LUMINYS

Pan-Tilt-Zoom (PTZ) Camera

User Manual

Rev. 1

Foreword

General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the PTZ camera. Please read it carefully before using the platform and store it safely for future reference.

Revision History

Revision	Content	Release Date
1	Initial Release	October 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.

Symbol	Definition
💡	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.
- Use the original manufacturer-provided packaging or equivalent high-quality packaging for safe transportation.
- Avoid applying excessive pressure, exposing the device to strong vibrations, or immersing it in liquid during transit.
- Keep the device away from humid, dusty, extremely hot or cold environments, as well as areas with strong electromagnetic radiation or unstable lighting conditions.
- Avoid placing heavy pressure on the device, exposing it to strong vibrations, or immersing it in liquid during storage.

Installation Requirements

- Ensure the power is off before connecting cables or installing/removing the device.
- For devices with grounding systems, properly ground them to prevent static damage, voltage induction, or electric shock.
- All installation and operation must follow local electrical safety standards.
- Use manufacturer-recommended accessories, installed by qualified personnel.
- Keep ventilation openings clear and install the device in a well-ventilated area.
- Avoid placing the device near heat sources or in direct sunlight to reduce fire risk.
- Ensure the power source is stable for reliable operation.
- Do not install the device in explosive, humid, dusty, extremely hot, or cold environments, or in areas with corrosive gas, strong electromagnetic interference, or unstable lighting.
- Avoid excessive force, vibration, or immersion during installation.
- Ensure ambient voltage is stable and meets the device’s power requirements.
- Protect the power cord from pressure or damage, especially around plugs, sockets, and connectors.
- Do not connect to multiple power sources simultaneously.
- It is recommended to use a lightning protector to enhance surge protection.

Operation Requirements

- Operate within the specified temperature and humidity range. Refer to the technical specifications for exact limits.
- Place the device on a stable surface.
- Keep liquids away from the device to prevent internal damage. If liquid enters, disconnect power, unplug all cables, and contact after-sales support.
- Do not plug or unplug RS-232, RS-485, or other ports while powered on to prevent port damage.
- Back up data regularly during setup and operation to prevent loss from abnormal conditions. The company assumes no responsibility for data security.
- The company is not liable for damage or malfunction resulting from overuse or improper operation.

Maintenance Requirements

- Have qualified personnel perform regular inspection and maintenance. Do not open or disassemble the device without professional supervision.
- Use only manufacturer-approved accessories and ensure maintenance is handled by professionals.

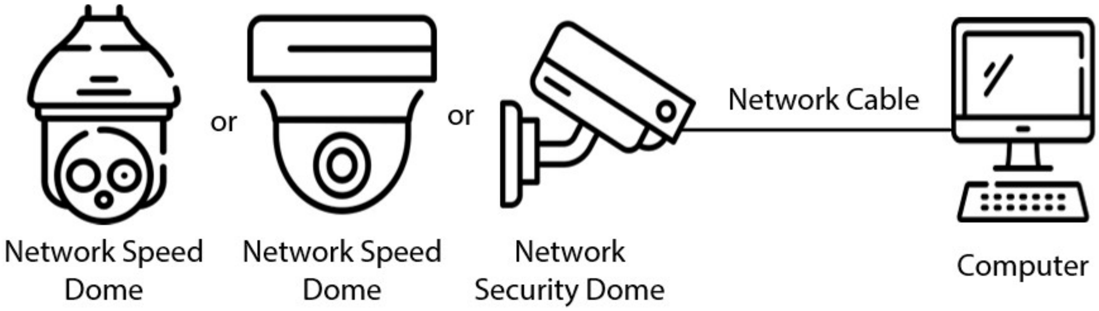
Table of Contents

Introduction

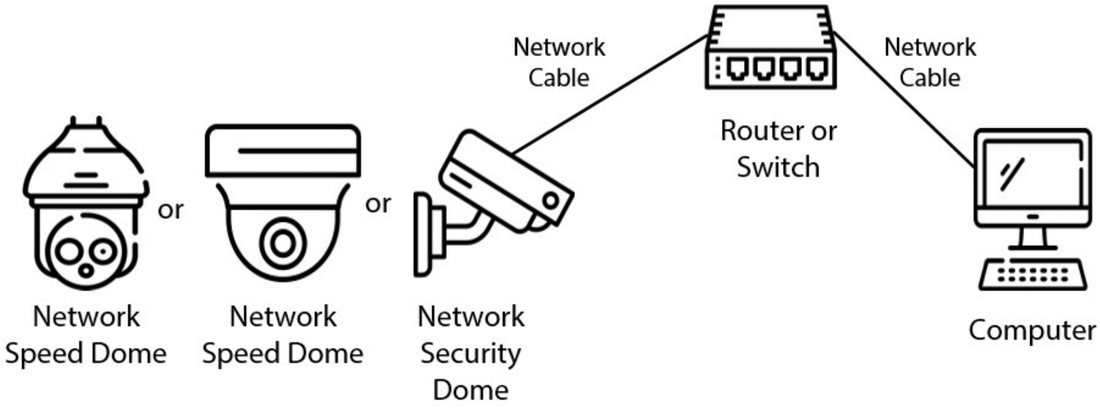
About the Device

The PTZ camera combines traditional camera functions with network technology. To access and manage it remotely, first obtain its IP address using LumiUtility.

Network Connection Diagrams



Direct Connection With a Network Cable



Connection via a Switch or Router

Functions

Functions may vary based on device model.

Basic Functions

Real-Time Monitoring

Real-time monitoring is designed to enhance security by allowing immediate detection of suspicious activities and enabling a prompt response to potential threats. Here are the capabilities of real-time monitoring:

- View the scene live as an event unfolds.
- While viewing the live image, you can enable audio and voice chat capabilities, as well as connect to a monitoring center for rapid analysis of any abnormalities detected.
- Adjust the PTZ to the best position.
- Capture snapshot and triple snapshot of any abnormalities in the monitoring image for later review and processing.
- Record abnormalities in the monitoring image for later review and processing.

- Configure encoding parameters and adjust the live view image.

Recording

- Automatically record based on a schedule.
- Play back and download recorded video and images.
- Record video after an alarm is triggered.

User Management

- Add, edit, and delete user groups, and manage user permissions based on the group.
- Add, edit, and delete users, and configure their permissions.
- Change the user's password.

AI Functions

Alarm

- Set alarm prompt mode and tone by type.
- View alarm messages.

Video Detection

- Supports motion, video tampering, and scene change detection.
- When an alarm is triggered, the system performs actions such as recording, alarm output, sending an email, PTZ operation, and taking a snapshot.

Video Metadata

- Supports intelligent motion detection (iMD) and monitors the movement of vehicles and persons in a scene.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

Audio Detection

- Detects audio input exceptions and changes in audio intensity.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

VCA

- Supports fence crossing, line crossing, intrusion, abandoned object, parking, aggregation, missing object, loitering detection, and more.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

Face Detection

- Detects human faces and displays attributes on the Live page.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

People Counting

- Supports people counting (entries, exits, and loitering time) and queue data with report generation.

- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

Video Metadata

- Detects people, non-motor vehicles, and motor vehicles and displays related attributes on the Live page.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

Alarms

- Alarms are triggered by external alarm input devices.
- When an alarm is triggered, the system initiates actions like recording, alarm output, sending an email, PTZ operation, and capturing a snapshot.

LumiSearch

- Find, track, and identify on LumiSearch-enabled NVRs.

Exceptions

- Detects SD card errors, network issues, unauthorized access, security breaches, and PTZ exceptions.
- Network alarms trigger recording and alarm output.
- PTZ alarms trigger alarm output.

Device Initialization

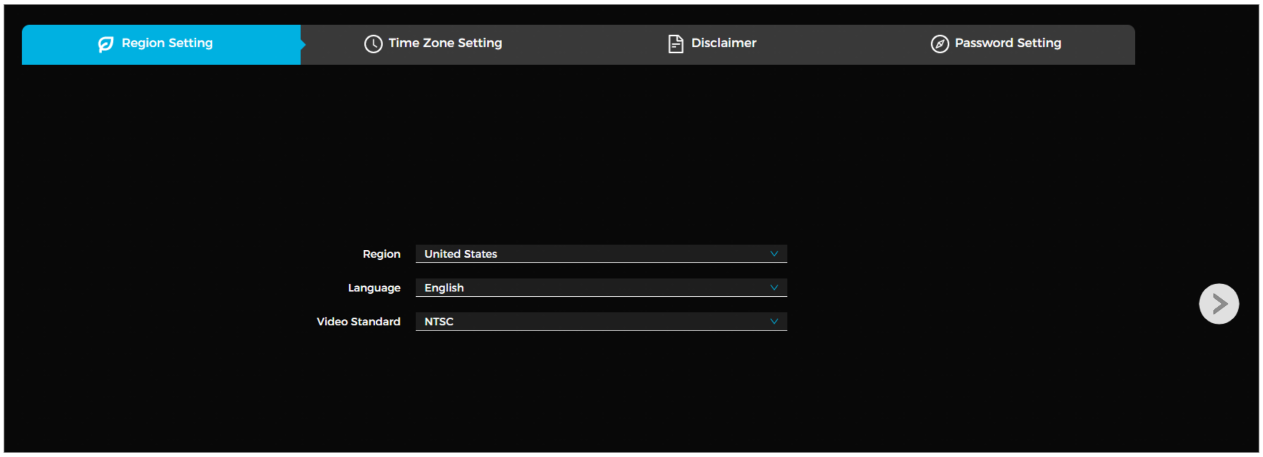
Device initialization is necessary for first-time use. This manual covers operations via the webpage, but initialization can also be done through LumiUtility, NVR, or platform devices. For device security, ensure the password is stored securely after initialization, and update it regularly. During initialization, make sure the IP address of both the computer and the device are on the same network.

Follow the steps below to initialize the device.

1. Open your browser, type the device's IP address into the address bar, and press Enter.

ⓘ The default IP address is 192.168.1.101.

