Network Video Recorder

Quick Start Guide

V1.1.0

Foreword

General

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

Symbols

The following symbols might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V1.0.1	• Updated the contents of startup wizard, configuring video recording schedule, adding the Device to smartphone client, SMD, and playback. • Added the contents of adding user, configuring alarm rules, and alarm message subscription to smartphone client.	September 2026
V1.0.0	First release.	July 2026

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

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

DANGER

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.

WARNING

- 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 Starting the Device.....1
1.1 Initialization.....1
1.1.1 Initializing the Device.....1
1.1.2 Startup Wizard.....5
1.1.3 Login.....12
1.2 Adding Users.....13
1.3 Configuring Alarm Rules.....14
1.4 Configuring Video Recording Schedule.....19
1.5 Configuring P2P Settings.....24
1.5.1 Enabling P2P Function.....24
1.5.2 Adding the Device to Smartphone Client.....25
1.5.3 Subscribing to Alarm Message on Smartphone Client.....26
1.6 Smart Motion Detection.....29
1.7 Live View.....32
1.8 Playback.....36
2 Web Operation.....42
2.1 Network Connection.....42
2.2 Web Login.....42
Appendix 1 Security Recommendation.....43

1 Starting the Device

Background Information

- For device security, connect the Device to the power adapter first and then connect the device to the power socket.
- The rated input voltage matches the power adapter requirements. Make sure the power wire connection is secure. Then press the power button.
- Always use a stable current supply. If necessary, use an Uninterruptible Power Supply (UPS) as the preferred alternative.

Procedure

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

Step 2 Connect the power cable.

Step 3 Press the power button on the front panel or the power switch on the rear panel to start up the device.

After the device starts, the system is in multiple-channel display mode by default.

The Device will verify the license during startup. If the verification fails, the icon is displayed on the screen. Contact the technical support.

1.1 Initialization

1.1.1 Initializing the Device

Background Information

For first-time use, set a login password for the admin account (default user).

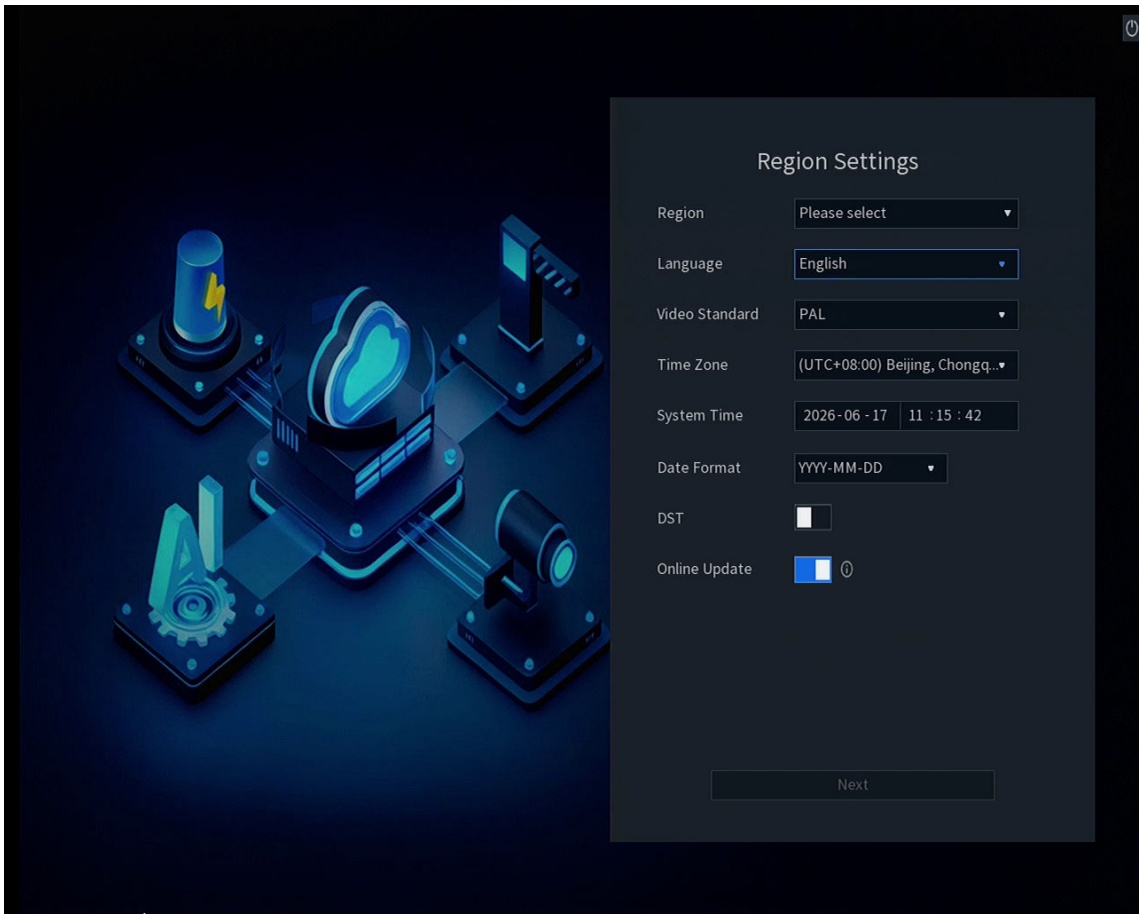
- For device security, keep your login password and change it regularly.
- The default IP address of the Device is 192.168.1.108.
- If a DHCP service exists in the network environment, use a tool to locate the device IP (device category: ARC).

Procedure

Step 1 Open the browser, enter the IP address, and then press the Enter key.

Step 2 Set the basic information, and then click **Next**.

Figure 1-1 Set the basic information



Click to power off the device.

Table 1-1 Description of basic parameters

Parameter	Description
Region	Select the region as needed.
Language	Select the language as needed.
Video Standard	Select a video standard. • PAL is mainly used in China, Middle East and Europe. • NTSC is mainly used in Japan, United States, Canada and Mexico. As a technical standard of processing video and audio signals, PAL and NTSC mainly differ in the encoding and decoding modes and field scanning frequency.
Time Zone	Select the time zone as needed.

Parameter	Description
System Time	Set the system date and time.
Date Format	Select a date format for the system.
(Optional) DST	Enable the Daylight Saving Time function. DST is a system to stipulate local time to save energy. If the country or region where the Device is located follows DST, you can enable DST to ensure that system time is correct.
(Optional) Online Update	Enable the system to automatically check the version and perform online updates.

Step 3 Set the initialization parameters.

Figure 1-2 Initialization settings

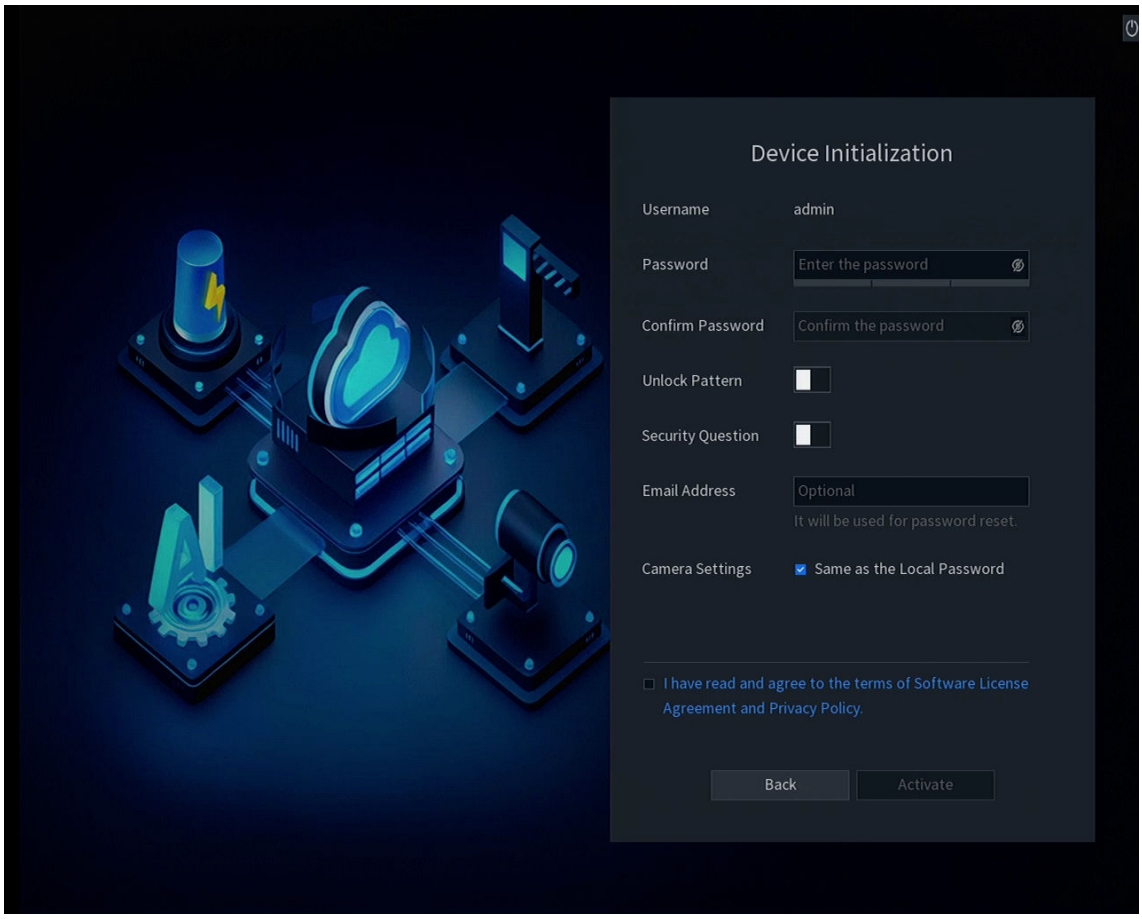


Table 1-2 Description of the initialization parameters

Parameter	Description
Username	The default user name is **admin**.

