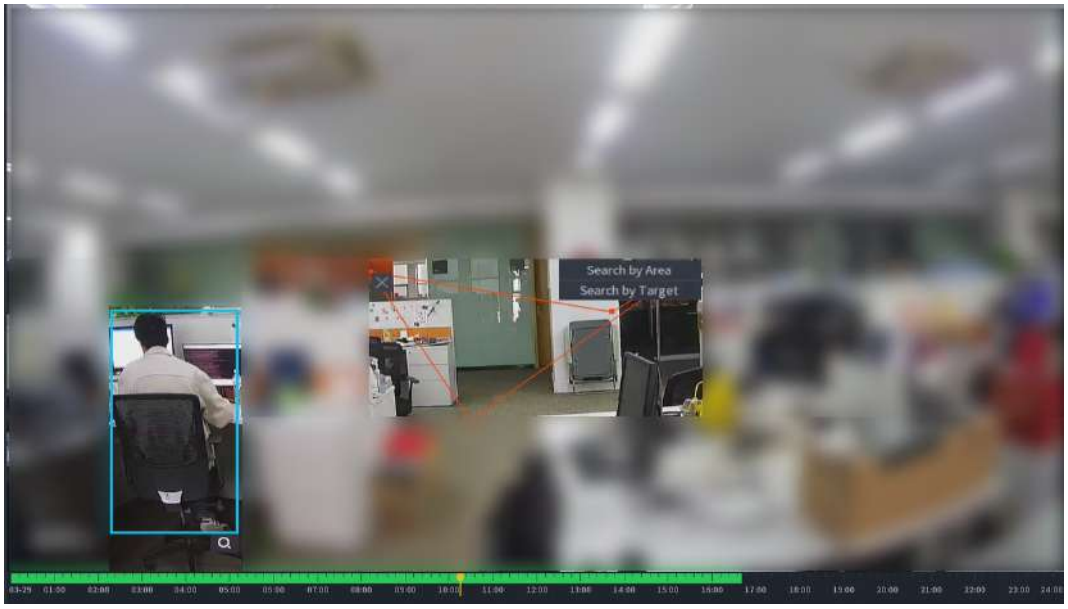
Step 1 In the main menu, select **APPLICATIONS** > **PLAYBACK** or select **Playback** in the live view page, and click to enter the general video playback page.

Step 2 Select the channel and click to play the video.

The timeline displays in green for periods where there is recorded footage.

Step 3 Click to freeze the image and the targets will be selected by the box in the image.

Figure 5-3 AcuPick

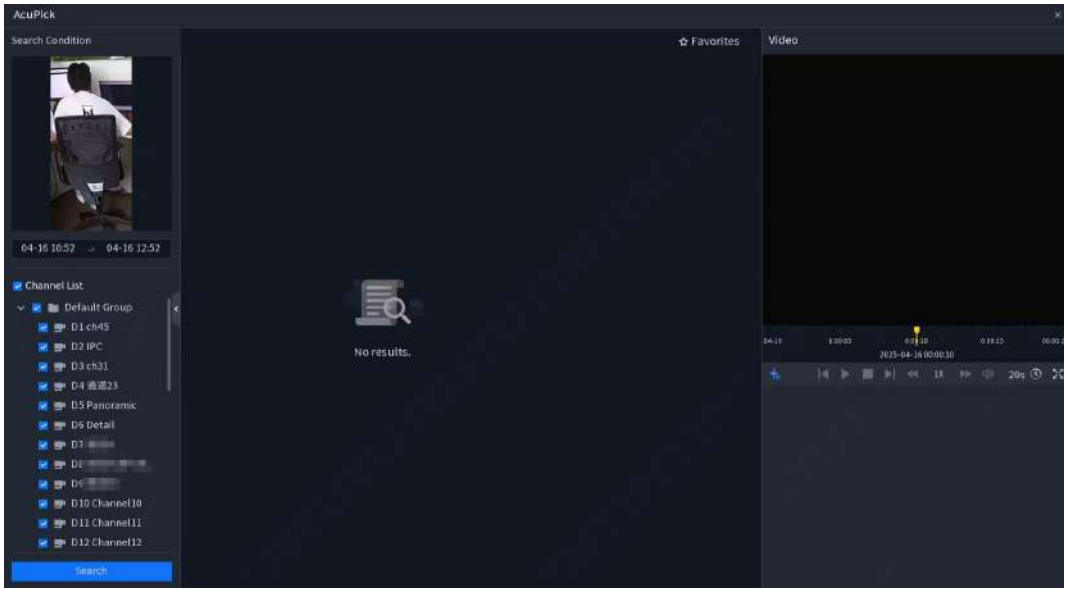


- Hover over the target box and click to perform the AcuPick function. Set the search criteria such as channel and time period, then click **Search**, and the query results will be displayed on the right side of the page.
- To define the search area, click the left mouse to draw the region, then right-click to select the search method.
  - ◇ Search by Area: Searches based on the drawn area and displays search results for all targets within that area.
  - ◇ Search by Target: Searches based on the targets selected within the drawn area and displays all search results for those targets.

Step 4 In the search result page:

- Hover over a search result and click to bookmark that result.
- Hover over a search result and click to hide that result.
- Select a search result and click to choose the file path and associated event recordings on the file backup page.
- Click to sort the search results.

Figure 5-4 Search results



Step 5 Double-click on the search results to automatically play the video recordings before and after the event report on the right side page.

5.1.3 Region of Interest

Procedure

Step 1 In the main menu, select **APPLICATIONS** > **PLAYBACK** or select **Playback** in the live view page, and click to enter the general video playback page.

Step 2 Select the channel and click to play the video.

The timeline displays in green for periods where there is recorded footage.

Step 3 Click to select the target, which supports choosing human, motor vehicle and animal.

The timeline displays in blue for periods where there is recorded footage.

Step 4 Configure the rule of region of interest.

Area drawing supports lines and irregular shapes. The time frame during which a target appears within that area is displayed in orange on the timeline. If the target appears in the recorded footage during that period, a list of target images will be displayed on the left-side page.

Related Operations

Hover the mouse over the image.

- Click to select the AcuPick target.
- Click to save the target image to an external storage device.

5.1.4 Video Clip

Extract the video footage from a specific time period in the recording file and save it to a USB device.

Procedure

Step 1 Log in to the main menu, select **PLAYBACK** or right-click the mouse in the live view page to select **Playback**, and then click to enter the playback page of general video.

Step 2 Select the playback window where the video needs to be edited.

Step 3 Enter the start and end times of the clip to be edited in 00:00:00 - 23:59:59.

Step 4 Click .

You can back the video clip up in the pop-up window.

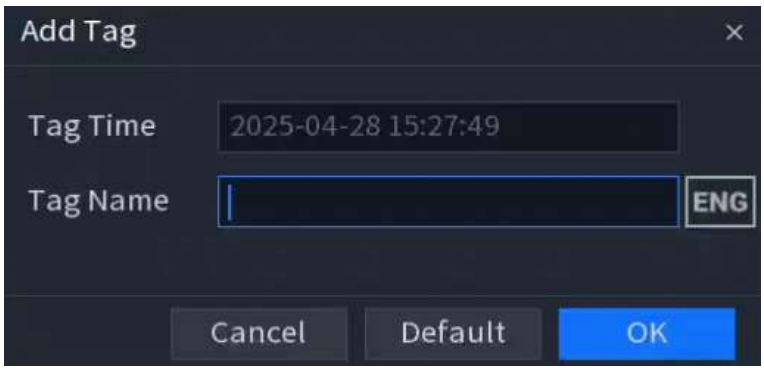
5.1.5 Tag Playback

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

Adding Tag

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

Figure 5-5 Configure the tag name



Playing back Tag

In the main menu, select **BACKUP** > **Tag** and click **Search**. On the tag list, double-click a file to play back.

To search for tagged videos by time, select the tag time and then click **Search**.

5.1.6 EPTZ Linkage

Turn on the EPTZ linkage function on the playback page. This function can simultaneously zoom in and track multiple humans and vehicles that trigger alarms. It provides rich details and a panoramic view at the same time.

Background Information

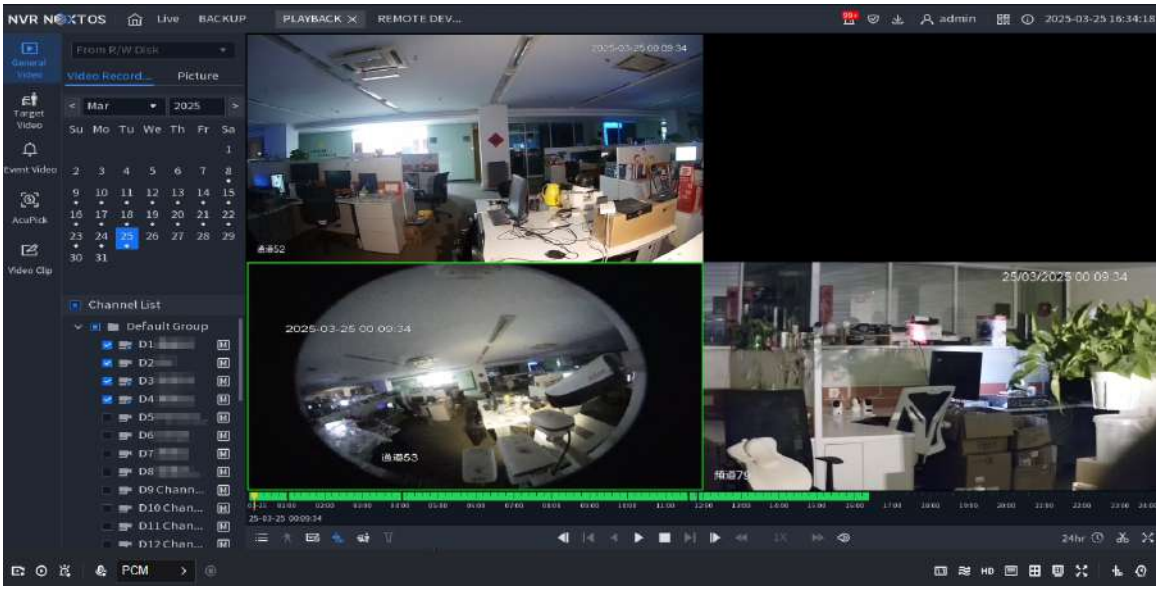
- Only supports the EPTZ linkage function in single channel and 4-channels playback modes.
- When selecting the 4-channels playback mode, only the EPTZ linkage function of one channel can be turned on at the same time.

Procedure

Step 1 Select **Main Menu** > **APPLICATIONS** > **PLAYBACK**, or right-click on the live view page and then select **Playback**.

Step 2 Select one channel, and then click .

Figure 5-6 EPTZ linkage for playback



Step 3 Turn on the EPTZ linkage function, and then configure parameters.

If a certain channel has turned on the EPTZ linkage function, the configuration will still take effect after exiting playback. When replaying the recording of this channel again, the EPTZ linkage effect is still displayed.

Figure 5-7 Setting the EPTZ linkage for playback

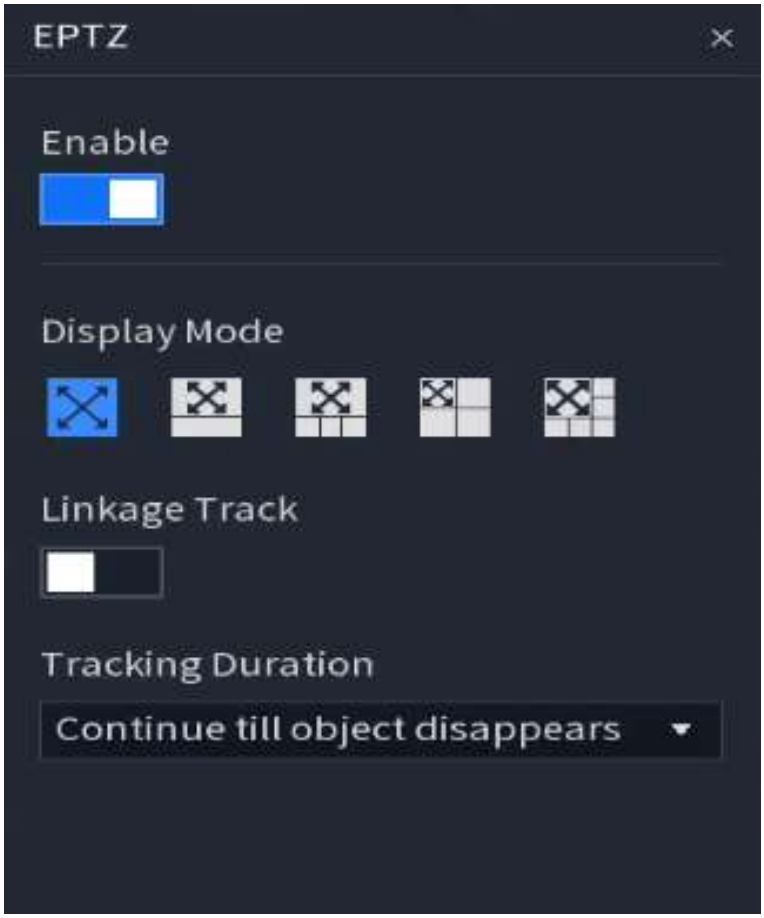


Table 5-3 Parameters description

Parameter	Description
Display Mode	Select the number of tracked channels. Full screen, 1+1, 1+3 and 1+5 modes are available, and full screen is selected by default.
Linkage Track	After **Linkage Track** is enabled, intelligent events will be tracked. It is disabled by default.
Tracking Duration	• Custom: Select the tracking duration time manually. For example, if you set from 30 seconds to 60 seconds, after tracking object A for 30 seconds, if object B appears, the camera will start tracking object B; if no other object appears in the process of tracking A, the camera will stop tracking object A after 60 seconds. • Continue till object disappears: The camera will stop tracking when the detected object disappears in the image.

Related Operations

When an intelligent event is triggered, the playback page will display the linkage track effect.

5.1.7 Fisheye De-Warp during Playback

When playing back the fisheye record file, you can use de-warp function to adjust video.

Prerequisites

This function is only available in AI mode. For switching the mode, see "6.1.2 Mode Setting". But for 5-EI NVR series, the fisheye function conflicts with the AI mode.

Procedure

Step 1 On the main menu, select **APPLICATIONS** > **PLAYBACK** > **General Video** or you can right-click the mouse to select **Playback** in the live view page.

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

Step 3 Right-click at the upper-right corner of the video image, and then you can go to the de-warp playback page. For detailed information, see "Installation mode" and "4.6 Fisheye De-Warp on Live View".

5.2 Target Video

Log in to the main menu, select **PLAYBACK** or right-click **Playback** in the live view page to enter the playback page. Click to enter the target video page.

Figure 5-8 Target video

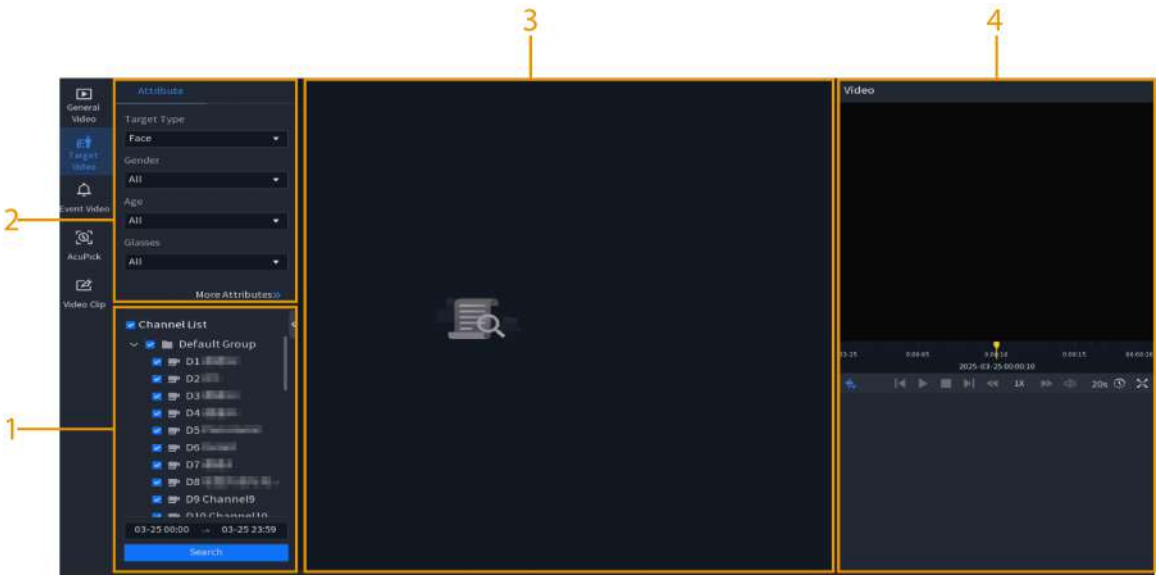


Table 5-4 Description of the target video page

No.	Name	Description
1	Channel list	Shows the device tree structure based on device grouping, and display the results according to the selected devices.

No.	Name	Description
2	Search method	• Search by attribute: Set the parameters for the search target and search the target based on the attributes. ◇ The similarity should be at least 50%. ◇ Multiple images can be uploaded. ◇ When using local upload, a storage device, such as a USB drive, must be connected in advance. ◇ Click to remove the uploaded images. • Search by picture: Click the **Picture** tab and upload images from the backup device or from the face database and set the similarity for retrieving the target.
3	Search result	The search result page allows for batch operations on the results.
4	Playback control	For details, see "Playback control description".

Search Result

- Export: select the results and click **Export** or below each image to export the images to the external storage device.
- Lock: select the results and click **Lock** or below each image to lock the results.
- Add tag: select the results and click **Add Tag** or below each image to add the tag for each image.
- Delete: select the results and click **Add Tag** or below each image to delete the result.

5.3 Event Video

Log in to the main menu, select **PLAYBACK** or right-click **Playback** in the live view page to enter the playback page. Click to enter the target video page.

Figure 5-9 Event video

Table 5-5 Description of the event video page

No.	Name	Description
1	Channel list	Shows the device tree structure based on device grouping, and display the results according to the selected devices.
2	Search method	Configure event types and target types, which are usually intelligent events.
3	Search result	The search result page allows for batch operations on the results.
4	Playback control	For details, see "Playback control description".

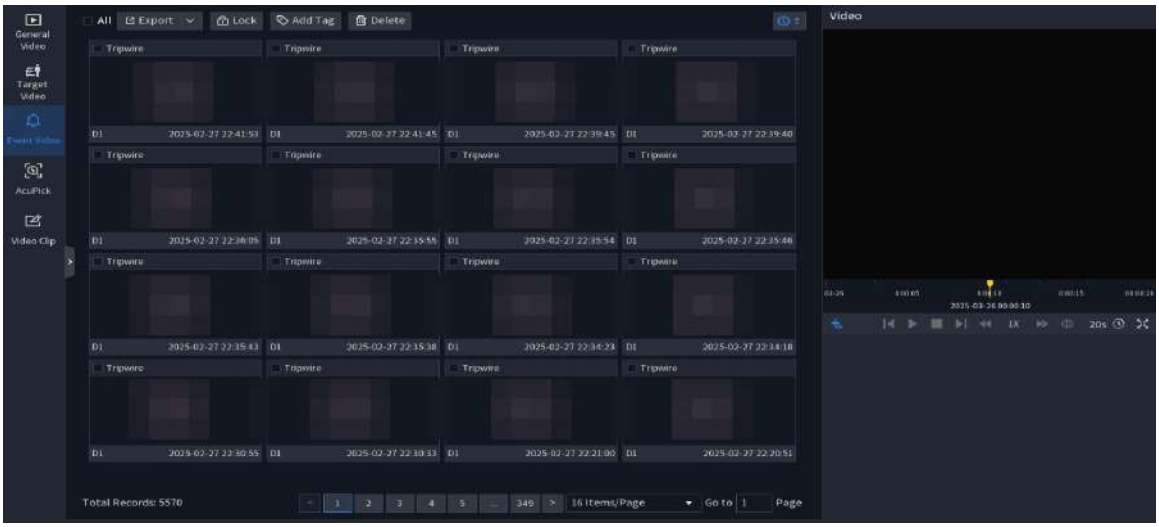
Search Method

1. Configure event types and target types.
2. Select channels in the channel list.
3. Click the time period and select the specific query time.
4. Click **Search**.

Search Results

- Export: select the results and click **Export** or below each image to export the images to the external storage device.
- Lock: select the results and click **Lock** or below each image to lock the results.
- Add tag: select the results and click **Add Tag** or below each image to add the tag for each image.
- Delete: select the results and click **Add Tag** or below each image to delete the result.
- Click under the image, select material, and then click **Next** to import it to the experience database to enable the target analysis.

Figure 5-10 Search result



5.4 Video Clip

Log in to the main menu, select **PLAYBACK** or right-click **Playback** in the live view page to enter the playback page. Click to enter the target video page.

Figure 5-11 Video clip

Table 5-6 Description of the target video page

No.	Name	Description
1	Calendar	Select the date.
2	Channel list	Shows the device tree structure based on device grouping, and display the results according to the selected devices.
3	Search result	The search result page allows for batch operations on the results.
4	Playback control	For details, see "Playback control description".

Search Result

1. Select the channel.
2. Select the date.

- Click below the video and select **4 Clips** to split the current video into 4 segments.
- Click below the video to split the current video into 60 segments.

- The channel video segment results are displayed in one-hour intervals by default, and periods without video are not shown as segments.
- When you perform a secondary video segmentation, for videos with a duration of less than one hour, the number of segments will be based on the actual recording duration.

6 Events

View and modify the intelligent functions and alarm settings of local and remote devices, and create a comparison database for the local device.

6.1 Local Events

Log in to the main menu, select **SETTINGS** > **EVENT**. In **Device List** , click **NVR**.

Figure 6-1 Local events

6.1.1 AI Function Overview

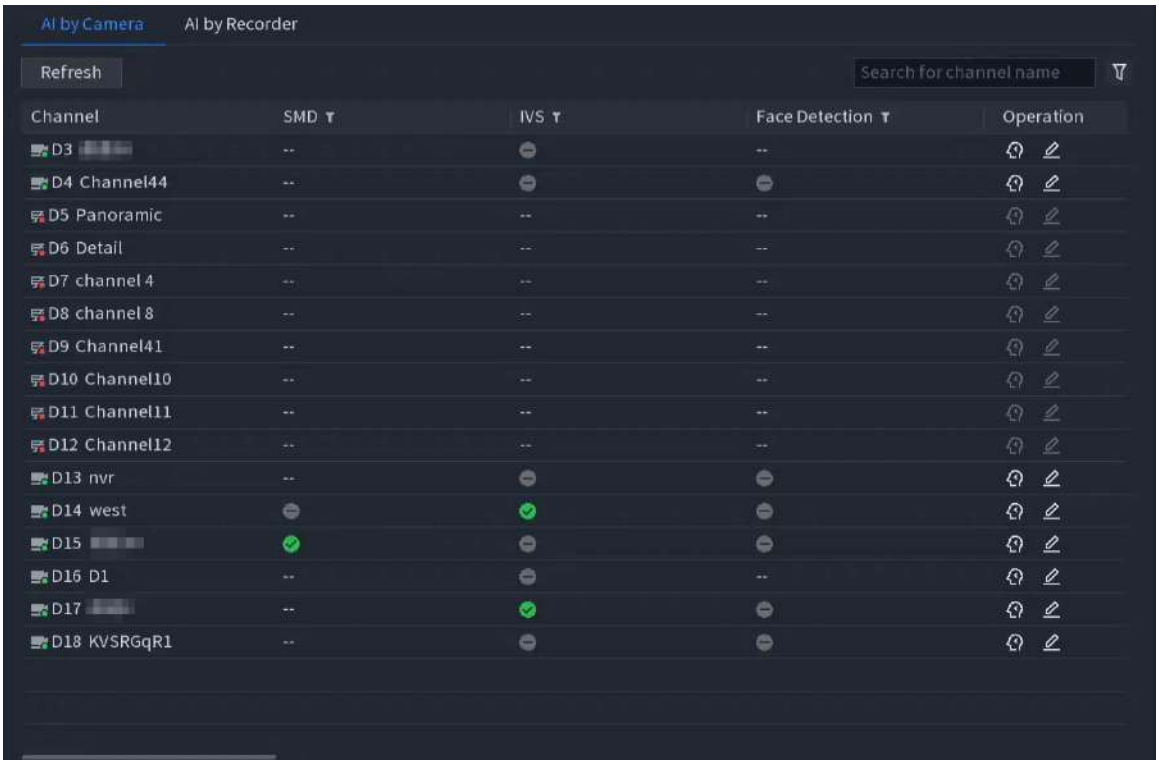
Supports modifying the front-end device configuration of the device, as well as viewing and configuring the front- and back-end device functions for any channel.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **AI Function Overview**.

Figure 6-2 AI function overview



Step 2 Select **AI by Camera** or **AI by Recorder**.

AI by recorder is only enabled when AI mode is selected.

- Click at the upper-right corner to filter the channels that support the corresponding intelligent functions.
- Click below **Operation** to modify the intelligent scheme of the camera.

  Only AI by camera supports modifying the smart plan, and some intelligent functions are mutually exclusive and cannot be enabled simultaneously.
- Click to modify the AI function settings of each channel. For details, see "6.2.2 AI Settings".

6.1.2 Mode Setting

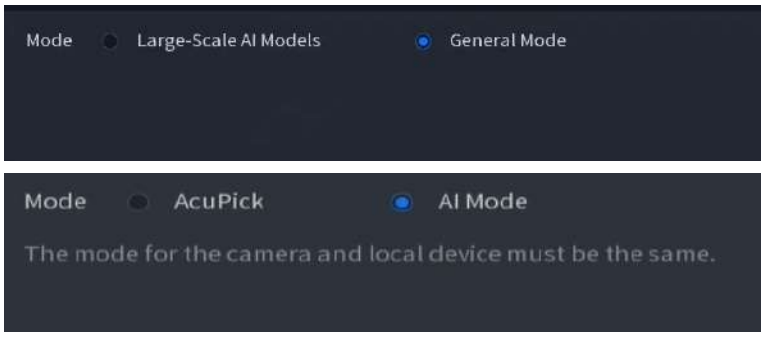
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

Step 2 Select **NVR** > **Mode**.

Step 3 Select the mode.

Figure 6-3 Mode selection

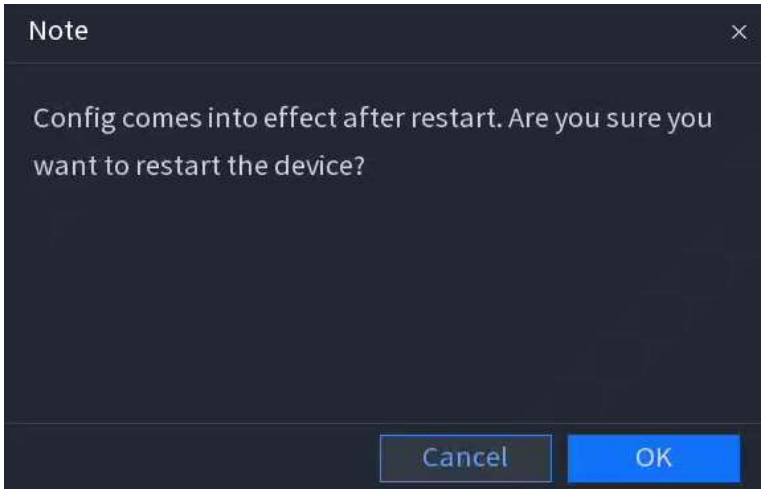


- Large-Scale AI Models/AcuPick: Once enabled, you can use the AcuPick and Wizseek function to search for and view targets during live view and playback.
- General Mode/AI Mode: Once enabled, you can use the AI functions in the live view page to filter and view different attribute targets in the footage, as well as playback targets that triggered AI events.

- The camera mode must be consistent with the device mode; Otherwise, some functions might not be available on the device.
- After you switch the device mode, a restart is required.
- In the mode of large-scale AI models, there are the following usage limitations:
  - The front-end devices must support AcuPick function.
  - Face detection, face recognition, perimeter detection, and SMD cannot be enabled.
  - The auxiliary screen cannot use 4K/8K display output.
  - Video playback of AcuPick search results does not support full-screen display output at 4K resolution.
  - The local face database and face searching by picture are not available.

Step 4 In the pop-up window, click **OK**.

Figure 6-4 Note of switching mode



6.1.3 AcuPick

Procedure

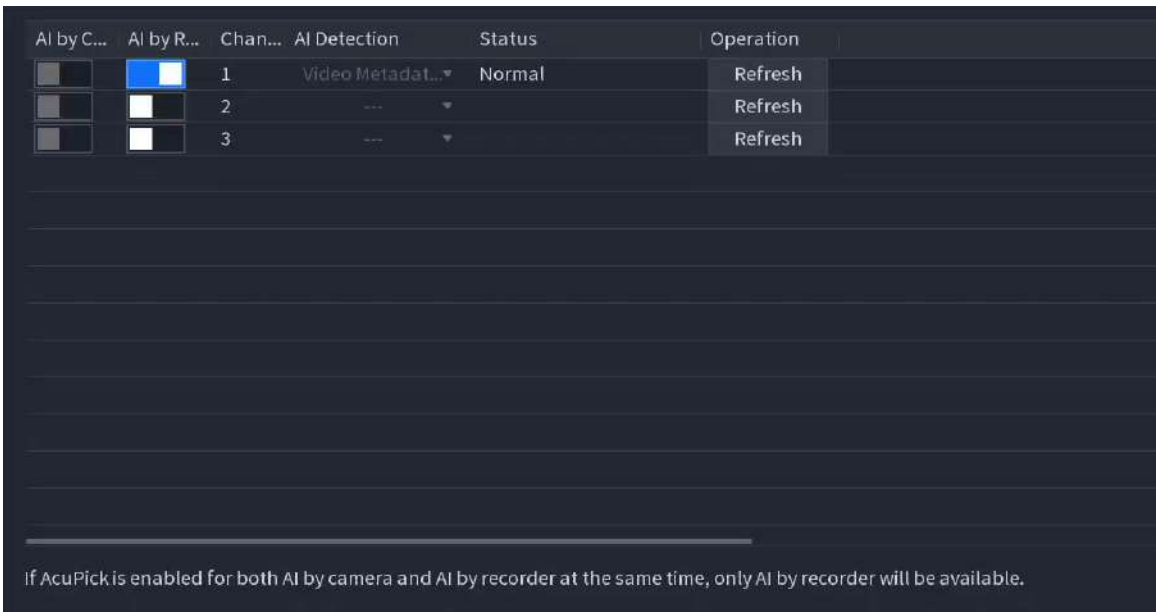
Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

Step 2 Select **NVR** > **AcuPick**.

Step 3 Enable or disable the corresponding channel's AI by camera or AI by recorder for AcuPick.

If AcuPick is enabled for both AI by camera and AI by recorder at the same time, only AI by recorder will be available.

Figure 6-5 AcuPick



6.1.4 Text Rule

Background Information

You can enable the configured text rules in "6.2.2.13 Text-Defined Alarms".

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

Step 2 Select **NVR** > **Text Rule**.

Step 3 In the text rule page, click **Add Rule**.

Step 4 Configure the parameters.

Figure 6-6 Text rule settings

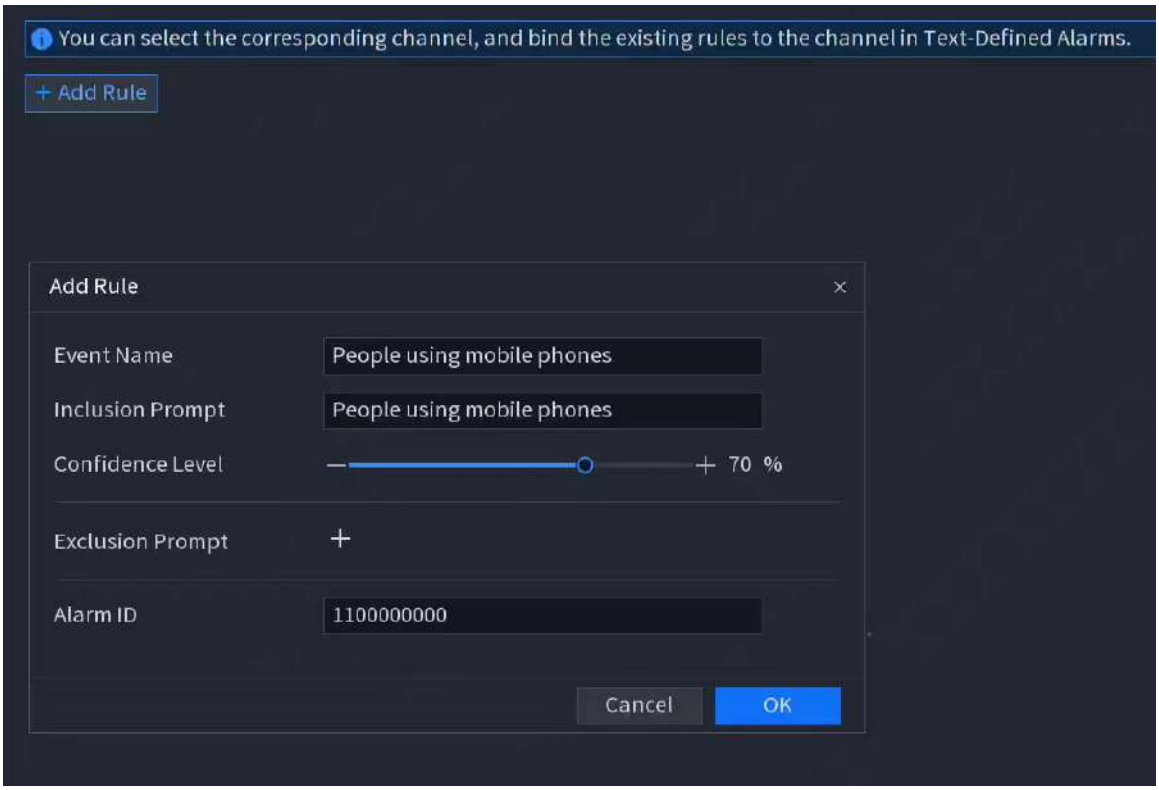


Table 6-1 Descriptions of the text rule parameters

Parameter	Description
Event Name	Configure the event name.
Inclusion Prompt	Set the inclusion prompt for target detection and alarm. When the target in the image matches the prompt and meets the confidence level, an alarm will be triggered.
Confidence Level	Set the confidence level, which indicates the similarity between the event image and the prompt feature comparison. The higher the level, the less likely an alarm will be triggered.
Exclusion Prompt	Set exclusion prompt words for calibrating detection results. When the target in the image matches the prompt words and meets the confidence level, the alarm will be filtered.
Alarm ID	Set alarm ID for linkage alarms.

6.1.5 Alarm Settings

6.1.5.1 Alarm-in Port

Set up alarm input detection. When the configured alarm rules are triggered, the system will execute alarm linkage actions.

Background Information

Alarm input detection includes local alarm, alarm box and network alarm.

- Local alarm: When the alarm-in port of the device is connected to an alarm device and local alarm settings are configured, the system will execute alarm linkage actions when the alarm signal is transmitted to the device through the alarm input port.

  If the camera supports remote voice communication and remote warning lights, it should allow configuration on the local alarm page, with the settings synchronized with the remote device.
- Alarm box: When the alarm-in port of the device is connected to the alarm box, configure the alarm for the alarm box. When the alarm signal is transmitted to the device through the alarm box, the system will execute alarm linkage actions.
- Network alarm: When the device receives an alarm signal transmitted over the network, the system will execute the alarm linkage actions.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, select **NVR** > **Alarm** > **Alarm-in Port**.

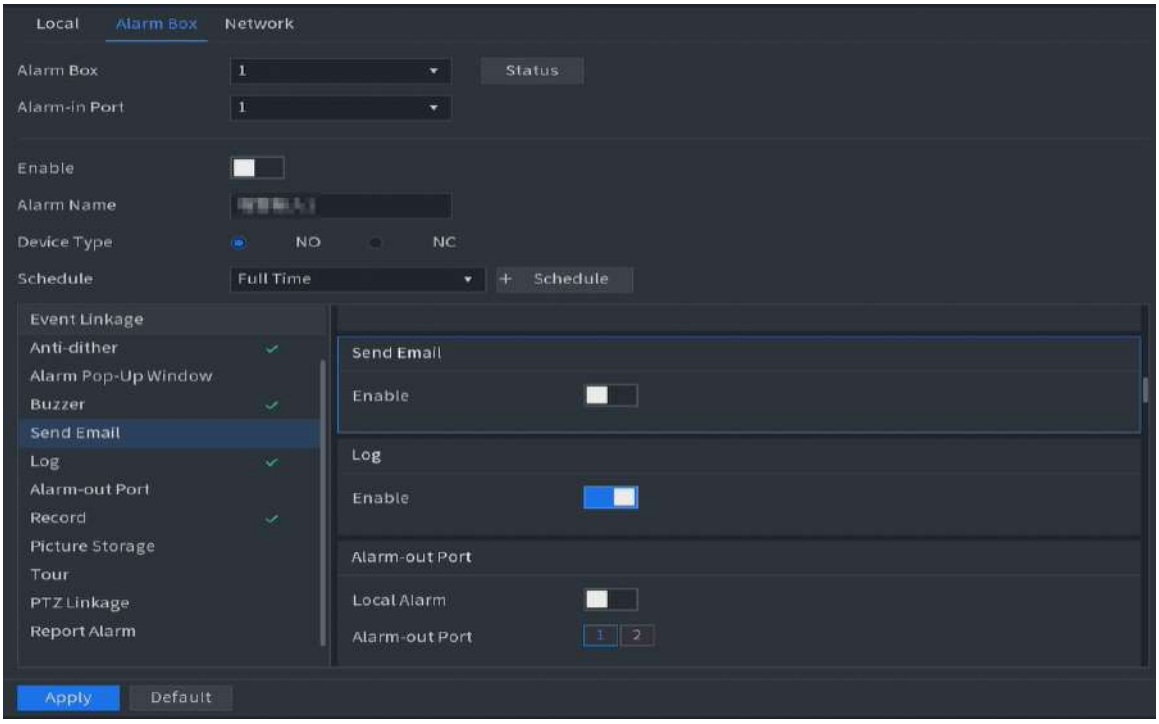
Step 2 Select the alarm method tab and configure the alarm-in port.

When the alarm method is set to **Alarm Box** , you need to configure the alarm box. Click **Status** to check the connection status of the alarm box.

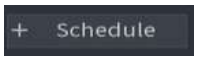
Step 3 Enable the function and set up the alarm information.

When network alarm is selected as the alarm method, **Device Type** is not available.

Figure 6-7 Alarm box



Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click 

to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.1.5.2 Alarm-out Port

Set the alarm output mode of the device to auto, manual, or off. When the alarm-out port is connected to an alarm device and the alarm linkage output function is enabled, the output mode must be set to **Auto** for the system to execute alarm linkage actions.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

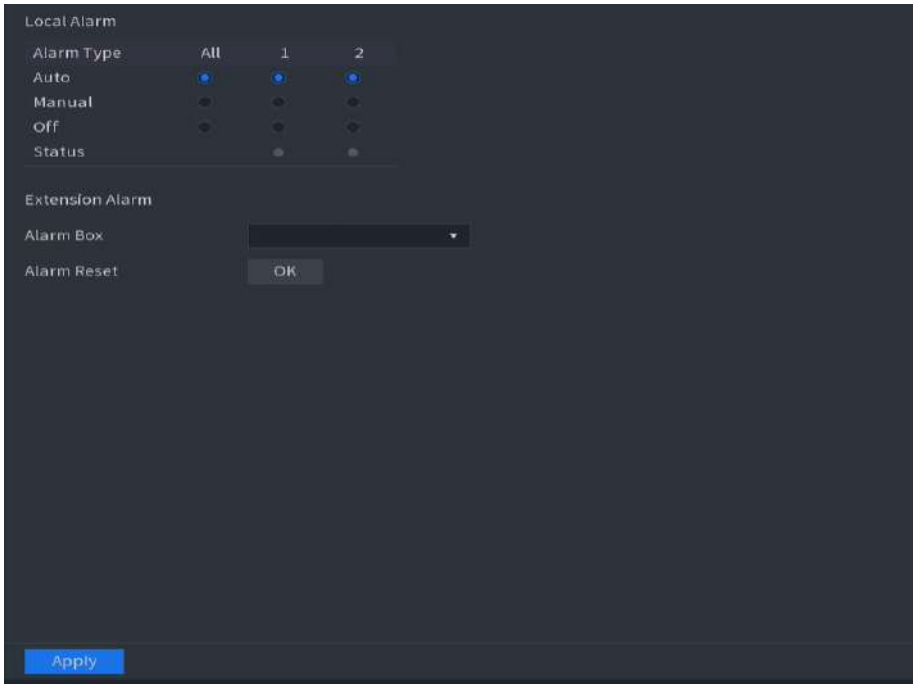
In **Device List**, click **NVR** > **Alarm** > **Alarm-out Port**.

Step 2 Set the local alarm output mode.

- **Auto** : Indicates that the alarm device only triggers the alarm when an event occurs.
- **Manual** : Indicates that the alarm device is in an alarm state continuously.
- **Off** : Indicates that the alarm output function is disabled.

In **All** list, you can simultaneously set the alarm mode for all alarm output channels.

Figure 6-8 Alarm mode



Step 3 Configure the extension alarm and select the alarm box.

- When the alarm device is in an alarm state, the status of the corresponding alarm output channel is displayed in green.
- In auto mode, when an alarm is triggered, clicking **OK** next to **Alarm Reset** will reset the alarm.

Step 4 Click **Apply**.

6.1.5.3 Exception

Set up exception event alarm detection. When issues arise with the hard drive, network, or other components, the system will execute alarm linkage actions.

Procedure

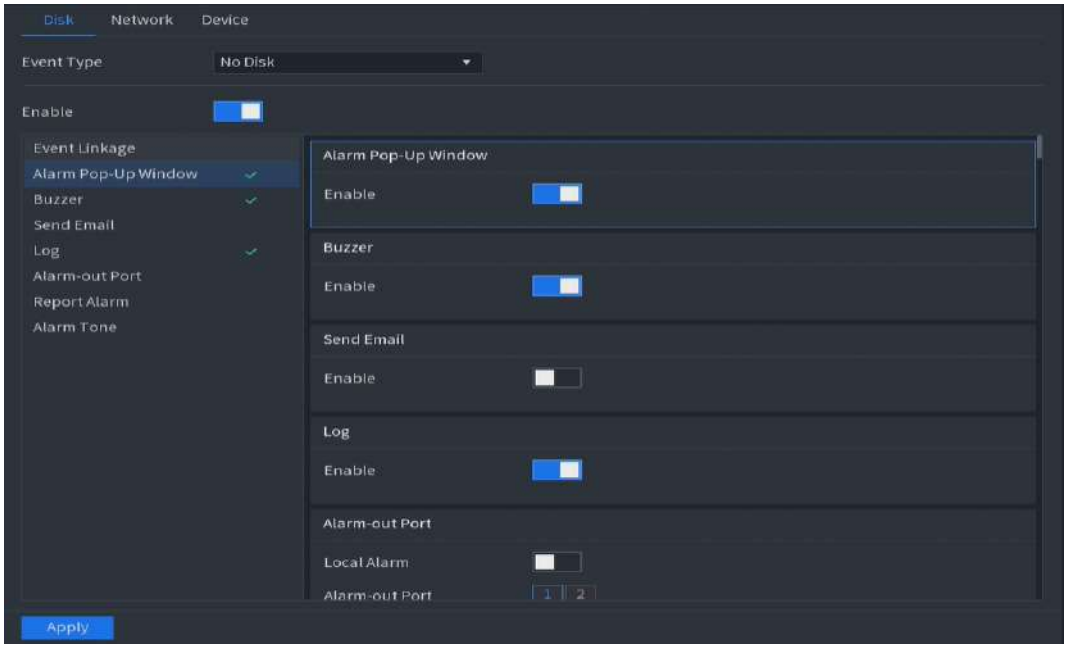
Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Alarm** > **Exception**.

Step 2 Click different exception tab and select the event type.

- **Disk** : Set up exception alarm detection for hard drive-related anomalies, including no hard drive, hard drive errors, insufficient storage capacity, quota capacity issues, and hard drive health anomalies.
- **Network** : Set up alarm detection for network-related anomalies, including network disconnection, IP conflicts, and MAC address conflicts.
- **Device** : Set up alarm detection for device component anomalies, specifically for abnormal fan speed.

Figure 6-9 Exception



Step 3 Enable the exception alarm and configure the alarm parameters.

When **Event Type** is set to **Low disk space warning**, you need to set a hard drive capacity lower limit. An alarm will be triggered only when the remaining available capacity on the hard drive falls below the specified value.

Step 4 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.1.5.4 One-click Disarm

Set up a one-click disarm function, allowing all linked alarm events to be turned off with one click based on actual needs.

Procedure

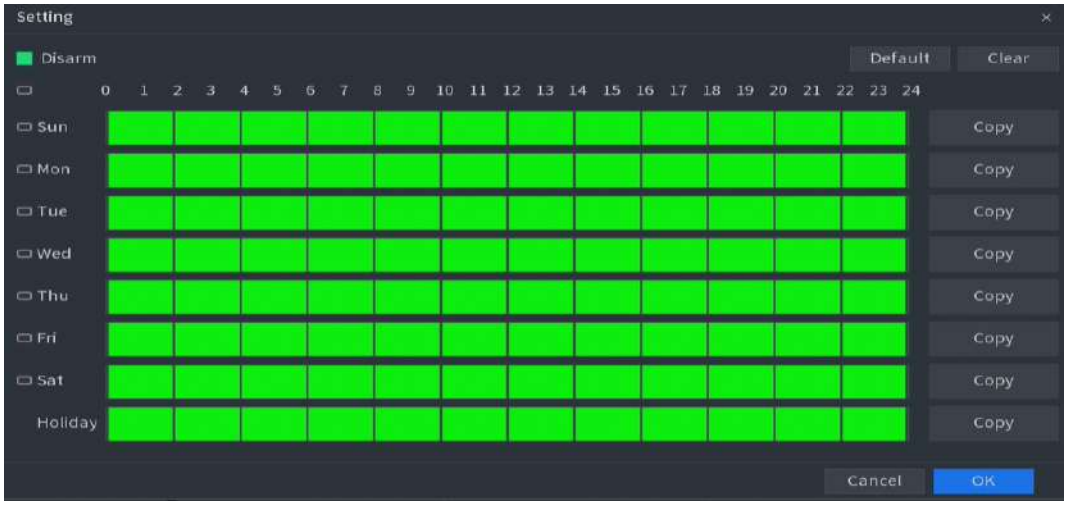
Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Alarm** > **One-click Disarm**.

Step 2 Select arm and disarm plans.

- Select **Disarm** to open the one-click disarm function.
- Select **Arm** to open the one-click arm function.
- Select **Disarm by Period** to open the disarm by period function. Disable the alarm during the set time period and enable it outside of that period. Click to set the time range for disarm by period.

Figure 6-10 Disarm by period setting



6.1.5.5 Custom Alarm

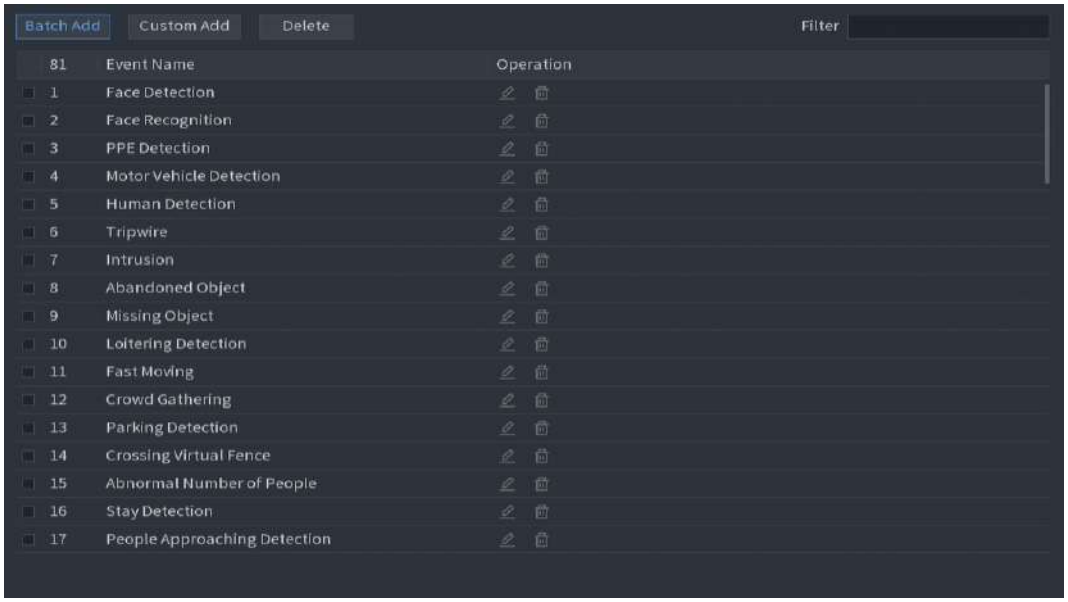
Customize and add event names, and configure the corresponding rules.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, select **NVR** > **Alarm** > **Custom Alarm**.

Figure 6-11 Custom alarm



Step 2 Add rules.

- **Batch Add** : Click **Batch Add** to add rules in batches which cannot be modified.
- **Custom Add** : Click **Custom Add** to customize the event name, event code and matching rule.

  Click to modify the event information; After selection, click **Delete** to remove them.

6.1.5.6 Arming Schedule

Set the arming and disarming time period for the alarm. The system will only trigger the corresponding alarm actions if the alarm is activated within this time period.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**. Select the channel in **Video Devices**, and select **AI Settings** > **SMD**.

This is just an example using SMD; please modify the settings according to your actual needs in the corresponding function.

Step 2 Click **+Schedule** on the right side of the **Schedule**.

Step 3 Configure the arming schedule.

1. Click ➕ to add the time plan.
2. Set the arming period.

Select for multiple dates and you can draw multiple date-time charts simultaneously.

- Method 1: On the timeline, hold down the left mouse button and drag to create the desired time period. Click the drawn area to delete that time segment.

Figure 6-12 Time plan table

- Method 2: Hover over the corresponding date and time period, and enter the period in the pop-up time input box.

Figure 6-13 Configure the time period

Step 4 Click **OK**.

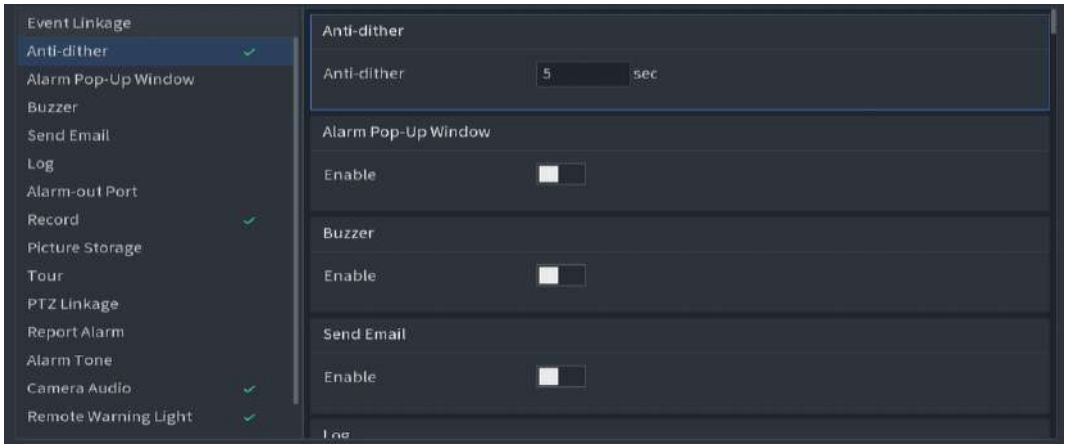
Related Operations

- Click **Default** to restore the timeline to its default configuration, which selects all time periods by default.
- Click **Clear** to remove all currently selected time periods from the timeline.
- Click to remove the schedule or the configured time periods.

6.1.5.7 Event Linkage

The event linkage can be configured in **AI Settings** and **Alarm** settings. After an alarm trigger or a smart event trigger, linked actions may be executed, including: **Anti-dither**, **Alarm Pop-Up Window**, **Buzzer**, **Send Email**, **Log**, **Alarm-out Port**, **Record**, **Picture Storage**, **Tour**, **PTZ Linkage**, **Report Alarm**, **Alarm Tone**, **Camera Audio**, **Remote Warning Light** and **Wireless Siren**.

Figure 6-14 Event linkage



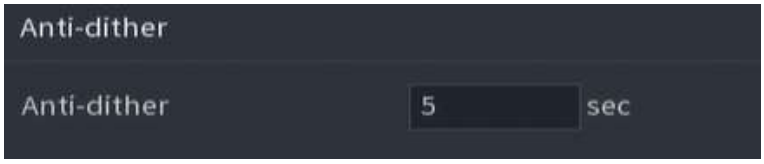
Anti-dither

Configure the anti-dither time and when it is triggered, the image will be processed for anti-dither. It is enabled by default.

The function is only available in

- **SMD** in **EVENT** > **AI Settings**.
- **Video Detection** in **Alarm**.
- **CAM Ext** in **Alarm**.

Figure 6-15 Anti-dither



Alarm Pop-Up Window

Enable the function and when it is triggered, the device will prompt an alarm pop-up window.

Buzzer

Enable the function and when linked actions are triggered, the device will trigger the buzzer.

Send Email

See "12.1.8 Email" to set the email in advance.

Enable the function and when an event is triggered, an email will be sent to the specified email address.

Log

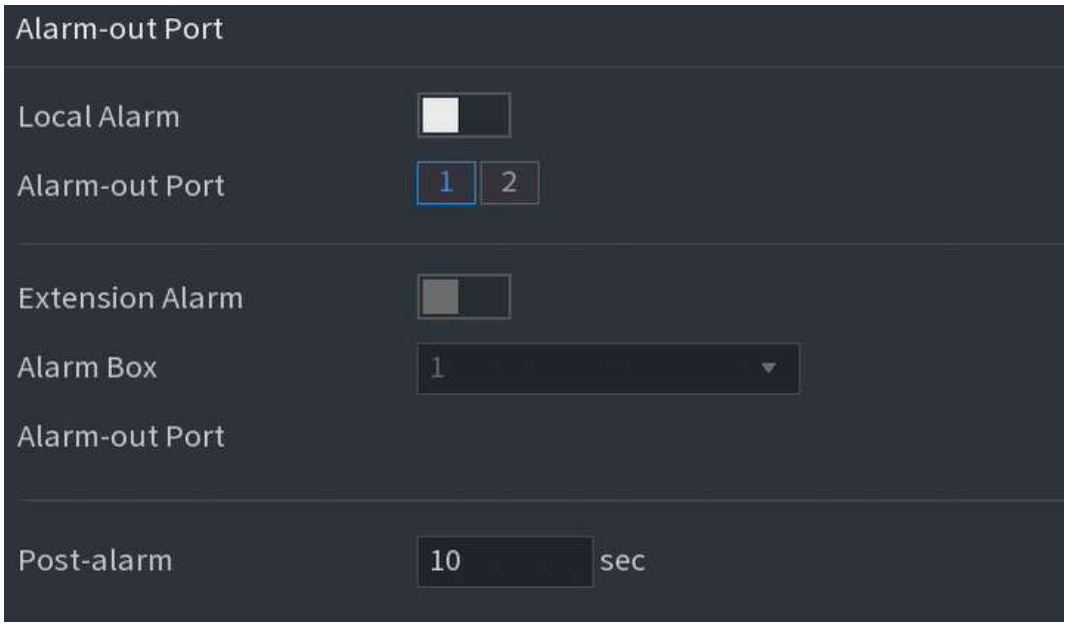
Enable the function and when a linkage is triggered, the system log will record the event information, which can be accessed from **APPLICATIONS** > **MAINTENANCE** > **Log**.

