Network Video Recorders

User Manual

V1.00

Contents

Disclaimer and Safety Warnings

Preface

The content of this section is designed to ensure that users use the product correctly to prevent dangers or property loss caused by improper operation. Before using this product, be sure to read this manual carefully. Please keep this manual properly for future reference.

About This Manual

- We recommend that you use this manual under the guidance of a professional.
- This manual is designed for use with multiple product models, and it is not possible to list the appearance and functions of each product individually. Please refer to the actual product for use.
- This manual is intended for multiple software versions, and the illustrations and descriptions in this manual may be different from the actual GUI and functions of the software.
- Despite our best efforts, technical or typographical errors may exist in this manual. Our company cannot be held responsible for any such errors and reserves the right to change the manual without prior notice.
- Users are fully responsible for the damages and losses that arise due to improper operation.
- Our company reserves the right to change any information in this manual without any prior notice or indication. Due to such reasons as product version upgrade or regulatory requirement of relevant regions, this manual will be periodically updated.
- This manual will be updated in real time according to the laws and regulations of the relevant regions. For specific details, please refer to the product's paper copy, QR code, or official website. In case of any discrepancy between the paper copy and the electronic version, the electronic version shall prevail.

About This Product

If the product you have chosen is a video product, please strictly adhere to the applicable laws and regulations. You can visit our official website to inquire about the relevant content.

Instructions for Use

- This document serves as a guide for use only. All statements, information, and suggestions contained in this document do not constitute any express or implied warranty.
- We assume no responsibility for any special, incidental, consequential, or indirect damages resulting from the use of this manual or the use of our products, including but not limited to losses due to loss of business profits, data or document loss, and product malfunction or information leakage caused by cyber-attack, hacker attack, and virus infections.
- Due to uncertain factors such as the physical environment, there may be discrepancies between the actual values of some data and the reference values provided in the manual. In case of any questions or disputes, the company's final interpretation shall prevail.

Formatting Conventions

The UI formatting conventions used in this document are as follows:

Format	Meaning
Bold	Bold means UI elements (button names, menu names, window names, etc.), e.g., Click **Save**.
>	Indicate a sequence of actions, e.g., click Device Management > Add Device, which means first click Device Management, and then click Add Device.

Symbol Conventions

This document uses various distinctive symbols to highlight areas that require special attention during the operation process. The meanings of these symbols are as follows:

Symbol	Meaning
	NOTE: Provides tips and additional information related to the operation and use of the product.
	CAUTION: Alerts to matters that requires attention during operation, as improper handling may lead to product damage, data loss, or functional abnormalities.
	WARNING: The annotations following this symbol demand extra attention, as improper handling could potentially cause personal injury.

Legal Statement

Copyright Statement

Trademark Acknowledgements

Export Compliance Statement

We comply with applicable export control laws and regulations worldwide, including that of the People's Republic of China and the United States, and abide by relevant regulations relating to the export, re-export and transfer of hardware, software and technology. Regarding the product described in this manual, we ask you to fully understand and strictly abide by the applicable export laws and regulations worldwide.

Disclaimer of Liability

- To the extent allowed by applicable law, in no event will we be liable for any special, incidental, indirect, consequential damages, nor for any loss of profits, data, and documents.
- The product described in this manual is provided on an "as is" basis. Unless required by applicable law, this manual is only for informational purpose, and all statements, information, and recommendations in this manual are presented without warranty of any kind, expressed or implied, including, but not limited to, merchantability, satisfaction with quality, fitness for a particular purpose, and noninfringement.
- Users must assume total responsibility and all risks for connecting the product to the Internet, including, but not limited to, network attack, hacking, and virus. We strongly recommend that users take all necessary measures to enhance the protection of network, device, data and personal information. We disclaim any liability related thereto but will readily provide necessary security related support.
- To the fullest extent permitted by applicable law, in no event shall we, our employees, licensors, or affiliates be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, loss of sales or business, loss of data, or costs of procurement of substitute goods or services, arising out of or related to your use or inability to use the product or service, even if advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so the above limitations may not apply to you.
- To the extent allowed by applicable law, in no event shall our total liability to you for all damages for the product described in this manual exceed the amount of money that you have paid for the product.

- When using this product, please strictly adhere to the applicable laws and regulations to avoid infringing upon the rights of third parties, including but not limited to intellectual property rights, data rights, or other privacy rights. You must also not use this product for the purposes of developing or facilitating the use of weapons of mass destruction, biological or chemical weapons, nuclear weapons, or for any other purposes that violate international norms and regulations.

Privacy Protection Reminder

Uniview complies with applicable privacy protection laws and is committed to protecting user privacy. You may want to read our full privacy policy at our website and get to know the ways we process your personal information.

Please be aware, using the product described in this manual may involve the collection of personal information such as face, fingerprint, license plate number, email, phone number, GPS. Please abide by your local laws and regulations while using the product.

Safety Warnings

The device must be installed, serviced and maintained by a trained professional with necessary safety knowledge and skills. Before you start using the device, please read through this guide carefully and make sure all applicable requirements are met to avoid danger and loss of property.

Storage, Transportation, and Use

- Store or use the device in a proper environment that meets environmental requirements, including and not limited to, temperature, humidity, dust, corrosive gases, electromagnetic radiation, etc.
- Make sure the device is securely installed or placed on a flat surface to prevent falling.
- Unless otherwise specified, do not stack devices.
- Ensure good ventilation in the operating environment. Do not cover the vents on the device. Allow adequate space for ventilation.
- Prevent water or other liquids from entering the device. It may cause device damage and risks such as electric shock and fire.
- Make sure the power supply provides a stable voltage that meets the power requirements of the device. Make sure the power supply's output power exceeds the total maximum power of all the connected devices.
- Verify that the device is properly installed before connecting it to power.
- Do not remove the seal from the device body without consulting us first. Do not attempt to service the product yourself. Contact a trained professional for maintenance.
- Always disconnect the device from power before attempting to move the device.
- Take proper waterproof measures in accordance with requirements before using the device outdoors.
- Warning: Operating this device in a residential environment may cause radio interference.

Power Requirements

- Install and use the device in strict accordance with your local electrical safety regulations.
- Use the recommended cordset (power cord) in accordance with the specified ratings.
- Only use the power adapter supplied with your device.
- Use a mains socket outlet with a protective earthing (grounding) connection.
- Ground your device properly if the device is intended to be grounded.

Battery Safety

Please use batteries properly; otherwise, there is a risk of fire or explosion.

- Warning: Using incorrect battery models can lead to explosion.
- If you need to replace the battery, it is recommended that you go to an authorized service center or have it replaced under professional supervision. We shall not be held responsible for any issues arising from unauthorized battery replacement.

- When replacing the battery, be sure to use a battery of the same type as the original. Using the wrong model for replacement (such as certain types of lithium batteries) may cause safety protection to fail.
- Batteries must not be exposed to overheat environments such as sunlight, fire, as this may lead to fire, explosion, or combustion.
- Do not dispose of batteries in fire or heating appliances. Do not squeeze, bend, or cut batteries, as it may cause explosion.
- Do not expose batteries to extremely high or low temperatures, or to very low-pressure environments, as this may cause explosion or leakage of flammable liquid/gas.
- For products or the included remote control containing a button cell battery: Do not ingest the battery-chemical burn hazard! If swallowed, a button cell battery can cause severe internal burns within 2 hours and may be fatal. Precautions (including but not limited to):
  - Keep new and used batteries away from children.
  - Stop using the product and keep it away from children if the battery compartment is not securely closed.
  - If you suspect that a battery may have been swallowed or inserted inside any part of the body, seek immediate medical attention.

Network Security

Please take all necessary measures to enhance network security for your device.

The following are necessary measures for the network security of your device:

- **Change the default password and set a strong password:** You are strongly recommended to change the default password after your first login and set a strong password of at least nine characters including all three elements: digits, letters and special characters.
  - Do not include the account name or the reverse of the account name.
  - Avoid using consecutive characters, such as 123, abc, etc.
  - Do not use overlapping characters, such as 111, aaa, etc.
- **Keep firmware up to date:** It is recommended that your device is always upgraded to the latest version for the latest functions and better security. Visit our website or contact your local dealer for the latest firmware.

The following are recommendations for enhancing network security of your device:

- **Change password regularly:** Change your device password on a regular basis and keep the password safe. Make sure only the authorized user can log in to the device.
- **Enable HTTPS/SSL:** Use SSL certificate to encrypt HTTP communications and ensure data security.
- **Enable IP address filtering:** Allow access only from the specified IP addresses.
- **Minimum port mapping:** Configure your router or firewall to open a minimum set of ports to the WAN and keep only the necessary port mappings. Never set the device as the DMZ host or configure a full cone NAT.
- **Disable the automatic login and save password features:** If multiple users have access to your computer, it is recommended that you disable these features to prevent unauthorized access.
- **Choose username and password discretely:** Avoid using the username and password of your social media, bank, email account, etc., as the username and password of your device, in case your social media, bank and email account information is leaked.
- **Restrict user permissions:** If more than one user needs access to your system, make sure each user is granted only the necessary permissions.
- **Disable UPnP:** When UPnP is enabled, the router will automatically map internal ports, and the system will automatically forward port data, which results in the risks of data leakage. Therefore, it is recommended to disable UPnP if HTTP and TCP port mapping have been enabled manually on your router.
- **SNMP:** Disable SNMP if you do not use it. If you do use it, then SNMPv3 is recommended.
- **Multicast:** Multicast is intended to transmit video to multiple devices. If you do not use this function, it is recommended you disable multicast on your network.
- **Check logs:** Check your device logs regularly to detect unauthorized access or abnormal operations.
- **Physical protection:** Keep the device in a locked room or cabinet to prevent unauthorized physical access.

- **Isolate video surveillance network:** Isolating your video surveillance network with other service networks helps prevent unauthorized access to devices in your security system from other service networks.

You may also obtain security information under Security Response Center at Uniview's official website.

Cleaning and Dust Removal

Regular dust removal significantly prevents overheating risks, extends hardware lifespan, and ensures stable operation. For dusty areas such as factories and warehouses, clean every 1 to 3 months; for normal offices, clean every 6 to 12 months.

Always power off the device, prevent static discharge, and handle all components gently during operation to avoid equipment damage due to improper operation. After shutting down the device, unplug the power cable to ensure it is completely powered off. It is recommended to allow internal components to cool before cleaning. Please wait at least 5 minutes for devices with fewer than 8 disks, and 15 minutes for devices with 8 or more disks. Pay special attention to cleaning the fan, cooler, internal power supply, etc.

- External cleaning: Use a lightly dampened and well-wrung anti-static cloth to clean dust and stains from the casing. Do not spray alcohol, detergent, or any other liquid directly onto the chassis surface; otherwise, the liquid may cause the interior component corrosion or conductive residue. For stubborn stains, apply a small amount of neutral cleaner to the cloth, wipe the stain, and promptly dry it with a dry cloth.
- Internal cleaning: Wear an anti-static wrist strap or gloves to prevent electrostatic discharge (ESD) damage to electronic components. Use a soft-bristled brush to gently remove accumulated dust from electronic components, fans, and ventilation ports. Stubborn dust may be cleaned using compressed air. Hold the can upright to prevent liquid from spraying out, and keep it at least 10 cm away from components to prevent damage or frost formation caused by rapid temperature change.

1 Initial Configuration

1.2 Device Login

First Login

1. After selecting your language, use the default password 123456 to log in and follow the on-screen instructions to change your password.

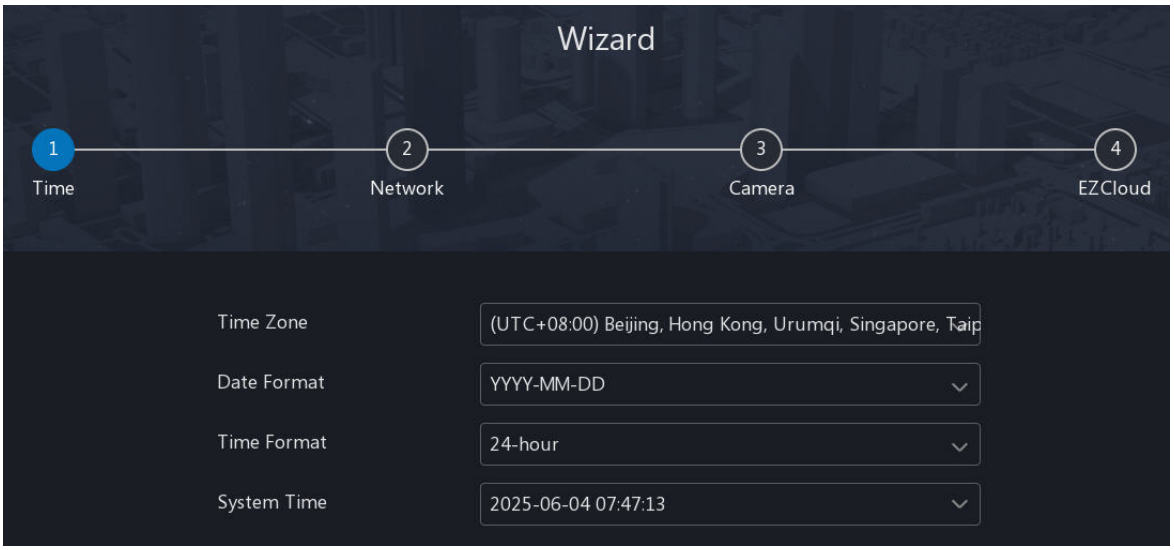
   It is recommended to save your email address in case you need to reset the password in the future; if no email address is saved, you will need to contact customer service to reset or retrieve your password.

2. (Optional) Draw the same pattern twice to set the pattern password. The pattern will be used as the primary unlock method. You may skip this step and proceed directly to the wizard.

Note: If you need to add or change the saved email, reset or disable the pattern password by clicking in User Management on the local interface.

Wizard

Follow the on-screen instructions to complete the configuration, or click number 4 and then click **Complete** to skip the wizard. You can configure it later in Basic Configuration on the local interface.



When configuring the network, make sure the router has DHCP enabled to automatically assign the IP address, subnet mask, and default gateway.

For detailed information about channel configuration, see Add Cameras.

To add the device to the app, ensure that EZCloud is enabled; otherwise, the device cannot be added to the app.

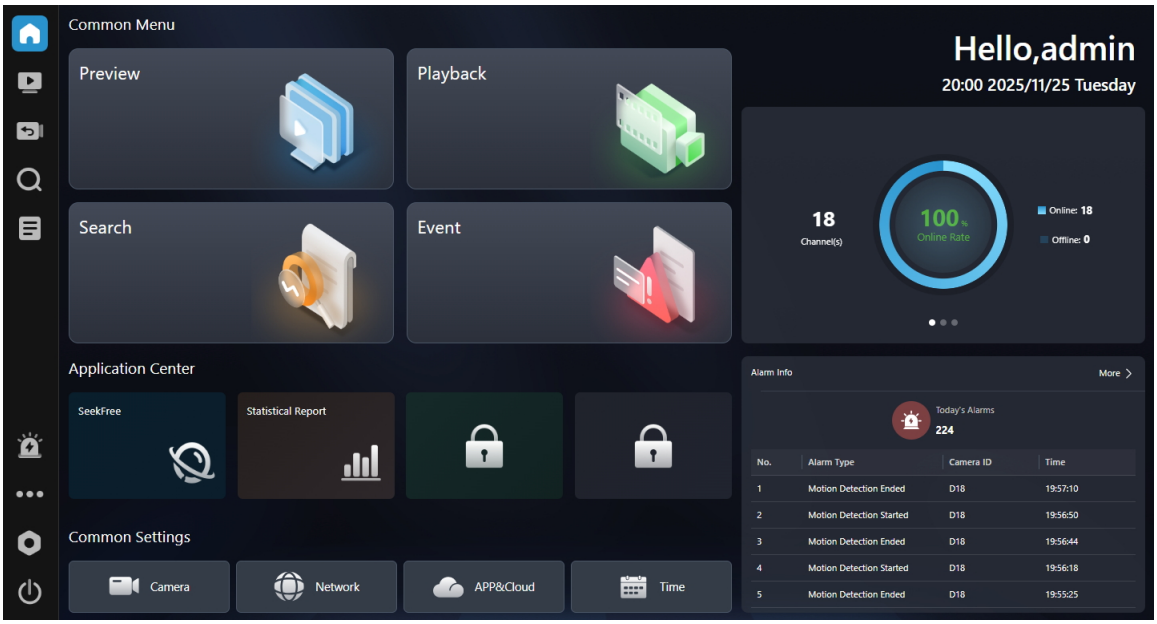
1.3 Reset Password

If you forgot the admin user's login password or want to reset the password, you can click **Forgot Password** on the login page and then follow the on-screen instructions to reset the password.

Note: If you perform a password reset operation on the web interface without a saved email address, you need to contact customer service (globalsupport@uniview.com) for assistance.

2 Home

The home page is divided into three sections from left to right: main menu, applications, and data dashboard.



Main Menu

The main menu contains all the functions. Click an icon to access the corresponding function. Each menu item is detailed in a specific chapter in this manual. You can search by the menu name to locate the relevant section.

Applications

The applications include three sections: Common Menu, Application Center, and Common Settings. You can click the links in the table below to view the corresponding descriptions for each function.

Module	Link
Common Menu	• Preview • Playback • Search • Event
Application Center	• Statistical Report • SeekFree
Common Settings	• IPC Configuration • Network • APP&Cloud • Time

Data Dashboard

The data dashboard displays the status of channels, network, and hard disks, as well as alarm information for all channels on the current day. Click **More** to view more alarms.

2.1 People Flow Counting

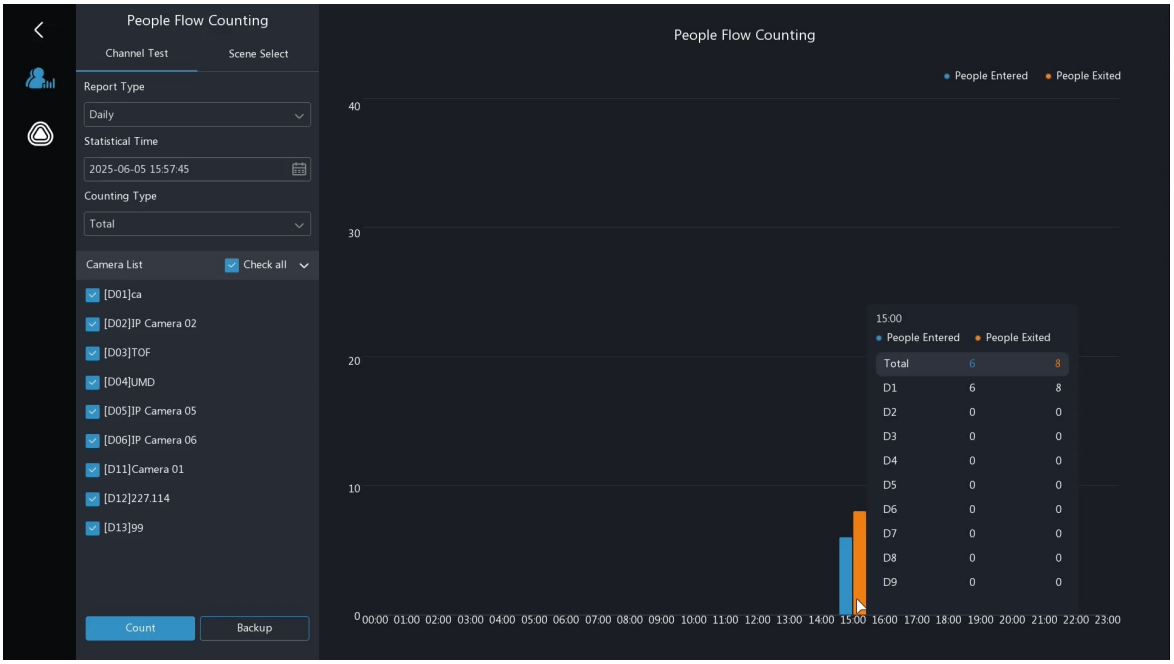
Search People Flow Counting data to view the number of people entered or exited within a specified time period. You can search by specified channel or scene, and by day, week, month, or year.

Note: For information about scene configuration, see People Present Alarm.

1. Go to **Home** > **Statistical Report** > **People Flow Counting**.
2. Configure the search criteria and click **Count** to view the results.

- Channel: Counts the number of people entered/exited by the selected channel.
- Scene: Counts the number of people entered/exited by the selected scene.

3. Click **Backup** to export search results in Excel format to the specified path in the USB drive (local interface) or computer (web interface).

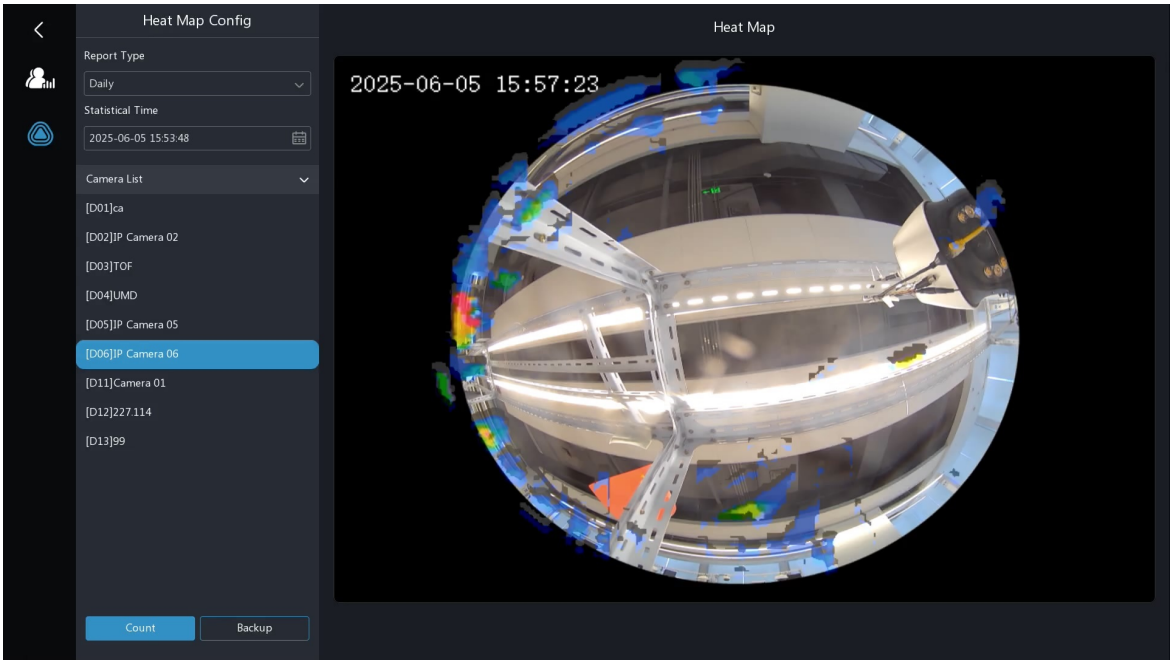


2.2 Heat Map Configuration

This feature is used with fisheye cameras and is commonly used to analyze people flow in supermarkets or retail stores. It can generate a heat map based on people flow data from a specific camera within a certain time period, helping infer the types of popular products.

Note: Please complete the heat map configuration on the camera's web interface. For detailed operations, refer to the *Network Camera User Manual*.

1. Go to **Home** > **Statistical Report** > **Heat Map Config**.
2. Configure the search criteria and click **Count** to view the results.
3. Click **Backup** to export the heat map image to the specified path on the USB drive (local interface).



2.3 SeekFree

SeekFree is a VCA function based on the large model algorithm, designed to help users quickly retrieve snapshots and recordings that meet search criteria. It can search images by image or text using various criteria, including keywords, target types, camera ID, time, and similarity.

When specific target details are unavailable, you can search by text to quickly retrieve a target image, which can then be used for a progressive search to obtain highly accurate results. It can improve the information retrieval efficiency and provide valuable clues for finding targets or people.

Note:

- This function is unavailable for certain smart functions, for example, high-rise littering.
- This function is unavailable if you enter sensitive keywords related to regulation violations, harmful content, or human rights infringements.

1. Go to **Home** > **SeekFree**.

Figure 2-1: SeekFree

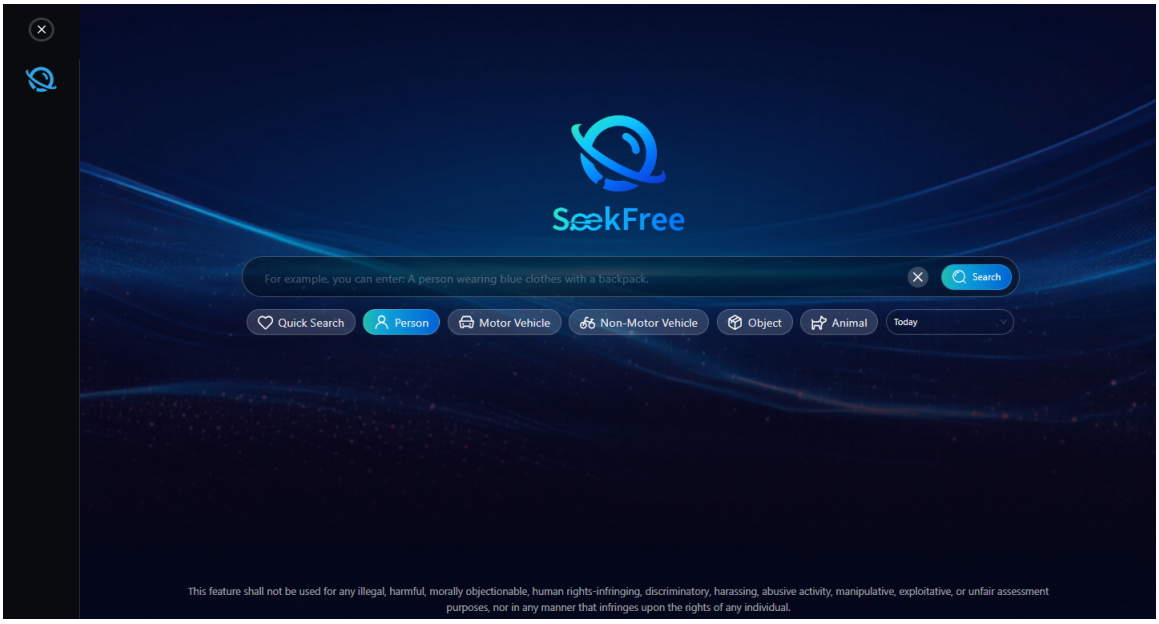
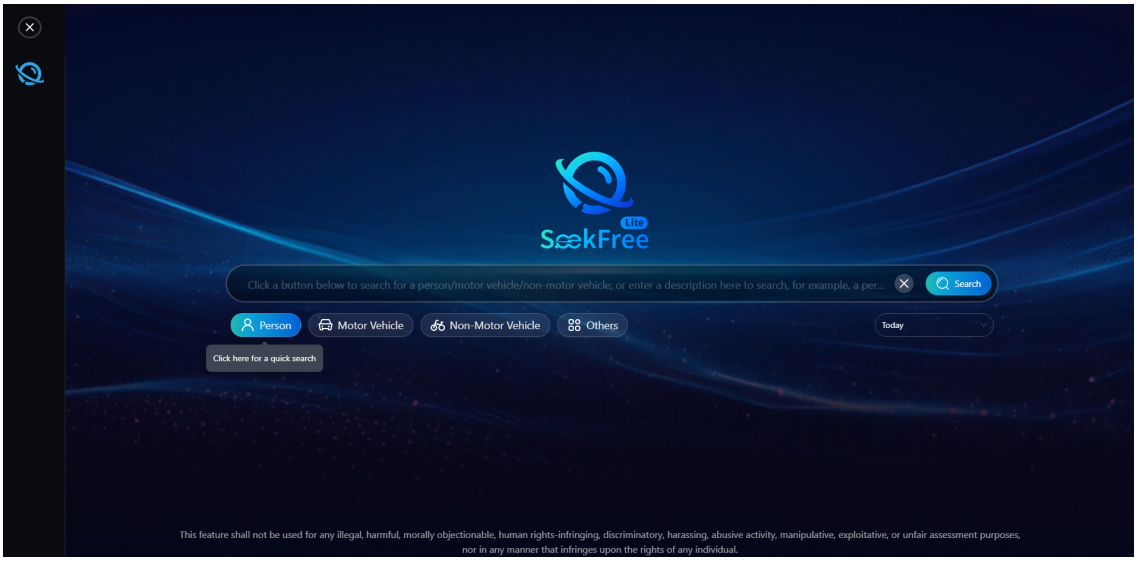


Figure 2-2: SeekFree Lite



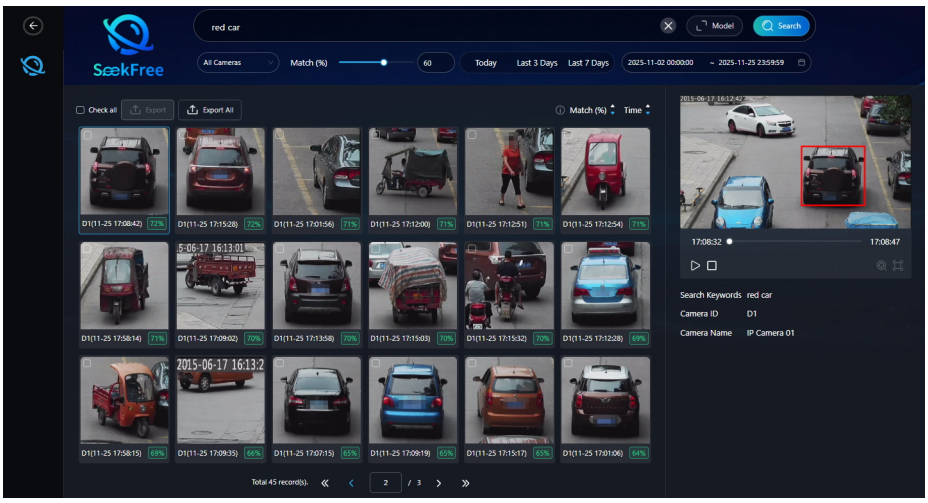
2. Configure the search criteria.

Parameter	Description
Keywords	Search for images by text. Enter the keywords to search for related results, such as black vehicle, person with an umbrella, etc. **Note:** This feature allows you to input keywords using a physical keyboard.
Icon	Click the corresponding icon based on the features of the search target to perform a search. Custom scenes and behaviors can be added.
Start/End Time	You can select 1 Day, 3 Days, or 7 Days, or click the drop-down list to set the start time and end time. Click the dropdown menu to select Today, Last 3 Days, Last 7 Days, or a custom time range for your search.

3. Click **Search** to view the results.

Note:

- All snapshots are displayed on the left, and the corresponding recording captured before and after the snapshot time is displayed on the right. The recording of the first search result is displayed by default. The top section allows further configuration of search channels, similarity threshold, and start/end time.
  - Camera ID：Select the camera(s) to search.
  - Match(%)：Select a similarity from the drop-down list to search for all content with a similarity score at or above that level. For example, if the similarity is set to 70%, the device will search for content with the similarity score ranging from 70% to 100%.
  - Start/End Time：You can select 1 Day, 3 Days, or 7 Days, or click the drop-down list to set the start time and end time.
- Click to play the recording in full screen.
- The search results can be sorted in ascending or descending order by similarity and time. You can click after similarity/time to switch the sorting mode.



4. Click **Export** or **Export All** to export search results to the specified path in the USB drive (local interface) or computer (web interface).

AcuSearch

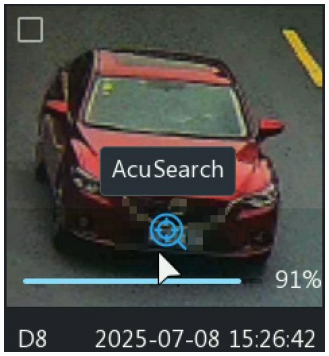
Select the target from the search results (snapshot or recording), and search for similar images.

Note: This function is only available for devices with an analyzer that supports AcuSearch. Before use, go to **Event** > **Smart Event** > **VCA Config** > **Analyzer Config**, and switch the analyzer mode to **AcuSearch/AcuTrack**.

1. Determine the search target.

- Target on the snapshot: Hover over the desired snapshot on the left and the AcuSearch icon appears. Click and the device will search for the target in the red box.

  Note: If there is no red box on the snapshot, click and the device will retrieve all supported targets in the image. Then select the desired target type and click to view the corresponding search results.



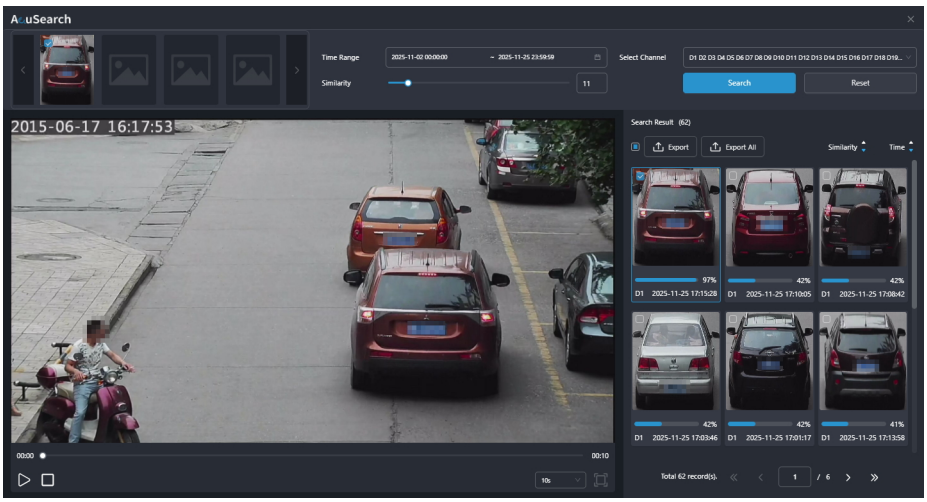
- Target on the recording: Select the target on the recording as needed.

  (1) Click at the bottom of the recording on the right.

  Note: This button is unavailable until the video playback is complete.

  (2) Click and drag to select the search target on the screen, and click **AcuSearch**.

2. View the search results.



Parameter	Description
Export / Export All	Click **Export** or **Export All** to export search results to the specified path in the USB drive (local interface) or computer (web interface)
Similarity Time	Search result sorting mode. The icons indicate that the results are sorted in ascending order by similarity and time. You can click to switch to descending order
/	Play/pause playback
	Stop playback
10s	The duration of the recording captured before and after the snapshot time. Available options: 10 seconds, 30 seconds, 5 minutes, and 15 minutes

3. Select the camera(s), set the start time, end time, and similarity, and then click **Search** to perform a secondary search for AcuSearch results.

3 Live View

3.1 Preview

The preview page consists of live view windows, channel status bar, window toolbar, bottom toolbar, smart preview, and people flow counting.

Channel Status Bar

The channel status bar appears in the top-right corner of a live view window under certain conditions.

Status	Description
	Audio is playing with live video
	Two-way audio is enabled
REC	Local recording is in progress
	An alarm has been triggered

Live View Window

Click anywhere in a live view window to display the live view window toolbar. The toolbar buttons are described in the Window Toolbar section below.

Double-click anywhere in a live view window to enter full screen; double-click again to exit.

Right-click anywhere in a live view window to display a shortcut menu for quick access to the corresponding functions.

Drag a live view window to another window to swap their images.

To control a PTZ camera in a live view window, hover over the window edge. When the cursor changes to an arrow icon, click and hold the mouse to adjust the view.

Note: This feature is available to the web interface only.

Hover over an idle window, click **+** to add a camera.

Note: The web interface does not support window swapping and quick camera adding.

Window Toolbar

Click anywhere in a live view window to display the window toolbar.

Toolbar Buttons	Description
	Two-way audio. When enabled, users at the NVR side can establish real-time audio communication with users at the camera side **Note:** Before use, audio input and output devices must be separately connected to the NVR and camera's AUDIO IN/OUT interfaces.
	PTZ. Click to enter full screen. Click the direction arrows to adjust the direction. Click to access **PTZ Advanced Settings** for more PTZ control operations: • : 3D Positioning. Drag to select an area on the image, and the camera will automatically rotate toward the selected area, zoom in and focus, and display the selected area clearly at an appropriate scale • : Shortcut operation. In full screen, hover over the window edge. When the cursor changes to an arrow icon, click and hold the mouse to adjust the view •  : Call a preset position. Select a preset position and call it For descriptions of other buttons, see PTZ Configuration. Click again to exit full screen
	Note: Before use, you need to switch the analyzer to **AcuSearch/AcuTrack**. For more details, see Analyzer Configuration. AcuSearch can search motor vehicle/non-motor vehicle/pedestrian targets based on the target image you selected on the live view or playback images. To use this function, click the button, select the target automatically/manually, and then click **OK**. By default, all images with a similarity of 60% or higher from all cameras on the current day will be retrieved. You can adjust the similarity threshold and search again
	Instant Playback: Play back the video recorded within the last 5 minutes (configured in Basic Configuration) from the current time

Toolbar Buttons	Description

	Click to show more buttons:
	• Snapshot: Manually capture the current image from the camera. You can view or export the snapshot, or enter the picture search page and select **Preview Snapshot** to view and export it
	• Digital Zoom: Zoom in on an area of the image. Move the mouse to the target position and then use one of the following methods to magnify the area:
	  • Method 1: Scroll the mouse wheel to zoom in or out
	  • Method 2: Click to zoom in according to the predefined zoom level
	  • Method 3: Drag to zoom in on the selected area
	  Right-click to exit digital zoom
	• Enable Digital Zoom: Available to the web interface only. Once enabled, you can perform digital zoom
	• Switch Stream: Switch the live stream. The available stream types depend on the camera's capability
	• Camera Info: Display the encoding format, frame rate, bitrate, and resolution details
	• Let Through: Used with vehicle management functions. When a plate mismatch alarm occurs and the camera cannot open the barrier gate automatically, you can open the barrier gate manually for the vehicle
	• Start Local Recording: Manually trigger to record video of the current channel and control the recording start time and duration. Manual recordings can be retrieved on the video search page by the **Manual** recording type and viewed in normal recording playback
	• Fisheye: Display the dewarped image
	  • Mount: Camera mount mode
	  • Display Mode: Divided into Original Image (uncorrected original image), Panoramic (corrected panoramic image), and PTZ (corrected partial image). Take Panoramic + 3PTZ as an example, the window with gray circle is the panoramic image, and the other three are PTZ images
	 
	  1. Select the mount mode and display mode, then click **Save**.
	  2. Select a PTZ window, drag in the window to view the corrected image at different positions; scroll the mouse wheel to zoom in/out on the corrected image. Alternatively, in the panoramic image window, drag the corresponding frame of a PTZ window to view the corrected image at different positions; scroll the mouse wheel in the frame to zoom in/out on the corrected image.

Bottom Toolbar

The bottom toolbar is displayed by default and can be hidden by clicking  .

Toolbar Button	Description
	Switch screen, allows you to choose the number of windows and window layout displayed on the preview page • Corridor mode: Changes the aspect ratio from standard 16:9 (landscape) to 9:16 (portrait) to adapt to corridor scenes **Note:** • To use corridor mode, be sure to physically rotate the camera 90° clockwise or counterclockwise during installation, then go to Video > **Image Enhancement** and set **Image Rotation** to **90° CCW** or **90° CW** accordingly • When corridor mode is enabled for a camera, it applies to all area-based operations for the camera (such as digital zoom and motion detection areas) • Wide mode: The live view window is wider, suitable for stitched live video images **Note:** Certain cameras can stitch images captured by two or more lenses into a single image to provide a wider field of view.
	Prev Screen/Next Screen: For example, the live view windows are divided into three groups, with group 2 currently displayed on the screen. Click the left or right arrow to switch to the previous or next group
	Unmute. Click to play audio in the current window. Audio can be played in only one window at a time
	IP Speaker. Used for two-way audio or audio broadcast. To stop two-way audio or broadcast, click the corresponding stop button; closing the pop-up window does not stop the two-way audio or broadcast •  : Two-way audio •  : Audio broadcast
	Multi-Sensor Preview: Display images of each multi-sensor camera in dedicated split-window views, one split-window per multi-sensor camera •  : PTZ. Adjust rotation direction • : Drag to zoom. Drag to select the area of interest on the panoramic channel's image (left/upper), and the PTZ channel will rotate to that area and zoom in •  : Manual tracking. First, configure detection rules. When the camera detects a motor vehicle/non-motor vehicle/pedestrian target, clicking the bounding box on the target will trigger the PTZ channel to track and zoom in on the target •  : Link. Click a point of interest on the panoramic channel's image (left/top), and the PTZ channel will rotate to that point and zoom in •  : Prev Screen/Next Screen. Click the arrow to switch to the previous or next multi-sensor camera's preview image •  : Full screen. Click to enter full screen. To exit full screen, click **Normal Mode** on the local interface or press **Esc** on the web interface •  : Exit. Click to exit multi-sensor preview
	Disarm/Arm. See Disarming Configuration for detailed information
	Full Screen. Click to enter full screen. To exit full screen, click **Normal Mode** on the local interface or press **Esc** on the web interface

Toolbar Button	Description
	Start Sequence. When live view windows are displayed across multiple screens, you can set a time interval to cycle through them. The sequence interval can be configured in Preview Configuration
	Normal Mode. Click to switch to smart preview mode

Smart Preview

Smart preview displays snapshots of motor vehicles, non-motor vehicles, faces, and human bodies captured in the three smart functions: face recognition, smart intrusion prevention (SIP), and vehicle recognition. Click on the bottom toolbar to switch to smart preview mode.

- Click to select the snapshot type to display.
- Click to select the snapshot type (alarm subscription) of smart functions to display, and set the snapshot attributes (attribute display configuration) to display.

Note:

Attribute configuration is only applicable to two alarm types: multi-target detection and road traffic (excluding motor vehicles).

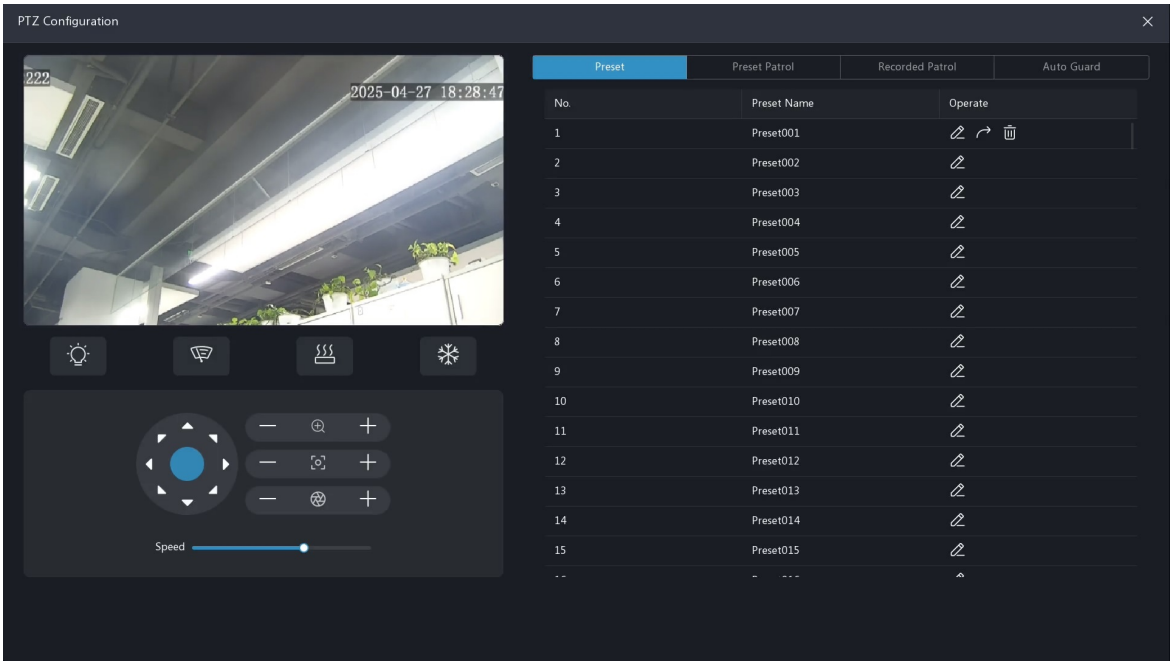
When multi-target detection is enabled, smart preview will only display the first two selected attributes in its real-time information when a face is detected within a person or non-motor vehicle.

People Flow Counting

This feature displays the real-time people flow statistics calculated by the people present alarm function. Click the drop-down list to select a scene to view the following data for that scene:

- People entered = Sum of people entered counted by all cameras
- People exited = Sum of people exited counted by all cameras
- People present = People entered - People exited
- People allowed = Critical people present alarm threshold - People present

3.2 PTZ Configuration



PTZ configuration includes PTZ control, preset position (or simply preset) configuration, preset patrol configuration, and auto guard configuration. Among these, PTZ control serves as the foundation for all other configurations. It is recommended to familiarize yourself with PTZ control before proceeding with other configurations.

After adding a PTZ camera, click 

on the live view toolbar of the preview page, click  > **PTZ Configuration** to enter the **PTZ Configuration** page.

PTZ Control

Button	Description
	Adjust the rotation direction
	• Zoom: Zoom in or out on the image **Note:** You may also use the mouse wheel to zoom in or out. • Focus: Focus the image • Iris: Adjust the image brightness
PTZ Speed	Adjust the rotation speed
	Turn on/off the light
	Turn on/off the wiper
	Turn on/off heating
	Turn on/off the snow removal

Preset

Preset the positions to monitor for quick recall.

1. Rotate the camera to the desired position.
2. Select a preset position number, click  to edit the preset position name, and then click **OK**.
   - Click  to call a preset position.
   - Click  to delete a preset position.

Preset Patrol

The PTZ camera patrols along a route made up of multiple preset presets.

1. Select a patrol route, and click **Add Keypoint**.

Parameter	Description
Preset	Select preset positions (see Preset)
Dwell Time (seconds)	The duration that the camera stays at a preset position
Patrol Speed	Rotation speed

2. Click **OK**, add keypoints, and click **OK** again to save the settings. Repeat the above steps to set multiple patrol routes.

   Note: Each camera can be configured with a maximum of 4 patrol routes, and each patrol route supports up to 8 preset positions.

   - Click **Start**/**Stop** to start or stop the patrol.
   - Click  to clear keypoints.

Route Patrol

The PTZ camera automatically rotates along the recorded route.

1. Click **Start Recording**, and operate pan/tilt/zoom to record the route.
2. Click **Stop Recording** to stop.
3. Click **Apply** to save the patrol route.

   Click **Start** or **Stop** to start or stop the route patrol.

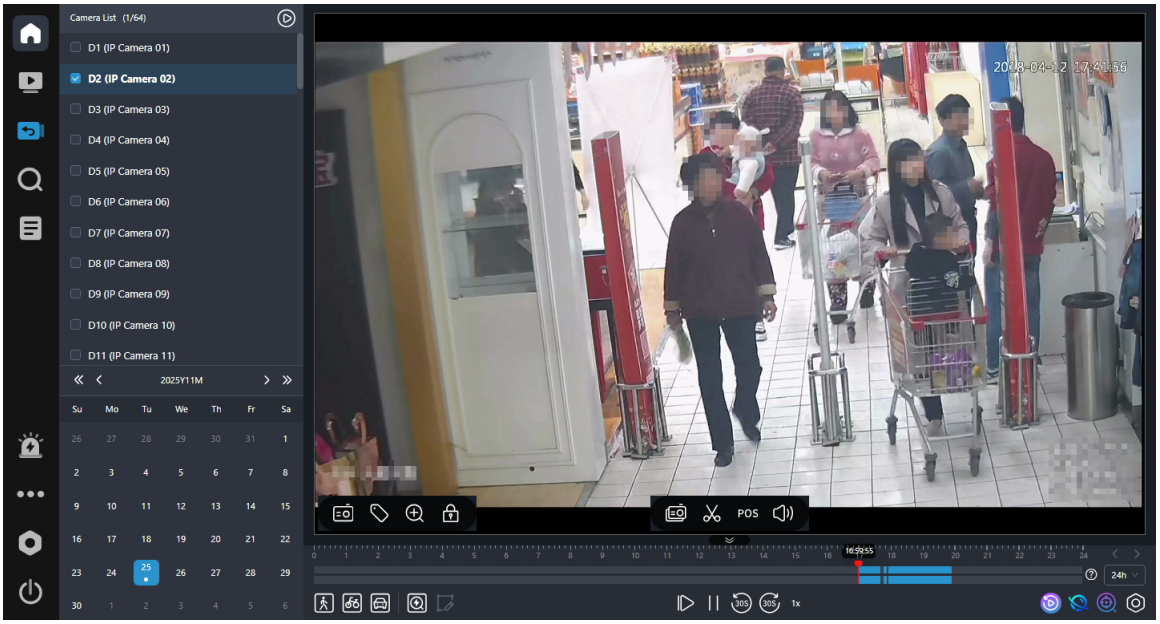
Auto Guard

If the PTZ camera is interrupted by other actions while executing a preset position, preset patrol, or route patrol, it will automatically resume the auto guard action (preset position or patrol route) after a waiting period.

Choose an auto guard mode (preset or patrol route), choose a preset or a patrol route (depending on the auto guard mode you have chosen), set the idle time, and then click **OK** to complete the setup.

4 Playback

The playback page consists of camera list, date selection area, playback window, window toolbar, and bottom toolbar. You can view camera recordings by date or event, and clip or export videos.



Camera List

Select the camera(s) to play recording(s) on the playback window(s). You can click to select the maximum number of cameras available for playback on all devices, or click to close the playback recordings of all current cameras.

Date Selection Area

The calendar uses different flags to indicate different recording types: blue for normal recording, red for event-triggered recording, and no flag for none.

Playback Window

Select the camera, and the playback window shows the recording. You can click in the right-upper corner of the window to close the recording. Click a window to display the window toolbar. See Window Toolbar for details.

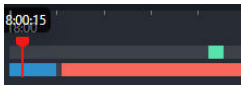
Window Toolbar

Click a window to display the window toolbar .

Icon	Description
	Take a snapshot • Local interface: The snapshots will be temporarily saved to , and will be deleted if you exit the playback page • Web interface: The snapshots will be saved to the local path
	Add a tag at the current time point to record the current video. You may search for recordings based on the tag keywords. See General Search for details

Icon	Description
	Zoom in. Move your mouse to the area you want to zoom in on, then use your scroll wheel to zoom in
	Lock the playback recording. Locking a recording file will prevent all the files stored in the same disk partition from being overwritten
	Click to enter the fisheye mode, and set the camera's mount mode and display mode for better playback effect **Note:** This button appears only for certain fisheye cameras.

Bottom toolbar

Icon	Description
	Playback timeline. Blue for normal recording, red for event-triggered recording, and green for smart recording
	Zoom in or out on the timeline. Alternatively, click on the timeline and use the scroll wheel to zoom in or out
	Normal mode: Show the progress bar including recordings of motor vehicle/ non-motor vehicle/pedestrian Smart mode: Show the progress bar including event recordings triggered by motor vehicle/non-motor vehicle/pedestrian Click to set the playback speed or enable/disable **Skip Normal Recordings** as needed
	Search for recordings of motion detection
	Forward by frame
	Play/pause
	Rewind/forward 30s, or click and choose from the **Interval** drop-down list
	Set the playback speed
	Normal mode/event mode
	SeekFree: Search for images by text, designed to help users quickly retrieve snapshots and recordings that meet search criteria Click the button, Go to **SeekFree**, See SeekFree for detailed configurations

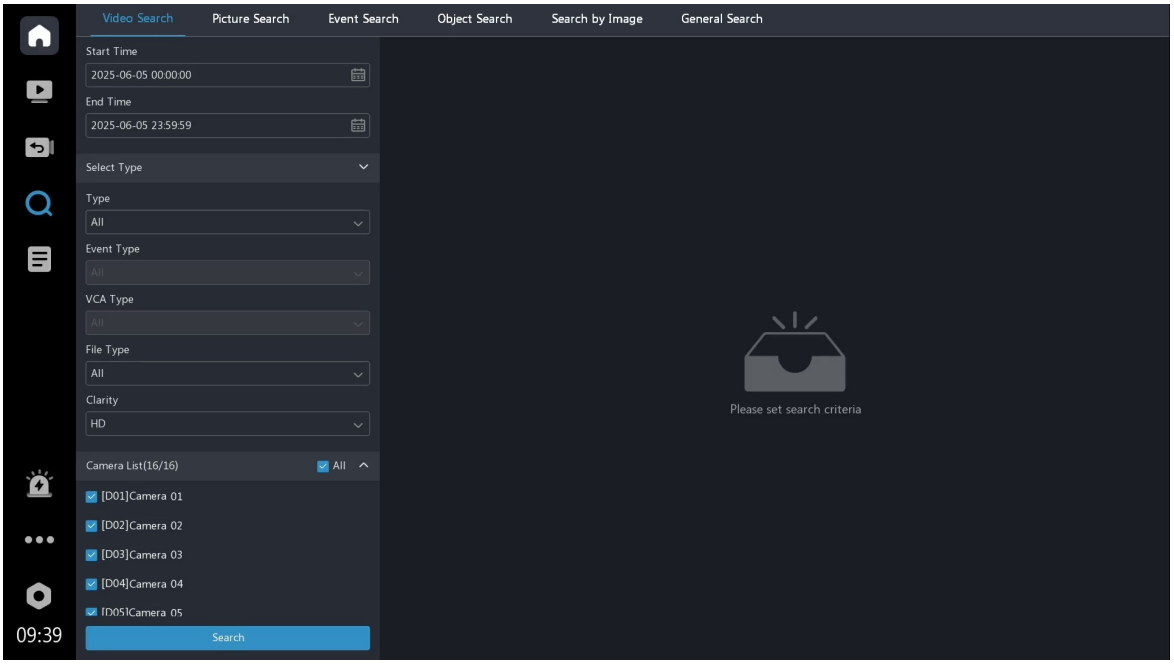
Icon	Description
	AcuSearch: Search for images of motor vehicles, non-motor vehicles, or pedestrians AcuTrack: Search for recordings of motor vehicles, non-motor vehicles, or pedestrians during a specified period of a day and display the search results on the timeline Click the button, drag to select the target, and choose **AcuSearch** or **AcuTrack** to view the accurate search results •  : Play the last or next recording •  : Back up the current recording to the storage device **Note:** • Before use, set the analyzer mode to **AcuSearch/AcuTrack**. See Analyzer Configuration for details • By default, the NVR searches for images/recordings of all cameras of the current day and with the similarity of 60%. You can reset the search conditions as needed, and the set similarity will be the default value the next time you perform the accurate search or tracking
	Click  to set the video clarity **Note:** • The clarity of playback is determined by video storage mode. The system plays HD recordings by default. To view SD recordings, ensure that the storage mode includes two streams. Otherwise, no images are displayed on the preview page after the clarity is changed to SD. See Stream Storage Mode for detailed configurations • If SD video is available in SD playback mode, SD video is played by default; it switches to HD video automatically when you double-click the window to maximize it in a multi-window layout
	Take a snapshot • Local interface: The snapshots will be temporarily saved to  , and will be deleted if you exit the playback page • Web interface: The snapshots will be saved to the local path
	Extract video clips from a specific time range. The video clips will be temporarily saved to  , and will be deleted if you exit the playback page
	Enable/disable POS. When enabled, POS OSD appears on the playback image **Note:** This function is available for certain NVRs.
	Turn on/off audio. You may drag the slider  to adjust the volume
	Full screen. Right-click to exit full screen
	File manager • Local interface: The playback snapshots, locked recordings, and video clips can be saved to an external storage device • Web interface: The video clips can be saved to the designated path

Playback Type

Type	Description	Steps
Normal Playback	• Play all recordings of the selected camera(s) • Play recordings triggered by motion detection in the specific area • Play recordings including motor vehicle/non-motor vehicle/pedestrian in the specific area	1. Select camera(s) and click the desired date to start playback. 2. (Optional) Click to play the event recordings triggered by motion detection. Click to specify the target type(s), and then the corresponding recordings including pedestrian, non-motor vehicle, or motor vehicle will be displayed. To view the recording in the specific area (smart search), follow the steps below (1) Click , and click to clear the existing areas. (2) Press and drag to redraw the area. (3) (Optional) Set the sensitivity to view the recordings under this sensitivity. To adjust the sensitivity, you may drag the slider Sensitivity on the local interface, or click and drag the slider on the web interface. (4) Click to play the recording of this area. • Local interface: Click to exit the current operation • Web interface: Click to exit the current operation
Event Playback	Play recordings triggered by the specific event	1. Click , click **Switch to Event Mode**, and select the camera(s). Click the desired date, and click All Events to choose an event type. 2. (Optional) Some events (for example, UMD) allow to view the event recordings triggered by pedestrian, non-motor vehicle, or motor vehicle. You can click to select one or more target type(s) to play the corresponding recordings.
Corridor Playback	Play recordings in corridor mode in multiple windows **Note:** This function is only available on the local interface.	Select the cameras (up to 3), click the desired date, and click

5 Search

5.1 Video Search

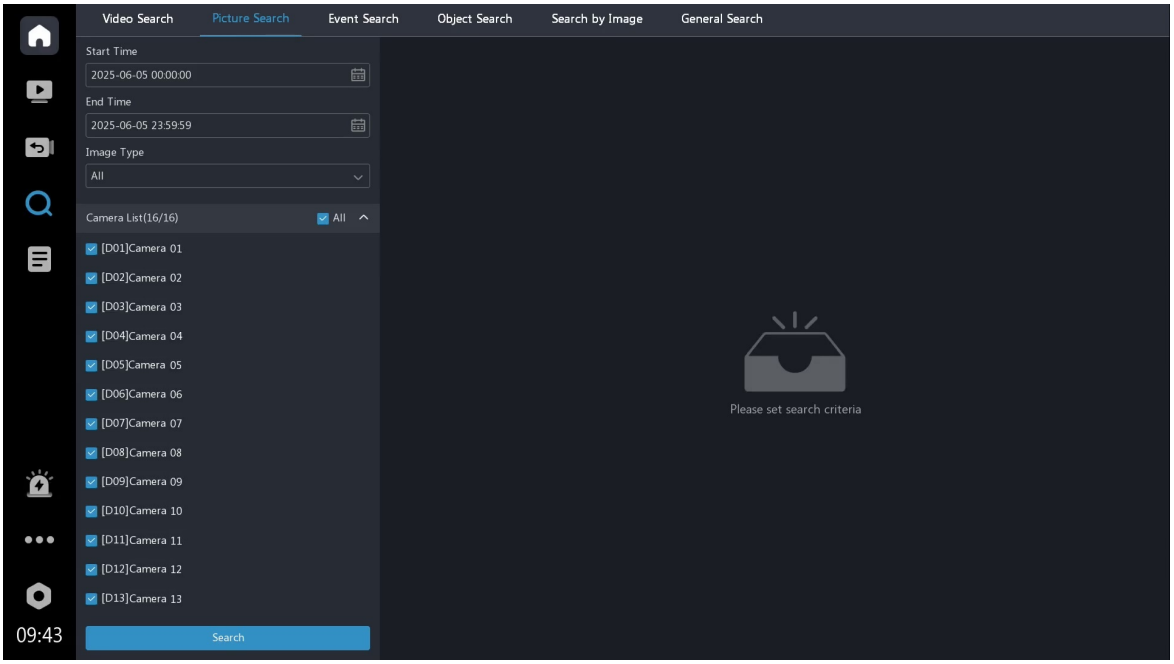


Configure the search criteria and click **Search** to view the results.