2. Set the region, language, and video standard. Click > when done.



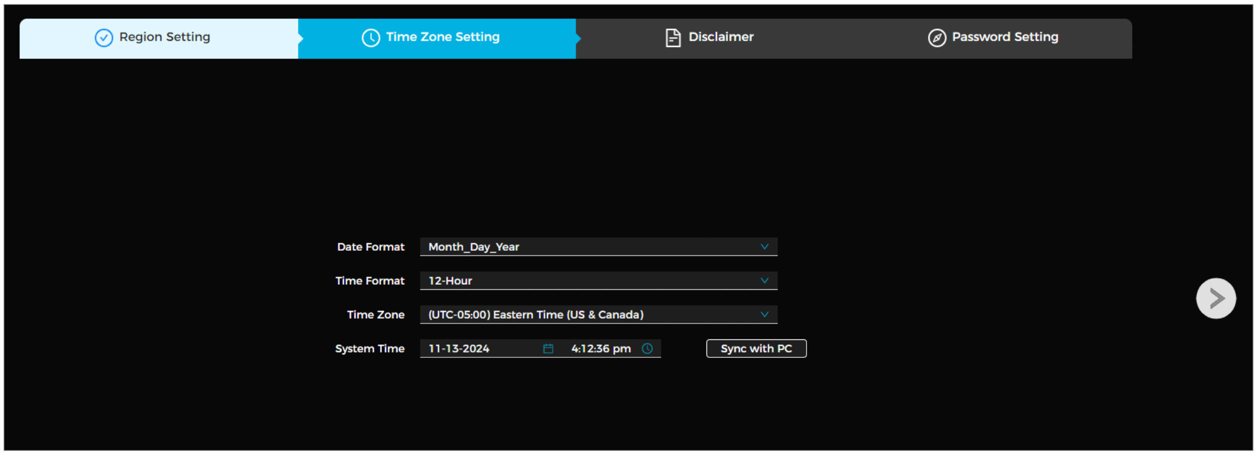
Region: United States

Language: English

Video Standard: NTSC

Region Setting

3. Set the time parameters. Click > when done.



Date Format: Month_Day_Year

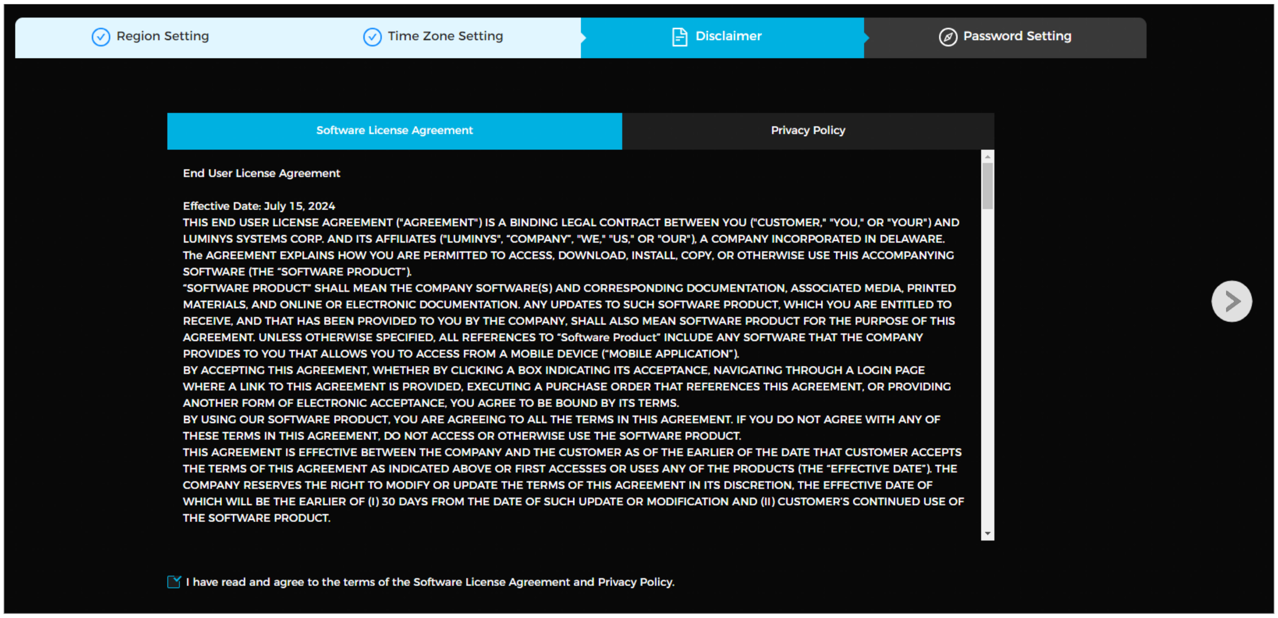
Time Format: 12-Hour

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

System Time: 11-13-2024 4:12:36 pm

Time Zone Setting

4. Agree to the terms of the Privacy Policy and Software License Agreement.



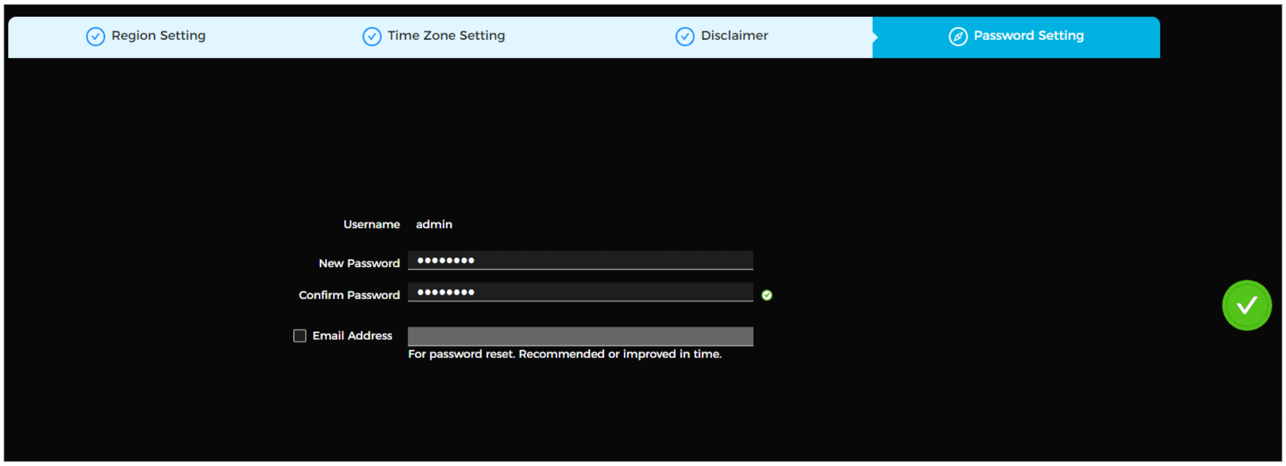
End User License Agreement

Effective Date: July 15, 2024
THIS END USER LICENSE AGREEMENT ("AGREEMENT") IS A BINDING LEGAL CONTRACT BETWEEN YOU ("CUSTOMER," "YOU," OR "YOUR") AND LUMINYS SYSTEMS CORP. AND ITS AFFILIATES ("LUMINYS", "COMPANY", "WE," "US," OR "OUR"), A COMPANY INCORPORATED IN DELAWARE. The AGREEMENT EXPLAINS HOW YOU ARE PERMITTED TO ACCESS, DOWNLOAD, INSTALL, COPY, OR OTHERWISE USE THIS ACCOMPANYING SOFTWARE (THE "SOFTWARE PRODUCT").
"SOFTWARE PRODUCT" SHALL MEAN THE COMPANY SOFTWARE(S) AND CORRESPONDING DOCUMENTATION, ASSOCIATED MEDIA, PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION. ANY UPDATES TO SUCH SOFTWARE PRODUCT, WHICH YOU ARE ENTITLED TO RECEIVE, AND THAT HAS BEEN PROVIDED TO YOU BY THE COMPANY, SHALL ALSO MEAN SOFTWARE PRODUCT FOR THE PURPOSE OF THIS AGREEMENT. UNLESS OTHERWISE SPECIFIED, ALL REFERENCES TO "Software Product" INCLUDE ANY SOFTWARE THAT THE COMPANY PROVIDES TO YOU THAT ALLOWS YOU TO ACCESS FROM A MOBILE DEVICE ("MOBILE APPLICATION").
BY ACCEPTING THIS AGREEMENT, WHETHER BY CLICKING A BOX INDICATING ITS ACCEPTANCE, NAVIGATING THROUGH A LOGIN PAGE WHERE A LINK TO THIS AGREEMENT IS PROVIDED, EXECUTING A PURCHASE ORDER THAT REFERENCES THIS AGREEMENT, OR PROVIDING ANOTHER FORM OF ELECTRONIC ACCEPTANCE, YOU AGREE TO BE BOUND BY ITS TERMS.
BY USING OUR SOFTWARE PRODUCT, YOU ARE AGREEING TO ALL THE TERMS IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH ANY OF THESE TERMS IN THIS AGREEMENT, DO NOT ACCESS OR OTHERWISE USE THE SOFTWARE PRODUCT.
THIS AGREEMENT IS EFFECTIVE BETWEEN THE COMPANY AND THE CUSTOMER AS OF THE EARLIER OF THE DATE THAT CUSTOMER ACCEPTS THE TERMS OF THIS AGREEMENT AS INDICATED ABOVE OR FIRST ACCESSES OR USES ANY OF THE PRODUCTS (THE "EFFECTIVE DATE"). THE COMPANY RESERVES THE RIGHT TO MODIFY OR UPDATE THE TERMS OF THIS AGREEMENT IN ITS DISCRETION, THE EFFECTIVE DATE OF WHICH WILL BE THE EARLIER OF (I) 30 DAYS FROM THE DATE OF SUCH UPDATE OR MODIFICATION AND (II) CUSTOMER'S CONTINUED USE OF THE SOFTWARE PRODUCT.

☑ I have read and agree to the terms of the Software License Agreement and Privacy Policy.

Disclaimer

5. Set a password for the admin account following the parameters listed in the table below.



Username admin

New Password ••••••••

Confirm Password ••••••••

□ Email Address

For password reset. Recommended or improved in time.

Parameter	Description
Username	The default is set to admin.
Password	The password must be between 8 to 32 characters long, without spaces, and include at least two types of characters from uppercase letters, lowercase letters, numbers, and special characters (excluding ' " ; : &). Ensure the password is secure by following the guidelines provided in the password security notice.
Confirm Password	
Email Address	Enter an email address for password reset, which is enabled by default. If you need to reset the admin account password, a security code will be sent to the provided email address.