Alarm-out Port

To set the alarm output mode to auto, see "6.1.5.2 Alarm-out Port".

Enable the function, select the alarm-out port, choose whether to enable the extension alarm based on actual conditions, select the alarm box, and then set the post-alarm time. When a linkage is triggered, the alarm-out devices will issue alarms, such as sirens or light warnings.

Figure 6-16 Alarm-out port

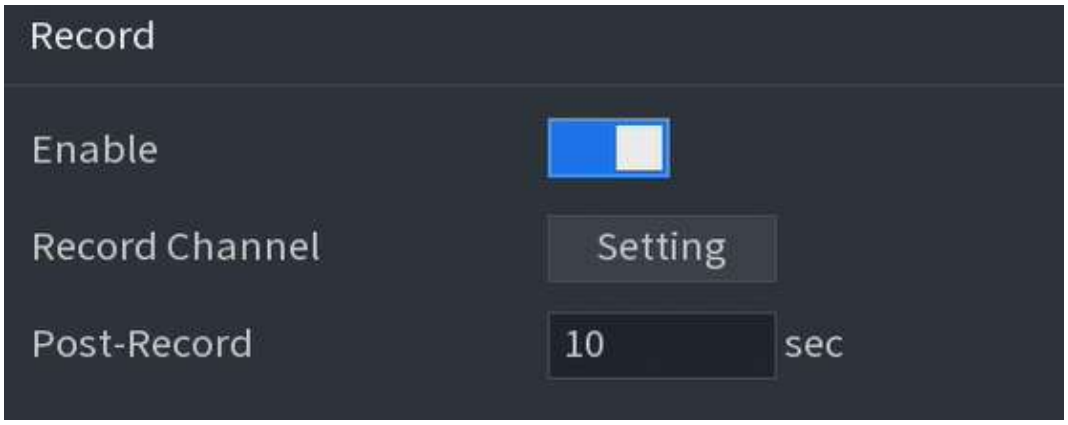


Record

Set the recording schedule in advance in "12.2.2 Schedule" to enable the auto recording for the corresponding channels and streams.

Enable the function, click **Setting** to select the record channel and configure the post-record time. When linked actions are triggered, the device will record videos.

Figure 6-17 Record



Picture Storage

Set the snapshot plans in advance in "12.2.2 Schedule" to enable the snapshot function for the corresponding channels.

After that, the device will capture images when linkage is triggered.

Tour

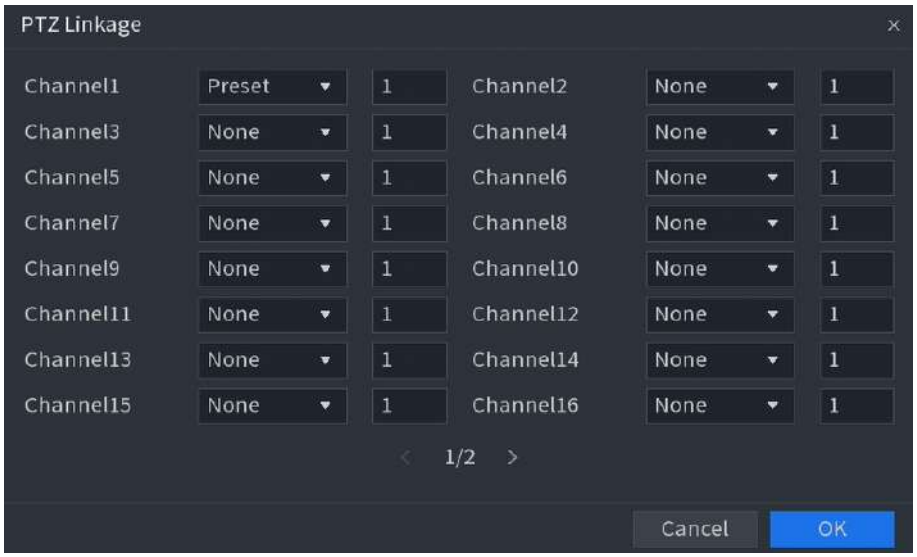
Enable the function and click **Setting** to select the channels for tour, with the option to choose multiple channels. When a linkage is triggered, the local page will display the selected channel images in tour. After the alarm ends, the local page will revert to the display prior to the alarm.

PTZ Linkage

Make sure the device is connected to PTZ devices, and PTZ devices has set presets, patrols, or tour. For details, see "4.5 PTZ".

1. Enable the function and click **Setting** to select the channels and set the PTZ action.
   - Select **Preset**, enter the preset ID in the box. When an alarm is triggered, the channel will automatically rotate to the preset position.
   - Select **Tour**, enter the tour group ID in the box. When an alarm is triggered, the channel automatically rotates along the planned tour group, moving between multiple presets.
   - Select **Pattern**, enter the pattern ID in the box. When an alarm is triggered, the channel automatically operates according to a fixed process, which includes a series of actions such as zooming, focusing, adjusting the aperture, and rotating in a specified direction.
2. Click **OK**.

Figure 6-18 PTZ linkage



Report Alarm

Enable and configure the alarm center in "12.1.11 Alarm Center".

Enable the function, click **Setting** to select the protocol type and event type, and then click **OK**. When the linkage is triggered, open the client on the alarm center; When the alarm is triggered, the client receives the alert.

Figure 6-19 Report alarm

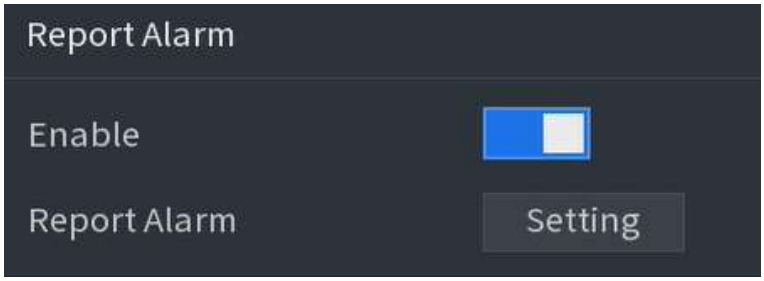
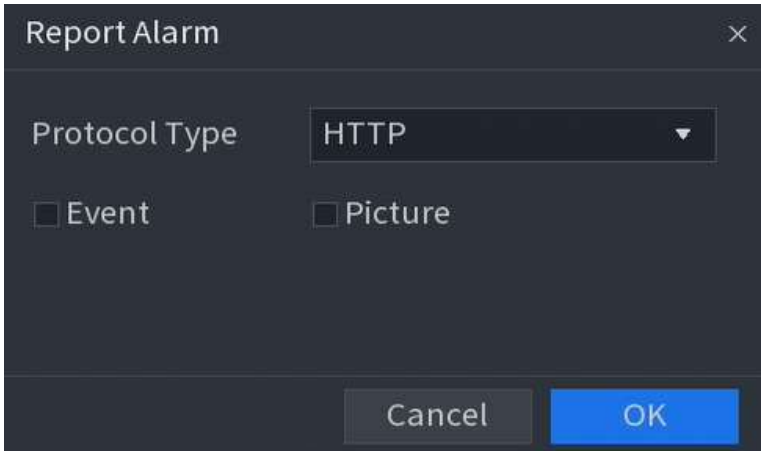


Figure 6-20 Configure the protocol type



Alarm Tone

Add the local audio files in "12.4.5.1 File Management".

Enable the function and select the audio file. When the linkage is triggered, the system will start playing the selected voice file.

6.1.6 Database

6.1.6.1 Face Database

6.1.6.1.1 Creating Local Face Databases

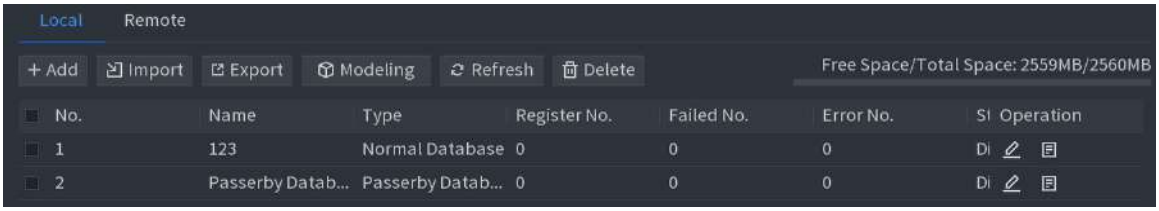
The created face database exists only on the local device and is suitable for face comparisons through AI by recorder.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

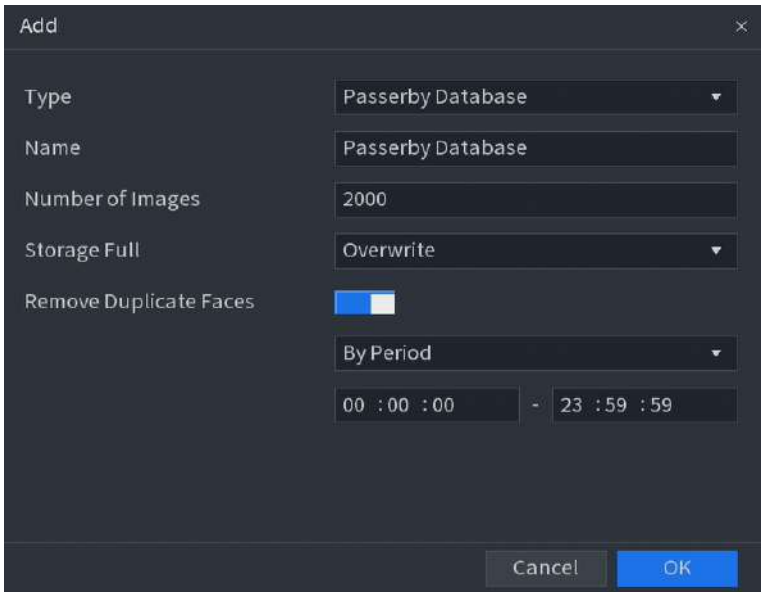
In **Device List**, select **NVR** > **Database** > **Face Database**.

Figure 6-21 Face database (local)



Step 2 Click + Add in the **Local** tab.

Figure 6-22 Create the face database (passerby database)



Step 3 Select the face database type, set the name, and then click **OK**.

When creating the passerby database, you need to configure the total number of images, the storage policy once the limit is reached, whether to enable face deduplication, as well as the collection method and time period.

Table 6-2 Passerby database parameters

Parameter	Description
Name	Enter a name for the passerby database.
Number of Images	Configure the number of images that the database can contain.
Storage Full	Select the storage strategy when space is full. • Stop: No more images can be added. • Overwrite: The newest images overwrite the oldest images. Back up the old images as necessary.
Time	Set the period in which the system removes duplicate face images from the database.

- **Register No.** : The number of registered individuals in the face database.
- **Failed No.** : The number of failed registrations.
- **Error No.** : The number of failed modeling.

Related Operations

- Add face images.

  Click to enter the face database page and manage the face images in the database. For details, see "6.1.6.1.3 Adding Images to Face Database".
- Edit registration information.

  Click to modify the registration information.
- Face database configuration.

  When you conduct face comparison with the linked face database, the face database can be configured. For details, see "6.2.2.5 Face Recognition".
- Delete the face database.

  Select one or more face images, and then click **Delete**.
- Model face images.

  The face images are modeled automatically after added to face database. You can also model face images manually.

  ◇ On the **Face Database** page, select a database, and then click **Modeling** to model all the face images in the database.

  ◇ On the **Details** page, select one or more face images, and then click **Modeling** to model the selected images.

6.1.6.1.2 Creating Remote Face Databases

The Device can get face databases from the remote devices, and also allows creating face databases for remote devices. The remote device face database is suitable for face recognition by the camera.

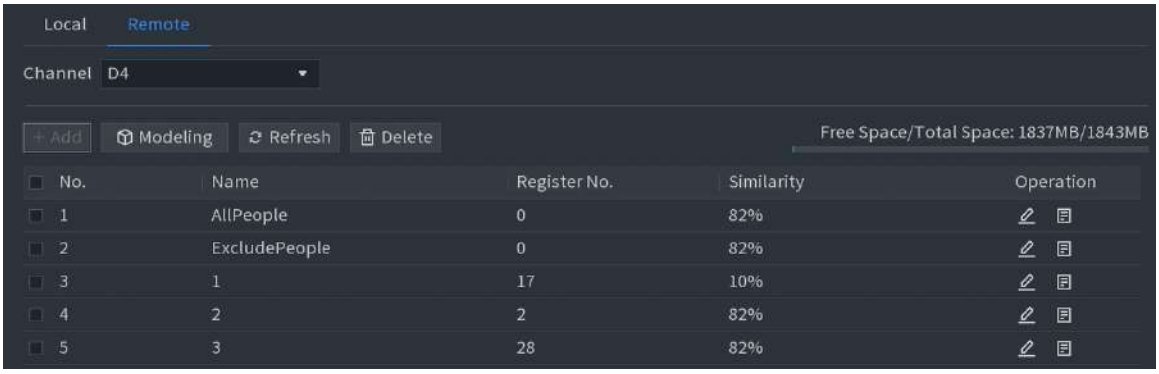
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Database** > **Face Database**.

Step 2 Select **Remote** as **Type**, select a channel and then click **Add**.

Figure 6-23 Face database (remote)



Step 3 Enter database name.

Step 4 Click **OK**.

Related Operations

- Add face images.

  Click to enter the face database page and manage the face images in the database. For details, see "6.1.6.1.3 Adding Images to Face Database".
- Edit registration information.

  Click to modify the registration information.
- Face database configuration.

  When you conduct face comparison with the linked face database, the face database can be configured. For details, see "6.2.2.5 Face Recognition".
- Delete the face database.

  Select one or more face images, and then click **Delete**.
- Model face images.

  The face images are modeled automatically after added to face database. You can also model face images manually.

  ◇ On the **Face Database** page, select a database, and then click **Modeling** to model all the face images in the database.

  ◇ On the **Details** page, select one or more face images, and then click **Modeling** to model the selected images.

6.1.6.1.3 Adding Images to Face Database

Adding Face Images One by One

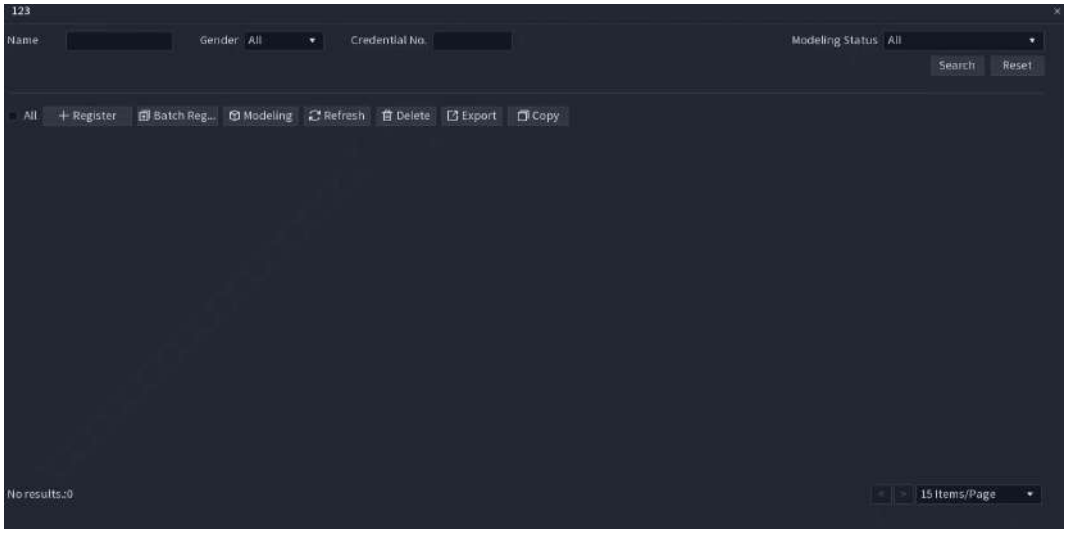
You can add one face image to the database. It is for the scenario that the registered human face picture amount is small.

1. Log in to the main menu, select **SETTINGS** > **EVENT**.

   In **Device List**, click **NVR** > **Database** > **Face Database**.

2. Click of the database that you want to configure.

Figure 6-24 Databases details



3. Click **+Register**.
4. Click to add a face image.
5. Select a face image and then enter the registration information.
6. Click **OK**.

   The system prompts the registration is successful.

7. On the **Details** page, click **Search**.

   The system prompts modeling is successful.

   If the system prompts modeling is in process, wait a while and then click **Search** again. If modeling failed, the registered face image cannot be used for face recognition.

Adding Face Images in Batches

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

1. Give a name to the face picture by referring to the following table.

Table 6-3 Naming rule

Naming Format	Description
Name	Enter the name.

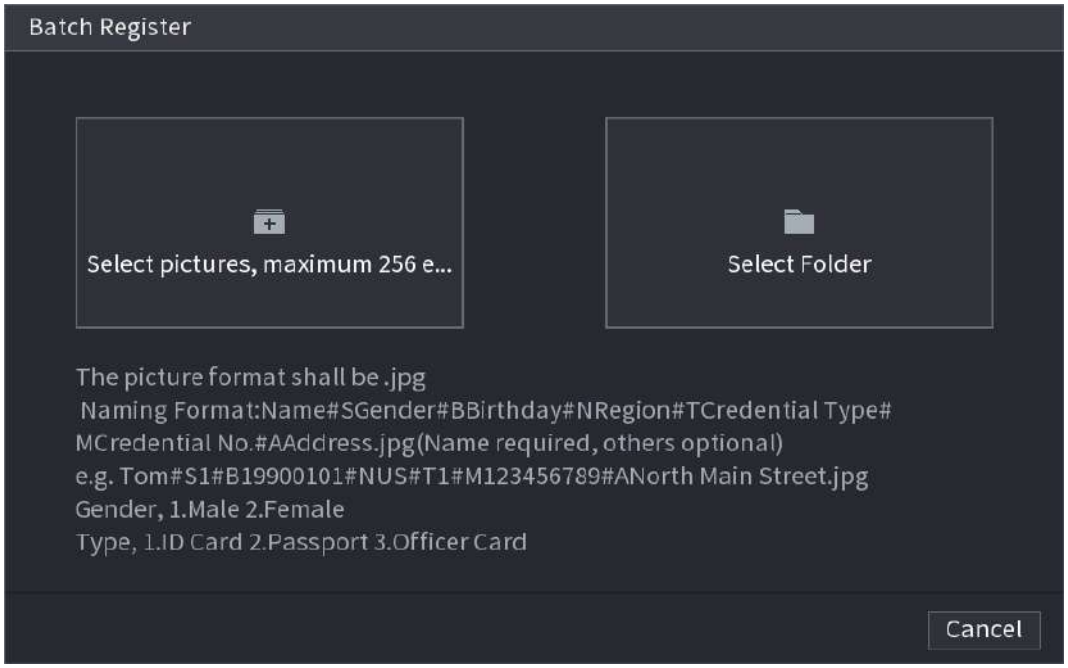
Naming Format	Description
Gender	Enter 1 or 2. 1 represents male, and 2 represents female.
Birthday	Enter numbers in the format of yyyy-mm-dd.
Region	Enter the abbreviation of region. For example, CN for China.
Credential Type	1 represents ID card; 2 represents passport; 3 represents officer card.
Credential No.	Enter the credential number.
Address	Enter the address.

2. Log in to the main menu, select **SETTINGS** > **EVENT**.

   In **Device List**, click **NVR** > **Database** > **Face Database**.

3. Click of the database that you want to configure.
4. Click **Batch Register**.

Figure 6-26 Batch register



5. Click or to import face images.
6. Click **OK**.

6.1.6.2 Vehicle Blocklist/Allowlist

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.

Background Information

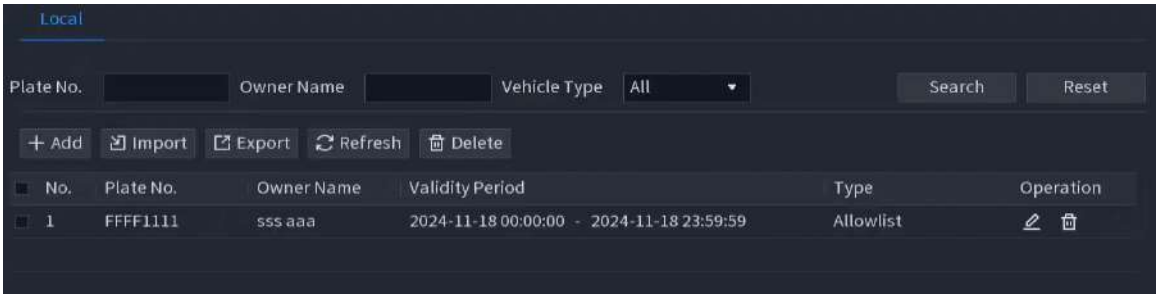
- With the blocklist and allowlist enabled, on the live view, the plate on the blocklist is displayed as red on the plate list and the plate on the allowlist is displayed as green. For the plate not on the blocklist or allowlist, the color is white.
- The added blocklist and allowlist will be synchronized to the connected ITC camera.

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Database** > **Vehicle Blocklist/Allowlist**.

Figure 6-27 Vehicle blocklist/allowlist



Step 2 Click **+Add**.

Step 3 Set plate information such as plate number, vehicle owner name, select **Blocklist** or **Allowlist**, and then set the validity period.

Step 4 Click **OK**.

Related Operations

- Search.

  Enter keywords for **Plate No.** and **Owner Name**, select type and then click **Search**.
- Import and export plate information.
  - Import: Click **Import** , select the corresponding file, and then click **Browse** to import the file.
  - Export: Click **Export** , select the file storage path and then click **Save**.
- Delete plate information.
  - Delete one by one: Click the of the corresponding plate number.
  - Delete in batches: Select the plate numbers and then click **Delete**.

6.1.6.3 Experience Database

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Database** > **Experience Database**.

Step 2 Click **Add**.

Figure 6-28 Add experience database

Step 3 Enter the name of the database and select the sample type.

Related Operations

- Add images.

  Click to enter the experience database page and manage the face images in the database.
- Edit database information.

  Click to modify the database information.
- Experience database configuration.

  When you conduct face comparison with the linked face database, the face database can be configured. For details, see "6.2.2.4 IVS".
- Delete the face database.

  Select one or more face images, and then click **Delete**.

6.1.6.4 Workwear Database

Procedure

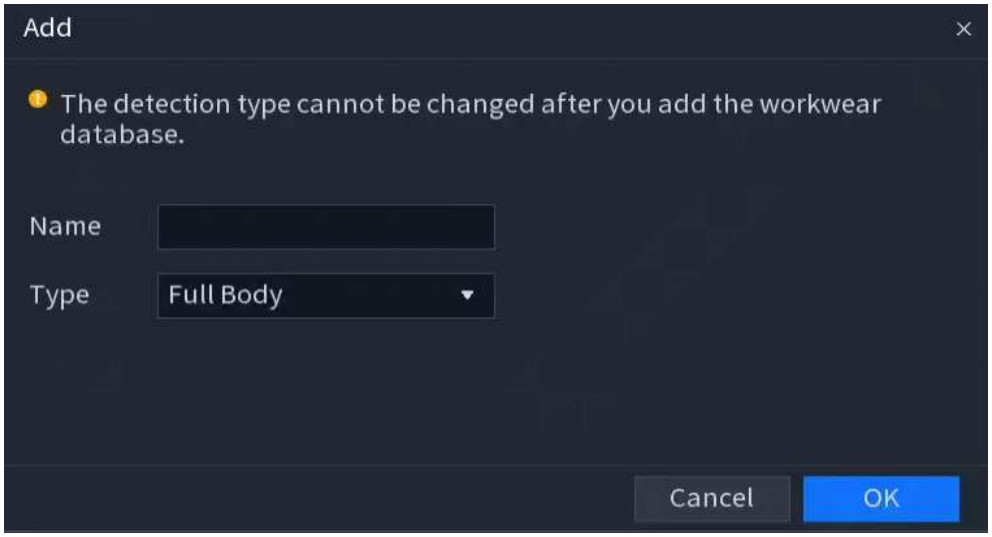
Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click **NVR** > **Database** > **Workwear Database**.

Step 2 Select the channel and Click **+Add**.

Step 3 Enter the name and select the type.

Figure 6-29 Add the workwear database



Step 4 Click **OK**.

6.1.6.5 Entries Frequency

After you set entries frequency, when the entries detected of a person reach or exceed the threshold, an alarm is triggered.

Prerequisites

Face database has been created and configured. For details, see "6.1.6.1 Face Database" and "6.2.2.4 IVS".

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, select **NVR** > **Database** > **Entries Frequency**.

Step 2 Click **Target Face Database** to select a database and then click **OK**.

Step 3 Click to enable the alarm detection for face database entries frequency.

Figure 6-30 Configure entries frequency parameters

Table 6-4 Entries frequency parameters

Parameter	Description
Statistical cycle	Set the cycle for counting the entries frequency.
Entries detected	Set the threshold of entries frequency. When the entries detected reaches or exceeds the threshold, an alarm is triggered.

Parameter	Description
Alarm name	The name is **Entries Frequency 111** by default. You can change the name.

Step 4 Click **Apply**.

6.2 Events of Remote Devices

6.2.1 Alarm Event Settings

6.2.1.1 Video Detection

By analyzing video images, the system checks for sufficient changes in the image. When a significant change occurs in the image (such as the appearance of moving objects or changes in the video scene), the system triggers an alarm response.

6.2.1.1.1 Motion Detection

After you set up motion detection, when a moving target appears in the surveillance footage and its speed exceeds the preset sensitivity threshold, the system triggers an alarm.

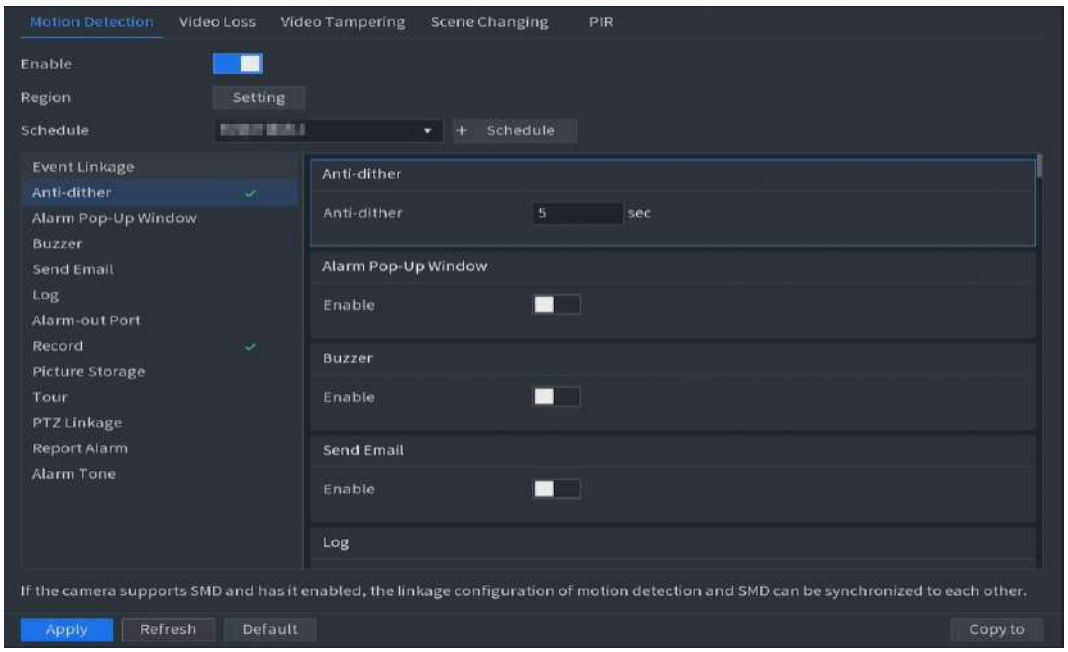
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Video Detection** > **Motion Detection** and enable the function.

Figure 6-31 Motion detection



Step 3 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 4 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.1.1.2 Video Loss

After enabling video loss detection, the system triggers an alarm when it detects that the video from a connected remote device has been lost.

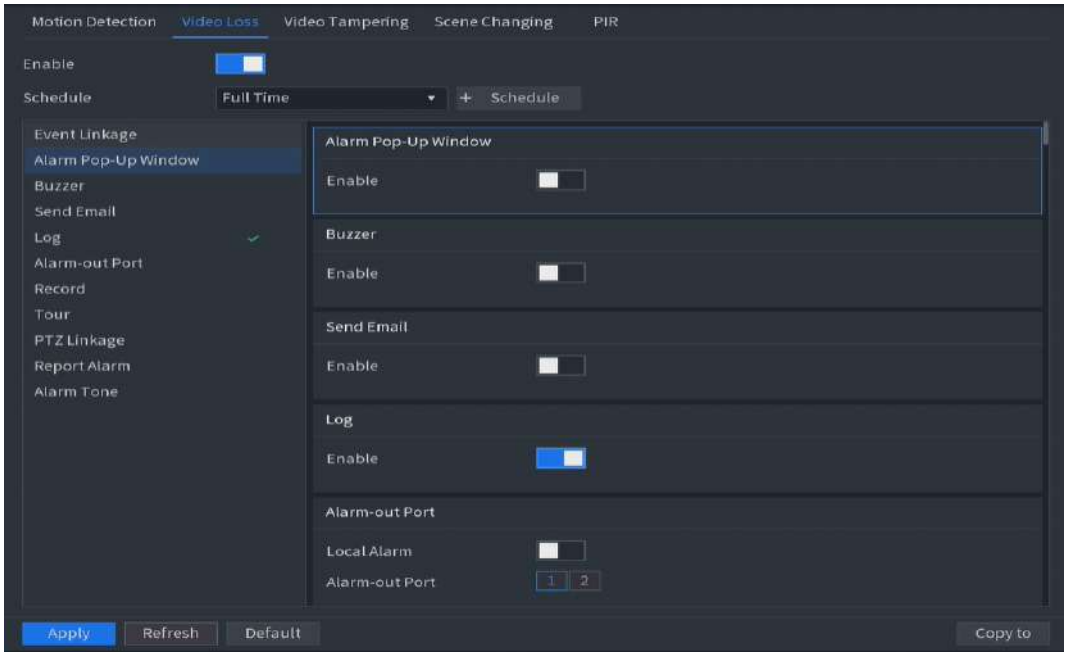
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Video Detection** > **Video Loss** and enable the function.

Figure 6-32 Video loss



Step 3 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 4 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.1.1.3 Video Tampering

When the camera lens is covered, or the video is displayed in a single color because of sunlight status, the monitoring cannot be continued normally. To avoid such situations, you can configure the tampering alarm settings.

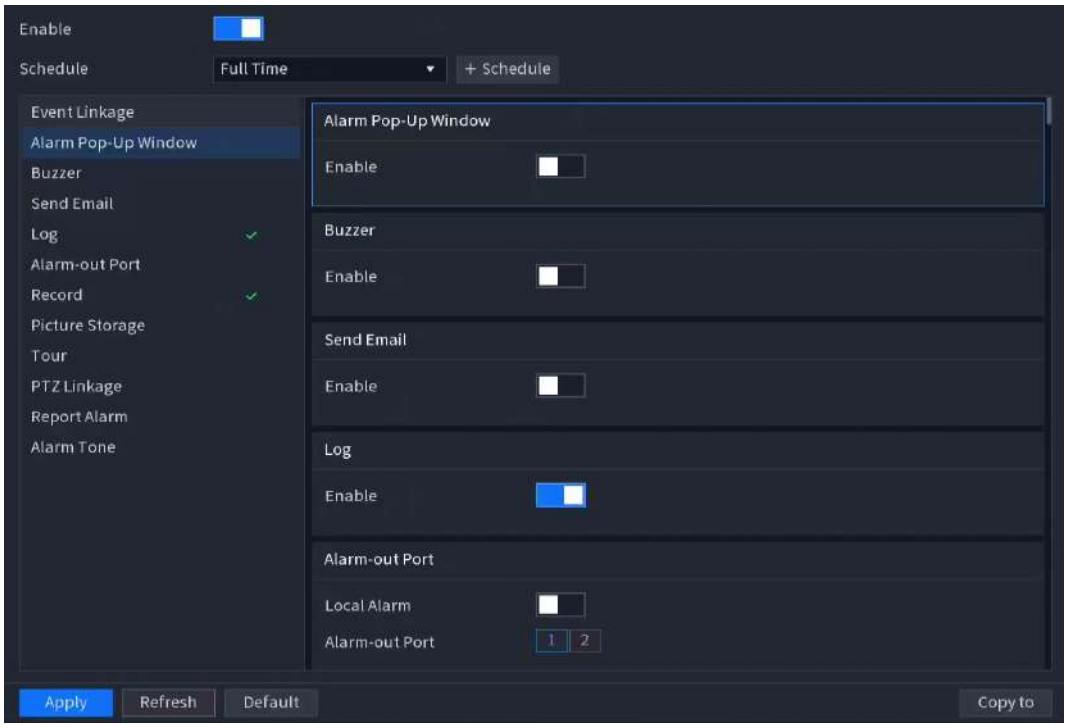
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Video Detection** > **Video Tempering** and enable the function.

Figure 6-33 Video tampering



Step 3 Click to enable the function.

Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.1.1.4 Scene Change

When the detected scene has changed, system performs alarm linkage actions.

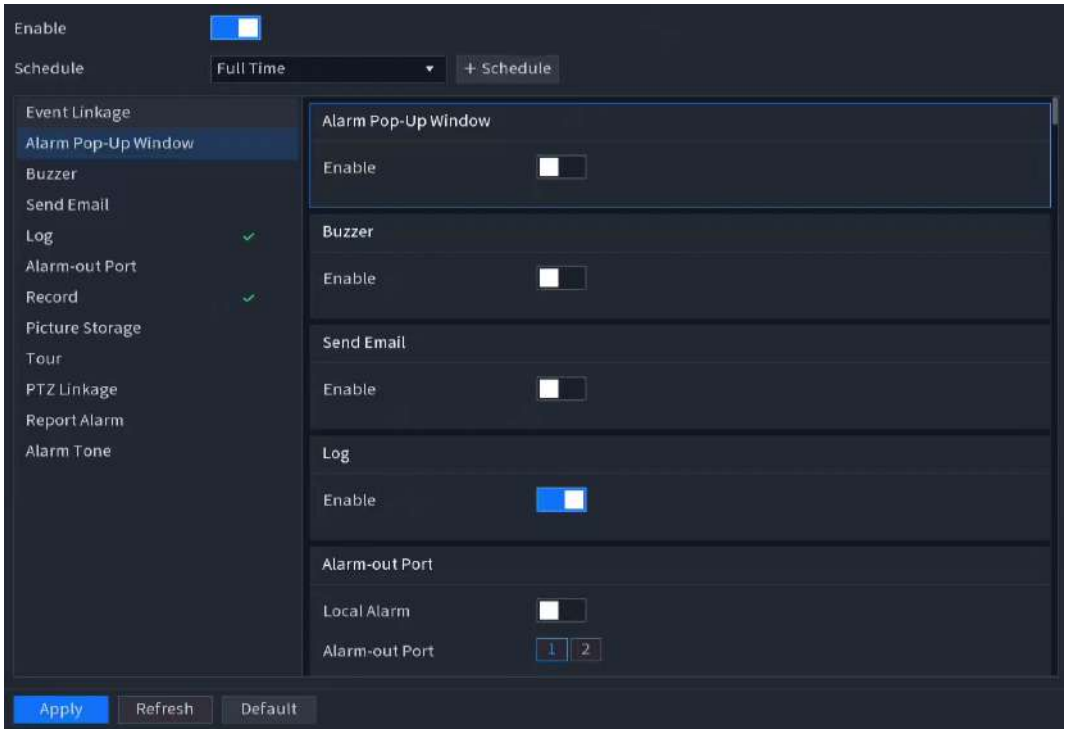
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Video Detection** > **Scene Changing** and enable the function.

Figure 6-34 Scene changing



Step 3 Click to enable the function.

Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.1.1.5 PIR Alarm

PIR function helps enhancing the accuracy and validity of motion detect. It can filter the meaningless alarms that are activated by the objects such as falling leaves and flies. The detection range by PIR is smaller than the field angle.

Background Information

PIR function is enabled by default if it is supported by the cameras. Enabling PIR function will get the motion detection to be enabled automatically to generate motion detection alarms.

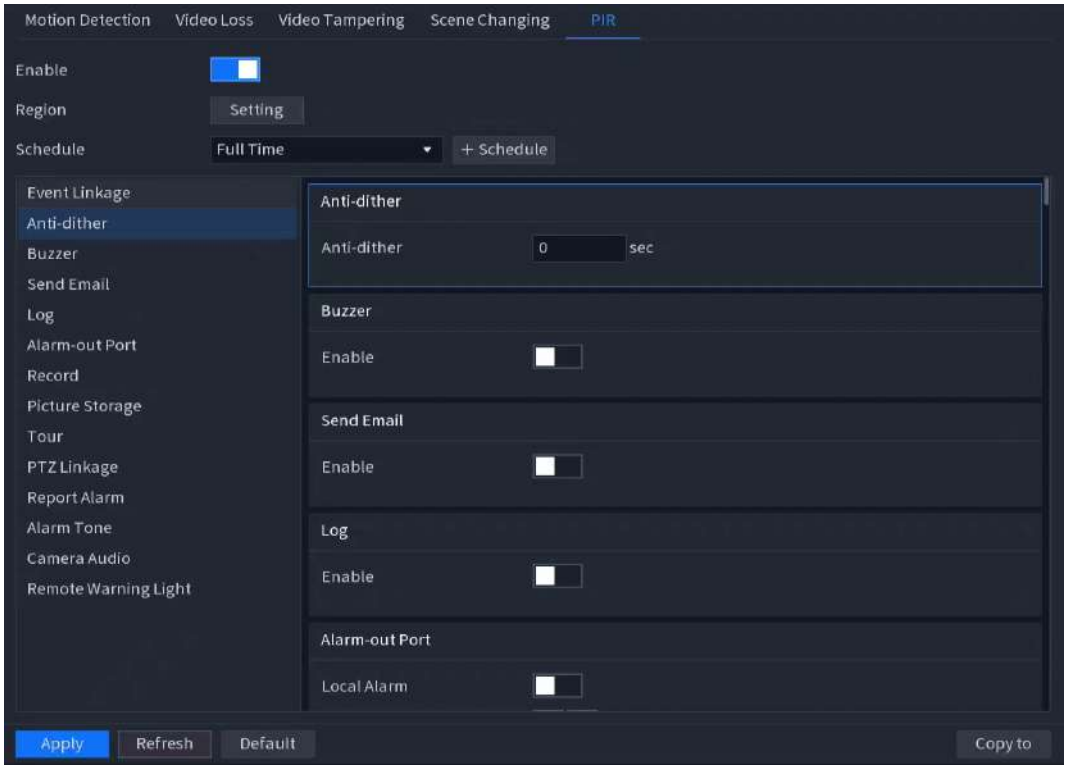
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Video Detection** > **PIR** and enable the function.

Figure 6-35 PIR alarm



Step 3 Click to enable the function.

Step 4 Configure the detection region.

1. Click **Setting** next to **Region**.
2. Point to the middle top of the page.
3. Select one region, for example, click .
4. Drag on the screen to select the region that you want to detect.
5. Configure the parameters.

Table 6-5 Detection region parameters

Parameter	Description
Name	Enter a name for the region.
Sensitivity	Every region of every channel has an individual sensitivity value. The bigger the value is, the easier to trigger an alarm.
Threshold	Adjust the threshold for motion detection. Every region of every channel has an individual threshold.

You can configure up to 4 detection regions. When any one of the four regions activates an alarm, the channel where this region belongs to will activate an alarm.

6. Right-click to exit the page.

Step 5 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 6 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

6.2.1.2 Audio Detection

The system can generate an alarm once it detects the audio is not clear, the tone color has changed or there is abnormal or audio volume change.

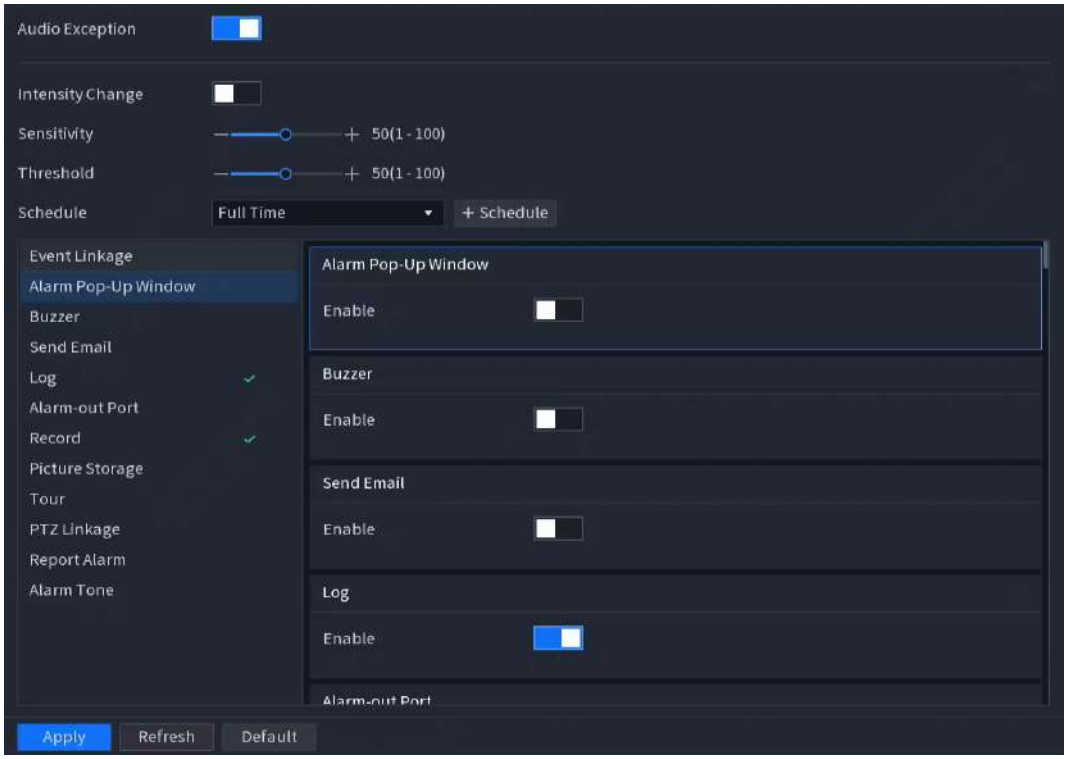
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **Audio Detection** and enable the function.

Figure 6-36 Audio detection



Step 3 Configure the parameters.

- **Audio Exception** : The system generates an alarm when the audio input is abnormal.
- **Intensity Change** : Set the sensitivity and threshold. An alarm is triggered when the change in sound intensity exceeds the defined threshold.

The higher the sensitivity value, the easier it is to trigger audio detection.

Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.1.3 External Alarm for the Camera

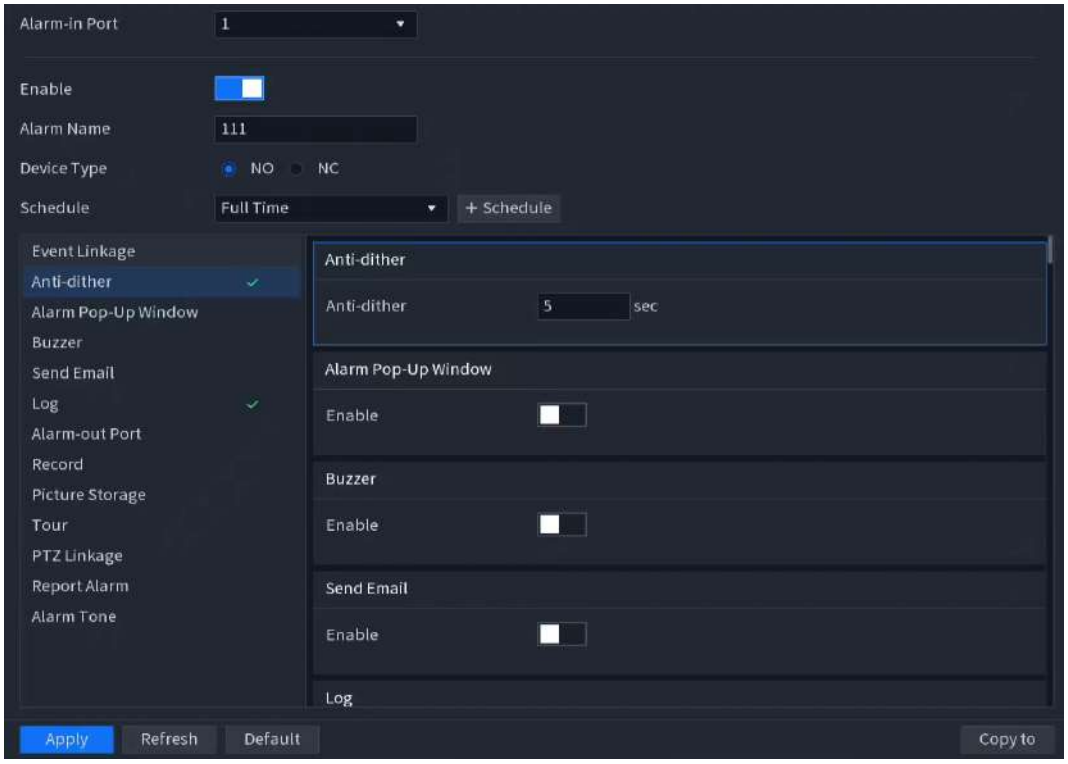
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **CAM Ext** and enable the function.

Figure 6-37 External alarm for the camera



Step 3 Select the alarm-in port, configure the alarm name, and then select the device type.

- NO (Normally Open): For active alarm triggering to reduce standby power consumption.
- NC (Normally Closed): For continuous line monitoring and fail-safe priority (e.g., circuit integrity assurance).

Step 4 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 5 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.1.4 Alarm for Camera Offline

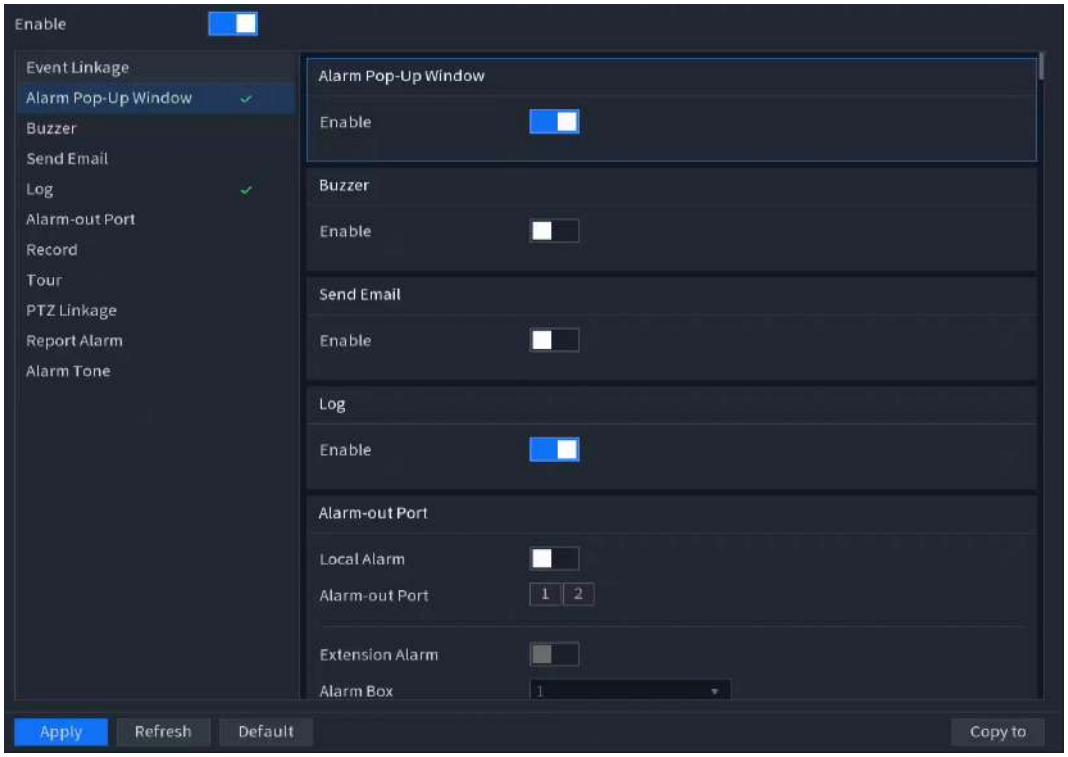
Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **CAM Offline** and enable the function.

Figure 6-38 Alarm for camera offline



Step 3 Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 4 Click **Apply**.

6.2.2 AI Settings

6.2.2.1 Overview

AI detection falls into AI by camera and AI by recorder.

- AI by camera: Some cameras themselves support AI detection. The cameras perform AI detection and send the detection results to the NVR for display. When using AI by camera, make sure to connect the Device to the cameras that support the corresponding AI detection functions.
- AI by recorder: The cameras send videos to NVR for detection, analysis and result display.

- Some models support AI by camera only.
- The AI functions might vary with models.
- Different AI functions might conflict with each other. You cannot enable two conflicting AI functions for the same channel.

6.2.2.2 Configuring Smart Plan

To use AI by camera for face detection, face recognition and other detection functions, you need to enable the corresponding smart plan first.

Procedure

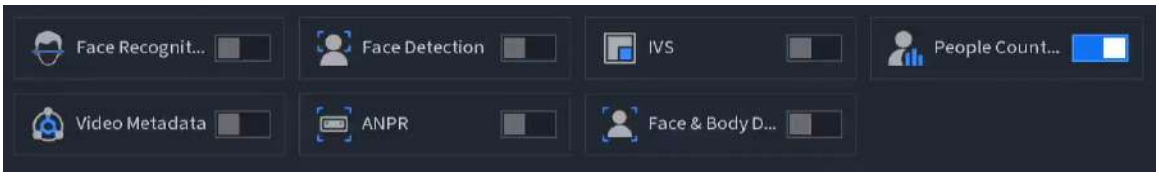
Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Smart Plan**.

- The page might differ depending on which smart plans that the remote device supports.
- If the channel is connected to a PTZ camera, you can set smart plans separately for each preset point.

Figure 6-39 Smart plan



Step 3 (Optional) Click **Add Preset**.

This function requires support from front-end devices.

Step 4 Enable the corresponding smart plans.

When a new smart plan to be enabled is mutually exclusive with an already enabled smart plan, the existing smart plan must be disabled before the new one can be enabled.

You can enable smart plans for different presets.

Step 5 Click **Apply**.

6.2.2.3 SMD

You can use SMD (Smart Motion Detection) to detect humans and vehicles in the video, and store the detection results in structured storage for fast retrieval.

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

The SMD linkage configuration is consistent with that of the motion detection. When there is a change in linkage for motion detection, the SMD linkage configuration will automatically synchronize with those of motion detection. The same applies in the opposite direction.

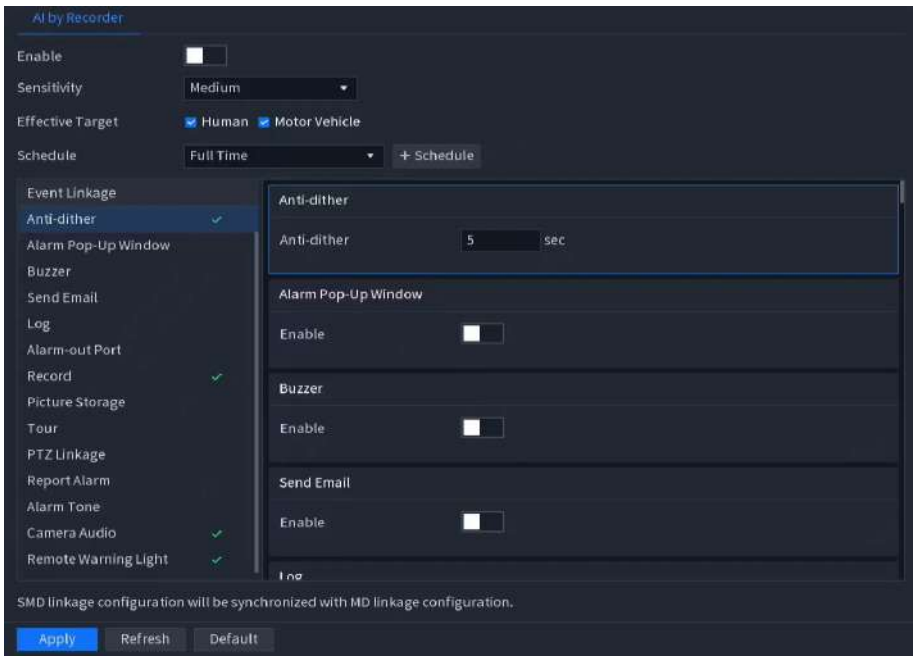
Procedure

Step 1 Log in to the main menu, and then select **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **SMD**, enable the function, and then configure the parameters.

Figure 6-40 SMD



Step 3 Configure the sensitivity.

The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur. The default value is recommended.

Step 4 Select effective target. You can select **Human** and **Motor Vehicle**.

Step 5 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 6 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

6.2.2.4 IVS

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

The IVS function processes and analyzes the images to extract the key information to match the specified rules. When the detected behaviors match the rules, the system triggers alarms.

- This function is available on select models.
- IVS and face detection cannot be enabled at the same time.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **IVS**.

Step 3 Select **AI by Camera** or **AI by Recorder**.

6.2.2.4.1 Smart Calibration

To reduce false alarms (for example, animals significantly shorter than humans) in perimeter detection, you can use far, mid, or near depth calibration to establish reference human height at any point in the frame, enabling height-based comparison to filter out detections that are not within the calibrated height range.