Search Type	Description
Recording Type	• Normal: Video recorded by the normal snapshot in Recording Schedule • Manual: Video recorded manually in Preview • Event: Partitioned video triggered by the target events
File Type	• Lock: The locked video segment will not be overwritten • Unlock: Unlock the file The recording can be locked/unlocked in Playback
Clarity	The supported clarity (HD or SD) varies with the storage method. See Stream Storage Mode for details

- Export/Export All: Export the selected recording(s) or all recordings to the specified path in the USB drive (local interface) or computer (web interface).
- Merge and Download: Merge multiple consecutive recordings from the same camera into one file for download (web interface only).

5.2 Picture Search

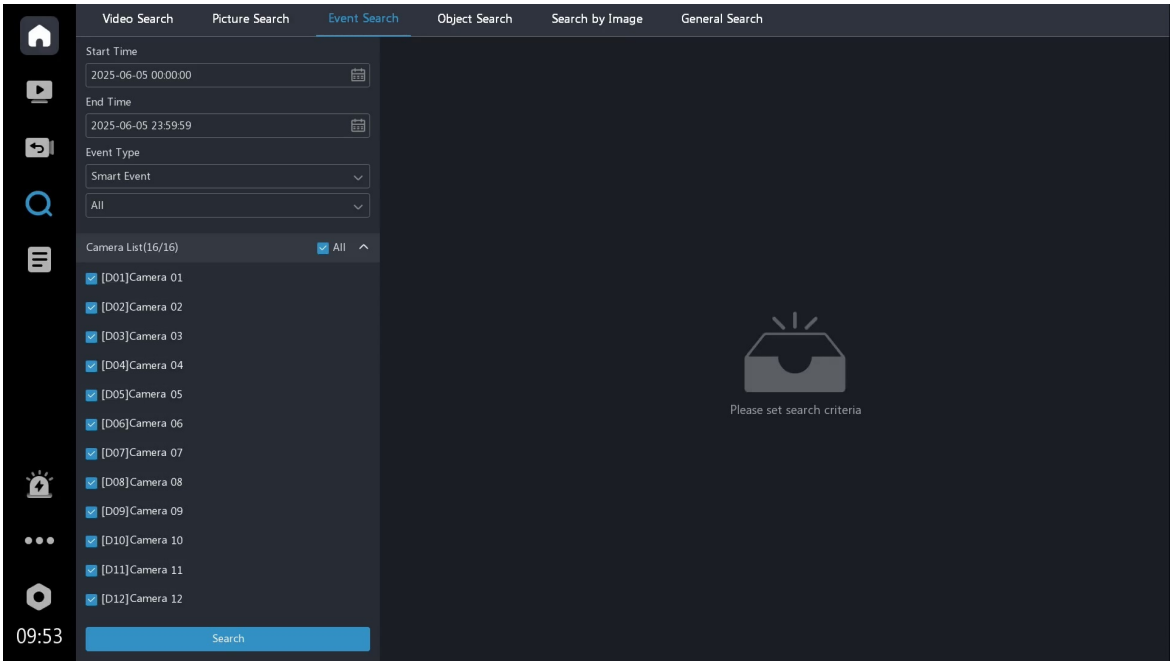


Configure the search criteria and click **Search** to view the results.

Picture Type	Description
Scheduled Snapshot	Show pictures captured by the normal snapshot in Snapshot Schedule
Preview Snapshot	Show pictures captured in Preview
Manual Snapshot	Show pictures captured in Manual Operations
Playback Snapshot	Show pictures captured in Playback
Event Type	Search for pictures captured by common and smart events

Export/Export All: Export the selected recording(s) or all recordings to the specified path in the USB drive (local interface) or computer (web interface).

5.3 Event Search



Configure the search criteria and click **Search** to view the results.

Smart Events

Search for recordings triggered by Smart Event, and show the results in tile mode with the trigger target as the cover image.

Export/Export All: Export the selected recording(s) or all recordings to the specified path in the USB drive (local interface) or computer (web interface).

- Local Interface: Select **Export as Image** or **Export as Video** as needed.
- Web Interface: Select **Export as Excel**, **Export as Image**, or **Export as Video** as needed.

Common Events

Search for recordings triggered by Common Event and show the results in list mode.

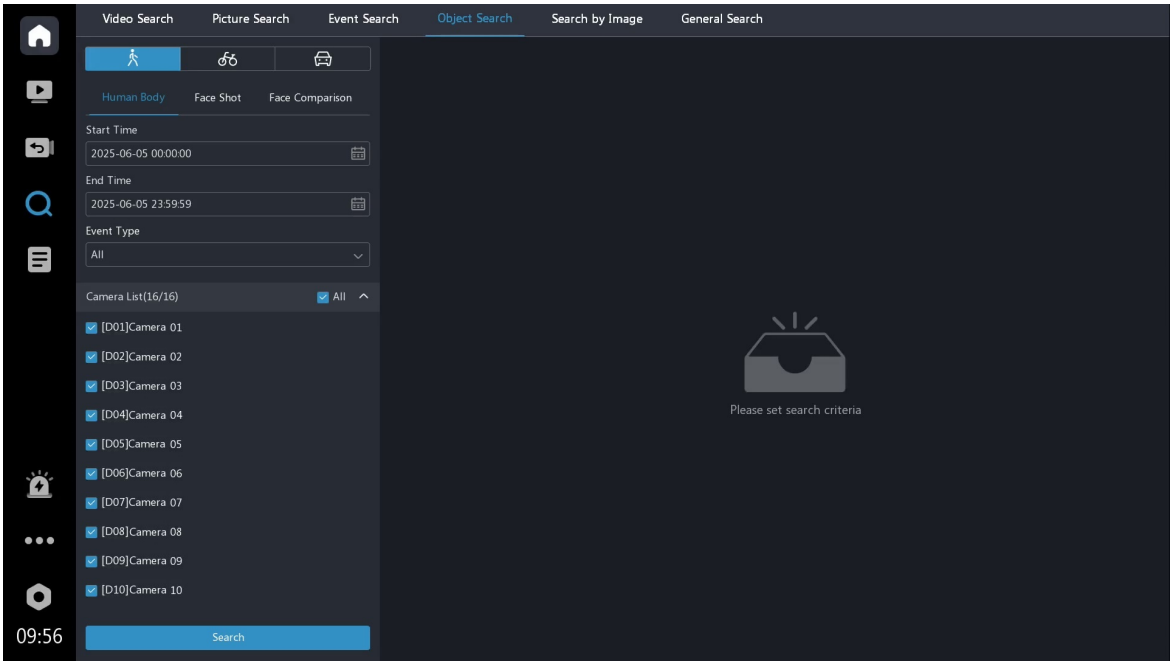
Export/Export All: Export the selected recording(s) or all recordings to the specified path in the USB drive (local interface) or computer (web interface).

5.4 Target Search

5.4.1 Person

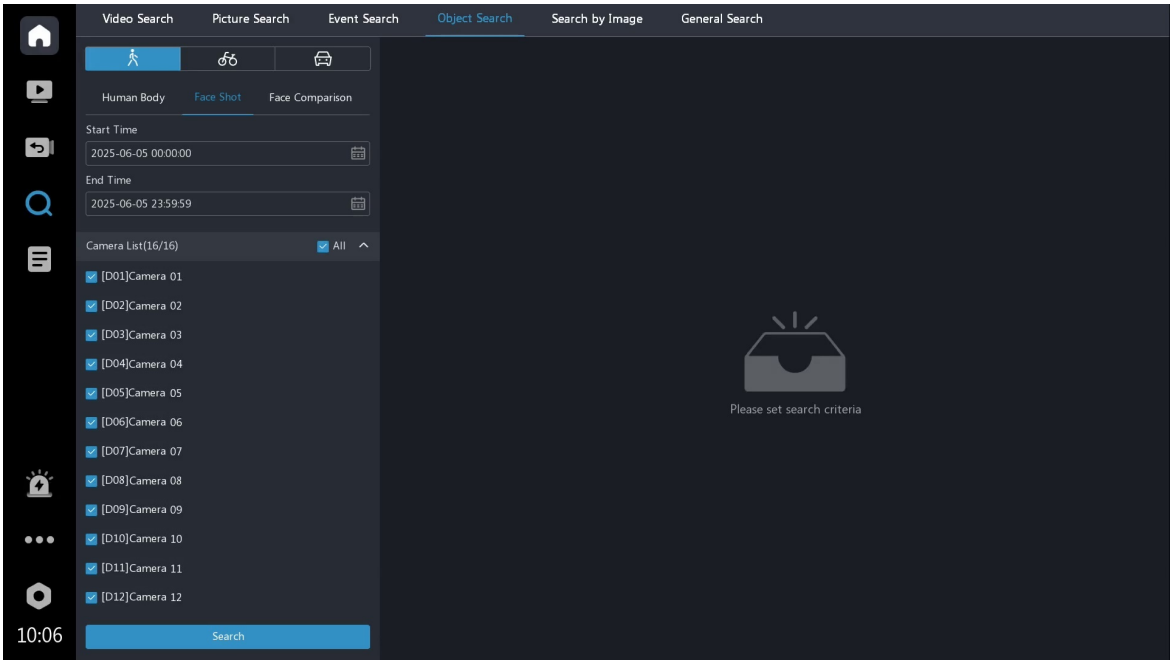
Configure the search criteria and click **Search** to view the results. You can click  in the top-right corner of the result list for further research.

Human Body Search



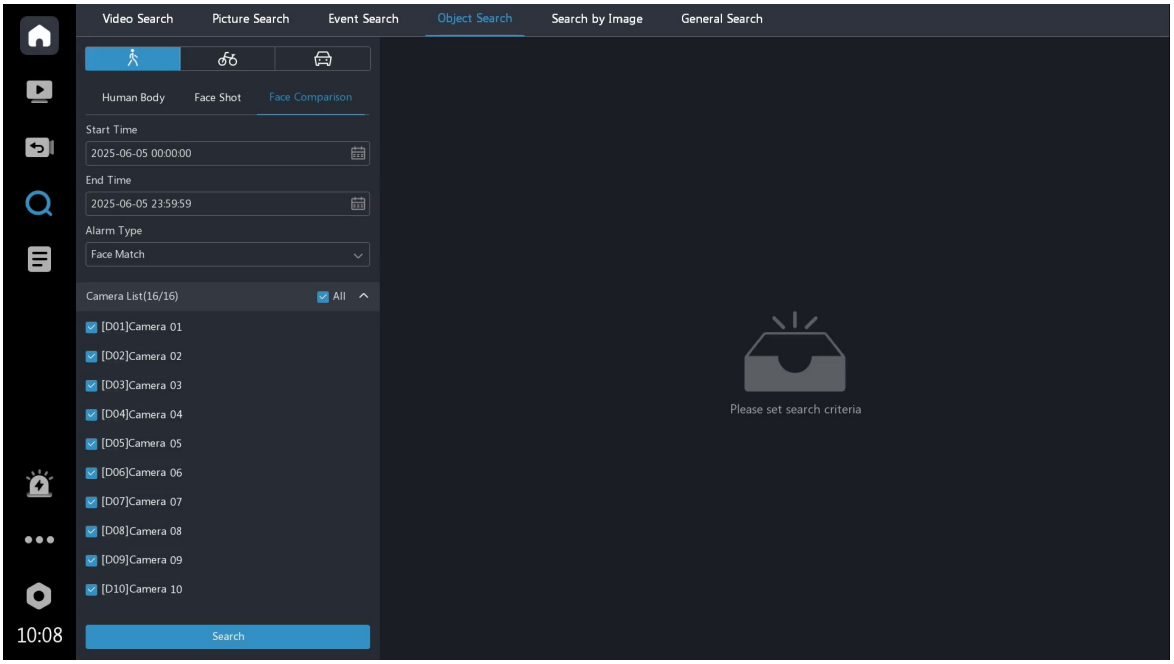
Function	Description
Export/Export All	Export/Export All: Export the selected file(s) or all files to the specified path in the USB drive (local interface) or computer (web interface) • Local Interface: Select **Export as Image** or **Export as Video** as needed • Web Interface: Select **Export as Excel**, **Export as Image**, or **Export as Video** as needed
All Attributes	View the attribute image **Note:** Only multi-target detection supports this feature.

Face Snapshot Search



Function	Description
Export/Export All	Export/Export All: Export the selected file(s) or all files to the specified path in the USB drive (local interface) or computer (web interface) • Local Interface: Select **Export as Image** or **Export as Video** as needed • Web Interface: Select **Export Excel**, **Export as Image**, or **Export as Video** as needed
Add to Face Library	Click ⊞ and complete the face information to add the face to the face library
Search by Image	Click **Search by Image** to redirect to Search by Image and perform a search using the selected image

Face Comparison Search

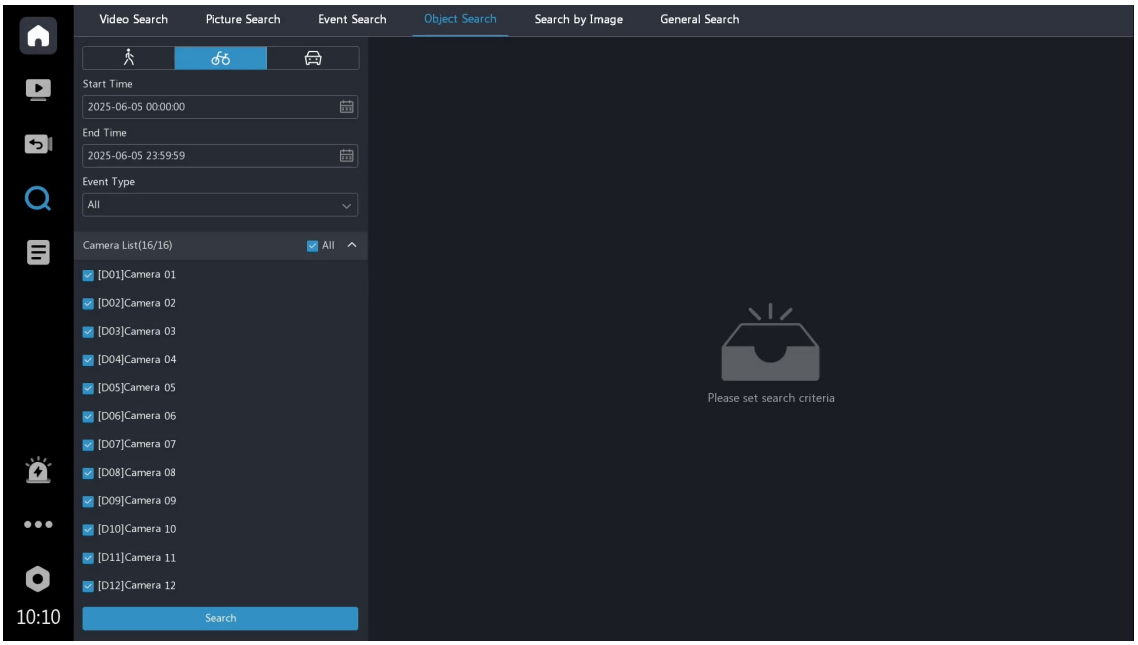


Function	Description
Export/Export All	Export/Export All: Export the selected file(s) or all files to the specified path in the USB drive (local interface) or computer (web interface) • Local Interface: Select **Export Results**, **Export as Image**, or **Export as Video** as needed **Note:** When **Export Results** is selected, other file type options cannot be selected. • Web Interface: Select **Export as Excel**, **Export as Image**, or **Export as Video** as needed
Add to Face Library	Hover over the face image on the left, click +, and complete the face information to add the face to the desired face library
Person Details	Hover over the face image on the right to view the matching results from the face library

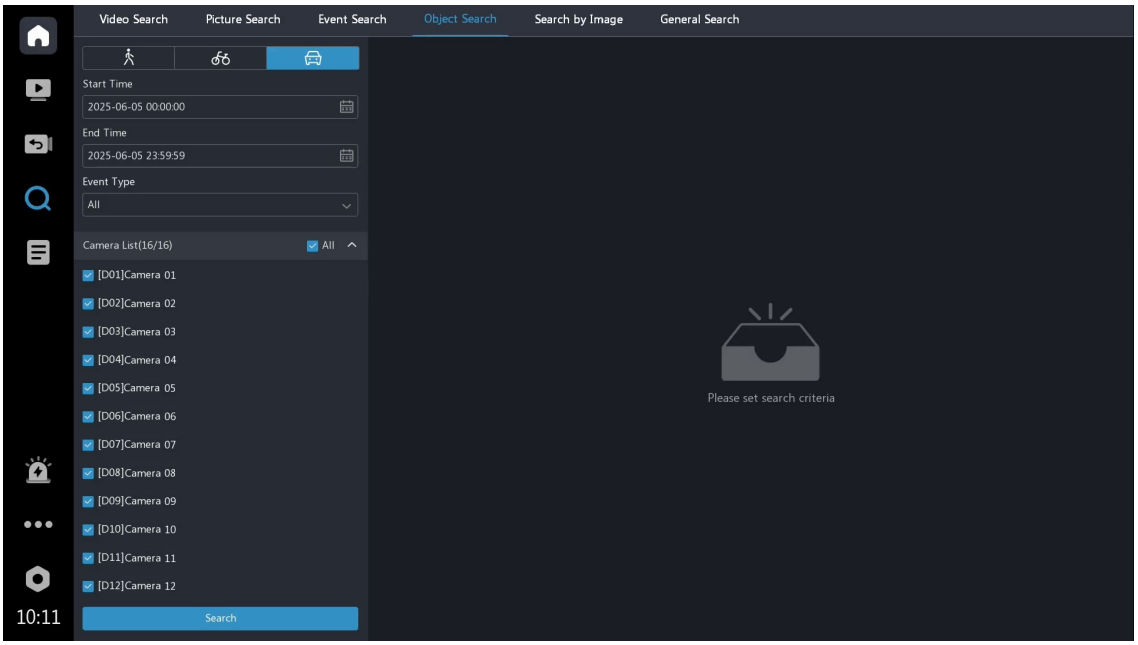
5.4.2 Motor Vehicle/Non-Motor Vehicle

Configure the search criteria and click **Search** to view the results. You can click in the top-right corner of the result list for further research.

- Non-Motor Vehicle



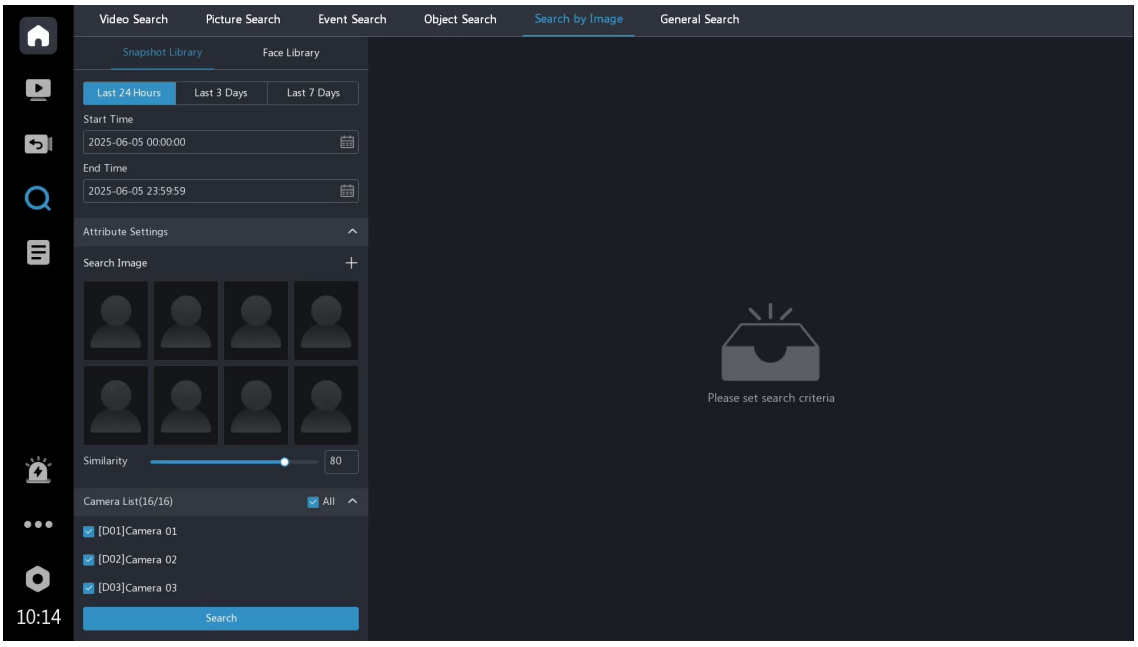
- Motor Vehicle



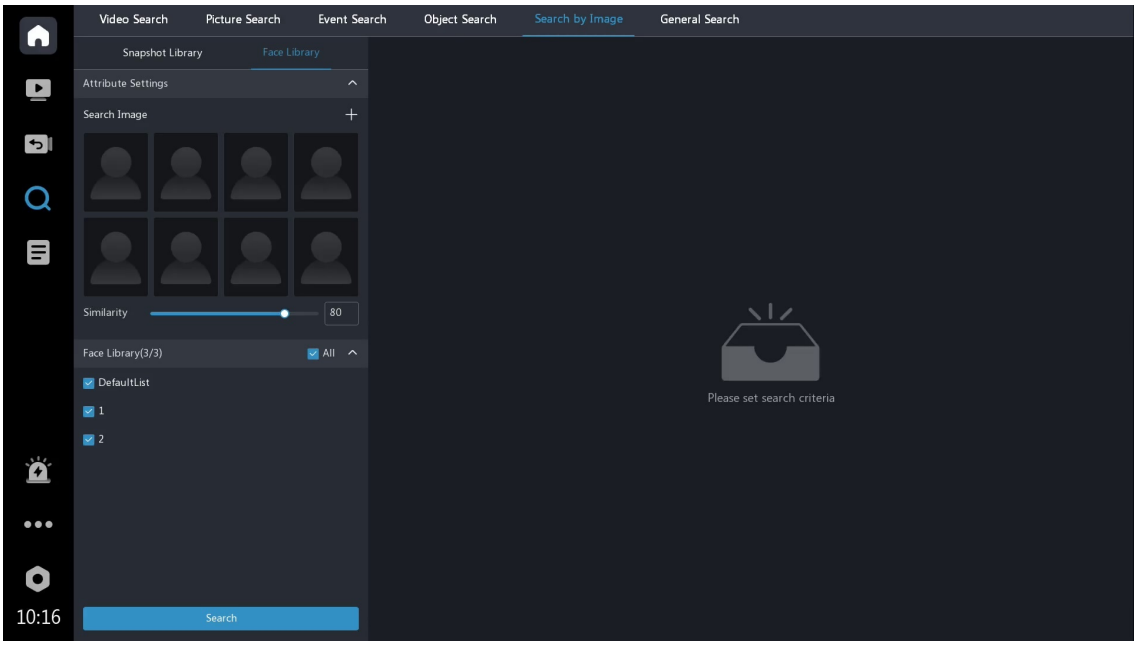
Function	Description
Export/Export All	Export/Export All: Export the selected file(s) or all files to the specified path in the USB drive (local interface) or computer (web interface) • Local Interface: Select **Export as Image** or **Export as Video** as needed • Web Interface: Select **Export as Excel**, **Export as Image**, or **Export as Video** as needed
All Attributes	View the attribute image **Note:** Only multi-target detection supports this feature.

5.5 Search by Image

- Snapshot Library: Select a snapshot from the camera as the comparison target.



- Face Library: Select an image from the face library as the comparison target.



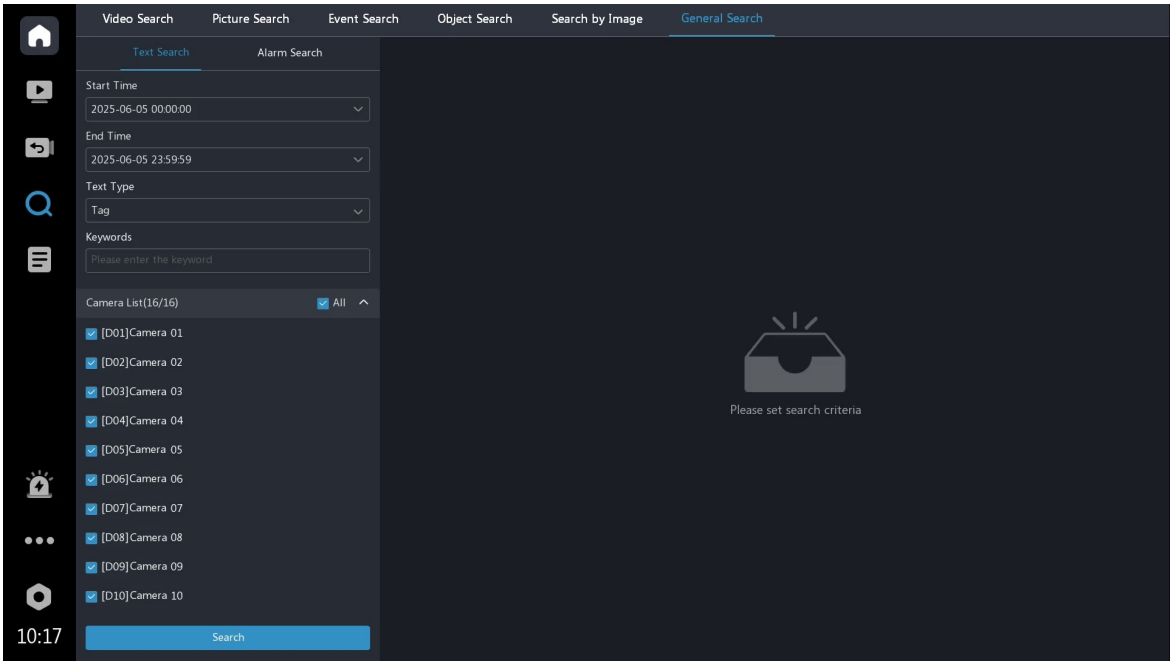
1. Click ⊕ to upload an image from the face library or local device.
2. Configure the search criteria and click **Search** to view the results.

Function	Description
Ascending/Descending	Click ⇅ to switch the display order
Export/Export All	Export the selected file(s) or all files to the specified path in the computer (web interface)

5.6 General Search

Configure the search criteria and click **Search** to view the results.

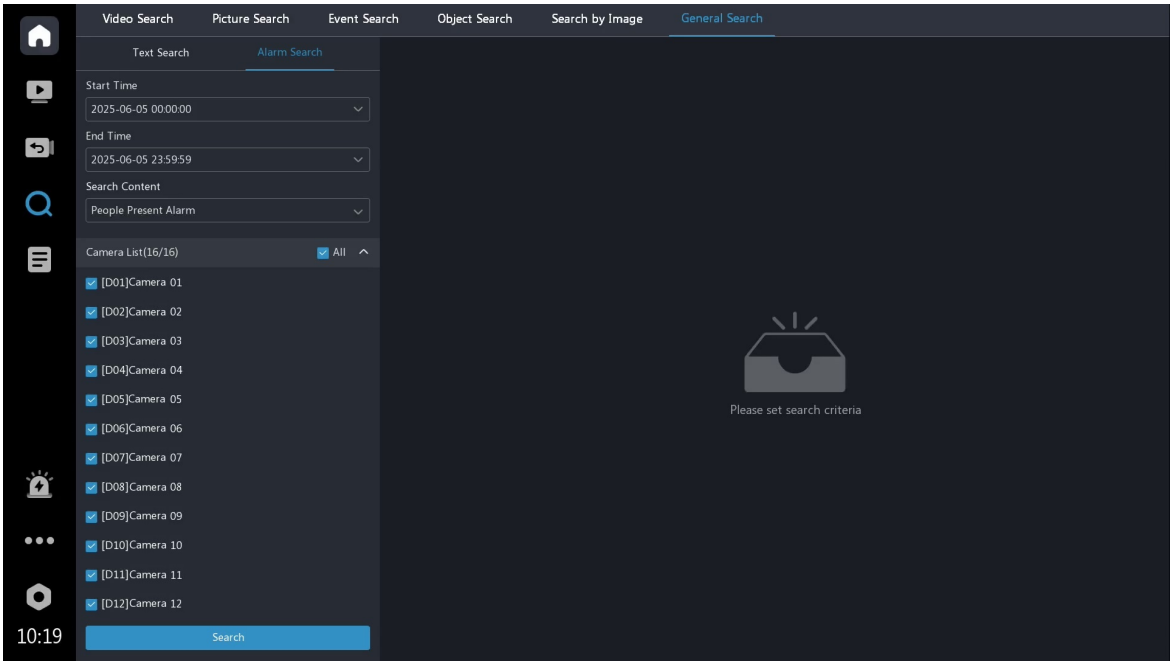
Text Search



- Tag Search: Search for recordings marked on tag information based on the tag keywords. See Playback for how to add a tag.
- POS Search: Search for recordings overlaid with POS information based on the POS keywords. See POS Configuration for details.

Function	Description
(Tag Search)	Edit the recording tag name
(Tag Search)	Delete the tag-marked recording
Export/Export All	Export/Export All: Export the selected recording(s) or all recordings to the specified path in the computer (web interface)

Alarm Search



- Alarm Input: Search for recordings triggered by Alarm Input.
- People Present Alarm: Search for recordings triggered by People Present Alarm.

Export/Export All: Export the selected recording(s) or all recordings to the specified path in the computer (web interface).

6 Event

The NVR supports multiple event detection and alarm, including common events and smart events. Please configure the event as needed.

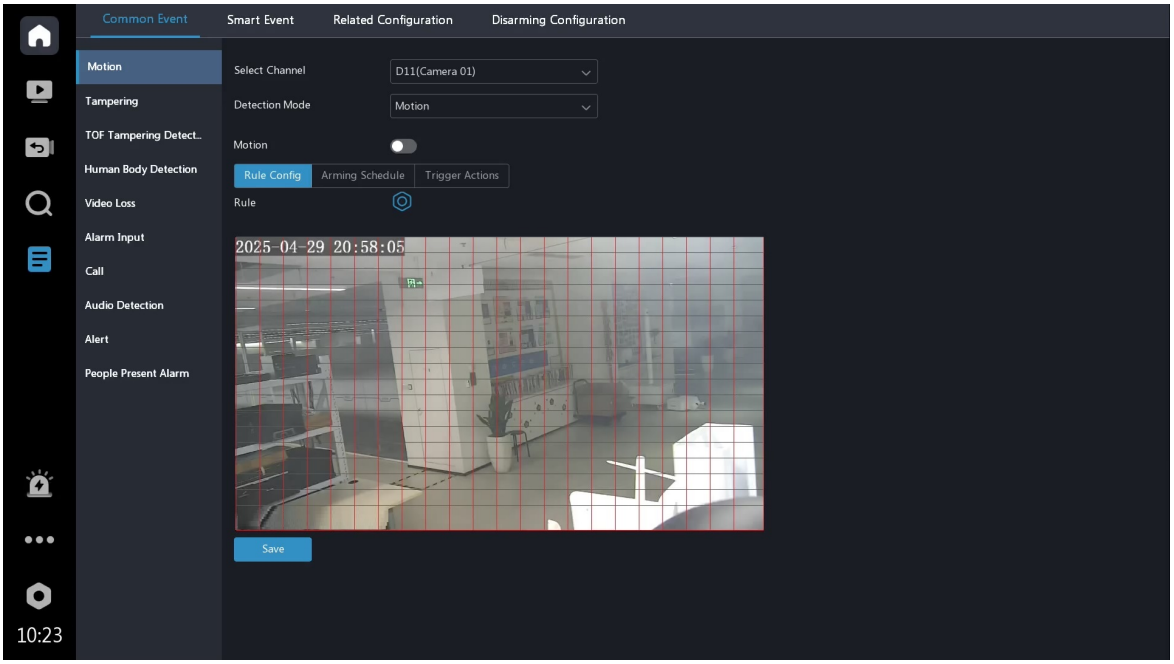
Note: After completing the settings for one camera, you can apply the same settings to other cameras by clicking **Copy To** (the button name may vary depending on the function) and selecting the desired parameters and camera(s).

6.1 Common Event

6.1.1 Motion Detection

6.1.1.1 Motion Detection

An alarm is triggered if the moving target is detected in the detection area. The detection results can be viewed on the playback, video search, picture search, event search, target search, camera alarm, and log pages. See Appendix for details on various search methods.



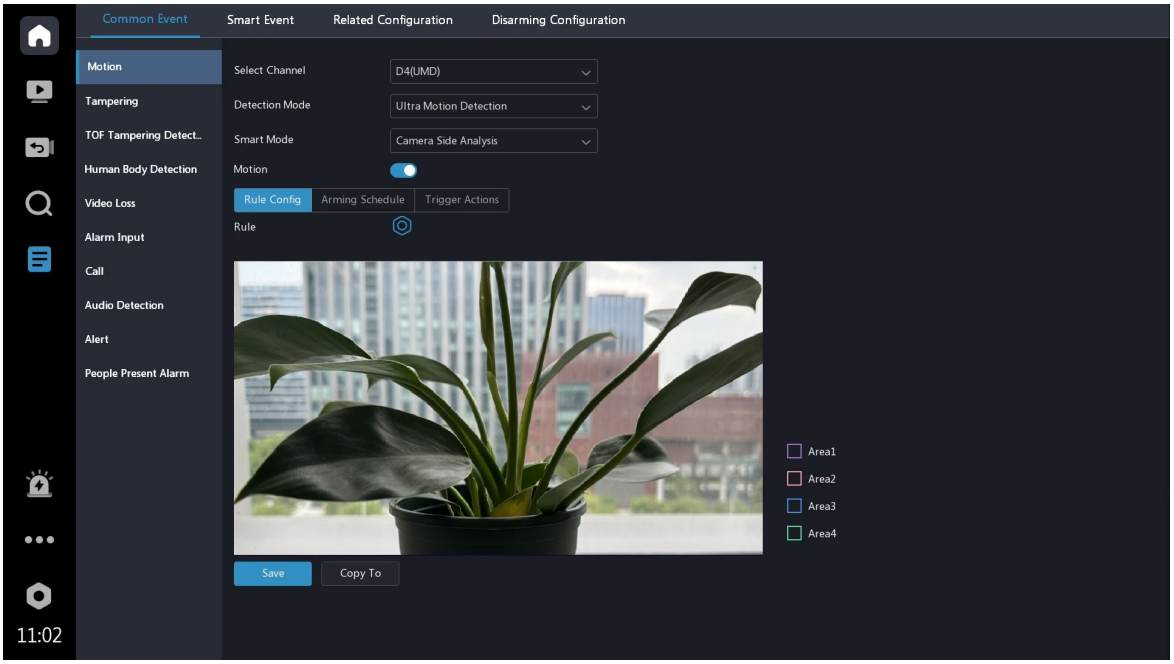
1. Select a channel, and click  to enable **Motion**.
2. Configure the detection rule (full screen detection by default).

Parameter	Description
Draw Area	• : Click the icon, click on the image and drag to clear or draw the detection area • : Detects all areas on the live video • : Click to delete the detection area
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.1.1.2 Ultra Motion Detection

The NVR takes snapshots and reports an alarm when motor vehicles, non-motor vehicles, or pedestrians are detected in the detection area. The detection results can be viewed on the playback, video search, picture search, event search, target search, camera alarm, and log pages. See Appendix for details.



1. Select a channel and smart mode, and click to enable **Motion**.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. (Optional) Select **NVR Side Analysis**, and set the minimum alarm interval (minimum time interval between two consecutive alarms). The algorithm used differs depending on the device model. The following takes a minimum alarm interval of 2 seconds as an example.

   - Algorithm 1: It limits the alarm reporting for the same target. If the same target continuously triggers alarms, the alarm will be reported at an interval of 2 seconds.
   - Algorithm 2: It limits the alarm reporting for all targets. If multiple targets trigger alarms simultaneously within 2 seconds, only the alarm triggered by the first target can be reported and the reset alarms will be discarded. The next alarm will be reported if a new target triggers an alarm after 2 seconds.

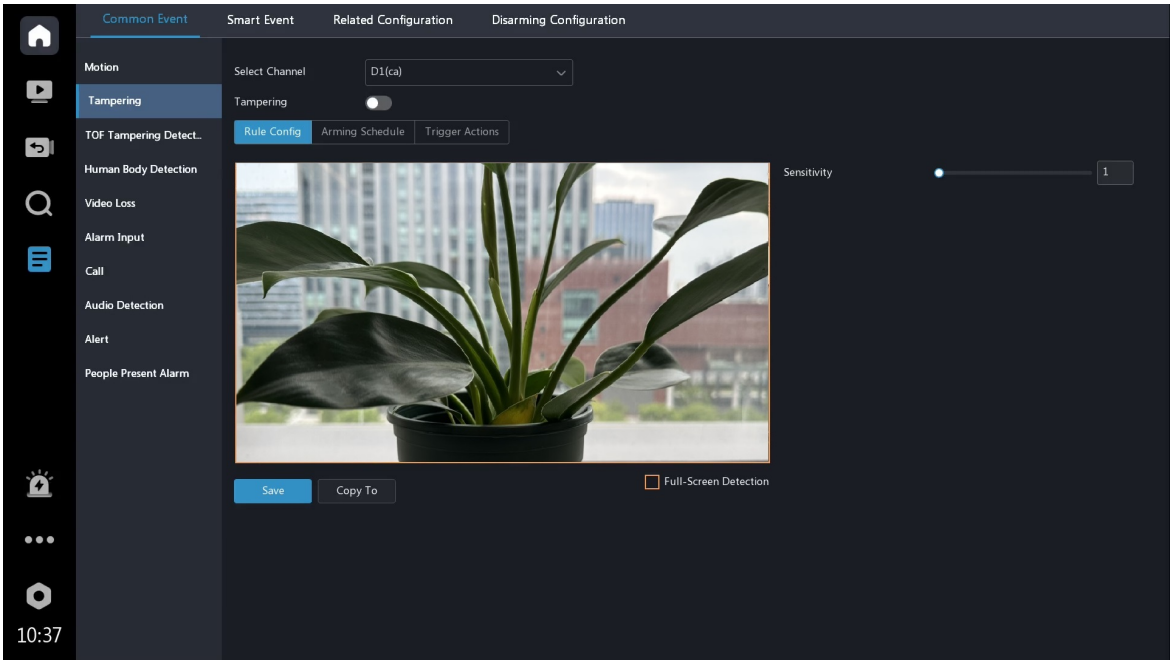
3. Configure detection rules. The 4 detection rules shall be set separately.

Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed shape. • Click to delete the detection area
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene
Snapshot Target	Select the target(s) as needed

4. Set Arming Schedule and Trigger Actions, and click **Save**.

6.1.2 Tampering Detection

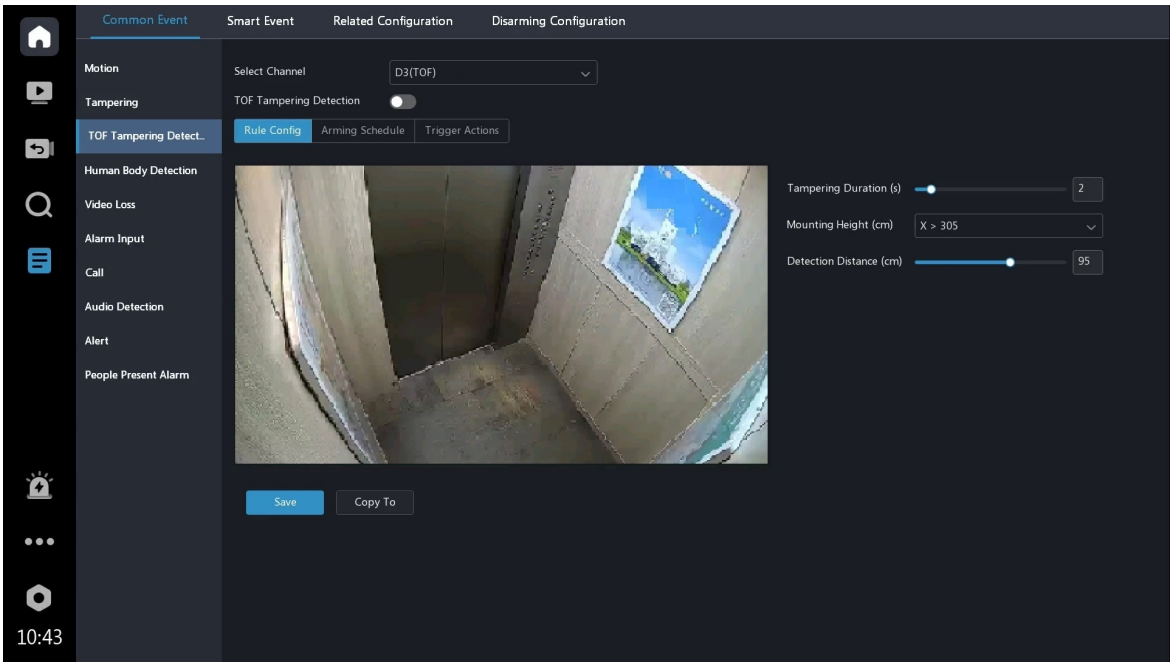
An alarm is triggered if the live video is tampered in the detection area. The camera is blocked when a target passes or stays on the live video that causing the video brightness to decrease significantly. The detection results can be viewed on the camera alarm and log pages. See Appendix for details on various search methods.



1. Select a channel, and click to enable **Tampering Detection**.
2. Set the sensitivity. The higher the sensitivity, the more likely a target will be detected, but the false alarm rate will increase. Set based on the scene and your actual needs.
3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.1.3 TOF Tampering Detection

TOF tampering detection employs a TOF sensor to detect tampering behaviors and trigger alarms, solving the issue of elevator entrance detection failure due to malicious tempering. An alarm will be triggered when the tampering duration and distance reach the set threshold. The detection results can be viewed on the camera alarm and log pages. See Appendix for details on various search methods.



1. Select a channel and smart mode, and click to enable **TOF Tampering Detection**.
2. Set other parameters as needed.

Parameter	Description
Tampering Duration (s)	An alarm is triggered when the tampering duration reaches the set value
Mounting Height (cm)	Set the camera mounting height according to the actual height of the elevator

Parameter	Description
Detection Distance (cm)	An alarm will be triggered when the obstruction target is within the detection distance from the sensor. A recommended value distance will be provided after selecting the mounting height, or you can enter a custom value

3. Set Arming Schedule and Trigger Actions, and click **Save**.

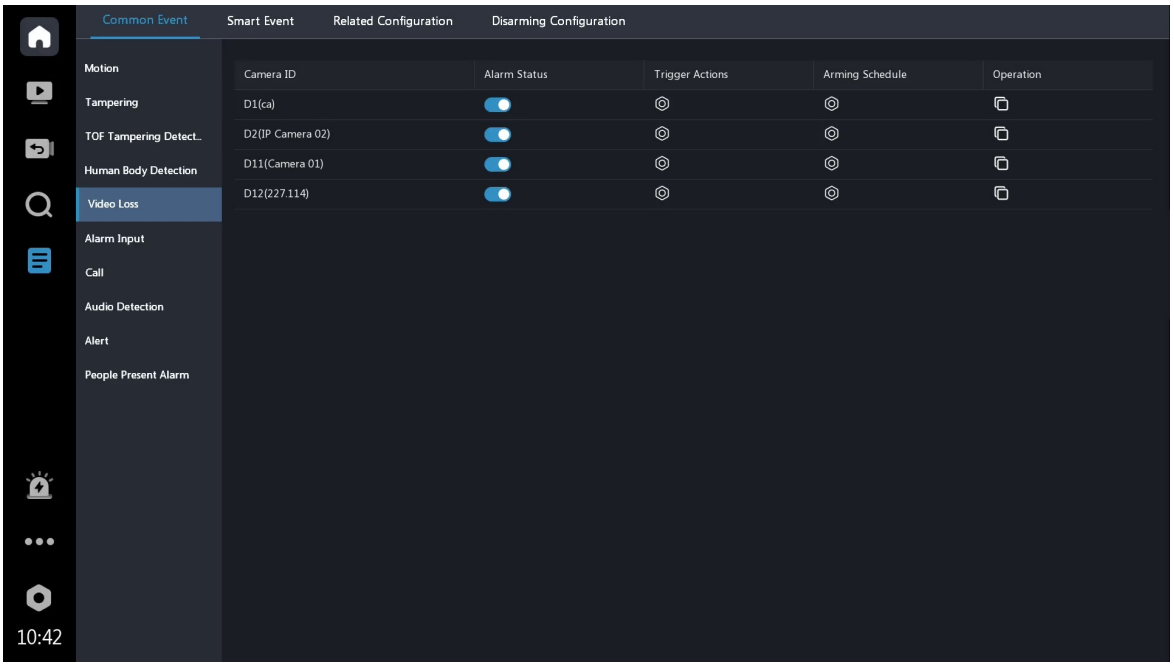
6.1.4 Human Body Detection

An alarm is triggered if the human body is detected in the detection area. The detection results can be viewed on the playback, video search, picture search, event search, camera alarm, and log pages. Please see Appendix for various search methods details.

1. Select a channel, and click  to enable **Human Body Detection**.
2. Draw the detection area. Click on the image and drag to draw 3 to 6 lines to form an enclosed shape.
3. Set the sensitivity. The higher the sensitivity, the more likely a target will be detected, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene.
4. Set Arming Schedule and Trigger Actions, and click **Save**.

6.1.5 Video Loss

An alarm is reported when the NVR loses video signals from a camera. The detection results can be viewed on the video search, picture search, event search, camera alarm, and log pages. Please see Appendix for various search methods details.

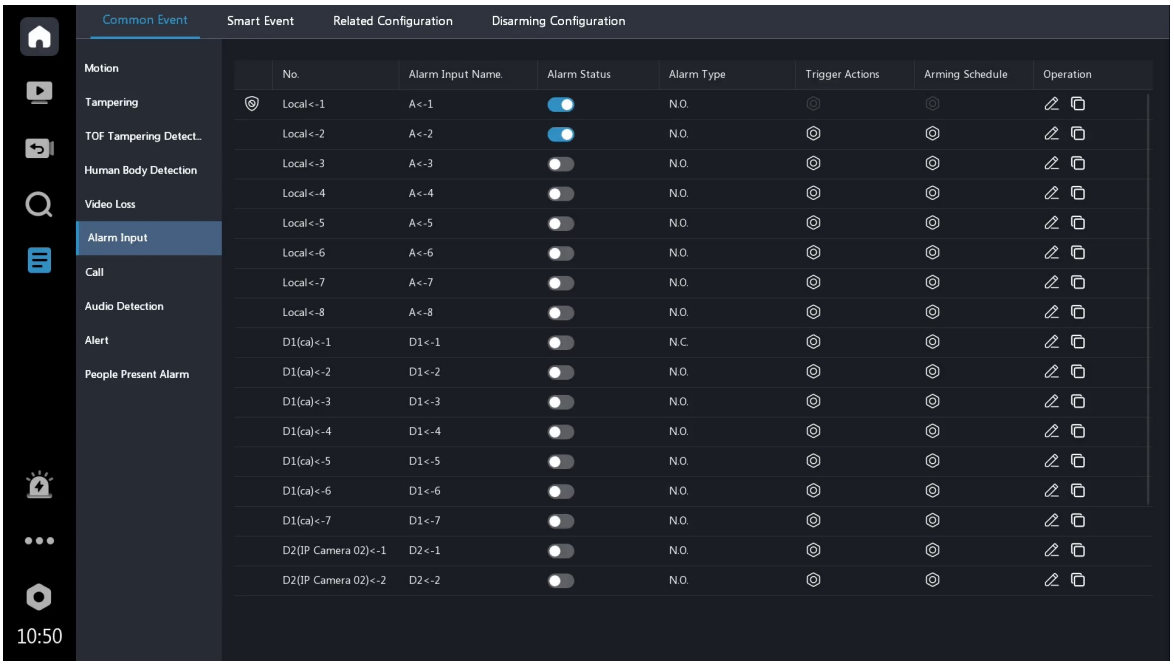


1. Video loss alarms are enabled for all channels by default. You can control the alarm status for each channel as required.
2. Set Arming Schedule and Trigger Actions, and click **Save**.

Note: Trigger actions including recording, preview, and snapshot are unavailable to this function.

6.1.6 Alarm Input

An alarm is triggered when a signal from an external alarm input device is detected. The detection results can be viewed on the video search, picture search, alarm search, camera alarm, and log pages. Please see Appendix for various search methods details.



The external alarm input devices include devices connected to the alarm input interfaces on the NVR, cameras, and alarm expansion devices.

- External alarm device connected to the alarm input interface on the NVR: Local < -1 means the first ALARM IN interface on the NVR, Local <-2 means the second ALARM IN interface on the NVR, and so on.
- External alarm device connected to the alarm input interface on the camera: D1 means the camera that added to the channel 1. D1< -1 means the first ALARM IN interface of the camera whose channel ID is 1. Likewise, D1< -2 means the second ALARM IN interface of the camera of the camera whose channel ID is 1.
- External alarm device connected to the alarm input interface on the alarm expansion device: M1 means the first alarm expansion device. M1<-1 means the first ALARM IN interface of this alarm expansion device. Likewise, M1<-1 means the second ALARM IN interface of this alarm expansion device.

Note: The alarm input channel is not displayed if the NVR or camera has no ALARM IN interface.

1. Enable **Alarm Status**, and click to configure the parameters.

Parameter	Description
(Optional) Disarm by Switch	This function is only available to Local<-1. When enabled, the disarming mode will switch to **Disarm by Switch** if Local < -1 receives the alarm input signal
Alarm Input Name	Set as needed
Alarm Type	The default is **N.O.**. Select the status as needed • N.O.: Choose this option if the alarm input device is normally closed. The device opens the circuit to input an alarm, triggers the NVR to open the alarm circuit and report an alarm • N.C.: Choose this option if the alarm input device is normally opened. The device closes the circuit to input an alarm, triggers the NVR to close the alarm circuit and report an alarm **Note:** Please ensure that **Alarm Status** is enabled before configuration.

2. Set Arming Schedule and Trigger Actions.

6.1.7 Call

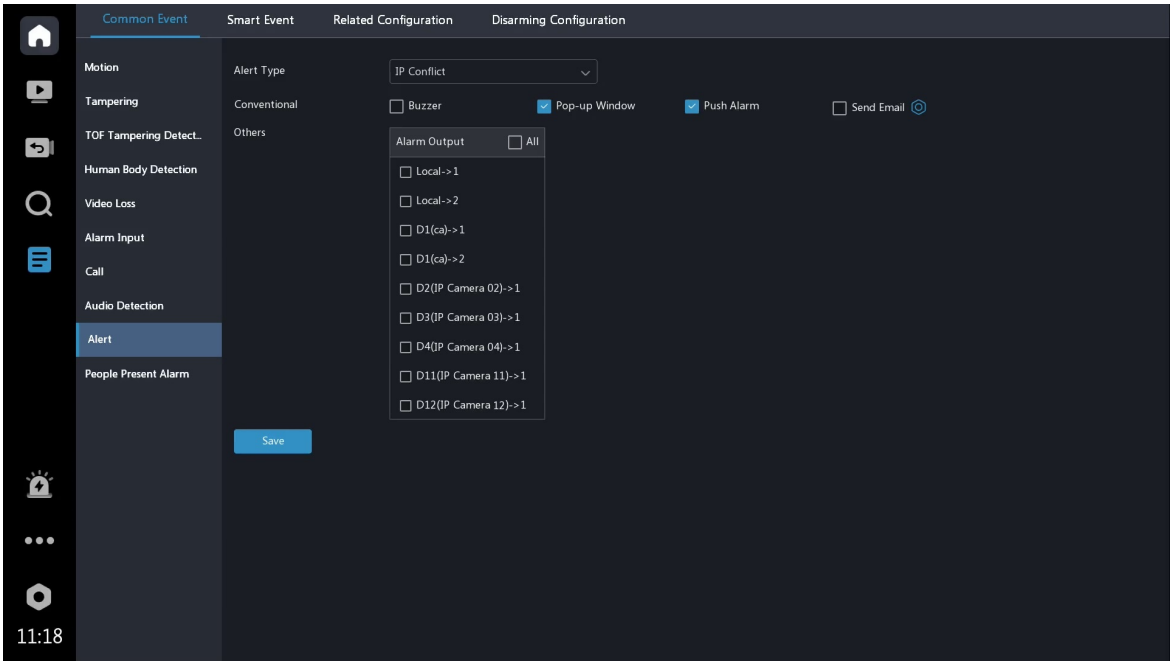
Connect the video doorbell to the NVR, and an alarm will be triggered when the doorbell is pressed. The detection results can be viewed on the playback, video search, picture search, event search, camera alarm, and log pages. Please see Appendix for various search methods details.

Note: The dual-channel doorbell must be connected to a call-supported channel.

The alarm status is enabled by default. Set Arming Schedule and Trigger Actions.