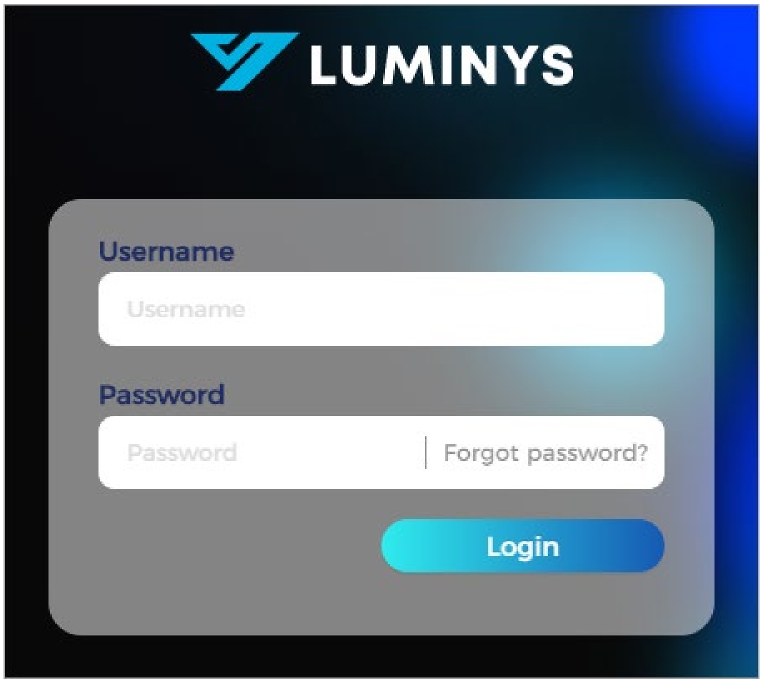
6. Click ✓ when done.

Login

Log in to the Webpage

Follow the instructions to download and install the plugin during the first login. The camera must be initialized before logging in to the webpage. For more details, refer to Device Initialization.

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



Login Screen

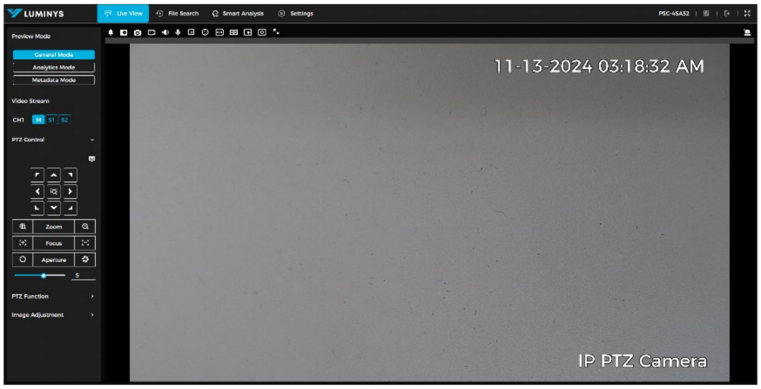
2. Enter the Device’s login credentials. The default username is admin.

ⓘ

- After 5 incorrect password attempts, the account is locked for 5 minutes.
- You can adjust the allowed attempts and lock duration under Unauthorized Access.

3. After logging in to the webpage, follow the on-screen instructions to download and install the plug-in.

After the plug-in installs, the webpage refreshes automatically, and video appears on the Live View page. The Live View page in this manual is for reference only; available functions may vary by model.



Live View Page

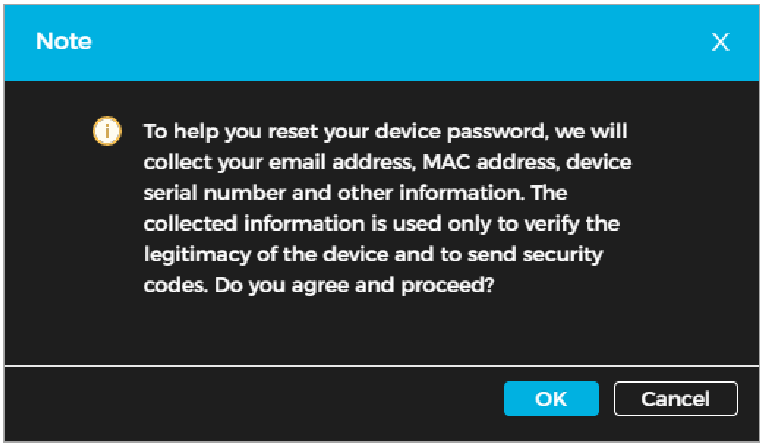
Password Reset

Luminys cameras allow you to reset the admin account password when needed. A security code will be sent to the email address provided during installation, and this code enables the user to reset the password.

Prior to resetting your password, ensure the password resetting service is enabled.

Follow the steps below to reset your password.

1. Open the browser, enter the device IP address in the address bar, and press Enter.
2. Click on "**Forgot password?**" to display the password resetting notice.
3. Read the notice and click **OK**.

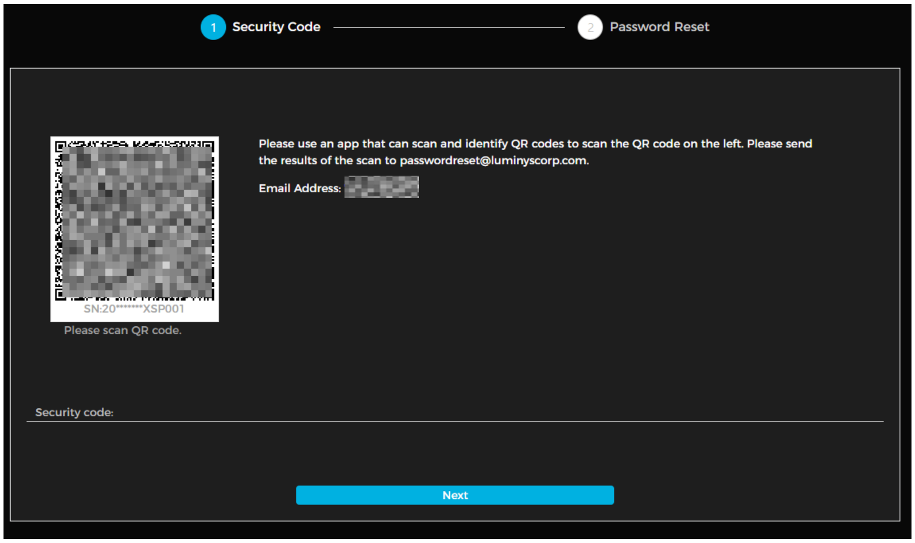


Note

To help you reset your device password, we will collect your email address, MAC address, device serial number and other information. The collected information is used only to verify the legitimacy of the device and to send security codes. Do you agree and proceed?

Password Reset Notice

4. Scan the QR code and obtain the encryption strings. Send the strings to passwordreset@luminyscorp.com to receive a security code. Enter the security code and click **Next**.
5. Reset the password via the **Password Reset** page.



Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to passwordreset@luminyscorp.com.

Email Address: [redacted]

SN:20*******XSP001

Please scan QR code.

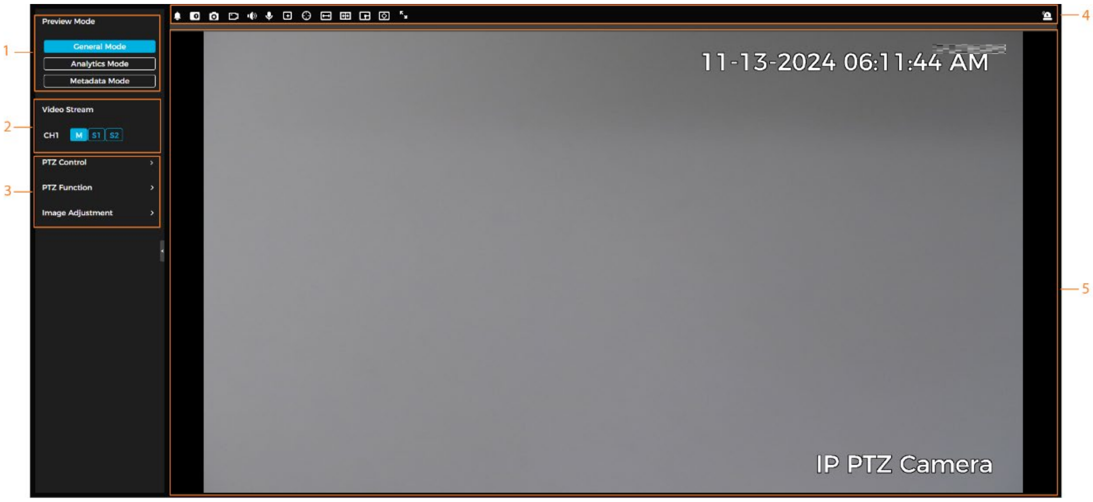
Security code:

Password Reset

Live View

Live View Page

Click Live View on the main page to open the Live View page. The Live View page in this manual is for reference only; available functions may vary by model.

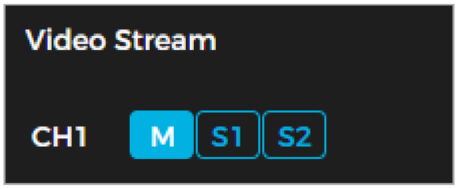


Live View Page

Number	Function	Description
1	Preview Mode	Switch the video display mode: general, face, or metadata.
2	Video Stream	Show the channel list. Select a channel and set the stream type.
3	Window Adjustment	Adjust live view image settings.
4	Live View Function Bar	Show shortcuts for available functions.
5	Live View	Display real-time video feed.

Video Stream

On the left side of the Live View page, select the stream type for each video channel.



Select Stream Type

- **Main Stream**: Provides higher resolution and larger bit rate, requiring more bandwidth. Used for recording and monitoring.
- **Sub Stream**: Provides lower bit rate and smoother playback, using less bandwidth. Typically used when bandwidth is limited.
- M indicates the main stream.
- S1 indicates sub stream 1.

- S2 indicates sub stream 2.

Live View Function Bar

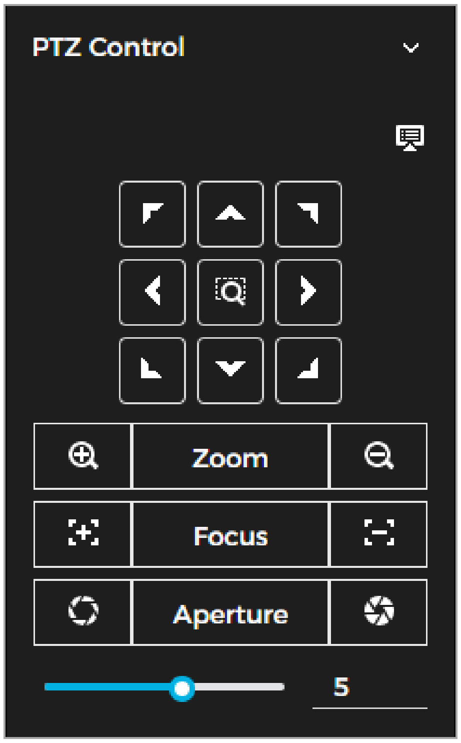
Refer to the table below to learn what the icons on the live view function bar mean.