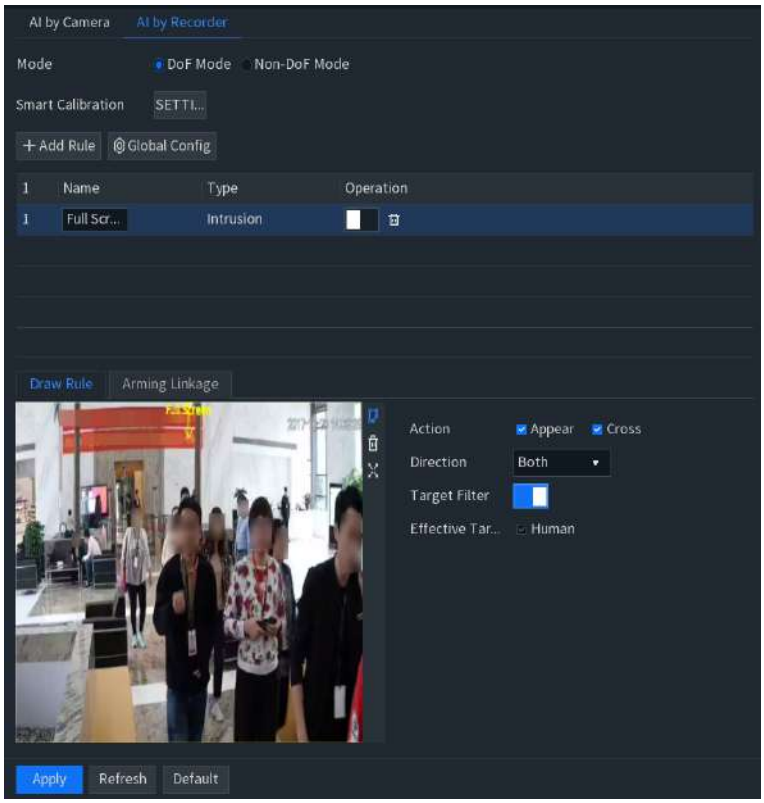
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

Step 2 Click the remote device channel in **Device List**.

Step 3 Click the **AI by Recorder** tab.

Figure 6-41 DoF mode



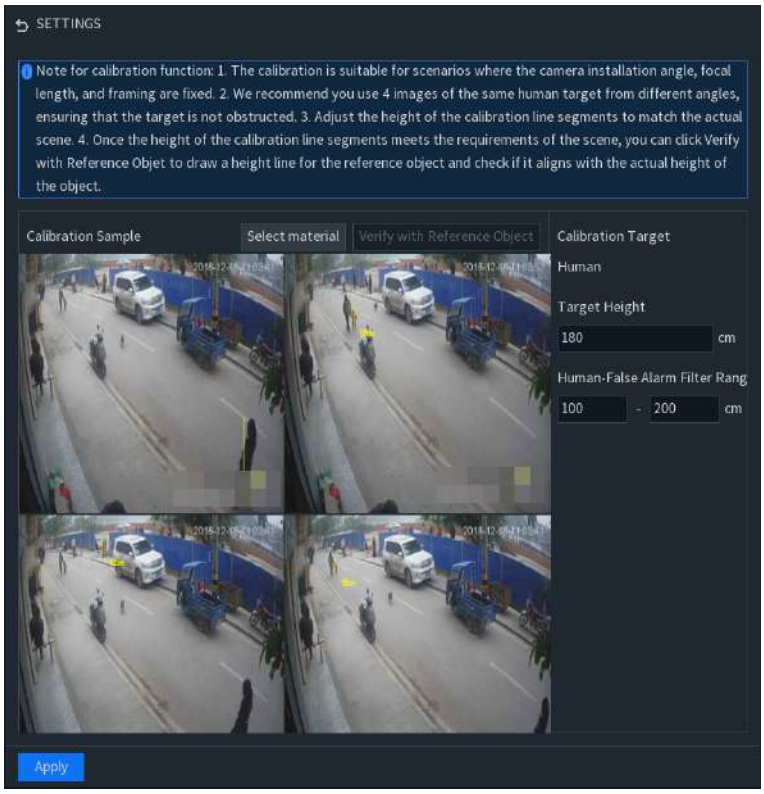
Step 4 Select **DoF Mode**.

- **DoF Mode** : You can enable smart calibration in this mode and this mode is enabled by default.

- **Non-DoF Mode** : Select the original size box filter page.

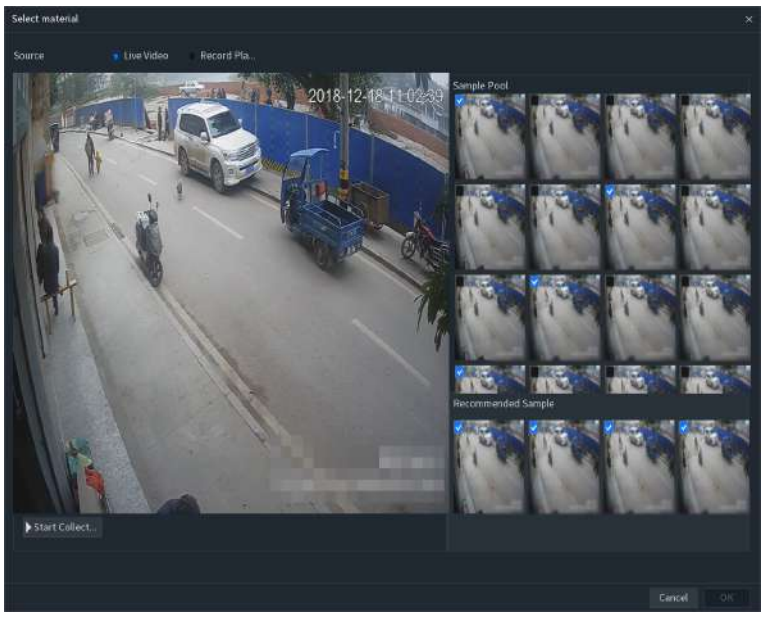
Step 5 Click **SETTINGS** beside **Smart Calibration** to enter the smart calibration page, and then click **Select material**.

Figure 6-42 Smart calibration



The target height is 180 cm and the human false alarm filter range is 100–200 cm by default. You can also enter the number by yourself.

Figure 6-43 Select material



Step 6 On the **Select material** page, select your material source.

Live Video is selected by default.

- **Live Video** :
  1. When the calibration person enters the image, click **Start Collecting** and the system starts capturing images.

     High-quality images will be pushed into the sample pool and the top 4 of them are displayed in the recommended sample.

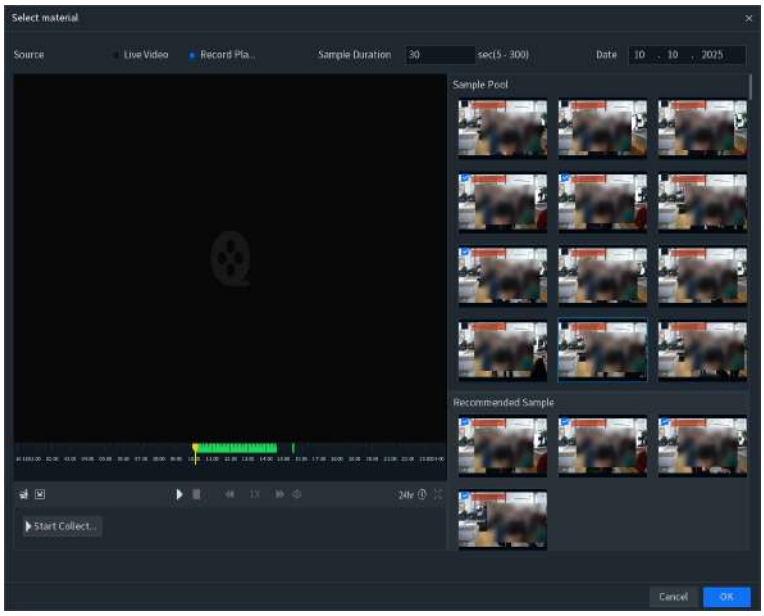
     To select photos manually, you have to click **Stop Collecting** to pause the image capture.
  2. Select images in the sample pool, and then click **OK**.

     At most 4 images can be selected.
- **Record Playback** :
  1. Select the image containing the calibration target in the playback video, and then click **Start Collecting** and the system starts capturing images.

     The system detects 30 seconds from the cursor position by default, with an adjustable range of 5–300 seconds.

     High-quality images will be pushed into the sample pool and the top 4 of them are displayed in the recommended sample.

Figure 6-44 Record playback



◇ To select photos manually, you have to click **Stop Collecting** to pause the image capture.

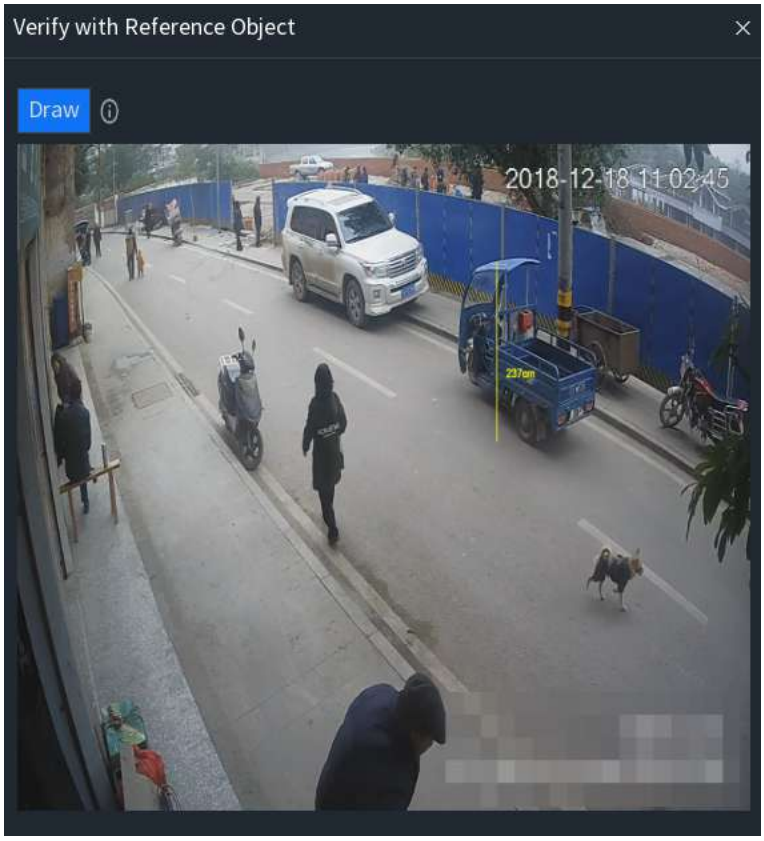
◇ You can select to enable the quick search, with options for **Human** and **Motor Vehicle**.

2. Select images in the sample pool, and then click **OK**.

At most 4 images can be selected.

After selecting the material, you can click **Verify with Reference Object** and click **Draw** to freeze the live video, draw a reference height line, and then verify whether it matches the actual object height.

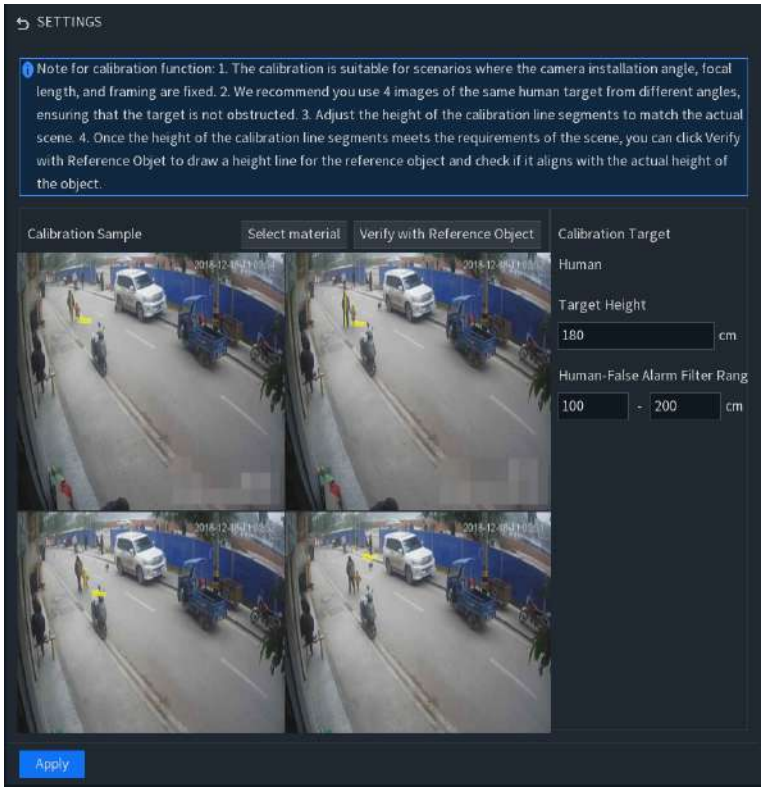
Figure 6-45 Reference object verification



If there is any deviation in height, you can return to the settings page and adjust the corresponding target height value on the right to match the reference object height.

Step 7 After that, you will return to the settings page. Drag the mouse to adjust the height of the calibration line.

Figure 6-46 Adjust the height



Step 8 Click to close the window, and then click **Apply**.

6.2.2.4.2 Tripwire

When the detection target crosses the warning line along the defined direction, the system performs an alarm linkage action.

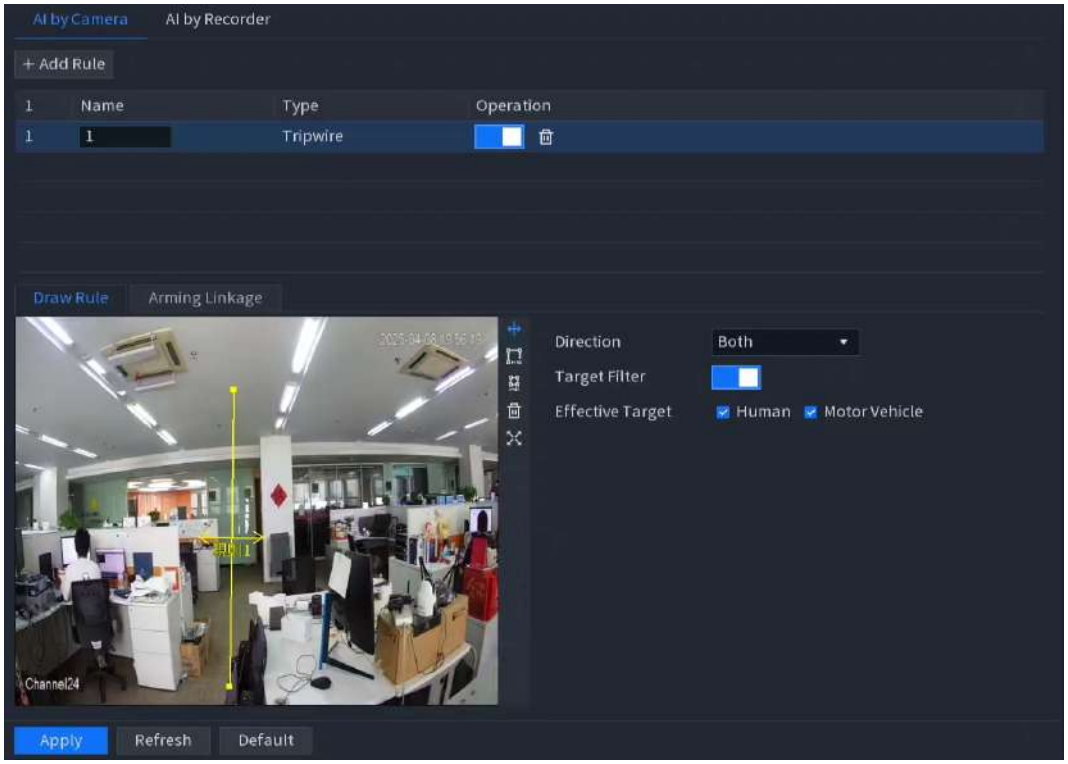
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

Step 2 Click the remote device channel in **Device List**.

Step 3 Click **Add Rule** to select **Tripwire**.

Figure 6-47 Tripwire



Step 4 Select the preset.

This function is only available when supported by the front-end devices.

Step 5 Enable the function in **Operation** list.

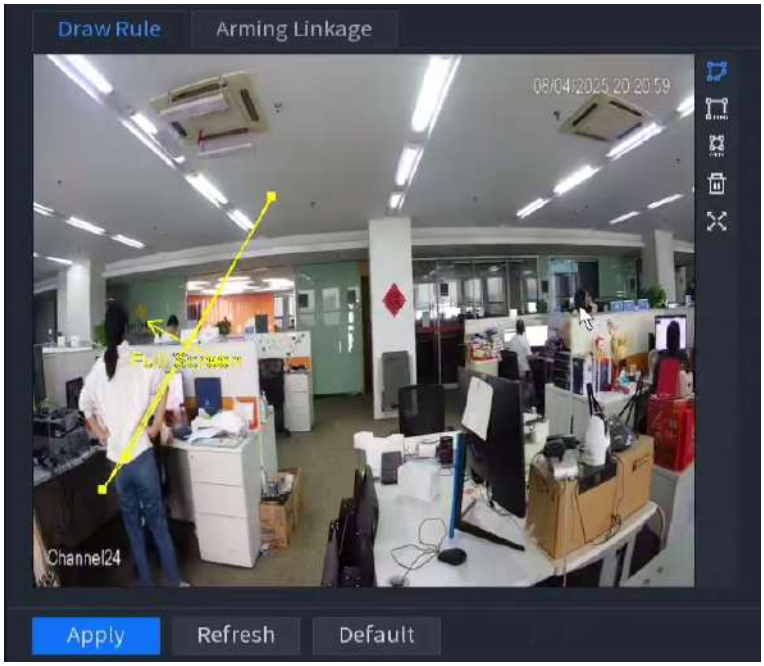
Step 6 (Only AI by recorder supports) Click **Global Config** to enable the self-learning function and configure the linked experience database.

If you haven't added an experience database, click **Experience Database** to create one. For details, see "6.1.6 Database".

Step 7 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-48 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

Table 6-6 Description of tripwire parameters

Parameter	Description
Name	Customize the rule name.
Direction	Set the tripwire direction, including A→B, B→A and A↔B.
Target Filter	Click , and then select effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

Step 8 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 9 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.3 Intrusion

When the detection target passes the edge of the monitoring area, and enters, leaves or traverses the monitoring area, the system performs an alarm linkage action.

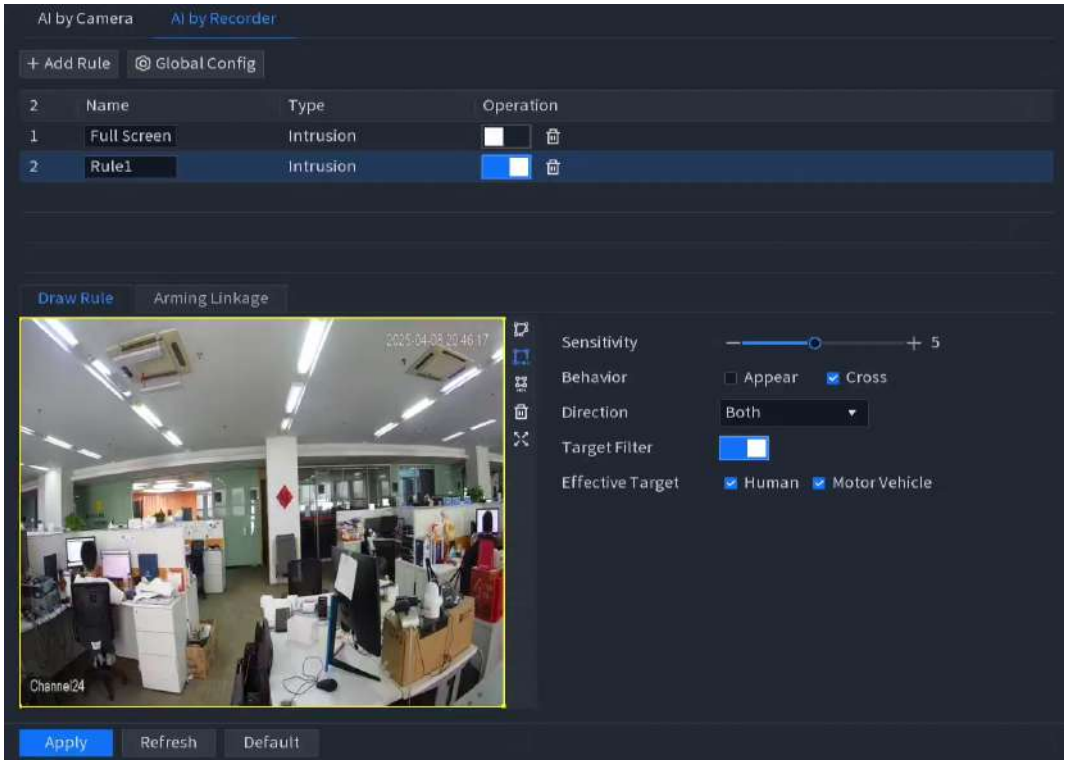
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Intrusion**.

Figure 6-49 Intrusion



Step 3 Select the preset.

This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

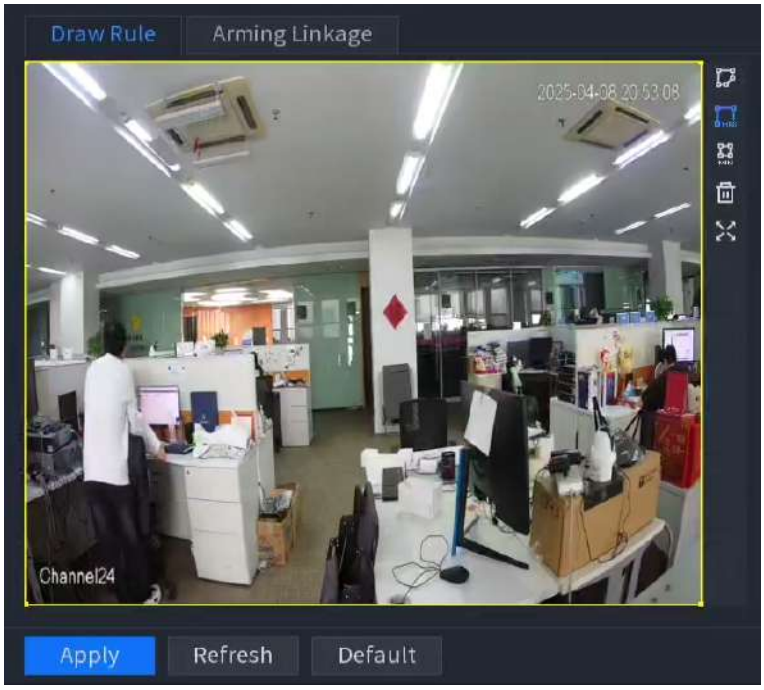
Step 5 (Only AI by recorder supports) Click **Global Config** to enable the self-learning function and configure the linked experience database.

If you haven't added an experience database, click **Experience Database** to create one. For details, see "6.1.6 Database".

Step 6 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-50 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

Table 6-7 Description of intrusion parameters

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity. The higher the value is, the easier the object that intrudes the warning area can be detected, but meanwhile the higher false alarm rate will be.
Direction	Set the direction to cross the area, including entering, exiting and both.
Target Filter	Click , and then select the effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

Step 7 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 8 Click the **Enable** checkbox, and then click **Apply**.

6.2.2.4.4 Abandoned Object

The system generates an alarm when there is an abandoned object in the specified zone.

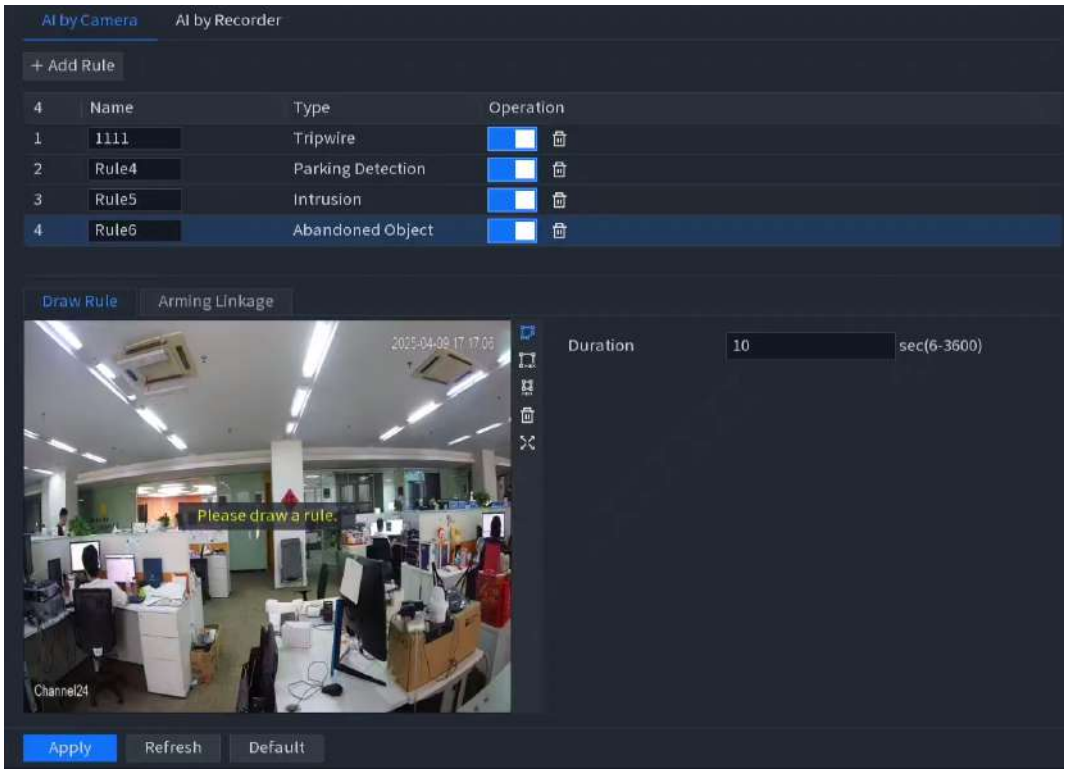
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Abandoned Object**.

Figure 6-51 Abandoned object



Step 3 Click **Add** to add a rule.

Step 4 In the **Type** list, select **Abandoned Object**.

Step 5 Select the preset.

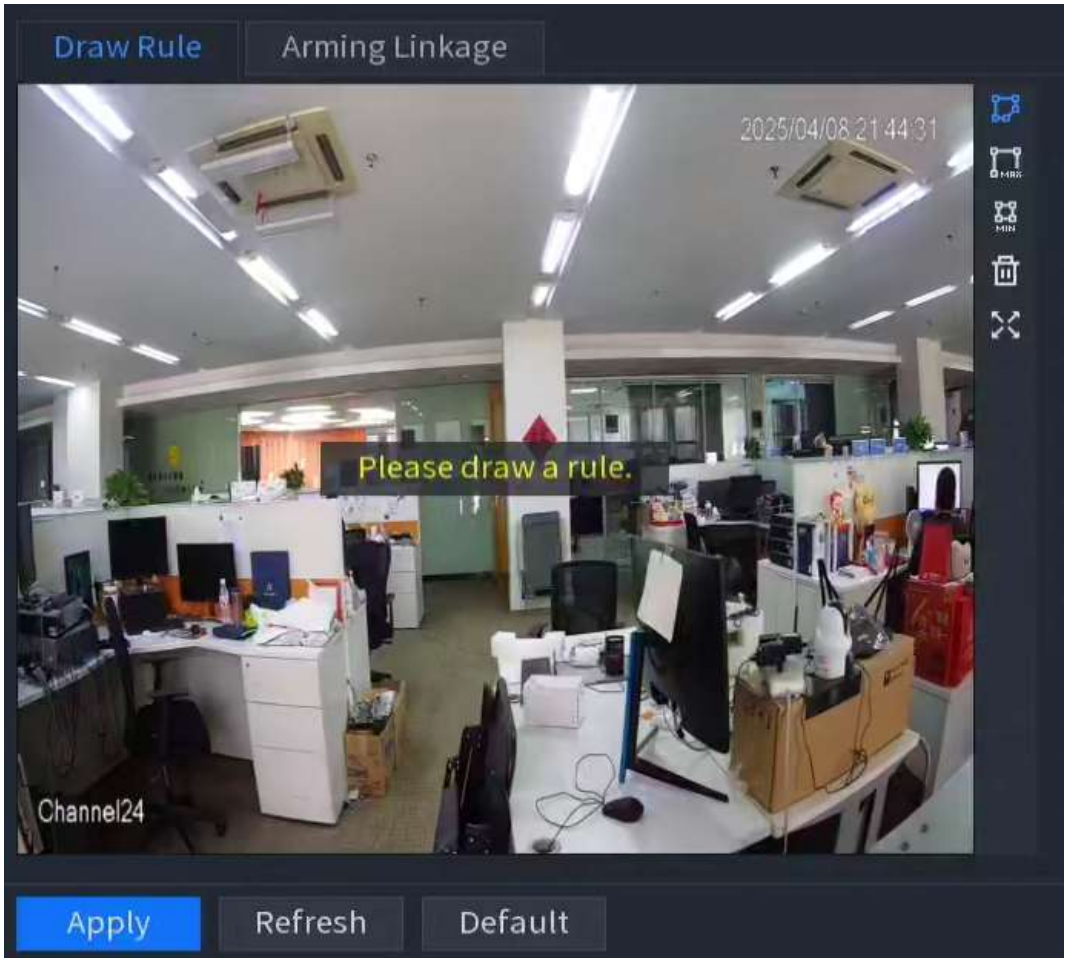
This function is only available when supported by the front-end devices.

Step 6 Enable the function in **Operation** list.

Step 7 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-52 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the detection duration period; An alarm will be triggered if the target exceeds the duration.

Step 8 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 9 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.5 Fast Moving

You can detect the fast moving object in the specified zone.

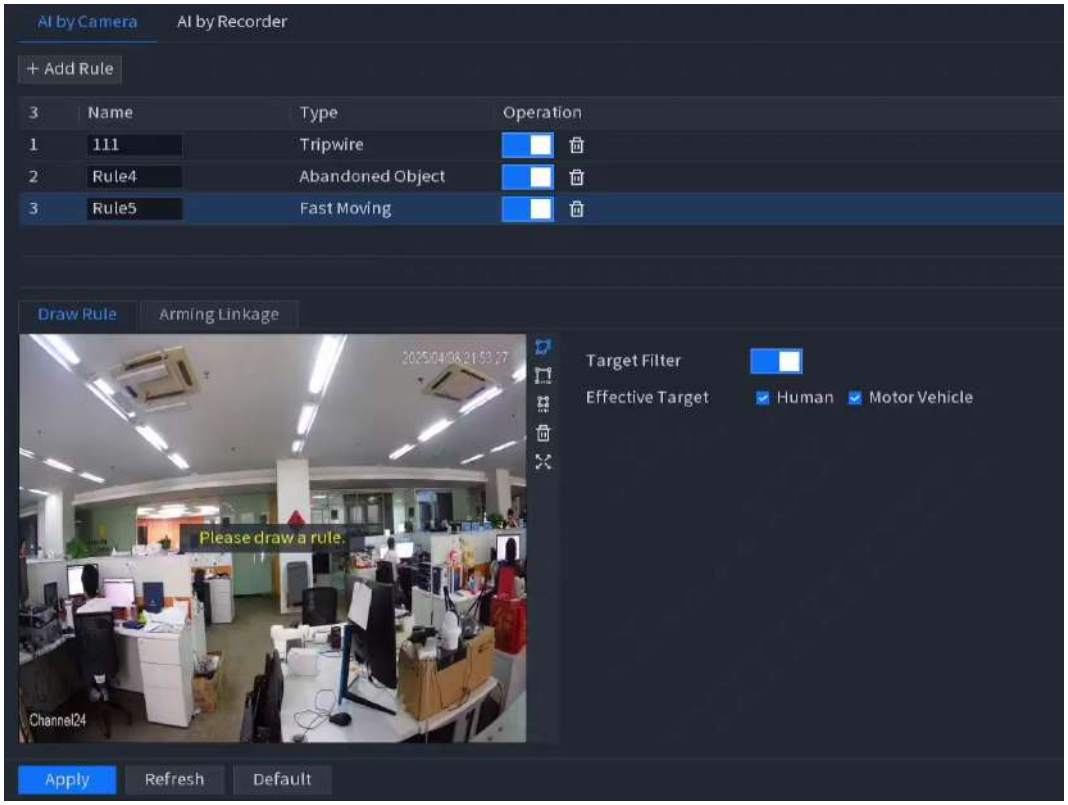
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Fast Moving**.

Figure 6-53 Fast moving



Step 3 Select the preset.

This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

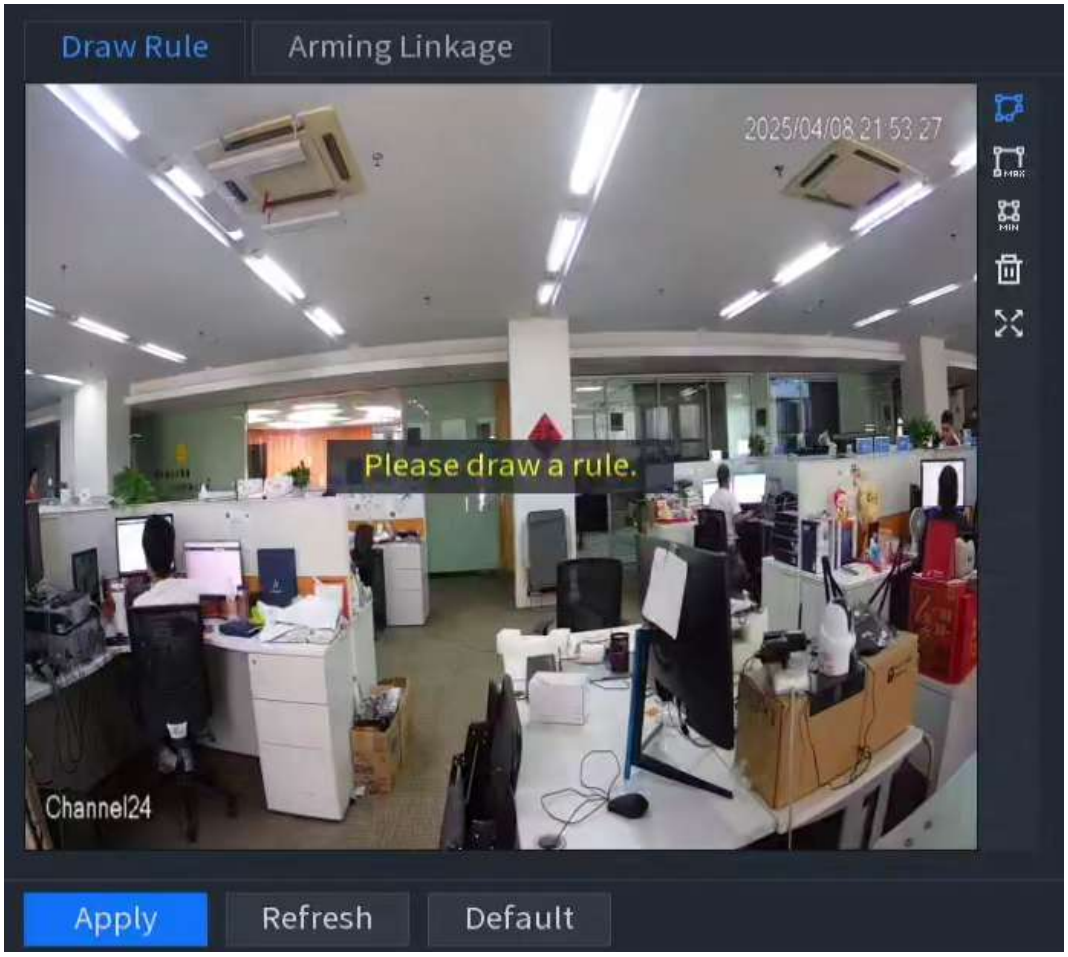
Step 5 (Only AI by recorder supports) Click **Global Config** to enable the self-learning function and configure the linked experience database.

If you haven't added an experience database, click **Experience Database** to create one. For details, see "6.1.6 Database".

Step 6 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-54 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Enable the target filter and select the effective target, with options for **Human** and **Motor Vehicle**.

Step 7 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 8 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.6 Parking Detection

When the detection target stays in the monitoring area longer than the set duration, the system performs alarm linkage action.

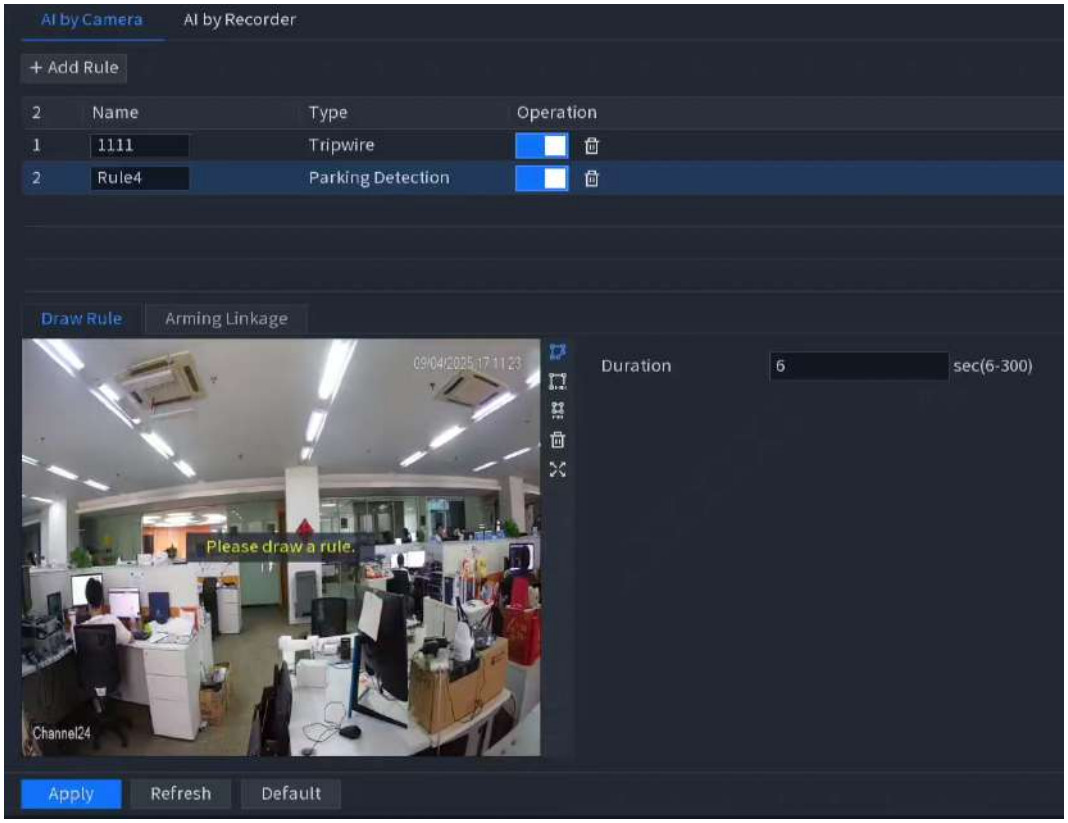
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Parking Detection**.

Figure 6-55 Parking detection



Step 3 Select the preset.

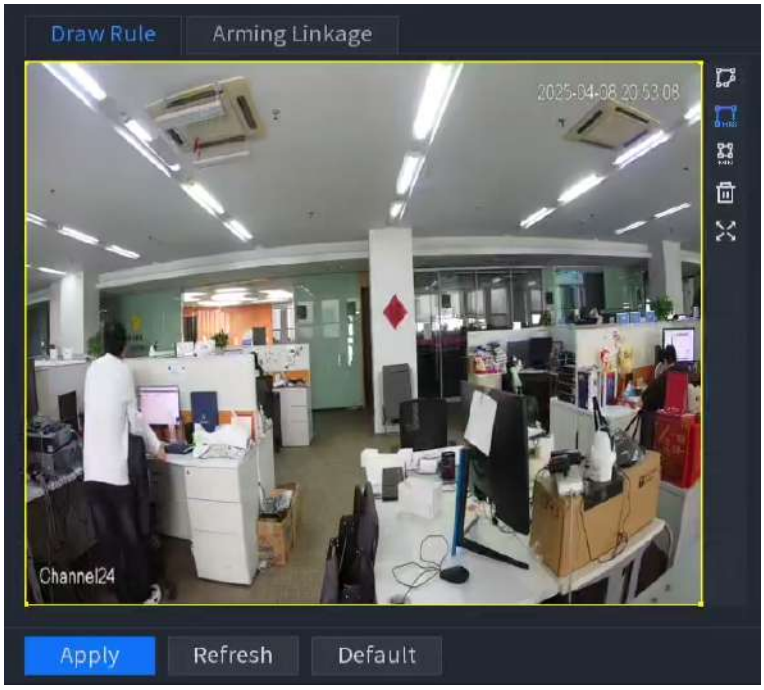
This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

Step 5 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-56 Draw rule



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the detection duration period; an alarm will be triggered if the target exceeds the duration.

Step 6 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.7 Crowd Gathering Estimation

The system generates an alarm once people are gathering in the specified zone longer than the defined duration.

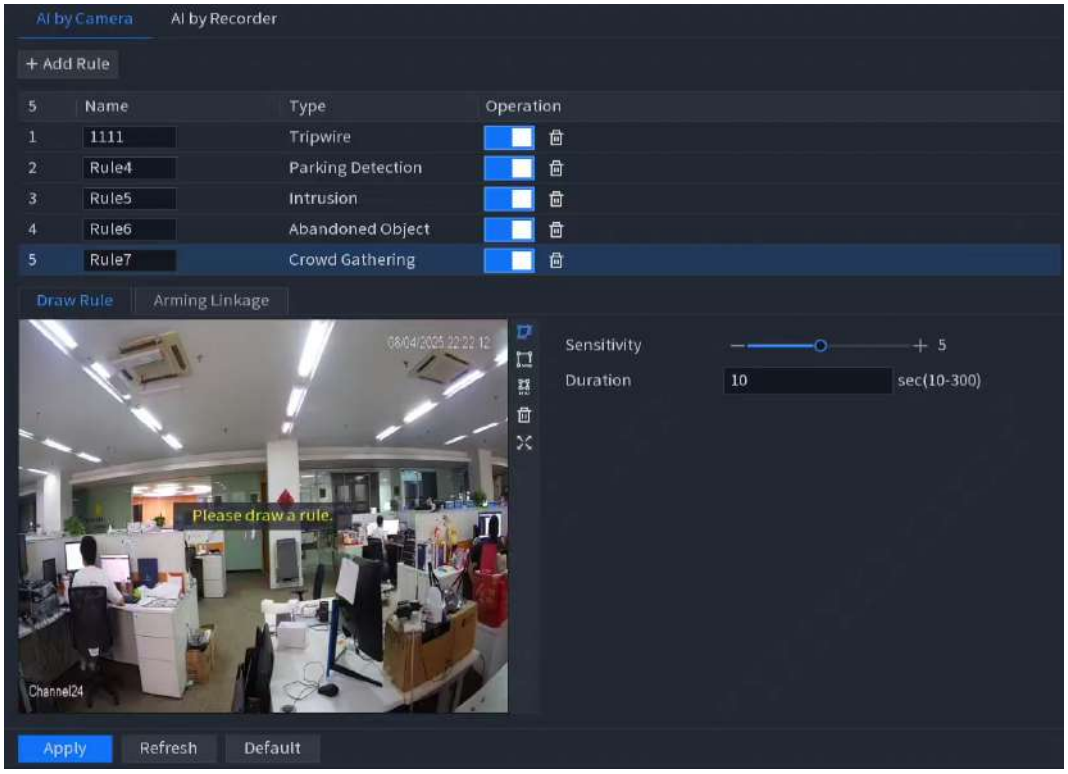
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Crowd Gathering**.

Figure 6-57 Crowd gathering



Step 3 Select the preset.

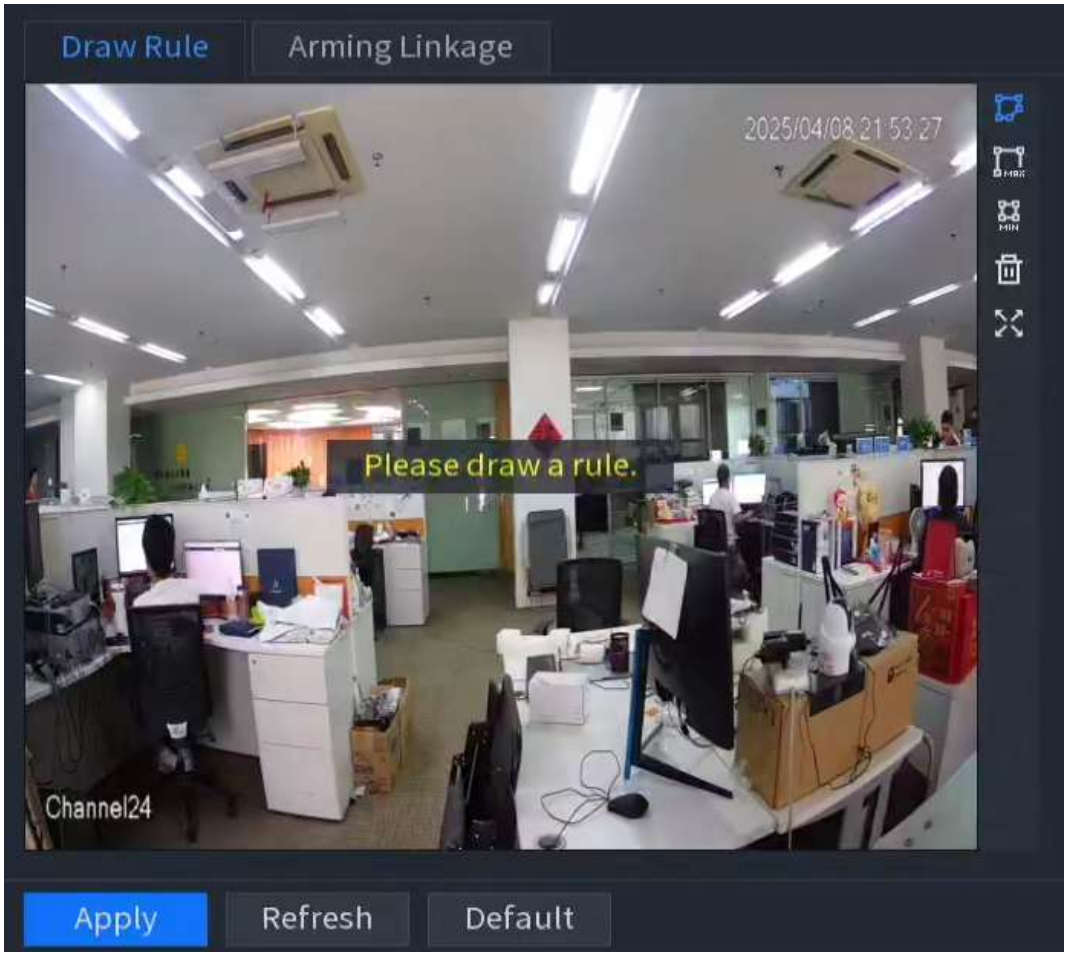
This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

Step 5 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-58 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

Table 6-8 Parameter description

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity. The higher the value, the easier it is to detect the crowd gathering but meanwhile the higher false alarm rate will be.
Duration	Set how long the crowd stays until the alarm is triggered.

Step 6 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.8 Missing Object

The system generates an alarm when there is missing object in the specified zone.

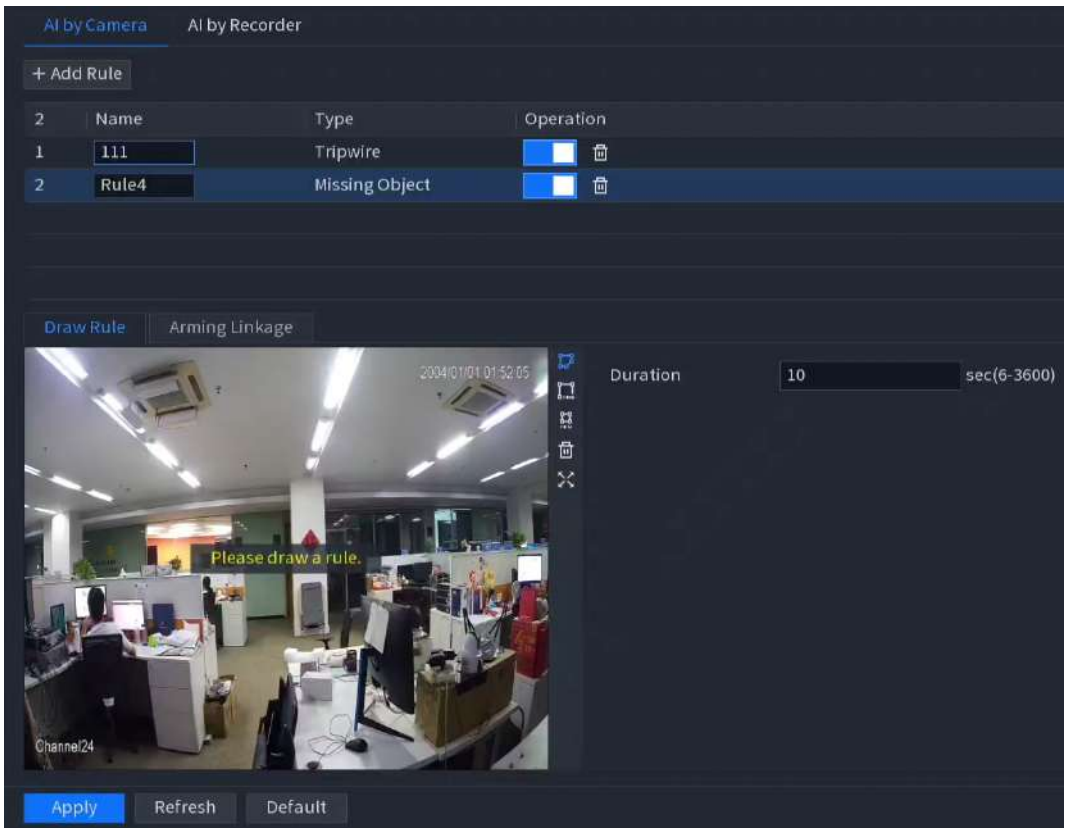
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Missing Object**.

Figure 6-59 Missing object



Step 3 Select the preset.

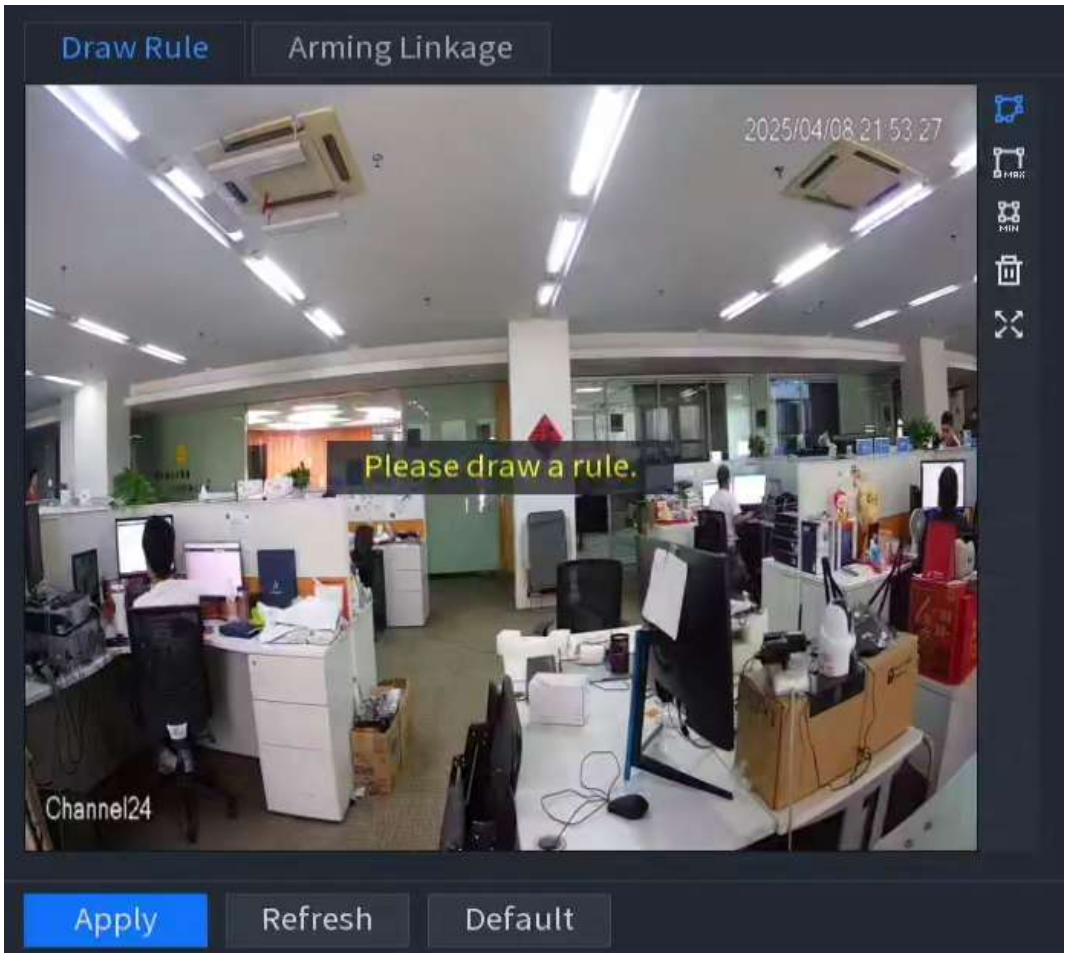
This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

Step 5 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-60 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the detection duration period; an alarm will be triggered if it exceeds the duration.

Step 6 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.4.9 Loitering Detection

The system generates an alarm once the detection target is staying in the detected zone longer than the defined duration.

