LUMINYS

Network Video Recorder

User Manual

Rev. 2

Foreword

General

This manual covers the functions and operation of the Luminys network video recorder (referred to as "the device"). Please read it thoroughly before use and keep it for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	March 2025
2	Added content about R5-exclusive features.	April 2025

Privacy Protection Notice

As a device user or data controller, you may collect personal data such as facial images, fingerprints, and license plate numbers. It's essential to comply with local privacy laws to safeguard individuals' rights. This includes providing clear identification of surveillance areas and necessary contact information.

Disclaimer

While we strive to ensure the accuracy and completeness of this document, we do not provide any formal guarantees. The use and results derived from this document are the sole responsibility of the user. We also reserve the right to modify its contents without prior notice.

About the Manual

- This manual is for reference only and may have minor discrepancies with the actual product.
- We are not liable for damages resulting from improper operation contrary to this manual.
- The manual will be updated to align with the latest laws and regulations. For more information, refer to the paper manual, scan the QR code, use our CD-ROM, or visit our official website. Minor differences may exist between electronic and paper versions.
- All designs and specifications are subject to change without notice. Product updates may lead to discrepancies between the manual and the actual product. Contact customer service for the latest information and documentation.
- There may be errors or inaccuracies in the descriptions of functions, operations, and technical data. We reserve the right of final interpretation in case of questions or disputes.
- If the manual cannot be opened, please update your reader software or try another compatible reader.
- All trademarks and company names mentioned are the properties of their respective owners.
- For assistance, visit our website or contact your supplier or customer service.
- We reserve the right of final interpretation in case of questions or disputes.

Safety Instructions

The following symbols might appear in the manual.

Symbol	Definition
⚠	Indicates a risk hazard that, if not avoided, may result in death, injury, property damage, data loss, decreased performance, or unpredictable outcomes.
	Offers methods to help you troubleshoot issues or save time.
ⓘ	Provides more context and information.

Important Safeguards and Warnings

Transportation and Storage Requirements

- Only transport and store the device under the allowed humidity and temperature conditions.

Installation Requirements

- Ensure the power adapter is disconnected from the power source before connecting it to the device.
- Adhere to local electrical safety codes and standards. Ensure a stable ambient voltage that matches the device's power supply requirements.
- Avoid exposing the battery to low air pressure or extreme temperatures (high or low).
- Do not throw the battery into a fire or furnace.
- Avoid cutting, puncturing, or applying mechanical pressure to the battery to prevent fire or explosion risks.
- Use only the standard power adapter or cabinet power supply provided. The use of nonstandard adapters may result in injury or damage, for which Luminys Systems Corporation assumes no responsibility.
- Do not place the device in direct sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Ensure the device is installed in a well-ventilated location without obstructing its ventilation.
- Install the device on a stable surface to prevent falling.
- Ensure the power supply meets **ES1 in IEC 62368-1** standards and does not exceed PS2. Verify power requirements on the device label.
- The device is a class I electrical appliance and must be connected to a power socket with protective earthing.
- Use power cords that meet local standards and rated specifications.
- Before connecting, verify that the input voltage matches the device's power requirements.
- Position the device near a power socket for easy access in emergencies or to quickly disconnect power.
- Ensure the power plug and appliance coupler are easily accessible to cut off power if needed.
- Non-professionals and unauthorized personnel should not open the device’s casing to prevent accidents or damage.

Operation Requirements

- Do not place the device in direct sunlight or near heat sources.
- Ensure the device is in an environment free from dampness, dust, or soot.
- Install the device on a firm and stable surface to prevent accidental falls.
- Avoid spilling or splashing liquids onto the device.
- Do not place containers filled with liquid on or near the device.
- Place the device in a well-ventilated area, ensuring ventilation openings are not blocked.
- Operate the device only within the specified range of power input and output.
- Refrain from taking apart the device to avoid damage or safety risks.
- Use the device within the recommended humidity and temperature levels.

- Replace old or unwanted batteries with new ones of the same type and model.

Maintenance Requirements

- The appliance coupler serves as the primary disconnection device for the device. Ensure it is positioned at an easily accessible angle.

Table of Contents

Introduction

About the Device

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

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

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

Features

Device functions may vary depending on the software and hardware version and the model you are using.

Real-Time Surveillance

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

Recording and Playback

- Supports recording and playing back videos of each channel.
- Supports slow-motion, sped-up, reverse, and frame-by-frame playback

Smart Detection

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

Alarm Linkage

- Supports multiple alarm linkage actions in response to an alarm event.

Online Updates

- Supports updating the program online.

Backup

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

Network Surveillance

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

Packing List

Review the list below to ensure all the device components are present and in good condition.

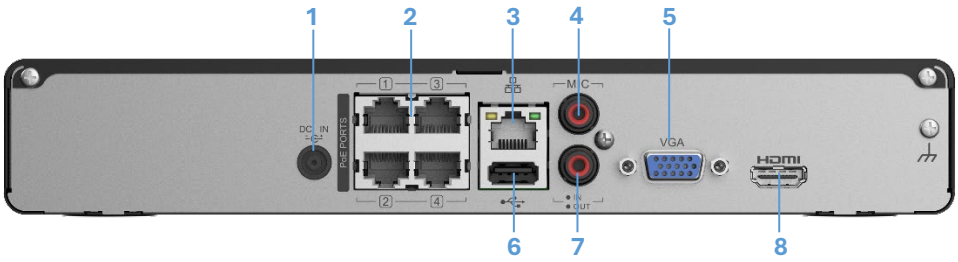
Item	Requirements
Packaging	• Ensure the packaging shows no signs of damage or distortion. • Verify no items are missing.
Label	• Confirm the label is intact and undamaged. • Verify no items are missing.
Casing	• Ensure the packaging shows no signs of damage or distortion. • Verify no items are missing.

NVR Structure

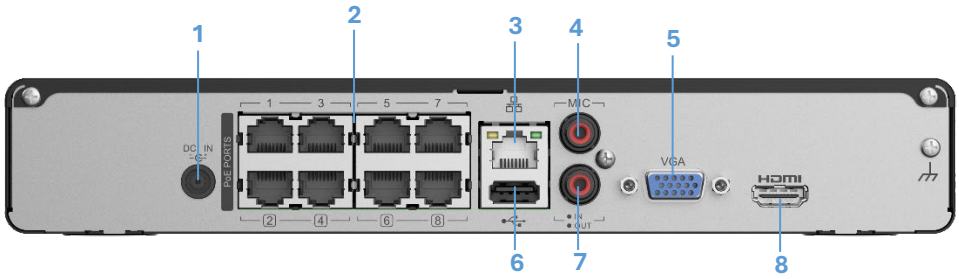
Mini 1U

Front Panel

Number	Part Name	Part Description
1	HDD Indicator Light	Displays a solid blue light to indicate a hard disk abnormality.
2	Network Indicator Light	Displays a solid blue light to signal a network abnormality.
3	Power Indicator Light	Displays a solid blue light when the device is on and operating normally.
4	USB Port	Connects peripheral devices.



Back Panel (4-Port PoE)



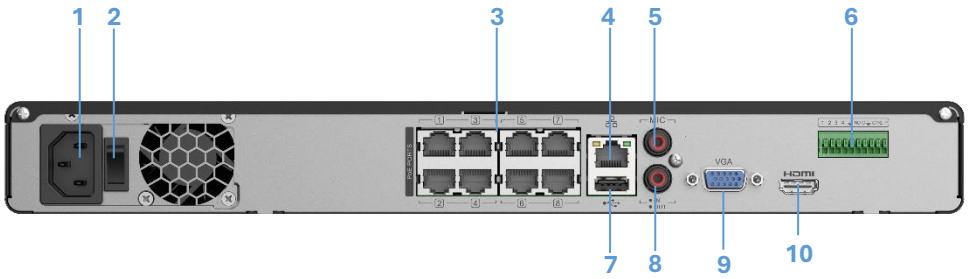
Back Panel (8-Port PoE)

Number	Part Name	Part Description
1	Power Input Port	Port to input power source.
2	PoE Ports	A built-in PoE switch to support PoE functions. This port can be used to power network cameras.
3	Network Port	Port to input a network cable.
4	Audio Input Port	Connects a compatible audio input device to enable two-way communication functionality.
5	VGA Port	Outputs analog video data to a connected display device.
6	USB Port	Connects external devices.
7	Audio Output Port	Connects a compatible audio output.
8	HDMI Port	Transmits uncompressed high-definition video and multi-channel audio data to a display device.

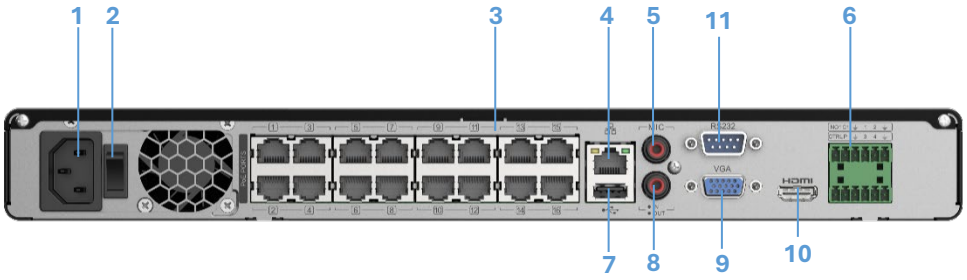
1U

Front Panel

Number	Part Name	Part Description
1	HDD Indicator Light	Displays a solid blue light to indicate a hard disk abnormality.
2	Network Indicator Light	Displays a solid blue light to signal a network abnormality.
3	Power Indicator Light	Displays a solid blue light when the device is on and operating normally.
4	USB Port	Connects peripheral devices.



Back Panel (8-Port PoE)

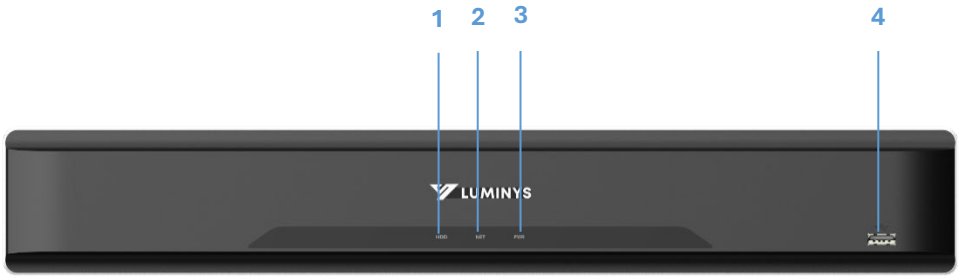


Back Panel (16-Port PoE)

Number	Part Name	Part Description
1	Power Input Port	Port to input power source.
2	Power Switch	Turns the switch on or off.
3	PoE Ports	A built-in PoE switch to support PoE functions. This port can be used to power network cameras.
4	Network Port	Port to input a network cable.
5	Audio Input Port	Connects a compatible audio input device to enable two-way communication functionality.
6	Alarm Output Ports	Outputs alarm signals to the alarm device: • NO: Normally open alarm output port. • C: Common alarm output port.
	CTRL (Controllable 12 V Power Supply Output)	Controls the output of the on-off button alarm relay, managing the alarm device with voltage presence or absence. It can also serve as a power input for certain alarm devices, such as alarm detectors.
	P (12 V Power Output Port)	Provides power to peripheral devices like cameras and alarm systems. Ensure the peripheral device's power consumption does not exceed 1 A.
	Alarm Input (Ports 1–4)	Receives signals from an external alarm source. ⓘ If the alarm input device uses external power, ensure it shares the same ground as the NVR.
7	USB Port	Connects external devices.

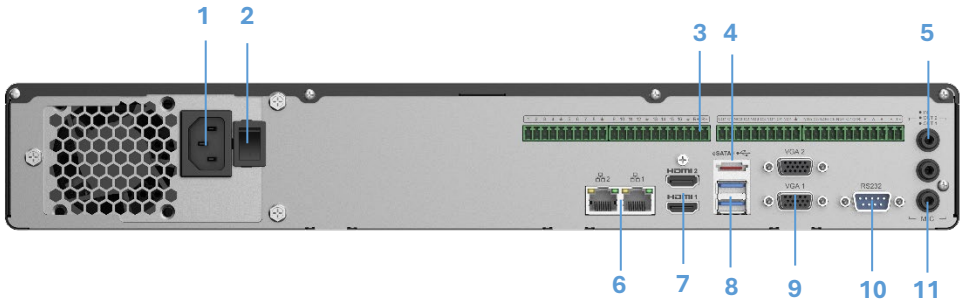
8	Audio Output Port	Connects a compatible audio output.
9	VGA Port	Outputs analog video data to a connected display device.
10	HDMI Port	Transmits uncompressed high-definition video and multi-channel audio data to a display device.
11	RS-232 Port	Used for configuring IP addresses or transferring transparent COM data.

1.5U



Front Panel

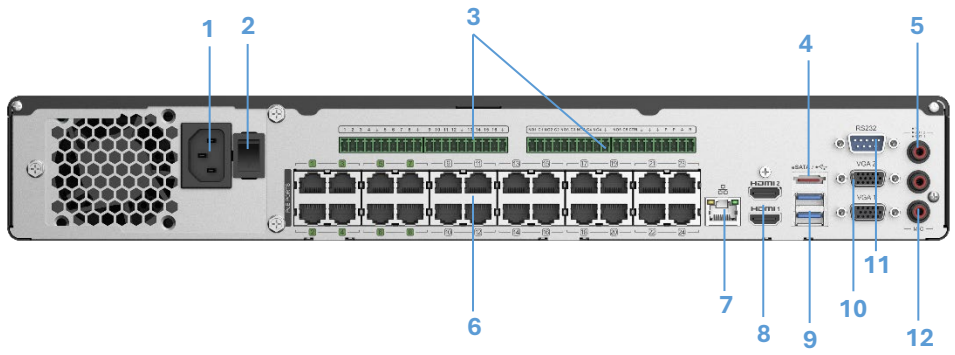
Number	Part Name	Part Description
1	HDD Indicator Light	Displays a solid blue light to indicate a hard disk abnormality.
2	Network Indicator Light	Displays a solid blue light to signal a network abnormality.
3	Power Indicator Light	Displays a solid blue light when the device is on and operating normally.
4	USB Port	Connects peripheral devices.



Back Panel

Number	Part Name	Part Description
1	Power Input Port	Port to input power source.
2	Power Switch	Turns the switch on or off.
3	Alarm Output Ports	Outputs alarm signals to the alarm device: • NO: Normally open alarm output port. • C: Common alarm output port.

	CTRL (Controllable 12 V Power Supply Output)	Controls the output of the on-off button alarm relay, managing the alarm device with voltage presence or absence. It can also serve as a power input for certain alarm devices, such as alarm detectors.
	P (12 V Power Output Port)	Provides power to peripheral devices like cameras and alarm systems. Ensure the peripheral device's power consumption does not exceed 1 A.
	Alarm Input (Ports 1–4)	Receives signals from an external alarm source. ⓘ If the alarm input device uses external power, ensure it shares the same ground as the NVR.
4	eSATA	Connects a device with an external SATA port. The HDD must be jumped if there is an external HDD connected.
5	Audio Input Port	Connects a compatible audio input device to enable two-way communication functionality.
6	Dual Network Port	Port to input a network cable.
7	HDMI Port	Transmits uncompressed high-definition video and multi-channel audio data to a display device.
8	USB Port	Connects external devices.
9	VGA Port	Outputs analog video data to a connected display device.
10	RS-232 Port	Used for configuring IP addresses or transferring transparent COM data.
11	Audio Output Port	Connects a compatible audio output.



Back Panel

Number	Part Name	Part Description
1	Power Input Port	Port to input power source.
2	Power Switch	Turns the switch on or off.
3	Alarm Output Ports	Outputs alarm signals to the alarm device: • NO: Normally open alarm output port. • C: Common alarm output port.
	CTRL (Controllable 12 V Power Supply Output)	Controls the output of the on-off button alarm relay, managing the alarm device with voltage presence or absence. It can also serve as a power input for certain alarm devices, such as alarm detectors.

	P (12 V Power Output Port)	Provides power to peripheral devices like cameras and alarm systems. Ensure the peripheral device's power consumption does not exceed 1 A.
	Alarm Input (Ports 1–4)	Receives signals from an external alarm source. ⓘ If the alarm input device uses external power, ensure it shares the same ground as the NVR.
4	eSATA	Connects a device with an external SATA port. The HDD must be jumped if there is an external HDD connected.
5	Audio Input Port	Connects a compatible audio input device to enable two-way communication functionality.
6	PoE Ports	A built-in PoE switch to support PoE functions. This port can be used to power network cameras.
7	Network Port	Port to input a network cable.
8	HDMI Port	Transmits uncompressed high-definition video and multi-channel audio data to a display device.
9	USB Port	Connects external devices.
10	VGA Port	Outputs analog video data to a connected display device.
11	RS-232 Port	Used for configuring IP addresses or transferring transparent COM data.
12	Audio Output Port	Connects a compatible audio output.

Installation

Follow the instructions outlined below to install an HDD to the Device and connect the Device to an alarm input and output device.

⚠ Follow local safety regulations during installation.

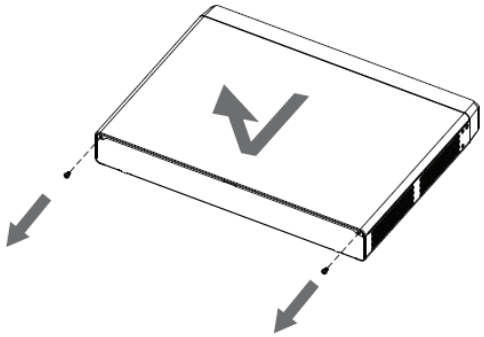
Installing an HDD

An HDD must be installed prior to using the Device. Follow the steps below to install an HDD if one is not pre-installed.

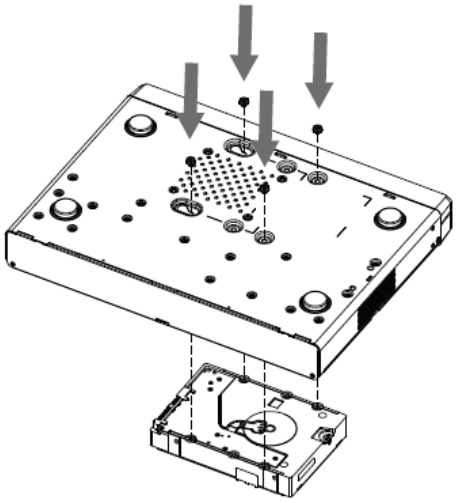
⚠ Unplug the Device's power source and put on anti-static gloves prior to installing an HDD.

Mini 1U

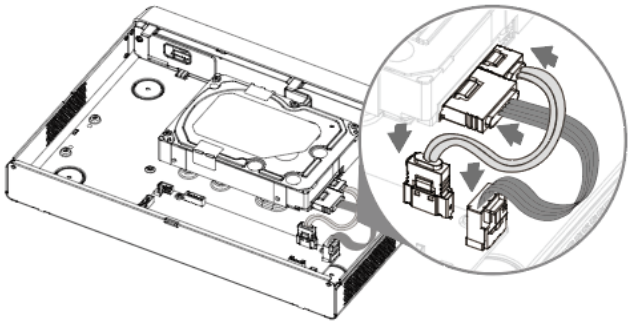
1. Loosen the screws securing the cover using a screwdriver.



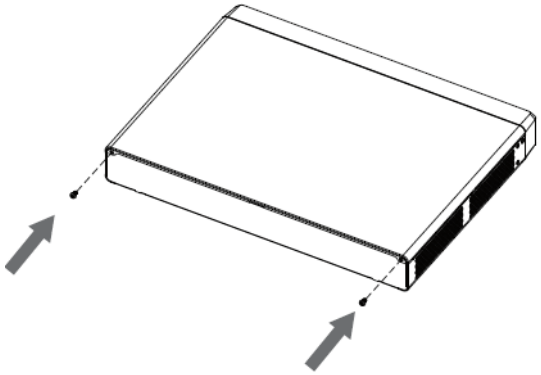
2. Align the four holes on the HDD with the corresponding holes on the device and securely fasten the screws to hold the HDD in place.



3. Connect the HDD's power and data cables to the device's corresponding ports.

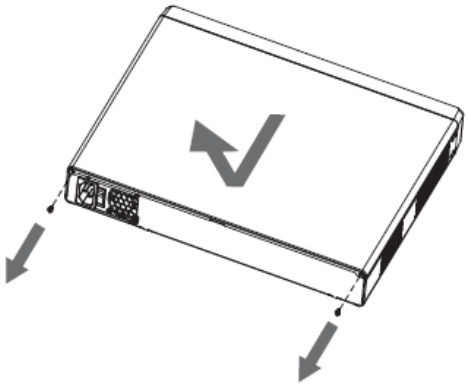


4. Replace the cover onto the device and tighten the screws securely to reattach.

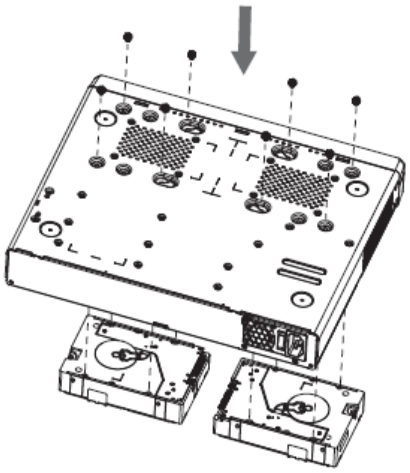


1U

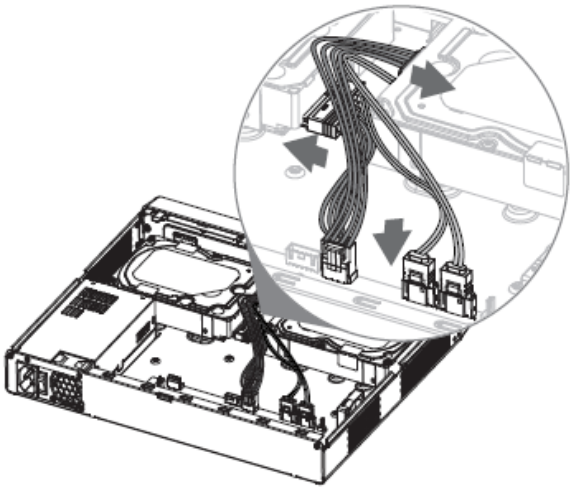
1. Loosen the screws securing the cover using a screwdriver.



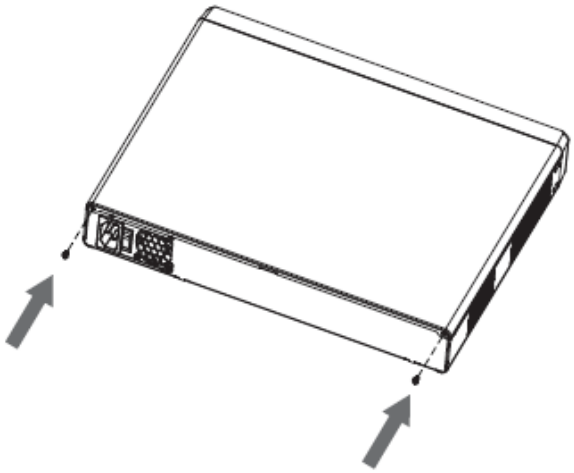
2. Align the four holes on the HDD with the corresponding holes on the device and securely fasten the screws to hold the HDD in place.



3. Connect the HDD's power and data cables to the device's corresponding ports.

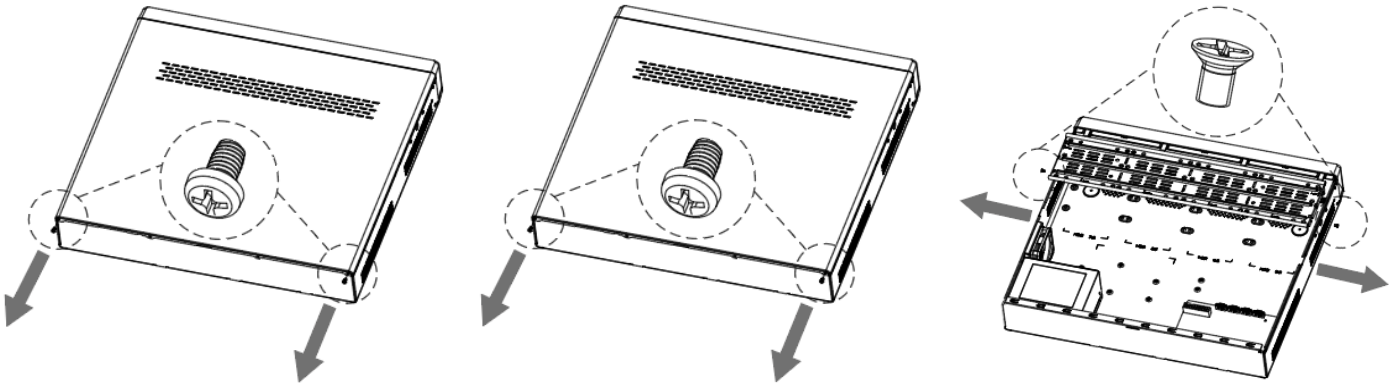


4. Replace the cover onto the device and tighten the screws securely to reattach.

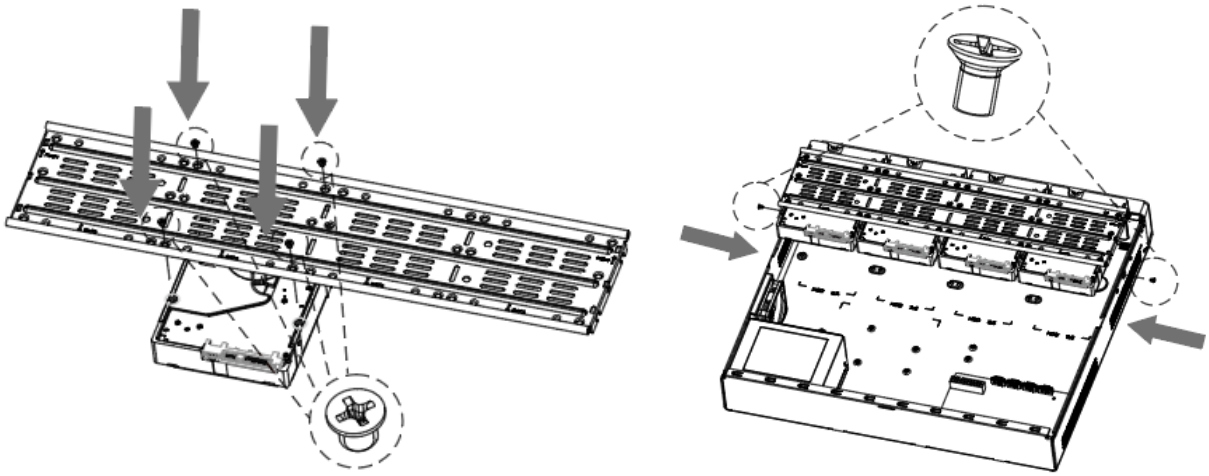


1.5U

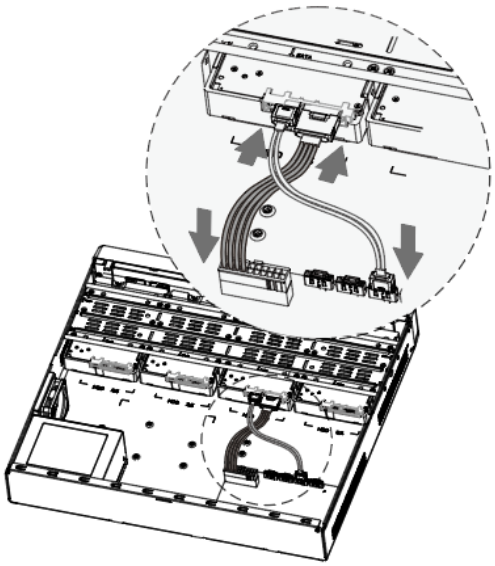
1. Remove the upper cover and set aside. Then, unfasten the screws on the sides of the HDD bracket and remove.



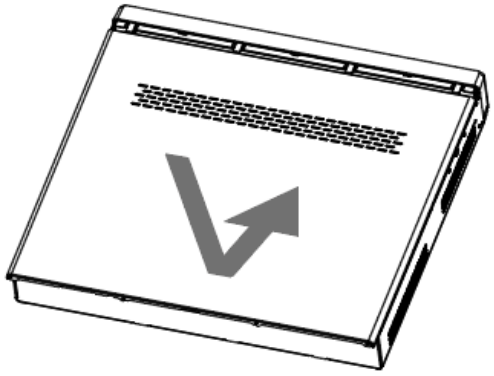
2. Align and screw the HDD to the bracket. Then, install the bracket and HDD using the side screws.

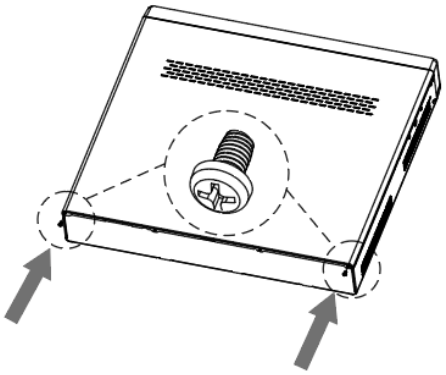


3. Connect the HDD's SATA and power cable to the device.



4. Reinstall the front cover.



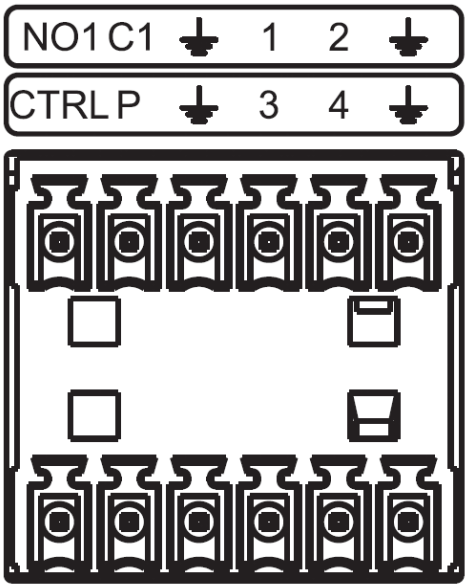


Connecting an Alarm Input and Output Device

Follow the instructions below to learn how to connect to an alarm input and output.

Alarm Ports on the NVR

ⓘ The alarm ports shown may vary depending on the device model.



Icon	Description
1–4	Receives signals from an external alarm source.
NO1 C1	Outputs alarm signals to the alarm device: • NO: Normally open alarm output port. • C: Common alarm output port.
⏚	Ground port.
CTRL	12V power supply output. Power is disabled when the alarm is canceled.
P	Provides power to peripheral devices such as a network camera. ⓘ Ensure the power supply for peripheral devices is below 1A.

Connecting an Alarm Input Device

Follow the steps below connect an alarm input device.

1. Connect the positive end (+) of the alarm input device to the alarm input port (ALARM IN 1–4).
2. Connect the external power supply to the alarm device.
3. Connect the negative end (⏚) to the ground port.

ⓘ

- Use any of the GND ports for grounding.
- Connect the NC port to the corresponding input port.
- Ensure proper grounding of the NVR for peripheral power supplies.

Connecting an Alarm Output Device

Follow the steps below connect an alarm output device.

1. Connect the external power supply to the alarm device.
2. Use the RS-485 A/B cable to connect PTZ decoders, if applicable.

Refer to the table for relay compatibility.

Icon		HFD23/005-1ZS	HRB1-S-DC5V
Material		AgNi + Gold Plating	AuAg10/AgNi10/CuNi30
Resistance Load Rating	Rated Switch Capacity	30 VDC, 1 A/125 VAC, 0.5 A	24 VDC, 1 A/125 VAC, 2 A
	Maximum Switch Power	62.5 VAC/30 W	250 VAC/48 W
	Maximum Switch Voltage	125 VAC/60 VDC	125 VAC/60 VDC
	Maximum Switch Currency	2 A	2 A
Insulation	Between Touches	400 VAC, 1 Minute	500 VAC, 1 Minute
	Between Touch and Winding	1000 VAC, 1 Minute	1000 VAC, 1 Minute
Time to Power On		Max. 5 ms	Max. 5 ms
Time to Power Off		Max. 5 ms	Max. 5 ms
Longevity	Mechanical	1 × 107 Times (300 Times/Minutes)	1 × 106 Times (300 Times/Minutes)
	Electrical	1 × 105 Times (30 Times/Minute)	2.5 × 104 Times (30 Times/Minute)
Working Temperature		-30 °C to 70 °C (-22 °F to 158 °F)	-40 °C to 70 °C (-40 °F to 158 °F)

Local Operations

ⓘ These instructions are for reference only and may differ slightly based on the device's actual interface.

Starting the Device

Prerequisites

Prior to starting the device, ensure the following prerequisites are met:

- Verify that the input voltage aligns with the device's power requirements.
- To enhance device stability and prolong HDD lifespan, use a power source with stable voltage and minimal interference, such as a UPS.
- Connect the power adapter to the device before plugging it into the power supply.

Procedure

1. Connect the device to a monitor and mouse.
2. Plug in the device’s power cord.
3. Turn on the power switch.

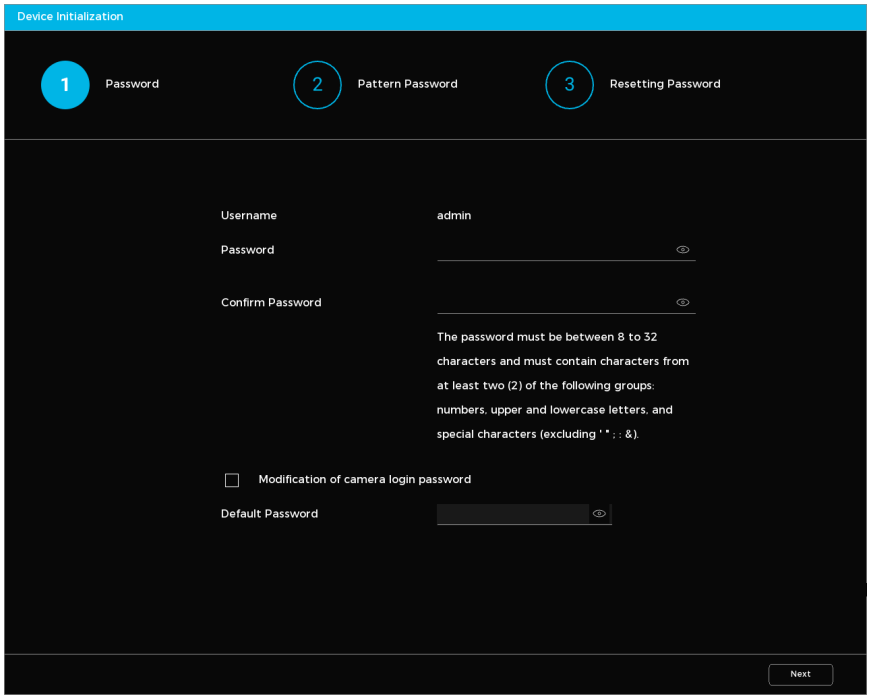
Initialization

Prerequisites

Ensure an administrator account and password and any relevant security settings are configured prior to initial use. It is recommended to update the administrator password to prevent unauthorized access.

Procedure

5. Power on the device. Select your preferred language and click **Next**.
6. Read and agree to the Software License Agreement and Privacy Policy.
7. Set an administrator password.

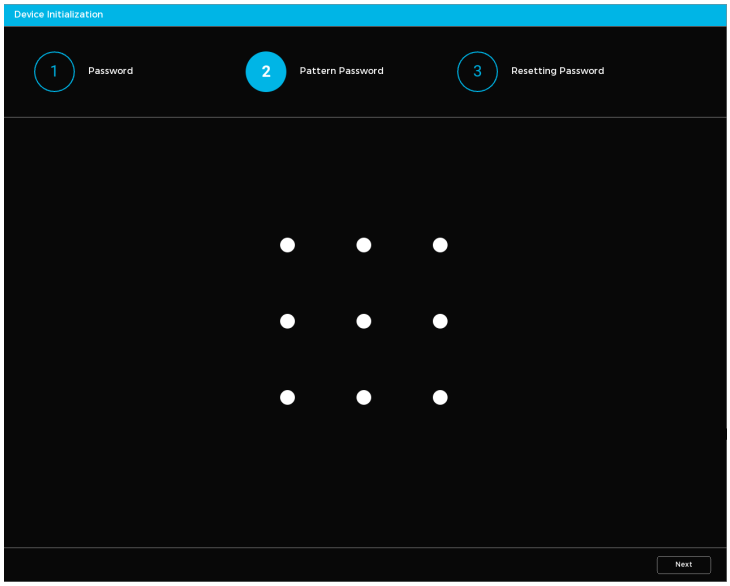


Administrator Password Setting Page

Parameter	Description
Username	The default username is set to admin.
Password	Enter in a password and confirm it.
Confirm Password	
Default Password	Check **Modification of camera login password** to set a default password for cameras.
Modification of camera login password	

8. (Optional) Set a pattern password. Hit **Next** to not set one.

ⓘ If set, the pattern password will become the default login method.



Unlock Pattern Screen

9. Input the Password Protection Information. This information will be used to recover and reset the device password.

ⓘ

- **Reserved Email Address**
  - A security code will be sent to this address in case of a password reset.
- **Security Questions**
  - The answers to these questions will be required for a password reset.

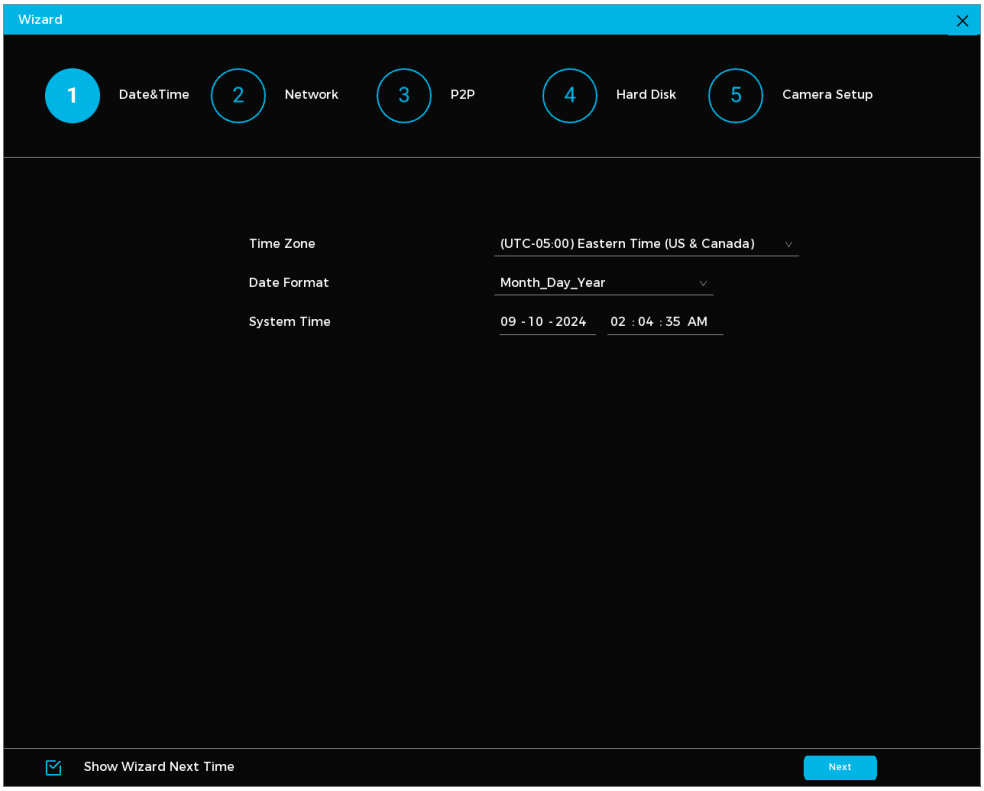
10. Click **Completed** when done. The Setup Wizard window will appear.