Icon	Function	Description
🔔	Sound Alarm	Shows the alarm sound status. Click the icon to manually turn the alarm sound on or off.
⊕	Digital Zoom	Zoom in on a selected area, and drag the image while zoomed in to view other sections. You can zoom in the live video using either method below: • Click the icon, then select an area in the live image to enlarge. Right-click to return to the original view. • Click the icon, then use the mouse wheel to zoom in or out.
📷	Snapshot	Takes a snapshot of the current screen and saves it to a set storage path.
📹	Record	Starts or stops video recording and saves files to a set storage path.
🔊	Audio Output	Enables or disables audio output for the selected channel.
🎤	Two-Way Talk	Turns two-way talk on or off.
⊞	Area Focus	Click the button, draw a box on the live view, and the camera will auto-focus on the selected area.
⌖	Manual Track	Click the button, draw a box on the live view, and the camera will auto-track and zoom in onto the selected area.
↔	W:H	Click the icon to switch the display ratio between **Original** and **Adaptive**.
▣	AI Rule	Click the icon and select **Enable** to show AI rules and detection boxes or **Disable** to hide them. This feature is enabled by default.
◲	Intelligence Area	Click the icon and select **Enable** to show the intelligent area or **Disable** to hide it.
◇	Anti-Aliasing	Click this icon to turn anti-aliasing on or off.
⤡	Full Screen	Click the icon to enter full-screen mode; double-click or press Esc to exit.
🚨	Alarm Output	Shows the alarm output status for the selected channel. When connected to an alarm output device, click the icon to manually turn alarm output on (red) or off (black).

Window Adjustment

PTZ Control

On the Live View page, click PTZ control on the left side to rotate the device, zoom in on images, and adjust the camera's iris.

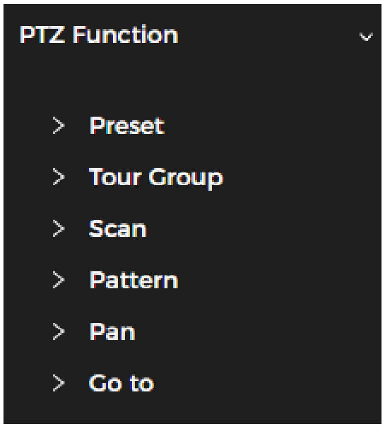


PTZ Control

Icon	Description
◤ ▲ ◥ ◀ 🔍 ▶ ◣ ▼ ◢	Control the device in eight directions: up, down, left, right, upper left, upper right, lower left, and lower right. Click the center icon, then select an area in the live view to make the PTZ quickly rotate and zoom to that area.
⊕ Zoom ⊖	Adjusts image magnification.
Focus	Adjusts the camera’s focal length.
Aperture	Controls image brightness.
5	Sets PTZ rotation speed. Higher values increase rotation speed (e.g., speed 8 is faster than speed 1).
🖥	Opens the PTZ menu for camera configuration, PTZ setup, system management, and related functions.

PTZ Function

On the Live View page, click PTZ Function on the left panel. Ensure the PTZ is configured prior to use. The value range for PTZ functions such as presets and tours depends on the selected PTZ protocol.



PTZ Function

Function	Description
Preset	Set a preset number, then click **View** to move the device to that position. The preset stores PTZ parameters such as pan, tilt, and zoom.
Tour Group	Set a tour number. Click **Start** to have the device rotate through the preset points in sequence. Click **Stop** to end the tour.
Scan	Set a scan number. Click **Start** to have the device scan between defined boundaries at a fixed speed. Click **Stop** to end the scan.
Pattern	Set a pattern number. Click **Start** to have the device follow the recorded PTZ actions, including focus and zoom changes. Click **Stop** to end the pattern.
Pan	Click **Start** to begin continuous 360° horizontal rotation at a set speed.
Go to	Set the horizontal angle, vertical angle, and zoom, then click **Go To** to move the device to the specified point.

Image Adjustment

Click **Image Adjustment** on the left panel of the Live View page, then drag the sliders to adjust brightness, contrast, hue, and saturation. These adjustments apply only to the webpage display and do not affect the camera's image settings.

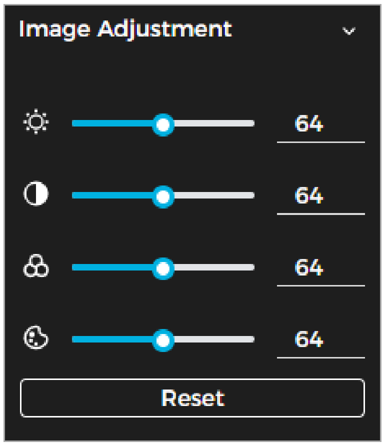


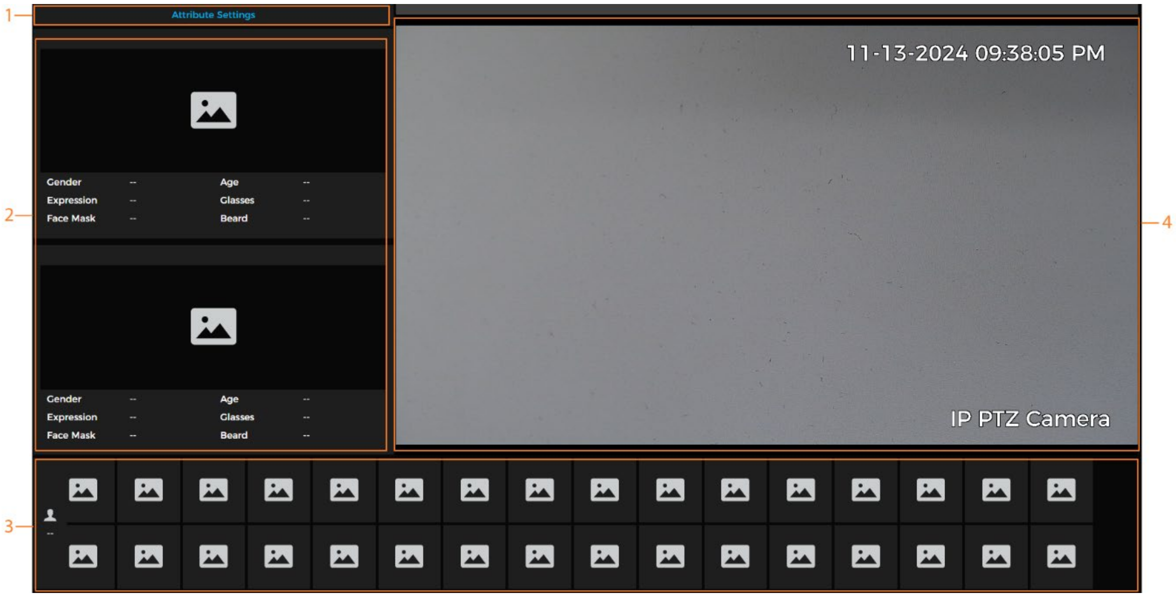
Image Adjustments

Icon	Function	Description
☼	Brightness Adjustment	Adjusts overall image brightness. Use when the image appears too dark or too bright; both light and dark areas change equally.

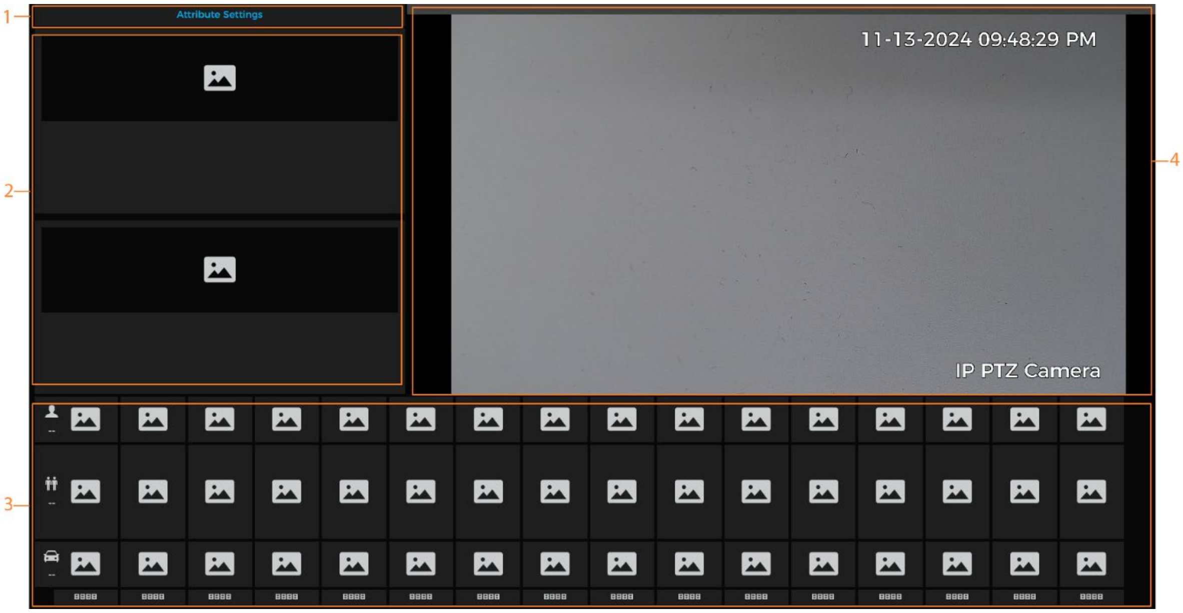
◐	Contrast Adjustment	Adjusts image contrast when brightness is fine but the image lacks definition.
⚭	Saturation Adjustment	Adjusts color intensity without affecting brightness.
🎨	Hue Adjustment	Adjusts color tone from lighter to deeper. The default value, set by the light sensor, is recommended.
Reset	Reset	Restores focus to default settings. You can also reset zoom if the image appears unclear or has been zoomed excessively.

Preview Mode

Three display modes are available: general, face, and metadata. For general mode, see the Live View Page section of the manual. Select **Analytics Mode** or **Metadata Mode** in the upper left corner of the Live View page to enable either of the modes. Before using face or metadata mode, configure the related AI functions in advance.