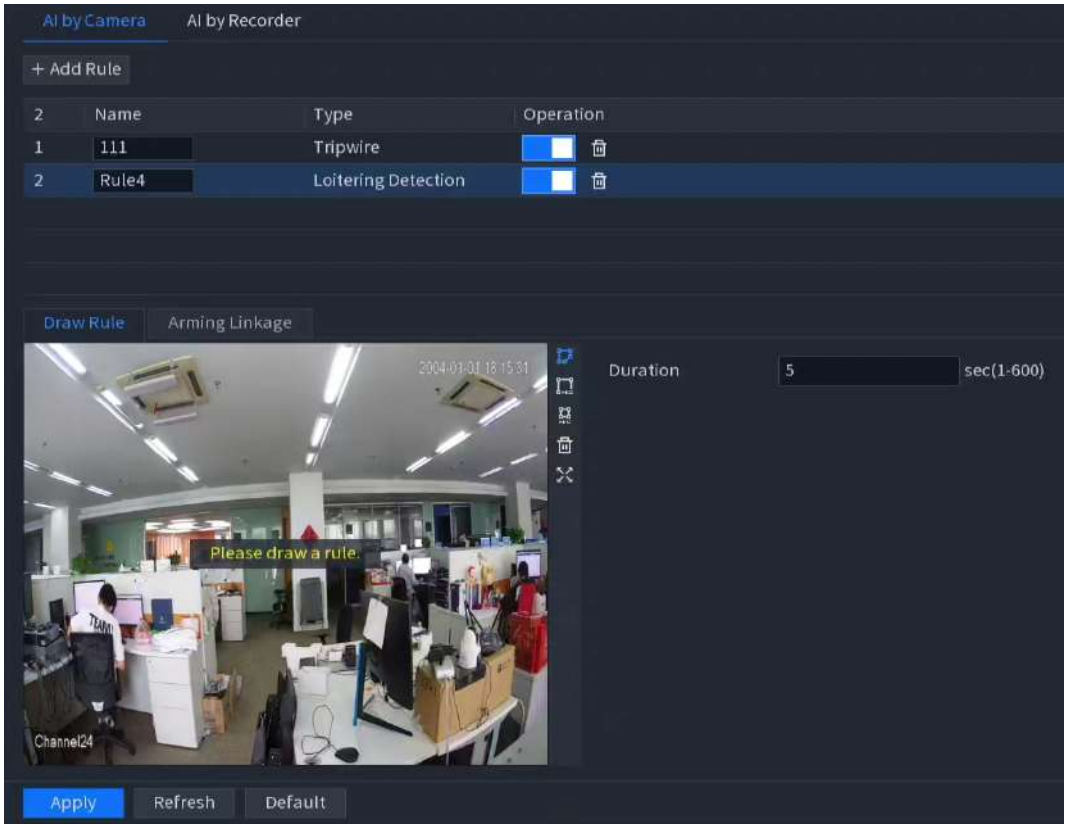
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Click **Add Rule** to select **Loitering Detection**.

Figure 6-61 Loitering detection



Step 3 Select the preset.

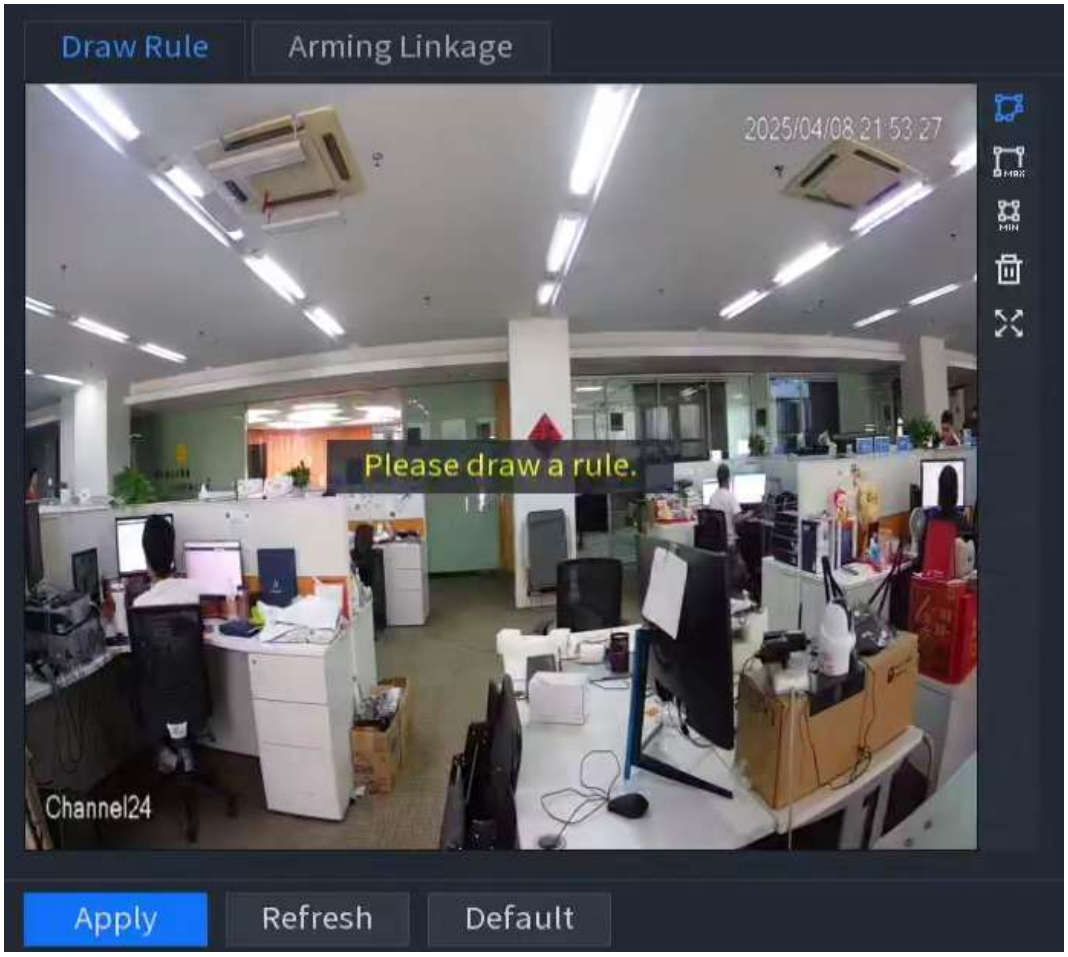
This function is only available when supported by the front-end devices.

Step 4 Enable the function in **Operation** list.

Step 5 Click **Draw Rule** to draw the detection rules.

1. Click to draw rules on the screen of the channel and right-click to finish the drawing. Click to delete any drawn detection rules.

Figure 6-62 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the detection duration period; an alarm will be triggered if it exceeds the duration.

Step 6 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Select the **Enable** checkbox, and then click **Apply**.

6.2.2.5 Face Recognition

Configure alarm rules for face recognition. Configure face recognition alarm linkage, where the detected face image is compared with the faces in the database. When the comparison results meet the predefined alarm criteria, the system performs the alarm linkage action.

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

The system compares the detected faces with the faces in the database to judge whether the detected face belongs to the database. When the similarity reaches the defined threshold, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Face Recognition**.

Step 3 Select **AI by Camera** or **AI by Recorder**.

Step 4 Enable the function.

- When you configure face database with AI by camera, if there is no available face database, see "6.1.6.1.2 Creating Remote Face Databases".
- When you configure face database with AI by recorder, if there is no available face database, see "6.1.6.1.1 Creating Local Face Databases ".

- Enable **AI by Camera**.
  1. Enable **Face Enhancement**.
  2. Configure the face similarity.
  3. Click in the operation list to enable the database.
- Enable **AI by Recorder**.
  - ◇ Select **General Alarm**.
    1. Click **Target Face Database** to add face databases.
    2. Configure the face similarity.
    3. Click in the operation list to enable the database.
  - ◇ Select **Stranger Alarm**.

    Click in the operation list to enable the database.

Step 5 Configure the alarm schedule.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.2.6 PPE Detection

Detects whether the person is wearing the workwear, hat, gloves, shoe covers and the like.

Prerequisites

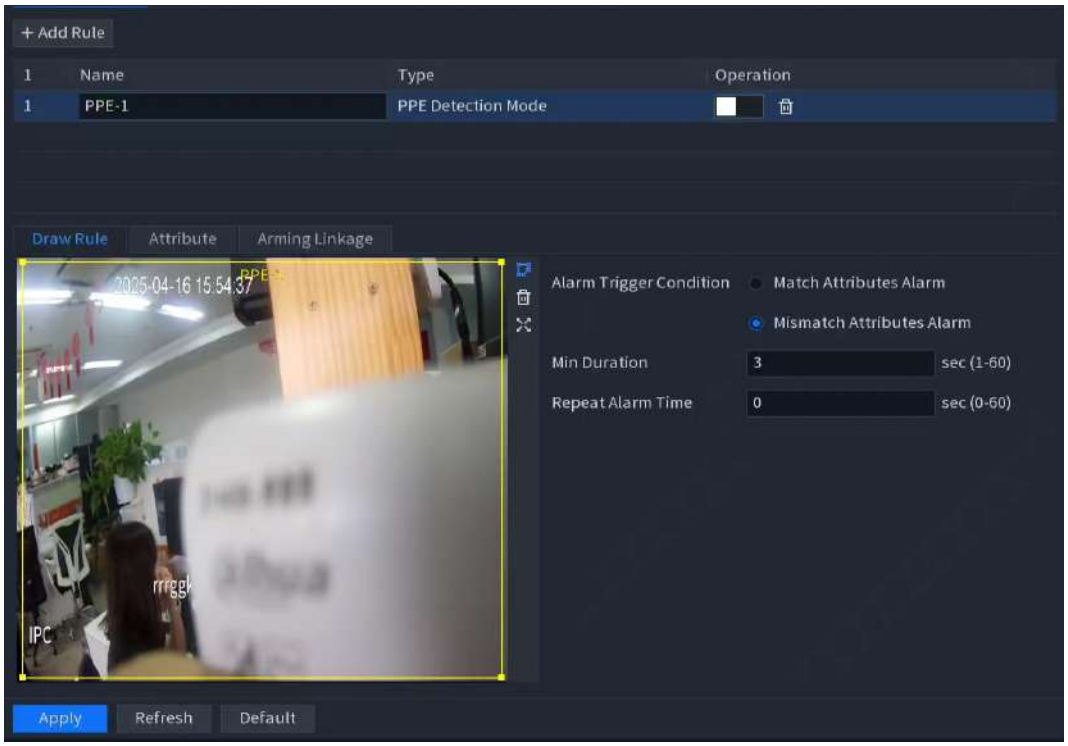
The front-end camera has AI function for PPE detection.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **PPE Detection**.

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

Figure 6-63 PPE detection



Step 3 Click in the operation list to enable the function.

Step 4 Click to configure a detection zone on the video.

- Modify the name of the rule in the list.
- Click to delete the drawn rule.
- Click to enter the full screen.

Step 5 Configure parameters for drawing rule.

Table 6-9 Draw rule parameters

Parameter	Description
Alarm Trigger Condition	Receives an alarm event according to the set rule and displays it on the live view. • Match attributes alarm: When the detected workwear matches the set attributes, an alarm is triggered. • Mismatch attributes alarm: When the detected workwear does not match the set attributes, an alarm is triggered.
Min Duration	Set the minimum time for the crowding in the detection area until an alarm is triggered.
Repeat Alarm Time	Set the repeat alarm time. If the alarm state persists, when reaching the repeat alarm time, the alarm is triggered again.

Step 6 Click the **Attribute** tab to configure the attribute parameters.

Figure 6-64 Parameters (detect by attribute)

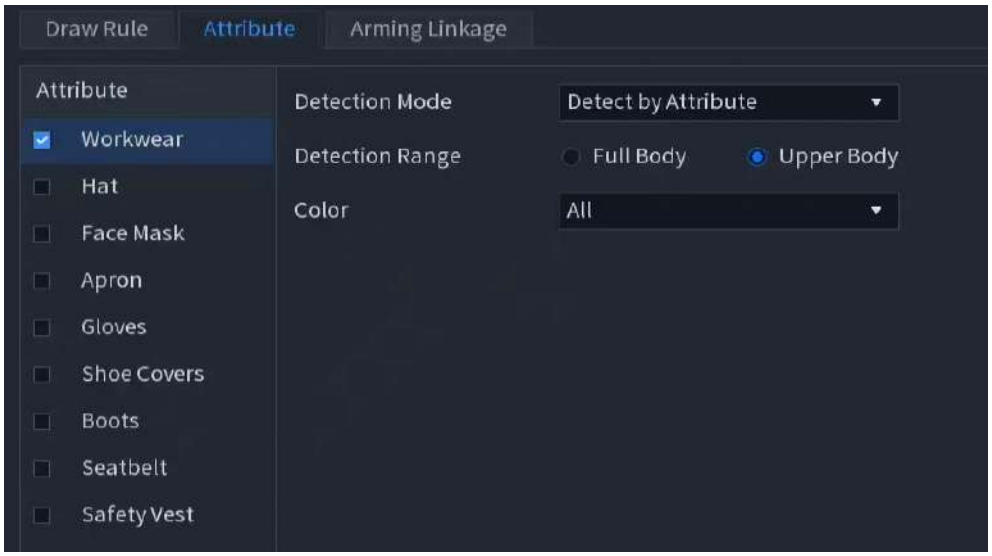


Figure 6-65 Parameters (registration mode)

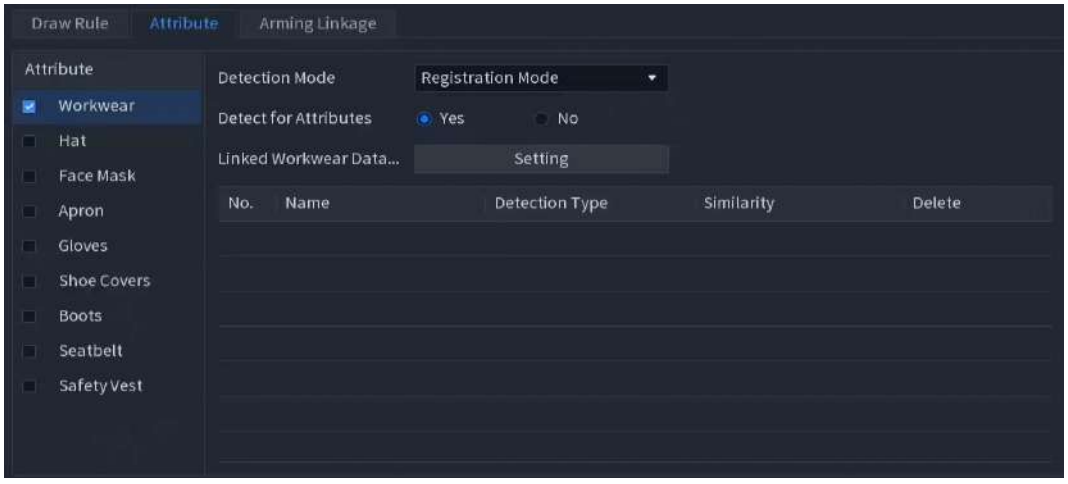


Table 6-10 Parameters description

Parameter	Description
Workwear	Select **Detection Mode**. • Detect by attribute: You need to set the detection range. • Registration mode: You need to link the workwear database that has been set for the front-end camera. Receives an alarm event based on the linked workwear database and displays it. 1. Click **Settings** next to **Linked Workwear Database**. 2. Select database, and then click **OK**.
Hat	Select **Detect for Attributes** , **Detection Range**, and **Color**.
Face Mask	Select **Detect for Attributes**.
Apron	
Gloves	
Shoe Covers	
Boots	
Seatbelt	
Safety Vest	

Step 7 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 8 Click **Apply**.

6.2.2.7 Video Metadata

When a metadata alarm is triggered, the system links the corresponding camera to record videos and logs, and then take snapshots. Other alarm linkage actions are not supported for video metadata.

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

The system analyzes real-time video stream to detect the existence of human, motor vehicle, and non-motor vehicle. Once a target is detected, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Video Metadata**.

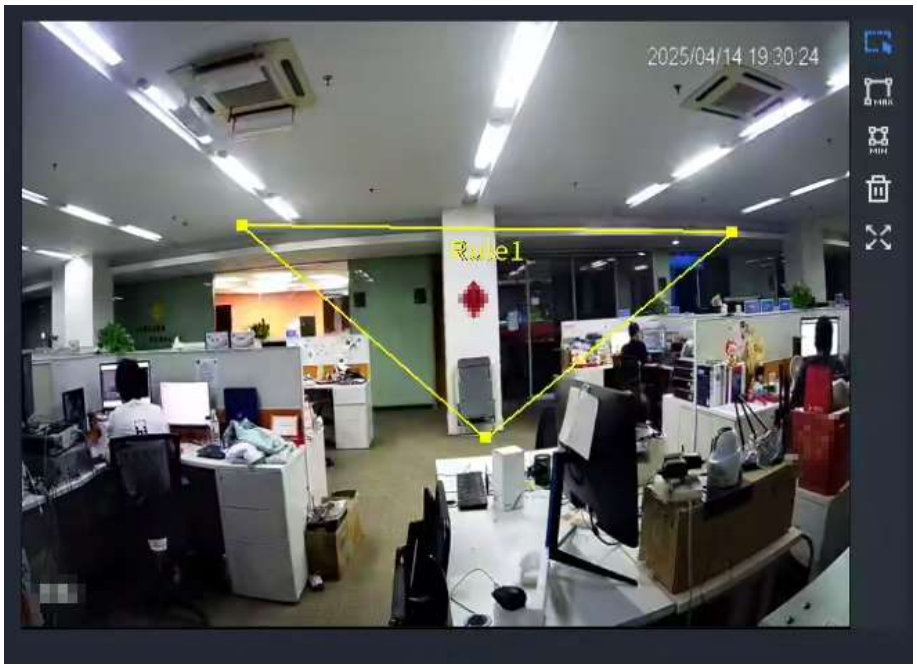
Step 3 Click **Add Rule** to add a rule.

Step 4 Enable the rule in the **Operation** list, and then set **Type** to **Human Detection**, **Non-motor Vehicle Detection** or **Motor Vehicle Detection**.

Step 5 Draw the detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing. Click to delete the rule area you drew.

Figure 6-66 Draw rules



2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

Step 6 Click **Apply**.

6.2.2.8 ANPR

The system extracts the plate number on the surveillance video, and then compare it with the specified plate information. When a match is detected, the system triggers an alarm.

Prerequisites

- To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

- For creating the vehicle allowlist and blocklist, see "6.1.6.2 Vehicle Blocklist/Allowlist".

Background Information

The system extracts the plate number on the surveillance video and then compare it with the specified plate information. When a match is detected, the system triggers an alarm.

Procedure

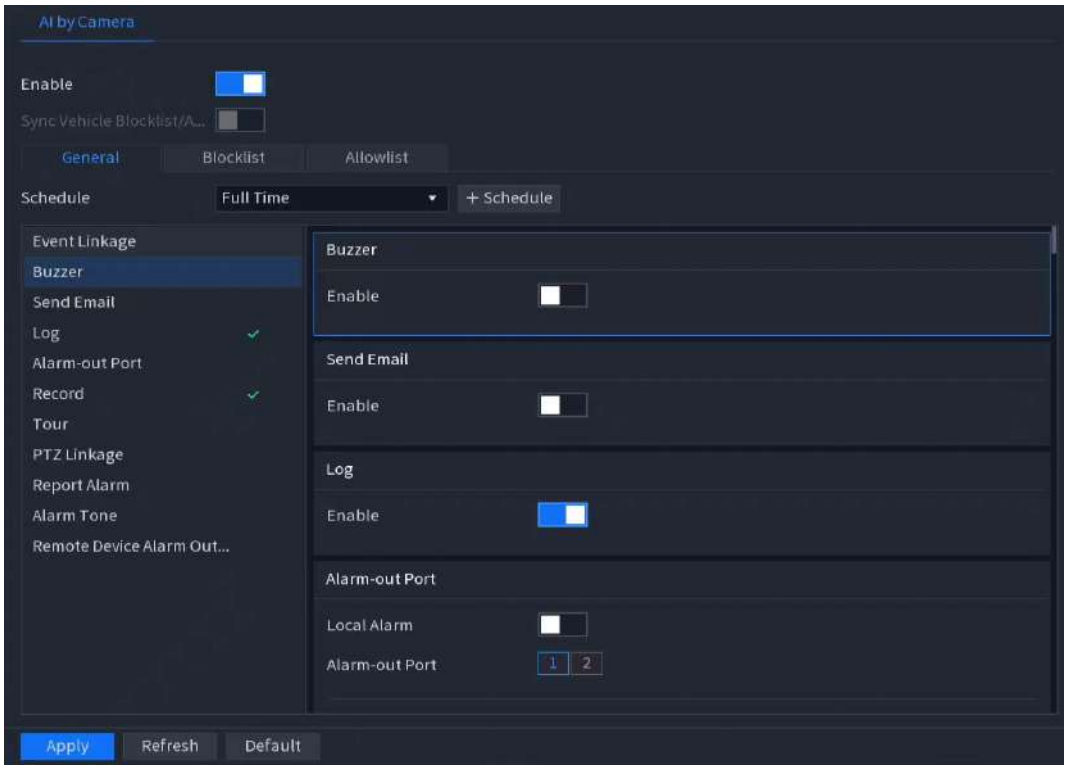
Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **ANPR**.

Step 3 Enable the ANPR function.

Figure 6-67 ANPR



Step 4 Click **General** , **Blocklist** or **Allowlist** tab.

Select **Sync Vehicle Blocklist/Allowlist** to synchronize the blocklist and allowlist of the device to the front-device end.

- General: After you set the alarm parameters under this tab, the system will trigger an alarm whenever it detects any license plate.
- Blocklist: After you set the alarm parameters under this tab, the system will only trigger an alarm when it detects a license plate that is on the blocklist.
- Allowlist: After you set the alarm parameters under this tab, the system will only trigger an alarm when it detects a license plate that is on the allowlist.

Step 5 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 6 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

6.2.2.9 Stereo Analysis

By drawing and setting the rules of stereo behavior analysis, the system can perform alarm linkage actions when the video matches the detection rule. Types of events include: people approach detection, fall detection, violence detection, people No. exception detection and people stay detection.

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

- This function requires access to a camera that supports stereo behavior analysis.
- Stereo analysis and IVS are mutually exclusive and cannot be enabled at the same time.

6.2.2.9.1 People Approach Detection

When two people stay in the same detection area longer than the defined duration or when the distance between two people is longer or shorter than the defined threshold, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **Add Rule** to select **People Approach Detection**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-11 Parameters of people approach detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity. The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.
Stay Time	Set how long two people stay in the same detection area until an alarm is triggered.
Repeat Alarm Time	Set the repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.
2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.2 Fall Detection

When someone falls from a height in the detection area and the duration of the action is greater than the defined threshold, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **+ Add Rule** to select **Fall Detection**.

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

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-12 Parameters of fall detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity. The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.
Duration	Set how long people fall in the same detection area until an alarm is triggered.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3. Click **OK**.

Step 5 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is triggered during the designated time.
2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 6 Click **Apply**.

6.2.2.9.3 Violence Detection

When the target in the detection region has grand body movements such as smashing and fighting, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **Add Rule** to select **Violence Detection**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-13 Parameters of violence detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.4 Abnormal Number of People Detection

When the system detects an abnormal number of people in the same detection area, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **Add Rule** to select **Abnormal Number of People Detection**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-14 Parameters of abnormal number of people detection

Parameter	Description
Name	Customize the rule name.

Parameter	Description
Sensitivity	Set the alarm sensitivity. The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.
Duration	Set the minimum time to trigger an alarm after the system detects an abnormal number of people.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.
Alarm People No.	Define the number of **Human** from zero to ten, and when the number of people in the area is greater than, equal to, or less than the defined threshold, an alarm is triggered.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.5 People Stay Detection

When the target stays in the detection area longer than the defined duration, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **Add Rule** to select **Abnormal Number of People Detection**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-15 Parameters of people stay detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set the alarm sensitivity. The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur..
Duration	Set low long people stay in the detection area until an alarm is triggered.
Repeat Alarm Time	Set the repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.6 Running Detection

When the target runs in the detection area, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **+ Add Rule** to select **Running Detection**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-16 Parameters of running detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.7 Warning Area Intrusion

When the detection target enters or exits the edge of the warning area, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **+ Add Rule** to select **Warning Area Intrusion**.

Step 3 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-17 Parameters of warning area intrusion

Parameter	Description
Name	Customize the rule name.
Direction	Set the direction to cross the area, including enter, exit and both.
Sensitivity	The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click + Schedule to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.
2. Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.9.8 Crossing Warning Line

When the target crosses warning line in the detection area, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Stereo Analysis**.

Step 2 Select a channel, and then click **Add Rule** to select **Crossing Warning Line**.

Step 3 Draw the detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 6-18 Parameters of crossing warning line

Parameter	Description
Name	Customize the rule name.
Direction	Dual direction is supported including from A to B and B to A.
Sensitivity	The higher the value, the easier it is to trigger an alarm. But meanwhile, the false alarm might occur.

3. Click **OK**.

Step 4 Click **Arming Linkage**.

1. Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 5 Click **Apply**.

6.2.2.10 Crowd Distribution

The system detects the crowd distribution. When the crowd density exceeds the defined threshold, an alarm is triggered.

Prerequisites

- To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".
- Make sure that the connected camera supports the crowd distribution function.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT** > **AI Settings** > **Crowd Distribution**.

Step 2 Click next to **Enable** to enable this function.

Step 3 (Optional) Enable **Crowd Density (Global)**.

Step 4 Enter the crowd density.

The unit is expressed in humans per square meter.

Step 5 Configure parameters.

Table 6-19 Crowd distribution parameters

Parameter	Description
Crowd Density (Global)	Click , and then configure the density threshold.
Crowd Density	

Step 6 Configure the schedule plan and event linkage.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the arming schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After you set the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

2. Set up alarm linkage actions. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

6.2.2.11 People Counting

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

An alarm is triggered when the number of people entering, leaving, passing or staying in the detection area exceeds the defined threshold.

Make sure that the connected camera supports people counting.

6.2.2.11.1 Configuring People Counting

The system supports counting the number of entry, exit, and staying people in the detection area. When the number exceeds the threshold, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

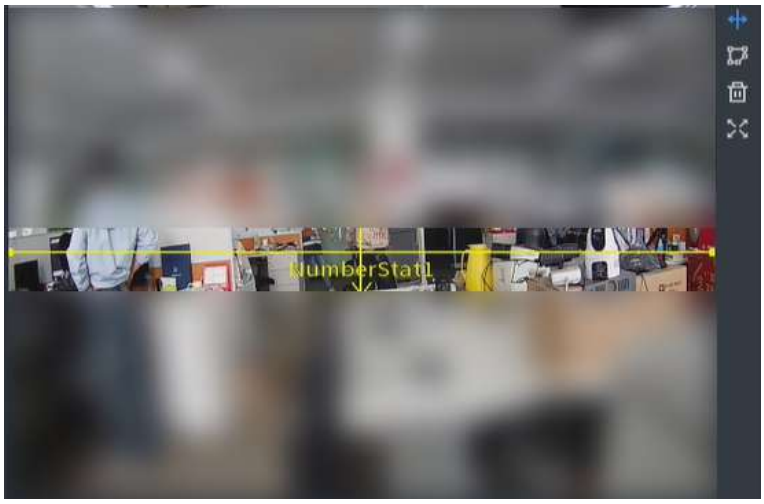
Step 2 Select **AI Settings** > **People Counting**.

Step 3 Click **Add Rule** to select **People Counting** and enable the rule in the **Operation** list.

Step 4 Click the **Draw Rule** tab.

1. Click , and then draw a line on the video image. Right-click the image to stop drawing. Click to delete the rule line you drew.

Figure 6-68 Draw the rule



2. Draw a detection area.

Click to draw a detection box and adjust its size and position.

In the drawing state, click to delete the drawn filter boxes.

3. Configure the parameters.

Table 6-20 People counting parameters

Parameter	Description
OSD	Click **Reset** next to **OSD** to clear the data of people counting.
Enter No.	An alarm is triggered when the number of people entering the detection zone exceeds the defined threshold.
Exit No.	An alarm is triggered when the number of people leaving the detection zone exceeds the defined threshold.
Stay No.	An alarm is triggered when the number of people staying the detection zone exceeds the defined threshold.
Pass No.	An alarm is triggered when the number of people passing the detection zone exceeds the defined threshold.

Step 5 Select the **Arming Linkage** tab.

Step 6 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 7 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 8 Click **Apply**.

6.2.2.11.2 Configuring Area People Counting

When the number of people in the detection area is larger or lower than the defined threshold, or when the staying period exceeds the defined duration, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **People Counting**.

Step 3 In the **People Counting** tab, click **Add Rule** to select **Area People Counting** and enable the rule in the **Operation** list.

Step 4 Click the **Draw Rule** tab.

1. Draw a detection area.

Click to draw a detection box and adjust its size and position.

Figure 6-69 Rule configuration

In the drawing state, click to delete the drawn filter boxes.

2. Configure the parameters.

Table 6-21 Area people counting parameters

Parameter	Description
Type	Configure the alarm detection type, with options for **GreaterEqual** , **LessEqual**, **= Threshold** and **≠ Threshold**.
In Area No.	Set the threshold for the number of people in the area. An alarm will be triggered if the number of people does not meet the threshold limit of the selected type.
Stay Time	Enter the staying time. An alarm will be triggered when the time people spend in the area exceeds the set value.

Step 5 Select the **Arming Linkage** tab.

Step 6 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 7 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 8 Click **Apply**.

6.2.2.11.3 Configuring Queuing

After configuring queuing alarm, the system can realize the corresponding linkage actions once the number of people in the queue or the waiting time has triggered an alarm.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **People Counting**.

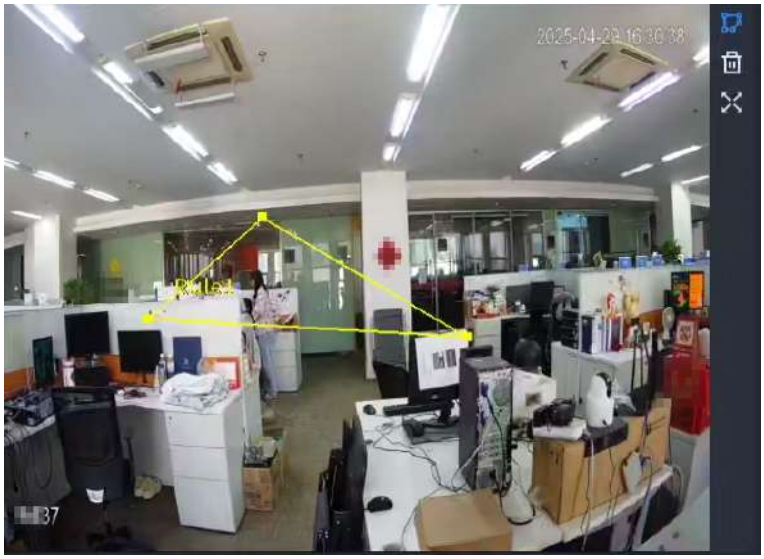
Step 3 In the **Queuing** tab, click **+ Add Rule** to select **Queuing** and enable the rule in the **Operation** list.

Step 4 Click the **Draw Rule** tab.

1. Draw a detection area.

   Click to draw a detection box and adjust its size and position.

Figure 6-70 Rule configuration



In the drawing state, click to delete the drawn filter boxes.

2. Enable **Queue People No. Alarm** or **Queue Time Alarm** and configure the parameters.

Table 6-22 Queuing parameters

Parameter	Description
Type	Configure the alarm detection type, with options for **GreaterEqual** , **LessEqual**, **= Threshold** and **≠ Threshold**.
Queue Time Alarm	Set the threshold for the number of people in line. An alarm will be triggered if the count does not meet the threshold limit of the selected type.
Queue Time	Enter the queuing time. An alarm will be triggered when the time people spend in the area exceeds the set value.

Step 5 Select the **Arming Linkage** tab.

Step 6 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is triggered during the designated time.

Step 7 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 8 Click **Apply**.

6.2.2.12 Heat Map

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

The Device can monitor the distribution of active objects in the detection area during a period of time, and display the objects on the heat map in different colors.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Heat Map**.

Step 3 Enable the function, select the schedule drop-down list, and then click **Schedule** to configure the alarm schedule. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 4 Click **Apply**.

6.2.2.13 Text-Defined Alarms

Deploy the rules generated from text-defined content onto the desired channels to enable intelligent detection.

Prerequisites

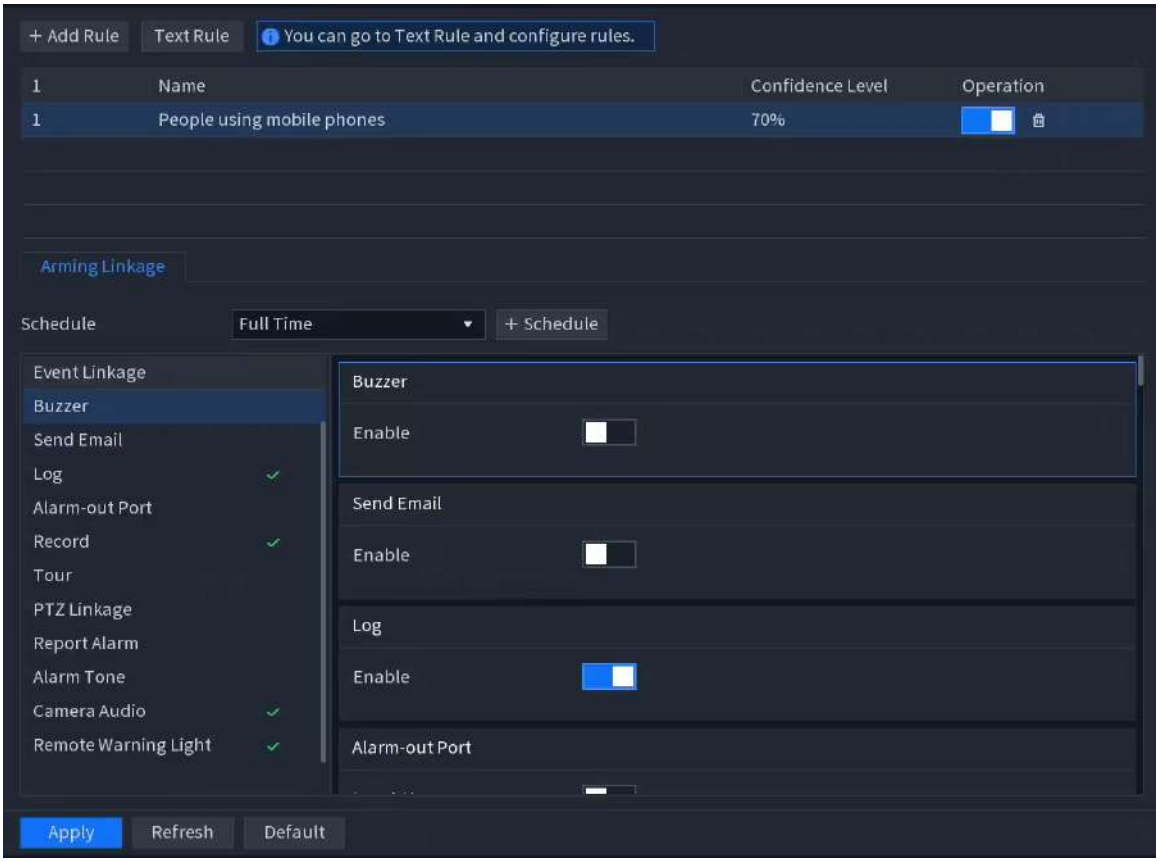
- For creating rules, see "6.1.4 Text Rule".
- For clicking to add the Wizseek target as the text rule, see "11 Wizseek".

Procedure

Step 1 Log in to the main menu, select **SETTINGS** > **EVENT**.

Step 2 Click one remote device channel, and then click **Text-Defined Alarms**.

Figure 6-71 Text-defined alarms



Step 3 Click **Add Rule** to select an existing rule.

Click **Text Rule** to go to the page to create new rules if there are no applicable rules.

Step 4 Enable the rule in the **Operation** list.

Step 5 Click the **Arming Linkage** tab.

1. Click the schedule drop-down list to select an existing alarm schedule.

   Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

   After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 6 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

6.2.2.14 Vehicle Density

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Background Information

You can configure the rules for traffic congestion and parking upper limit, and view the counting data on the live view.

- Traffic congestion: The system counts the vehicles in the detection area. When the counted vehicle number and the continuous congestion time exceed the configured values, an alarm is triggered and the system performs an alarm linkage.
- Parking upper limit: The system counts the vehicles in the detection area. When the counted vehicle number exceeds the configured value, an alarm triggered and the system performs an alarm linkage.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Vehicle Density**.

Step 3 Click **Add Rule** and enable the rule in the **Operation** list.

You can select **Traffic Congestion** or **Parking Upper Limit**.

Step 4 Click the **Draw Rule** tab and draw the detection rule.

1. Click to draw the rule on the video image. Right-click the image to stop drawing.

   Click to delete the rule area you drew.

Figure 6-72 Draw rules

2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

   In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the minimum duration; if it exceeds the threshold after the object is left or taken, an alarm will be triggered.

Step 5 Click **Apply**.

6.2.2.15 Smart Object Detection

You can configure rules and set parameters. When someone is taking or placing an item in the monitoring area, an alarm is triggered.

Prerequisites

To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Smart Object Detection**.

The target type includes luggage, bag, box, and non-motor vehicle.

Step 3 Click **Add Rule** and enable the rule in the **Operation** list.

You can select **Smart Abandoned Object** and **Smart Missing Object**.

Step 4 Click the **Draw Rule** tab and draw the detection rule.

1. Click to draw the rule on the video image. Right-click the image to stop drawing.

   Click to delete the rule area you drew.

Figure 6-73 Draw rules

2. Draw a filter box.

   Click to draw the maximum size filter box, click to draw the minimum size filter box, and then adjust their size and position.

   After you set the maximum and minimum sizes for the detection target, the alarm will only be triggered when the size of the detection target is between the minimum and maximum sizes.

In drawing mode, click to delete the drawn filter box.

3. Configure the parameters.

   Set the minimum duration; if it exceeds the threshold after the object is left or taken, an alarm will be triggered.

Step 5 Select the **Arming Linkage** tab.

Step 6 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 7 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 8 Click **Apply**.

6.2.2.16 Smart Sound Detection

When the detected sound matches the alarm rules, an alarm is triggered.

Prerequisites

- To use AI by camera, you need to enable the smart plan first. For details, see "6.2.2.2 Configuring Smart Plan".
- Ensure that the camera can detect the sound.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **EVENT**.

In **Device List**, click the remote device channel.

Step 2 Select **AI Settings** > **Smart Sound Detection**.

Step 3 Enable the function, and then elect sound type, sensitivity, and threshold as needed.

Table 6-23 Parameters of smart sound detection

Parameter	Description
Sound Type	Select **Glass Breaking** , **Scream** or **All**.
Sensitivity	Set the alarm sensitivity. The higher the value, the easier to detect the smart sound but meanwhile the higher false alarm rate will be.
Threshold	When the sound level exceeds the threshold, an alarm is triggered.

Step 4 Select the **Arming Linkage** tab.

Step 5 Click the schedule drop-down list to select an existing alarm schedule.

Click **Schedule** to add the alarm schedule and set the period. For details, see "6.1.5.6 Arming Schedule".

After setting the alarm period, the system will only trigger the corresponding alarm if an alarm is activated during the designated time.

Step 6 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 7 Click **Apply**.

7 Searching Events and Reports

7.1 Event Center

7.1.1 Searching Real-Time Events

In the main menu, select **APPLICATIONS** > **EVENT CENTER** > **Real-Time Events**.

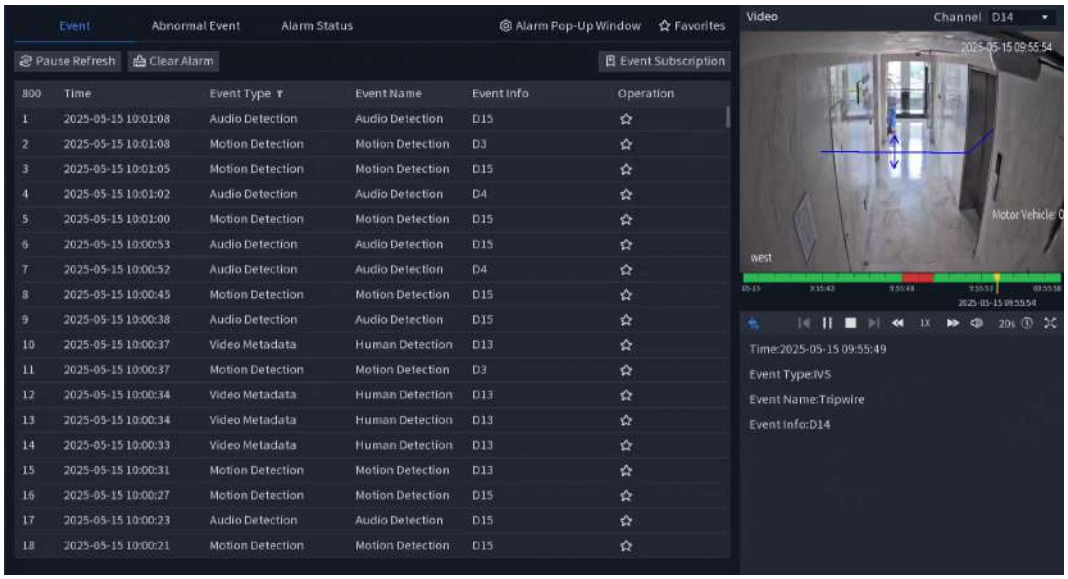
- **Refresh/Pause Refresh** : Enable real-time refresh or pause real-time refresh recording.
- **Clear Alarm** : Clear the alarm records of the current page.
- **Event Subscription** : Click to select the subscribed events; only the subscribed events will display records.
- **Alarm Pop-Up Window** : Click to choose whether to enable alarm pop-up windows and set the duration for the pop-up display.
- **Favorites** : Click to view the saved event records.

Event

1. Click **Event** to view the event history.
2. Click the event and view the event replay records on the right side.

   For the playback control, see Table 5-2 .
3. Click to collect event records.

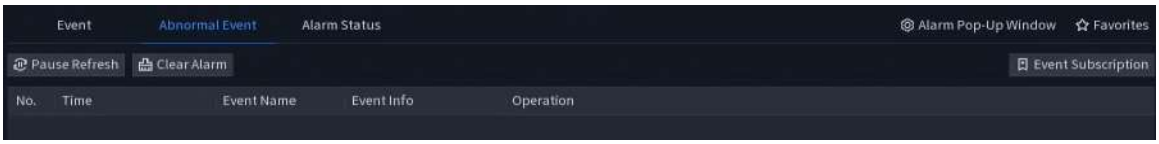
Figure 7-1 View alarm events



Abnormal Event

1. Click **Abnormal Event** to view the event records.
2. Click to collect the event records.

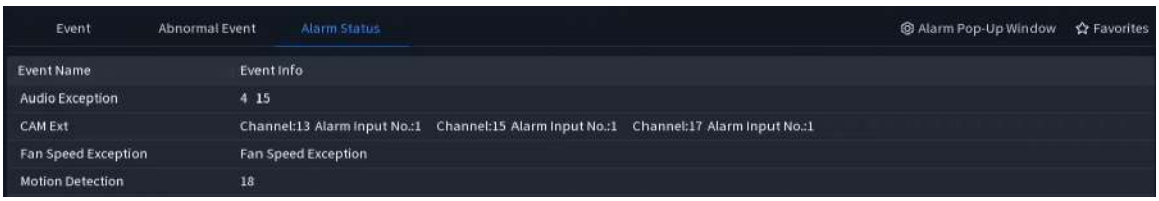
Figure 7-2 View abnormal events



Alarm Status

Click **Alarm Status** to view the event information.

Figure 7-3 View the alarm status



7.1.2 Searching Event History

Procedure

Step 1 In the main menu, select **APPLICATIONS** > **EVENT CENTER** > **Event History**.

Step 2 Select the event type.

- **All** : Search all events of the Device.
- **Abnormal Event** : Search the Device's own abnormal events, such as network disconnection.
- **AI Event** : Search all detection events related to AI features.
- **Alarm Event** : Search all local alarms, alarm box events, network alarm events, and custom alarm events.

Step 3 Select the searching type. You can select **All** , **Disk**, **Network** and **Device**.

When you select **AI Event** in **Type**, selection is not available in **Event Type**.

Step 4 Configure the searching period.

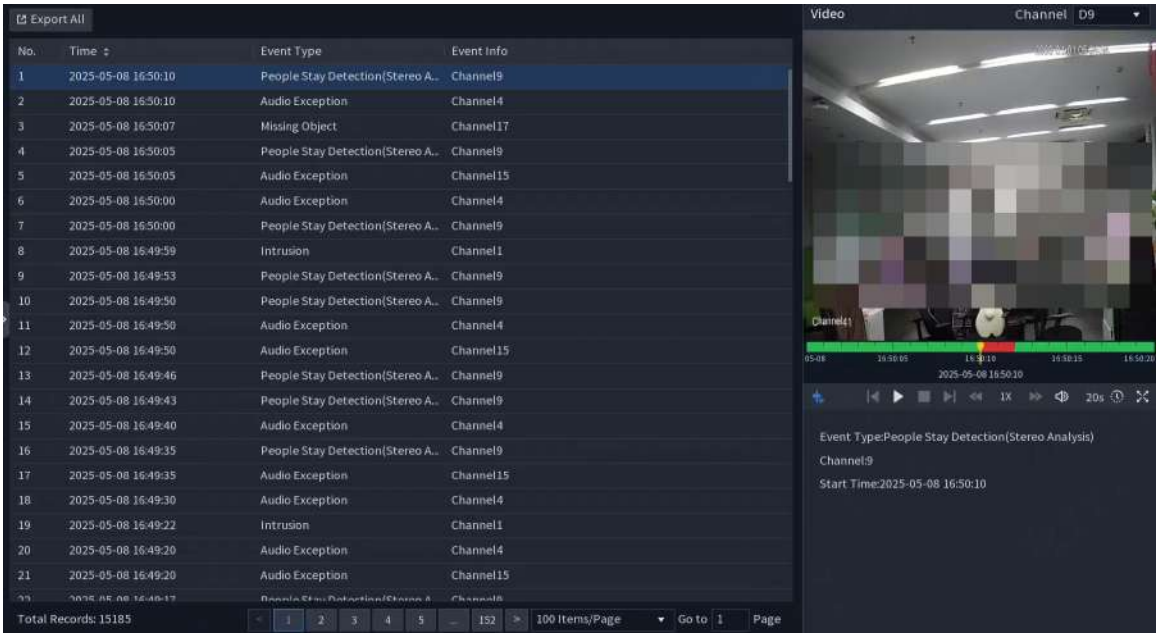
Quick search for today's, yesterday's, and the past 2, 3, or 7 days of data is supported.

Step 5 Click **Search**.

Click **Export All** to export the search results.

For the playback control, see Table 5-2 .

Figure 7-4 Search results



7.2 Report Search

7.2.1 Face Statistics

Search for face statistics reports within a specified time period, and also support exporting the facial statistics reports.

Background Information

- Data follows the principle of full coverage; We recommend you back it up in a timely manner based on need.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on the external storage media can be deleted using methods such as formatting. Please be advised.

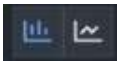
Procedure

Step 1 In the main menu, select **AI REPORT** > **Face Statistics**.

Step 2 Select the report type, and then set the time range.

Step 3 Click **Search**.

Related Operations

- Click  to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

7.2.2 People Counting

Search for the people counting report within a specified channel and time period, and also support exporting the people counting report.

Background Information

- Data follows the principle of full coverage; We recommend you back it up in a timely manner based on need.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on the external storage media can be deleted using methods such as formatting. Please be advised.

Procedure

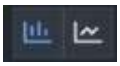
Step 1 In the main menu, select **AI Report** > **People Counting**.

Step 2 Select the channel in the channel list, select the counting rule, counting type, stay time, region and report type, and then set the time range.

The search range cannot exceed 24 hours.

Step 3 Click **Search**.

Related Operations

- Click  to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

7.2.3 Crowd Density

Search for crowd density reports within a specified channel and time period, with the option to export the crowd density report as well.

Background Information

- Data follows the principle of full coverage; it is recommended to back it up in a timely manner based on need.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on the external storage media can be deleted using methods such as formatting.

Procedure

Step 1 In the main menu, select **AI Report** > **Crowd Density**.

Step 2 Select the channel and report type, set time range, and then click **Search**.

Related Operations

- Click to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

7.2.4 Vehicle Density

Search for vehicle density reports within a specified channel and time period, with the option to export the vehicle density report as well.

Background Information

- Data follows the principle of full coverage; it is recommended to back it up in a timely manner based on need.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on the external storage media can be deleted using methods such as formatting.

Procedure

Step 1 In the main menu, select **AI Report** > **Vehicle Density**.

Step 2 Select the channel and report type, set time range, and then click **Search**.

Related Operations

- Click to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

7.2.5 Video Metadata

Search for video metadata reports within a specified channel and time period, with the option to export the video metadata report as well.

Background Information

- Data follows the principle of full coverage; it is recommended to back it up in a timely manner based on need.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on the external storage media can be deleted using methods such as formatting.

Procedure

Step 1 In the main menu, select **AI Report** > **Video Metadata**.

Step 2 Select the channel, direction and report type, set time range, and then click **Search**.

Related Operations

- Click to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

7.2.6 Heat Map

Search for and view heatmap reports for a specified channel, with the option to export the heatmap report. The heatmap queries are divided into general and fisheye.

Background Information

- **General** : Query the heatmap report for general cameras.
- **Fisheye** : Query the heatmap report for the number of people captured by the fisheye camera. It is necessary to ensure that the fisheye camera supports and has enabled the people counting function.

Procedure

Step 1 In the main menu, select **AI Report** > **Heat Map**.

Step 2 Select the channel, heat map type, set the time range, and then click **Search**.

Related Operations

- Click to change the display form of statistics.
- Export statistics

  Click **Export**, select the file type and export the statistics in the form of the picture or excel.

8 Backup

8.1 Video Backup

Procedure

Step 1 In the main menu, select **BACKUP** and click to enter the video backup page.

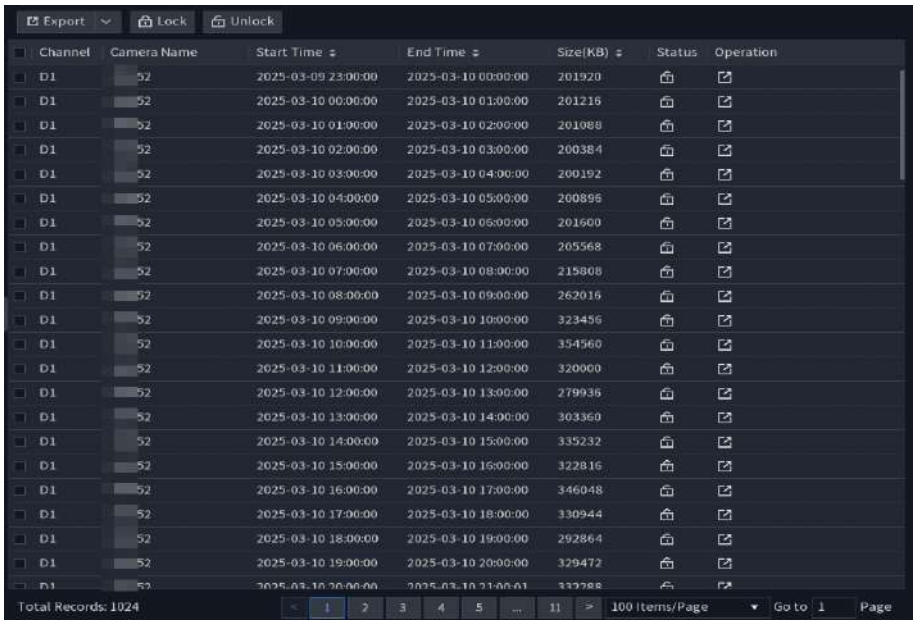
Step 2 Select the video type, stream type and file status, and then set the time range.

Step 3 Select the channel in the channel list and click **Search**.

Step 4 Select the video files to be backed up.

Step 5 Click **Export** or in the operation list to export the files.

Figure 8-1 Video backup



Step 6 Select the storage device and click **Backup**.

- In the backup operation menu, you can deselect the files that do not need to be backed up.
- Select **Combine Video** to merge multiple backed-up video clips into one video.

Related Operations

Click **Lock** or **Unlock** to modify the file status.

8.2 Picture Backup

Procedure

Step 1 In the main menu, select **BACKUP** and click to enter the picture backup page.

Step 2 Select the time range and select the channels in **Channel List**.

Step 3 Click **Search**.

Step 4 Select pictures to be backed up.

Step 5 Click **Export** or in the operation list to export the files.

Step 6 Select the storage device and click **Backup**.

Related Operations

Click **Lock** or **Unlock** to modify the file status.

8.3 Tag Backup

Procedure

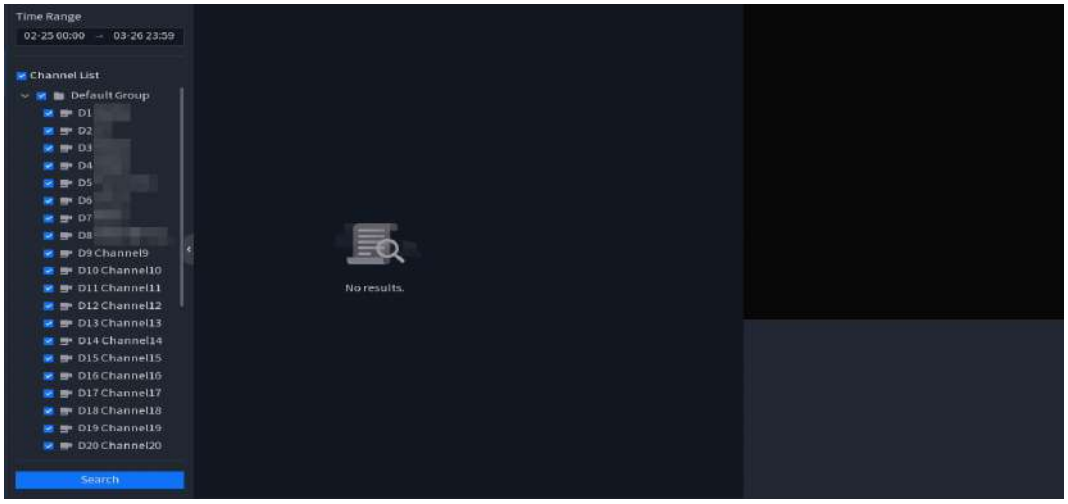
Step 1 In the main menu, select **BACKUP** and click to enter the picture backup page.

Step 2 Click to set the time range.

Step 3 Select the channel in the channel list and click **Search**.

Step 4 Select the picture files to be backed up.

Figure 8-2 Video backup



Step 5 Click **Export** or in the operation list to export the files.

Step 6 Select the storage device and click **Backup**.

9 Maintenance

9.1 Log

You can view and search for the log information, or back up log to the USB device. By reviewing the logs, we can identify some abnormal access activities. To ensure the system operates normally, we recommend you regularly check the logs and promptly check any abnormal conditions.

Background Information

- Data follows the principle of full coverage, and we recommend you back up regularly as needed.
- When the device is restored to factory settings, all data except that on external storage media will be erased. Data on the external storage media can be deleted through methods such as formatting.