Setup Wizard

Follow the setup wizard prompts to configure basic device settings.

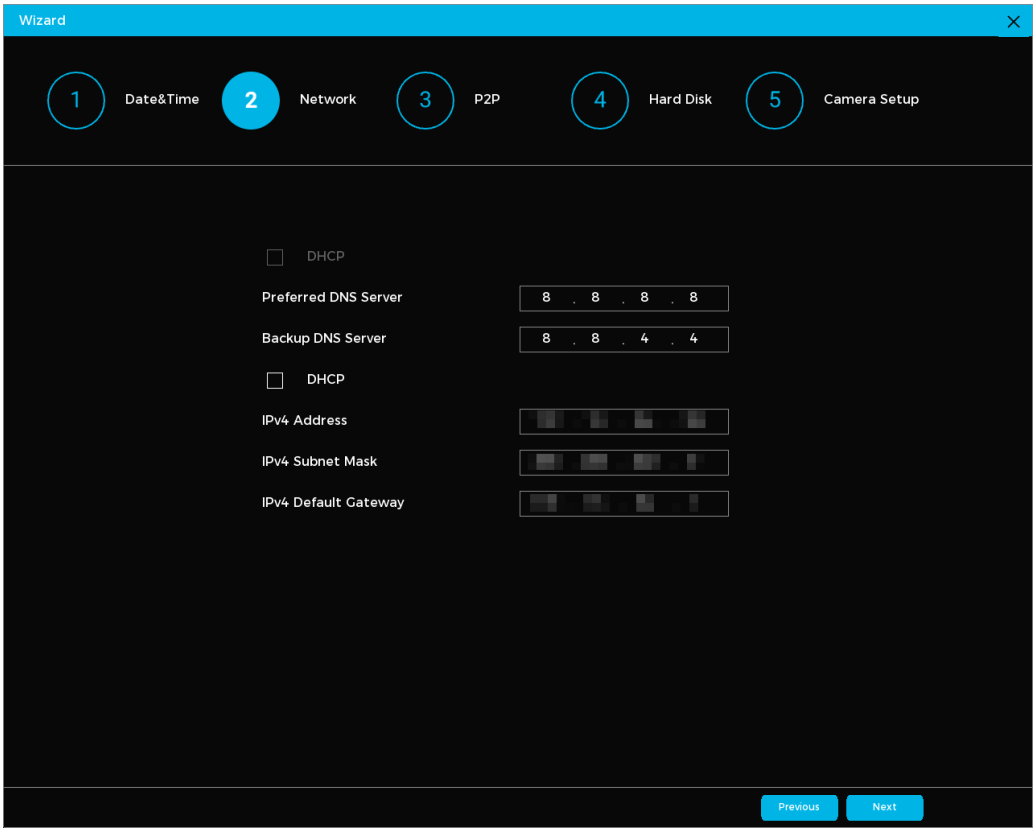
1. Set the time zone, date format, and system time.

ⓘ The setup wizard will be initiated after a device restart if the checkbox next to Show Wizard Next Time is selected.



Setup Wizard (Step 1)

2. Configure your network settings.

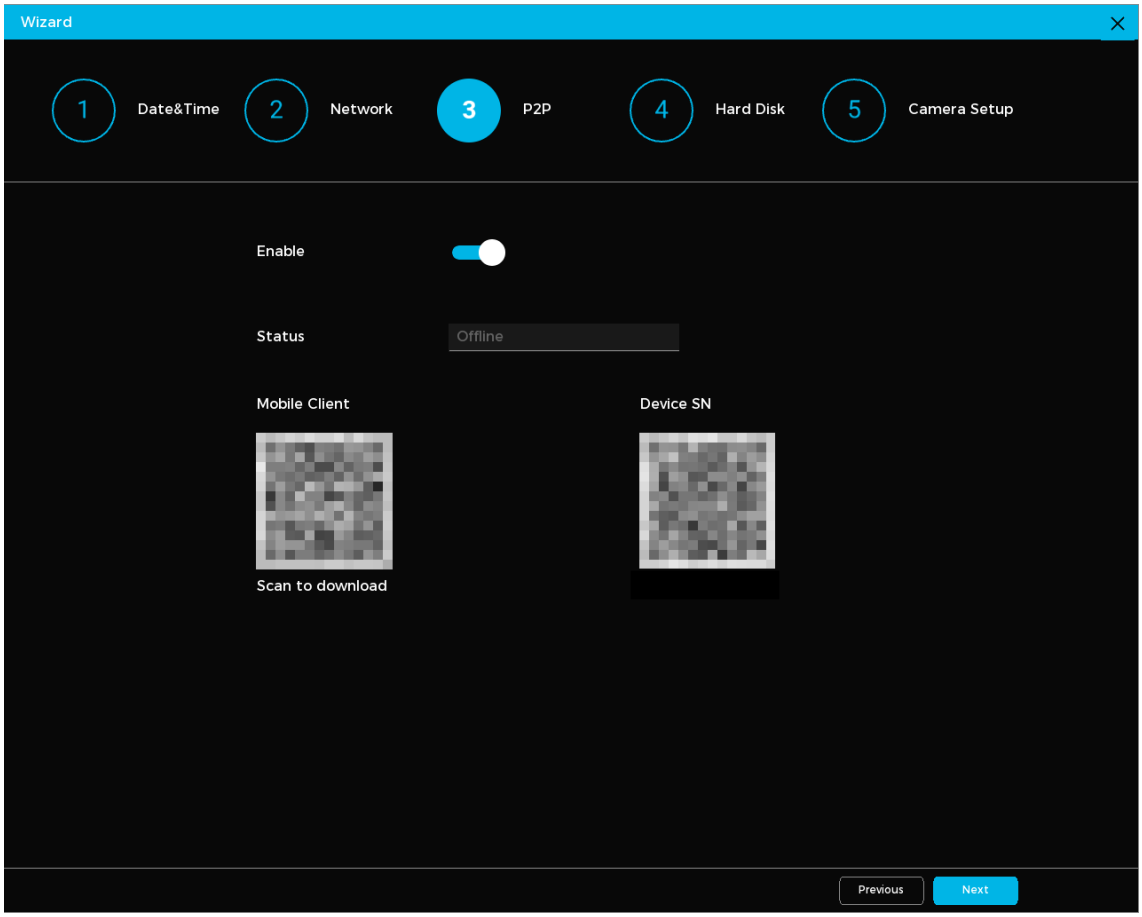


Network Setting Parameters

Parameter	Description
DHCP	Allow the system to assign a dynamic IP address to the Device automatically, eliminating the need for manual configuration. • The first DHCP is designated for the DNS server. • The second DHCP is designated for the Device.
Preferred DNS Server	Set the preferred and backup DNS server address.
Backup DNS Server	
IPv4 Address	Input the IPv4 address, subnet mask, and default gateway. Ensure they are all within the same network segment.
IPv4 Subnet Mask	
IPv4 Default Gateway	

3. Enable P2P (Peer-to-Peer). Click **Next**. Scan the QR code under Device SN with the LumiViewer mobile app to add and connect a device

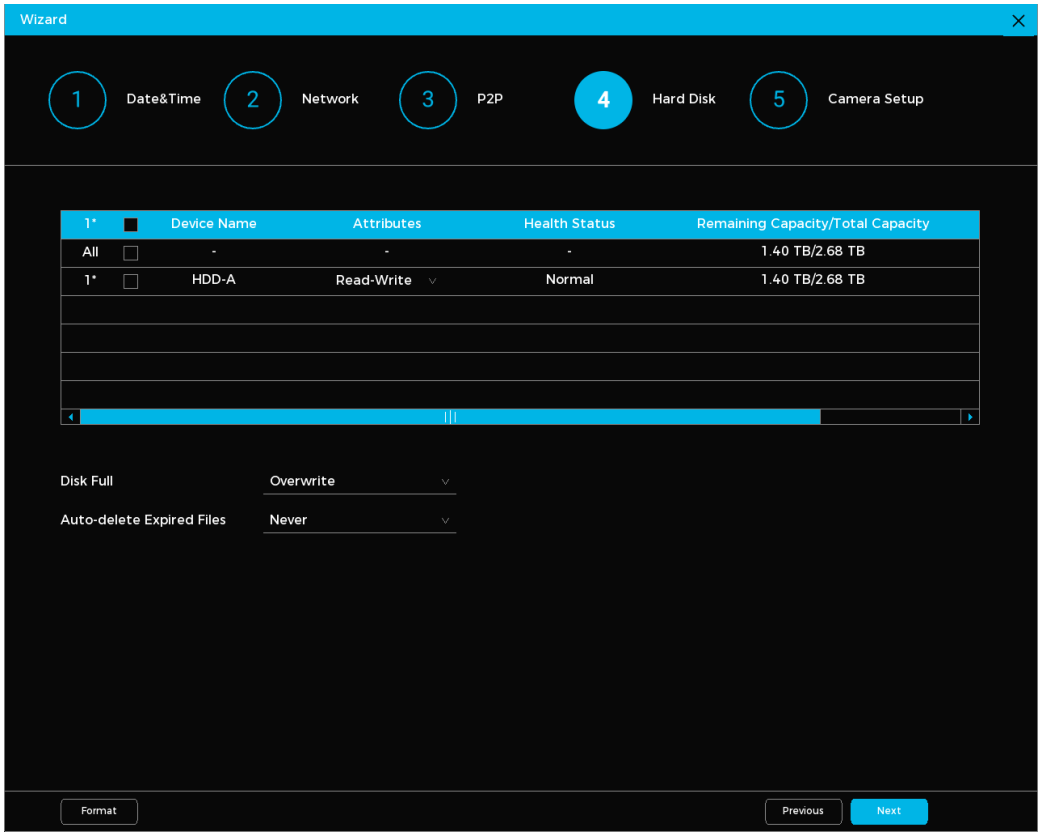
ⓘ When the P2P function is enabled and the device is connected to the Internet, the system collects information like your email address and MAC address for remote access.



4. In the disk list, review the HDD details, set the HDD type, select the storage strategy, and then click **Next**.

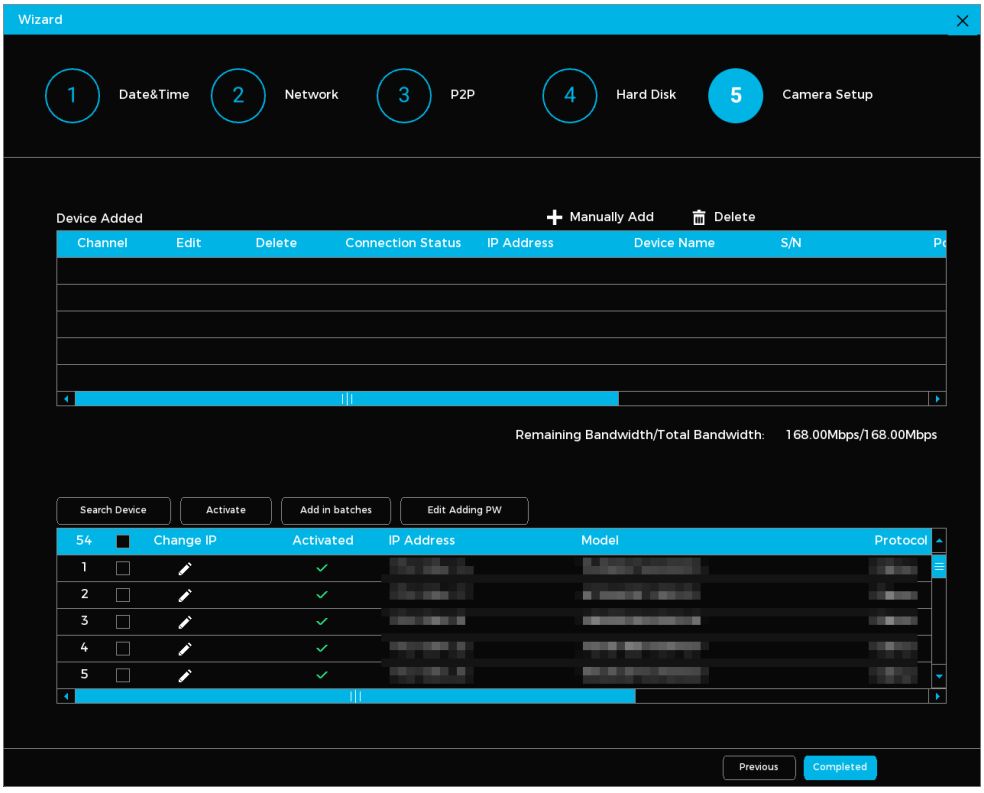
- **To set the HDD type**: Navigate to the Attributes column. Select **Read-Write**, **Read-only**, or **Redundancy**.
- **To format the HDD**: Select an HDD, click **Format**, and follow the onscreen prompts.

  ⚠ Formatting the HDD will erase all existing data.
- **To select a storage strategy**:
  - Configure settings for when the disk is full.
  - Choose **Stop** to stop recording when disk storage is full.
  - Choose **Overwrite** to overwrite the oldest files when disk storage is full.
- **Select if you want to automatically delete expired files**.
  - Choose **Never** if you do not want to automatically delete expired files.
  - Choose **Custom** to select how long to keep expired files before they are automatically deleted.



5. Connect any remote devices. You can connect devices by searching or by adding them manually.

- **To add by search**:
  - Click Search by Device.
  - Choose the devices to add from the search results. Click **Add in batches.**



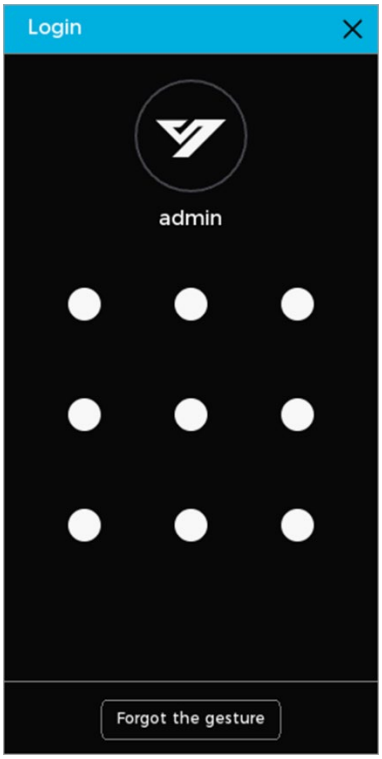
6. Click **Completed** when done.

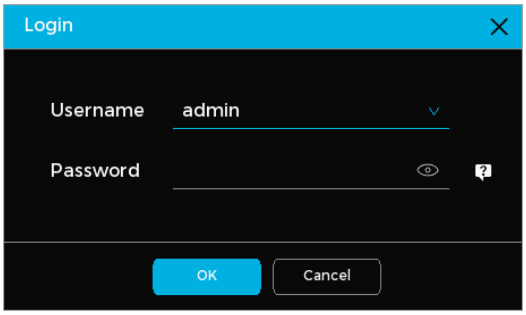
Login Procedure

Follow the steps below to log in to the Device.

1. Click the live view page. If you configured the pattern password, it will be displayed by default. Click **Forgot the gesture** to use the device password login.

ⓘ Click to reset your password.





2. Enter the password and click **OK**.

Live View

Follow the steps to view the live video from different channels.

1. Select a window.
2. Double-click a channel in the channel list.

The channel will be displayed in the selected window.

Live View Control Bar Parameters

You can view the live view control bar by hovering the cursor over the bottom middle portion of the channel window. The control allows you to instantly playback video, zoom in locally, take a snapshot, use the intercom, switch streams, and control PTZ functions.

Live View Control Bar

Icon	Function	Description
	Instant Playback	Review up to 60 minutes of footage. You may configure the playback time in settings by going to **System → General → Basic Configuration**.
	Digital Zoom	Click the icon. Select the area you would like to magnify and release the mouse button. You may also point to the area to enlarge or shrink and scroll to zoom in or out. Right-click the channel window to return to the original view.
	Manual Snapshot	Take a snapshot of the current video channel. They will be automatically saved to the connected USB storage device.
	Two-Way Talk	This function is only available when the remote device supports bidirectional talk.
	IP Speaker Talk	To use this function, the IP speaker must be bound to a channel.
	Mainstream and Substream Toggle	Switch between the mainstream and substream(s). The mainstream is suitable for local recording and provides HD video surveillance. Substreams are best for network transmission and when network bandwidth is limited.
	PTZ Control	Access PTZ control settings.

Navigation Bar

The navigation bar is located at the bottom of the live page and provides access to additional features.

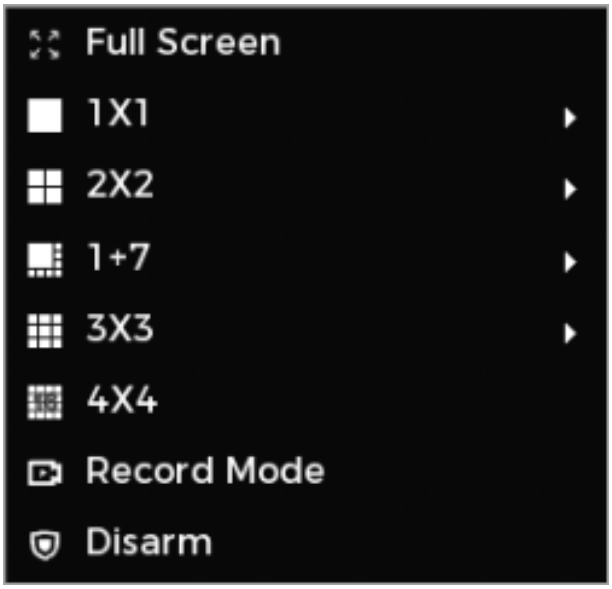
Navigation Bar

Icon	Description
	Go to the next screen.
	Go to the previous screen.
	Arrange view layout.
	Enable or disable auto-switch.
	Enter full-screen mode.

☆	Save a customized preview view layout. Any saved combinations will be displayed on the left side of the preview screen.

Shortcut Menu

You can access the shortcut menu by right-clicking on the live page. The shortcut menu allows you to choose between full and split-screen mode, configure the record mode, and disarm devices.



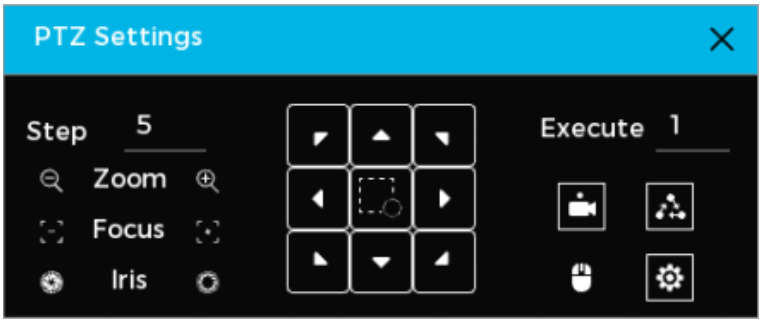
Shortcut Menu

Pan-Tilt-Zoom (PTZ)

The PTZ control feature allows you to remotely control the physical positioning of a PTZ camera. This enables different potential views of an area for full-coverage surveillance.

Operating the PTZ Control Panel

Click the in the live view control bar to access the PTZ control panel.



PTZ Control Panel

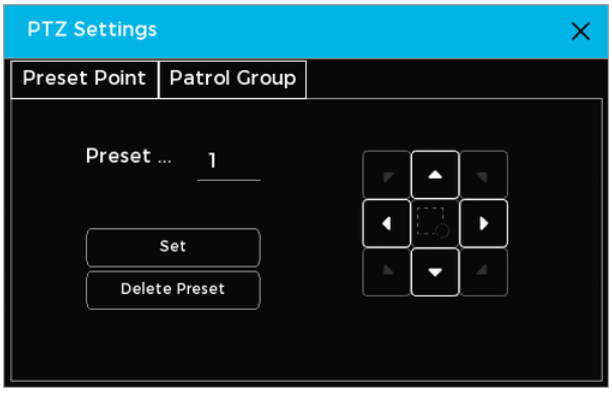
Parameter	Description
Step	Refers to the speed of movement for the PTZ. A greater value will result in a higher movement speed.
Zoom	Zoom In Zoom Out

Focus	Distance Focus Close-Up Focus
Iris	Make an image darker. Make an image brighter.
	Use this button to quickly position the PTZ. • **Position**: Click the icon and then select an area on the live page. The PTZ will adjust to center the selected area/point. • **Zoom**: Click the icon. Click and drag a square onto the area you would like to magnify. Drag the square upward to zoom out. Drag the square downward to zoom in. ⓘ A smaller square will result in higher magnification.
	Allows you to control the PTZ's direction manually using a mouse.
	Set a preset point to automatically adjust the PTZ to a specific position.
	Create patrol groups for automated camera movements.
	Configure preset points and patrol group settings.

Configuring PTZ Presets

Follow the steps below to configure PTZ presets.

1. Click on the PTZ control panel. Select Preset Point.
2. Use the arrows to move the camera to the desired position.
3. Assign a preset point number.
4. Click **Set** to save.



PTZ Presets

Configuring Patrol Groups

Follow the steps below to configure PTZ patrol group presets.

1. Click  on the PTZ control panel. Select Patrol Group.
2. Use the arrows to move the camera to the desired position.
3. Assign a patrol group number.
4. Assign a preset point number.
5. Click **Set** to save.

ⓘ A patrol group can include multiple preset points. To remove a preset, click **Delete Preset** if available (may not be available with some protocols).

Using PTZ Presets

Follow the steps below to use a PTZ preset.

1. Enter the preset number in the **Execute Box** on the PTZ control panel.
2. Click  to enable or disable the preset.

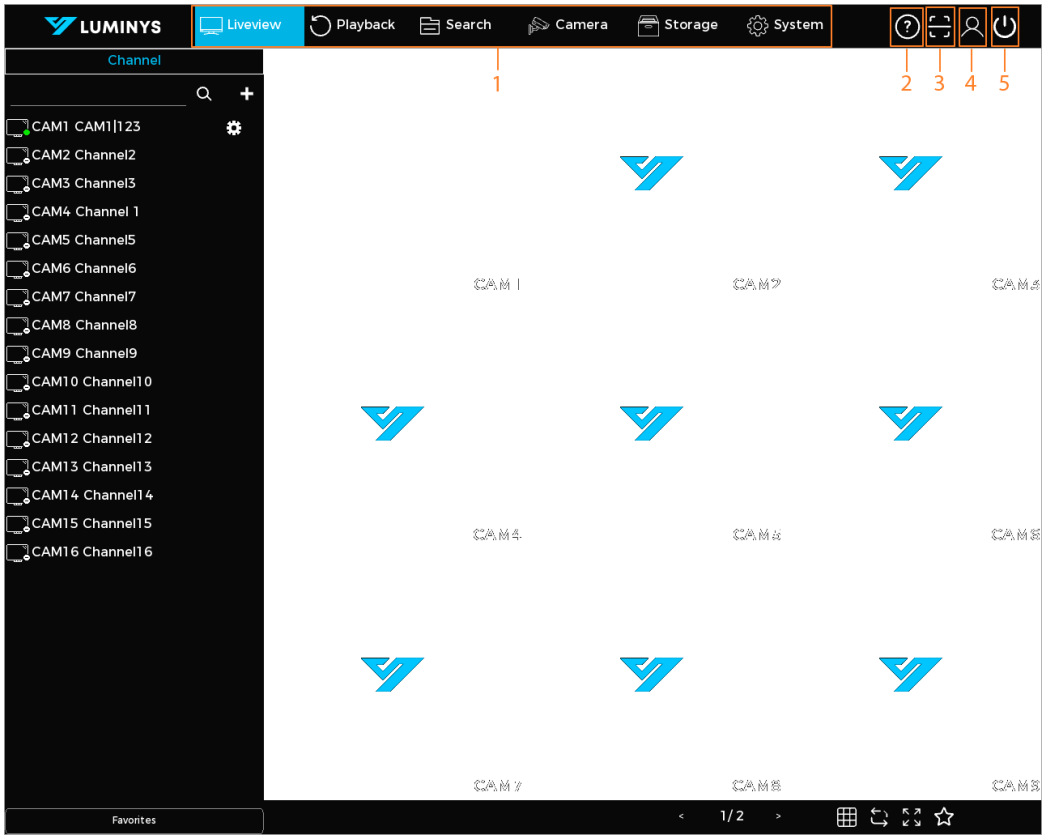
Using Patrol Groups

Follow the steps below to use a PTZ patrol group.

1. Enter the patrol group number in the **Execute Box** on the PTZ control panel.
2. Click  to enable or disable the patrol group.

Main Menu Tiles

The main menu tiles are located at the top of the Live View page after logging in.



Main Menu Icons

Number	Function	Description
1	Function Tiles	Click any tile to open the corresponding page.
2	Help	Scan the QR code to download the user manual.
3	Scan	Scan the QR code to download the mobile app or add your device for remote management.
4	Login	Log out of the current account and/or switch to a different user.
5	Power	Restart or shut down the device.

Playback

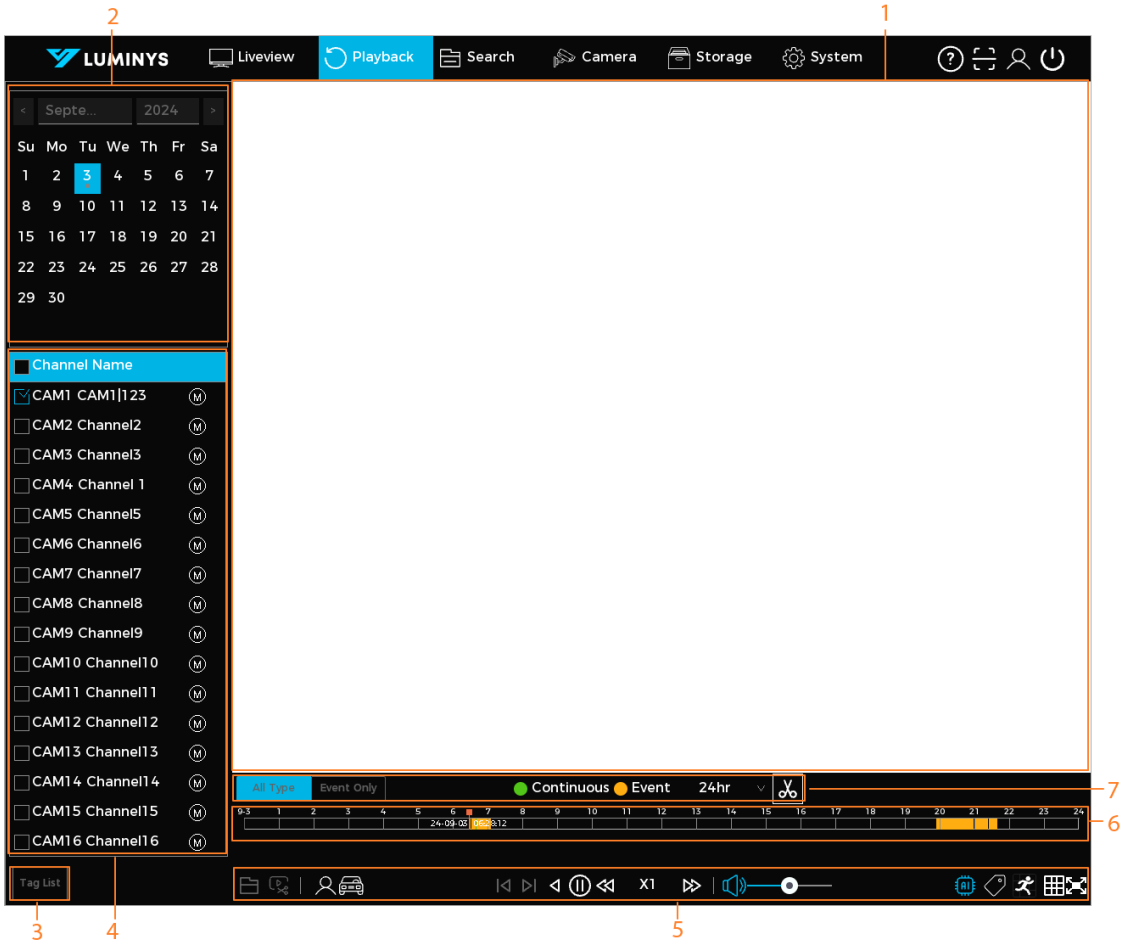
Instant Playback

Navigate to the live view control bar to playback up to 60 minutes of previously recorded footage. See **Live View Control Bar Parameters** for more information.

Playback Page

Click **Playback** from the main menu to display the playback page.

ⓘ The image is for reference only and may differ.



Playback Page

Number	Function	Description
1	Display Window	Plays back recorded video. Supports single-channel and multi-channel playback. ⓘ • The default viewing mode is single-channel playback. • Click the grid icon to alter the display window as needed. • You can zoom when in single-channel playback mode. Click and hold the area you would like magnified. Release to zoom into the selected area. Right-click to reset to the normal view.
2	Calendar	The calendar can be used to search using specific dates. ⓘ • The selected date will be highlighted. • Any available video will appear below the date after the search.
3	Tag List	View and manage any videos that have been tagged with specific search criteria.
4	Channel List	Select one or more channels to view playback videos. • The window layout is determined by the number of channels selected. Single-channel playback will display in single view, while two to four channels will be in split view. • Click  or  to toggle between the main and substream(s).
5	Playback Control Bars	See “Playback Controls” for detailed information.
6	Time Bar	Displays the type and time period of the recorded video. • Four-channel layouts will have four (4) time bars shown. Other layouts have one (1) time bar displayed. • Click the colored portion of the time bar to begin playback from a specific time. • Scroll or drag the bar to zoom or see a specific timeframe. • Click and hold the time bar. The mouse pointer will change to a hand icon. Drag to view the target time’s playback. • Move the vertical line on the time bar to rapidly view the video in I-frame format. • You can point to the time bar to show thumbnails of the current video (single-channel mode only).
7	Record Type	You can search based on the type of video recorded. • Selecting **Normal** displays all recordings. • Selecting **General Segments** will show video of when no event is detected (marked in green). • Selecting **Event Segments** will show video of when an event has been detected (marked in yellow).

	Time Bar Unit	Set the viewing period (24 hr., 2 hr., or 30 min.)
	Clip	Click the scissors icon to clip and save a video segment.

Playback Controls

The playback controls allow you to find and play videos, images, and video clips. Follow the steps below to begin video playback and use the playback controls.

ⓘ This section uses video playback as an example and is for reference only.

1. Click **Playback**. Select to play recordings from an external device.
2. Choose **Normal** or **Event** as the search criteria.
3. Choose the desired **date** and **channel** to search.
4. Click to select a playback time.

The system will begin to playback the selected video. The playback controls can be used to manage the viewing process.

Playback Controls

Icon	Description
	Play video from an external device. Click to return to the current playback mode.
	Split the recordings of a single day as required. You can display the split recordings on the display window. Click to return to the current playback mode.
	Use smart playback to display video based on target type (Human or Vehicle).
	Displays the previous or next frame. • Pause the video and click or to play video frame-by-frame. • Click to resume normal playback.
	Reverse playback button. • **Normal Mode**: Click the icon to rewind. • **Rewind Mode**: Click to resume normal playback.
	Click to begin playback. Click again to stop playback.
	Stop or pause current playback.
	Slow down playback speed. • **Normal Mode**: Click to reduce the playback speed. • **Sped-Up Mode**: Click to return to normal playback speed.
	Increase playback speed.

	• **Normal Mode**: Click to increase the playback speed. • **Sped-Up Mode**: Click to return to normal playback speed.
	Increase or decrease playback volume.
	Display or hide AI rules on the playback screen.
	Add a tag to the playback video for easy search and retrieval.
	Enable smart playback to focus on specific events (i.e., AI-detected activities).
	Choose the number of channels to display in the playback video (1, 4, 9, or 16).
	Switch to full-screen mode.

Quick Search

The Device can detect events within a defined segment of video. You can search for footage with events using Quick Search.

Prerequisites

Enable motion detection before using Quick Search by going to **Camera → Basic Event → Motion Detection**.

Procedure

Follow the steps below to use the Quick Search function.

1. Click **Playback** to access the playback interface.
2. Set search conditions. Play back the desired video channel. For details, see "**Playback Controls**."
3. Click  .
4. Define the detection area.
5. Click  to view video segments with detected motion.
6. Click  again to return to view all recordings.

ⓘ

- The motion detection area cannot be displayed full screen.
- Smart playback is only available when using single-channel playback. You must click on a specific channel use it if using Smart Channel
- When playing footage with motion detected, you cannot change the time bar unit nor do reverse or frame-by-frame playback.

Clip

The Clip feature allows you to save sections of video during playback to an external USB storage device. Follow the steps below to use this feature.

1. Click **Playback** to access the playback interface.
2. Set the search criteria. See "**Playback Controls**" for more information.
3. Use the time bar to set the start and end time. You can select the times by clicking .
4. Click to save the clip to the storage device.

Tag Playback

The Tag Playback feature allows you to mark a video with a tag for easy search and retrieval.

Adding a Tag

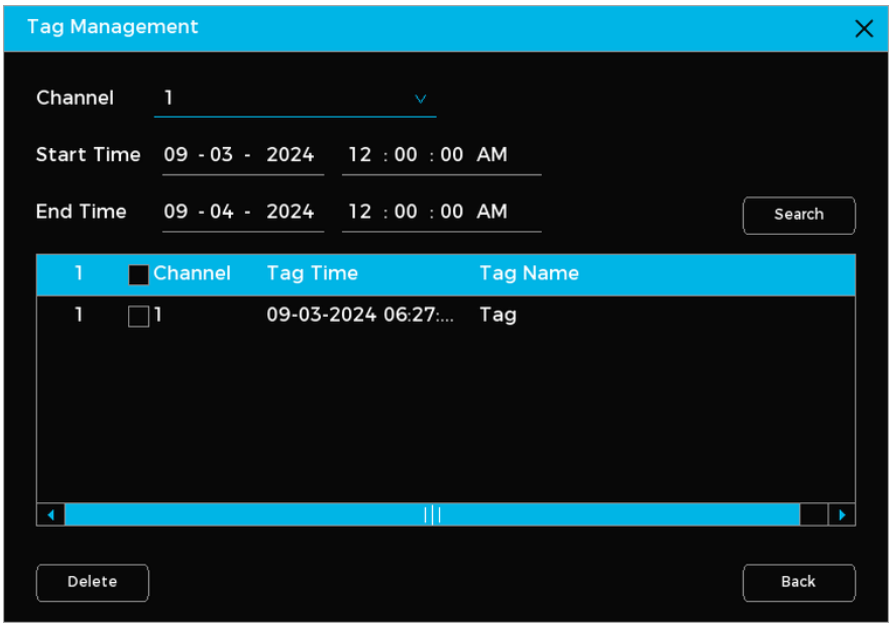
Click during playback to create a tag.

Playing Back a Video Based on Tags

During single-channel playback, click Tag List to display a list of tags created. Click the tag on the list to play back the associated video.

Managing Tags

Click to search, edit, and delete tags.



- **To search for tags**: Select the channel number. Enter the start and end time. Click **Search**.
- **To edit tags**: Double-click a tagged video and rename it.
- **To delete tags**: Select the tagged video(s) to be deleted. Click **Delete**.

File Search

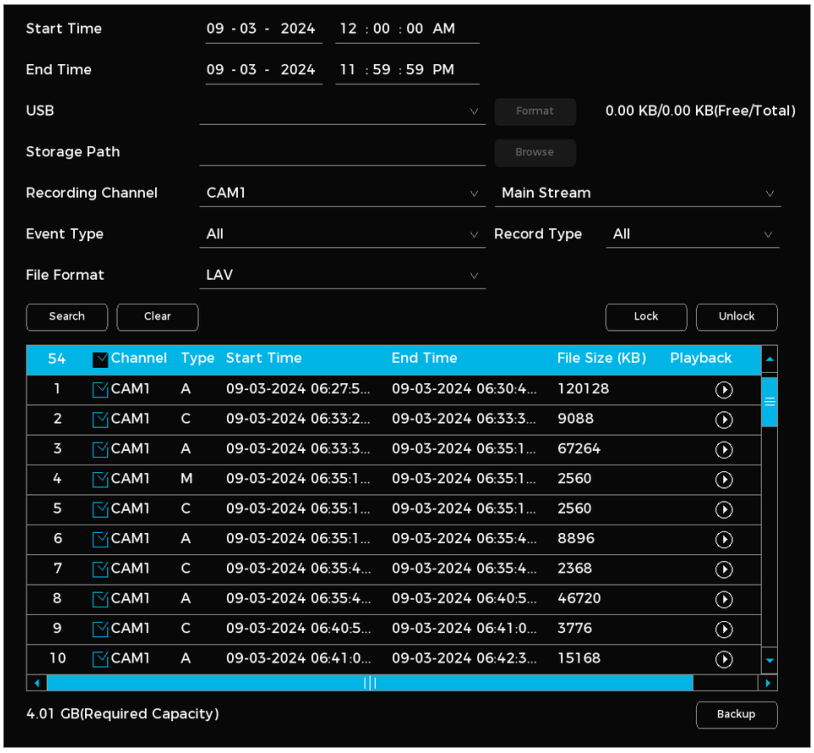
Searching for Video

Follow the steps below to search for video.

1. Navigate to **File Search → Video** from the main menu.
2. Set the search parameters (time, channel, event type). Click **Search**.
3. View the search results at the bottom of the page.

ⓘ

- Use the **Clear** button to reset the search field.
- You can back up any search results to a connect storage device.