Analytics Mode

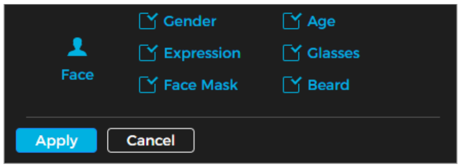


Metadata Mode

Number	Function	Description
1	Attribute Settings	Click to adjust the display properties of captured images.
2	Details	Shows the captured image and related details.
3	Captured Image	Enables statistics for faces, human bodies, motor vehicles, and non-motor vehicles. Click an image to view detailed capture information.
4	Live View	Displays the live monitoring video.

Configure Detection Properties

In face or metadata mode, click Attribute Settings. Select the properties to display on the Live View page, then click Apply. The available properties vary by mode.



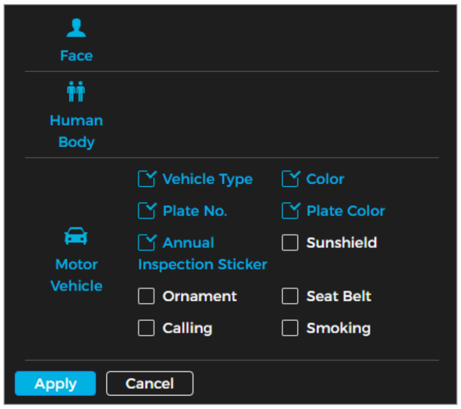
Face

☑ Gender ☑ Age

☑ Expression ☑ Glasses

☑ Face Mask ☑ Beard

Detection Properties (Analytics Mode)



Face

Human Body

Motor Vehicle

☑ Vehicle Type ☑ Color

☑ Plate No. ☑ Plate Color

☑ Annual Inspection Sticker ☐ Sunshield

☐ Ornament ☐ Seat Belt

☐ Calling ☐ Smoking

Detection Properties (Metadata Mode)

Record

The following section introduces the functions and operations of video playback.

How to Playback Video

This section explains how to search and play back video archives. This function is only available on cameras with an SD card. Before playback, set up the record storage method, record schedule, and record control.

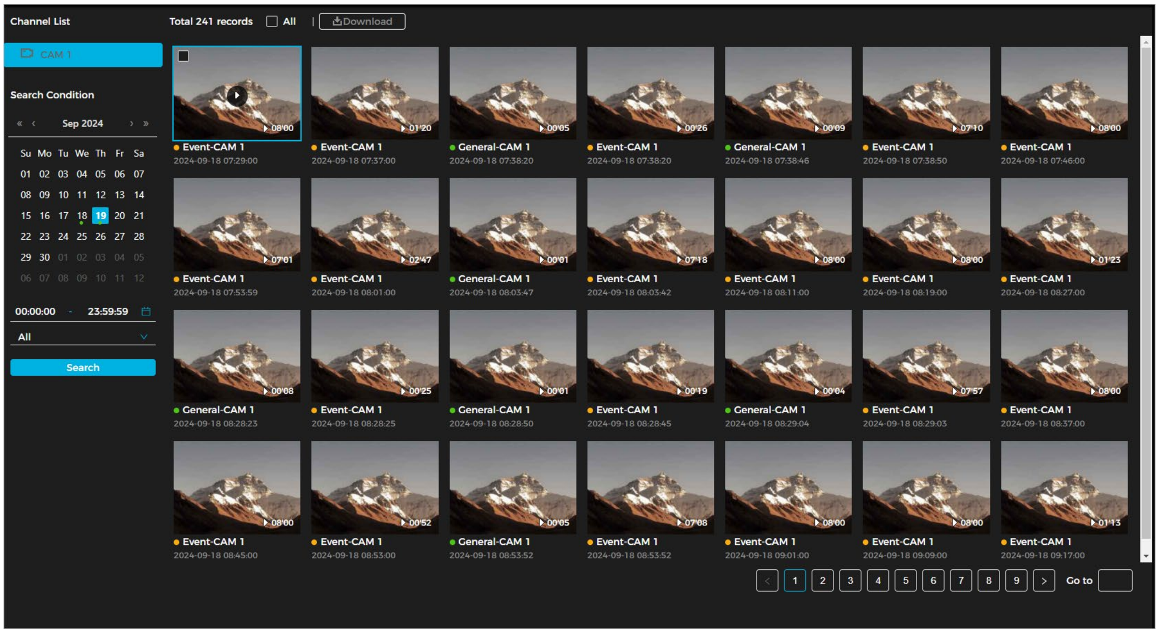
Follow the steps below to play back a video.

1. Navigate to **File Search → Video → Video Archive Search**.
2. Select the channel, recording type (All, General, Event), and recording time.

ⓘ

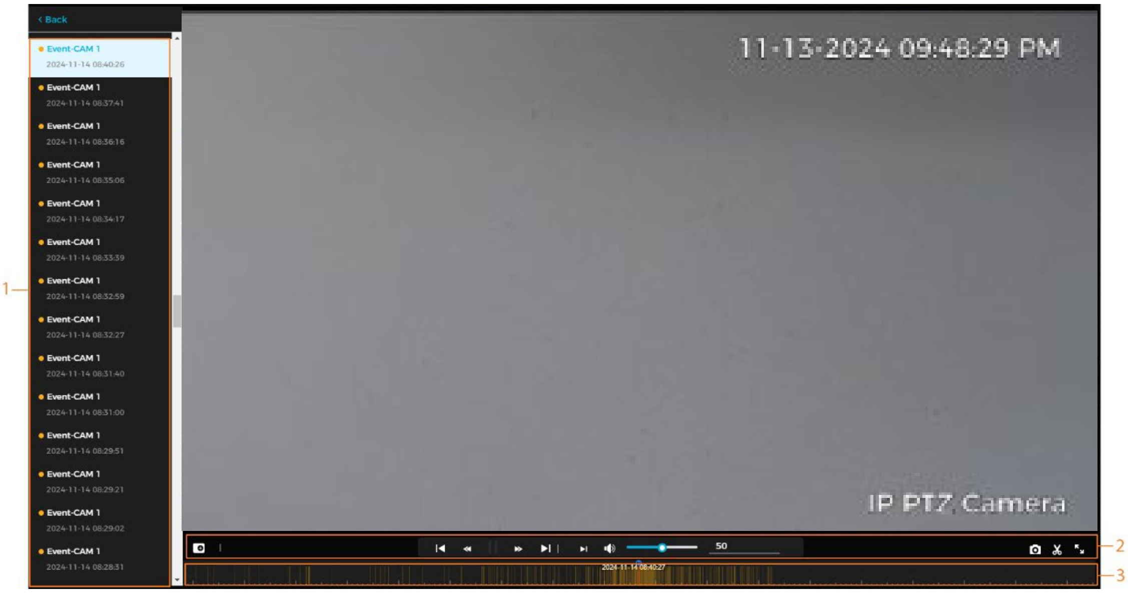
- When choosing Event as the record type, you can specify event types like Motion Detection, Video Tampering, and Scene Changing.
- Days with recorded video are marked with a green dot.

3. Click **Search**.



Search Video

4. To display the video playback page, place the pointer to the searched video, then click the ● icon to play back the selected video.



Video Playback

Number	Function	Description
1	Recorded Video List	Displays all searched recorded video files. Click any file for playback. Click **Back** at the upper-left corner to go to the Video Archive Search page.
2	Digital Zoom	There are two ways to zoom in on a selected area of a video image. • Click the icon highlighted in the figure above. Next, select the area in the video to zoom in. Then, right-click on the image to resume to the original size. In the zoom-in state, drag the image to check other areas.

			- Click the icon highlighted in the figure above. Next, scroll the mouse wheel in the video to zoom in or out.
	Play Control Bar	⏮	Plays back the previous video recorded in the video list.
		⏪	Slows down the playback.
		⏸	Stops playing back recorded videos.
		▶	Plays back recorded videos.
		⏩	Speeds up the playback.
		⏭	Plays back the next recorded video in the recorded video list.
		⏭	Plays the next frame.
	Sound	🔇	Mutes the sound.
		🔊	Adjusts the Volume.
	Snapshot	📷	Captures an image and saves it to the configured storage path.
	Video Clip	✂	Clips and saves a specific recorded video. For details, see **Clipping Video**.
	Full Screen	⛶	Click the icon to enter full-screen mode. Double-click or press Esc to exit
3	Progress Bar		Shows the record type along with the corresponding time. - Click any point in the colored area to start playback from that moment. - Each recording type is represented by a specific color, which can be referenced in the Record Type bar.

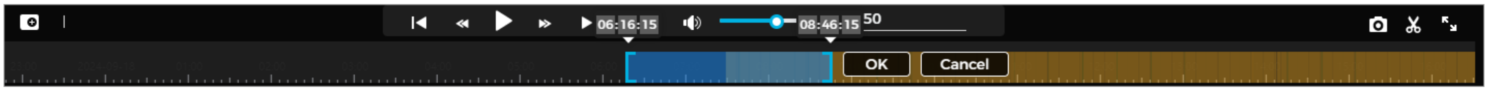
Related Operations

- Click **Download** to save selected videos locally.

How to Clip a Video

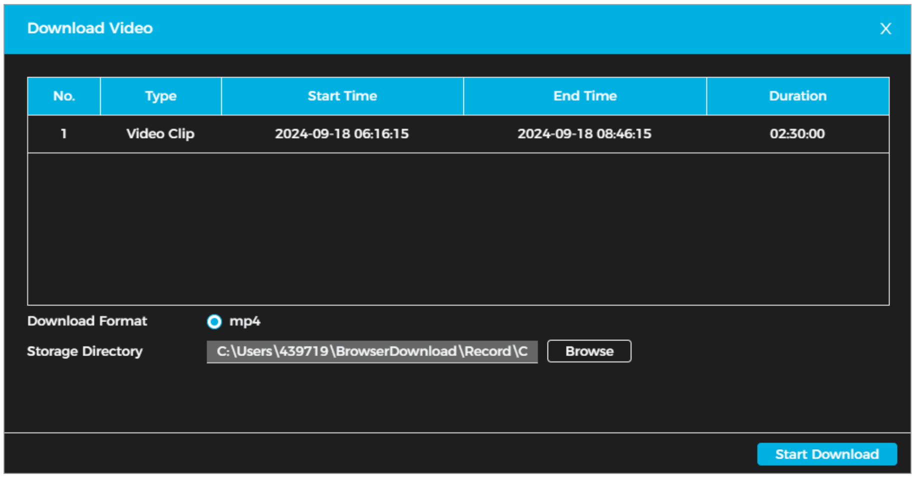
Follow the steps below to clip a video.