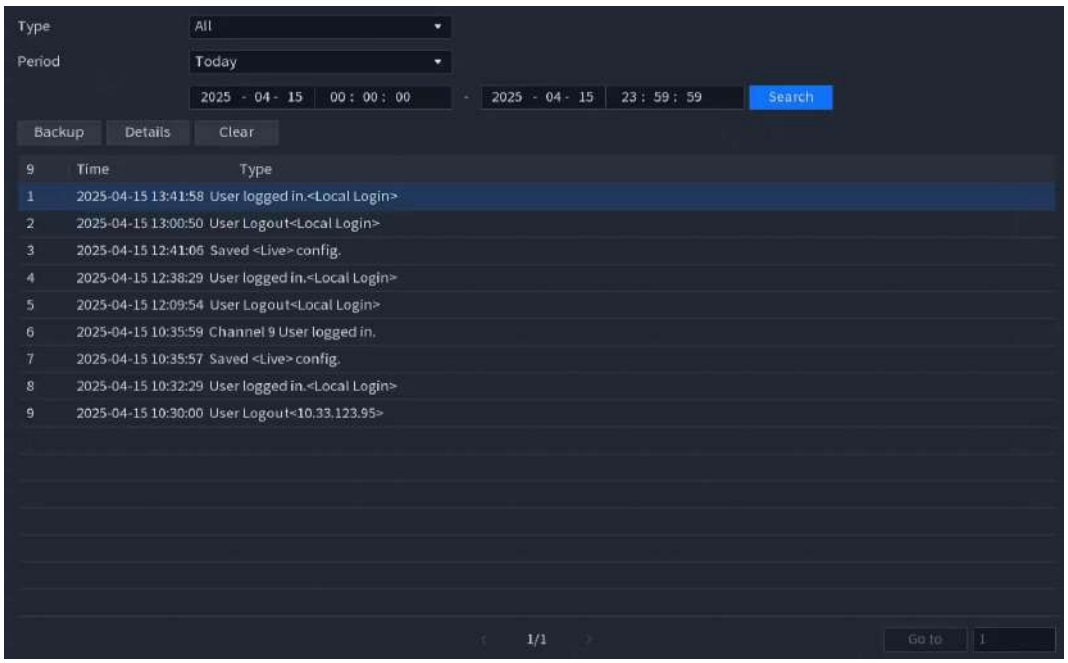
Procedure

Step 1 In the main menu, select **APPLICATIONS** > **MAINTENANCE** > **Log**.

Step 2 Configure the type and period, and then click **Search**.

- Click **Backup** to select the backup file path. You can back up the log information to a USB device.
- Click **Details** to view the detailed log information.
- Click **Clear** to clear all logs.

Figure 9-1 Log



9.2 System Information

9.2.1 Version

Select **Main Menu** > **MAINTENANCE** > **System Info** > **Version**.

You can view the version information.

9.2.2 Intelligent Algorithm

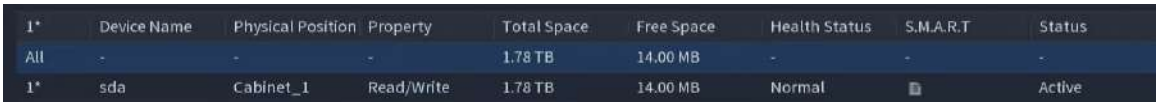
Select **Main Menu** > **MAINTENANCE** > **System Info** > **Intelligent Algorithm**.

You can view version information for AI functions such as face detection, face recognition, IVS, and video metadata.

9.2.3 Disk

You can view the HDD quantity, HDD type, total space, free space, status, and S.M.A.R.T information.

Figure 9-2 Disk information



1*	Device Name	Physical Position	Property	Total Space	Free Space	Health Status	S.M.A.R.T	Status
All	-	-	-	1.78 TB	14.00 MB	-	-	-
1*	sda	Cabinet_1	Read/Write	1.78 TB	14.00 MB	Normal		Active

Select **Main Menu** > **MAINTENANCE** > **System Info** > **Disk**.

Table 9-1 Description of disk information parameters

Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Property	Indicates HDD type.
Total Space	Indicates the total capacity of HDD.
Free Space	Indicates the usable capacity of HDD.
Health Status	Indicates the health status of the HDD.
S.M.A.R.T	View the S.M.A.R.T reports from HDD detecting.
Status	Indicates the status of the HDD to show if it is working normally.

9.2.4 Record

You can view the record information.

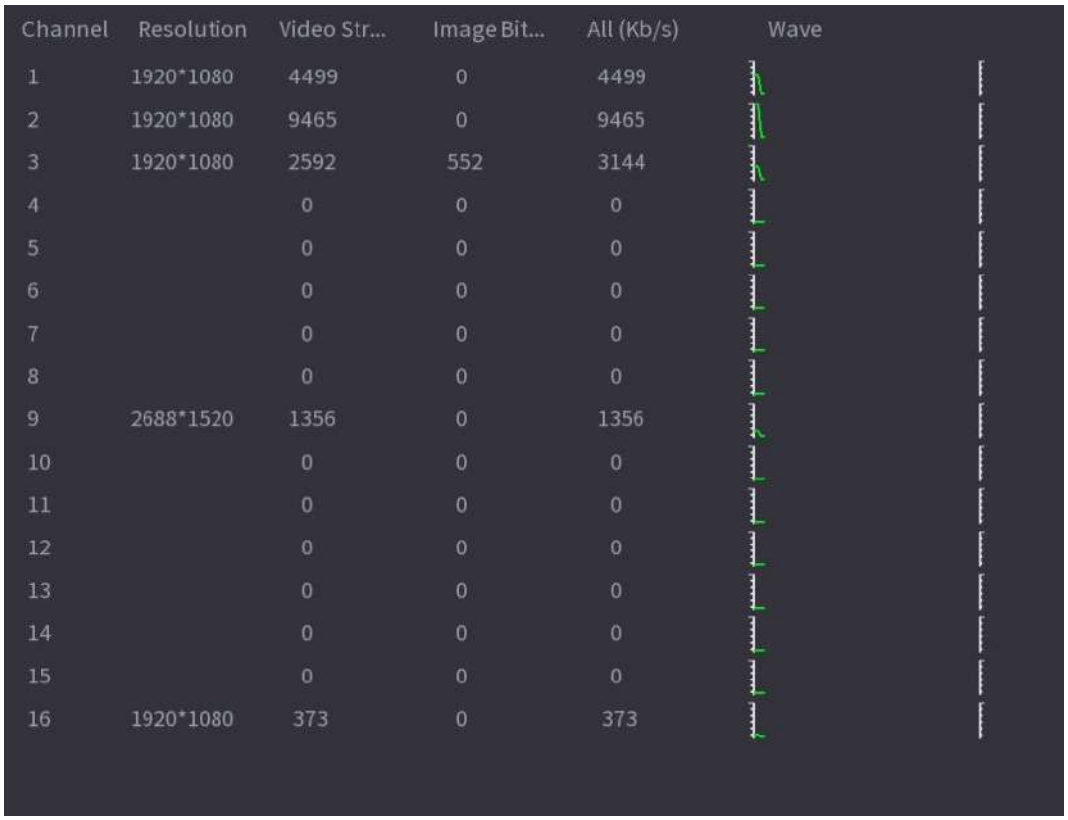
Select **Main Menu** > **MAINTENANCE** > **System Info** > **Record**.

9.2.5 BPS

You can view current video bit rate (kb/s) and resolution.

Select **Main Menu** > **MAINTENANCE** > **System Info** > **BPS**.

Figure 9-3 BPS



9.2.6 Device Status

You can view fan running status such as speed, CPU temperature, and memory.

Select **Main Menu** > **MAINTENANCE** > **System Info** > **Device Status**.

Figure 9-4 Device status

9.2.7 Online User

The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

Select **Main Menu** > **MAINTENANCE** > **System Info** > **Online User**.

You can view the online user information or block any user for a period of time. To block an online user, click and then enter the time that you want to block this user. The maximum value you can set is 65535.

9.3 Maintenance Management

9.3.1 Update

9.3.1.1 Upgrading File

Procedure

Step 1 Insert a USB storage device containing the upgrade files into the USB port of the Device.

Step 2 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Update**.

Step 3 Click **Update**.

Step 4 Click the file that you want to upgrade.

The selected file is displayed in the **Update File** box.

Step 5 Click **Start**.

9.3.1.2 Online Upgrade

When the Device is connected to the Internet, you can use online upgrade function to upgrade the system.

Background Information

Before using this function, you need to check whether there is any new version by auto check or manual check.

- Auto check: The device checks if there is any new version available at intervals.
- Manual check: Perform real-time check whether there is any new version available.

Ensure the correct power supply and network connection during upgrading; otherwise the upgrading might be failed.

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Update**.

Step 2 Check whether there is any new version available.

There are two updating methods below.

- Auto-check for updates: Enable the auto-check for updates.
- Manual check: Click **Manual Check** and the system starts checking the new versions. After checking is completed, the system displays the check result.

- If the **It is the latest version** text is displayed, you do not need to upgrade.
- If the text indicates there is a new version, go to the step 3.

Step 3 Click **Update now** to update the system.

9.3.1.3 Uboot Upgrade

- Under the root directory in the USB storage device, there must be "u-boot.bin.img" file and "update.img" file saved, and the USB storage device must be in FAT32 format.
- Make sure the USB storage device is inserted; otherwise the upgrading cannot be performed.

When starting the device, the system automatically checks whether there is a USB storage device connected and any upgrade file, and if yes and the check result of the upgrade file is correct, the system will upgrade automatically. The Uboot upgrade can avoid the situation that you have to upgrade through serial and TFTP when the Device is halted.

9.3.2 Device Maintenance

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

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Maintenance**.

Figure 9-5 Maintenance

Step 2 Configure the parameters.

- **Auto Restart** : Enable the device to restart at the idle time.
- **Emergency Maintenance** : When the device has an update power outage, running error and other problems, and you cannot log in, then you can use the emergency maintenance function to restart the device, clear configuration, update the system, and more.

Step 3 Click **Apply**.

9.3.3 Import/Export

You can export or import the device system settings if there are several devices that require the same setup.

Background Information

- The **Import/Export** page cannot be opened if the backup operation is ongoing on the other pages.
- When you open the **Import/Export** page, the system refreshes the devices and sets the current directory as the first root directory.
- Click **Format** to format the USB storage device.

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Import/Export**.

Step 2 Insert a USB storage device into one of the USB ports on the Device.

Step 3 Click **Refresh** to refresh the page.

The connected USB storage device is displayed.

Step 4 Click **Export**.

There is a folder under the name style of "Config_xxxx". Double-click this folder to view the backup files.

9.3.4 Default

9.3.4.1 Restoring Defaults on the Local Page

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

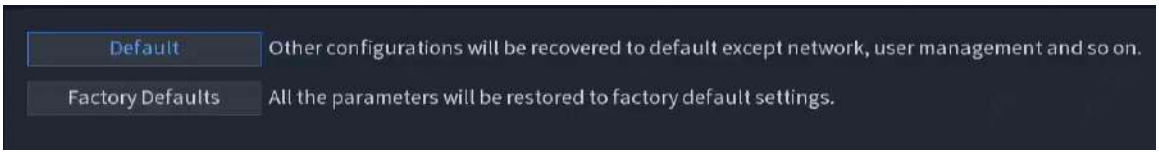
Background Information

This function is for admin account only.

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Default**.

Figure 9-6 Default



Step 2 Restore the settings.

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

9.3.4.2 Resetting Device through the Reset Button

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

Background Information

After resetting, all the configurations will be lost.

The reset button is available on select models.

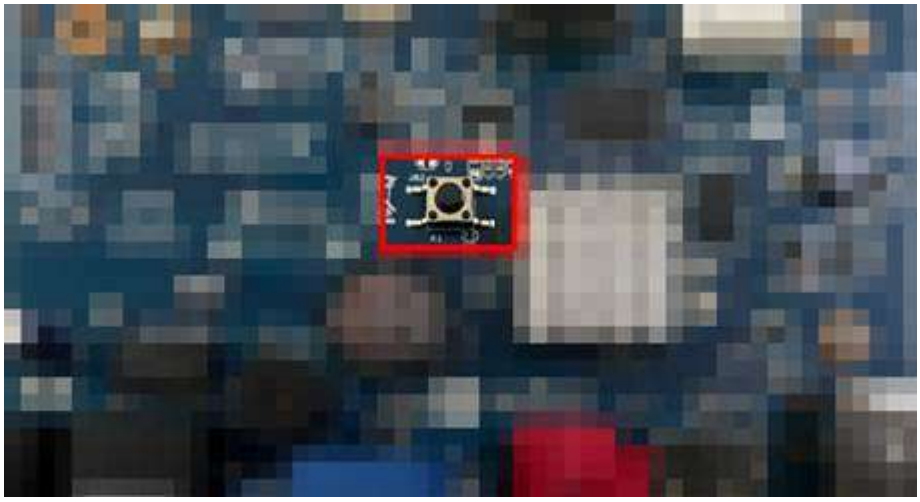
Procedure

Step 1 Disconnect the Device from power source, and then remove the cover panel.

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

Step 3 Press and hold the reset button for 5 seconds to 10 seconds.

Figure 9-7 Reset button



Step 4 Restart the Device.

After the Device restarts, the settings have been restored to the factory default.

9.3.5 Advanced Maintenance

When exception occurs, export data to check details.

Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Advanced Maintenance**.

9.3.6 Network Detection

9.3.6.1 Network Load

Network load means the data flow which measures the transmission capability. You can view the information such as data receiving speed and sending speed.

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Network Detection** > **Network Load**.

Figure 9-8 Network load

Step 2 Click the LAN name that you want to view, for example, **LAN1**.

The system displays the information of data sending speed and receiving speed.

- System displays LAN1 load by default.
- Only one LAN load can be displayed at one time.

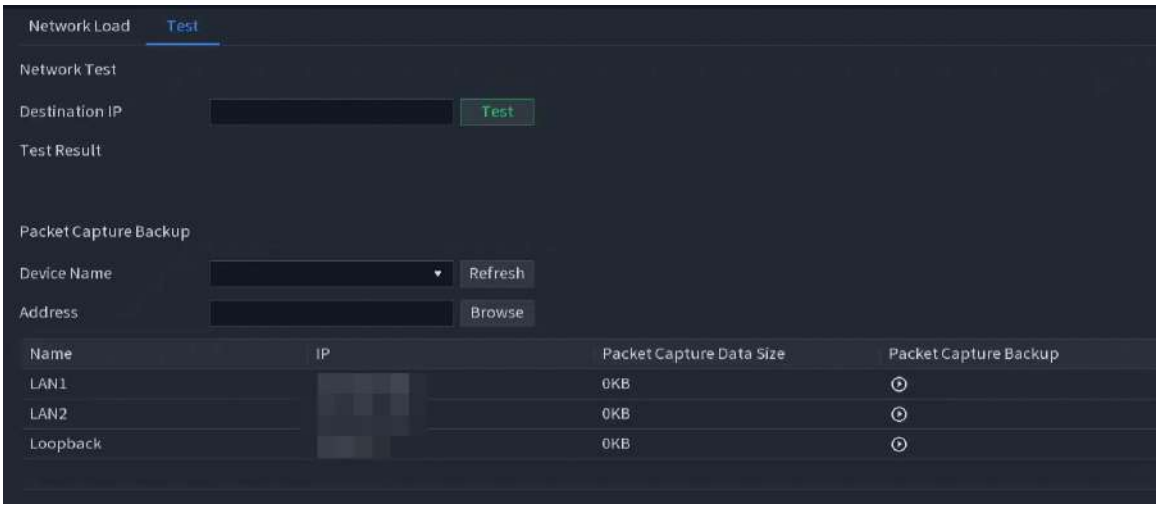
9.3.6.2 Network Test

You can test the network connection status between the Device and other devices.

Procedure

Step 1 Select **Main Menu** > **MAINTENANCE** > **Maintenance Management** > **Network Detection** > **Test**.

Figure 9-9 Test



Step 2 In the **Destination IP** box, enter the IP address.

Step 3 Click **Test**.

After testing is completed, the test result is displayed. You can check the evaluation for average delay, packet loss, and network status.

10 Vehicle Entrance and Exit

In the main menu of the vehicle entrance and exit, you can add entrance and exit camera to view the entrance and exit scenes, configure the vehicle blocklists and allowlists, and enable the ANPR function. The system can detect and record vehicle entrance and exit information along with access records, and provide real-time alarms on the page.

Figure 10-1 Vehicle entrance and exit

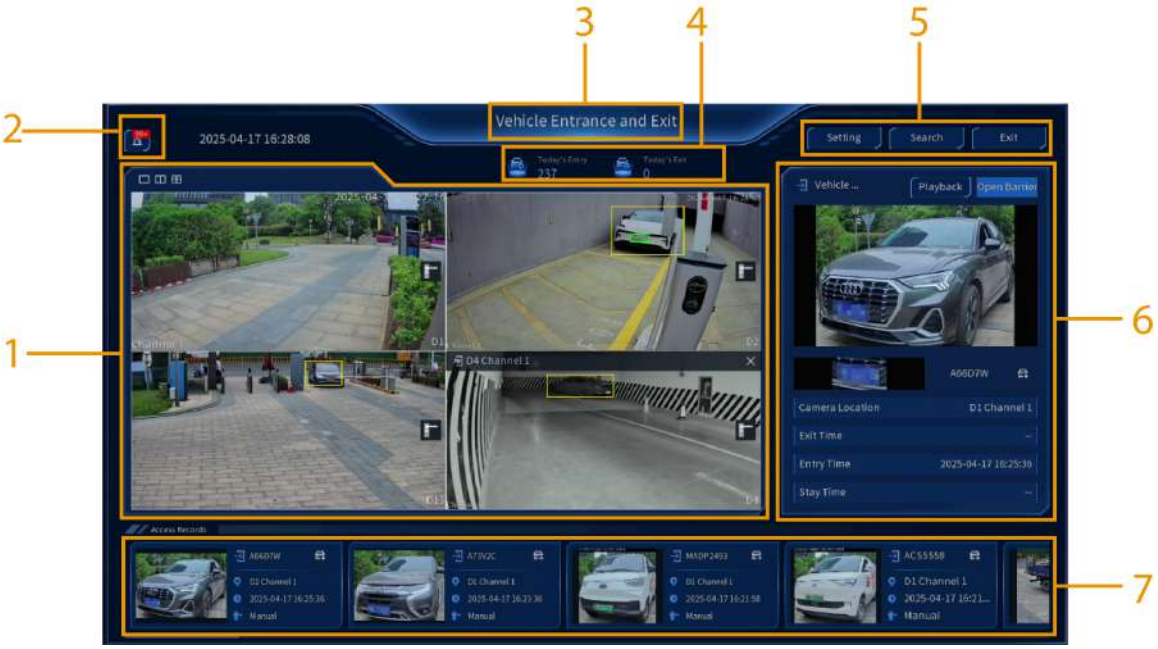


Table 10-1 Description of vehicle entrance and exit

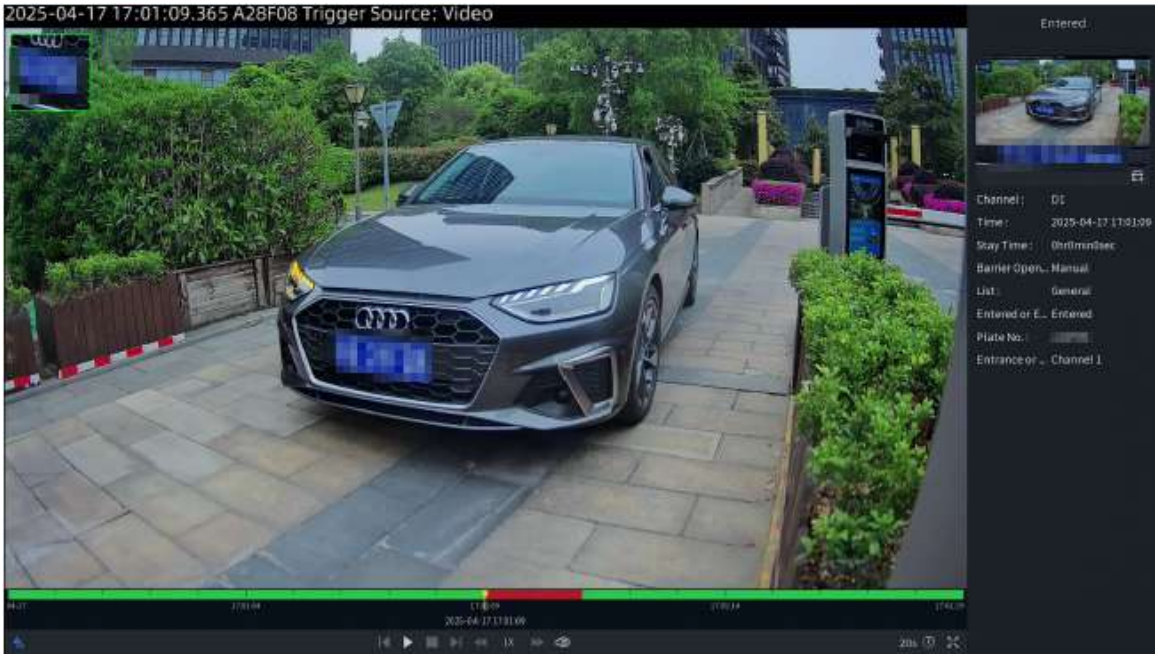
Number	Description
1	Live view of the channels, which supports 4 channels at most. You can choose **1 Splits** , **2 Splits** and **4 Splits**. Click **Add Entrance and Exit Camera** to select channels and entrance or exit type. The displayed channels are all online and support the ANPR function.
2	Real-time events. Click this icon to view the alarm information, including abnormal events, alarm status and AI events.
3	The title of the vehicle entrance and exit page. You can customize it.
4	Number of vehicle entry and exit records for the day.
5	• **Setting** : Configure the vehicle blocklist and allowlist and ANPR functions. For details, see "6.1.6.2 Vehicle Blocklist/Allowlist" and "6.2.2.8 ANPR". • **Search** : Search vehicle entry and exit information and playback. • **Exit** : Exit the vehicle entrance and exit page and go back to the main menu.

Number	Description
6	Vehicle entry and exit detail page, displaying vehicle entry and exit information. Upon opening, it shows the exit/entry status video and allows switching between exit and entry information and videos. If there is no video available, the switch button will be grayed out. It supports viewing vehicle playback, adding vehicles to a blocklist, and manually opening the gate.
7	Vehicle access records.

View the Playback

Click **Playback** or double-click any card in the channel record. In the playback page, click to add vehicles to the blocklist.

Figure 10-2 Playback page



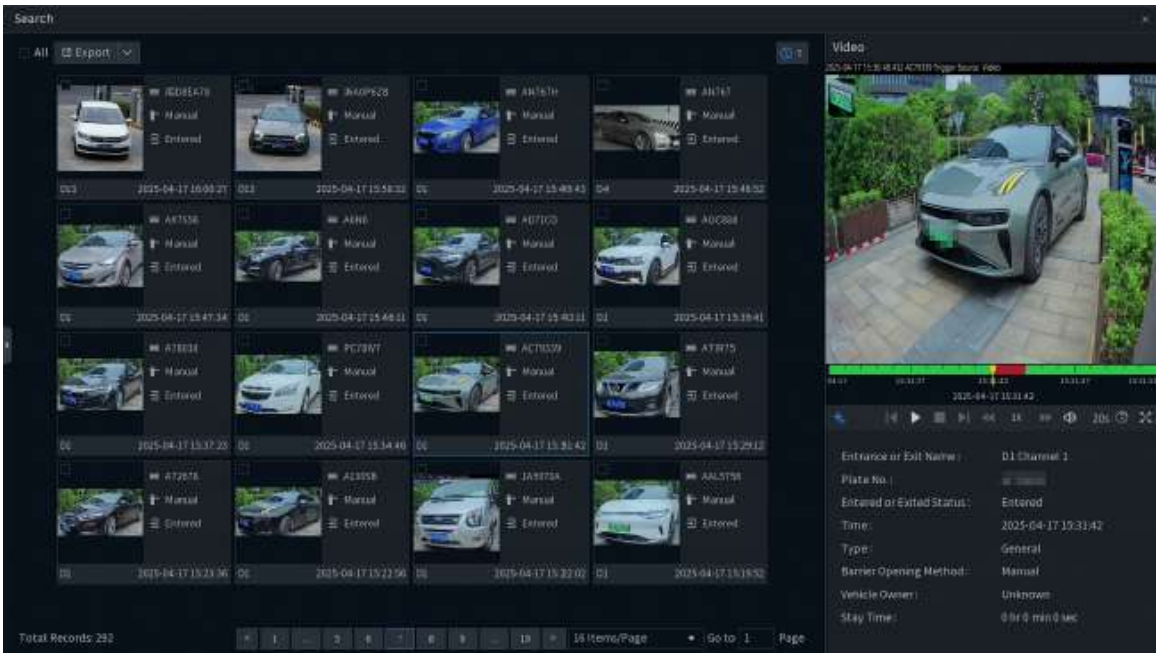
Search for Vehicle Entry and Exit Records

Click **Search** at the upper-right corner to enter the search page. Enter the plate number, select entry and exit type, license plate type, barrier opening method and vehicle owner, select the channel and period, and then click **Search**.

Double-click the search result to play the video associated with vehicle recognition events. You can also export videos, images and lists from the result cards. For the playback control, see "5.1 General Video".

Click **Export** to export the videos and images associated with the search results.

Figure 10-3 Search for vehicle entry and exit records



11 Wizseek

The Wizseek enables searching images by text, by multi-attribute and by multi-target filtering.

Procedure

Step 1 In the main menu, select **APPLICATIONS** > **WIZSEEK**.

This function is available on select models.

Step 2 Enter the search content, set search conditions (including time and channel), then click **Search**.

It supports the following 3 methods for entering search content:

- Enter content in the search box.
- Select search targets by choosing from preset target attributes above the search box.

  For example, when you select **Human** , **white** in **Top**, and then the search box will automatically populate with the information: "A person is wearing a white coat."
- In the **Search Suggestions** area, select the desired search term.

  Click to refresh the search term.

Figure 11-1 Wizseek

Step 3 View the search results.

Hover over the search results to display more operations.

Figure 11-2 Search results

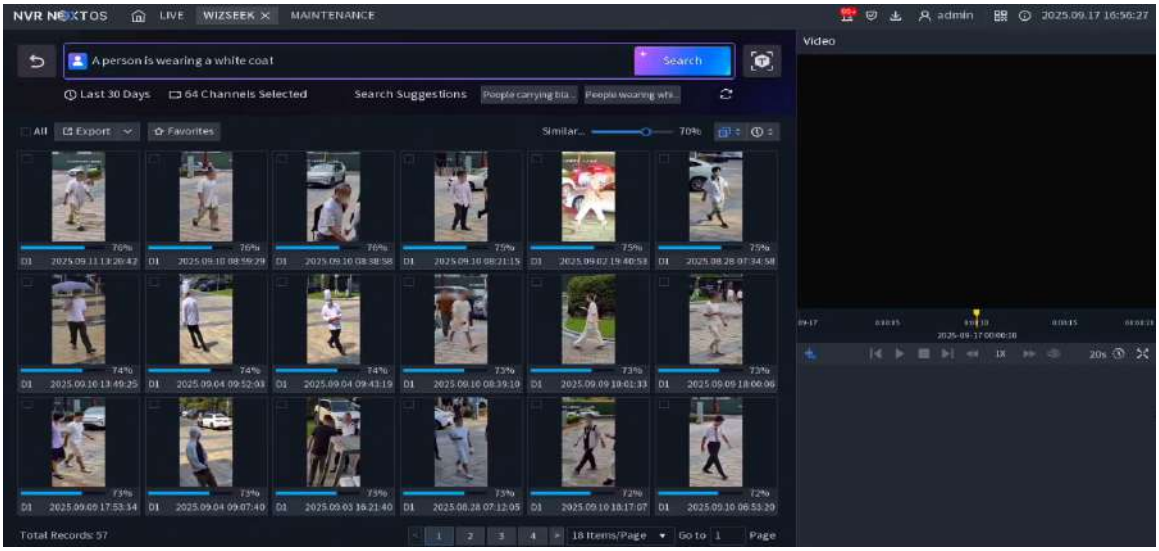


Table 11-1 Related operations of search results

Function	Operation
Favorites	Click ☆ or select multiple search results, and then click **Add to Favorites** to add search results to your favorites. Click **Favorites** to enter your favorites The supported operations in favorites are similar to those listed below and can be performed accordingly.
Text-Defined Alarms	Click at the right side of the search box to quickly navigate to the text-defined alarms page and create the current search content as a text rule.
Sort by Similarity/ Time	Click Similar... 70% at the right side of the search box to sort search results by similarity (highest to lowest) or by time (ascending/ descending).

Function	Operation
Playback Video	On the search results panel, select a result. ● Click to play back the video, and the playback page supports the following operations: ◇ Click to stop playing back the video. ◇ Click to pause playing back the video. ◇ Click or to play the previous or next video. ◇ Click to adjust the volume. ◇ Click to select the AI rule and AI area. ◇ Click to adjust the time range for playback viewing. ◇ Click to view the video in full screen. ● Click to select the face, human body or motor vehicle. Click to enable the second AcuPick action. ● Click to enable the privacy masking. Click again to remove it. ● Click to close the video.
Import files	Select the results, click **Import** in the search results panel, and then import them to the external storage device.
AcuPick	On the search results panel, click to search the target by image.
Map Tracks	On the search results panel, click to view the target map track.

12 Local Settings

12.1 Network Settings

Set the basic network parameter information and network applications for the device.

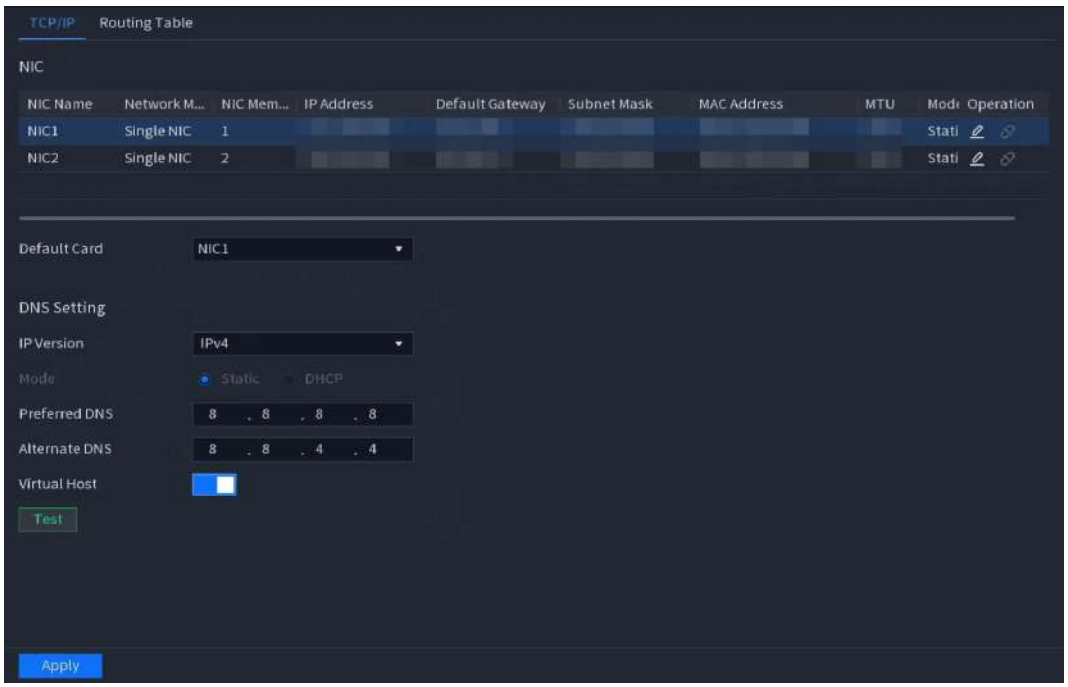
12.1.1 TCP/IP

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

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **TCP/IP**.

Figure 12-1 TCP/IP



Step 2 Click to configure the card, and then click **OK**.

Figure 12-2 TCP/IP

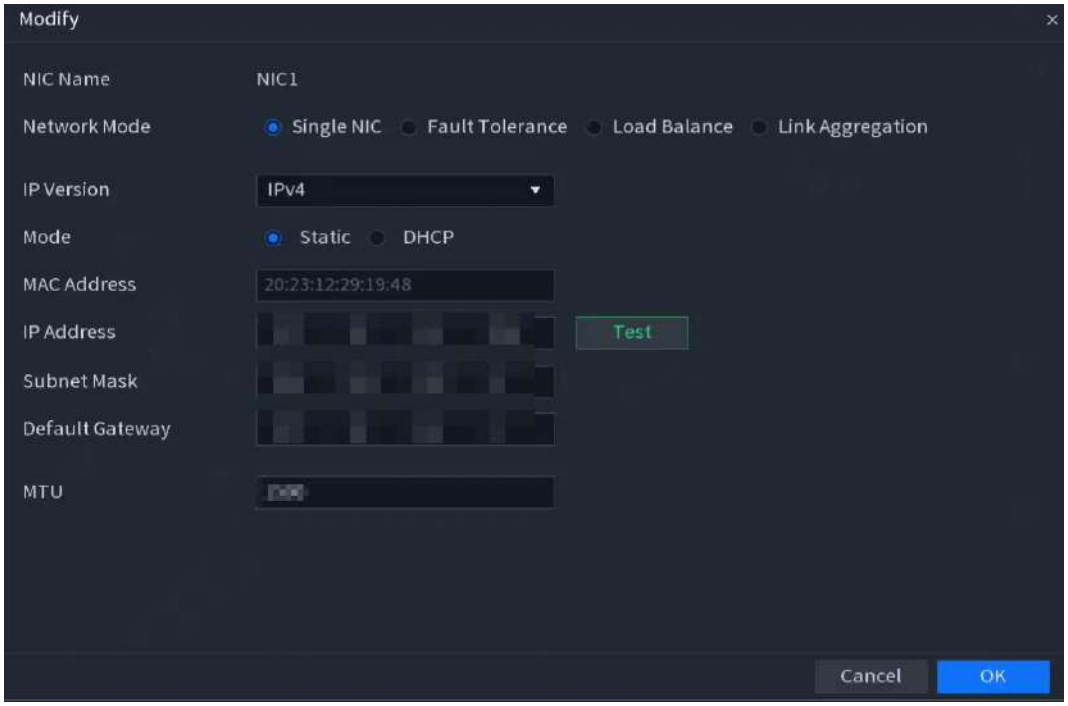


Table 12-1 TCP/IP parameters

Parameter	Description
Network Mode	• **Single NIC** : The current NIC card works independently. If the current NIC card is disconnected, the Device becomes offline. • **Fault Tolerance**: 2 NIC cards share one IP address. Normally only one NIC card is working. When this card fails, the other NIC card will start working automatically to ensure the network connection. The Device is regarded as offline only when both NIC cards are disconnected. When you select **Fault Tolerance** , you need to select the other NIC in **NIC Member**. • **Load Balance**: 2 NIC cards share one IP address and work at the same time to share the network load averagely. When one NIC card fails, the other card continues to work normally. The Device is regarded as offline only when both NIC cards are disconnected. When you select **Load Balance** , you need to at least select 2 binding NICs in **NIC Member**. • **Link Aggregation**: Multiple network cards share a single IP address to increase bandwidth or achieve redundancy through aggregation. When one network card fails, the other can still function normally. During network monitoring, the device's network connection is only lost when both network cards are disconnected. In environments with poor network conditions, the bandwidth of the network cards is more stable under dynamic aggregation. When you select **Link Aggregation** , you need to at least select 2 NICs in **NIC Member**. The Device with single Ethernet port does not support this function.
NIC Member	When the network mode is **Fault Tolerance** or **Load Balance**, you need to select the checkbox to bind NIC cards. • Make sure that at least two NIC cards are installed. • NIC cards using different ports such as optical port and electrical port cannot be bound together. • After binding NIC cards, you need to restart the Device to make the change effective.
IP Version	Select IPv4 or IPv6. Both versions are supported for access.
MAC Address	Displays the MAC address of the Device.
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to set IP address manually. • If you want to manually configure the IP information, disable the DHCP function first. • If PPPoE connection is successful, the IP address, subnet mask, default gateway, and DHCP are not available for configuration.

Parameter	Description
IP Address	Enter the IP address and configure the corresponding subnet mask and default gateway. ● The IP address and default gateway must be on the same network segment. ● Click **Test** to check whether the IP address is available.
Subnet Mask	
Default Gateway	
MTU	Displays the MTU value of the NIC card.

Step 3 On the **TCP/IP** page, configure the DNS server.

This step is compulsive if you want to use the domain service.

- Obtain DNS server automatically.

  When there is DHCP server on the network, you can enable **DHCP** so that the Device can automatically obtain a dynamic IP address.
- Configure DNS server manually.

  Select the IP version, and then enter the IP addresses of preferred and alternate DNS server.

Step 4 Select a NIC card as the default card.

Step 5 Click **Apply**.

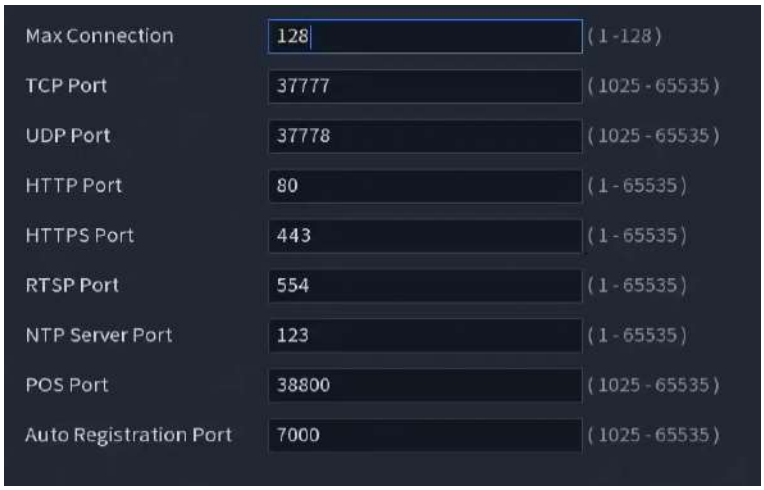
12.1.2 Port

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

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Port**.

Figure 12-3 Port



Step 2 Configure the parameters.

The parameters except **Max Connection** take effect after the device restarts.

Table 12-2 Description of port parameters

Parameter	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as web client, platform, and mobile client.
TCP Port	Transmission control protocol port. Enter the value according to your actual situation.
UDP Port	User datagram protocol port. Enter the value according to your actual situation.
HTTP Port	The default value setting is 80. You can enter the value according to your actual situation. If you change the HTTP port number to, for example, 70, then you need to enter 70 after the IP address when logging in to the Device through the browser.
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 is 554. You can enter the value according to your actual situation.
POS Port	POS data transmission port. The value range from 1 through 65535. The default value is 38800.
Auto Registration Port	The auto registered port. Supports adding cameras through auto registration.

Step 3 Click **Apply**.

12.1.3 External Wi-Fi

The Device can be connected to wireless network with an external Wi-Fi module.

Prerequisites

Make sure that external Wi-Fi module is installed on the Device.

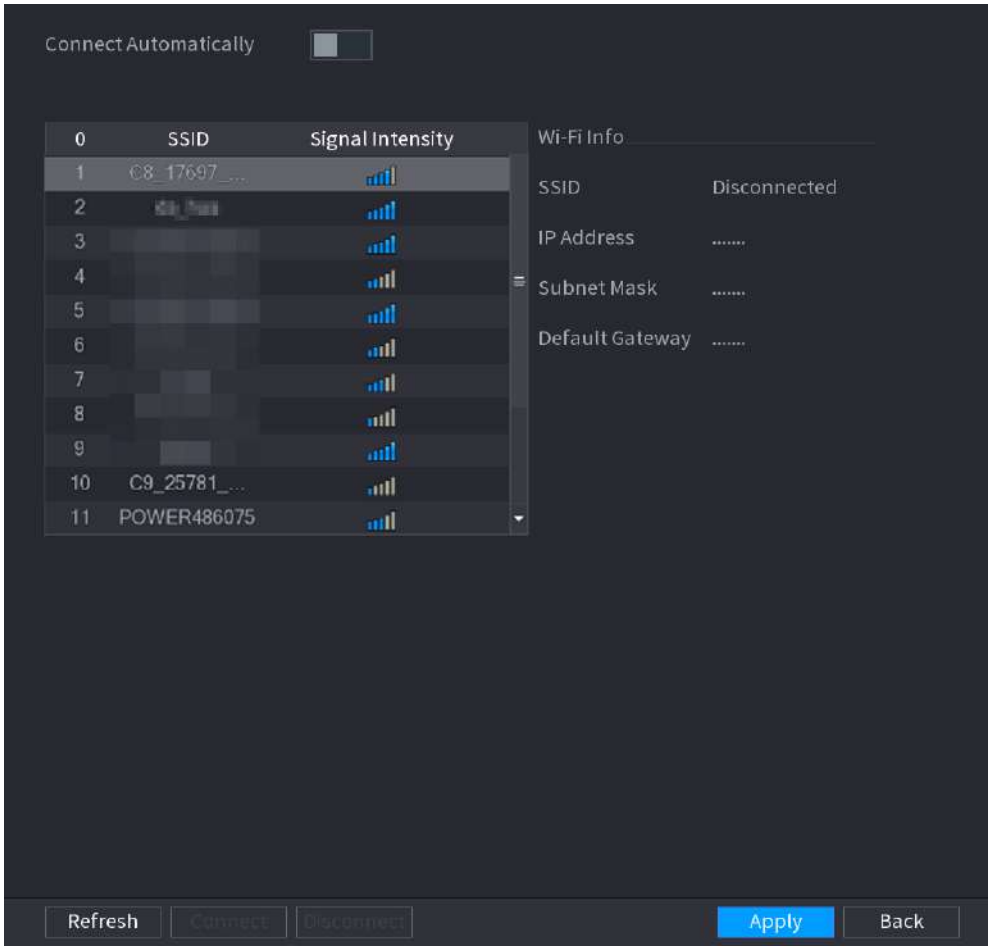
Background Information

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Wi-Fi**.

Figure 12-4 Wi-Fi



Step 2 Configure the parameters.

Table 12-3 Wi-Fi parameters

Parameter	Description
Connect Automatically	After the function is enabled, the NVR will connect to the nearest site that was previously successfully connected after the Device starts.
Refresh	Search for the sites again.
Disconnect	Disconnect the current connection.
Connect	Select an available site and then click **Connect** to connect to the Wi-Fi.

Step 3 Click **Apply**.

After the connection is successful, a Wi-Fi connection signal flag appears in the upper-right corner of the live view page.

12.1.4 3G/4G

Prerequisites

Make sure that 3G/4G module is installed on the device.

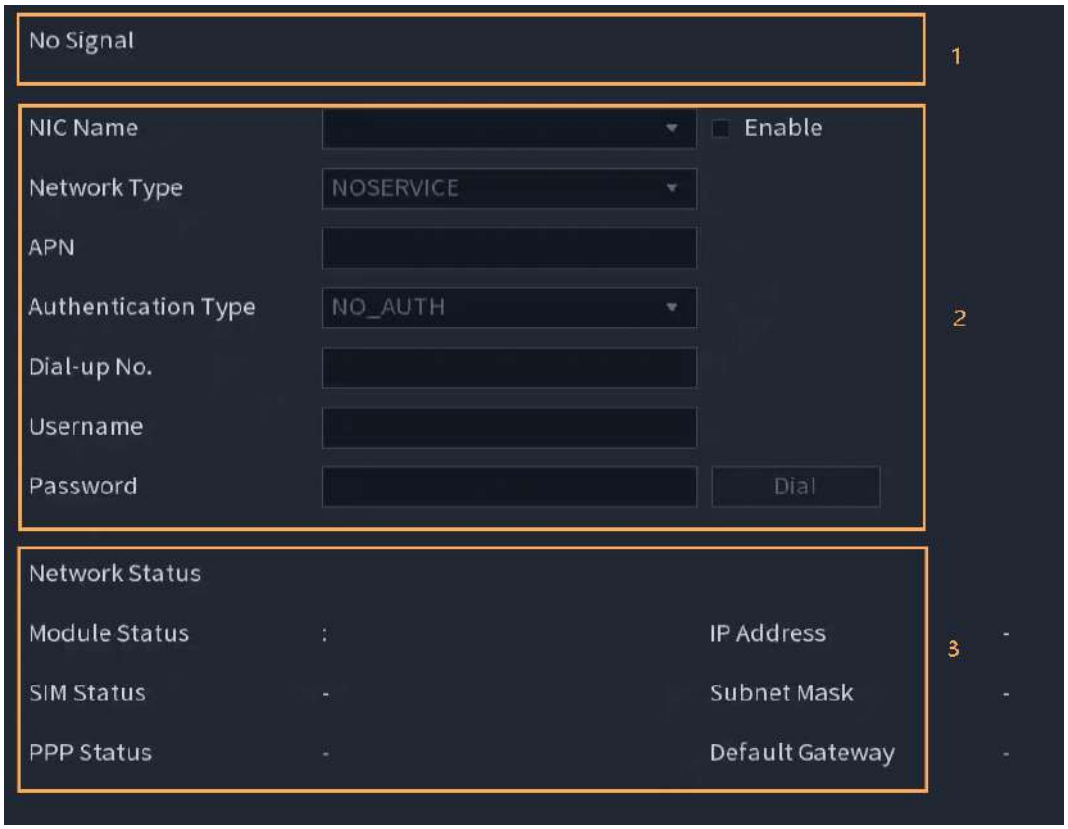
Background Information

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Wi-Fi**.

Figure 12-5 3G/4G



The page is divided into three main areas:

- Zone 1 displays a 3G/4G signal indication.
- Zone 2 displays 3G/4G module configuration information.
- Zone 3 displays the status information of the 3G/4G module.

Zone 2 displays the corresponding information when the 3G/4G module is connected, while Zone 1 and Zone 3 will only display the corresponding content when the 3G/4G is enabled.

Step 2 Configure parameters.

Table 12-4 3G/4G parameters

Parameter	Description
NIC Name	Select a NIC name.
Network Type.	Select a 3G/4G network type to distinguish between 3G/4G modules from different vendors.
APN, Dial-up No.	Main parameters of PPP dial.

Parameter	Description
Authentication Type	Select PAP, CHAP or NO_AUTH. NO_AUTH represents no authentication for 3G/4G.
Username and Password	Dial-up user information.

Step 3 Click **Apply**.

12.1.5 PPPoE

PPPoE is another way for the device to access the network. You can establish network connection by configuring PPPoE settings to give the device a dynamic IP address on the WAN.

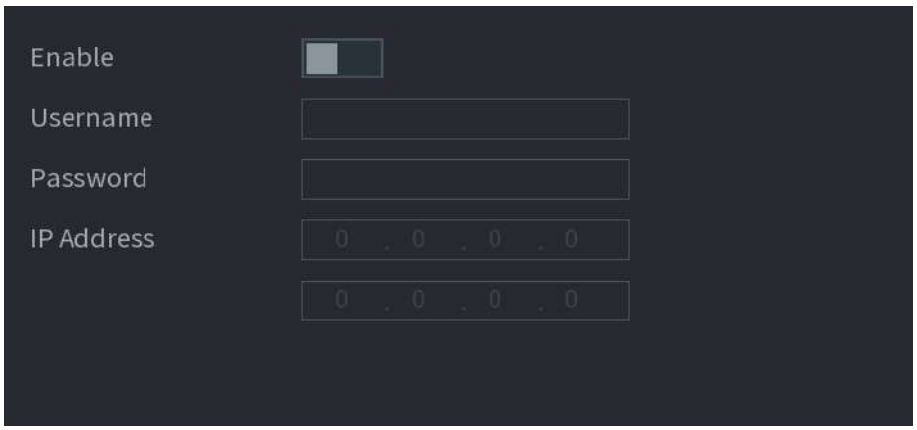
Prerequisites

To use this function, firstly you need to obtain the username and password from the Internet Service Provider.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **PPPoE**.

Figure 12-6 PPPoE



Step 2 Enable the PPPoE function.

Step 3 Enter the username and password provided by the Internet Service Provider.

Step 4 Click **Apply**.

The IP address appears on the PPPoE page. You can use this IP address to access the Device.

When the PPPoE function is enabled, the IP address on the **TCP/IP** page cannot be modified.

12.1.6 DDNS

When the IP address of the device changes frequently, the DDNS function can dynamically refresh the correspondence between the domain on DNS and the IP address. You can access the device by using the domain.

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 **Main Menu** > **SETTINGS** > **NETWORK** > **DDNS**.

Figure 12-7 DDNS

Step 2 Enable DDNS and then configure the parameters.

After you enable DDNS function, the third-party server might collect your device information.

Table 12-5 DDNS parameters

Parameter	Description
Type	Displays the type and address of DDNS service provider.
Server Address	• For **Dyndns DDNS**, the default address is members.dyndns.org. • For **NO-IP DDNS**, the default address is dynupdate.no-ip.com. • For **CN99 DDNS**, the default address is members.3322.org.

Parameter	Description
Domain	Enter the domain name that you have registered on the website of DDNS service provider.
Username	Enter the username and password obtained from DDNS service provider. You need to register the username, password and other information on the website of DDNS service provider.
Password	
Interval	Enter the interval at which you want to update the DDNS.

Step 3 Click **Apply**.

Enter the domain name in the browser on your computer, and then press the Enter key. If the web page of the device is displayed, the configuration is successful. If not, the configuration failed.

12.1.7 UPnP

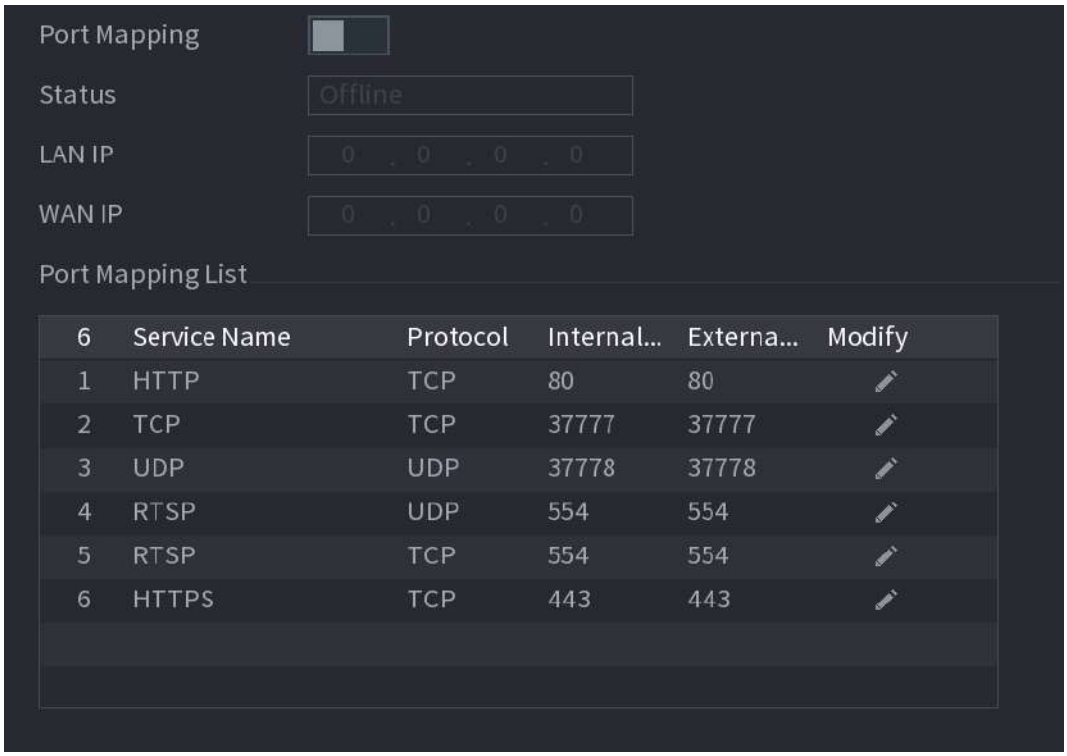
Background Information

You can map the relationship between the LAN and the WAN to access the device on the LAN through the IP address on the WAN.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **UPnP**.

Figure 12-8 UPnP



Step 2 Configure the settings for the UPnP parameters.

Table 12-6 UPnP parameters

Parameter	Description
Port Mapping	Enable the UPnP function.
Status	Indicates the status of UPnP function. ● Offline: Failed. ● Online: Succeeded.
LAN IP	Enter IP address of router on the LAN. After mapping succeeded, the system obtains IP address automatically.
WAN IP	Enter IP address of router on the WAN. After mapping succeeded, the system obtains IP address automatically.
Port Mapping List	The settings on port mapping list correspond to the UPnP port mapping list on the router. ● Service Name: Name of network server. ● Protocol: Type of protocol. ● Internal Port: Internal port that is mapped on the Device. ● External Port: External port that is mapped on the router. ● To avoid the conflict, when setting the external port, try to use the ports from 1024 through 5000 and avoid popular ports from 1 through 255 and system ports from 256 through 1023. ● When there are several devices on the LAN, properly arrange the ports mapping relations to avoid mapping to the same external port. ● When establishing a mapping relationship, ensure the mapping ports are not occupied or limited. ● The internal and external ports of TCP and UDP must be the same and cannot be modified. ● Click to modify the external port.

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

In the browser, enter http*://WAN IP: External IP port*. You can visit the device on the LAN.

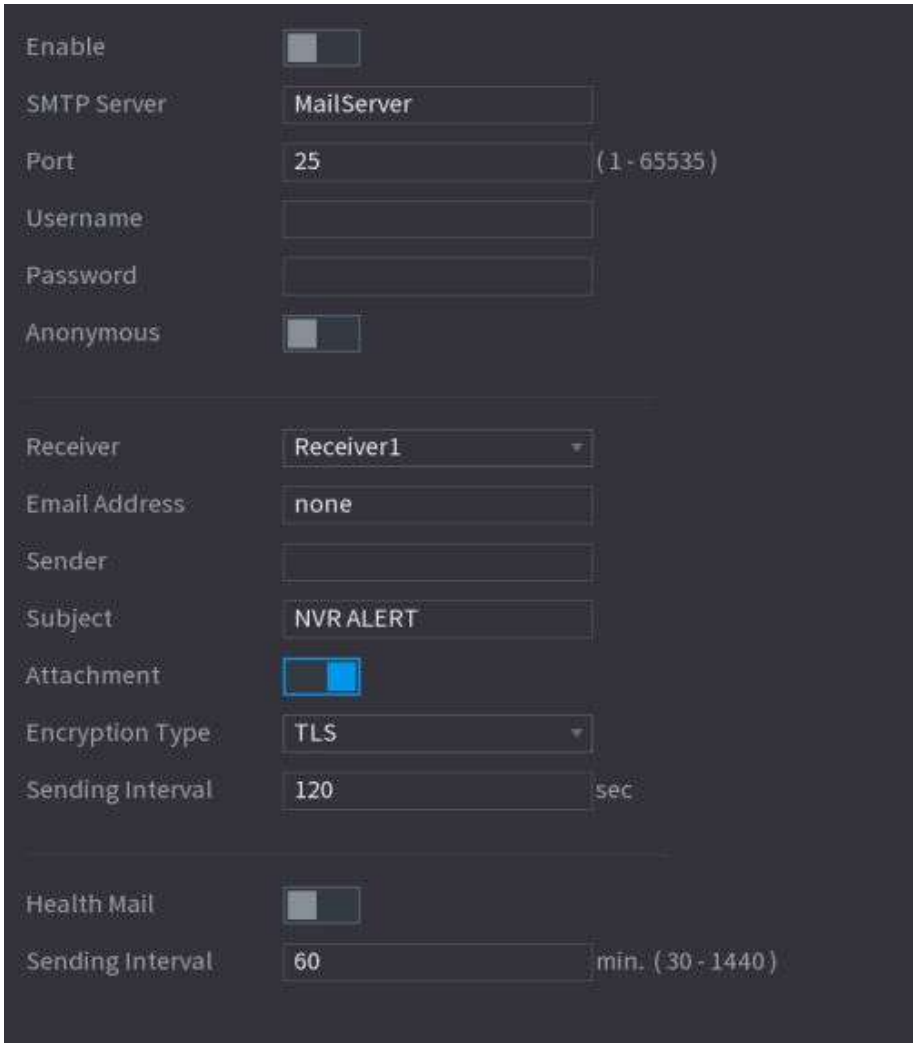
12.1.8 Email

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

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Email**.

