Network Video Recorder

User Manual

Revision 1.0

Preface

This manual introduces the functions and operations of the Network Video Recorder. Please read it carefully before using the device, and keep this manual in a safe place for future reference.

Privacy Notice

As a device user or data controller, you may collect personal data from others, such as facial images, audio, fingerprints, and license plate numbers. You are required to comply with local privacy protection laws and regulations by implementing measures to protect the legitimate rights and interests of others, including but not limited to the following: providing clear and visible identification to inform people of the presence of monitoring areas and offering the necessary contact information.

Safety Instruction

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a moderate or low potential hazard that, if not avoided, could result in minor or moderate injury.
⚠ CAUTION	Indicates potential risks that, if not mitigated, may lead to property loss, data loss, performance degradation, or unpredictable outcomes.
TIPS	Providing ways to help you solve problems or save time.
NOTE	Provide additional information as a text supplement.

About the Manual

- This manual is for reference only. There may be slight differences between the manual and the product.
- We are not responsible for any losses resulting from the operation of the product in a manner that does not comply with the manual.
- The manual will be updated in accordance with the latest laws and regulations of the relevant jurisdictions. For detailed information, please refer to the printed user manual, use our CD, scan the QR code, or visit our official website. This manual is for reference only. There may be slight differences between the electronic version and the printed version.
- All designs and software are subject to change without prior written notice. Product updates may result in some discrepancies between the actual product and the manual. Please contact customer service for the latest Process and supplementary documentation.
- There may be errors in printing, or deviations in the descriptions of functions, operations, and technical data. In case of any questions or disputes, we reserve the right to make the final interpretation.
- If you are unable to open the manual (PDF format), please upgrade your reader software or try other mainstream reader software.
- All trademarks, registered trademarks, and company names in the manual are the property of their respective owners.
- If you encounter any issues while using the equipment, please visit our website to contact the supplier or customer service.
- In case of any uncertainties or disputes, we reserve the right of final interpretation.

Important Safety Instruction and Warning

Transportation Requirements

Transport the device under permitted humidity and temperature conditions

Storage Requirements

Store the device under permitted humidity and temperature conditions.

Operation Requirements

- Please do not place the device in direct sunlight or near a heat source.
- Please keep the device away from moisture, dust, and smoke
- Install the device on a stable surface to prevent it from falling.
- Please do not spill or splash liquids onto the device, and ensure that there are no containers with liquids on the equipment to prevent liquids from entering the interior of the device.
- Place the device in a well-ventilated area and do not obstruct its ventilation openings.
- Operate the device within the rated input and output power range.
- Please do not disassemble the device.
- Use the device under allowed humidity and temperature conditions.
- Replace unwanted batteries with new batteries of the same type and model.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly follow to local electrical safety regulations and standards. Ensure that the environmental voltage is stable and meets the power supply requirements of the device.
- Do not expose the battery to extremely low pressure or extremely high or low temperatures. Additionally, it is strictly prohibited to throw the battery into fire or an oven, and cutting or

applying mechanical pressure to the battery is also forbidden. This is to avoid the risk of fire and explosion.

- Please use a standard power adapter or cabinet power supply. We do not accept any liability for injuries or damages caused by the use of non-standard power adapters.
- Please do not place the device in direct sunlight or near heat sources.
- Please keep the device away from moisture, dust, and ash
- Place the device in a well-ventilated area and do not block its ventilation openings
- Install the device on a stable surface to prevent it from falling.
- The power supply must comply with the ES1 requirements of the IEC 62368-1 standard and must not exceed PS2. Please note that the power supply requirements are subject to the device label.
- This device is a Class I electrical appliance. Ensure that the device's power supply is connected to a power outlet with protective grounding.
- Use power cables that comply with local requirements and have rated specifications.
- Before connecting the power supply, please ensure that the input voltage matches the power requirements of the device.
- When installing the equipment, please ensure that the power plug and electrical connectors are easily accessible for power disconnection.
- Install the equipment near the power outlet for easy access in case of an emergency power shutdown.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.

Maintenance Requirements

The appliance coupler is a disconnection device. Please maintain it at a convenient angle during use.

Contents

Introduction

Overview

This device is a high-performance network video recorder. It supports local real-time viewing, multi-channel display, local storage of recorded files, as well as remote management and control functions.
The device works in conjunction with network cameras, network video servers, and other device to form a powerful monitoring network through central management software. In the network system, data is transmitted via network cables between the monitoring center and the monitored area. There is no need to connect audio or video cables from the monitoring center to the monitored area, allowing you to enjoy the advantages of simple connectivity and low maintenance costs.
The device can be widely used in areas such as public security, water conservancy, transportation, and education.

Features

NOTE
The actual functionality may vary depending on the software and hardware versions and models you are using.

Real-time Surveillance

- Connect to the monitor via VGA or HDMI port for real-time monitoring.
- Supports both HDMI and VGA output simultaneously.
- Shortcut menu for preview.
- Supports multiple popular PTZ decoder control protocols. Supports preset, tour and pattern.

Playback

- Supports independent real-time recording for each channel. At the same time, it supports features such as intelligent search, fast forward playback, network monitoring, recording search, and downloading.
- Supports slow playback, fast playback, reverse playback, and frame-by-frame playback.
- Support for time title overlay, allowing you to view the exact event time.
- Support for the expansion of designated areas.

Smart Playback

NOTE
This feature is only available on certain models.

- VCA playback. It can filter and replay records that meet the established criteria.
- Face detection playback. It can filter and replay records that contain faces.
- Facial recognition playback. It can filter records of specific license plate numbers or records of all license plate numbers.
- LPR playback. It can screen out the records with a specific vehicle plate number or all the records with car plate numbers.
- Smart search. It includes smart features such as attribute-based search and image-based search, enabling users to quickly retrieve target records.

Alarm

- Simultaneously respond to external alarms. Based on your predefined relay settings, the system is capable of correctly processing alarm inputs and sending screen or voice prompts to the user.
- Support the configuration of the central alarm server so that the system can automatically notify users of alarm information. Alarm inputs can come from various connected peripheral devices.
- Send alert information to you via email.

AI

NOTE
AI functions are only available on certain models and vary by model.

- Face detection. The system can detect faces in video images.
- Face recognition. The system can compare detected faces in real-time with images in the facial database.
- People counting. The system is capable of effectively counting the number of people and their flow direction.
- Heat map. The system can monitor active objects within a specific area.
- License plate recognition (LPR). The system can effectively monitor the passing vehicles.

Online Update

For network video recorders (NVR) connected to the internet, it supports online application upgrades.

Storage

- By making the appropriate settings (such as alarm settings and schedule settings), you can back up the relevant audio/video data in the network video recorder.

- You can record online, and the recording files will be saved on the computer of the client.

Network Surveillance

- Audio/video data compressed by IPC or NVS is transmitted to the client via the network, where the data is then decompressed and displayed.
- Supports up to 128 simultaneous connections.
- Transmit audio/video data through protocols such as HTTP, TCP, UDP, multicast, and RTP/RTCP.
- Transmit some alarm data or alarm information via SNMP.
- Supports web access in WAN/LAN.

Window Split

Using video compression and digital processing technology, multiple windows are displayed on a single monitor. It supports real-time viewing with 1, 4, 8, 9, 16, 25, 36, and 64 window splits, as well as 1, 4, and 9 window splits during playback.

Record

Supports regular recordings, motion recordings, alarm recordings, and intelligent recordings. Recorded files can be saved on a hard drive, USB device, client computer, or network storage server, allowing you to search or replay saved files locally or via network/USB devices.

Backup

Supports network backup and USB recording backup. You can back up the recorded files to network storage servers, external USB 2.0 devices, and DVDs, among other devices.

Network Management

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

Peripheral Device Management

- Support for peripheral control, allowing you to freely set control protocols and connection ports.
- Supports transparent data transmission via RS-232 and RS-485.

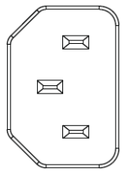
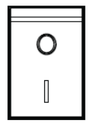
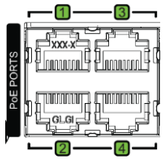
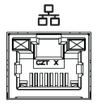
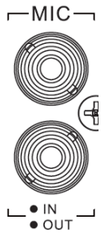
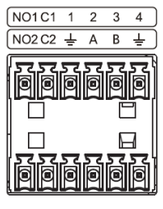
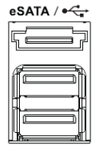
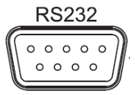
Structure

The following table introduces the panel descriptions of all NVR products.

NOTE

The panel layout, port types, and the number of ports may vary among different models; please refer to the actual product for confirmation.

Rear panel description

Pattern	Name	Description
	Power input port	Inputs power.
	Power switch	Turns on or off the Device.
	PoE ports	Built-in switch. Support PoE function. You can use this port to provide power to the network camera.
	Network port	Connects to the network cable.
	Audio input port	Two-way talk input port which receives the audio signals from the devices such as microphone and pickup.
	Audio output port	Outputs the audio signals to the devices such as the sound box.
	Alarm input ports	Receive signals from the external alarm source. NOTE When your alarm input device is using external power, make sure the device and the NVR have the same ground.
	Alarm output ports	Output alarm signals to the alarm device. • NO: Normally open alarm output port. • C: Common alarm output port.
	eSATA Port	The external SATA port allows for the connection of devices with SATA ports. When connecting an external hard drive, the hard disk drive (HDD) requires appropriate jump wire handling.
	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
	VGA port	Outputs analog video data to the connected display with VGA port.
	HDMI port	High Definition Media Interface. Transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device.
	RS-232 port	Use the port for general COM debugging to configure IP address or transfer transparent COM data.

Basic Operations

NOTE

The interfaces are only for reference and may differ from the actual interface.

Starting the Device

Precondition

- Ensure that the input voltage meets the power supply requirements of the device.
- To ensure the stable operation of the device and extend the lifespan of the hard disk drive, please adhere to the relevant standards and use a power supply that provides stable voltage with minimal interference. It is recommended to use an uninterruptible power supply (UPS).
- Please ensure that the device is connected to the power adapter before connecting it to the power source.

Process

1. Connect the device to the monitor, then connect a mouse.
2. Connect the power cable, and then turn on the power switch.

Initialization

Background Information

When using for the first time, you need to configure a password and related protective measures for the default administrator account.

NOTE

For the safety of the device, we strongly recommend that you properly safeguard the administrator password and change it regularly.

Process

1. Turn on the Device, select the language, and then click **Next**.
2. Read the **Software License Agreement** and **Privacy Policy**, select **I have read and agree to the terms and conditions of the Software License Agreement and Privacy Policy.**, and then click **Next**.
3. Configure the password for admin, and then click **Next**.

Password parameters

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

4. Set unlock pattern.

   NOTE

   - The pattern you wish to set must pass through at least four points.
   - If you do not wish to set up an unlock pattern, click **Next**.
   - Once you have configured the unlock pattern, the system will require the use of the unlock pattern as the default login method. If you have not configured an unlock pattern, you will need to enter a password to log in.

5. Configure the password protection information.
   - Reserved email address.
     In the **Reserved Email Address** box, enter your email address. If you forget your password, you can use this email address to obtain the security code required to reset your password.
   - Security questions.
     Select a security question and enter the corresponding answer. If you have forgotten your password, please enter the correct answer to the question, and then you can reset your password.
6. Click **Completed**.
   The **Setup Wizard** window appears.

Setup Wizard

Complete the basic settings according to the setup wizard.

Process

1. Configure data and time, and then click **Next**.
   You can select the time zone and data format, set the system time and daylight saving time.

NOTE

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

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

Network parameters

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

3. Enable the P2P function, then click **Next**.
   You can use the mobile client to scan the QR code under **Device SN** to add the device for remote management.

   CAUTION

   After you enable the P2P function and connect to the Internet, the system will collect the information such as email address and MAC address for remote access.
4. On the disk list, view the HDD information and configure the HDD type, configure the storage strategy, and then click **Next**.
   - Set HDD type.
     In the **Attributes** column, select **Read-Write**, **Read-only** or **Redundancy** to set the HDD type.
   - Format HDD.
     Select an HDD, click **Format**, and then follow the on-screen prompt to format the HDD.

     NOTE

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

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

Disk management parameters

Parameter	Description
Disk Full	The storage policy that will be used when no more storage space is available. • Stop: Stop Recording. • Overwrite: The latest document overrides the oldest document
Auto-delete Expired Files	Configuration whether to allow the device to automatically delete expired content. • Select **Never** if you do not wish to use the function. • Select **Custom**, then configure the duration for which you wish to retain the old files.

5. Connect to the remote devices.

   NOTE

   You can add remote devices by searching or by manually adding them. This section takes searching as an example for adding.

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

6. Click **Completed**.

Login

Log in to the device for more operations.

Process

1. Click the **Live view** page.
   - If you have configured an unlock pattern, the unlock pattern login window will be displayed. Click **Forgot the gesture** to switch to password login.
   - If you have not configured an unlock pattern, the password login window will be displayed.
2. Log in to the Device.

- Draw the unlock pattern.

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

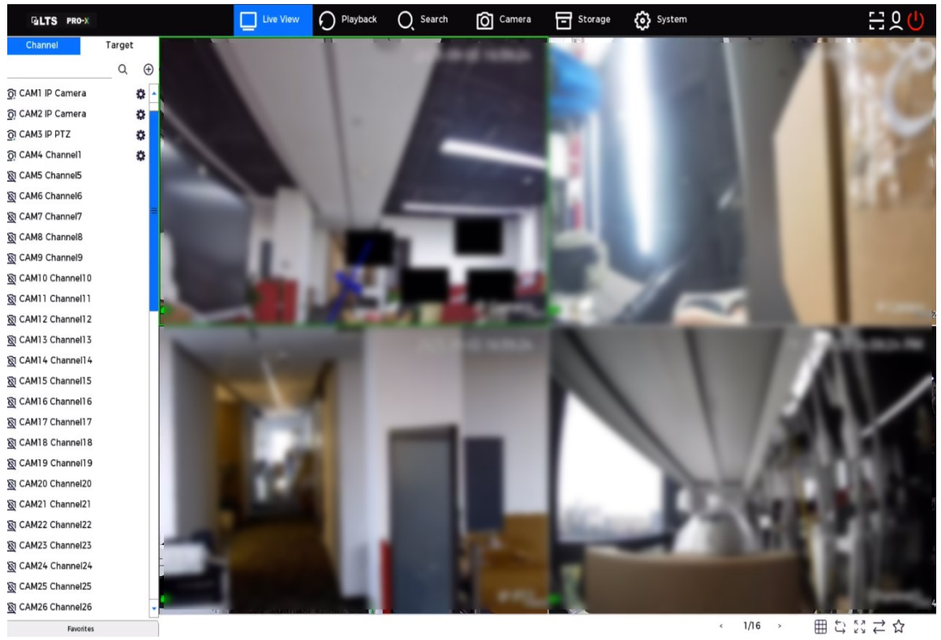
NOTE

If you forget your password, click  to reset it.

Main Menu

After logging in, you can directly see the **Live view** page. You can select the tiles in the middle at the top of the page to enter the corresponding configuration page as needed.

Main menu



Main menu description

No.	Name	Description
1	Function tiles	Click the selected tile to open the corresponding configuration page.
2	Scan	Scan the QR code to download mobile APP or add the Device for remote management.
3	Login	Logout the current account or switch user.
4	Power	Restart or shut down the device.

Live View

On the live view page, you can view the video images of different channels.
Select a window, double-click a channel in the channel list, and then the channel will be displayed in the selected window.

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

Live View Control Bar

Point to the bottom center position of the channel window, and the live view control bar will appear. Through the control bar, you can perform operations such as instant playback, digital zoom, manual snapshot, intercom, tracking, stream switching, PTZ control, and X Search.

Live view control bar

Live view control bar description

Icon	Function	Description
	Instant Playback	You can replay the recorded video from five minutes to sixty minutes. NOTE Go to **System** > **General** > **Basic Configuration** to configure the duration of instant playback.
	Digital Zoom	• Click the icon, and then select an area. Once you release the mouse button, the area will be enlarged. • Point to the area you want to zoom in or out, then scroll the mouse to zoom in or out. NOTE Right-click on the channel window to restore it to its original state.
	Manual Snapshot	Take snapshots of the current video channel. The snapshots are automatically saved to the connected USB storage device.
	Two-Way Talk	Enable voice interaction between the device and remote devices. NOTE This feature is only available when the remote device supports two-way talk.
	IP Speaker Talk	Enable the IP speaker talk function. NOTE You need bind the IP speaker and the channel to enable this function.
	E Tracking	Click the icon to enable the E Tracking function, and then you can view local E Tracking live videos. NOTE This function is available only when the remote device supports E Tracking.
	Stream Switching	Switch between the main stream and sub stream. • M: Main stream. Suitable for local recording and storage to achieve high-definition monitoring. • S: Sub stream. When network bandwidth is limited, it is suitable for network transmission.
/	Fisheye Lens	Click the icon to enter the fisheye mode. NOTE You cannot use the fisheye and X Search simultaneously.
	PTZ Control	Open the PTZ settings window.
	X Search	Achieve accurate and quick search on the connected NVR.

Navigation Bar

In the lower right corner of the live view page, you can access the functionality to perform actions through the feature icons on the navigation bar.

Navigation bar

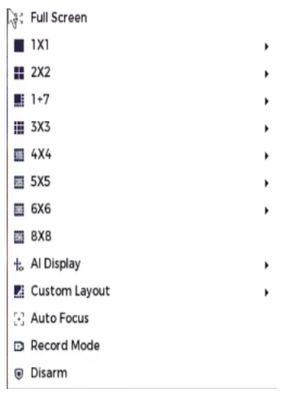
Navigation bar description

Icon	Description
<	Go to the next screen.
>	Go to the previous screen.
	Select view split mode.
	Enable or disable auto switch.
	Click the icon to enter full-screen mode.
	Click the icon to switch back and forth between the auxiliary screen and the main screen.
	Save user's custom layout in the preview interface and display the saved combinations on the left side of the preview screen.

Shortcut Menu

Right-click on the live page, and a shortcut menu will appear. You can select full screen mode or split mode, configure record mode, auto focus and AI display, switch arming and disarming function.

Shortcut menu



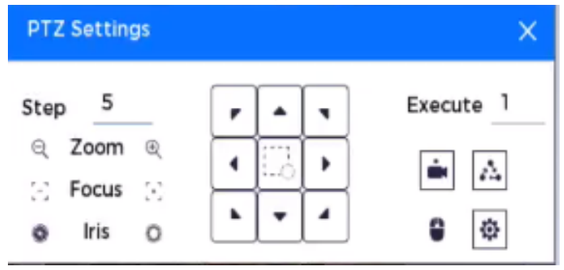
PTZ

PTZ is a mechanical platform that carries the camera and protective cover, allowing for remote overall control. PTZ can move horizontally and vertically, providing the camera with a comprehensive field of view.

PTZ Control Panel

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

PTZ control panel



PTZ control panel description

Parameter	Description
Step	The larger the value, the faster the movement speed of the PTZ.
Zoom	• : Zoom out. • : Zoom in.
Focus	• : Focus far. • : Focus near.
Iris	• : Image darker. • : Image brighter.
	Fast positioning button. • Positioning: Click the icon, and the click any point on the live page. The PTZ will turn to this point and locate this point in the center. • Zooming: Click the icon, and then drag to draw a square on the view. The square supports zooming. ◦ Dragging upward is to zoom out, and dragging downward is to zoom in. ◦ The smaller the square, the larger the zoom effect. NOTE This feature is only available on certain models.
	Enable direction control through mouse operation.
	Enable the preset point.

Parameter	Description
	Enable the patrol group.
	Click the icon to set parameters of **Preset Point** and **Patrol Group**.

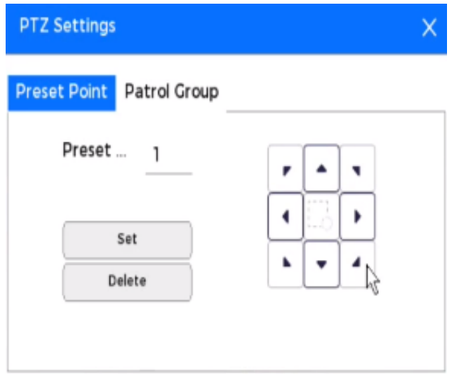
PTZ Function Settings

Preset Point

Process

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

Preset



2. Click the direction arrows to rotate the camera to a desired position.
3. Enter a number to indicate the preset point.
4. Click **Set**.

Configuring Patrol Group

Process

1. On the PTZ control panel, click , then select **Patrol Group**.
2. Click the direction arrows to rotate the camera to a desired position.
3. Enter a patrol number.
4. Enter a number for the preset point, then click **Set**.
   A preset point has been established for this patrol. You can continue to set more preset points.

NOTE

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

PTZ Functions Usage

After configuring the PTZ settings, you can use the PTZ functions through the PTZ control panel.

Using Presets

Process

1. Enter the preset number in the **Execute** box of the PTZ control panel.
2. Click to call the preset.
3. Click again to end the call.

Using Patrol Groups

Process

1. Enter the patrol number in the **Execute** box of the PTZ control panel.
2. Click to call the patrol group.
3. Click again to end the call.

Playback

Instant Playback

You can quickly view previously recorded videos ranging from 5 to 60 minutes through the real-time view control bar. For more details on instant playback, please refer to "5.1 Live View Control Bar".

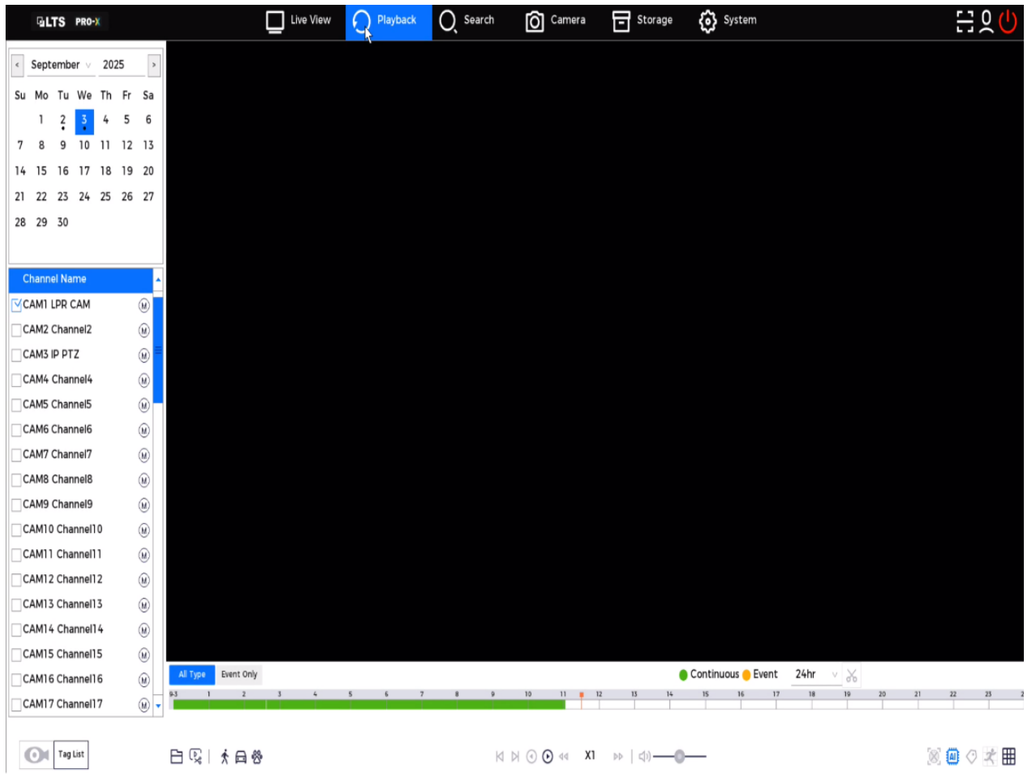
Playback Page

Click **Playback**. The **Playback** page will be displayed.

NOTE

The image below is for reference only.

Playback



Playback page description

No.	Function	Description
1	Display window	Display the recorded video. Supports playback in single-channel or multi-channel. NOTE • The display window defaults to single-channel mode. • Click to split the display window as needed. • In single-channel playback mode, click and hold the area you wish to enlarge, then release to zoom in on the selected area. To exit the zoomed-in state, right-click on the image.
2	Calendar	Select the search time. NOTE The selected date is highlighted. Appears below the date of the recorded video.
3	Fisheye	Click the icon to enter the fisheye mode.
	Tag list	View and manage the tagged videos found after search.
4	Channel list	Select one or more channels to play back on the channel list. • The window segmentation is determined by the number of selected channels. If one channel is selected, playback will be displayed in a single-channel view; if two to four channels are selected, playback will be displayed in a four-channel view. • Click M or S switch the streams. M is main stream. S is sub stream.
5	Playback controls bar	Playback control buttons. Please refer to "6.3 Playback Controls" for detailed information.

No.	Function	Description
6	Time Bar	Displays the type and time period of the current recorded video. • Click the colored area to start playback from a certain time. • Click and hold the time bar. When the mouse pointer changes to a hand icon, you can drag to view the playback of the target time. • Rolling on the time bar will zoom in on the time bar. • You can drag the vertical line on the timeline to quickly view the playback content in I-frame format • When playing a video in single-channel mode, you can hover the mouse over the timeline to display a thumbnail of the current video. • In the 4-channel layout, 4 time bars are displayed; in the other view layouts, only 1 time bar is displayed.
7	Record type	Select the recording type to search for. • Display all recordings normally. Green indicates general records on the time bar. • Event displays motion recordings, alarm recordings, and smart recordings. Yellow indicates event records on the time bar.
	Time bar unit	Select **24hr**, **2hr**, **1hr**, or **30min** as the unit of time bar.
	Clip	Click to clip the recorded content, and then save the specified segment.

Playback Controls

You can search for and play back videos, images or video clips. The operation is similar. This section takes video playback as an example.

Process

1. Select **Playback**, then click to play the recording from an external device.
2. Select the **Normal** or **Event** as the search type.
3. Select the date and channel.
4. Click or any position on the time bar.

   The system begins playback. You can use the playback controls to manage the playback process.

Playback controls

Playback controls description

Icon	Function
	Click it to play the recording from external devices. Click to exit the current playback mode.
	Click it to split the day's recordings as needed, then display them on the display window. Click to exit the current playback mode.
	Select a target type for smart playback. You can select **Human**, **Vehicle** or **Animal**.
	Displays previous frame/next frame. • Click or to play back the video frame by frame when the playback is paused, . • Click to resume normal playback mode in frame by frame playback mode,.
	Rewind. • Click it to rewind the video in normal play mode. • Click to resume normal playback mode in rewinding mode, .
	Click it play the video. Click again to stop the playing.
	Stop the current playback process.
	Slow playback. • Click it to set the speed of slow playback in normal playback mode. • Click it to slow down the speed of fast playback in fast playback mode.
	Fast playback. • Click it to set the speed of fast playback in normal playback mode. • Click it icon to speed up slow playback in fast playback mode..
	Adjust the volume.
	X Search

Icon	Function
	Click it to display or hide AI rules.
	Click it to tag the video.
	Click it to display 1, 4, 9 or 16 videos on the display window.

Clip

During playback, you can clip parts of the video and save them to a USB storage device.

Process

1. Select **Playback**.
2. Set the search criteria and play back video. For more details, refer to "Playback Controls".
3. Click the time bar to select the start time, then click  .
4. Click the time bar to select the end time, then click  .
5. Click  to save the file.

Tag Playback

During video playback, you can add tags to mark important timestamps in the video. After playback ends, you can search for the corresponding video using the time or tag keywords, and then play it.

Adding Tag

During system playback, click  , then configure the tag name.

Playing back Tag

During single-channel playback, click  , then double-click a file in the tab list to play it.

Managing Tags

Click  in label list.

- Search for the tagged video: Select channel number, start time and end time, then click **Search**.
- Change the tag name: Double-click a tagged video, then enter the new name.
- Delete tags: Select one or more tagged videos, then click **Delete**.

Search

You can search videos, pictures, and smart events.

Searching for Video

Process

1. Go to **Search** > **Video**.
2. Set related parameters, then click **Search**.
   You can click **Clear** to remove the completed information.
   The search results are displayed at the bottom of the page, and you can back them up.

Search for video

Video search parameters

Parameter	Description
Start Time	Set the start time and end time for video search.
End Time	
USB	Select a USB from the drop-down list. NOTE Click **Format** to format the USB.
Storage Path	Click **Browse** to select the storage path.
Recording Channel	Select the recording channel, then select **Main Stream** or **Sub Stream** as needed.
Event Type	Select the event type as needed. Supports selecting **All**, **External Alarms**, **Motion Detection**, **Continuous Recording**, or **VCA**.
Record Type	Select the record type as needed. Supports for selecting **All** or **Lock**.
File Format	Select the file format as needed. Supports for selecting **LAV** or **MP4**.

Related Operations

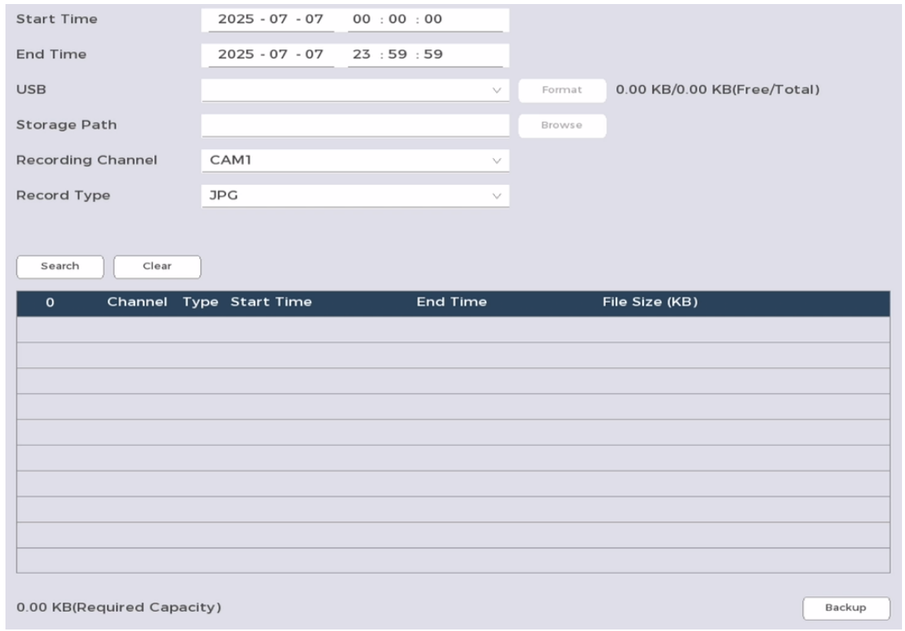
- Click **Lock** to lock the selected recordings.
- Click **Unlock** to unlock the selected recordings.

Searching for Picture

Process

1. Go to **Search** > **Picture**.
2. Set related parameters, then click **Search**.
   You can click **Clear** to remove the completed information.
   The search results are displayed at the bottom of the page, and you can back them up.

Search for picture



Picture search parameters

Parameter	Description
Start Time	Set the start time and end time for the picture search.
End Time	
USB	Select a USB from the drop-down list. NOTE Click **Format** to format the USB.
Storage Path	Click **Browse** to select the storage path.
Recording Channel	Select the recording channel.
Record Type	Select the record type as needed. Only **JPG** format is supported.

Smart Search

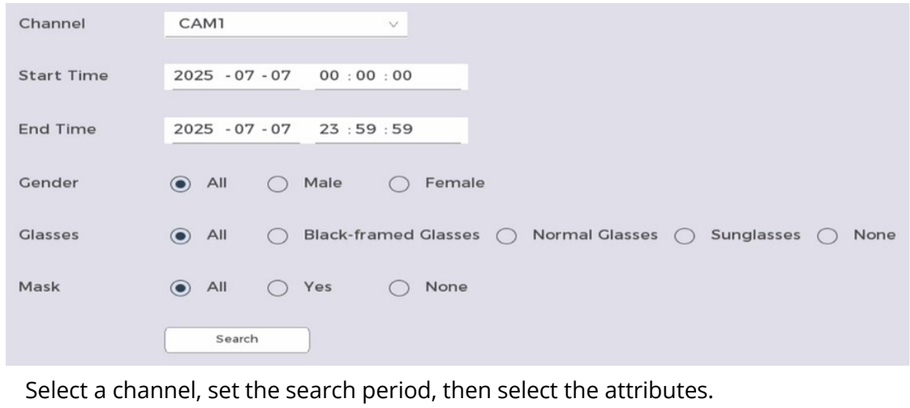
Face Search

You can search for and play back detected faces.

Process

1. Go to **Search** > **Smart Search** > **Face Search**.

Face search



2. Select a channel, set the search period, then select the attributes.
   You can select one or more channels, or select **All**.
3. Click **Search** and the results will be displayed.

Related Operations

- Play.
  Select an image and click to start play back.
  TIPS
  Double-click the playback image to toggle between full-screen playback and thumbnail playback.
- Sort.
  Click to sort the images by time.
- Export.
  Click to export the search results in an Excel format.
- Back up.
  Select one or more images, click , and then select the storage path.
- Add tag.
  Select one or more images, and then click .

- Lock.
  Select one or more images, and the click to lock the images.

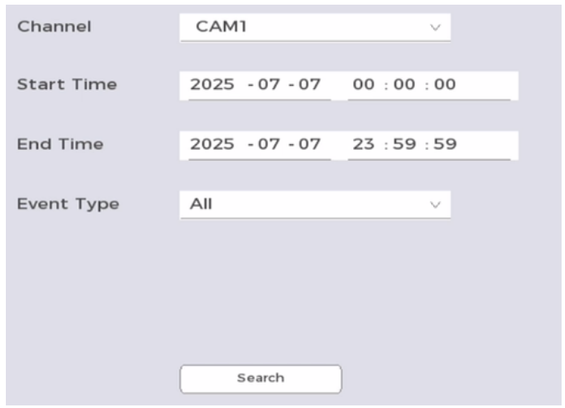
VCA Search

Search for the VCA detection results.

Process

1. Go to **Search** > **Smart Search** > **VCA Search**.

VCA search



2. Select a channel, and then set the start time and end time. You can select one or more channels, or select **All**.
3. Select an event type.
4. Click **Search** and the results will be displayed.