1. Click the ✂ icon.
2. To clip the video, locate the progress bar. Then, drag the clipping box to select the start time and end time of the target video.



Clip Video Screen

3. Click **OK** to download the clipped video.
4. Select the download format. Click **Browse** to set the file storage path.



No.	Type	Start Time	End Time	Duration
1	Video Clip	2024-09-18 06:16:15	2024-09-18 08:46:15	02:30:00

Download Format ● mp4

Storage Directory C:\Users\439719\BrowserDownload\Record\C

Download Video Screen

5. Click **Start Download**.

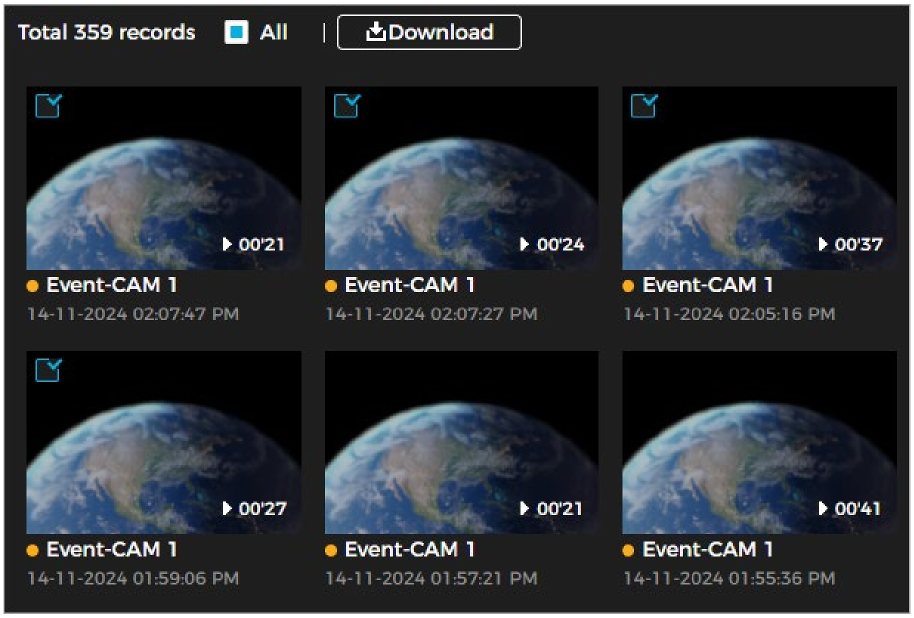
How to Download a Video

Videos can be downloaded individually or as a batch. Follow the steps below to download a video to a defined path.

ⓘ

- Simultaneous playback and downloading are not supported.
- Operations may vary by browser.

1. Navigate to **File Search → Video → Video Archive Search**.
2. Select the channel, record type, record time.
3. Click **Search**.
4. Select the videos to be downloaded by clicking the □ at the top corner of each video or next to All.



Total 359 records ■ All

▶ 00'21 Event-CAM 1 14-11-2024 02:07:47 PM

▶ 00'24 Event-CAM 1 14-11-2024 02:07:27 PM

▶ 00'37 Event-CAM 1 14-11-2024 02:05:16 PM

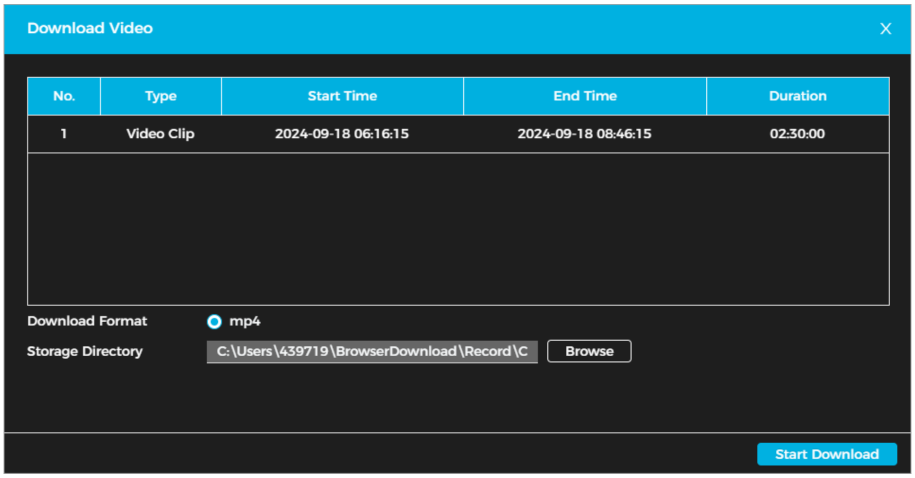
▶ 00'27 Event-CAM 1 14-11-2024 01:59:06 PM

▶ 00'21 Event-CAM 1 14-11-2024 01:57:21 PM

▶ 00'41 Event-CAM 1 14-11-2024 01:55:36 PM

Select Video Files

5. Select the download format. Click **Browse** to set the file storage path.



Download Video

No.	Type	Start Time	End Time	Duration
1	Video Clip	2024-09-18 06:16:15	2024-09-18 08:46:15	02:30:00

Download Format ● mp4

Storage Directory C:\Users\439719\BrowserDownload\Record\C

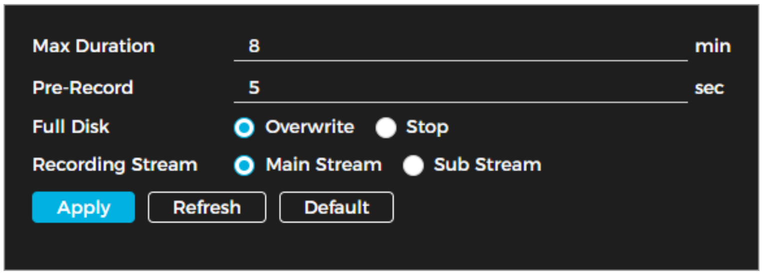
Download Video Screen

6. Click **Start Download**.

How to Set Recording Parameters

In this section, learn to set parameters such as pack duration, pre-event record, disk full, record mode, and record stream. To set your preferred recording parameters, do the following:

1. Navigate to **File Search → Video → Recording Settings**.



Max Duration 8 min

Pre-Record 5 sec

Full Disk ● Overwrite ○ Stop

Recording Stream ● Main Stream ○ Sub Stream

Record Settings Screen

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

Parameter	Description
Max. Duration	Refers to the time packing each video file.
Pre-Record	The duration of recorded video saved before an alarm event is triggered. For example, if set to 5 seconds, the system records video starting 5 seconds before the alarm occurs. If an alarm or motion detection triggers recording while recording is not already enabled, the system includes the pre-event recording time in the saved video file.
Full Disk	• **Overwrite**: When the disk is full, the earliest recording is overwritten with current video. • **Stop**: When the disk is full, the recording is stopped, and no additional video can be recorded until space becomes available.
Record Stream	Select **Mainstream** or **Substream**.

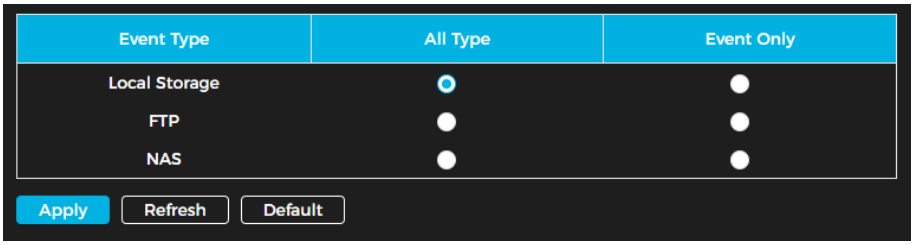
3. Click **Apply**.

Storage

This section explains how to configure the storage method for recorded videos.

Local Storage

1. Navigate to **File Search → Video → Storage**.
2. Select **All Type** or **Event Only** for **Local Storage** to save video on the local SD card.
3. Click **Apply**.



Event Type	All Type	Event Only
Local Storage	◉	○
FTP	○	○
NAS	○	○

Local Storage Screen

Network Storage

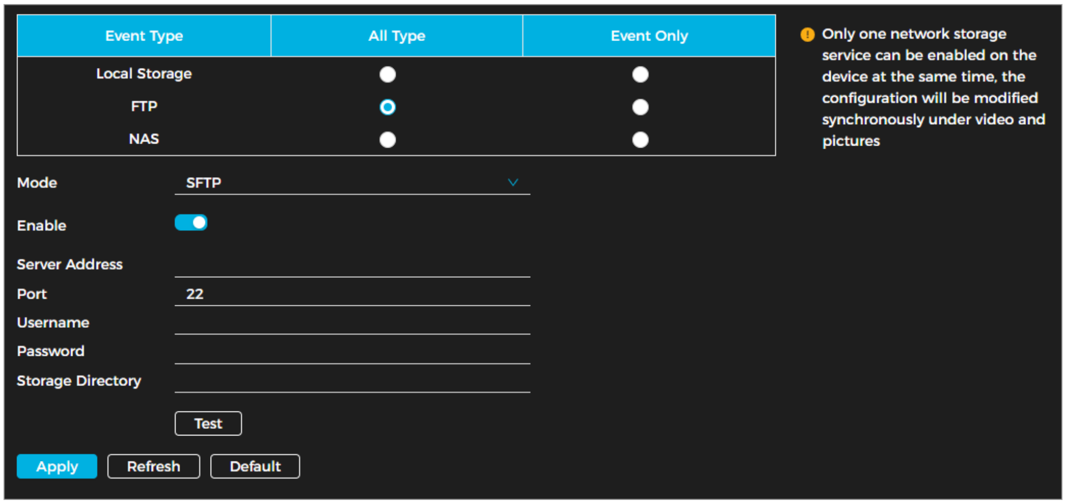
You can store videos on the network using an FTP or NAS server. In case of a network error, videos can be backed up using the internal SD card.

FTP

1. Navigate to **File Search → Video → Storage**.
2. Select **All Type** or **Event Only** for **FTP** to save video to an FTP server. You may choose FTP or SFTP from the dropdown menu.

ⓘ SFTP is recommended for enhanced network security.

3. Click ○ to enable the FTP function.



Event Type	All Type	Event Only
Local Storage	○	○
FTP	◉	○
NAS	○	○

Only one network storage service can be enabled on the device at the same time, the configuration will be modified synchronously under video and pictures

Mode: SFTP

Enable: ●

Server Address:

Port: 22

Username:

Password:

Storage Directory:

FTP

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

Parameter	Description
Server Address	The FTP server's IP address.
Port	The FTP server's port number.
Username	The username for the FTP server.