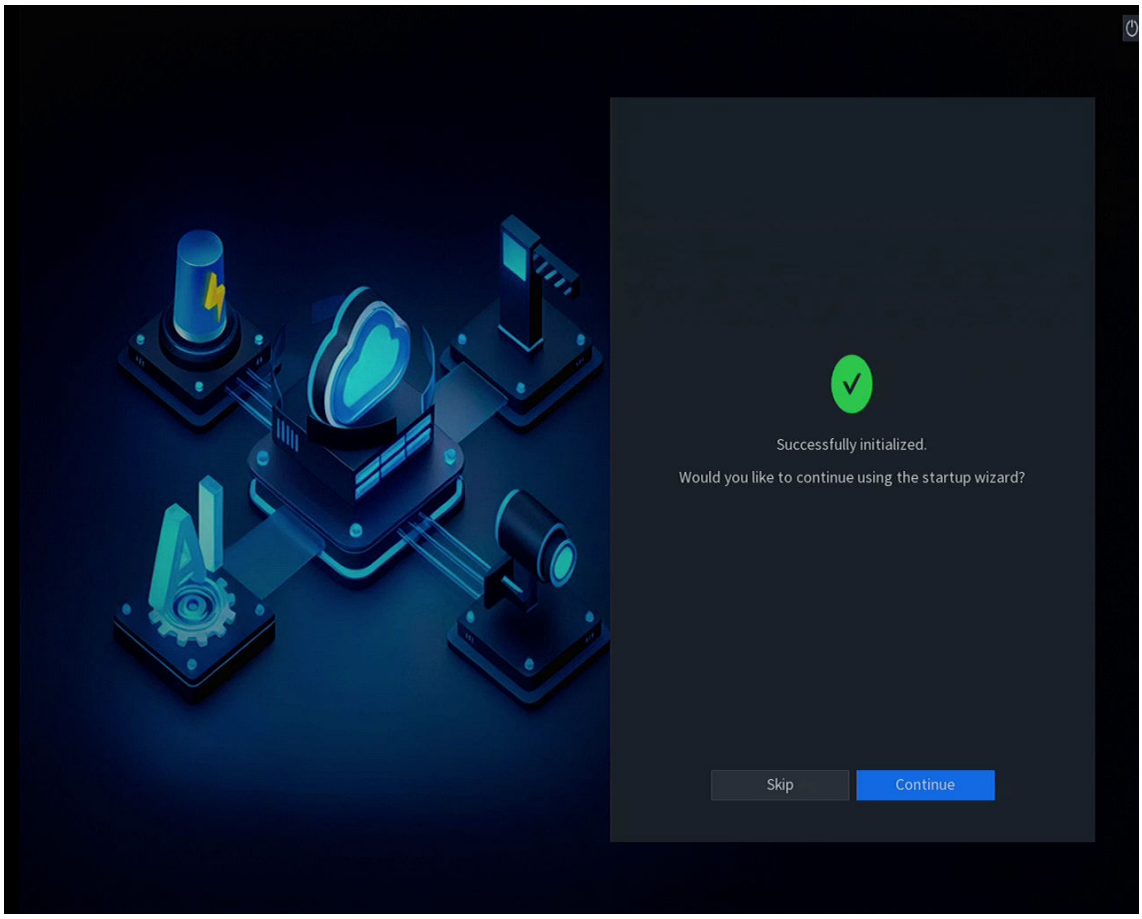
Parameter	Description
Password	Set the login password for the admin user and confirm the password. • The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). • For your device security, create a strong password.
Confirm Password	
(Optional) Unlock Pattern	Enable the unlock pattern function, and then click **Draw** to draw the pattern. • This function is disabled by default. • A pattern lock must connect at least 4 dots. • After setting a pattern lock, the system will use this pattern for login by default.
(Optional) Security Question	Enable this function, and then configure the security questions and answers for resetting the password.
(Optional) Email Address	Enter the email address that is used to reset the password.
(Optional) Camera Settings	Select the **Same as the Local Password** checkbox to disable the camera login password setting, and then the camera password uses the login password of the **admin** user.

Step 4 Click **Activate**.

The Device is initialized.

- Click **Continue** to continue using the startup wizard. For details, see "1.1.2 Startup Wizard".
- Click **Skip** if the startup wizard is not required.

Figure 1-3 Initialization success



1.1.2 Startup Wizard

After initialization, the system goes to **Startup Wizard**. You can complete functional settings such as Device network connection, cloud access configuration, remote device addition and HDD settings to use the Device quickly.

Background Information

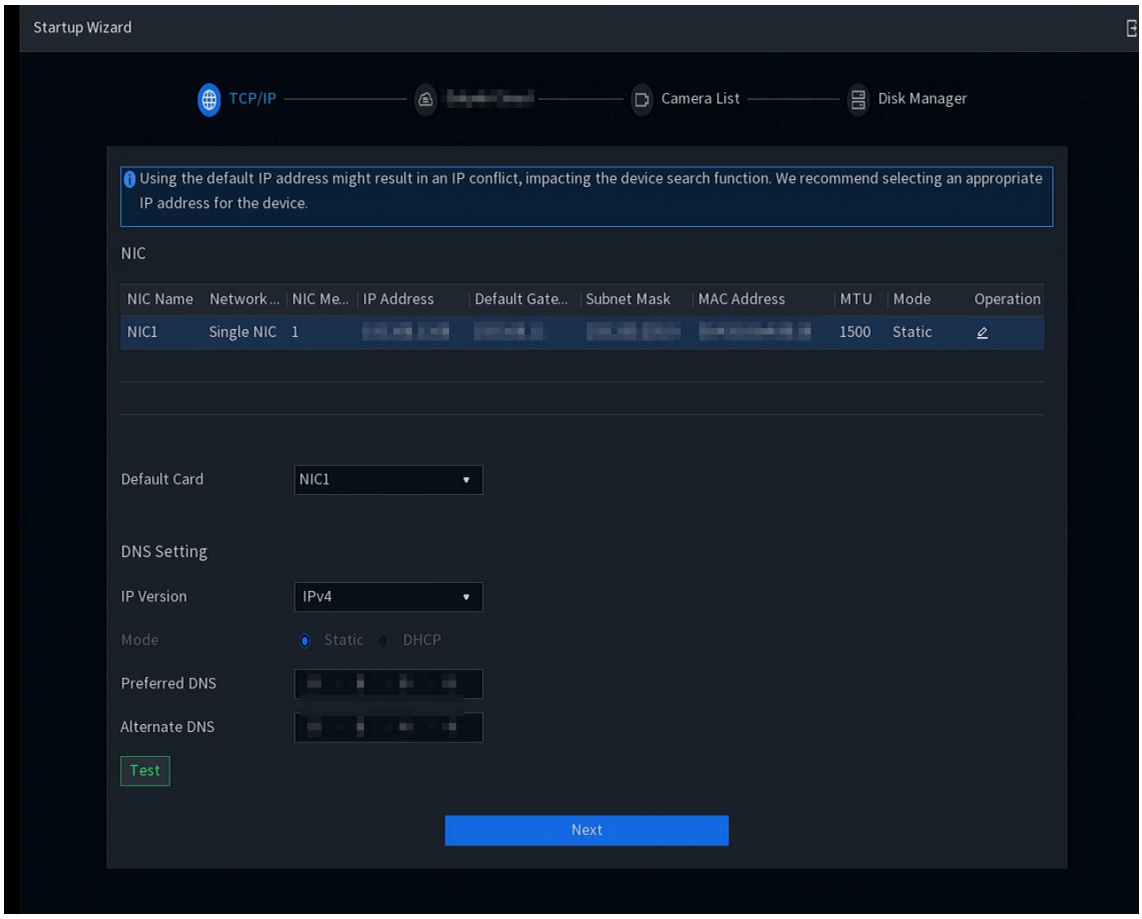
Startup Wizard is displayed only when you log in to the Device for the first time or have restored the Device to factory settings.

Procedure

Step 1 Configure the network parameters, and then click **Next**.

Network Mode might vary with models. Configure the IP address of the network adapter according to the actual connection situation.

Figure 1-4 TCP/IP



1. Click of the corresponding NIC.
2. Configure parameters, and then click **OK**.

Figure 1-5 Modify NIC parameters

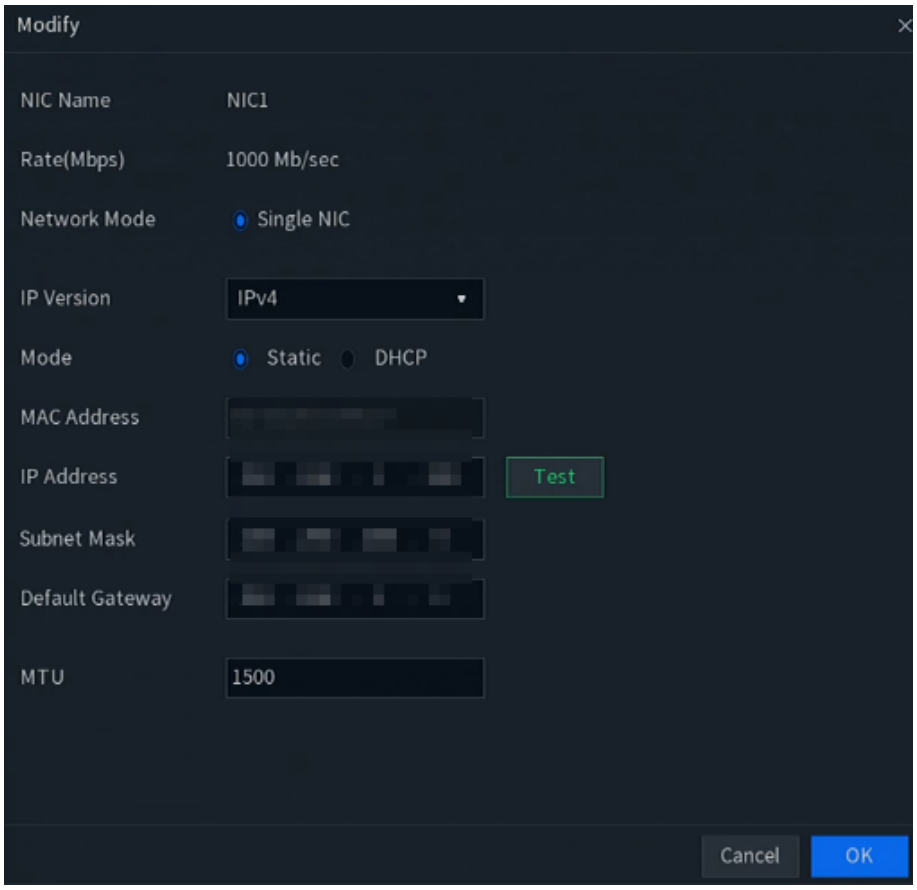


Table 1-3 Description of network parameters

Parameter	Description
NIC Name	Displays the name of the currently edited network adapter.
Rate (Mbps)	Displays the maximum network transmission speed that the current NIC supports.

Parameter	Description
Network Mode	Select the network mode of the Device. • **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.
IP Version	Select **IPv4** or **IPv6**. Both versions are supported for access.
Mode	Select the method for obtaining the DNS (Domain name system) server address. • **Static** : Enter the **IP Address**, **Subnet Mask** and **Default Gateway** to set a static IP address for the Device. • **DHCP** : When there is a DHCP server on the network, you can enable DHCP. The system allocates a dynamic IP address to the Device. There is no need to set IP address manually.

Parameter	Description
MAC Address	Displays the MAC address of the Device.
IP Address	When **Mode** is select to **Static**, you must set the IP address, 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	
MTU	Set the NIC MTU (Maximum transmission unit) value. The default setup is 1500 bytes. Please be advised that changing MTU value might result in NIC restart, network offline and affect current running operation.

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

3. On the **Default Card** drop-down list, select the default NIC.
4. (Optional) Configure the DNS server.

   This step is required if you want to use domain service.

   You can obtain DNS server address or manually enter it.