6.1.8 Alert

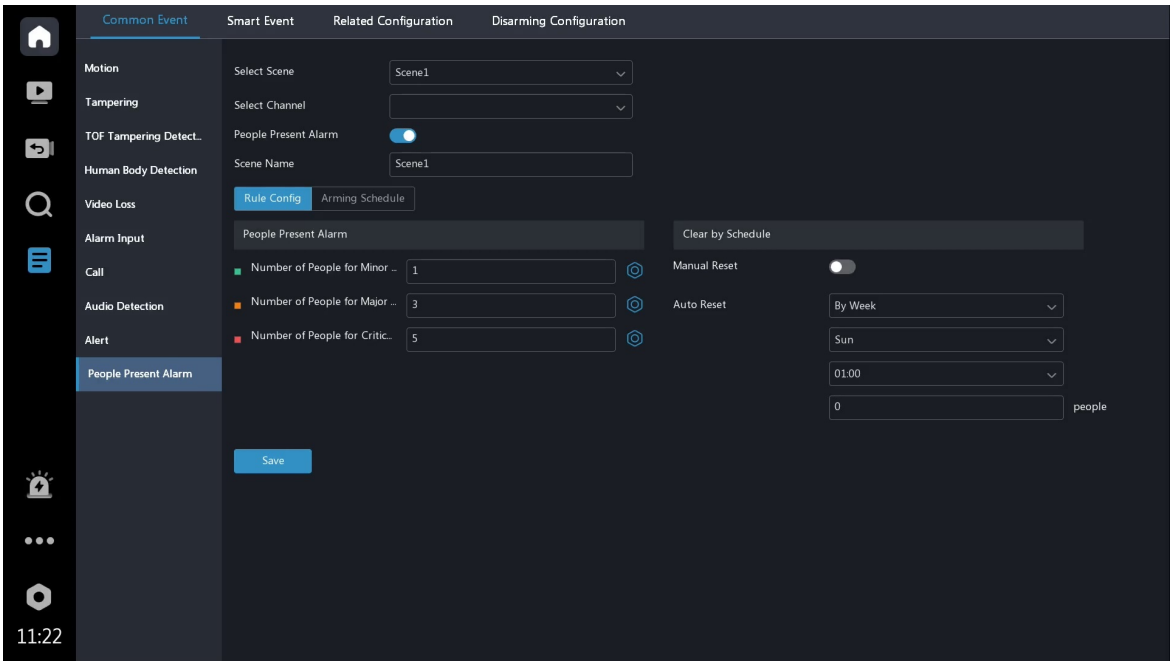
An alarm is triggered when the device alert is detected. The detection results can be viewed on the device alarm and log pages. Please see Appendix for various search methods details.



1. Select an alert type.
   - IP Conflict: IP cameras use the same IP address on the network
   - Network Disconnected: The NVR is disconnected from the network
   - Disk Offline: No disk or a disk is not properly connected
   - Disk Abnormal: A disk is in position but cannot work normally
   - Illegal Access: Incorrect username/password
   - Hard Disk Space Low: The disk space is about to use up
   - Hard Disk Full: The disk space has been used up
   - Array Damaged: The number of lost physical disks in an RAID exceeds the limit
   - Array Degraded: Some physical disks are lost in an RAID but the number of the lost disks is still below the limit
   - Recording/Snapshot Abnormal: Recordings/snapshots cannot be stored normally because the disk is offline or abnormal
   - Failed to Upload Recording to FTP Server: Recording upload failed due to FTP configuration error
2. Set Trigger Actions for each abnormal type separately, and click **Save**.

6.1.9 People Present Alarm

The device calculates the number of people present based on people counting statistics from all entry/exit cameras in the scenes. An alarm is triggered when the count exceeds the set threshold. The detection results can be viewed on the video search, event search, alarm search, camera alarm, and log pages. See Appendix for details on various search methods.



Note: Before use, make sure that People Flow Counting is enabled for the cameras bound to the scene.

1. Select a scene and camera, enable **People Present Alarm**, and set the scene name as needed. Up to 4 scenes are allowed, and each scene can bind to multiple cameras.
2. Set the number of people for minor, major, and critical alarms separately, and click to set Trigger Actions.
3. Set the time to clear people counting data. This feature will clear people counting statistics (people entered and exited) on the smart preview page, and reset the number of people present to the initial count.

   Note: This operation does not affect the people counting OSD on the camera's live video, or NVR statistics and data reporting.

   Set the initial number of people as needed.

   - Manual Reset: When enabled, the initial number of people in current scene can be set as needed.
   - Auto Reset: When **Manual Reset** is disabled, you can set the auto reset strategy by day, week, or month. The system will adjust the number of people in this scene to the set initial number at specified intervals.

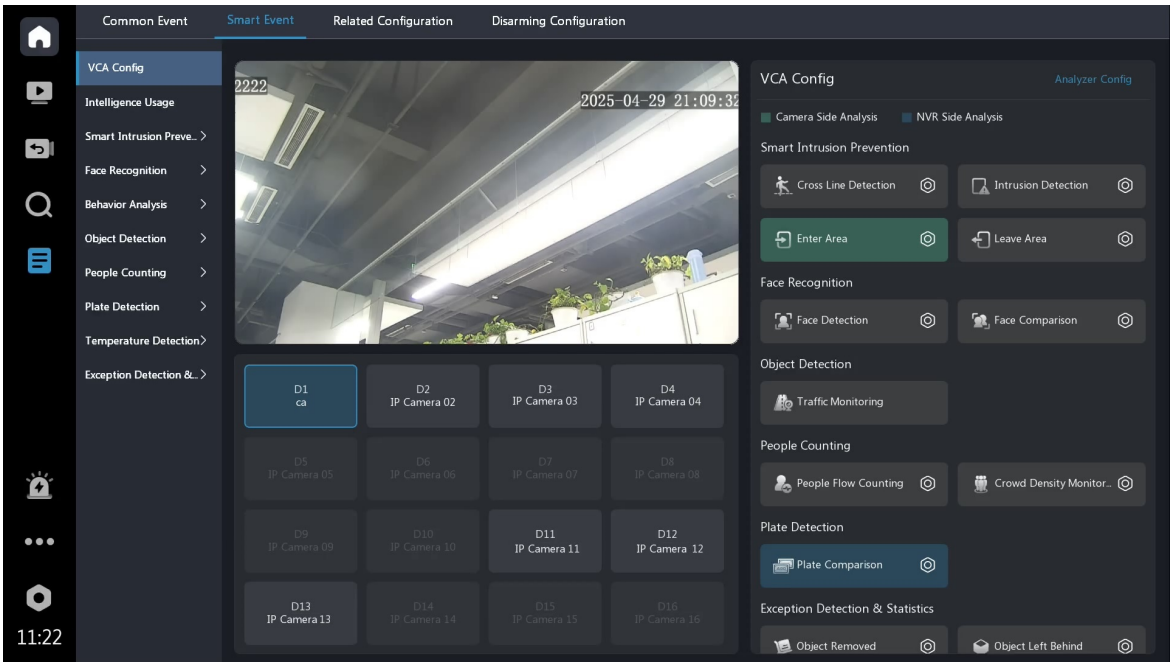
Initial number of people	Description
0	It is recommended to use the default value in the following scenes: • When setting the initial number of people, make sure that there are no people present in the scene • When setting the initial number of people, the scene contains a small number of people, but this will not affect the alarm results (when an alarm is triggered in this scene, the actual number of people will exceed the number of people triggered by the alarm due to a certain margin)
Positive	There are a defined number of people present in the scene (corresponding to a positive value), which affects the people present alarm
Negative	Pre-allocate a certain number of people to enter the scene (corresponding to a negative value), so that this part of the population will not affect the people present alarm

4. Set Arming Schedule, and click **Save**.
5. On the smart preview page, you can check whether the corresponding scene is normal and view the real-time people flow statistics in the area, including the people entered, exited, and allowed.

   Note: People allowed = Critical people present alarm threshold - People present

6.2 Smart Event

6.2.1 VCA Configuration



VCA functions are not available if there is no disk in slot 1.

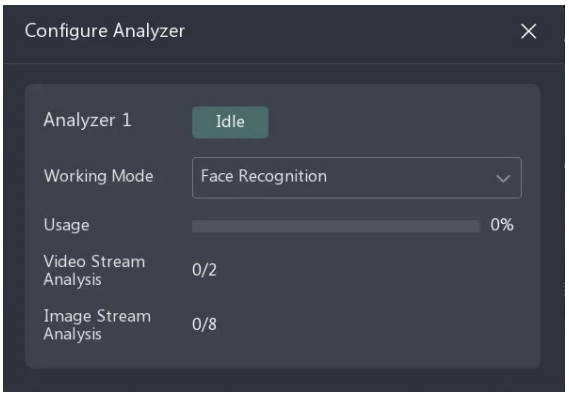
Function Configuration

1. Select a channel to view its VCA configuration information. The function that has configured the camera side analysis or NVR side analysis is highlighted.
   - Camera Side Analysis: The camera detects the VCA function and reports alarms to the NVR.
   - NVR Side Analysis: The NVR detects the VCA function and generates alarms.

   Note:
   - Before you enable camera side analysis, make sure the camera is connected via the private protocol.
   - The NVR side analysis depending on the device capability. Click **Analyzer Config** in the upper-right corner to choose the working mode. The device will automatically restart when the mode changes.
   - When the camera goes online for the first time, the system will automatically sync camera-side configuration and enabled/disabled state to the NVR side; When the camera goes online again, the system will automatically sync camera-side configuration to the NVR side, however, the enabled/disabled state will not be synced.
   - When the camera goes online, if the channel enabled/disabled state on the IPC is not consistent with the NVR, and the NVR-side analysis is enabled while the camera-side analysis is disabled, then a prompt will appear and ask if you want to sync NVR enabled/disabled state to the IPC.
2. Click to configure the smart function.

Analyzer Configuration

Analyzer is a smart hardware unit used to process face recognition, smart intrusion prevention, behavior analysis, ultra motion detection, multi-target detection, accurate search, etc. The analyzer occupies the video stream when the NVR analyzes videos reported by the camera, that is, functions using standalone NVR-side analysis occupy the video stream. The analyzer occupies the image stream when the NVR analyzes images reported by the camera (currently, only camera-side face detection and NVR-side face comparison will consume the capacity of image stream analysis).



- Single-Channel Video Stream Usage Description

Analyzer Mode	Supported VCA Functions	Usage
Face Recognition	Face Detection, Face Recognition	10% (for one or multiple functions)
Smart Intrusion Prevention (SIP)	Cross Line Detection, Intrusion Detection, Enter area, Leave area	
Behavior Analysis	Long Stay Detection	10% (for one or multiple analysis models)
	Fall Detection, Smoke and Fire Detection, People Flow Counting	10% (for each function)
Ultra Motion Detection	Ultra Motion Detection	10%
Multi-Target Detection	Multi-Target Detection	
Face Recognition + Smart Intrusion Prevention	The same as the functions supported by face recognition and smart intrusion prevention modes	Enabling single or multiple functions within the same category consumes a fixed 10% of total capacity (non-cumulative); enabling functions across different categories results in additive capacity consumption
Face Recognition + Smart Intrusion Prevention + Behavior Analysis	The same as the functions supported by face recognition, smart intrusion prevention, and behavior analysis modes	

- Single-Channel Image Stream Usage Description

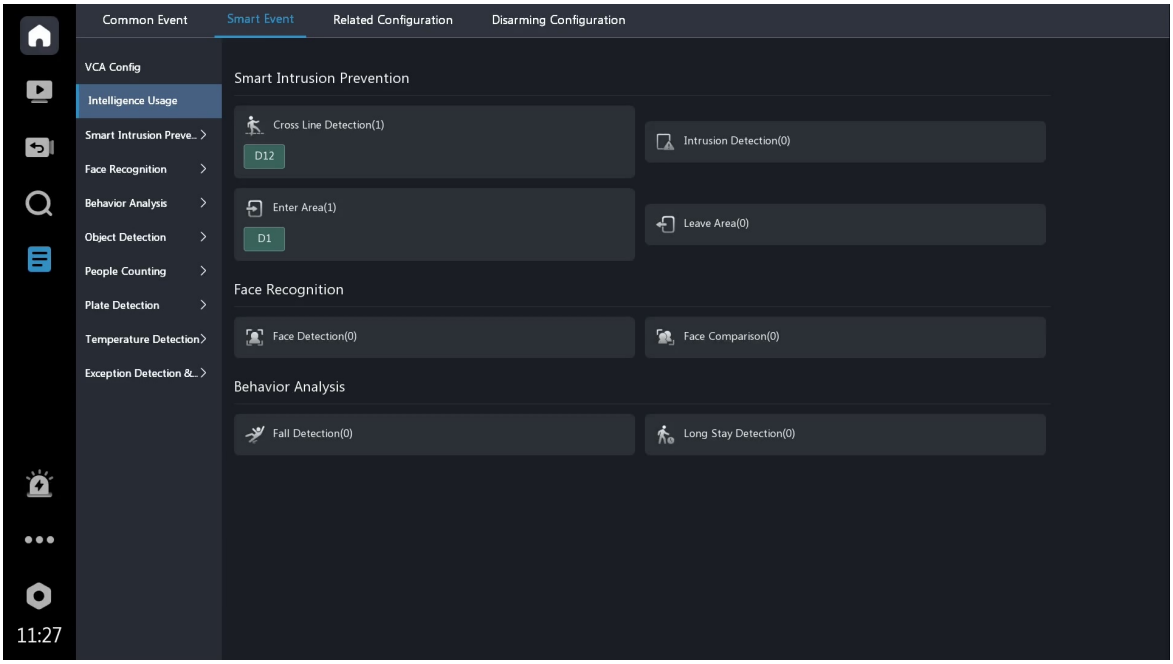
  Only camera-side face detection and NVR-side face comparison will consume 5% capacity of image stream analysis.

Note: Multi-channel stream usage is the sum of single-channel stream usage.

6.2.2 Intelligence Usage

View the usage status of the intelligent functions for the online channels.

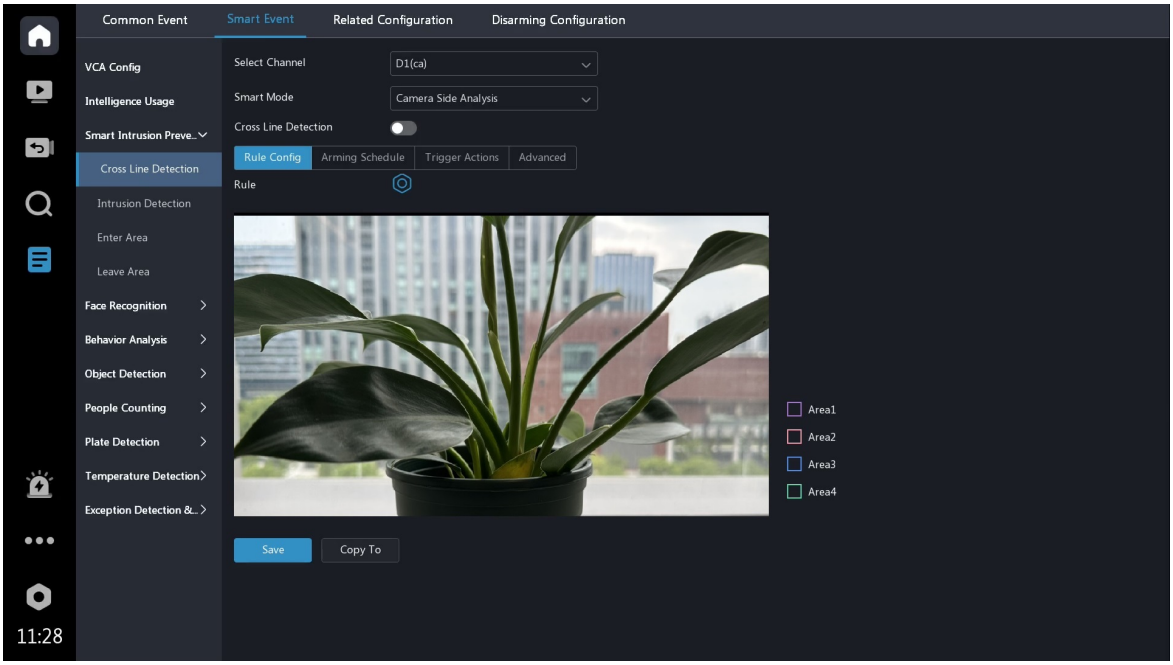
- : Camera side analysis
- : NVR side analysis



6.2.3 Smart Intrusion Prevention

Function	Description
Cross Line Detection	An alarm is triggered when targets cross a specified virtual line in a specified direction
Intrusion Detection	An alarm is triggered when targets enter a specified detection area for a preset time
Enter Area	An alarm is triggered when targets enter a specified detection area
Leave Area	An alarm is triggered when targets leave a specified detection area

The detection results can be viewed on the preview, playback, video search, picture search, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click , select an area, and configure the rule.

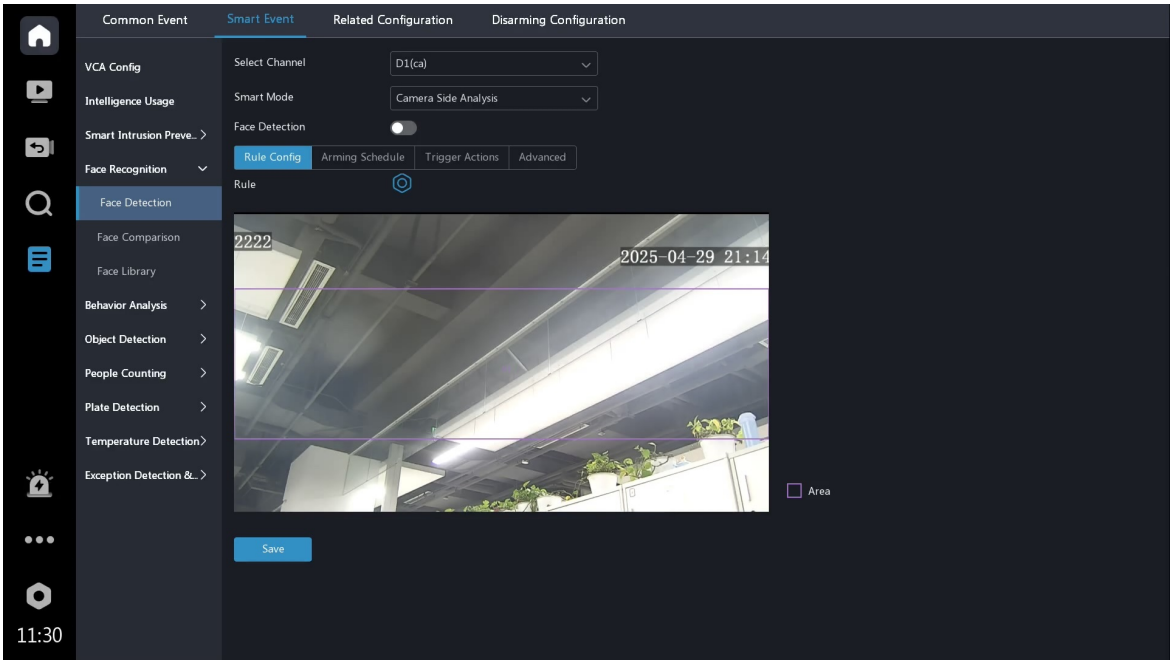
Parameter	Description
Draw Tripwire (Cross Line Detection)	• Click , click on the image and drag to draw a tripwire • Click to delete the current tripwire
Draw Area (Intrusion Detection/Enter Area/ Leave Area)	Draw the detection area with 3 to 6 sides **Note:** When camera side analysis is selected, the maximum number of sides allowed for drawing is determined by the camera's capability, up to a 12-sided polygon. • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Trigger Direction (Cross Line Detection)	Select the direction from which the target crosses the line to trigger an alarm • A<->B: A cross line alarm is triggered when a target crossing the line from A to B or from B to A is detected • B->A: A cross line alarm is triggered when a target crossing the line from B to A is detected • A->B: A cross line alarm is triggered when a target crossing the line from A to B is detected
Percentage (Intrusion Detection)	An intrusion alarm will be triggered if the proportion of the target size to the detection area size reaches the set value. Set based on the scene and your actual needs
Priority	Currently not supported
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene
Snapshot Target	Select the target(s) as needed

3. (Optional) Configure the target size to be detected. The target larger than the max. size and smaller than the min. size will not be detected.
   (1) Enter the **Advanced** page, and select the target type.
   (2) To modify the maximum and minimum sizes, drag the slider or drag the points of the detection box on the live view page.
4. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.4 Face Recognition

6.2.4.1 Face Detection

The NVR takes snapshots and reports an alarm when faces are detected in a specified detection area. The detection results can be viewed on the playback, target search, camera alarm, and log pages. See Appendix for details on various search methods.



1. Select a channel and smart mode, and click to enable **Face Detection**.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Configure the rule.

Parameter		Description
Detection Area	Specify Area	Draw the detection area with 3 to 6 sides • Click , and click on the image to draw 3 to 6 points. Double-click the left mouse, and the first and last points will be automatically connected to form the detection area • Click to delete the detection area
	Full Screen	Detect all faces in the live video
Sensitivity		The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene

3. Complete the advanced settings.

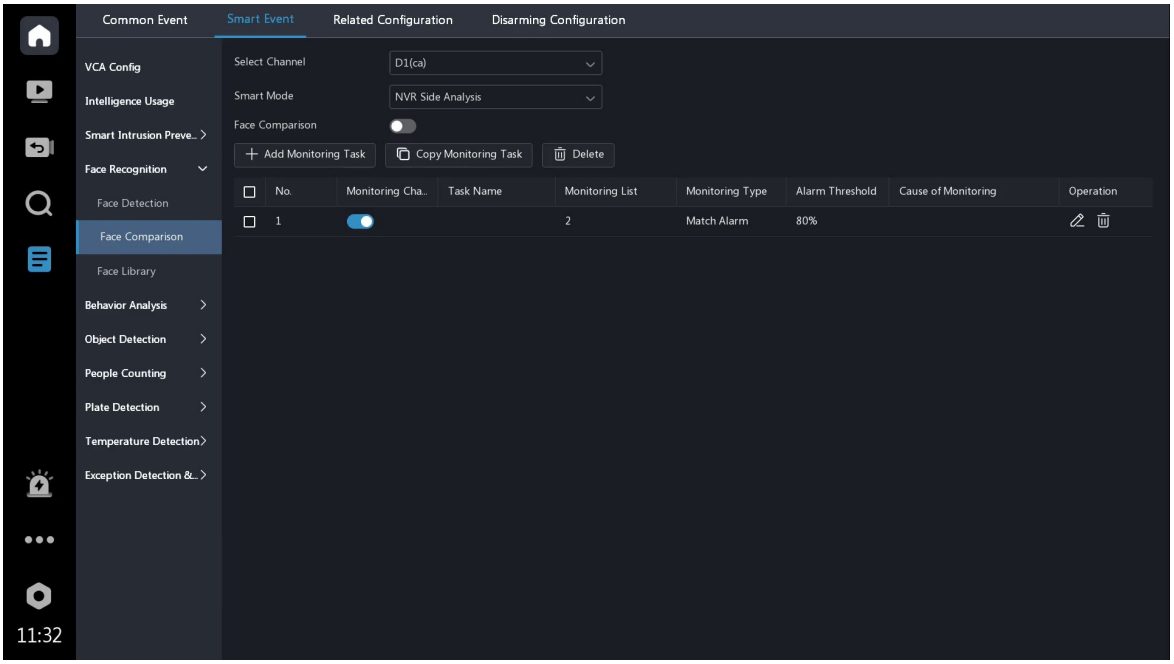
Parameter	Description
Min. Pupillary Distance	This refers to the distance between the pupils of the two eyes. The device will detect faces in the live video based on the set value. If the pupillary distance of the detected target is less than the set value, it will be automatically filtered out and not captured **Note:** The default value varies by image resolution, and the valid range varies by NVR model.
Number of Snapshots	The number of snapshots to be captured when the detection rule is triggered by the same face
Face Width Range	Configure the face size to be detected. The face larger than the max. size and smaller than the min. size will not be detected
Face Selection	When enabled, the face selection mode and selection configuration take effect

Parameter	Description
Face Selection Mode	• Quality Priority: Set the **Number of Selected Photos**, then the NVR selects the specified number of snapshots with the best quality from all the snapshots captured when a face is detected to report • Speed Priority: Set the **Number of Selected Photos** and **Selection Timeout**, then the NVR selects the specified number of snapshots from the moment that a face is detected till **Selection Timeout** is up to report • Periodic Selection: Set the **Selection Interval**, for example, 600ms, then the NVR selects a face snapshot every 600ms to report • Quick Report: A face snapshot that exceeds the set score will be reported, and a higher quality snapshot will be reported to replace the previous one **Note:** Only NVR side analysis supports quick report.

4. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.4.2 Face Comparison

This function compares captured faces with face images in face libraries. An alarm is reported and related actions are triggered based on the set monitoring task when an alarm occurs. To use face comparison, you need to enable Face Detection first. The real-time snapshots can be viewed on the preview page, and other search results can be viewed on the target search, camera alarm, and log pages. See Appendix for details on various search methods.



1. Select a channel and smart mode, and click to enable **Face Comparison**.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. (Optional) A monitoring task of "DefaultList 80% Match Alarm" is enabled by default. You can click to edit the task.

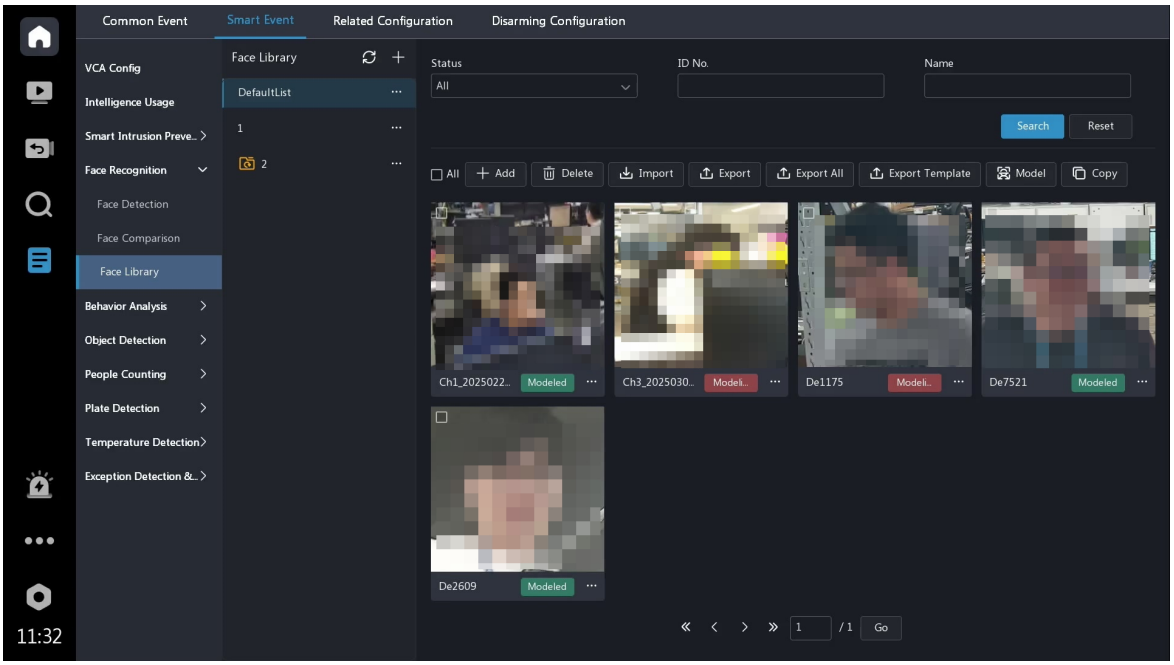
3. Click **Add Monitoring Task**, and configure the parameters.

Parameter	Description
Task Name	Set as needed
Monitoring Task	It is enabled by default
Cause of Monitoring	Enter as needed

Parameter	Description
Monitoring List	Select a face library for face comparison **Note:** If there is no available library, click **Add Face List** to create a face list to monitor.
Monitoring Type	• Match Alarm: A match alarm occurs when the similarity between a detected face and a face image in the monitoring list reaches the alarm threshold • Not Match Alarm: A not match alarm occurs when the similarity between a detected face and a face image in the monitoring list fails to reach the alarm threshold • All: An alarm occurs when a face is detected
Alarm Threshold	An alarm is triggered when the face similarity reaches the set threshold
Arming Schedule	See Arming Schedule for details
Match Trigger Action/Not Match Trigger Action	Set the actions to be triggered by a match alarm or a not match alarm. See Trigger Actions for details

- : Edit the monitoring task.
- : Delete the monitoring task; select multiple monitoring tasks, and click **Delete** to delete them.

6.2.4.3 Face Library



Key Operations

1. Configure the face library. There is a default face library.

Parameter	Description
Add	Click , and set the library name. (Optional) Select the **Set as Dynamic Library** check box to set it as a dynamic library. The captured face image that does not match any face image in the face library will be automatically added to the dynamic library **Note:** • If there is no dynamic face library, you can add a new face library and set it as a dynamic library. You can only configure a dynamic library while adding a face list • Only 1 dynamic library is allowed. To change the dynamic library, you need to delete the original dynamic library and add a new one
Edit	Click , and click **Edit** to modify the library name
Delete	Click , and click **Delete** to delete the face library **Note:** Deleting a face library will also delete its related historical alarm records. Please handle with caution.
	Indicates that the face library is a dynamic library

2. Import face data.

- Import one by one: Click **Add**, and enter the face information.

Parameter	Description
Face Image	Click image on the left to import the desired face image
Face Library	Select a face library to import the face image
Other Fields	Non-required fields, fill in as needed

- Import in batches

(1) Click **Export Template** and choose the destination folder.

Note: A USB flash drive must be connected to the NVR for local interface operation.

(2) Fill in the face information in the CSV file according to the exported template instructions, and organize the face images in the Image folder.

Note:

- The face images must be in JPG format with a maximum size of 4MB; otherwise, the import will fail. Images not in JPG format must be properly converted using professional image converter tool. Manual file extension changes are unacceptable.
- The image names specified in the template must exactly match the file names in the Image folder.

(3) Click **Import**, choose the file or folder to be imported, and click **Import**.

Note: The number of images allowed for a file depends on the library capacity of the device.

Other Operations

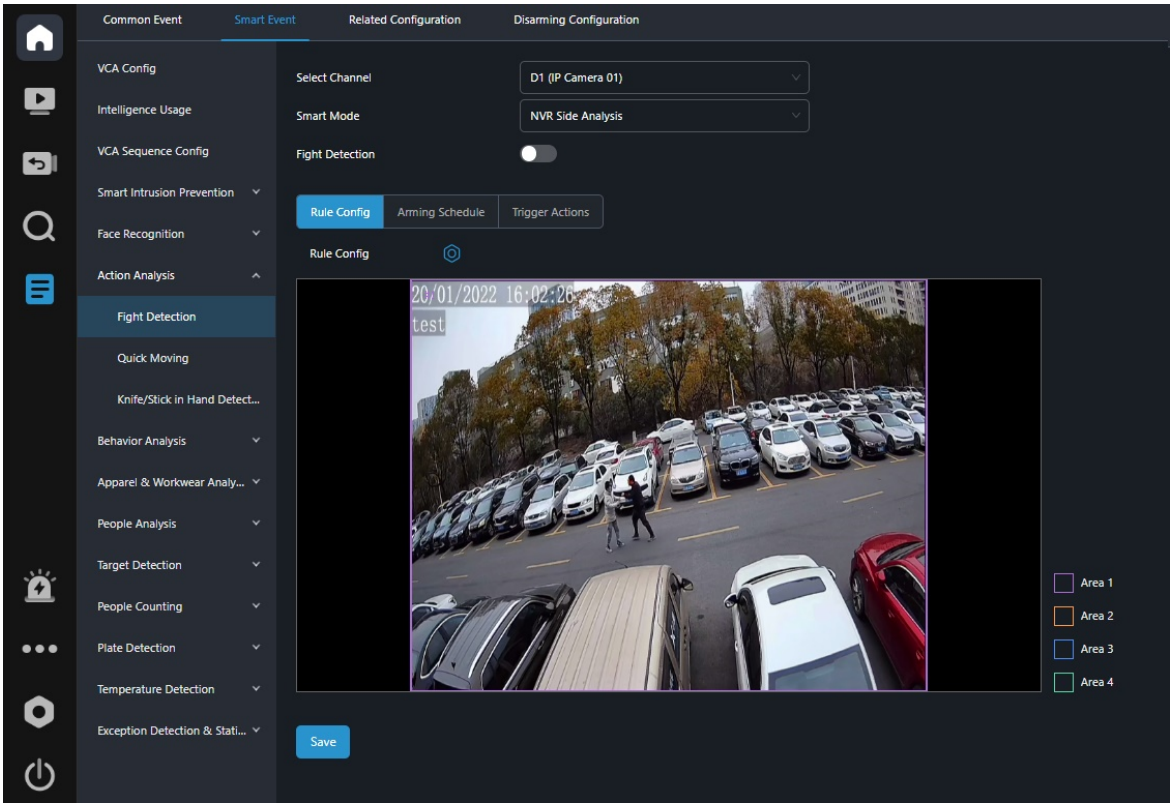
Parameter	Description
Search	• Configure the search criteria and click **Search** to view the results • Click **Reset** to clear the search criteria
Select all	Click **All** to automatically select all faces under the current face library **Note:** You can select or deselect the face image(s).
Delete	Delete the selected face image(s)

Parameter	Description
Export/Export All	Export the selected face(s) or all faces to the specified path in the USB drive (local interface) or computer (web interface)
Model	Select face image(s) that has not been modeled or has failed to be modeled, and click **Model** for manual modeling
Copy	Select the face image(s), and click **Copy** to import them to other face libraries as needed, excluding the dynamic library
More	Click ···, and edit, model, copy, or delete the face image as needed

6.2.5 Action Analysis

Function	Introduction
Fight Detection	This function triggers an alarm when two or more people fighting in the specified detection area are detected
Quick Moving	This function triggers an alarm when people moving quickly is detected in the specified detection area
Knife/Stick in Hand Detection	This function triggers an alarm when people holding a knife/stick in hand is detected in the specified detection area

The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click to configure the detection rule.

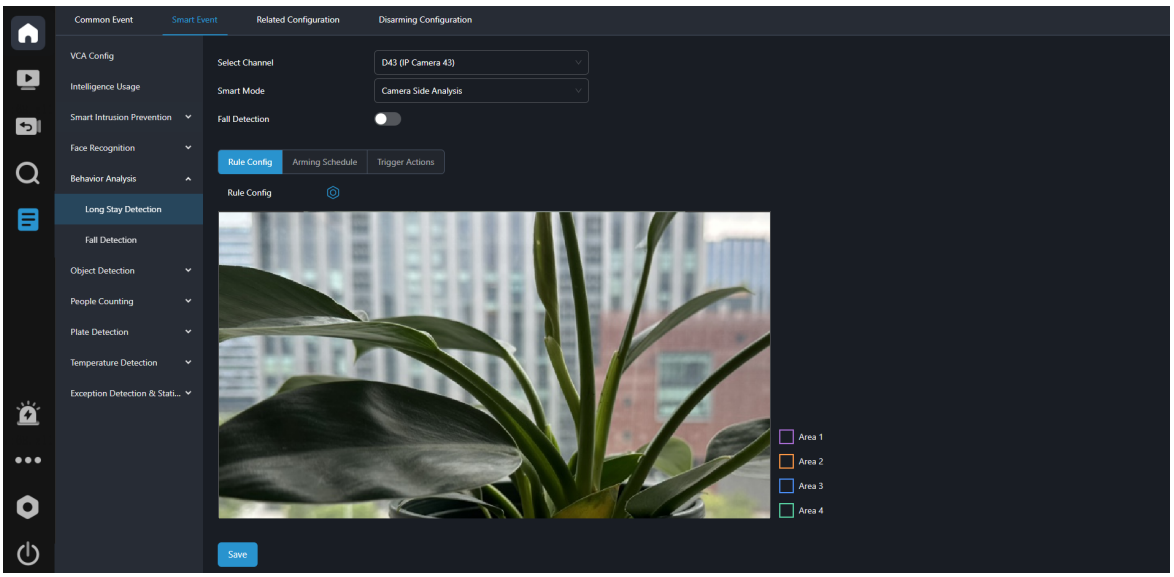
Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Alarm Interval	The device keeps analyzing the scene to assess the continuity of an ongoing behavioral event. This parameter can refrain the device from reporting the same alarm repeatedly within a specified time range
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.6 Behavior Analysis

Function	Introduction
Climbing Detection	This function triggers an alarm when people climbing is detected in the specified detection area
Long Stay Detection	This function triggers an alarm when the target stays in the specified detection area longer than the set time threshold
Fall Detection	This function triggers an alarm when people falling is detected in the specified detection area
Sleep on Duty Detection	This function triggers an alarm when the target rests his/her head on the table in the specified detection area and remains still for a certain length of time
Absence Detection	This function triggers an alarm when the total number of people in the specified detection area is less than the set number for a certain length of time
Calling Detection	This function triggers an alarm when people calling using a mobile phone is detected in the specified detection area
Rat Detection	This function triggers an alarm when moving rats are detected in the specified detection area
Using Mobile Phone Detection	This function triggers an alarm when the target uses a mobile phone for a certain length of time

The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click to configure the detection rule.

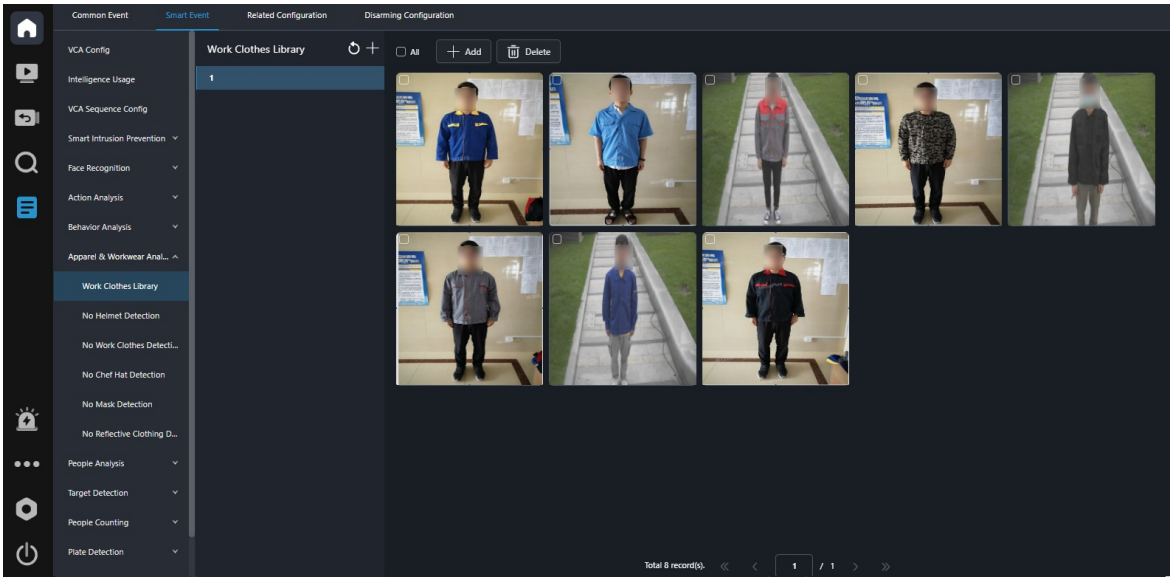
Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Draw Detection Line (Climbing Detection)	Draw the height detection line as needed
Alarm Interval	The device keeps analyzing the scene to assess the continuity of an ongoing behavioral event. This parameter can refrain the device from reporting the same alarm repeatedly within a specified time range
Time Threshold(s)	An alarm will be triggered if a target stays in the detection area and performs certain behavior for the set time. You can set it based on the actual scene or on-site commissioning
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene
Maximum Sleep Duration(s)	Set the threshold for the maximum sleep duration
Max. Absence Duration(s)	Set the absence duration threshold
Min. People Present	Set the threshold for the minimum number of people present

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.7 Apparel & Workwear Analysis

6.2.7.1 Work Clothes Library

Key Operations



1. Configure the work clothes library.

Parameter	Description
Add	Click , and set the library name as needed.
Edit	Click , choose **Edit**, and change the name as needed.
Delete	Click , and choose **Delete**. **Note:** Deleting the work clothes library will disable No Work Clothes Detection of the monitored channels.

2. Click **Add** to inport work clothes data.

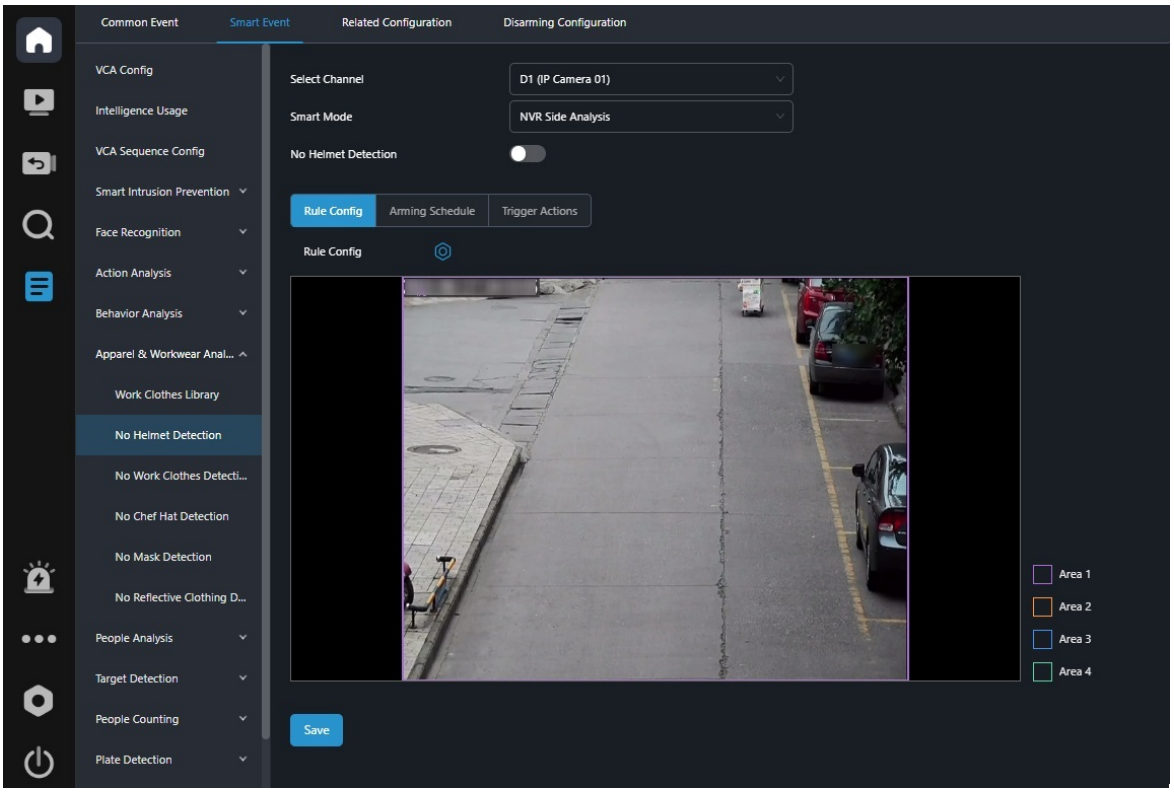
Other Operations

Parameter	Description
All	Click to select all work clothes data in the current work clothes library **Note:** You can select or deselect the work clothes data one by one.
Delete	Delete the selected work clothes
	Delete a work clothes

6.2.7.2 No Helmet Detection/No Work Clothes Detection/No Chef Hat Detection/ No Mask Detection/No Reflective Clothing Detection

Function	Description
No Helmet Detection	This function triggers an alarm when people not wearing a helmet is detected in the specified detection area
No Chef Hat Detection	This function triggers an alarm when people not wearing a chef hat is detected in the specified detection area
No Mask Detection	This function triggers an alarm when people not wearing a mask is detected in the specified detection area
No Work Clothes Detection	This function triggers an alarm when people not correctly wearing the specified work clothes is detected in the specified detection area
No Reflective Clothing Detection	This function triggers an alarm when people not wearing the reflective clothing is detected in the specified detection area

The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click to configure the detection rule.

Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Sensitivity	The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene

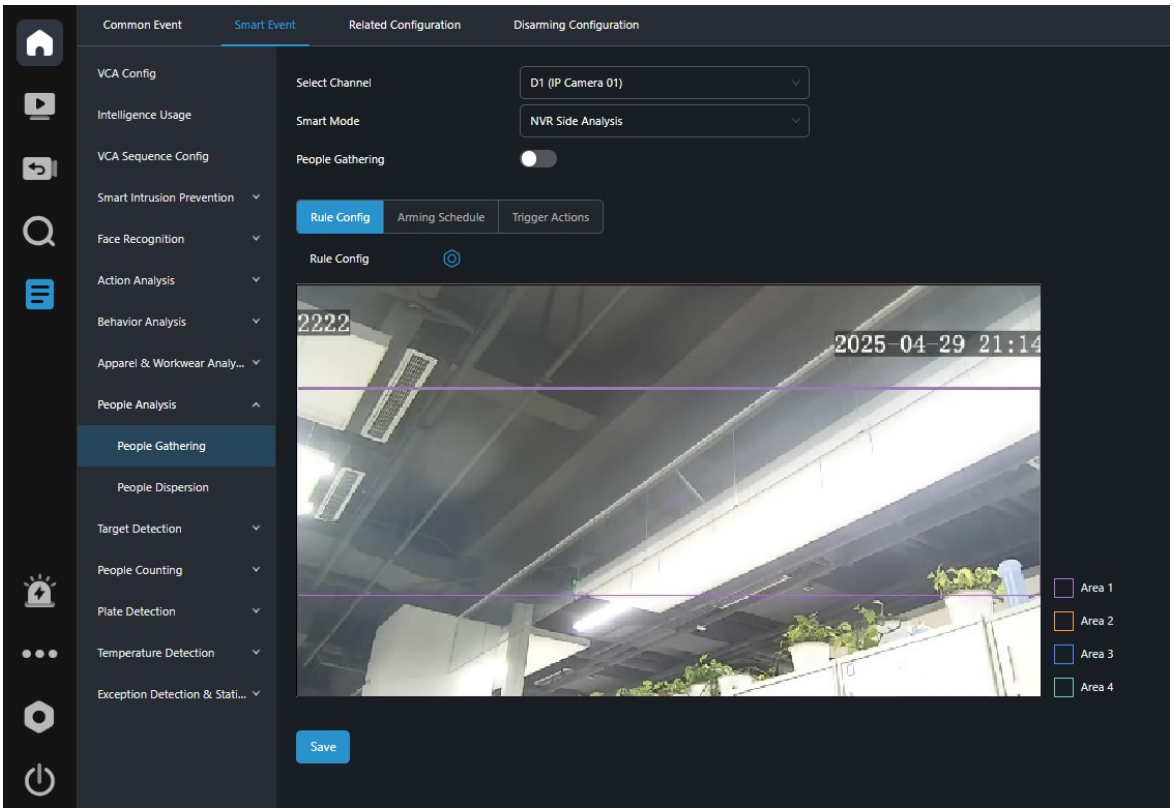
3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.8 People Analysis

6.2.8.1 People Gathering

An alarm is triggered when the number of people in the specified detection area reaches the maximum threshold or a increase in people reaches the preset threshold within the set time period.

The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click , select an area, and configure the detection rule.

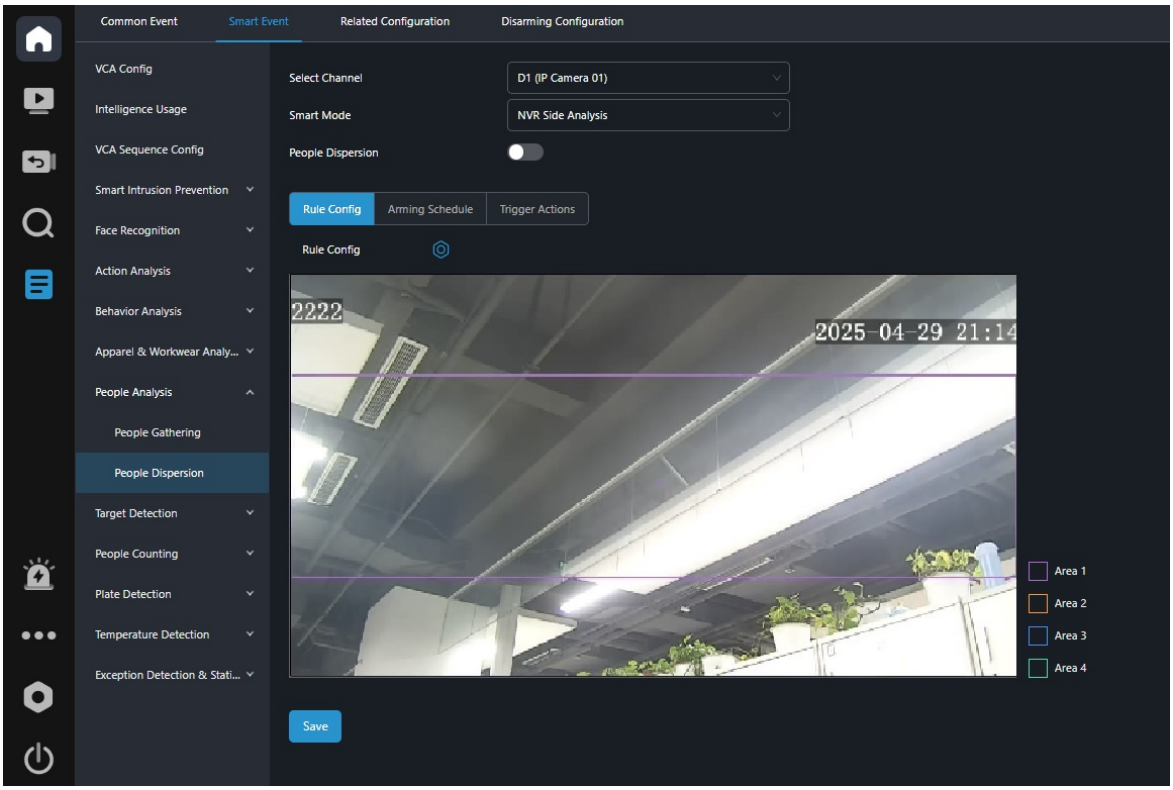
Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Total People Threshold	Set the threshold for the maximum number of people
Time Duration (s)	Set the duration to recognize the people increase
People Increase	Set the threshold for people increase

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.8.2 People Dispersion

An alarm is triggered when the number of people in the specified detection area reaches the minimum threshold or a decrease in people reaches the preset threshold within the set time period.

The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click , select an area, and configure the detection rule.

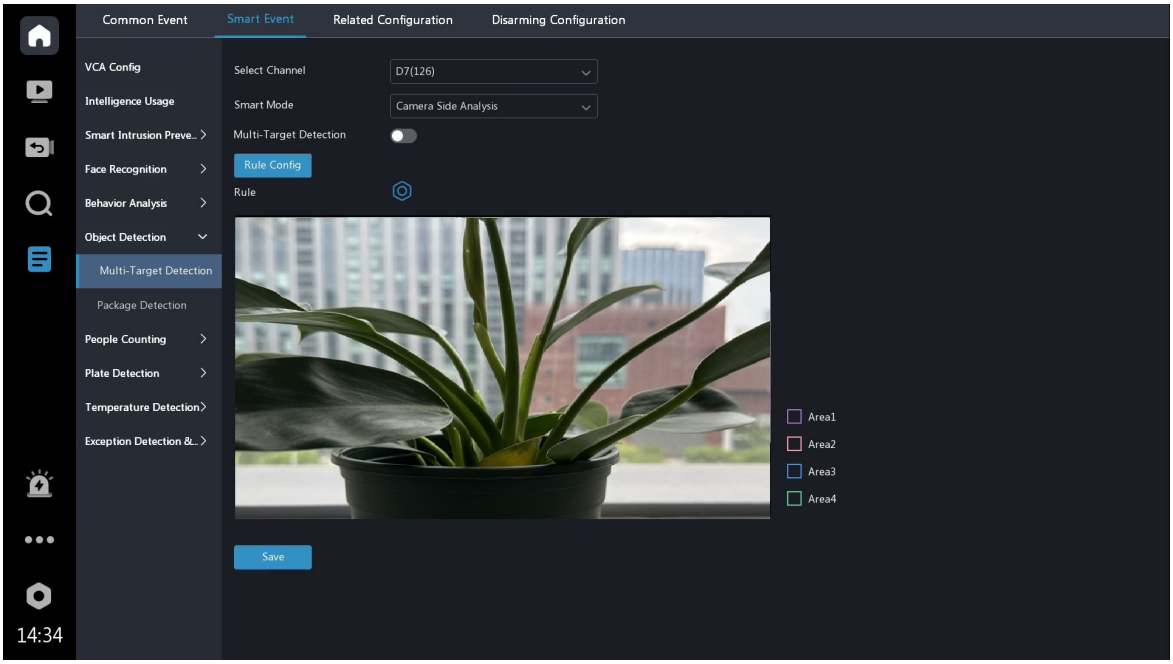
Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Total People Threshold	Set the threshold for the minimum number of people
Time Duration (s)	Set the duration to recognize the people decrease
People Decrease	Set the threshold for people decrease

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.9 Target Detection

6.2.9.3 Multi-Target Detection

The NVR takes snapshots and reports an alarm when the motor vehicles, non-motor vehicles, or pedestrians are detected in the specific detection area. The detection results can be viewed on the playback, event search, camera alarm, and log pages. See Appendix for details on various search methods.



1. Select a channel and smart mode, and click to enable **Multi-Target Detection**.

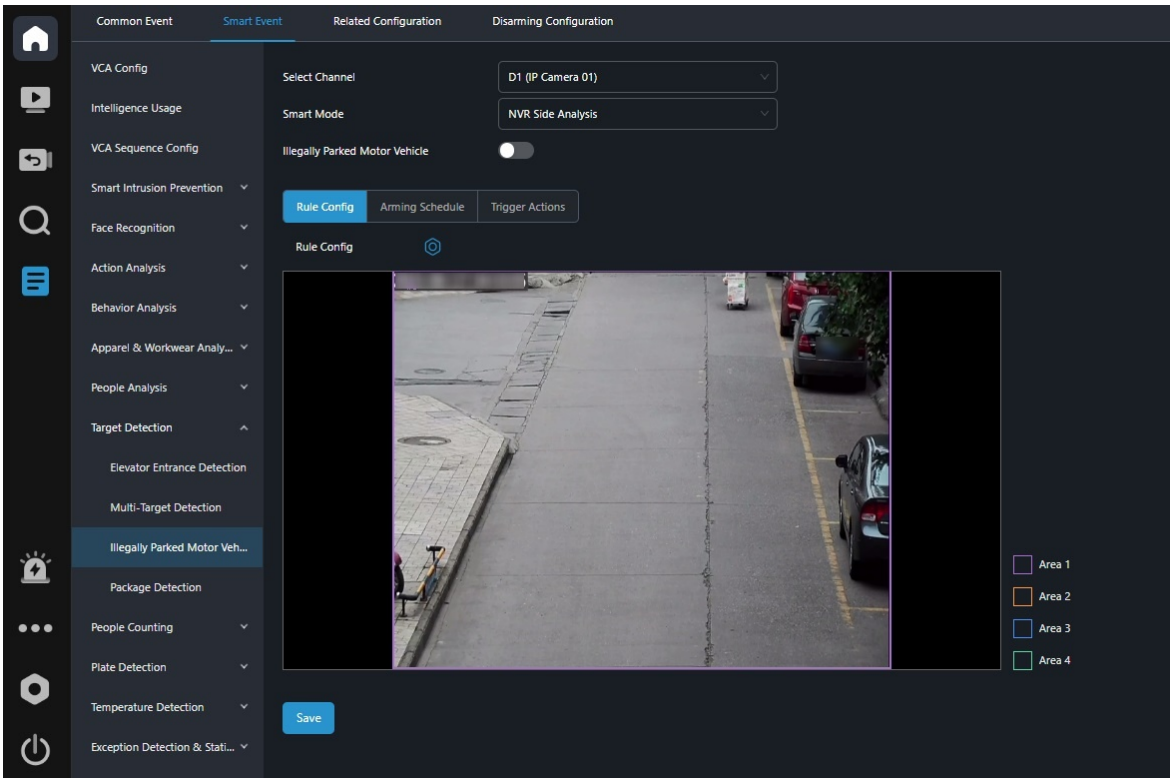
   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click to configure the detection rule.