Figure 12-9 Email



Step 2 Click to enable the function.

Step 3 Configure the email parameters.

Table 12-7 Email parameters

Parameter	Description
SMTP Server	Enter the address of SMTP server of 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.
Receiver	Select the receiver to receive the notification. You can select up to three receivers.
Email Address	Enter the email address of mail receivers.
Sender	Enter the sender's email address. You can enter up to three senders separated by comma.

Parameter	Description
Subject	Enter the email subject. You can enter Chinese, English and numerals with the length limited to 64 characters.
Attachment	Enable the attachment function. When there is an alarm event, the system can attach snapshots as an attachment to the email.
Encryption Type	Select the encryption type from **NONE** , **SSL**, or **TLS**. For SMTP server, the default encryption type is **TLS**.
Sending Interval (Sec.)	Set the interval at which the system sends an email for the same type of alarm event to avoid excessive pileup of emails caused by frequent alarm events. The value ranges from 0 to 3600. 0 means that there is no interval.
Health Mail	Enable the health test function. The system can send a test email to check the connection.
Sending Interval	Set the interval at which the system sends a health test email. The value ranges from 30 to 1440. 0 means that there is no interval.
Test	Click **Test** to test the email sending function. If the configuration is correct, the receiver's email account will receive the email. Before testing, click **Apply** to save the settings.

Step 4 Click **Apply**.

12.1.9 SNMP

You can connect the device with some software such as MIB Builder and MG-SOFT MIB Browser to manage and control the device from the software.

Prerequisites

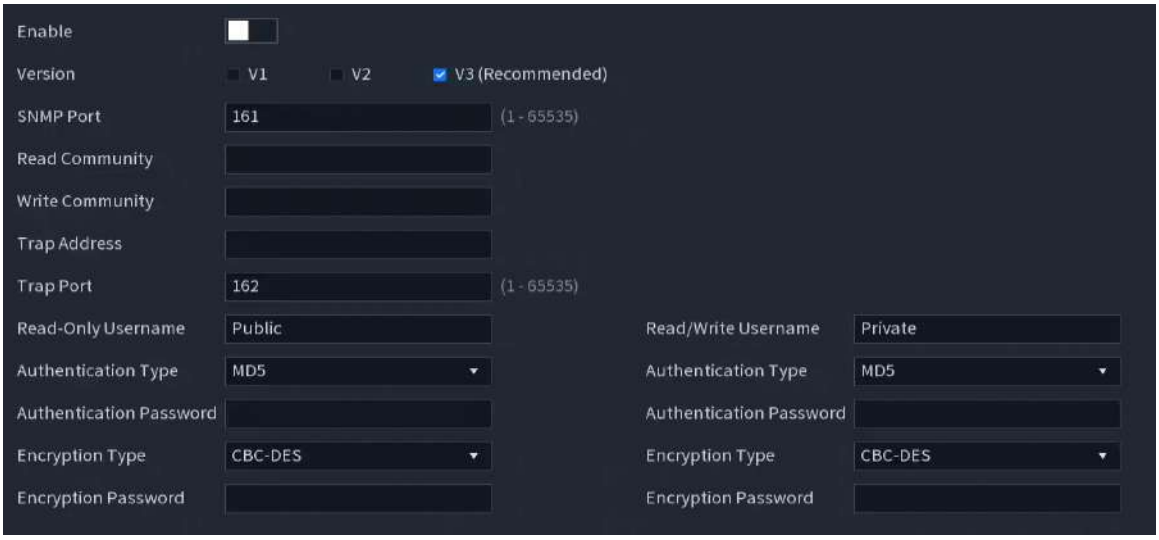
- Install the software that can manage and control the SNMP, such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the MIB files that correspond to the current version from the technical support.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **SNMP**.

Figure 12-10 SNMP



Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 12-8 SNMP parameters

Parameter	Description
Version	Select the checkbox of SNMP version that you are using. The default version is **V3**. There is a risk if you use V1 or V2.
SNMP Port	Enter the monitoring port on the agent program.
Read Community	Enter the read and write strings supported by the agent program.
Write Community	
Trap Address	Enter the destination address for the agent program to send the Trap information.
Trap Port	Enter the destination port for the agent program to send the Trap information.
Read-Only Username	Enter the username that is allowed to access the Device and has the read-only permission.
Read/Write Username	Enter the username that is allowed to access the Device and has the read and write permission.
Authentication Type	Select MD5 or SHA. The system recognizes the type automatically.
Authentication Password	Enter the password for authentication. The password should be no less than eight characters.
Encryption Type	Select an encryption type. The default setting is CBC-DES.
Encryption Password	Enter the encryption password.

Step 4 Click **Apply**.

Step 5 Compile the two MIB files by MIB Builder.

Step 6 Run MG-SOFT MIB Browser to load in the module from compilation.

Step 7 On the MG-SOFT MIB Browser, enter the device IP that you want to manage, and then select the version number to query.

Step 8 On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the channels quantity and software version.

12.1.10 Multicast

When you access the device from the network to view the video, if the access is exceeded, the video will not display. You can use the multicast function to group the IP to solve the problem.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Multicast**.

Step 2 Configure the parameters.

Table 12-9 Multicast parameters

Parameter	Description
Enable	Enable the multicast function.
IP Address	Enter the IP address that you want to use as the multicast IP. The IP address ranges from 224.0.0.0 through 239.255.255.255.
Port	Enter the port for the multicast. The port ranges from 1025 through 65000.

Step 3 Click **Apply**.

You can log in to the web page via multicast.

On the web login page, on the **Type** list, select **Multicast**. The web will automatically obtain the multicast IP address and join the multicast group. Then you can view the video through multicast function.

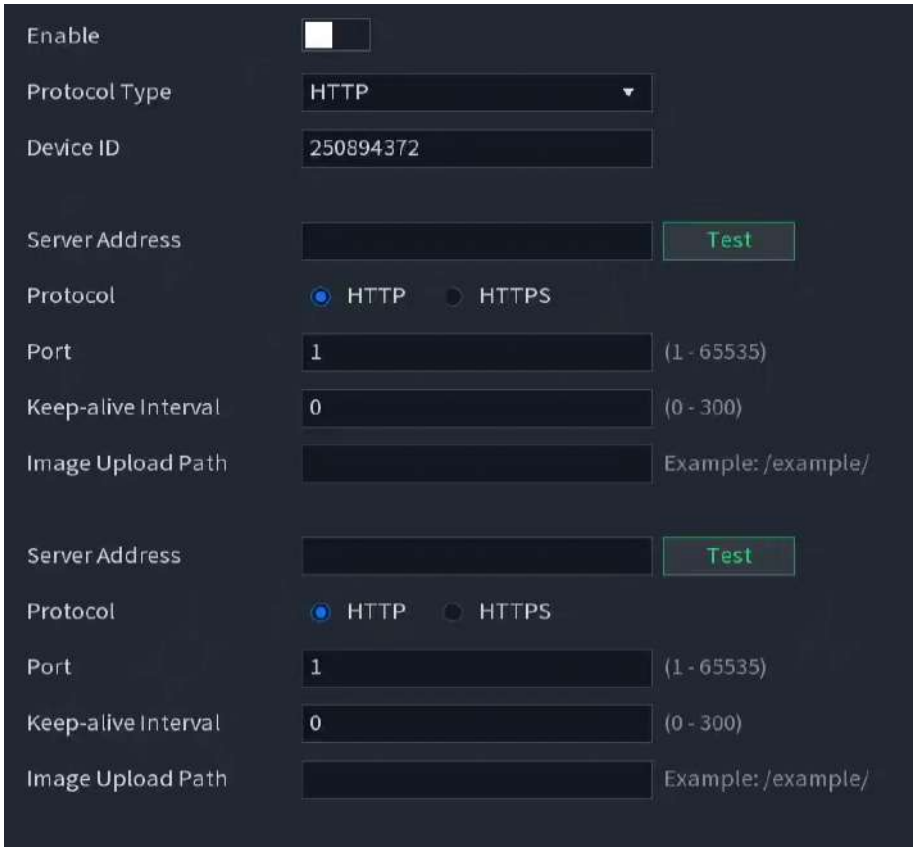
12.1.11 Alarm Center

You can configure the alarm center server to receive the uploaded alarm information.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Alarm Center**.

Figure 12-11 Alarm center



Step 2 Click to enable the function, and then select a protocol type.

You can select **Private Protocol** or **HTTP**.

Step 3 Configure the parameters.

When selecting **HTTP** , you need to enter the server address, port, and then select **HTTP** or **HTTPS** as needed.

Table 12-10 Alarm center parameters

Parameter	Description
Server Address	The IP address and communication port of the computer installed with alarm client.
Port	
Keep-alive Interval	Enter the keep-alive interval maintaining connection between the Device and the server.
Image Upload Path	Enter the path for uploading the image.

Step 4 Click **Apply**.

12.1.12 Auto Registration

You can register the device into the specified proxy server which acts as the transit to enable the client software to access the device.

Prerequisites

- The proxy server has been deployed.

- The device, the proxy server and the device running the client software are on the same network.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Auto Registration**.

Figure 12-12 Auto Registration

Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 12-11 Register parameters

Function	Description
Server Address	Enter the IP address or domain name of the server that you want to register to.
Port	Enter the port of the server.
Sub-Device ID	Enter the ID allocated by the server.

Step 4 Click **Apply**.

12.1.13 P2P

P2P is a kind of convenient private network penetration technology. Instead of applying for dynamic domain name, mapping ports or deploying transit server, you can add NVR devices to the app for remote management.

Background Information

This function will consume the device traffic when the device is online.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **P2P**.

Step 2 Enable the P2P function.

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.

Step 3 Click **Apply**.

The P2P function is enabled. You can use your phone to scan the QR code under **Mobile Client** to download and install the mobile client. After that, you can use the mobile client to scan the QR code under **Device SN** to add the Device for remote management. For details on the app operation, see the user's manual of the app.

12.1.14 Cluster IP

When the main device malfunctions, the sub device can use the main device configuration and virtual IP address to replace the work (monitor or record) accordingly. When you use the virtual IP to access the device, you can still view the real-time video and there is no risk of record loss.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **NETWORK** > **Cluster IP**.

Step 2 Enable the cluster IP function.

Step 3 Enter the IP address, subnet mask, and default gateway.

Step 4 Click **Apply**.

12.2 Storage Settings

12.2.1 Configuring Basic Parameters

You can set basic storage parameters.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **Basic**.

Figure 12-13 Basic storage

Step 2 Set parameters.

Table 12-12 Basic storage 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.
Create Video Files	Configure the time length and file length for each recorded video.
Delete Expired Files	Configure whether to delete the old files. • Select **Auto** and then configure how long you want to keep the old files. • Select **Never** if you do not want to use this function. Deleted files cannot be recovered.
Sleep Strategy	• **Auto** : The system sleeps automatically after idling for a period of time. • **Never** : The system keeps running all the time.

Step 3 Click **Apply**.

12.2.2 Schedule

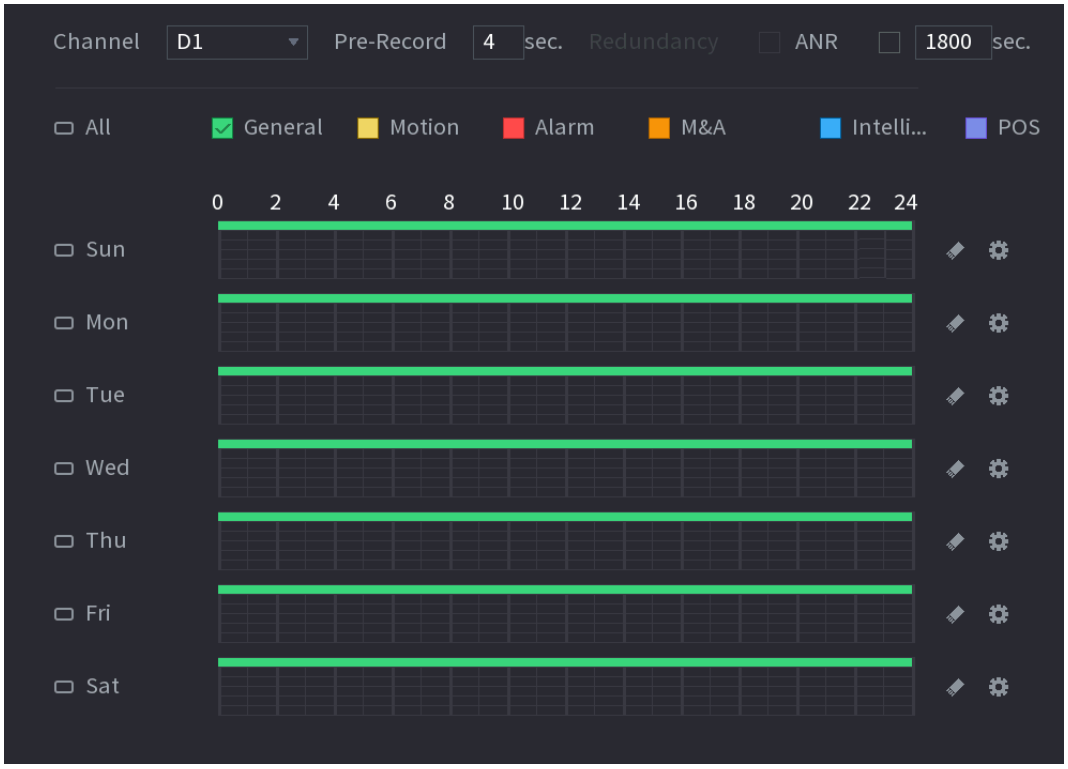
12.2.2.1 Configuring Video Recording Schedule

After you set the schedule for videos, the device will record videos according to the period you set. For example, if the alarm recording period is from 6:00–18:00 on Monday, the device will make a recording on Mondays from 6:00-18:00.

Procedure

Step 1 Right-click the live view, and then select **Main Menu** > **SETTINGS** > **STORAGE** > **Schedule** > **Record**.

Figure 12-14 Video schedule



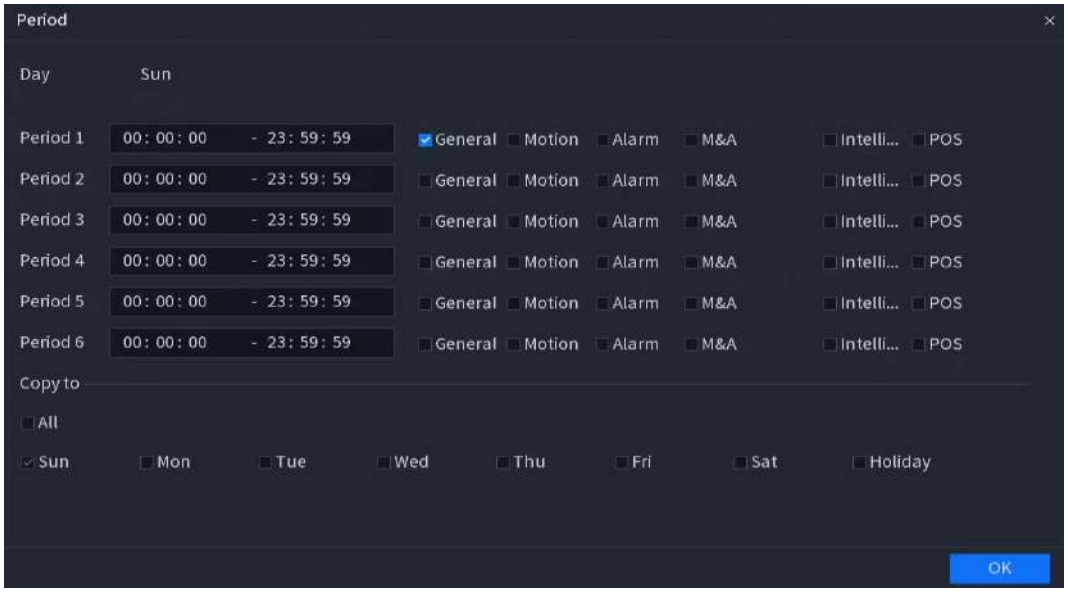
Step 2 Configure the parameters.

Table 12-13 Video schedule parameters

Parameter	Description
Channel	Select a channel to record a video.
Pre-record	Enter the amount of time that you want the pre-recording to last. A recording will be made prior to the event.

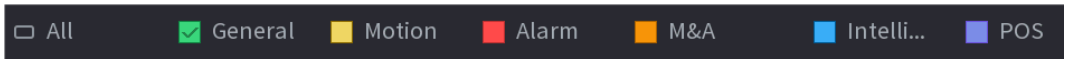
Parameter	Description
Redundancy	If there are several HDDs installed to the Device, you can set one of the HDDs as the redundant HDD to save the recorded files into different HDDs. If one of the HDDs becomes damaged, you can find the backup on the other HDD. ● Select **Main Menu** > **STORAGE** > **Disk Manager**, and then set a HDD as redundant HDD. ● Select **Main Menu** > **STORAGE** > **Schedule** > **Record**, and then select the **Redundancy** checkbox. ◇ If the selected channel is not recording, the redundancy function will take effect the next time that you record, whether or not you select the checkbox. ◇ If the selected channel is recording, the current recorded files will be packed, and then start recording according to the new schedule. ● This function is for some models only. ● The redundant HDD only backs up the recorded videos but not snapshots.
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.
Period	Set a period during which the configured recording setting is active. The system only activates the alarm in the defined period.
Copy to	Click **Copy to** to copy the settings to other channels.

Figure 12-15 Period



Step 3 Set one or more recording types from **General** , **Motion** (motion detection), **Alarm**, **M&A** (motion detection and alarm), **Intelligent** and **POS**.

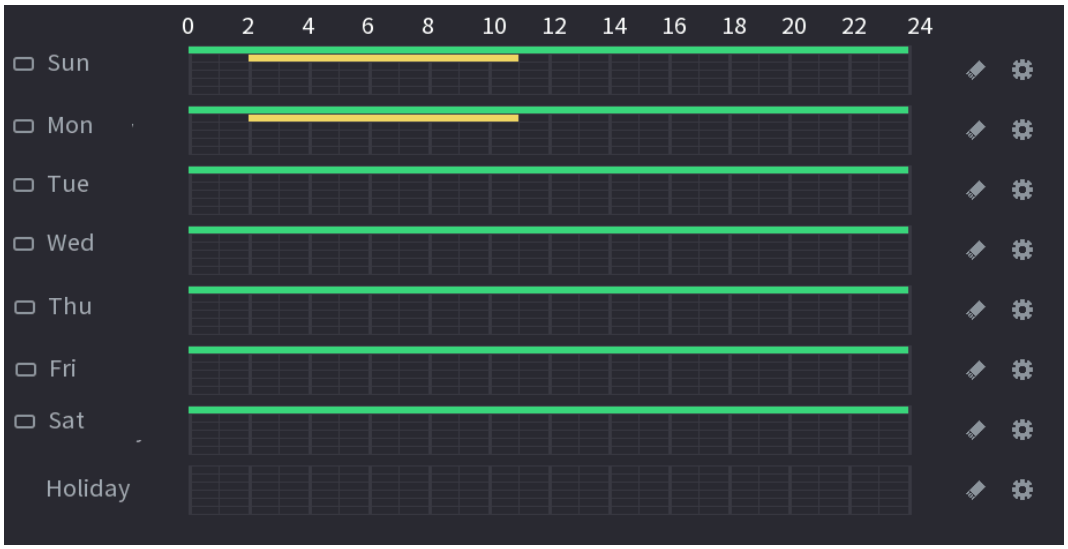
Figure 12-16 Recording type



Step 4 Set recording period.

If you have added a holiday, you can set the recording period for the holiday.

Figure 12-17 Set record period



- Define the period by drawing.
  1. Select a corresponding date to set.
     - Define for the whole week: Click next to **All**. All the icon switch to . You can define the period for all the days simultaneously.

- Define for several days of a week: Click before each day one by one. The icon switches to . You can define the period for the selected days simultaneously.

2. On the timeline, drag to define a period.
   - Once the time period overlaps, the recording priority is: **M&A** > **Alarm** > **POS** > **Intelligent** > **Motion** > **General**.
   - Select a recording type and then click the of the corresponding date to clear the corresponding period.

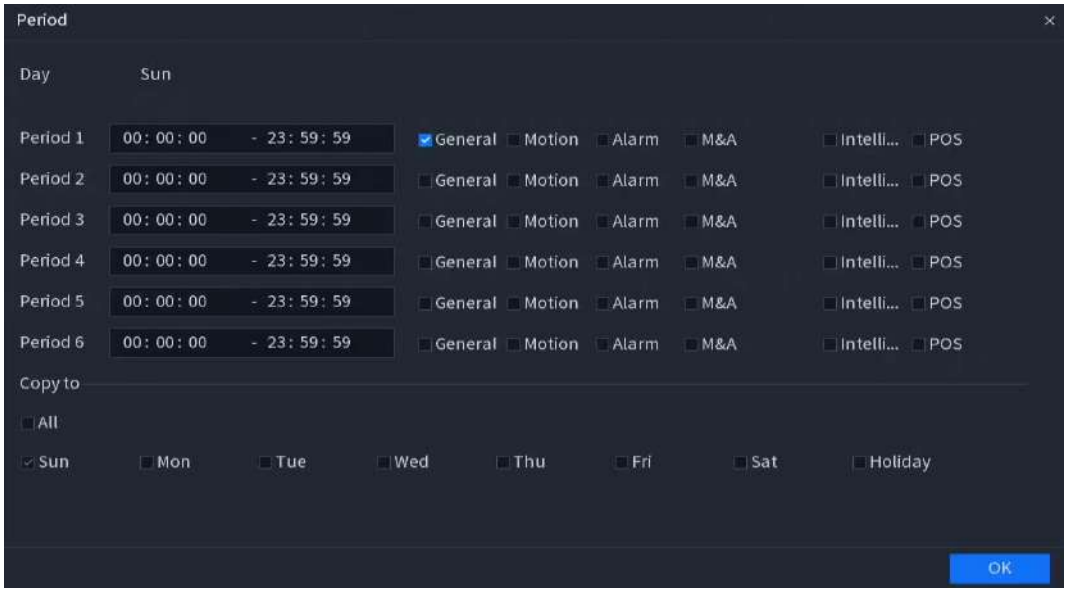
Figure 12-18 Set period by drawing

The MD record and alarm record function are both null if you enabled the function of MD&Alarm.

- Define the period by editing.

1. Select a date and then click .

Figure 12-19 Set period by editing



2. Set the recording type for each period.
   - ◇ 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.
3. Click **Apply**.

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

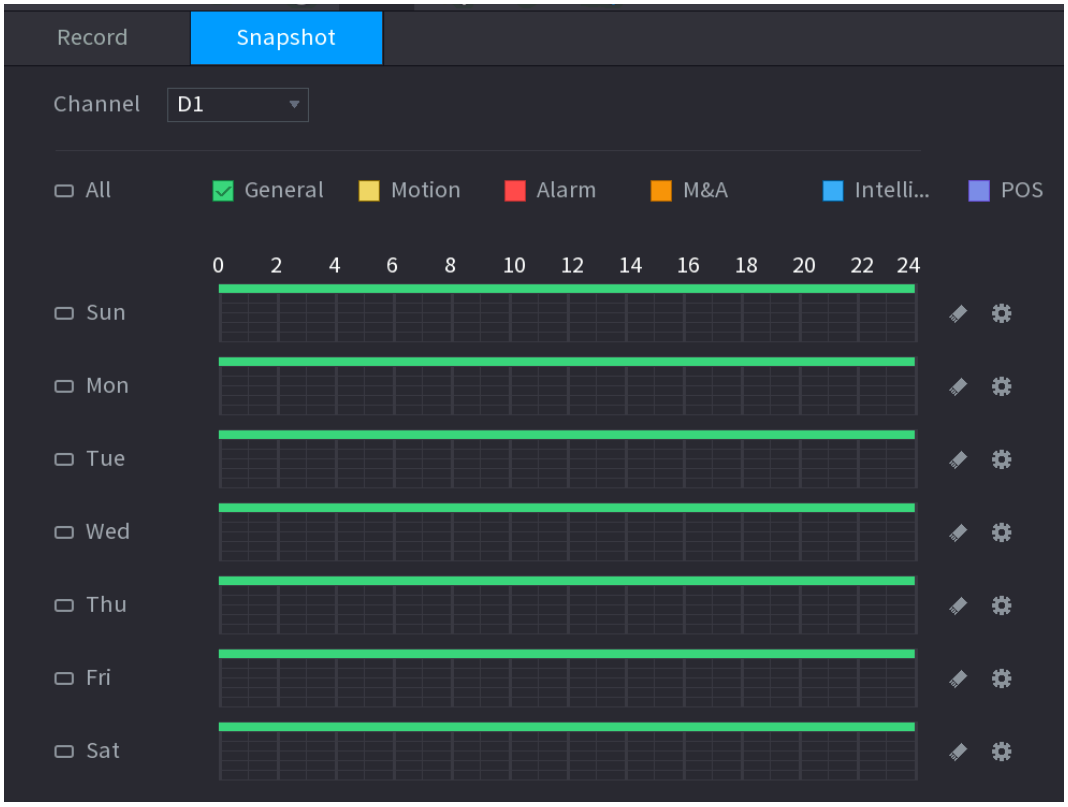
12.2.2.2 Configuring Snapshot Schedule

Configure recording schedule for snapshots.

Procedure

Step 1 Right-click the live view, and then select **Main Menu** > **SETTINGS** > **STORAGE** > **Schedule** > **Snapshot**.

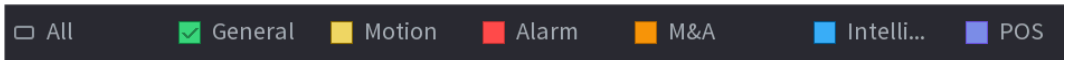
Figure 12-20 Snapshot



Step 2 Select a channel to set schedule snapshot.

Step 3 Set a recording type.

Figure 12-21 Recording type



Step 4 Set snapshot period. For details, see "12.2.2.1 Configuring Video Recording Schedule".

Step 5 Click **Apply**.

12.2.2.3 Configuring Recording Mode

Background Information

After you set schedule record or schedule snapshot, you need to enable the auto record and snapshot function so that the system can automatically record or take snapshot.

- Auto: The system automatically records the videos and snapshots according to the defined schedule.
- Manual: The system records general files for the entire day.

You need to have storage authorities to use the **Manual** recording mode.

Procedure

Step 1 Right-click the live view, and then select **Main Menu** > **SETTINGS** > **STORAGE** > **Record Mode**.

Figure 12-22 Recording mode

Step 2 Configure parameters.

Table 12-14 Recording mode parameters

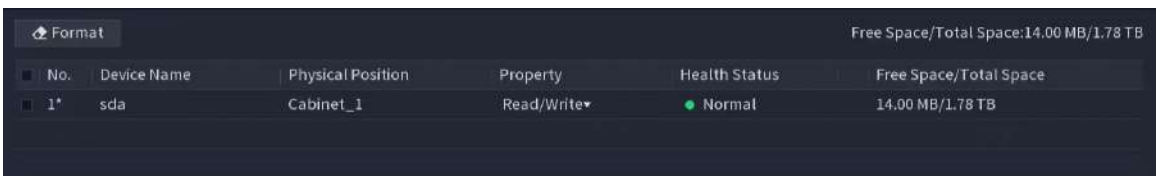
Parameter	Description
Channel	Displays all the connected channels. You can select a single channel or select **All**.
Recording status	• Auto: Automatically make recordings according to the schedule. • Manual: Makes a general recording within 24 hours for the selected channel. • Off: Do not record.
Snapshot status	Enable or disable the scheduled snapshot for the corresponding channels.

Step 3 Click **Apply**.

12.2.3 Disk Management

Select **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Manager**, and then you can set HDD properties and format HDD.

Figure 12-23 Disk management



View HDD Information

You can view the physical position, properties, status and storage capacity of each HDD.

Configure HDD Properties

In the **Properties** column, you can set read and write, read-only and redundant HDD.

When there are two or more HDDs installed on the Device, you can set one HDD as redundant disk to back up recorded files.

Format HDD

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

- Formatting will erase all data in the HDD, proceed with caution.
- You can select whether to erase the HDD database. If the HDD database is erased, the AI search data and the uploaded audio files will be deleted.

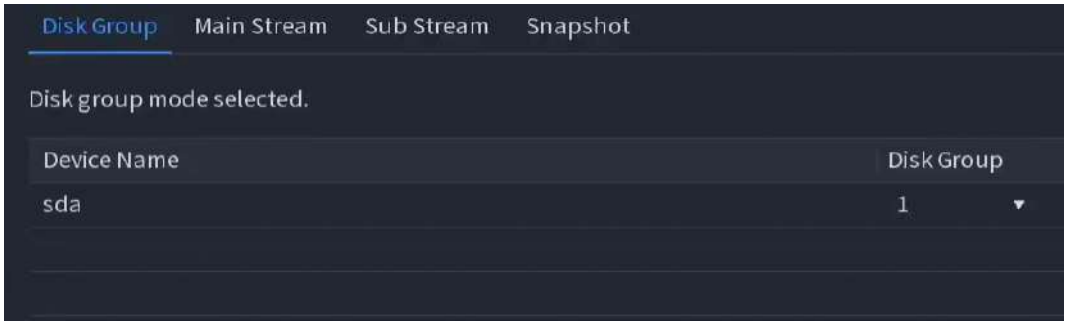
12.2.4 Disk Group

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 **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Group**.

Figure 12-24 Disk group



Step 2 (Optional) If **Disk Quota is selected** is shown on the page, click **Switch to Disk Group Mode** and then follow the on-screen instructions to format disks.

Step 3 Select the group for each HDD, and then click **Apply**.

After configuring HDD group, under the **Main Stream** tab, **Sub Stream** tab and **Snapshot** tab, configure settings to save the main stream, sub stream and snapshot to different disk groups.

12.2.5 Disk Quota

You can allocate a certain storage capacity for each channel to manage the storage space properly.

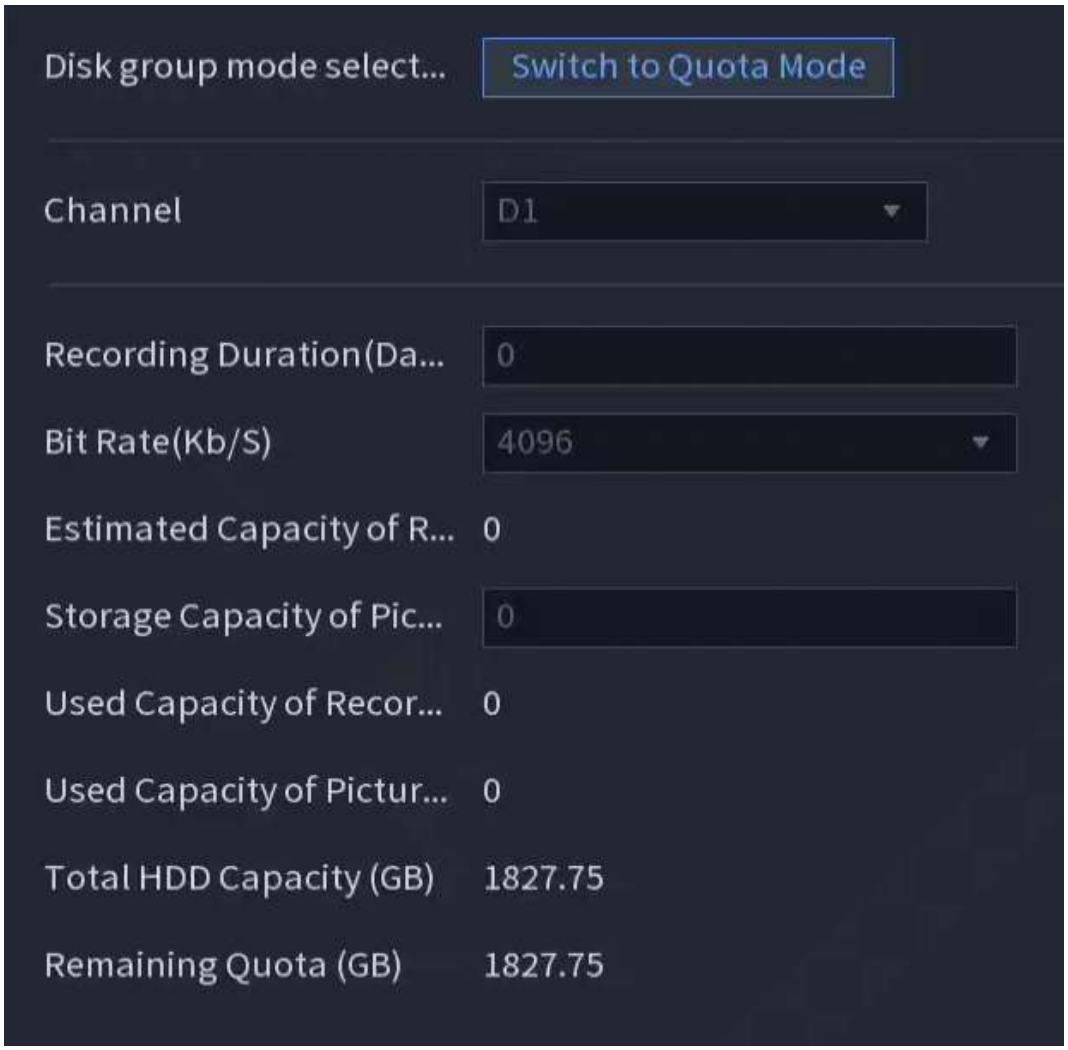
Background Information

- If **Disk group mode selected.** is shown in the page, click **Switch to Quota Mode**.
- Disk quota mode and disk group mode cannot be selected at the same time.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Quota**.

Figure 12-25 Disk Quota



Step 2 (Optional) If **Disk group mode selected** is shown on the page, click **Switch to Quota Mode** and then follow the on-screen instructions to format disks.

Step 3 Select a channel and set the record duration, bit rate and storage capacity of picture.

Step 4 Click **Apply**.

12.2.6 Disk Check

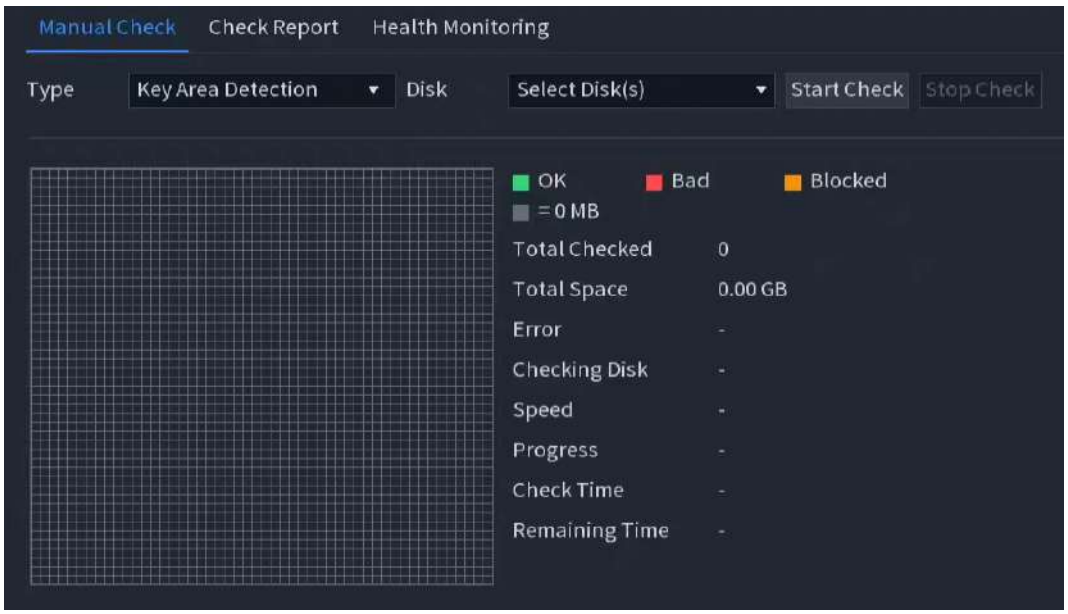
The system can detect HDD status so that you can clearly understand the HDD performance and replace the malfunctioning HDD.

12.2.6.1 Manual Check

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Check** > **Manual Check**.

Figure 12-26 Manual check



Step 2 Select the detection type.

- Key area detect: The system detects the used space of the HDD through the built-in file system. This type of detection is efficient.
- Global detection: The system detects the entire HDD through Window. This type of detection takes time and might affect the HDD that is recording.

Step 3 Select the HDD that you want to detect.

Step 4 Click **Start Check**.

The system starts detecting the HDD and displays the detection information.

When system is detecting HDD, click **Stop Check** to stop current detection. Click **Start Check** to detect again.

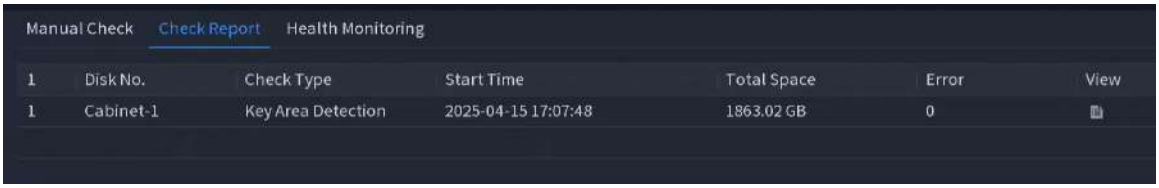
12.2.6.2 Detection Report

After the detection, you can view the detection report.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Check** > **Check Report**.

Figure 12-27 Check report



Step 2 Click to view detection results and S.M.A.R.T report.

Figure 12-28 Results

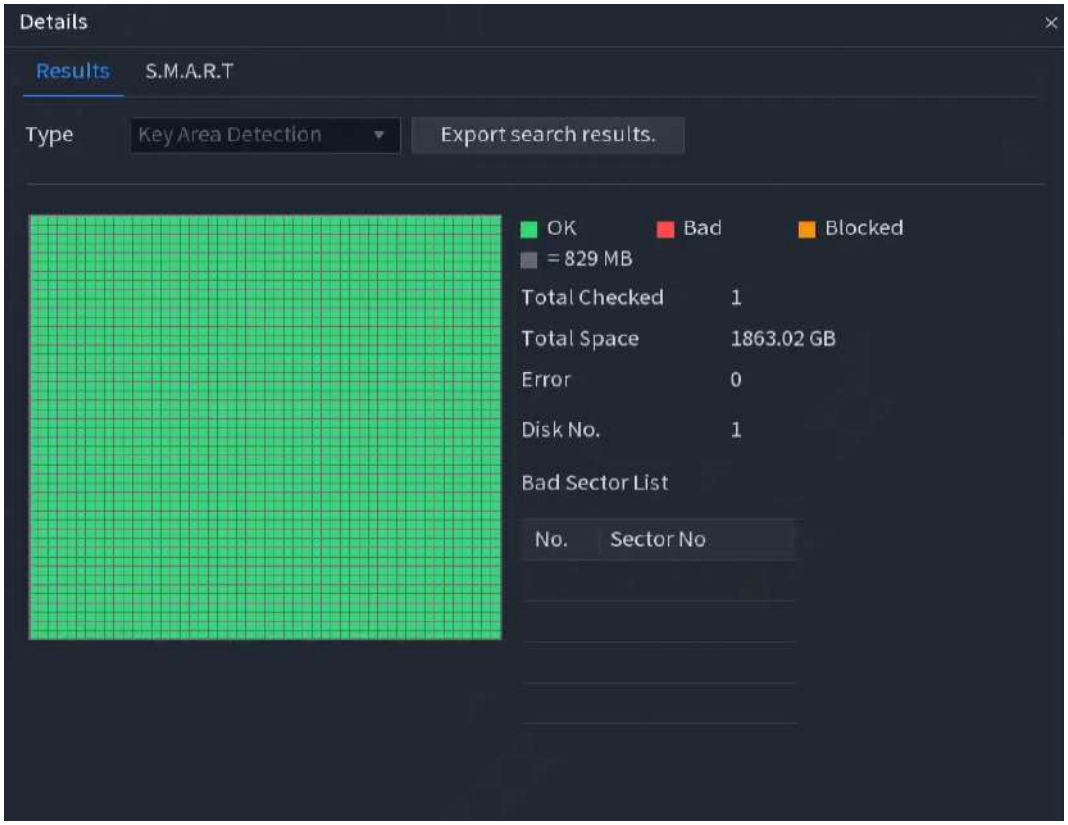
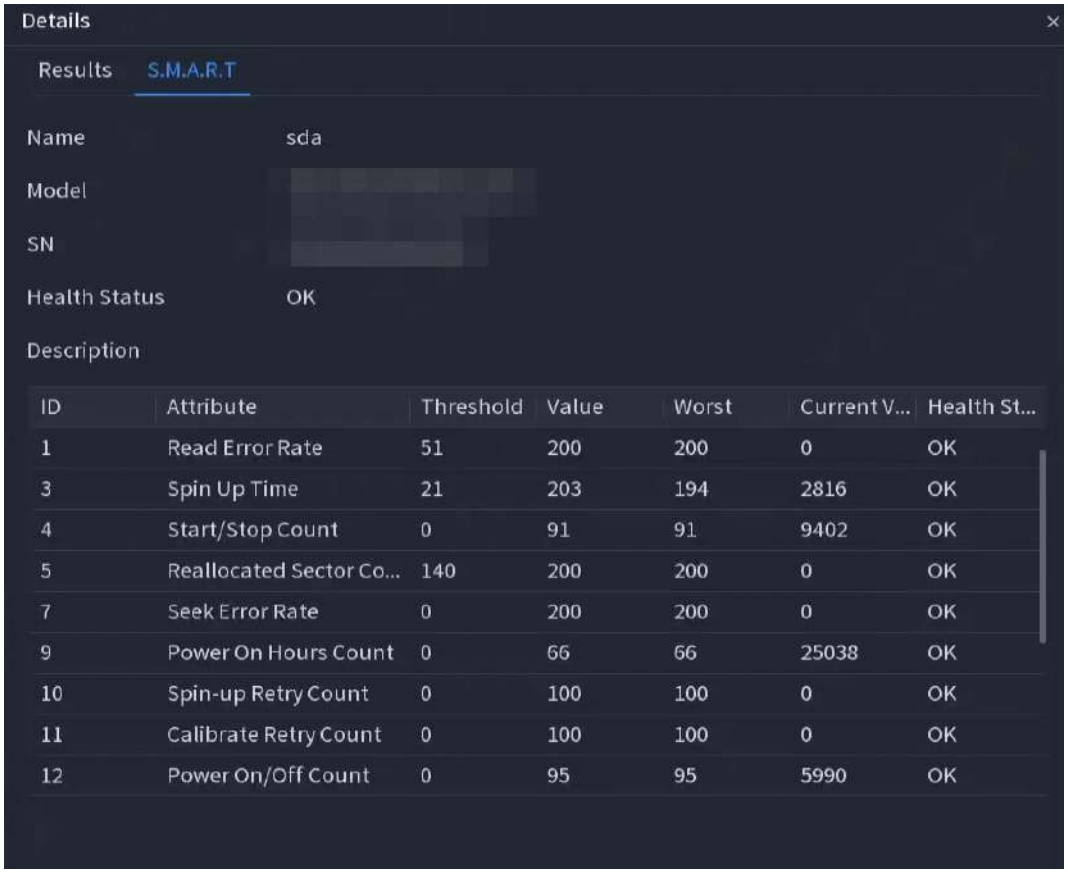


Figure 12-29 S.M.A.R.T



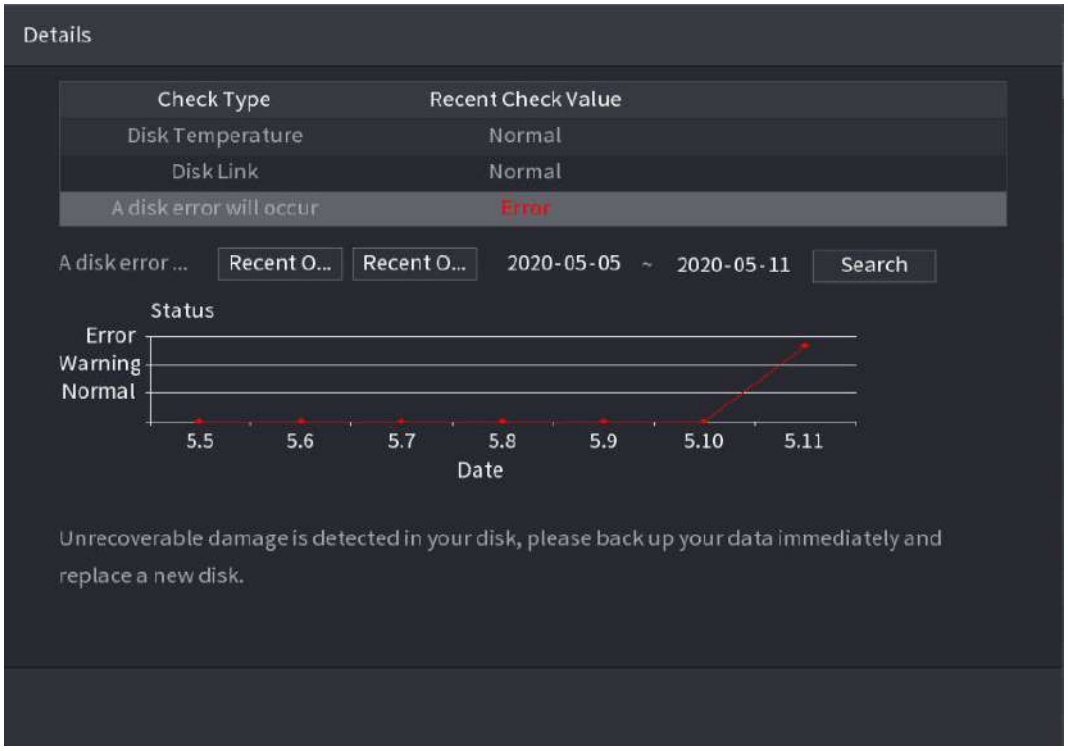
12.2.6.3 Disk Health Monitoring

Monitor health status of disks, and repair if any exceptions are found so as to avoid data loss.

Select **Main Menu** > **SETTINGS** > **STORAGE** > **Disk Check** > **Health Monitoring**.

Click to show disk details page. Then select **Check Type** , set time period, and then click **Search**. The system shows the details of disk monitoring status.

Figure 12-30 Disk details



12.2.7 Record Estimate

Record estimate function can calculate how long you can record video according to the HDD capacity, and calculate the required HDD capacity according to the record period.

Procedure

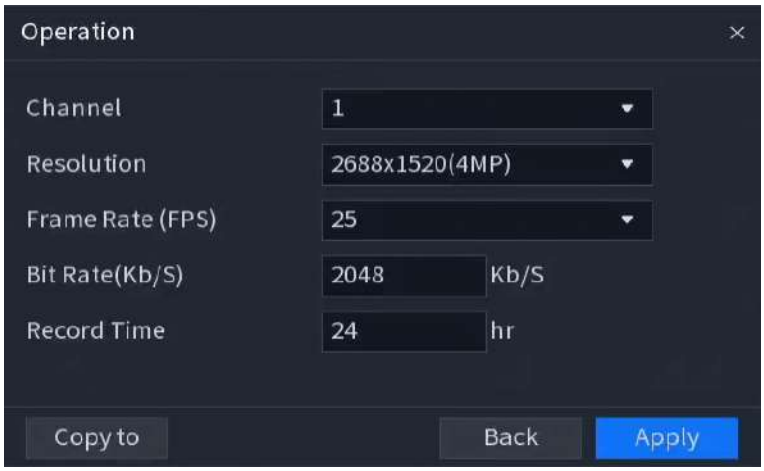
Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **Rec Estimate**.

Figure 12-31 Record estimation

Step 2 Click .

You can configure the **Resolution** , **Frame Rate**, **Bit Rate** and **Record Time** for the selected channel.

Figure 12-32 Modify channel settings



Step 3 Click **Apply**.

Then the system will calculate the time period that can be used for storage according to the channels settings and HDD capacity.

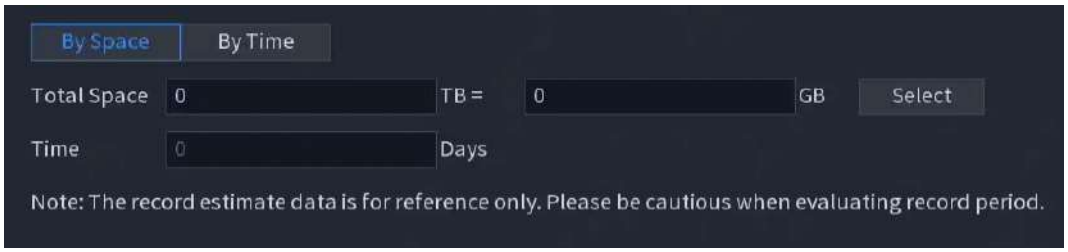
Click **Copy to** to copy the settings to other channels.

12.2.7.1 Calculating Recording Time

Procedure

Step 1 On the **Rec Estimate** page, click the **By Space** tab.

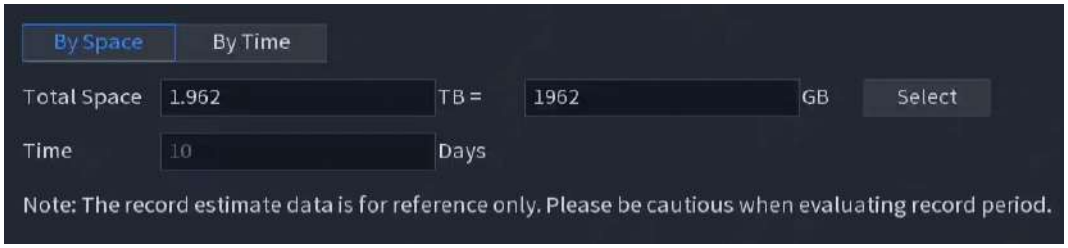
Figure 12-33 By space



Step 2 Click **Select**.

Step 3 Select the checkbox of the HDD that you want to calculate.

Figure 12-34 Recording time

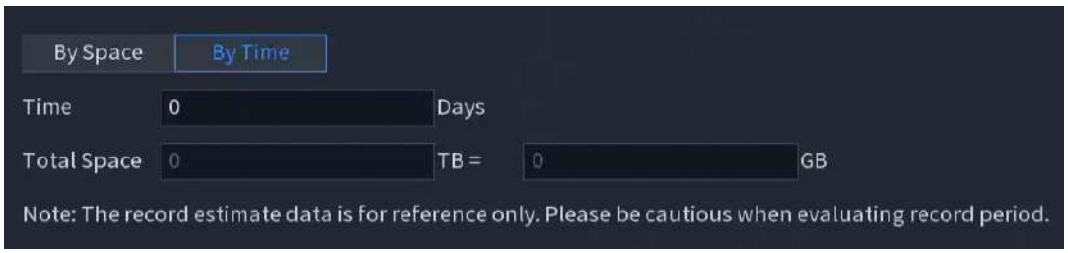


12.2.7.2 Calculating HDD Capacity for Storage

Procedure

Step 1 On the **Rec Estimate** page, click the **By Time** tab.

Figure 12-35 By time



Step 2 In the **Time** box, enter the time period that you want to record.

In the **Total Space** box, the required HDD capacity is displayed.

12.2.8 FTP

You can store and view the recorded videos and snapshots on the FTP server.

Prerequisites

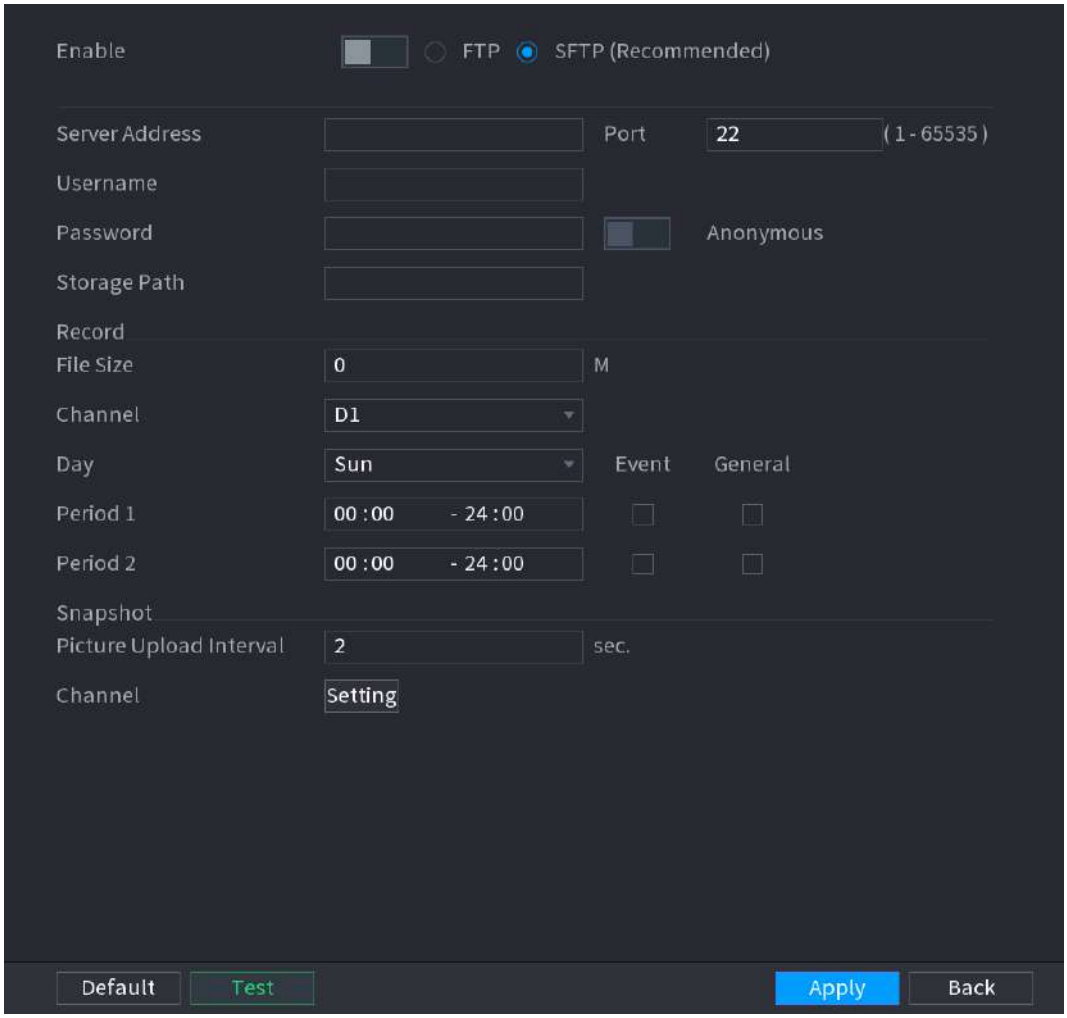
Purchase or download a FTP (File Transfer Protocol) server and install it on your PC.