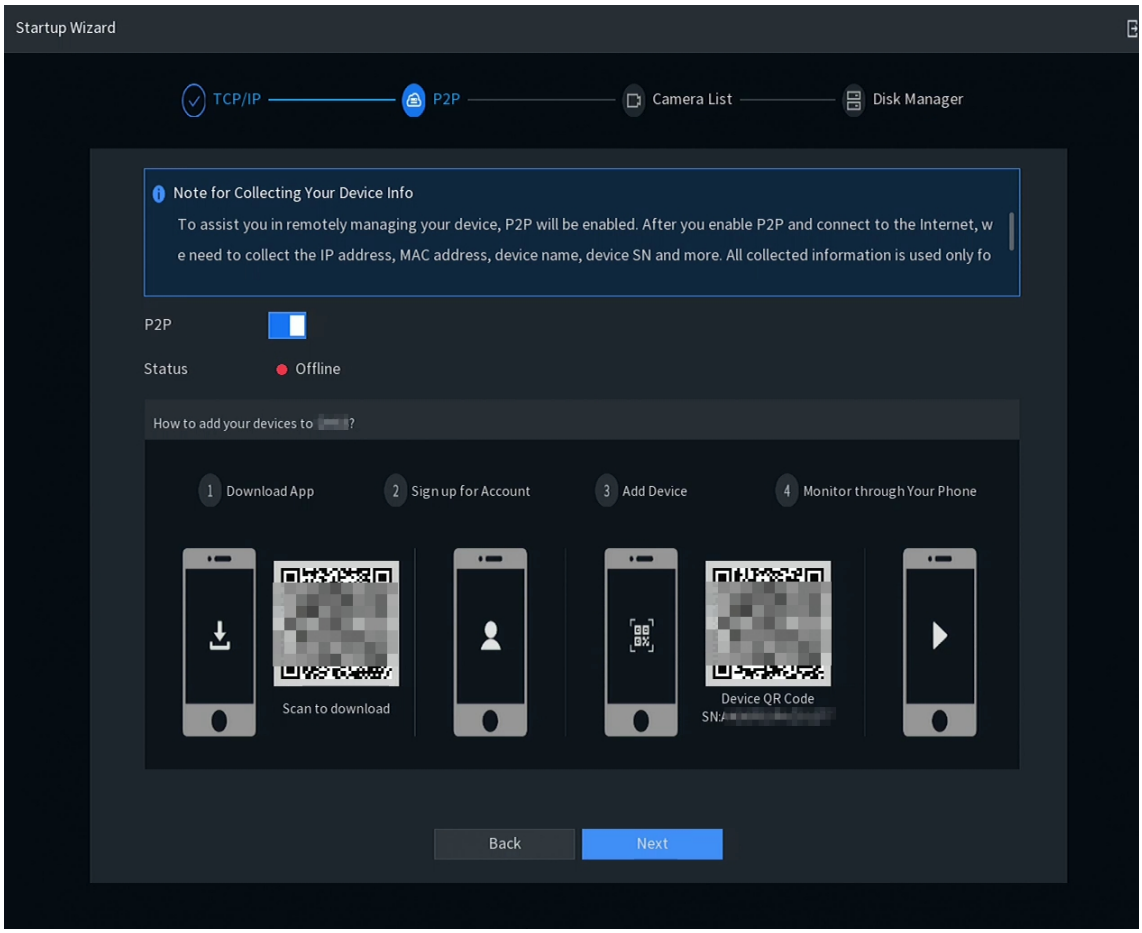
   - Automatically get the DNS server address: When there is a DHCP server in the network, you can enable **DHCP**, and then the Device gets a dynamic IP address.
   - Enter the DNS server address: Select **IP Version**, and then configure the preferred DNS server and alternate DNS server.
5. Click **Next**

Step 2 (Optional) Enable **P2P** , and then click **Next**.

You can 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 is connected to the WAN.
- The **Status** becomes **Online** after you successfully configure **P2P**.

Figure 1-6 P2P

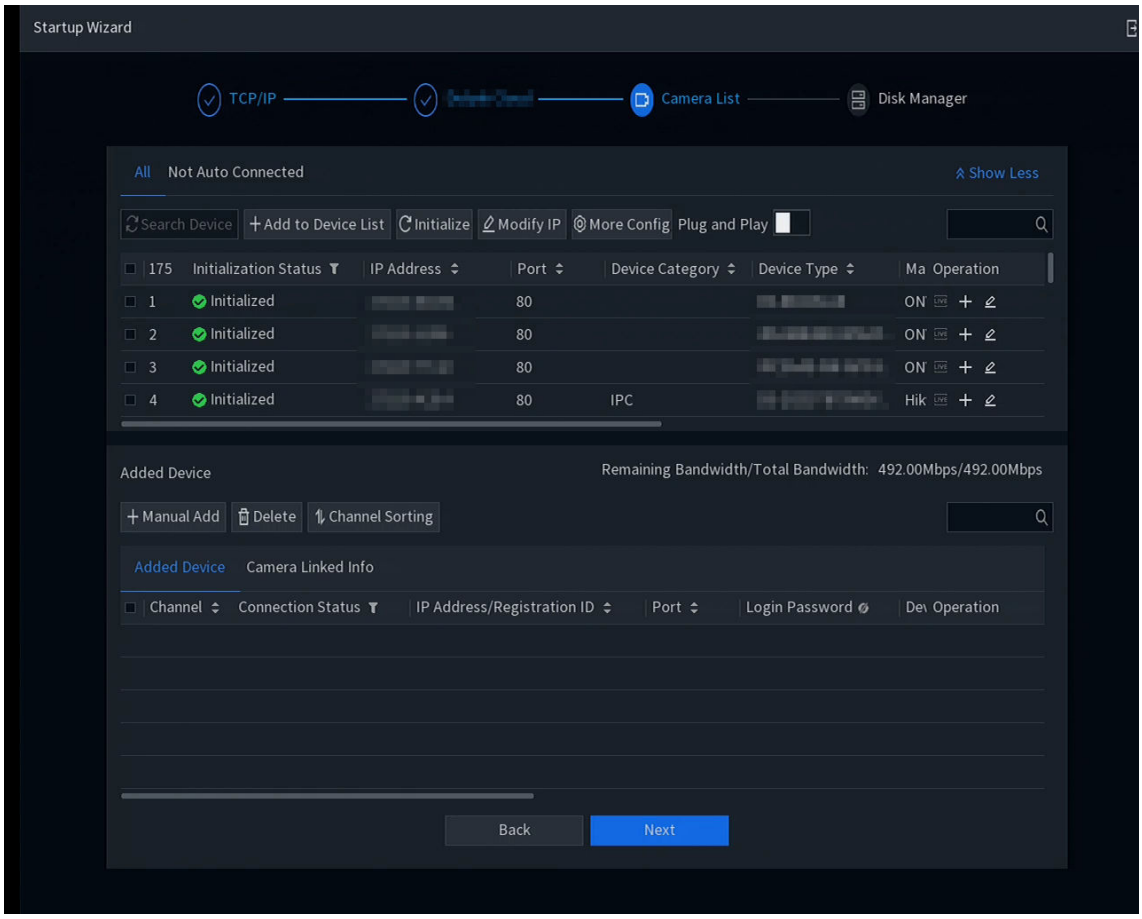


Step 3 Add cameras according to the actual situation, and then click **Next**.

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

- The number of supported cameras varies by models.
- The system supports adding cameras through searching, manual addition and batch addition. This section uses adding by searching as an example.
- Initialize the camera before adding it to the Device.
- When connecting a camera to the NVR through the PoE port, the NVR will automatically initialize the camera. By default, the camera adopts the password and email information of the NVR.
- For non-PoE cameras on the local area network, manual camera initialization enables the camera to adopt the password and email information of the NVR.

Figure 1-7 Camera list



- Click next to **Plug and Play** to enable the **Plug and Play** function.
- Click **Search Device** to search the camera.

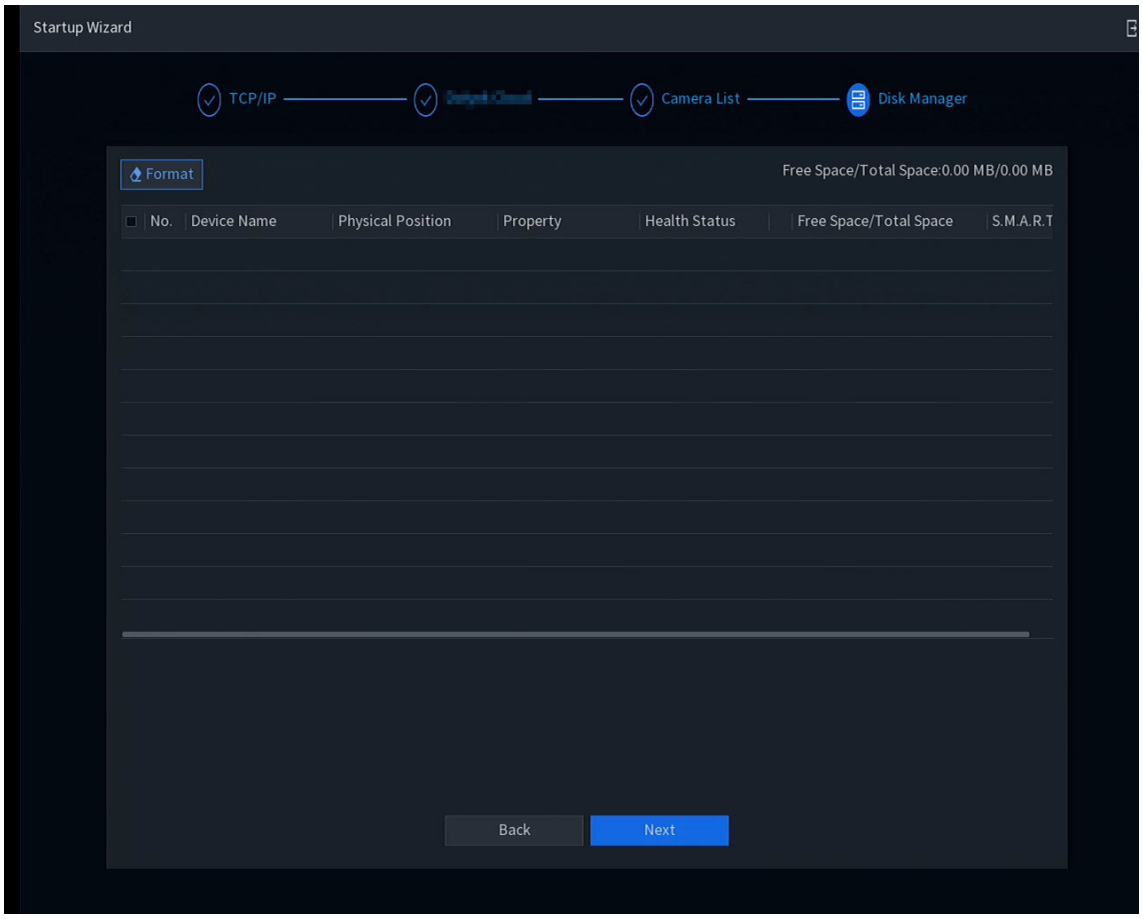
  The devices found are displayed in the upper pane, excluding devices already added.

- To view the live image of a camera, click **LIVE**, and then enter the user name 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.

Step 4 Manage HDD.

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

Figure 1-8 Disk manager



Step 5 Click **Next**.

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

1.1.3 Login

Log in to the Device to perform local operations.

Procedure

Step 1 In the **LIVE** interface, right-click any menu button.

Step 2 Select the login type, including **Password Login** and **Pattern Login**.

Step 3 Log in to the Device.

- Enter the user name and password, and then click **Login** to log in to the Device.
- Draw the pattern to log in to the Device.