Related Operations

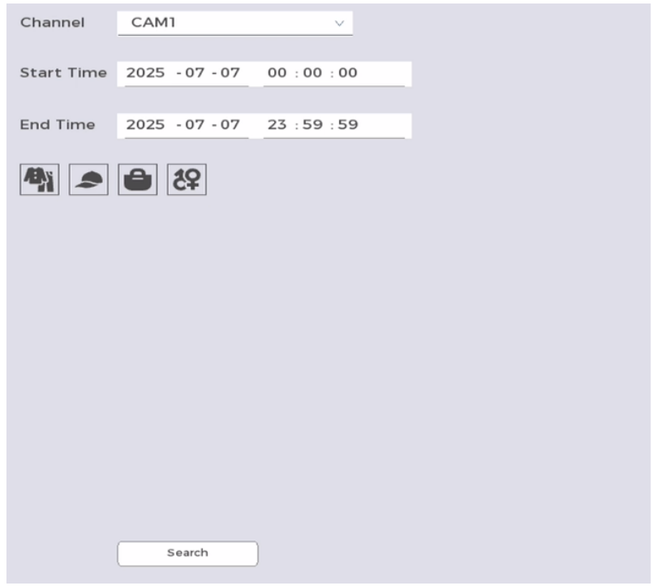
- Play.
  Select an image and then click to play back.
- Sort.
  Click to sort the images by time.
- Export.
  Click to export the search results in an Excel format.
- Back up.
  Select one or more images, click , then select the storage path.
- Add tag.
  Select one or more images, and then click .
- Lock.
  Select one or more images, and the click to lock the images.

Human Detection

Process

1. Go to **Search** > **Smart Search** > **Human Detection**.

Human detection



2. Select a channel, and then set the start time and end time. You can select one or more channels, or select **All**.
3. Set related parameters as needed.
4. Click **Search**.

NOTE

For privacy protection, facial features have been deliberately blurred.

Search results

Related Operations

- Play.
  Select an image and click to play back.
- Sort.
  Click to sort the images by time.
- Export.
  Click to export the search results in an Excel format.
- Back up.
  Select one or more images, click , then select the storage path.
- Add tag.
  Select one or more images, then click .
- Lock.
  Select one or more images, then click .

Vehicle Detection

Search for the vehicle detection results.

Process

1. Go to **Search** > **Smart Search** > **Vehicle Detection**.

Vehicle Detection

2. Select a channel, and then select the target type from **Allow List**, **Block List**, **Standard**, or **All**.
   You can select one or more channels, or select **All**.
3. Configure related parameter.
4. Click **Search** and the results will be displayed.

Related Operations

- Play.
  Select an image and click to play back.
- Sort.
  Click to sort the images by time.
- Export.
  Click to export the search results in an Excel format.
- Back up.
  Select one or more images, click , and then select the storage path.
- Add tag.
  Select one or more images, then click .
- Lock.
  Select one or more images, then click to lock the images.

MD2.0 Search

Search for the motion detection results.

Process

1. Go to **Search** > **Smart Search** > **MD2.0 Search**.

MD2.0 search

2. Select a channel, and then select the target type from **All**, **Human** and **Vehicle**.
   You can select one or more channels, or select **All**.
3. Set the time period.
4. Click **Search** and the results will be displayed.

Related Operations

- Play.
  Select an event and click to play back.
- Back up.
  Select one or more events, click **Backup**, then select the storage path to back up the search result.

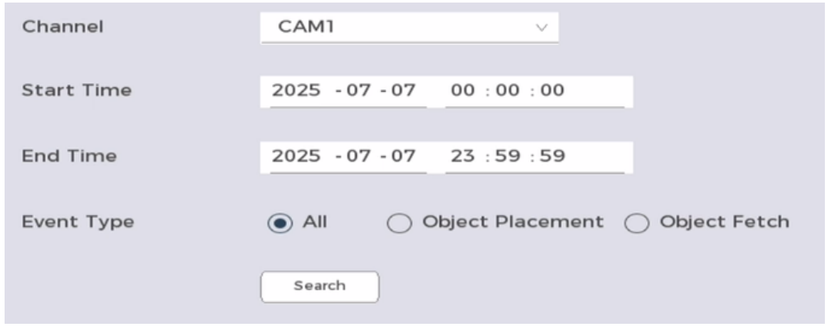
Object Monitoring

An alarm will be triggered when someone takes luggage, bags, or boxes out of the monitored area or places them into the monitored area.

Process

1. Go to **Search** > **Smart Search** > **Object Monitoring**.

Object Monitoring



2. Select a channel, and then set the time period.
   You can select one or more channels, or select **All**.
3. Select the event type.
   - **Object Placement**: Place the item within the monitoring area.
   - **Object Fetch**: Remove items from the monitoring area.
4. Click **Search** and the results will be displayed.

Related Operations

- Play.
  Select an image and click to play back.
- Sort.
  Click to sort the images by time.
- Export.
  Click to export the search results in an Excel format.
- Back up.
  Select one or more images, click , then select the storage path.
- Add tag.
  Select one or more images, then click .
- Lock.
  Select one or more images, then click .

X Search

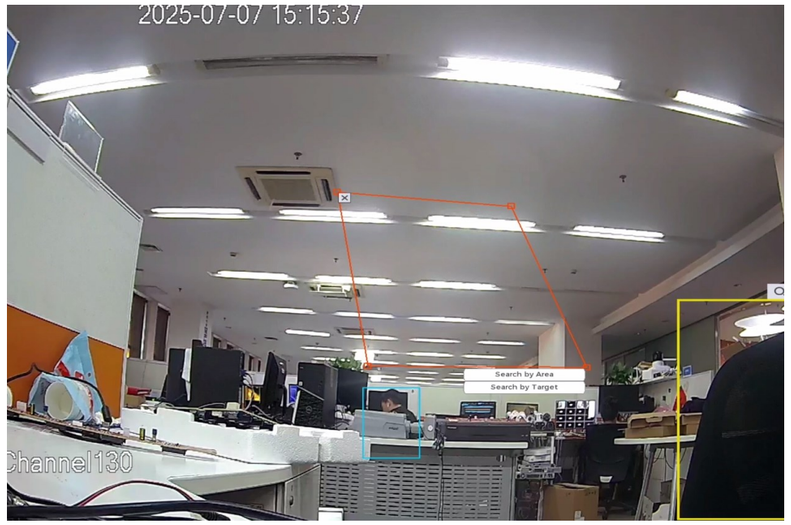
You can perform X Search on both live view and playback pages. X Search includes quick search of video metadata and SMD. You can search for people, motor vehicles and animals.

X Search Operation

Process

1. Click in **Live View** or **Playback** Page, then the video image will be frozen.
2. Select automatic search or manual search.

X Search



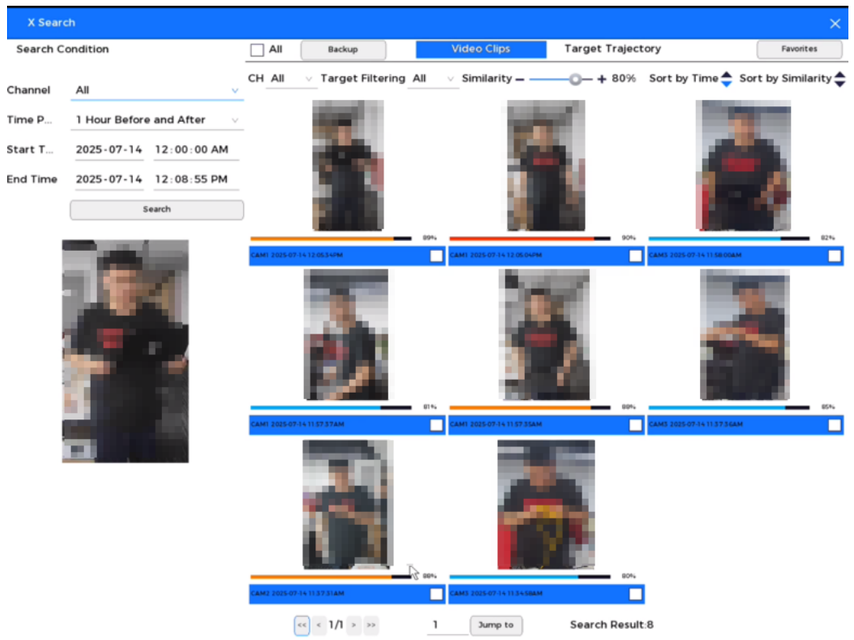
- The target will be automatically detected and displayed with a target box on the image. When the mouse pointer is moved over the target, the target box will be highlighted, and a search button will be displayed. Click the search button or double-click to search for the target. Set the search criteria, such as channel and time period, and then click search; the query results will be displayed on the right side of the page.
- Move the mouse pointer outside the target box, then click to manually select the area. Irregular areas are supported. Once the area is drawn, you can choose the search method.
  - Search by Area: Searches based on the drawn area and displays search results for all targets within that area.
  - Search by Target: Searches based on the targets selected within the drawn area and displays all search results for those targets.

3. In the search result page:

- Drag the **Similarity** slider to adjust the similarity.

- Hover over a search result and click ★ to bookmark that result.
- Hover over a search result and click 👁 to hide that result.
- Select a search result and click Backup to choose the file path and related event recordings on the file backup page.
- Click ⇕ to sort the search results.
- Click **Target Trajectory** to display search results on the map trajectory. Click the **Play Tracks** button, and the playback area will play the recorded videos in the order they appear in the list.

Search result



Attribute Search

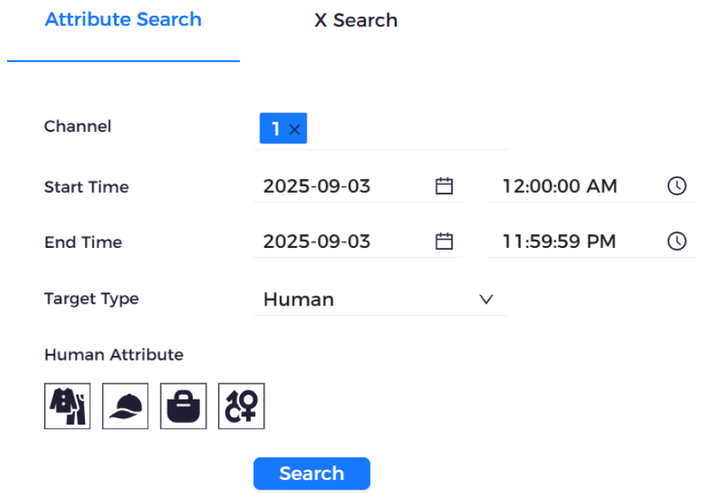
Process

1. Go to **Search** > **Smart Search** > **X Search** > **Attribute Search**.
2. Configure the channel, period, target type and other search criteria to perform the search.

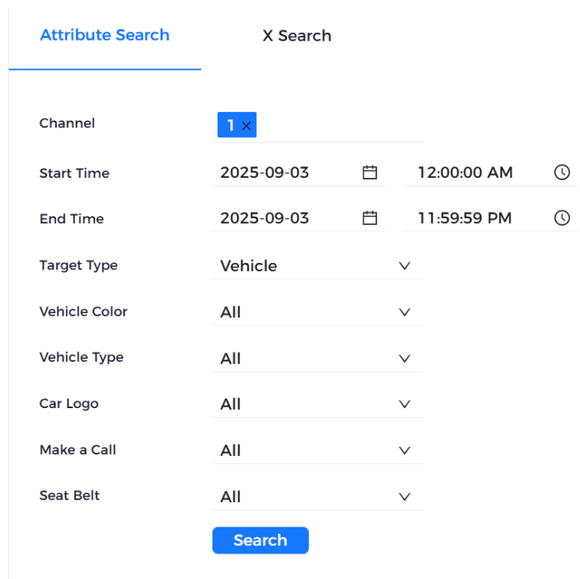
NOTE

You can select Human or Vehicle for the target type.

Attribute Search (human)



Attribute Search (vehicle)

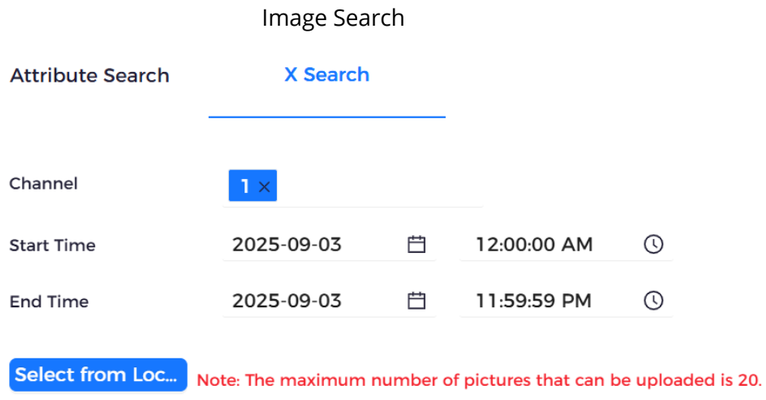


3. Click **Search**, then you can view the search results.

Image Search

Process

1. Go to **Search** > **Smart Search** > **X Search** > **X Search**.
2. Click **Select from Local** to import images from external devices. The device will automatically extract and display human bodies and motor vehicles in the images.
3. Select the target you wish to search for, configure the search criteria and search for the target.



Smart Report

People Counting

Search for the people counting report within a specified channel and time period, and also support exporting the people counting report.

Background Information

- Data follows the principle of comprehensive coverage; we recommend that you back up as needed in a timely manner.
- When the device is restored to factory settings, all data will be cleared except for the data on external storage media. Data on external storage media can be deleted through methods such as formatting. Please take note.

Process

1. Go to **Search** > **Smart Report** > **People Counting**.
2. Select the channel, counting rule, counting type, stay time, region and report type, and then set the time range.

   NOTE

   The Maximum search duration is 24 hours.
3. Click **Search**.

Related Operations

Click **Export**, select the file type and export the statistical data in the form of an image or Excel.

Heat Map

Search for and view heat map reports for a specified channel, with the option to export the heat map report.

Process

1. Go to **Search** > **Smart Report** > **Heat Map**.
2. Select the channel, set the time range, then click **Search**.

Related Operations

Click **Export**, select the file type and export the statistical data in the form of an image or Excel.

Metadata Report

Search for video metadata reports within the specified channel and time period, and optionally export the video metadata reports.

Background Information

- Data follows the principle of comprehensive coverage; it is recommended to back up in a timely manner as needed.
- When the device is restored to factory settings, all data will be erased except for the data on external storage media. Data on external storage media can be deleted through methods such as formatting.

Process

1. Go to **Search** > **Smart Report** > **Metadata**.
2. Select the channel, direction and report type, set time range, and then click **Search**.

Related Operations

Click **Export**, select the file type and export the statistical data in the form of an image or Excel.

Camera

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

Camera Registration

Adding Remote Devices

Add remote devices to the Network Video Recorder (NVR) to receive, store, and manage the video streams from remote devices.

NOTE

Before adding a remote device, please ensure that the device has completed initialization.

Adding Remote Devices from Search

Background Information

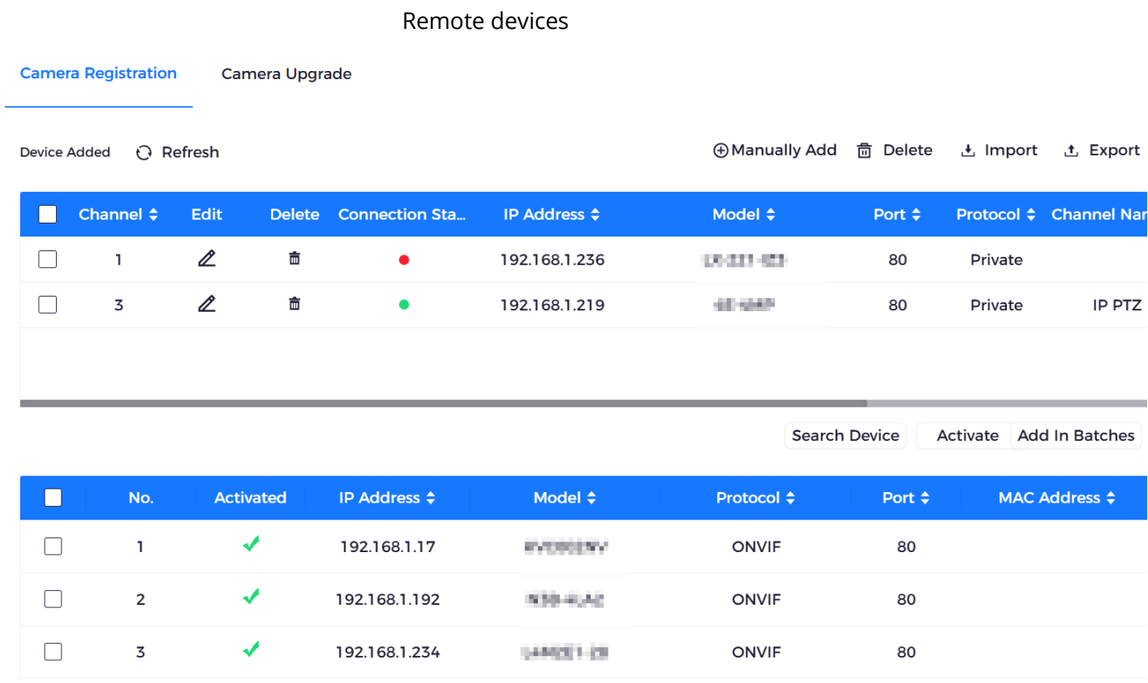
Search for remote devices on the same network as the NVR, and then add the remote devices from the search results

NOTE

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

Process

1. Go to **Camera** > **Camera Registration** > **Camera Registration**.



2. Click **Search Device**.
3. Select one or more remote devices from the search results, then click **Add in batches**.
   You can view the added devices in **Device Added** list.

Related Operations

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

- **DHCP**: No need to enter the IP address, subnet mask, and default gateway. The device will automatically assign an IP address to the camera.
- **Static**: Need to enter IP address, subnet mask, and default gateway.

NOTE

When you change the IP addresses of multiple devices simultaneously, please enter an incremental value. The system can automatically assign IP addresses by adding the fourth decimal digit of the IP address one by one.

If an IP conflict occurs when changing the static IP address, the system will notify you of the issue. If you change the IP addresses in bulk, the system will automatically skip the conflicting IPs and start assigning based on the incremental value.

Adding Remote Devices Manually

Background Information

Manually configure the IP address, username, password, and other information of the remote

device to add the device.

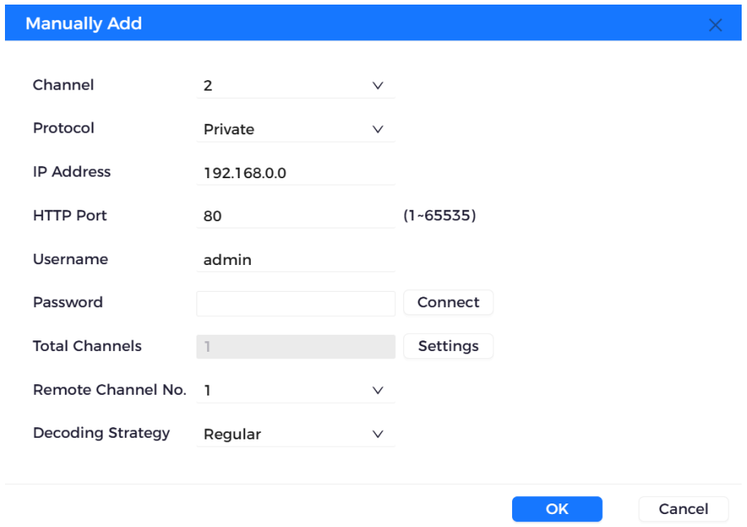
NOTE

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

Process

1. Go to **Camera** > **Camera Registration** > **Camera Registration**.
2. Click ➕ to add manually.

Manually add



3. Configure parameters.

Parameters of manual add

Parameter	Description
Channel	Assign a channel to the remote device.
Manufacturer	Select the manufacturer of the remote device.
IP Address	Enter the IP address of the remote device.
HTTP Port	Enter the HTTP port of the remote device.
Username	Enter the username and password of the remote device.
Password	
Total Channels	Click **Connect** to obtain the total number of channels for the remote device.
Remote Channel No.	Select one or more remote channels you wish to connect to.
Decoding strategy	Select a decoding strategy from **Real-time**, **Regular**, and **Smooth**.

4. Click **OK**.

Related Operations

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

Importing Remote Devices

Precondition

Connect a USB storage device to the NVR.

Background Information

NOTE

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

Process

1. Go to **Camera** > **Camera Registration** > **Camera Registration**.
2. Click ⬆ to export the template.

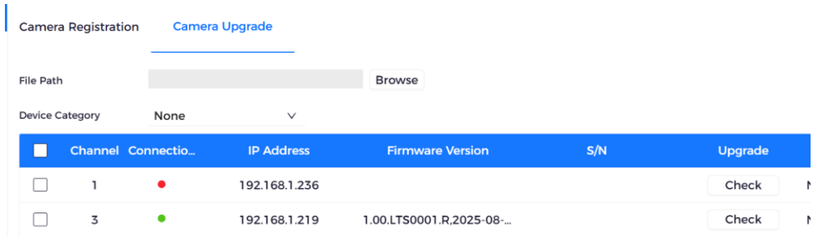
   NOTE

   When exporting the template, you need to disable backup encryption.
3. Complete the template.
4. Click ⬇ to import the template.
5. Click **OK**.

Camera Upgrade

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

Camera upgrade



- Local update.
  1. Connect a USB storage device containing the update file to the NVR.
  2. Select one or more remote devices.
  3. Click **Local Update**.
  4. Select the update file to start updating.
- Online update.
  1. Select the available new version of the remote device.
  2. Click **Online Upgrade**

  TIPS

  You can filter remote devices by the list of **Device Category**.

Check PoE Status

Go to **Camera** > **PoE** to check the PoE ports status.

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

Figure 8-4 PoE

Number of Connected Ports/Total Ports 0/16 Actual Power/Total Power (W) 0.0/130.0

Port	Channel	Status	Link Quality	Signal Enhanceme...	Link Rate (Mbps)	Power (W)
1	1		-	Close	-	-
2	2		-	Close	-	-
3	3		-	Close	-	-
4	4		-	Close	-	-
5	5		-	Close	-	-
6	6		-	Close	-	-
7	7		-	Close	-	-
8	8		-	Close	-	-

Switch Operation Mode

After setting **Switch Operation Mode**, when the IPC connects to the PoE port, the system will automatically assign an IP address to the IPC based on the defined IP segment, and the device will automatically connect to the IPC.

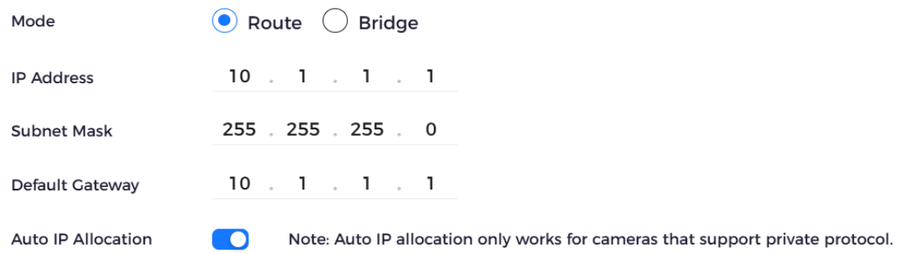
Precondition

- Only models with PoE ports support this function.
- Please do not connect the PoE port to the switch, as this will result in a connection failure.
- This function is enabled by default. We recommend to use the default setting.
- When connecting to a third-party IPC, please ensure that the IPC supports the ONVIF protocol and has DHCP enabled.

Process

1. Go to **Camera** > **PoE**.

Operating mode



2. Select **Route** or **Bridge** in **Mode** as needed.
   Route is the default mode.
3. Configure IP address, subnet mask, and default gateway.
   You cannot configure these parameters in the bridge mode.

   NOTE

   Please do not set the IP address to the same network segment as the device. We recommend using the default settings.
4. Click **Apply**.

Image Attributes

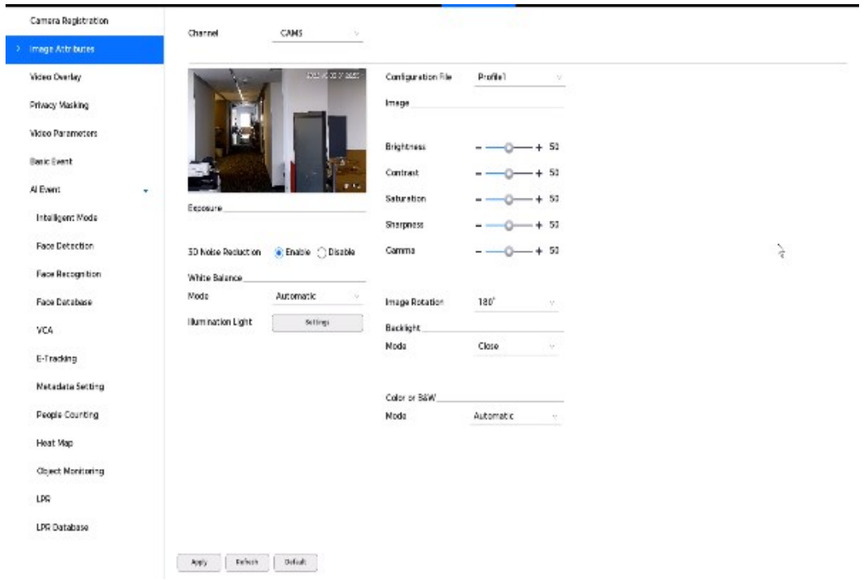
Process

1. Go to **Camera** > **Image Attributes**.

NOTE

Parameters may vary depending on the selected channel; please refer to the actual page for operational information.

Image attributes



2. Select a channel and configure the parameters.

Parameters of image attributes

Parameter	Description
Brightness	The larger the value, the clearer the image.
Contrast	The larger the value, the more pronounced the contrast between the bright areas and the dark areas.
Saturation	The bigger the value, the more intense the color.
Sharpness	The bigger the value, the more obvious the image edge.
Gamma	Change the image brightness and improve the image dynamic range in a nonlinear manner. The higher the value, the brighter the image; the lower the value, the darker the image.
Mirror Image	Select **Enable** to switch the left and right side of the video image. NOTE This feature is only available on certain models.
Image Rotation	Set the video display orientation.
3D Noise Reduction	Processing multi-frame images (no less than 2 frames) to reduce noise by utilizing the frame information between the previous and subsequent frames
Backlight Mode	• **Close**: Disable backlight mode. • **Backlight Compensation**: Enables the camera to clearly capture the image of the target's dark areas when shooting against the light.
White Balance Mode	Enable white balance to ensure accurate color representation in the image. This feature will alter the overall tone of the image. NOTE White balance modes may vary depending on the camera.
Color or B&W Mode	Switches the video image between the color mode and the black & white mode. • **Automatic**: The camera outputs color images or black and white images based on environmental conditions. • **Full Color**: The camera outputs only color images. • **Black & White**: The camera outputs only black and white images.

3. Click **Apply**.

Smart Light

This section introduces the configuration of smart light.

Process

1. Go to **Camera** > **Smart Light**.

   NOTE

   This function is only available when the selected camera equipped with smart light.

2. Select the camera channel and click to enable the function.
3. Select mode.
   - Steady: You can set the light mode from **Keep Lighting** and **Flicker**. For **Flicker** mode, you can adjust the flicker speed from **Low**, **Medium** and **High**.
   - Wave: The light mode is fixed as **Flicker**, you can adjust the flicker speed from **Low**, **Medium** and **High**.
   - Event: The smart light is keep lighting with blue color by default. When the AI event is triggered, the light will flicker with red color.

4. Click **Schedule** to set smart light schedule. You can set 6 periods at most for each day of a week. Click **OK** to save the schedule.
5. Click ▾ to select the day of a week. Set the light color, light brightness and light mode of each period.
6. (Optional) After finish settings of the day, you can click check box to copy the same settings to other days.
7. Click **Apply**.

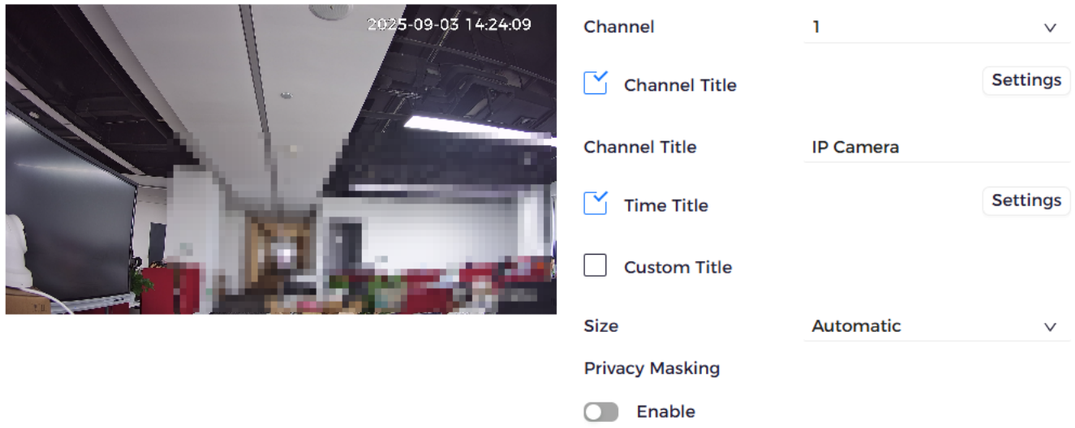
Video Overlay

Configure the overlay information on the live view page.

Process

1. Go to **Camera** > **Video Overlay**.

Overlay



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

   NOTE
3. Click **Apply**.

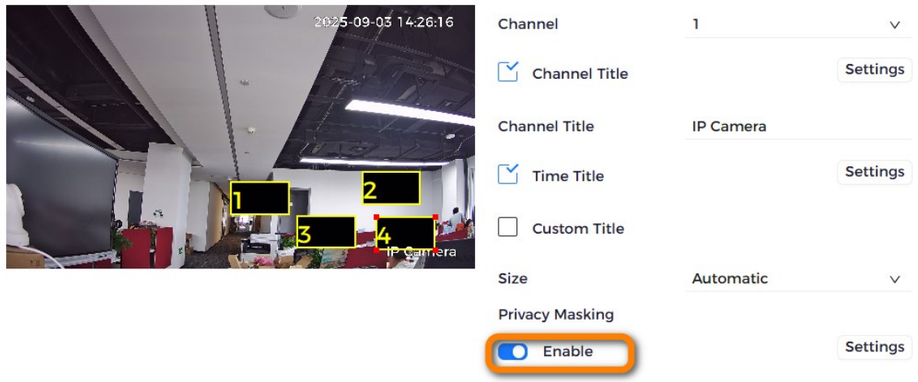
Privacy Masking

You can mask certain areas of the image to protect privacy.

Process

1. Go to **Camera** > **Privacy Masking**.

Privacy masking



2. Select a channel, then configure the masking.
   1. Click ▬ to enable privacy masking.
   2. Click **1**, **2**, **3** or **4** to add a mask blocks to the image.

      NOTE

      A maximum of 4 mask blocks can be added to each channel.
   3. Adjust the position and size of the masking block.
3. Click **Apply**.

Video Parameters

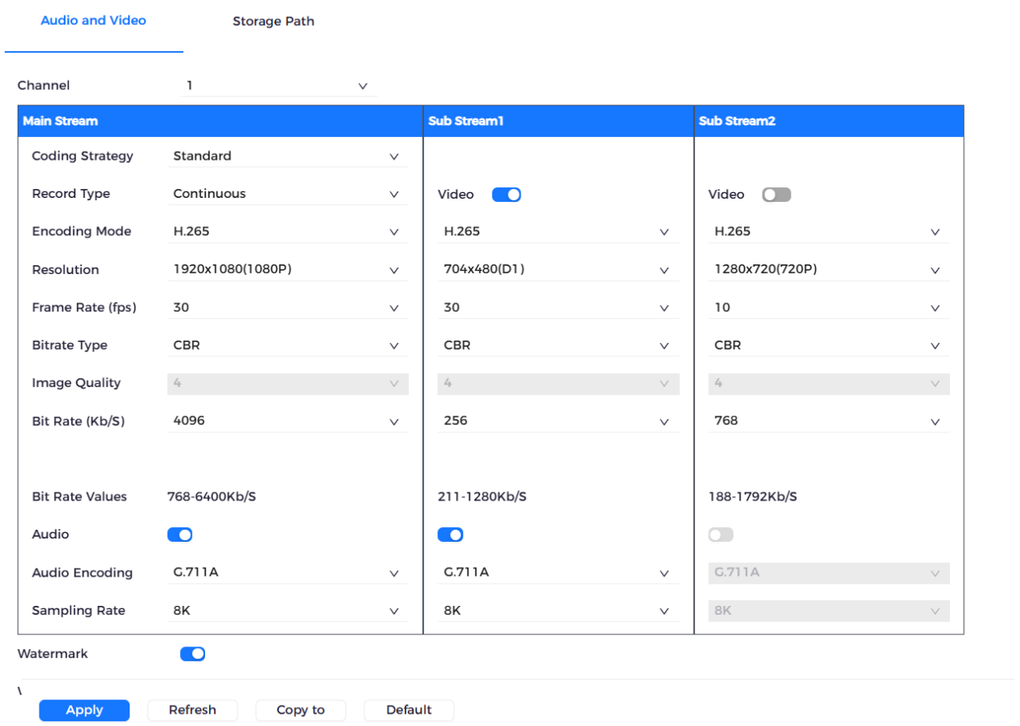
Background Information

Configure video encoding settings based on the actual bandwidth.