Parameter	Description
Start Time End Time	Set the start and end time for the video search.
USB	Connect a USB device from the dropdown list. Click **Format** to format the USB if required.
Storage Path	Choose the storage path for the file.
Recording Channel	Select the channel to search. Choose Mainstream for HD footage or Substream for bandwidth-optimized footage.
Event Type	Filter the search by the following event types: • All • External Alarms • Motion Detection • Continuous Recording • VCA (Video Content Analytics)
Record Type	Select the record type as required (All or Lock).
File Format	Select the file format as required (LAV or MP4).

Related Operations

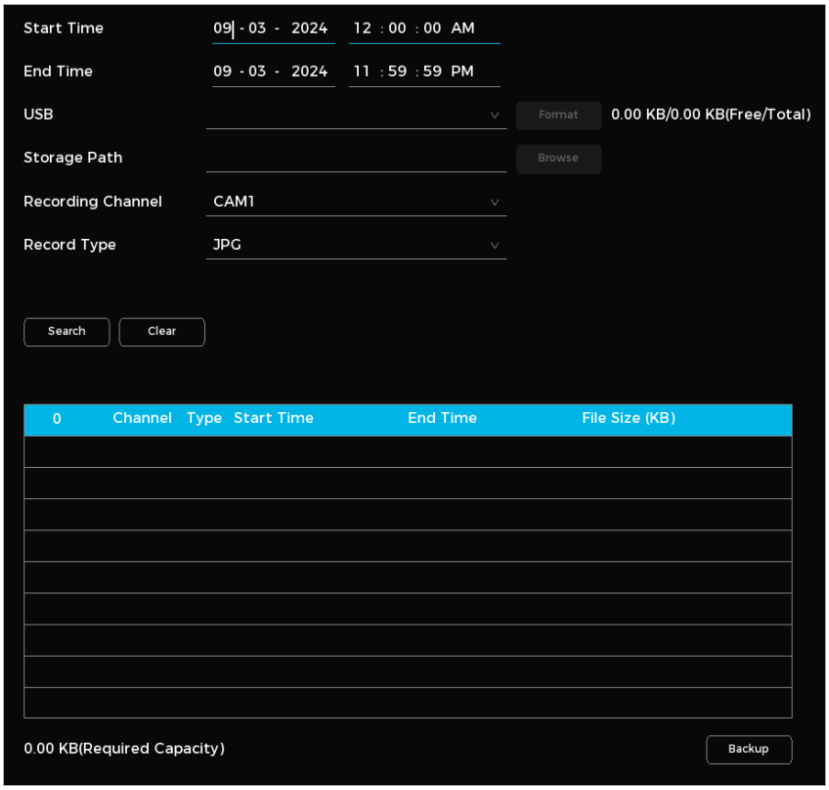
- Click **Lock** to lock selected recordings.
- Click **Unlock** to unlock selected recordings.

Searching for Images

Follow the steps below to search for images.

1. Navigate to **File Search → Picture**.
2. Set the search parameters. Click **Search.**
3. View the search results at the bottom of the page.

ⓘ Use the **Clear** button to reset the search field.



Parameter	Description
Start Time	Set the start and end time for the image search.
End Time	
USB	Connect a USB device from the dropdown list. Click **Format** to format the USB if required.
Storage Path	Choose the storage path for the file.
Recording Channel	Select the channel to search.
Record Type	Select the file format (only JPG is supported).

Smart Search

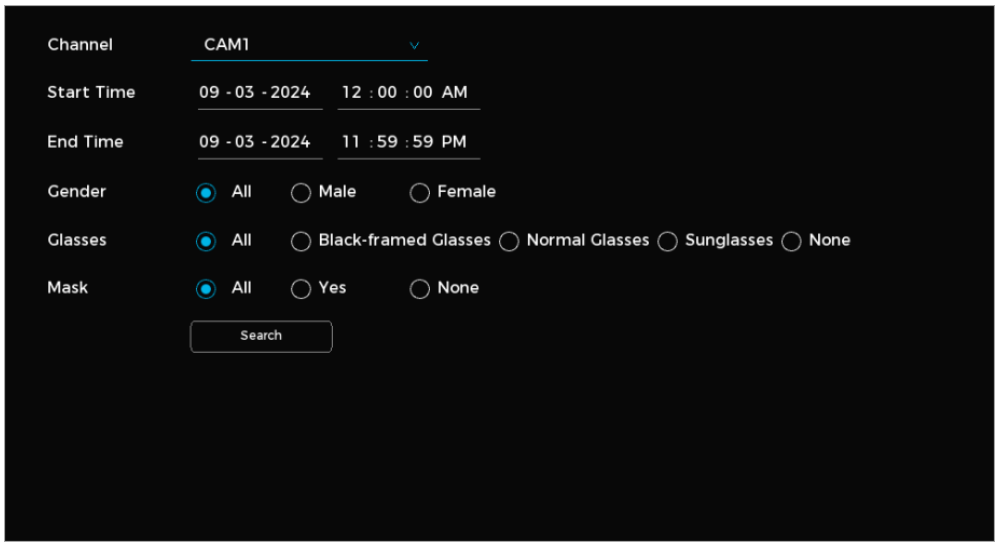
Face Search

Follow the steps below to search for and play back video with detected faces.

1. Navigate to **File Search → Smart Search → Face Search** from the main menu.
2. Select the channel to search, start and end time, and desired attributes.

- **Gender**: Male, Female, or All.
- **Glasses**: Black-Framed Glasses, Normal Glasses, Sunglasses, None, or All.
- **Mask**: Yes, No, or All.

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



Face Search

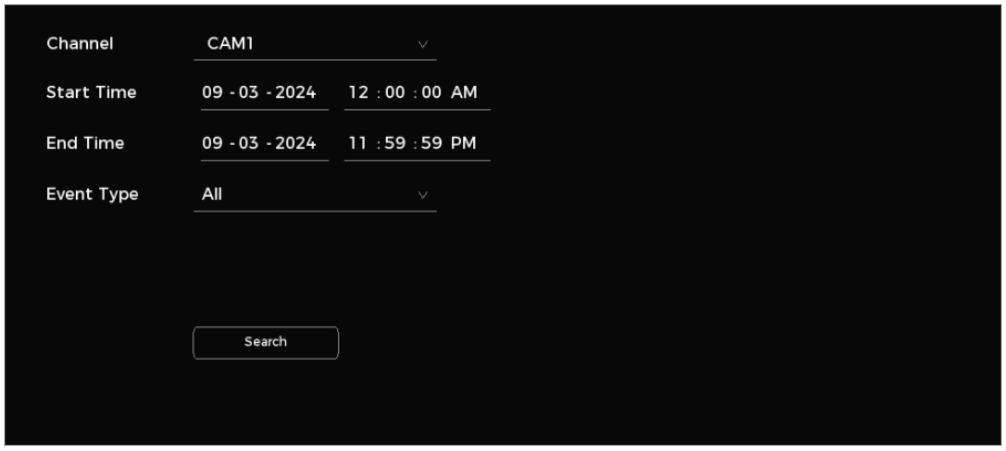
Related Operations

- **To play back footage**: Select an image. Click . You can double-click an image to switch between full-screen and thumbnail playback mode.
- **To sort video and images chronologically**: Click .
- **To export search results as an Excel document**: Click .
- **To back up a video or image**: Select one or more images. Click . Choose a storage path.
- **To add a tag to a video or image**: Select one or more images. Click .
- **To lock an image or video from being overwritten**: Select one or more images. Click .

Video Content Analytics (VCA) Search

Follow the steps below to search for and play back video with VCA events.

1. Navigate to **File Search → Smart Search → VCA Search** from the main menu.
2. Select which channel(s) to search from and the start and end time.
3. Select the event type.
4. Click **Search**.



VCA Search

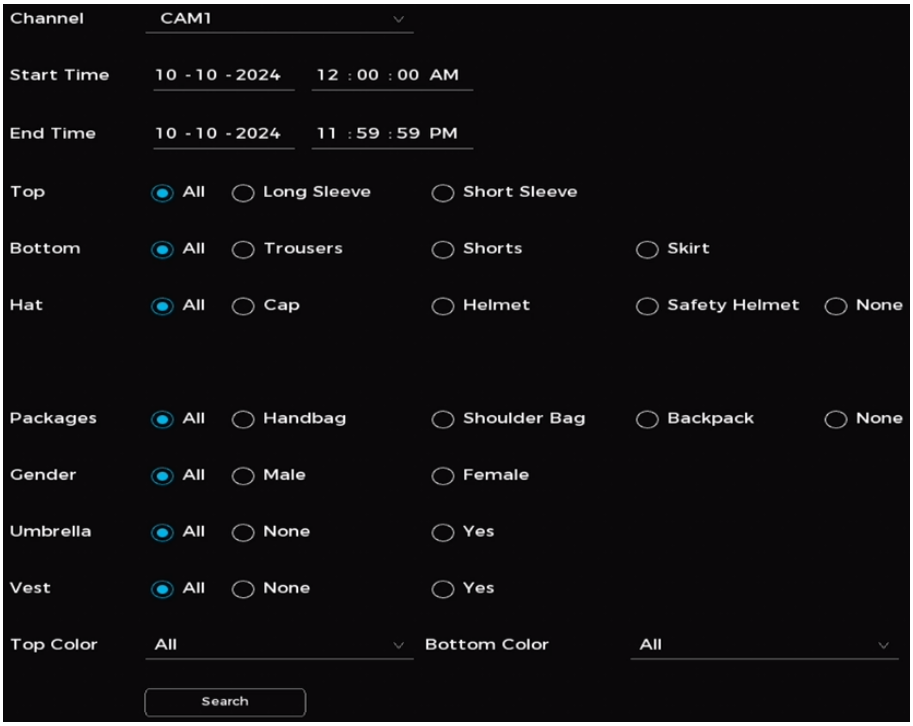
Related Operations

- **To play back footage**: Select an image. Click . You can double-click an image to switch between full-screen and thumbnail playback mode.
- **To sort video and images chronologically**: Click .
- **To export search results as an Excel document**: Click .
- **To back up a video or image**: Select one or more images. Click . Choose a storage path.
- **To add a tag to a video or image**: Select one or more images. Click .
- **To lock an image or video from being overwritten**: Select one or more images. Click .

Human Detection (R5 Models Only)

Follow the steps below to search through video using human detection.

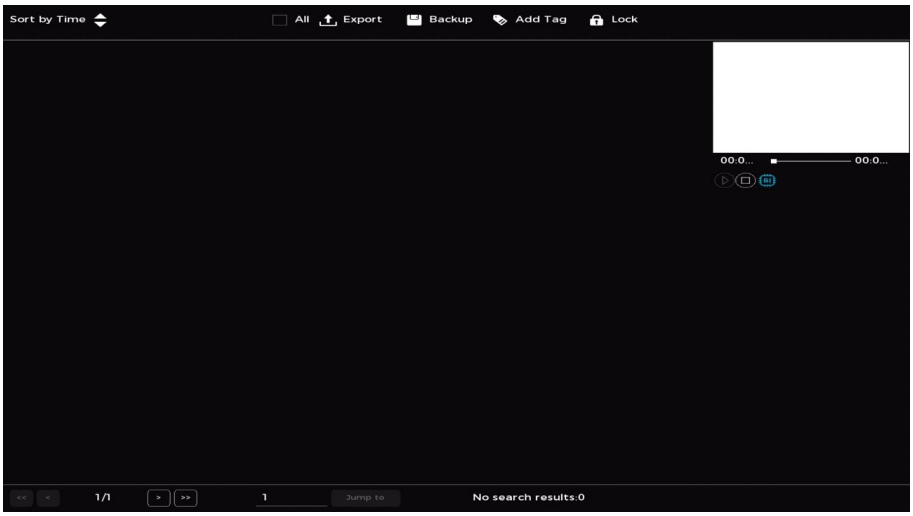
1. Navigate to **Search →Smart Search → Human Detection**.



Human Detection

2. Select a channel (single channel, multiple channels, all channels). Set the start and end time.
3. Set the parameters as required.
4. Click **Search**.

ⓘ Faces will be blurred for privacy protection.



Search Results Page

Related Operations

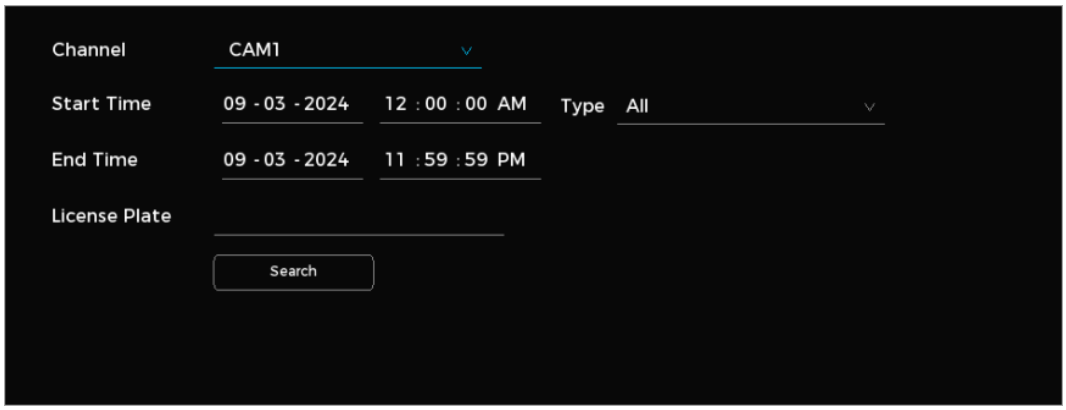
- **To play back footage**: Select an image. Click  . You can double-click an image to switch between full-screen and thumbnail playback mode.
- **To sort video and images chronologically**: Click  .
- **To export search results as an Excel document**: Click  .

- **To back up a video or image**: Select one or more images. Click . Choose a storage path.
- **To add a tag to a video or image**: Select one or more images. Click .
- **To lock an image or video from being overwritten**: Select one or more images. Click .

License Plate Recognition (LPR) Search

Follow the steps below to search for license plate results.

1. Navigate to **File Search → Smart Search → LPR Search** from the main menu.
2. Select a channel (one channel, multiple channels, all channels) and a target type (Allowlist, Blocklist, Standard, All).
3. Set the start and end time for the search.
4. Click **Search** to display the results.



LPR Search

Related Operations

- **To play back footage**: Select an image. Click . You can double-click an image to switch between full-screen and thumbnail playback mode.
- **To sort video and images chronologically**: Click .
- **To export search results as an Excel document**: Click .
- **To back up a video or image**: Select one or more images. Click . Choose a storage path.
- **To add a tag to a video or image**: Select one or more images. Click .
- **To lock an image or video from being overwritten**: Select one or more images. Click .

Intelligent Motion Detection (iMD) Search

Follow the steps below to use the iMD Search feature to find videos with motion detection events.

1. Navigate to **File Search → Smart Search → iMD Search** from the main menu.
2. Select a channel (single channel, multiple channels, all channels) and choose a target type (All, Human, Vehicle).
3. Set the start and end time for the search.
4. Click **Search** to display the results.

iMD Search

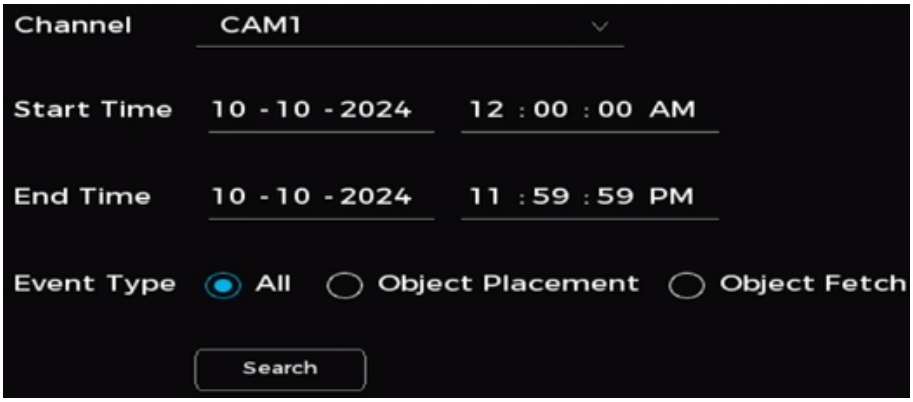
Related Operations

- **To play back video**: Select an event. Click  .
- **To back up video**: Select one or more events. Click **Backup**. Choose a storage path.

Object Monitoring (R5 Models Only)

Follow the steps below to find videos with object monitoring events.

1. Navigate to **Search →Smart Search → Object Monitoring**.



Object Monitoring

2. Select a channel (single channel, multiple channels, all channels). Set the start and end time.
3. Choose between two event types: **Object Placement** (an item is removed from the monitoring area) or **Object Fetch** (an item is placed in the monitoring area).
4. Click **Search**.

Related Operations

- **To play back footage**: Select an image. Click  . You can double-click an image to switch between full-screen and thumbnail playback mode.
- **To sort video and images chronologically**: Click  .
- **To export search results as an Excel document**: Click  .
- **To back up a video or image**: Select one or more images. Click  . Choose a storage path.
- **To add a tag to a video or image**: Select one or more images. Click  .
- **To lock an image or video from being overwritten**: Select one or more images. Click  .

Camera

Configuring Remote Devices

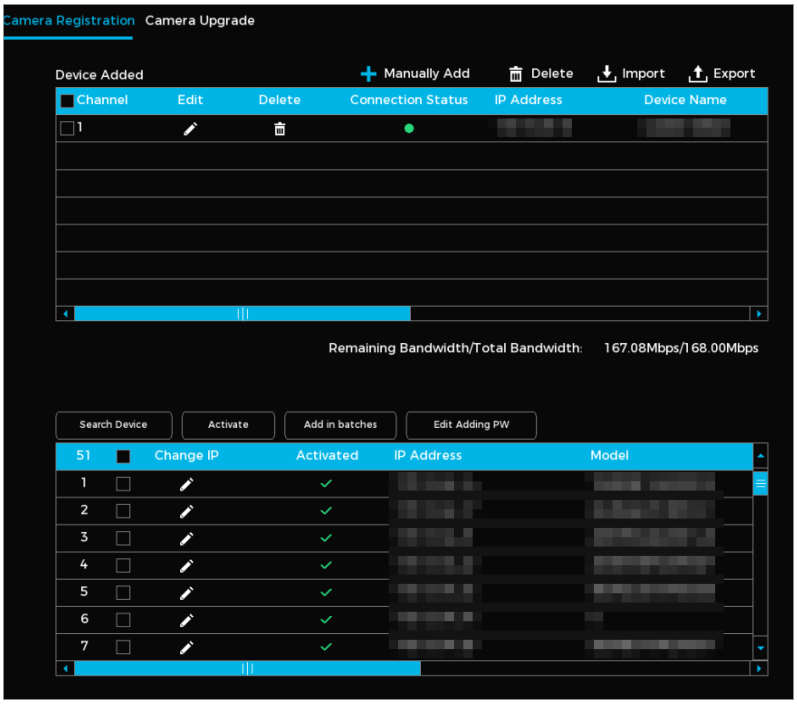
Add remote devices to receive, store, and manage video from connected cameras.

Adding a Remote Device From Search

You can add a remote device by searching for it if the device is on the same network as the NVR. This method is best when the specific IP address of the remote device is unknown and to simplify device discovery and connection.

Follow the steps below to add a remote device from search.

1. Navigate to **Camera → Camera Registration → Camera Registration**.
2. Click Search Device.
3. Select one or more devices from the search results. Click **Add in Batches**. Added devices will appear in the **Devices Added** list.



Related Operations

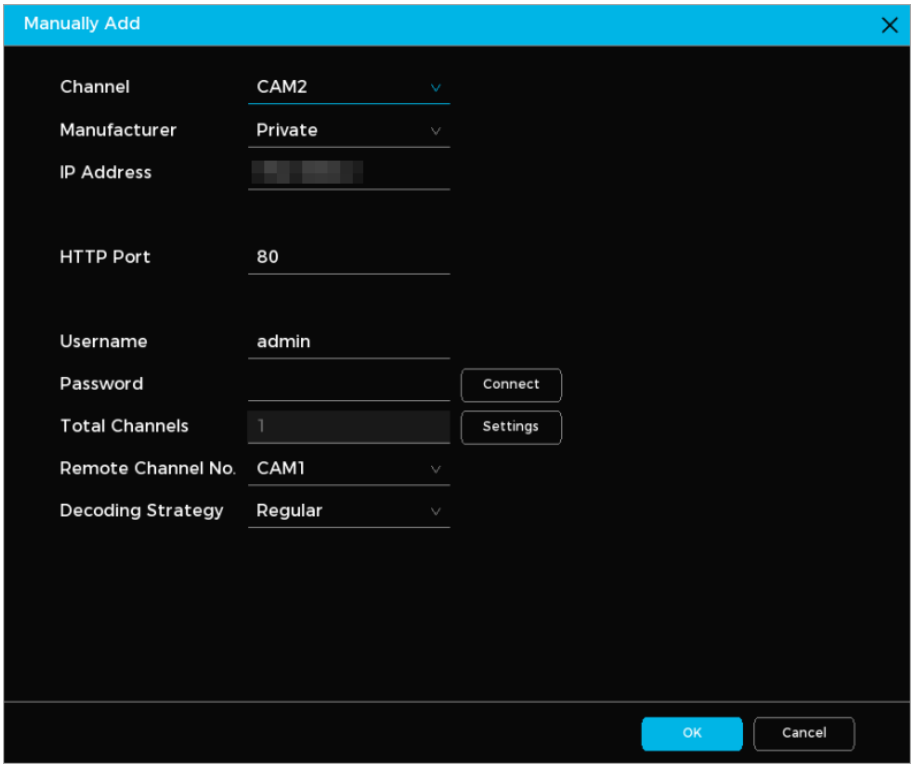
- **To change a device's IP address**: Click  to edit the device's IP address.
- Select **DHCP** to automatically assign the device's IP address, subnet mask, and default gateway.
- Select **Static** to manually configure the device's IP address, subnet mask, and default gateway.
- **To change the IP addresses of multiple devices simultaneously**: Enter an incremental value. The system will automatically adjust the fourth decimal digit of the IP address in sequential order.
- The system notifies you of IP conflicts when modifying a single device's address. If conflicts occur during bulk updates, it automatically skips conflicting addresses and assigns new ones incrementally based on the specified value.

Adding Remote Devices Manually

You can add a remote device manually by inputting its IP address, username, password, and other relevant details. This method is best if there are a small number of remote devices to add with their IP addresses, usernames, and passwords already set.

Follow the steps below to add a device manually.

1. Navigate to Camera → Camera Registration → Camera Registration.
2. Click  .
3. Configure the parameters (see the table below).
4. Click **OK** when done.



Manual Add Parameters

Parameter	Description
Channel	Assign the device to a channel.
Manufacturer	Input the device manufacturer.
IP Address	Enter the device's IP address.
HTTP Port	Enter the device's HTTP port number.
Username	Enter the device username.
Password	Enter the device password.
Total Channels	Enter the total number of channels available on the device.
Remote Channel No.	Connect one or more remote channels.
Decoding Strategy	Choose real-time, regular, or smooth decoding.
Encrypt	Select automatic, TCP, UDP, or multicast encryption.

Related Operations

- To modify device parameters: Click  .
- To delete a device: Click  .
- To change the device login password: Click Edit Adding PW to update the camera login password.

Importing Remote Devices

To import remote devices, connect a USB storage device to the system. This method works best when adding multiple devices with different IP addresses, usernames, and passwords.

Follow the steps below to import remote devices from a USB storage device.

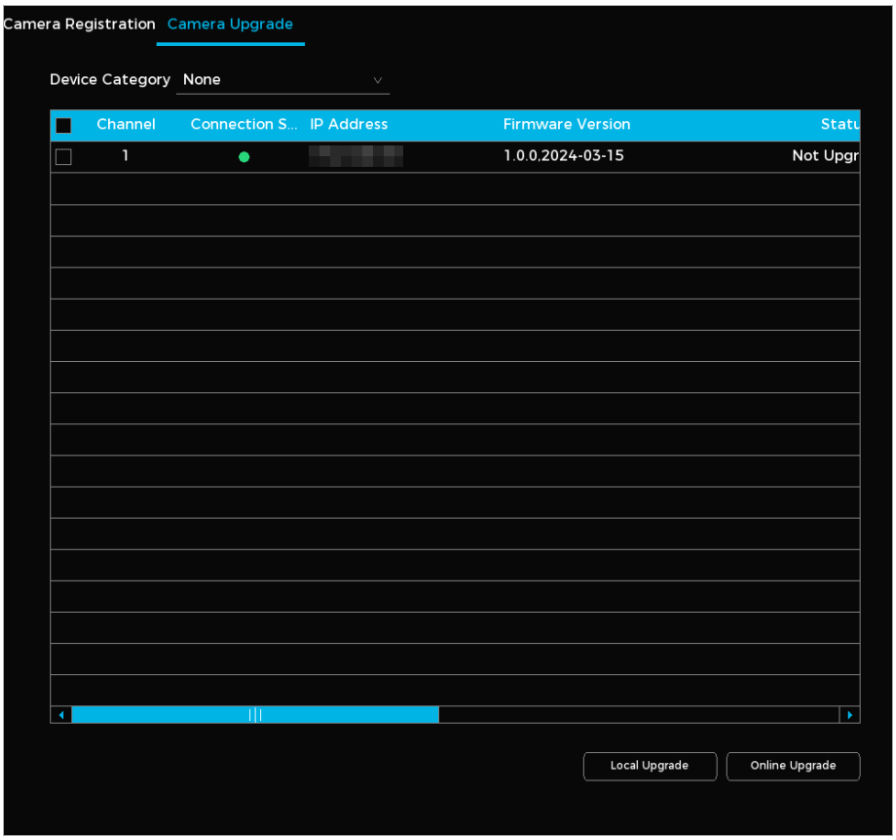
1. Navigate to Camera → Camera Registration.
2. Click . This will export the template to enter device information.

ⓘ You must disable backup encryption before exporting the template.

3. Fill in the template.
4. Import the template by clicking .
5. Click **OK**.

Upgrading Remote Devices

Go to **Camera → Camera Registration → Camera Update** to upgrade the firmware or settings of connected remote devices. You can update devices locally or online.



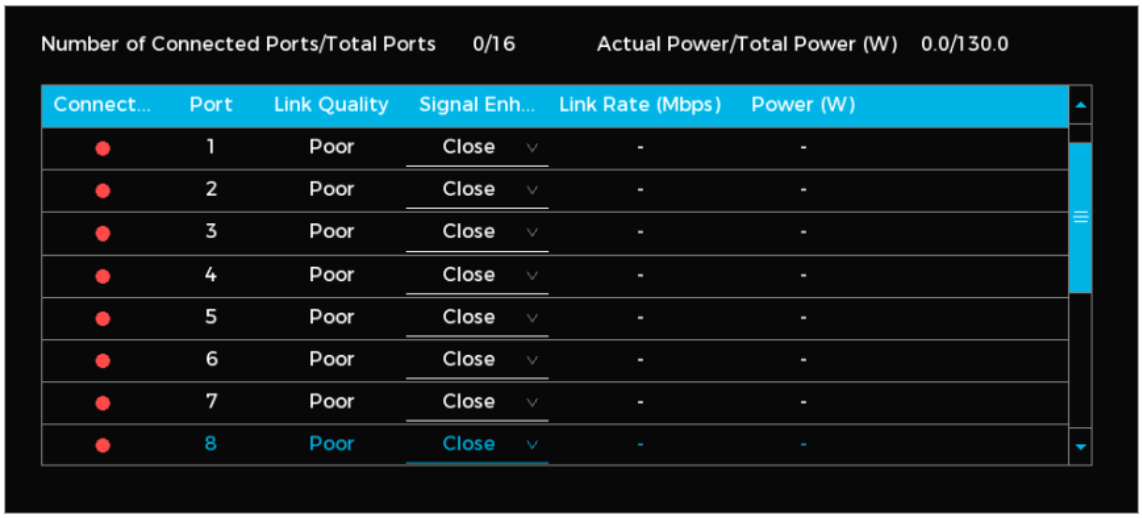
Camera Upgrade Page

- **To update locally**: Connect a USB storage device with the update to the system. Choose the devices to update. Click **Local Upgrade**. Select the update file to begin updating.
- **To update online**: Select the devices to update. Click **Online Upgrade**.

ⓘ Click **Device Category** to filter remote devices for easier selection.

Checking PoE Port Status

To check the status of PoE ports, navigate to **Camera → PoE**. You can turn signal enhancement mode on and off as needed.



PoE Port Status

Configuring Switch Operation Mode

After setting the switch operation mode, the system automatically assigns an IP address to any IP camera connected to a PoE port, aligning it with the designated IP segment for seamless connection.

Before configuring switch operation mode, ensure the following prerequisites are met:

- Only NVRs with PoE ports support this feature.
- Do not connect a PoE port to an external switch to prevent connection failure.
- Switch Operation Mode is enabled by default. It is not recommended to change the default settings.
- When using third-party equipment, ensure ONVIF protocols are supported and DHCP is enabled.

Follow the steps below to configure switch operation mode.

1. Navigate to **Camera → PoE**.
2. Select **Route** (default) or **Bridge** in **Mode** as required.
3. Configure the IP address, subnet mask, and default gateway. Do not set the IP address on the same network segment as the Device. It is recommended to use the default setting.

ⓘ You cannot set these parameters in Bridge mode.

4. Click **Apply**.

Configuring Image Attributes

You can adjust image parameters such as contrast, brightness, and saturation. Follow the steps below to enable configuring image attributes.

1. Navigate to Camera → Image Attributes.
2. Select a channel to configure image attributes.
3. Click **Apply** when done.

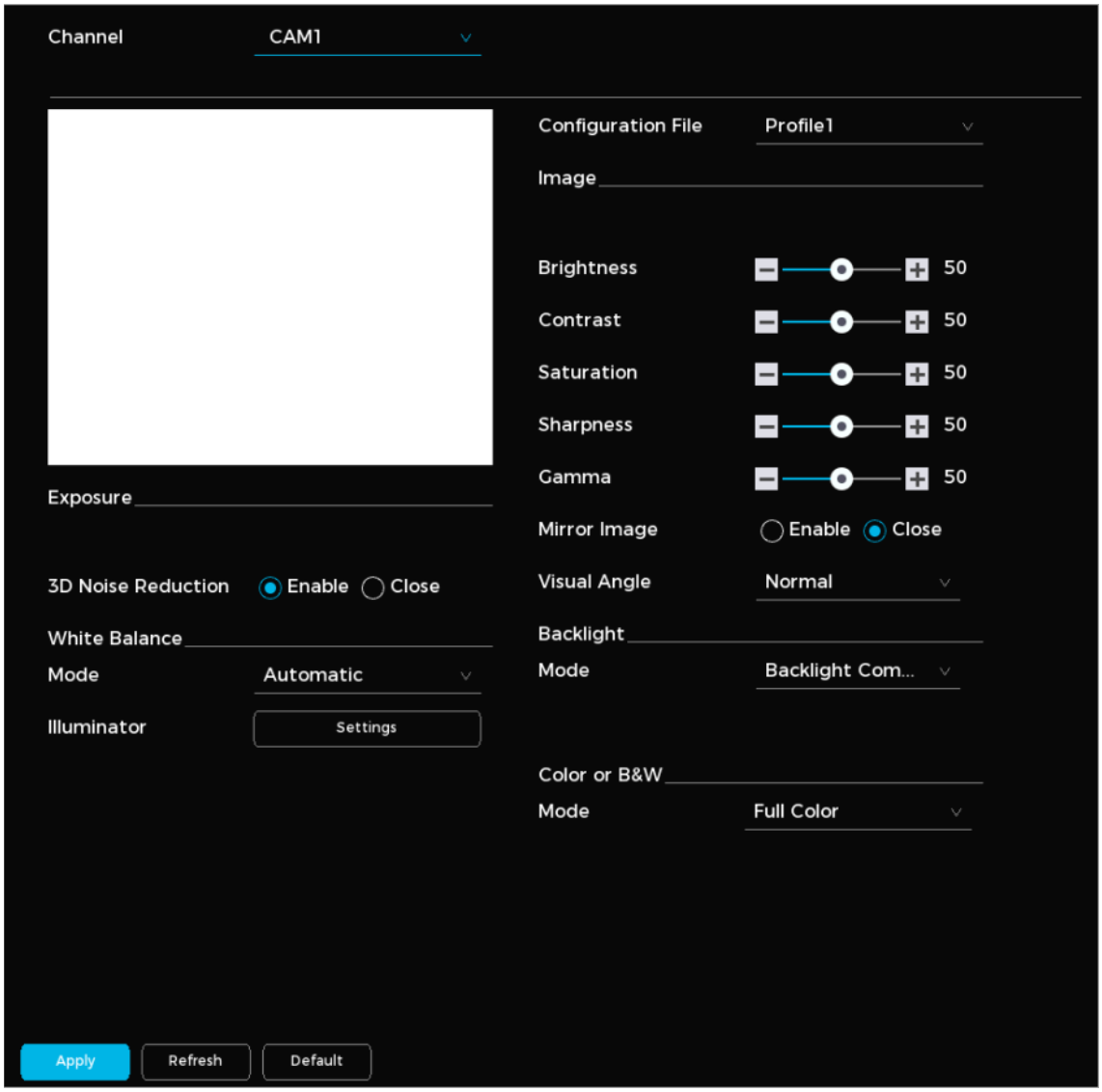


Image Attributes

Parameter	Description
Configuration File	Select a configuration file. Attributes may vary based on file.
Brightness	Adjust the brightness of an image. Higher values result in a brighter image.
Contrast	Enhance the contrast between light and dark areas. Higher values result in more contrast.
Saturation	Control the color intensity of an image. Higher values result in more vivid colors.
Sharpness	Enhance the image edges. Higher values make the edges more distinct.
Gamma	Change the brightness and dynamic display range of an image. Higher values result in a brighter image.
Mirror Image	Flip an image (only available on select models).
Visual Angle	Set which direction the video displays.

Backlight Mode	• **Close**: Turn off backlight mode. • **Backlight Compensation**: Clarifies dark areas when shooting against light. • **Wide Dynamic Range (WDR)**: Balances brightness and enhances darker areas. • **Highlight Compensation**: Reduces halo effects when filming in extremely strong light.
3D Noise Reduction	Reduces noise in between frames.
White Balance Mode	Adjusts overall hue of images to accurately reproduce colors (varies by camera model).
Day and Night Modes	Switch between full-color or black-and-white images depending on lighting conditions. • **Automatic**: Changes mode based on lighting conditions. • **Full Color**: Produces color images only. • **Black and White**: Products monochrome images only.
Illuminator	Control brightness and clarity in low-light environments. • **Automatic**: Adjusts brightness and clarity automatically. • **Manual**: Manually adjust brightness and clarity. • **Close**: Turns off the built-in illuminator.

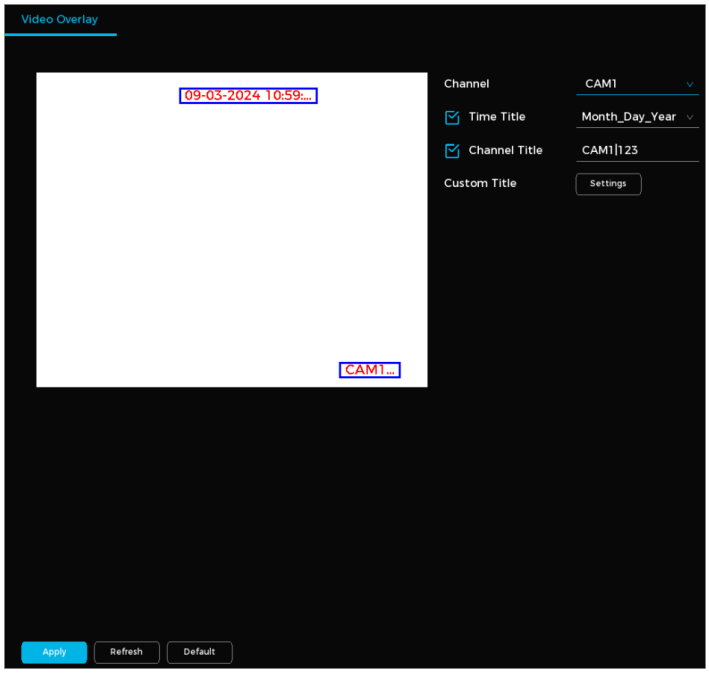
Configuring Overlay Settings

Follow the steps below to configure the image overlay settings.

1. Navigate to Camera → Video Overlay.
2. Select a channel.
3. Configure time title, by enabling and setting the desired time format.
4. Configure the channel title, by enabling and setting the channel name.

ⓘ Click **Settings** to next to **Custom Title** for more customization on the overlay information.

5. Click **Apply** when done.



Video Overlay Information

Configuring Privacy Masking

You can mask part of the image for privacy reasons. Follow the steps below to enable privacy masking.

1. Navigate to Camera → Privacy Masking.
2. Select a channel.
3. Click  to enable the feature.
4. Click 1, 2, 3, or 4 to add the mask.
5. Adjust the size and portion of the mask(s) as needed.
6. Click **Apply** when done.

Configuring Video Settings

You can configure the video encoding settings based on actual bandwidth.

1. Navigate to Camera → Video Parameters.
2. Configure the video encoding parameters.
3. Click **Apply** when done.

Video Setting Parameters

Parameter	Description
Channel	Select which channels to configure settings for.
Smart Encoding	Reduces bit stream for non-essential recording to maximize storage space.
Record Type	Select **Normal**, **Motion Detection**, or **Alarm** for the mainstream.

Encoding Mode	• H.265 (Recommended): Main profile encoding offers enhanced compression, minimizing storage and bandwidth usage. • H.264H: High-profile encoding provides superior quality and compression efficiency compared to standard H.264. • H.264: General profile encoding for broader compatibility. • H.264B: Baseline profile encoding for low-latency or low-complexity scenarios. • MJPEG: High bitrate encoding best suited for static scenes or scenarios requiring frame-by-frame clarity.
Resolution	Select the recording resolution. The maximum possible resolution will depend on device model.
Frame Rate (FPS)	Change FPS based on application. Higher FPS provides smoother, clearer images but require more bandwidth.
Bitrate Type	• **CBR (Constant Bitrate)**: Maintains a constant bitrate; best suited for environments with minimal movement. • **VBR (Variable Bitrate)**: Adjusts bitrate based on activity; best suited for high-traffic environments.
Image Quality	A higher value will result in better image quality. (Only available with VBR)
I-Frame Interval	Refers to the time between two reference frames. A higher interval will reduce file size but reduce image quality.
Bit Rate (Kb/S)	• **Mainstream**: Better image quality with higher bitrates. • **Substream**: Constant stream will result in the bitrate fluctuating close to the specified value; when the stream is variable, the bitrate fluctuates with the image but stays close to the maximum specified value.
Audio Encoding	Choose the desired audio encoding format.
Sampling Rate	Adjust how frequently audio is sampled. A higher value will improve quality but require more bandwidth.