Figure 1-9 Login (password)

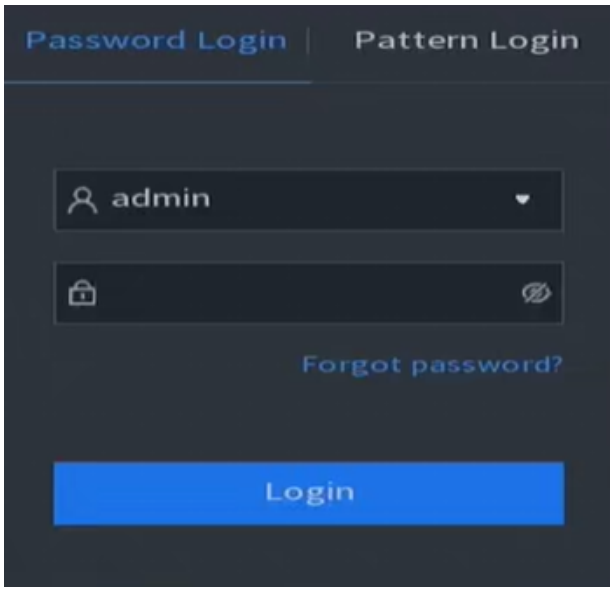


Figure 1-10 Login (pattern)

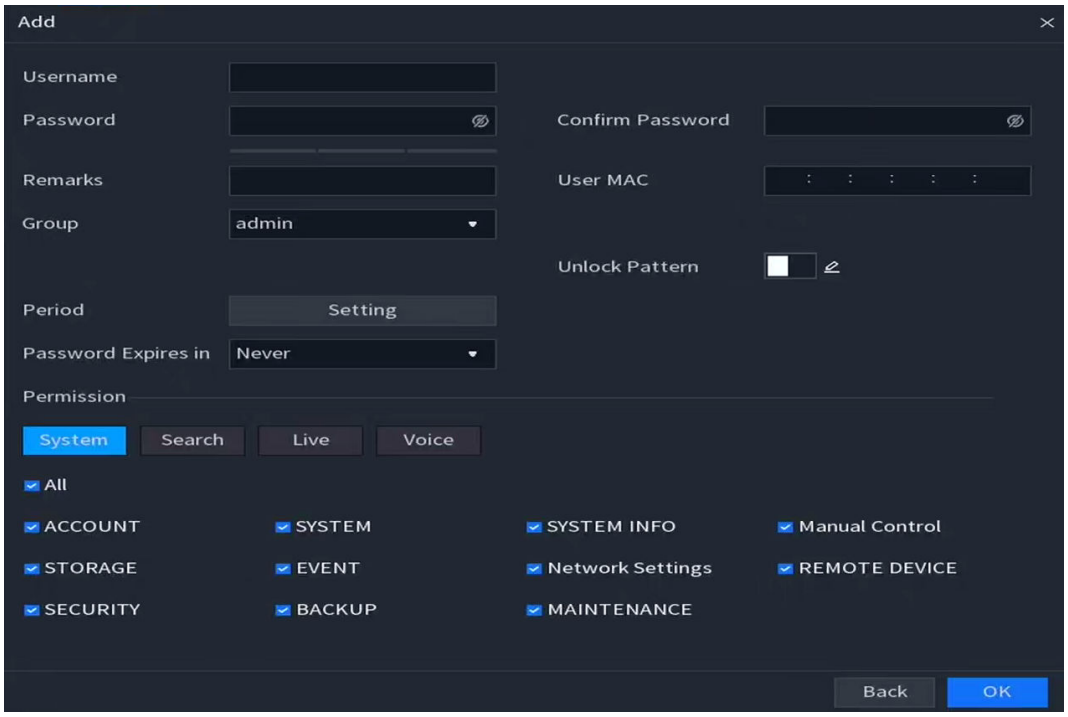
1.2 Adding Users

Procedure

Step 1 Select **Main Menu** > **SETTINGS** > **SYSTEM** > **Account** > **User**.

Step 2 Click **Add**.

Figure 1-11 Adding user



Step 3 Configure the parameters.

For more information about the parameters, see the user manual of the Device.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete the user.

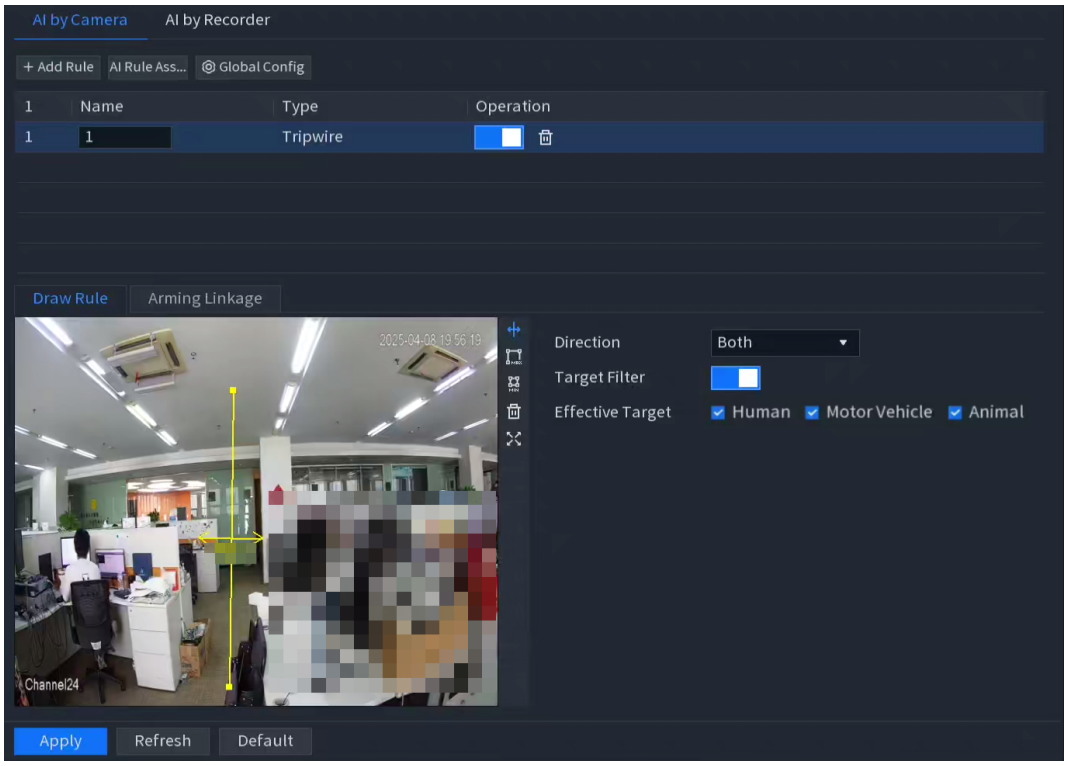
1.3 Configuring Alarm Rules

Tripwire and intrusion are native-supported features of the NVR. For more information about other alarm rules, see user manual of the device.

Tripwire

1. Select **Main Menu** > **SETTINGS** > **EVENT**.
2. Click the remote device channel in **Device List**.
3. Click **Add Rule** to select **Tripwire**.

Figure 1-12 Tripwire



4. Select the preset.

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

5. Enable the function in **Operation** list.
6. (Optional) Click **Global Config** to enable the self-learning function and configure the linked experience database.

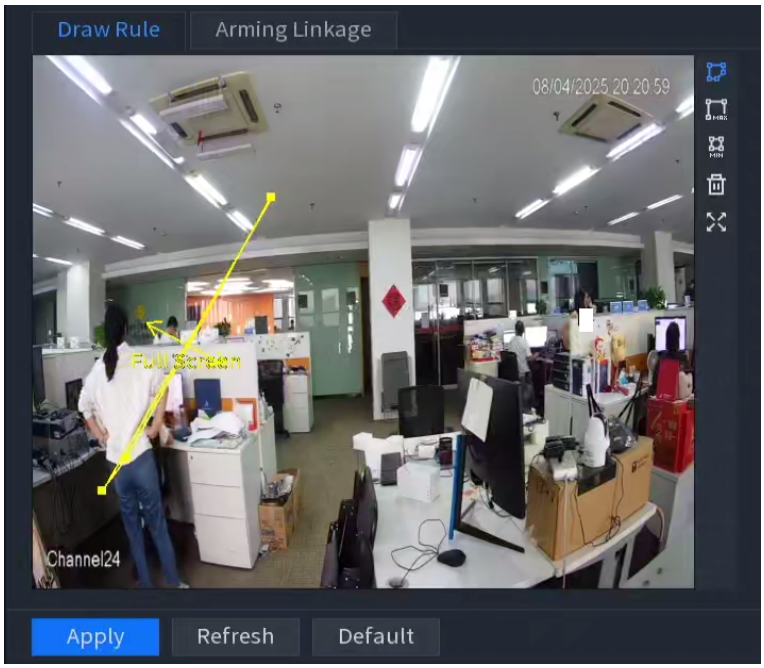
   If you haven't added an experience database, click **Experience Database** to create one.

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

   Some cameras support automatic line drawing by the AI function. Click **AI Rule Assist** and wait for the automatic generation of the rule area. Select the area to be monitored, and then click **Apply** to automatically create the rule.

   a. 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 1-13 Draw rules



b. 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.

c. Configure the parameters.

Table 1-4 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** , **Motor Vehicle** and **Animal** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

d. Click **Arming Linkage**.

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

Click **Schedule** to add the arming schedule and set the period.

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

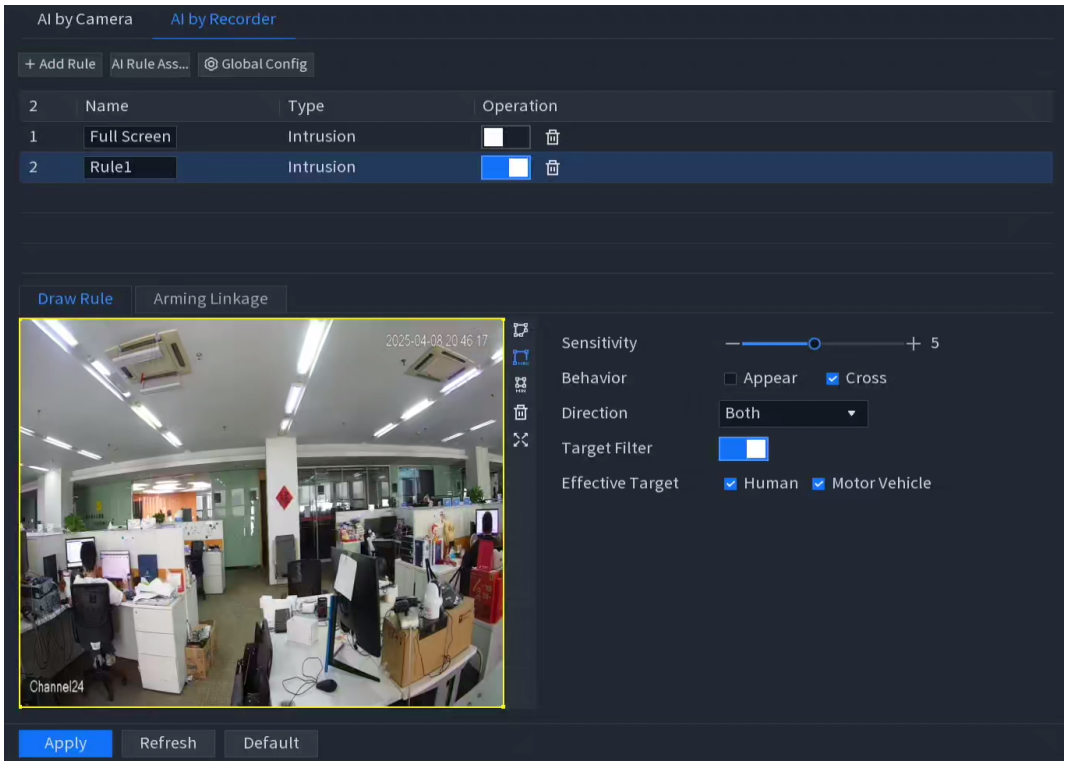
ii. Set alarm linkage actions.