Parameter		Description
Detection Area	Specify Area	Draw the detection area with 3 to 6 sides • Click , and click on the image to draw 3 to 6 points. Double-click the left mouse, and the first and last points will be automatically connected to form the detection area • Click to delete the detection area
	Full Screen	Detects all areas in the live video
Sensitivity		The higher the sensitivity, the more likely the detection rule will be triggered, but the false alarm rate will increase. Please adjust the sensitivity based on the actual scene
Snapshot Target		Select the target(s) as needed

6.2.9.4 Illegally Parked Motor Vehicle

This function triggers an alarm when a motor vehicle parks in the specified detection area. The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click to configure the detection rule.

Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , and click on the image to draw 3 to 6 points. Double-click the left mouse, and the first and last points will be automatically connected to form the detection area • Click to delete the detection area
Alarm Interval	The device keeps analyzing the scene to assess the continuity of an ongoing behavioral event. This parameter can refrain the device from reporting the same alarm repeatedly within a specified time range
Duration (s)	Set the illegal parking time threshold for motor vehicles

3. Set Arming Schedule and Trigger Actions, and click **Save**.

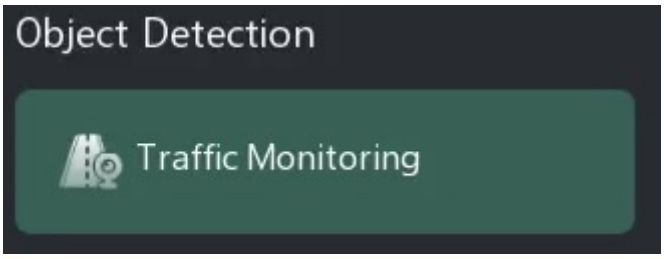
6.2.9.5 Package Detection

Select a channel, enable **Package Detection**, and set Trigger Actions.

6.2.9.6 Traffic Monitoring

The traffic monitoring function can capture motor vehicles, motorcycles, non-motor vehicles, and pedestrians on the roads or in parks, and can identify and monitor specific vehicles, specific license plates, etc. The detection results can be viewed on the event search and target search pages. See Appendix for details on various search methods.

Please log in to the camera's web interface to configure traffic monitoring function. See *Network Camera User Manual* for details. The NVR can only enable/disable the reception of alarm information from road monitoring.

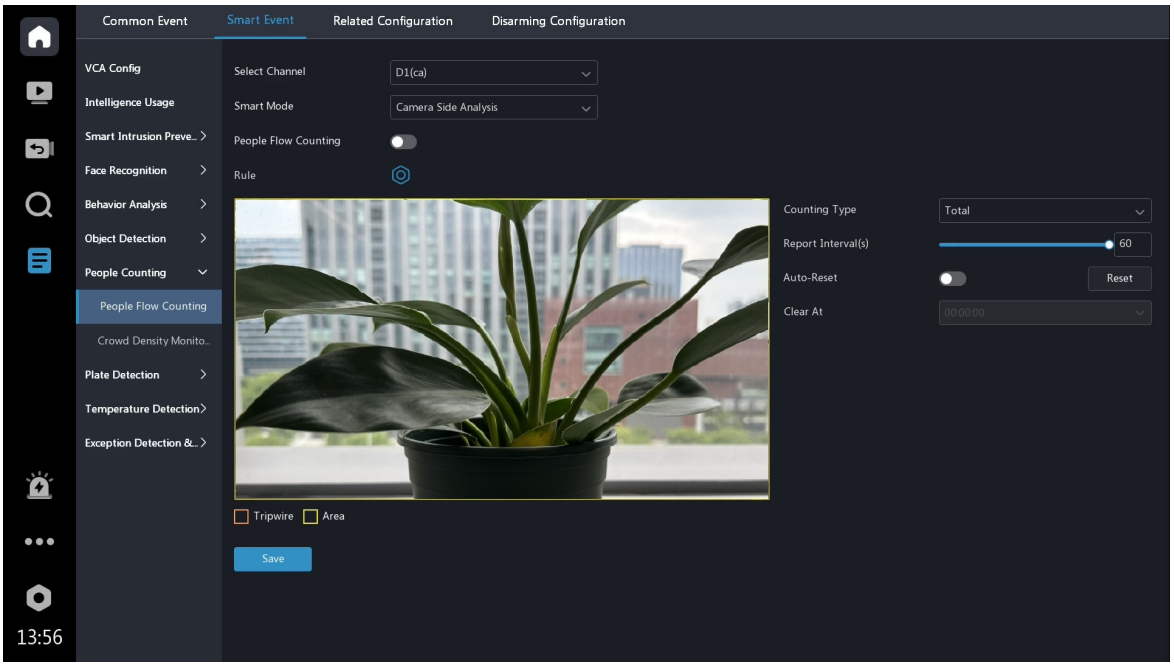


Note: Traffic monitoring has no configuration page on the local interface. Please select a channel and enable this function on the VCA Configuration page.

6.2.10 People Counting

6.2.10.1 People Flow Counting

This function counts people passing a specified tripwire in the specific detection area, including people entered, people exited, and total people entered and exited. Enable **People Counting** for **OSD Content** in Video OSD, and the search results will be displayed on the live video and playback pages.



1. Select a channel and smart mode, and click to enable **People Flow Counting**.
2. Click to configure the detection rule.

Parameter	Description
Draw Tripwire	• Click , click on the image and drag to draw a tripwire • Click to delete the current tripwire
Trigger Direction	Select the direction from which the target crosses the tripwire to trigger an alarm • A- >B: A to B is entry, B to A is exit • B- >A: B to A is entry, A to B is exit

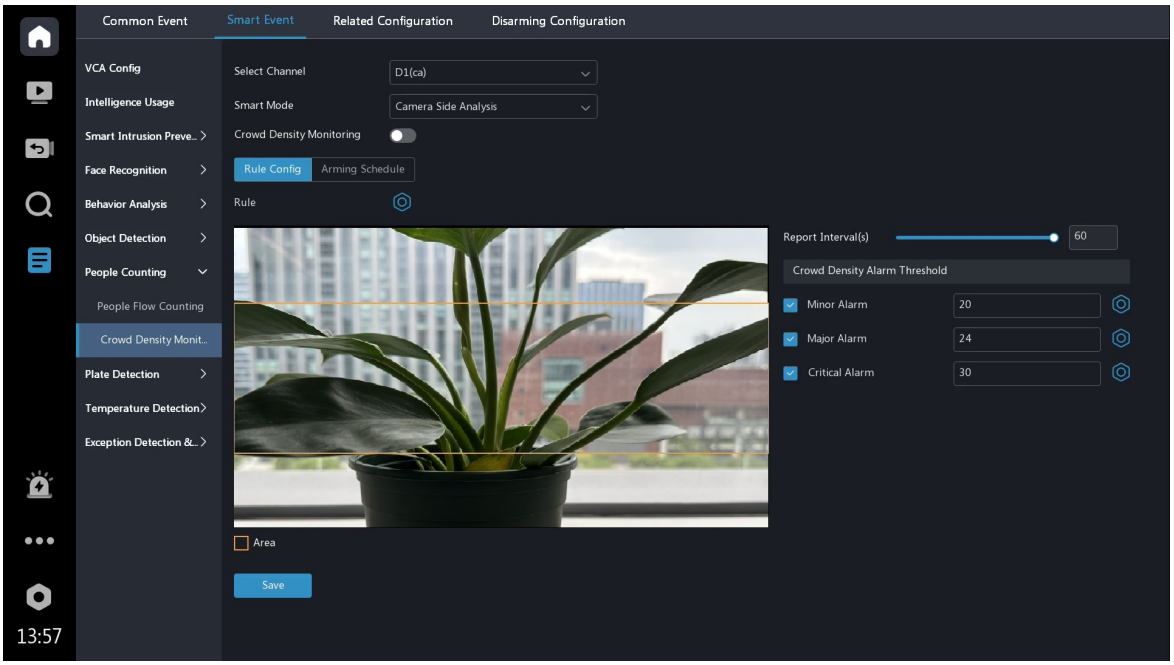
Parameter	Description
Draw Area	Draw the detection area **Note:** When camera side analysis is selected, the maximum number of sides allowed for drawing is determined by the camera's capability, up to a 12-sided polygon. • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area

3. Complete other configurations.

Parameter	Description
Counting Type	• Total: Displays the total number of people entering and leaving the area • People Entered: Displays the number of people entering the detection area. An entry is counted as a person crosses the tripwire in the direction of the arrow and passes through the detection area • People Exited: Displays the number of people leaving the detection area. An exit is counted as a target crosses the tripwire in the opposite direction of the arrow and passes through the detection area **Note:** People that loiter in the detection area, cross the tripwire only, or cross the detection area only are not counted.
Report Interval(s)	The NVR reports people flow statistics to the upper platform at set intervals after the upper platform subscribes to the function
Reset	Clear the people counting statistics manually **Note:** This operation does only affect the people counting OSD on the camera's live video, and does not affect NVR statistics and data reporting.
Auto-Reset	When enabled, the system will clear the people counting statistics based on the set time
Clear At	Clear people counting statistics on the OSD at the set time every day. You can set it as needed

6.2.10.2 Crowd Density Monitoring

This function monitors the total number of people in a specified area and triggers an alarm if the number exceeds the set alarm threshold.



1. Select a channel and smart mode, and click to enable **Crowd Density Monitoring**.
2. Configure the detection rule.

   (1) Click to draw the detection area.

Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides **Note:** When camera side analysis is selected, the maximum number of sides allowed for drawing is determined by the camera's capability, up to a 12-sided polygon. • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area

   (2) Configure other parameters.

Parameter	Description
Report Interval (s)	The device reports crowd density statistics to the upper platform at set intervals. The upper platform must subscribe to the function to receive the statistics
Crowd Density Alarm Threshold	Select minor, major, or critical alarm as needed, and configure the alarm threshold
right to the threshold	• Alarm Sound: Set the audio file and the number of times that the audio file to be played by the camera when an alarm occurs • Flashing Light: Set the duration and brightness that the illuminator flashes when an alarm occurs

3. Set Arming Schedule, and click **Save**.

6.2.11 Plate Detection

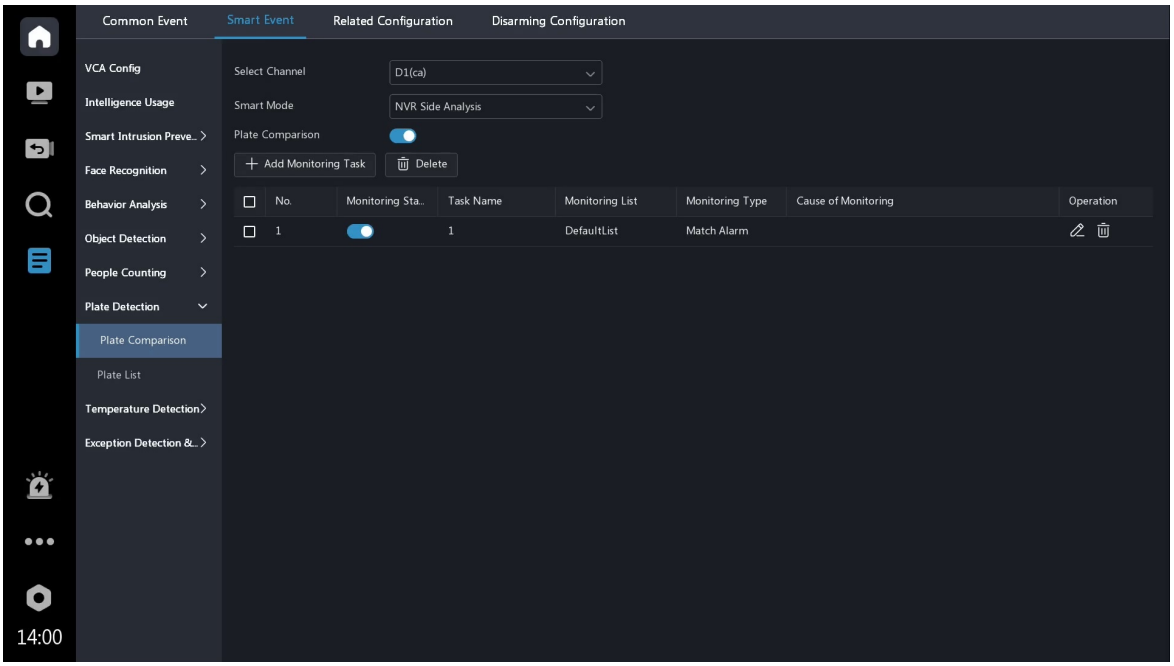
Detect license plates in the live video and compare them with those of the plate library. An alarm is triggered when a captured plate number matches one in the monitoring list.

6.2.11.1 Plate Comparison

Configure vehicle monitoring tasks so that the NVR can report alarms according to the matching result of the captured plate numbers and the plate numbers in plate lists. The real-time snapshots can be viewed on the

preview page, and other search results can be viewed on the camera alarm, event search, target search, and log pages. See Appendix for details on various search methods.

Note: To use plate comparison function, enable **Plate Detection** in VCA Configuration or configure VIID Local, and configure Plate List.



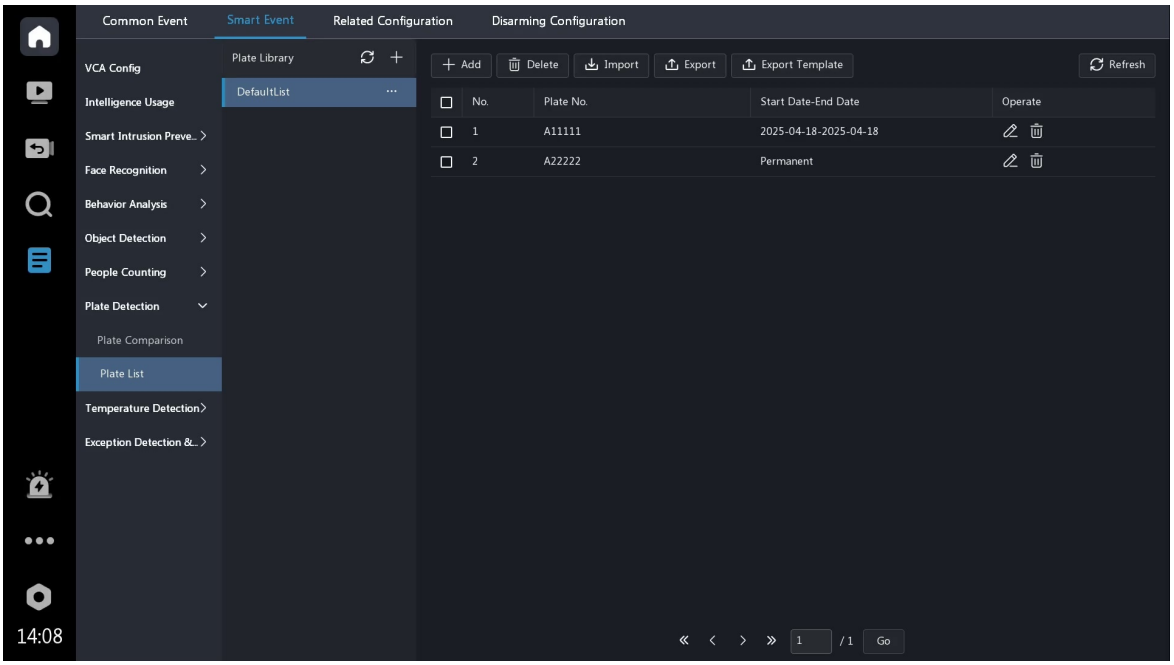
1. Select a channel and smart mode, and click to enable **Plate Comparison**.
2. Click **Add Monitoring Task**, configure the parameters, and click **Save**.

Parameter	Description
Task Name	Set as needed
Monitoring Task	Enable/disable the monitoring task
Cause of Monitoring	Enter as needed
Monitoring List	Select the plate library for comparison
Monitoring Type	• Match Alarm: An alarm is reported when a captured plate number matches a plate number in the monitoring list • Not Match Alarm: An alarm is reported when a captured plate number does not match a plate number in the monitoring list • All: An alarm occurs when a plate is detected
Arming Schedule	Set Arming Schedule
Match Trigger Action/Not Match Trigger Action	Set the actions to be triggered by a match alarm or a not match alarm. See Trigger Actions for details

3. (Optional) Click to edit the monitoring task. Click to delete a task; or select multiple tasks and click **Delete** to delete them.

6.2.11.2 Plate List

Configure plate lists and plate information for Plate Comparison.



1. Edit the plate list or add a plate list.
   - Edit: Click ··· of the default list, choose **Edit**, modify the list name, and click **OK**.
   - Add: Click ＋, enter the list name, and click **OK**.
2. Add plate numbers.
   - Add one by one: Click **Add**, enter the plate number, and click **OK**.
     When **Set Validity Period** is enabled, the plate will only be valid during the set validity period; when disabled, the plate will be valid permanently.
   - Add in batches (a USB device is required for local interface, not required for web interface)

     (1) (Connect the USB device to the NVR) Click **Export Template**, choose the location to save the template, and click **OK**.

     (2) (Connect the USB device to the PC) Open the template and enter the plate information.

     (3) (Reconnect the USB device to the NVR) Click **Import**, select the template, and click **OK** to add plates in batch.

     Note: The plates added in batches are valid permanently by default.
3. (Optional) Manage the plates.
   - : Edit the plate information as needed.
   - /Delete: Delete the plate(s).
   - Export: Export the selected plate(s) or all plates.
   - Refresh: Refresh the plate list.

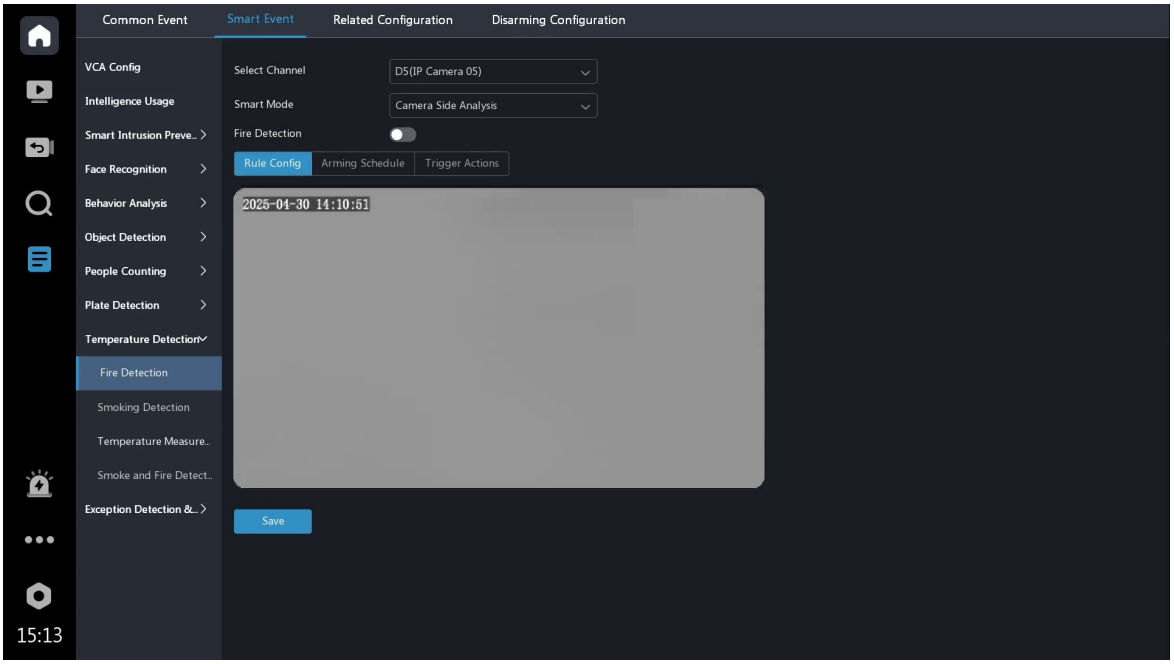
6.2.12 Temperature Detection

This function receives temperature alarms reported from the camera. An alarm is triggered and reported when the camera detects a temperature that exceeds the set threshold or other specified behaviors. The real-time snapshots can be viewed on the preview page, and other search results can be view on the playback, event search, target search (only for smoking detection), camera alarm, and log pages. See Appendix for details.

Event	Description
Fire Detection	An alarm is triggered when fire in the environment is detected
Smoking Detection	An alarm is triggered when people smoking is detected
Temperature Measurement	An alarm is triggered when the temperature exceeds the set alarm threshold

Event	Description
Smoke and Fire Detection	An alarm is triggered when smoke and fire are detected

Note: These functions should be configured on the camera's web interface before use.

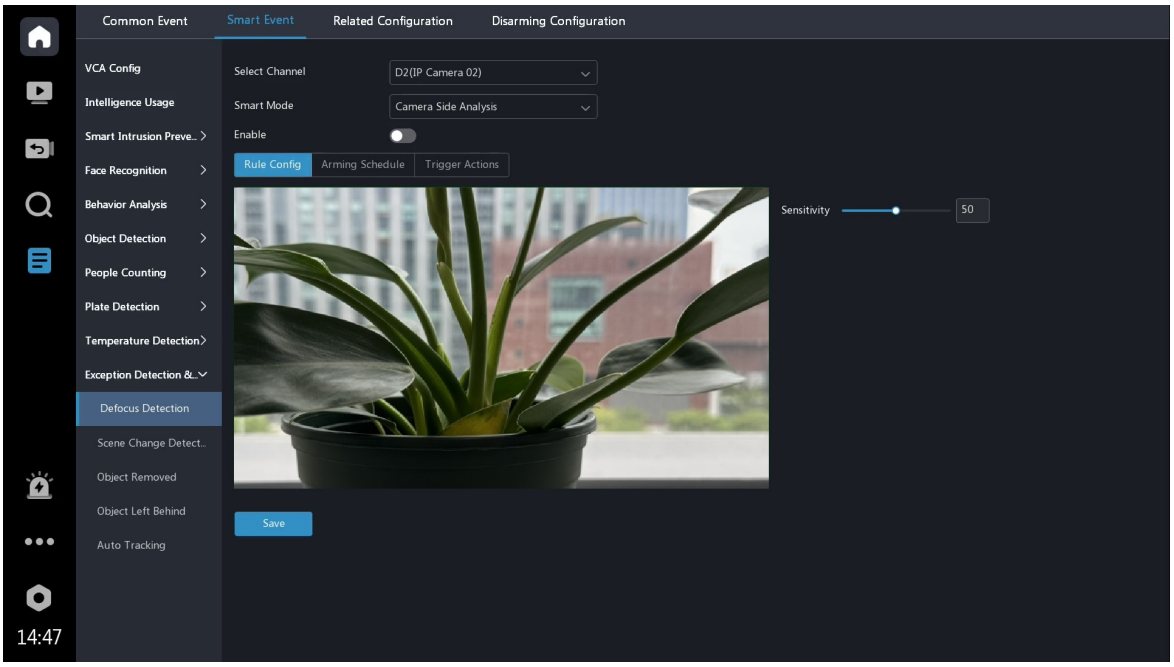


1. Select a channel and smart mode, and click to enable the function.
2. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13 Exception Detection & Statistics

6.2.13.1 Defocus Detection

An alarm is triggered when the lens defocus is detected. The detection results can be viewed on the playback, camera alarm, and log pages. See Appendix for details on various search methods.

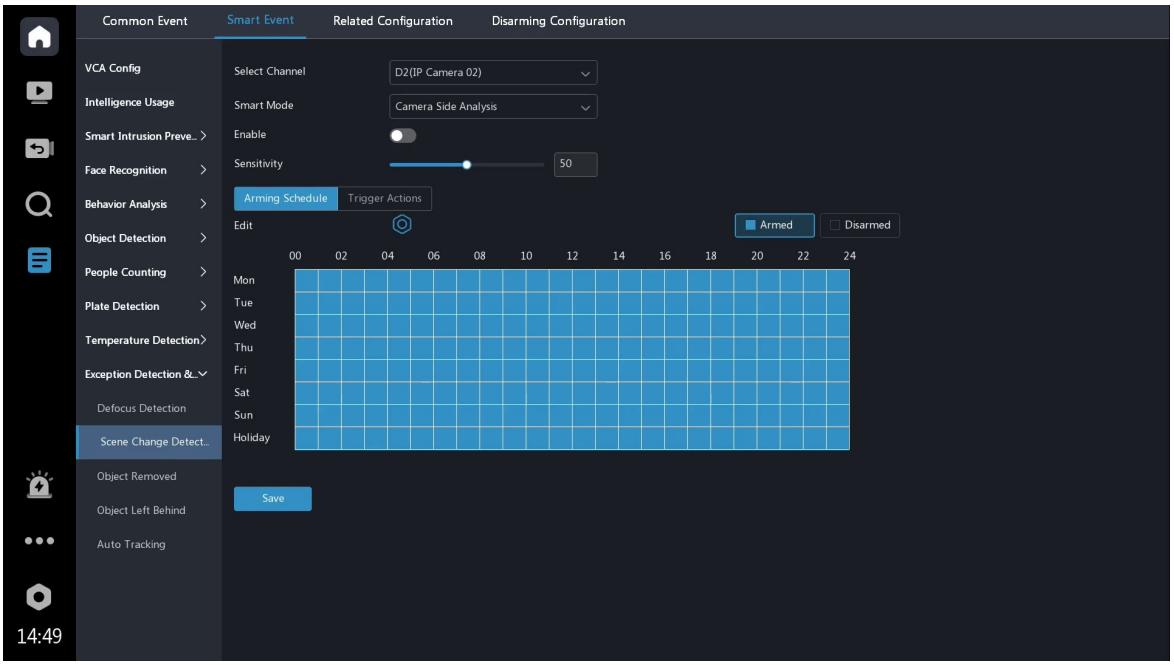


1. Select a channel and smart mode, and click to enable the function.

2. Set the sensitivity. The higher the sensitivity, the more likely the detection will be triggered, but the false alarm rate will increase. Please adjust the based on the actual scene.
3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13.2 Scene Change

Scene change detection detects the change of surveillance scene caused by external factors such as camera movement. The NVR takes snapshots and reports an alarm when the detection rule is triggered. The detection results can be viewed on the playback, camera alarm, and log pages. See Appendix for details on various search methods.

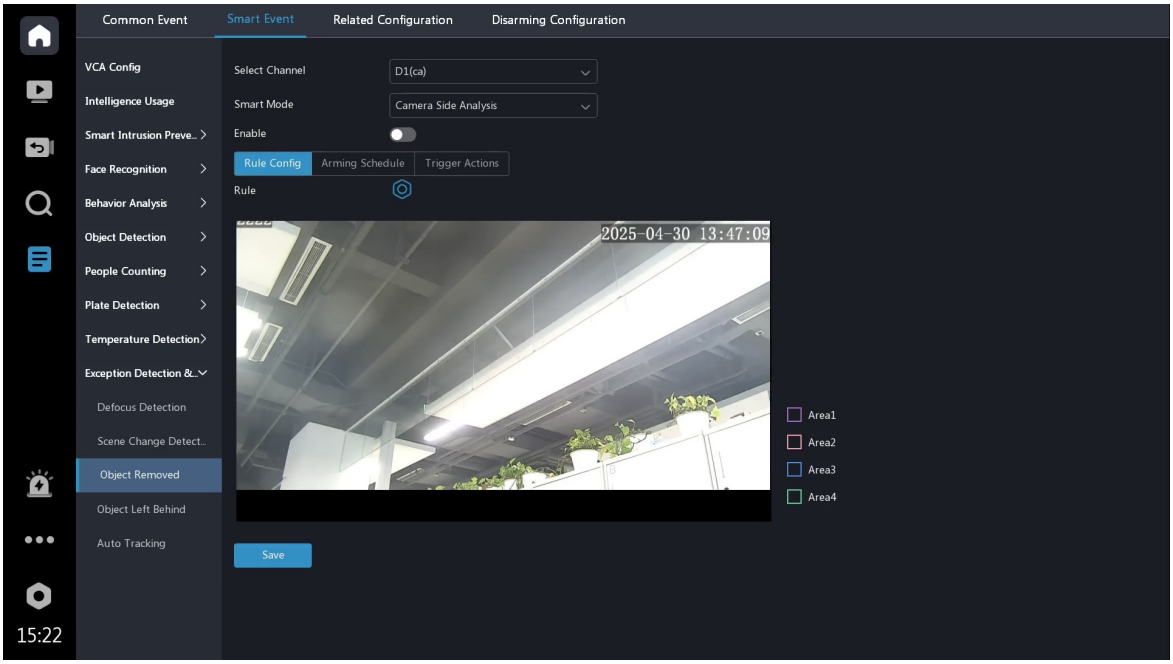


1. Select a channel and smart mode, and click  to enable the function.
2. Set the sensitivity. The higher the sensitivity, the more likely the detection will be triggered, but the false alarm rate will increase. Please adjust the based on the actual scene.
3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13.3 Object Removed

An alarm is triggered when the object is removed from a specified detection area for a preset time. The detection results can be viewed on the playback, camera alarm, and log pages. See Appendix for details on various search methods.

Note: If the surveillance scene changes, the device will detect objects based on the new scene.



1. Select a channel and smart mode, and click to enable the function.
2. Click , select an area, and configure the detection rule.

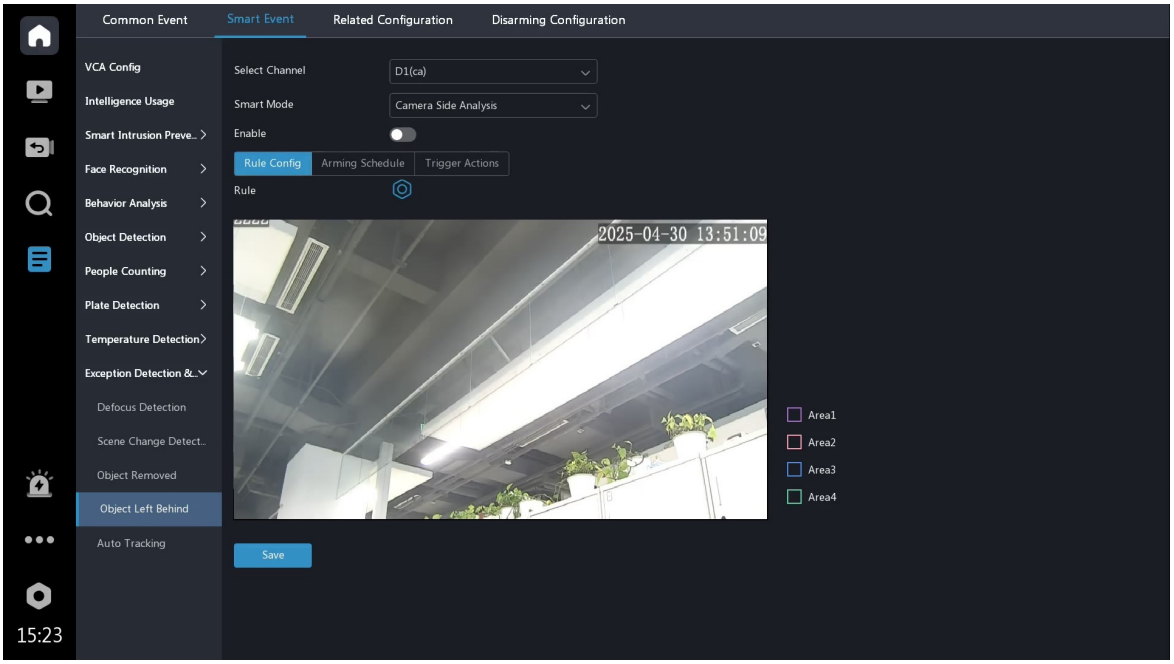
Parameter		Description
Draw Area		Draw the detection area with 3 to 6 sides Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area
		Click to delete the detection area
Time Threshold(s)		An alarm will be triggered if an object is removed from the detection area for the set time. Please adjust it based on the actual scene
Sensitivity		The higher the sensitivity, the more likely the detection will be triggered, but the false alarm rate will increase. Please adjust it based on the actual scene

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13.4 Object Left Behind

An alarm is triggered when the object is left behind in a specified detection area for a preset time. The detection results can be viewed on the playback, camera alarm, and log pages. See Appendix for details on various search methods.

Note: If the surveillance scene changes, the device will detect objects based on the new scene.



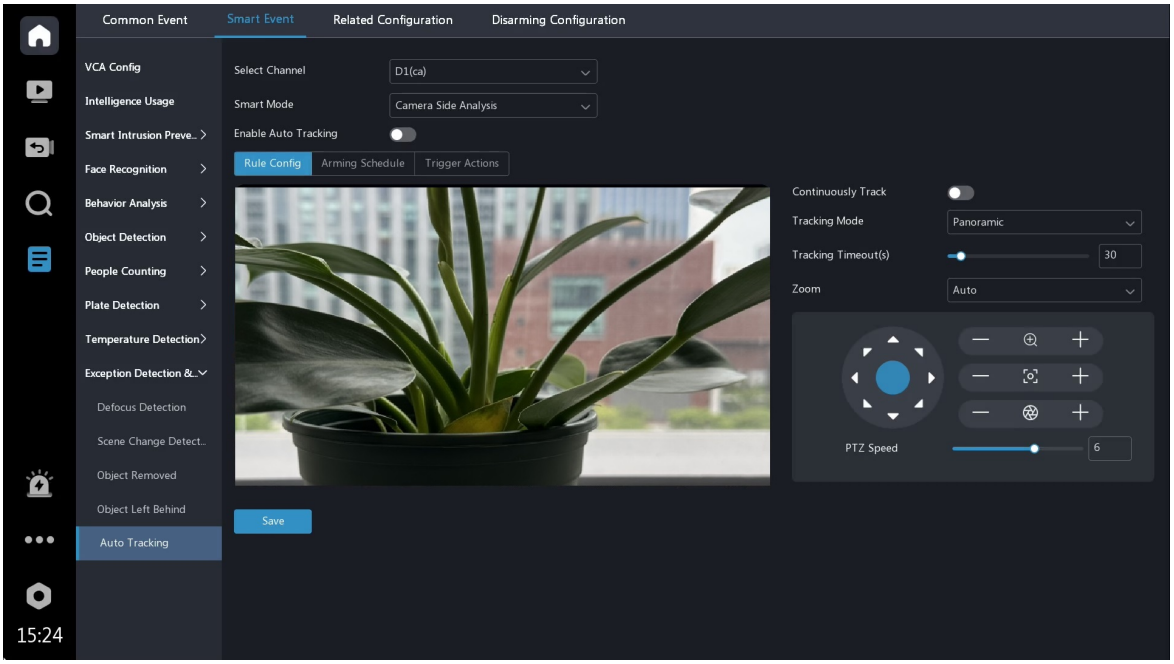
1. Select a channel and smart mode, and click to enable the function.
2. Click , select an area, and configure the detection rule.

Parameter		Description
Draw Area		Draw the detection area with 3 to 6 sides Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area
		Click to delete the detection area
Time Threshold(s)		If an object is left behind in the detection area for the set time, an alarm will be triggered. Please adjust it based on the actual scene
Sensitivity		The higher the sensitivity, the more likely the detection will be triggered, but the false alarm rate will increase. Please adjust it based on the actual scene

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13.5 Auto Tracking

This function automatically recognizes the moving targets on the live video and tracks the first target detected. The detection results can be viewed on the playback, camera alarm, and log pages. See Appendix for details on various search methods.



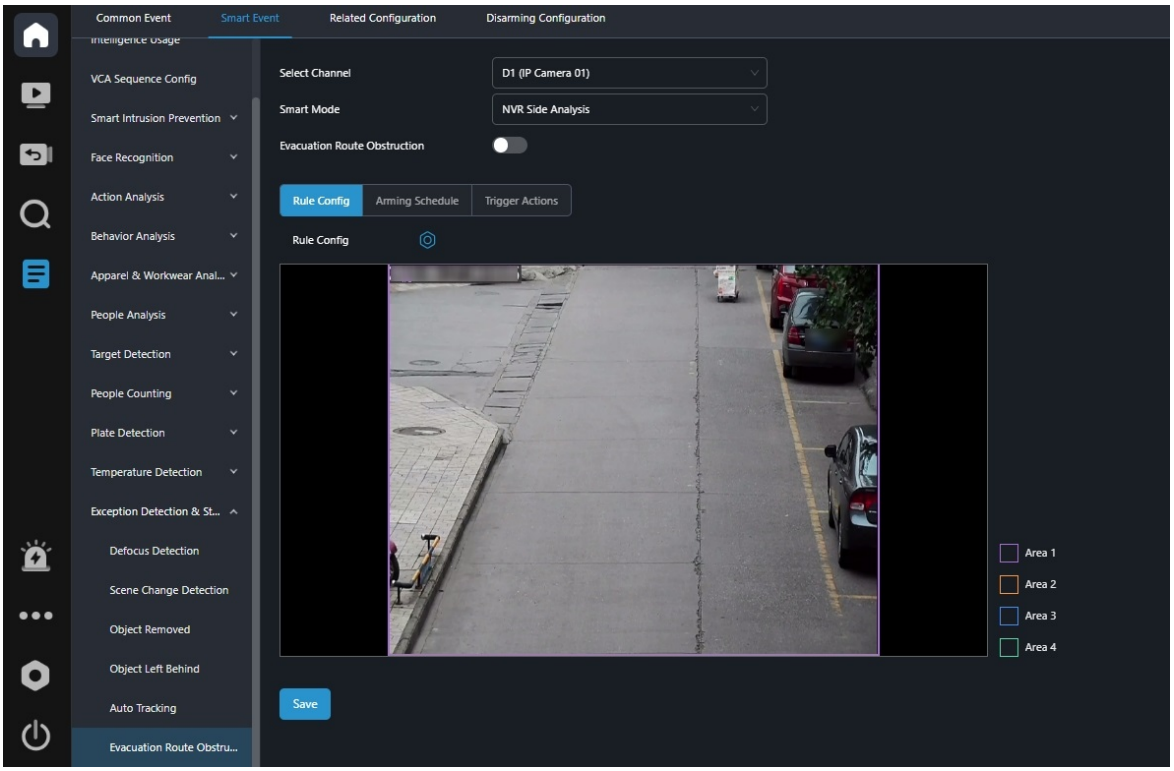
1. Select a channel and smart mode, and click  to enable the function.
2. Configure the detection rule.
   The local interface offers limited configuration options. To complete all configurations, please access the camera's web interface.

Parameter	Description
Continuously Track	The camera continuously tracks the target that triggers the tracking rule until the target disappears
Tracking Mode	Panoramic: The detection area is full screen
Tracking Timeout (s)	The camera stops tracking when the set time is reached
Zoom	• Auto: The camera automatically adjusts the zoom ratio according to the target distance during tracking • Current Zoom: The camera keeps the current zoom ratio during tracking
PTZ Configuration	Set the PTZ original position to which the camera will automatically return after the tracking target disappears

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.2.13.6 Evacuation Route Obstruction

This function triggers an alarm when a large target is detected on the evacuation route and it remains on the route for a certain length of time. The detection results can be viewed on the playback, event search, camera alarm, and log pages. Please see Appendix for various search methods details.



1. Select a channel and smart mode, and click to enable the function.

   Note: Please complete Analyzer Configuration if you select **NVR Side Analysis**.

2. Click and configure the detection rule.

Parameter	Description
Draw Area	Draw the detection area with 3 to 6 sides • Click , click on the image and drag to draw 3 to 6 lines to form an enclosed detection area • Click to delete the detection area
Alarm Interval	The device keeps analyzing the scene to assess the continuity of an ongoing behavioral event. This parameter can refrain the device from reporting the same alarm repeatedly within a specified time range
Duration(s)	Set the time threshold for escape route obstruction

3. Set Arming Schedule and Trigger Actions, and click **Save**.

6.3 Related Configuration

6.3.1 Email

See Send Email for details.

6.3.2 Buzzer

See Buzzer for details.

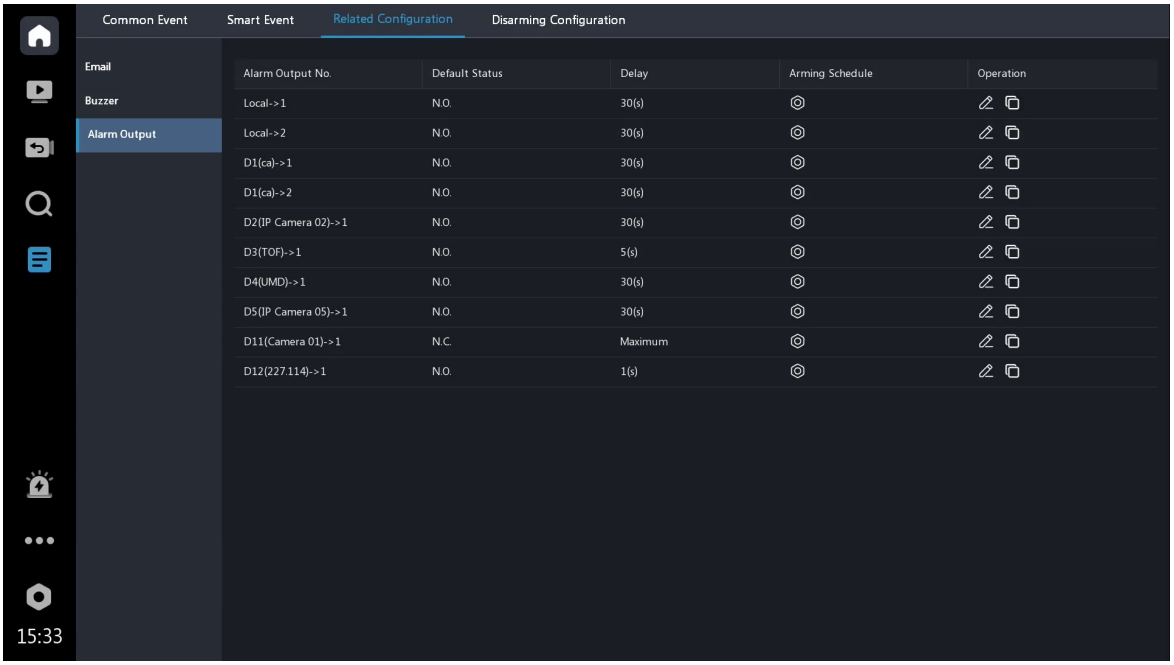
6.3.3 Alarm Output

Configure the alarm mode and arming schedule for external alarm output devices.

The external alarm output devices include devices connected to the alarm output interfaces on the NVR, cameras, and alarm expansion devices.

- External alarm device connected to the alarm output interface on the NVR: Local ->1 means the first ALARM OUT interface on the NVR. Likewise, Local ->1 means the second ALARM OUT interface on the NVR.
- External alarm device connected to the alarm output interface on the camera: D1 means the camera that added to the channel 1. D1->1 means the first ALARM OUT interface of the camera whose channel ID is 1. Likewise, D1> -2 means the second ALARM OUT interface of the camera of the camera whose channel ID is 1.
- External alarm device connected to the alarm output interface on the alarm expansion device: M1 means the first alarm expansion device. M1->1 means the first ALARM OUT interface of this alarm expansion device. Likewise, M1->2 means the second ALARM OUT interface of this alarm expansion device.

Note: The alarm output channel is not displayed if the NVR or camera has no ALARM OUT interface.



1. Click to configure alarm parameters.

Parameter	Description
Default Status	The default is **N.O.**. Select the status as needed • N.O.: Choose this option if the external device is normally open • N.C.: Choose this option if the external device is normally closed
Alarm Duration	• Custom: When enabled, you can set the length of time as needed. After an alarm is cleared on the NVR, the third-party alarm device continues alarm till the end of the set duration • Maximum: When enabled, you cannot set the delay period. The third-party alarm device continues alarm until you clear it manually

2. Set Arming Schedule.

6.3.4 Arming Schedule

The event detection function will take effect during the time periods specified in the arming schedule.

A 24/7 arming schedule is enabled by default.

Note:

- The number of arming time periods available varies by function and device.
- If a SIP camera is connected to the NVR and configured with camera side analysis of **Intrusion Detection**, **Cross Line Detection**, **Enter Area**, **Leave Area**, or **Human Body Detection**, the arming schedule configured for these functions on the NVR will be synced to the camera.

Draw a Schedule

The drawing area uses a 24-hour timeline as the x-axis and days of the week/holidays as the y-axis, with each day divided into 1-hour time grids. Set the arming schedule by clicking and dragging on the time grids.

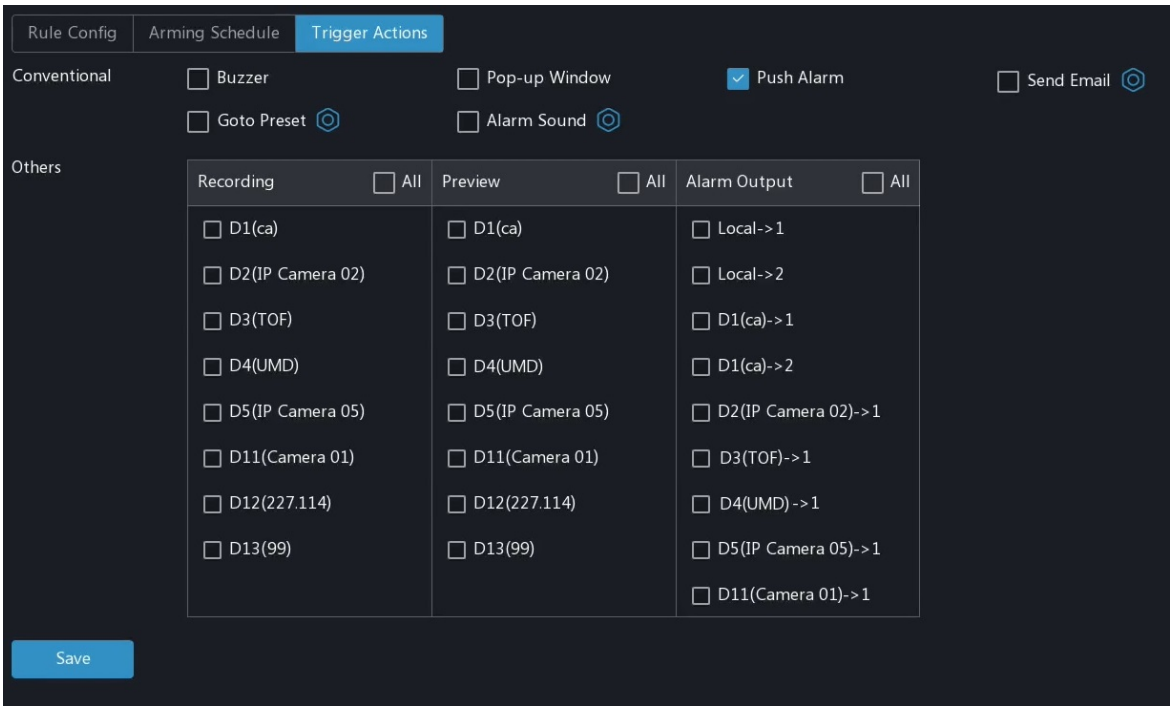
1. Click **Armed** or **Disarmed**.
2. Click or drag on blank areas to draw grids. Hover over the grid to show the corresponding time period information.
3. (Optional) If the schedule does not start or end at a whole point, hover over the drawing area and modify the time period as needed.

Edit a Schedule

1. Click , and set the arming schedule as needed.
2. Select a day or holiday, and set the start time and end time for arming time periods.
3. (Optional) To apply the same schedule to other days or holiday, select the desired day(s) or holiday, and click **OK**.

6.3.5 Trigger Actions

Set actions to be triggered when an alarm occurs to alert user or the specified people.



Buzzer

The NVR makes a buzzing sound when an alarm occurs.

You can change the alarm mode and duration at **Event** > **Related Configuration** > **Buzzer**.

- Custom: Set the alarm duration as needed. When an alarm occurs, the buzzer will alarm continuously within the alarm duration, and stop automatically if the alarm ends first within the duration.
- Maximum: When an alarm occurs, the buzzer will alarm continuously.
  - No new alarm: For example, when the storage array fully degrades, the alarm will persist for up to 600 seconds.
  - With new alarm: The buzzer stops if a new alarm occurs; otherwise, it will alarm continuously.
  - Illegal access (subsequent login attempt after 5 consecutive invalid password attempts): Trigger 3 consecutive buzzer beeps.

Note: To stop a buzzer alarm manually, see Manual Operations for details.

Pop-up Window

When an alarm occurs, a pop-up window will appear on the preview page displaying the event type, camera information, and alarm time. You can also view the alarm recording.

Note:

- Up to 10 latest alarms will be displayed.
- The pop-up window must be confirmed or closed manually.
- After the pop-up window is closed, you can search for alarms in Log.

Push Alarm

An alarm information will be pushed to the upper platform when an alarm occurs.

Including UMS, VMS, EZStation, VM, VMP, UCS, app, etc.

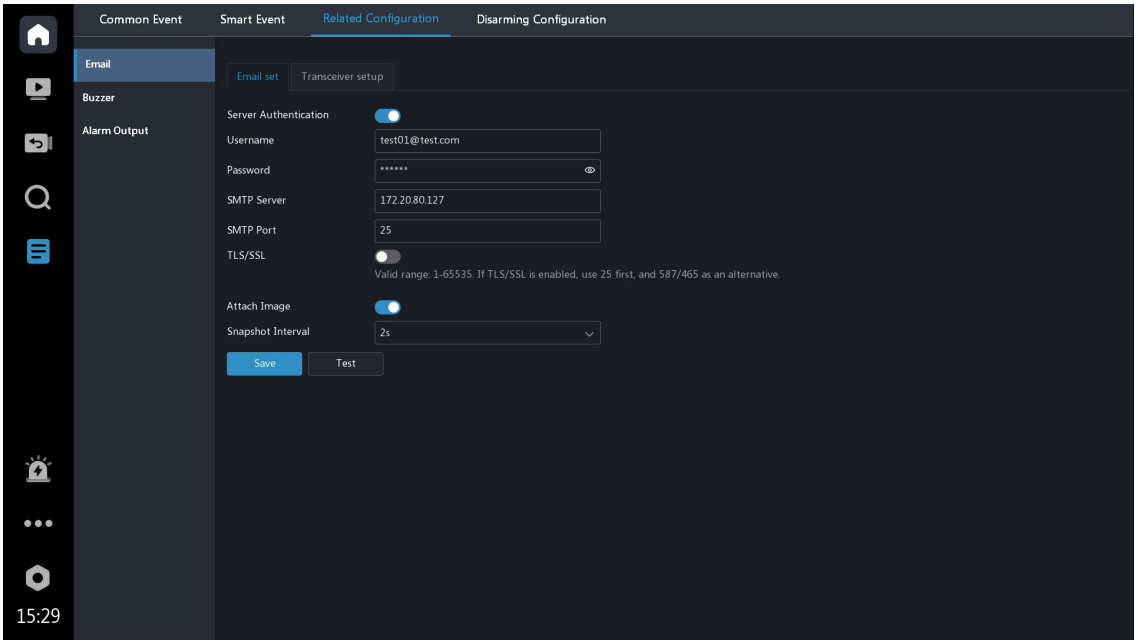
This function is enabled by default.

Note: Besides alarm messages, some smart events can push snapshots, detection properties, etc.

Send Email

When an alarm occurs, the system sends an email with alarm information to the recipient's mailbox through the set sender.

1. Configure email at **Event** > **Related Configuration** > **Email** before use.



Parameter	Description
Server Authentication	When enabled, the email can be sent correctly and reliably from sender to recipient
Username/Password	Username and password of the SMTP server. Usually it is the username and password of the email box
SMTP Server	SMTP server address provided by the mailbox service provider
SMTP Port	Use the default port
TLS/SSL	When enabled, communication security will be improved by encrypting emails via TLS or SSL. This feature requires the SMTP server to support TLS/SSL
Attach Image	When enabled, the NVR will send an email attached with alarm information and snapshot(s) when an alarm occurs **Note:** This feature is only available for certain VCA functions.
Snapshot Interval	The time interval between consecutive captures of the same alarm target

2. Enter the **Transceiver setup** tab, enter the sender and recipient information. Up to 6 recipients are allowed.

   Note: The recipient's address can be the same as the sender's address.

3. Click **Test**, and the system will check the recipient address by sending it a test email.
4. Click **OK** to save the settings.
5. Return to the **Trigger Actions** page, click , and enable monitoring channel for the recipient(s) desired.

Goto Preset

A PTZ camera moves to a preset position when an alarm occurs. It is recommended to be used with Recording, which allows users to store or view live video conveniently.

1. Configure the presets for the PTZ camera in PTZ Configuration before use.

   Note: The NVR cannot obtain presets configured on the camera's web interface, but all presets configured on the NVR will sync to the connected cameras.

2. Click , select the preset for the camera you want to perform the action, and enable **Operation**. Multiple PTZ cameras are allowed.

Alarm Sound

The selected IP speaker plays alarm audio when an alarm occurs.

Click , enable **IP Speaker**, select the audio file, and set the repeat mode as needed.

Camera Alarm Sound

The selected camera plays an audio alarm when an alarm occurs.

1. Click , and select the alarm mode.
   - Custom Mode: Set the start time and end time in which the camera plays the alarm sound at the specified duration.

     Note: Up to 4 time periods are allowed per day, and the time periods cannot overlap.
   - Day/Night Mode: Select day or/and night mode(s) during which alarm sound is enabled. The camera automatically switches to day or night mode based on the ambient brightness.

     Note: The day/night mode is available on certain cameras only.

Parameter	Description
Audio	Select the audio file to be played by the camera when an alarm occurs. The audio files should be configured on the camera's web interface **Note:** The number of default audio files varies depending on the camera model. Only certain cameras support audio file import.
Repeat	The number of times the audio file to be played when an alarm occurs

2. (Optional) To apply the same settings to other days, select **All** or the desired day(s) after **Copy To**.

Camera Flashing Light

The illuminator of the selected camera flashes when an alarm occurs.

1. Click , select the alarm mode, and set the blink time.
   - Custom Mode: Set the start time and end time in which the camera flashes at the specified duration.

     Note: Up to 4 time periods are allowed per day, and the time periods cannot overlap.
   - Day/Night Mode: Select day or/and night mode(s) during which alarm sound is enabled. The camera automatically switches to day or night mode based on the ambient brightness.

     Note: The day/night mode is only available to certain cameras.
2. (Optional) To apply the same settings to other days, select **All** or the desired day(s) after **Copy To**.

Recording

Recording should be enabled for recording search on the playback, video search, event search, and target search pages. Select the linked camera(s) to store recordings when an alarm occurs.

Note: Some VCA functions can view the corresponding recordings via snapshots from event/target search, even if **Recording** is disabled.

- Preparation: Please make sure Recording Schedule is enabled for the cameras that require recording storage.
- Linkage: Multiple cameras can be linked for event-triggered recordings from various viewpoints.

Preview

The NVR plays the live video of the specified camera(s) when an alarm occurs.

- To perform this action, configure **Max. Alarm-Triggered Live View Windows** (1/4/9 available) in Preview Configuration first.
- When an alarm occurs, the live view page shows the live video from the linked camera(s) with a red frame; when the alarm ends, the live view page returns to the original state.

Max. Alarm-Triggered Live View Windows	Description
1 Window	The live view page plays live video in one window. If more than one camera is linked, the live video switches at 5s
4 Windows	The live view page plays the live video of each camera in 4-split mode. If more than 4 cameras are linked, the live video switches at 5s
9 Windows	The live view page plays the live video of each camera in 9-split mode. If more than 4 cameras are linked, the live video switches at 5s

Snapshot

The event-triggered snapshot in **Picture Search** requires **Snapshot** to be enabled. The NVR triggers the linked camera to capture a snapshot when an alarm occurs.

Note: Some VCA functions can retrieve snapshots without enabling **Snapshot**.

- Preparation: Make sure Snapshot Schedule is enabled for the cameras that require snapshot storage.
- Linkage: Multiple cameras can be linked for event-triggered snapshots from various viewpoints.

Alarm Output

A third-party device is triggered to raise an alarm when it receives an alarm output by the NVR.