For the created FTP user, you need to set the write permission; otherwise the upload of recorded videos and snapshots will be failed.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **FTP**.

Figure 12-36 FTP



Step 2 Configure the parameters.

Table 12-15 FTP parameters

Parameter	Description
Enable	Enable the FTP upload function.
FTP type	Select FTP type. ● FTP: Plaintext transmission. ● SFTP: Encrypted transmission (recommended).
Server Address	IP address of FTP server.
Port	Enter the port of the FTP server. ● FTP: The default is 21. ● SFTP: The default is 22.
Username	Enter the username and password to log in to the FTP server. If you enable the anonymity function, you can log in anonymously without entering the username and password.
Password	
Anonymous	

Parameter	Description
Storage Path	Create folder on FTP server. ● If you do not enter the name of remote directory, the system automatically creates the folders according to the IP and time. ● If you enter the name of remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.
File Size	Enter the length of the uploaded recorded video. ● If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. ● If the entered length is more than the recorded video length, the whole recorded video can be uploaded. ● If the entered length is 0, the whole recorded video will be uploaded.
Picture Upload Interval	● If this interval is longer than snapshot interval, the system takes the recent snapshot to upload. For example, the interval is 5 seconds, and snapshot interval is 2 seconds per snapshot, the system uploads the recent snapshot every 5 seconds. ● If this interval is shorter than snapshot interval, the system uploads the snapshot per the snapshot interval. For example, the interval is 5 seconds, and snapshot interval is 10 seconds per snapshot, the system uploads the snapshot every 10 seconds. ● To configure the snapshot interval, go to **Main Menu** > **REMOTE DEVICE** > **Camera Setting** > **Encode** > **Snapshot**.
Channel	Select the channel that you want to apply the FTP settings.
Day	Select the week day and set the time period that you want to upload the recorded files. You can set two periods for each week day.
Period 1, Period 2	
Record type	Select the record type (Alarm, Intel, MD, and General) that you want to upload. The selected record type will be uploaded during the configured time period.

Step 3 Click **Test** to validate the FTP connection.

If FTP connection failed, check the network and FTP settings.

Step 4 Click **Apply**.

12.2.9 iSCSI

Internet Small Computer Systems Page (iSCSI) is a transport layer protocol that works on top of the Transport Control Protocol (TCP), and enables block-level SCSI data transport between the iSCSI initiator and the storage target over TCP/IP networks. After the network disk is mapped to the NVR device through iSCSI, the data can be stored on the network disk.

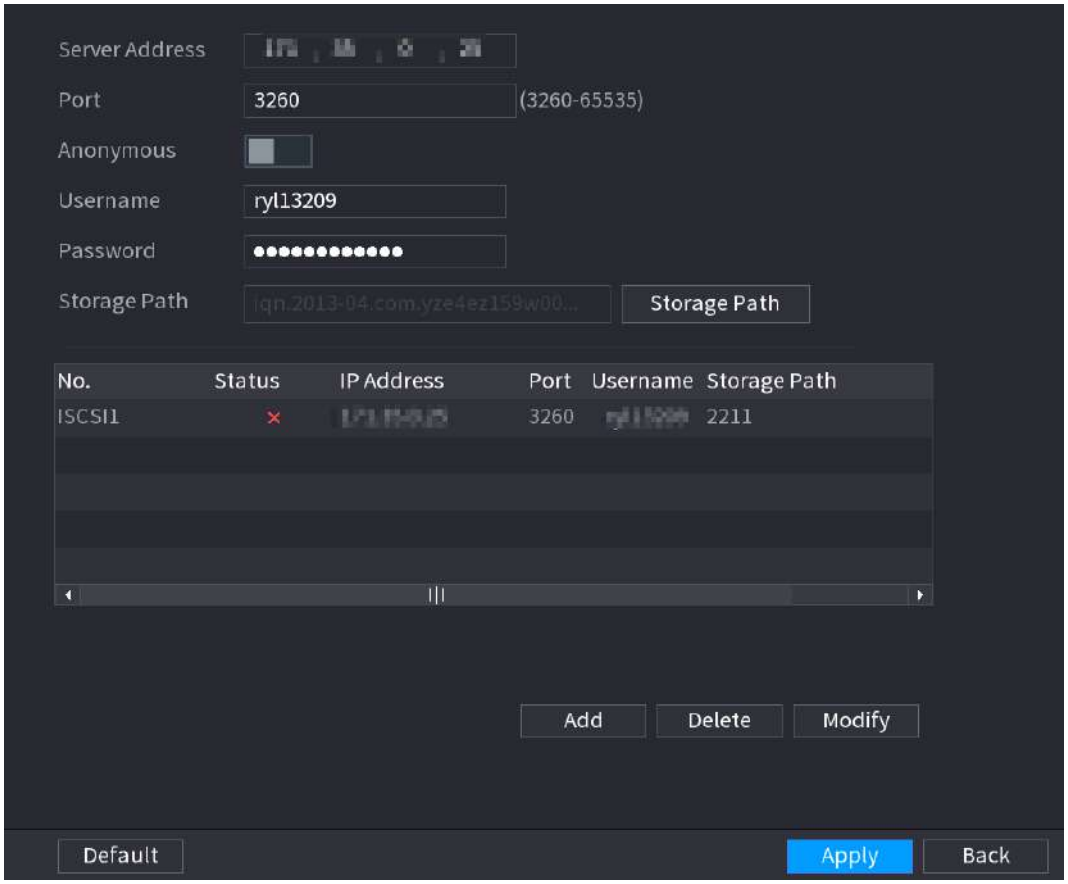
Background Information

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **STORAGE** > **iSCSI**.

Figure 12-37 iSCSI



Step 2 Set parameters.

Table 12-16 iSCSI parameters

Parameter	Description
Server Address	Enter the server address of iSCSI server.
Port	Enter the port of iSCSI server, and the default value is 3260.
Storage Path	Click **Storage Path** to select a remote storage path. Each path represents an iSCSI shared disk and these paths are generated when created on the server.
Username, Password	Enter the username and password of iSCSI server. If anonymous login is supported by iSCSI server, you can enable **Anonymous** to log in as an anonymous user.

Step 3 Click **Apply**.

12.3 POS Settings

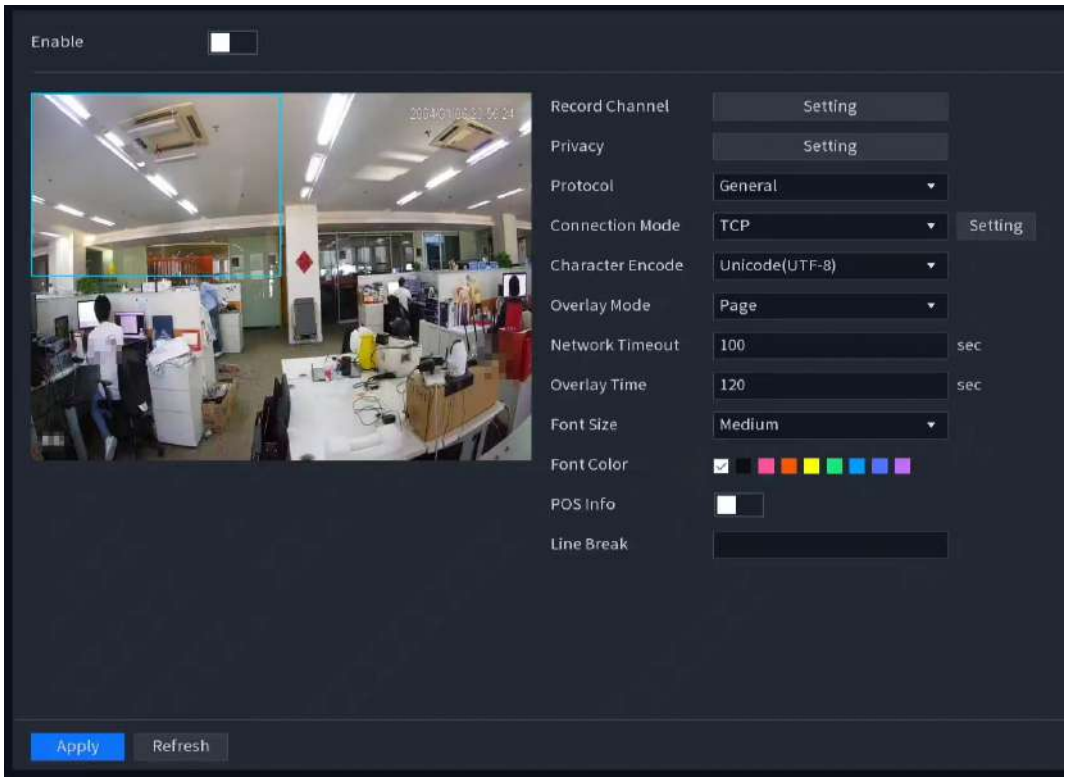
Background Information

You can connect the device to the POS (Point of Sale) machine and receive the information from it. This function applies to the scenarios such as supermarket POS machine. After connection is established, the device can access the POS information and display the overlaid text in the channel window.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **POS** > **POS Setting**.

Figure 12-38 POS settings



Step 2 Configure the POS parameters.

Table 12-17 POS parameters

Parameter	Description
POS Name	In the POS Name list, select the POS machine that you want to configures settings for. Click to modify the POS name. ● The POS name must be unique. ● You can enter up to 21 Chinese characters or 63 English characters.
Enable	Enable the POS function.
Record Channel	Click to select a channel to record.
Privacy	Enter the privacy contents.
Protocol	Select a protocol. Different machines correspond to different protocols.

Parameter	Description
Connection Mode	Select the connection protocol type. Click , the **IP Address** window is displayed. In the **Source IP** box, enter the IP address (the machine that is connected to the Device) that sends messages.
Character Encode	Select a character encoding mode.
Overlay Mode	In the **Overlay Mode** list, Select **Turn** or **ROLL**. • Turn: Once the information is at 16 lines, system displays the next page. • ROLL: Once the information is at 16 lines, system rolls one line after another to delete the first line. When the local preview mode is in 4-split, the turn/ROLL function is based on 8 lines.
Network Timeout	When the network is not working correctly and cannot be recovered after the entered timeout limit, the POS information will not display normally. After the network is recovered, the latest POS information will be displayed.
Overlay Time	Enter the time that how long you want to keep the POS information displaying. For example, enter 5, the POS information disappear from the screen after 5 seconds.
Font Size	Select **Small** , **Medium**, or **Big** as the text size of POS information
Font Color	In the color bar, click to select the color for the text size of POS information.
POS Info	Enable the POS Info function, the POS information displays in the live view/ WEB.
Line Break	There is no line delimiter by default. After you set the line delimiter (HEX), the overlay information after the delimiter is displayed in the new line. For example, the line delimiter is F and the overlay information is 123F6789, NVR displays overlay information on the local preview page and Web as: 123 6789

Step 3 Click **Apply**.

12.3.1 Privacy Setup

Procedure

Step 1 Click **Setting** next to **Privacy**.

Figure 12-39 Privacy

Step 2 Set privacy information.

Step 3 Click **OK**.

12.3.2 Connection Mode

Connection type is UDP or TCP.

Procedure

Step 1 Select **Connection Mode** as **UDP**, **TCP_CLINET** or **TCP**.

Step 2 Click **Setting**.

Figure 12-40 IP address

Step 3 For **Source IP** and **Port**, enter the POS IP address and port.

Step 4 Click **OK**.

12.4 System Settings

12.4.1 General Settings

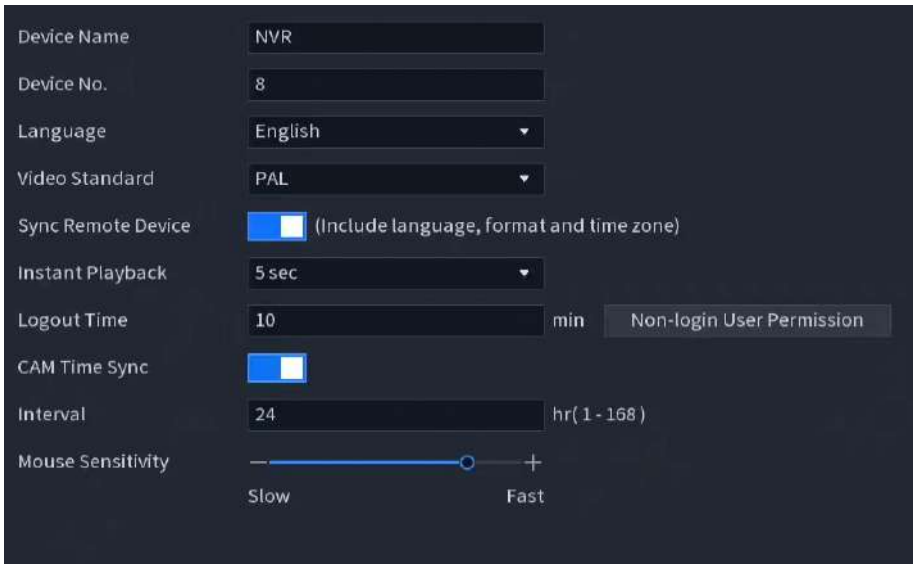
12.4.1.1 Basic

You can set device basic information such as device name, and serial number.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **General** > **Basic**.

Figure 12-41 Basic settings



Step 2 Configure parameters.

Table 12-18 Basic parameters

Parameter	Description
Device Name	Enter the Device name.
Device No.	Enter a number for the Device.
Language	Select a language for the Device system.
Video Standard	Select **PAL** or **NTSC** as needed.
Sync Remote Device	Enable this function; the NVR can synchronize information with the remote device such as language, format and time zone.
Instant Playback	In the **Instant Play** box, enter the time length for playing back the recorded video. The value ranges from 5 to 60. On the live view control bar, click the instant playback button to play back the recorded video within the configured time.
Logout Time	Enter the standby time for the device. The device automatically logs out when it is not working in the configured period. You need to log in to the device again. The value ranges from 0 to 60. 0 indicates there is not standby time for the Device. Click **Non-login User Permission**. You can select the channels that you want to continue monitoring when you logged out.
CAM Time Sync	Syncs the Device time with IP camera.

Parameter	Description
Interval	Enter the interval for time sync.
Mouse Sensitivity	Adjust the speed of double-click by moving the slider. The bigger the value is, the faster the speed is.

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

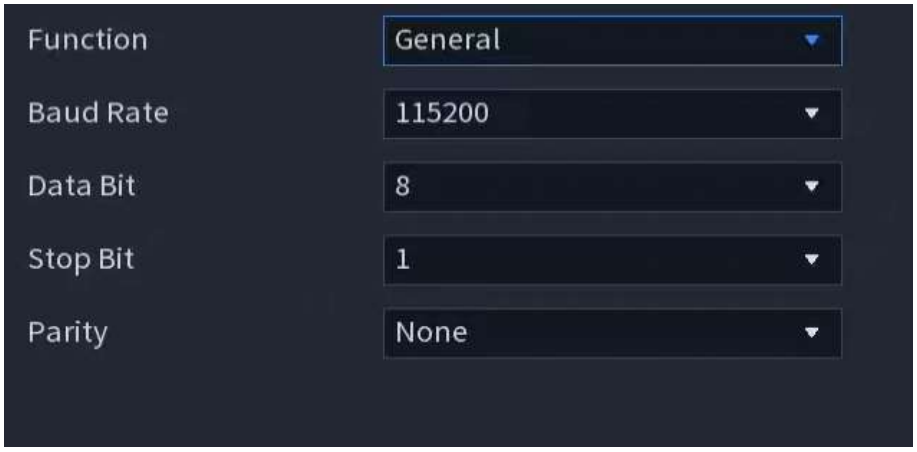
12.4.1.2 Serial Port

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

Procedure

Step 1 Select **MAIN MENU** > **SETTINGS** > **SYSTEM** > **General** > **Serial Port**.

Figure 12-42 Serial port



Step 2 Configure parameters.

Table 12-19 Serial port parameters

Parameter	Description
Function	Select serial port control protocol. • Console: Upgrade the program and debug with the console and mini terminal software. • Keyboard: Control this Device with special keyboard. • Adapter: Connect with PC directly for transparent transmission of data. • Protocol COM: 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 Bit	It ranges from 5 to 8, which is 8 by default.

Parameter	Description
Stop Bit	It includes 1 and 2.
Parity	It includes none, odd, even, mark and null.

Step 3 Click **Apply**.

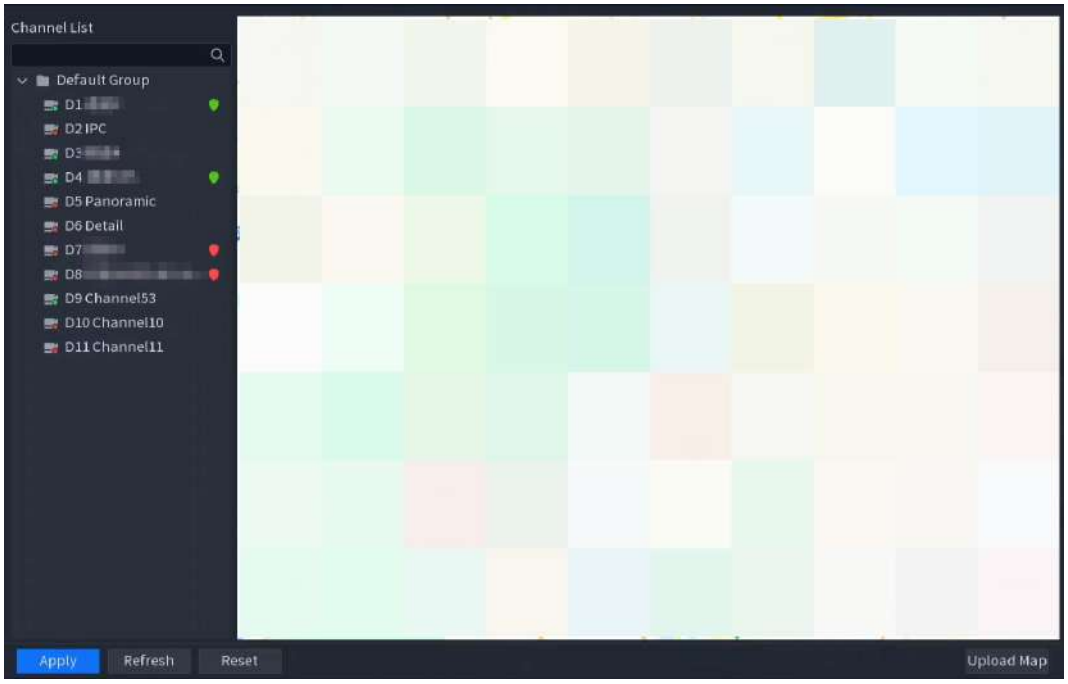
12.4.1.3 E-map

You can view the target's trajectory through the E-map with the AcuPick function. A clear E-map should be uploaded and you are required to drag devices to corresponding locations.

Procedure

Step 1 Select **MAIN MENU** > **SETTINGS** > **SYSTEM** > **General** > **E-map**.

Figure 12-43 E-map



Step 2 Click **Upload Map** to upload the E-map.

Step 3 Select devices on the left list to drag them to the map location.

Step 4 Click **Apply**.

12.4.2 Time

12.4.2.1 Date and Time

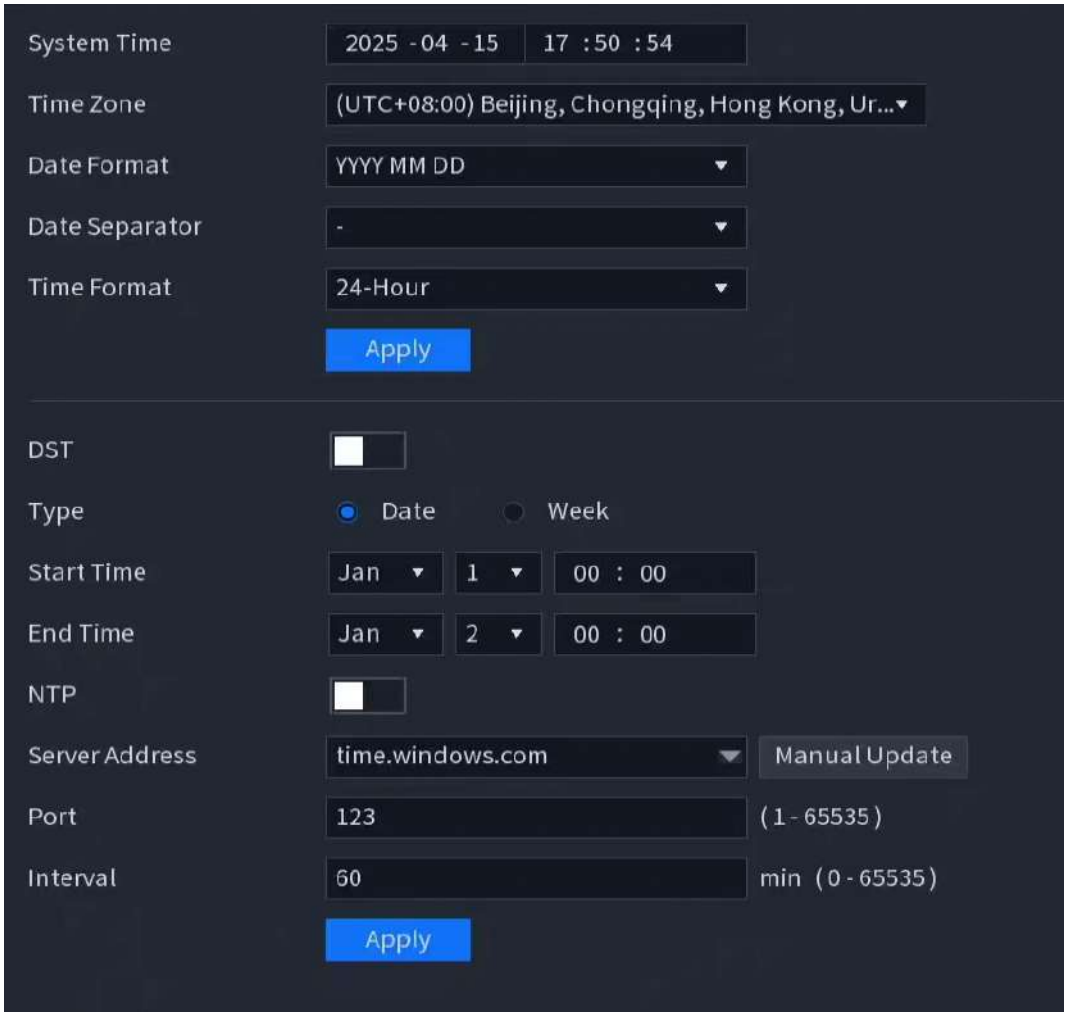
You can set device time. You can enable NTP (Network Time Protocol) function so that the device can sync time with the NTP server.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Time** > **Date&Time**.

Step 2 Click **Date&Time** tab.

Figure 12-44 Date and time



Step 3 Configure the settings for date and time parameters.

Table 12-20 Description of data and time parameters

Parameter	Description
System Time	In the **System Time** box, enter time for the system. After clicking the time zone list, you can select a time zone for the system, and the time will 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.
Time Zone	In the **Time Zone** list, select a time zone for the system.
Date Format	In the **Date Format** list, select a date format for the system.
Date Separator	In the **Date Separator** list, select a separator style for the date.
Time Format	In the **Time Format** list, select **12-HOUR** or **24-HOUR** for the time display style.

Parameter	Description
DST	Enable the Daylight Saving Time function. Click **Week** or **Date**.
Type	
Start Time	Configure the start time and end time for the DST.
End Time	
NTP	Enable the NTP function to sync the Device time with the NTP server. If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the **Server Address** box, enter the IP address or domain name of the corresponding NTP server. You can directly select **time.windows.com** or **time.google.com**. Click **Manual Update**, the Device starts syncing with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the **Interval** box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

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

12.4.2.2 Holiday

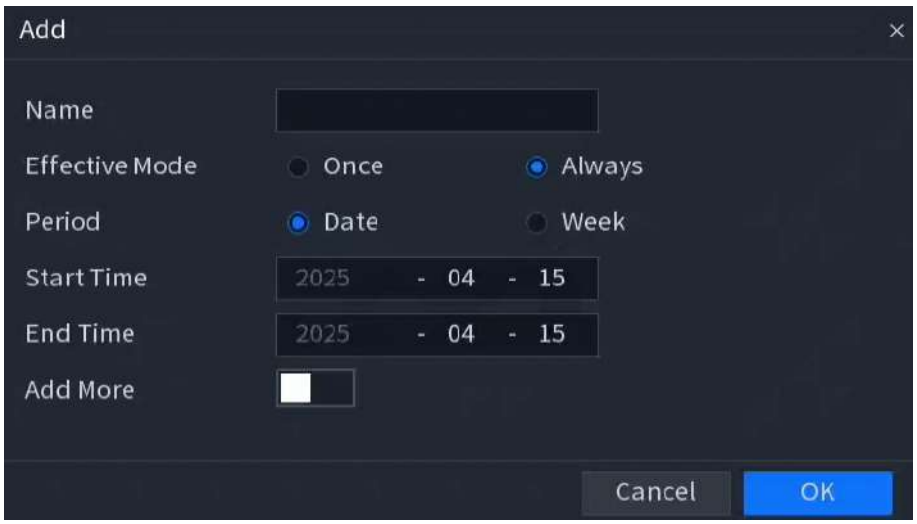
Here you can add, edit, and delete holiday. After you successfully set holiday information, you can view holiday item on the record and snapshot period.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Time** > **Holiday**.

Step 2 Click **Add** to add the holiday.

Figure 12-45 Add the holiday



Step 3 Configure holiday name, effective mode, period and starting and ending times.

Click **Add more** to add new holiday information.

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

- Click under **Status**, you can enable or disable the holiday.
- Click to change the holiday information. Click to delete current date.

Step 5 Click **Next** to save settings.

12.4.3 Output and Display

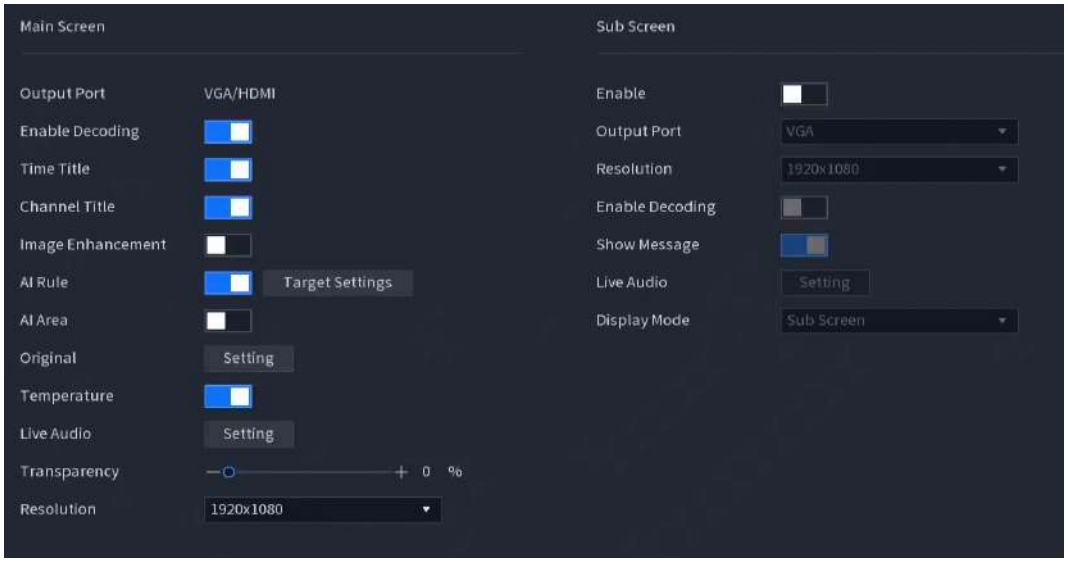
12.4.3.1 Display

You can configure the display effect such as displaying time title and channel title, adjusting image transparency, and selecting the resolution.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Display** > **Display**.

Figure 12-46 Display



Step 2 Configure parameters.

Table 12-21 Description of display parameters

Parameter	Description
Main Screen/Sub Screen	Configure the output port format of both screens. ● When sub screen is disabled, the format of main screen is HDMI/VGA simultaneous output. ● When sub screen is enabled, the format of main screen and sub screen are non-simultaneous outputs. ◇ When output port of sub screen is set to **HDMI** , the output port of main screen is set to **VGA** by the device. ◇ When output port of sub screen is set to **VGA** , the output port of main screen is set to **HDMI** by the device.
Enable Decoding	After it is enabled, the device can normally decode.
Time Title/Channel Title	Enable it and the date and time of the system will be displayed in the preview screen.
Image Enhancement	Enable it to optimize the preview image edges.
AI Rule	Enable it to display the AI rules in the live view page. This function is available on select models.
AI Area	Enable it to display the AI area in the live view page. This function is available on select models.
Original	Click **Setting**, and then select the channel to restore the corresponding channel image to the original scale.
Temperature	Click to measure the temperature of the heat sources in the image, which also includes tracking high and low temperatures.
Live Audio	Configure audio input on live view. You can select **Audio 1** , **Audio 2**, and **Mixing**. For example, if you select **Audio 1** for **D1** channel, the sound of audio input port 1 of camera is playing. If you select **Mixing**, the sound of all audio input ports are playing.
Transparency	Set the transparency of the local menu of the NVR device. The higher the transparency, the more transparent the local menu.
Resolution	Support 1920 × 1080, 1280 × 1024 (default), 1280 × 720.
Show Message	Click to enable the show message function of the sub screen.

Step 3 Click **Apply**.

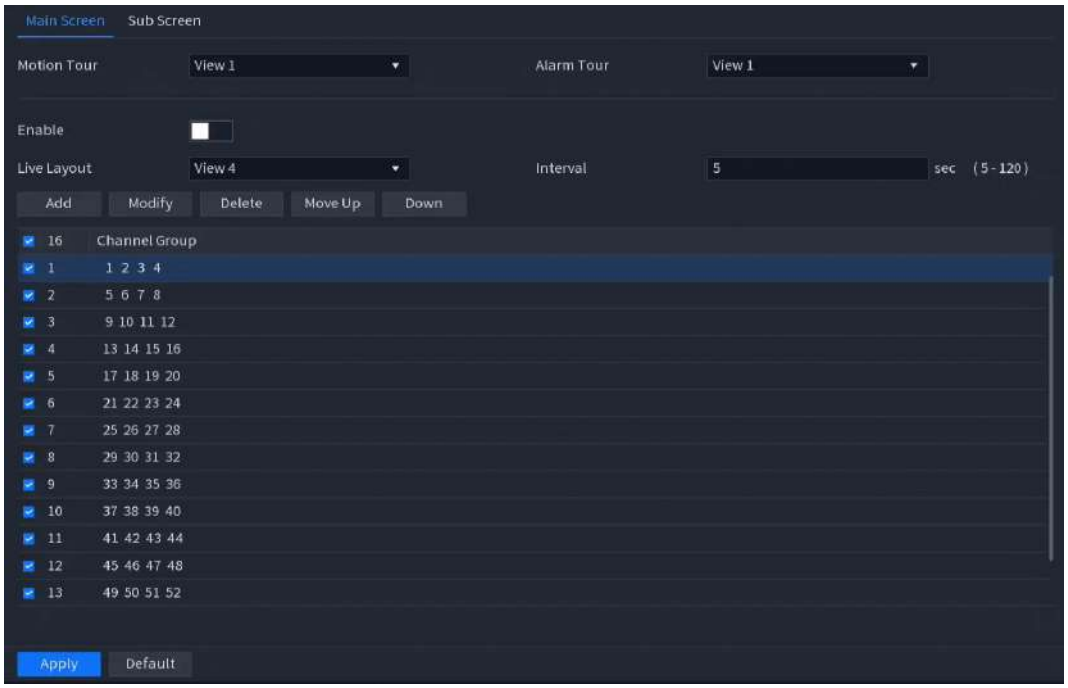
12.4.3.2 Tour Settings

You can configure a tour of selected channels to repeat playing videos. The videos display 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 **Main Menu** > **SETTINGS** > **SYSTEM** > **Display** > **Tour Settings** > **Main Screen**.

Figure 12-47 Tour



- On the upper right of the live view screen, use the left mouse button or press Shift to switch between (image switching is allowed) and (image switching is not allowed) to turn on/off the tour function.
- On the navigation bar, click to enable the tour and click to disable it.

Step 2 Configure the tour setting parameters.

Table 12-22 Tour parameters

Parameter	Description
Enable Tour	Enable tour function.
Interval	Enter the amount of time that you want each channel group displays on the screen. The value ranges from 5 seconds to 120 seconds, and the default value is 5 seconds.
Motion Tour, Alarm Tour	Select the View 1 or View 8 for **Motion Tour** and **Alarm Tour** (system alarm events).
Live Layout	In the **Live Layout** list, select **View 1**, **View 4**, **View 8**, or other modes that are supported by the Device.

Parameter	Description
Channel Group	Displays all channel groups under the current Window Split setting. • Add a channel group: Click **Add**, in the pop-up **Add Group** channel, select the channels to form a group, and then click **Save**. • Delete a channel group: Select the checkbox of any channel group, and then click **Delete**. • Edit a channel group: Select the checkbox of any channel group and then click **Modify**, or double-click on the group. The **Modify Channel Group** dialog box is displayed. You can regroup the channels. • Click **Move up** or **Move down** to adjust the position of channel group.

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

12.4.4 Account

You can manage users, user group and ONVIF user, and set admin security questions.

12.4.4.1 User

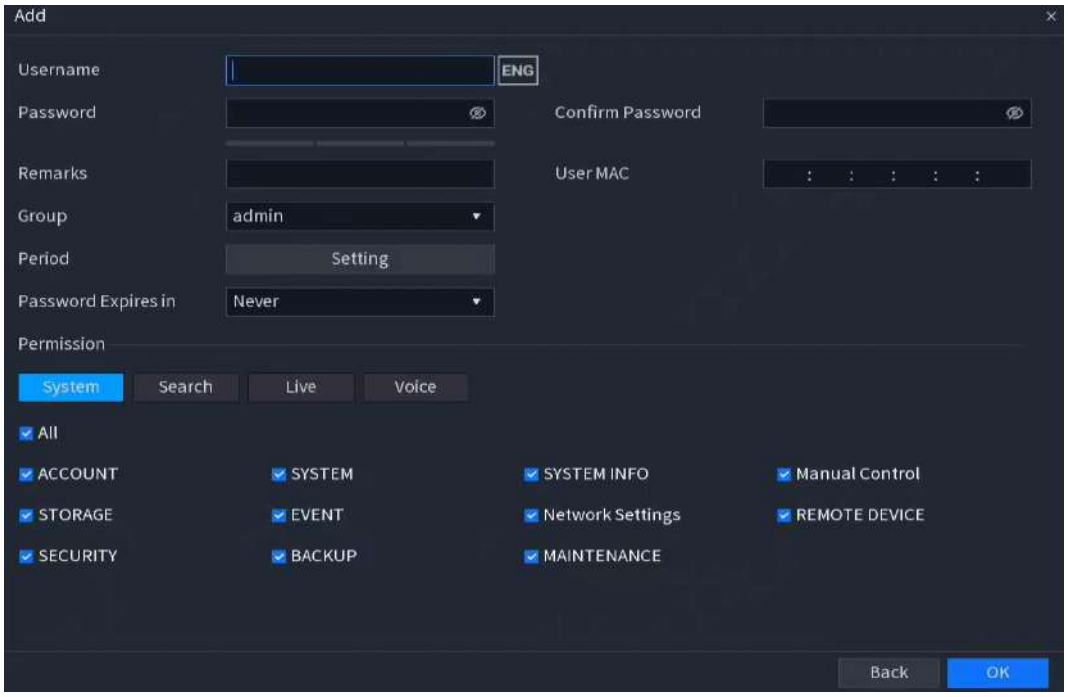
12.4.4.1.1 Adding User

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **User**.

Step 2 Click **Add**.

Figure 12-48 Add user



Step 3 Configure the parameters.

Table 12-23 Parameters of adding user

Parameter	Description
Username	Enter a username and password for the account.
Password	
Confirm Password	Enter the password again to confirm it.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address.
Group	Select a group for the account. The user rights must be within the group permissions.
Period	Click **Setting** to define a period during which the new account can log in to the Device. The new account cannot access the device during other periods.
Password Expires in	Select a period that password expires and until that time, a new password is required.
Permission	Select the checkboxes to grant permissions to the user. To manage the user account easily, when defining the user account permission, do not give the authority to the common user account higher that the advanced user account.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete the user.

12.4.4.1.2 Modifying Password

We recommend you change the password regularly to enhance device security.

Background Information

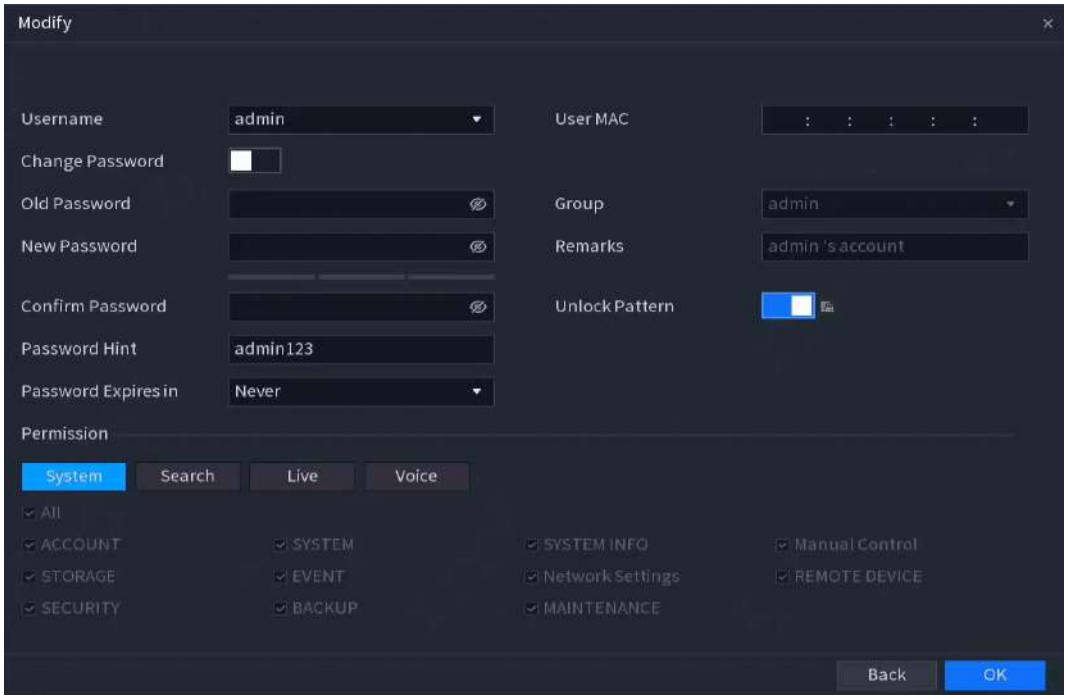
Users with account permissions can change the password of other users.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **User**.

Step 2 Click of the corresponding user.

Figure 12-49 Modify Password



Step 3 Click to enable the modify password function.

Step 4 Enter old password and then enter new password twice.

- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- For your device security, create a strong password.

Step 5 Click to enable the unlock pattern function, and then click to draw the pattern.

Step 6 Modify user's permission.

Select **System** , **Search**, **Live**, or **Voice** to rearrange user's permissions.

Step 7 Click **OK**.

12.4.4.2 Group

The accounts of the Device adopt two-level management modes: user and user group. Every user must belong to one group, and only one group.

Background Information

The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

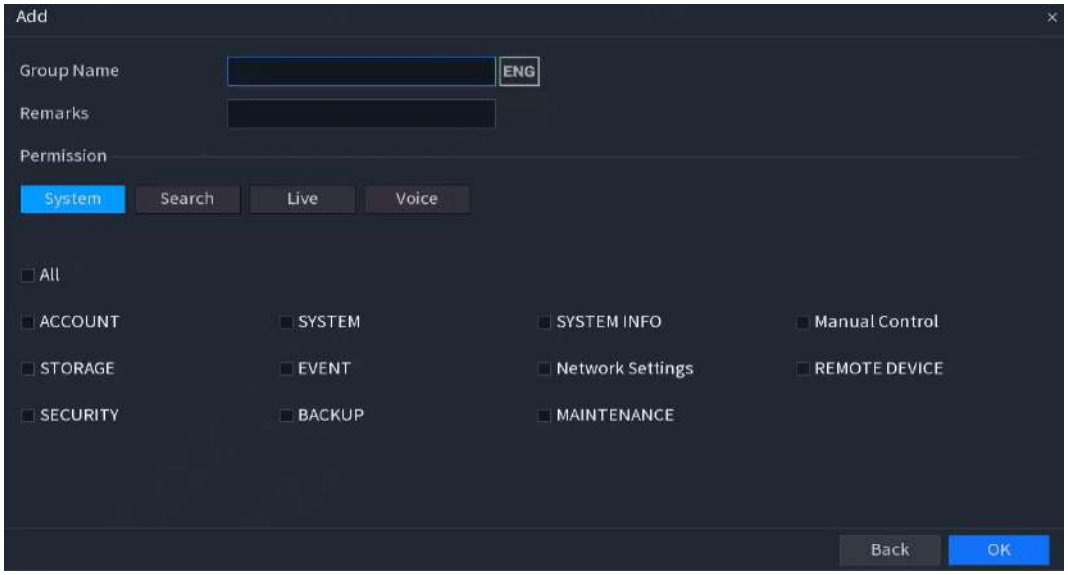
Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **Group**.

Step 2 Click **Add**.

Step 3 Enter the group name, and then enter some remarks if necessary.

Figure 12-50 Add group



Step 4 Select the checkboxes to select permissions.

Step 5 Click **OK**.

Click to modify the corresponding group information and click to delete the group.

12.4.4.3 ONVIF User

To connect the camera from the third party to the NVR via the ONVIF protocol, you need to use a verified ONVIF account.

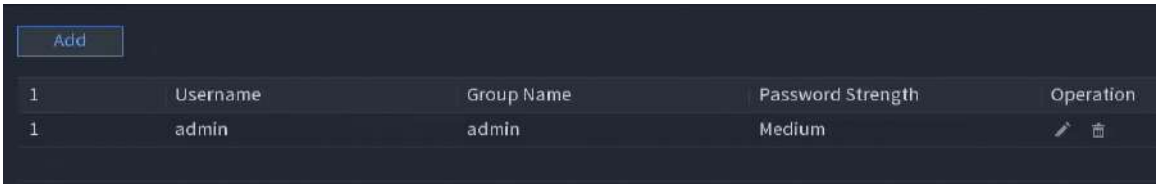
Background Information

The default ONVIF user is **admin**. It is created after you initialize the NVR and cannot be deleted.

Procedure

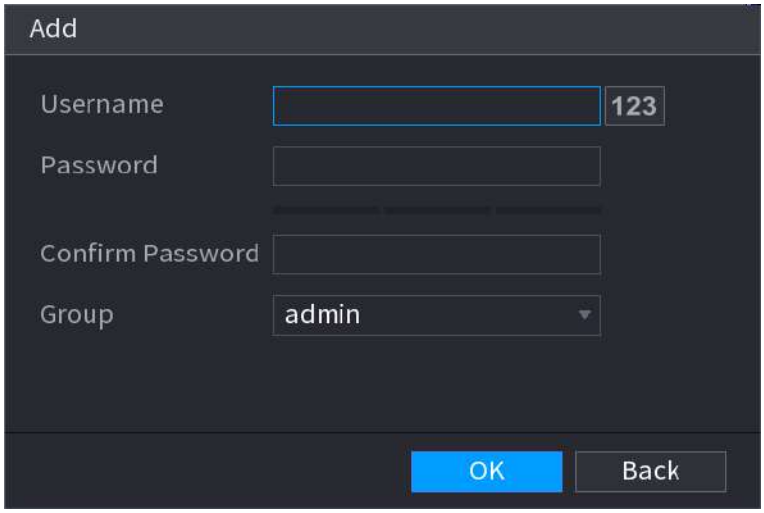
Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **ONVIF User**.

Figure 12-51 ONVIF user



Step 2 Click **Add**.

Figure 12-52 Add ONVIF user



Step 3 Configure username, password and user group.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete current user.

12.4.4.4 Password Reset

You can reset the password when you forget the password.

12.4.4.4.1 Enabling Password Reset

Enable the password reset function and configure the linked email address and security questions that are used to reset the password.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **Password Reset**.

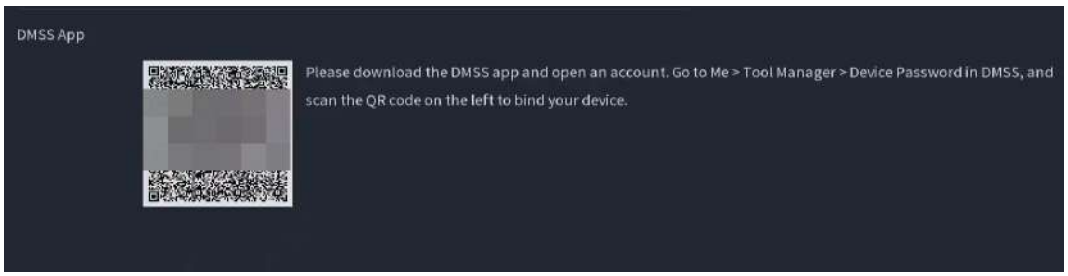
Step 2 Enter an email address to receive the security code used to reset the password.

The password reset function is enabled by default.

Step 3 Configure security questions and answers.

Step 4 (Optional) Follow the on-screen instructions to bind the device to DMSS app.

Figure 12-53 Bind device



Step 5 Click **OK**.

12.4.4.4.2 Resetting Password on Local Page

Procedure

Step 1 Right-click the live view and then select any item on the shortcut menu.

- If you did not configure unlock pattern, the password login window is displayed.
- Click **Password Login** tab to switch to password login.

Figure 12-54 Pattern login

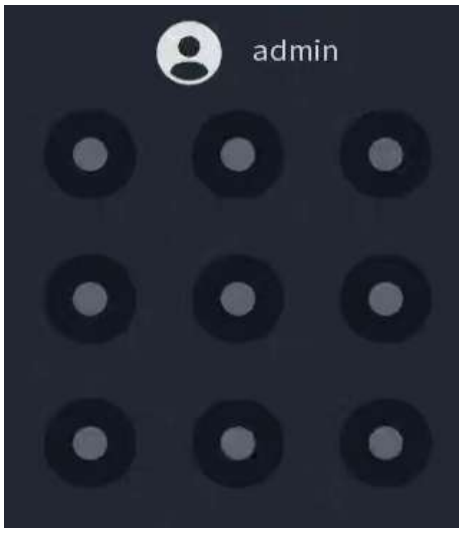
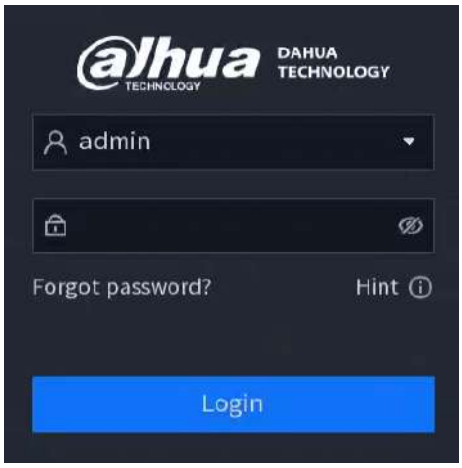


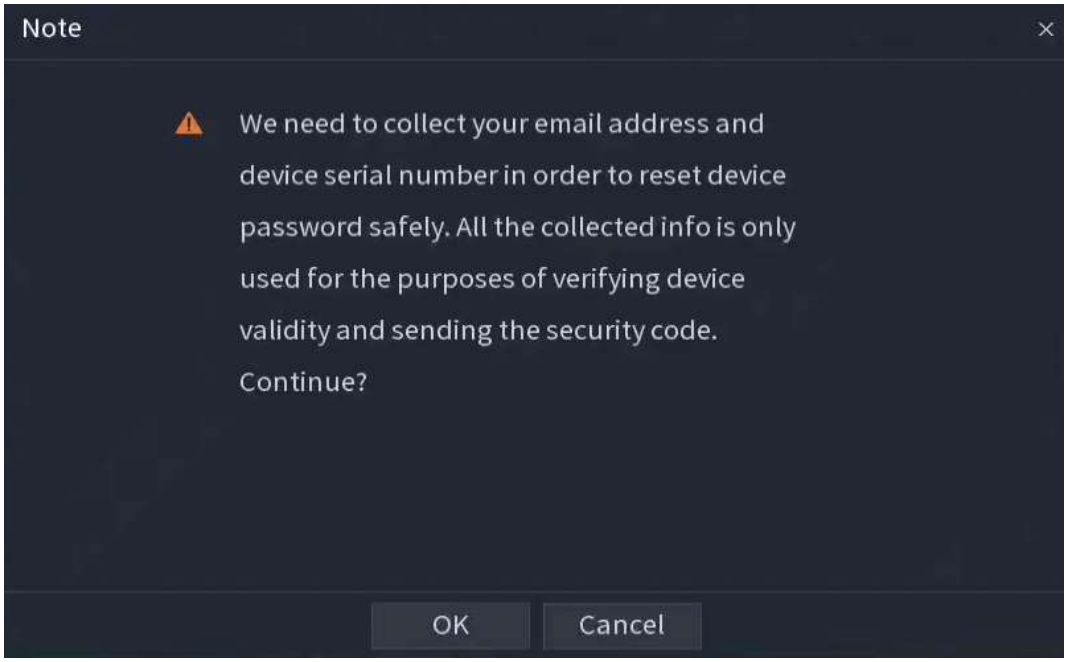
Figure 12-55 Password login



Step 2 Click **Forgot password?**.

- If you have set the linked email address, the system will notify you of data collection required for resetting password. Click **OK**.
- If you did not set 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.

Figure 12-56 Notification on data collection



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

Step 4 Click **Next**.

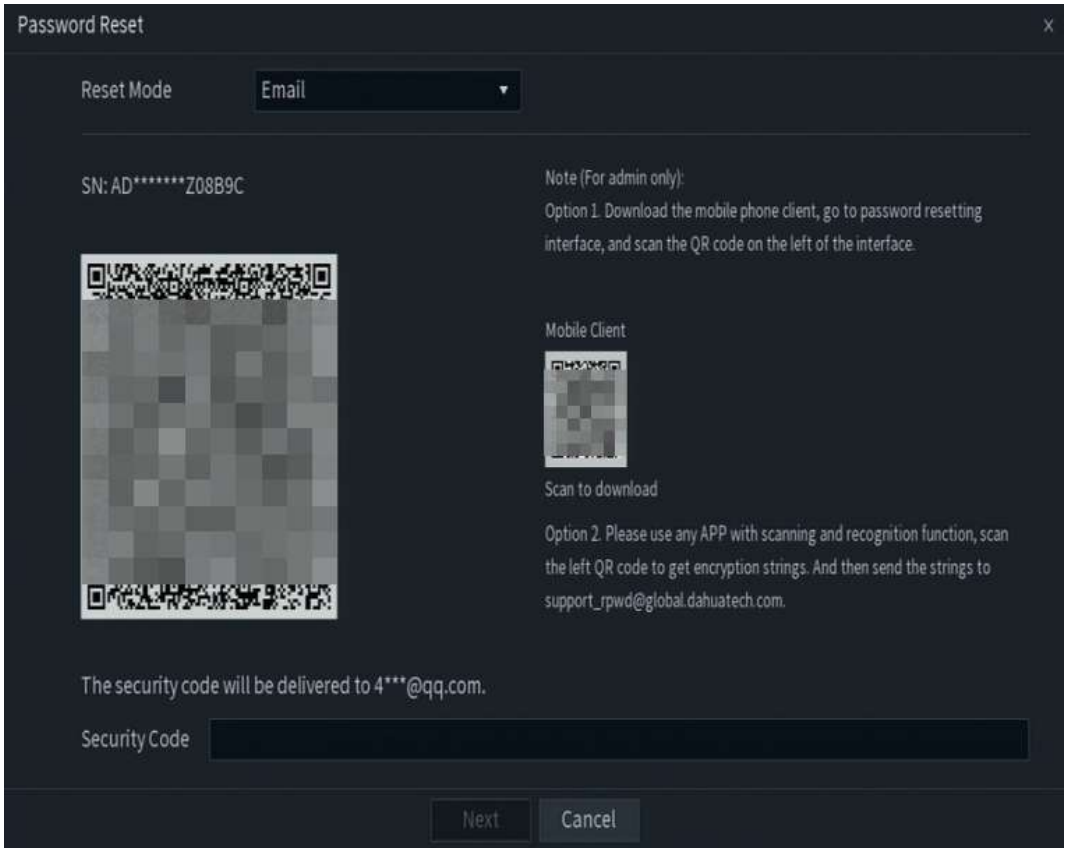
After clicking **Next** , the system will collect your information for password reset, purpose and the information includes but not limited to email address, MAC address, and device serial number. Read the prompt carefully before clicking **Next**.

Step 5 Reset the password.

- Email.

  Select **Email** as the reset mode, and then follow the on-screen instructions to get the security code in your linked email address. After that, enter the security code in the **Security Code** box.