Process

1. Go to **Camera** > **Video Parameters**.

Video parameters



2. Configure the parameters.

Video settings

Parameter	Description
Channel	Select a channel that you want to configure settings for.
Coding Strategy	The parameter is set to **Standard** by default.
Record Type	The parameter is set to **Continuous** by default.
Encoding Mode	• H.265 (recommended): Main profile encoding. This format is recommended for use. • H.264B: Baseline profile encoding. • H.264: General profile encoding. • H.264H: High profile encoding. Low bit stream with high definition. • MJPEG: In this format, images require a higher bitrate value to ensure clarity.
Resolution	Select the video resolution. NOTE The maximum available resolution may vary by model.
Frame Rate (FPS)	Configure the frame rate of the video. The higher the value, the clearer and smoother the image. The frame rate will vary with changes in resolution.
Bitrate Type	• **CBR** (Constant Bitrate): The bit rate varies slightly around a defined value. When the monitored environment is expected to have only minor changes, we recommend selecting constant flow. • **VBR** (Variable Bitrate): The bit rate varies with changes in the monitored scene. When significant changes in the monitoring environment are anticipated, please select variable streaming.
Image Quality	The larger the value, the better the image quality. NOTE This parameter is available when the **Bitrate Type** is **VBR**.
Bit Rate (Kb/S)	• Main stream: The higher the bitrate, the better the image quality. • Sub stream: For constant flow, the bit rate varies around the defined value; for variable flow, the bit rate changes with the image, but the maximum value remains close to the defined value.
Audio Encoding	Select an audio encoding format.
Sampling Rate	Set the number of times to sample sound per second. The larger the value, the more natural the sound.

3. Click **Apply**.

Basic Event

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

tampering.

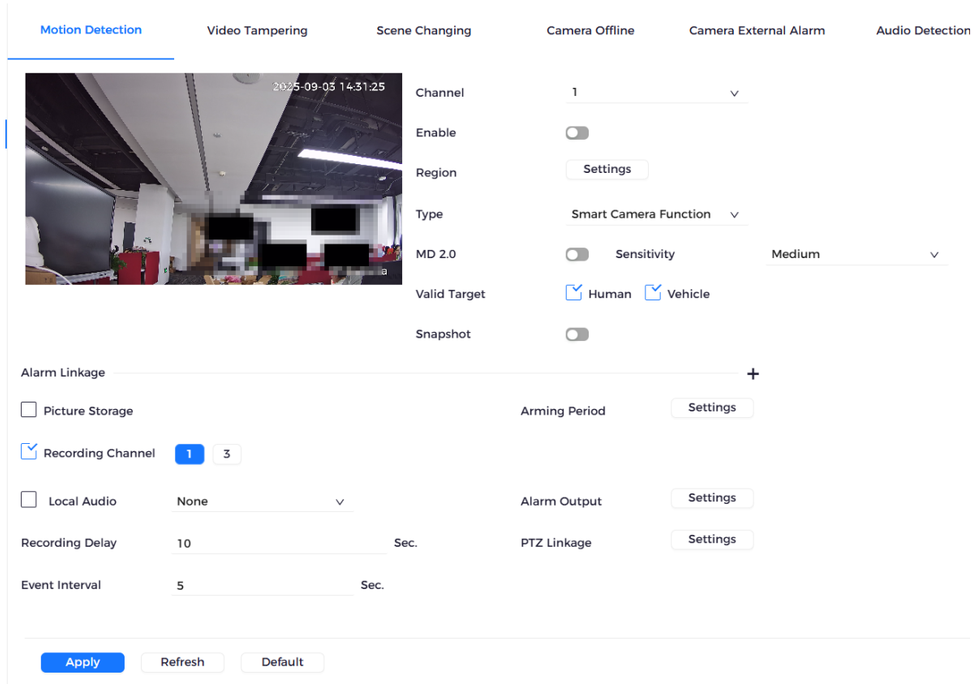
Motion Detection Alarms

When a moving object appears and reaches the set sensitivity threshold at a sufficiently fast speed, the alarm will be triggered.

Process

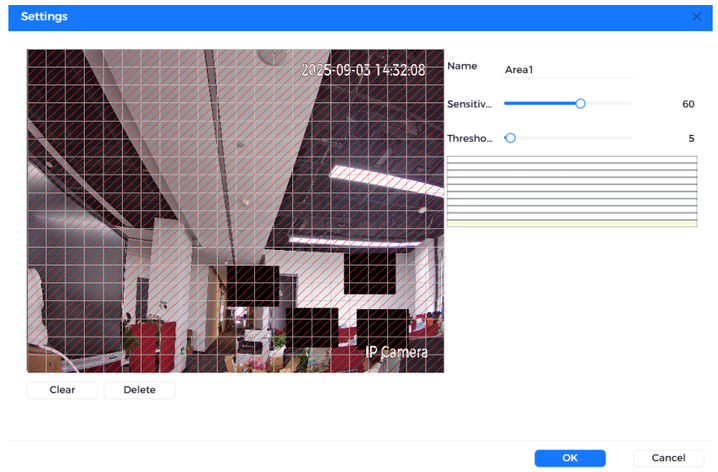
1. Go to **Camera** > **Basic Event** > **Motion Detection**.

Motion detection



2. Select a channel, then click next to **Enable** to enable motion detection.
3. Click **Settings** next to **Region** to configure the detection area.
   1. Point to the middle top of the page.

Detection region



   2. Configure the parameters.
      - **Name**: Enter a name to identify this area.
      - **Sensitivity**: Configure the sensitivity for motion detection. The higher the value, the greater the likelihood of triggering an alarm, but the false alarm rate will also increase. We recommend using the default settings.
      - **Threshold**: An alarm will be triggered when the percentage of detected targets in the detection area reaches or exceeds the defined threshold.

NOTE

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

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

The higher the sensitivity, the easier it is to trigger the alarm.

NOTE

When the MD2.0 function is enabled, it can only detect human or vehicles, and then trigger an alarm.

5. Configure the alarm linkage parameters.

NOTE

The alarm linkage parameters may vary based on different event type.

Alarm settings

Parameter	Description
Arming Period	Click **Settings** to set the arming period for motion detection.

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click  to enable the local alarm, then select alarm output port as needed. NOTE Ensure that the alarm status of the alarm output port is configured. For more details, refer to "Alarm Output".
PTZ Linkage	Select the checkbox, then click **Settings** to configure PTZ linkage. NOTE Ensure that PTZ control is configured. For more details, refer to "PTZ".
Recording Channel	Select one or more channels for recording. NOTE Ensure that the recording schedule and recording mode are configured in **Storage** > **Recording Plan**.
Beep	The device emits a beep when an alarm occurs.
Pop-up Alert	Enable screen prompts for detected motion.
Remote Voice	Click **Setting** next to **Remote Voice** to configure the remote voice.
IP Speaker	Select the checkbox and then click **Settings** to bind an IP speaker with the camera. NOTE Ensure that the IP speaker device has been added. For more details, refer to "IP Speaker Settings".
Event Interval	Configure the time period from the end of motion detection to the end of the alarm linkage action.
Alarm Delay	When an alarm delay is configured, the alarm will continue for an extended period after it ends.
Recording Delay	Configure the duration for which the device continues to record after the alarm has ended.

Parameter	Description
Local Audio	Enable the local audio function. You can choose a local audio as alarm sound. NOTE Ensure that you have uploaded local audio files. For more details, refer to "Uploading Audio File".
Send Email	Enable the system to send emails to notify you of an alarm event. NOTE • This feature is only available on certain models. • Ensure that the email function is configured in **System** > **Network** > **Basic** > **Email**.
Picture Storage	When an alarm occurs, the system will take a snapshot of the selected channel and store it on the device. NOTE Ensure that the snapshot schedule and snapshot mode are configured. For more details, refer to "Recording Plan".
Remote Warning Light	Click **Setting** next to **Remote Warning Light** to configure the remote voice.
Automatic Tracking	The tracking action is automatically triggered by tripwire or intrusion alarms according to the pre-defined rules. NOTE Make sure you have added the device that supports the function in **Camera** > **Camera Registration**.
Tracking Duration	The default tracking duration is set at 15minutes. NOTE Make sure you have added the device that supports automatic tracking function.

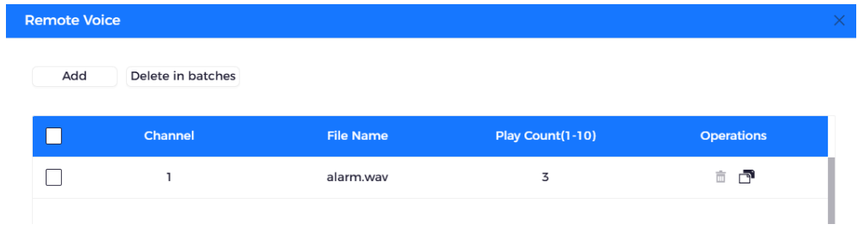
6. Click **Setting** next to **Remote Voice** to configure the remote voice.
   1. Click **Add**, and the page displays all channels that have successfully connected and support the remote voice configuration.

NOTE

If a certain channel is selected in **Remote Voice** and that channel supports remote voice configuration, the remote voice configuration for that channel will be displayed by default, and you will not be able to delete or reset the playback count.

2. Select the voice file from the **File Name** drop-down list.
3. Configure **Play Count**. It supports a maximum of 10 times.
4. Click **Copy** to copy the current channel's remote voice configuration to other channels.
5. Click to delete a channel. Select multiple channels, and then click **Delete in batches** to delete multiple channels.

Set the remote voice



NOTE

If multiple channels of remote voice settings have been configured, multiple channels can link to the corresponding voice configuration when an alarm event is triggered.

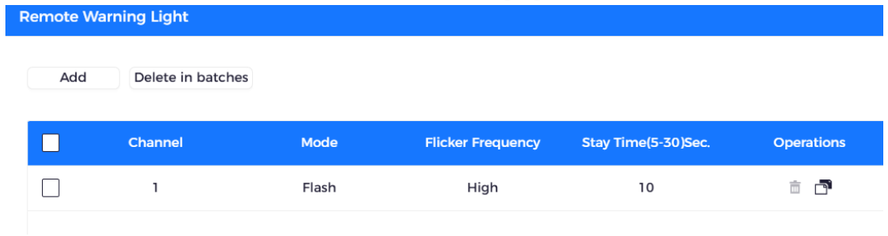
7. Click **Setting** next to **Remote Warning Light** to configure the remote voice.
   1. Click **Add**, and the page will display all channels that have been successfully connected and support remote warning light configuration.

      NOTE

      If a certain channel is selected in **Object Monitoring** and that channel supports remote warning light configuration, the remote warning light configuration for that channel will be displayed by default and cannot be deleted.

      a. Select **Mode** and **Flicker Frequency** of the remote warning light.
      b. Configure **Stay Time**. It supports a maximum of 30 seconds.
      c. Click **Copy** to copy the remote warning light configuration of the current channel to other channels.
      d. Click to delete a channel. Select multiple channels, and then click **Delete in Batches** to delete multiple channels.

Set the remote warning light



   2. Select the channel to add the remote warning light, and then click **OK**.
      If the configuration of remote warning lights for multiple channels has been completed, when an alarm event is triggered, multiple channels can link to the corresponding remote warning lights.

8. Click **Apply**.

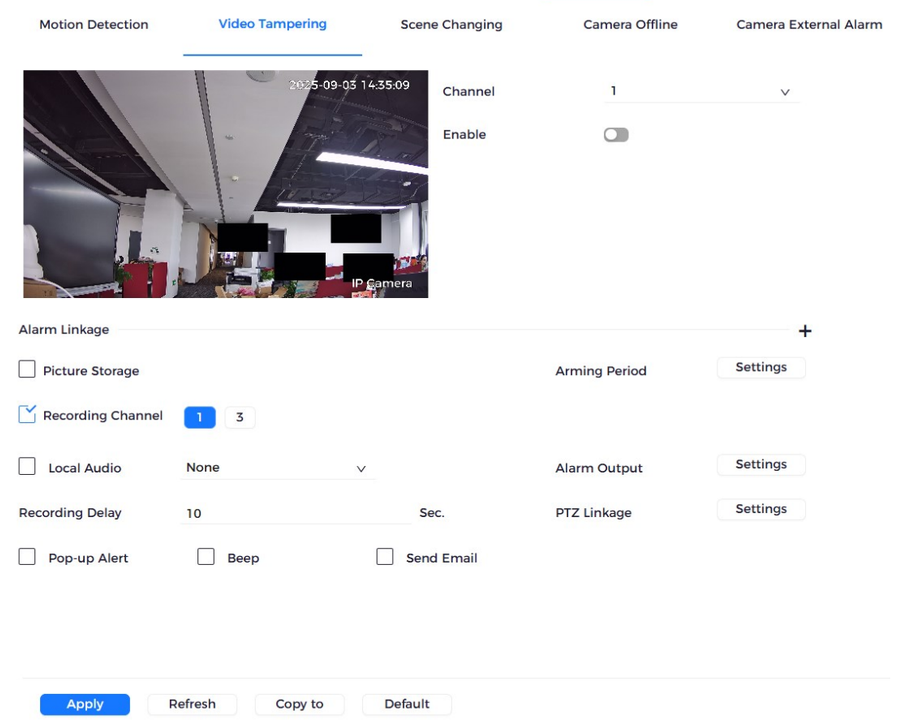
Video Tampering Alarms

Video tampering occurs when the camera lens is obstructed, or when the video displays a single color due to sunlight conditions or other reasons. You can configure alerts for this situation.

Process

1. Go to **Camera** > **Basic Event** > **Video Tampering**.

Video tampering



2. Select a channel, then click to enable video tampering.
3. Configure other parameters. For more details, refer to "Alarm settings".
4. Click **Apply**.

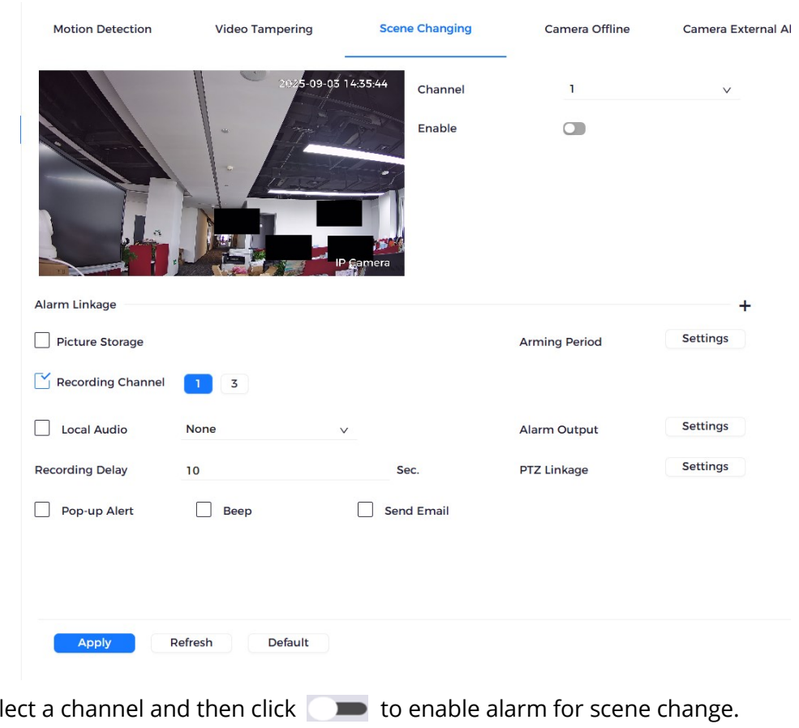
Scene Changing Alarms

When the system detects a change in the scene, it will trigger an alarm.

Process

1. Go to **System** > **Events** > **Video Detection** > **Scene Changing**.

Scene changing



2. Select a channel and then click to enable alarm for scene change.
3. Configure alarm linkage parameters. For more details, refer to "Alarm settings".
4. Click **Apply**.

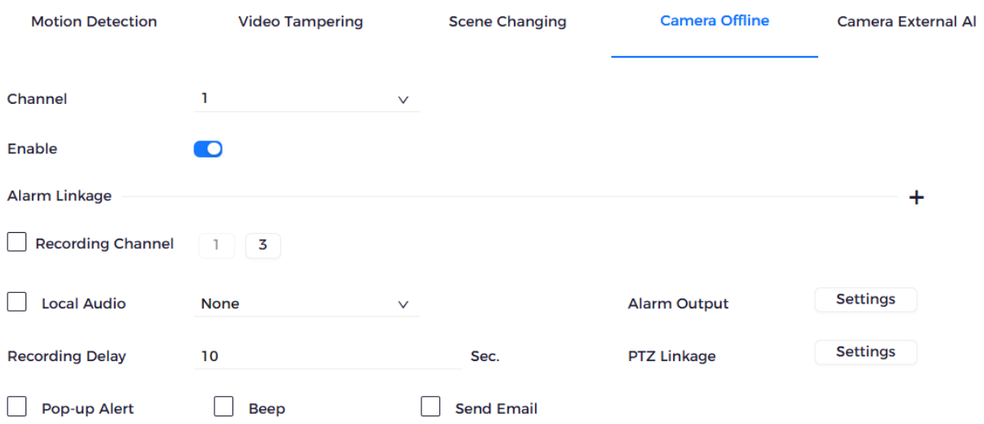
Camera Offline

When the camera is offline, an alarm will be triggered.

Process

1. Go to **Camera** > **Basic Event** > **Camera Offline**.

Camera Offline



2. Select a channel, then click to enable alarm for camera offline.
3. Configure alarm linkage parameters. For more details, refer to "Alarm settings".
4. Click **Apply**.

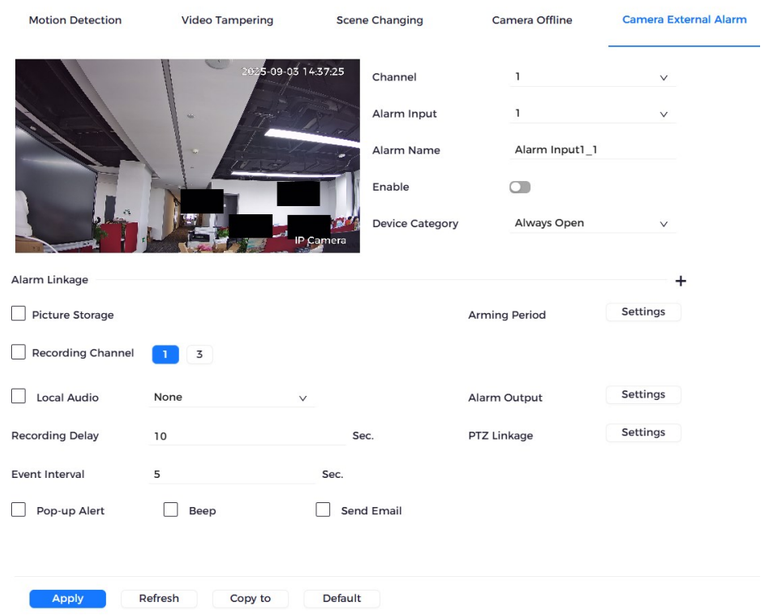
Camera External Alarm

When the external alarm device of the camera is triggered, the alarm signal will be transmitted to the device, and then the system will execute the alarm linkage operation.

Process

1. Go to **Camera** > **Basic Event** > **Camera External Alarm**.

Camera external alarm



2. Select a channel, then enter the alarm name.
3. Click to enable the alarm.
4. Select the device category from **Always Closed** and **Always Open**.
5. Configure alarm linkage parameters. For more details, refer to "Alarm settings".
6. Click **Apply**.

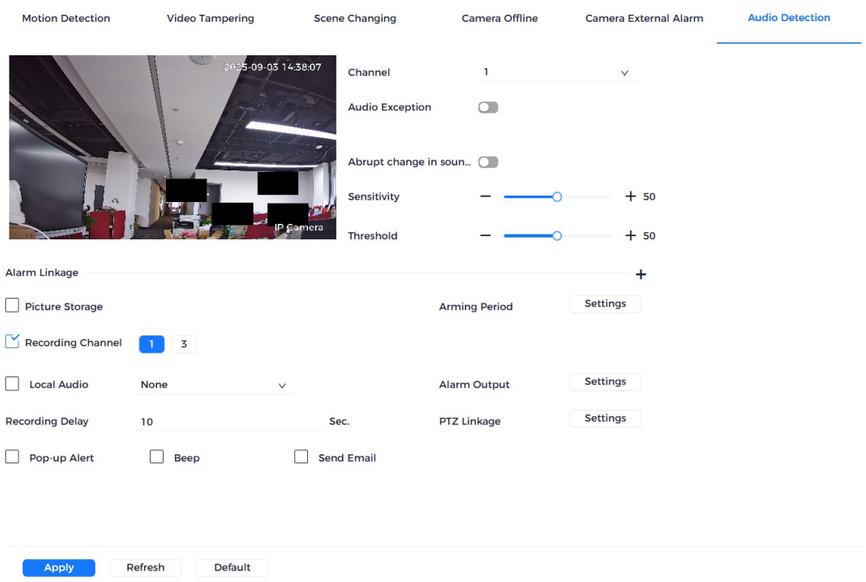
Audio Detection

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

Process

1. Go to **Camera** > **Basic Event** > **Audio Detection**.

Audio detection



2. Select a channel, then click to enable detection of audio exception and intensity change.
   - **Audio Exception:** When there is an audio input anomaly, the system will generate an alarm.
   - **Abrupt Change:** Set sensitivity and threshold. An alarm will be triggered when the change in sound intensity exceeds the defined threshold.
3. Configure alarm linkage parameters. For more details, refer to "Alarm settings".
4. Click **Apply**.

Configuring AI Event

Intelligent Mode

Camera AI Mode

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

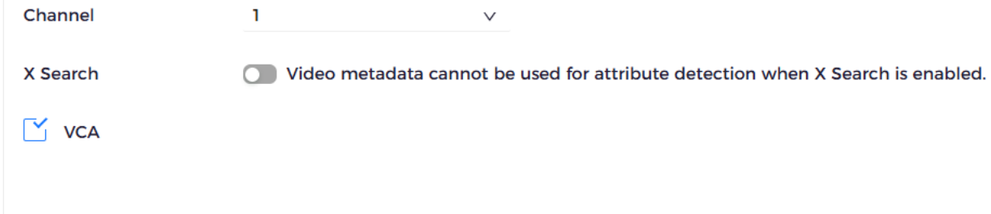
Process

1. Go to **Camera** > **AI Event** > **Intelligent Mode**> **Camera AI Mode**.
2. Select a channel.

NOTE

The available smart functions vary by camera.

VCA option



3. Click the checkbox next to the corresponding smart mode to enable it.

   NOTE

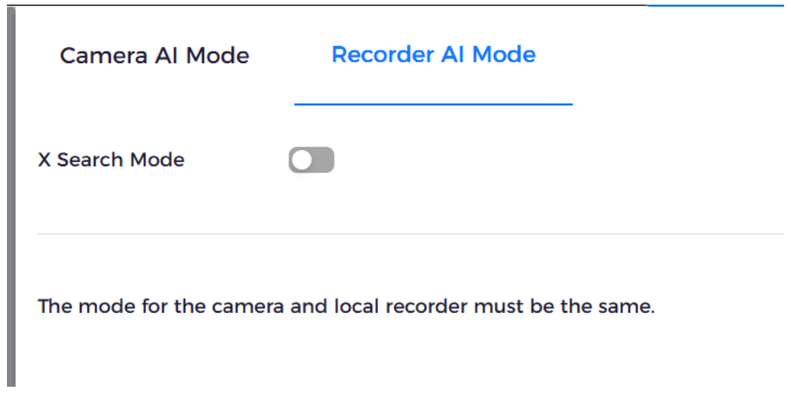
   If the channel is connected to a PTZ camera, you can set smart functions for each preset point individually.
4. Click **Apply**.

Recorder AI Mode

Process

1. Go to **Camera** > **AI Event** > **Intelligent Mode**> **Recorder AI Mode**.
2. Select the mode.

Select Mode



- X Search: Enable the **X Search Mode**. you can use the X Search function to accurately search for and view targets during live view and playback.

NOTE

If you enabled the X Search function, the incoming bandwidth will drop to 236Mbps, and AI by recorder function will not available.

3. In the pop-up window, click **OK**.

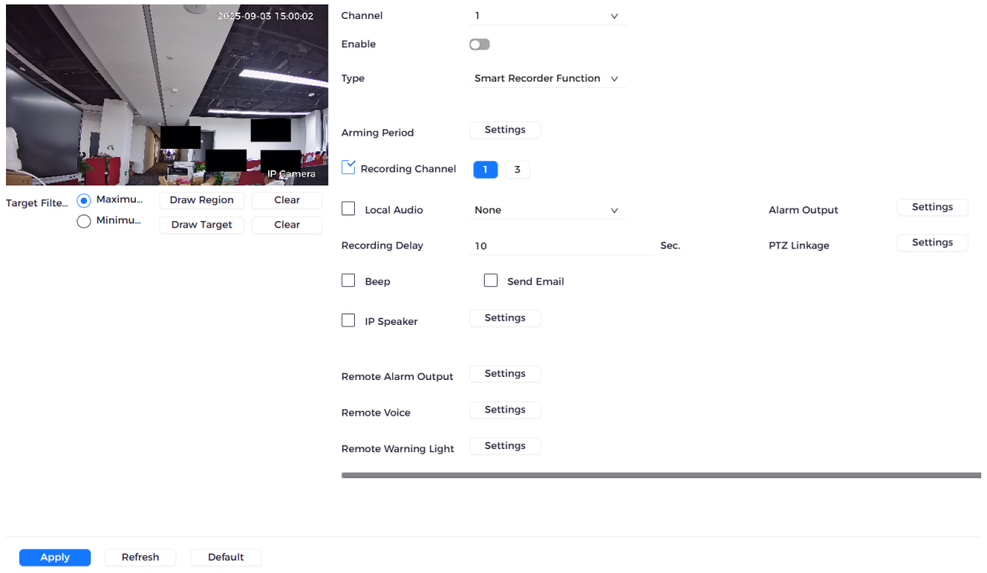
Face Detection

Configure the alarm rules for face detection. An alarm will be triggered when a face is detected within the detection area.

Process

1. Go to **Camera** > **AI Event** > **Face Detection**.

Face detection

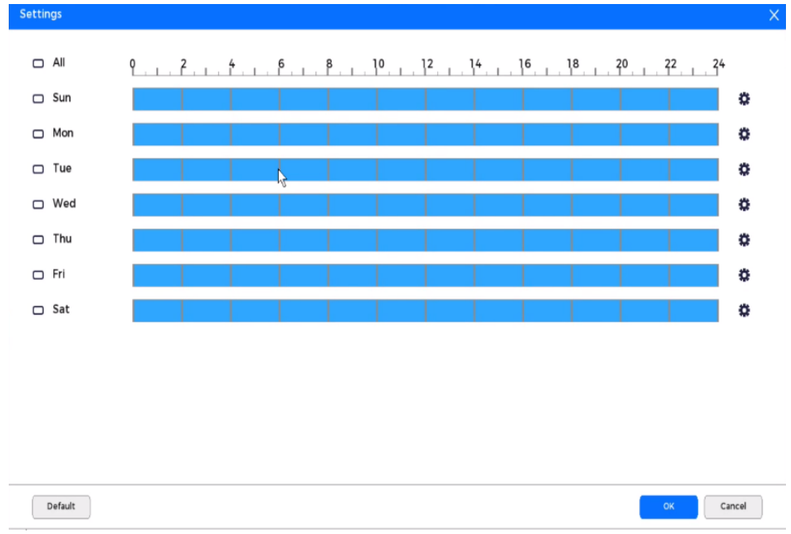


2. Select a channel, then click to enable the face detection.
3. Click **Settings** next to **Rules** to draw the minimum or maximum size to filter the target. When the detected target size is between the maximum size and the minimum size, the system will trigger an alarm.
4. Click **Settings** next to **Arming Period** to configure the arming period.

   The arming period is highlighted. You can configure the period in 2 ways.

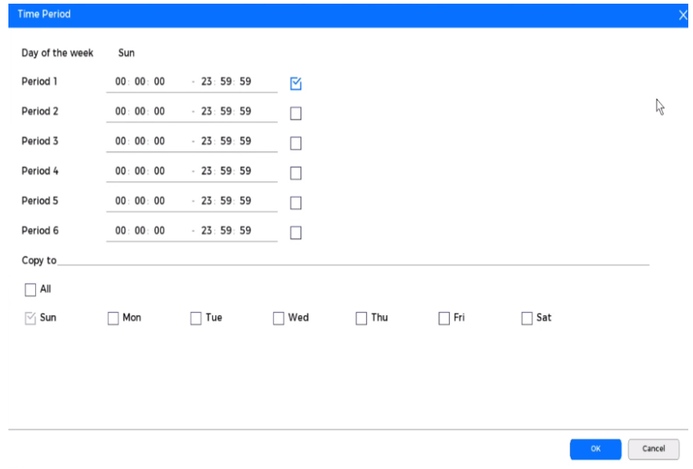
   - Drag along the timeline to define the time period. You can click on the orange section to remove the time period

Arming period (1)



   - Click to define the arming period for each day within a week.
     - You can set up to 6 time slots for each day.
     - Under **Copy to**, select **All** to apply the settings to all the days of the week, or select specific days to which you wish to apply the settings.

Arming period (2)



5. Configure the alarm linkage. For more details, refer to "Alarm settings".
6. Click **Apply**.

Face Recognition

Configure facial recognition alarm rules. Set up facial recognition alarm linkage, which compares detected facial images with those in the database. When the comparison results meet the predefined alarm criteria, the system will execute the alarm linkage operation.

Background Information

The system will compare the detected faces with the faces in the database to determine whether the detected faces belong to the database. An alarm will be triggered when the similarity reaches the defined threshold.

Process

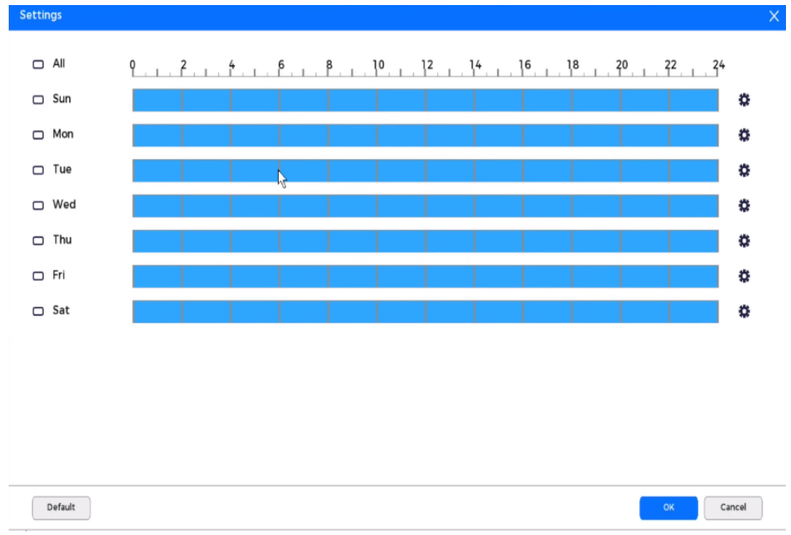
1. Go to **Camera** > **AI Event** > **Face Recognition**.
2. Select **Smart Camera Function** or **Smart Recorder Function**.
3. Enable the function.

   NOTE

   - When you configure face database with Smart Camera Function, if there is no available face database, please refer to "Face Database"
   - When you configure face database with Smart Recorder Function, if there is no available face database, please refer to "Face Database"
   - Select **Smart Camera Function**.
     1. Enable **Face Enhancement**.
     2. Configure the face similarity.
     3. Click in the operation list to enable the database.
   - Select **Smart Recorder Function**.
     1. Click **Settings** behind **Arm Face Database** to add database.
     2. Click to configure the face similarity.
     3. Click in the operation list to enable the database.
4. Configure the alarm schedule. Click **Settings** behind **Arming Period** to set the period.

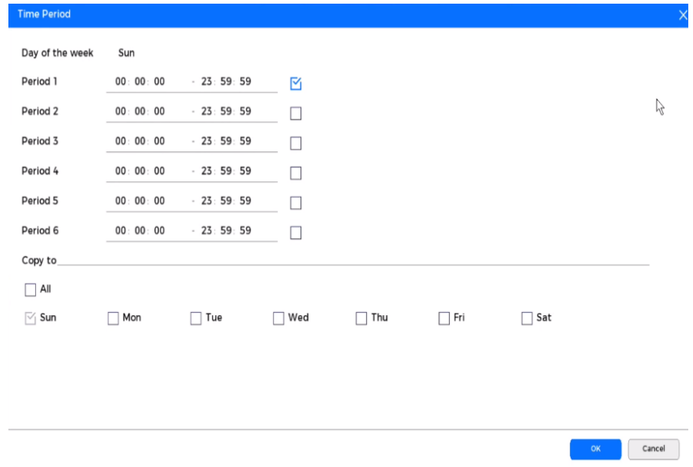
   The arming period is highlighted. You can configure the period in 2 ways.
   - Drag on the time line to define the period. You can click on the orange section to remove the time period.

Arming period (1)



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

Arming period (2)



5. Set alarm linkage actions. For more details, refer to "Alarm settings".
6. Click **Apply**.

Face Database

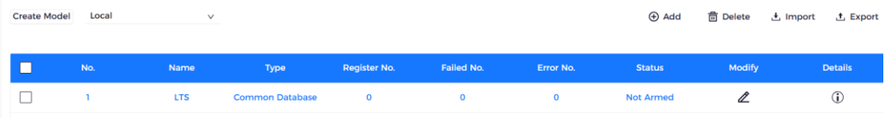
Local Face Database

The created face database exists only on the local device and is used for facial comparison through the smart recording function.

Process

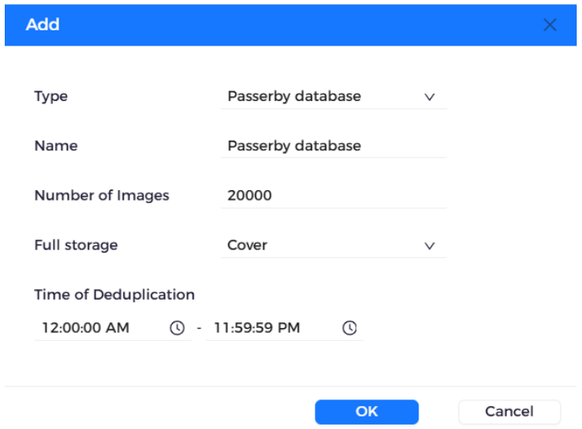
1. Go to **Camera** > **AI Event** > **Face Database**.

Face database (local)



2. Select **Local**, then click ➕.

Create the face database (passerby database)



3. Select the face database type, set the parameters, then click **OK**.

Passerby database parameters

Parameter	Description
Name	Enter a name for the passerby database.
Number of Images	The number of images that can be included in the configuration database.
Full storage	Select the storage strategy when the storage is full. • Stop: Unable to add more images. • Cover: The latest image overlays the oldest image. Backup the old image as needed.
Time of Deduplication	Set the time period for the system to remove duplicate facial images from the database.