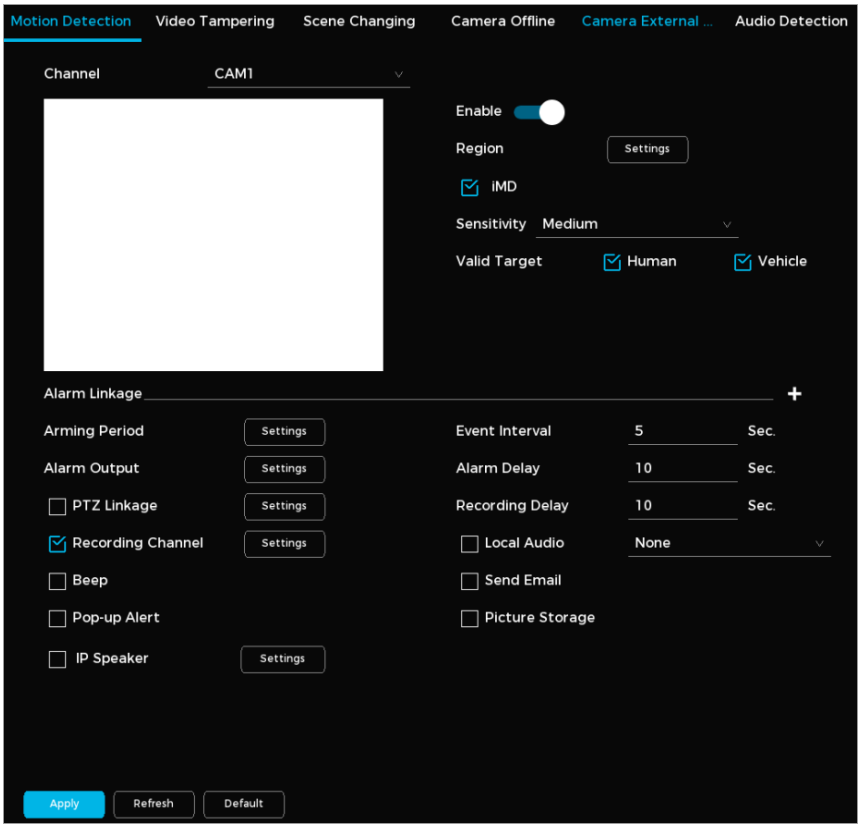
Configuring Basic Event Alarms

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

Set a Motion Detection Alarm

Follow the steps below to set an alarm for when an object moves quickly enough to exceed the defined sensitivity threshold.

1. Navigate to Camera → Basic Event → Motion Detection.



Motion Detection Alarm Parameters

2. Select a channel.
3. Click to enable the alarm.
4. Click **Settings** next to **Region** to set the detection area.
5. Point to the middle-top of the page for configuration.
6. Set the region name.
7. Set the motion detection sensitivity. A higher value will create a greater chance of false alarms.
8. Set the threshold. This refers to the required percentage of the detected target area to trigger an alarm. The alarm activates when this threshold is met or exceeded.

   ⓘ You can set up four detection regions. An alarm will be triggered if motion is detected in any of the four regions.
9. Select the checkbox next to iMD. Adjust the sensitivity and choose a target type (human or vehicle).

ⓘ Higher sensitivity may result in more false alarms. When iMD is enabled, only human or vehicle movements will be detected and trigger an alarm.

10. Configure the other following parameters.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage.

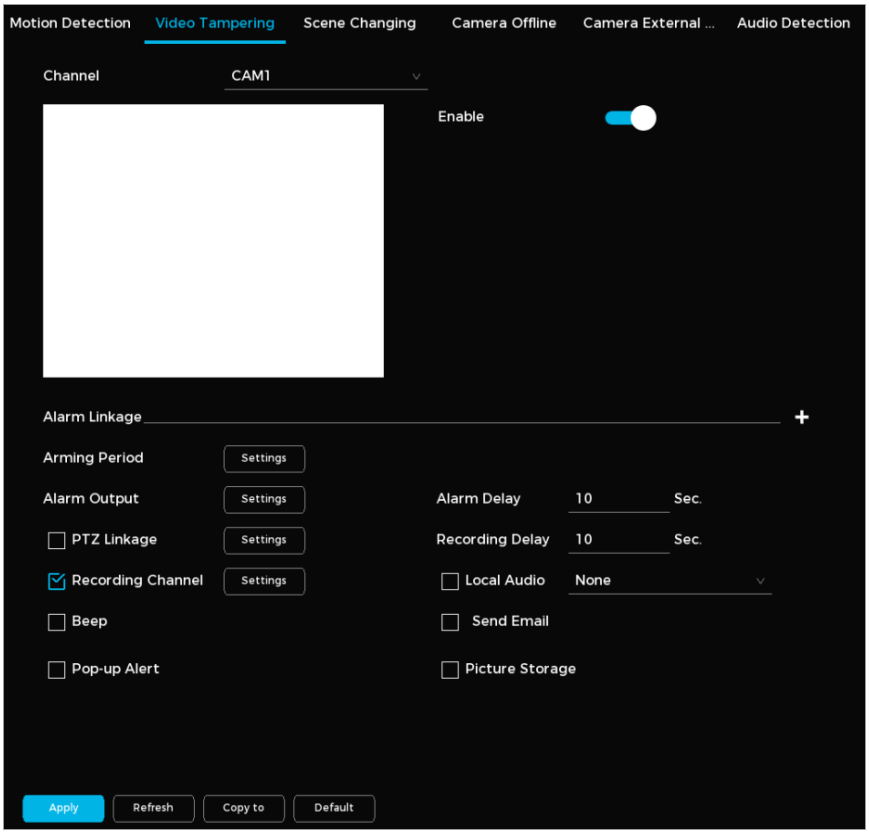
	ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

11. Click **Apply** when done.

Set a Video Tampering Alarm

Video tampering happens when the camera lens is blocked, or the footage appears in a single color due to lighting or other factors. Follow the steps below to set alarms for video tampering.

1. Navigate to Camera → Basic Event → Video Tampering.



Video Tampering Alarm Parameters

2. Select a channel.
3. Click to enable the alarm.
4. Configure the following parameters.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.

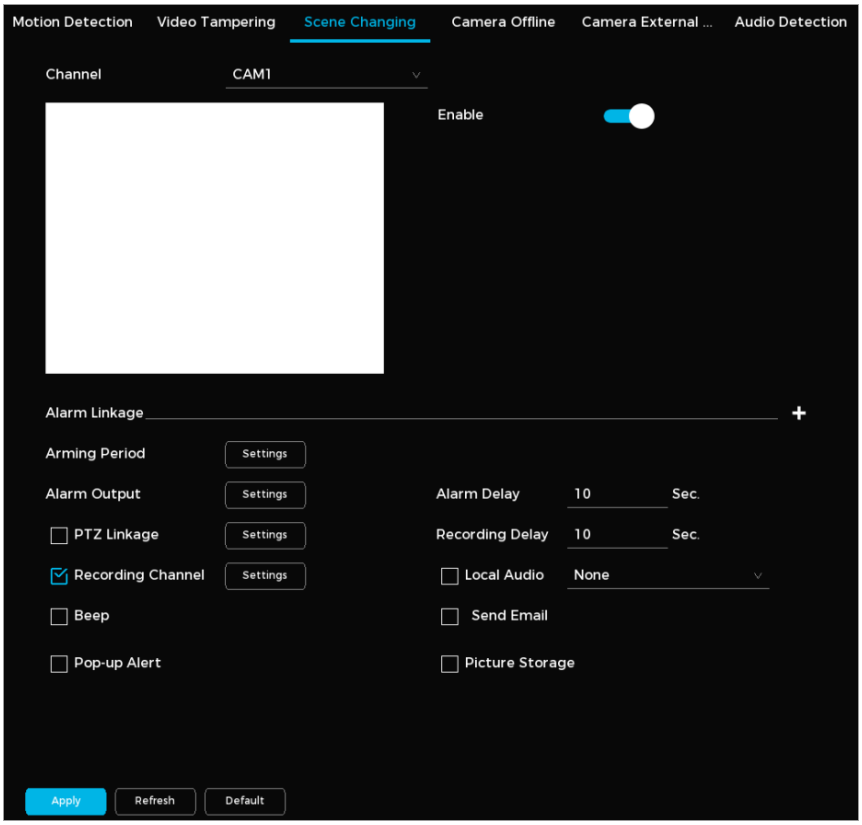
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

5. Click **Apply** when done.

Set a Scene Change Alarm

Follow the steps below to set an alarm when a scene change is detected.

1. Navigate to System → Events → Video Detection → Scene Changing.



Scene Changing Alarm Parameters

2. Select a channel.
3. Click  to enable the alarm.
4. Set the following parameters: **Arming Period**, **Alarm Output**, **PTZ Linkage**, and **Recording Channel**. See the table below for more details.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.

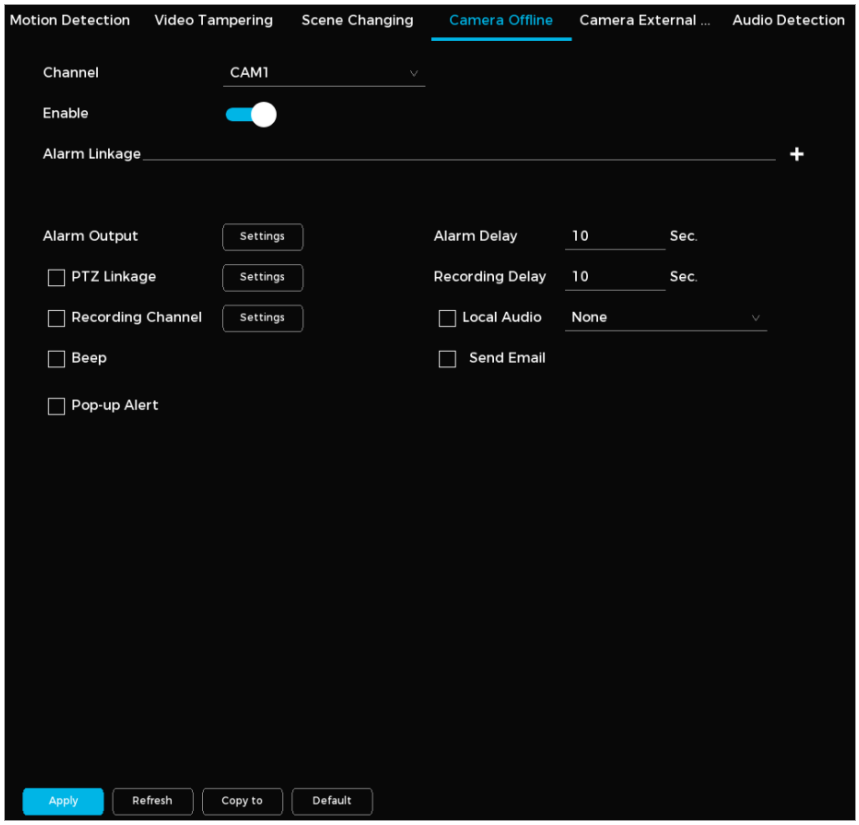
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

5. Click **Apply** when done.

Set an Alarm for When a Camera Goes Offline

Follow the steps below to set an alarm to trigger when the camera goes offline.

1. Navigate to Camera → Basic Event → Camera Offline.



Camera Offline Alarm Parameters

2. Select a channel.
3. Click to enable the alarm.
4. Set the following parameters: **Alarm Output**, **PTZ Linkage**, **Recording Channel**, **Beep**, and **Pop-Up Alert**. See the table below for more details.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.

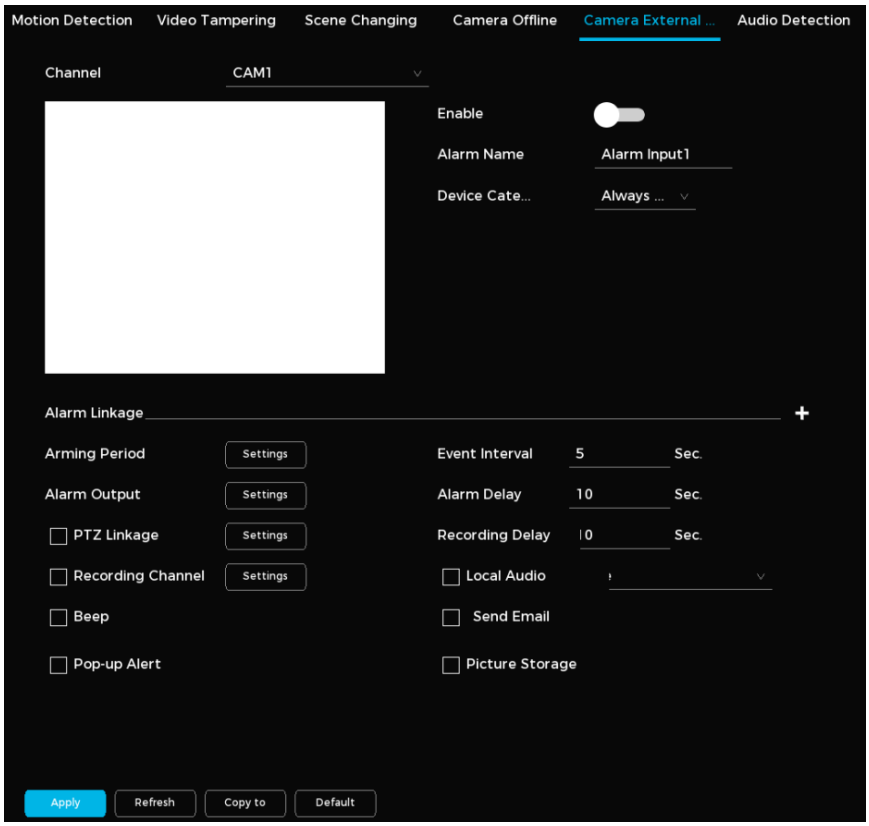
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

5. Click **Apply** when done.

Configure an External Alarm Device

When an external alarm device is triggered, the system receives the signal and activates linked alarm actions. Follow the steps below to configure an external camera alarm.

1. Navigate to **Camera → Basic Event → Camera Offline**.



External Alarm Parameters

2. Select a channel and alarm name.
3. Click to enable the alarm.
4. Choose **Always Open** or **Always Closed** for the device category.
5. Configure other parameters. See the table below for more details and information.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.

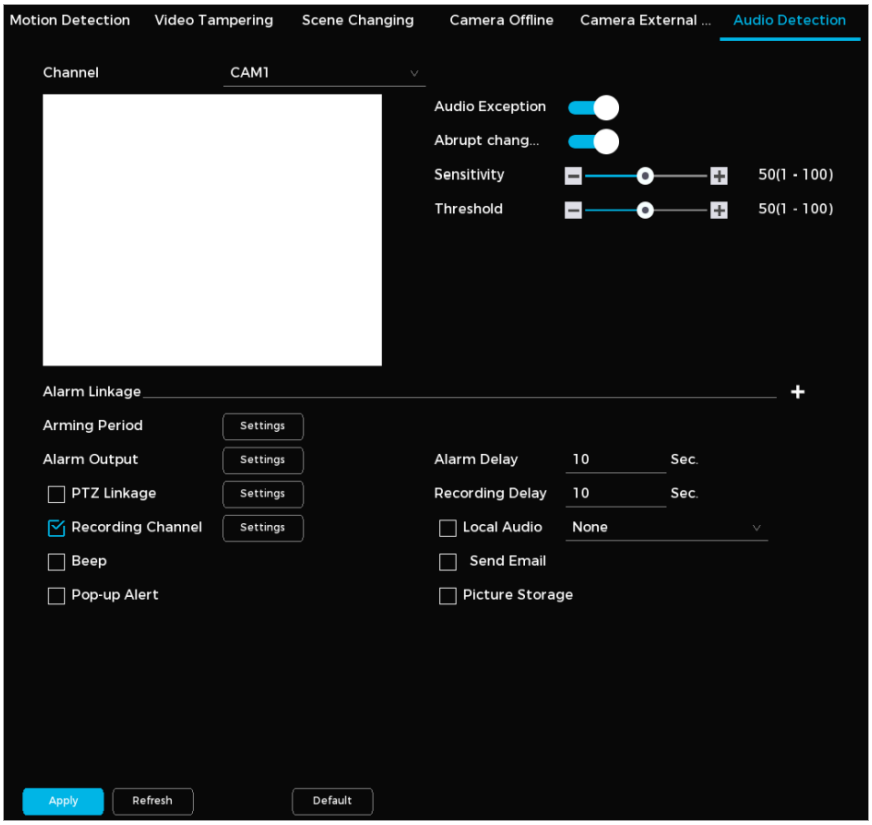
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

6. Click **Apply** when done.

Configure an Audio Detection Alarm

You can set an alarm to trigger when the system detects audio abnormalities, tone changes, or significant volume fluctuations. Follow the steps below to configure an audio detection alarm.

1. Navigate to Camera → Basic Event → Audio Detection.



Audio Detection Alarm Parameters

2. Select a channel.
3. Click to enable detecting audio exceptions (abnormal audio output) and volume changes.

ⓘ Audio exceptions refer to any audio input the system considers abnormal. Volume change alerts are based on the user-defined sensitivity and threshold.

4. Adjust other settings such as Alarm Linkage, Alarm Output, and Recording Channels. See the table below for more details and information on these parameters.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.

Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

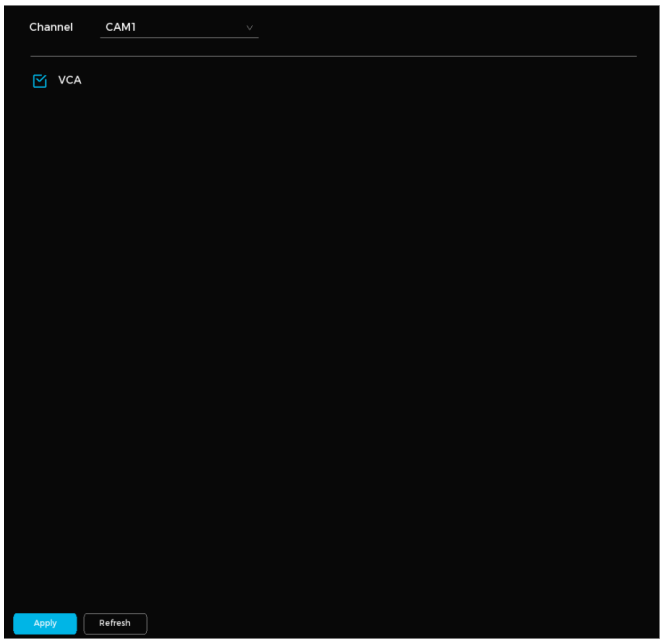
5. Click **Apply** when done.

Configuring AI Events

Enable Intelligent Mode

You must enable Intelligent Mode to use features like face detection, VCA, and other smart functions on network cameras. Follow the steps below to enable intelligent mode.

1. Navigate to Camera → AI Event → Intelligent Mode.
2. Select a channel. The system will display the available intelligent functions for the connected camera.



Intelligent Mode Screen

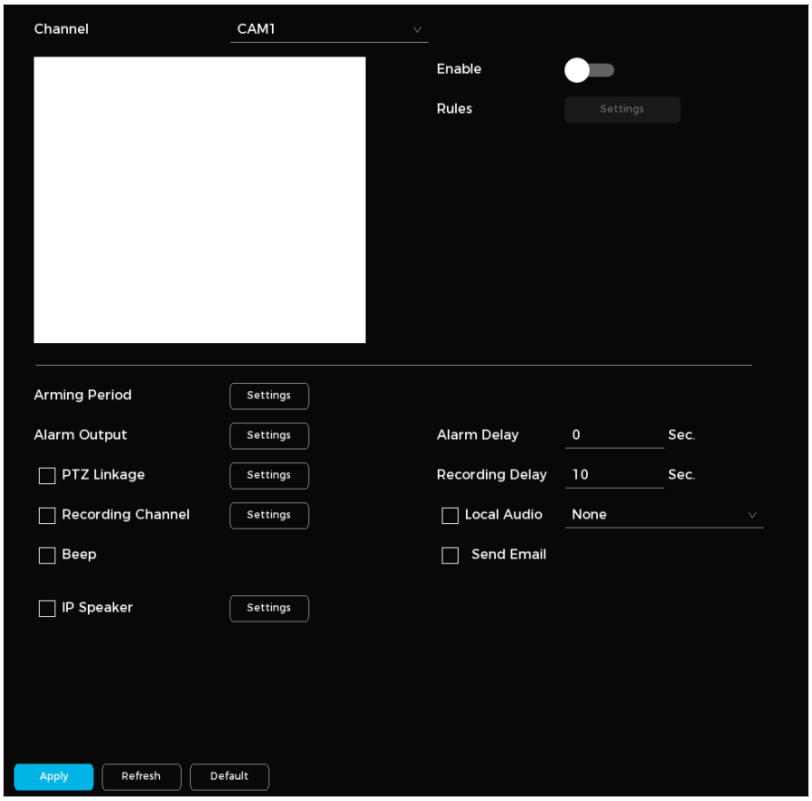
3. Select the box next to the desired intelligent function(s).
4. Click **Apply** when done.

ⓘ

- The available intelligent functions will vary based on camera model.
- You can configure intelligent functions separately for each preset point for PTZ cameras.

Configure a Face Detection Alarm

1. Navigate to Camera → AI Event → Face Detection.

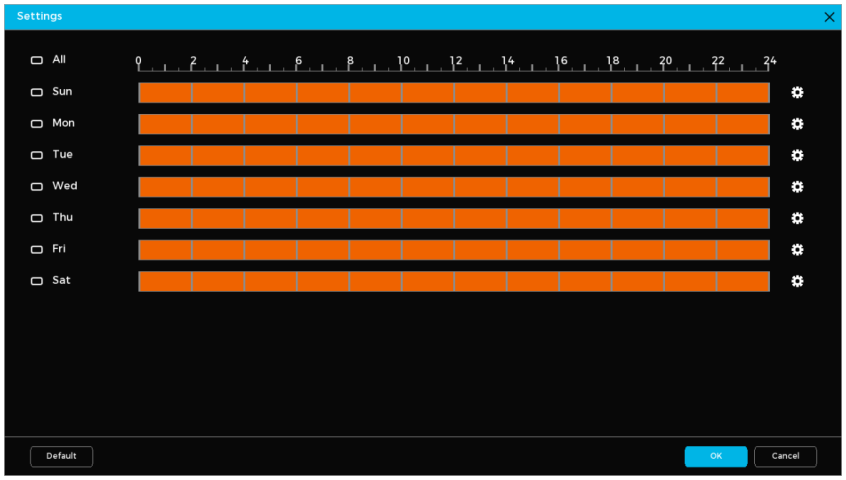


Face Detection Alarm Parameters

2. Select a channel.
3. Click to enable the alarm.
4. Click **Settings** next to **Rules**.
5. Define the minimum size (the smallest size a target must be to trigger an alarm) and the maximum size (the largest size a target can be to trigger an alarm).

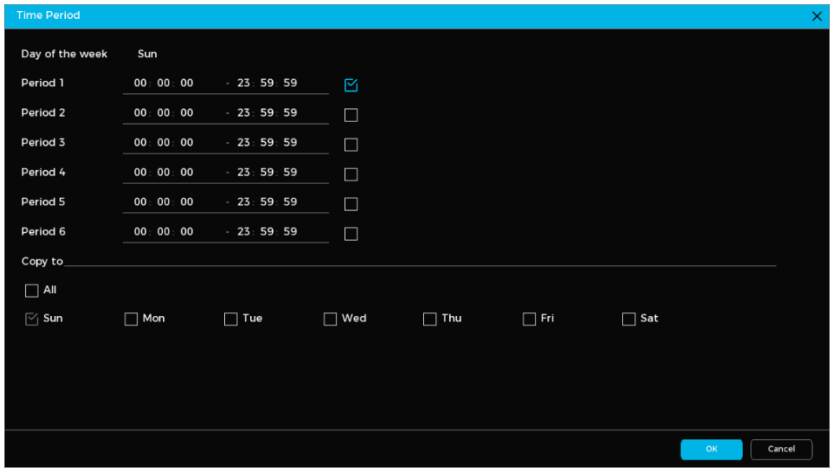
ⓘ An alarm will trigger when a target falls between these two sizes.

6. Click **Settings** next to **Arming Period** to set the time the alarm will be active. Drag the timeline to set the arming period visually. Click the orange bar of the timeline to disable a selected period.



Arming Period Screen (1)

7. Click  to configure specific periods for each day of the week. Each day is divided into six configurable periods. You may use the same configuration for all days or specific days by going to **Copy to** and selecting **All** or checking the box next to specific days.



Arming Period Screen (2)

8. Configure the alarm linkage actions. See the table below for more details and information on these parameters. Not all parameters listed in the table may be applicable.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.

Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

9. Click **Apply** when done.

Configure a Video Content Analytics (VCA) Alarm

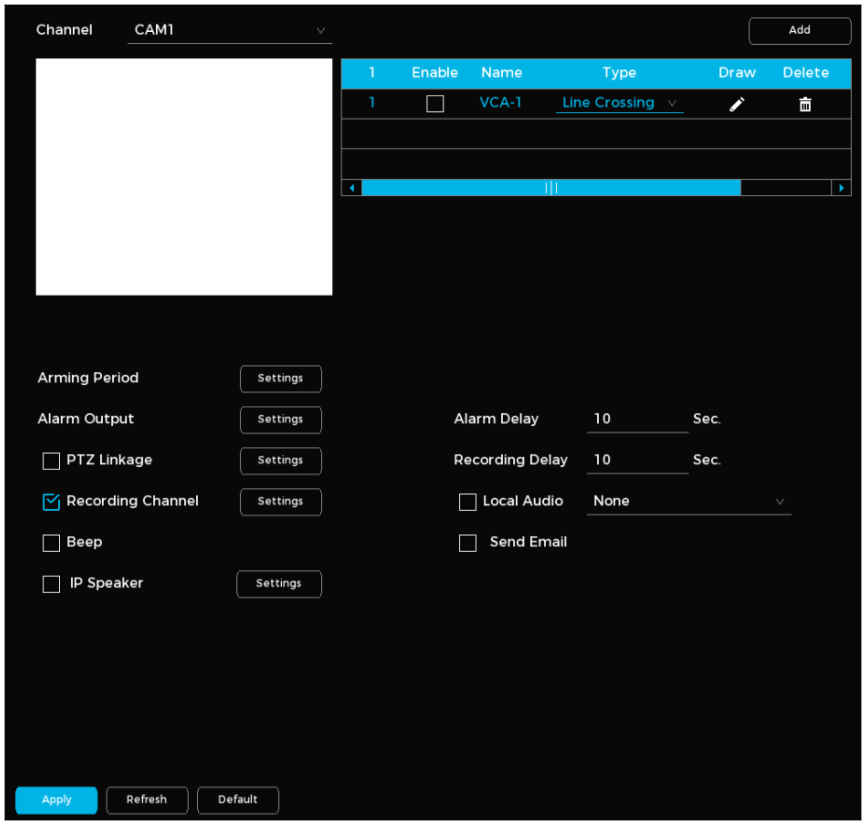
Read the table below to learn more about VCA functions.

Function	Description	Use Cases
Fence Crossing	Alerts when the target crosses the warning line in the defined direction, activating the configured alarm linkages.	Ideal for monitoring roads, secured areas with clear perimeters, and restricted zones.
Line Crossing	Alerts when a target crosses a user-defined line in a specific direction.	Ideal for monitoring entryways, gates, or areas with strict directional control.
Intrusion	Alerts when a target enters a protected area and stays beyond the set duration.	Ideal for monitoring parking lots, loading docks, and warehouses where unauthorized access is prohibited.
Abandoned Object	Alerts when an object is left in the monitoring area for a prolonged period.	Ideal for airports, train stations, and high-security zones.
Missing Object	Alerts when an object is removed from a monitoring area during a set time.	Ideal for retail environments, exhibition spaces, or storage facilities.
Parking Detection	Alerts when a parked vehicle stays in a monitored area longer than allowed.	Ideal for enforcing parking regulations in loading zones, private lots, and restricted parking areas.
Aggregate Detection	Alerts when a group of people is gathered in a monitored area beyond a density and time threshold.	Ideal for monitoring public areas, event venues, or government/corporate buildings.
Fast Moving	Alerts when an object moves quickly through a monitoring area.	Ideal for detecting sudden, rapid movements. Can be used in corridors, long hallways, or outdoor areas where speed is a concern.
Loitering Detection	Alerts when a target lingers in the monitoring area beyond a specified amount of time.	Ideal for parks, lobbies, or areas with limited-stay permissions.

Follow the steps below to set a VCA alarm.

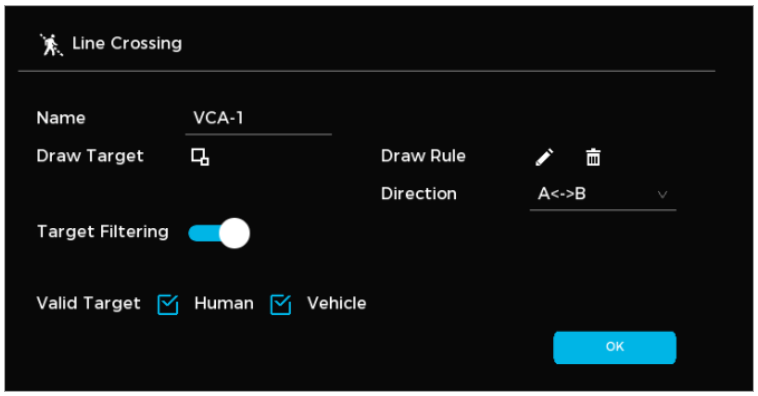
ⓘ Line Crossing and Intrusion are used as examples.

1. Navigate to **Camera → AI Event → VCA**.



VCA Alarm Parameters

2. Select a channel. Click **Add** to create a new rule.
3. Check the box under **Enable**.
4. In the **Type** column, select the VCA type.
5. Click  to set the alarm rule parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

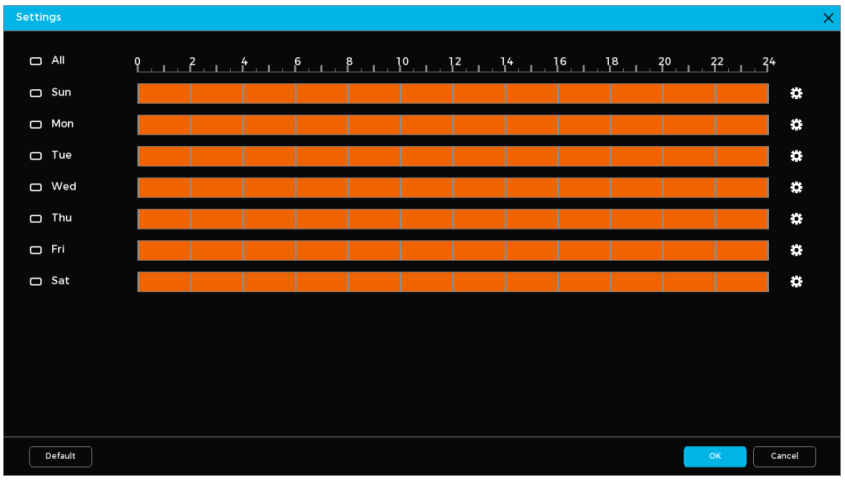


Alarm Rule Parameters Example Screen

Parameter	Description
Name	Enter a rule name for identification.
Draw Target	Set the target size by clicking  .
Draw Rule	Drag to create a line (straight, broken, or pol

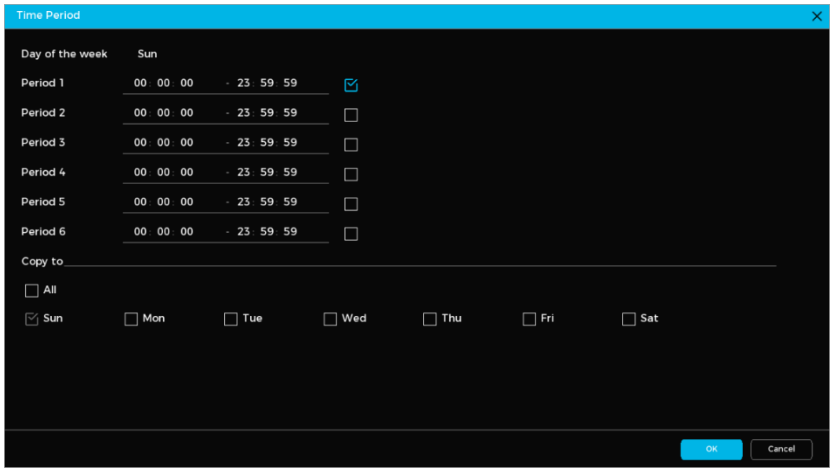
Direction	Specify a detection direction (A → B, B → A, A ←→ B).
Target Filtering Valid Target	Click to select a valid target. Human and Vehicle are selected by default.

6. Click **OK**.
7. Click **Settings** next to **Arming Period** to set the time the alarm will be active. Drag the timeline to set the arming period visually. Click the orange bar of the timeline to disable a selected period.



Arming Period Screen (1)

8. Click to configure specific periods for each day of the week. Each day is divided into six configurable periods. You may use the same configuration for all days or specific days by going to **Copy to** and selecting **All** or checking the box next to specific days.



Arming Period Screen (2)

9. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.

PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

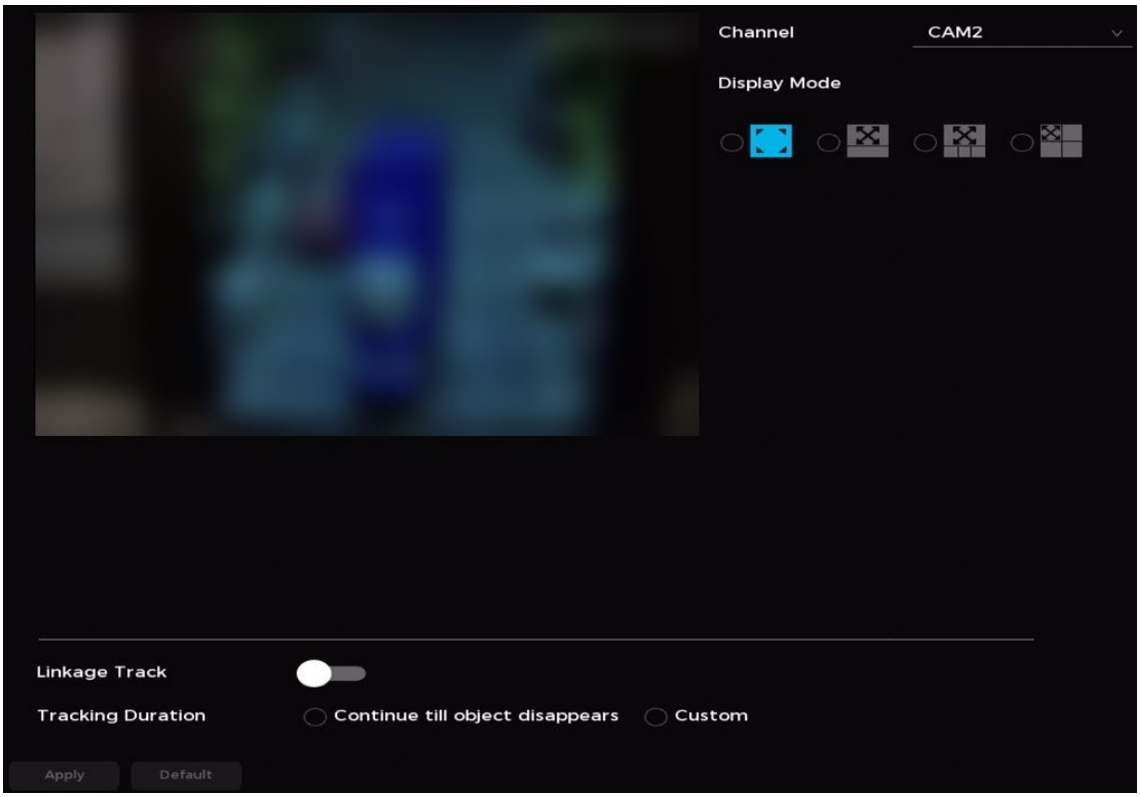
10. Click **Apply** when done.

Configure LumiTracking (R5 Models Only)

LumiTracking focuses on and tracks multiple alarm targets to provide rich details and panoramic views. Follow the steps below to set up LumiTracking.

ⓘ This function is only available when a LumiTracking-enabled NVRs is paired with a LumiTracking-enabled camera.

1. Navigate to **Camera → AI Event → LumiTracking**.
2. Set the following parameters.



LumiTracking

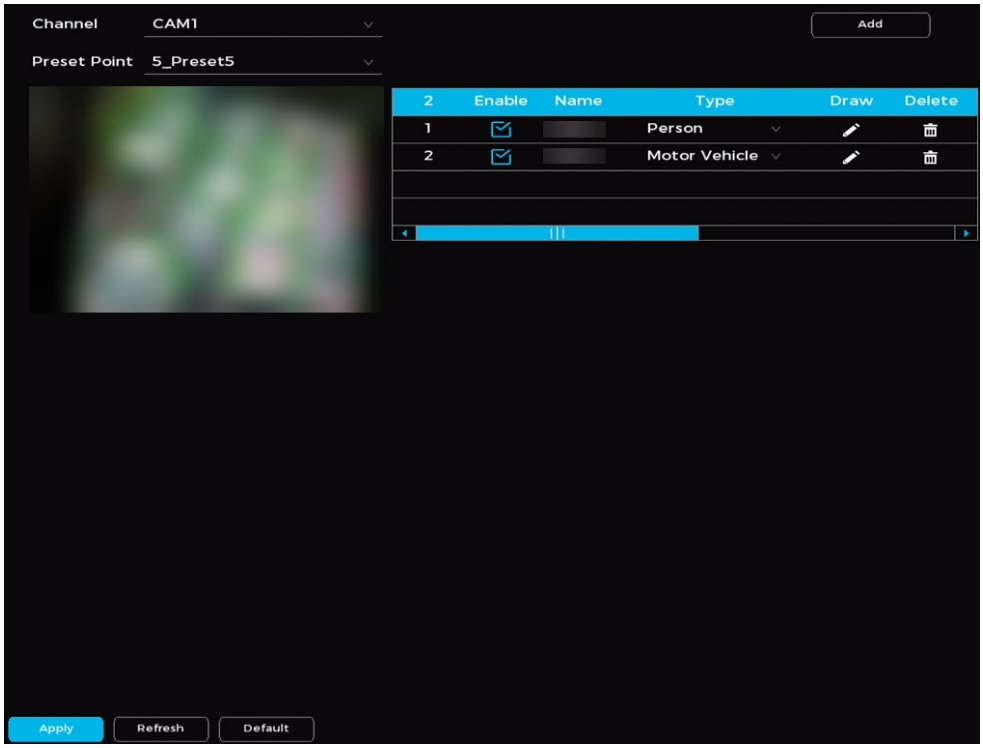
Parameter	Description
Channel	Choose the linkage channel.
Display Mode	Choose the number of tracked channels. The following display options are available: full screen (default), 1 + 1, and 1 + 3.
Linkage Tracking	Enable this function to track intelligent events. Linkage tracking is disabled by default.
Tracking Duration	Select between two tracking durations: • **Custom**: Manually set the tracking duration. For example, if the range is 30 to 60 seconds, the camera will track object A for at least 30 seconds. If object B appears after 30 seconds, the camera will switch to tracking B. If no new object appears, tracking of A ends after 60 seconds. • **Continue till object disappears**: The camera will track the detected object until it exits the monitoring area.