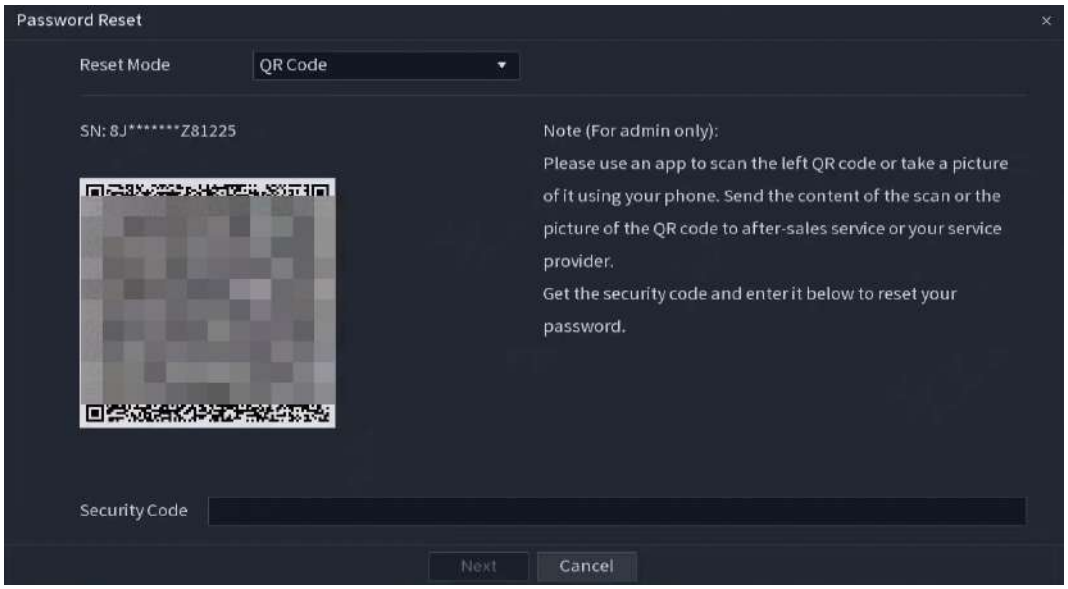
Figure 12-57 Reset mode (email)



- App.

  Select **QR Code** as the reset mode, and then follow the on-screen instructions to get the security code on the DMSS app. After that, enter the security code in the **Security Code** box.

Figure 12-58 Reset mode (app)



- Security question.

  Select **Security Question** as reset mode and then answer the security questions.

If you did not configure the security questions in advance, **Security Question** is not available on the **Reset Mode** list.

Step 6 Click **Next**.

Step 7 Enter the new password and then enter the password again to confirm it.

Step 8 Click **OK**.

The password is reset.

Step 9 (Optional) When the system prompts whether to synchronize the password with the remote devices accessed through the private protocol, click **OK** to synchronize the password.

12.4.5 Audio

The audio function is to manage audio files and set schedule play function. It is to realize audio broadcast activation function.

This function is available on select models.

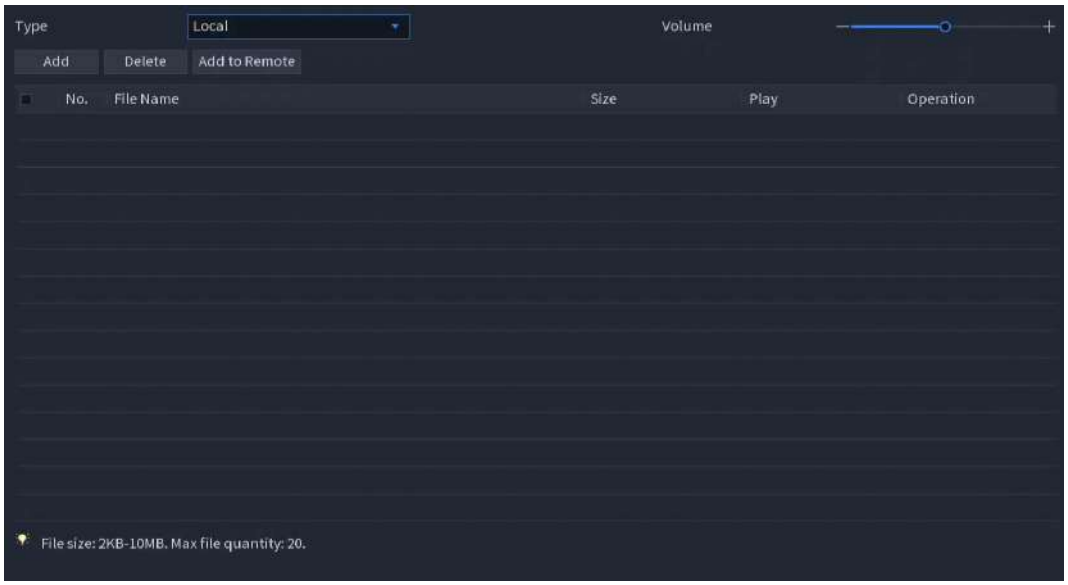
12.4.5.1 File Management

You can add audio files, listen to audio files, rename and delete audio files, and configure the audio volume.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Audio** > **File Management**.

Figure 12-59 File management



Step 2 Click **Add**.

Step 3 Select the audio file, and then click **Import**.

Supports MP3 and PCM audio format.

Step 4 Click **OK** to start importing audio files from the USB storage device.

If the importing is successful, the audio files will display in the **File Management** page.

12.4.5.2 Audio Play

You can configure the settings to play the audio files during the defined time period.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Audio** > **Audio Play**.

Figure 12-60 Audio play

Step 2 Configure the parameters.

Table 12-24 Schedule parameters

Parameter	Description
Period	In the **Period** box, enter the time. Select the checkbox to enable the settings. You can configure up to six periods.
File Name	In the **File Name** list, select the audio file that you want to play for this configured period.
Interval	In the **Interval** box, enter the time in minutes for how often you want to repeat the playing.
Loop	Configure how many times you want to repeat the playing in the defined period.
Output Port	Includes two options: MIC and Audio. It is MIC by default. The MIC function shares the same port with talkback function and the latter has the priority. Some series products do not have audio port.

- The finish time for audio playing depends on audio file size and the configured interval.
- Playing priority: **Alarm event** > **Audio talk** > **Trial listening** > **Schedule audio file**.

Step 3 Click **Apply**.

12.4.5.3 Broadcast

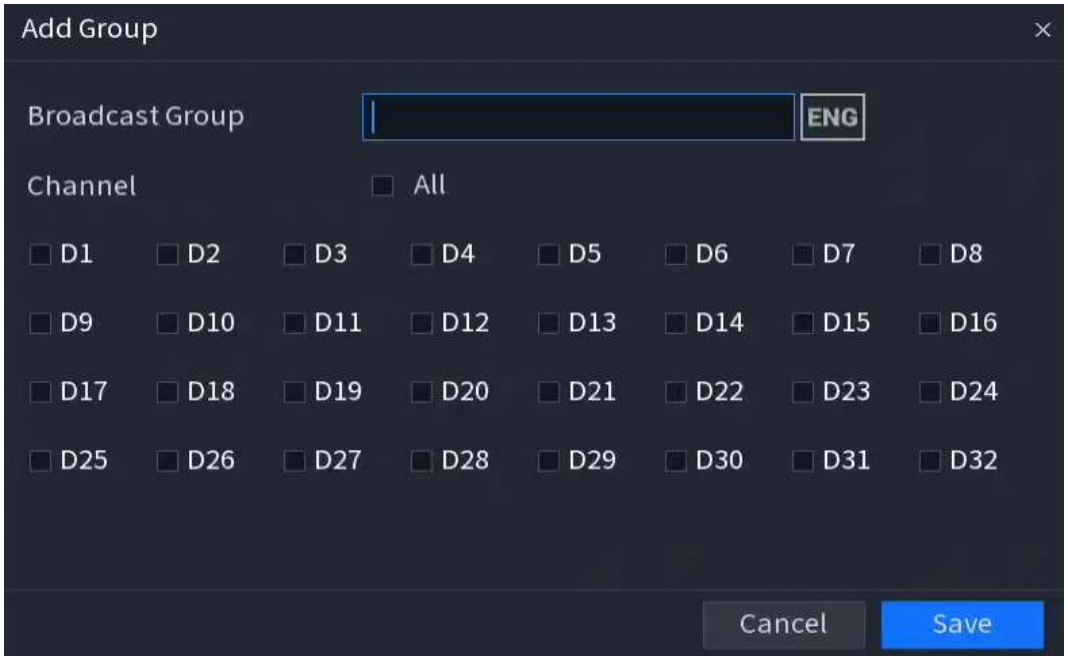
System can broadcast to the camera, or broadcast to a channel group.

Procedure

Step 1 Select **Mani Menu** > **SETTINGS** > **SYSTEM** > **Audio** > **Broadcast**.

Step 2 Click **Add Group**.

Figure 12-61 Add group (1)

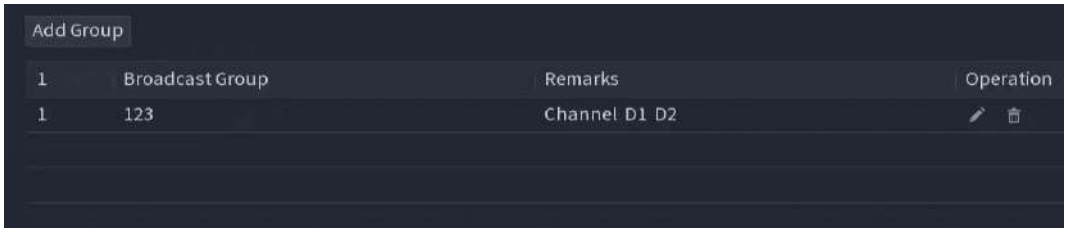


Step 3 Input group name and select one or more channels.

Step 4 Click **Save** to complete broadcast group setup.

- On the broadcast page, click to change group setup, click to delete group.
- After complete broadcast setup, on the preview page and then click on the navigation bar, device pops up broadcast dialogue box. Select a group name and then click to begin broadcast.

Figure 12-62 Add group (2)



12.4.6 Security

12.4.6.1 Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information on the security status of the device.

Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **System Status** to view the security status.

Detecting User and Service

The green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there is a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- User Status: When one of device users or ONVIF users uses weak password, the icon will be in orange to warn risk. You can click **Details** to optimize or ignore the risk warning.

Figure 12-63 Security status

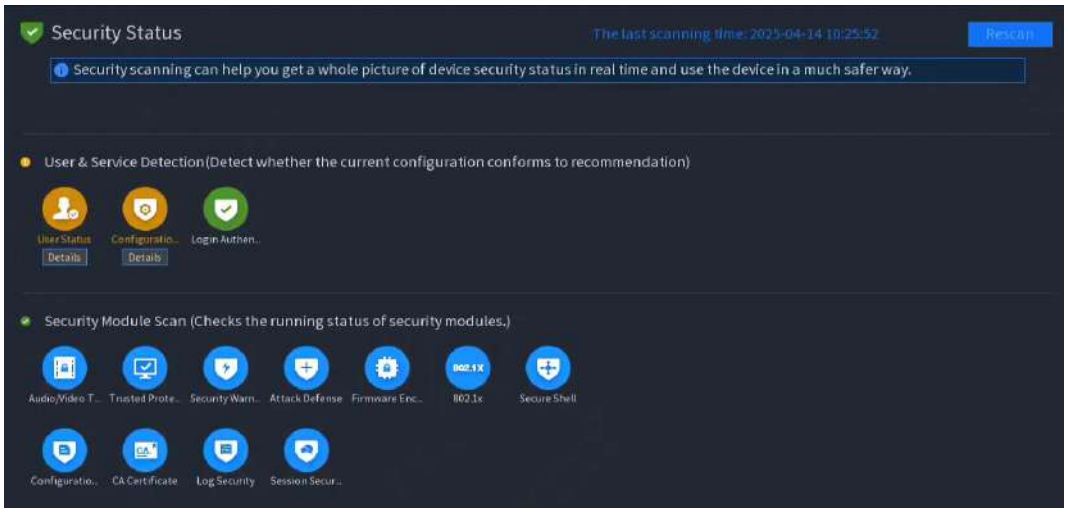
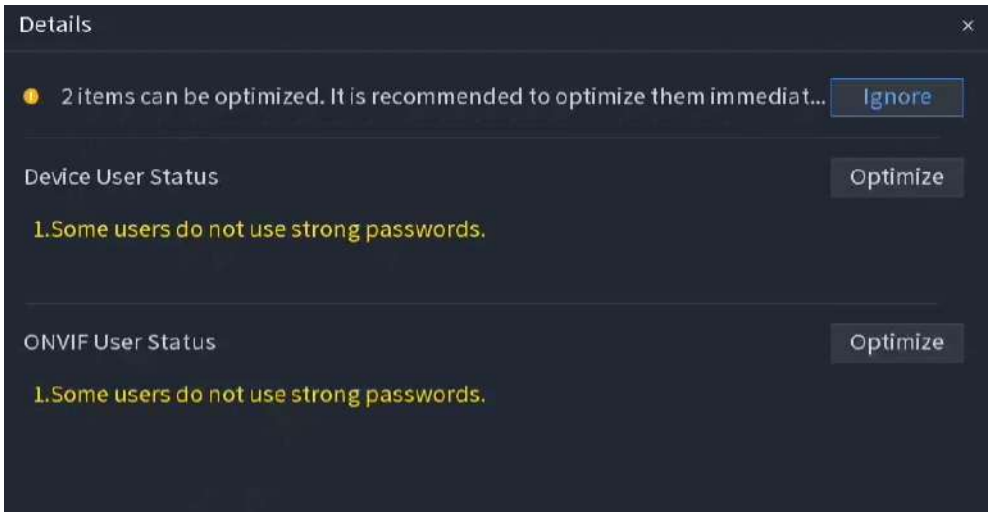
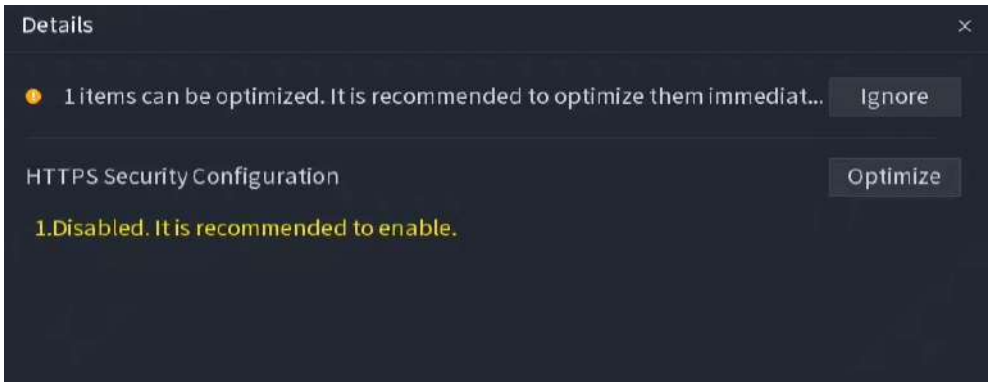


Figure 12-64 Details (1)



- Configuration Security: When there is a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

Figure 12-65 Details (2)



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, point to the icon to see the on-screen instructions.

Re-scanning Security Status

You can click **Rescan** to scan security status.

12.4.6.2 System Service

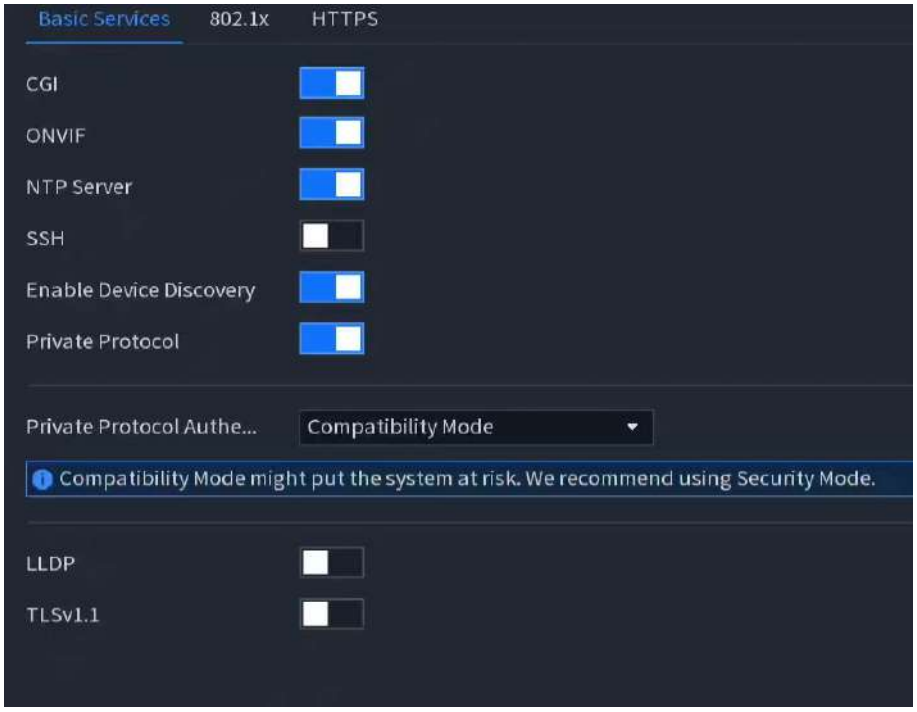
You can set NVR basic information such as basic services, 802.1x and HTTPS.

12.4.6.2.1 Basic Services

Procedure

Step 1 Select **Main Menu** > **SYSTEM** > **Security** > **System Service** > **Basic Services**.

Figure 12-66 Basic services



Step 2 Enable the system services.

There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled. Disable these functions when they are not needed.

Table 12-25 Basic service parameters

Parameter	Description
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default.
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default.
NTP Server	After this function is enabled, a NTP server can be used for time synchronization. This function is enabled by default.
SSH	After this function is enabled, you can use SSH service. This function is disabled by default.
Enable Device Discovery	After this function is enabled, the NVR can be found by other devices through searching.
Private Protocol Authentication Mode	• Security Mode (Recommended): Uses Digest access authentication when connecting to NVR. • Compatible Mode: Select this mode when the client does not support Digest access authentication.

Parameter	Description
LLDP	Enable the LLDP service. The Link Layer Discovery Protocol (LLDP) allows two different devices to collect hardware and protocol information about neighboring devices, which is useful in troubleshooting the network.
TLSv1.1	Enable the TLSv1.1 encryption protocol.

Step 3 Click **Apply**.

12.4.6.2.2 802.1x

The Device needs to pass 802.1x certification to enter the LAN.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **802.1x**.

Figure 12-67 802.1x

Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters.

Table 12-26 802.1x parameters

Parameter	Description
Authentication Mode	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details of creating certificates, see "12.4.6.4 CA Certificate".
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

Step 4 Click **Apply**.

12.4.6.2.3 HTTPS

We recommend you enable HTTPS function to enhance system security.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **System Service** > **HTTPS**.

Figure 12-68 HTTPS

Step 2 Enable HTTPS function.

Step 3 (Optional) Enable **Auto Redirect to HTTPS** to redirect to HTTPS automatically.

Step 4 Click **Certificate Management** to create or import a HTTPS certificate from USB drive. For details about importing or creating a CA certificate, see "12.4.6.4 CA Certificate".

Step 5 Select a HTTPS certificate.

Step 6 Click **Apply**.

12.4.6.3 Attack Defense

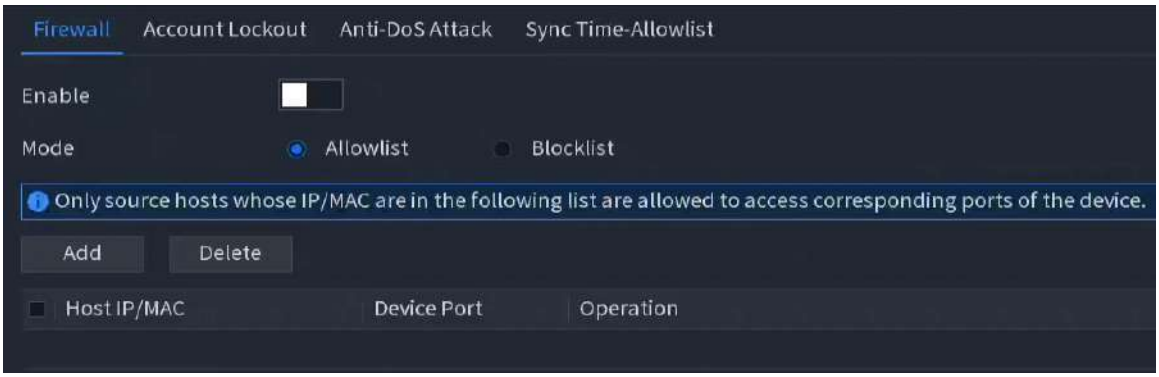
12.4.6.3.1 Firewall

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

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Firewall**.

Figure 12-69 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 hosts through a specific IP address, a network segment, or a MAC address.

- IP address.

  Enter the IP address, start port and end 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**.

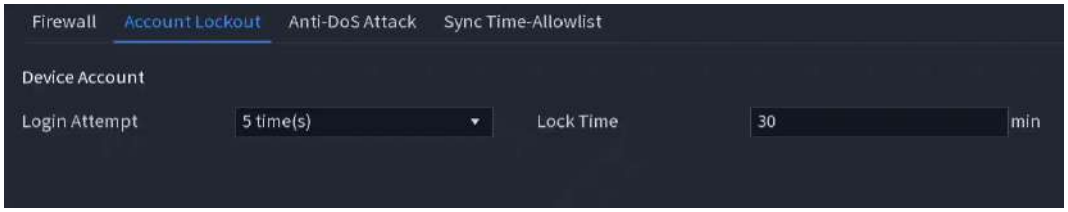
Step 5 Click **Apply**.

12.4.6.3.2 Account Lockout

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Account Lockout**.

Figure 12-70 Account lockout



Step 2 Configure parameters.

Table 12-27 Account lockout parameters

Parameter	Description
Login Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number.
Lock Time	Set how long the account is locked for.

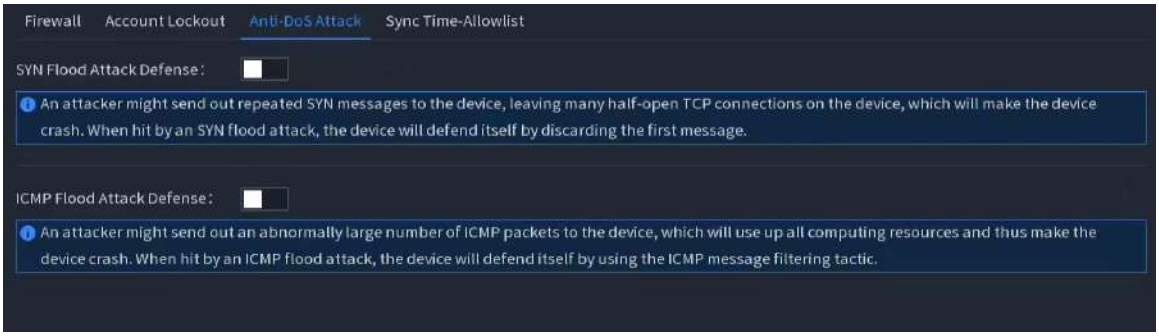
Step 3 Click **Apply**.

12.4.6.3.3 Anti-DoS Attack

Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Anti-DoS Attack**.

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attack.

Figure 12-71 Anti-Dos attack



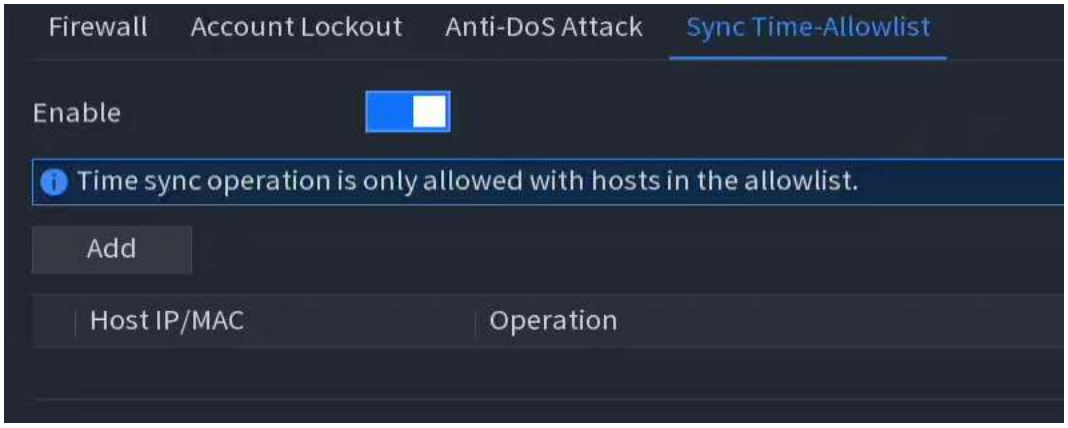
12.4.6.3.4 Sync Time-Allowlist

You can configure which hosts are allowed to synchronize time with the Device.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Attack Defense** > **Sync Time-Allowlist**.

Figure 12-72 Sync time-allowlist



Step 2 Click to enable the function.

Step 3 Click **Add** to add trusted hosts for time synchronization.

- If you set **Type** to **IP Address**, enter the IP address, and then click **OK**.
- If you set **Type** to **IP Segment**, enter the start address and end address, and then click **OK**.

Step 4 Click **Apply**.

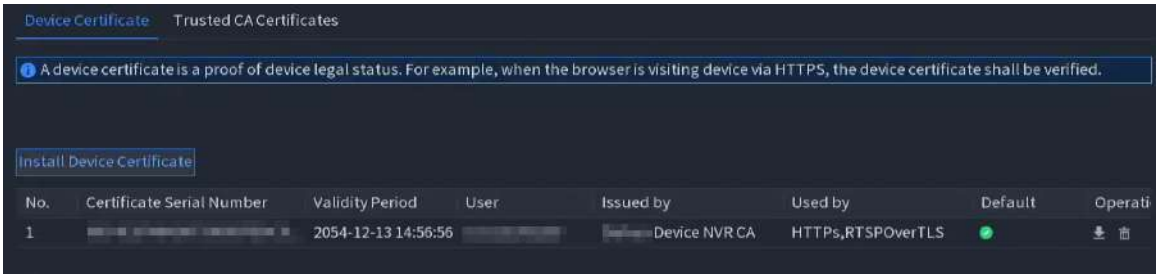
12.4.6.4 CA Certificate

12.4.6.4.1 Device Certificate

Procedure

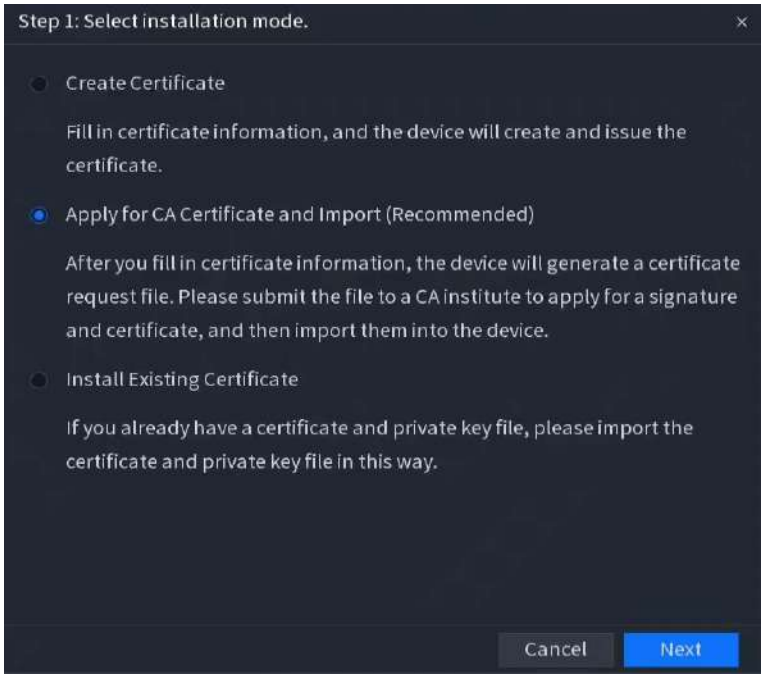
Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **CA Certificate** > **Device Certificate**.

Figure 12-73 Device certificate



Step 2 Click **Install Device Certificate** to select the installation mode.

Figure 12-74 Select installation mode



- Create certificate manually
  1. Select **Create certificate**.
  2. Fill in certificate information.
  3. Click **Create and install certificate**.
- Apply for a CA certificate and import it (recommended)
  1. Select **Apply for CA Certificate and Import (Recommended)**.
  2. Fill in certificate information.
  3. Click **Create** to save the certificate request file to the backup device.
  4. Use the request file to apply for a certificate from a third-party CA.
  5. Import the certificate.
- Install the existing certificate
  1. Select **Install Existing Certificate**.
  2. Select the file path and enter the private key and password.
  3. Click **Import**.

- Click to download the certificate.

- Click to delete the certificate.

Deleted certificates cannot be recovered, please proceed with caution when deleting.

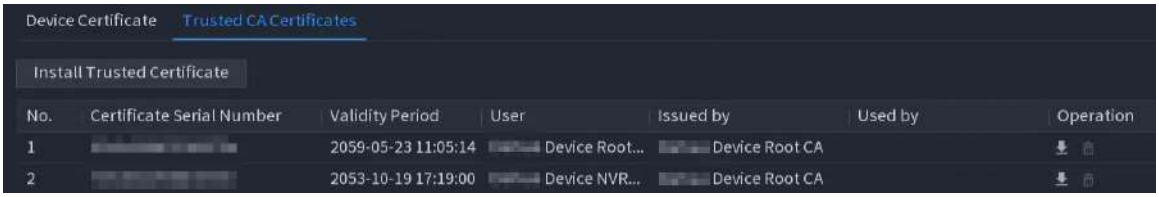
Once the certificate is created, you can view the created certificate in the **Device Certificate** page.

12.4.6.4.2 Trusted CA Certificates

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **CA Certificate** > **Trusted CA Certificates**

Figure 12-75 Trusted CA certificates



Step 2 Click **Install Trusted Certificate**.

Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import**.

12.4.6.5 Audio/Video Encryption

The device supports audio and video encryption during data transmission.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **A/V Encryption** > **Audio/Video Encrypted Transmission**.

Figure 12-76 Audio and video encrypted transmission

Step 2 Configure parameters.

Table 12-28 Audio and video transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "12.4.6.4 CA Certificate".

Step 3 Click **Apply**.

12.4.6.6 Security Warning

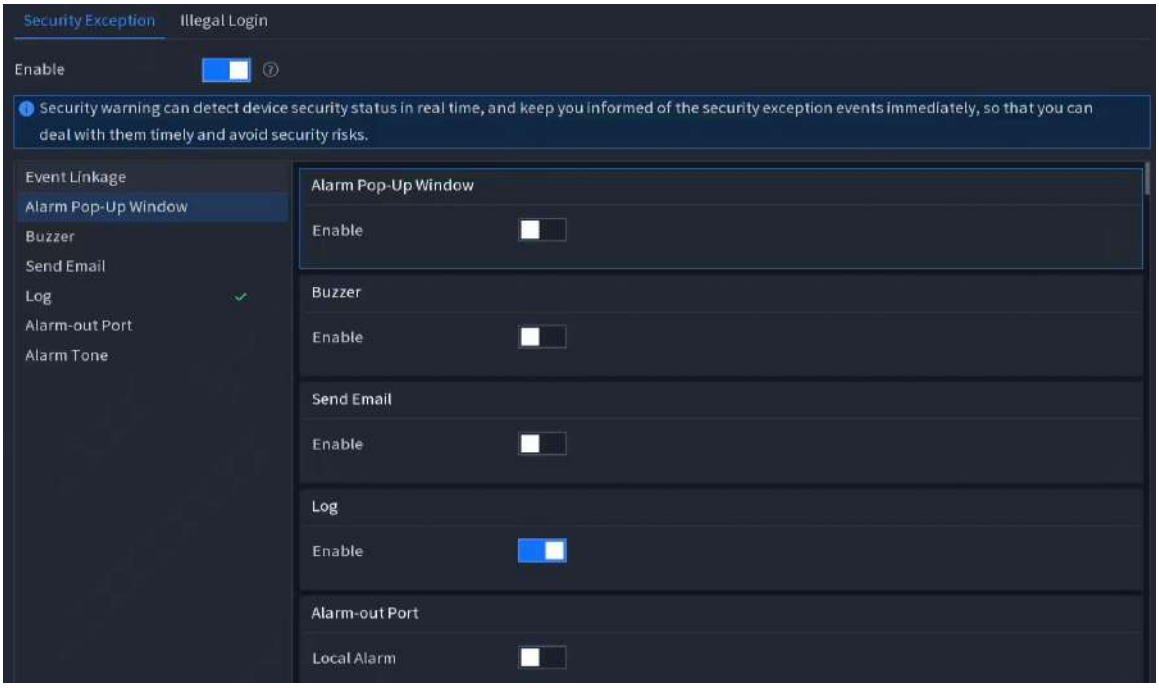
12.4.6.6.1 Security Exception

The device gives warnings to the user when a security exception occurs.

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Security Warning** > **Security Exception**.

Figure 12-77 Security exception



Step 2 Click to enable the function.

Click to view the list of security exception events.

Step 3 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

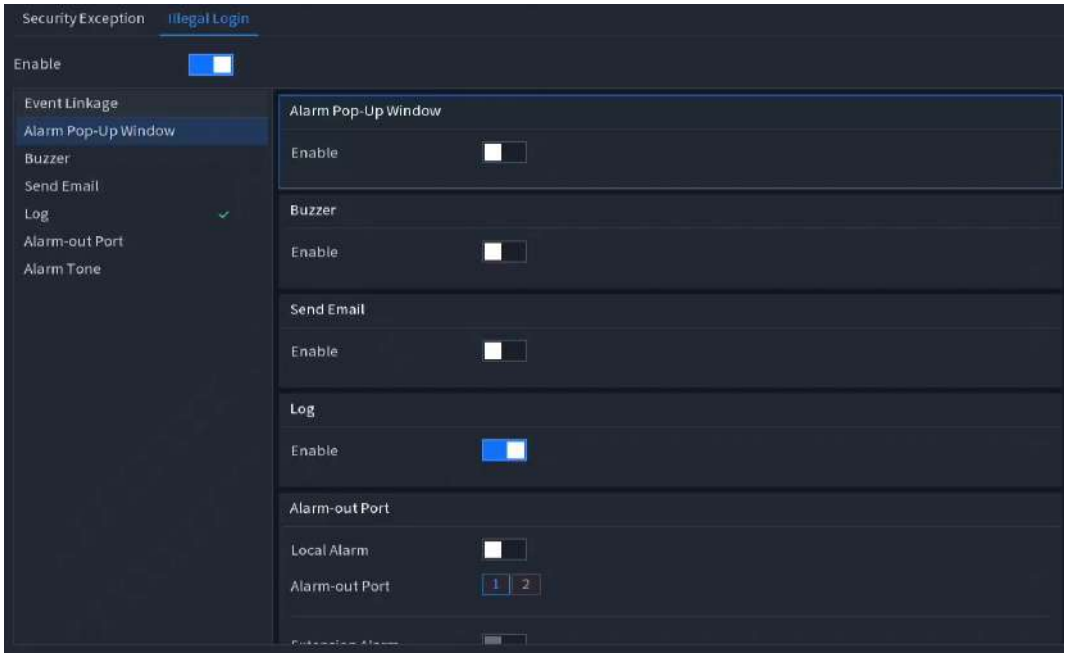
Step 4 Click **Apply**.

12.4.6.6.2 Illegal Login

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Security Warning** > **Illegal Login**.

Figure 12-78 Illegal login



Step 2 Click to enable the function.

Step 3 Configure alarm linkage. For details, see "6.1.5.7 Event Linkage".

Step 4 Click **Apply**.

12.4.6.7 Security Authentication

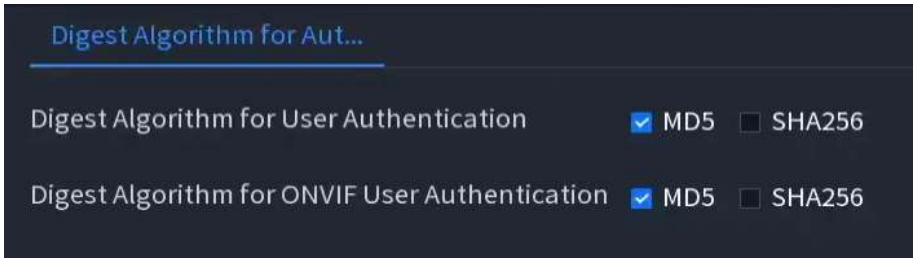
Select the digest algorithm for authentication you wish to use on the current page.

Procedure

Step 1 Log in to the main menu, select **Main Menu** > **SETTINGS** > **SYSTEM** > **Security** > **Security Authentication** > **Digest Algorithm for Authentication**.

Select the digest algorithm for user authentication and digest algorithm for ONVIF user authentication.

Figure 12-79 Select digest algorithm for authentication



Step 2 Click **Apply**.

13 Web Operation

- The figures in the Manual are used for introducing the operations and only for reference. The actual page might be different dependent on the model you purchased.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Besides Web, you can use our Smart PSS to login the device. For detailed information, see Smart PSS user's manual.

13.1 Network Connection

Background Information

- The factory default IP of the Device is 192.168.1.108.
- The device supports monitoring on different browsers such as Safari, Firefox, Google to perform the functions such as multi-channel monitoring, PTZ control, and device parameters configurations.

Procedure

Step 1 Check to make sure the device has connected to the network.

Step 2 Configure the IP address, subnet mask and gateway for the computer and the device. For details about network configuration of the device, see "12.1 Network Settings".

Step 3 On your computer, check the network connection of the device by using "ping ***.***.***.***". Usually the return value of TTL is 255.

13.2 Web Login

Procedure

Step 1 Open the browser, enter the IP address of the Device, and then press Enter.

Step 2 Enter the username and password.

- The default administrator account is **admin**. The password is the one that was configured during initial settings. To ensure your account security, we recommend you keep the password properly and change it regularly.
- Click to display the password.

Step 3 Click **Login**.

13.3 Web Main Menu

After you have logged in to the webpage, the main menu is displayed.

Figure 13-1 Navigation menu (1)

Figure 13-2 Navigation menu (2)

Table 13-1 Description of the navigation menu

Icon	Description
	Click the icon to quickly return to the main menu.
	Point to the icon to view the alarm information. You can view the alarm information about **Abnormal Event**, **Alarm Event**, and **AI Event**. You can click **Setting** under the corresponding tab to view the desired event alarm information.
LIVE	Click the icon to enter the live view page. You can view the real-time video of each channel and enable the audio talk, PTZ functions and so on.
	Click the icon to view the arming plan.
	Click the icon to view the downloading results.
admin	Click the icon to log out, restart the device, or shut down the device.
	Click the icon to view the QR codes for downloading the mobile client for cloud access, the device serial number, and the product information.
	Click the icon to view the current device information.

Figure 13-3 Main menu (APPLICATIONS)

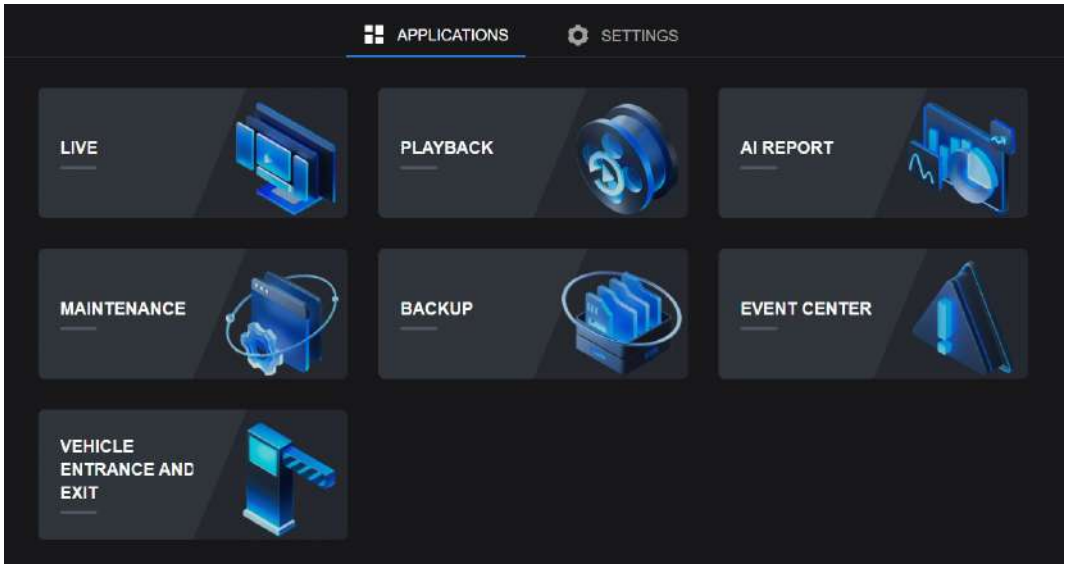


Table 13-2 Description of main menu (APPLICATIONS)

Function	Description
LIVE	View the real-time video of each channel.
PLAYBACK	View video playback and snapshot search.
AI REPORT	View the report of AI events.
MAINTENANCE	View the device logs and information, and manage device maintenance and upgrades.
BACKUP	Back up playback and pictures.
EVENT CENTER	Search for real-time and history events.
VEHICLE ENTRANCE AND EXIT	License plate recognition access management and vehicle entry/exit record inquiry.

Figure 13-4 Main menu (SETTINGS)

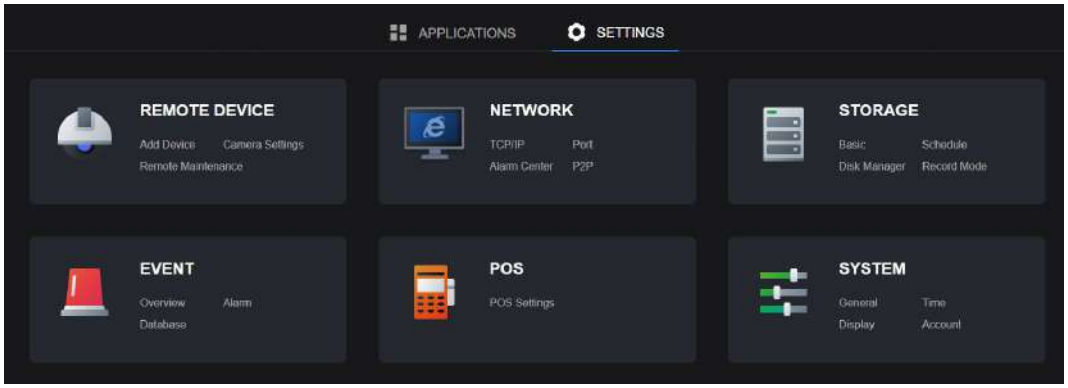


Table 13-3 Description of main menu (SETTINGS)

Function	Description
REMOTE DEVICE	Add remote devices, configure video device screen settings, and manage the maintenance of remote devices.
NETWORK	Modify the network and port settings of the local device, and configure the alarm center.
STORAGE	Modify the basic configuration of the local device, recording and snapshot schedule, hard disk management, and recording mode.
EVENT	View and modify the AI functions and alarm settings of the local device and remote devices, and create a database.
POS	View and modify the POS settings.
SYSTEM	View and modify the basic settings of the local device.

14 Glossary

- **DHCP**: DHCP (Dynamic Host Configuration Protocol) is one of the TCP/IP protocol cluster. It is mainly used to assign temporary IP addresses to computers on a network.
- **DDNS**: DDNS (Dynamic Domain Name Server) is a service that maps Internet domain names to IP addresses. This service is useful to anyone who wants to operate a server (web server, mail server, ftp server and more.) connected to the internet with a dynamic IP or to someone who wants to connect to an office computer or server from a remote location with software.
- **eSATA**: eSATA (External Serial AT) is an page that provides fast data transfer for external storage devices. It is the extension specifications of a SATA page.
- **GPS**: GPS (Global Positioning System) is a satellite system, protected by the US, safely orbiting thousands of kilometers above the earth.
- **PPPoE**: PPPoE (Point to Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site. Now the popular mode is ADSL and it adopts PPPoE protocol.
- **Wi-Fi**: Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The standard is for wireless local area networks (WLANs). It is like a common language that all the devices use to communicate to each other. It is actually IEEE802.11, a family of standard The IEEE (Institute of Electrical and Electronics Engineers Inc.)
- **3G**: 3G is the wireless network standard. It is called 3G because it is the third generation of cellular telecom standards. 3G is a faster network for phone and data transmission and speed Is over several hundred kbps. Now there are four standards: CDMA2000, WCDMA, TD-SCDMA and WiMAX.
- **Dual-stream**: The dual-stream technology adopts high-rate bit stream for local HD storage such as QCIF/CIF/2CIF/DCIF/4CIF encode and one low-rate bit stream for network transmission such as QCIF/CIF encode. It can balance the local storage and remote network transmission. The dual-stream can meet the difference band width requirements of the local transmission and the remote transmission. In this way, the local transmission using high-bit stream can achieve HD storage and the network transmission adopting low bit stream suitable for the fluency requirements of the 3G network such as WCDMA, EVDO, TD-SCDMA.
- **On-off value**: It is the non-consecutive signal sampling and output. It includes remote sampling and remote output. It has two statuses: 1/0.

Appendix 1 HDD Capacity Calculation

Calculate the total capacity needed by each device according to video recording (video recording type and video file storage time).

1. According to Formula (1) to calculate storage capacity q_i that is the capacity of each channel needed for each hour, unit Mbyte.

$$q_i = d_i \div 8 \times 3600 \div 1024 \quad (1)$$

In the formula: d_i means the bit rate, unit Kbit/s

2. After video time requirement is confirmed, according to Formula (2) to calculate the storage capacity m_i, which is storage of each channel needed unit Mbyte.

$$m_i = q_i \times h_i \times D_i \quad (2)$$

In the formula:

h_i means the recording time for each day (hour)

D_i means number of days for which the video shall be kept

3. According to Formula (3) to calculate total capacity (accumulation) q_T that is needed for all channels in the device during **scheduled video recording**.

$$q_T = \sum_{i=1}^{c} m_i \quad (3)$$

In the formula:

c means total number of channels in one device

4. According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in device during **alarm video recording (including motion detection)**.

$$q_T = \sum_{i=1}^{c} m_i \times a\% \quad (4)$$

In the formula:$a\%$ means alarm occurrence rate

Appendix 2 Mouse Operation

Appendix Table 2-1Mouse operation

Operation	Description
Left click mouse	When you have selected one menu item, left click mouse to view menu content.
	Modify checkbox or motion detection status.
	Click combo box to pop up drop-down list
	In input box, you can select input methods. Left click the corresponding button on the panel you can input numeral/English character (lower case/ upper case). Here ← stands for backspace button. __ stands for space button. In English input mode: _ stands for input a backspace icon and ← stands for deleting the previous character. In numeral input mode: _ stands for clear and ← stands for deleting the previous numeral.
Double left click mouse	Implement special control operation such as double click one item in the file list to playback the video.
	In multiple-window mode, double left click one channel to view in full-window. Double left click current video again to go back to previous multiple-window mode.
Right click mouse	In real-time monitor mode, pops up shortcut menu.
	Exit current menu without saving the modification.
Press middle button	In numeral input box: Increase or decrease numeral value.
	Switch the items in the checkbox.
	Page up or page down.
Move mouse	Select current control or move control.
Drag mouse	Select motion detection zone.
	Select privacy mask zone.

Appendix 3 Compatible Network Camera List

Please note all the models in the following list for reference only. For those products not included in the list, please contact your local retailer or technical supporting engineer for detailed information.

Appendix Table 3-1Compatible network camera list

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
AXIS	P1346	5.40.9.2	H264	√	ONVIF/Private
	P3344/ P3344-E	5.40.9.2	H264	√	ONVIF/Private
	P5512	—	H264	√	ONVIF/Private
	Q1604	5.40.3.2	H264	√	ONVIF/Private
	Q1604-E	5.40.9	H264	√	ONVIF/Private
	Q6034E	—	H264	√	ONVIF/Private
	Q6035	5.40.9	H264	√	ONVIF/Private
	Q1755	—	H264	√	ONVIF/Private
	M7001	—	H264	√	Private
	M3204	5.40.9.2	H264	√	Private
	P3367	HEAD LFP4_0 130220	H264	√	ONVIF
	P5532-P	HEAD LFP4_0 130220	H264	√	ONVIF
ACTi	ACM-3511	A1D-220-V3.12.15-AC	MPEG4	√	Private
	ACM-8221	A1D-220-V3.13.16-AC	MPEG4	√	Private
Arecont	AV1115	65246	H264	√	Private
	AV10005DN	65197	H264	√	Private
	AV2115DN	65246	H264	√	Private
	AV2515DN	65199	H264	√	Private
	AV2815	65197	H264	√	Private
	AV5115DN	65246	H264	√	Private
	AV8185DN	65197	H264	√	Private
Bosch	NBN-921-P	—	H264	√	ONVIF
	NBC-455-12P	—	H264	√	ONVIF
	VG5-825	9500453	H264	√	ONVIF
	NBN-832	66500500	H264	√	ONVIF
	VEZ-211-IWTEIVA	—	H264	√	ONVIF

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	NBC-255-P	15500152	H264	√	ONVIF
	VIP-X1XF	—	H264	√	ONVIF
Brikcom	B0100	—	H264	√	ONVIF
	D100	—	H264	√	ONVIF
	GE-100-CB	—	H264	√	ONVIF
	FB-100A	v1.0.3.9	H264	√	ONVIF
	FD-100A	v1.0.3.3	H264	√	ONVIF
Cannon	VB-M400	—	H264	√	Private
CNB	MPix2.0DIR	XNETM1120111229	H264	√	ONVIF
	VIPBL1.3MIRVF	XNETM2100111229	H264	√	ONVIF
	IGC-2050F	XNETM2100111229	H264	√	ONVIF
CP PLUS	CP-NC9-K	6.E.2.7776	H264	√	ONVIF/Private
	CP-NC9W-K	6.E.2.7776	H264	√	Private
	CP-ND10-R	cp20111129ANS	H264	√	ONVIF
	CP-ND20-R	cp20111129ANS	H264	√	ONVIF
	CP-NS12W-CR	cp20110808NS	H264	√	ONVIF
	VS201	cp20111129NS	H264	√	ONVIF
	CP-NB20-R	cp20110808BNS	H264	√	ONVIF
	CP-NT20VL3-R	cp20110808BNS	H264	√	ONVIF
	CP-NS36W-AR	cp20110808NS	H264	√	ONVIF
	CP-ND20VL2-R	cp20110808BNS	H264	√	ONVIF
	CP-RNP-1820	cp20120821NSA	H264	√	Private
	CP-RNC-TP20FL3C	cp20120821NSA	H264	√	Private
	CP-RNP-12D	cp20120828ANS	H264	√	Private
	CP-RNC-DV10	cp20120821NSA	H264	√	Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	CP-RNC-DP20FL2C	cp20120821NSA	H264	√	Private
Dynacolor	ICS-13	d20120214NS	H264	√	ONVIF/Private
	ICS-20W	vt20111123NSA	H264	√	ONVIF/Private
	NA222	—	H264	√	ONVIF
	MPC-IPVD-0313	k20111208ANS	H264	√	ONVIF/Private
	MPC-IPVD-0313AF	k20111208BNS	H264	√	ONVIF/Private
Honeywell	HIDC-1100PT	h.2.2.1824	H264	√	ONVIF
	HIDC-1100P	h.2.2.1824	H264	√	ONVIF
	HIDC-0100P	h.2.2.1824	H264	√	ONVIF
	HIDC-1300V	2.0.0.21	H264	√	ONVIF
	HICC-1300W	2.0.1.7	H264	√	ONVIF
	HICC-2300	2.0.0.21	H264	√	ONVIF
	HDZ20HDX	H20130114NSA	H264	√	ONVIF
LG	LW342-FP	—	H264	√	Private
	LNB5100	—	H264	√	ONVIF
Imatek	KNC-B5000	—	H264	√	Private
	KNC-B5162	—	H264	√	Private
	KNC-B2161	—	H264	√	Private
Panasonic	NP240/CH	—	MPEG4	√	Private
	WV-NP502	—	MPEG4	√	Private
	WV-SP102H	1.41	H264	√	ONVIF/Private
	WV-SP105H	—	H264	√	ONVIF/Private
	WV-SP302H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SP306H	1.4	H264, MPEG4	√	ONVIF/Private
	WV-SP508H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP509H	—	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	WV-SW316H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW355H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW352H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW152E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW558H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW559H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP105H	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW155E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF336H	1.44	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF132E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF135E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF346H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF342H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SC385H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SC386H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SP539	1.66	H264, MPEG4	√	ONVIF
	DG-SC385	1.66	H264, MPEG4	√	ONVIF
PELCO	IXSOLW	1.8.1-20110912-1.9082-A1.6617	H264	√	Private
	IDE20DN	1.7.41.9111-O3.6725	H264	√	Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	D5118	1.7.8.9310-A1.5288	H264	√	Private
	IM10C10	1.6.13.9261-O2.4657	H264	√	Private
	DD4N-X	01.02.0015	MPEG4	√	Private
	DD423-X	01.02.0006	MPEG4	√	Private
	D5220	1.8.3-FC2-20120614-1.9320-A1.8035	H264	√	Private
Samsung	SNB-3000P	2.41	H264, MPEG4	√	ONVIF/Private
	SNP-3120	1.22_110120_1	H264, MPEG4	√	ONVIF/Private
	SNP-3370	1.21_110318	MPEG4	√	Private
	SNB-5000	2.10_111227	H264, MPEG4	√	ONVIF/Private
	SND-5080	—	H264, MPEG4	√	Private
	SNZ-5200	1.02_110512	H264, MPEG4	√	ONVIF/Private
	SNP-5200	1.04_110825	H264, MPEG4	√	ONVIF/Private
	SNB-7000	1.10_110819	H264	√	ONVIF/Private
	SNB-6004	V1.0.0	H264	√	ONVIF
Sony	SNC-D H110	1.50.00	H264	√	ONVIF/Private
	SNC-CH120	1.50.00	H264	√	ONVIF/Private
	SNC-CH135	1.73.01	H264	√	ONVIF/Private
	SNC-CH140	1.50.00	H264	√	ONVIF/Private
	SNC-CH210	1.73.00	H264	√	ONVIF/Private
	SNC-D H210	1.73.00	H264	√	ONVIF/Private
	SNC-D H240	1.50.00	H264	√	ONVIF/Private
	SNC-D H240-T	1.73.01	H264	√	ONVIF/Private
	SNC-CH260	1.74.01	H264	√	ONVIF/Private
	SNC-CH280	1.73.01	H264	√	ONVIF/Private
	SNC-RH-124	1.73.00	H264	√	ONVIF/Private
	SNC-RS46P	1.73.00	H264	√	ONVIF/Private
	SNC-ER550	1.74.01	H264	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	SNC-ER580	1.74.01	H264	√	ONVIF/Private
	SNC-ER580	1.78.00	H264	√	ONVIF
	SNC-VM631	1.4.0	H264	√	ONVIF
	WV-SP306	1.61.00	H264, MPEG4	√	SDK
	WV-SP306	1.61.00	H264	√	ONVIF
	SNC-VB600	1.5.0	H264	√	Private
	SNC-VM600	1.5.0	H264	√	Private
	SNC-VB630	1.5.0	H264	√	Private
	SNC-VM630	1.5.0	H264	√	Private
SANYO	VCC-HDN4000PC	—	H264	√	ONVIF

Appendix 4 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: 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 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.

2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner**

   Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access Web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, we recommend you to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

   We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188