Related Operations

- Add face images.
  Click 🖼 to go to the face database page and manage the face images in the database.
- Edit registration information.
  Click ✎ to modify the registration information.
- Face database configuration.
  When performing face comparison with the linked face database, the face database can be configured.
- Delete the face database.
  Select one or more face images, and then click **Delete**.

Remote Face Database

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

Process

1. Select **Camera** > **AI Event** > **Face Database**.
2. Select **Remote**, then click ➕.
3. Enter database name.
4. Click **OK**.

Related Operations

- Add face images.
  Click 🖼 to enter the face database page and manage the face images in the database.
- Edit registration information.
  Click ✎ to modify the registration information.
- Face database configuration.
  When you conduct face comparison with the linked face database, the face database can be configured.
- Delete the face database.
  Select one or more face images, and then click **Delete**.

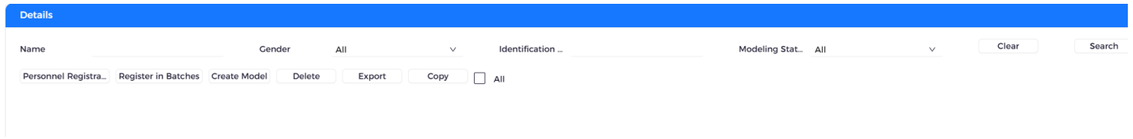
Adding Images to Face Database

Register Face Image on by one

You can add one face image to the database. This is for situations where there are fewer registered face images.

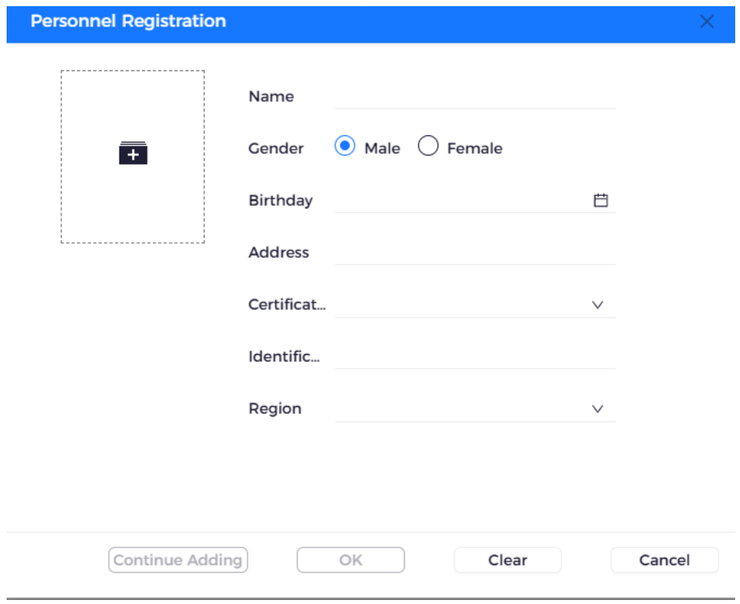
1. Go to **Camera** > **AI Event** > **Face Database**.
2. Click of the database that you want to configure.

Database details



3. Click **Personnel Registration**.

Personnel Registration



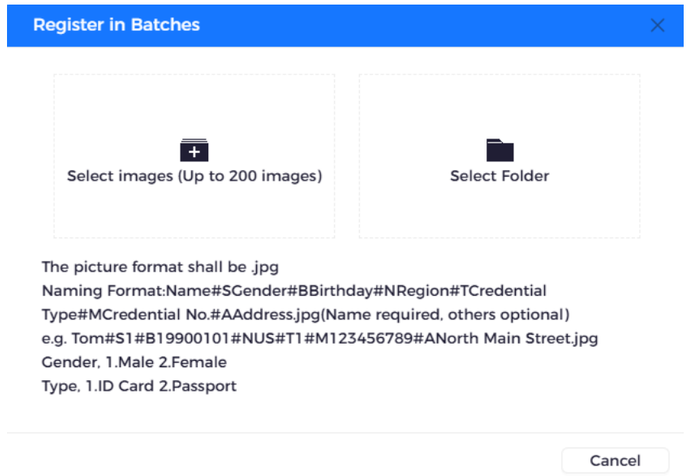
4. Click to add a face image.
5. Select a face image and enter the registration information.
6. Click **OK**, and the system will prompt that the registration was successful.
7. On the **Details** page, click **Search**. The system will prompt modeling is successful.

Register in Batches

The system supports batch addition if you wish to import multiple face images simultaneously.

1. Go to **Camera** > **AI Event** > **Face Database**.
2. Click of the database you wish to configure.
3. Click **Register in Batches**.

Register in Batches



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

VCA

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

Background Information

VCA functions

Function	Description	Scene
Line Crossing	When the target crosses the warning line from the defined direction of movement, the alarm is triggered, and the system subsequently executes the configured alarm linkage.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Intrusion		
Abandoned Object	When an object is abandoned in the detection area for longer than the configured time, the system will trigger an alarm and execute the configured alarm linkage.	The targets in the scene are sparse, and there are no obvious and frequent changes in lighting. It is recommended to use simple scenes within the detection area.

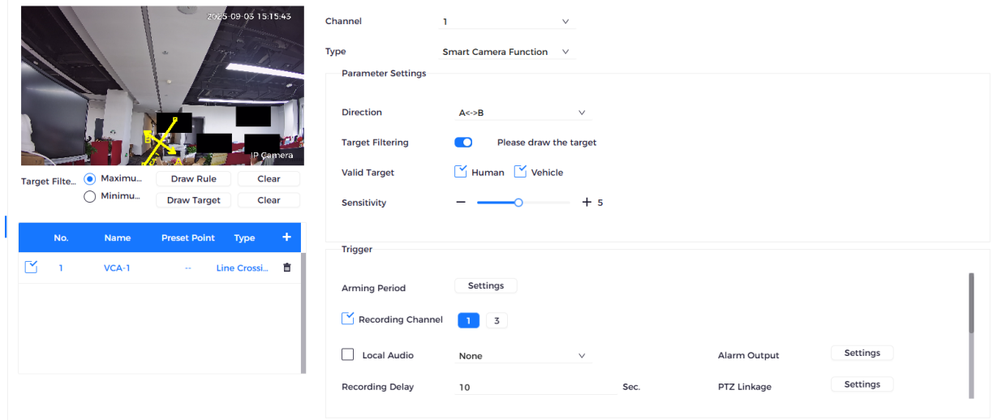
Function	Description	Scene
Missing Object	When an object is removed from the detection area within the defined time, the system will trigger an alarm and execute the configured alarm linkage.	• In scenarios with dense targets, frequent obstructions, and crowd congestion, the likelihood of missed alarms may increase. • In scenarios with complex foregrounds and backgrounds, false alarms may be triggered due to abandoned or missing objects.
Parking Detection	When the target stays over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.
Aggregate Detection	When a crowd gathers or the crowd density is high, an alarm will be triggered, and the system will execute the configured alarm linkage.	Medium or long-distance scenes, such as outdoor squares, government entrances, and station entrances and exits. Not suitable for short-distance perspective analysis.
Loitering Detection	When the target loiters over the shortest alarm time, the system will trigger an alarm and then execute the configured alarm linkage. After the alarm is triggered, if the target remains in the area within the alarm time interval, the alarm will be triggered again.	Scenes such as park and hall.

In this section, crossing the line and intrusion behavior are presented as examples of configuring VCA rules.

Process

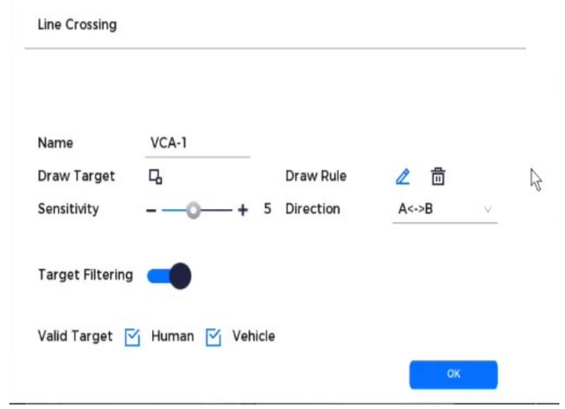
1. Go to **Camera** > **AI Event** > **VCA**.

VCA



2. Select a channel, then click **Add** to add a rule.
3. Select the **Enable** checkbox.
   1. In the **Type** column, select **Line crossing and intrusion**.
   2. Click .

Line crossing and intrusion



3. Configure the related parameters.

Line crossing and intrusion parameters

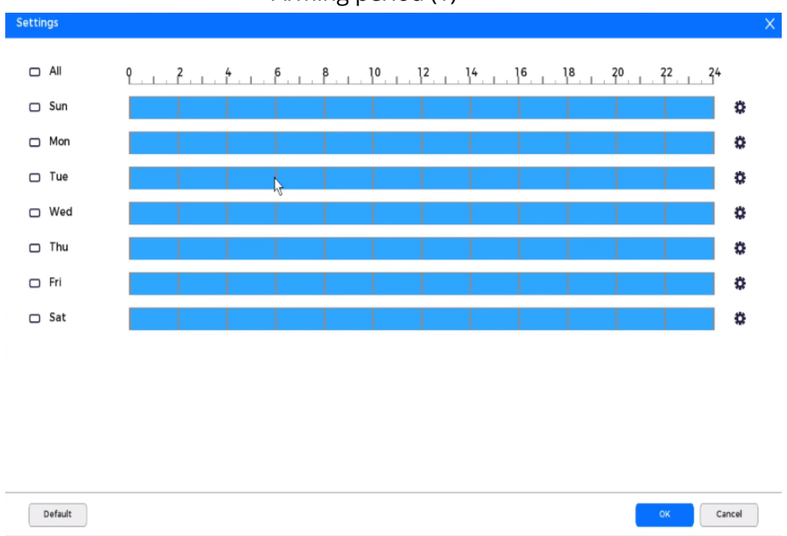
Parameter	Description
Name	Rule name.
Draw Target	Click to draw the minimum or maximum size to filter the target. The system only triggers an alarm when the detected target size is between the maximum size and the minimum size.

Parameter	Description
Draw Rule	Drag to draw a line. The line can be a straight line, a polyline, or a polygon.
Sensitivity	You can set the sensitivity for alarm. The higher the value, the easier it is to detect fast-moving objects, but at the same time, the false positive rate also increases.
Direction	Select a line direction, including A→B, B→A and A↔B.
Target Filtering Valid Target	Click and select valid target. **Human** and **Vehicle** are selected by default.

4. Click **OK**.

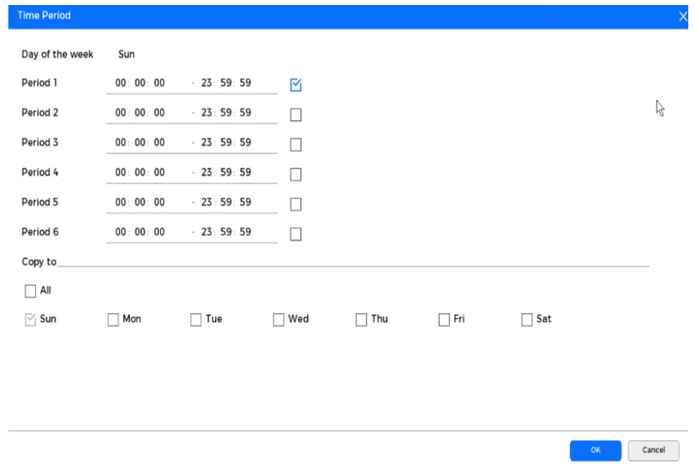
4. Click **Settings** next to **Arming Period** to configure the arming period.
   The arming period is highlighted. You can choose 2 ways to configure the period.
   - Drag along the timeline to define the time period. You can click on the orange section to remove the time period.

Arming period (1)



   - Click to define the arming period for each day of the week.
     - You can set up to 6 periods for each day.
     - Under **Copy to**, select **All** to apply the settings to all the days of the week, or choose specific days on which you wish to apply the settings.

Arming period (2)



5. Configure the alarm linkage. For more details, refer to "Alarm settings".
6. Click **Apply**.

E Tracking

The function can simultaneously zoom in and track multiple persons and vehicles that trigger alarms. It provides both rich detail and a panoramic view.

Process

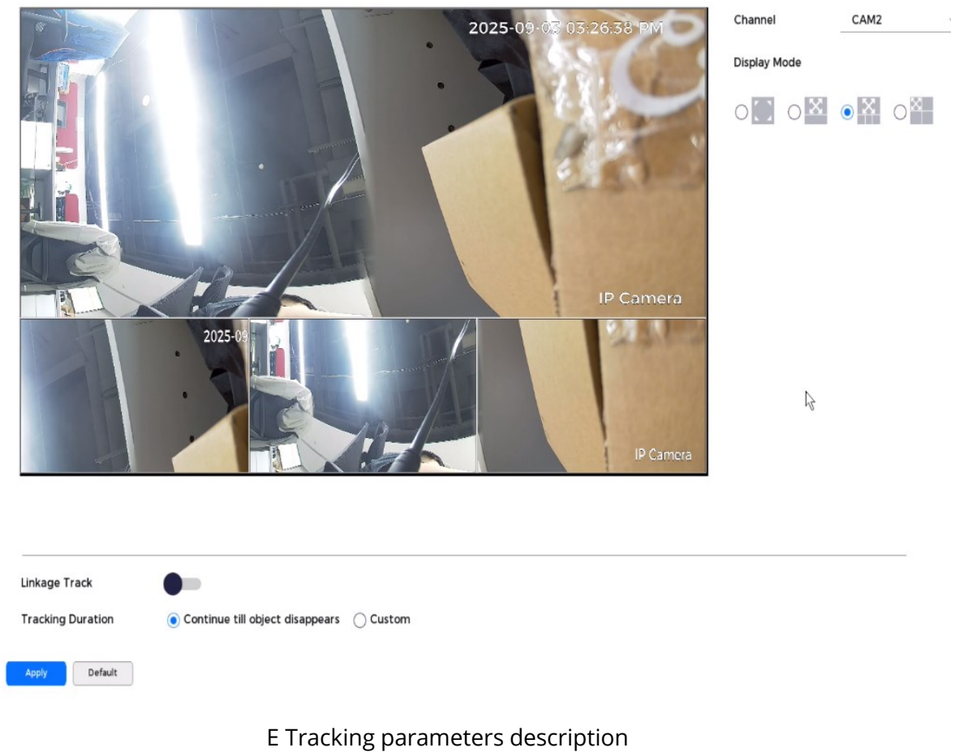
1. Go to **Camera** > **AI Event** > **E-Tracking**.

   NOTE

   You can configure E-Tracking only when the camera supports the function.

2. Configure the parameters.

E-Tracking



E Tracking parameters description

Parameter	Description
Channel	Select the channel.
Display Mode	Select the number of tracking channels. Full screen, 1+1, and 1+3 modes are available, and full screen is default.
Linkage Track	After enabling **Linkage Track**, intelligent events will be tracked. By default, this function is disabled.
Tracking Duration	• Custom: Manually select the tracking duration. For example, if you set it from 30 seconds to 60 seconds, after tracking object A for 30 seconds, if object B appears, the camera will start tracking object B; if no other objects appear during the tracking of object A, the camera will stop tracking object A after 60 seconds • Continue till object disappears: When the detected object disappears from the image, the camera will stop tracking.

3. Click **Apply**.

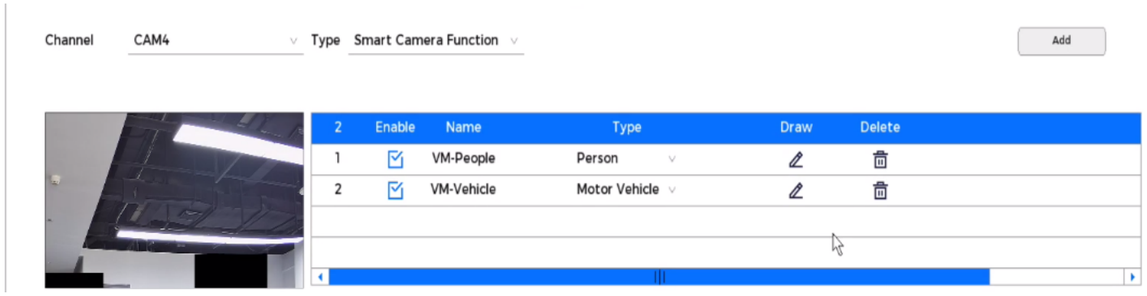
Metadata Setting

When a metadata alarm is triggered, the system will link the corresponding camera to record video and logs, and take snapshots. Video metadata does not support other alert linkage operations.

Process

1. Go to **Camera** > **AI Event** > **Metadata Setting**.

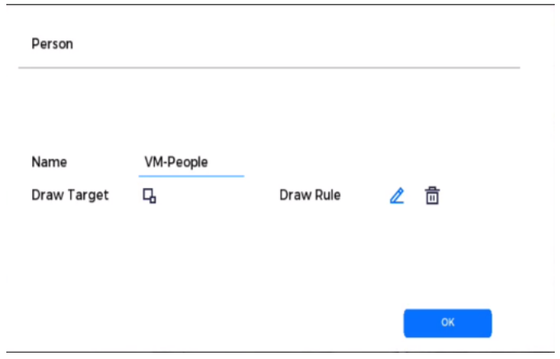
Metadata setting



2. Select a channel, and then click **Add**.

   Click 🗑 to delete the rule.
3. Select the **Enable** checkbox, and then set **Type** to **Person** or **Motor Vehicle**.
4. Draw detection rules.
   1. Click ✎ and draw a detection area. Right-click the image to finish drawing.

      Person detection

   2. Enter the rule name.
   3. Click ⧉ to draw the minimum or maximum size to filter the target.

      The system will trigger an alarm only when the size of detected target is between the maximum and the minimum size.
   4. Select the related preset point.
   5. Click **OK**.
5. Click **Apply**.

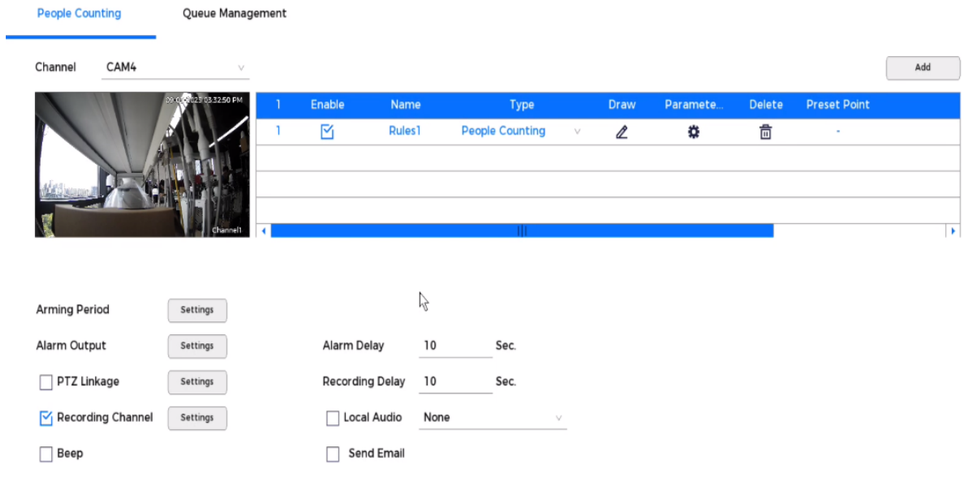
People Counting

The system counts the number of people entering and exiting the detection area. An alarm will be triggered when the number of people entering, exiting, or remaining exceeds the threshold.

Process

1. Go to **Camera** > **AI Event** > **People Counting**.

People counting

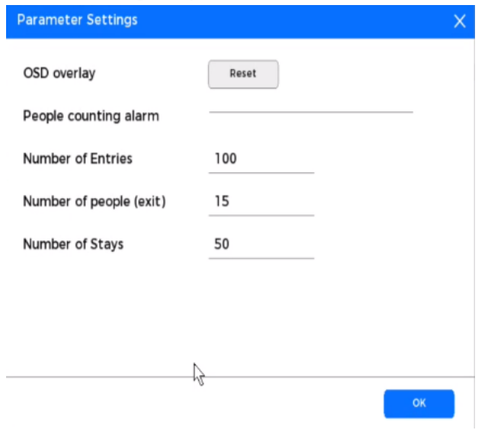


2. Select a channel and click **Add**.
3. Select the **Enable** checkbox, then set **Type** to **People Counting**.
4. Set people counting rule.
   1) Click to draw people counting rule. Right-click the image to finish drawing.

People counting rule

   2) Set the rule name and preset point, then select direction.
   3) Click **OK**.
5. Click under **Parameters** and configure the parameters.

Configure parameters

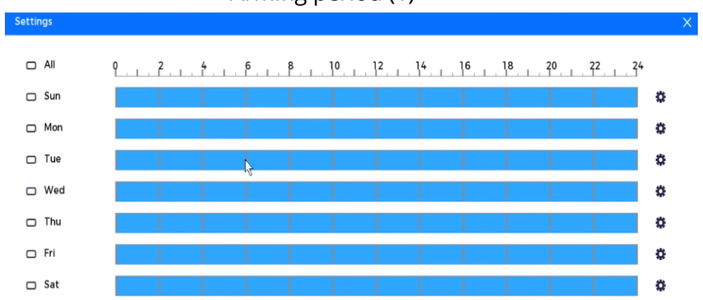


People counting parameters

Parameter	Description
Number of Entries	When the number of people entering the detection area exceeds the set threshold, the alarm will be triggered.
Number of People (Exit)	When the number of people leaving the detection area exceeds the set threshold, an alarm will be triggered
Number of Stays	When the number of people remaining in the detection area exceeds the set threshold, an alarm will be triggered.

6. Click **Settings** next to **Arming Period** to configure the arming period.
   The arming period is highlighted. You can choose 2 ways to configure the period.
   - Drag on the time line to define the period. You can click on the blue section to remove the time period.

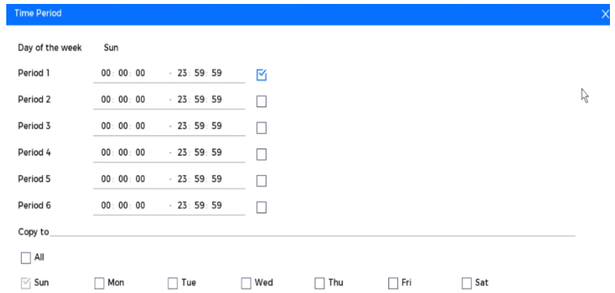
Arming period (1)



   - Click to define the arming period for each day of the week.
     - You can set up to 6 periods for each day.
     - Under **Copy to**, select **All** to apply the settings to all the days of the week, or choose

specific days to which you wish to apply the settings.

Arming period (2)



7. Configure the alarm linkage. For more details, refer to "Alarm settings".
8. Click **Apply**.

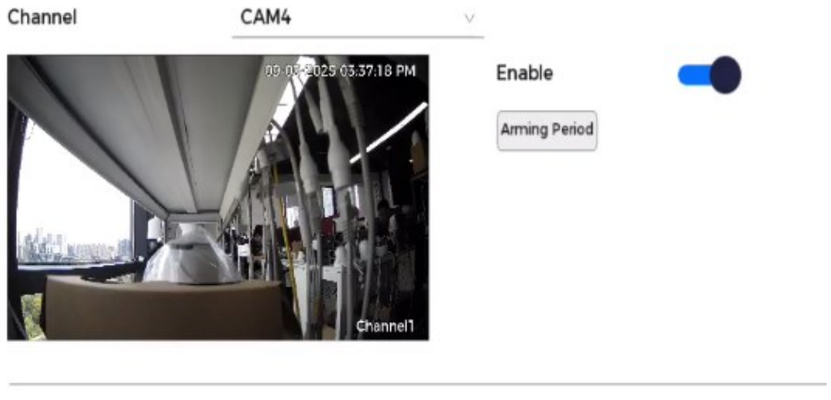
Heat Map

Heat map technology can monitor the distribution status of active objects within a specified area over a period of time and display it on the heat map using different colors.

Process

1. Go to **Camera** > **AI Event** > **Heat Map**.

Heat map



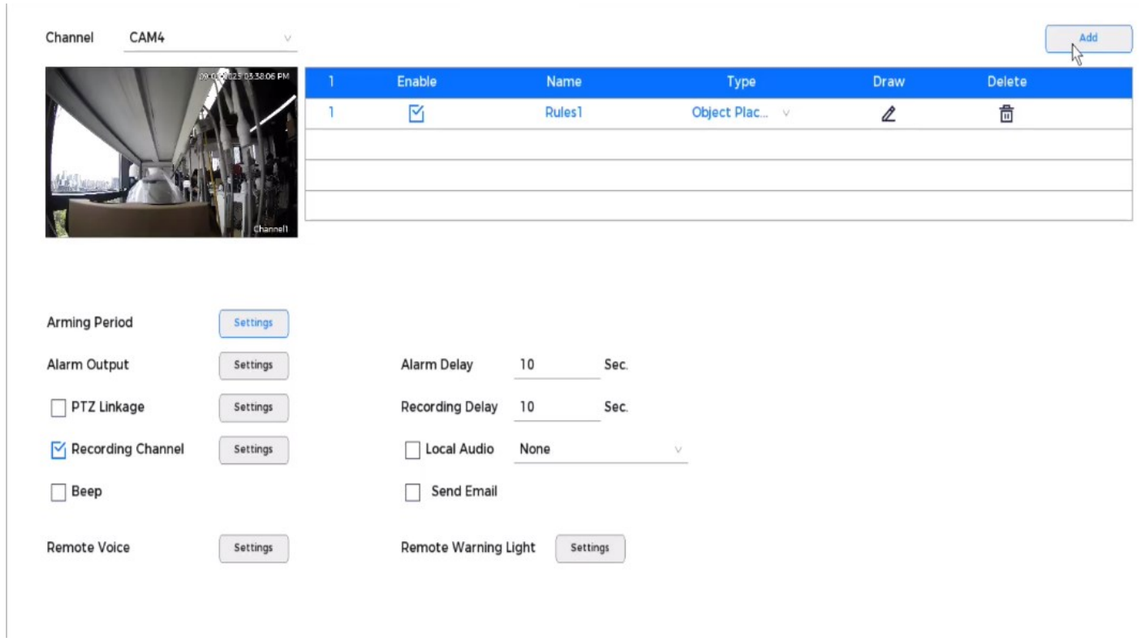
2. Click to enable the function.
3. Click **Apply**.

Object Monitoring

Process

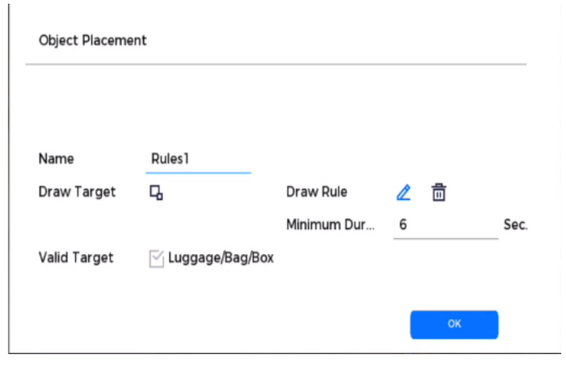
1. Go to **Camera** > **AI Event** > **Object Monitoring**.

Object Monitoring



2. Select a channel, then click **Add**.
   Click to delete the rule.
3. Select the **Enable** checkbox, and then set **Type** to **Object Placement** or **Object Fetch**.
4. Draw a detection rule.

Draw a rule



1) Click , then draw a detection area. Right-click the image to finish drawing.
2) Click to draw the minimum or maximum size to filter the target.

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

NOTE

Click to delete the draw rule.

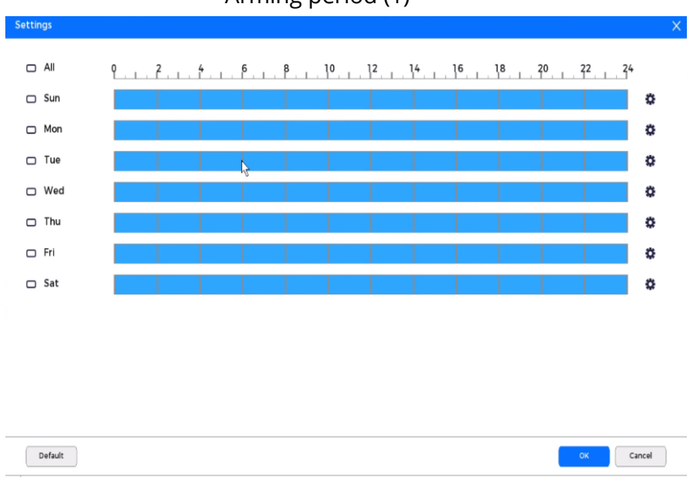
3) Set the rule name and minimum duration.
4) Select the checkbox next to **Luggage/Bag/Box** to confirm the valid target.
5) Click **OK**.

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

The arming period is highlighted. You can choose 2 ways to configure the period.

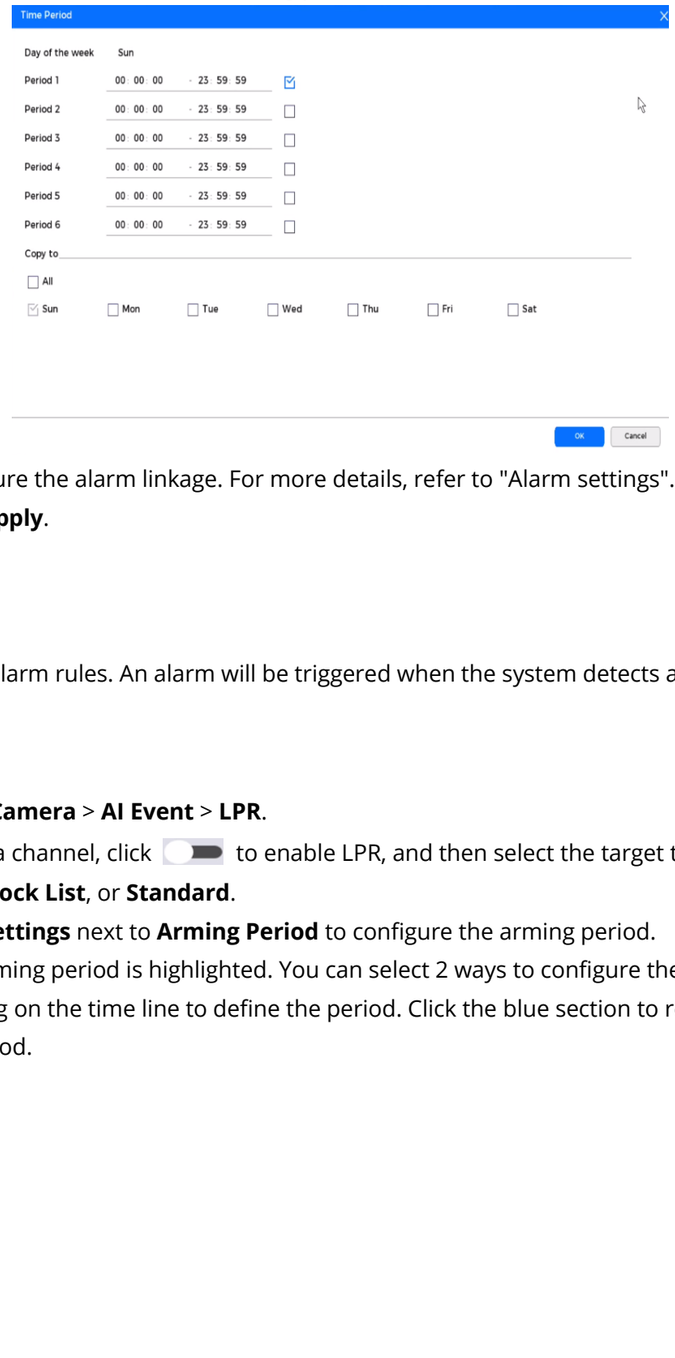
- Drag on the time line to define the period. Click on the blue section to remove the time period.

Arming period (1)



- Click to define the arming period for each day of the week.
  - You can set up to 6 periods for each day.
  - Under **Copy to**, select **All** to apply the settings to all the days of the week, or choose specific days to which you wish to apply the settings.

Arming period (2)



6. Configure the alarm linkage. For more details, refer to "Alarm settings".
7. Click **Apply**.

LPR

Configure LPR alarm rules. An alarm will be triggered when the system detects a specific license plate.

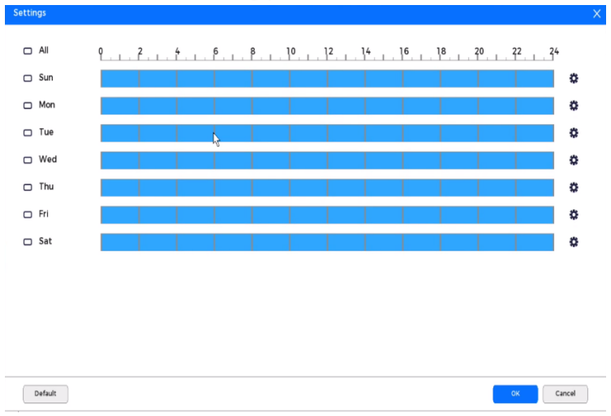
Process

1. Go to **Camera** > **AI Event** > **LPR**.
2. Select a channel, click to enable LPR, and then select the target type from **Allow List**, **Block List**, or **Standard**.
3. Click **Settings** next to **Arming Period** to configure the arming period.

   The arming period is highlighted. You can select 2 ways to configure the period.

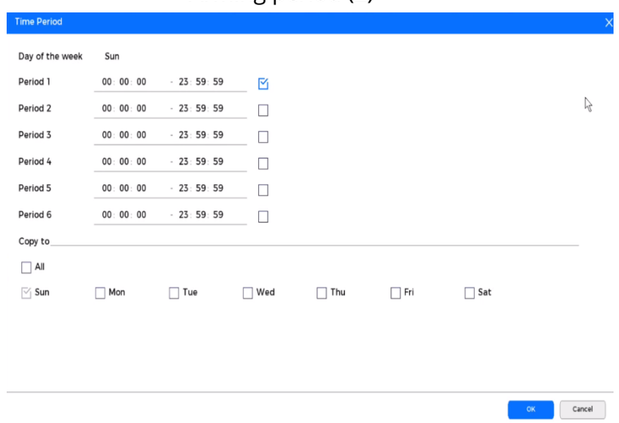
   - Drag on the time line to define the period. Click the blue section to remove the time period.