3. Click **Apply**.

Configure Metadata Settings (R5 Modes Only)

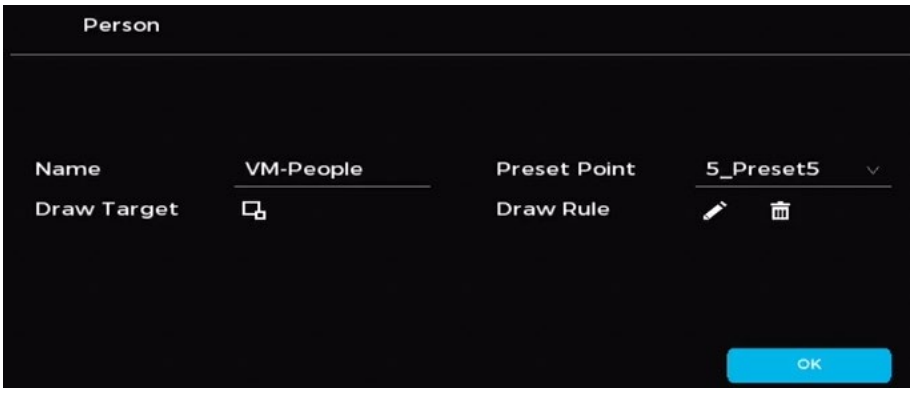
You can configure automatic alarm linkage actions if a metadata alarm is triggered. The corresponding camera will automatically record video, generate logs and capture snapshots. Other alarm linkage actions are not supported by video metadata. Follow the steps below to configure metadata settings and alarm linkage actions.

1. Navigate to **Camera → AI Event → Metadata Setting**.



Metadata Setting

2. Choose a channel. Click **Add** to set a rule. You can click the trashcan icon to delete the rule.
3. Select **Enable**. Set the **Type** to Person or Motor Vehicle.
4. Click the pencil icon to draw the detection area. Right-click the image to set the area.
5. Enter the rule name.
6. Click to set the minimum and maximum target size. The alarm will trigger when the target is between the minimum and maximum size.
7. Choose the corresponding preset point.
8. Click **OK**.



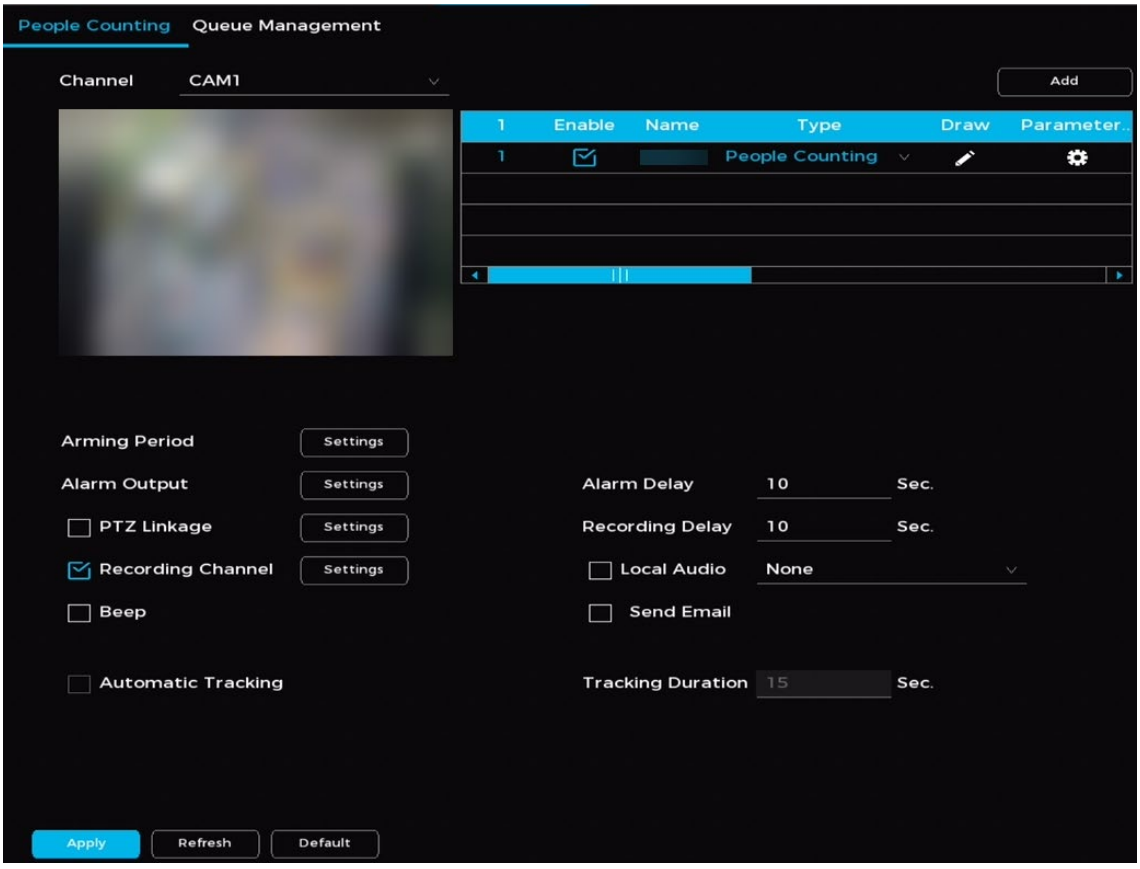
Setting Rule Parameters for Person Target Type

9. Click **Apply** to set the rule.

Configure People Counting (R5 Models Only)

You can configure automatic alarm linkage actions if the number of entries, exits, or congregating individuals exceeds the threshold. Follow the steps below to configure people counting rules and alarm linkage actions.

1. Navigate to **Camera → AI Event → People Counting**.

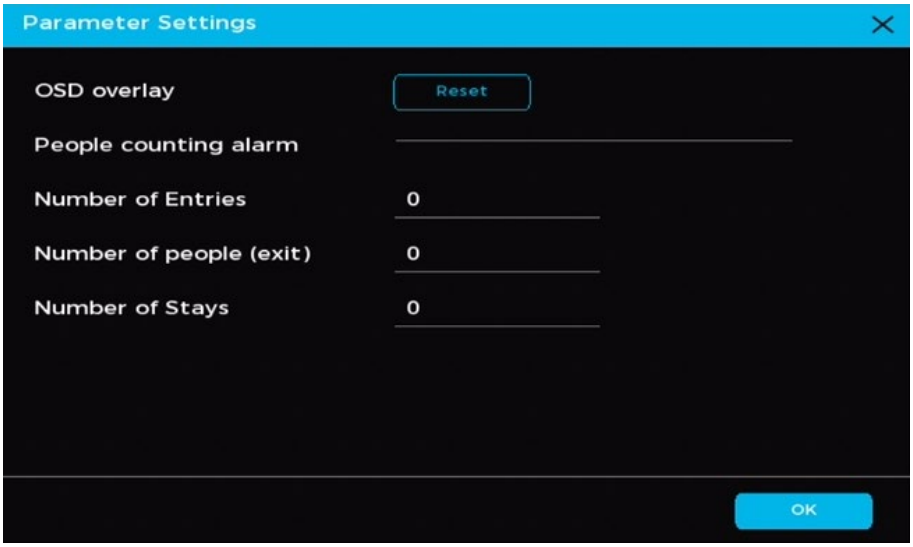


People Counting

2. Choose a channel. Click **Add** to set a rule.
3. Select the checkbox next to **Enable**. Set the **Type** to People Counting.
4. Click the pencil icon to draw the detection area. Right-click the image to set the area.
5. Set the rule name, preset point, and direction.
6. Click **OK**.

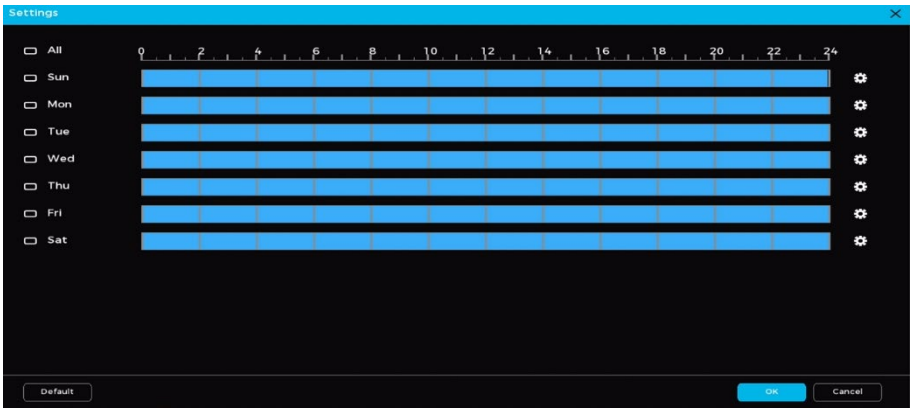
People Counting Rule

7. Click  to configure the rule parameters



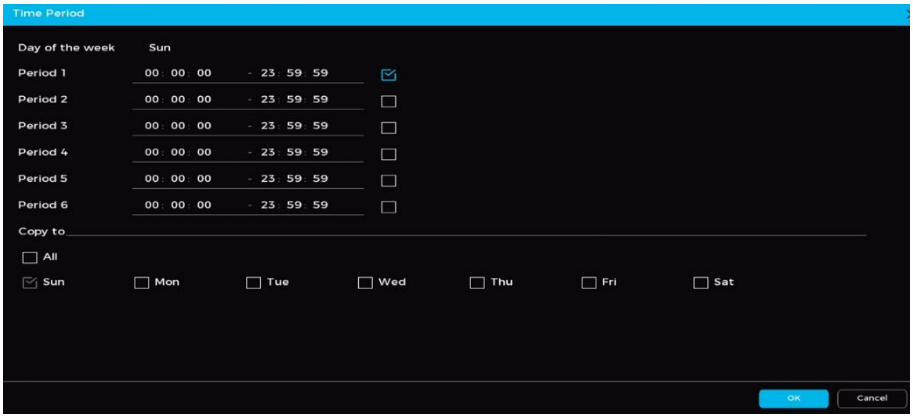
Parameter	Description
Number of Entries	Triggers an alarm when the number of people entering the detection zone exceeds the set threshold.
Number of People (Exit)	Triggers an alarm when the number of people exiting the detection zone exceeds the set threshold.
Number of Stays	Triggers an alarm when the number of people remaining in the detection zone exceeds the set threshold.

8. Click **Settings** next to **Arming Period**.
9. Set the arming period using one of the following methods:
    a. Drag the timeline to set the arming period. Click the blue segment to deactivate that specific time range.



Arming Period (a)

b. Click to cog icon to set the arming schedule for each day of the week. You can configure up to six time periods per day. Use **Copy to** option to apply the schedule to all days or specific days.



Alarm Linkage (b)

10. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

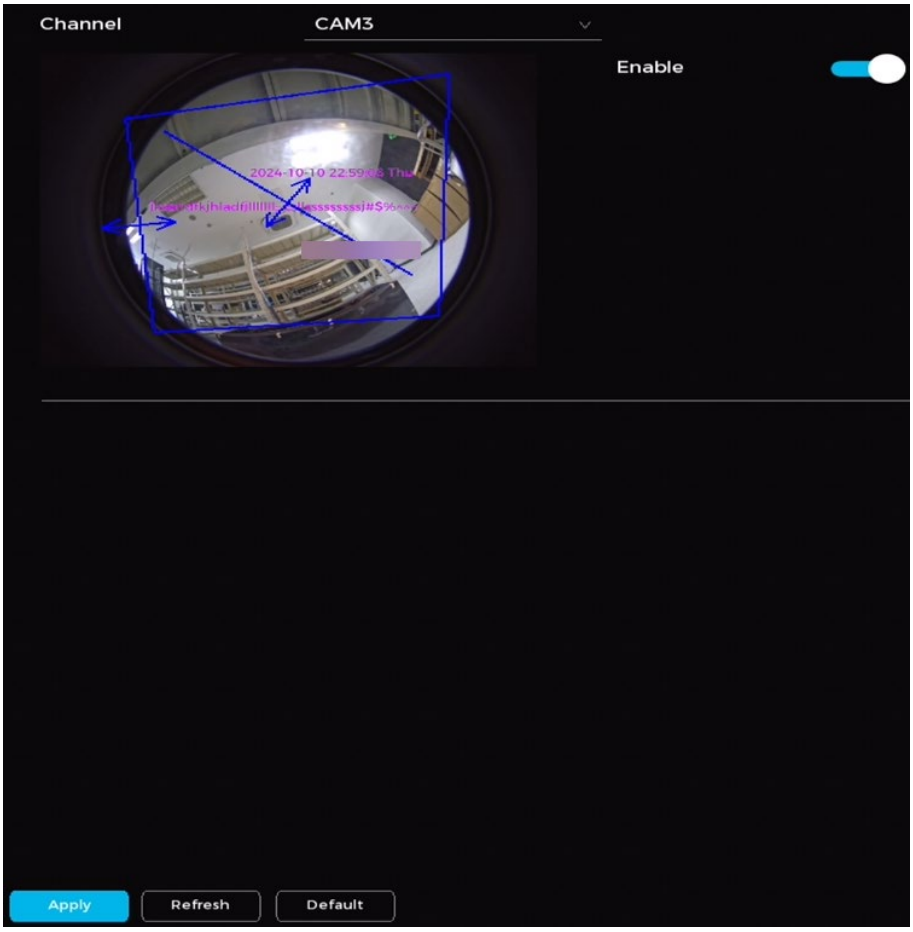
Parameter	Description
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Automatic Tracking	Automatically activate tracking when a tripwire or intrusion alarm is triggered. ⓘ Ensure the device supports this function by navigating to **Camera → Camera Registration**.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Tracking Duration	Set the tracking duration. The default is 15 minutes. ⓘ Ensure the device supports supports automatic tracking by navigating to **Camera → Camera Registration**.

11. Click **Apply** when done.

Configure Heat Map (R5 Models Only)

Heat map technology tracks the movement and distribution of active objects within a defined zone over a set time period, using color gradients to visually represent activity levels. Follow the steps below to configure heat maps.

1. Navigate to **Camera → AI Event → Heat Map**.



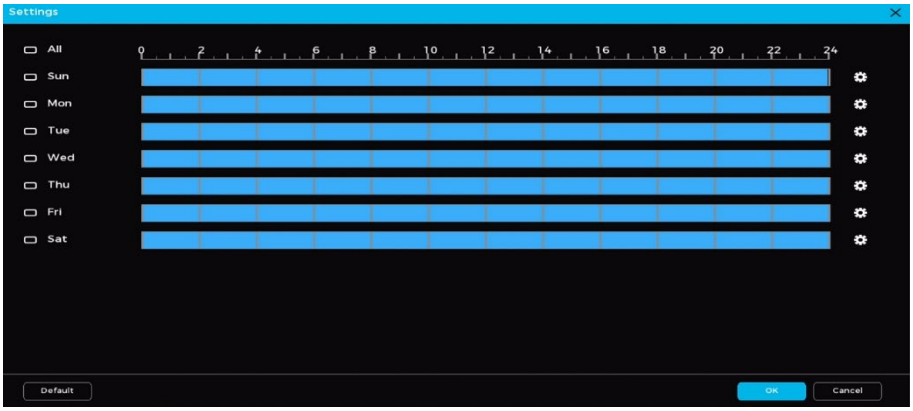
Heat Map

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

Configure Object Monitoring (R5 Models Only)

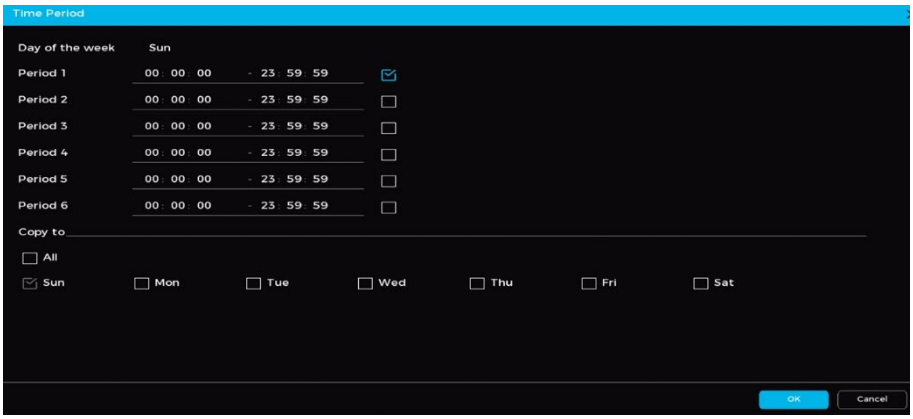
Follow the steps below to configure object monitoring.

1. Navigate to **Camera → AI Event → Object Monitoring**.
2. Choose a channel. Click **Add** to set a rule.
3. Select the checkbox next to **Enable**. Set the **Type** to Object Placement or Object Fetch.
4. Click the pencil icon to draw the detection area. Right-click the image to set the area.
5. Set the rule name and minimum duration.
6. Select the checkbox next to **Luggage/Bag/Box.**
7. Click **OK**.
8. Set the arming period using one of the following methods:
    a. Drag the timeline to set the arming period. Click the blue segment to deactivate that specific time range.



Arming Period (a)

b. Click to cog icon to set the arming schedule for each day of the week. You can configure up to six time periods per day. Use **Copy to** option to apply the schedule to all days or specific days.



Alarm Linkage (b)

9. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Remote Voice	Follow the steps to set up remote voice. 1. Click **Setting** next to **Remote Voice**. 2. Click **Add** to display all connected channels that support remote voice configuration. If a channel is selected in Remote Voice and supports this feature, its configuration will appear by default. You won't be able to delete or reset its play count. 3. Select a voice file from the **File Name** drop-down menu.

	4. Set the Play Count (up to 10 times). 5. Click **Copy** to apply the current channel's voice settings to other channels 6. Click the trash icon to remove a single channel. To delete multiple channels, select them and click **Delete in batches**. ⓘ When remote voice is configured on multiple channels, each channel can trigger its linked voice configuration during an alarm event.  *Remote Voice Configuration*
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Remote Warning Light	Follow the steps to set up the remote warning light. 1. Click **Setting** next to **Remote Warning Light**. 2. Click **Add** to view all channels that are successfully connected and support remote warning light configuration. 3. If a channel is selected in Object Monitoring and supports remote warning light configuration, its settings will appear by default and cannot be deleted. 4. Choose the **Mode** and **Flicker Frequency** for the remote warning light. 5. Set the **Stay Time**—up to a maximum of 30 seconds. 6. Click **Copy** to apply the current channel's warning light settings to other channels. 7. Click the delete icon to remove a single channel or select multiple channels and click **Delete in batches** to remove them all at once. 8. Select the desired channel to add the remote warning light, then click **OK.** 9. If multiple channels have remote warning light configurations, they will each trigger their respective lights when an alarm event occurs. 10. Click **Apply** to save the settings.

Remote Warning Light

10. Click **Apply** when done.

Configure a License Plate Recognition (LPR) Alarm

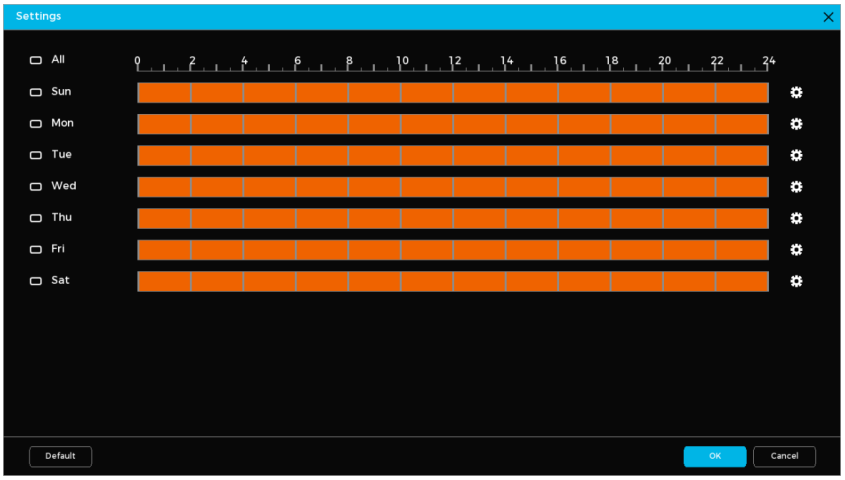
Follow the steps below to set an alarm to trigger when the system identifies a specific license plate.

1. Navigate to **Camera → AI Event → LPR**.
2. Click  to enable the alarm.
3. Select the target type: **Allowlist**, **Blocklist**, **Standard**, **All**.

ⓘ

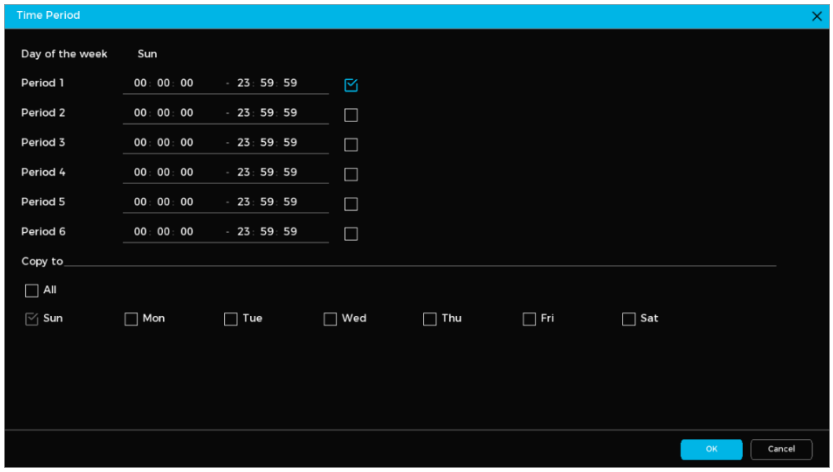
- **Allowlist**: Alerts to plates on an approved list.
- **Blocklist**: Alerts to plates on a restricted list.
- **Standard**: Alerts to all detected plates.
- **All**: Combines allowlist and blocklist functionalities.

4. Click **Settings** next to **Arming Period** to set the time the alarm will be active. Drag the timeline to set the arming period visually. Click the orange bar of the timeline to disable a selected period.



Arming Period Screen (1)

5. Click  to configure specific periods for each day of the week. Each day is divided into six configurable periods. You may use the same configuration for all days or specific days by going to **Copy to** and selecting **All** or checking the box next to specific days.



Arming Period Screen (2)

6. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.

Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

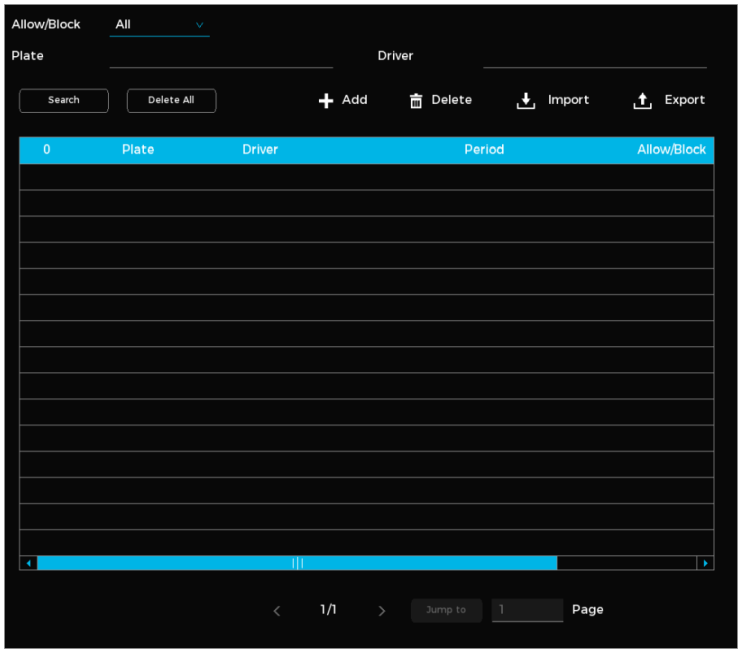
7. Click **Apply** when done.

Configure the License Plate Recognition (LPR) Database Settings

You can add plate numbers to the blocklist or allowlist for vehicle management. The system compares detected plates with these lists and triggers the corresponding alarm linkage.

Follow the steps below to configure the LPR database settings.

1. Navigate to **Camera → AI Event → LPR Database**.



LPR Database

2. Click  .
3. Add the plate number and the driver's name.
4. Choose a list type (Allow or Block).
5. Set the Validity Period.
6. Click **OK** when done.

Related Operations

- **To search**: Enter a plate number or driver keyword, select a type, and click Search to find the entry.
- **To import plate information**: Click  . Click **Browse** and select the file to import.
- **To export plate information**: Click  . Select the file storage path. Click **Save**.
- **To delete individual plate information**: Select the specific plate number. Click  .
- **To delete batches of plate information**: Select multiple plate numbers to delete. Click **Delete All**.

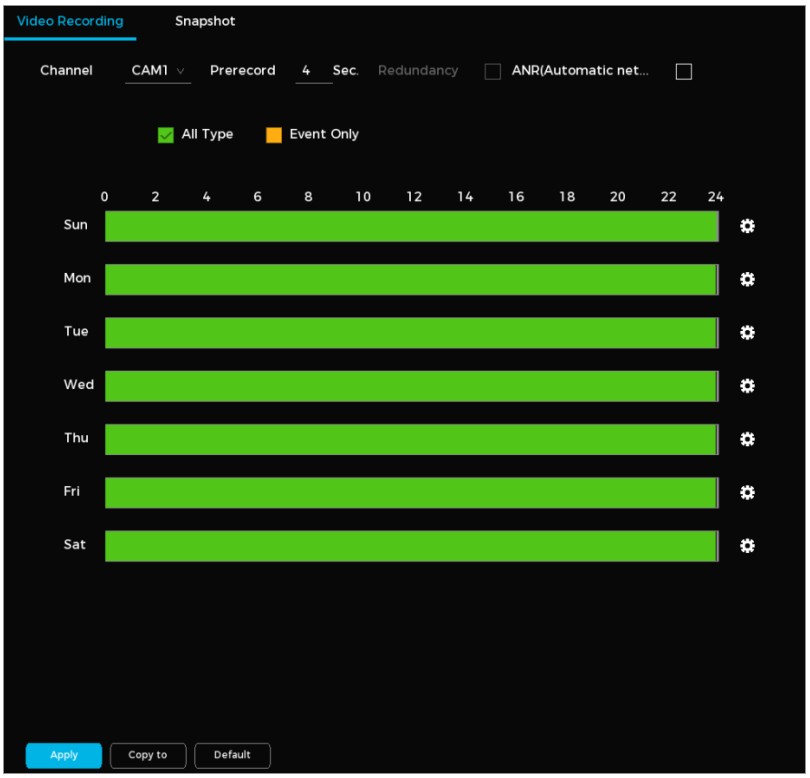
Storage

Optimize recording management by configuring storage options, including recording plans, modes, and strategies. Proper setup ensures efficient data retrieval and retention.

Configure the Recording Plan

This section covers setting up recording plans for video and images. While focused on video, the steps for images are similar. Follow the steps below to configure these settings to capture and store critical events securely.

1. Navigate to Storage → Recording Plan.



Recording Plan

2. Configure the recording settings. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Channel	Select the channel(s) for video recording.
Prerecord	Set the pre-event recording duration to capture moments before the event is triggered.
Redundancy	Enable redundancy for the channel. If the device has multiple hard drives, designate one as a redundant HDD to back up recordings. • If the channel is not recording, redundancy activates with the next recording, regardless of the checkbox selection. • If the channel is recording, current files are saved, and recording continues per the new schedule. ⓘ • This feature is only available on select device models. • Only video (not images) can be backed up using redundancy.

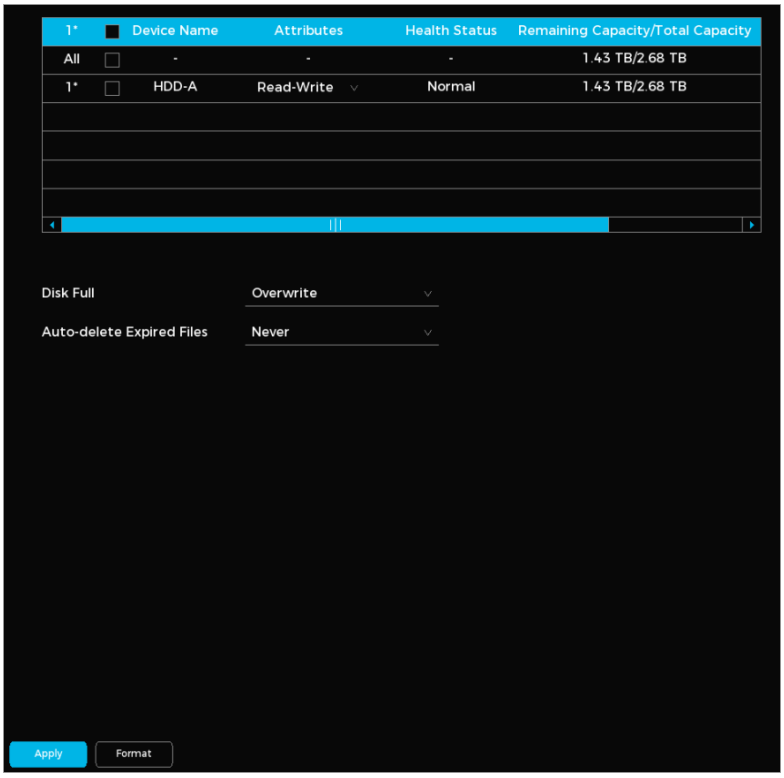
Automatic Network Replenishment (ANR)	Ensures continuous recording if the NVR loses connection with the IP camera. When reconnected, the NVR downloads the recorded files from the IP camera. Set the maximum upload period for recordings. If the offline time exceeds this limit, only recordings within the set period will be uploaded. ⓘ Make sure the SD card is installed and the recording function is enabled on the IP camera.
Event Type	Select either **All Type** or **Event Only** recordings. The default is All Type.
Time Period	Set the time periods for active recording. Drag on the timeline to set the time period or click ⚙ to configure manually.
Default	Return to the default recording plan settings.
Copy to	Copy the recording plan to other channels.

3. Click **Apply** when done.

Configure the Storage Strategy

Follow the steps below to configure the storage strategy.

1. Navigate to **Storage → Disk Management**.



Disk Management

2. Configure the disk management parameters. See the table below for more details.

Parameter	Description
Disk Full	Set the system's action when storage reaches capacity. • Choose **Stop** to stop recording when disk storage is full. • Choose **Overwrite** to overwrite the oldest files when disk storage is full
Auto-Delete Expired Files	Set the frequency for automatic deletion of expired files.

	• Choose **Never** if you do not want to automatically delete expired files. • Choose **Custom** to select how long to keep expired files before they are automatically deleted.

3. Set the HDD type. Navigate to the Attributes column. Select **Read-Write**, **Read-only**, or **Redundancy**.

ⓘ

- **Read-Write**: Allows both reading and writing data on the disk.
- **Read-Only**: Restricts the disk to reading data only.
- **Redundancy**: Configures the disk for backup purposes.

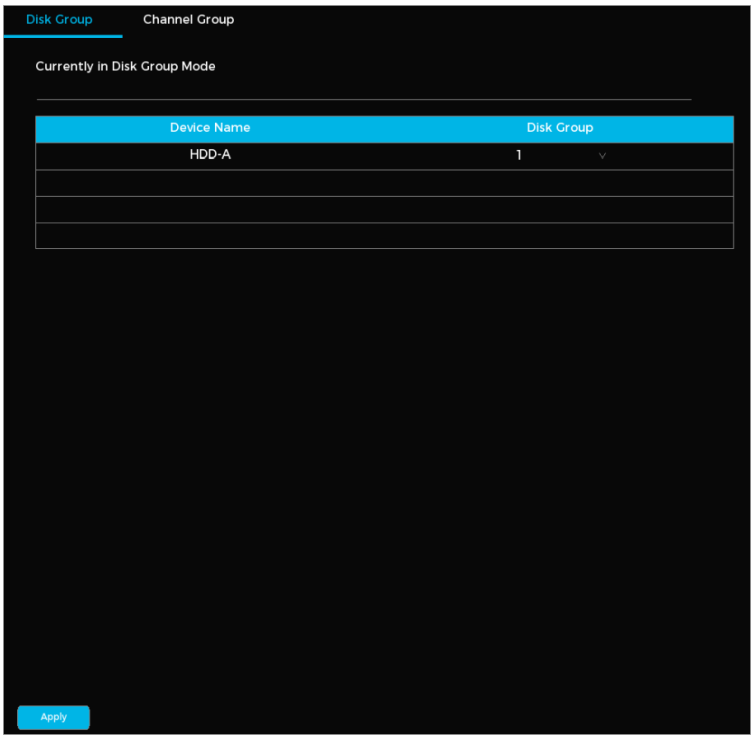
4. Format the HDD. Select an HDD, click **Format**, and follow the onscreen prompts.

⚠ Formatting the HDD will erase all existing data.

Configure the Disk Group

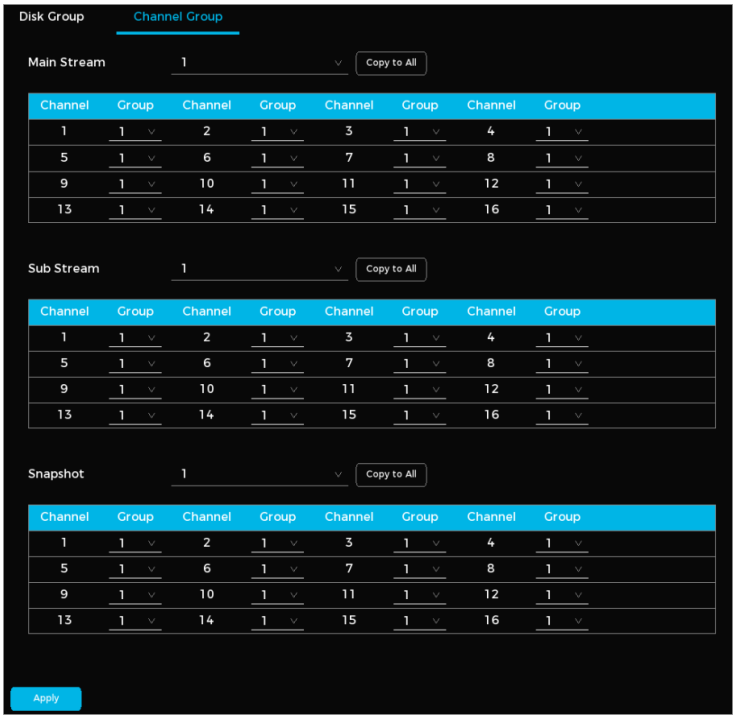
Follow the steps below to configure the disk group to manage storage efficiently. By default, the installed HDD and RAID are assigned to Disk Group 1. You can assign HDDs for mainstream, substream, or snapshot operations based on your storage requirements.

1. Navigate to **Storage → Disk Group**.



Disk Group

2. Select a disk group for each HDD.
3. Click **Apply** to save the disk group configuration.
4. Go to the **Channel Group** tab. Assign groups for mainstream, substream, and snapshot.



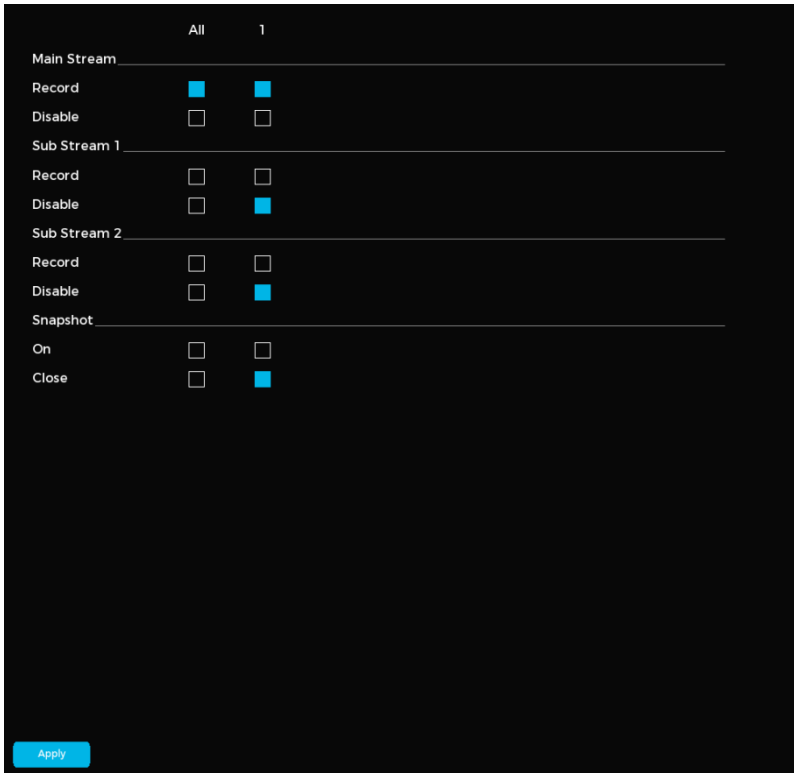
Channel Group Tab

5. Click **Apply** when done.

Configure the Recording Mode

Follow the steps below to enable or disable video recording for each channel. When enabled, the device records continuously.