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

Intrusion

1. Select **Main Menu** > **SETTINGS** > **EVENT**.
2. Click the remote device channel in **Device List**.
3. Click **Add Rule** to select **Intrusion**.

Figure 1-14 Intrusion



4. Select the preset.

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

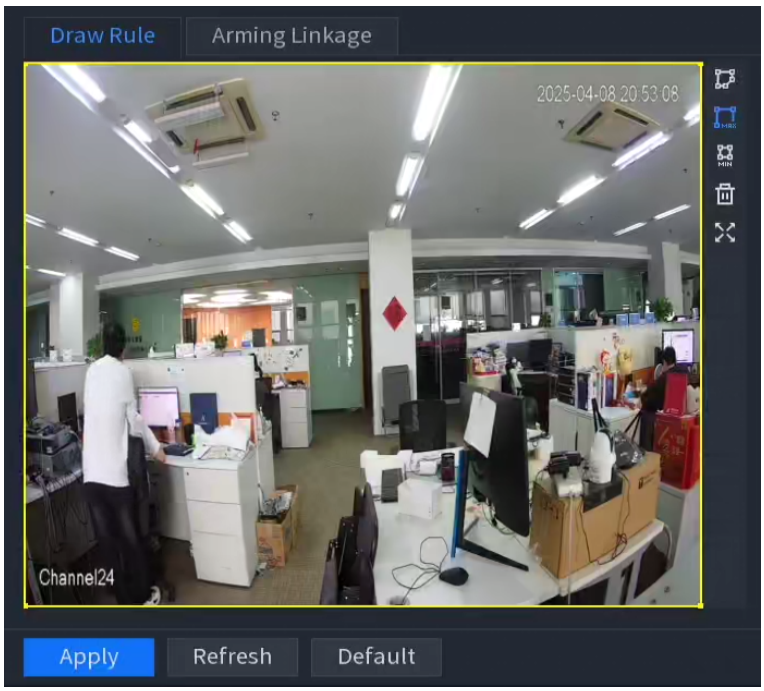
5. From the **Operation** list, enable the function.
6. (Optional) Click **Global Config** to enable the self-learning function and configure the linked experience database.

   If you haven't added an experience database, click **Experience Database** to create one.
7. Click **Draw Rule** to draw the detection rules.

Some cameras support automatic line drawing by the AI function. Click **AI Rule Assist** and wait for the automatic generation of the rule area. Select the area to be monitored, and then click **Apply** to automatically create the rule.

a. 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 1-15 Draw rules



b. 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.

c. Configure the parameters.

Table 1-5 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.

Parameter	Description
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.

8. Click **Arming Linkage**.
   a. From the **Schedule** drop-down list, select an existing alarm schedule.

      Click **Schedule** to add the arming schedule and set the period.

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

   b. Set alarm linkage actions.
9. Select the **Enable** checkbox, and then click **Apply**.

1.4 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 1-16 Video schedule

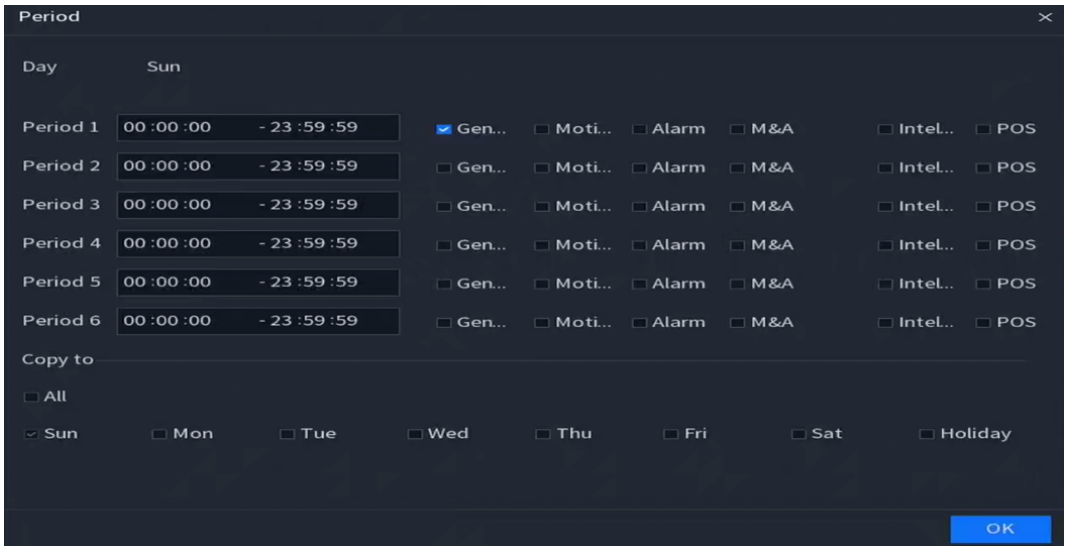
Step 2 Configure the parameters.

Table 1-6 Description of 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.
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, 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 IPC 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.

Parameter	Description
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 1-17 Period



Step 3 Set one or more recording types.

Figure 1-18 Recording type

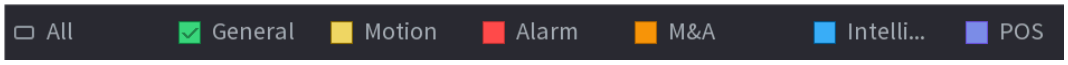


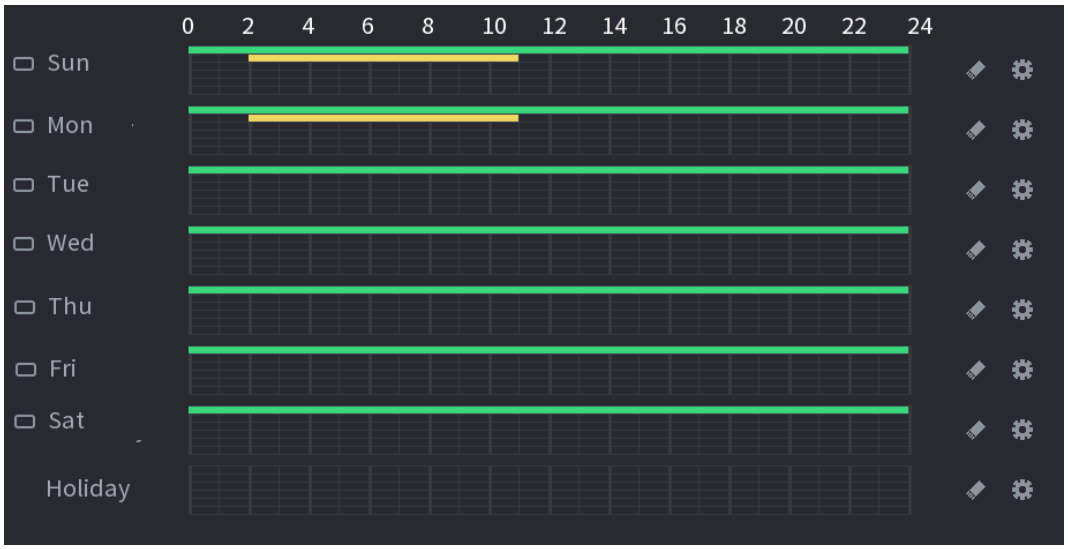
Table 1-7 Recording types and trigger descriptions

Recording type	Trigger condition	Combination rules
General	The device records all videos for the specified time frame.	• When both **General** and other recording types are selected for the same time period, General recording is always active. When motion detection, alarm or smart detection events occur, the corresponding event markers will be added to the recording. • When both **Intelligent** and other recording types are selected for the same time period, Intelligent events take priority. The corresponding recording will be triggered when conditions for other events are met.
Motion	The device records video only when the motion detection is triggered.	
Alarm	The device records video when any linkage abnormal alarm is triggered.	
M&A	M&A recording combines motion recording and alarm recording. The device records video when the motion detection and any alarm is triggered.	
Intelligent	The device records video when the smart detection is triggered.	
POS	The device records video when the POS machine is used to make a payment.	

Step 4 Set the recording period.

If you have added a holiday, you can set the recording period for the holiday.

Figure 1-19 Set record period

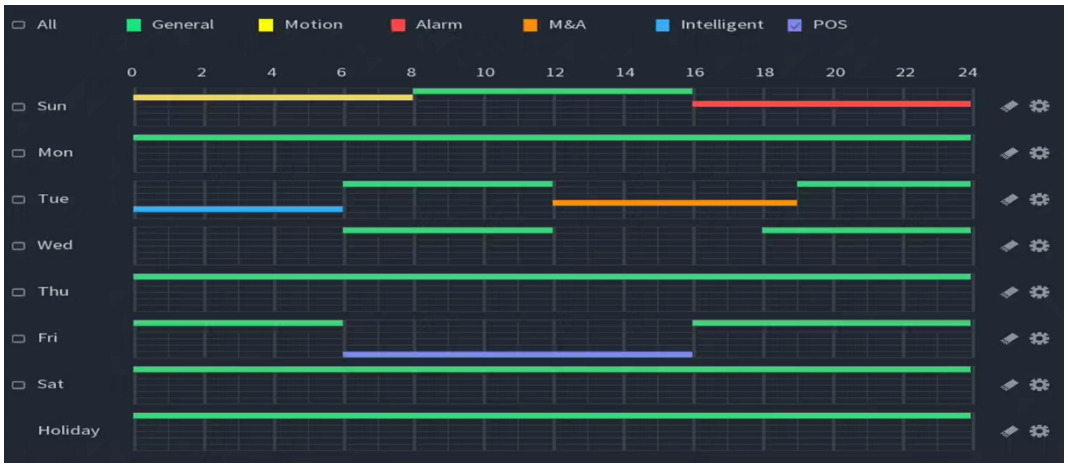


- Define the period by drawing.
  1. Select a corresponding date to set.

- Define for the whole week: Click next to **All**. All the icons 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.
   - When the time periods overlap, 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.

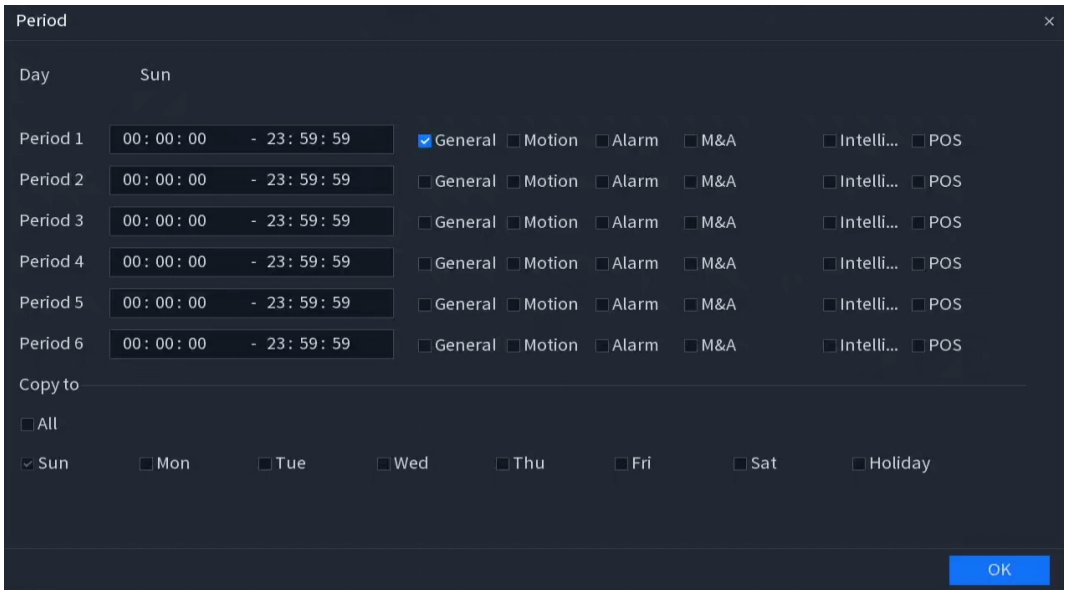
Figure 1-20 Set period by drawing



The Motion record and alarm record functions are both disabled if you enabled M&A.