Arming period (1)



- Click ⚙ to define the arming period for each day of the week.
  - You can set up to 6 periods for each day.
  - Under **Copy to**, select **All** to apply the settings to all the days of the week, or choose specific days to which you wish to apply the settings

Arming period (2)



4. Configure the alarm linkage. For more details, refer to "Alarm settings".
5. Click **Apply**.

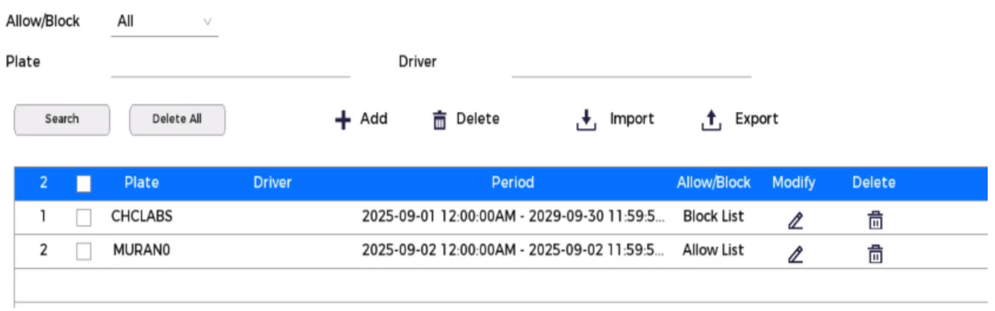
LPR Database Settings

In order to facilitate vehicle management, you can add license plate numbers to the blacklist or whitelist. The system can compare the detected license plate information with the plates on the blacklist and whitelist, and then trigger the corresponding alarm linkage.

Process

1. Go to **Camera** > **AI Event** > **LPR Database**.

LPR Database



2. Click ➕ to add manually.
3. Set up license plate information such as plate number, driver name, select **Block List** or **Allow List**, then set validity period.
4. Click **OK**.

Related Operations

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

Storage

Configure the recording plan, recording mode, storage strategy and other storage related information.

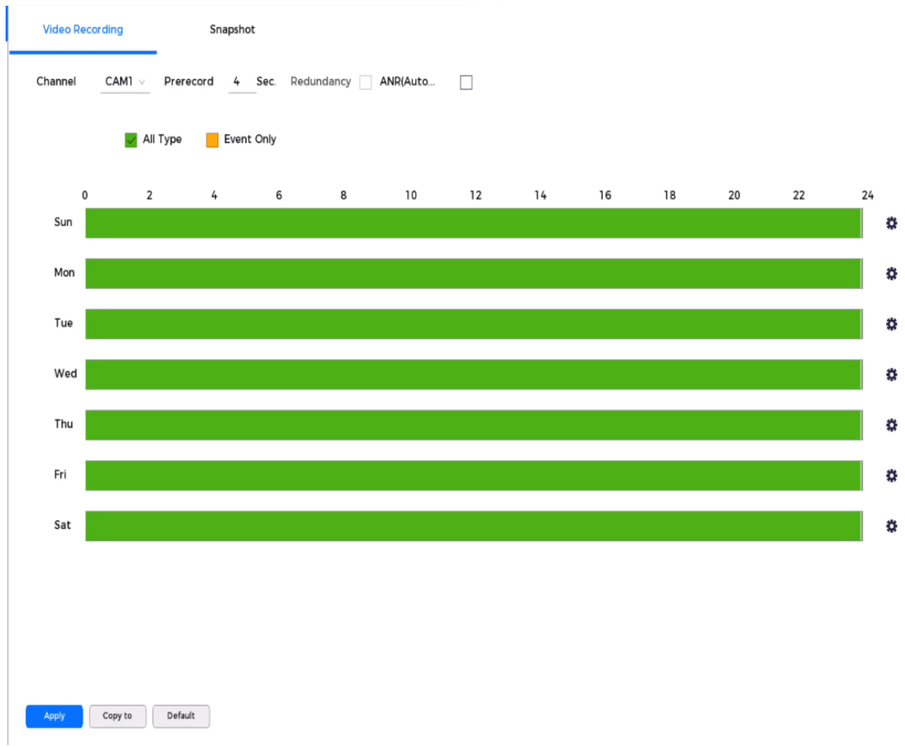
Recording Plan

Configure the recording plans. This part takes video recording as an example. This section uses video recording as an example, with snapshot schedules being configured similarly.

Process

1. Go to **Storage** > **Recording Plan**.

Video recording



2. Configure recording settings.

Video recording parameters

Parameter	Description
Channel	Select a channel to record videos.
Prerecord	Set the record duration before the event occurs.
Redundancy	Enable redundancy for the channel. If two or more hard drives are installed on the device, you can designate one of them as a redundant drive to back up recorded files. • If the selected channel is not currently recording, the redundancy feature will take effect during the next recording session, regardless of whether the checkbox is selected. • If the selected channel is currently recording, the ongoing recording will be packaged, and the device will then commence recording according to the new schedule. NOTE • This feature is only available on select models. • The redundant hard drive only backs up videos, not snapshots.
Automatic network replenishment (ANR)	Set the ANR (auto network resume) function. • When the connection between the NVR and IPC fails, the IPC will continue recording. Once the network is restored, the NVR can download the recorded files even while disconnected from the IPC. This is implemented to help prevent data loss from currently connected IPC channels. • Set a maximum recording upload period. If the offline duration exceeds the specified period you set, the IPC will only upload recording files within the designated timeframe. NOTE Ensure the SD card is installed and enable the recording function on the IPC
Event type	Select **All Type** or **Event Only**. The default is **All Type**.
Time Period	Set a period during which the configured recording settings are active. • Drag on the timeline to set the time period. • You can also click ⚙ to set the period.

Parameter	Description
Default	Restore the recording plan to default settings.
Copy to	Copy the recording plan settings to other channels.

3. Click **Apply**.

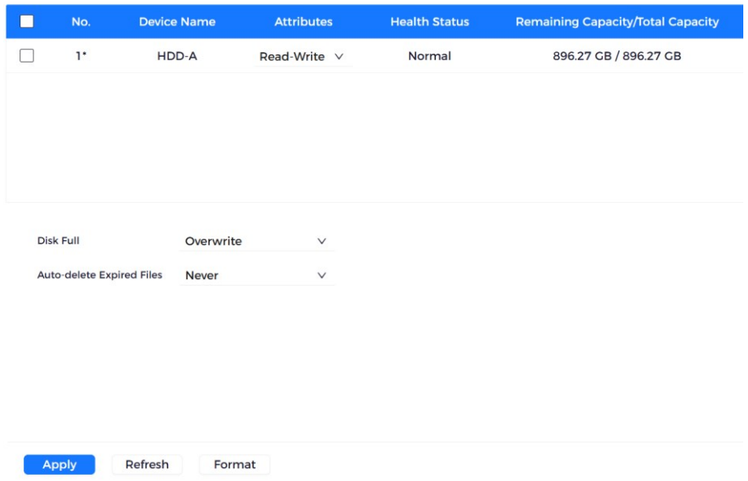
Storage Strategy

Configure storage strategy and manage hard disk drives.

Process

1. Go to **Storage** > **Disk Management**.
2. Configure the storage strategy.

Disk management



Disk management parameters

Parameter	Description
Disk Full	Storage strategy to be used when no more storage space is available. • Stop: Stop recording. • Overwrite: The latest document overrides the oldest document.
Auto-delete Expired Files	Configuration allows the device to automatically delete expired content. • If you do not wish to use this feature, please select **Never**. • Select **Custom**, then configure the duration for which you wish to retain the old files.

3. On the disk list, view the hard disk information and configure the hard disk type.
   - Set hard disk type.
     In the **Attributes** column, select **Read-Write**, **Read-only** or **Redundancy** to set the hard disk type.
   - Format hard disk.
     Select a hard disk, then click **Format**, and then follow the on-screen prompt to format the hard disk.

     ⚠ CAUTION

     Formatting will erase all data on the hard disk.

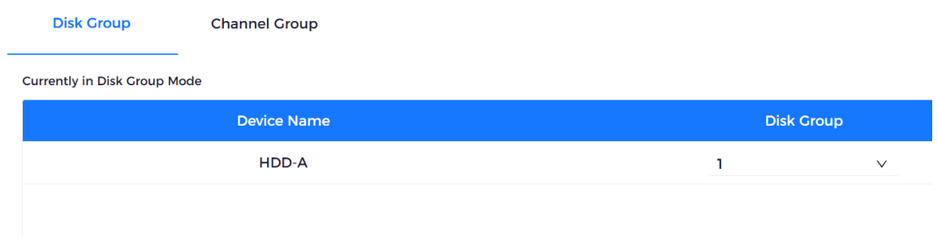
Disk Group

By default, the installed hard disk drives and the created RAID are located in Disk Group 1. You can configure the hard disk groups and set them up for main-stream, sub-stream, and snapshot operations.

Process

1. Go to **Storage** > **Disk Group** > **Disk Group**.

Disk group



2. Select the group for each hard disk drive, and then click **Apply**.
   After configuring hard disk drive group, under the **Channel Group** tab, configure the settings to save main stream, sub stream and snapshot to different disk groups, and then click **Apply**.

Channel Group

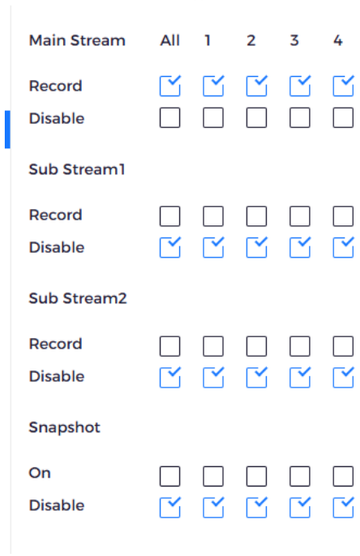
Recording Mode

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

Process

1. Go to **Storage** > **Recording Mode**.

Recording mode



2. Enable or disable recording for each channel.

NOTE

If you wish to configure the same recording mode for all channels, you can select **All**.

3. Click **Apply**.

Disk Quota

Allocate a certain storage capacity for each channel to properly manage the storage space.

Background Information

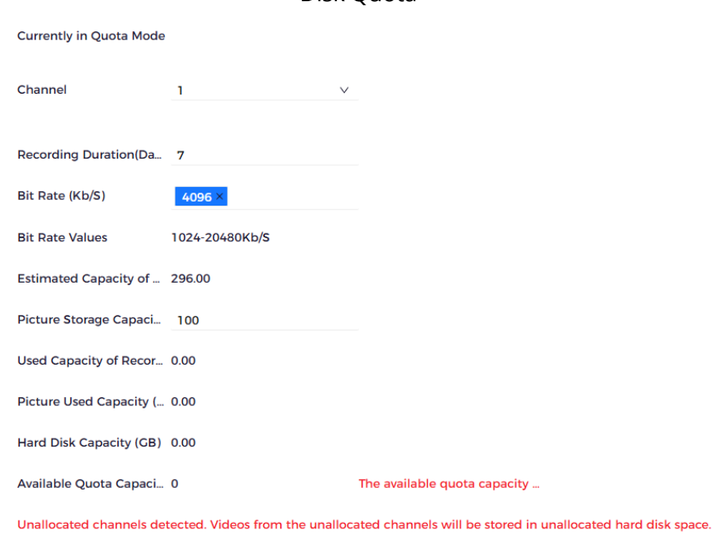
NOTE

Disk quota mode and disk group mode cannot be selected simultaneously.

Process

1. Go to **Storage** > **Disk Quota**.

Disk Quota



2. (Optional) If the page displays **Currently in Disk Group Mode**, click **Switch to Quota Mode**, then follow the on-screen instructions to **format the disk.**
3. Select a channel and set the record duration, bit rate and picture storage capacity.
4. Click **Apply**.

Disk Calculator

This function can calculate how long you can record video according to the HDD capacity, and

calculate the required HDD capacity according to the record period.

Process

1. Select **Storage** > **Disk Calculator**.
2. Click , you can configure the **Resolution**, **Frame Rate**, **Bit Rate** and **Record Time** for the selected channel.
3. Click **Apply**. Then the system will calculate the time period that can be used for storage according to the channels settings and HDD capacity.

NOTE

Click **Copy to** copy the settings to other channels.

Estimate by Capacity

Process

1. On **Disk Calculator** page, click **Estimate by Capacity**.
2. Click **Select**.
3. Select the checkbox of the hard drive disk that you want to calculate, then click **Apply**.

Estimate by Time

Process

1. On the **Disk Calculator** page, click **Estimate by Time**.
2. Enter the time period you wish to record in the **Time** box. The required hard disk capacity will be displayed in the **Total Space** box.

Disk Detection

The system is capable of detecting the status of the hard disk drive (HDD) so that you can clearly understand the performance of the HDD and replace any faulty HDDs.

Manual Detection

Process

1. Go to **Storage** > **Disk Detection** > **Manual Detection**.

Manual detection

2. Select the detection type.
   - Key Area Detection: The system detects the used space of the hard drive through the built-in file system. This detection method is efficient.
   - Complete Detection: The system performs a window detection of the entire hard disk drive (HDD). This type of detection requires time and may affect the hard disk drive that is currently being recorded.
3. Select the hard drive that you want to detect.
4. Click **Start Checking**.

   The system begins to detect the hard drive and displays the detection information.

   NOTE

   When the system is detecting the hard drive, click **Stop Checking** to stop current detection. Click **Start Checking** to initiate the detection again.

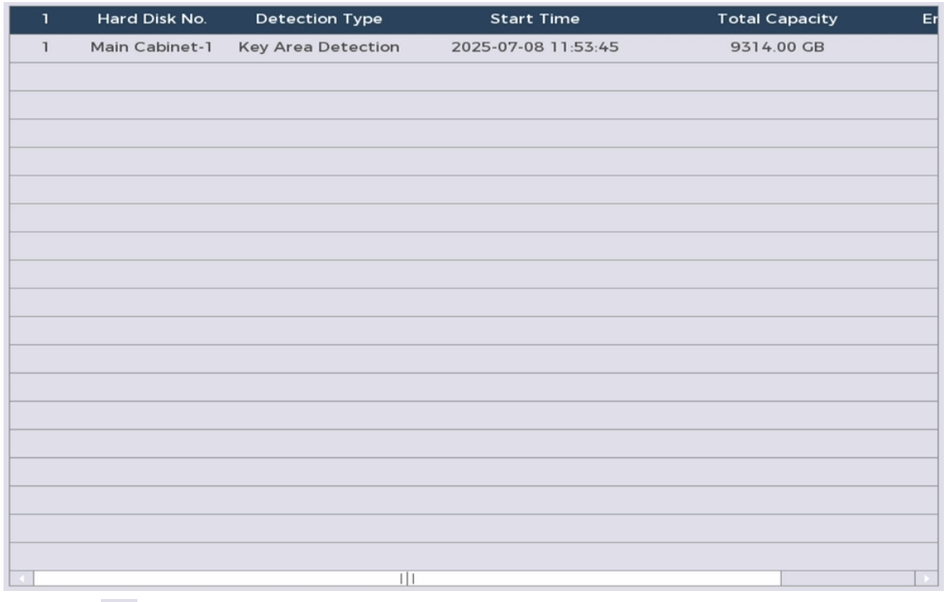
Detection Report

You can view the detection report after the detection,

Process

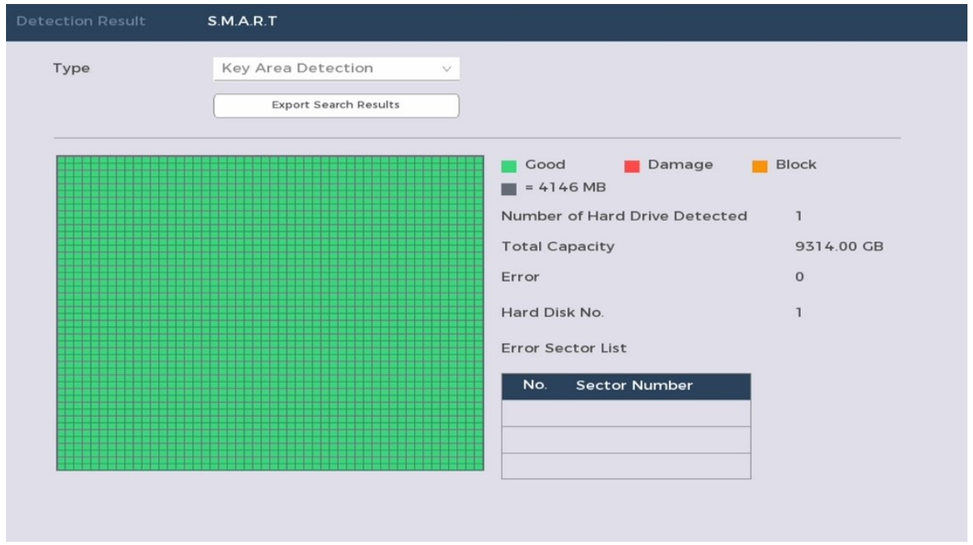
1. Go to **Storage** > **Disk Detection** > **Detection Report**.

Check report

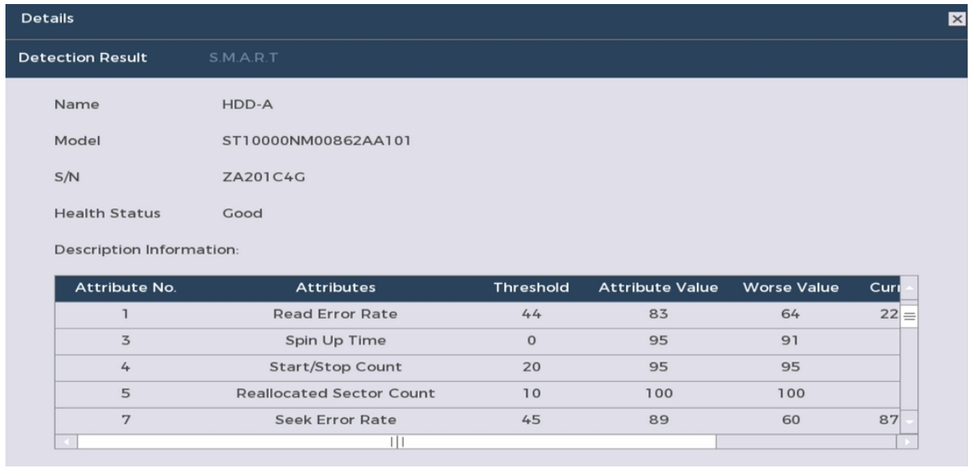


2. Click to view detection results and S.M.A.R.T report.

Results



S.M.A.R.T



RAID Management

RAID (Redundant Array of Independent Disks) is a data storage virtualization technology that combines multiple physical hard drive components into a single logical unit to achieve data redundancy, performance enhancement, or both.

NOTE

The RAID function is only available on certain models.

Disk quantity for different RAID types

RAID type	Required disk quantity
RAID 0	At least 2.
RAID 1	Only 2.
RAID 5	At least 3. We recommend using 4 disks to 6 disks.
RAID 6	At least 4.
RAID 10	

Create RAID

RAID has different levels, such as RAID 5 and RAID 6. Each level varies in terms of data protection, data availability, and performance. You can create different types of RAID

according to your needs.

Background Information

⚠ CAUTION

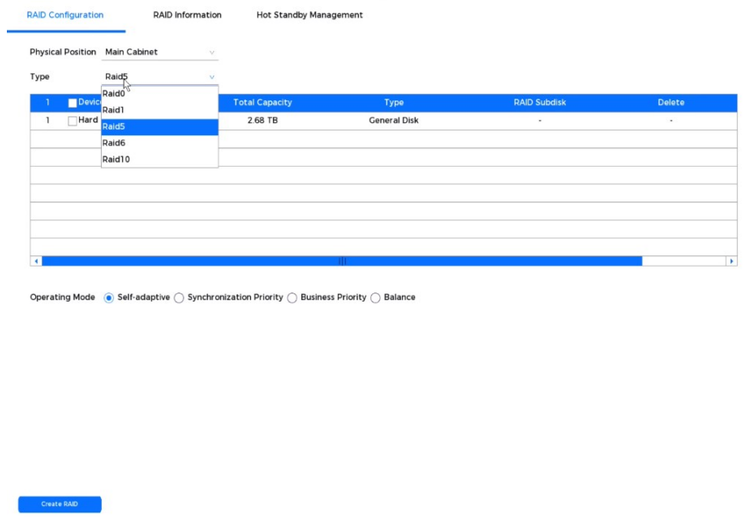
When creating a RAID, the disks in the RAID group will be formatted. Please back up your data in a timely manner.

Create different types of RAID as needed.

Process

1. Select **Storage** > **RAID Management** > **RAID Configuration**.

RAID management



2. Select RAID type and operating mode.

   The operating mode determines how the system allocate resources.

   - **Self-Adaptive**: Automatically adjusts RAID synchronization speed based on business status.
     - Perform high-speed synchronization when there is no business operation.
     - During business operations, perform low-speed synchronization.
   - **Sync First**: Resource priority is allocated to RAID synchronization.
   - **Business First**: Resources are prioritized for business operations.
   - **Balance**: Resources are evenly distributed for RAID synchronization and business operations.

3. Create RAID. Select disks, click **Create RAID**, then follow the on-screen instructions to create RAID.

Related Operations

- Change operating mode.

  Click ✎ to change the operating mode of the RAID group.
- Delete RAID.

  Click 🗑 to delete the RAID group.

  NOTE

  When you delete a RAID group, the disks in the RAID group will be formatted.

RAID Information

Select **Storage** > **RAID Management** > **RAID Information**. You can view the RAID information, including total capacity, type, status and more.

Hot Standby Management

Create a hot standby disk. When a disk of the RAID group malfunctions, the hot standby disk can replace the malfunctioning disk.

Process

1. Select **Storage** > **RAID Management** > **Hot Standby Management**.

Hot Standby

2. Click ✎ to modify it.
3. You can select **Private Hot Standby** or **Global Hot Standby**.
   - **Private Hot Standby**: Select the target disk, and the current disk will serve as the hot standby disk for the selected target disk.
   - **Global Hot Standby**: The current disk will serve as the hot standby disk of the entire RAID.
4. Click **OK**.

NOTE

Click 🗑 to delete a hot spare disk.

FTP

Store and view the recorded videos and snapshots on the FTP server.

Precondition

Purchase or download an FTP (File Transfer Protocol) server and install it on your personal computer.

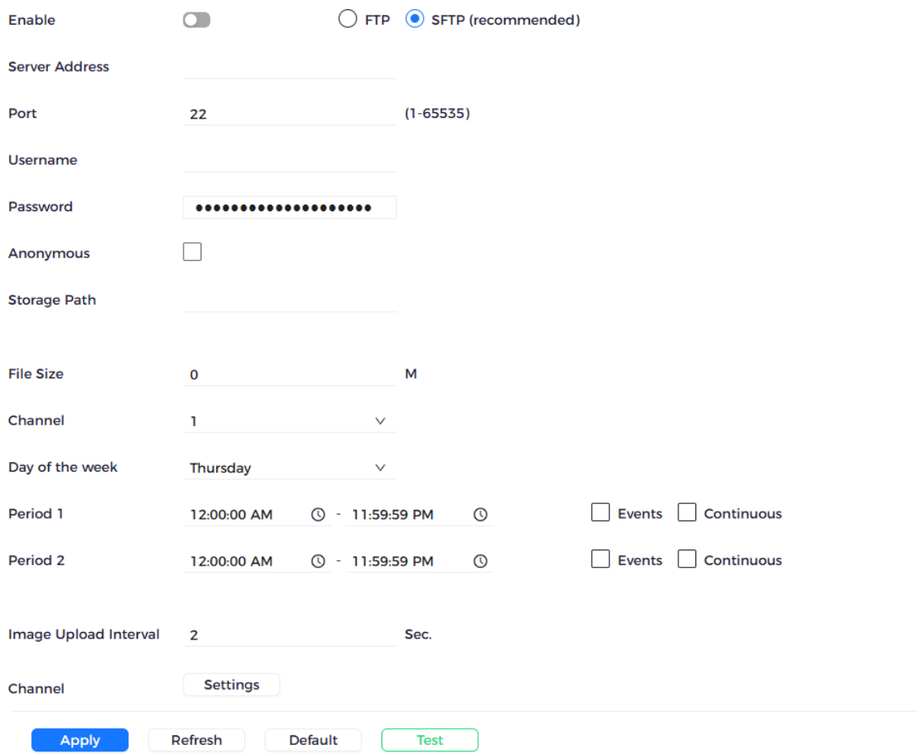
NOTE

For the created FTP user, you need to set write permissions; otherwise, the recorded videos and snapshots will not be able to upload.

Process

1. Go to **Storage** > **FTP**.

FTP



2. Configure the parameters.

FTP parameters

Parameter	Description
Enable	Enable the FTP upload function.
FTP type	Select FTP type. • FTP: Plaintext transmission. • SFTP: Encrypted transmission (recommended).
Server Address	IP address of FTP server.
Port	The port of the FTP server. • FTP: The default port is 21. • SFTP: The default port is 22.
Username	Enter the username and password to log in to the FTP server. f you enable the anonymous feature, you can log in anonymously without entering a username and password.
Password	
Anonymous	
Storage Path	Create a folder on FTP server. • If you do not enter the name of the remote directory, the system will automatically create a folder based on the IP and time. • If you enter the name of a remote directory, the system will first create a folder with the entered name in the FTP root directory, and then automatically create folders based on the IP and time.
File Size	Enter the length of the uploaded recorded video. • If the input length is shorter than the length of the recorded video, only a portion of the recorded video can be uploaded. • If the input length exceeds the length of the recorded video, the entire recorded video can be uploaded. • If the input length is 0, the entire recorded video will be uploaded.
Image Upload Interval	• If this interval exceeds the snapshot interval, the system will upload the most recent snapshot. For example, if the interval is 5 seconds and the snapshot interval for each snapshot is 2 seconds, the system will upload the most recent snapshot every 5 seconds. • If this interval is shorter than the snapshot interval, the system will upload snapshots according to the snapshot interval. For example, if the interval is 5 seconds and the snapshot interval for each snapshot is 10 seconds, the system will upload a snapshot every 10 seconds.

Parameter	Description
Channel	Select the channel to which you want to apply the FTP settings.
Day of the week	Select the day of the week and set the time slots during which you would like to upload the recorded files. You can set two time slots for each Sunday.
Period 1, Period 2	

3. Click **Test** to verify the FTP connection.
   If FTP connection failed, check the network and FTP settings.
4. Click **Apply**.

iSCSI

The Internet Small Computer Systems Interface (iSCSI) is a transport layer protocol that operates on top of the Transmission Control Protocol (TCP), enabling block-level SCSI data transfer between iSCSI initiators and storage targets over TCP/IP networks. After mapping network disks to NVR devices via iSCSI, data can be stored on the network disks.

Process

1. Go to **Storage** > **iSCSI**.

   NOTE

   This feature is only available on certain models.
2. Click **Add** to add the iSCSI server.

iSCSI parameter

Parameter	Description
Server Address	The server address of iSCSI server.
Port	The iSCSI server port, the default value is 3260.
Storage Path	Click **Storage Path** to select a remote storage path. Each path represents an iSCSI shared disk, and these paths are generated when created on the server.
Username, Password	The username and password of iSCSI server.

3. Click **Confirm**, then click **Apply**.

System

Configure the system settings, such as date, accounts, display output and more.

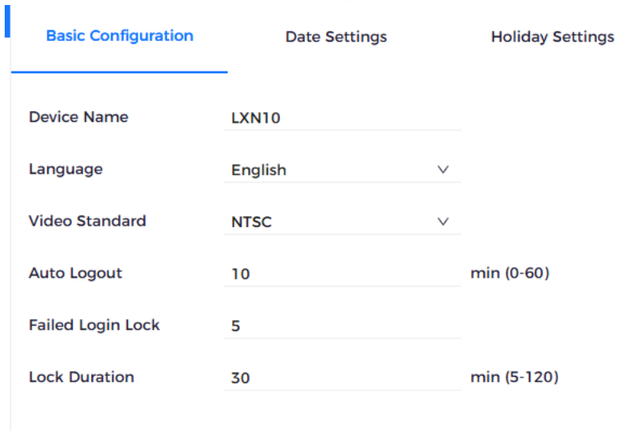
General System Settings

Basic Configuration

Process

1. Go to **System** > **General** > **Basic Configuration**.

Basic configuration



2. Configure the parameters.

Parameters of basic configuration

Parameter	Description
Device Name	Enter the device name.
Language	Displays the system language.
Video Standard	Select **PAL** or **NTSC** as needed.
Instant Playback	Configure the duration of instant playback. On the live page, click to play back recorded file from 5 to 60 minutes prior.
Auto Logout	Enter the inactive time before logout. The device will automatically log out after the inactive time has elapsed Click **Log out of View Settings** to select the channels you wish to continue monitoring after logging out.
Failed Login Lock	Configure the number of allowed failed login attempts before the account is locked for a period of time.
Duration	Configuration duration: If the number of failed login attempts reaches the defined threshold, the account will be locked for the defined duration.
Mouse Sensitivity	Adjust the double-click speed.

3. Click **Apply**.

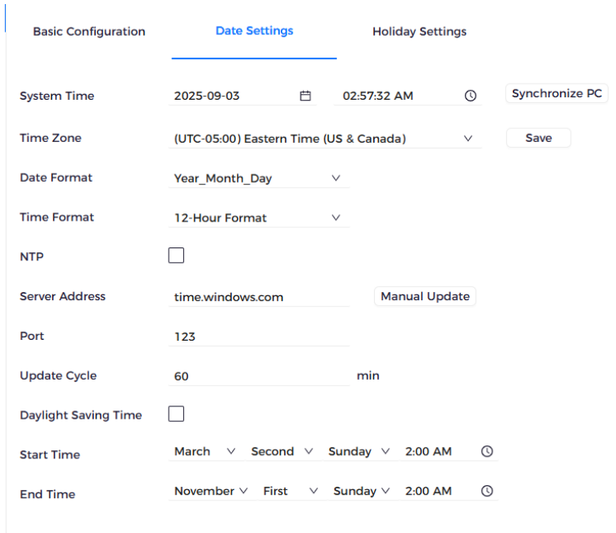
Date Settings

Configure date and time settings.

Process

1. Go to **System** > **General** > **Date Settings**.

Date settings



2. Configure the parameters.

Parameters of date and time

Parameter	Description
System Time	Enter the system time in the **System Time box**. By clicking on the time zone list, you can select a time zone for the system, and the time will be automatically adjusted. ⚠ CAUTION Please do not change the system time arbitrarily; otherwise, the recorded videos will be unsearchable. It is recommended to avoid recording during the system time change or to stop the recording first before making any changes.
Time Zone	Select a time zone, then click **Save**.
Date Format	Select a date format.
Time Format	Select **12-Hour Format** or **24-Hour Format**.
NTP	After enabling the NTP function, the system time will automatically synchronize with the NTP server. 1. Click to enable the function. 2. Configure the address and port of the NTP server. 3. Set the update cycle.
Daylight Saving Time	If your country or region observes daylight saving time, you can enable this feature to ensure the system time is accurate. 1. Click to enable the function. 2. Set the start time and end time.

3. Click **Apply**.

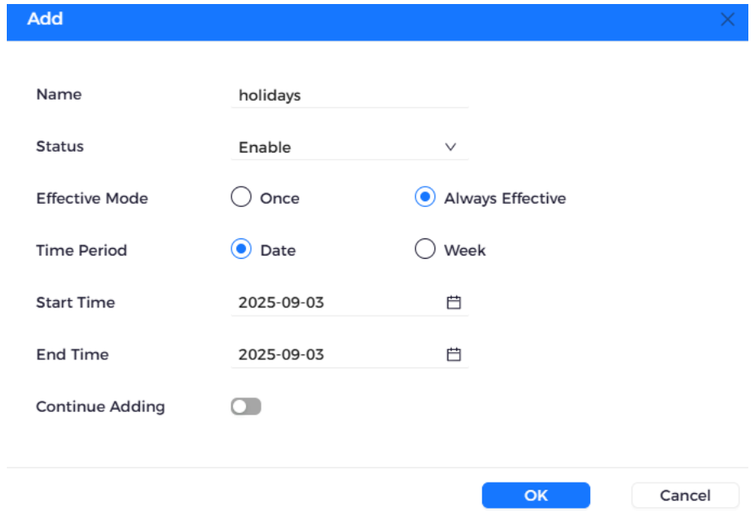
Holiday Settings

Add holidays and configure a separate recording schedule for them.

Process

1. Go to **System** > **General** > **Holiday Settings**, then click **Add**.

Add holidays



2. Configure the holiday name, effective mode, and time period.
3. (Optional) Enable **Continue** to add more holidays.
4. Click **OK** to add current holiday to the list.

Related Operations

- Click to change the holiday information.
- Click to delete current date.
- Go to **Storage** > **Recording Plan** to configure the recording plan for the holiday. For details, see "Recording Plan".

User Management

Add and manage users, ONVIF users, as well as set the information for password resets.

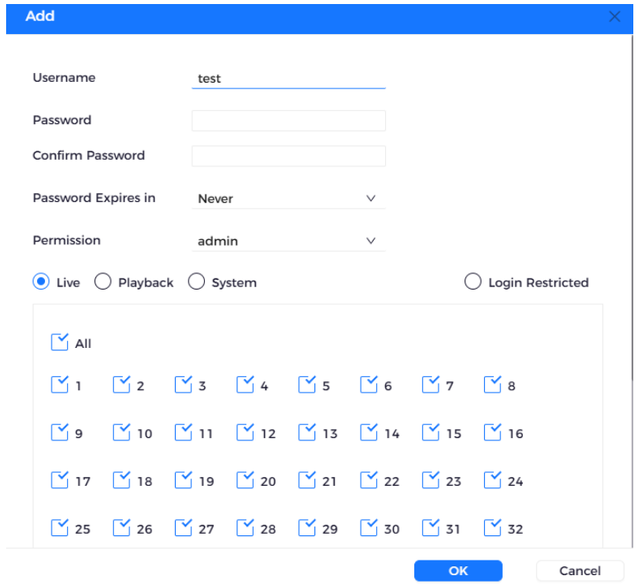
Adding Users

Users can access and manage devices. The default administrator for the device is admin, and it cannot be modified or deleted. You can add more users and grant permissions to users within the scope of the corresponding user group.