HTTP

The third-party platform can set the information they want to receive via the HTTP protocol, such as alarm information, video loss information, etc.

Example of URL format: Http://platform address to receive alarm information/alarm channel/alarm type. The URL content is customizable. The alarm channel and alarm type in the example should be filled in according to the third-party platform's interface instructions.

Auto Tracking

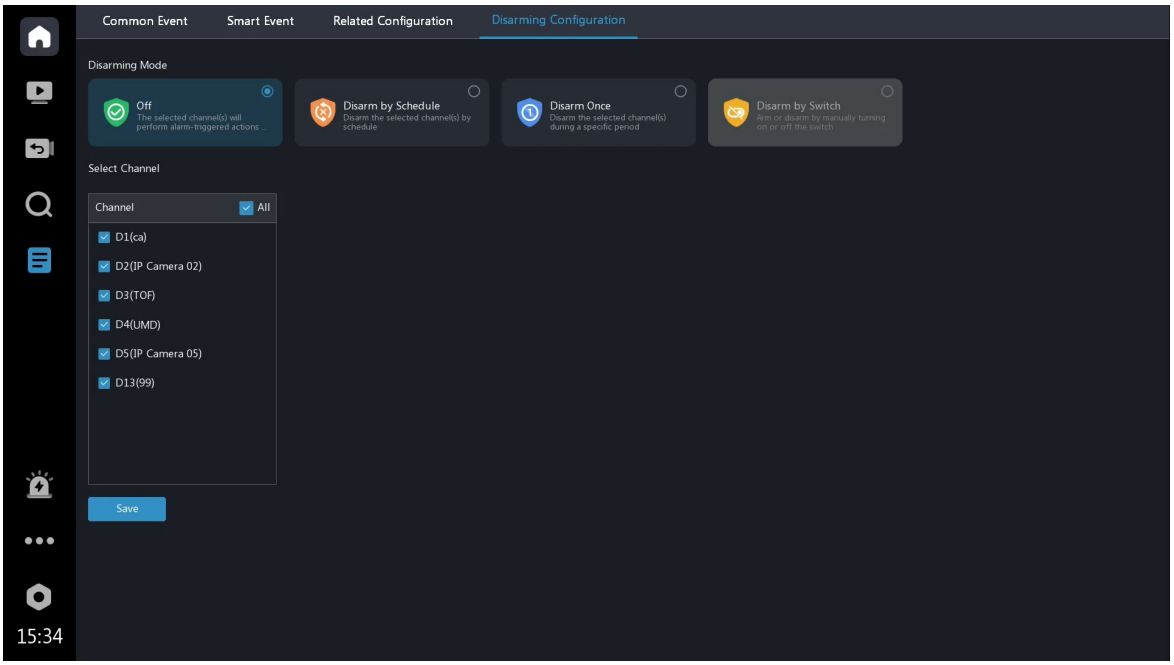
The camera will automatically track the alarm target when an alarm occurs.

Note: This function runs independently of Auto Tracking.

6.4 Disarming Configuration

Cancel alarm-triggered actions of NVRs or IPCs with one click.

Note: The alarm sound of the disarming actions means the IPC alarm sound.



Off

The device performs alarm-triggered actions according to the set arming schedule.

Note: Click on the preview page, and the disarming mode will be switched to **Disarm by Schedule**.

Disarm by Schedule

The device is disarmed during specific time periods per week.

1. Click **Disarm by Schedule**.
2. Select channels, actions, and outputs to be disarmed as needed.
3. Set Arming Schedule, and click **Save**.

Note: Click on the preview page, and the disarming mode will be switched to **Off**.

Disarm Once

The device is disarmed during a specified time period.

1. Click **Disarm Once**.
2. Set the disarming start time and end time, select channels, actions, and outputs to be disarmed as needed, and click **Save**.

Note: Click on the preview page, and the disarming mode will be switched to **Off**; click again to switch the disarming mode to **Disarm by Schedule**.

Disarm by Switch

It is required to enable **Disarm by Switch** for the alarm input interface on the NVR. See Disarm by Switch for details.

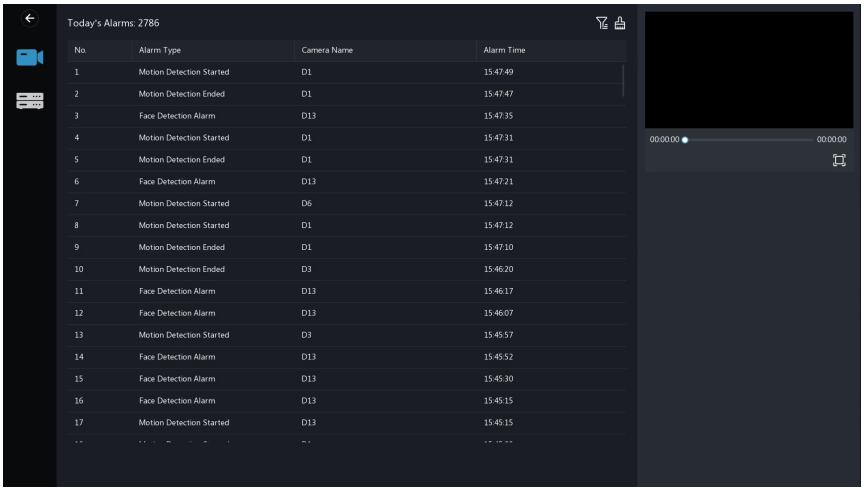
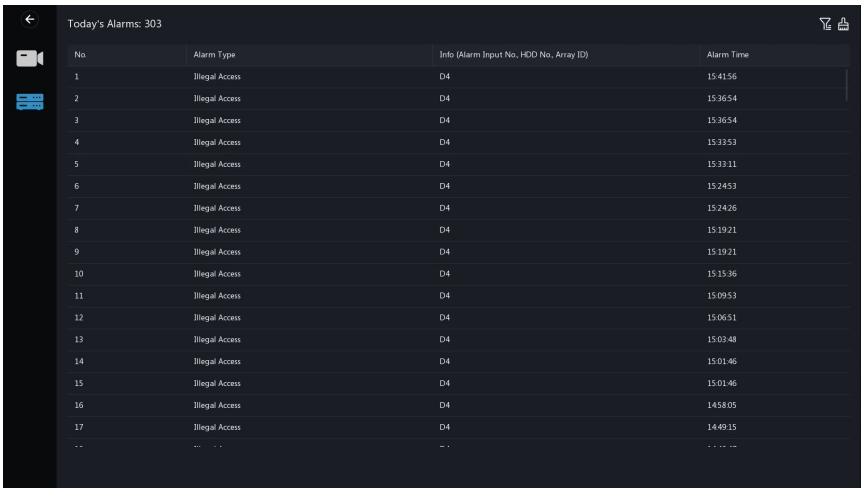
1. The disarm by switch mode cannot be controlled on the local/web interface manually. When the Local <-1 port receives the alarm input signal, the disarming mode will automatically switch to **Disarm by Switch** and return to the original mode once the alarm signal is restored.

   Note: You can also switch to other available modes manually.

2. Select channels, actions, and outputs to be disarmed as needed.

Note: Click on the preview page, and the disarming mode will be switched to **Off**; click again to switch the disarming mode to **Disarm by Schedule**.

7 Alarm

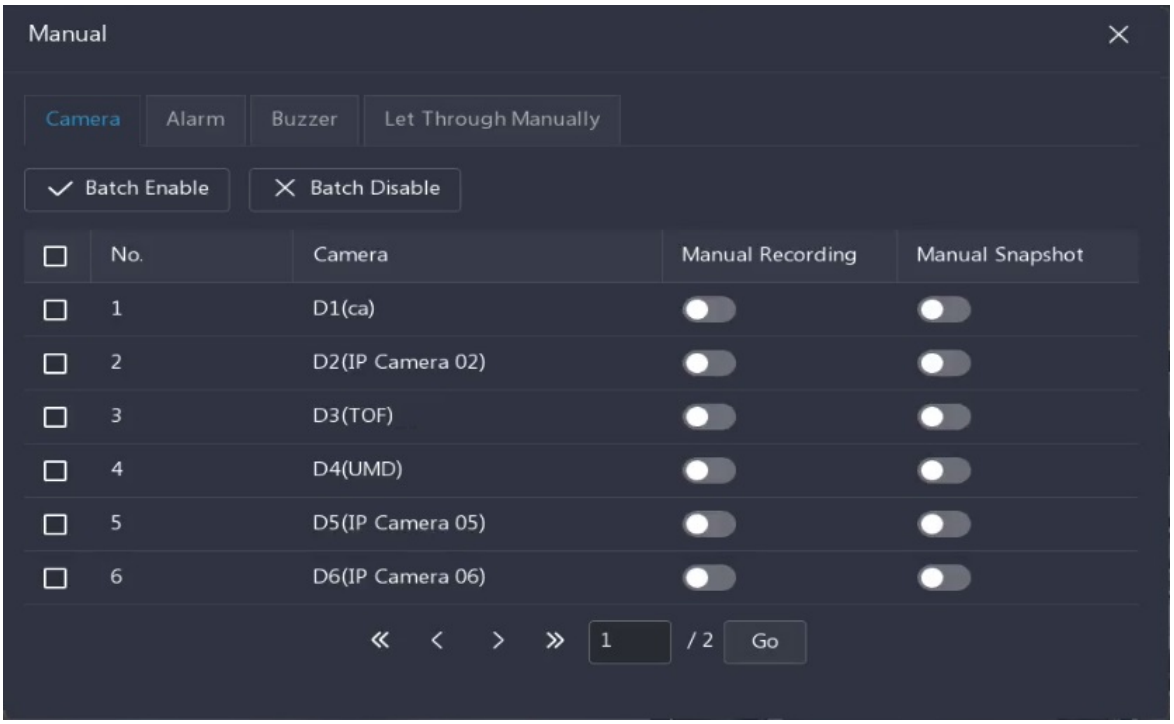
Alarm Type	Description
Camera Alarm	Display today's alarms for all cameras in real time, with the option to view alarm recordings 
Device Alarm	Display today's alarms for the device in real time 

- : View today's alarms by the alarm type.
- : Clear all alarm messages displayed on the current screen.

8 More

8.1 Manual Operations

Note: It is named **Manual** on the web interface.



Camera

Enable/disable **Manual Recording** or **Manual Snapshot** as needed.

- Manual Recording: Manually trigger recording for one or multiple channels, with controllable start time and duration as needed. This recording can be searched through the **Manual** recording type filter in video search, or viewed on the normal playback page. This is the same function as **Start Local Recording** on the preview page, with synced on/off status for single-channel recording.
- Manual Snapshot: Manually trigger continuous snapshots for one or multiple channels, with the interval time consistent with that set in event snapshot in Snapshot Schedule.

Note: When enabled, snapshots will be captured continuously. Please disable the function when no longer needed.

Alarm

You can trigger alarm output(s) manually.

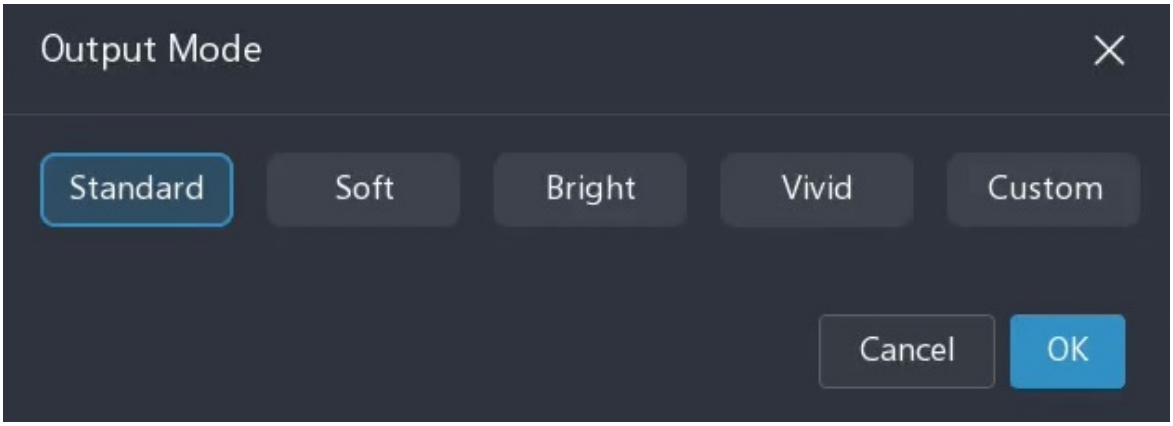
Buzzer

You can disable buzzer alarm manually.

Let Through Manually

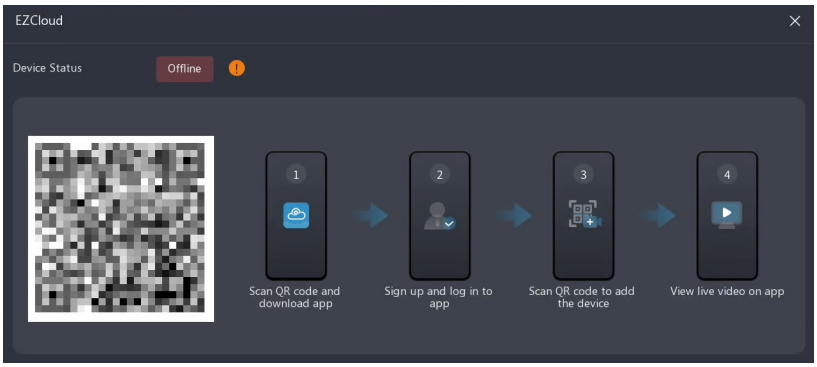
If a license plate not match alarm occurs and the barrier fails to open automatically, you can trigger the camera to lift the barrier(s) manually.

8.2 Output Mode



The output effect displayed on the local interface.

8.3 EZCloud



Follow the on-screen instructions to add the device to EZCloud.

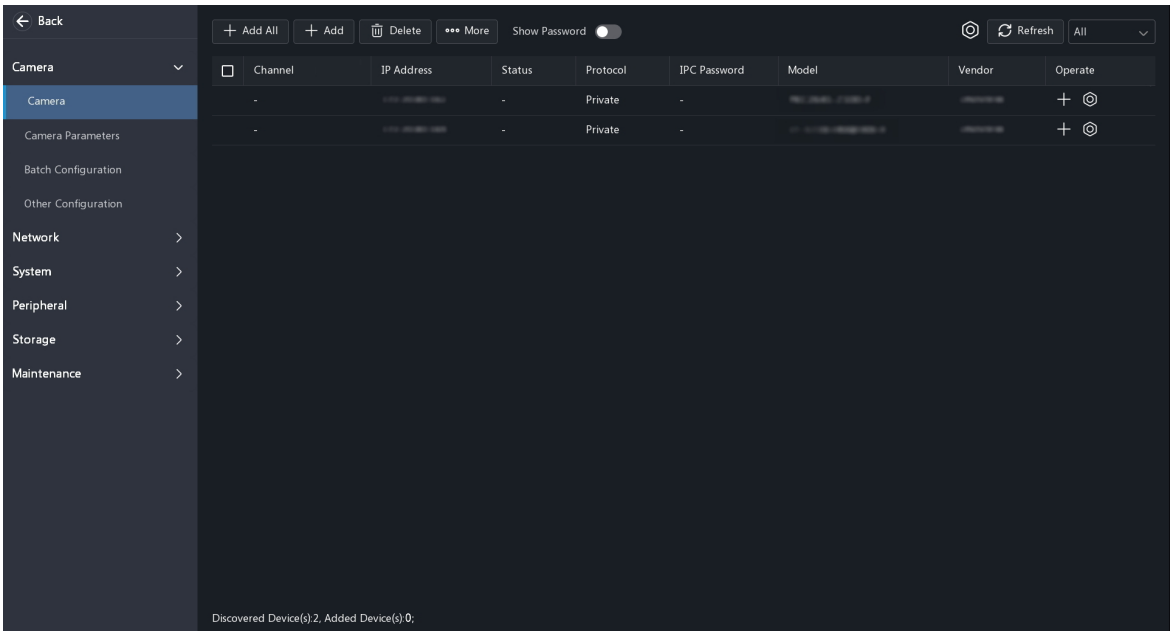
8.5 Main/Aux Monitor

When two or more video output interfaces of the devices, such as HDMI and VGA, are connected to the monitor, you can switch mouse control between the main monitor and auxiliary monitor. The synchronization of display effects between multiple monitors depends on the output mode of multiple video interfaces.

9 Settings

9.1 Camera

9.1.1 Camera Management



9.1.1.1 Add Camera

The device supports four ways to add cameras: auto-search, add one by one, batch import, and plug-and-play. It is advised to connect each camera to only one device to avoid management confusion.

Note: Before adding a camera, please ensure network connectivity between the camera and the device.

The device supports adding cameras from both LAN and WAN. However, alarms from WAN or cross-WAN cameras may fail to be sent to the device.

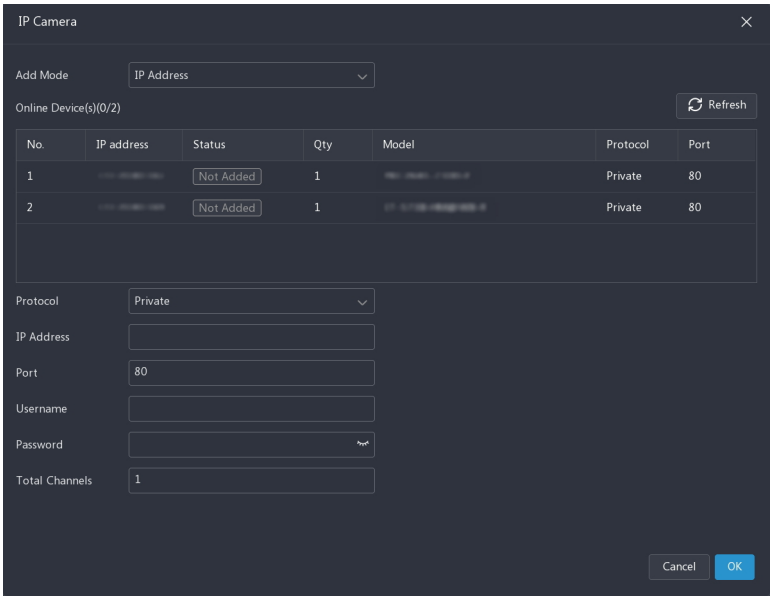
For a camera to successfully send alarms to the NVR across NAT, the camera's IP address and port must be reachable by the NVR.

Note: The alarm listening port for the NVR is 20002. The port number increments by 2 for each additional channel subscription.

Networking Type	Analysis	Result
The NVR and cameras are behind different NATs	• When the NVR subscribes to camera alarms, the subscription address is the NVR's private IP address, therefore it is unreachable • The NVR's alarm listening port is not mapped, therefore it is unreachable	The NVR cannot receive alarms from cameras
The NVR is behind NAT, while the cameras are outside the NAT	• When the NVR subscribes to camera alarms, the subscription address is the NVR's private IP address, therefore it is unreachable • The NVR's alarm listening port is not mapped, therefore it is unreachable	The NVR cannot receive alarms from cameras

Networking Type	Analysis	Result
The NVR is outside the NAT, while the cameras are behind NAT	• When the NVR subscribes to camera alarms, its IP address is reachable from outside the camera's NAT • The alarm listening port is reachable from outside the NAT	The NVR can theoretically receive alarms from cameras, but certain gateway restrictions may cause anomalies

9.1.1.1.1 Add Cameras One by One



1. Click **Add**.
2. Choose a method to add the camera.

Method	Applicable Networking	Notes

IP Address	• Add LAN camera
	• Add WAN camera
	• Add cross-WAN camera
	  • The camera needs to enable port forwarding.
	  • The camera only supports 1-layer NAT traversal
	Note: When adding WAN or cross-WAN cameras, ensure that the NVR has WAN access.
		-

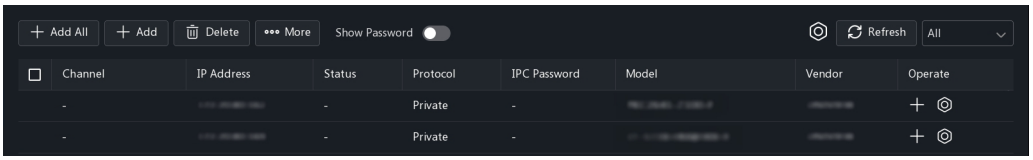
EZDDNS/Domain Name		The following two scenarios can use this method to add cameras: • Adding the camera using a domain name • Dynamic camera address; before adding the camera, ensure that DDNS is enabled on the camera

3. Configure other parameters.

Parameter	Description
Protocol	The protocol used to connect the camera to the device. Pay attention to the following before use • Private: Used to add our company's cameras. If you need to use the smart functions of our company's cameras, select the Private protocol • Custom: Add cameras using the RTSP protocol supported by the camera brand. Cameras added via custom protocols only support live view and playback; configuration is unavailable
IP Address	Camera's IP address
Server Address	DDNS server's IP address

Parameter	Description
Domain Name	Camera's domain name
Port	Camera's port
Username/Password	Username and password used to log in to the camera
Total Channels/Select Channels	For multi-channel cameras, you need to specify the total number of remote channels and select the channels to be added to the device

9.1.1.1.2 Add Cameras by Auto Search (applicable to non-PoE models and semi-PoE models)

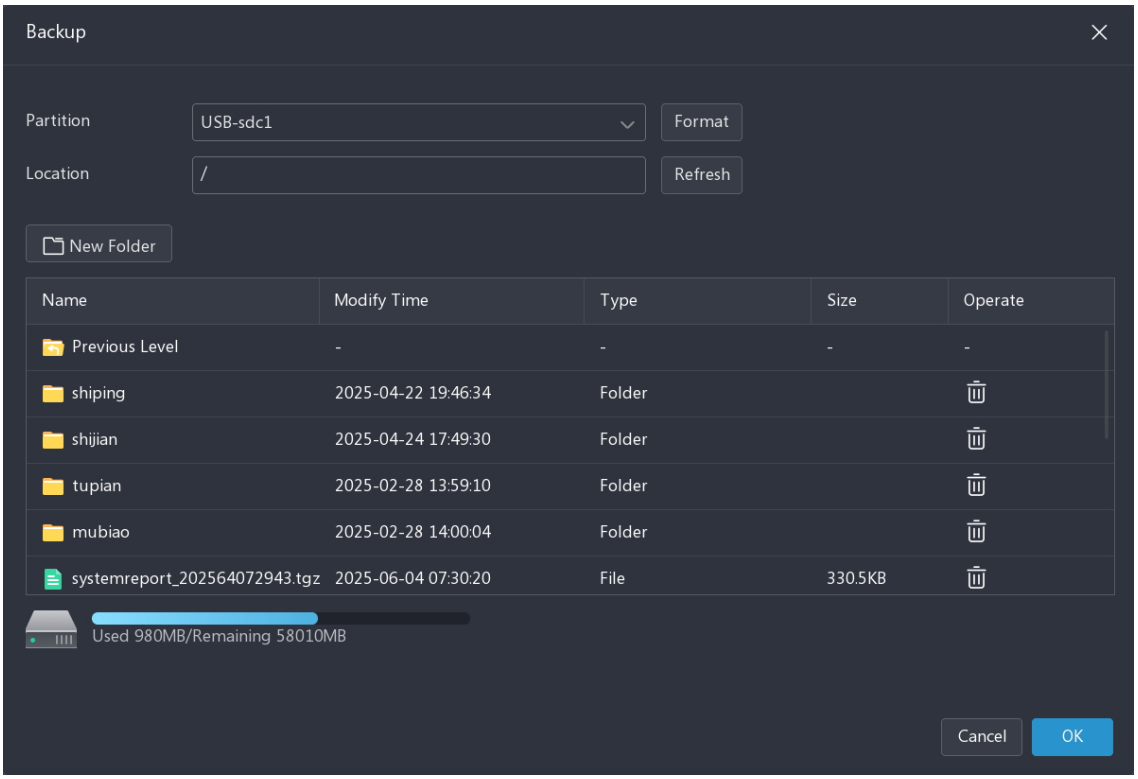


Method	Step 1: Search cameras	Step 2: Add cameras
Automatically search and add cameras in the same network segment	By default, the device automatically searches for all cameras in the same network segment as the device and displays them on the **Camera** page	• Add one camera: Click the corresponding ➕ to add the camera • All cameras: Click **Add All** to add cameras in the displayed order, up to the total number of channels supported by the device **Note:** The device uses the default password 123456 to add the automatically discovered cameras. If a camera fails to go online, you can click ✏ and change 123456 to the correct login password of the camera in order to bring it online.
Automatically search and add cameras in the specified network segment	1. Click **More**, and select **Search Segment** 2. Enter the IP addresses 3. Click **OK** to start searching	

9.1.1.1.3 Add Cameras by Batch Import

Note: A USB drive is required for the local interface (not for the web interface).

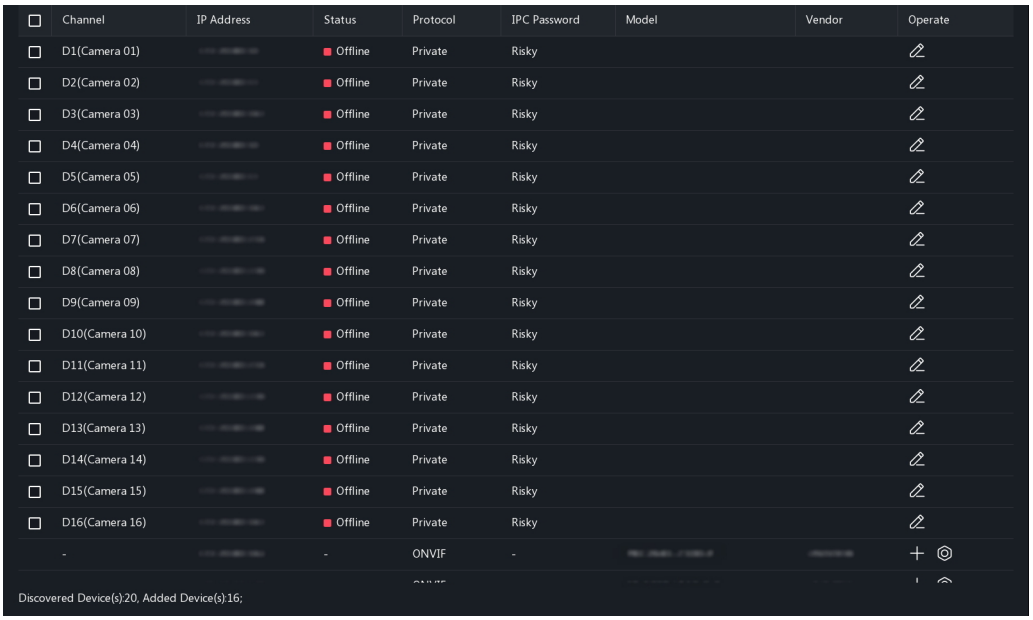
1. Insert the USB drive into the device, choose **More** > **Export**, choose the export path, and then click **Backup** to export the template.



2. Insert the USB drive into the computer, open the template file, and fill in camera information.
3. Insert the USB drive back into the device, click **More** > **Import**, select the template file, and then click **Import** to batch add cameras.

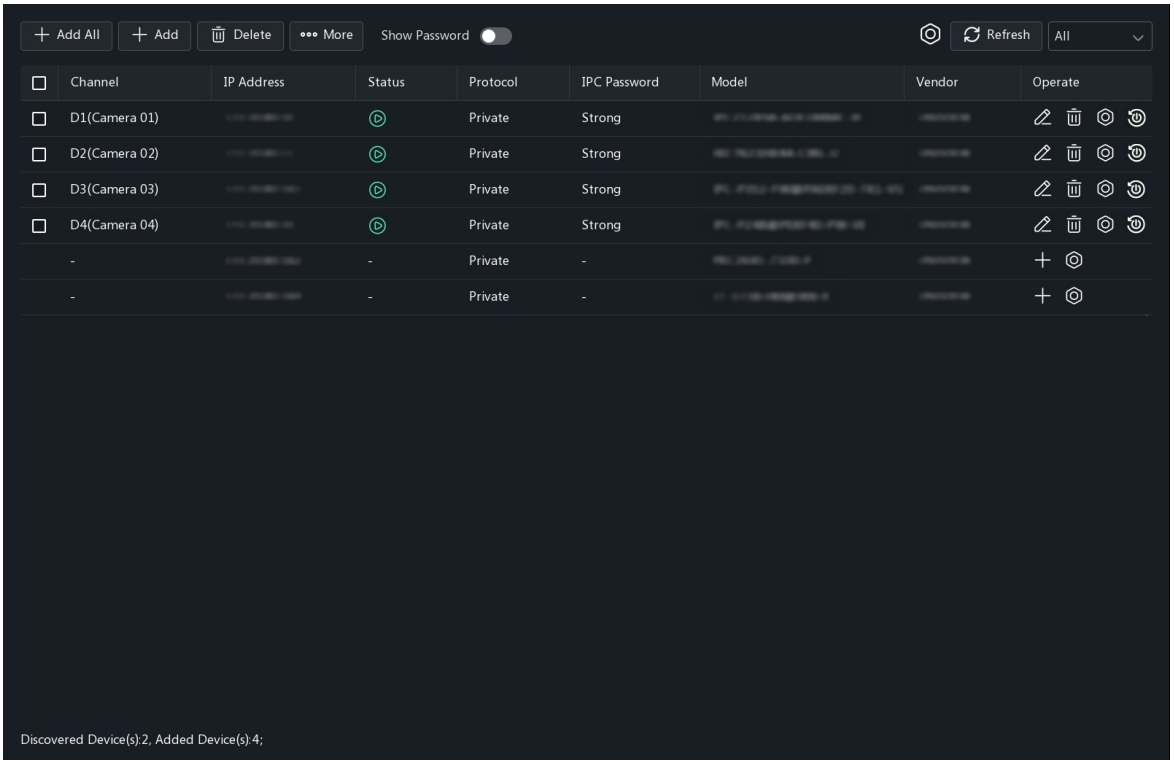
9.1.1.1.4 Add Cameras by Plug and Play (applicable to PoE Models)

Add cameras to the device by connecting cameras to the PoE ports of the device with Ethernet cables. The network port IDs correspond to the channel IDs.



Apart from directly connecting cameras with Ethernet cables, you can also click  to choose other methods, such as using an IP address, to add cameras.

9.1.1.2 Manage Camera



Parameter	Description
Channel	On the web interface, you can click the camera name to enter the camera's login page
/Delete	Click to delete a camera, or select multiple cameras and click **Delete** to delete the selected cameras

Parameter	Description	
More	Sort Camera	Adjust the channel IDs and their display order on the camera page and preview page • Total number of cameras ≤ 32: 1. Drag the camera to the desired position 2. Right-click to confirm • Total number of cameras > 32: • Method 1: Hold down and drag the camera up or down, and then click **Save** • Method 2: 1. Click to change the camera to "waiting to be sorted" status, leaving its original ID blank 2. Click to insert the "waiting to be sorted" camera into the first blank line, and repeat the process until there are no more cameras waiting to be sorted 3. Click **Save** **Note:** • If there are cameras waiting to be sorted, the configuration cannot be saved. • After adjusting the channel IDs, the correspondence between historical recordings and cameras will change, and the currently enabled smart functions will be effective after re-configuration. • This feature is not available to PoE model. • This feature is not available on the web interface.
	Batch Change Camera Password	If multiple cameras with the same password fail to go online because of incorrect passwords, you can use this feature to change the passwords in batches to the correct login password **Note:** This feature will not change the camera's login password.
	Default Password	The startup wizard and auto-search-and-add features add cameras using the default password 123456. If the camera's login password is not 123456, you can use this feature to change the default 123456 to the actual login password of the camera, which will then be used for adding subsequent cameras
Show Password	Click to enable this feature, enter the device password, and then you can view the password of all cameras in plain text. Click to disable this feature **Note:** This feature is only available to the admin user on the local interface.	

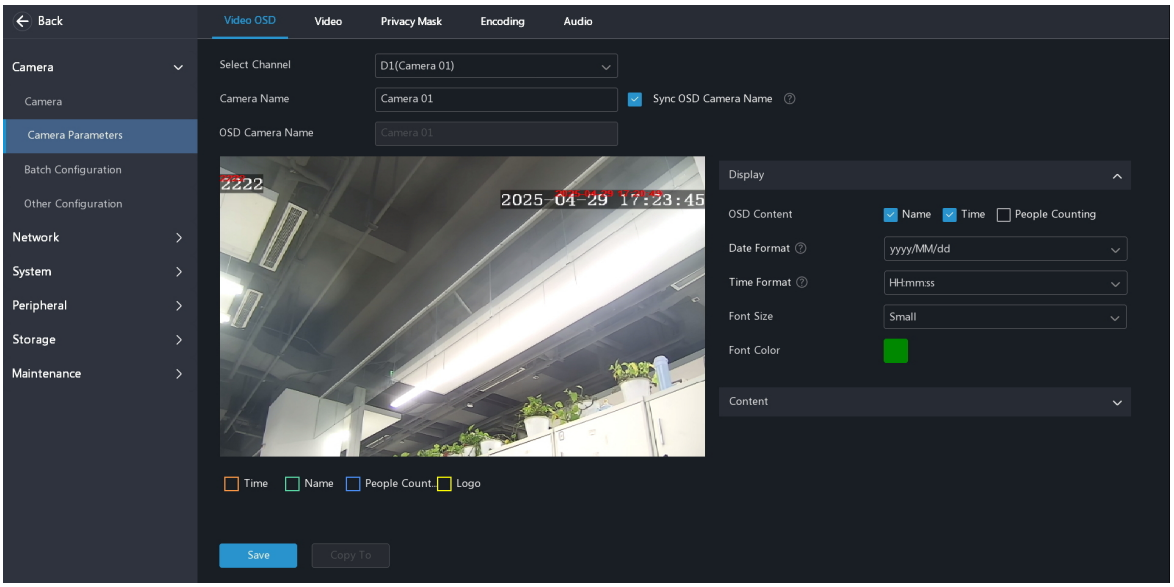
Parameter	Description	
	Auto Switch to U-Code	This feature helps save storage space and bandwidth by using more efficient compression techniques while ensuring video quality. If this feature is enabled, cameras will automatically switch to the corresponding mode upon first connection to the device • Off: This feature is turned off, and the cameras retain their individual settings • Basic Mode: Offers low compression rate with excellent video quality • Advanced Mode: Offers a high compression rate, with slightly lower video quality compared to the Basic Mode **Note:** Whenever a camera is added to the device, it is treated as the first connection. Cameras that have already been added, as well as those that were added, went offline, and then came back online, will not switch modes automatically
Refresh	Refresh the display	
All/Offline/Not Added	Shows cameras in the corresponding status	
	Restart device	
Status	• : The camera is online. You can click to view the live video from the camera • Offline: The camera is offline. You can hover over the icon to view the reason, and click to view the solution • : The camera has been added to another device. You can hover over the icon to view that device's IP address • : The camera is not added	
Operation	• : Modify protocol, password, and other camera information • : Modify the camera's IP address and other network settings	

9.1.2 Camera Parameters

Note: After configuring and saving camera parameters, you can click **Copy To** to copy the selected contents to other cameras.

9.1.2.1 Video OSD

Configure the style and content of OSD on the images of different cameras.

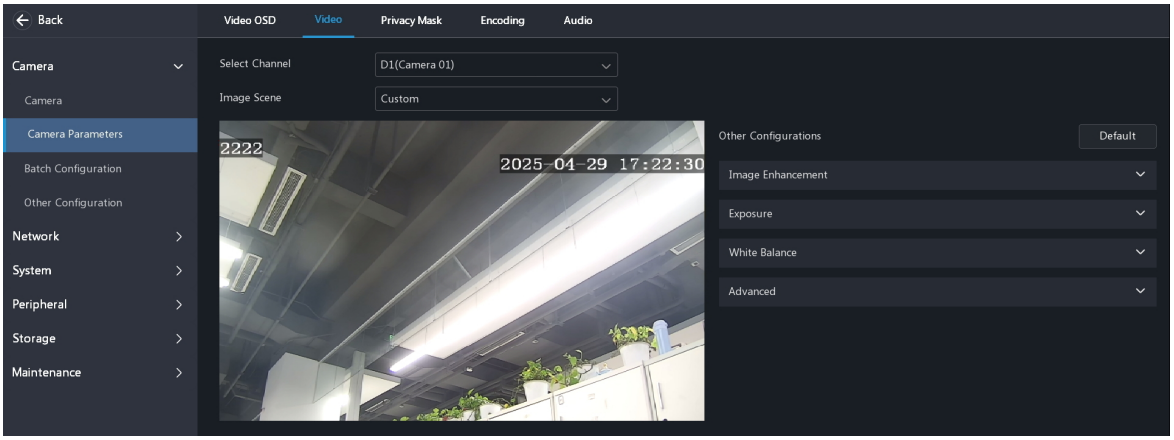


1. Select the channel and configure the parameters as needed.

Parameter	Description
Camera Name	Camera names are automatically assigned and displayed by default on camera related pages (e.g., camera management, preview). The camera names can be changed as needed to distinguish between multiple cameras
OSD Camera Name/ Sync OSD Camera Name	The camera name displayed on the video image, helps quickly distinguish between different cameras during live view and playback. The default OSD camera name is the camera name; to set a custom OSD camera name, deselect **Sync OSD Camera Name**
Display	Configure the OSD display content and style • OSD Content: Select the OSD content to display, including OSD camera name, device time, and people counting (requires the configuration of People Flow Counting event, including people entered and exited) You can drag the OSD box on the left preview image to adjust the OSD display position • Date Format/Time Format: Set as needed • Display Logo: Set as needed (supported by some cameras only) • Font Size/Font Color: Set as needed
OSD Overlay	Enable and customize other OSD content as needed

2. Click **Save**.

9.1.2.2 Video Parameters



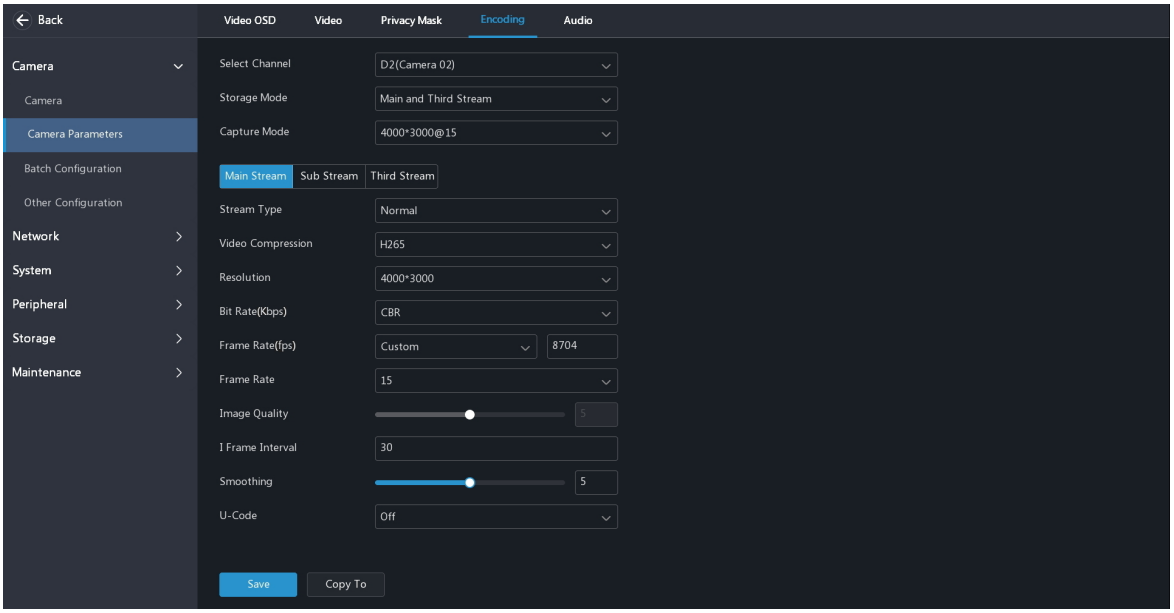
Select the channel, and then select the desired scene.

- Custom: Custom image effects
- Indoor: Suitable for indoor scenes
- General: Suitable for outdoor scenes
- Starlight: Suitable for low-light scenes, enhancing brightness and clarity
- Road/Park Highlight Compensation: Suitable for road/park scenes with strong direct light (e.g., vehicle headlights) to reduce glare and capture clear license plates
- Wide Dynamic Range (WDR): Suitable for high-contrast scenes by dynamically balancing bright and dark areas in real time
- Face: Suitable for scenes requiring face capture
- Mixed traffic: Suitable for road scenes with motor vehicles, non-motor vehicles, and pedestrians
- Perimeter: Suitable for scenes where perimeter detection is required
- Standard: Suitable for most scenes
- Bright: Enhance image brightness based on the Standard mode
- Vivid: Improve the vividness of the image colors based on the Standard mode
- Test: For testing objective metrics (not recommended for normal use)

Note: You can choose scenes when only the camera is added via the private protocol. Different scenes correspond to different image effects (different image settings). You can use the default settings or make adjustments as needed. Clicking **Default** will restore default settings for the selected scene.

9.1.2.3 Encoding Parameters

Configure the stream parameters sent from cameras and the way the device stores streams.



Stream Parameters from Camera

Parameter	Description
Capture Mode	The maximum resolution and frame rate of videos captured by the camera. The resolution and frame rate of each stream cannot exceed those set by the capture mode **Note:** The capture mode is configurable only when the camera is added via the private protocol.

Parameter	Description

Main Stream	The video quality of the main stream, sub stream, and third stream decreases progressively. You can use the default settings or adjust them as needed.
	To adjust the settings, select the stream type first, and then proceed to the parameters below (you can configure parameters for scheduled, event, and network transmission recordings separately)
	• Main Stream:
	  • Scheduled: General main stream parameters
	  • Event: Main stream parameters for event recordings (if you prefer better video quality for event recordings over general recordings, you can increase the bitrate and frame rate accordingly)
	• Sub/Third Stream: For network transmission, with general sub/third stream parameters
	Note: By default, the camera sends the main stream to the device. You can select the stream type on the camera's web interface.

Sub Stream	
Third Stream	

Stream Storage Mode

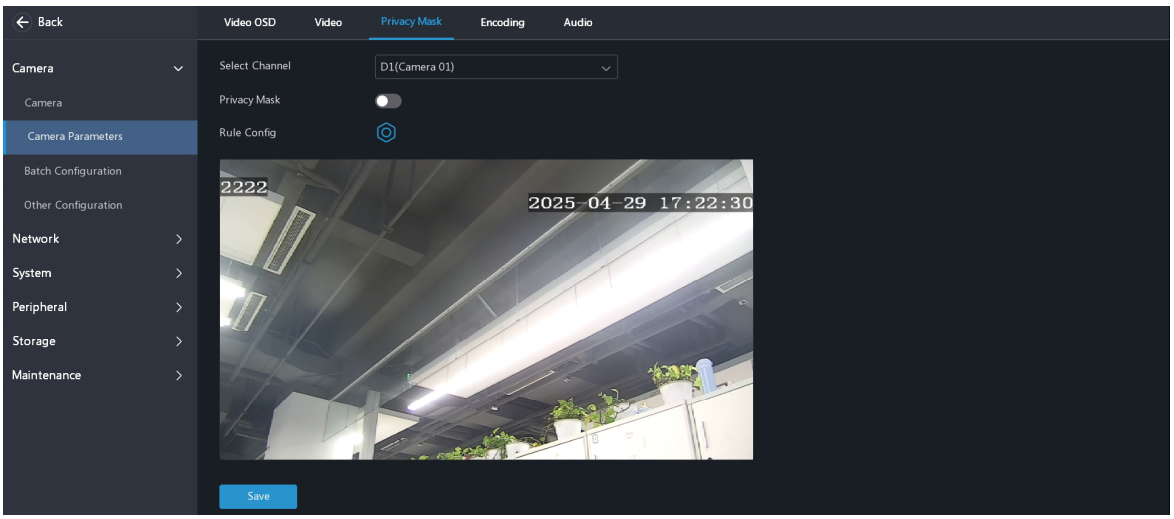
Different storage modes correspond to different video recording formats, affecting both storage space and image quality at different resolutions. The best quality stream is used for HD recordings, the second best for SD recordings. If only one stream is available in the storage mode, SD recording will not be available. Choose the storage mode based on your disk capacity and actual requirements.

Note: This configuration only affects the device's recording storage method; it does not alter the streams sent by the camera. If you change the streams sent by the camera, please also change the storage mode accordingly.

Storage Mode	Recording Clarity	
	High Definition	**Standard Definition**
Main Stream	Main Stream	No recording (black screen)
Sub Stream	Sub Stream	No recording (black screen)
Main and Sub Stream	Main Stream	Sub Stream
Main and Third Stream	Main Stream	Third Stream
Sub and Third Stream	Sub Stream	Third Stream

9.1.2.4 Privacy Mask

Privacy mask covers sensitive areas in the video. On certain cameras, the mask can track camera movement and image zoom to maintain continuous coverage of the designated area.



1. Select the channel, and enable **Privacy Mask**.

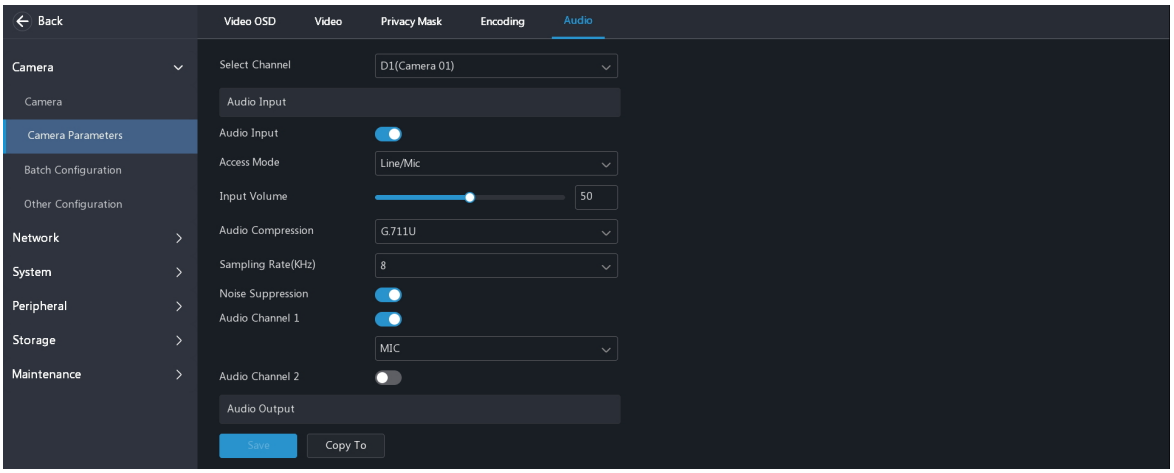
2. Click , and draw the mask area.

   (1) Click on the local interface (or on the web interface), and then drag on the image to draw a mask area.
   Drag the mask area to change its position; drag its four vertices to change the size; click to delete the mask area; click to clear all mask areas on the local interface.

   (2) Click **OK** to save the drawing and exit.

3. Click **Save**.

9.1.2.5 Audio Parameters



1. Select the channel, and configure the audio input and output parameters of the camera.

   - Audio Input: To collect audio from the camera, enable **Audio Input** and configure the parameters below.

Parameter	Description
Access Mode	The way the camera captures audio • Line/Mic: Capture audio using a device connected to the Line interface or using the camera's built-in microphone • RS485: Capture audio using an audio device connected to the RS485 interface (requires setting **Port Mode** to **Sound Pickup** on the camera's web interface) **Note:** The camera only supports connecting certain brands of audio devices; contact our technical support for details.
Input Volume	Drag the slider to adjust the audio volume captured by the camera
Audio Compression	Maintain audio quality while using compression to save storage space and bandwidth **Note:** Using different encoding formats for audio and audio devices may lead to issues such as incompatibility and degraded audio quality. These problems can be resolved by adopting a unified format.
Sampling Rate (KHz)	The number of samples taken per second; the higher the sampling rate, the more accurate the reproduced audio
Noise Suppression	Used to suppress audio noise. Enable as needed
Audio Channel 1/2	Enable audio channel as needed, and select the audio to be captured **Note:** Only one audio channel can be enabled at a time.

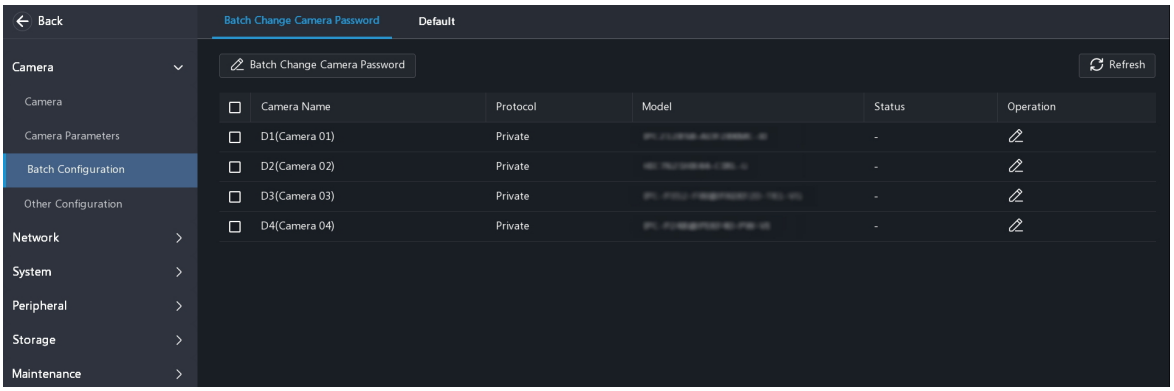
   - Audio Output:

Parameter	Description
Audio Output	How the camera plays audio • Speaker: Plays audio through the camera's built-in speaker • Line: Plays audio through an audio device (e.g., a speaker) connected to the Line interface
Output Volume	Drag the slider to adjust the master volume
Alarm Volume	Drag the slider to adjust the alarm volume

2. Click **Save**.

9.1.3 Batch Configuration

9.1.3.1 Batch Change Camera Password

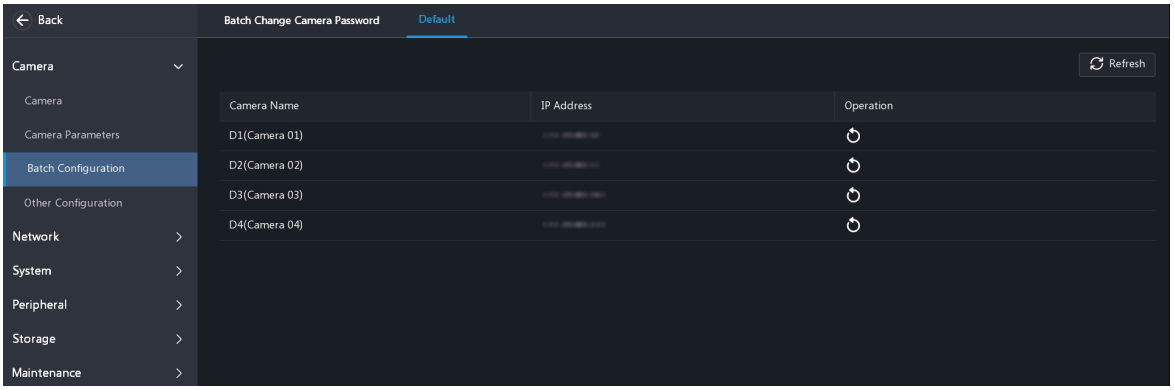


1. Select a camera and click to change its login password. Select multiple cameras, and click **Batch Change Camera Password** to change their passwords.
   - New Password/Confirm: Enter the new password.
   - Sync Password: The camera's password is changed to the admin password of the NVR.
2. Click **OK**.

Note:

- If the passwords for multiple channels under a single IP camera are changed separately, the camera's password will be determined by the last changed channel.
- If the passwords for multiple channels under a multi-IP camera are changed separately, each IP address's password will be determined by the last changed channel under that IP.

9.1.3.2 Restore Defaults

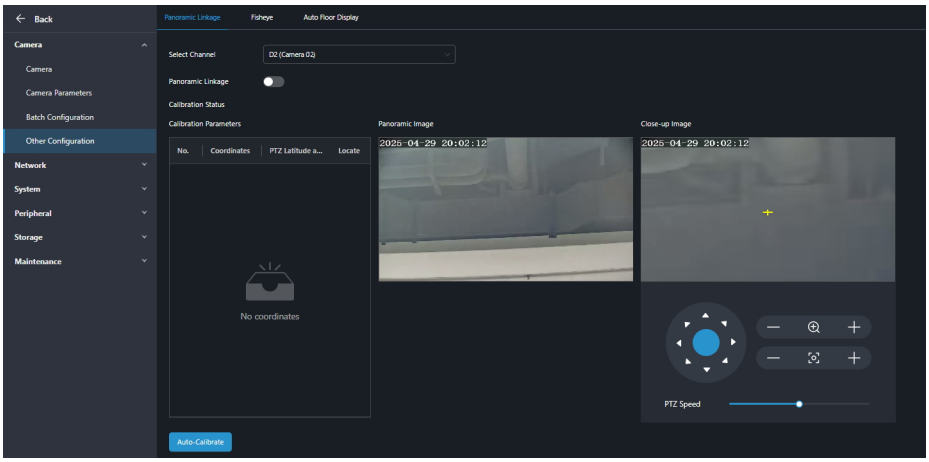


Click for a camera, click **OK**, and the camera will restore default settings and restart. Cameras added to the NVR via the network must be added again after a factory default reset.

9.1.4 Other Configuration

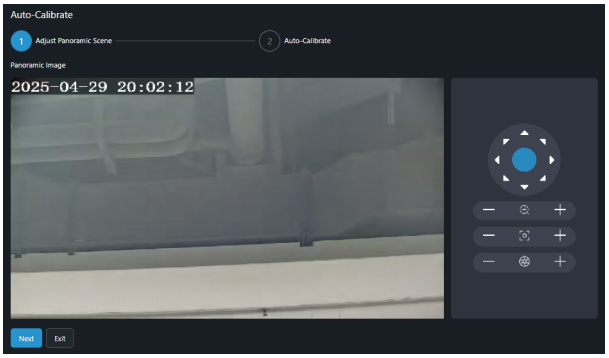
9.1.4.1 Panoramic Linkage

A panoramic linkage camera uses the panoramic camera to capture a panoramic image and the PTZ camera to capture a close-up image, allowing you to zoom in on a specific area of the panoramic image. This function links the panoramic and PTZ cameras. Click any point on the panoramic image, and the PTZ camera will automatically rotate to the corresponding position and provide a detailed close-up image.

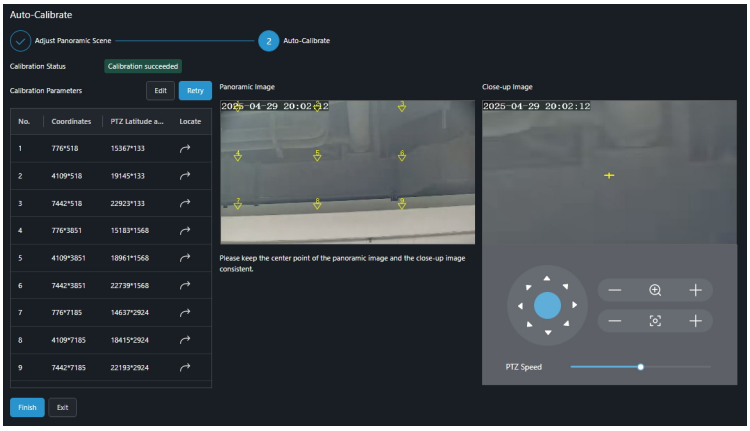


1. Select the channel, and enable **Panoramic Linkage**.
2. Click **Auto-Calibrate**, and set the calibration points to link the panoramic camera and PTZ camera.

   (1) When the panoramic camera supports the PTZ function, adjust the panoramic scene and click **Next**.



   (2) On the **Auto-Calibrate** page, the system automatically calibrates multiple points evenly on the panoramic image and displays the corresponding close-up image, ensuring that the center point of the close-up image is consistent with the calibration point on the panoramic image. This will match the panoramic image with multiple close-up images one by one.