1. Navigate to **Storage → Recording Mode**.



Recording Mode

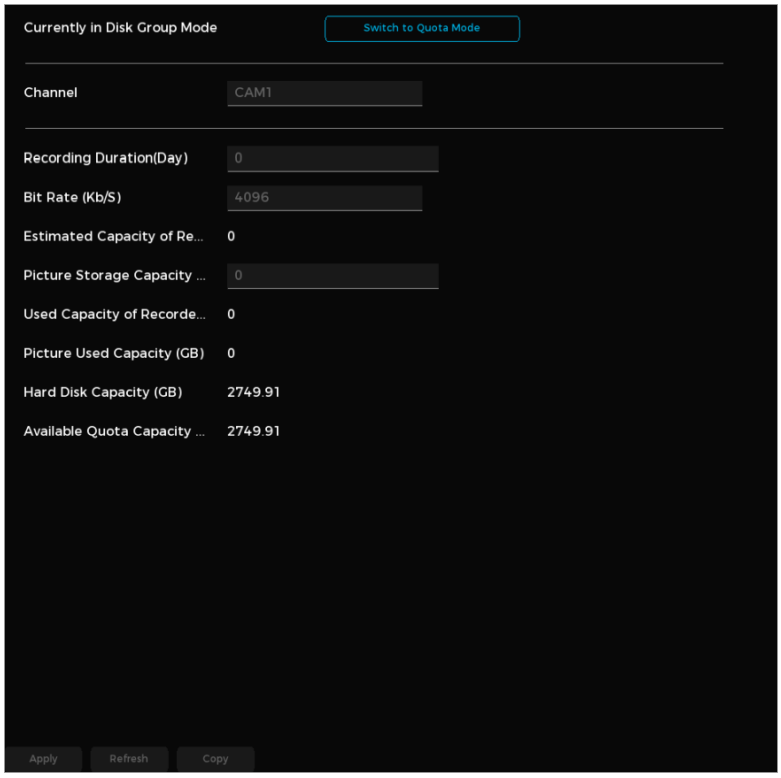
2. Enable recording for each channel. You can select **All** to configure the same recording mode for all channels.
3. Click **Apply** when done.

Configure the Disk Quota

Follow the steps below to allocate specific storage capacities for each channel and optimize storage management.

ⓘ Disk quota mode and disk group mode cannot be enabled at the same time. If Disk Group Mode is active, click Switch to Quota Mode.

1. Navigate to **Storage → Disk Quota**.



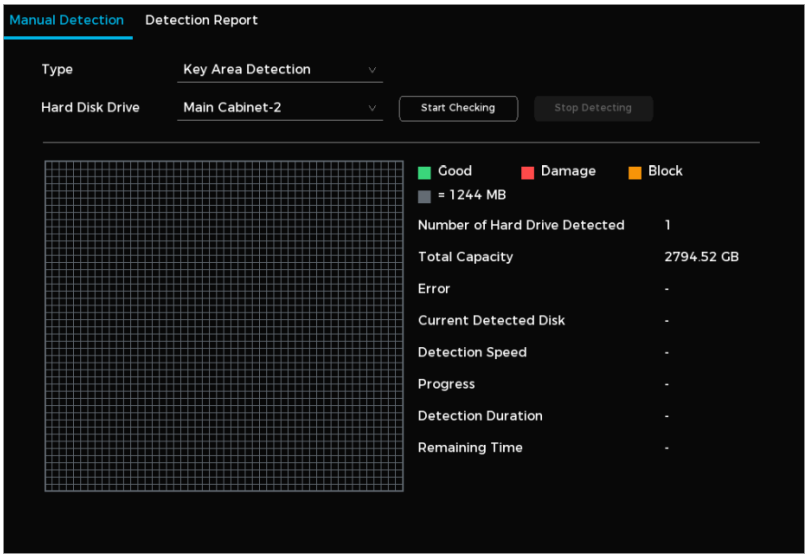
Disk Quota

2. (Optional) If Disk Group Mode is active, click Switch to Quota Mode. Follow the on-screen instructions to format the disks.
3. Select the channel.
4. Set the following parameters: **Recording Duration (days)**, **Bit Rate (kbit/s)**, and **picture/storage capacity**.
5. Click **Apply** when done.

Configure Disk Detection

The system can detect the HDD status, allowing you to replace damaged drives and monitor their performance. Follow the steps below to configure disk detection functionalities.

1. Navigate to **Storage → Disk Detection → Manual Detection**.



Disk Detection

2. Choose the detection type: Key Area Detect or Global Detection.

ⓘ

- **Key Area Detect**: Analyzes the used HDD space using the built-in file system. Ideal for quick checks.
- **Global Detection**: Analyzes the entire HDD. Ideal for more thorough analysis but may affect active drives.

3. Select the desired HDD from the list.
4. Click **Start Checking**. You can stop the current detection at any time by clicking **Stop Checking**. To restart detection, click **Start Checking** again.

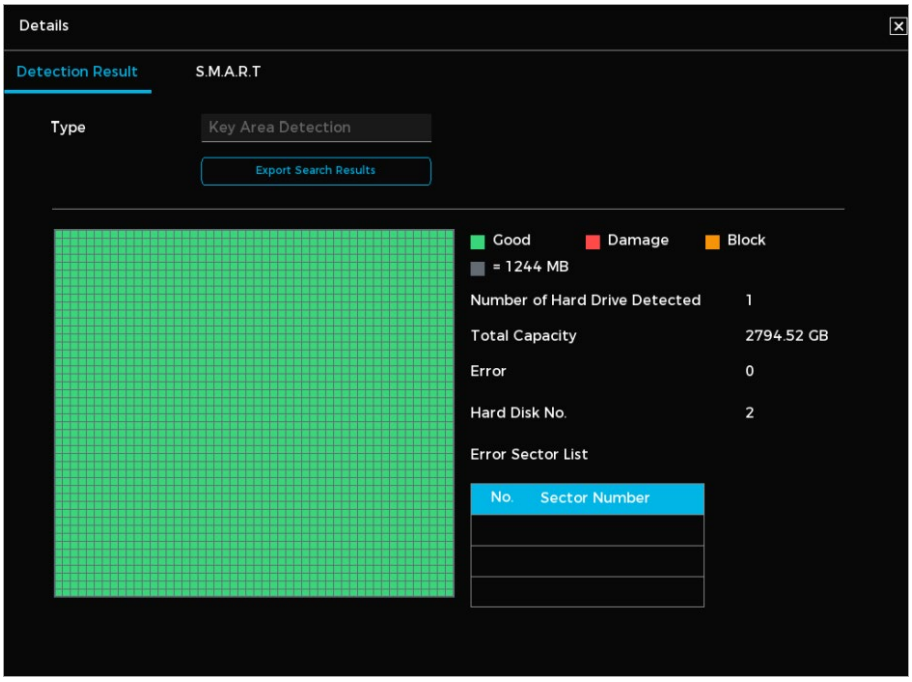
View a Detection Report

After HDD detection, you can view detailed results to assess the performance and condition of your storage drives. Follow the steps below to view a detection report.

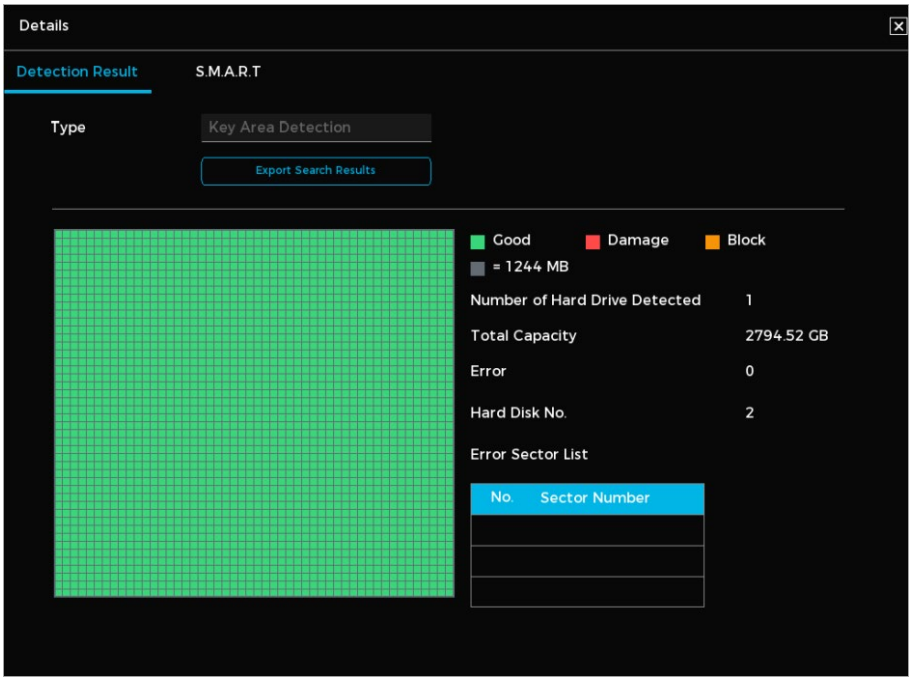
1. Navigate to **Storage → Disk Detection → Detection Report**.

Detection Report

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



Detection Results



S.M.A.R.T. Report

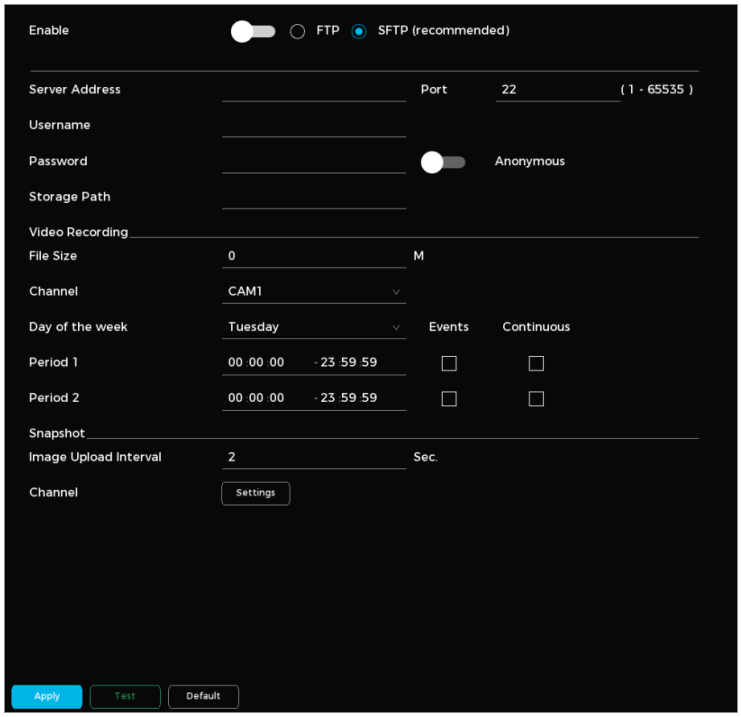
Configure a File Transfer Protocol (FTP)

You can store and manage recorded videos and snapshots directly on an FTP server. Prior to setting up an FTP, ensure the following prerequisites are met:

- An FTP server is installed on your PC or other suitable device
- The FTP user account has write permissions

Follow the steps below to configure an FTP.

1. Navigate to **Storage → FTP**.



File Transfer Protocol (FTP)

2. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Enable	Enable FTP functionality.
FTP Type	Choose between FTP (plain text transmission) and SFTP (encrypted transmission). SFTP is recommended.
Server Address	IP address of the FTP server.
Port	Specify the port number for the FTP. ⓘ • The default port number for FTP is 21. • The default port number for SFTP is 22.
Username Password Anonymous	Enter the FTP server login information. If **Anonymous** is enabled, no credentials are required.
Storage Path	Specify where files will be uploaded. • If no remote directory is specified, folders will be created based on time and IP address. • If a remote directory is specified, the system creates a folder under the FTP root directory using the specified name.
File Size	Set the maximum file size for upload. Set the value to 0 to upload the entire video regardless of size. • If the file size is less than the actual video length, only part of the video will be uploaded. • If the file size is greater than or equal to the video length, the entire video will be uploaded.

Image Upload Interval	Set how often images are uploaded. • If the interval is longer than the snapshot interval, recent snapshots are uploaded (e.g., snapshots every 5 seconds, upload every 10 seconds). • If shorter, the system uploads the most recent snapshot.
Channel	Select the channel to apply the FTP settings.
Day of the Week	Set the upload schedule. You can select the specific day(s) to upload recorded files or set up to two time periods a day to upload.
Period 1, Period 2	

3. Click **Test** to check the FTP connection. If the connection fails, check your network and FTP settings.
4. Click **Apply** when done.

System

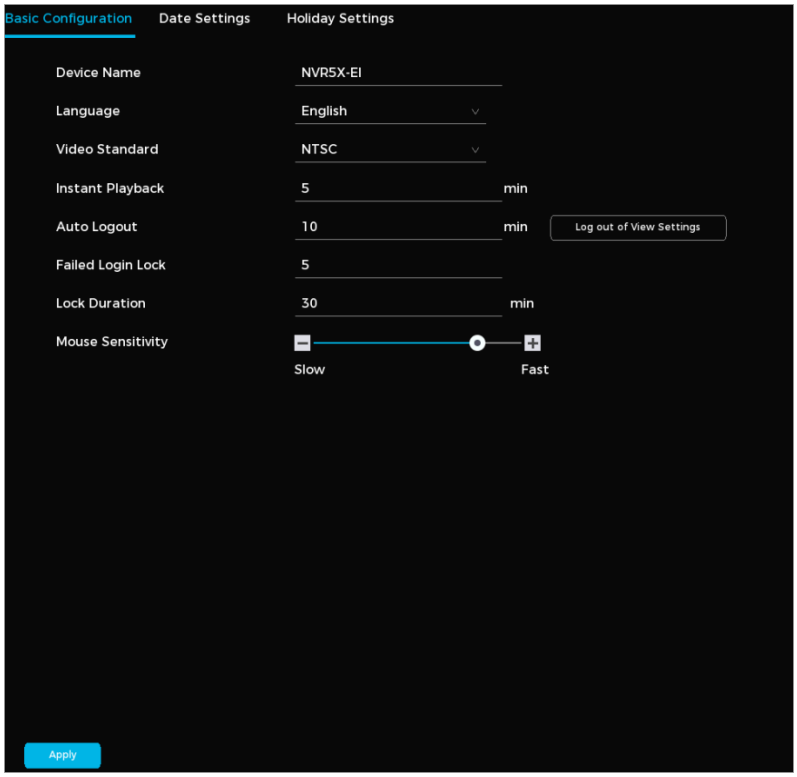
You can change the system settings including date, accounts, display output, and more.

Configure System Settings

Configure Basic System Settings

Follow the steps below to set up basic settings such as video standard, logout time, and mouse sensitivity.

5. Navigate to **System → General → Basic Configuration**.



Basic System Settings

6. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Device Name	Enter the device name.
Language	Choose the system language.

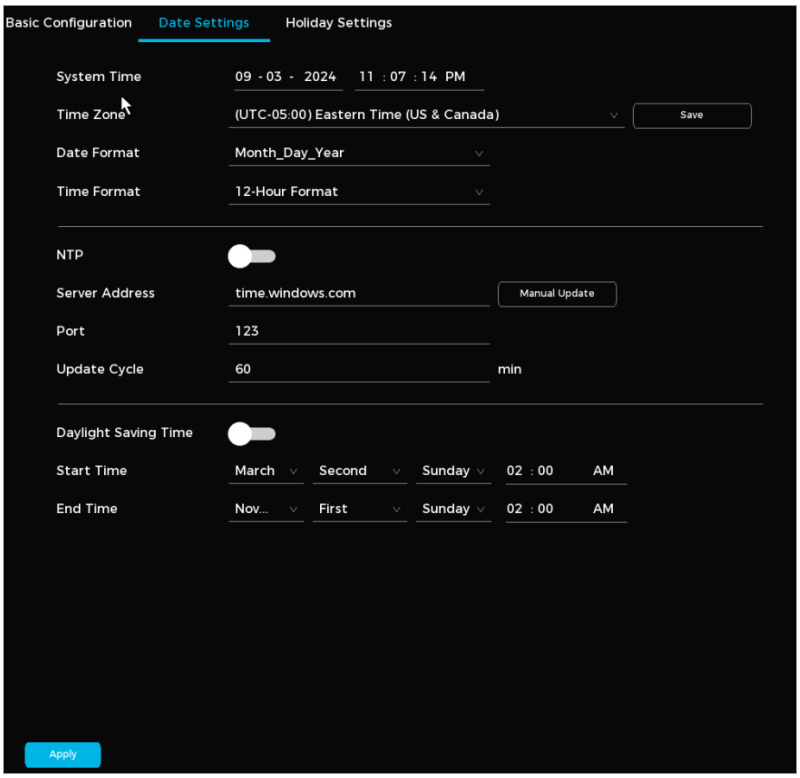
Video Standard	Choose between PAL or NTSC based on your region.
Instant Playback	Set the playback duration (5 to 60 minutes). You can play back footage by clicking on the live page.
Auto Logout	Set the inactivity time for automatic logout. Click **Log out of View Settings** to select channels for monitoring after logout.
Failed Login Lock	Set the maximum number of attempted logins before an account is locked.
Duration	Set the time an account is restricted after it is locked.
Mouse Sensitivity	Change the mouse speed between **Slow** and **Fast**.

7. Click **Apply** when done.

Configure Date and Time Settings

Follow the steps below to change the date and time settings.

1. Navigate to **System → General → Date Settings**.



Date and Time Settings

2. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
System Time	Enter the current time into this field. Click the Time Zone to select your region. The time will automatically adjust based on your selection. ⚠ Avoid changing the system time randomly, as it may affect video search. To prevent data conflicts, pause recording or adjust settings during inactive periods.
Time Zone	Choose the time zone you are in.
Date Format	Select your preferred format for the system date.
Time Format	Choose between the 12-hour or 24-hour format.

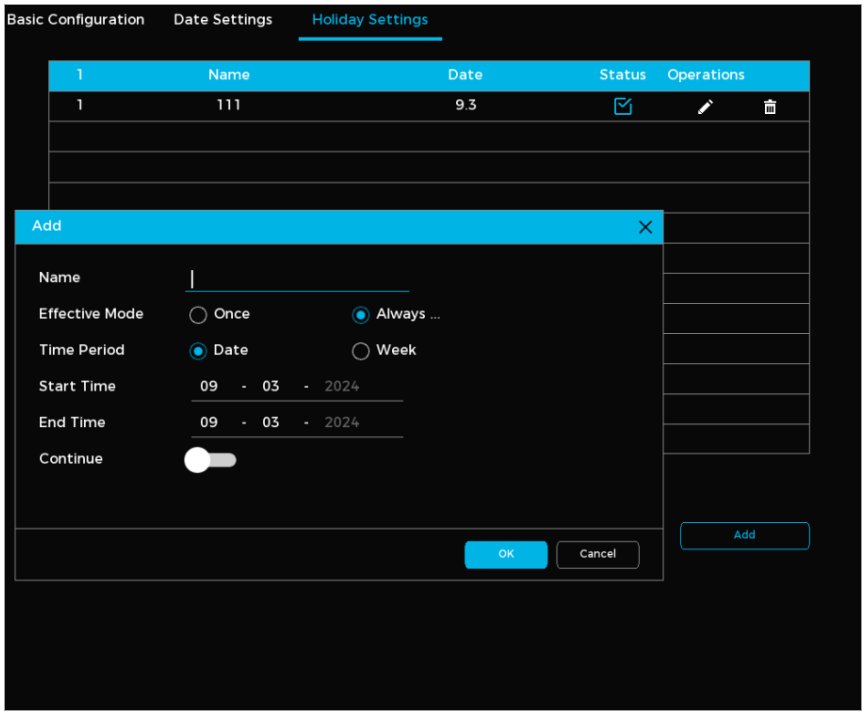
NTP	Use the Network Time Protocol (NTP) to keep the system clock accurate by syncing with an external time server. 1. Click  to enable NTP synchronization. 2. Enter the server address (e.g., time.windows.com) and port number (default: 123). 3. Set the update interval to control synchronization frequency. 4. Click **Apply**.
Daylight Saving Time	Automatically adjust the system clock for daylight saving time based on regional requirements. 1. Toggle  to enable daylight saving adjustments. 2. Set the start and end dates for daylight saving time. 3. Click **Apply**.

3. Click **Apply** when done.

Configure Holiday Settings

Follow the steps below to set the recording plan when a holiday occurs.

1. Navigate to **System → General → Holiday Settings.**
2. Click **Add**.



Holiday Recording Plan Settings

3. Set the holiday name, effective mode (Once, Always, or Week), and the applicable time.
4. (Optional) Click  next to **Continue** to configure additional holidays at the same time.
5. Click **OK** to add the holiday to the list. You can edit an existing holiday by clicking  . You can delete holidays by clicking  . To assign a specific recording plan for a holiday, navigate to **Storage > Recording Plan**.

Configure Account Settings

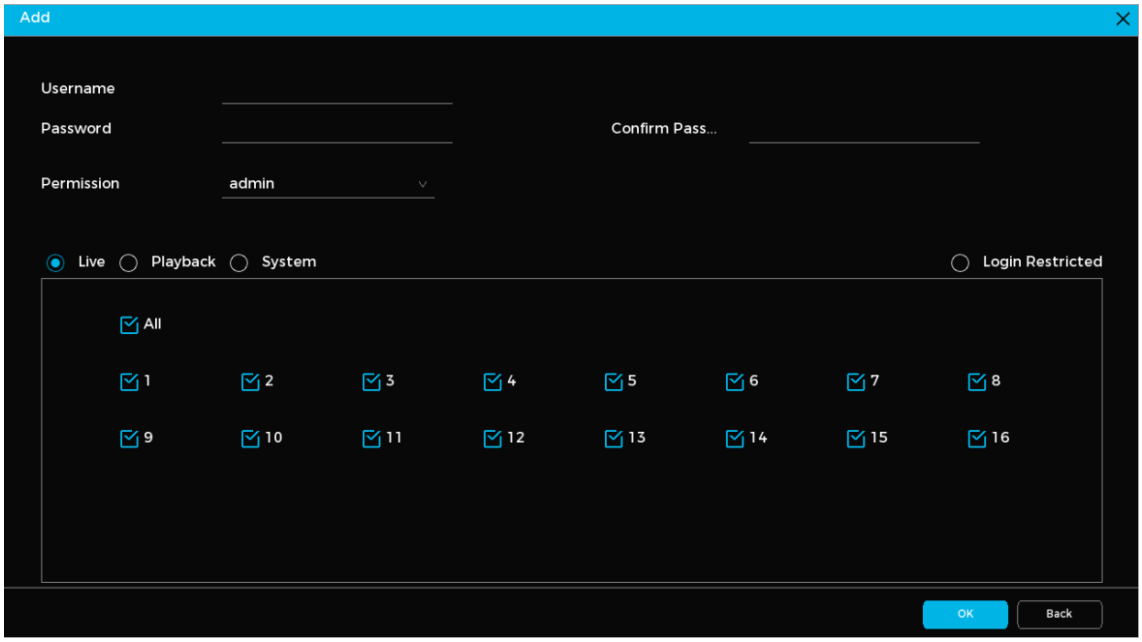
Administrators can create and manage user accounts, including ONVIF users and user groups. The built-in admin account is fixed and cannot be deleted or modified.

Add Users

Users can access and manage the device based on their assigned role. The default 'admin' account is fixed and cannot be modified or deleted. Additional users can be created with specific permissions, limited to their designated user group.

Follow the steps below to add a user.

1. Navigate to **System → User Management → User**.
2. Click **Add**.



Add User

3. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Username	Assign a unique username for the user.
Password	Create and confirm the user password.
Confirm Password	
Login Restricted	Enable this feature to set a specific time when the user can login. You must provide the User MAC address.
Permission	Assign the user to a specific permission group. A user's permissions cannot exceed the limitations of the group they are assigned to.

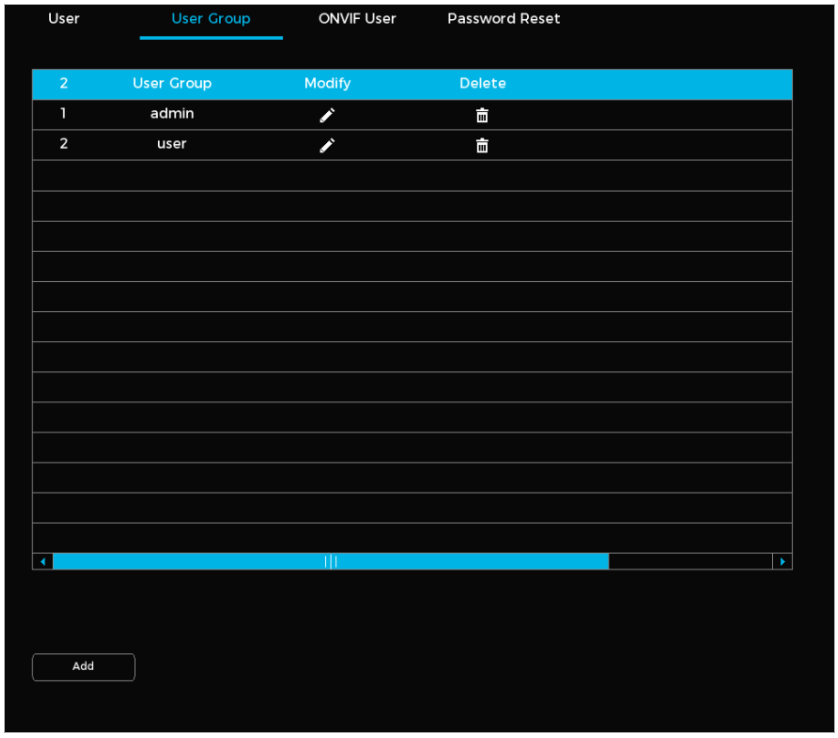
4. Select the boxes under **Live**, **Playback**, and **System** as required.
5. Click **OK** when done.

Add a User Group

User accounts follow a two-tier management structure with individual users and user groups. Each user must be assigned to one group, and only one group can be linked to a user at a time. By default, the system includes two predefined groups—admin and user—that cannot be deleted. Additional groups can be created to define custom permissions.

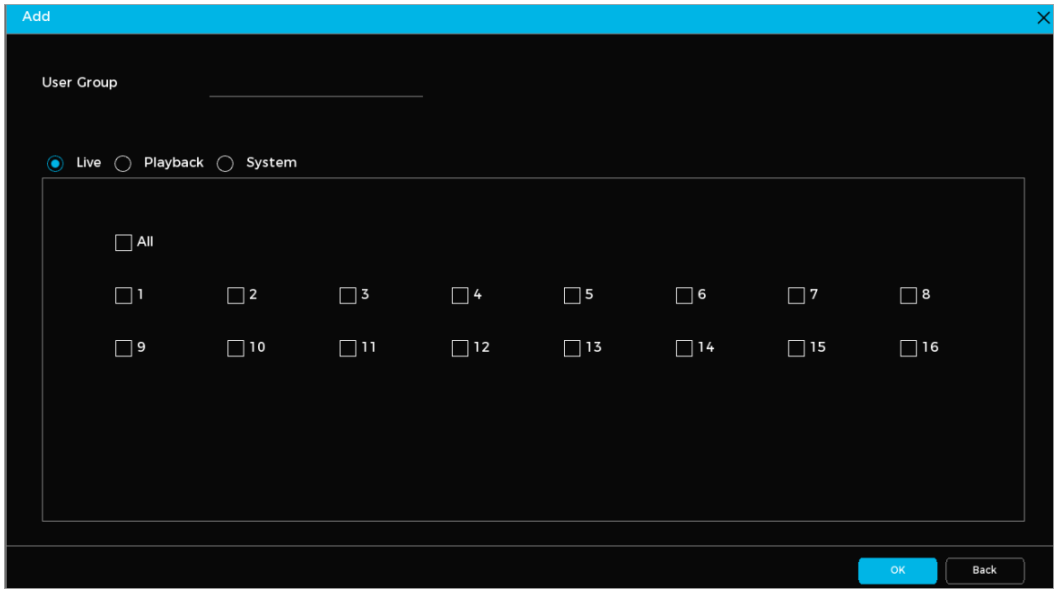
Follow the steps below to add a user group.

1. Navigate to **System → User Management → User Group**.



User Group Management

2. Click **Add**.

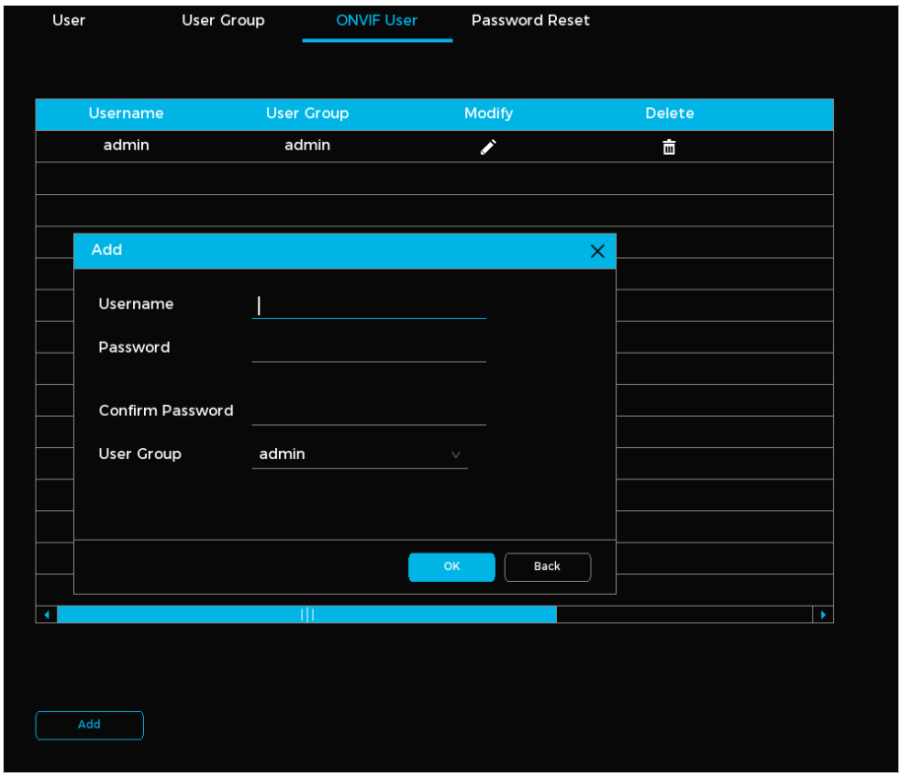


Add a User Group

3. Enter the **Group Name** for the new user group.
4. Check the boxes under **Live**, **Playback**, and **System** as required.
5. Click **OK** when done.

Add ONVIF Users

1. Navigate to **System** → **User Management** → **ONVIF User**.
2. Click **Add**.



Add an ONVIF User

3. Set the username, password, and user group.

ⓘ The three default ONVIF user groups are admin, operator, and user. You cannot add an ONVIF user group manually.

4. Click **OK**.

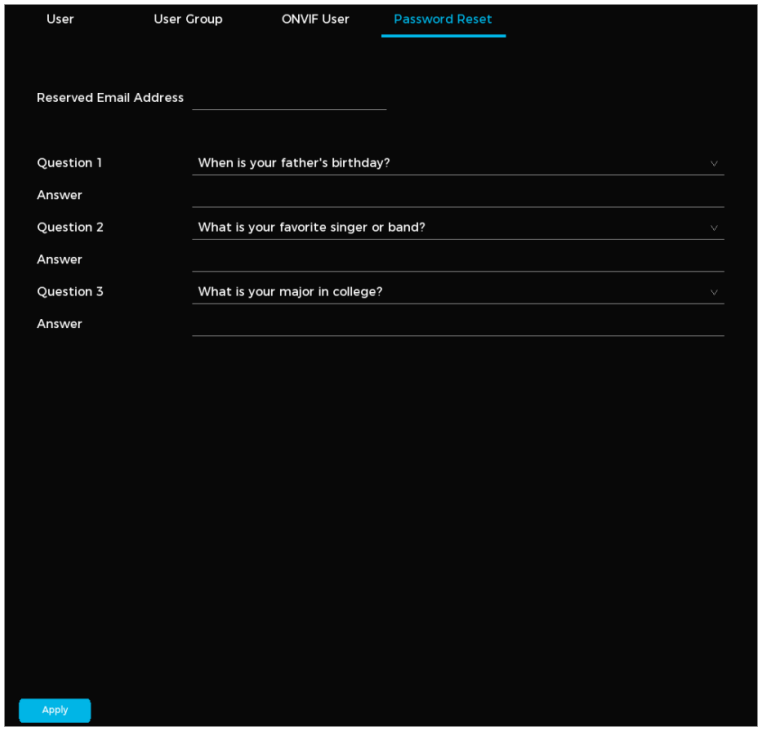
Reset a Password

The system offers several methods to reset forgotten passwords, including linked email addresses and security questions.

Configure a Password Reset

Follow the steps below to enable password recovery by setting a linked email address and creating security questions.

1. Navigate to **System → User Management → Password Reset**.



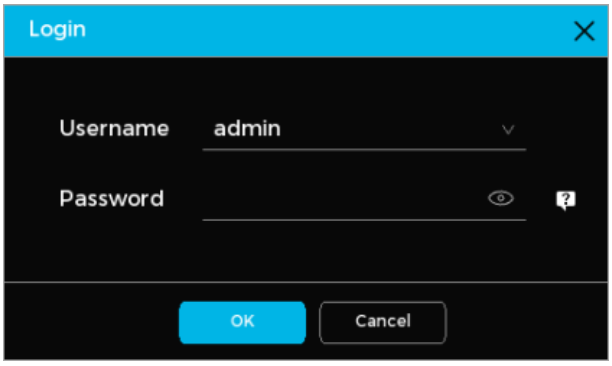
Password Reset

2. Enter a valid email address in the Reserved Email Address line. You will receive security codes for password recovery at this address.
3. Choose three security questions and input answers for them.
4. Click **Apply**.

Reset Your Password on a Local Interface

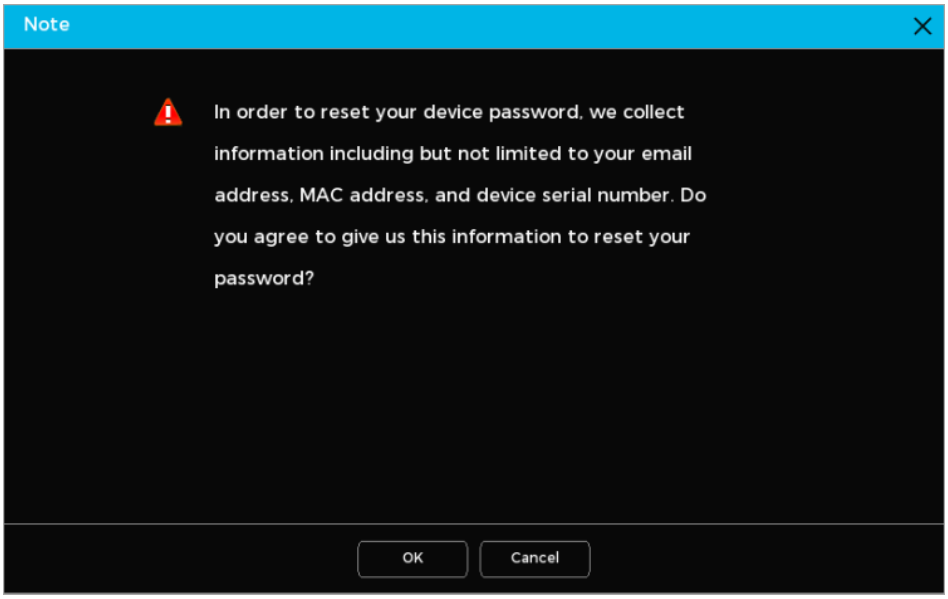
Follow the steps to reset your password using a device's local interface.

1. Power on your device.
2. Navigate to the login page.



Device Login Page

3. Click . If an email is linked to the device, the system will display a notification regarding data collection for the password reset. If no email address is linked, the system will prompt you to enter one.

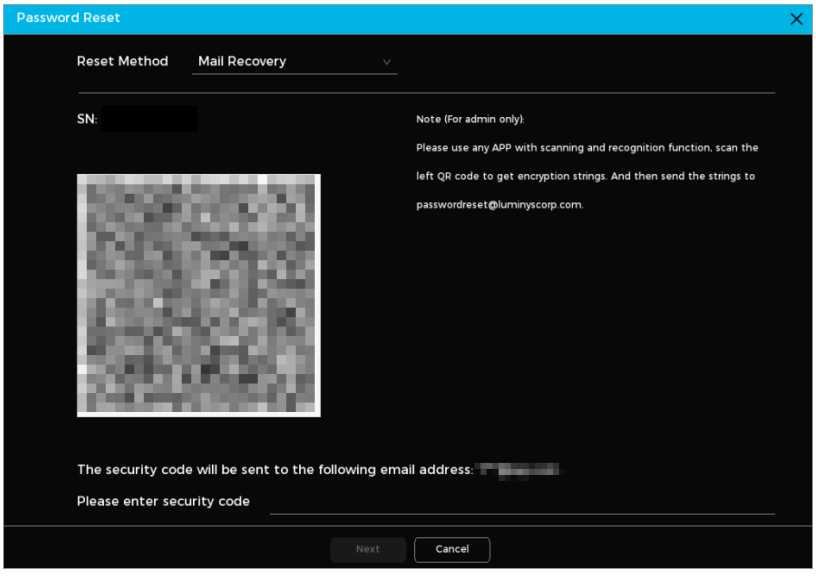


Data Collection Notice

4. Follow the instructions provided in the email to complete the reset process.

ⓘ You may also obtain the security code by scanning the QR code. A security code is valid for 24 hours.

5. Click **Next** after entering the security code.



Security Code Page

6. Set and confirm your new password.
7. Hit **OK** when done.

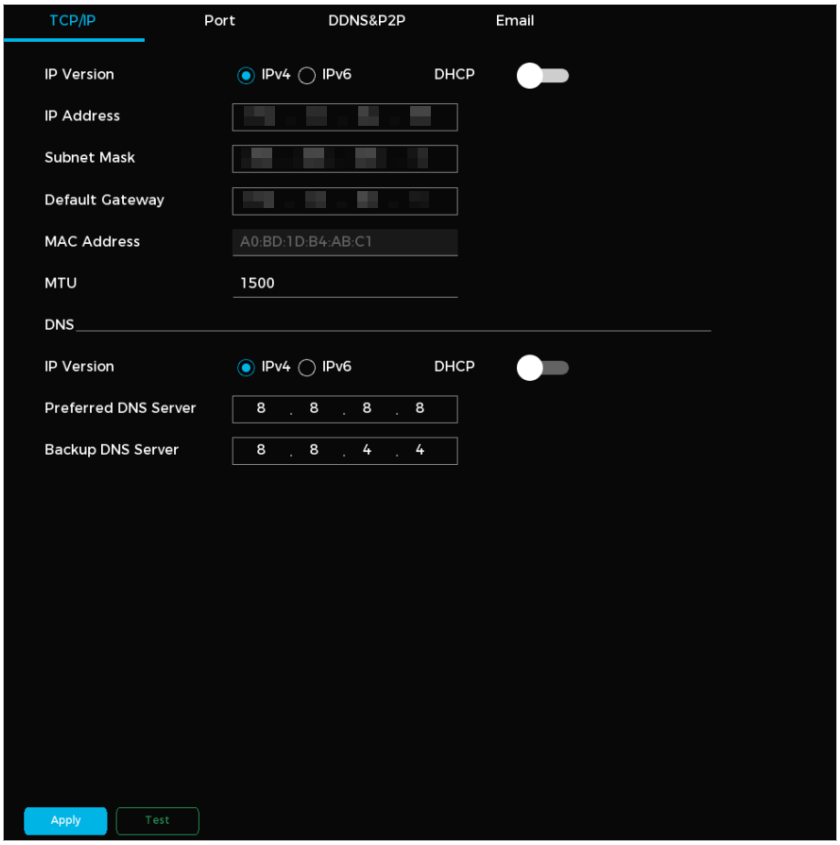
Configure Network Settings

Configure the network settings to enable seamless communication between the Device and other connected devices.