Process

1. Go to **System** > **User Management** > **User**.
2. Click **Add**.

Add user



3. Configure the parameters.

Parameters of adding user

Parameter	Description
Username	Enter the user's name.
Password	Enter the password, then re-enter the password to confirm.
Confirm Password	
Password Expires in	Select the password expiration time as needed; you can also customize the time.
Login Restricted	Select **Login Restricted** to set the time periods during which new users can log into the device. Users will not have access to the device during other time periods. NOTE You need enter the **User MAC** information.
Permission	Select a group for the user. NOTE The user's permissions must not exceed the permissions of the user group.

4. Select the checkbox under the **Live** tab, **Playback** tab, and **System** tab as needed.
5. Click **OK**.

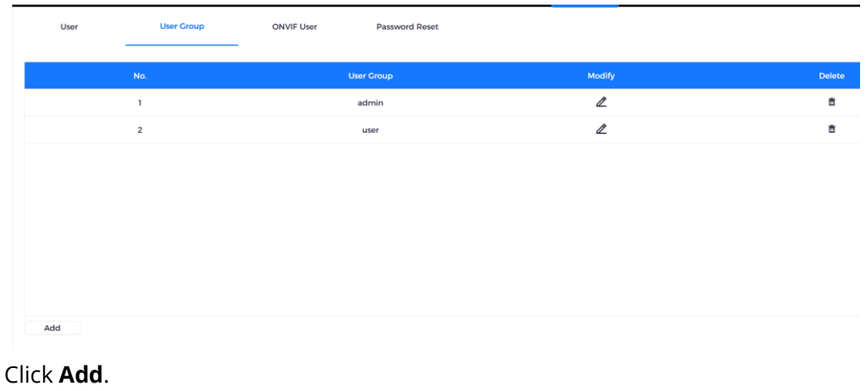
Adding User Groups

The account management of this device adopts a two-level management model: users and user groups. Each user must belong to a group, and a user can only belong to one group. The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

Process

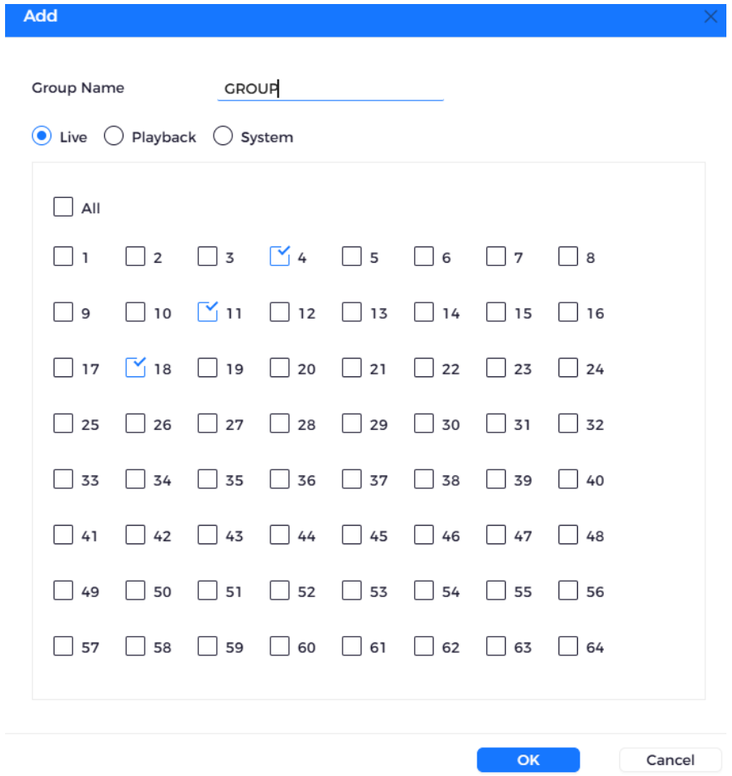
1. Go to **System** > **User Management** > **User Group**.

User group



2. Click **Add**.

Add user group



3. Enter the group name.
4. Select the checkbox under the **Live** tab, **Playback** tab, and **System** tab as needed.
5. Click **OK**.

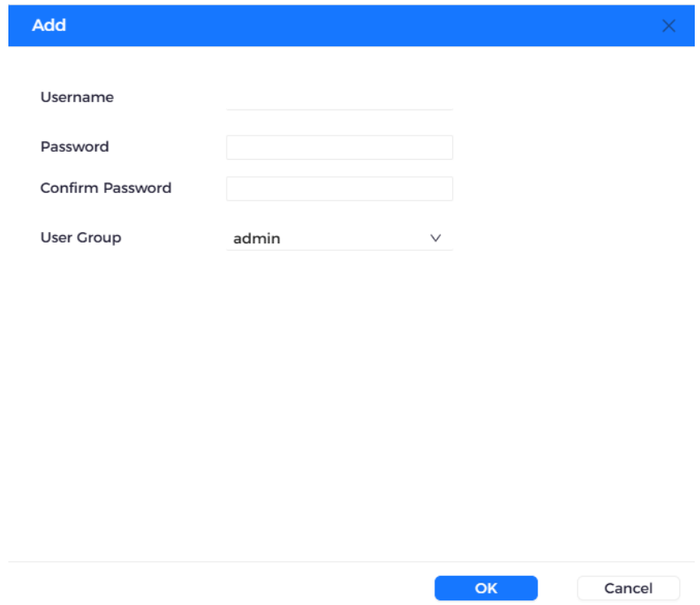
Adding ONVIF Users

Devices from other manufacturers can connect to this device using a verified ONVIF account through the ONVIF protocol.

Process

1. Go to **System** > **User Management** > **ONVIF User**.
2. Click **Add**.

Add ONVIF user



3. Configure username, password and user group.

NOTE

By default, there are three ONVIF user groups: Administrator, Operator, and User. You cannot manually add ONVIF user groups.

4. Click **OK**.

Resetting Password

If you have forgotten your password, you can reset it using your email address or by answering the security question.

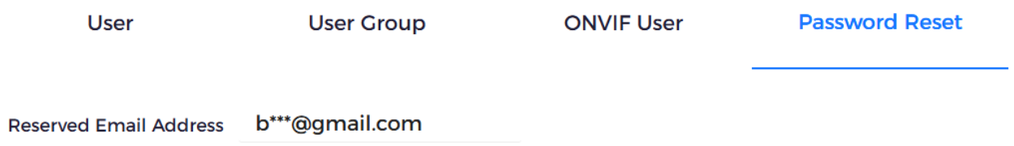
Configuring Password Reset

If you have forgotten your password, you can reset it using your email address or by answering the security question.

Process

1. Go to **System** > **User Management** > **Password Reset**.

Password reset



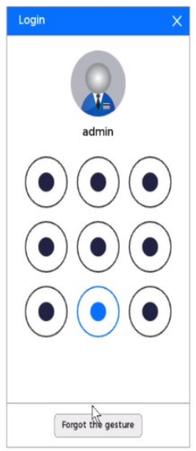
2. Enter an email address to receive the security code for resetting your password.
3. Click **Apply**.

Resetting Password on Local Interface

Process

1. After the device is powered on, click the live page.

Login



2. Click “forgot password”
   - If you have configured a linked email address, the system will notify you of the data collection required to reset your password.
   - If you have not yet configured the linked email address, the system will prompt you to enter an email address. Please enter the email address and then click **Next** Subsequently, the system will inform you of the data collection required to reset your password.
3. Read the prompt, then click **OK**.
4. Reset the password by **Mail Recovery**.
   Obtain the security code from the associated email address as instructed on the screen, and then enter the security code.

NOTE

- You can obtain the security code twice by scanning the same QR code. After that, you need to refresh the page and then scan the QR code again to obtain the security code.
- The security code sent to your email is valid for 24 hours. Please check your inbox in a timely manner.

5. Click **Next**.
6. Enter the new password, then re-enter the password to confirm.
7. Click **OK**.

Network Settings

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

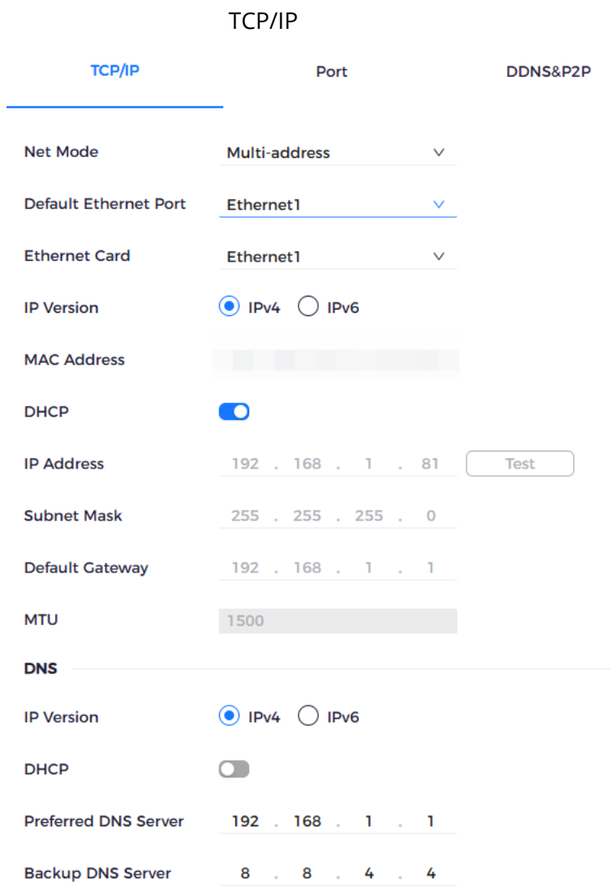
Basic Settings

TCP/IP

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

Process

1. Go to **System** > **Network** > **Basic** > **TCP/IP**.



2. Configure the TCP/IP.

TCP/IP parameters

Parameter	Description
Net Mode	• **Multi-address**: The current Ethernet card works independently. If the current Ethernet card is disconnected, the Device becomes offline. • **Fault Tolerance**: Two Ethernet cards share one IP address. Normally only one Ethernet card is working. When this card fails, the other Ethernet card will start working automatically to ensure the network connection. The Device is regarded as offline only when both Ethernet cards are disconnected. • **Load Balance**: Two Ethernet cards share one IP address and work at the same time to share the network load averagely. When one Ethernet card fails, the other card continues to work normally. The Device is regarded as offline only when both Ethernet cards are disconnected.
Default Ethernet Port	Select the default Ethernet port.
Ethernet Card	Select the Ethernet card. When the net mode is **Fault Tolerance** or **Load Balance**, only **Bond** can be selected. NOTE • Make sure that at least two Ethernet cards are installed. • Ethernet cards using different ports such as optical port and electrical port cannot be bound together. • After binding Ethernet cards, you need to restart the Device to make the change effective.
IP Version	Both IPv4 and IPv6 are supported.
DHCP	Enable the system to allocate a dynamic IP address to the Device. There is no need to manually set IP address.
IP Address	Enter the IP address and configure the subnet mask and default gateway. NOTE • The IP address and the default gateway must be on the same network segment. • Click **Test** to check if the IP address is available.
Subnet Mask	
Default Gateway	
MAC Address	Display device's MAC address.
MTU	Displays the MTU value of the network adapter.

3. Configure the DNS server information, including the IP version, as well as the IP addresses of the preferred DNS server and the alternate DNS server.
4. Click **Apply**.

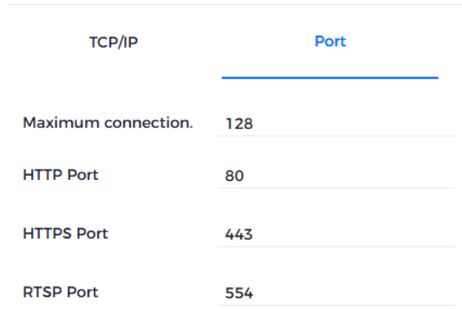
Port

You can configure the maximum number of connections to the device that can be accessed simultaneously through the web, platform, mobile, or other clients, and configure the settings for each port.

Process

1. Go to **System** > **Network** > **Basic** > **Port**.

Port



2. Configure the parameters.

Port parameters

Parameter	Description
Maximum connection	Set the maximum number of connections (1-128).
HTTP Port	The default value is set to 80. If you change the port number, for example, 90, then when logging into the device's web interface, you should enter 90 after the IP address.
HTTPS Port	HTTPS communication port. The default value is 443. You can enter this value according to the actual situation.
RTSP Port	The default value is set to 554. You can enter this value according to the actual situation.

3. Click **Apply**.

DDNS

After enabling Dynamic Domain Name System (DDNS), the system will dynamically update the relationship between the domain name and the IP address on the DNS server when the device's IP address changes frequently. You can remotely access the device using the domain name.

Precondition

Check the DDNS types supported by the device, and then log in to the website provided by the DDNS service provider to register the domain name and other information.

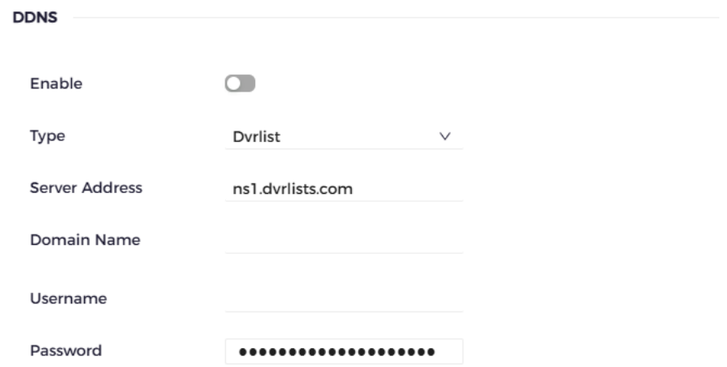
NOTE

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

Process

1. Go to **System** > **Network** > **Basic** > **DDNS&P2P**.

DDNS



2. Click to enable the function.
3. Configure the parameters.

DDNS parameters

Parameter	Description
Type	Displays the type and address of the DDNS service provider. • **Dvrlist**: the default address is nsl.dvrlists.com. • **NO-IP DDNS**: the default address is dynupdate.no-ip.com.
Server Address	
Domain Name	Enter the domain name you registered on the DDNS website.
Username	Enter the username and password from the DDNS service provider.
Password	
Update Cycle	Configure DSNS service update cycle.

4. Click **Apply**.
   If the configuration is successful, you can access the device's web interface using the domain name.

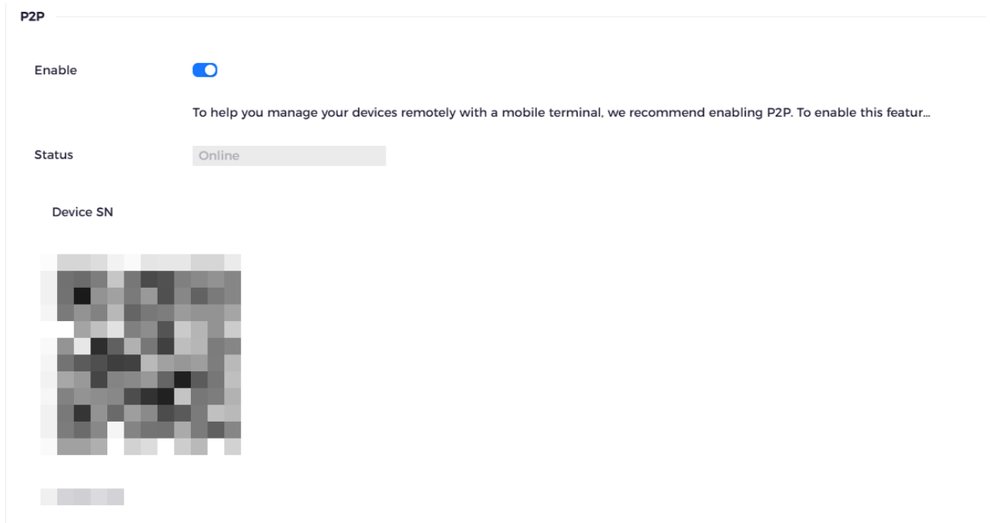
P2P

P2P is a peer-to-peer technology. After downloading the mobile application and registering the device with the application, you can remotely manage the device on your phone.

Process

1. Go to **System** > **Network** > **Basic** > **DDNS&P2P**.

P2P



2. Click to enable the function.
3. Click **Apply**.

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

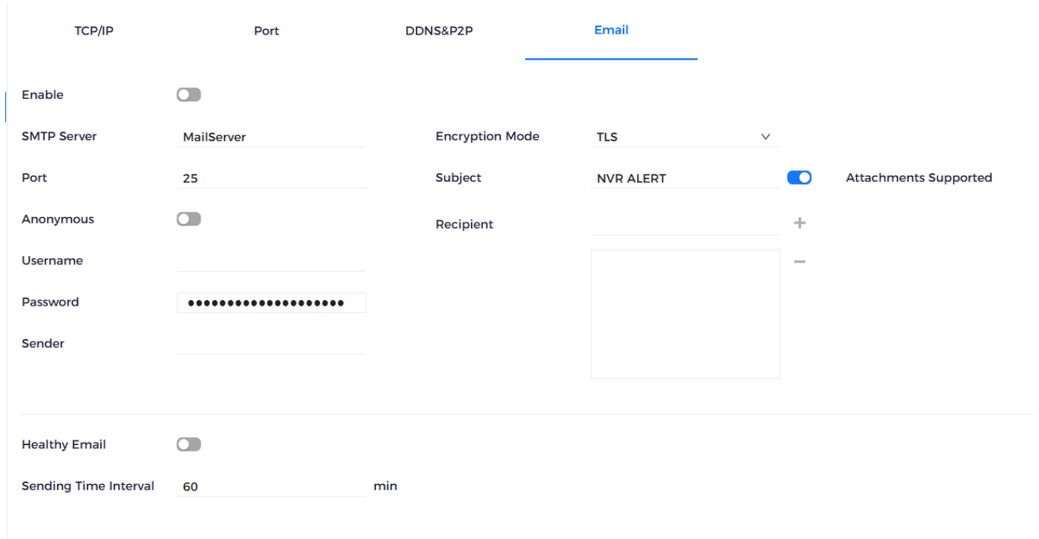
Email

Configure the email settings so that the system can send emails as notifications when an alert event occurs.

Process

1. Go to **System** > **Network** > **Basic** > **Email**.

Email



2. Click to enable the function.
3. Configure the parameters.

Email parameters

Parameter	Description
SMTP Server	The SMTP server address of the sender's email account.
Port	The port of SMTP server. The default value is 25.
Username	The username and password of sender's email account.
Password	
Anonymous	Enable anonymous login.
Recipient	Select the number of recipients to receive notifications. This device supports a maximum of three email recipients.
Email Name	Enter the email address of mail recipient.
Sender	Enter the sender's email address. You can enter up to three senders separated by commas.
Subject	Enter the email subject.
Attachments supported	After enabling the attachment feature, when an alarm event occurs, the system will attach a snapshot as an attachment to the email.
Encryption Mode	Select **None**, **SSL**, or **TLS**. NOTE For SMTP server, the default encryption type is **TLS**.

Parameter	Description
Healthy Mail	Enable the system to send a test email to check the connection.
Sending Time Interval	Set the interval time for the system to send health test emails.

4. Click **Apply**.
5. (Optional) Click **Test** to test the email sending. If configured correctly, the recipient will receive the email.

Advanced Settings

UPnP

You can map the relationship between the Local Area Network (LAN) and the Wide Area Network (WAN) to access devices on the LAN via the IP address on the WAN.

Configuring Router

Process

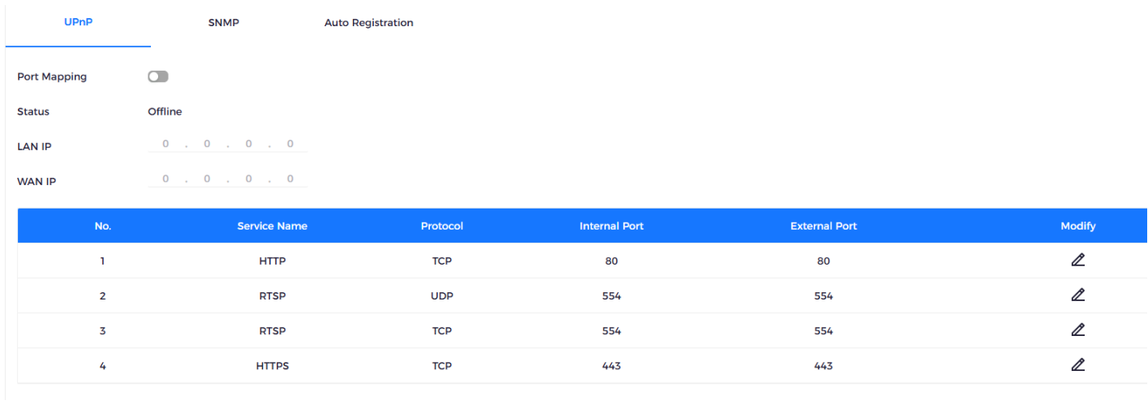
1. Log in to the router to set the WAN port, then enable the IP address to connect into the WAN.
2. Enable the UPnP function on the router.
3. Connect the Device with the LAN port on the router to access the LAN.
4. Go to **System** > **Network** > **TCP/IP**, configure the IP address within the router's IP address range, or enable the DHCP function to automatically obtain an IP address.

Configuring UPnP

Process

1. Go to **System** > **Network** > **Advanced** > **UPnP**.

UPnP



2. Configure the UPnP parameters.

UPnP parameters

Parameter	Description
Port Mapping	Enable the UPnP function.
Status	Shows the status of UPnP function. • Online: Succeeded. • Offline: Failed.
LAN IP	Enter router's IP address in the LAN. NOTE After the mapping is successful, the system will automatically obtain the IP address.
WAN IP	Enter router's IP address on the WAN. NOTE After the mapping is successful, the system will automatically obtain the IP address.

Parameter	Description
Port Mapping Table	The settings on port mapping table correspond to the UPnP port mapping list on the router. • Service Name: Network Server Name. • Protocol: Protocol type. • Internal Port: The internal port mapped on the device. • External Port: The external port mapped on the router. NOTE • To avoid the conflict, when setting the external port, try to use the ports from 1024 through 5000 and avoid popular ports from 1 through 255 and system ports from 256 through 1023. • When there are multiple devices in the local area network, it is important to arrange the port mapping relationships reasonably to avoid mapping to the same external port. • When establishing the mapping relationship, ensure that the mapping ports are not occupied or restricted. • The internal and external ports for TCP and UDP must be the same and cannot be modified. • Click to modify the external port.

3. Click **Apply** to complete the settings.
   Enter http://WAN IP: External IP port in the browser. You can access devices in the local area network.

SNMP

You can connect the device to some software, such as MIB Builder and MG-SOFT MIB Browser, in order to manage and control the device through the software.

Precondition

- Install software capable of managing and controlling SNMP, such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the MIB file corresponding to the current version from technical support.

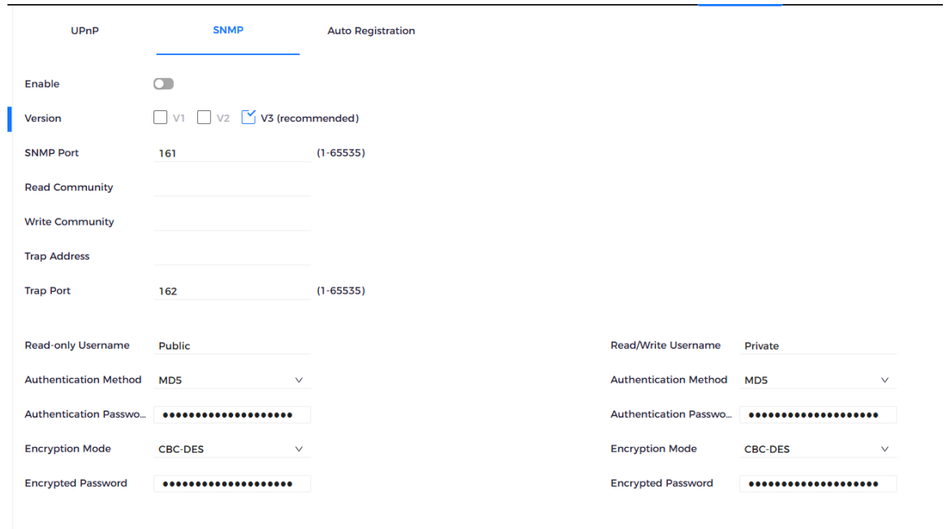
NOTE

This feature is only available on certain models.

Process

1. Go to **System** > **Network** > **Advanced** > **SNMP**.

SNMP



2. Click to enable the function.
3. Configure the parameters.

SNMP parameters

Parameter	Description
Version	Select the checkbox for the SNMP version. NOTE The default version is **V3**. There are risks associated with using V1 or V2.
SNMP Port	Enter the monitoring port on the agent program.
Read Community	Enter agent program supports read and write strings..
Write Community	
Trap Address	Enter the target address for the agent program to send the Trap information.
Trap Port	Enter the target port for the agent program to send the Trap information.
Read-Only Username	Enter the username that allows access to the device with read-only permissions.
Read/Write Username	Enter the username that is allowed to access the device and has read and write permissions.
Authentication Type	Select MD5 or SHA. The system will automatically identify the type.

Parameter	Description
Authentication Password	Enter the password for authentication. The password must be at least eight characters long.
Encryption Mode	Select an encryption type. The default setting is CBC-DES.
Encrypted Password	Enter the encryption password.

4. Click **Apply**.
5. Compile the two MIB files using the MIB Builder.
6. Run the MG-SOFT MIB Browser to load the compiled module.
7. On the MG-SOFT MIB Browser, enter the IP address of the device you wish to manage, and then select the version number you want to query.
8. On the MG-SOFT MIB Browser, unfold the tree-structured directory to obtain the configurations of the Device, such as the number of channels and software version.

Auto Registration

Register the Device with a designated proxy server, which acts as an intermediary for client software to access the device.

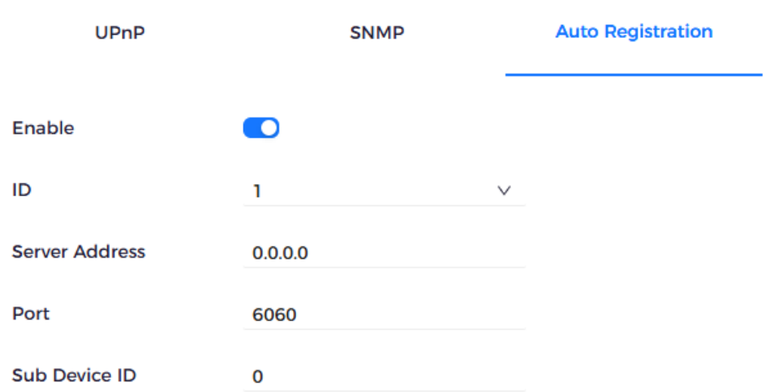
Precondition

- The Device, the proxy server and the device running the client software are located on the same network.
- The proxy server has been deployed.

Process

1. Go to **Main Menu** > **Network** > **Auto Register**.

Auto Registration



2. Click to enable the function.
3. Configure the parameters.

Auto registration parameters

Function	Description
Server Address	The IP address or domain name of the server that you wish to register.
Port	Enter the server port.
Sub Device ID	Enter the ID allocated by the server.

4. Click **Apply**.

Cluster IP

When the main device fails, the sub-device can correspondingly take over the operation (monitoring or recording) using the configuration and virtual IP address of the main device. When accessing the device via the virtual IP, real-time video can still be viewed, and there is no risk of losing recorded data.

Process

1. Go to **System** > **Network** > **Advanced** > **Cluster IP**.
2. Enable cluster IP.
3. Enter the IP address, subnet mask, and default gateway.
4. Click **Apply**.

Security Settings

Configure the basic services, HTTPS function, and firewall for the Device.

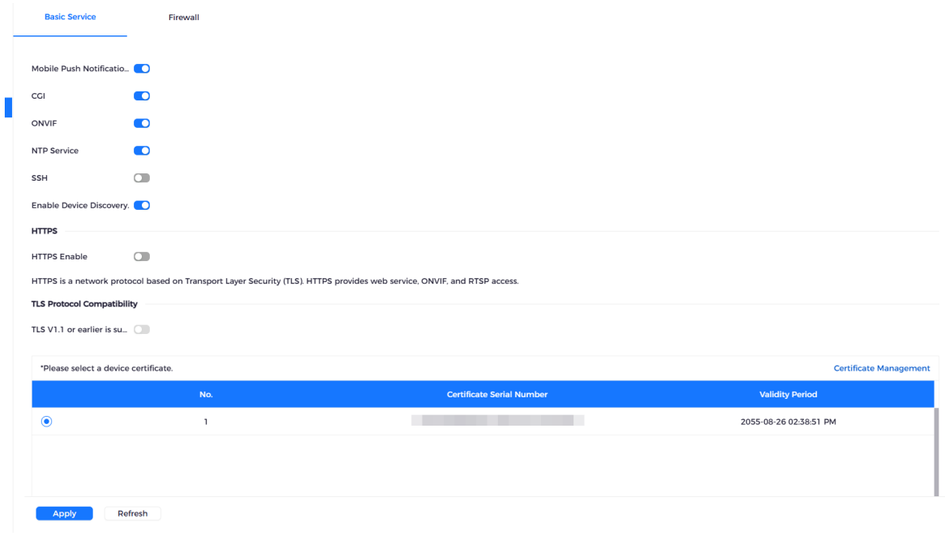
Basic Services

Enable basic services such as mobile push notifications, ONVIF, NTP, and SSH. HTTPS helps protect user information, ensuring device security and data safety. We recommend enabling this feature.

Process

1. Configure basic services.
   1) Go to **System** > **Network** > **Security** > **Basic Service**.

Basic service



2) Click to enable the system services.

Basic system services

Parameter	Description
Mobile Push Notification	You can receive alarm information from the Device on the mobile client after enabling this feature, NOTE To reduce security risks, please disable this feature when it is not needed.
CGI	If this feature is enabled, remote devices can be added via the CGI protocol. This feature is enabled by default.
ONVIF	After the function is enabled, remote devices can connect to this device via the ONVIF protocol. NOTE To reduce security risks, please disable this feature when it is not needed.
NTP Service	After enabling this function, you can use the NTP server for time synchronization.
SSH	After enabling this feature, you can access the device via the SSH protocol for system debugging and IP configuration. NOTE To reduce security risks, please disable this feature when it is not needed.
Enable Device Discovery	Enable the device to be discoverable by other devices through search.

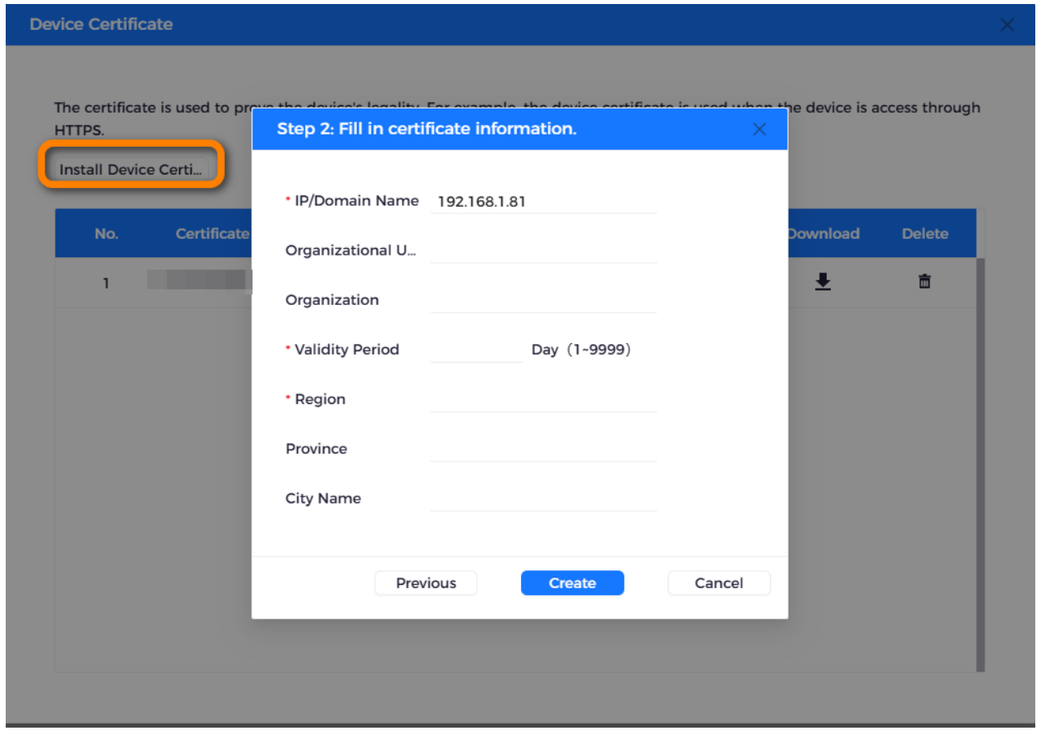
3) Click to enable the HTTPS function.
4) Click to enable compatibility with the TLS protocol.

NOTE

Transport Layer Security (TLS) provides privacy and data integrity between two communication applications.

5) Click **Certificate Management** to create an HTTPS certificate.
   a. Click **Install Device Certificate**.
   b. Configure the related parameters.
   c. Click **Create**.