   (3) (Optional) If the automatic calibration is not accurate, you can calibrate the calibration points. Click for the calibration point, and the PTZ camera will display the corresponding close-up image. Make sure that the center point of the close-up image matches the calibration point of the panoramic image. If they do not match, you can calibrate them using the two methods below.

   - Automatically calibrate again: Click **Retry** to calibrate points again.

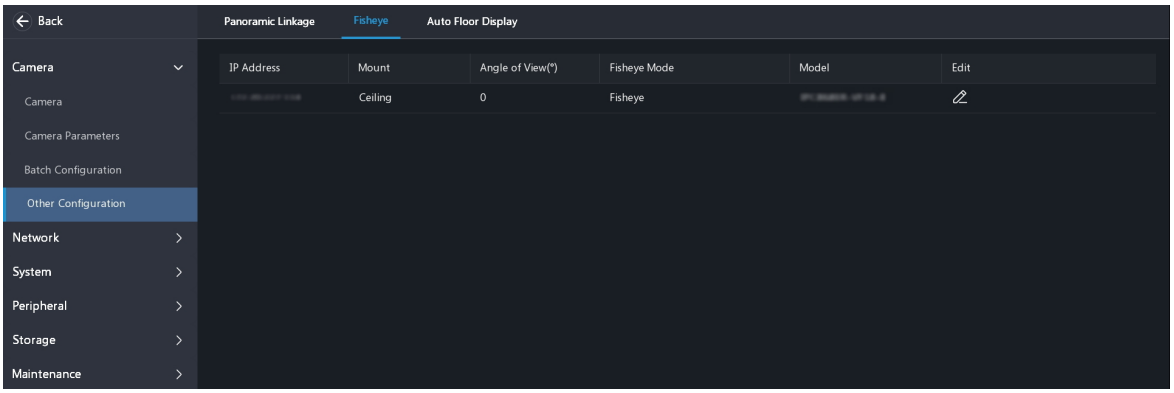
After the automatic calibration is complete, confirm whether the calibrations points are accurate.

- Manually calibrate:
  1. Click **Edit**, click for the calibration point to be calibrated, manually adjust the position and zoom of the close-up image using the PTZ configuration function in the lower-right corner, and click to complete its calibration.
  2. Repeat the above operations to calibrate all remaining points.
  3. Click **Finish Editing**.

(4) After confirming the accuracy of the calibration points, click **Finish** to link the panoramic and PTZ cameras.

3. After the linkage is complete, you can use the multi-sensor preview function in Preview to drag to zoom, manually track, and click to link.
   - Drag to zoom: Left-click and drag at any position on the panoramic image to draw a rectangular box. The corresponding area will be magnified on the close-up image to show details.
   - Manually track: Click any target on the panoramic image, and the PTZ camera will automatically track the target and show the close-up image. If the target disappears from the monitoring area, the PTZ camera will rotate to the auto guard position or the system default position.
   - Click to link: Click anywhere on the panoramic image, the close-up image displays the clicked point at the image center.

9.1.4.2 Fisheye Configuration



Click to configure the parameters for the fisheye camera, and click **OK**.

Parameter	Description
Mount	Select a mode based on the actual mount method
Angle of View (°)	Set the viewing angle of the fisheye camera
Fisheye Mode/Remote Camera ID	Select a fisheye mode as needed. Each fisheye mode maps to certain channels of the fisheye camera

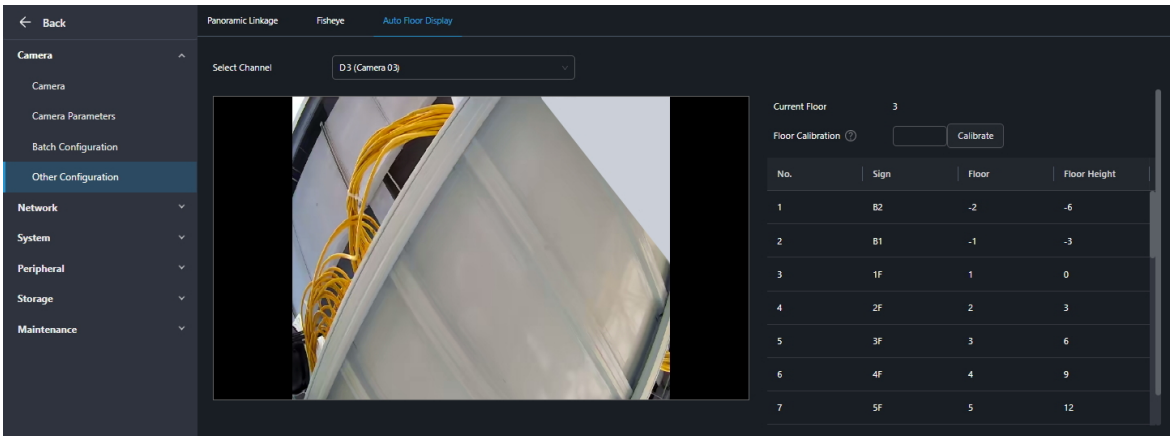
Fisheye cameras provide large wide-angle views, but the image captured is distorted. You may set the display mode using the fisheye function in Preview to output a normal image by correcting the shooting angle of the fisheye.

9.1.4.3 Auto Floor Display

Receive real-time floor reported by cameras to determine the elevator's current floor when the floor information cannot be obtained directly from the camera image.

If the floor displayed is inaccurate, enter the correct floor and click **Calibrate**.

Note: Please configure the auto floor display function on the camera's web interface first.

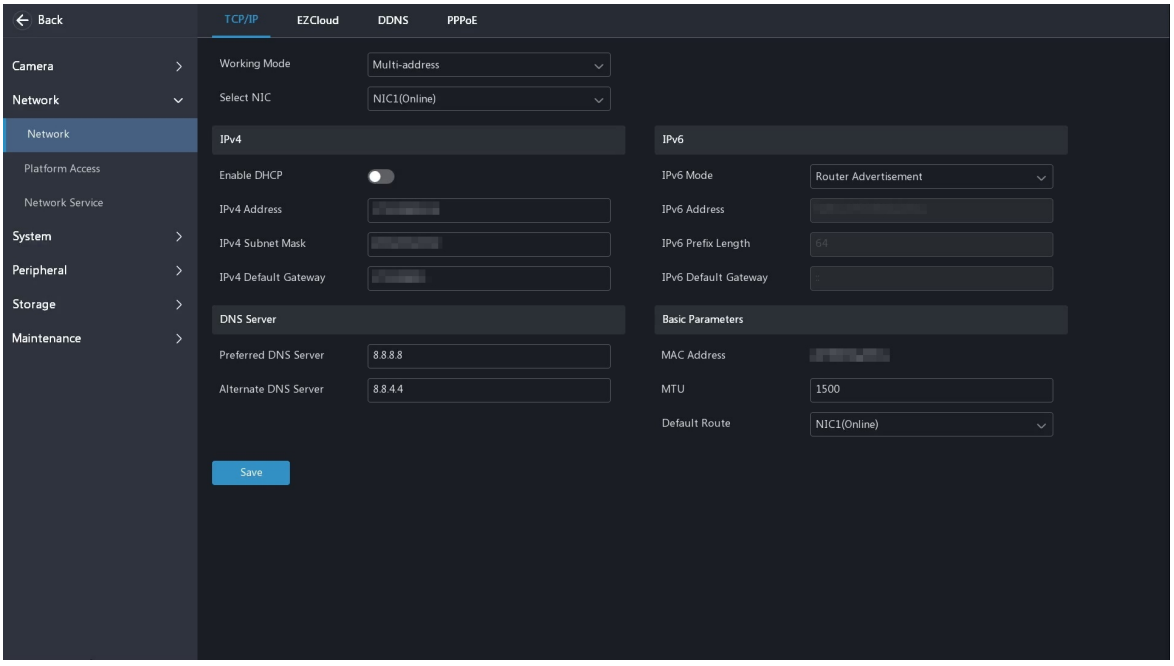


9.2 Network

Note: The default IP address for network port 1 is 192.168.1.30, for network port 2 is 192.168.2.30, and so on.

9.2.1 Network Parameters

9.2.1.1 TCP/IP



1. Configure the network parameters.

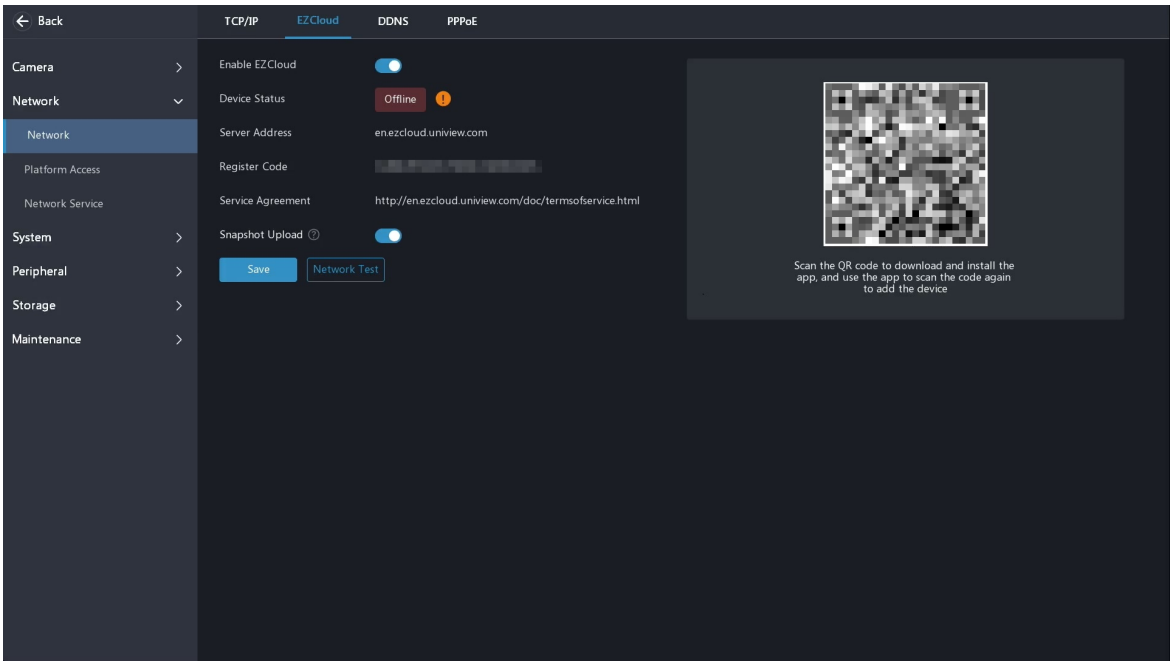
Parameter	Description
Working Mode	• Multi-address: Multiple NICs work independently. You need to configure the NICs separately. Choose an NIC as the default route. When the NVR connects to an external network, data will be forwarded via the default route • Load Balance: Multiple NICs use the same IP address and work together to share the sending and receiving bandwidth • Net Fault-tolerance: Multiple NICs use the same IP address. If the primary NIC fails, the standby NIC takes over seamlessly to ensure uninterrupted network connection **Note:** For a multi-NIC NVR, switching working modes with 802.1x and ARP protection enabled will disable 802.1x and ARP protection.
Select NIC	Select an NIC

Parameter	Description
IPv4	• DHCP enabled: The NVR can automatically obtain an IP address from the DHCP server • DHCP disabled: You need to set the IP address manually
IPv6	• Router Advertisement/DHCP: The IP address is assigned automatically • Manual: You need to set the IP address manually **Note:** To access the web interface using an IPv6 address, make sure the IPv6 addresses of the NVR and PC are connected. To use functions such as live view and playback, make sure the IPv4 addresses of the NVR and PC are also connected.
DNS Server	A DNS server will be used by the device to convert a domain name into an IP address if the domain name is used to add an IP address
Basic Parameters	• MAC Address: A unique identifier of the device hardware, used for data transfer and device identification on the LAN • MTU: Maximum packet size supported by the device **Note:** The MTU must be in the range of 576 to 1500. To use IPv6, you must set MTU to between 1280 to 1500. • Default Route: It must designate a specific NIC for data forwarding when a multi-NIC device assesses the address that is not on the same network segment
PoE NIC IP Address	The NVR with PoE ports can configure the IPv4 address of the internal NIC

2. Click **OK**.

9.2.1.2 EZCloud

Add the device to EZCloud. Make sure that the device is connected to the network before use.

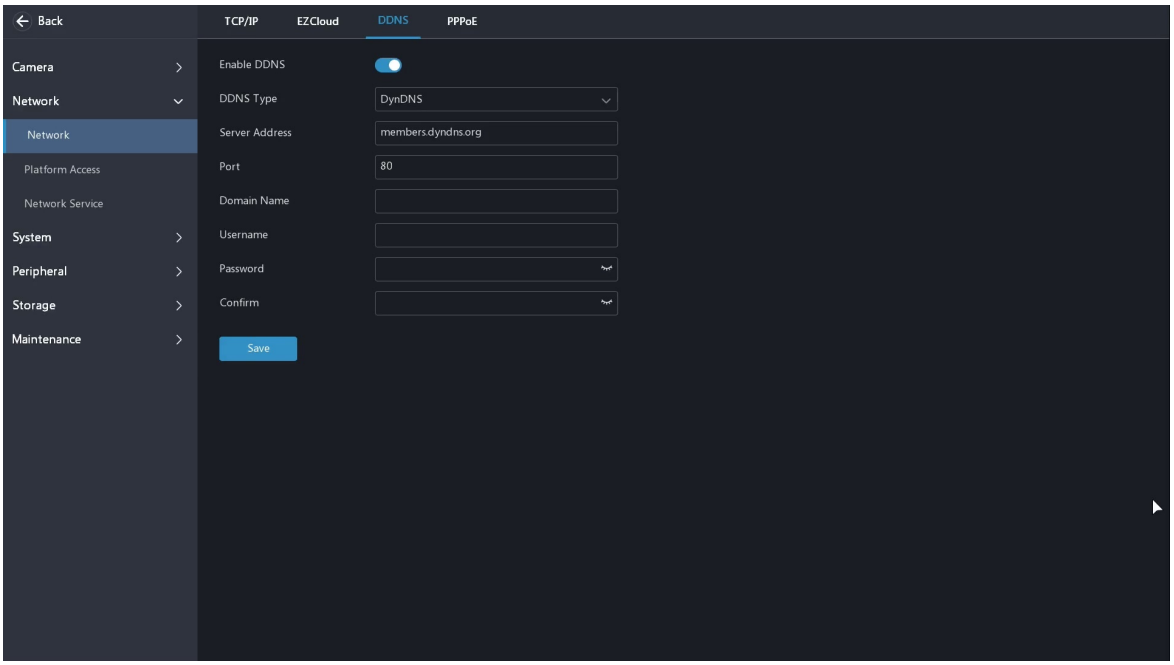


1. Follow the on-screen instructions to download the app.
2. Enable or disable the following functions as needed.
3. Click **Save**, and add the NVR to cloud using the app.

9.2.1.4 DDNS

When a device's public IP address changes dynamically, configuring a domain name enables external clients to know the current public IP address via the domain name.

Note: Please configure the port mapping before use.



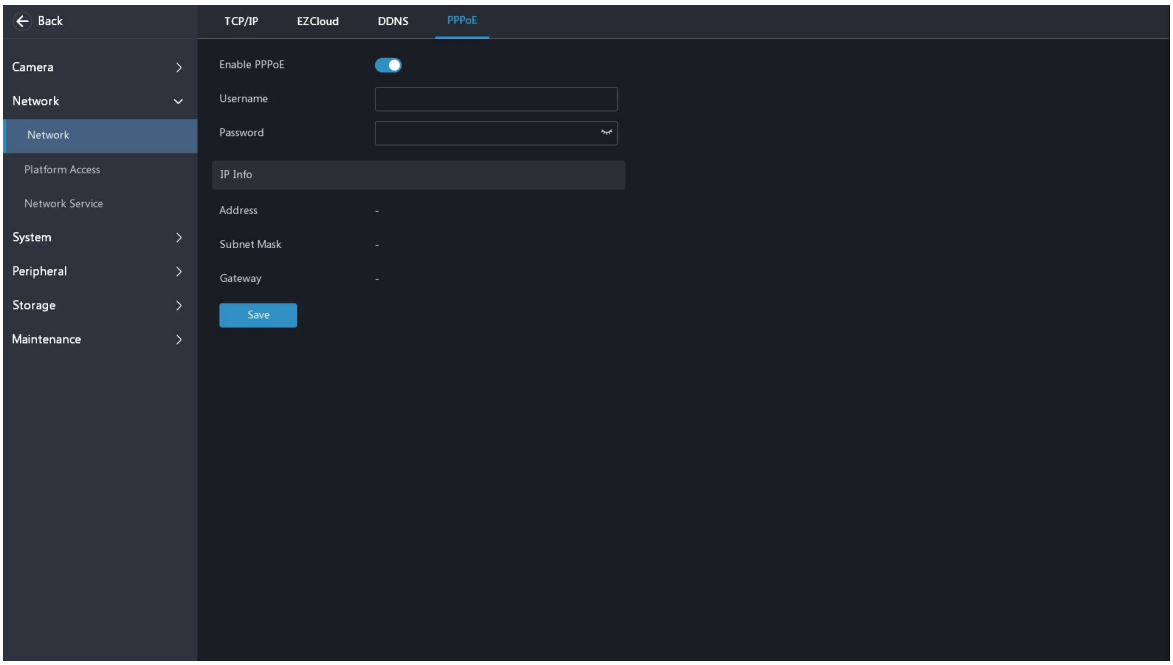
1. Enable DDNS, and configure the parameters.

DDNS Type	Description	Server Address	Domain Name	Username/ Password	Port
DynDNS/No-IP	Third-party DDNS service provider	Assigned when signing up for an account on the official website		Username/ password for your account	Default: 80
EZDDNS	DDNS service provided by Uniview	Keep default address	Custom. Click **Test** to check its validity	/	Default: 80

2. Click **Save**. You can access the device's web interface using the domain name by entering the URL in the web browser. Refer to the following formats:
   - DynDNS/No-IP: http://domain name:external port number
   - EZDDNS: http://server address/domain name

9.2.1.5 PPPoE

Use Point to Point Protocol over Ethernet (PPPoE) to connect the NVR to network. When PPPoE is enabled, TCP/IP cannot be configured.



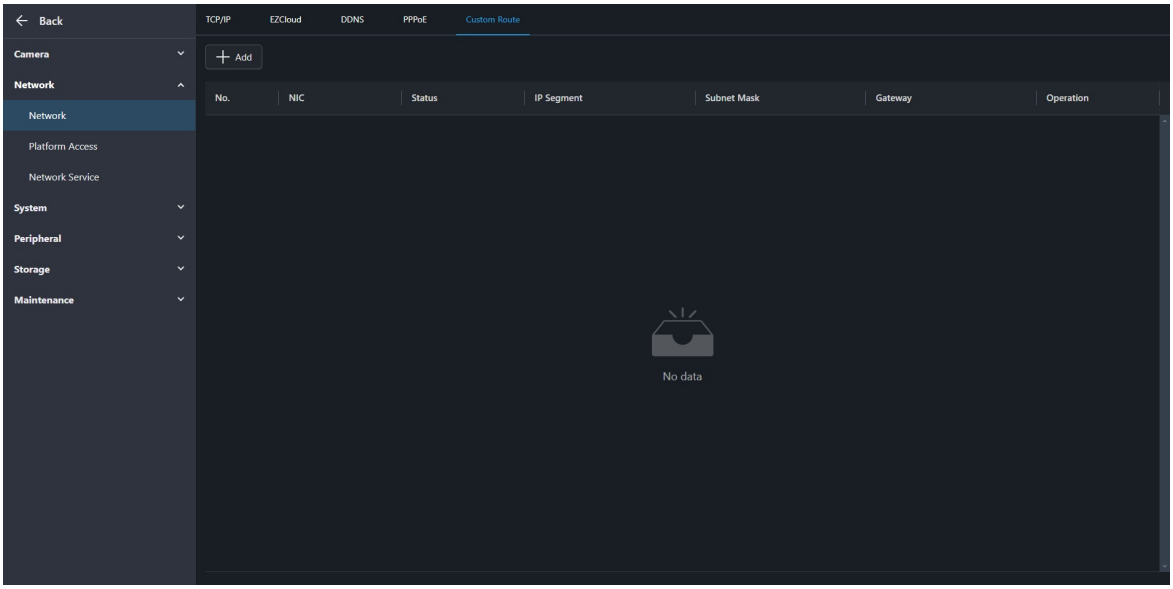
Note:

- For a multi-NIC device, dial-up shall be performed on the NIC that is configured as the default route.
- Please disable UNP first before use.

Click to enable **PPPoE**, enter the username and password provided by the Internet Service Provider (ISP), and click **Save**. IP information is displayed when dial-up succeeds.

9.2.1.7 Custom Route

When a multi-NIC device accesses a non-same network segment address, it must designate a NIC for data forwarding. The custom route can designate a NIC for different non-same network segment addresses. The custom route takes precedence over the default route.



1. Click **Add**, click to enable **Route**, and configure the parameters.

Parameter	Description
Route	Enable or disable as needed
NIC	Select an NIC
Destination IP Segment	A specified address in a different network segment. The device accesses this segment's address via a custom route

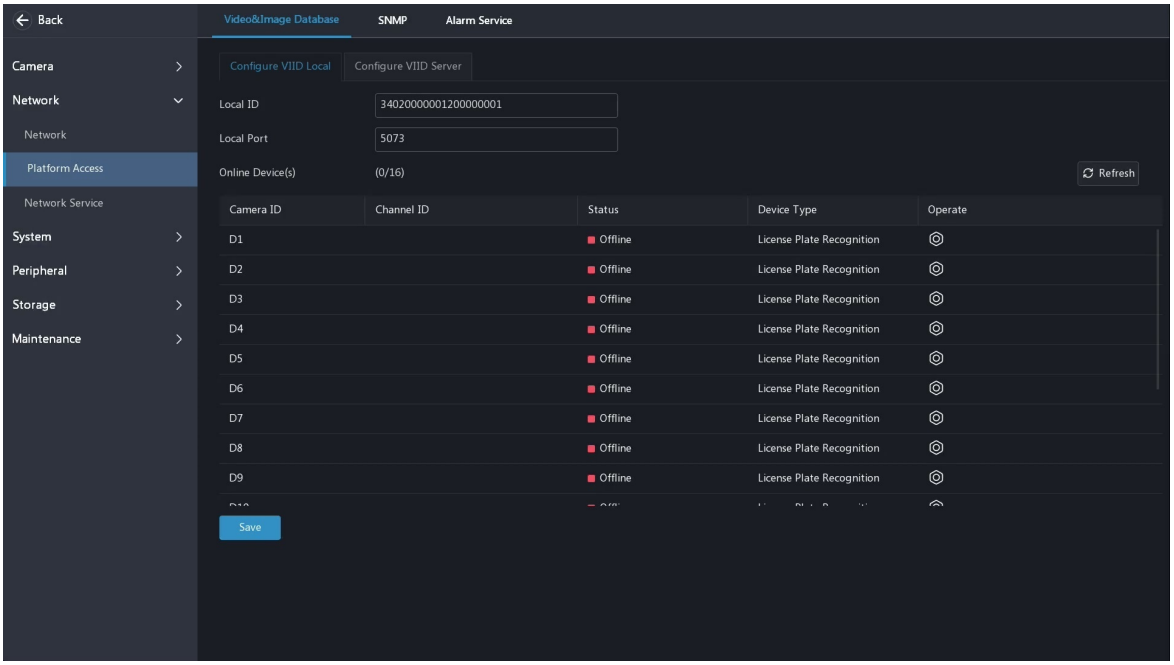
Parameter	Description
Subnet Mask	The subnet mask of the specified network segment
Gateway	Align with the gateway of the selected NIC. See TCP/IP for details

2. Click **OK**.

9.2.2 Platform Access

9.2.2.3 VIID Local Configuration

Configure the basic parameters for the NVR to operate as a downstream device, and display the online status of the cameras connected to it.



1. Configure the basic parameters.

Parameter	Description
Local ID	Device ID, used to distinguish different types of devices when connecting upper platforms, consists of 8-digit center code + 2-digit industry code + 3-digit type code + 7-digit serial number
Local Port	Default: 5073

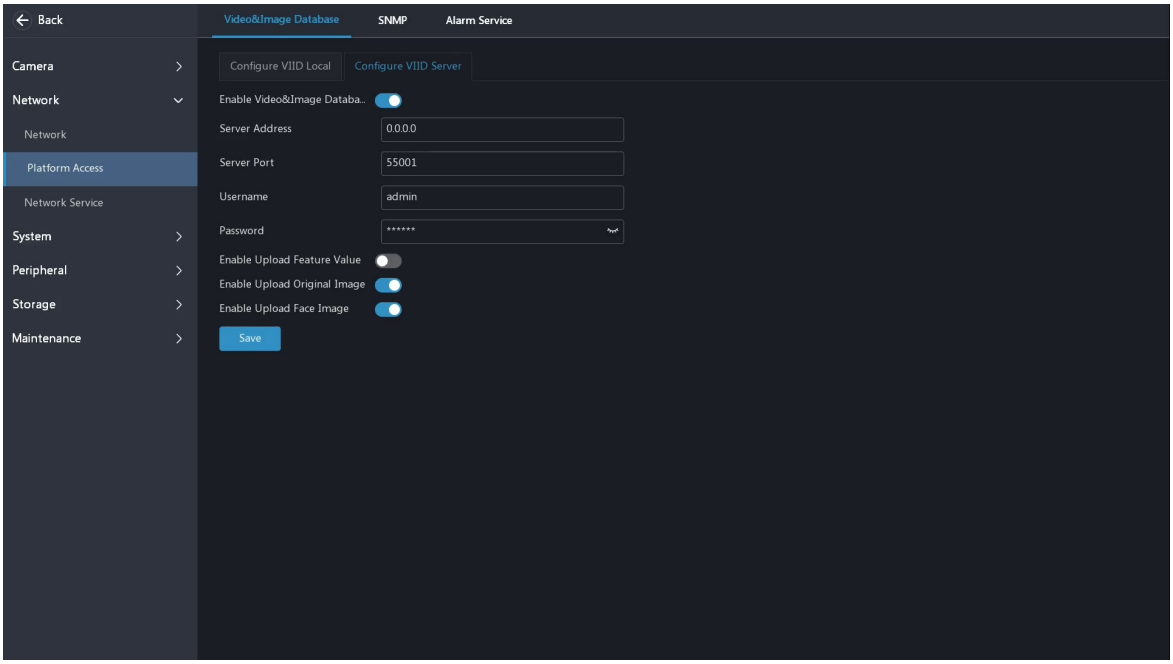
2. Choose a camera, and click to configure the camera parameters.

Parameter	Description
Channel ID	Camera's VIID ID, used to connect the camera to the NVR
Device Type	Divided into two types by usage: • License Plate Recognition: Usually installed on road checkpoints to capture license plates of passing vehicles • Collection Device: Used to capture faces or license plates
Advanced Configuration	Configure as needed

3. Click **Save**.

9.2.2.4 VIID Server Configuration

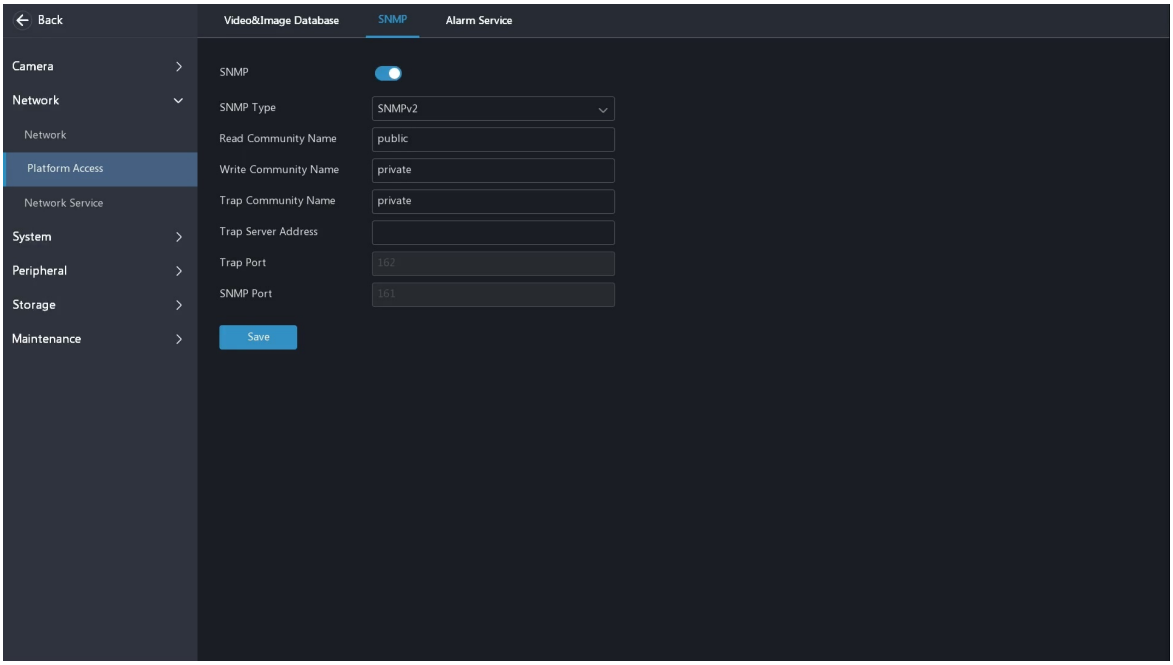
Connect the upper VIID platform and select the content you want to upload. Make sure that VIID local configuration is completed before connecting the NVR to the upper VIID platform.



Configure the server address, server port, username, and password for the VIID platform, select the content you want to upload, and click **Save**.

9.2.2.5 SNMP

The NVR can transfer certain configuration information to the upper platform using SNMP, including basic device information (name, model, etc.), hard disk information (total number, capacity, etc.), camera information (model, version number, etc.), and device usage status (memory, CPU occupancy, etc.).

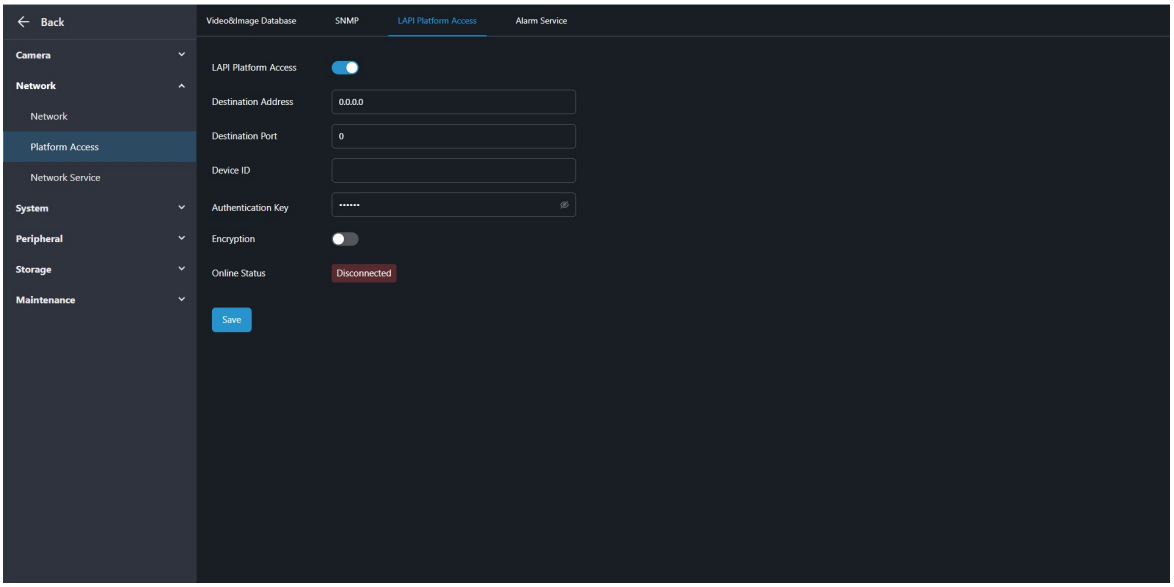


Parameter	SNMPv2	SNMPv3
Read Community Name	This name is used for authentication when the platform reads NVR data. Please set a complex name	/
Write Community Name	This name is used for authentication when the platform edits NVR data. Please set a complex name	/

Parameter	SNMPv2	SNMPv3
Authentication Password	/	Password used by the platform to access the NVR
Encryption Password	/	Password used to encrypt data sent from the NVR to the platform

9.2.2.7 LAPI

Access the upper platform via the LAPI protocol so that the platform can manage the NVR.



1. Click to enable **LAPI Platform Access**, and configure the parameters.

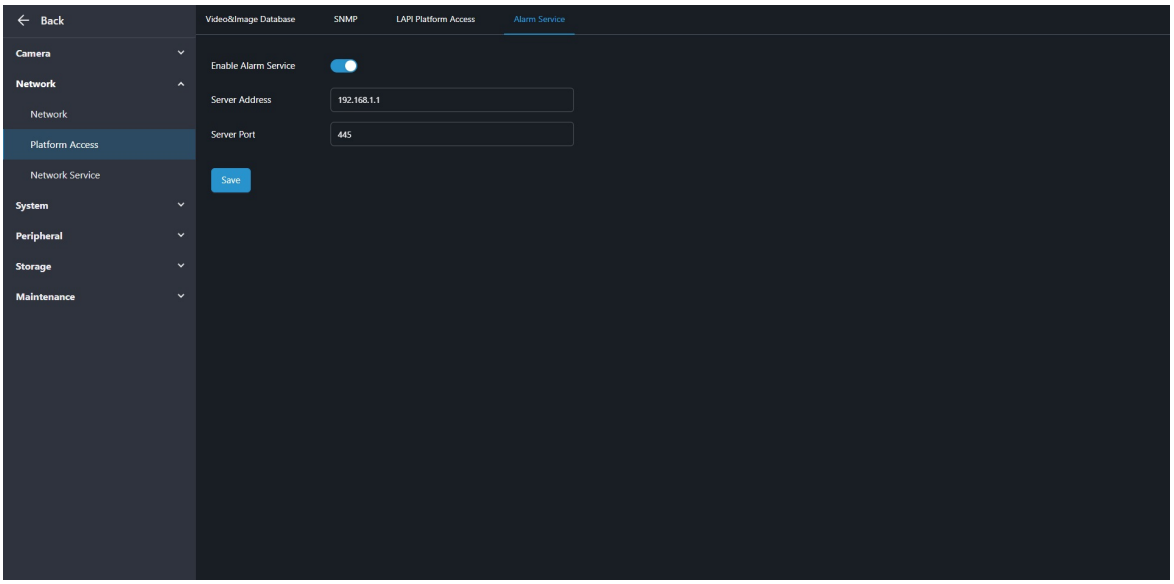
Parameter	Description
Destination Address/ Destination Port	Upper platform's IP address/port
Device ID	Device serial number is recommended for use
Authentication key	Upper platform's login password

2. Click **Save**. The online status will change to **Connected** when the connection is successful.

9.2.2.8 Alarm Service

Send alarm messages to the upper platform.

Note: This configuration only enables the sending of alarm-related packets to the alarm host. The specific alarm methods on the alarm host need to be configured separately.



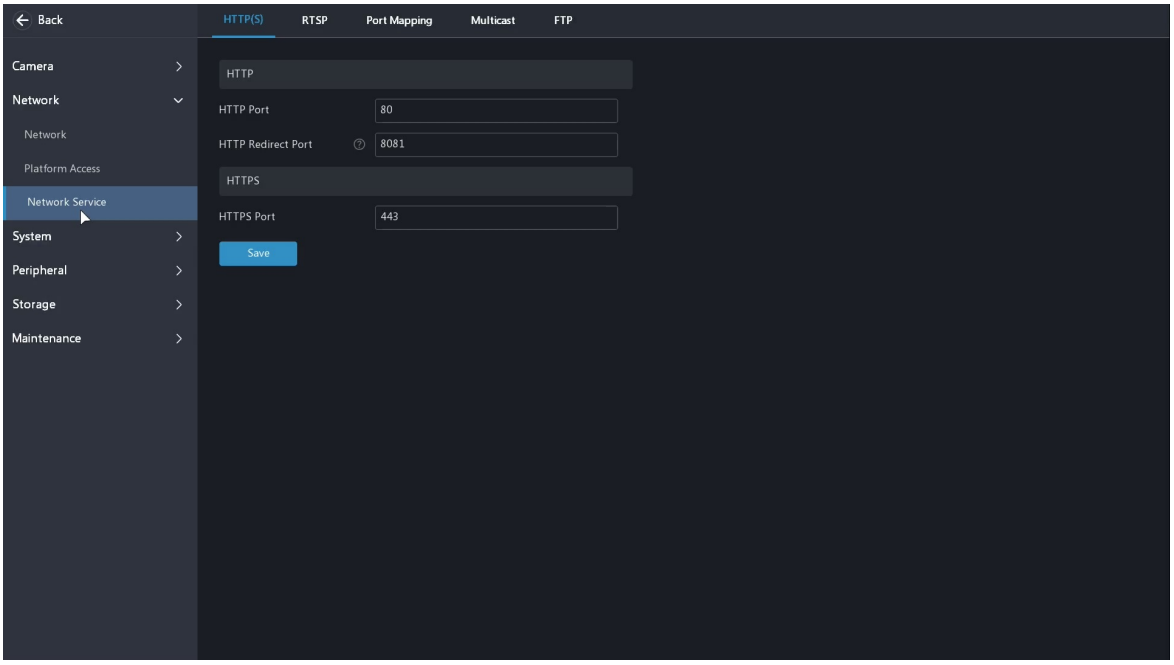
Click  to enable **Alarm Service**, configure the server address and port, and click **Save**.

9.2.3 Network Service

9.2.3.1 HTTP(S)

Configure the port used for the HTTP(S) protocol.

Note: The port number range is 1 to 65535, among which, ports 21, 23, 2000, 3702, and 60000 are reserved for other purposes. Duplicate ports are not allowed.

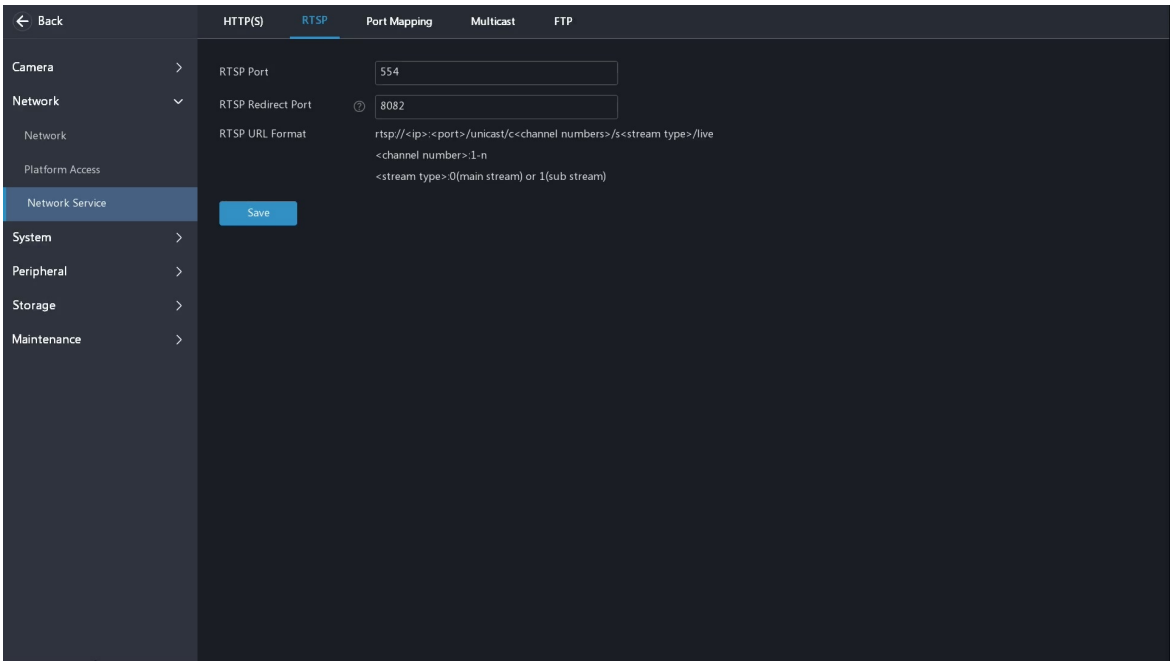


9.2.3.2 RTSP

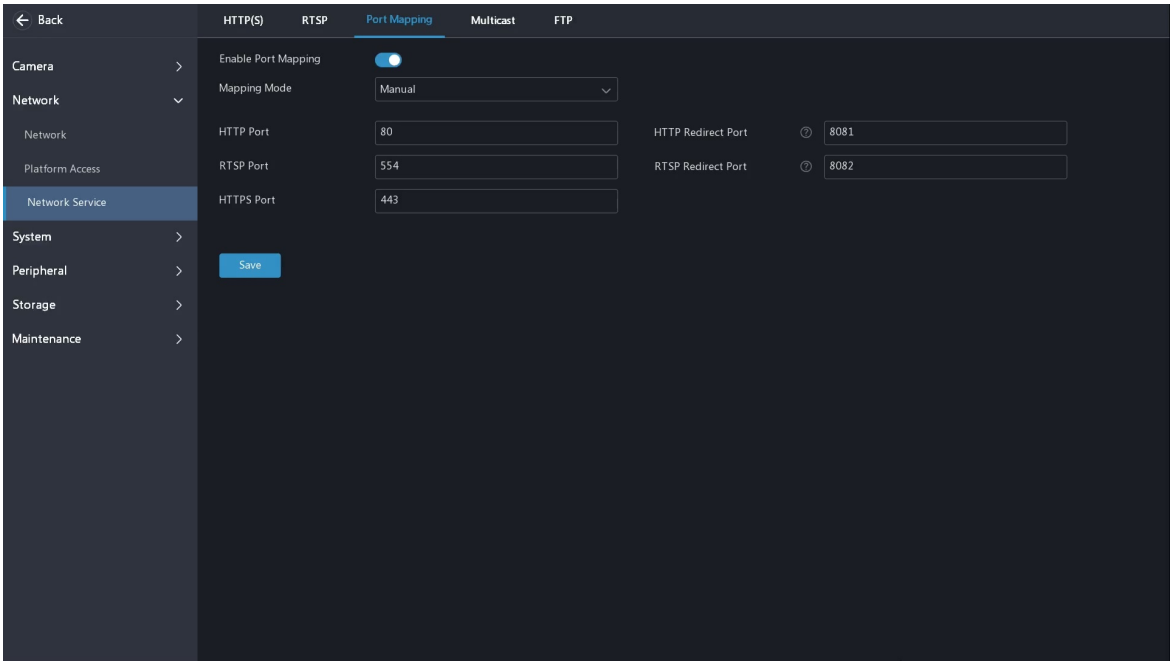
Configure the port used for the RTSP protocol.

Note:

- The port number range is 1 to 65535, among which, ports 21, 23, 2000, 3702, and 60000 are reserved for other purposes. Duplicate ports are not allowed.
- The upper platform can access the live video of a camera using the displayed RTSP URL.



9.2.3.3 Port Mapping



Map the internal IP address and port number to an external IP address and port number, enabling WAN clients to access the LAN device by entering **external IP:external port** in a web browser.

Note:

- External Port: The port number of the router's WAN port IP address.
- External IP Address: The IP address of the router's WAN port.
- Internal Port: The port number of the router's LAN port IP address to which the device is connected. See HTTP(S) or RTSP for manual configuration.
- Internal IP Address: The IP address of the router's LAN port to which the device is connected.
- Redirect Port: On the **Camera** page of the NVR's web interface, clicking the name of an online camera can redirect to its web interface.

Manual

You need to configure the external port for the corresponding service on the router, and then fill in the port number on the device.

UPnP

The external port number assigned via UPnP.

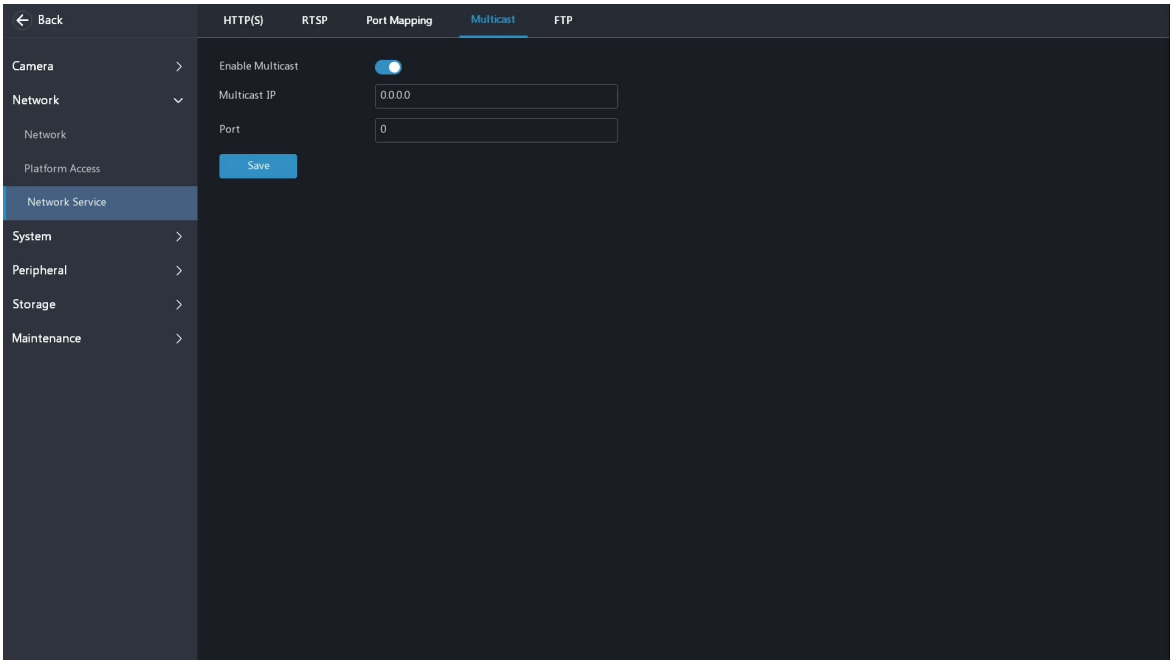
Note:

- Please enable UPnP on the router before use.
- The assigned port number is usually the same as the NVR's internal port number. If not, an external port must be added after the external IP address in order to access the HTTP service via the external IP address. For example, the router's external IP address is 10.2.2.10, and the external HTTP port is 82, then you can access the web interface by entering http://10.2.2.10:82 in the browser's address bar.

UPnP Mapping	Description
Auto	The NVR automatically negotiates with the router to assign an external port number
Manual	The NVR negotiates with the router using a specified port number

9.2.3.4 Multicast

When the number of users accessing the web client has reached the upper limit and live video is unavailable, you can use multicast to solve this issue.



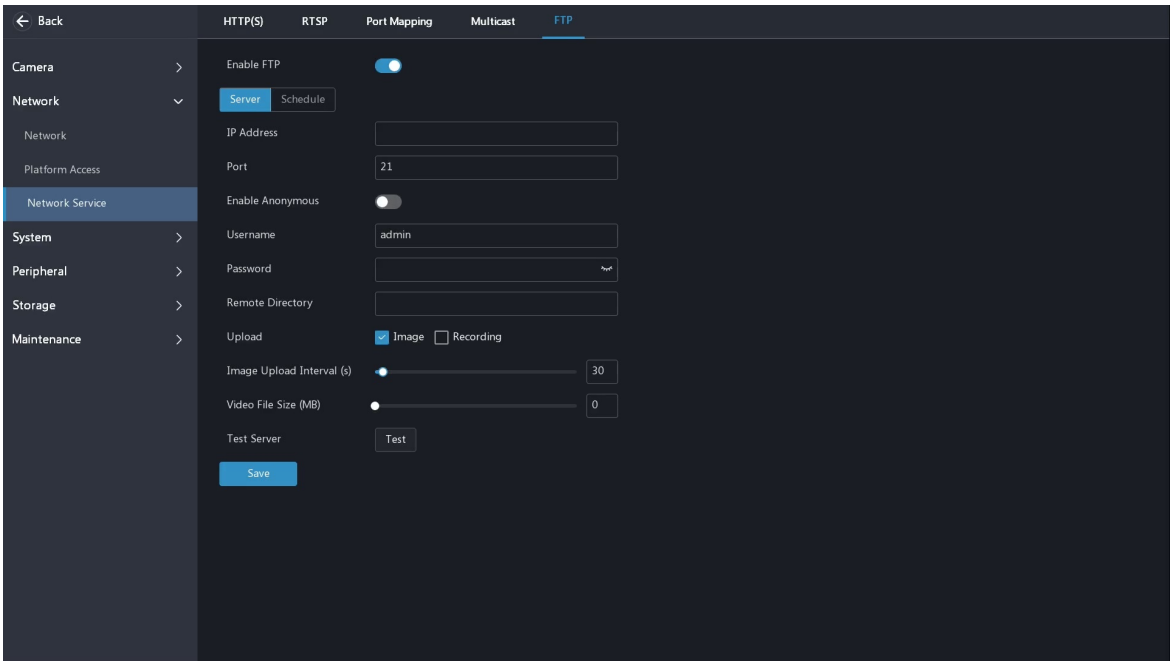
1. Click to enable **Multicast**, and enter the multicast IP address and port number.
2. Click **Save**.
3. Log in to the device's web interface, enter the **Client** page, and set **Live View Protocol** to **Multicast**. Now live view is available through multicast.

Note:

- IP multicast addresses are class-D addresses. 224.0.1.0 - 238.255.255.255 can be used on the Internet.
- In the range of 224.0.0.0 - 239.255.255.255, some are reserved for special uses. For example, 224.0.0.0 - 244.0.0.255 can only be used on the LAN, where packets with these addresses will not be forwarded by a router; 224.0.0.1 is used by all the hosts on the subnet; 224.0.0.2 is used by all the routers on the subnet; 224.0.0.5 is used by OSPF routers; 224.0.0.13 is used by PIMv2 routers; and 239.0.0.0 - 239.255.255.255 are private addresses (e.g., 192.168.x.x).

9.2.3.5 FTP

Configure FTP so that the NVR can automatically upload images and recordings to the FTP server.



1. On the **Server** tab, click  to enable **FTP**, and configure the parameters.

Parameter	Description
IP Address	FTP server address
Port	FTP server port. The default is 21. You can set it as needed
Enable Anonymous	When enabled, the NVR will connect to the FTP server as anonymous user without username/password required
Username/Password	Username/password used to access the FTP server
Remote Directory	Storage path for images and recordings **Note:** • For example, if the remote directory is abc, then the created folder is FTP > abc > 206.2.5.8 > 2022-10-08 > D5. If the remote directory is abc/efg/xyz, then the created folder is FTP > abc > efg > xyz > 206.2.5.8 > 2022-10-08 > D5. • If the remote directory is empty, the system will create folders under the root directory based on IP, time, and channel, for example, FTP > 206.2.5.8 > 2022-10-08 > D5. • Pictures and recordings are stored under **pictures** and **records** folders respectively.
Upload	Select **Image** or/and **Recording**. See the schedule configuration for the upload type
Image Upload Interval (s)	The device uploads images captured within the set periods to the FTP server at the set interval. You can set it as needed

2. Click **Test** to test the connection between the NVR and the FTP server.
3. On the **Schedule** tab, select a channel, and configure the upload schedule.

Note: To apply the upload schedule to other days, select **All** or other day(s), and click **Save**.

Parameter	Description
Day	You can configure the upload schedule for each day individually
Time Period	Time periods for uploading images or recordings

Parameter	Description
Upload Type	Types of images or recordings uploaded within the specified time periods

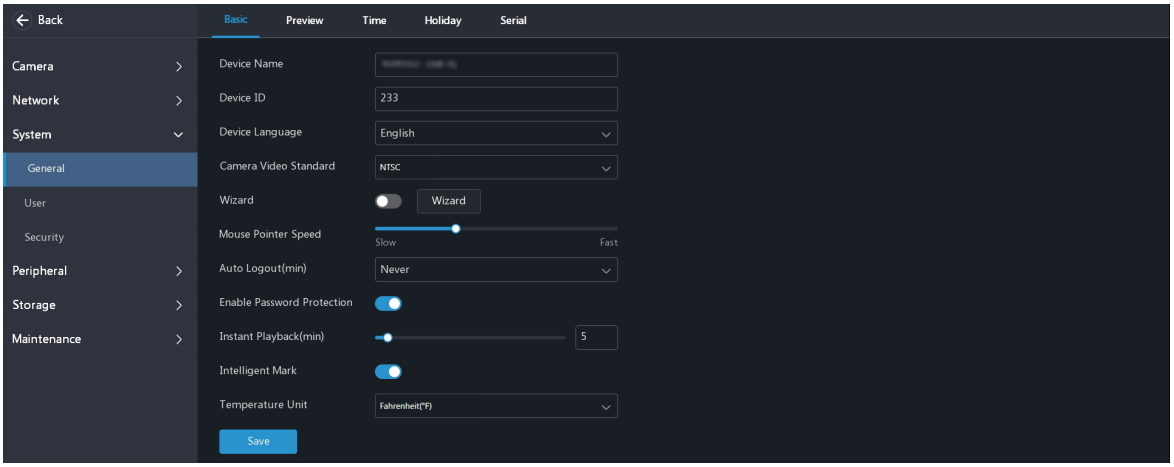
4. Click **Save**.
5. (Optional) To apply the current upload schedule to other cameras, click **Copy To**, select the desired camera(s), and click **OK**.

9.3 System

9.3.1 General Configuration

9.3.1.1 Basic Configuration

Note: Some configuration items are unavailable on the web interface.

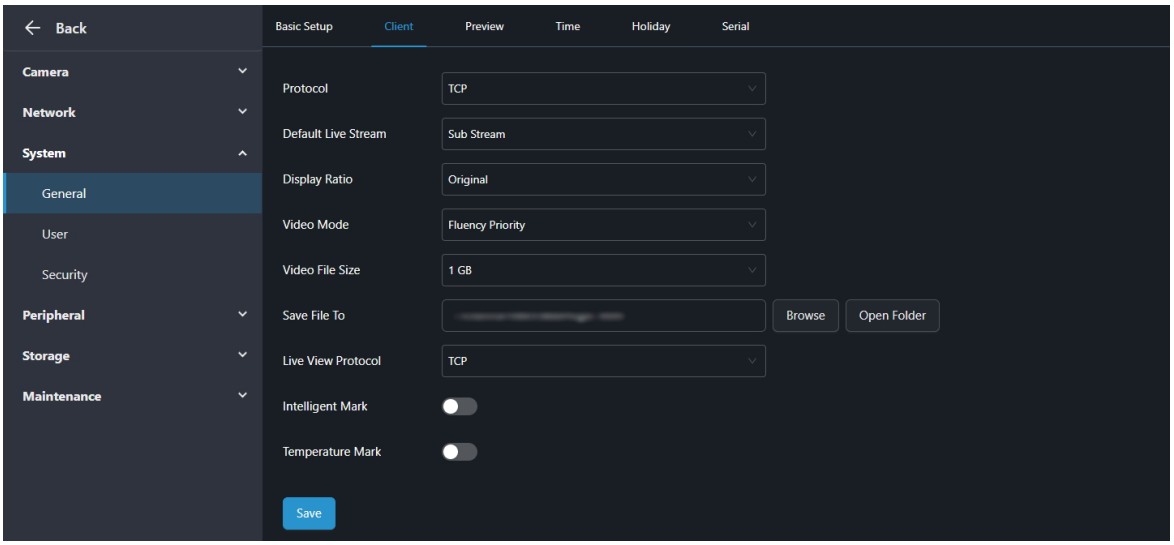


Parameter	Description
Device Name/Device ID	Set as needed. Used to distinguish devices if you have more than one device
Device Language	Change the system language **Note:** The device will restart after you change the system language and click **Save**.
Camera Video Standard	The camera video standard includes PAL and NTSC. Using different standards for the camera and monitor may cause image ghosting or flickering. This issue can be resolved by using the same standard for both • Please select: The NVR does not set the same standard for all online cameras, with each camera using its original video standard • PAL/NTSC: Set the video standard for all online cameras to PAL/NTSC, and change the bit rate of the default capture mode in Encoding Parameters. The video standard is automatically configured each time a camera goes online. If certain cameras require a different video standard, you can change it on the cameras' web interface after they go online **Note:** • The option **Please select** will disappear after selecting PAL or NTSC • The PAL standard (25/50 fps at 50Hz) delivers richer image details and lower color distortion, while the NTSC standard (30/60 fps at 60Hz) provides smoother motion images and more vibrant colors

Parameter	Description
Wizard	Wizard appears automatically when the NVR starts up for the first time, and you can perform simple configurations. For later configuration, click **Wizard** on this page; or enable **Wizard** and the startup wizard appears every time the device starts up
Mouse Pointer Speed	Drag the slider to adjust the speed
Auto Logout(min) Enable Password Protection	If you are not on the live view page and don't perform any operation, you will log out automatically when the set time is over, and the live view page will be displayed. You need to enter the login password for interface operations **Note:** This feature is enabled by default, and can only be disabled by admin. When disabled, you can perform interface operations without entering the password.
Instant Playback (min)	Set the duration for instant playback in Preview
Intelligent Mark	The **Preview** page displays all rules and the corresponding target boxes drawn in Event. The meanings of different colored lines/boxes are as follows: • Yellow line/box: Drawn tripwire or detection area • Green box: Targets that do not trigger the event alarm • Red box: Targets that trigger the event alarm
Temperature Unit	Set as needed. Used for Temperature Detection by the temperature sensing camera

9.3.1.2 Client Configuration

Note: This feature is only available on the web interface.