Configure TCP/IP Settings

Follow the steps below to configure the device's network parameters, including the IP address and DNS settings, to align with your network's requirements.

1. Navigate to **System → Network → Basic → TCP/IP**.



TCP/IP Settings

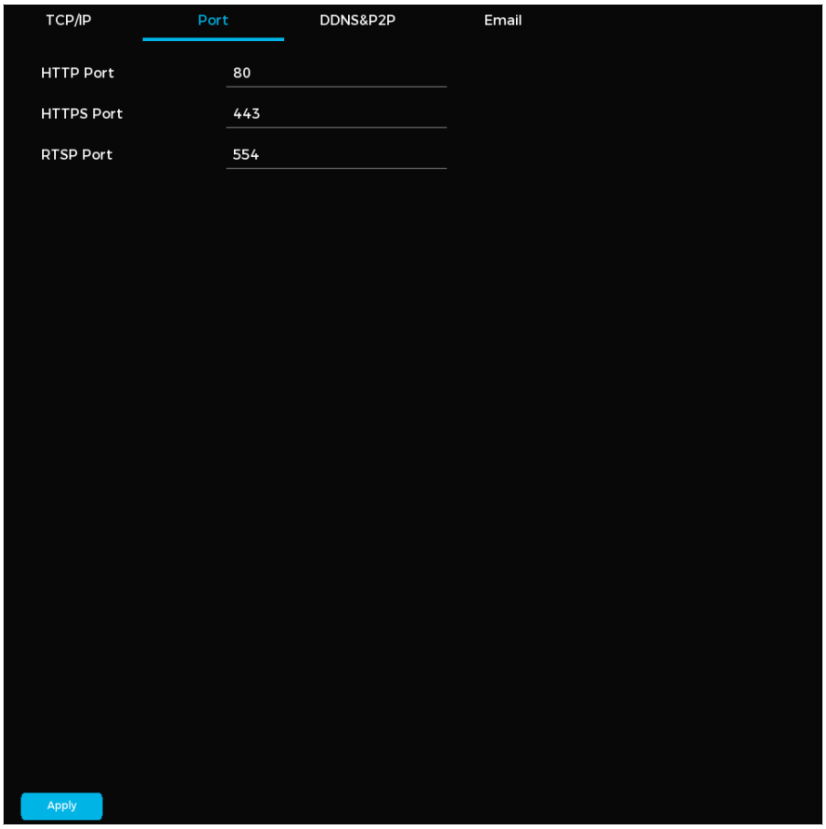
2. Configure the parameters. See the table below for more details. Not all the parameters listed in the table may be applicable.

Parameter	Description
IP Version	Choose between IPv4 and IPv6.
DHCP	Enable DHCP to allow the system to automatically assign a dynamic IP address. Manual configuration is not required when DHCP is enabled.
IP Address Subnet Mask Default Gateway	Enter the desired IP address for the device and configure the appropriate subnet mask and gateway settings. ⓘ • Ensure the IP address and default gateway are in the same network segment. • Click **Test** to ensure the specified IP address is accessible.
MAC Address	The system automatically displays the unique MAC address assigned to the device's network interface.
MTU	Displays the MTU size of the network adapter.

3. Set the IP version, primary DNS server address, and backup DNS server address.
4. Click **Apply**.

Configure Port Settings

1. Navigate to **System → Network → Basic → Port**.



Port Settings

2. Configure the parameters. See the table below for more details. Not all the parameters listed in the table may be applicable.

Parameter	Description
HTTP Port	Default value: 80. If changed (e.g., to 90), append the port number to the IP address for web access (e.g., http://[IP Address]:90).
HTTPS Port	Default value: 443. This port is used for secure HTTPS connections. You can modify this value according to your network requirements.
RTSP	Default value: 554. This port is used for Real-Time Streaming Protocol (RTSP). Adjust the value as needed for your streaming setup.

3. Click **Apply**.

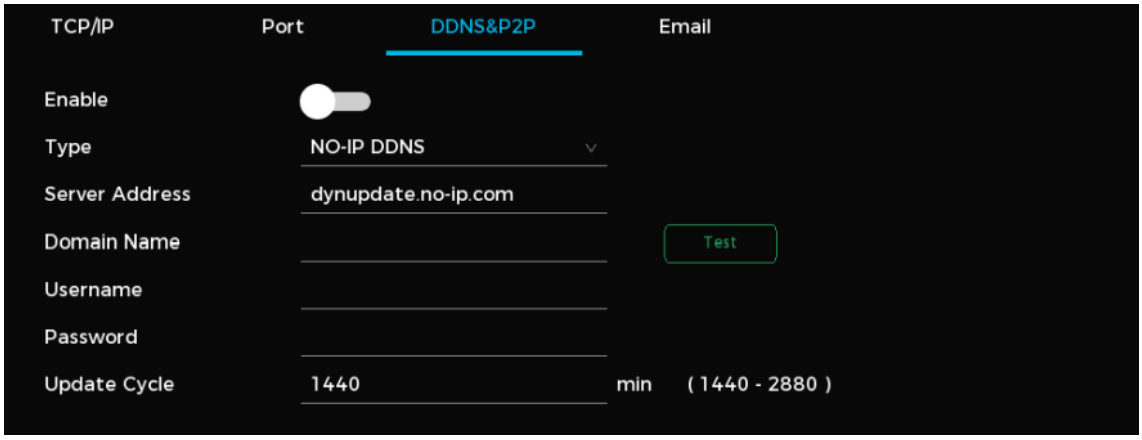
Configure DDNS Settings

Enabling DDNS ensures a consistent connection when the device's IP address changes frequently by dynamically updating the domain name and IP address mapping on the DNS server.

Before setting up DDNS, verify the supported DDNS types for the device. Then, log in to the DDNS service provider's website to register the required domain name and provide the necessary details. After registration, you can access the DDNS website to view and manage connected devices under your account.

Follow the steps below to configure DDNS settings.

1. Navigate to **System → Network → Basic → DDNS&P2P.**



DDNS Settings

2. Click  to enable the function.
3. Configure the parameters. See the table below for more details. Not all the parameters listed in the table may be applicable.

Parameter	Description
Type	Select the type of DDNS service provider. • **DvrList**: Default address is nsl.dvrlist.com. • **NO-IP DDNS**: Default address is dynupdate.no-ip.com. • **CN99 DDNS**: Default address is members.3322.org
Server Address	
Domain Name	The domain name you registered with the DDNS service provide.
Username	Enter the login information for the DDNS service provider.
Password	
Update Cycle	Set the time interval for updating the DDNS service. Values usually range between 1440–2880 minutes

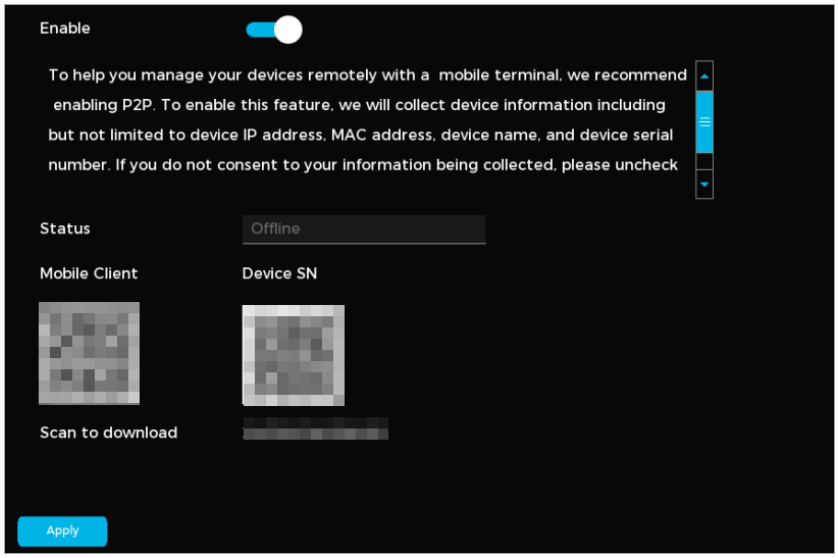
4. Click **Apply**. You can access the device's web interface using the registered domain name.

Configuring P2P Settings

P2P (peer-to-peer) enables remote device management through our mobile app. After downloading the app and linking the device, you can monitor its operations from your phone.

Follow the steps below to enable this feature.

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



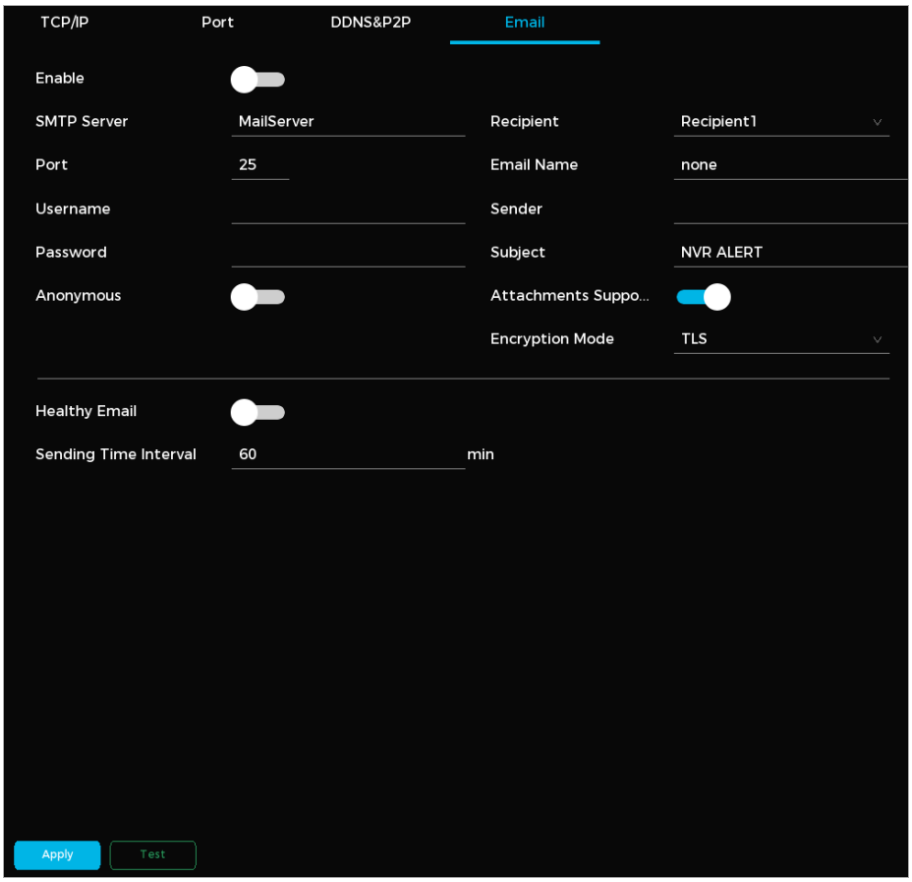
P2P Settings

2. Click  to enable the function.
3. Click **Apply**. Once enabled, use the mobile app to scan the QR code under "SN QR Code" for easy device addition and remote control.

Configure Email Settings

Follow the steps below to set up email notifications when an alarm event occurs.

1. Navigate to **System → Network → Basic → Email**.



Email Notifications

2. Click  to enable the function.

3. Configure the parameters. See the table below for more details. Not all the parameters listed in the table may be applicable.

Parameter	Description
SMTP Server	Enter the SMTP server address for the sender's email account.
Port	Specify the SMTP server port. The default number is 25.
Username	Enter the sender's email login information.
Password	
Anonymous	Enable anonymous login.
Recipient	Define up to three recipients for email alerts.
Email Name	Enter the recipient's email address.
Sender	Input up to three sender email addresses.
Subject	Input the email subject line for alarm notifications.
Attachments Supported	Enable to support the inclusion of attachments in notification emails.
Encryption Mode	Choose None, SSL, or TLS. The default encryption for an SMTP server is TLS.
Healthy Mail	Enable to periodically send a test email to check system health.
Sending Time Interval	Set the interval (in minutes) for sending test emails when Healthy Mail is enabled.

4. Click **Apply**.

5. Use the **Test** button to verify the email configuration is operational. If the test fails, check the SMTP details.

Configure UPnP Settings

Follow the steps below to establish a connection between the LAN and WAN to allow access to the device on the LAN via its WAN IP address

Configure the Router

1. Log in to the router.
2. Configure the WAN port.
3. Activate UPnP functionality.
4. Connect the Device to the router's LAN port.
5. Navigate to System → Network → TCP/IP on the device.
6. Assign an IP address within the router's range or enable DHCP.

Configure UPnP

1. Navigate to **System → Network → Advanced → UPnP**.

UPnP

2. Configure the parameters. See the table below for more details. Not all the parameters listed in the table may be applicable.

Parameter	Description
Port Mapping	Enable UPnP functionality to allow automatic port forwarding.
Status	Shows current UPnP connection status. An **online** status indicates the mapping process succeeded. An **offline** status indicates the mapping process fails.
LAN IP	Input the IP address of the router on the LAN. If mapping is successful, the system will assign an IP address automatically.
WAN IP	Input the WAN-side IP address of the router. If mapping is successful, the system will automatically retrieve the IP address.
Port Mapping Table	Displays port mapping relationship configurations. • **Service Name**: Network service name. • **Protocol**: Protocol type (i.e. TCP/UDP). • **Internal Port**: Port number for device that is used for communication. • **External Port**: Port number mapped on the router for external access. ⓘ • Avoid using common or reserved ports (e.g., 1–255 or system-assigned ports 256–1023). Use ports within 1024–5000 • For multiple devices on the LAN, ensure unique external ports to prevent conflicts. • Verify ports are not blocked, restricted, or in use by other services.

	• Internal and external ports must match the communication protocol (TCP/UDP). • Click  to adjust the external port mapping.

3. Click **Apply**. Visit the Device by going to http://WAN IP:External IP Port in your browser.

Configure SNMP Settings

SNMP allows integration with third-party software for network management. Tools like MIB Builder or MG-SOFT MIB Browser can be used to control and monitor the device remotely.

Prior to configuring SNMP settings, ensure the following prerequisites are met:

- Check if your device supports SNMP settings. This feature is limited to select device models.
- Install SNMP-compatible software (e.g., MIB Builder or MG-SOFT MIB Browser) on your computer.
- Obtain the latest MIB files for your device's firmware version from technical support.

Follow the steps below to configure SNMP settings.

1. Navigate **System → Network → Advanced → SNMP**.

SNMP Settings

2. Click  to enable the function.

3. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Version	Choose which version of SNMP protocol to use. The default is V3.
SNMP Port	Specify the port number for SNMP monitoring. The default port number is 161 (range: 1–65535).
Read Community	Enter the read/write strings accepted by the agent program.
Write Community	

Trap Address	Enter the IP address to send SNMP trap messages.
Trap Port	Enter the port number for the agent program to send trap information.
Read-Only Username	Enter the username with read-only access permission to the device.
Read/Write Username	Enter the username with read and write access permission to the device.
Authentication Type	Select either MD5 or SHA. The system will automatically detect the chosen type.
Authentication Password	Set a password for authentication. The password must be at least eight characters long.
Encryption Mode	Select an encryption type. The default is CBC-DES.
Encrypted Password	Input the encryption password as required.

4. Click **Apply**.
5. Compile the two MIB files using MIB Builder software.
6. Launch the MG-SOFT MIB Browser to load the compiled module.
7. Use the MG-SOFT MIB Browser to input the device IP you want to manage, select the query version, and view relevant configurations.
8. Navigate the tree-structured directory within the MG-SOFT MIB Browser to explore device configurations, including channel counts and software version details.

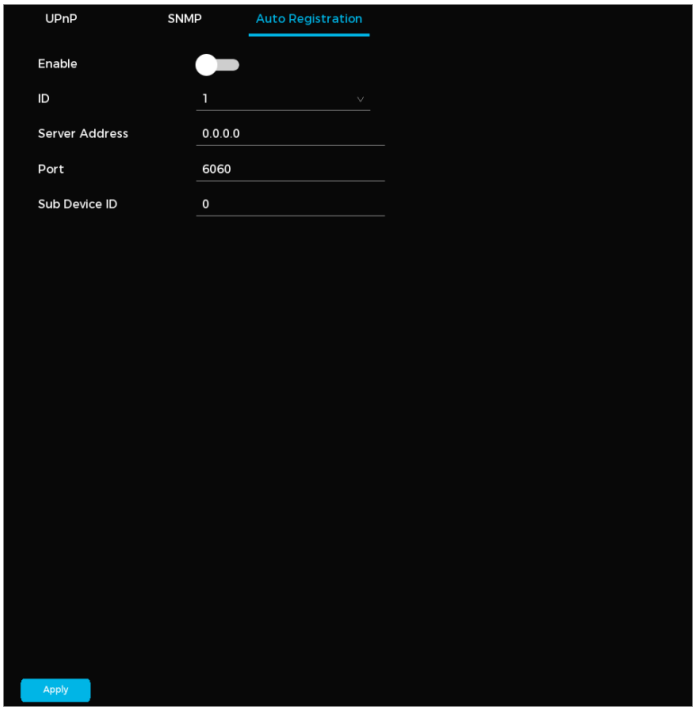
Configure Auto-Registration Settings

Prior to configuring auto-registration settings, ensure the following prerequisites are met:

- The proxy server is properly deployed and functional.
- The Device, proxy server, and client software are on the same network.

Follow the steps below to set up the Device to connect with a proxy server, enabling the client software to access the Device over the network.

1. Navigate to **Main Menu → NETWORK → Register**.



Auto-Registration Settings

2. Click  to enable the function.

3. Configure the parameters. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Server Address	Enter the IP address or domain name of the server you want to register with.
Port	Enter the server port.
Sub Device ID	Enter the ID given by the server.

4. Click **Apply**.

Configure Security Settings

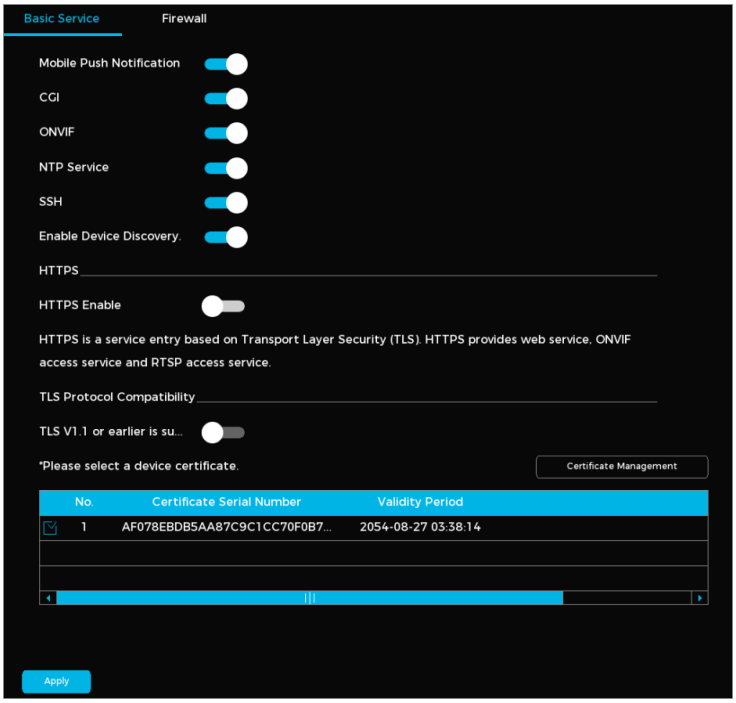
Set up essential security features, including basic services, HTTPS functionality, and the device firewall, to improve system and user protection.

Configure Basic Security Settings

Activate core services such as mobile push notifications, ONVIF, NTP, and SSH for optimal device performance and compatibility. Enabling HTTPS adds an extra layer of security, protecting user data and enhancing system security. HTTPS activation is strongly recommended for improved protection.

Follow the steps below to configure basic settings.

1. Navigate to **System → Network → Security → Basic Services**.



Basic Security Settings

2. Click the desired function. See the table below for more details.

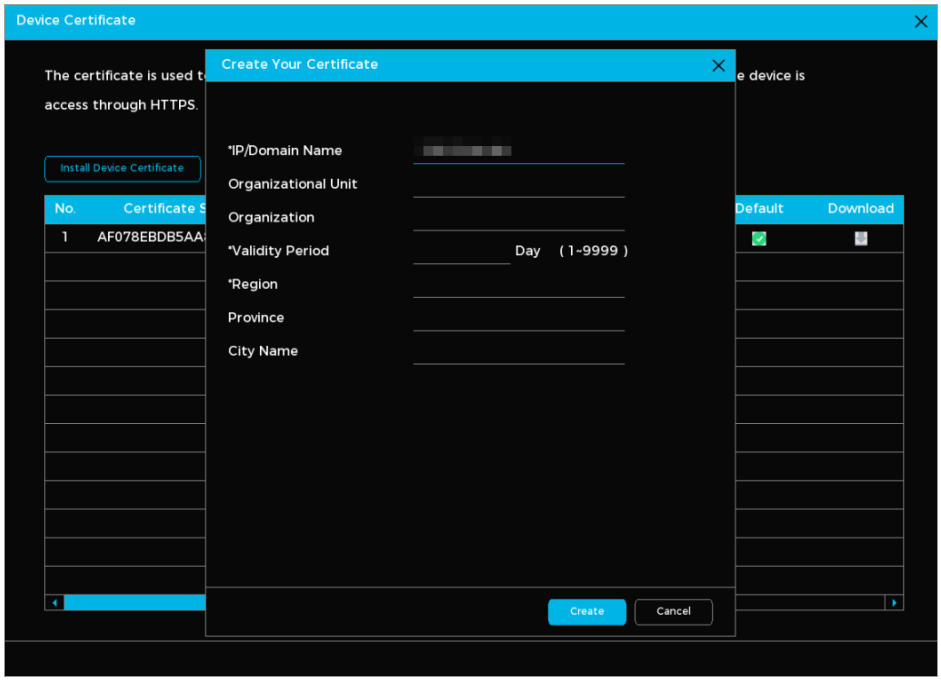
Parameter	Description
Mobile Push Notification	When enabled, alarm notifications are sent to the mobile device. To minimize security risks, disable this function when not required.
CGI	Allows for remote devices to be added via CGI protocol. This function is enabled by default.

ONVIF	Allows for remote devices to be added via ONVIF protocol. To minimize security risks, disable this function when not required.
NTP Service	Allows for time synchronization with the NTP server once enabled.
SSH	Allows system debugging and IP configuration via SSH protocol once enabled. To minimize security risks, disable this function when not required.
Enable Device Discovery	Makes the device discoverable by other devices.

3. Click  to enable HTTPS.
4. Click  to enable TLS protocol compatibility.

ⓘ TLS (Transport Layer Security) secures communication by maintaining data integrity and privacy between applications.

5. Open **Certificate Management** to create an HTTPS certificate.
6. Click **Install Device Certificate**.
7. Configure the parameters.
8. Click **Create**.



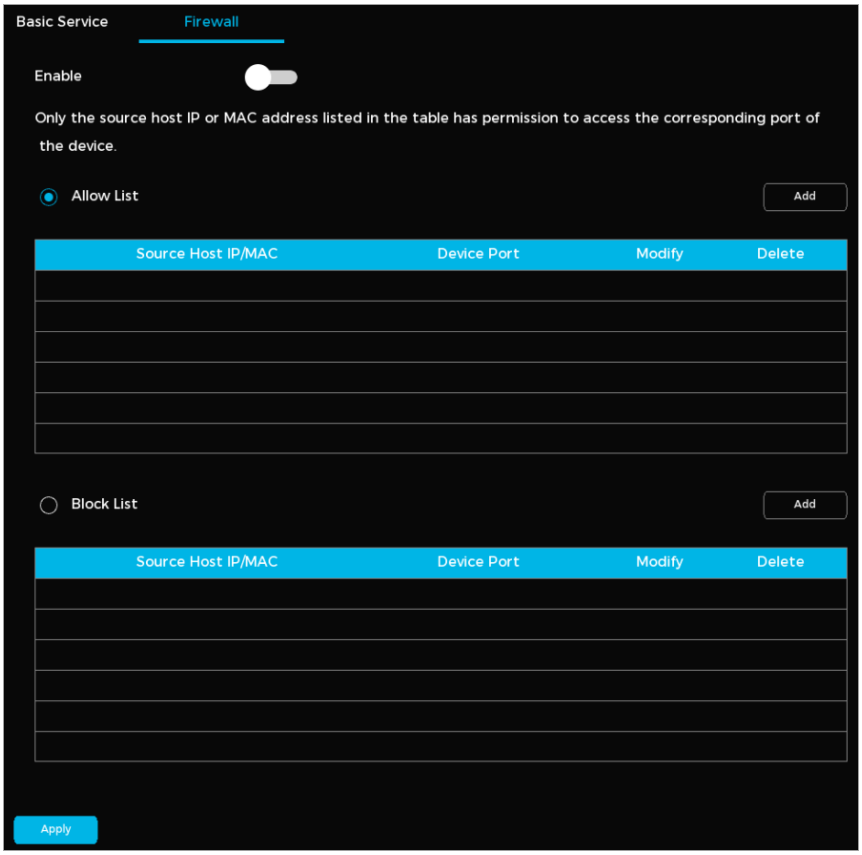
Certificate Management

9. Click **Apply** to save the certificate settings.

Configure Firewall Settings

Follow the steps below to configure firewall settings and define hosts that are permitted or restricted from accessing the Device.

1. Navigate to **System → Network → Security → Firewall**.



Firewall Parameters

2. Click  to enable the function.
3. Choose a firewall mode: Allowlist (only hosts listed can access the device) or Blocklist (restricts hosts listed from accessing the device).
4. Click **Add**.
5. Specify the IP address (including starting and ending port), IP segment (including starting and ending address and ports), or MAC address.
6. Click **Apply**.

Configure IP Speaker Settings

Follow the steps below to manually configure IP speakers and link them with a camera.

1. Navigate to **System → Network → IP Speaker**.
2. Click **Manually Add**.
3. Fill in the speaker's details.
4. Click **Settings** to link the speaker with a camera.
5. Click **Apply**.

Related Operations

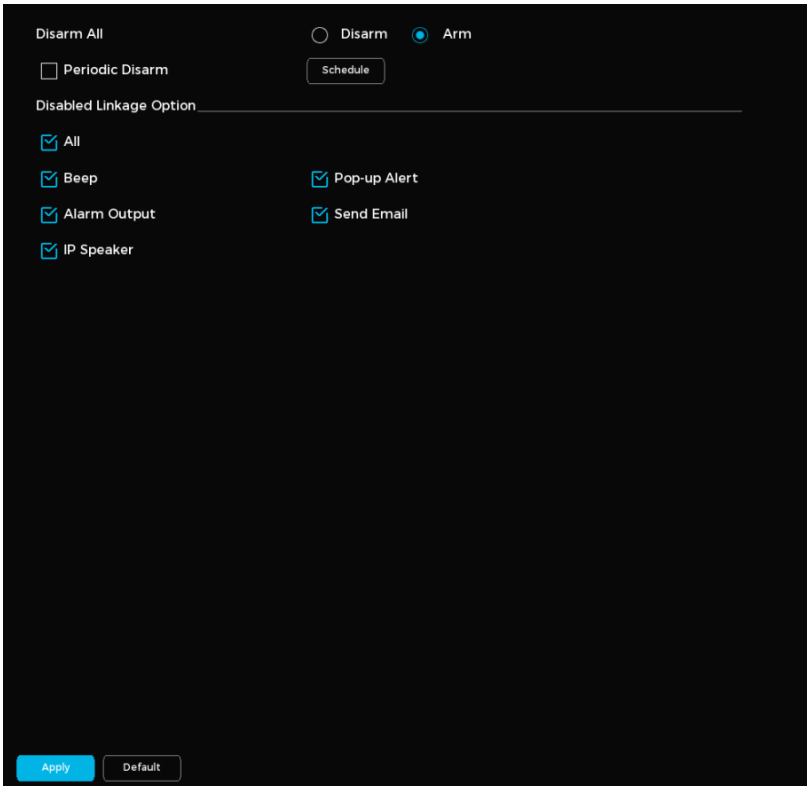
- **To modify the speaker's details**: Click  .
- **To delete the speaker**: Click  .

Configure Alarms

Disarm All Alarms

Follow the steps below to disarm all alarms.

1. Navigate to **System → Alarm → Disarm All**.



Disarm Alarms

2. Enable the disarm function. You can select **Disarm All** or **Periodic Disarm**.

ⓘ

- **Disarm All**: You must select Arm (the alarm will remain active continuously until you select Disarm).
- **Periodic Disarm**: Select **Disarm for Disarm All**. Click **Schedule** to define a disarm schedule (the alarm will deactivate during specified times).

3. Choose which alarm linkage features to disable. See the table below for details.

Parameter	Description
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Send Email	Enable email notifications when an alarm is triggered.

	ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.

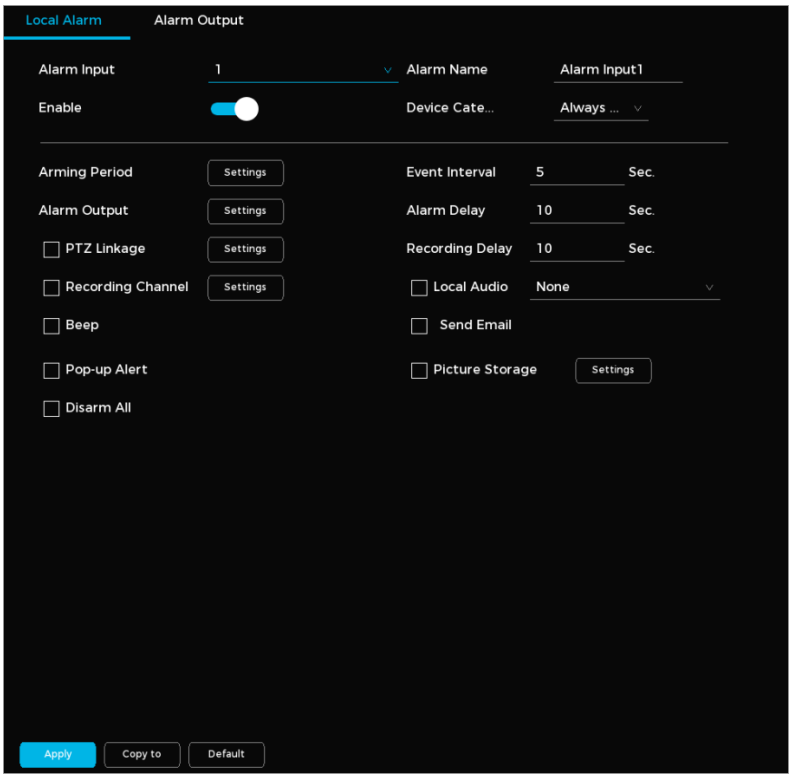
4. Click **Apply** when done.

Configure Local Alarm Settings

When an alarm device is connected to the NVR's alarm input port, the system detects the signal and triggers the configured alarm linkage actions.

Follow the steps below to configure local alarm settings.

1. Navigate to **System → Alarm → Alarm Settings → Local Alarm**.



Local Alarm Settings

2. Select an **Alarm Input**. Set an alarm name.
3. Click  to enable the alarm.
4. Choose between **Always Closed** or **Always Open** from the **Device Category** dropdown.
5. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording.

	ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

6. Click **Apply** when done.

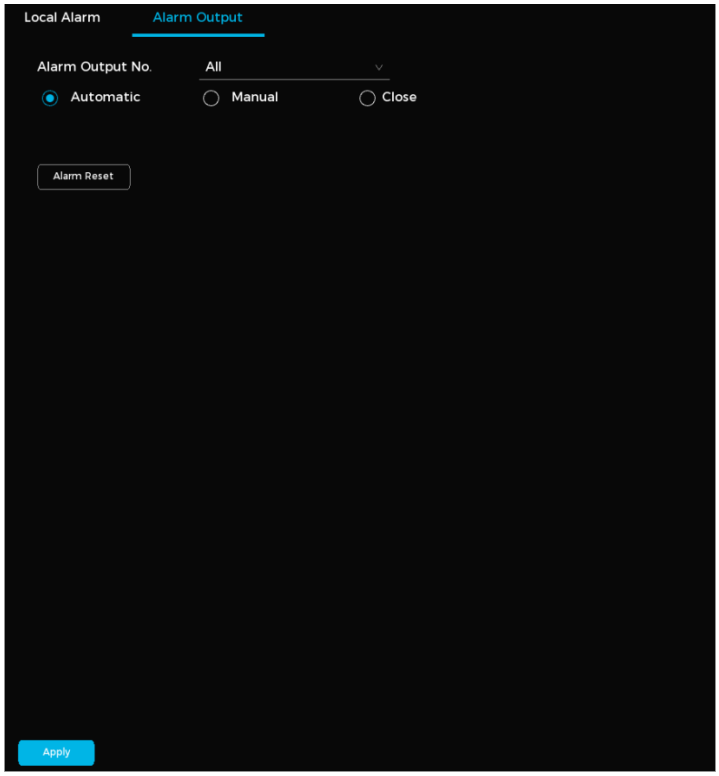
Configure Alarm Output

You can set the alarm output mode to **Automatic**, **Manual**, or **Close** to control the alarm device's behavior after connecting to the NVR alarm output port. In **Automatic** mode, the system triggers alarm linkage actions when an alarm event occurs.

- **Automatic Mode**: The system automatically generates an alarm when an alarm event occurs.
- **Manual Mode**: The alarm device remains active in alarming mode at all times.
- **Close Mode**: The alarm output function is disabled, and no alarm is triggered.

Follow the steps below to set the alarm output.

1. Navigate to **System → Alarm → Alarm Settings → Alarm Output**.
2. Select the Alarm Output No.
3. Select the alarm output mode.



4. Click **Apply**.

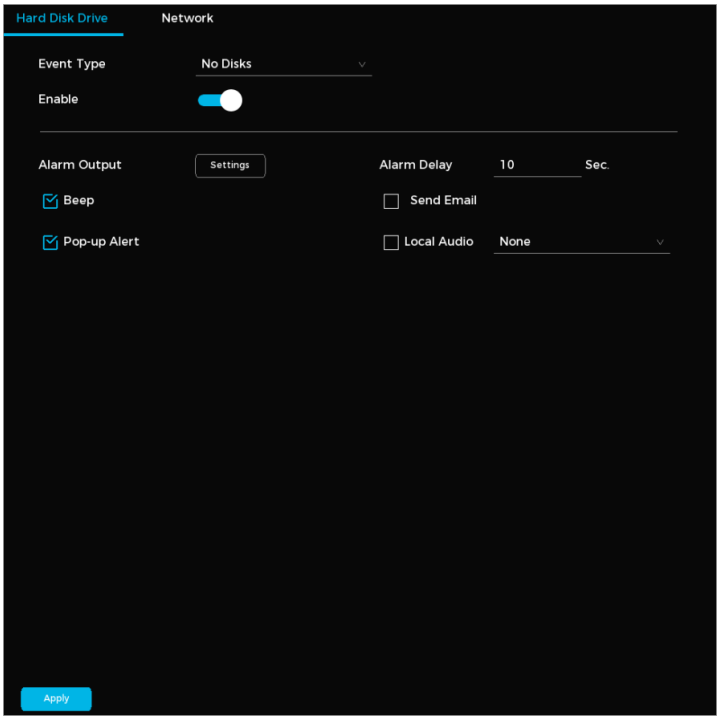
Related Operations

- **Alarm Reset**: Clears all current alarm statuses.
- **Status**: View updated alarm output status.

Configure Storage Error Alarms

Follow the steps below to set an alarm to trigger when a storage-related issue occurs.

1. Navigate to **System → Alarm → Exception → Hard Disk Drive**.



Storage Error Alarm Settings

2. Choose one of the following from the **Event Type** dropdown menu: **No Disks** (no disk is detected), **Hard Disk Error** (triggers if a disk malfunctions), or **Insufficient Storage Capacity** (triggers when storage is low).
3. Click  to enable the alarm.
4. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

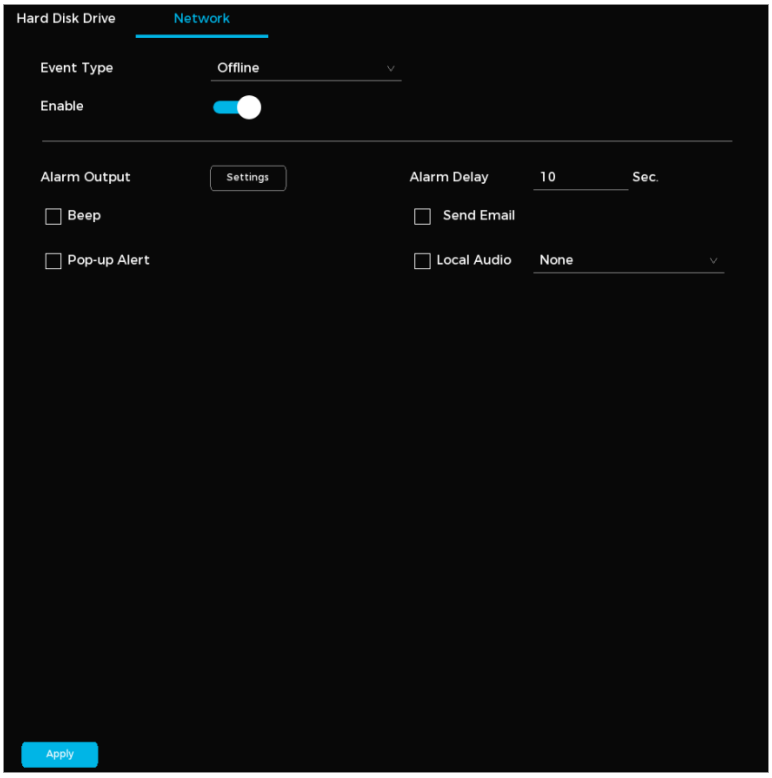
Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

5. Click **Apply**.

Configure Network Error Alarms

Follow the steps below to configure an alarm when a network error occurs.