- Define the period by editing.
  1. Select a date, and then click .

Figure 1-21 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.

1.5 Configuring P2P Settings

You can use the QR code to connect a smartphone to the NVR for management.

Make sure that the NVR has been connected to the Internet, and if yes, in the **Status** box of the P2P interface, it shows **Online**.

1.5.1 Enabling P2P Function

P2P is a convenient private network penetration technology. Instead of applying for dynamic domain name, mapping ports or deploying transit server, you can add 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 access. For more information about the app operation, see the user manual of the app.

1.5.2 Adding the Device to Smartphone Client

You can add devices by manually entering the device SN, scanning the QR code, entering the IP of the device, or by searching on LAN. This topic uses adding the device by scanning the QR code as an example for smartphone client management. For more information about the app operation, see the user manual of the app.

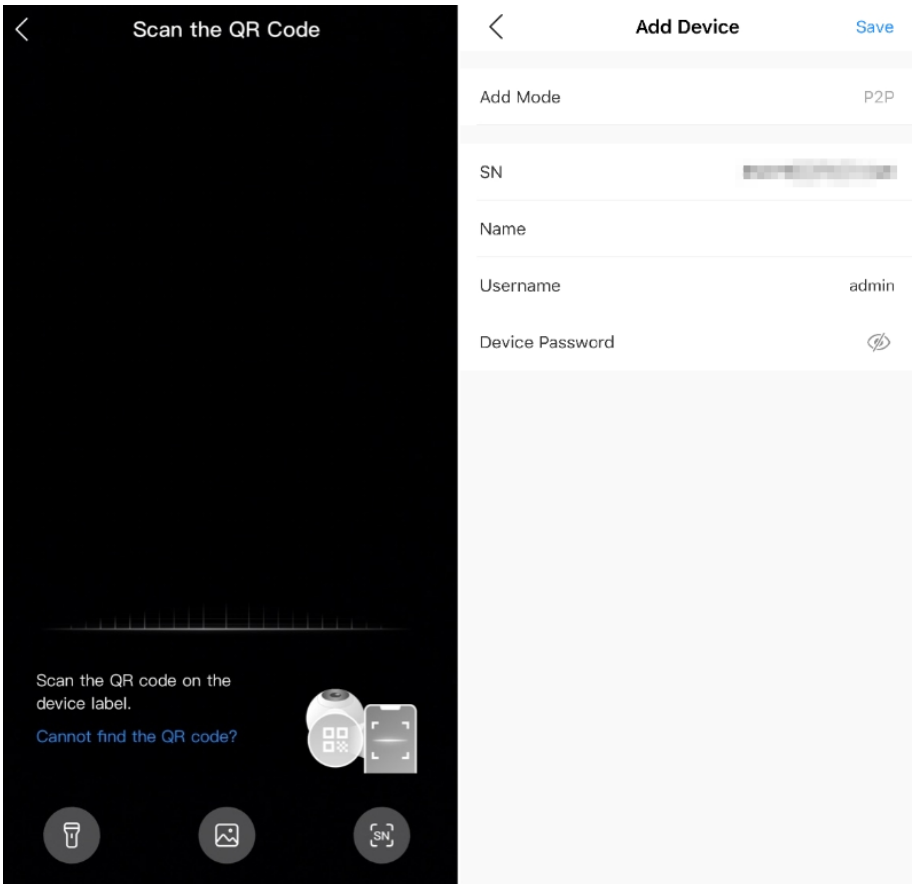
Procedure

Step 1 On the **Home** screen, tap ⊕, and then select **Scan the QR Code**.

Step 2 Add a device.

- Scan the device QR code directly, or tap and import the QR code picture to add a device.
- Tap SN, and then enter the device SN to manually add a device.

Figure 1-22 Add by SN/QR code



Step 3 Select the device type.

Step 4 On the **Add Device** screen, customize the device name, enter the user name and the device password, and then tap **Save**.

1.5.3 Subscribing to Alarm Message on Smartphone Client

You can subscribe for alarm messages, and then alarm notifications will be pushed to smartphone client when an alarm is triggered.

Procedure

Step 1 Log in to the main menu, tap ••• next to the NVR, and then tap **Device Details**.

Step 2 Tap **Notifications**.

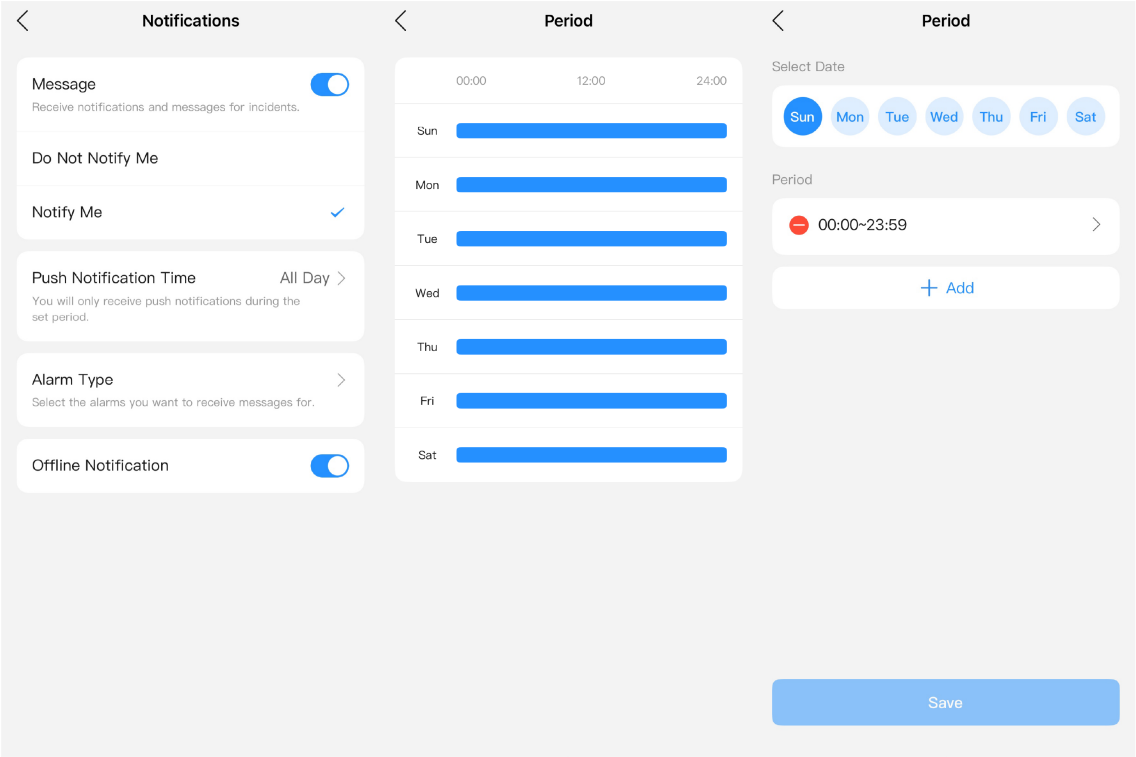
Step 3 Tap next to **Message** to enable the function.

You can select whether to send the notification when there is a message.

- Tap **Do not Notify Me** to not receive message notifications.

- Tap **Notify Me** , tap **Push Notification Time**, tap the weekday, and then set the time period to set the message push time period. You can tap **Add** to add more time period.

Figure 1-23 Set the time period

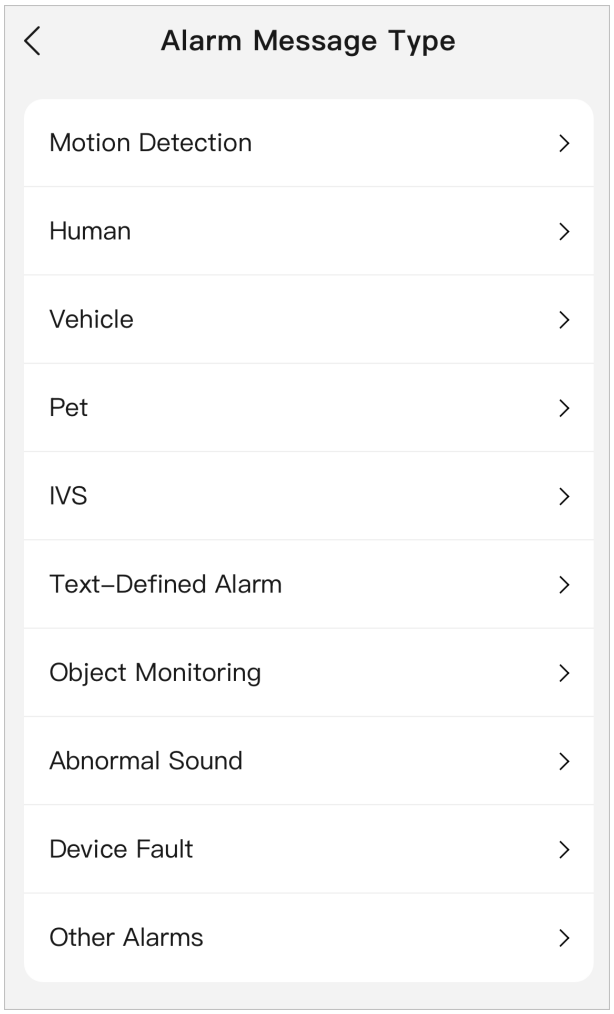


Step 4 Tap **Alarm Type**.

Step 5 Tap **IVS**.

For more information about the alarm message type, see the user manual of the app.

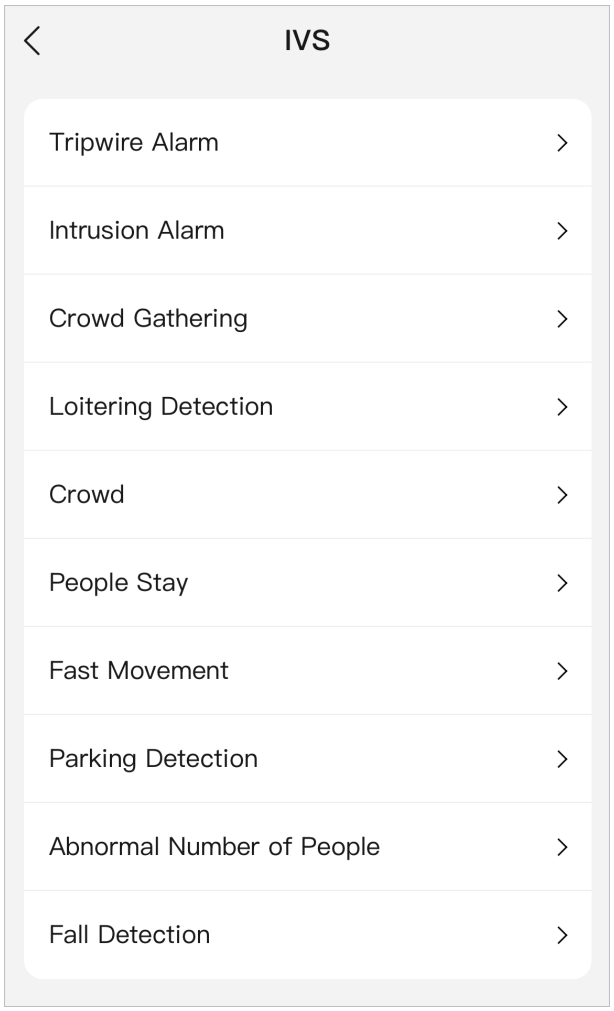
Figure 1-24 Alarm message type



Step 6 Tap **Tripwire Alarm** and **Intrusion Alarm**, select the channels, and then tap **Save** to subscribe for alarm messages.