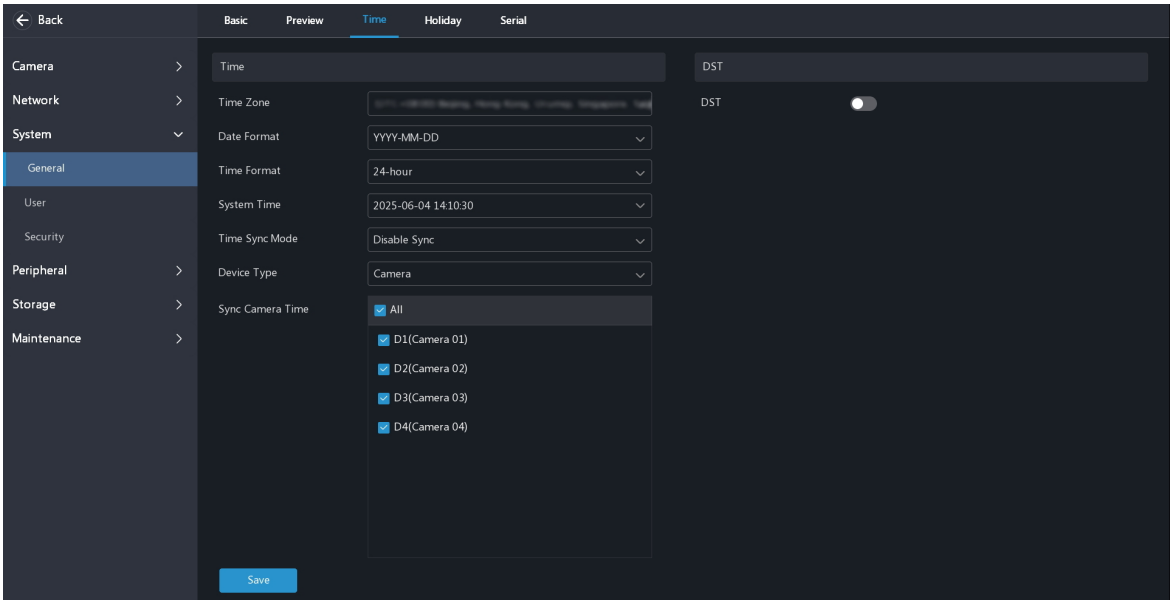


Parameter	Description
Protocol	The communication protocol between the device and web interface
Default Live Stream	Live stream
Display Ratio	Original: Displays images with original size Full: Displays images according to the window size (stretch images to fit the window)
Video Mode	Fluency Priority: High fluency but high latency Real Time Priority: Low latency but low fluency
Video File Size	The size of a package when downloading a video

Parameter	Description
Save File To	Storage path for all files downloaded or exported from the web interface
Live View Protocol	Stream distribution method when multiple web clients access the same camera's live video • TCP: The live video is sent via the TCP protocol. The number of live video streams is determined by the number of web clients received • Multicast: The live video is sent via the multicast protocol. The multicast address should be configured. The NVR sends one live view stream, which is split into multiple streams by the switch and sent to multiple web clients
Intelligent Mark	The **Preview** page displays all rules and the corresponding target boxes drawn in Event. The meanings of different colored lines/boxes are as follows: • Yellow line/box: Drawn tripwire or detection area • Green box: Targets that do not trigger the event alarm • Red box: Targets that trigger the event alarm
Temperature Mark	Displays the temperature measured by the temperature sensing camera on the preview page

9.3.1.3 Time Configuration

Select the time zone, data format, and time format, and configure the parameters as needed.



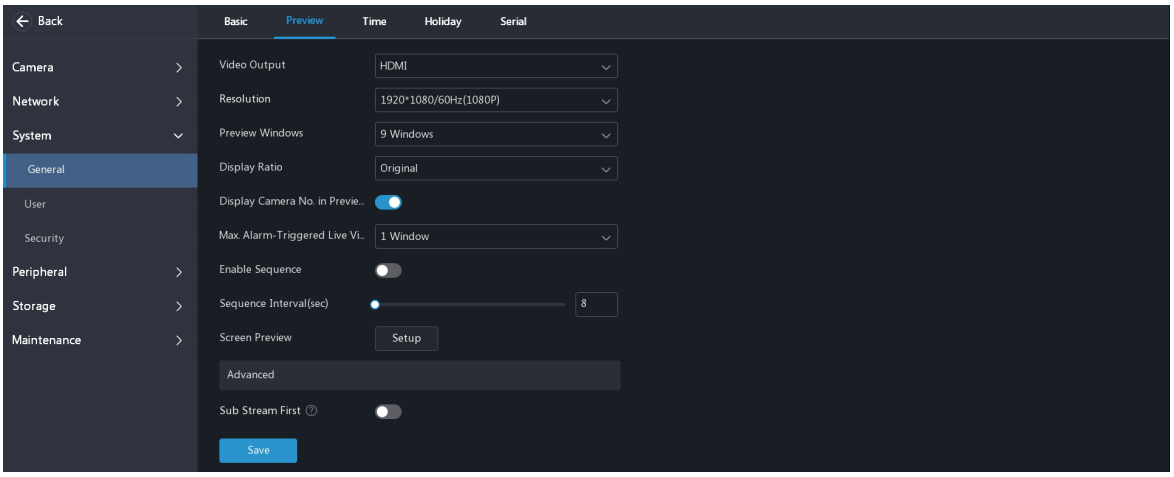
Parameter	Description	
Time Sync Mode	Disable Sync	Set the system time manually **Note:** If the device's battery is low, a prompt will appear on the screen, **Device time error. Please replace the button battery on the motherboard and reset the time**.

Parameter	Description	
	Sync with NTP Server	Sync the system time with the NTP server • If the device can access to the network, it will search for and fill in the NTP server address. You can select the update interval • If the device cannot access to the network, enter the NTP server address and select the update interval **Note:** The port number is 123 by default.
	Sync with Cloud Server	Add the device to the cloud and sync the system time with the cloud server (See EZCloud for details)
Device Type/Sync Camera Time	Sync the device time to the connected camera and IP speaker. If the camera time is not synced, the recording time may be confused **Note:** • Time sync occurs when a camera or IP speaker goes online for the first time, and then occurs every 30 minutes • Time sync status of the camera and IP speaker can be configured separately • When Sync Camera Time is disabled, the NVR will not sync time with the connected cameras. However, if the cameras go offline and then go online again, the NVR will sync time with the cameras.	
DST	Configure DST as needed	

9.3.1.4 Preview Configuration

Configure the basic preview parameters and display mode.

Note: Some configuration items are unavailable on the web interface.



Basic Preview Configuration

Parameter	Description
Video Output	Outputs the system display to an external display device

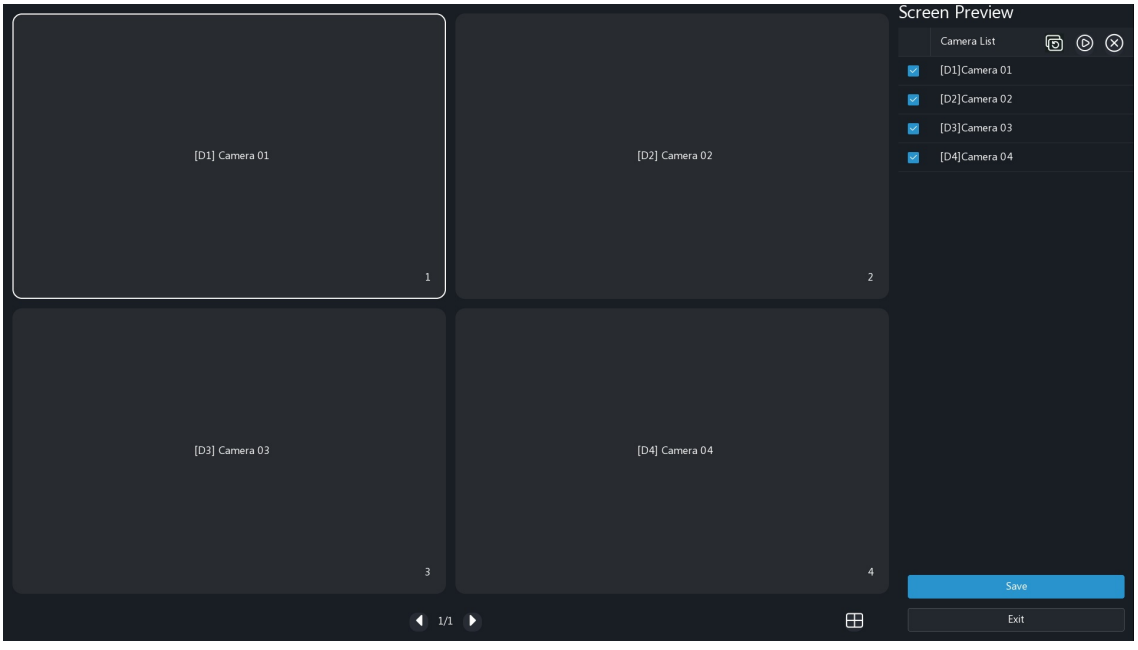
Parameter	Description
Output Mode	Supports simultaneous output and independent output. The output mode is only available to certain device • Simultaneous Output: If the HDMI and VGA interfaces share the same video source and two monitors are connected to the NVR (one via HDMI and the other via VGA), the same image will be output on both monitors. Mouse operations are synced across both monitors • Independent Output: When HDMI and VGA function as independent output interfaces, connect two monitors to the device's HDMI and VGA interfaces respectively. Different images can be output simultaneously by configuring main/aux monitor. Mouse operations on one monitor will not be synced to the other monitor. You can switch between main/aux monitor to control the output on both monitors.
Resolution	Choose the resolution as needed
Preview Windows	Displays images in the desired window layout
Display Ratio	• Full: Displays images according to the window size (stretch images to fit the window) • Original: Displays images with original size
Display Camera No. in Preview	Displays camera IDs in live view windows
Max. Alarm-Triggered Live View Windows	Three options: 1/4/9 windows. See Preview for details
Enable Sequence	Click to enable sequence. See Preview for details
Sequence Interval(sec)	Set as needed

Screen Preview Configuration

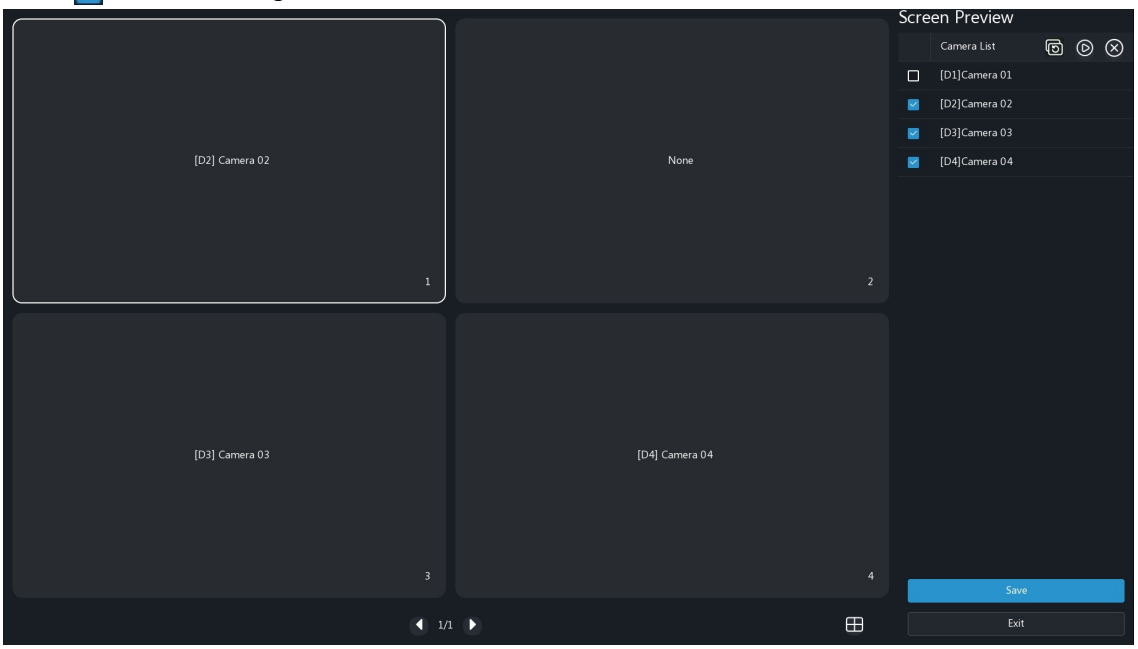
By default, camera IDs correspond to live view windows: D1 to window 1, D2 to window 2, and so on. You can change the correspondence relationship as follows. The example below shows how to switch D1 and D2.

Note: You may also drag an image on the live view page to swap windows, and then view the changed window-channel binding relationship on this page. But this method requires the configuration permission in User Management, and it cannot switch windows that are not on the same screen.

1. Click window 1 on the left side. Window 1 is selected.

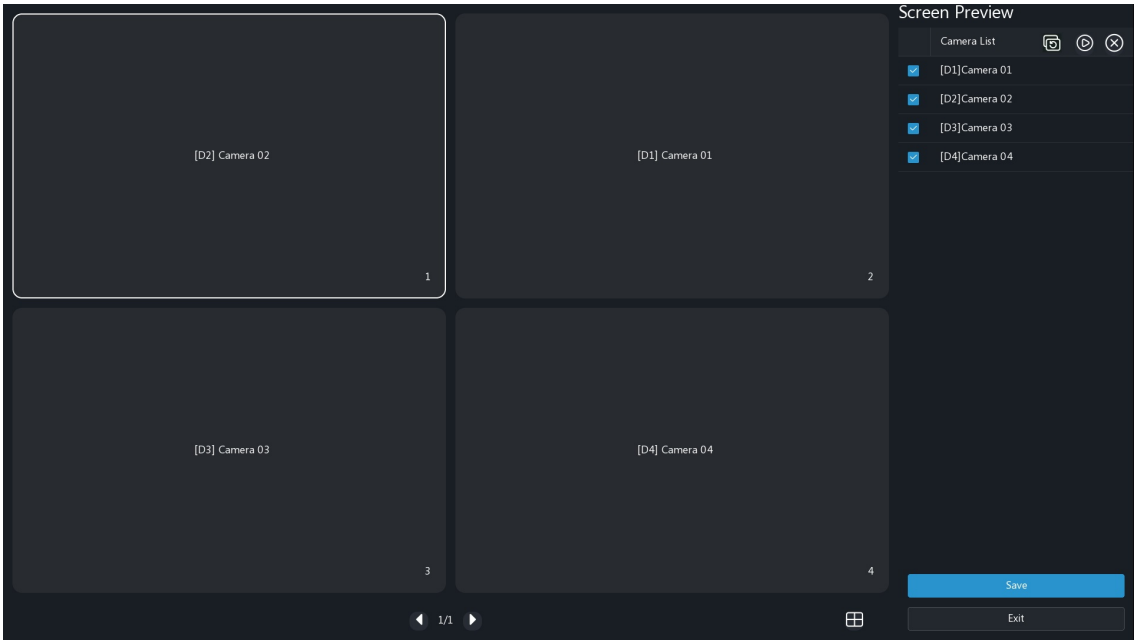


2. Select for D2 on the right-side camera list. Now window 1 shows D2, and window 2 shows None.



Note: The D1 camera is not selected on the right-side camera list, which means the camera is not bound to any window.

3. Click window 2 on the left side, and the window 2 is selected. Select for D1 on the right-side camera list, and the window 2 shows D1, which means D1 and D2 have switched windows with each other.



4. On the local interface, click **Save**, and click **Exit** to return to the preview page.
   On the web interface, click **OK** to save all settings and exit the page.

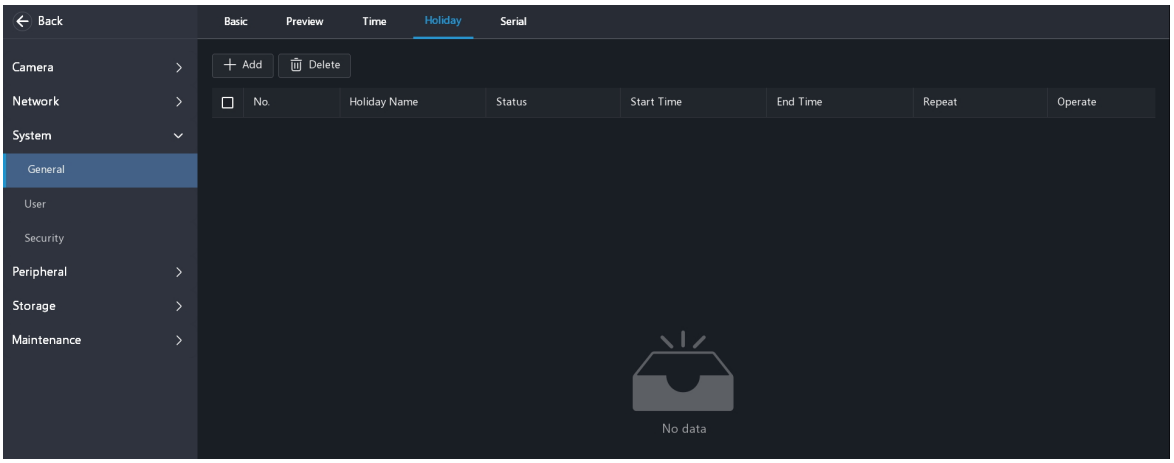
Note: If the preview page displays a "Insufficient Resources" message and automatically closes preview on video outputs not connected to any monitors, you can click to re-open it.

Advanced Configuration

Sub Stream First: Click to enable **Sub Stream First**, and the sub stream is used for live view in a multi-window layout by default.

9.3.1.5 Holiday Configuration

The regular recording or snapshot schedule repeats weekly. If the regular schedule cannot meet your requirements, you can create a special recording or snapshot schedule by designating certain times as holidays.



Add Holiday

Click **Add**, and configure the parameters.

Parameter	Description
Holiday Name	Set as needed
Status	The new holiday is enabled by default
Repeat	• No: The holiday is effective once only in the specified year. Specify a year for the holiday • Yes: The holiday is effective every year
Mode	• By Day: Set the holiday in the specified format: year/month/day • By Week: Set the holiday in the specified format: year/month/week/day of the week
Start Time/End Time	Set according to the specified format

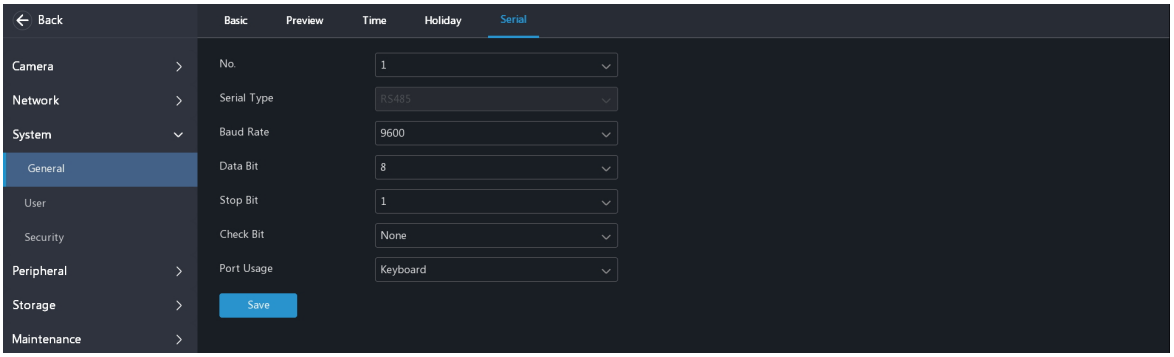
Manage Holiday

Parameter	Description
	Delete the holiday
	Edit the holiday
	Enable/disable the holiday

9.3.1.6 Serial Port Configuration

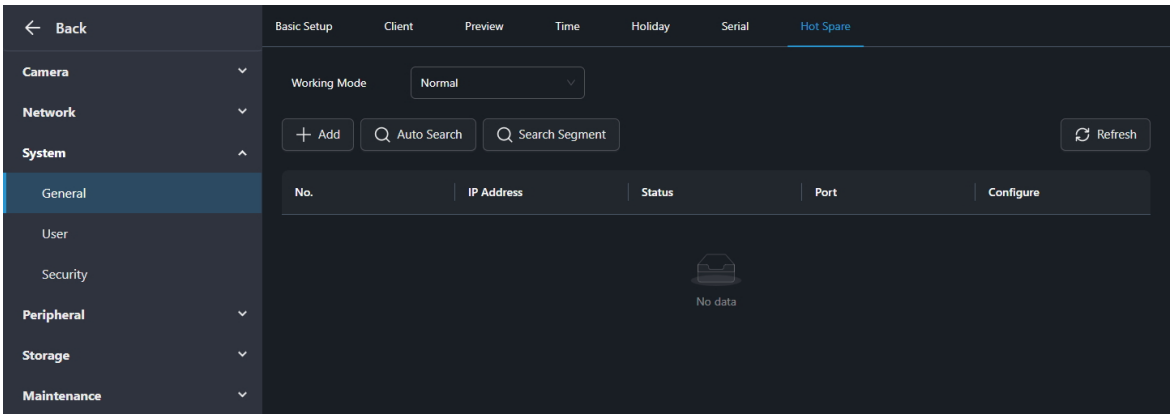
To add a keyboard to the NVR via the RS485 connection and use the keyboard to control the NVR, make sure that serial port settings configured on the NVR match those on the keyboard.

Configure the serial parameters as needed (generally keep the defaults) and click **Save**.



9.3.1.7 Hot Spare Configuration

After hot spare configuration is complete, when the NVR fails (due to network anomaly, power loss, etc.), the hot spare takes over to replace the faulty NVR. When the faulty NVR recovers, it takes over the hot spare, and the hot spare transfers stored recordings to the recovered NVR to ensure uninterrupted camera recording storage.

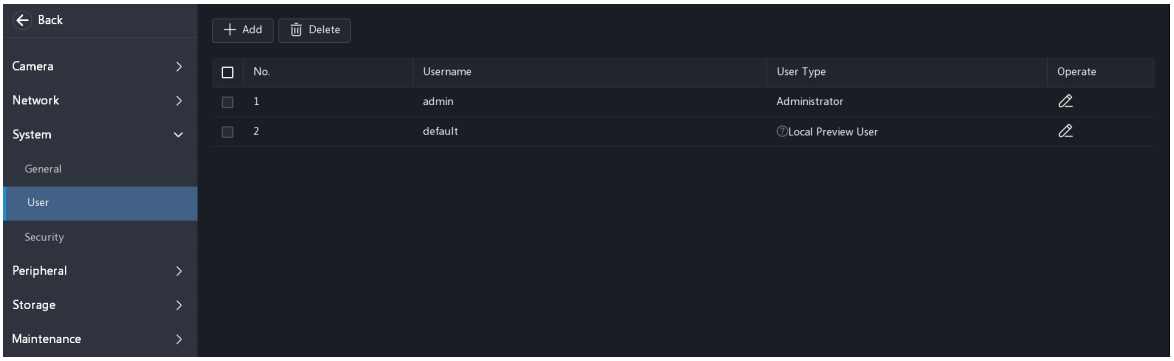


Switching the working mode will restart the device. Some of the functions, parameters, and interface will change after the device restarts.

Working Mode	Description
Normal	The NVR is used as a working device, and you need to add a hot spare to activate the hot spare function: • Custom Add: Click **Add**, and enter the backup device's IP address and password • Auto Search: Click **Auto Search** to search for devices on the same network segment. Select the desired device, click **OK**, and click to change the password into the correct one • Search Segment: Click **Search Segment**, enter the start and end IP addresses, and click **Search**. The discovered IP devices are listed. Select the desired device, click **OK**, and click to change the password into the correct one **Note:** A working device can only add a hot spare, and the number of cameras on the hot spare must be less than that on the working device; otherwise, the hot spare cannot be added.
Hot Spare	The NVR is used as a hot spare to provide backup for other working devices **Note:** Multiple working devices can add a same hot spare. If multiple working devices fail simultaneously, only one can be replaced by the hot spare; the rest wait for backup.

9.3.2 User Management

Users are entities that manage and operate the system. A user type is a set of operation permissions. After a user type is assigned to a user, the user has all the permissions defined in the type.



The system supports four user types:

User Type	Description
admin	The default super administrator, which has the maximum permissions. The initial password is **123456** **Note:** Only admin can add or delete users and edit other users' permissions.
default	The default reserved user that is used to preview the screen when no user is logged in. For example, users can still preview the screen after automatic logout when screensaver expires. The user cannot be added or deleted, only has live view and two-way audio permissions by default, and can be configured by admin only **Note:** If the default user is forbidden to use live view and two-way audio on a camera, the preview page will not display the live view of the camera, and a prompt appears on the corresponding window, **The user does not have permission**.
Operator	By default, an operator has basic permissions and camera permissions
Guest	By default, a guest only has camera permissions

Add User

Click **Add**, and add an operator or guest as needed.

Parameter	Description
Username	Set as needed
Password/Confirm	Set a strong password
Pattern	Click to enable **Pattern**, and follow on-screen instructions to set a pattern **Note:** It is only available on the local interface.
Basic Permissions/Smart Permissions/Camera Permissions	Set as needed **Note:** The smart permissions are only available on the local interface.

Delete User

Only the operator and guest users can be deleted. Click to delete the user; or select the user(s) you want to delete, and click **Delete**.

Edit User

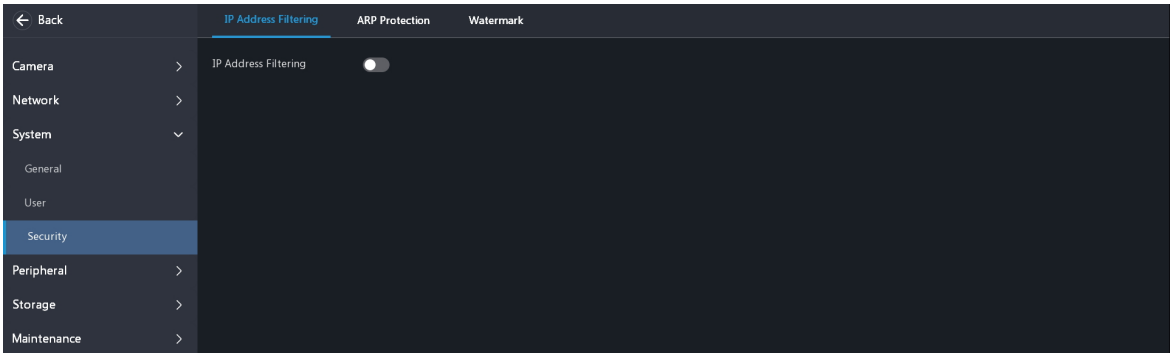
On the web interface, click and edit the user information as required. On the local interface, click , enter the user password, and edit the user information as required.
The following functions are available when you edit the admin user.

Parameter	Description
Change Online Private Protocol Camera Password	Change the login password for all online cameras connected via a private protocol to the admin user's password
Email	Enter your email address in case you need to reset the password. See Reset Password for details

9.3.3 Security Configuration

9.3.3.1 IP Address Filtering

IP address filtering allows users to access the NVR's web interface with certain source IP addresses, ensuring the device security.

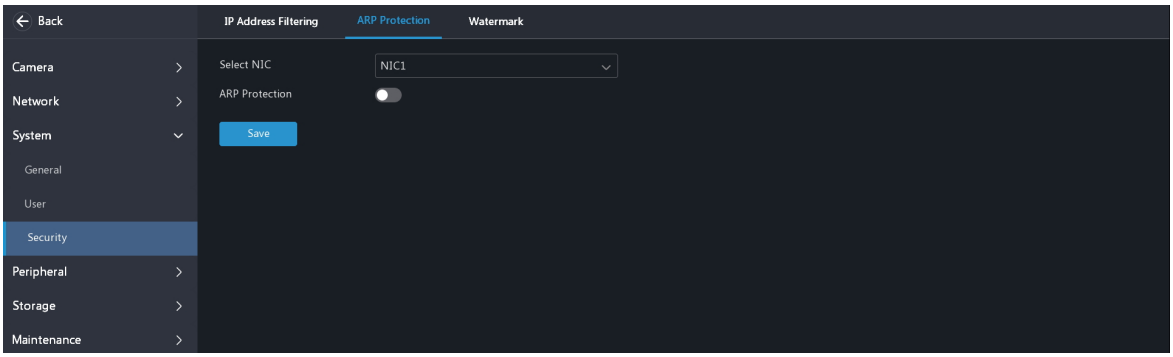


1. Click to enable **IP Address Filtering**, and choose **Allowlist** or **Blocklist**.
   - Blocklist: Access is forbidden if the IP is on the blocklist.
   - Allowlist: Access is allowed only when the IP is on the allowlist. If Allowlist is selected but is empty, remote access will be forbidden.
2. Click **Add**, and enter the start and end IP addresses.
   If you only set the start IP address on the local interface, only one IP address will be added.
3. Click **OK**.
   - : Edit the IP address.
   - /Delete: Delete the IP address.

9.3.3.2 ARP Protection

The Address Resolution Protocol (ARP) dynamically maps an IP address to a MAC address. In a local area network, ARP is necessary for devices to communicate with each other through MAC addresses. ARP attacks exploit ARP vulnerabilities to forge IP addresses and MAC addresses. ARP protection can bind the gateway's IP address and an MAC address to prevent ARP spoofing.

Note: For multi-NIC devices, this feature will be disabled automatically if you change the NIC's working mode in TCP/IP.



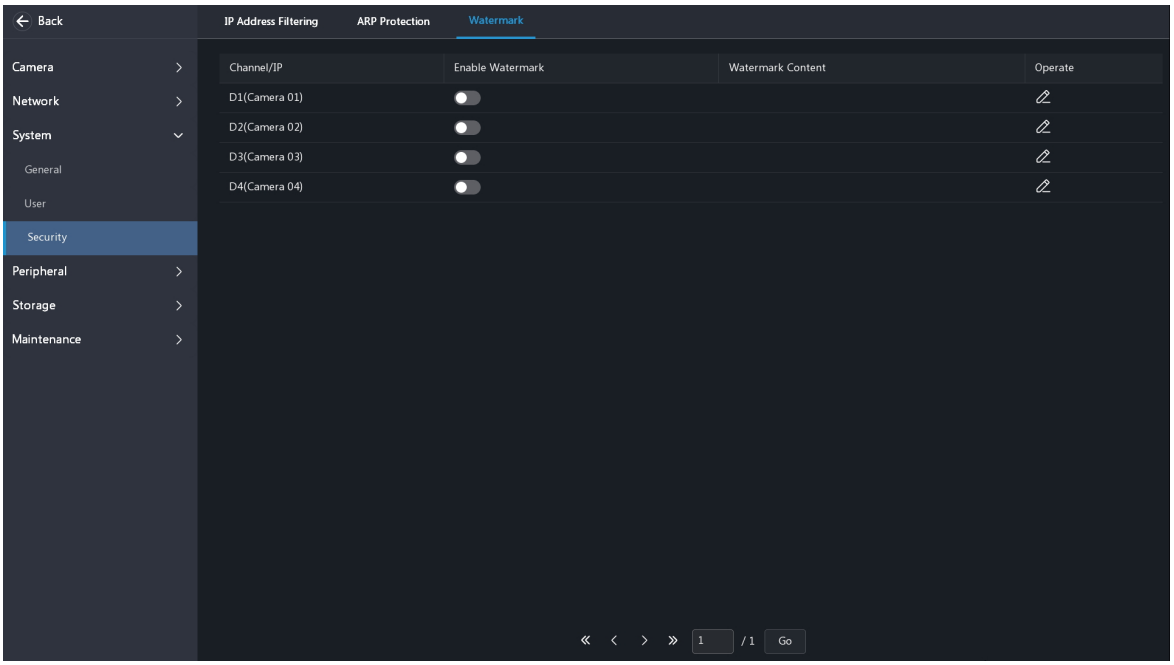
1. Select an NIC, click to enable **ARP Protection**, and configure the parameters.

Parameter	Description
Gateway	Use the gateway in TCP/IP. No configuration required
Gateway MAC Address	Custom: Enter the gateway's physical address in the network switch
	Auto: Automatically obtains the gateway's physical address in the network switch

2. Click **Save**.

9.3.3.3 Watermark

Use watermark to encrypt custom information in videos to prevent video tampering or deletion.



Local interface: Click to enable watermark for the desired camera, click , and enter watermark contents.
Web interface: Choose a camera, click to enable watermark, enter watermark contents, and click **Save**.

Note: You must use the EZPlayer to view watermarks in exported videos.

9.3.3.4 SSH

Please do not enable this function except for device maintenance and debugging.

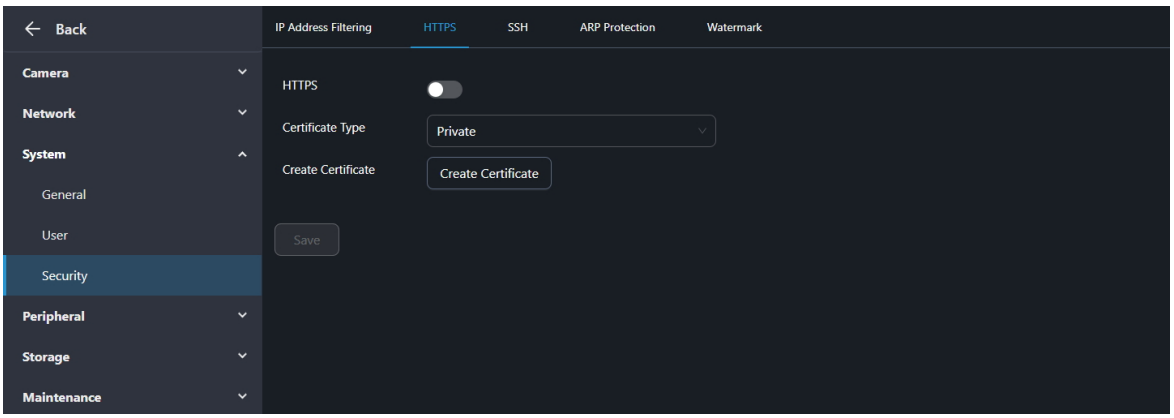
Note: It is only available on the web interface.

9.3.3.5 HTTPS

Use a digital certificate to encrypt the data transmitted between the client (browser) and the device, ensuring secure data transmission.

Note:

- It is only available on the web interface.
- Please do not create or delete certificates with HTTPS enabled.
- Private certificates are not inherently secure and may trigger "untrusted certificate" warnings in browsers. For higher security, it is recommended to generate a Certificate Signing Request (CSR) and obtaining a CA-signed certificate from a trusted Certificate Authority.



Private Certificate

A self-signed certificate generated by the device.

1. Click **Create Certificate**, enter the certificate information, and click **OK**.
   - Country/Region: Country or region code.

- Hostname/IP: Device's IP address.
- Valid Days: Set as needed.

2. Click to enable **HTTPS**, and click **Save**.
3. Log out from the account, log in again using Https:// IP address, and install the certificate in your browser's **Trusted Root Certificate Authorities** folder for normal login.

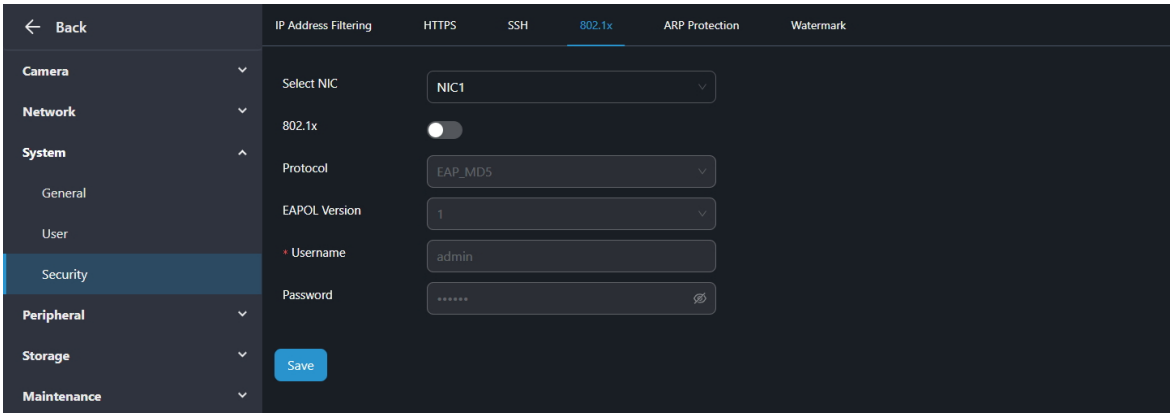
Certificate Request

A digital certificate signed by a trusted certificate authority (CA).

1. Click **Create Certificate**, enter the certificate information, and click **OK** to create a certificate request.
   - Country: Country code.
   - Hostname/IP: Device's IP address.
2. Click **Download** to download the certificate request and send it to the certificate authority for signing.
3. Click , select the signed .crt file, and click **Upload**.
4. Click to enable **HTTPS**, and click **Save**.
5. Log out from the account, and log in again using Https:// IP address.

9.3.3.6 802.1x

If the switch has enabled 802.1x authentication, the device needs to enable 802.1x when it accesses the network. After entering the username and password used for authentication, the device can access the network.



Note: For multi-NIC devices, this feature will be disabled automatically if you change the NIC's working mode in TCP/IP.

1. Select an NIC, click to enable **802.1x**, and configure the parameters.

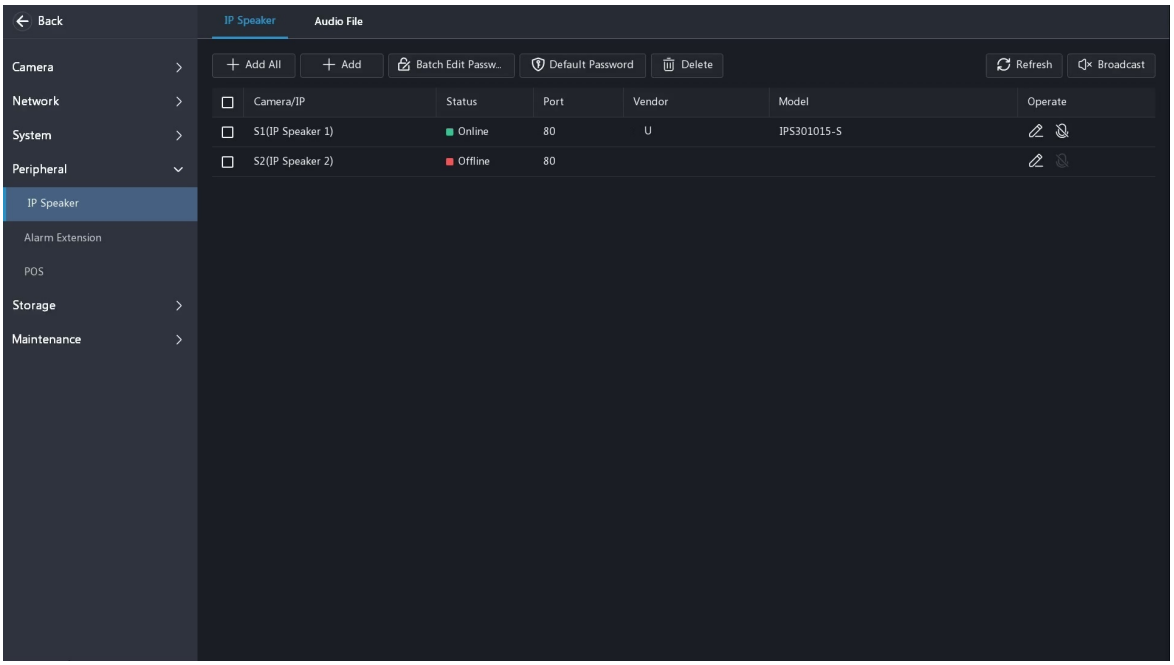
Parameter	Description
Protocol	Default: EAP-MD5
EAPOL Version	Choose **1** or **2**. It must be the same version configured on the network switch
Username/Password	Must be the username and password configured on the network switch

2. Click **Save**.

9.4 Peripheral

9.4.1 IP Speaker

9.4.1.1 IP Speaker



Enter the **IP Speaker** page, and the system automatically searches for IP speakers and lists the discovered. Click **Refresh**, and the system refreshes the list and IP speaker status.

After the configuration is complete, you can click the IP Speaker button in the bottom toolbar on the preview page to start the two-way audio or audio broadcast.

Note: Please connect an external microphone to the NVR before you use the two-way audio and audio broadcast.

Add IP Speaker

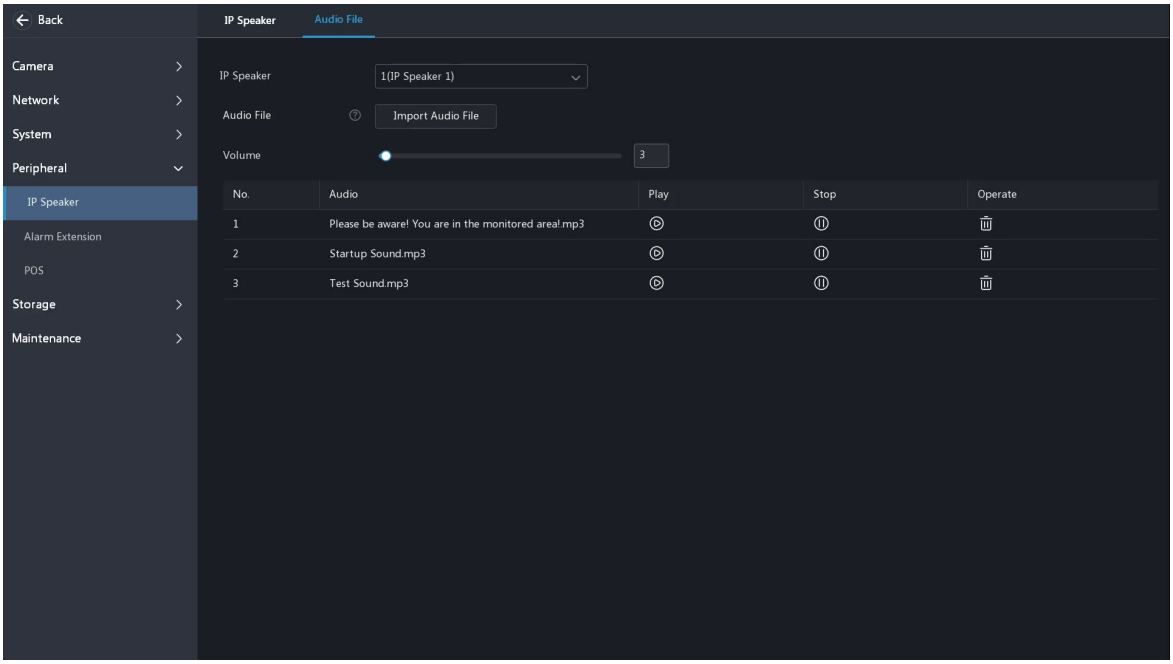
1. Add IP speakers.
   - Option 1: Click **Add**, enter the device information, click **OK**, and then check the device status. If the IP speaker is offline, hover over the icon to view the reason for the failure.
   - Option 2: Click **Add All** to add all the discovered IP speakers (if not exceeding the upper limit).
2. Test the two-way audio and audio broadcast functions.
   - Click to test the two-way audio.
   - Select the IP speaker(s), and click **Broadcast** to start audio broadcast.

Manage IP Speaker

Operation	Description
	Edit the IP speaker
Batch Edit Password	Batch change the password used to add IP speakers
Default Password	Password used to automatically add IP speakers
Delete	Select the IP speaker(s) you want to delete, and then click **Delete**

9.4.1.2 Audio File

Configure the audio file to be played by an IP speaker when an alarm occurs. It must be used with Alarm Sound.



Note: Only certain IP speakers have default audio files.

You can use the default audio file, or select an IP speaker, and click **Import Audio File** to import the desired audio file.

Operation	Description
Volume	Adjust the audio volume of the IP speaker
	Click to test the audio to be played by the IP speaker. Click to stop playing
	Edit the file name
	Delete the file

9.4.2 POS Configuration

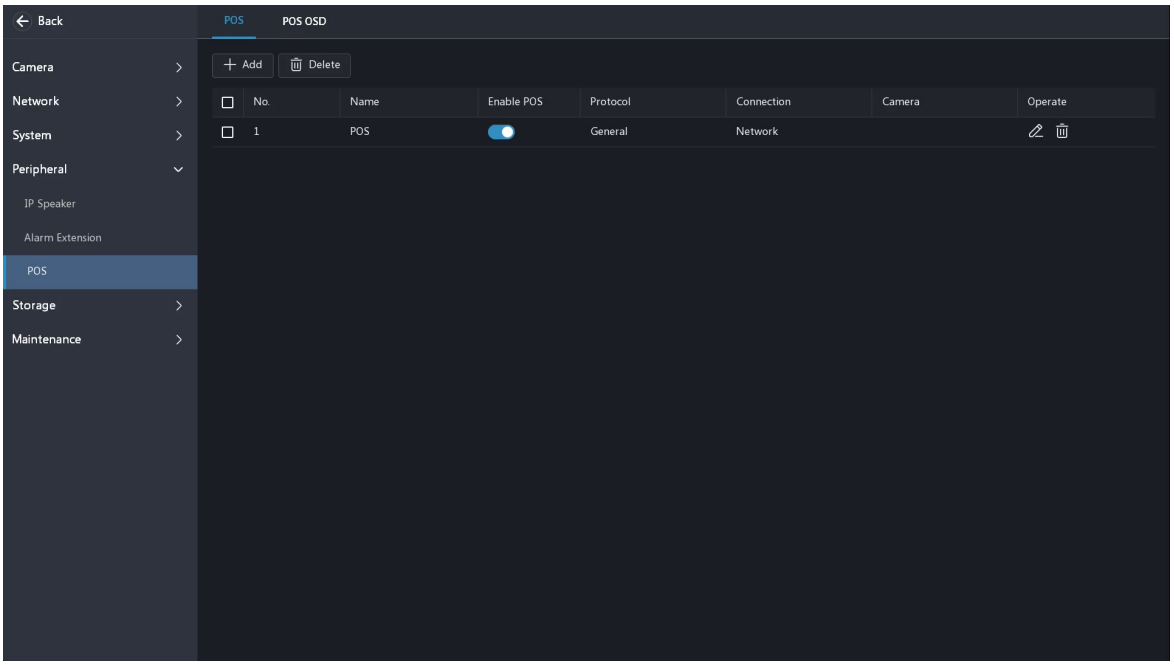
Overlay transaction information to live video and recorded videos for check and audit.

Complete POS Configuration and POS OSD Configuration before use. After the configuration is complete, POS information can be displayed or viewed on the following pages:

- Live view page: Displays the POS information in real time
- Playback page: Click POS in the bottom toolbar to view the information
- General search page: Set **Text Type** to **POS Search** to search for POS recordings based on the overlaid text information on the POS page

9.4.2.1 POS Configuration

Add POS and configure POS protocols.



1. Click **Add**, and configure the parameters.

Parameter	Description
Name	Set a name that is easy to recognize. The POS name must be unique
Enable POS	It is enabled by default
Select Protocol	• General: The POS is directly connected to the NVR **Note:** Choose this option with caution. POS connection may fail due to different protocols of different POS machine vendors. • AVE: The POS machine transmits data to the AVE device, and the AVE device connects to the NVR **Note:** AVE is a device that supports multiple POS protocols. It integrates POS data in different formats and converts them into data transmittable via TCP/UDP.
	Only applicable to the General protocol. Click **Set Protocol**. The start identifier, end identifier, and line delimiter must be converted into hexadecimal values using Notepad+ before being entered • Start Identifier: (Optional) The NVR starts receiving POS data from the start identifier • Stop Identifier: (Optional) The NVR stops receiving POS data at the received stop identifier • Line Delimiter: (Optional) The NVR inserts a line break into POS data at the line delimiter • Ignore Characters: (Optional) The NVR displays ignored POS data as * • Time Start Identifier: (Optional) Start time of POS data • Time End Identifier: (Optional) End time of POS data
Connection	Transmission Protocol: Includes TCP and UDP. Transaction data are sent to the NVR via TCP or UDP
	Local Receiving Port: Port that the NVR uses to receive data. Set an unused port
	Source IPv4 Address: IP address that the POS machine uses to send data
	Source Port: Port that the POS machine uses to send data

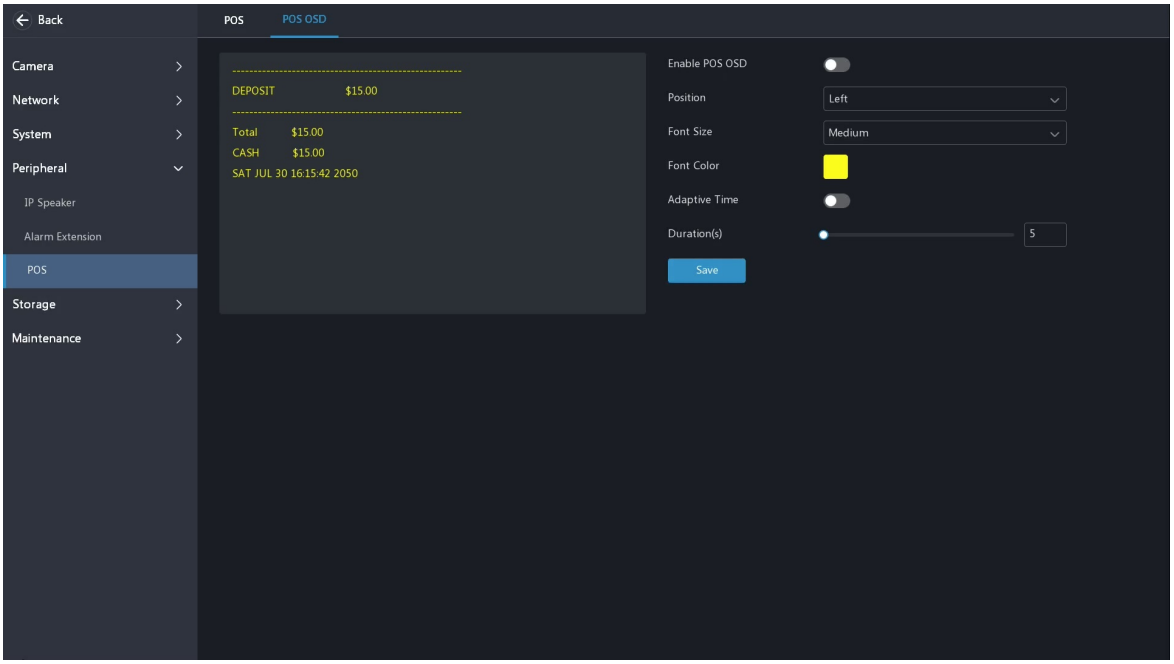
Parameter	Description
	Destination IPv4 Address: Not required. Address that the NVR uses to forward the received POS data
	Destination Port: Not required. Port that the NVR uses to forward the received POS data
	Timeout: Time that the NVR receives POS data before it stops. If a stop identifier is configured, the NVR stops receiving POS data at the stop identifier; if no stop identifier is configured, the NVR stops receiving POS data when the timeout expires. The AVE protocol does not involve start and stop identifiers. Therefore, it is necessary to configure a timeout for the NVR to stop receiving POS data and to display POS information. If no timeout is configured, the NVR does not stop receiving POS data, and POS information cannot be displayed
Select Channel	Select the channel(s) to which you want to overlay POS data

2. Click **OK**.

Operation	Description
	Edit the POS
	Delete the POS
	Disable the POS

9.4.2.2 POS OSD Configuration

Configure POS OSD parameters.



1. Enable **POS OSD**, and configure the parameters.

Parameter	Description
Position	POS OSD position • Left: In the upper-left corner of the image • Center: In the middle of the image • Right: In the upper-right corner of the image
Duration(s)	Length of time that POS OSD is displayed on the live video and playback pages

Parameter	Description
Auto	Displays POS OSD according to the POS data duration obtained based on **Time Start Identifier** and **Time End Identifier**. For **Time Start Identifier** and **Time End Identifier**, see POS Configuration
Font	Font size and color of POS OSD

2. Click **Save**.

9.4.3 Radar Configuration

NVR can receive realtime people counting data from the radar devices, and then transfer the data to UCS if connected to the cloud.

Note: The NVR does not store and search data.

1. Click **Add Radar**, and configure the parameters.

Parameter	Description
Address	IP address of the radar device
Port	Default: 80
Username	Username used to log in to the radar device
Password	Password used to log in to the radar device

2. Click **OK**.

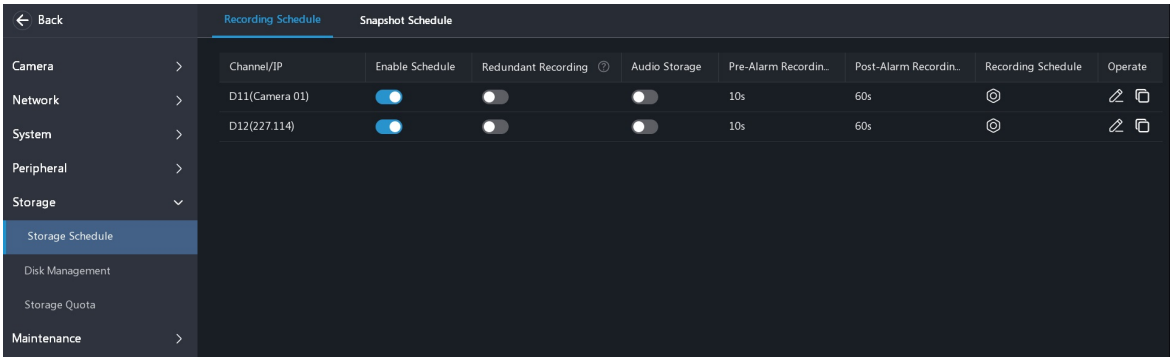
Operation	Description
	Edit the radar information
	Delete a radar device
Delete Radar	Select the radar device(s) you want to delete, and click **Delete Radar**
Refresh	Refresh the latest radar list

9.5 Storage

9.5.1 Storage Schedule

Note: By default, the NVR creates a normal recording schedule on a weekly basis for the current year. When special time periods require unique recording schedules (e.g., a specific annual date, a year-specific date, a specific week each month, or a specific week of specific month), you can set Holiday Configuration to create a special schedule.

9.5.1.1 Recording Schedule



A 24/7 normal recording schedule is enabled by default. To disable it, click  .