1. Navigate to **System → Alarm → Exception → Network.**



Network Error Alarm

2. Select one of the following event types: **Offline** (when network connection is lost), **IP Conflict** (when duplicate IP addresses are detected), or **MAC Conflict**.
3. Click  to enable the alarm.
4. Configure the alarm linkage actions. See the table below for more details. Not all parameters listed in the table may be applicable.

Parameter	Description
Arming Period	Click **Settings** to set the time for motion detection monitoring.
Alarm Output	Click **Settings** next to Alarm Output. Click  to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
PTZ Linkage	Select the checkbox. Click **Settings** to configure PTZ linkage. ⓘ Ensure PTZ control has been configured.
Recording Channel	Select the channel(s) for recording. ⓘ Ensure the recording plan and mode are set by going to **Storage → Recording Plan**.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
IP Speaker	Select the checkbox. Click **Settings** to bind an IP speaker with the camera. ⓘ Ensure the IP speaker is added to the system.
Event Interval	Set the time between the end of a motion detection event and the end of an alarm linkage action.

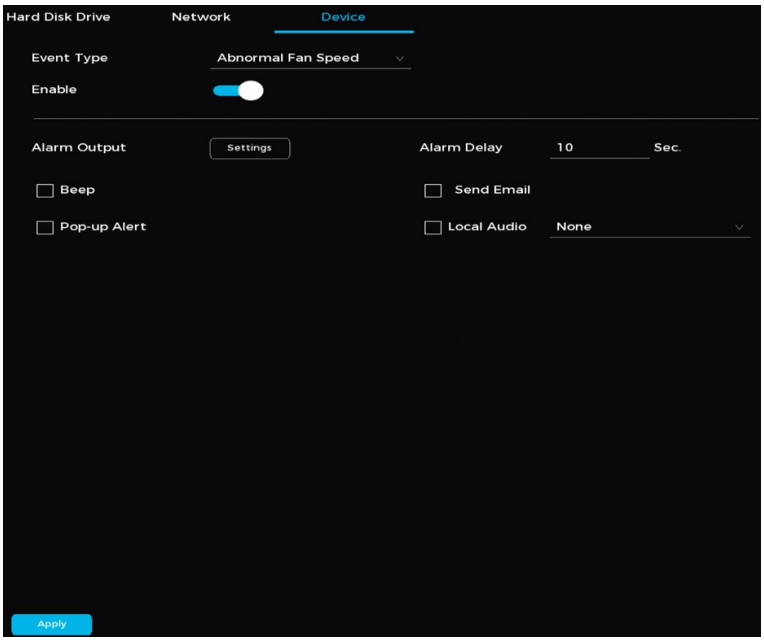
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.
Recording Delay	Set the length of time a device will continue to record after an alarm ends.
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.
Picture Storage	Enabling this feature will have the system take snapshots of the selected channel when an alarm occurs and store them on the device. ⓘ Ensure the snapshot channel and snapshot mode has been configured.

5. Click **Apply**.

Configure Device Error Alarms (R5 Models Only)

Follow the steps below to configure device error alarms.

1. Navigate to **System → Events → Exception → Device.**



Device Error Alarm

2. Choose an event from the **Event Type** dropdown menu.
3. Click to enable the alarm.
4. Configure the parameters. See the table below for more details. Not all parameters may be applicable.

Parameter	Description
Alarm Output	Click **Settings** next to Alarm Output. Click to enable the local alarm. Select the required alarm output port. ⓘ Ensure the alarm state for the output port is configured.
Beep	Enable a beeping noise when an alarm is triggered.
Pop-Up Alert	Enable a pop-up window to appear when motion is detected.
Alarm Delay	When configured, the alarm will continue to play for a period after the alarm duration ends.

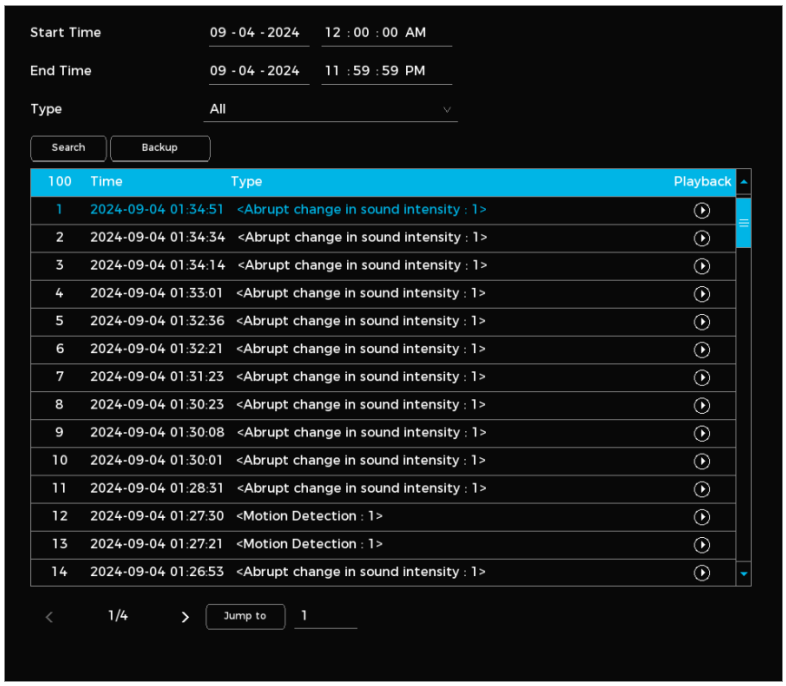
Local Audio	Enable this feature to choose a local audio file as an alarm sound.
Send Email	Enable email notifications when an alarm is triggered. ⓘ This function is only available on select models. Ensure email functionality has been configured by going to **System → Network → Basic → Email**.

5. Click **Apply** when done.

Search for Alarm Information

Follow the steps to retrieve, view, and back up alarm information.

1. Navigate to **System → Alarm → Event Search**.
2. Define the search period.
3. Specify the event type.
4. Click **Search**.



Alarm Information Search

Related Operations

- **To view details**: Select a record. Double click.
- **To back up alarm records**: Click **Backup** to export and save alarm records to a USB storage device.
- **To play recorded video**: Click  .

View Alarm Status

To view current alarm status, navigate to **System → Alarm → Event Search.**

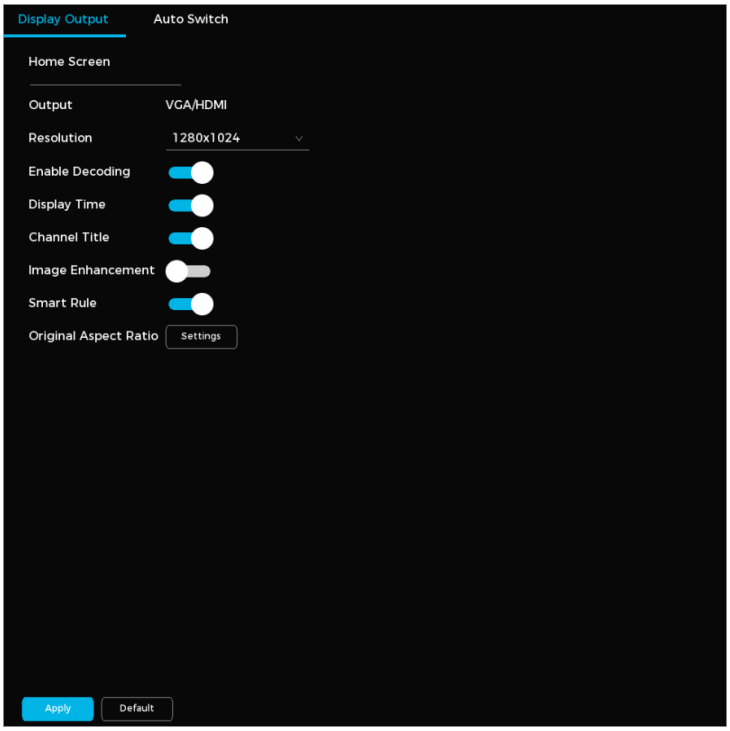
Alarm Status

Configure Display Settings

Configure Display Output

Follow the steps below to customize the display settings to show the time, title, and channel information. You can also adjust image transparency, define resolution, and modify other related settings.

1. Navigate to **System → Display → Display Output**.



Display Output Settings

2. Configure the parameters. See the table below for more details.

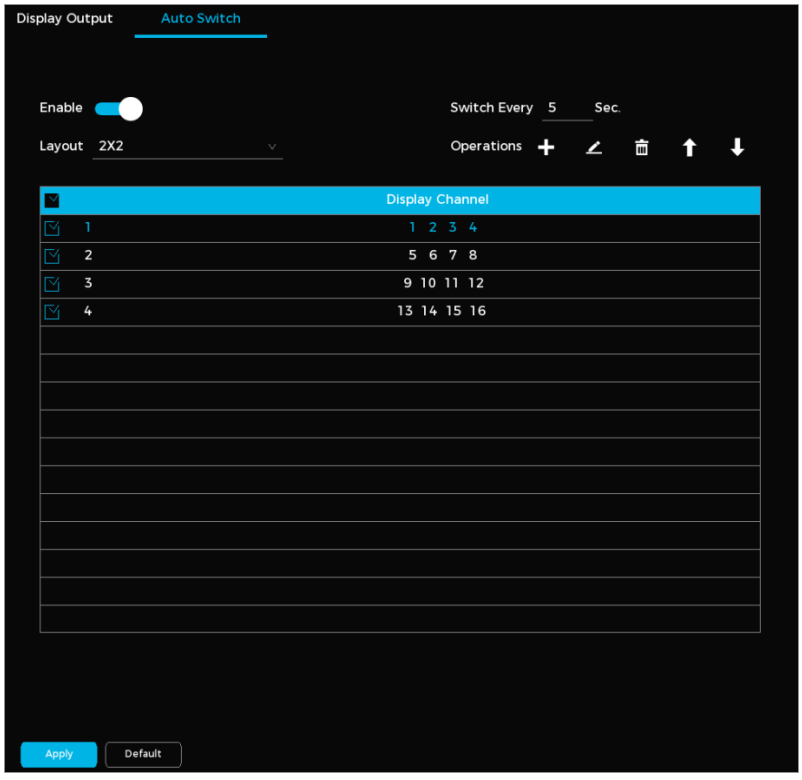
Parameter	Description
Resolution	Select a video display resolution. The default is 1280 x 1024.
Enable Decoding	Enable the decoding feature for live streams.
Display Time	Show the time on live channel windows.
Channel Title	Show the channel name, number, and recording status.
Image Enhancement	Optimize live images for enhanced clarity and visibility.
Smart Rule	Display intelligent rule overlays in live channel windows.
Original Aspect Ratio	Click **Settings**. Choose channels to maintain the original image scale.

3. Click **Apply**.

Configure Auto-Switch

Follow the steps below to set up a channel tour to play videos in sequence. Based on the configured channel groups, videos are displayed one after another. The system automatically switches to the next group after the preset duration.

1. Navigate to **System → Display → Auto Switch**.
2. Click  to enable the function.



Auto-Switch

3. Set the parameters. See the table below for more details.

Parameter	Description
Switch Every	Specify the seconds between switching channel groups.
Enable Decoding	Set the screen layout (i.e. 2 x 2, 3 x 3).

Display Time	Select the channel groups for the auto-switching tour. Use the operation buttons to add, modify, delete, or reorder channel groups as needed.

4. Click **Apply**. You can enable or disable the tour by clicking  .

Configure Audio Settings

Upload an Audio File

Follow the steps below to add, listen to, rename, and delete audio files. You can also adjust the volume settings.

1. Navigate to **System → Audio → Audio File**.
2. Click **Upload**.
3. Select the audio file. Click **Import**.

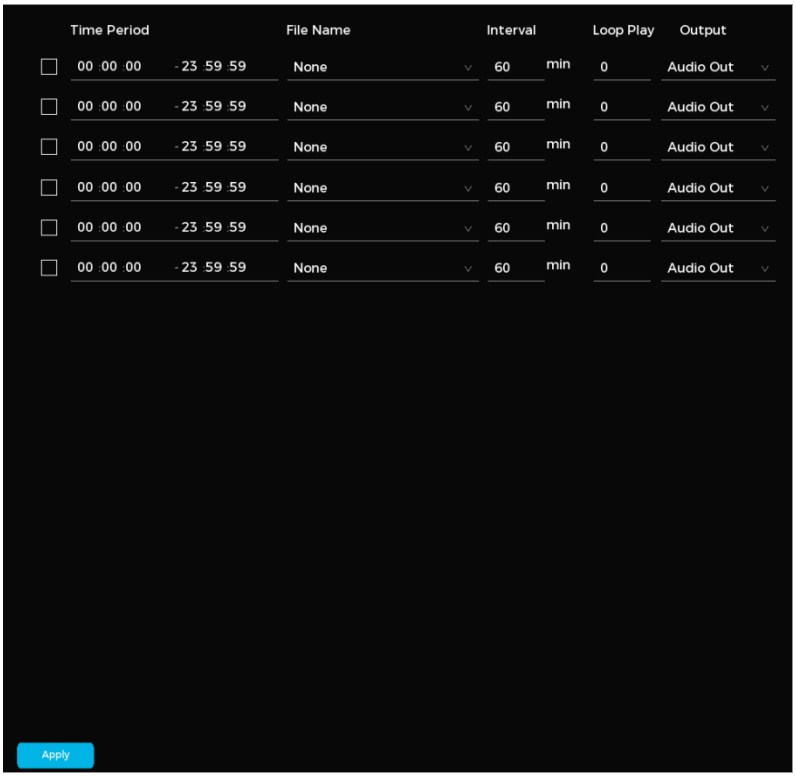
ⓘ Only MP3 and PCM file formats are supported.

4. Click **OK** to begin the import. The uploaded files will be listed under **Audio File** page.

Configure Audio Play

Follow the steps below to schedule specific audio files to play for a set duration.

1. Navigate to **System → Audio → Audio Play**.



Audio Play

2. Set the parameters. See the table below for more details.

Parameter	Description
Period	Specify the seconds between switching channel groups.
File Name	Set the screen layout (i.e. 2 x 2, 3 x 3).
Interval	Select the channel groups for the auto-switching tour. Use the operation buttons to add, modify, delete, or reorder channel groups as needed.

Loop	Specify how many times the audio file should repeat within the scheduled playback period.
Output	Choose between **MIC** and **Audio** options. By default, **MIC** is selected. The MIC function shares the same port as the talkback feature, which takes priority when both are active. Not all models will have an audio port.

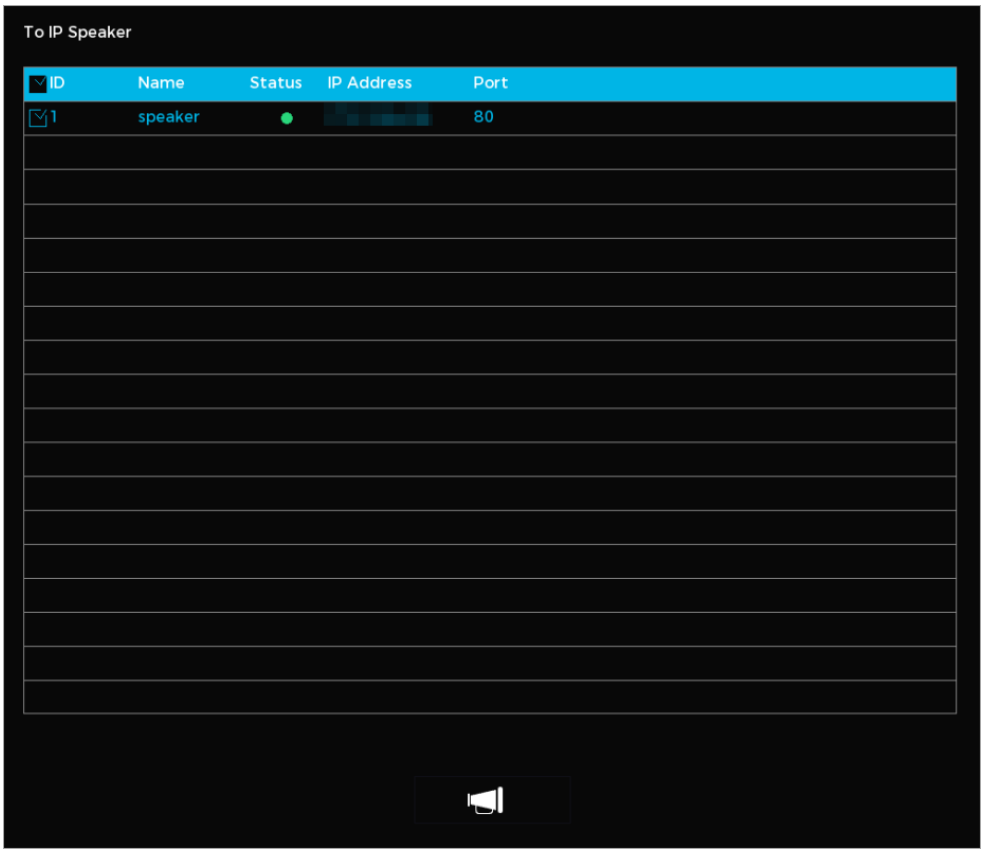
ⓘ The playback duration depends on the selected audio file size and the configured interval.

3. Click **Apply**.

Broadcast to IP Speaker

Follows the steps below to set up the system to broadcast to an IP speaker. Ensure at least one speaker is linked to the system prior to setup.

1. Navigate to **System → Audio → To IP Speaker**.



Broadcast to IP Speaker

2. Select the IP speaker.
3. Click  to broadcast.

Maintenance

Go to **System Maintain** to update the system, restore factory settings, and manage other maintenance tasks.

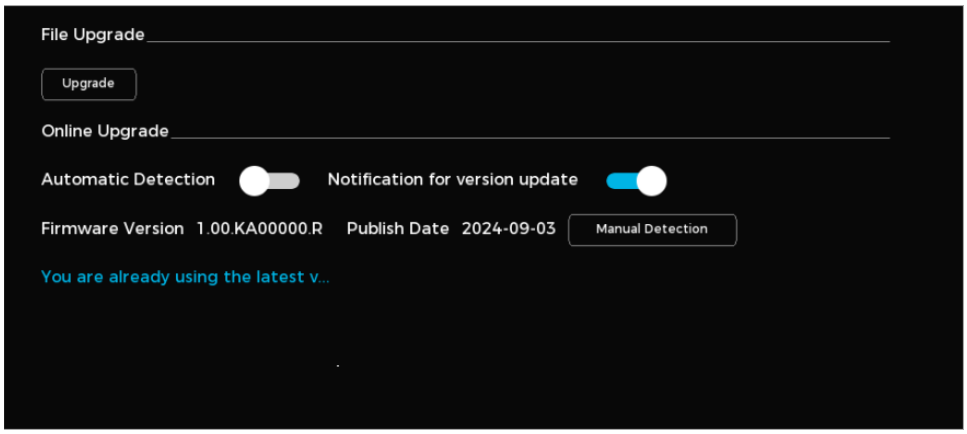
Update the System

You can update the system using either the File Update method or the Online Update.

File Update

Follow the steps below to update the system via file update.

1. Connect a USB storage device with the system update file into the Device.
2. Navigate to **System → System Maintain → Upgrade**.



File Upgrade

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

Online Update

Follow the steps below to update the system online. Ensure the Device is connected to the network prior to updating.

1. Navigate to System → Maintain → Upgrade.
2. Check for updates. You can enable **Automatic Detection** or **Manual Detection**.

ⓘ If the message "You are already using the latest version" appears, no update is needed.

3. Click **Upgrade Now**.

Restore Defaults

If the system encounters performance issues or configuration errors, use the **Restore Defaults** feature to reset it to factory settings and resolve the issues.

Restore Defaults on the Local Interface

Follow the steps below to restore the device's default settings on the local interface.

1. Navigate to System → System Maintain → Default.
2. Click **Restore** to reset the configurations.

ⓘ All settings except network configurations and user management settings will be restored to their defaults.

Reset the Device via the Reset Button

Follow the steps below to restore the device to its factory settings using the reset button on the mainboard.

ⓘ This feature is only available on select device models.

1. Power off the device.
2. Remove the device cover.
3. Press and hold the reset button on the mainboard for 5 to 10 seconds. The device will be restored to factory settings upon reset.

ⓘ The location of the reset button will vary depending on device model.

Export and Import System Configurations

You can back up or restore the system configuration file to prevent data loss. Backups allow you to recover settings if the device is reset or reconfigured.

⚠ Configuration files cannot be imported or exported while another backup process is in progress.

Export System Configurations

1. Navigate to **System → System Maintain → Import/Export**.

Configuration Maintenance

2. Connect a USB storage device to the system.
3. Click **Export**. The configurations will be saved in a folder named **Config_[YYYYMMDDhhmmss]**.

Importing System Configurations

1. Connect the USB storage device with the configuration file to the system.
2. Navigate to **System → System Maintain → Import/Export**.
3. Select the configuration folder. The default folder name follows the format **Config_XX**.
4. Click **Import**. The device will automatically restart once the configurations are imported.

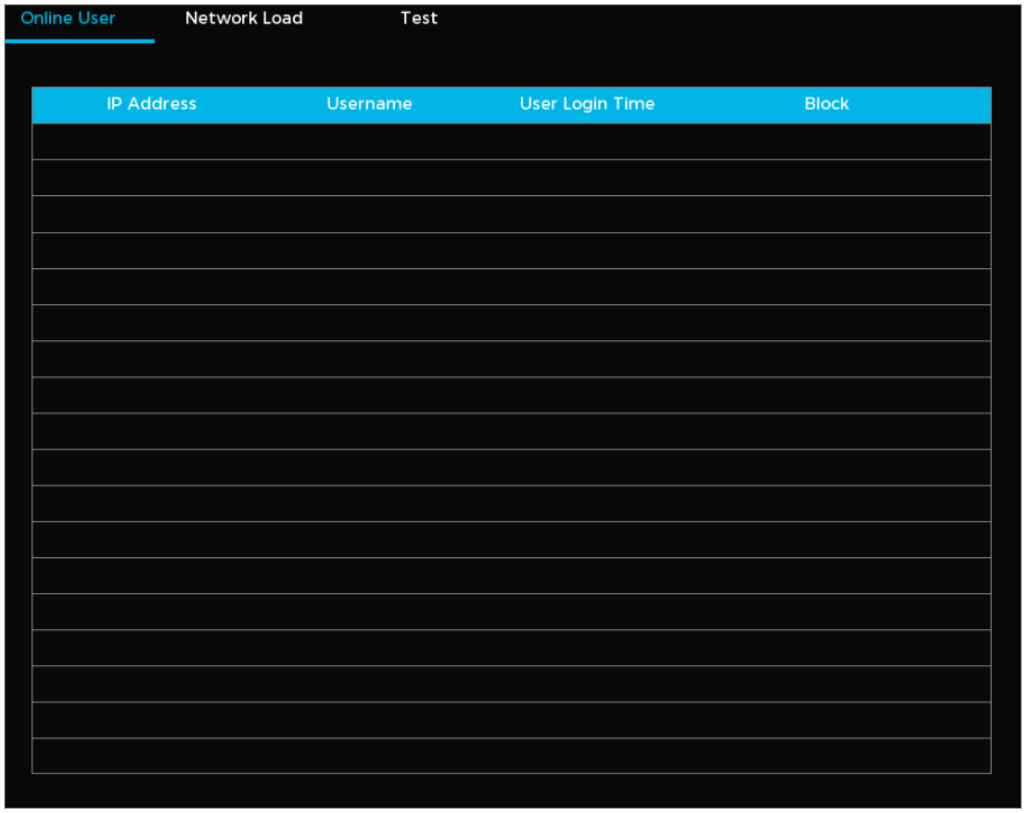
⚠ Any previous configurations will be overwritten.

View Network Information

Monitor and manage network activity by viewing details of online users, analyzing network load, and testing the network connection.

View Online Users

Go to **System → System Maintain → Network → Online User** to view details of users currently logged into the system, including their IP address, username, login time, and status. You can also block a specific user from accessing a device by locating the user on the list and clicking the block icon.



Online Users

View Network Load

Follow the steps below to monitor the device's data transmission performance by tracking the sending and receiving rates of connected networks. This helps diagnose potential network bottlenecks or other issues in real-time.

1. Navigate to **System → System Maintain → Network → Network Load**.
2. Click the **LAN name** in the list to view its associated sending and receiving rates. Only one LAN network can be viewed at a time.

Test the Network

To diagnose and troubleshoot network issues, test the device's connection to other networked equipment. The packet capture feature helps identify and resolve potential network problems.

1. Navigate to **System → System Maintain → Network → Test**.
2. Connect a USB storage device to the system to save the captured packets.
3. Click **Refresh** to detect the connected USB device. Once detected, the **Device Name** field will update with the name of the USB storage device.
4. Click **Browse** to specify where the packets should be stored.
5. Click  to initiate packet capture and backup. Click the icon again to stop capturing.

ⓘ

- Simultaneous packet capturing across multiple network adapters is not supported.

- Packet capturing allows you to navigate to other pages for different operations. Return to the **Test** page to stop the capture when you're finished.

6. Enter the destination IP address. Click **Test**. You can view the load of one network adapter at a time.

Configure Automatic Reboot

Enabling automatic reboot allows the device to restart during idle times, helping maintain optimal system performance and stability. Follow the steps below to configure automatic reboot.

1. Navigate to **System → System Maintain → Auto Reboot**.
2. Specify a time for the automatic reboot to occur during system inactivity.
3. Click **Apply**.

System Information

The **System Information** section provides detailed information about the device's status and includes log search functionalities.

View System Information

Navigate to **System → System Info → Device Info** to review comprehensive details about the device's operational status.

Version Information

- Device Model
- Alarm Input/Output Configuration
- Firmware Version
- System Version
- ONVIF Version
- Other System Attributes

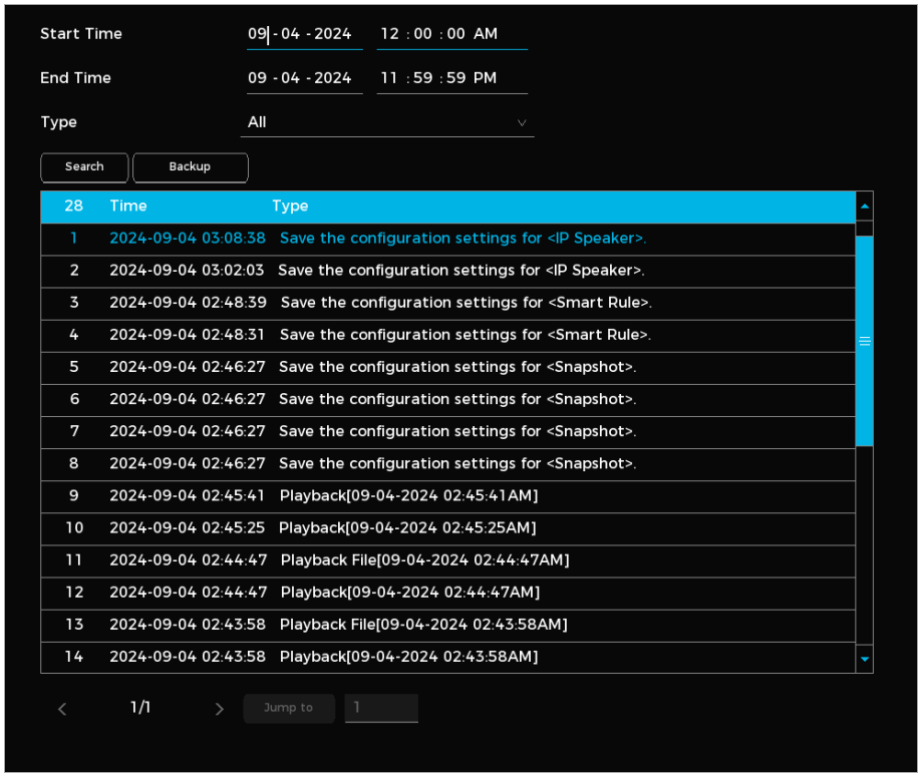
Disk Information

- Disk Name and Location
- Total and Available Storage Capacity
- Health Status
- **Stream Information**
  - The resolution and stream rate of each channel.
  - Use the Waveform feature to analyze the real-time stream's stability and fluctuation patterns
- **Network Information**
  - DHCP and Static IP Settings
  - IPv4/IPv6 Addresses, Subnet Masks, and Gateway Details
  - Mac Addresses and DNS Configurations

Search for Logs

You can search and review logs to monitor system operations and identify issues. Logs related to system operations are saved in the device’s memory, while other logs are stored on the HDD. If the HDD is unavailable, all logs are saved in the device’s memory instead. Formatting the HDD will preserve logs, but if the HDD is removed, stored logs may no longer be accessible.

1. Navigate **System → System Info → Log Info**.
2. Specify the time frame to retrieve logs.
3. Choose the type of logs you want to search for.
4. Click **Search**.



Log Search Results

Related Operations

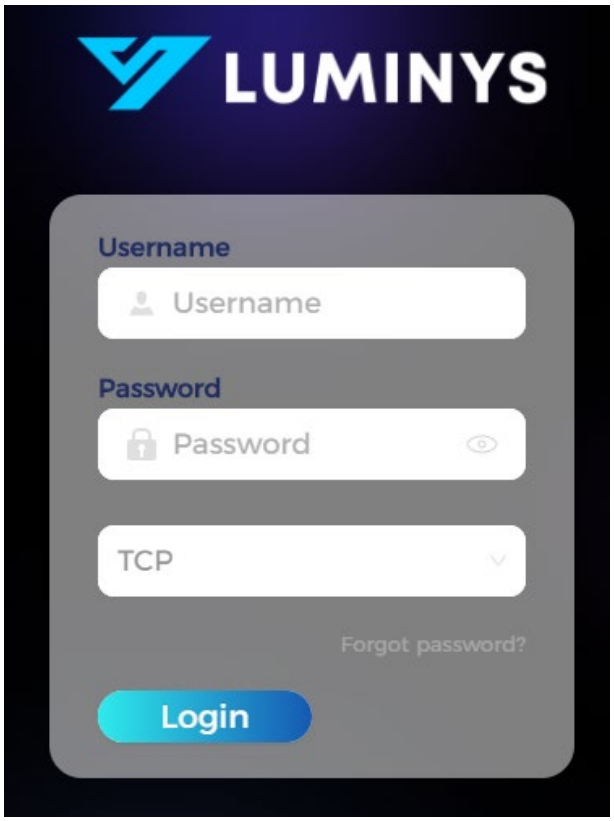
- **To view details**: Select a log from the list. Double click. Use the previous or next buttons to navigate between log entries.
- **To backup logs**: Click **Backup**.

Web Operations

Log in to the Web

Prior to logging in, ensure your computer and the Device's IP address are within the same network segment. Follow the steps below to log in to the device web interface.

1. Navigate to the Device's IP address using the browser's address bar.

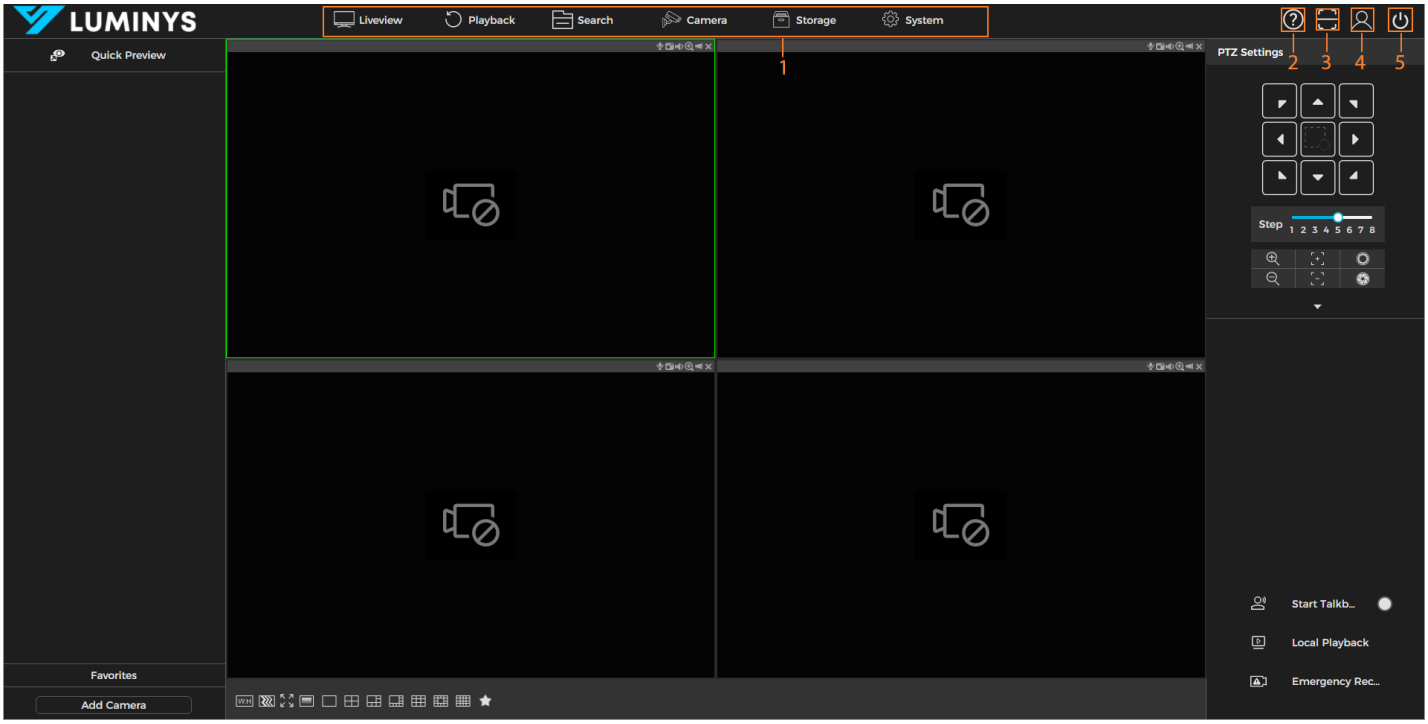


Login Screen

2. Enter the Device's login credentials.
3. Hit **Login**.

Web Main Menu

The main menu will be displayed after logging in.



Web Main Menu

Number	Name	Description
1	Function Tiles	Click on any tile to open its corresponding configuration page for further actions.
2	Help	Scan the QR code to download the user manual directly to your device.
3	Scan	Use the QR code to download the mobile app and add the device for remote management.
4	Login	Click this option to log out of the current account safely.
5	Shut Down	Select this option to restart or completely shut down the device.

Appendix 1: HDD Capacity Calculation

To calculate the HDD capacity required for video storage, use the following formula:

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

To calculate for recording, use the following formula:

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

Example Calculation

For a single-channel recording, the HDD capacity occupied per hour is 200 MB/hour. If you use a 4-channel device for 24-hour continuous recording for an entire month (30days), the required HDD space would be calculated as: 4 channels × 30 days × 24 hours × 200 MB/hour = 576 GB.

According to the formula, the recording file size for 1 channel in 1 hour at different stream values is as follows

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

HDD Capacity

ⓘ The table is for reference purposes only, and actual data may vary depending on specific conditions and configurations.

Appendix 2: Cybersecurity Recommendations

Account Management

1. **Use complex passwords.**

Follow the guidelines below to create a strong password:

- The password should be at least 8 characters long.
- Include at least two types of characters: uppercase letters, lowercase letters, numbers, and symbols.
- Avoid using the account name or its reverse.
- Do not use consecutive characters (e.g., 123, abc).
- Do not use repeating characters (e.g., 111, aaa).

2. **Change passwords periodically.**

It's advisable to regularly change the device password to minimize the risk of it being guessed or cracked.

3. **Allocate accounts and permission appropriately.**

Add users based on service and management needs, assigning the minimum necessary permissions

4. **Enable account lockout function.**

The account lockout function is enabled by default. Keep it enabled to enhance account security; after multiple failed login attempts, the corresponding account and source IP address will be locked.

5. **Set and update password reset information in a timely manner.**

The device supports a password reset function. To reduce the risk of unauthorized access, update this information promptly if there are any changes. When setting security questions, avoid using easily guessed answers

Service Configuration

1. **Enable HTTPS.**

It’s recommended to enable HTTPS for secure access to web services

2. **Change passwords periodically.**

If your audio and video data contents are important or sensitive, use encrypted transmission function to reduce the risk of your audio and video data being eavesdropped on during transmission.

3. **Allocate accounts and permission appropriately.**

It's advisable to disable services such as SSH, SNMP, SMTP, UPnP, and AP hotspot when not in use or required to reduce attack surfaces. If these services are necessary, consider the following safe modes:

- **SNMP**: Use SNMP v3 with strong encryption and authentication passwords.
- **SMTP**: Use TLS for accessing the mailbox server.
- **FTP**: Use SFTP with complex passwords.
- **AP Hotspot**: Use WPA2-PSK encryption with complex passwords.

4. **Enable account lockout function.**

It is advisable to change the default ports for HTTP and other services to any port between 1024 and 65535 to reduce the risk of being targeted by threat actors.

Network Configuration

1. **Enable Allowlist.**

It is recommended to enable the allow list function and only permit IP addresses on the allow list to access the device. Be sure to add your computer's IP address and any supporting device IP addresses to the allow list

2. **MAC address binding.**

It is advisable to bind the gateway's IP address to the device's MAC address to mitigate the risk of ARP spoofing.

3. **Build a secure network environment.**

To enhance device security and reduce potential cyber risks, the following measures are recommended:

- **Disable Port Mapping**: Turn off the port mapping function on the router to prevent direct access to internal devices from the external network.
- **Network Partitioning**: Based on actual network needs, partition the network. If there is no communication requirement between two subnets, consider using VLANs and gateways to achieve network isolation.
- **Implement 802.1x Access Authentication:** Establish an 802.1x access authentication system to minimize the risk of unauthorized terminal access to the private network.

Security Auditing

1. **Check online users.**

Check online users regularly to identify illegal users

2. **Check device logs.**

Review logs to learn about the IP addresses attempting to log in and track key operations performed by authorized users

3. **Configure network logs.**

The device can only retain a limited number of logs. To save logs for an extended period, it's recommended to enable the network log function to synchronize critical logs to a network log server for future reference

Software Security

1. **Update firmware on time.**

It is important to update device firmware to the latest version to ensure access to the latest features and security enhancements. If the device is connected to the public network, enable the automatic detection function for online upgrades to receive timely firmware update notifications from the manufacturer

2. **Update client software on time.**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended to implement physical protection for devices, especially storage devices. Consider placing them in a dedicated machine room or cabinet and establish access control and key management to prevent unauthorized personnel from damaging hardware and peripheral equipment (e.g., USB flash drives, serial ports).