The number of channels is determined by the models and quantities of added cameras.

Figure 1-25 IVS



1.6 Smart Motion Detection

This topic shows how to configure Smart Motion Detection (SMD).

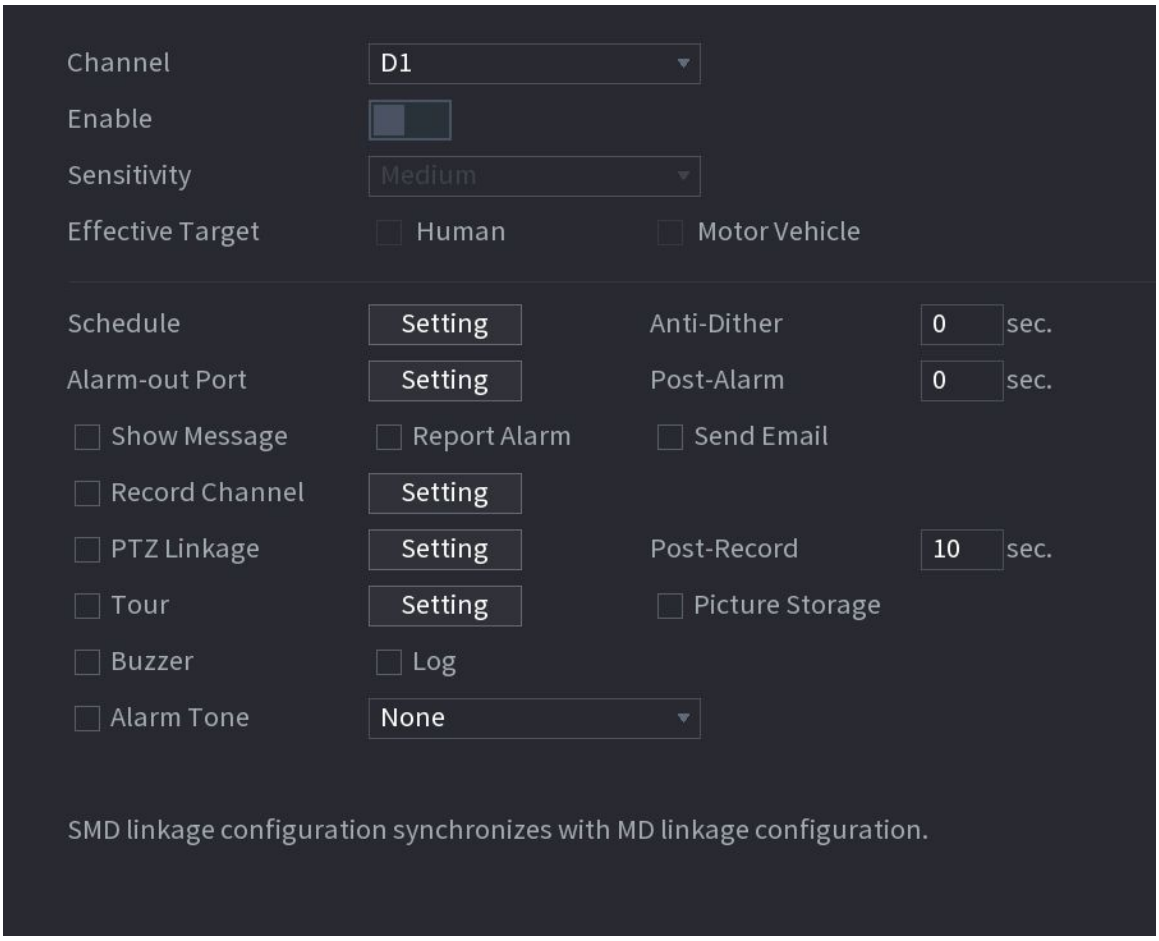
Background Information

Smart Motion Detection (SMD) is an ideal monitoring feature for low-population areas where you want an alert for humans or vehicles anywhere in the scene without having to set rules and draw lines.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameter** > **SMD**.

Figure 1-26 SMD configuration



Step 2 Select and enable a channel, and then configure parameters.

Table 1-8 Description of SMD parameters

Parameter	Description
Sensitivity	The higher the value is, the easier it is to trigger an alarm. But at the same time, the false alarm may occur. The default value is recommended.
Effective Target	Choose human or motor vehicle or both.
Schedule	Configure the period and in the set time range, and the corresponding configuration item will be linked to start the alarm.
Anti-Dither	Indicates the time taken from the end of motion detection to the end of alarm linkage action. The range is 0 seconds to 600 seconds.
Alarm-out Port	The alarm device (such as lights and sirens) is connected to the alarm output port. When an alarm occurs, the NVR device transmits the alarm information to the alarm device.

Parameter	Description
Post-Alarm	When the alarm ends, the alarm is extended for a period of time. The time range is from 0 seconds to 300 seconds.
Show Message	Check box to enable a pop-up message in your local host PC.
Report Alarm	Select the check box. When an alarm occurs, the NVR device uploads an alarm signal to the network (including the alarm center). • This function is available on select models. • You need to set the alarm center first.
Send Email	Select the check box. When an alarm occurs, the NVR device sends an email to the set mailbox to notify the user. You need to set the email first.
Record Channel	Select the check box and select the needed recording channel (support multiple choices). When an alarm occurs, the NVR device activates the channel for recording. You need to enable intelligent recording and auto recording first.
Post-Record	At the end of the alarm, the recording extends for a period of time. The time range is from 10 seconds to 300 seconds.
PTZ Linkage	Select the check box and click **Setting** to select the channel and PTZ action. When an alarm occurs, the NVR device associates the channel to perform the corresponding PTZ action. For example, activate the PTZ in channel one to turn to the preset point X. • You need to set the corresponding PTZ actions first. • The SMD-triggered alarm for PTZ linkage can only link to preset points, and cannot link to patrols or tour.

Parameter	Description
Tour	Select the check box and select the channel for tour. When an alarm occurs, the local interface of the NVR device displays the selected channel screen. • You need to set the time interval and mode for tour first. • After the tour is over, the preview interface is restored to the screen split mode before the tour.
Picture Storage	Select the Snapshot check box to take a snapshot of the selected channel. To use this function, select **Main Menu** > **CAMERA** > **Encode** > **Snapshot**, select **Event** in **Type** list.
Buzzer	Select the check box to activate the buzzer when an alarm occurs.
Alarm Tone	Check the box and then select the corresponding audio file from the drop-down list. System plays the audio file when the alarm occurs. You need to add audio file first.

Step 3 Click **Apply**.

1.7 Live View

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. For more information about the live view page of the device, see the user manual of the device.

Figure 1-27 Live view page

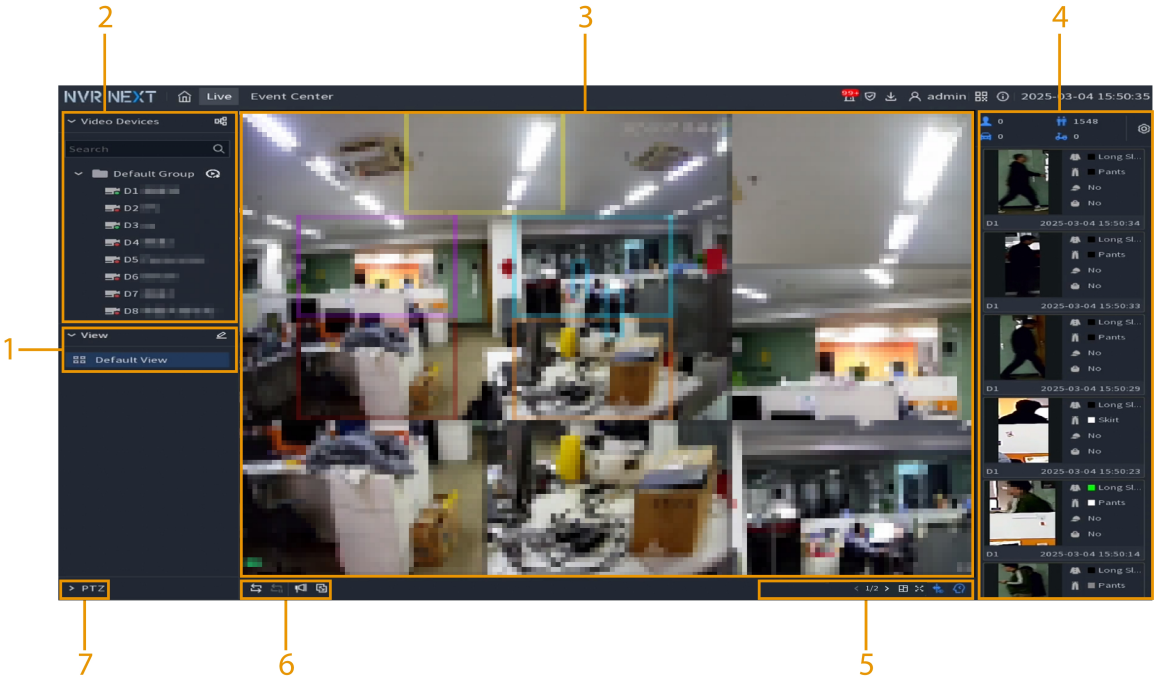


Table 1-9 Page description

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.
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.
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	• 1/2 is used to switch the channel display. • is used to modify the content shown in the display.

No.	Module	Description
6	Channel switching and broadcasting	• Click to start tour and click to pause or proceed with tour. • Click to enable the voice broadcast function. ◇ You can select **Video Device** or **IP Speaker** for the function. ◇ For the talking function, reuse the device (for example, IPC) talk button; if the device is associated with an IP speaker, talk with the speaker; if not associated, talk with the device. • Click to switch channels to display on the main or secondary screen.
7	PTZ settings	Adjust the PTZ settings of devices.

View

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

   Select and hold the left mouse button on a channel and drag it to the live view.

   In the adding view page, you can click to configure advertisement resources in binding settings.