1. Click  , and configure the recording schedule.

Schedule Type	Description
Normal	Records video during specified time periods **Note:** If an event has configured alarm-trigger recording and occurs within the normal schedule, the event recording will be triggered.
Event	Records video in the event of an event-triggered alarm during specified time periods **Note:** The event recording schedule will only be effective if the event has configured the alarm-triggered recording.
None	No recording

2. Configure the recording schedule by drawing or editing the schedule.

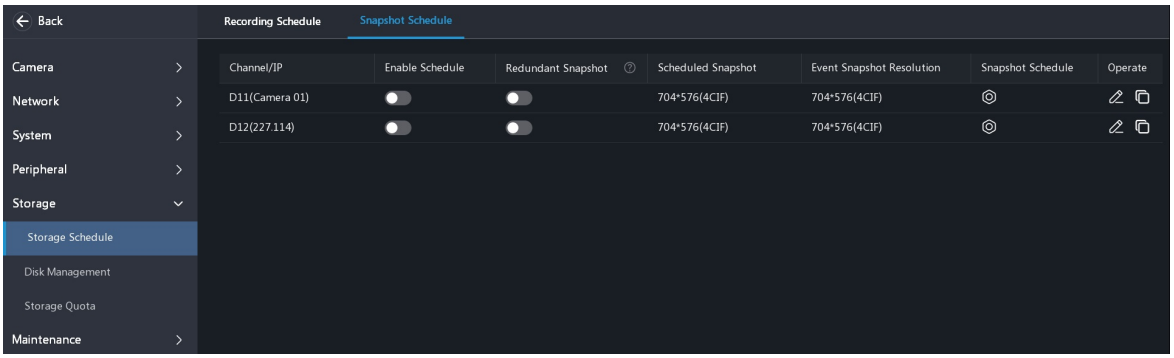
Method	Steps
Draw	The drawing area uses a 24-hour timeline as the x-axis and days of the week/ holidays as the y-axis, with each day divided into 1-hour time grids. Configure the recording schedule by clicking and dragging on the time grids. (1) Select a recording schedule type. (2) Click or drag on blank areas to draw grids. Hover over the grid to show the time period information. (3) (Optional) If the schedule does not start or end at a whole point, hover over the drawing area and modify the time period as needed. (4) Click **Save**.
Edit (only available on the web interface)	Configure the recording schedule by entering the specific start time and end time, and other parameters. (1) Click **Edit**. (2) Select a day or holiday. (3) Set time periods and the corresponding recording types. (4) (Optional) To apply the same settings to other days, select the desired day(s) or holiday after **Copy To**. (5) Click **OK**, and click **Save**.

3. Click  to configure the recording duration before or after an alarm is triggered by the event.
4. Configure other parameters.

Parameter	Description
Redundant Recording	When enabled, recordings can be stored to redundant disks synchronously to prevent video loss in case of read/write disk failure **Note:** You need to configure the redundant disk before use. See Disk Management for details.
Audio Storage	When enabled, the recording with audio can be stored **Note:** If the camera does not capture audio, the audio will not be recorded even if **Audio Storage** is enabled.

5. To apply the same settings to other cameras, click  , select the desired camera(s), and click **OK**.

9.5.1.2 Snapshot Schedule



A 24/7 normal snapshot schedule is enabled by default. To disable it, click .

1. Click , and configure the snapshot schedule.

Schedule Type	Description
Normal	Captures images at set intervals during specified time periods **Note:** If an event has configured alarm-trigger snapshot and occurs within the normal schedule, the event snapshot will be triggered.
Event	Captures images during specified time periods when the event occurs and captures images again at set intervals **Note:** The event snapshot schedule will only be effective when the alarm-triggered snapshot is set for Common Event (such as motion detection, human body detection, video loss, alarm input, call, audio detection, etc.).
None	No snapshot

2. Configure the snapshot schedule by referring to Recording Schedule.
3. Click to configure other parameters.

Parameter	Scheduled Snapshot	Event Snapshot
Resolution	When **Auto** is selected, the resolution aligns with the HD playback stream's resolution. The maximum adaptive resolution is 1080P	
Image Quality	When resolution remains constant, the higher the image quality, the clearer the detail, but the larger the file size	
Snapshot Interval	The time interval between two snapshots during specified time periods	The time interval between two snapshots during the ongoing events

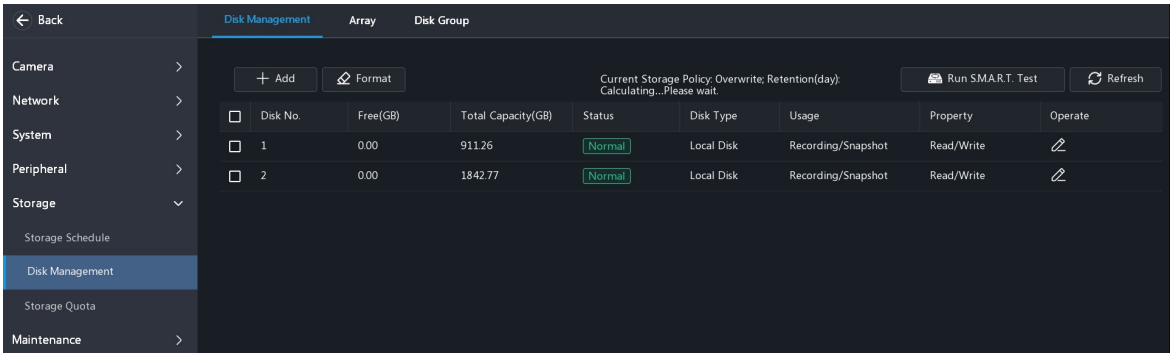
4. (Optional) Click , and the recordings can be stored to redundant disks synchronously to prevent video loss in case of read/write disk failure.

   Note: You need to configure the redundant disk before use. See Disk Management for details.

5. (Optional) To apply the same settings to other cameras, click , select the desired camera(s), and click **OK**.

9.5.2 Disk Management

9.5.2.1 Disk Management



Edit Disk Usage and Property

The local disk can be edited directly. The expansion disk (NAS, eSATA, disk enclosure) must be added first before editing. See Add Expansion Disk for details. Click and select the usage and property.

- Recording/Snapshot: The hard disk is used to automatically store recordings or snapshots. The property is available.
  - Read/Write: The recordings and snapshots can be stored and viewed.
  - Read Only: The recordings and snapshots can only be stored.
  - Redundant: Recordings and snapshots are saved to read/write disks and redundant disks simultaneously. To view recordings and snapshots on a redundant disk, you need to change the disk property to **Read Only**.
- Backup: The hard disk is used to manually back up recordings, snapshots, logs, etc. No need to select the property.

Note: The hard disk will be formatted when the usage changes.

Add Expansion Disk

NVR can expand storage resources by connecting an external storage device and adding a network storage device.

- External Storage Device

  You can connect external disks to the NVR, including eSATA and disk enclosure. The NVR must have the corresponding interface. After connecting, the external disks are displayed on the **Disk Management** page. You can click / to remove or add the eSATA disk.

- Network Storage Device

  Add devices that provide data storage services over the network. The following describes how to add a NAS.

  1. Click **Add**, and select the usage and type (see Edit Disk Usage and Property for usage details).
  2. Select the protocol according to the network where the device and NAS are located.
     - NFS protocol: Moderate security but good performance. Used to add NAS servers to the LAN.

       Enter the NAS server address (IP address or domain name) and directory (a folder path where the NAS server store videos and images).
     - SMB/CIFS protocol: Good security. Used to add NAS servers to the public network for security.

       Enter the NAS server address, directory, username, and password.

Note:

- Make sure that the corresponding protocol has been configured on the NAS before adding the NAS.
- To use SMB/CIFS protocol, make sure that the NAS server has enabled UPnP or the ports 445 and 139 have been mapped manually on the router.
- You can click to delete the NAS.

Format a Disk

Do not perform this action when the device runs normally.

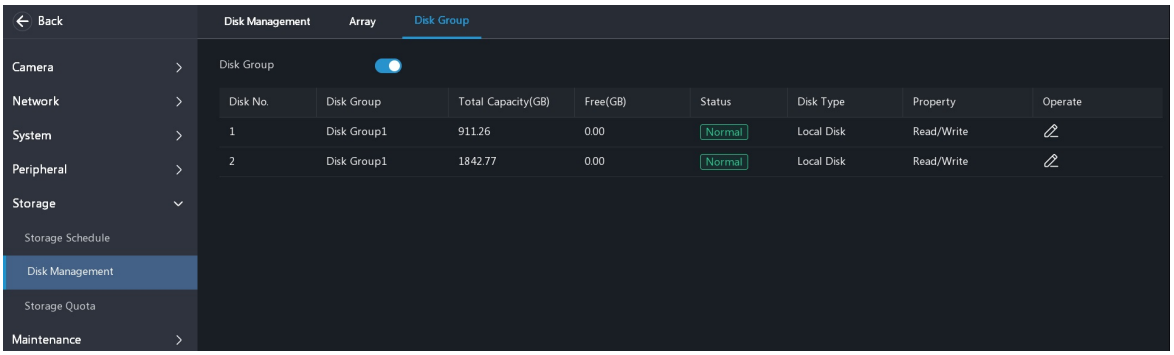
Select the disk you want to format, click **Format**, and click **OK**.

RUN S.M.A.R.T. Test

Detect and evaluate the disk health status. See Run S.M.A.R.T. Test for details.

9.5.2.2 Disk Group Configuration

To store the specified camera data on the specified hard disk, you can group disks and arrays, and configure the disk group information for the camera.



Note:

- Redundant disks cannot be assigned to any disk group.
- Disk group information will be initialized if any disk in the group is formatted.

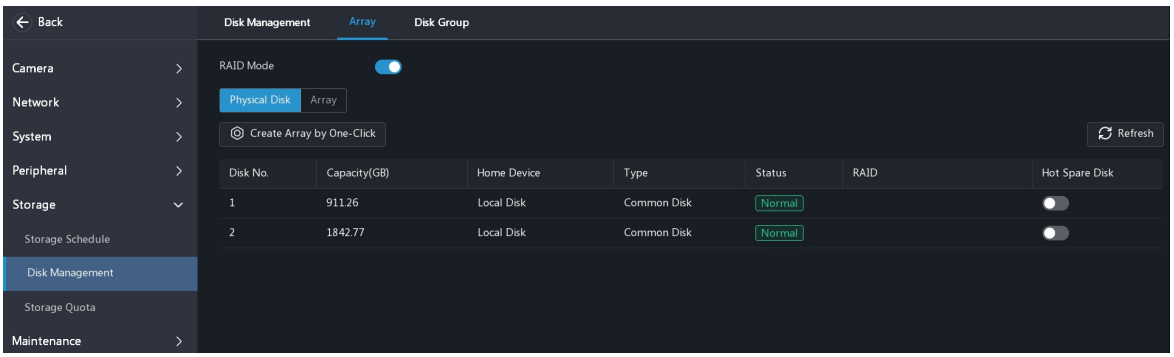
1. Click to enable **Disk Group**.
2. The disk group for the disk or array is disk group 1 by default. You can click to select the desired disk group.
3. Enter the **Storage Quota** page, click and select the disk group for the camera.

   Note: By default, the disk group for the newly added camera is disk group 1.

9.5.2.3 Array Configuration

The array can improve disk storage performance and data security by optimizing data distribution and providing redundancy mechanisms.

Note: Only local hard disks and disks in an expansion enclosure can be used to create arrays, but they cannot be used at a time.



Click , and click **OK** to enable **RAID Mode**.

Automatically Create an Array

On the **Physical Disk** tab, click **Create Array by One-Click**, then the system automatically completes array creation based on the number of available disks.

Available Disks	Array Type
2	RAID1

Available Disks	Array Type
3	RAID5
≥4	RAID5, a hot spare disk will be created automatically **Note:** A hot spare disk can automatically replace a failed disk in any RAID array to ensure stable array operation.

Manually Create an Array

You can manually create arrays if you have specific requirements for array configuration. To maximize storage space when creating manual arrays, follow these matters:

- Make sure all disks are used to create arrays. Disks that are not used to create arrays are unusable.
- Please select disks with the same or similar capacity. When creating the array, the available space for each disk is determined by the capacity of the smallest disk. Disks with a larger capacity can only use the same space.

1. Enter the **Physical Disk** tab.
2. (Optional) Select a disk and click  to set it as a hot spare disk.

   Note:

   - No hot spare disk will be created automatically if you create arrays manually. To ensure successful automatic array rebuilding and stable system operation, it is recommended to set a hot spare disk, and the capacity of the hot spare disk must not be less than that of the smallest disk in the array.
   - If there are multiple arrays and you require highly stable arrays, you can configure multiple hot spare disks. When multiple arrays degrade, the hot spare disks are used to rebuild them in order of disk number. However, too many global hot spare disks may cause waste of disk resources, so please set them as required.
3. Enter the **Array** tab, and click **Create**.
4. Enter the array name, select the array type, and select the desired disk(s). The number of disks required (excluding hot spare disk) may vary depending on the array type. You can refer to the following table.

<table>
<tr><th>Array Type</th><th>Number of Disks</th><th>Number of Sub-array Disks</th><th>Number of Disks Required</th></tr>
<tr><td>RAID0</td><td>2 to 8</td><td rowspan="5">-</td><td rowspan="5">The same as the number of disks</td></tr>
<tr><td>RAID1</td><td>2</td></tr>
<tr><td>RAID5</td><td>3 to 8</td></tr>
<tr><td>RAID6</td><td>4 to 8</td></tr>
<tr><td>RAID10</td><td>4 to 16, an integer multiple of 2</td></tr>
<tr><td>RAID50</td><td>6 to 16</td><td>3 to 8</td><td rowspan="2">An integer multiple of the number of sub-array disks. For example, if the number of sub-array disks is 4, the number of disks required is 8</td></tr>
<tr><td>RAID60</td><td>8 to 16</td><td>4 to 8</td></tr>
</table>

5. Click **OK**.

Rebuild an Array

You can rebuild an array to recover the data if the array is damaged or degraded. You can maintain disks in time by checking the disk status on the **Array** tab.

Array Status	Description
Normal	The array is functional
Degraded	A state between **Normal** and **Damaged**

Array Status	Description
Damaged	Some physical disks in the array are not functional properly and the number of functional disks is less than the minimum number of disks required for the array

Note:

- For example, in a RAID 5 array with 4 disks, the array is in **Degraded** state when 1 disk is abnormal, and in **Damaged** state when 2 disks are abnormal.
- To be alerted when an array is degraded or damaged, you can configure alarm-triggered actions in Alert.

Rebuild Mode	Description	Operation Steps
Auto	A degraded array can be automatically rebuilt in ten minutes if a hot spare disk is available and the capacity of the hot spare disk is not less than that of the smallest disk in the array **Note:** After rebuilding, replace the failed disk in time and set the replaced disk as a global hot spare to ensure the stable operation of the array.	No operation required
Manual	• A degraded array that is found manually can be rebuilt when the array meets the criteria for auto-rebuilding but the 10-minute threshold is not reached • A degraded array can only be rebuilt manually if no hot spare disk is available	1. Enter the **Array** tab, and click **Create**. 2. Select the initialization type. • Normal: Low rebuilding speed but low data loss risk • Quick: Fast rebuilding speed but high data loss risk 3. Select a disk number of an available disk to replace the failed disk. 4. Click **OK**.

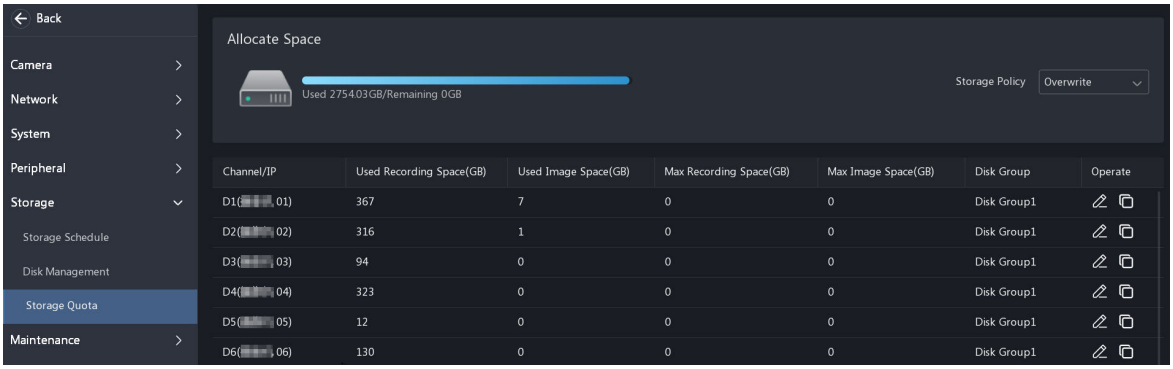
Delete Array

Deleting an array will invalidate the array and delete all the disk data; Back up important data before operation.

Click for the array you want to delete, and click **OK**.

Note: When array mode is disabled (without array deletion), the stored data cannot be searched until the array is re-enabled.

9.5.3 Storage Quota



Allocate Space

Allocate appropriate storage space for each camera to meet the specific retention period requirements.

Click to allocate space for the camera.

Parameter	Description
Disk Group	If **Disk Group** is enabled, it is required to select a disk group for the camera
Max Recording Space	Used to store HD stream videos, smart snapshots, POS data, people flow data, and heat map images
Max Image Space	Used to store common snapshots, such as snapshots captured by schedule or manually

Configure Storage Policy

Data storage policy when the storage is full. Select a policy from the **Storage Policy** drop-down list.

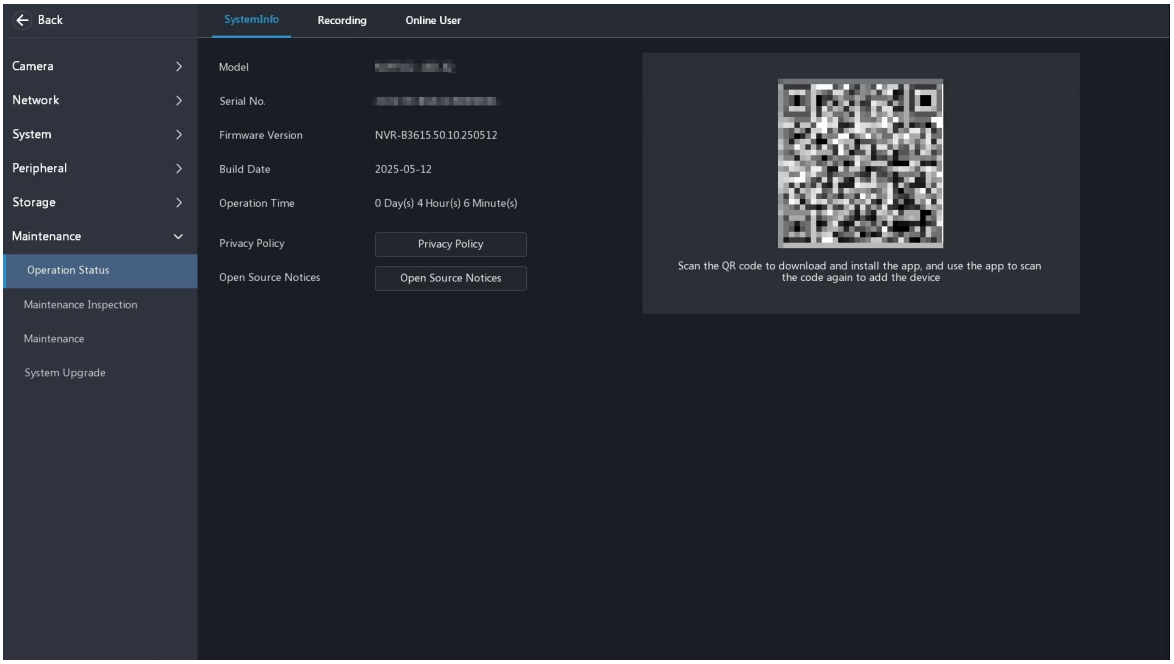
Storage Policy	Description
Overwrite	When the storage is full, the oldest data will be overwritten to continuously use the storage space. This policy applies to scenarios where continuous recording is required but complete data storage is not necessary. The disk space is divided into allocated space and remaining space according to whether the disk is used for storage by cameras. If no disk group is configured, the camera can use the total capacity of all hard disks; if a disk group is configured, the camera can only use the total capacity of the specified disk group • If a camera is not allocated storage space, it will use the remaining space of the disk or disk group **Note:** As the remaining disk space is variable, please allocate storage space with caution. For example, on a device with 20GB disk capacity and two cameras, if camera 1 is allocated 10GB, camera 2 will use the remaining 10GB if it is not allocated storage space. In this case, camera 2 can store the last 5 days of recordings. However, if camera 3 is added to the device, there will be less storage space available to camera 2, and fewer days of recordings can be stored. • If a camera is allocated storage space, it will use that space for data storage
Stop	This option is only effective to cameras that have been allocated storage space. When the allocated space of a camera is used up, new recordings/snapshots will not be saved. You need to manually release or expand storage space. This policy applies to scenarios requiring complete data storage

Note: You can configure Alert to timely monitor the camera storage space when the storage is full or almost full.

9.6 Maintenance

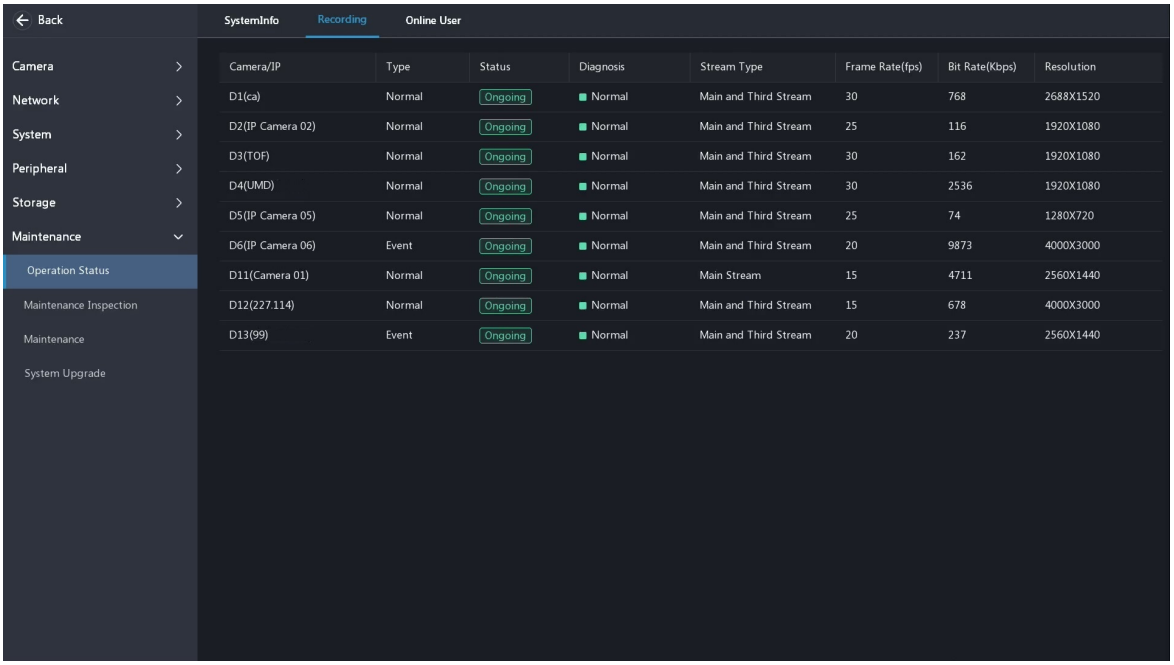
9.6.1 Operation Status

View system information, recording status, and online users.



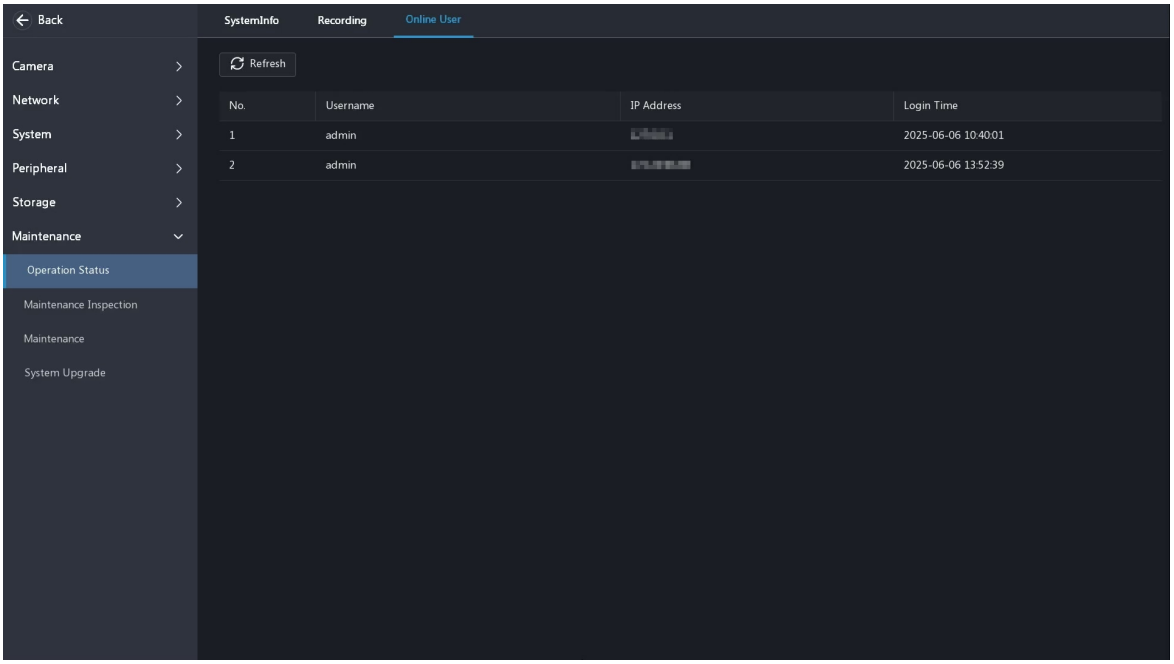
9.6.1.1 Recording Status

View the recording status of the connected cameras.



9.6.1.2 Online User

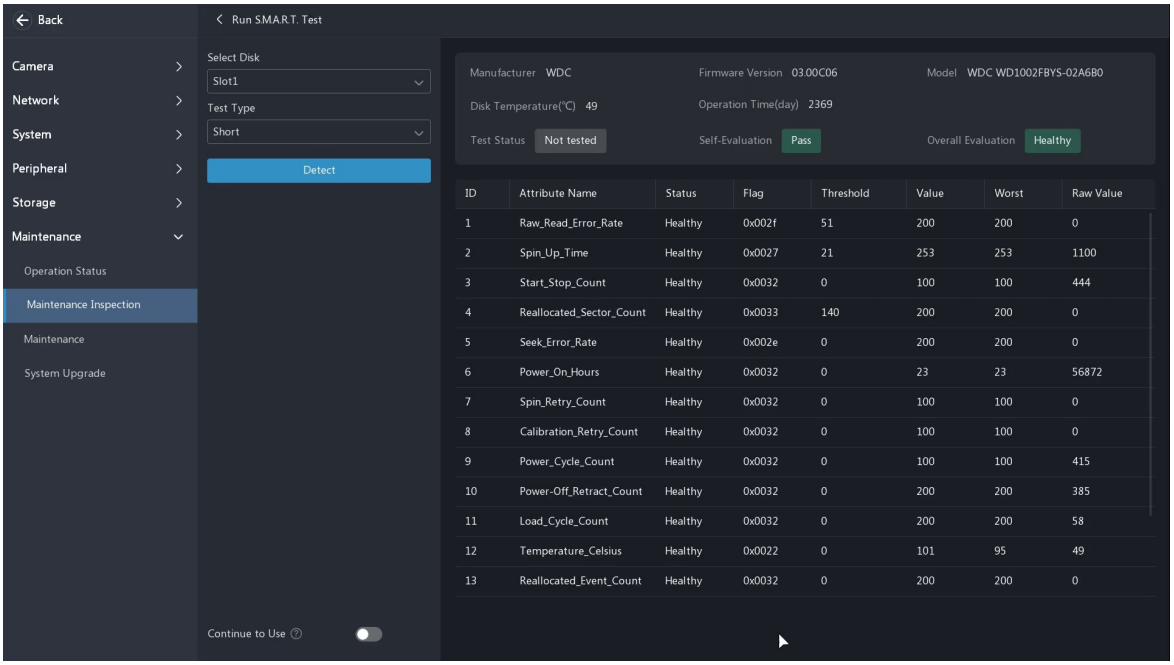
View online user information.



9.6.2 Maintenance Inspection

9.6.2.1 Run S.M.A.R.T. Test

S.M.A.R.T. tests the hard disk including its head, platter, motor, circuit, etc. and evaluates the disk health status.



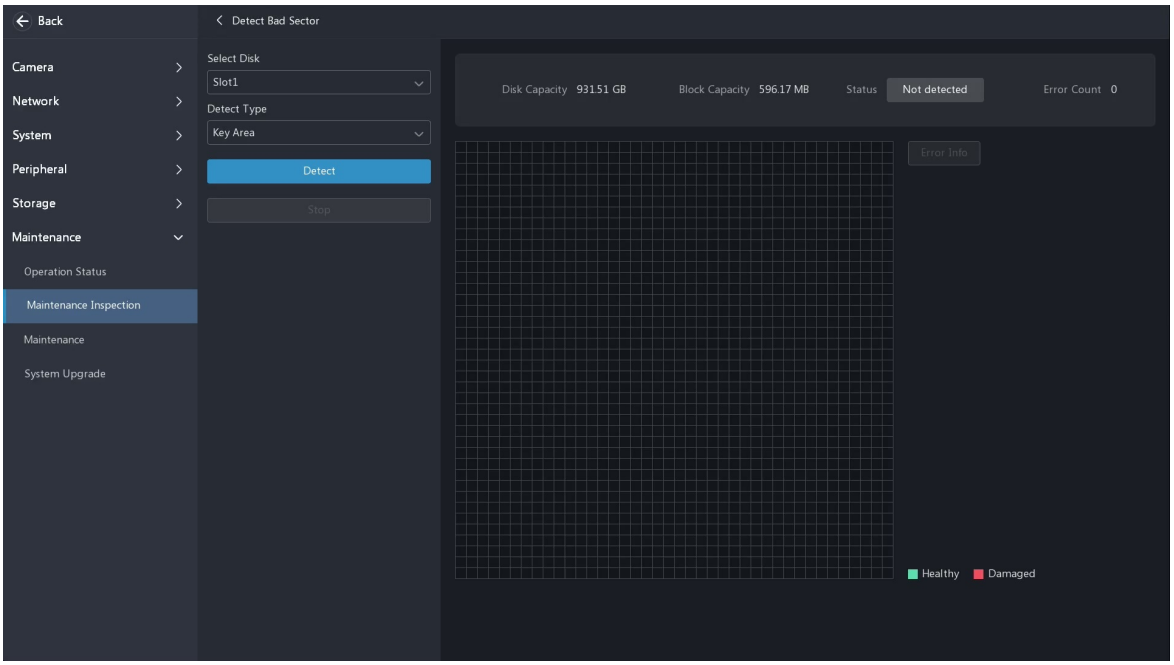
Choose the disk slot and test type, and click **Detect**.

- Short: Less test contents, faster speed.
- Extended: More comprehensive and thorough, longer time.
- Conveyance: Detects problems in data transmission.

The overall evaluation provides three kind of status: Healthy, Failure, Bad Sectors. If the disk fails in the self-assessment but the device needs to continue using the hard disk, you can click to enable **Continue to Use**. However, this may incur great risks. Please choose carefully.

9.6.2.2 Bad Sector Detection

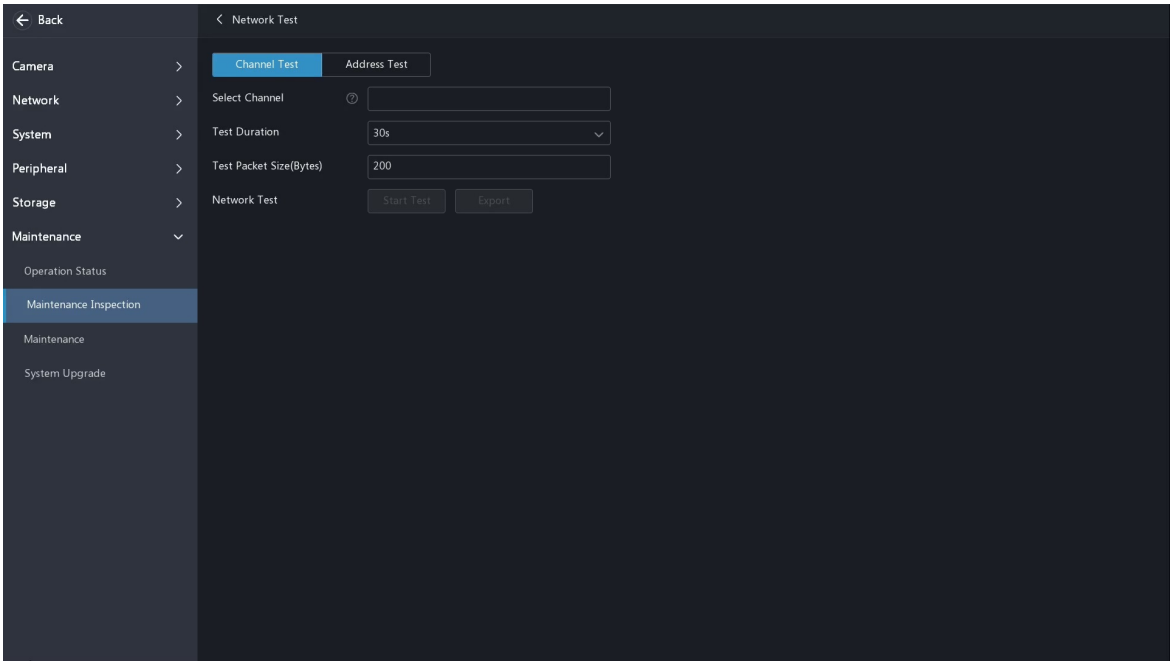
Detect bad sectors in hard disks in a read-only manner.



Choose the disk slot and detection type, and click **Detect**. The detection stops automatically when the error count reaches 100.

9.6.2.3 Network Test

Monitor the network latency, packet loss rate, etc.



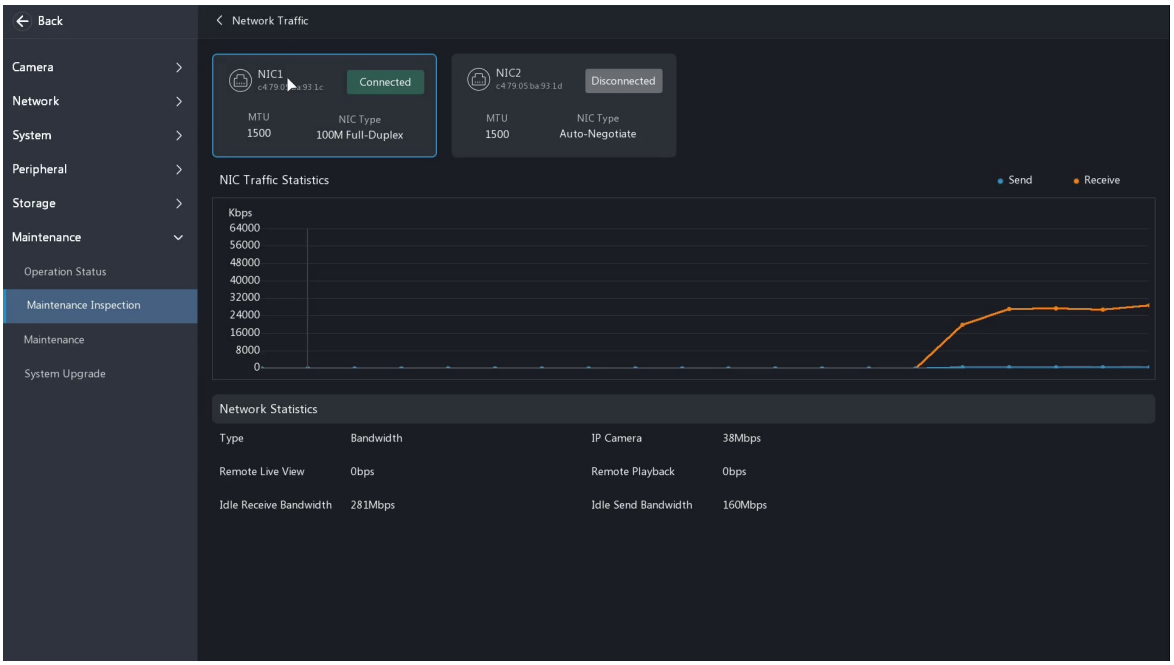
1. Choose the test mode.
   - Channel Test: Detect the network conditions of the channels added to the device. You can choose multiple channels.
   - Address Test: Detect the network conditions of other devices connected to the device. For example, enter the IP address of the upper platform, and the system will detect the network conditions between the device and the upper platform.
2. Select the channel(s) or enter the address you want to test, and configure the test parameters.
   - Test Duration: The system will test the network status of the channel/address during this time duration.
   - Test Packet Size (Bytes): The size of a detection packet. Set according to the actual network condition.
3. Click **Start Test**, and export the results as needed.

- Local interface: Close the test results page, and click **Export** to export the results to an external storage device.
- Web interface: Export the results to your computer.

The exported file is a .tgz package, including ping logs of all the test targets and one summary file.

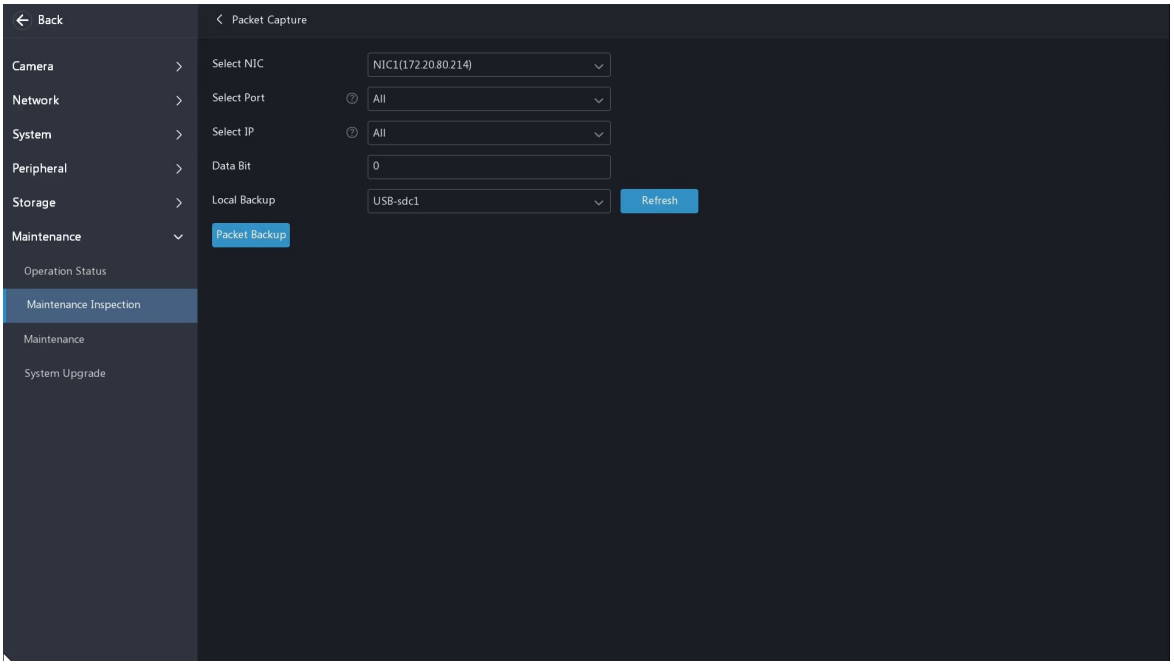
9.6.2.4 Network Traffic

View network interface card (NIC) information including connection status, physical address, MTU, NIC type, and real-time traffic.



9.6.2.5 Packet Capture

Capture, view, and save network packets for network security.



1. Choose an NIC and configure the parameters.

Parameter	Description
Select NIC	• NIC 1/2/3...: Capture transmission packets of the NIC • Loopback interface: Capture operation packets of the device

Parameter	Description
Select Port/IP	• All: Capture packets of all the ports and IPs connected to the device • Specify: Capture packets of the specified ports and IPs • Filter: Capture packets except those of the specified ports and IPs
Data Bit	It is 0 by default, which indicates that there is no size limit for the captured packet data. You can set it as needed

2. Set the port and IP.
3. Set the data bit.
4. On the local interface, choose a destination path, and click **Packet Backup**. On the web interface, click **Start**.
5. Save the captured data.

   Local interface: After the task is complete, click **OK** on the progress page, and the captured data will be saved to the root directory of the USB storage device.

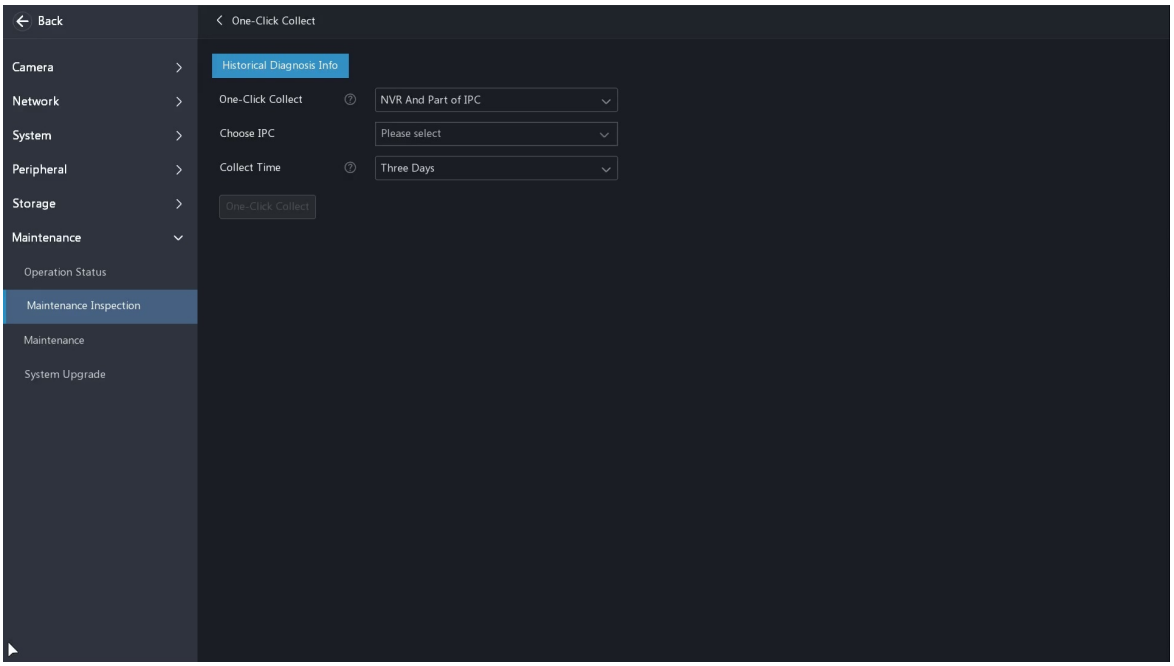
   Web interface: After the task is complete, the export button is highlighted. Click **Export** to save the captured data to your computer.

Note:

- The device cannot capture packets if a capturing task is already started on the web interface.
- The file containing the captured packets is named in this format: NIC_YYYYMMDD_hhmmss.pcap, for example, eth0_20220815_163632.pcap.
- When UNP or PPPoE dial-up succeeded, a virtual NIC appears in the NIC list. You can also capture packets of the NIC.

9.6.2.6 One-Click Collect

Collect NVR and camera diagnosis information.

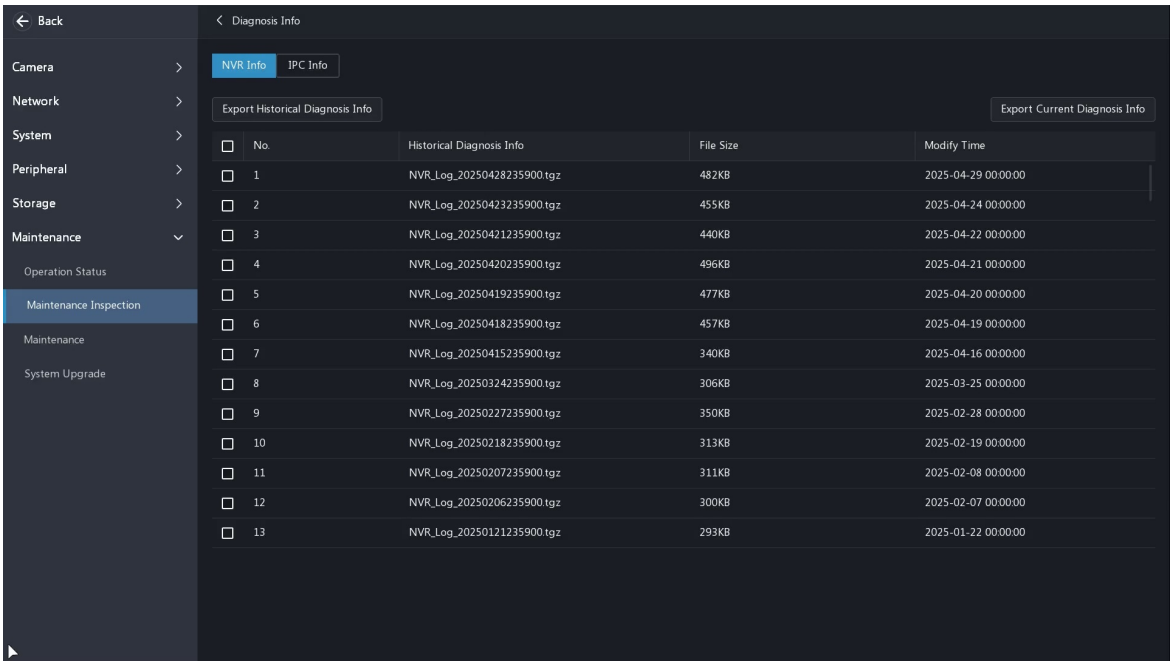


Choose the camera and select a number of days of diagnosis information to be collected, and click **One-Click Collect**.

Note: Choose the days according to the actual requirements. The export process may take a long time if you choose **All**.

9.6.2.7 Diagnosis Information

View and back up diagnosis information of the NVR and the connected cameras. The NVR keeps 14 days of diagnosis information and overwrites the earliest when the storage is full.

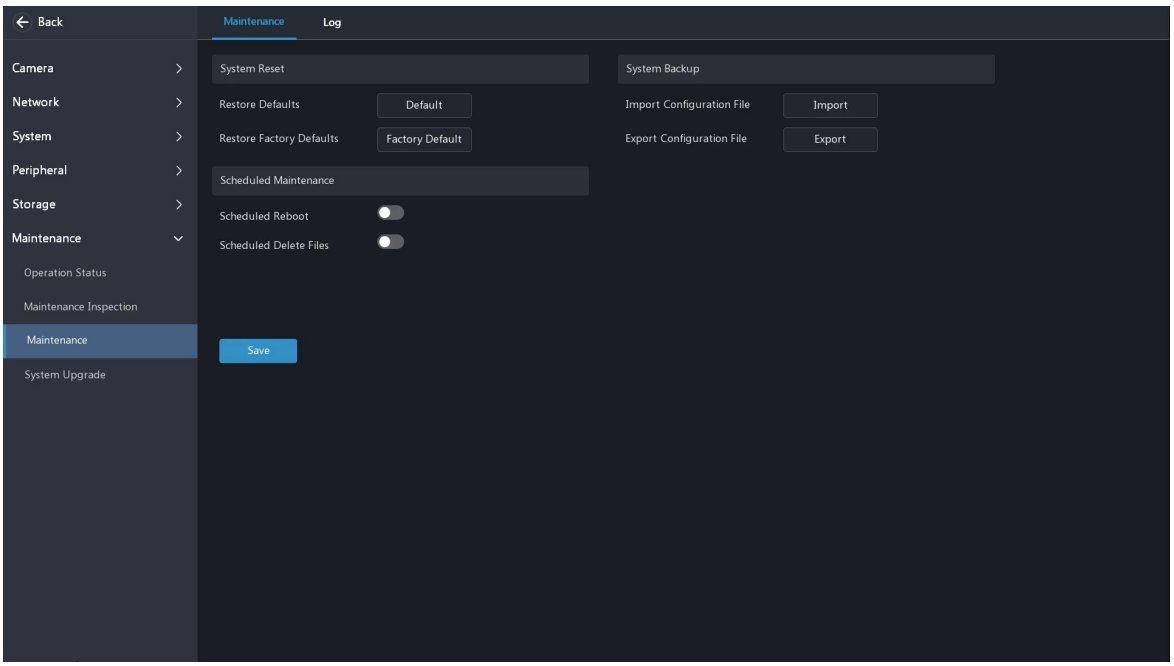


- Export Current Diagnosis Info: Diagnosis information since the latest startup. Click **Export Current Diagnosis Info**, choose the destination path, and click **OK**.
- Export Historical Diagnosis Info: All the historical diagnosis information in the list. Select the desired item(s), click **Export Historical Diagnosis Info**, choose the destination path, and click **OK**.

Note: The button on the web interface is **Batch Export Historical Diagnosis Info**.

9.6.3 Maintenance

9.6.3.1 Maintenance



System Reset

- Restore Defaults: Restore default settings except network settings, user settings, and time settings.
- Restore Factory Defaults: Restore all default settings.

Note: Either option will not delete the recordings and operation logs.

System Backup

Import or export system configurations.

Note:

- Importing configurations will restart the device. If power is disconnected during the process, the system will be unusable.
- Only admin can import or export configurations.

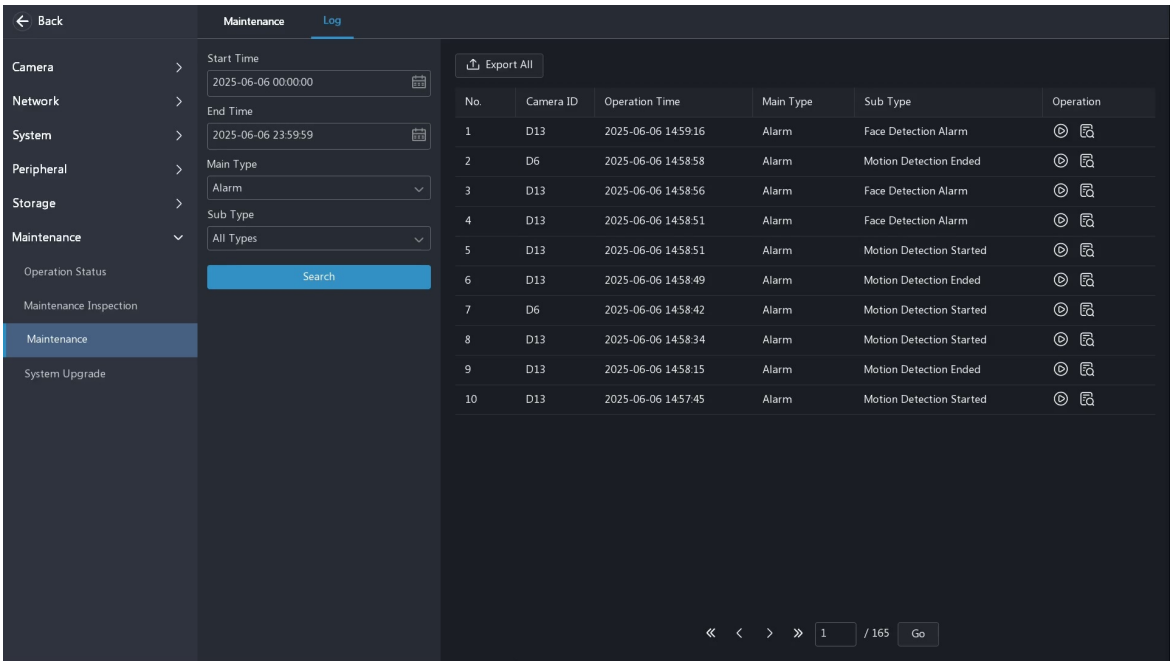
Scheduled Maintenance

The system can restart or delete files automatically at the pre-set time. Only admin can perform this operation.

- Scheduled Reboot: The system restarts automatically at the set time.
- Scheduled Delete Files: The system automatically deletes files saved before the set time.

9.6.3.2 Log Search

Search the logs to view the device operation status and alarm details.



Select the start time, end time, main type, and sub type, and click **Search**.

- Click , and click to play the video recorded at the current log time.
- Click to view the log details.
- Click **Export All** to export logs.

Note:

- The playback function is not available to certain log types.
- The video is 11 minutes long (1 minute before the alarm and 10 minutes after the alarm). Post-alarm video for some recent logs may be less than 10 minutes because the video storage is less than 10 minutes.

9.6.4 System Upgrade

9.6.4.1 NVR Upgrade

Upgrade the firmware of the NVR.

Cloud Upgrade

Click **Check for Update**. The system checks for updates.

- Upgrade the version if a new version is found.

Device Function	Upgrade Step
Major firmware upgrade unsupported	Click **Upgrade** and wait on this page for the process to complete.
Major firmware upgrade supported	1. Click **Download Version** and view the download progress. **Note:** The version download runs in the background, so you can freely switch pages or perform other operations during this process. 2. Once the download is complete, click **Upgrade** and wait on this page for the process to complete.

- An upgrade is unavailable if the current version is the latest one.

Local Upgrade

Select the upgrade file in the USB storage device, and click **Upgrade** to start.

Note: If the upgrade failed, the failure cause will be displayed, and the device will restart automatically. Fix the problem and then try again.

9.6.4.2 IPC Upgrade

Upgrade the firmware of the IPC. This function is only applicable to cameras connected via the private protocol.

- Cloud Upgrade

  Click **Check for Update**. The system checks for updates.

  - If updates are available, the new version number and its build date are displayed. Click to upgrade a camera, or select multiple cameras and then click **Upgrade** to upgrade in batches.
  - If no updates are available, the system indicates that the current version is already the latest.
- Local Upgrade

  1. Click to upgrade a camera, or select multiple cameras and then click **Batch Local Upgrade**.
  2. On the **Batch Upgrade Camera** page, select the upgrade file in the USB storage device, and then click **Upgrade**.

10 Power

Device restart, logout, and shutdown.

Appendix

The following introduces various search methods for alarm results.

Function usage instructions:

- To search recordings on the playback, video search, and event search pages, the camera must have alarm-triggered recording enabled.

  Note: For the smart events, the alarm-triggered recording for the set camera is unavailable to other cameras.
- To search pictures on the picture search page, the camera must have alarm-triggered snapshot enabled.
- When the event-triggered recording for smart events is disabled, alarm results can still be searched on the event search and target search pages. As smart events have no alarm-triggered snapshot configuration, the relevant pictures can be searched directly.

Search Page	Search Criteria	Description
Preview	Camera that currently plays the live view	Shows real-time snapshots of the subscribed alarm types

Search Page	Search Criteria	Description
Playback	In the event mode • Specified date • One camera • Event type	The event recordings are displayed green/red highlights on the playback timeline, and can be clipped, exported, or locked as needed. Recording duration = Alarm recording time + Pre-alarm recording time + Post-alarm recording time **Note:** By default, the pre-alarm recording time is 10 seconds and the post-alarm recording time is 60 seconds. The pre-alarm recording is only available during the event recording time periods set in Recording Schedule.
Video Search	• Start time and end time • One camera, multiple cameras	Shows partition recordings triggered by the event alarm in list mode; recordings can be locked or exported as needed **Note:** One partition of the hard drive is 256M, with 252MB for video storage (actual usage ≤252MB) and the remaining 4MB for index data. Therefore, the exported video file will not exceed 252MB.
Picture Search		Shows pictures in list mode; pictures can be exported as needed
Event Search		• Smart events: Search for recordings by event type. The results are displayed in tile mode, with alarm-triggered targets as thumbnails. The recordings and pictures can be exported as needed • Common events: The recordings from event start to end are displayed in list mode and can be exported as needed
Target Search		Search for event recordings by target type and event type. The results are displayed in a tile mode with alarm-triggered as thumbnails. The recordings and pictures can be exported as needed
Alarm Search		Shows recordings in list mode; recordings can be exported as needed
Camera Alarm	• Today • All cameras	Shows the recordings when the alarm is triggered and the recordings before and after the alarm is triggered in list mode; recordings can be exported as needed • Local interface: 1min pre-alarm recordings + 10min post-alarm recordings • Web interface: 5s pre-alarm recordings + 10s post-alarm recordings
Log Search	• Start time and end time • All cameras	