Password	The password for the FTP server.
Storage Directory	The destination path accessible to the FTP server.

5. Click **Apply**.

6. Click **Test** to check if the FTP function is operational.

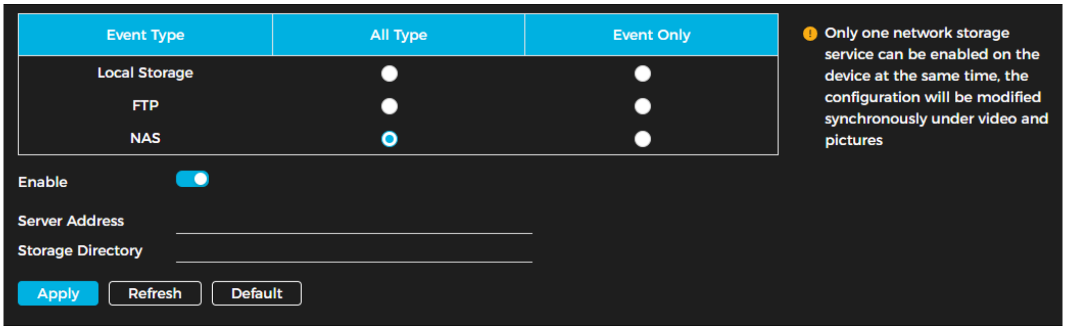
NAS

Follow the steps below to save video in the NAS.

1. Select **File Search → Video → Storage**.

2. To save the recorded videos in the NAS server, select **All Type** or **Event Only** for NAS.

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



Event Type	All Type	Event Only
Local Storage	○	○
FTP	○	○
NAS	●	○

Only one network storage service can be enabled on the device at the same time, the configuration will be modified synchronously under video and pictures

Enable: On

Server Address:

Storage Directory:

Parameter	Description
Server Address	NAS server IP address.
Storage Directory	NAS server destination path.

4. Click **Apply**.

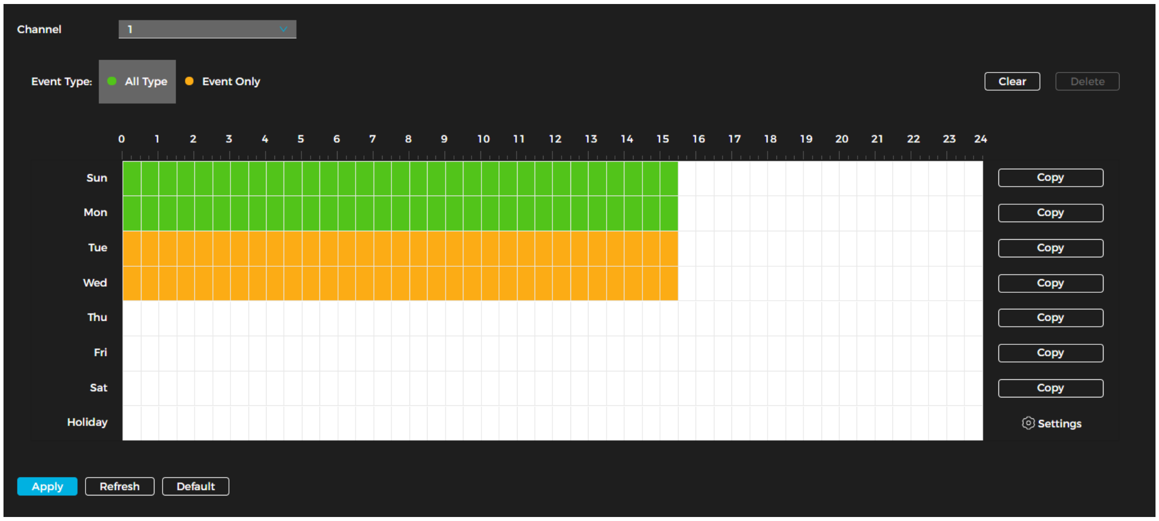
How to Set the Recording Plan

After enabling the corresponding alarm type (All Type or Event Only), the record channel links to the recording.

You can set specific days as holidays. When Record is selected in the holiday schedule, the system follows the defined holiday recording settings.

Follow the steps below to set the recording plan.

1. Navigate to **File Search → Video → Schedule**.



Channel: 1

Event Type: 🟩 All Type 🟧 Event Only

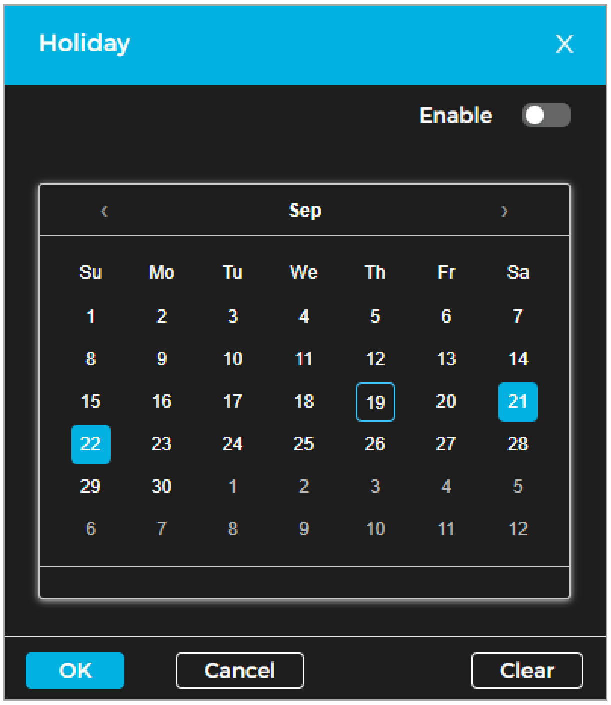
Recording Plan Schedule

2. Select a record type, then press and drag the left mouse button to set the normal recording period on the timeline. Green indicates an all-type record plan, while yellow represents a motion record plan.

ⓘ

- Click **Copy** next to a day, then select the target days in the prompt window to apply the configuration to the selected days. Check the **All** box to copy the settings to every day.
- Up to six periods can be set per day.

3. Click **Apply**.
4. Click **Settings** to set holidays.
5. Click ○ to enable the holiday schedule. Choose the days to set as holidays. Click **Clear** to remove the selection(s).



Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Holiday Schedule

6. Click **OK**.

ⓘ If the holiday schedule differs from the general schedule, the holiday schedule takes priority. For example, when the holiday schedule is enabled and the day is marked as a holiday, the system follows the holiday schedule for snapshots or recording. Otherwise, it follows the general schedule.

Snapshot and Archive Search

This section explains the functions and operations related to picture playback.

How to Play Back a Snapshot

Prior to playback, ensure the following prerequisites are met:

- The camera has an SD card.
- The snapshot time range, storage method, and plan is configured.

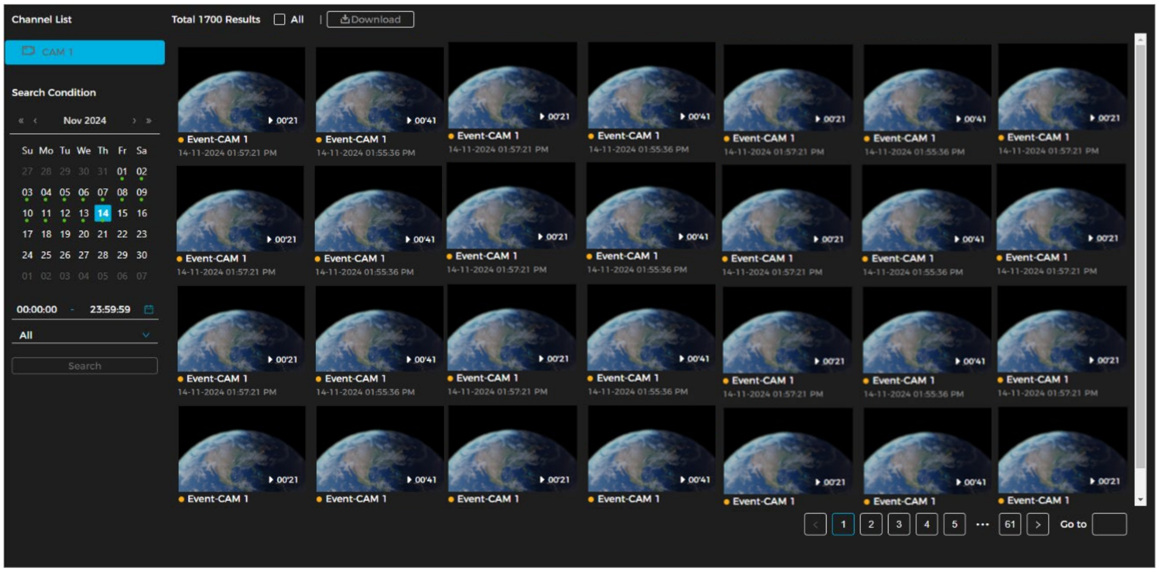
Follow the steps below to play back a snapshot.

1. Navigate to **File Search → Snapshot → Snapshot Archive Search**.
2. Select the channel, snapshot type (All, General, Event), and snapshot time.

ⓘ

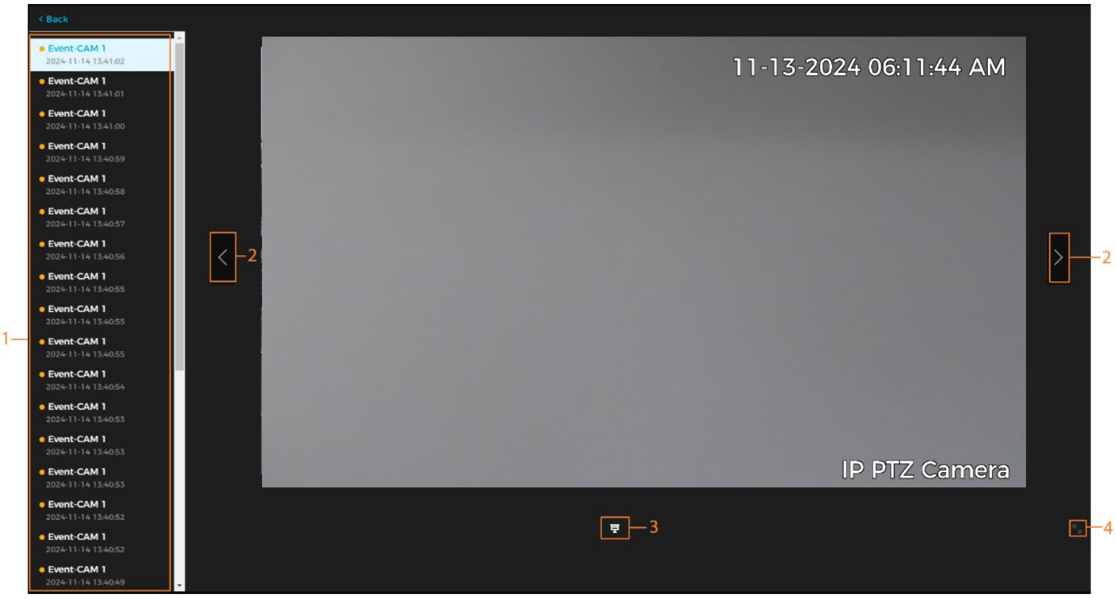
- When choosing Event as the record type, you can specify event types like Motion Detection, Video Tampering, and Scene Changing.
- Days with recorded video are marked with a green dot.