Figure 1-28 Binding settings

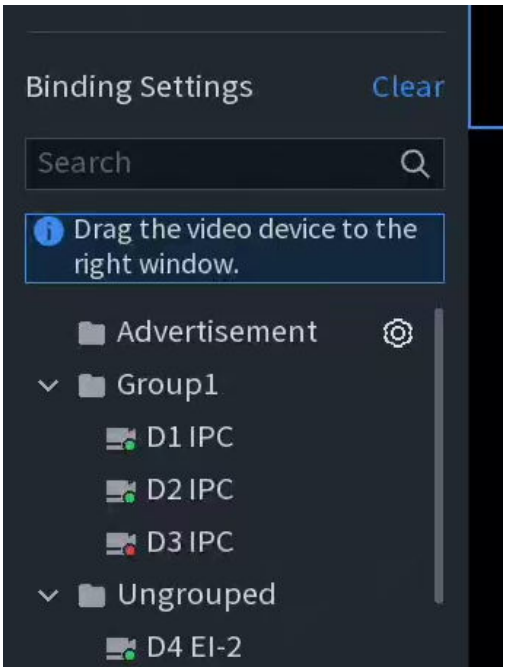
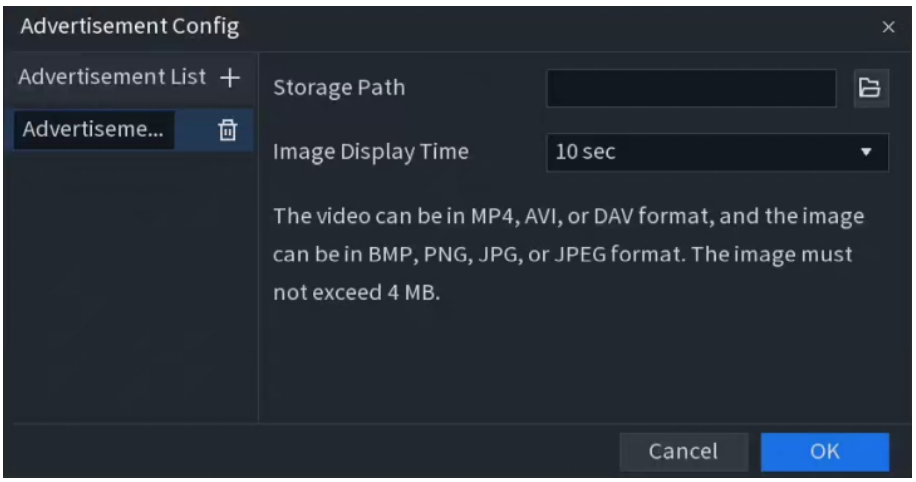


Figure 1-29 Advertisement configurations



Select the layout, drag an advertisement from the left list and drop it onto a pane in the right view layout to bind it. Click **Save** to save the view.

Advertisement playback is supported in both layout editing and live view modes. Manual pause and volume adjustment for video advertisements are also supported.

3. Click to delete the view layout.

Channel Display and Layout

- 1/2 : 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 1-30 AI live view

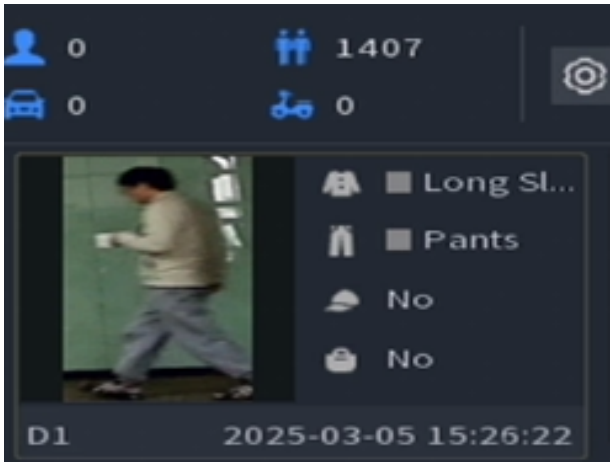
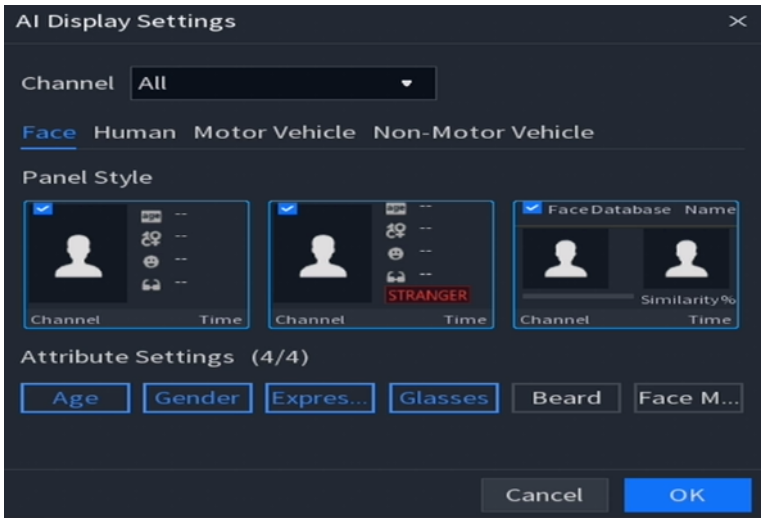


Figure 1-31 AI display settings



1.8 Playback

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. For more information about the playback page of the device, see the user manual of the device.

Figure 1-32 General video

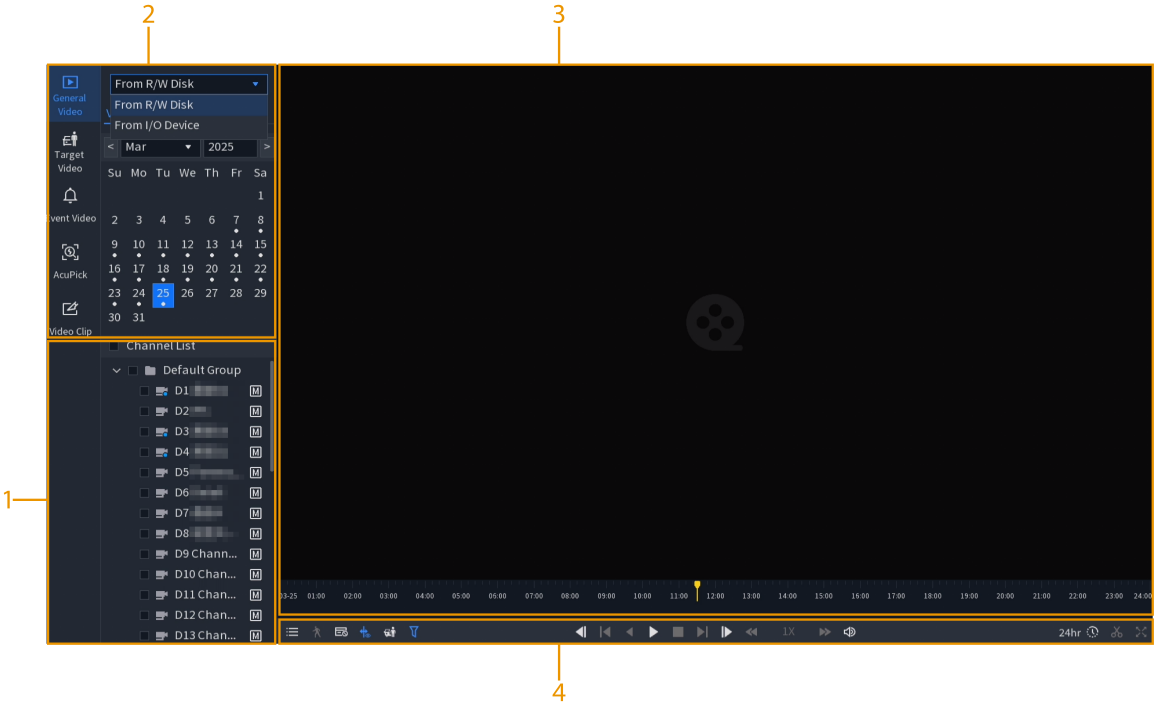


Table 1-10 Description of the general video page

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.

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.
- Click to configure the EPTZ.
- Click to set the fisheye dewarping.
- 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 wheel to 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.
- The timeline 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 1-33 Playback control

Table 1-11 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.
	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.
,	Displays 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.
24hr	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.

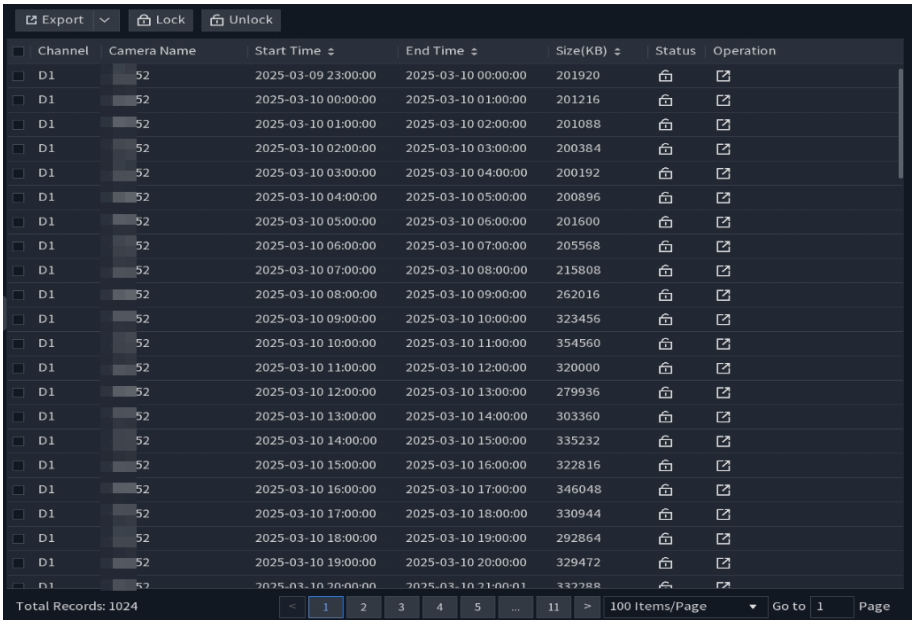
Icon	Function
	View the videos in full screen.

Video Backup

An external storage device is required to back up the video files.

1. In the main menu, select **BACKUP**, and then click to enter the video backup page.
2. Select the video type, stream type and file status, and then set the time range.
3. Select the channel in the channel list, and then click **Search**.
4. Select the video files to be backed up.
5. Click **Export** or in the operation list to export the files.

Figure 1-34 Video backup



6. Select the storage device, and then 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.

7. (Optional) Click **Lock** or **Unlock** to modify the file status.

Picture Backup

An external storage device is required to back up the picture.

1. In the main menu, select **BACKUP**, and then click to enter the picture backup page.
2. Select the time range and select the channels in **Channel List**.
3. Click **Search**.
4. Select pictures to be backed up.
5. Click **Export** or in the operation list to export the files.
6. Select the storage device, and then click **Backup**.
7. (Optional) Click **Lock** or **Unlock** to modify the file status.

2 Web Operation

2.1 Network Connection

Background Information

- The factory default IP of the Device is 192.168.1.108.
- The device supports monitoring through different browsers such as Safari, Firefox, and Google Chrome. You can perform functions such as multi-channel monitoring, PTZ control, and device parameters configuration.

Procedure

Step 1 Check to make sure the device has connected to the network.

Step 2 Configure the IP address, subnet mask and default gateway for the computer and the device. For more information about the network configuration of the device, see the user manual of the device.

Step 3 On your computer, check the network connection using "ping ***.***.***.***". Usually the return value of TTL is 255.

2.2 Web Login

Procedure

Step 1 Open the browser, enter the IP address of the Device, and then press Enter.

Step 2 Enter the user name and password, select a login type.

- 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**.

Related Operations

Click the language box on the upper-right corner of the page, select the corresponding language to switch the corresponding language.

Appendix 1 Security Recommendation

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**

   The 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, it is recommended 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;
   - Establish 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**

   It is recommended 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).