Create certificate



2. Click **Apply**.

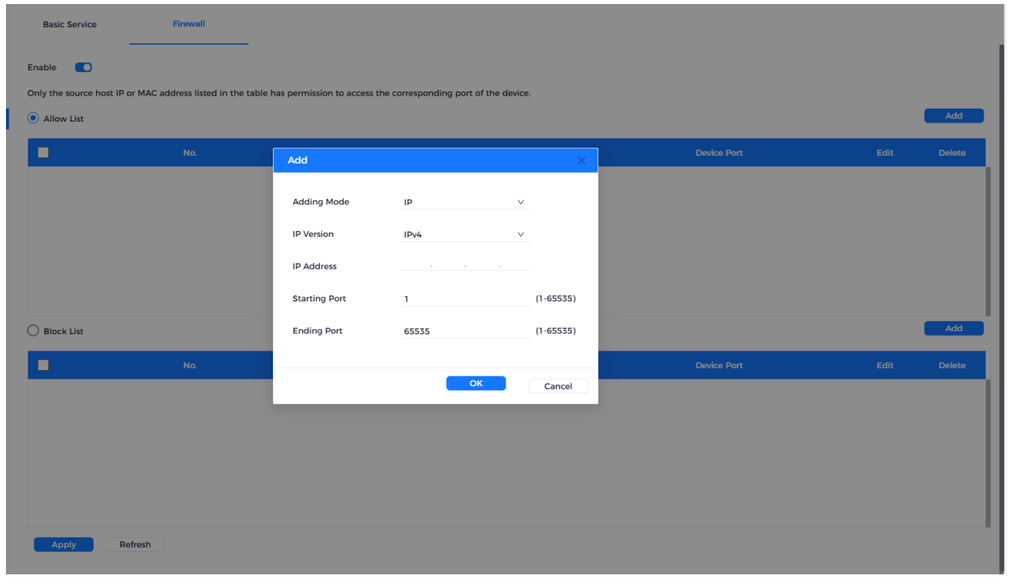
Firewall

You can configure to allow or prohibit access to the device's host.

Process

1. Go to **System** > **Network** > **Security** > **Firewall**.

Firewall



2. Click  to enable the firewall.
3. Select a firewall mode.
   - Allow list: Hosts on the allowlist can access the device.
   - Block list: Hosts on the blacklist are prohibited from accessing the device.
4. Click **Add**, then select a type for the allowlist or blocklist.
   You can allow or deny access to the device for specific IP addresses, IP addresses on specific network segments, or specific MAC addresses.
   - IP address.
     Enter the IP address, starting port and ending port, then click **OK**.
   - IP segment.
     Enter the start address and end address, starting port and ending port, then click **OK**.
   - MAC address.
     Enter the MAC address, and then click **OK**.
5. Click **Apply**.

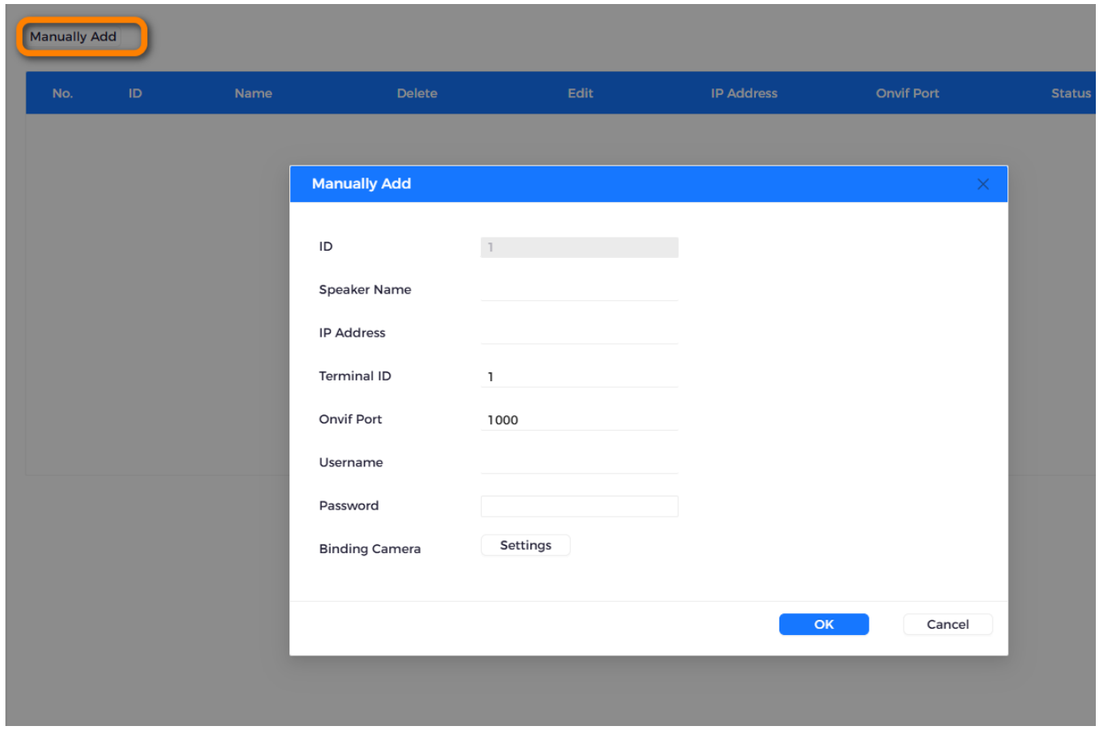
IP Speaker Settings

Add IP speakers and bind the speakers to the camera.

Process

1. Go to **System** > **Network** > **IP Speaker**.

IP Speaker



2. Click **Manually Add** to add IP speaker.
3. Enter the IP speaker information.
4. Click **Settings** to bind the IP speaker with a camera.
5. Click **Apply**.

Related Operations

- Click to edit IP speaker information.
- Click to delete IP speaker.

Alarm Settings

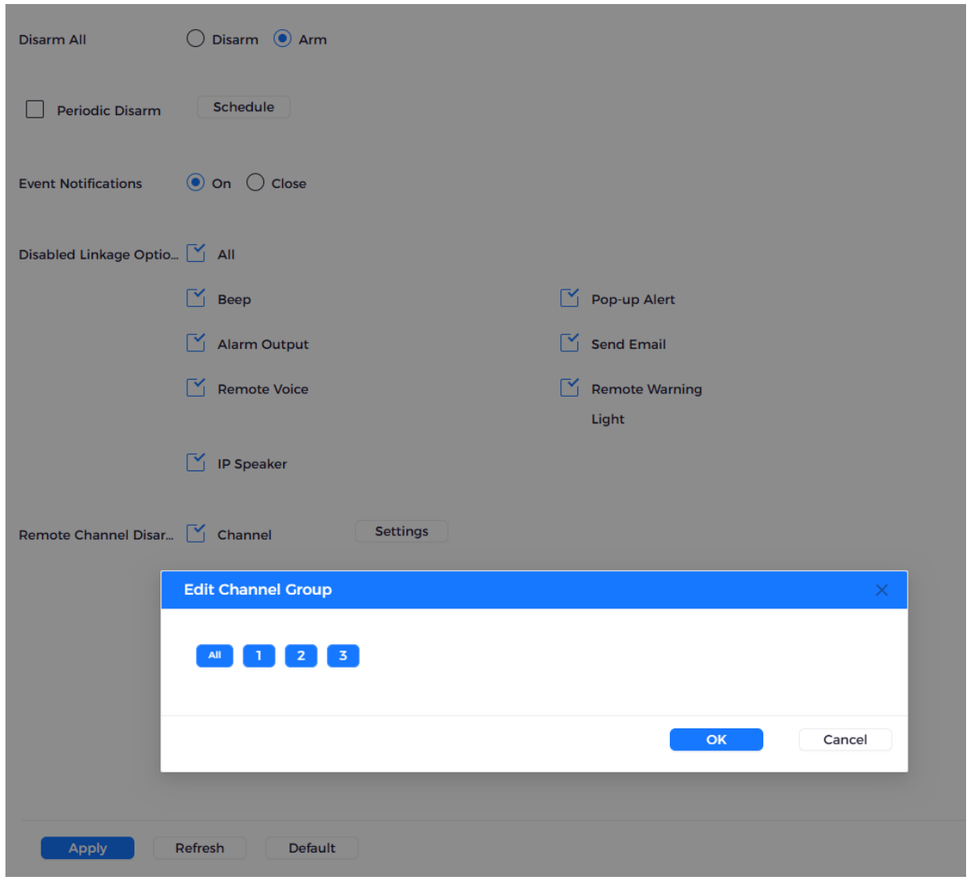
Disarming All

You can disarm all alarm linkage actions with a single click.

Process

1. Go to **System** > **Alarm** > **Disarm All**.

Disarm all



2. Enable disarm all or periodic disarm.
   - Disarm all: Select **Arm** to enable the function.
     The alert will take effect at any time.
   - Periodic disarm: Select **Disarm** for **Disarm All**, then click **Schedule** to set the disarm period.
     The alarm will take effect at a specific time.

     NOTE

     Periodic disarm can only be used when **Disarm All** is turned off.
3. Enable **Event Notifications** as needed.
   You can select **On** or **Close**.
4. Select the alarm linkage actions.

Alarm linkage actions

Parameters	Description
Beep	The device emits a beep when an alarm occurs.

Parameters	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, then select alarm output port as needed. NOTE Ensure that the alarm status of the alarm output port is configured. For more details, refer to "10.4.2.2 Alarm Output".
Remote Voice	Click **Setting** next to **Remote Voice** to configure the remote voice.
IP Speaker	Enable IP Speaker alarm.
Pop-up Alert	Enable screen prompts for detected motion.
Send Email	Enable the system to send an email to notify you of an alarm event. NOTE • This feature is only available on certain models. • Ensure that the email function has been configured in **System** > **Network** > **Basic** > **Email**.
Remote Warning Light	Click **Setting** next to **Remote Warning Light** to configure the remote voice.

5. To disarm remote channels, select the checkbox at **Channel**, then click **Settings** to select channels.

   NOTE

   This function is only effective when the connected camera supports one-click disarming.

6. Click **Apply**.

Alarm

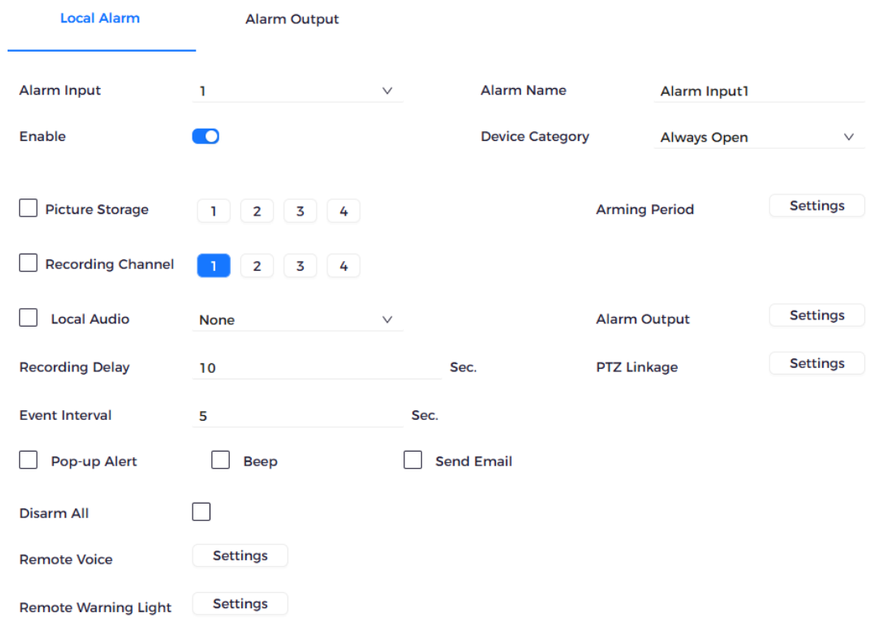
Local Alarms

After connecting the alarm device to the NVR alarm input port, when an alarm signal is sent to the NVR from the alarm input port, the system will execute the alarm linkage operation.

Process

1. Go to **System** > **Alarm** > **Alarm Settings** > **Local Alarm**.

Local Alarm



2. Select an alarm input and set the alarm name.
3. Click to enable the alarm.
4. Select the device category from **Always Closed** and **Always Open**.
5. Configure the arming period and alarm linkage information. For more details, refer to Alarm setting .
6. Click **Apply**.

Alarm Output

Set proper alarm output mode to automatic, manual or close. After connecting the alarm device to the alarm output port of the NVR and setting the mode to automatic, the system will perform alarm linkage operations when an alarm occurs.

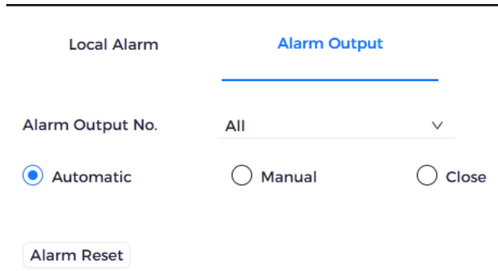
Background Information

- Automatic: The system generates an alarm once an alarm event occurs, .
- Manual: The alarm device is always in the alarming mode.
- Close: Close the alarm output function.

Process

1. Go to **System** > **Alarm** > **Alarm Settings** > **Alarm Output**.
2. Select the alarm mode.

Alarm output



3. Click **Apply**.
   - View the alarm output status on the live page.
   - Click **Alarm Reset** to clear all alarm output statuses.

Exception

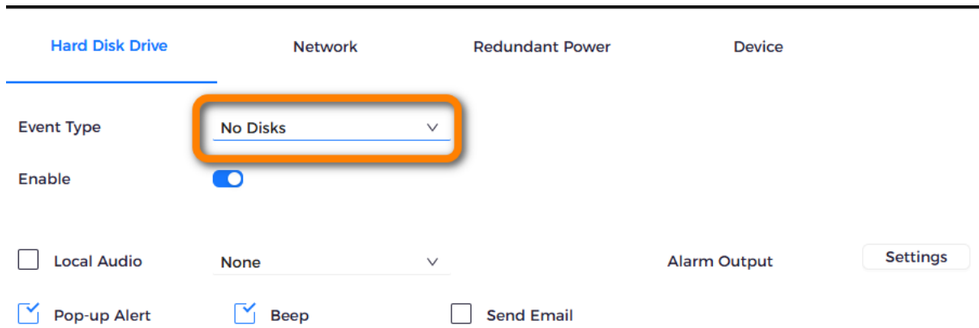
Configuring Storage Error Alarms

An alarm will be triggered when a storage error occurs.

Process

1. Go to **System** > **Alarm** > **Exception** > **Hard Disk Drive**.

HDD alarm



2. Select an event type from **No disks**, **Hard Disk Error** and **Insufficient storage capacity**.
3. Click to enable the alarm.
4. Configure other parameters.

Alarm settings

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, and then select alarm output port as need. NOTE Ensure that the alarm status of the alarm output port is configured. For more details, refer to "Alarm Output".
Beep	Select the checkbox to enable the device to beep when an alarm occurs.
Pop-up Alert	Enable screen prompts of an alarm events.
Alarm Delay	When alarm delay is configured, the alarm will continue for an extended period after it ends.
Send Email	Enable the system to send emails to notify you of alarm events. NOTE • This feature is only available on certain models. • Ensure that the email function is configured in **Main Menu** > **Network Settings** > **Email**.
Local Audio	Enable the local audio function. You can select a local audio as alarm sound. NOTE Ensure you have uploaded local audio files. For more details, refer to "Uploading Audio File".

5. Click **Apply**.

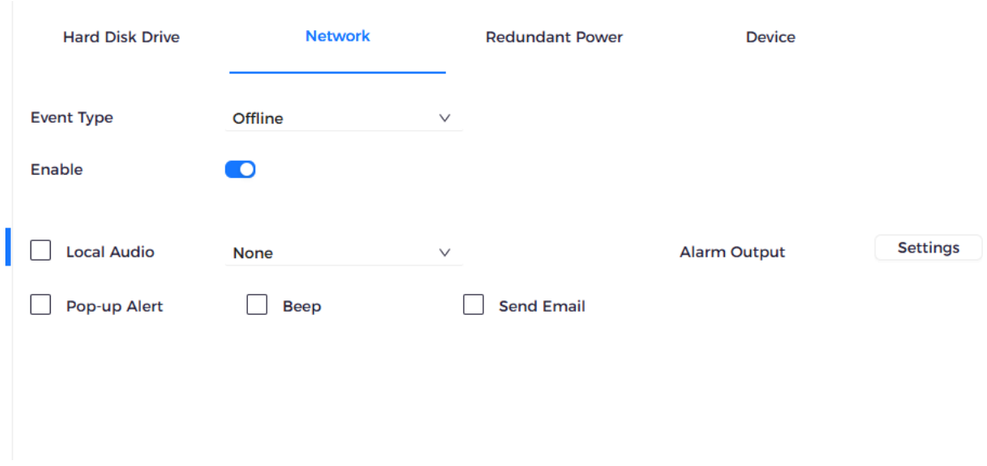
Configuring Network Error Alarms

An alert will be triggered when a network error occurs.

Process

1. Go to **System** > **Alarm** > **Exception** > **Network**.

Network alarm



2. Select an event type from **Offline**, **IP Conflict** and **MAC conflict**.
3. Click to enable the alarm.
4. Configure other parameters.

Alarm settings

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, then select alarm output port as needed. NOTE Ensure that the alarm status of the alarm output port has been configured. For more details, refer to "Alarm Output".
Beep	Check the box to enable the device to beep when an alarm occurs.
Pop-up Alert	Enable screen prompt of alarm events.
Alarm Delay	When an alarm delay is configured, the alarm will persist for a longer period after it has ended.
Send Email	Enable the system to send emails to notify you of alarm events. NOTE • This feature is only available on certain models. • Ensure that the email function has been configured in **Main Menu** > **Network Settings** > **Email**.
Local Audio	Enable the local audio function. You can select a local audio as alarm sound. NOTE Ensure you have uploaded local audio files. For more details, refer to "Uploading Audio File".

5. Click **Apply**.

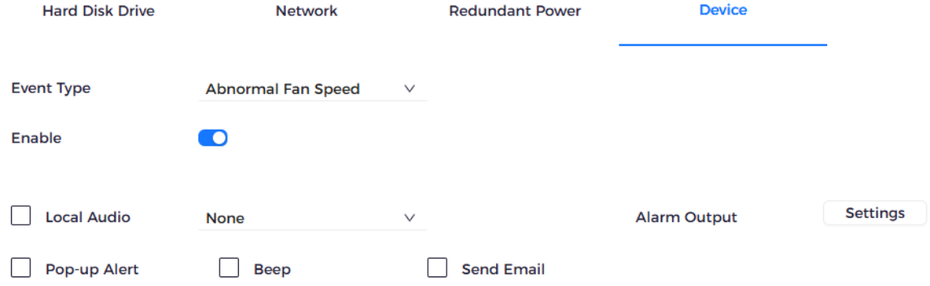
Configuring Device Error Alarms

An alarm will be triggered when the device encounters an error.

Process

1. Go to **System** > **Events** > **Exception** > **Device**.

Device alarm



2. Select an event type from **Event Type**.
3. Click to enable the alarm.
4. Configure other parameters.

Alarm settings

Parameter	Description
Alarm Output	Click **Settings** next to **Alarm Output**, click to enable the local alarm, then select alarm output port as needed. NOTE Ensure that the alarm status of the alarm output port has been configured. For more details, refer to " Configuring Alarm Output".

Parameter	Description
Beep	Select the checkbox to enable the device to beep when an alarm occurs.
Pop-up Alert	Enable screen prompt of alarm events.
Alarm Delay	When an alarm delay is configured, the alarm will continue for an extended period after it ends.
Send Email	Enable the system to send emails to notify you of alarm events. NOTE • This feature is only available on certain models. • Ensure that the email function has been configured in **Main Menu** > **Network Settings** > **Email**.
Local Audio	Enable the local audio function. You can select a local audio as alarm sound. NOTE Ensure you have uploaded local audio files. For more details, refer to " Uploading Audio File".

5. Click **Apply**.

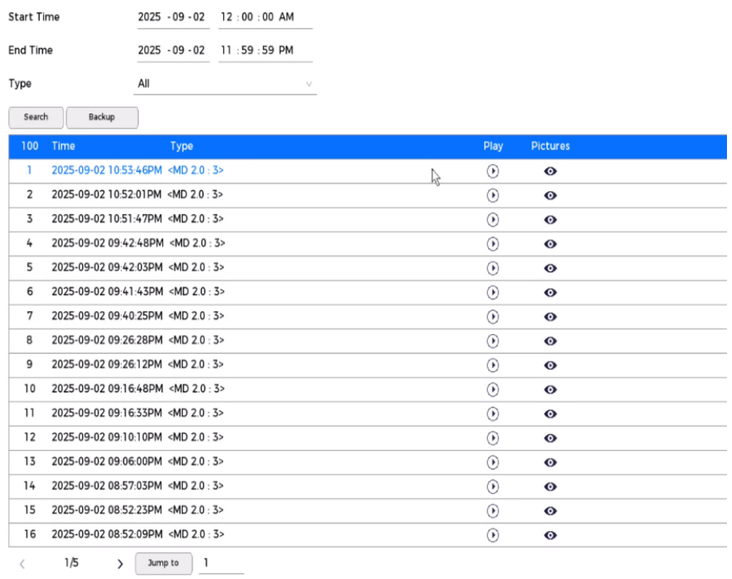
Event Search

Search, view and back up alarm information.

Process

1. Go to **System** > **Alarm** > **Event Search**.
2. Set the time period, then select an event type.
3. Click **Search**.

Search results



Related Operations

- View details.
  Select a record, then double-click it to view the details.
- Back up.
  Click **Backup** to save the alarm information to a USB storage device.
- Play recorded video.
  Click to play the recorded video of the alarm event.
- view the snapshot.
  Click to view the event snapshot.

Alarm Status

Go to **System** > **Alarm** > **Event Search** to view alarm status.

Alarm status

Alarm Type	Alarm Status
Motion Detection	2 3
Network Disconnection Event	Offline 2

Display Settings

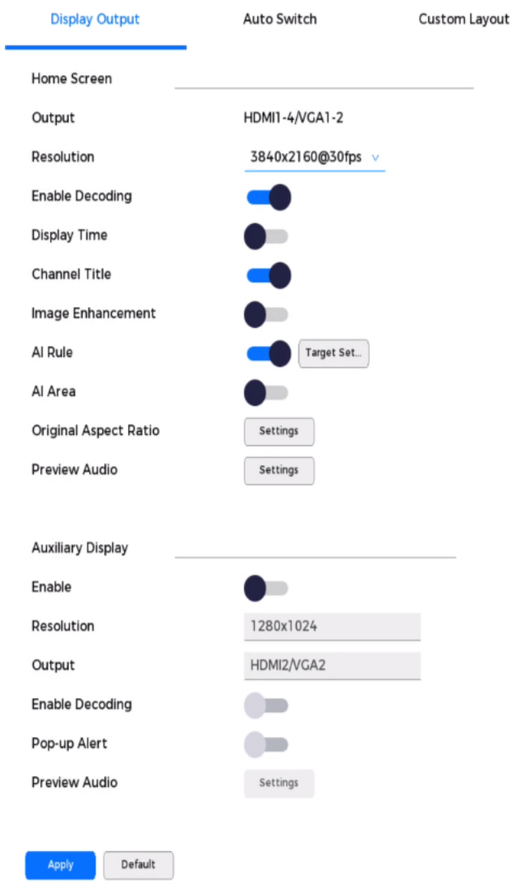
Display Output

Configure whether to display time title and channel, adjust image transparency, set the resolution.

Process

1. Go to **System** > **Display** > **Display Output**.

Display output



2. Configure the display parameters.

Display parameters

Parameter	Description
Resolution	Select a resolution for the video. The default setting is 1280 × 1024.
Enable Decoding	Enable the decoding.
Display Time	Displays time information in every live channel window.
Channel Title	Displays channel name, channel number and recording status in every live channel window.
Image Enhancement	After enabling this feature, the system will optimize real-time images.
AI Area	Enable AI area display.
AI Rule	Displays smart rule in every live channel window.
Original Aspect Ratio	Click **Settings**, select one or more channels to restore the channel image to its original aspect ratio.
Preview Audio	Click **Settings**, then click to enable the preview audio. Configure audio input in the real-time view. You can adjust the volume and audio sensing input. For example, when you select **Audio Mixing Output**, the sound from all audio input ports will be played

3. Configure the auxiliary screen.
   1. Click to enable the function.
   2. Configure display parameters.
4. Click **Apply**.

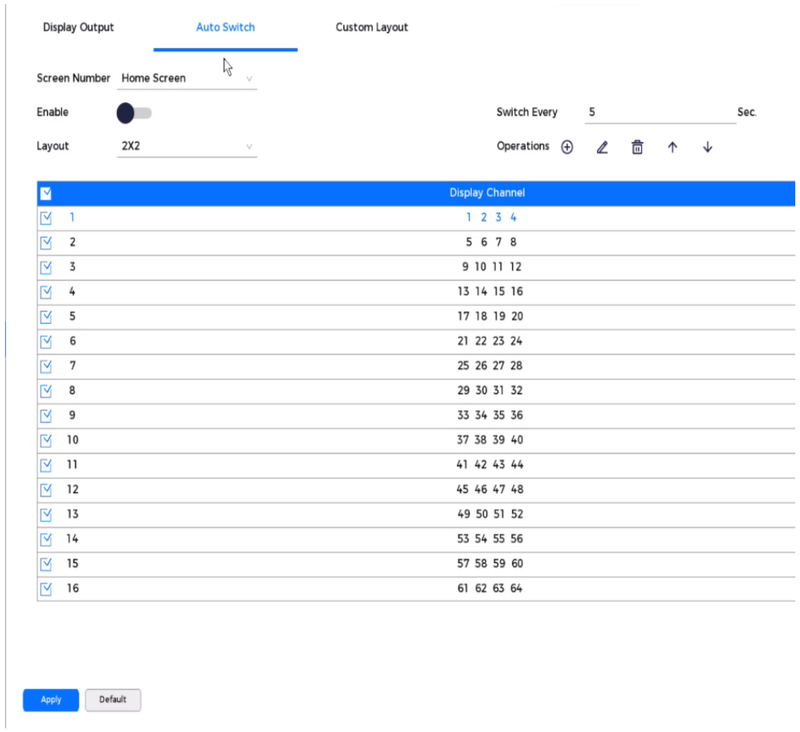
Auto Switch

You can configure the looping playback of the selected channel to repeat the video. The videos will be displayed sequentially according to the channel groups configured in the looping settings. The system will display one channel group for a certain period of time and then automatically switch to the next channel group.

Process

1. Go to **System** > **Display** > **Auto Switch**.
2. In **Screen Number**, select **Home Screen** or **Auxiliary Screen**.
3. Click to enable the function.

Auto Switch



4. Configure the parameters.

Tour parameters

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

5. Click **Apply**.

Related Operations

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

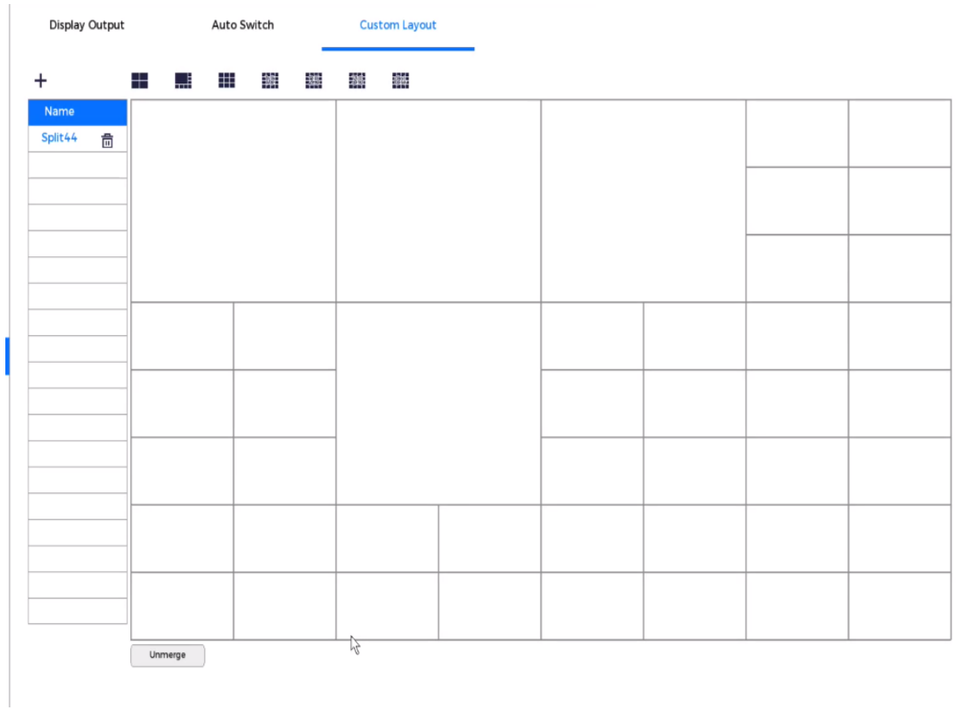
Custom Layout

You can set custom layout and using in **Live View**.

Process

1. Go to **System** > **Display** > **Custom Layout**.

Custom Layout



2. Click to add a layout.
3. Click the layout icons to select layout type, you can select from Split4, Split8, Split9, Split16, Split25, Split36 and Split 64.
4. Click **Apply**.

Related Operations

Right-click on **Live view** page, select **Custom Layout**, then you can select the layout type which you already set in this section.

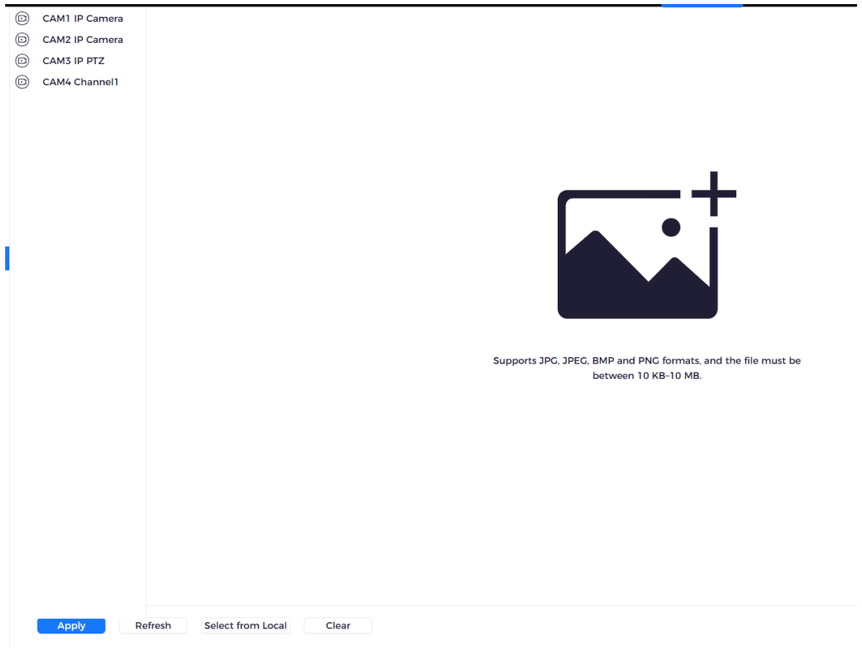
X Search Map Settings

You can view the target's trajectory through the map with the X Search function. A clear map should be uploaded and you are required to drag devices to corresponding locations.

Process

1. Go to **System > X Search Map.**

Map



2. Click **Select from Local** to upload the map.
3. Select devices on the left list to drag them to the map location.
4. Click **Apply**.

Audio Settings

The function is to manage audio files and set up scheduled playback.

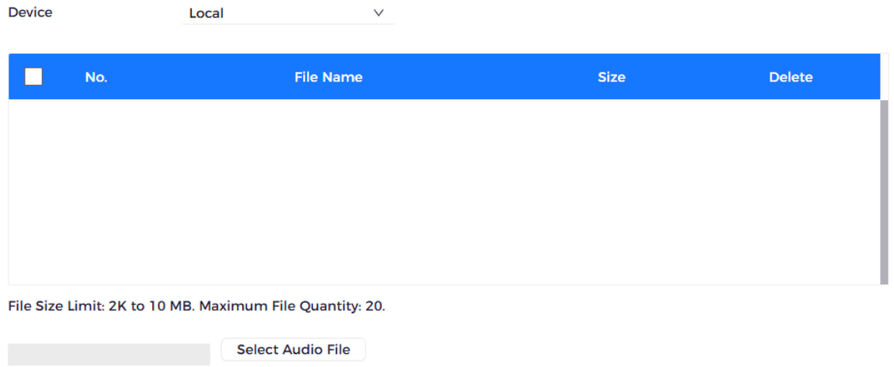
Uploading Audio File

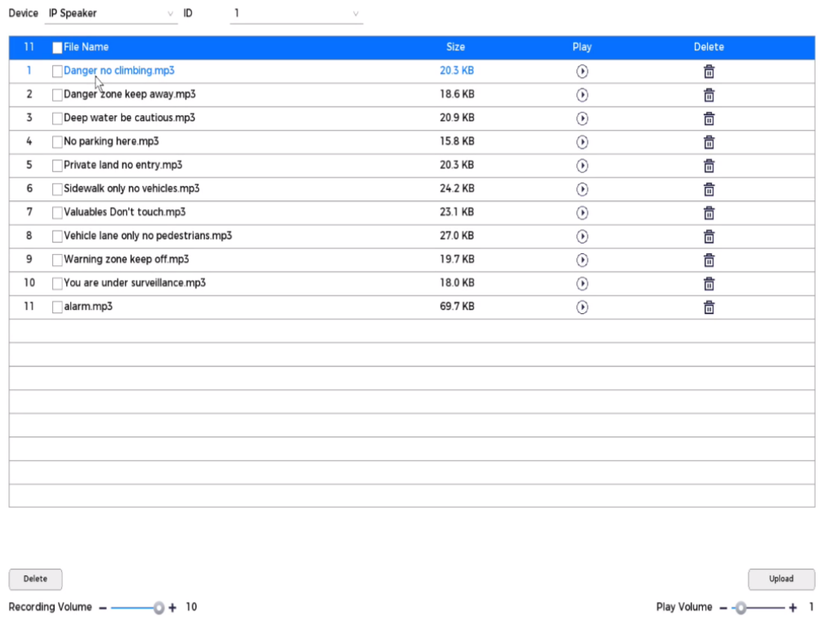
Add, rename, delete audio files and configure the audio volume.

Process

1. Go to **System** > **Audio** > **Audio File**.

Audio File





2. Click **Upload**.
3. Select an audio file from local storage, and then click **Import**.
   MP3 and PCM audio format are supported.
4. Click **OK** to start importing audio files from the USB storage device.
   If the import is successful, the audio files will display in current page.

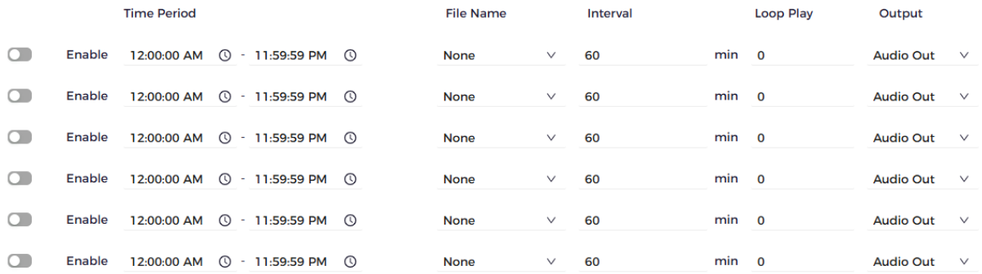
Audio Play

Configure the settings to play audio files within a defined time period.

Process

1. Go to **System** > **Audio** > **Audio Play**.

Audio Play



2. Configure the parameters.

Schedule parameters

Parameter	Description
Period	Enter the time in the **Period** box. Check the box to enable the settings. You can configure up to six time periods.
File Name	In the **File Name** list, enter the time you wish to repeat playback (in minutes).
Interval	In the **Interval** box, enter the time in minutes for how often you want to repeat the playing.
Loop	Configure the number of times you wish to repeat playback within the defined time period.
Output	Includes two options: MIC and Audio. The default is MIC. The MIC function shares the same port with talkback function, which takes precedence. NOTE Some series products do not have audio port.

NOTE

The completion time of audio playback depends on the size of the audio file and the configured interval.

3. Click **Apply**.

To Speak

System can broadcast to the IP speaker.

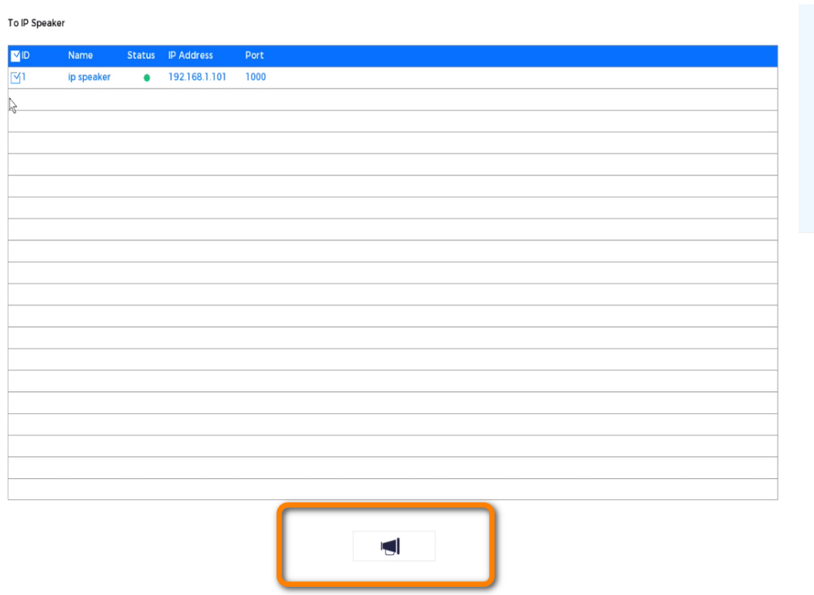
Precondition

You must have added at least one IP speaker to use this function. For how to add an IP speaker, see "IP Speaker Settings" for more details.

Process

1. Go to **System** > **Audio** > **To Speak**.

To IP speaker



2. Select an IP speaker, then click to broadcast to the IP speaker.

System Maintain

System Update

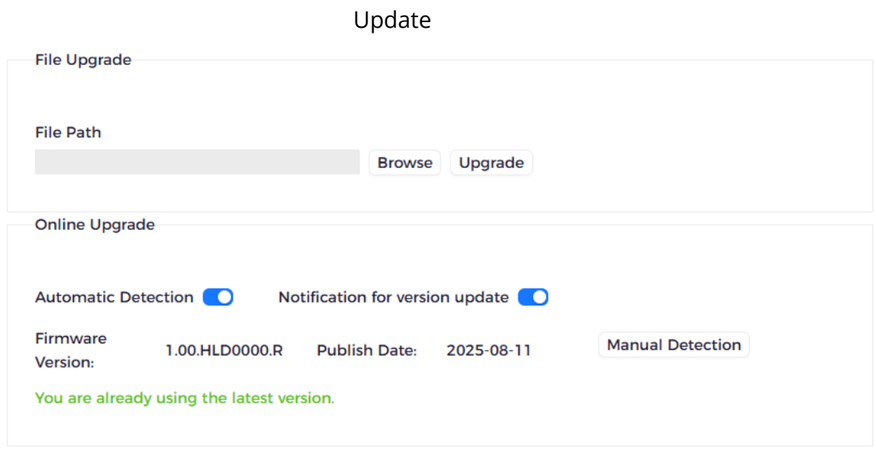
Upgrade the system through file update and online update.

File Update

Process

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

2. Go to **System** > **System Maintain** > **Upgrade**.



3. Click **Upgrade**.
4. Select the update file.
5. Click **OK**.

Online Update

Once the device is connected to the network, you can update the system online.

Process

1. Go to **System** > **Maintain** > **Upgrade**.
2. Check for available updates.
   - Automatic detection: Click to enable automatic detection.
   - Manual detection: Click **Manual Detection** to immediately check the version.

   If the system prompts **You are already using the latest version**, there is no need to update. If the system indicates that a new version is available, please proceed to the next step.
3. Click **Upgrade now**.

Restoring Defaults

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

Restoring Defaults on the Local Interface

Restore the device to its default settings on the local interface.

Process

1. Go to **System** > **System Maintain** > **Default**.
2. Restore the settings.
   - **Restore**: Restore all configurations to default settings, excluding network settings and user management.
   - **Default**: Restore all the configurations to factory default settings.

Resetting Device through the Reset Button

Background Information

Use the reset button on the mainboard to restore the Device to factory default.

NOTE

This button is only available on certain models.

Process

1. Turn off the device power, and then remove the cover.
2. Press and hold the reset button for 5 seconds to 10 seconds.

   NOTE

   The location of the reset button may vary by model.
3. Restart the Device.

   After the restart, the settings will be restored to factory default values.

Export and Import System Configurations

Export the device's configuration file for backup purposes. When the device fails, you can import the backed-up configuration file for recovery.

NOTE

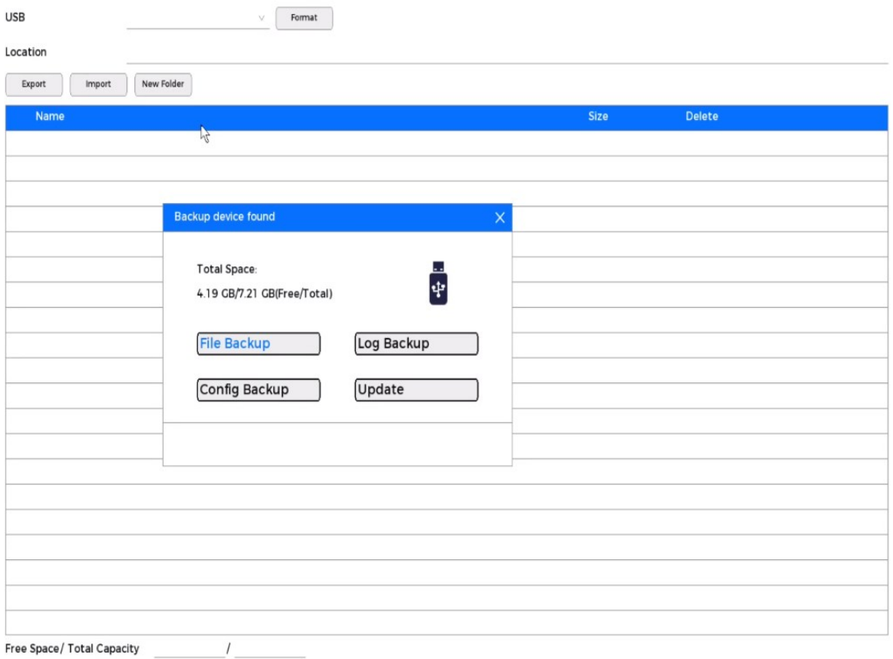
You cannot import or export system configuration while other pages are undergoing the backup process.

Export

Process

1. Go to **System** > **System Maintain** > **Import/Export**.

Configuration maintenance



2. Connect the USB storage device to the Device.
3. Click **Export**.
   The configuration has been exported to a folder.
   Double-click the folder to view the backup files.

Import

Process

1. Connect a USB storage device with the configuration files to the Device.
2. Go to **System** > **System Maintain** > **Import/Export**.
3. Select the configuration folder (under a name of "Config_XX").
4. Click **Import**.
   The device will restart after importing the configuration.

CAUTION

The imported configurations will overwrite the original configurations.

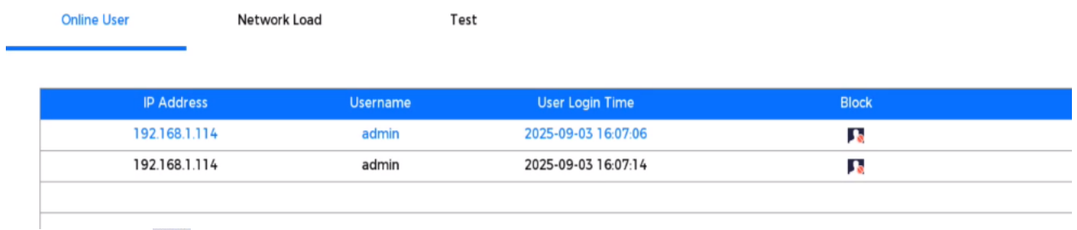
Viewing Network Information

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

Online User

Go to **System** > **System Maintain** > **Network** > **Online User**, then you can view the online users information.

Figure 10-41 Online user



You can click to prevent the user from logging into the device.

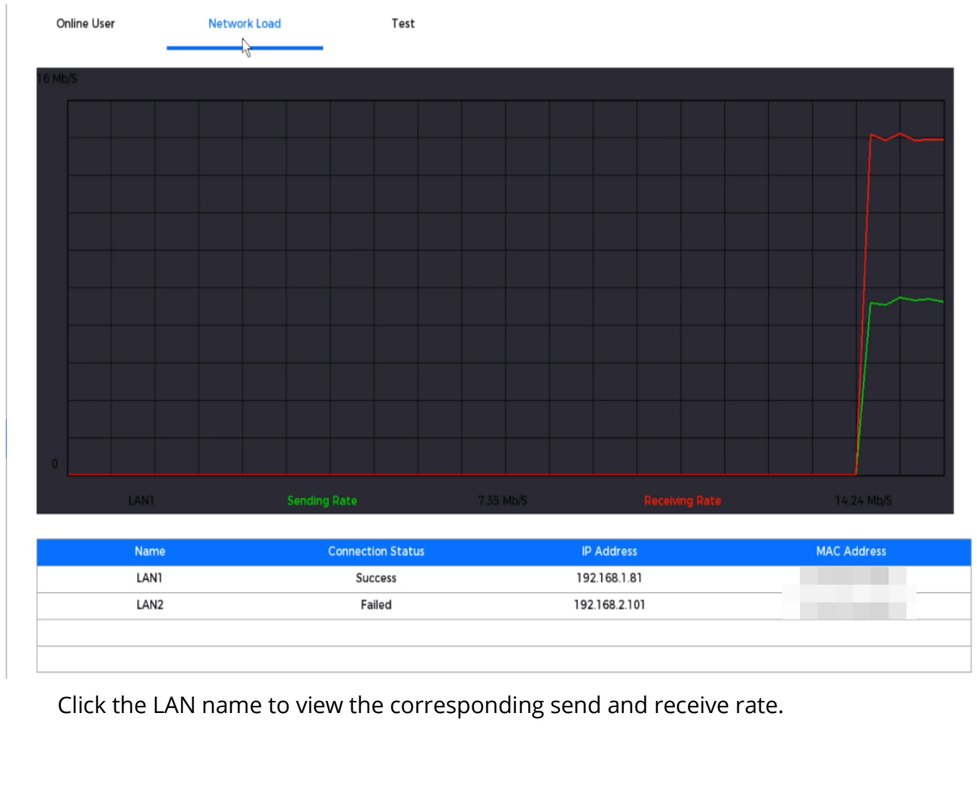
Network Load

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

Process

1. Go to **System** > **System Maintain** > **Network** > **Network Load**.

Network load



Name	Connection Status	IP Address	MAC Address
LAN1	Success	192.168.1.81	
LAN2	Failed	192.168.2.101	

2. Click the LAN name to view the corresponding send and receive rate.

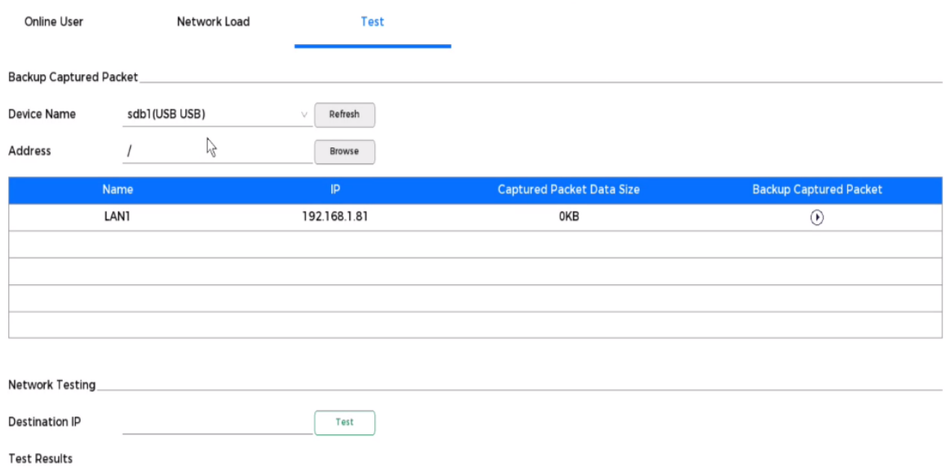
Test

You can test the network connection between the device and other devices, and capture packets when there are network anomalies with the device. The captured packets can assist technical support in diagnosing and resolving network issues.

Process

1. Go to **System** > **System Maintain** > **Network** > **Test**.

Test



2. Capture the packets.
   1) Connect a USB storage device to the Device.
   2) Click **Refresh**.
      After the Device detects the connected USB device, the name of the USB device will appear in the **Device Name** box.
   3) Click **Browse** to select the storage path.
   4) Click ⏵ to start packet capture and backup. Click it again to stop.

      NOTE

      - You cannot capture packets from multiple network adapters simultaneously.
      - During the packet capture, you can navigate to other pages to perform operations and return to the test page later to stop the packet capture
3. Enter the destination IP address, then click **Test**.

   NOTE

   You can view the load of one network adapter at a time.
   After the test is completed, review the test results for average latency, packet loss rate, and network status.

Auto Reboot

When the device has been running for an extended period, you can enable automatic restart of the device during idle times.

Process

1. Go to **System** > **System Maintain** > **Auto Reboot**.

2. Select a time for automatic restart.
3. Click **Apply**.

System Info

View device information and search for log information.

Viewing System Information

Go to **System** > **System Info** > **Device Info** to view the version information, disk information, stream information, and more.

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

Searching for Logs

Background Information

You can search for and view logs.

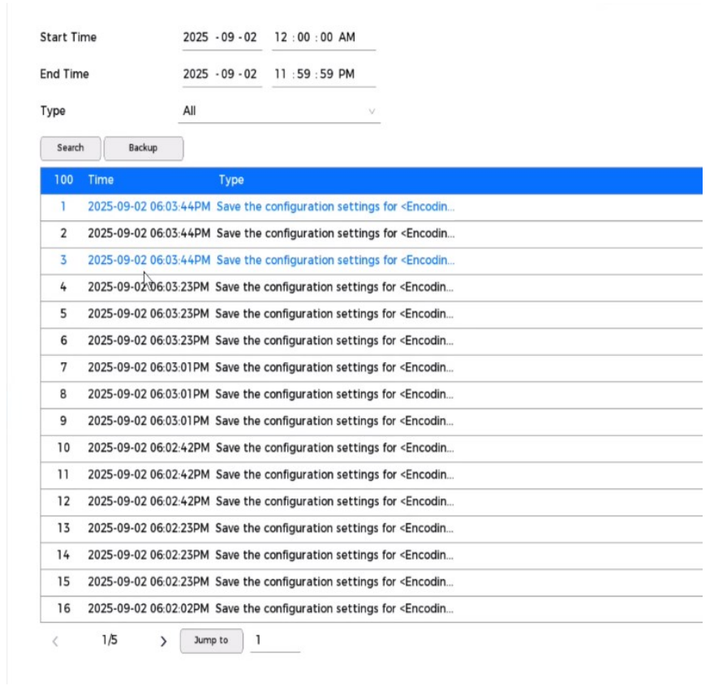
NOTE

- If a hard disk drive (HDD) is installed, the system operation logs will be stored in the device's memory, while other types of logs will be saved to the hard disk drive. If no hard disk drive is installed, other types of logs will also be stored in the device's memory.
- If you format the hard drive, the logs will not be lost. However, if you remove the hard drive from the device, the logs may be lost.

Process

1. Go to **System** > **System Info** > **Log Info**.
2. Set the search time period.
3. Select the log type.
4. Click **Search**.
   Search results have been displayed.

Search results



Related Operations

- View details.
  Select a log, then double-click a log to view details. Click **Previous** or **Next** to view details of other logs.
- Back up.
  Click **Backup** to save the logs to a USB storage device.

Web Operations

Logging in to the Web

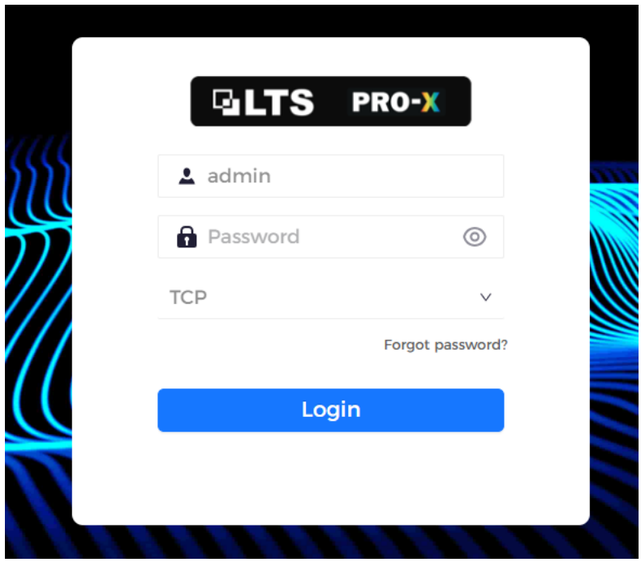
Precondition

Ensure that the IP addresses of your computer and devices are on the same network segment.

Process

1. Enter the device's IP address in the browser's address bar, and then press the Enter key.

Login

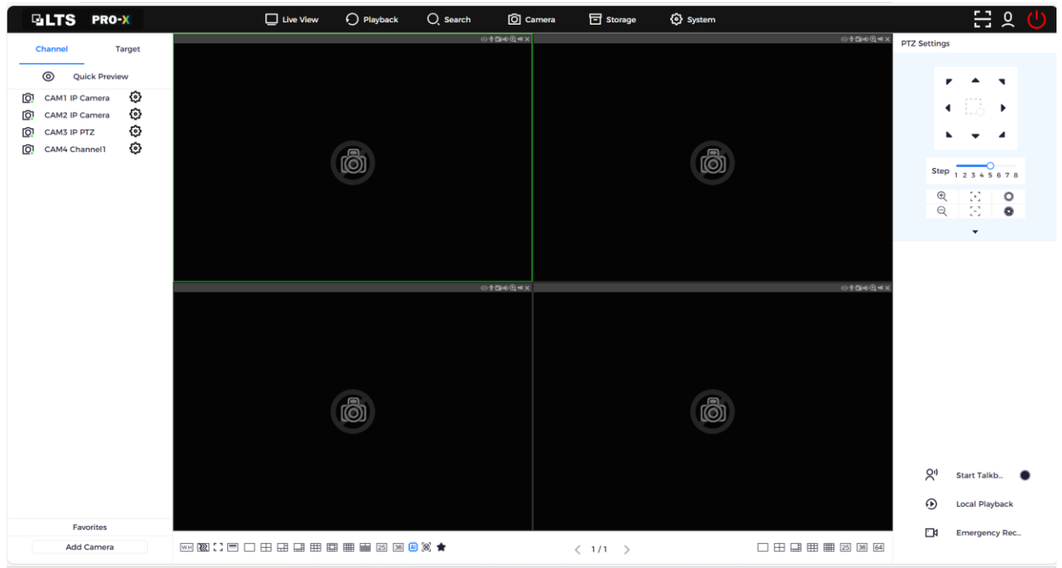


2. Enter username and password.
3. Click **Login**.

Web Main Menu

After login, the main menu is displayed.

Web main menu



Main menu description

No.	Name	Description
1	Function tiles	Click each tile to open the corresponding configuration page.
2	Scan	Scan the QR code to download mobile APP and add the Device for remote management.
3	Login	Click to logout current account.
4	Shut down	Restart or shut down the Device.

Cluster Service

The cluster function, also known as cluster redundancy, is a kind of deployment method that can improve the reliability of the device. In the cluster system, there is a number of main devices and another number of sub devices (the N+M mode), and they have a virtual IP address (the cluster IP). When the main device fails, the corresponding sub device will take over the job automatically. When the main device recovers, the sub device will transmit the configuration data, cluster IP address and videos recorded during the failure to the main device which then takes over the job again.

In the N+M cluster system, there is a management server, the DCS (Dispatching Console) server, which is responsible for timely and correct scheduling management of the main and sub devices. When you create a cluster, the current device is used as the first sub device and the DCS server by default.

NOTE

This function is available on select models.

Configuring Cluster IP

When the main device fails, the sub-device can appropriately take over the operation (monitoring or recording) using the configuration and virtual IP address of the main device. When accessing the device via the virtual IP, you can still view live video without the risk of losing recorded data.

Process

1. Log in to the web as the admin user.
2. Go to **System** > **Cluster Service**> **Cluster IP**.
3. Click **Enable**.
4. Configure **IP Address**, **Subnet Mask** and **Default Gateway**.
5. Click **Apply**.

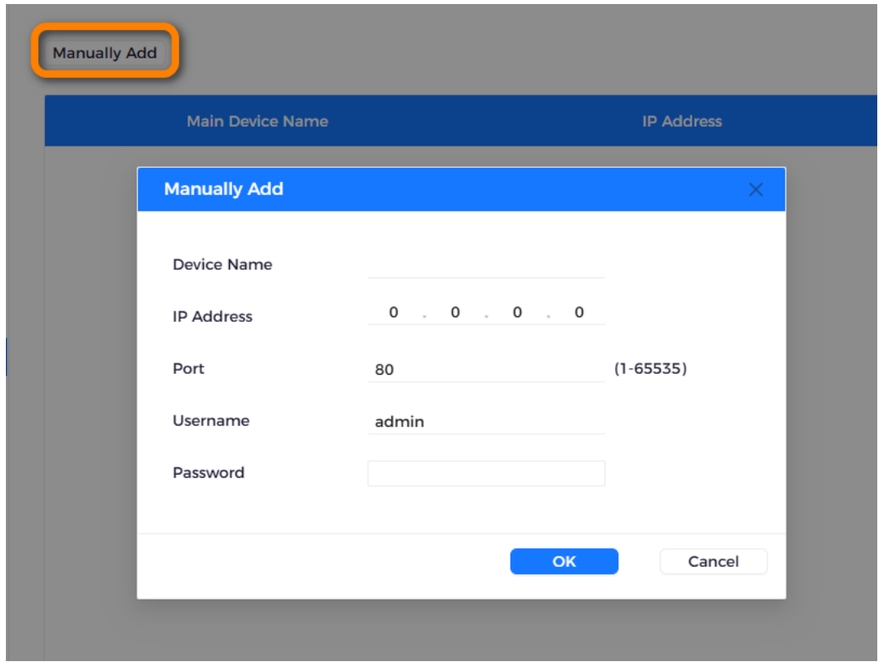
Primary Device

Add several main devices manually. After you enable the cluster function, you can view IP address, working status and connection log of the main device.

Process

1. Go to **System** > **Cluster Service** > **Primary Device**.
2. Click **Manually Add**.

Manually add



3. Configure parameters.

Parameters of adding main device

Parameter	Description
Device Name	Customize the device name.
IP Address	Enter the IP address of the NVR.
Port	Set the TCP port number of the server. The default value is 80. NOTE You can view the current TCP port number in **System** > **Network** > **Basic** > **Port**.
Username/Password	Enter the username and password of the NVR.

4. Click **OK**.

Sub Device

When you add the first sub device, the default IP is the device IP address that logs in on the web. Go to **System** > **Cluster Service** > **Sub Device**, you can add sub devices. For details, refer to "Primary Device".

NOTE

When adding the first sub device, you need not enter the IP address, because the first sub device is the current device by default.

After you added main device and sub device, you need to enable cluster function. Refer to "Configuring Cluster Control" for more information.

Video Return

After the main device has recovered, the videos recorded on the sub device during the failure period can be transferred to the main device.

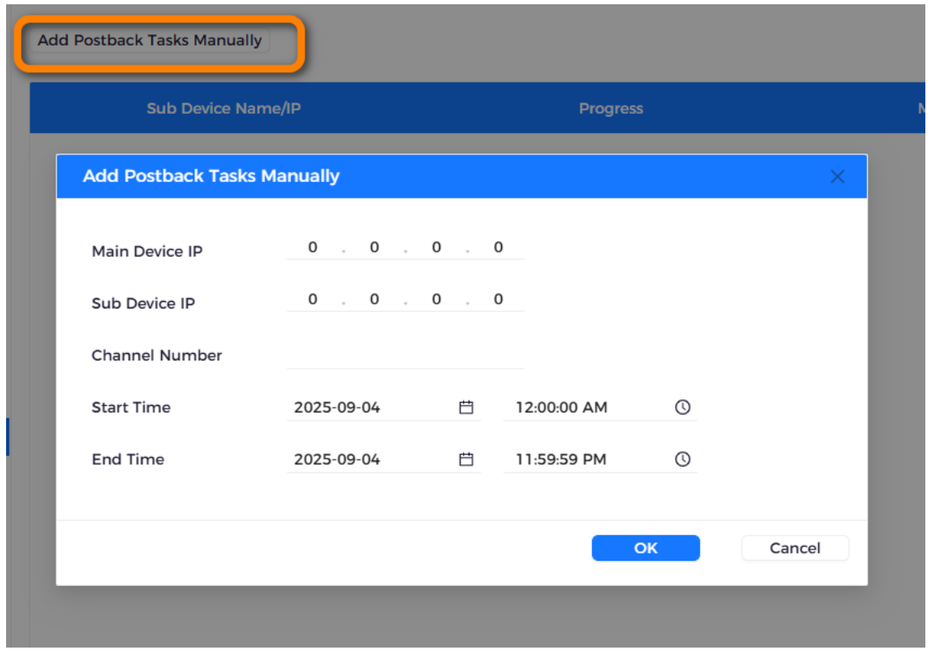
Precondition

The main device works normally.

Process

1. Go to **System** > **Cluster Service** > **Video Return**.
2. Click **Add Postback Tasks Manually**.

Add Postback Tasks Manually



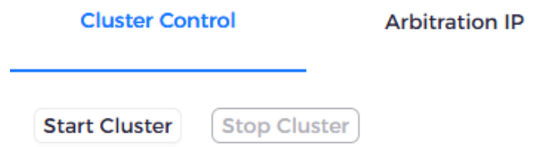
3. Configure the device IP, channel number, and time period.
4. Click **OK**.

Cluster Control

Cluster Control

Go to **System** > **Cluster Service** > **Cluster Control** to enable or disable cluster.

Start cluster



You can see the corresponding prompt if you successfully enabled cluster service.

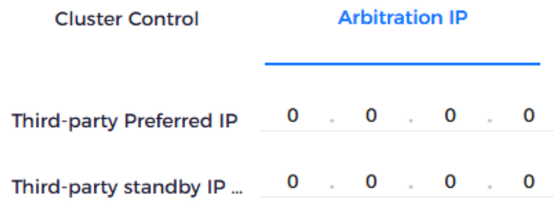
Arbitrage IP

When there are only 2 devices in the cluster, a third-party device is required to determine whether the main device is faulty, so arbitration IP must be set for the cluster to perform a normal replacement operation. The arbitration IP can be the IP address of another device, computer or gateway.

Process

1. Go to **System** > **Cluster Service** > **Cluster Control** > **Arbitrage IP**.

Arbitrage IP



2. Configure the preferred and standby IP.
3. Click **Apply**.

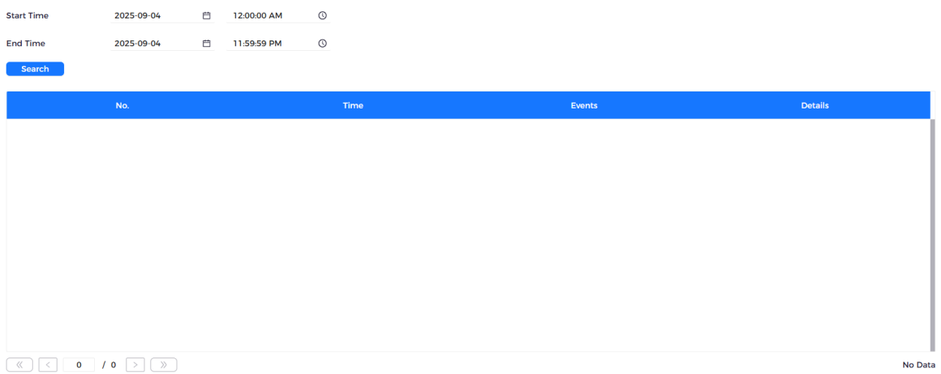
Cluster Log

Search for and view cluster logs.

Process

1. Go to **System** > **Cluster Service** > **Cluster Log**.

Cluster log



2. Select the start time and end time.
3. Click **Search**.

HDD Capacity Calculation

Use the following formula to calculate the HDD capacity:
Total capacity (MB) = Channel number × Demand time length (hour) × HDD capacity occupied per hour (MB/hour)
According to this formula, the formula for calculating recording time is as follows:

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

For example, for single-channel recording, the hard disk capacity used is 200 MB/hour. If you use a four-channel device for continuous recording for one month (30 days) at 24 hours a day, the required hard disk space is: 4 channels × 30 days × 24 hours × 200 MB/hour = 576 G. Therefore, you will need five 120 G hard drives or four 160 G hard drives.
According to the formula, the file size of one channel recorded within one hour at different flow rates is as follows:

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

NOTE
The table is for reference only. The data in actual situations may vary.

Cybersecurity Recommendations

Mandatory measures to ensure the network security of basic device:

- Timely Update Firmware and Client Software
  - According to the standard Processs of the technology industry, keep the firmware of devices (such as video recorders and IP cameras) up to date to ensure that the system is equipped with the latest security patches and fixes. When devices are connected to public networks, it is recommended to enable the "automatic check for updates" feature to receive timely information about firmware updates released by the manufacturer.
  - Download and use the latest version of the client software.
- Use Complex Passwords with Combination of Characters, Numbers and Symbols
  Please refer to the following suggestions for setting a password:
  - The length must not be less than 8 characters;
  - Combine at least two types of characters in the password, including uppercase letters, lowercase letters, numbers, and symbols;
  - Do not contain the account name or the reverse order of the account name;
  - Do not use consecutive characters, such as abcdefgh and 12345678;
  - Do not use overlapping characters, such as aaaaaaaaa and 11111111.

Constructive suggestions on improving device network security:

- Change Passwords Regularly
  We recommend that you change your password regularly to reduce the risk of it being guessed or cracked.
- Configure and Update Password Reset Information in Time
  The device supports the password reset function. Please promptly configure the information related to password reset, including the end user's email address and password protection questions. If any information changes, please update it accordingly in a timely manner. When setting password protection questions, do not use simple questions with easily obtainable answers.
- Enable Account Lock
  Account locking is enabled by default. We recommend that you keep this setting to ensure account security. Multiple failed login attempts will result in the corresponding account and its source IP address being locked.
- Physical Protection
  It is recommended to implement physical protection for equipment, especially storage devices. For instance, placing the equipment in dedicated computer rooms and cabinets, and enforcing strict access control permissions and key management to prevent unauthorized personnel from having physical contact, such as damaging hardware and making unauthorized connections with removable devices (e.g., USB flash drives and serial ports).
- Reset Default HTTP and Other Service Ports
  It is recommended to change the default HTTP and other server ports. We suggest changing them to any number between 1024 and 65535 to reduce the risk of exposing the ports in use to external threats.
- Enable HTTPS
  It is recommended to enable HTTPS in order to access web services through a secure communication channel.
- Bind IP and MAC Address to Device
  To reduce the risk of ARP spoofing, we recommend binding the gateway's IP address and MAC address to the device.
- Assign Accounts and Privileges Reasonably
  Add user accounts cautiously and assign them the minimum set of permissions based on business needs and management requirements.
- Disable Unnecessary Services and Apply Secure Modes
  If not needed, we recommend that you disable certain services, such as SNMP, SMTP, and UPnP, to reduce risks.
  If necessary, we recommend using safe mode, including but not limited to the following services:
  - SNMP: Select SNMP v3 and set the strong encryption password and authentication password.
  - SMTP: Select TLS to access the mailbox server.
  - FTP: Select SFTP and set a strong password.
  - AP hotspot: Select WPA2-PSK encryption mode and set a strong password.
- Establish a Secure Network Environment
  The following actions are strongly recommended to ensure the safety of the equipment and reduce potential network risks:
  - Disable the port mapping function of the router to prevent external networks from directly accessing internal network devices.
  - Partition and isolate the network according to actual network requirements. If there is no communication requirement between two sub-networks, it is recommended to implement network isolation through VLANs, network segmentation, and other technologies.
  - Establish an 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
  - Enable IP/MAC address filtering function to restrict the range of hosts allowed to access the device.
- Security Auditing
  - Check online users: Regularly check online users to prevent unauthorized logins.
  - Check the device logs: Obtain the IP address used to log into the device and its main

operations from the logs.

- Network Log
  Due to limited storage capacity, the stored logs could not be fully retained. If you need to keep logs for an extended period, we recommend enabling the network logging feature to ensure that critical logs can be synchronized to the network log server for tracking.