3. Click **Search**.



Picture Search

4. Click ▶ to play back the desired snapshot.



Snapshot Playback

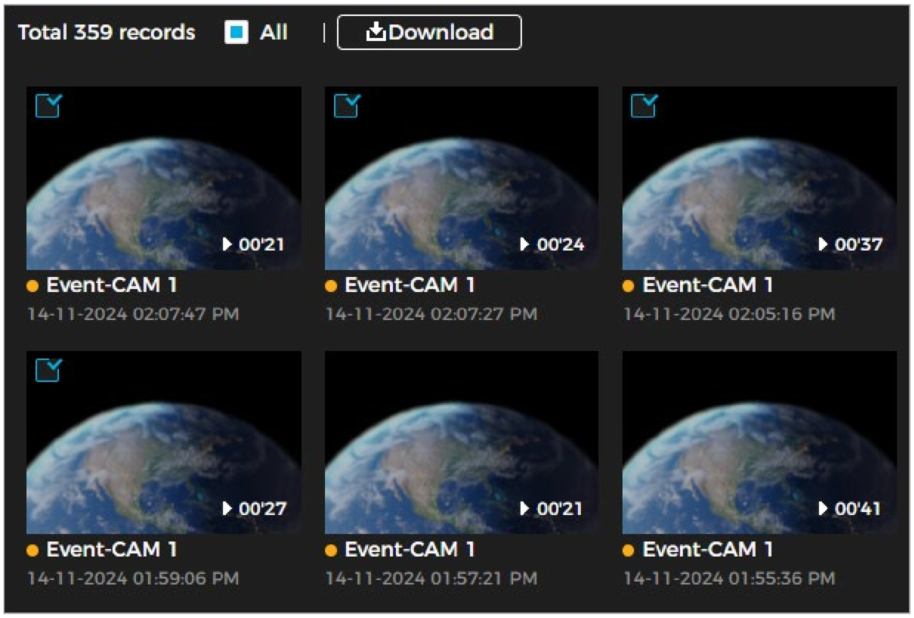
Number	Function	Description
1	Snapshot List	Displays all the searched snapshots. Click on any file to play it back. Click Back in the upper-left corner to return to the Snapshot Archive Search page.
2	Manual Display	< displays the previous snapshot in the snapshot list. > displays the next snapshot in the snapshot list.
3	Slide Show	displays the snapshots list one by one in slide show mode.
4	Full Screen	displays the snapshot in full-screen mode. Double-click the image or press the Esc button to exit full-screen mode

How to Download a Snapshot

Follow the steps below to download a snapshot. You can download a single image or batches of images.

ⓘ Operation may vary based on browser.

1. Navigate to **File Search → Snapshot → Snapshot Archive Search**.
2. Select the channel, snapshot type, and snapshot time.
3. Click **Search**.
4. Select the snapshots to be downloaded by clicking the ■ at the top corner of each video or next to All.



Event-CAM 1 14-11-2024 02:07:47 PM

Event-CAM 1 14-11-2024 02:07:27 PM

Event-CAM 1 14-11-2024 02:05:16 PM

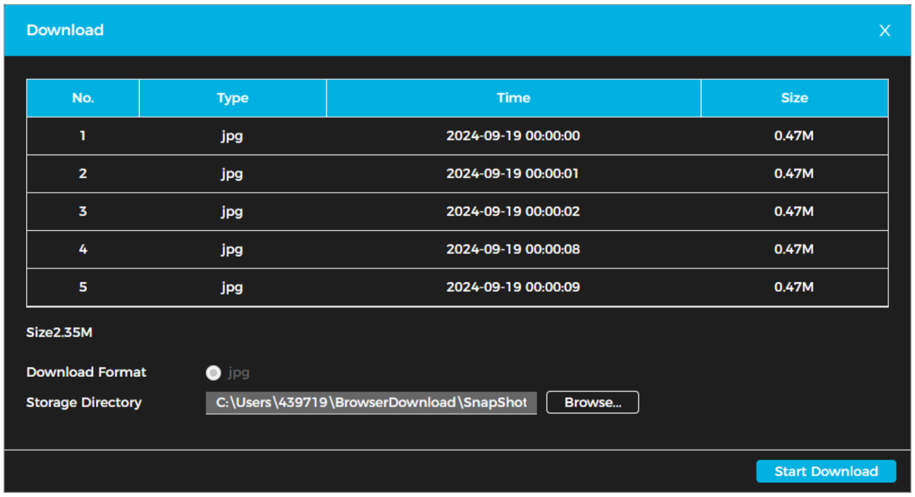
Event-CAM 1 14-11-2024 01:59:06 PM

Event-CAM 1 14-11-2024 01:57:21 PM

Event-CAM 1 14-11-2024 01:55:36 PM

Snapshot Download Selection

5. Click **Download**.
6. Select the download format. Click **Browse** to set the file storage path.



No.	Type	Time	Size
1	jpg	2024-09-19 00:00:00	0.47M
2	jpg	2024-09-19 00:00:01	0.47M
3	jpg	2024-09-19 00:00:02	0.47M
4	jpg	2024-09-19 00:00:08	0.47M
5	jpg	2024-09-19 00:00:09	0.47M

Size2.35M

Download Format ● jpg

Storage Directory C:\Users\439719\BrowserDownload\SnapShot

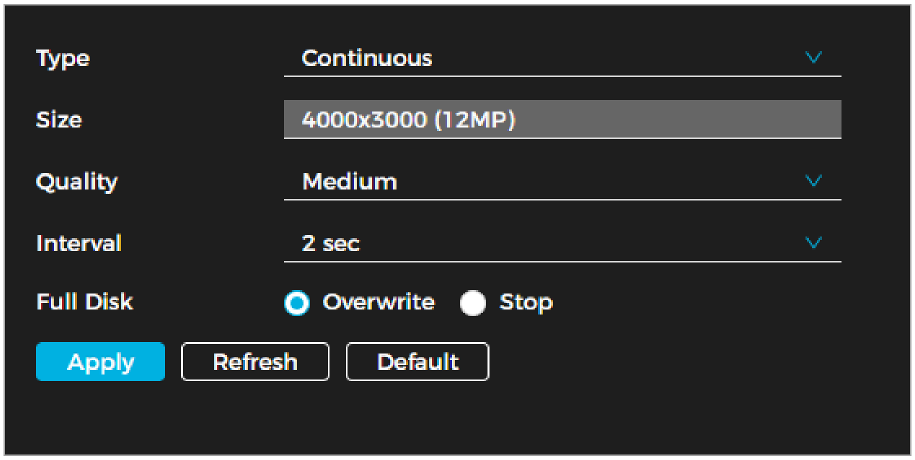
Download Snapshot Screen

7. Click **Start Download**.

How to Set Snapshot Parameters

Follow the steps below to configure snapshot settings.

1. Navigate to **File Search → Snapshot → Snapshot Settings**.
2. Set the parameters. See the table for more details.



Type: Continuous

Size: 4000x3000 (12MP)

Quality: Medium

Interval: 2 sec

Full Disk: ● Overwrite ○ Stop

Snapshot Parameters

Parameter	Description
Type	You can choose between **Continuous** and **Event**. • **Continuous**: Captures images within the configured period. • **Event**: Captures images when a configured event, such as Motion Detection, Video Tampering, or Scene Changing, is triggered. Ensure that the corresponding event detection and snapshot function are enabled.
Size	This will be the same as the mainstream resolution.
Quality	A higher value will result in better image quality.
Interval	Configure the snapshot frequency. Select **Automatic** to adjust the frequency as required.
Full Disk	• **Overwrite**: When the disk is full, the earliest recording is overwritten with current video. • **Stop**: When the disk is full, the recording is stopped, and no additional video can be recorded until space becomes available.

3. Click **Apply**.

How to Set a Storage Method for Snapshots

For detailed instructions, refer to the **Storage** section of this manual.

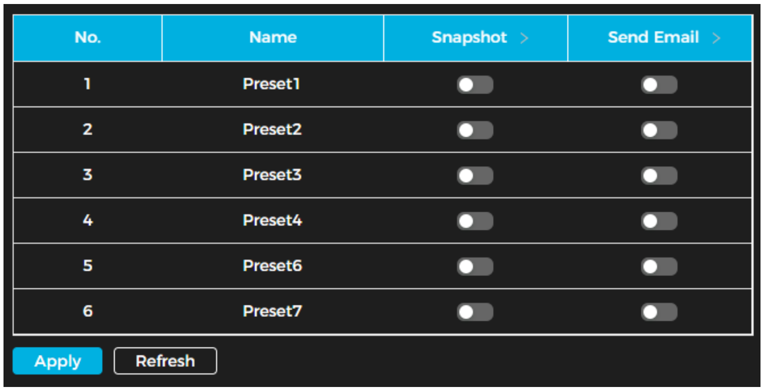
How to Set a Snapshot Plan

Based on the configured snapshot plan, the system activates or deactivates snapshots at the specified times. For detailed instructions, refer to **How to Set the Recording Plan**.

How to Snapshot by Location

Follow the instructions below to snapshot by preset location.

1. Navigate to **File Search → Snapshot → Snapshot by Location**.
2. Enable the function by clicking ○. You can also enable email notifications when a snapshot is taken by clicking ○ under Send Email.
3. Click **Apply**.



No.	Name	Snapshot >	Send Email >
1	Preset1	○	○
2	Preset2	○	○
3	Preset3	○	○
4	Preset4	○	○
5	Preset6	○	○
6	Preset7	○	○

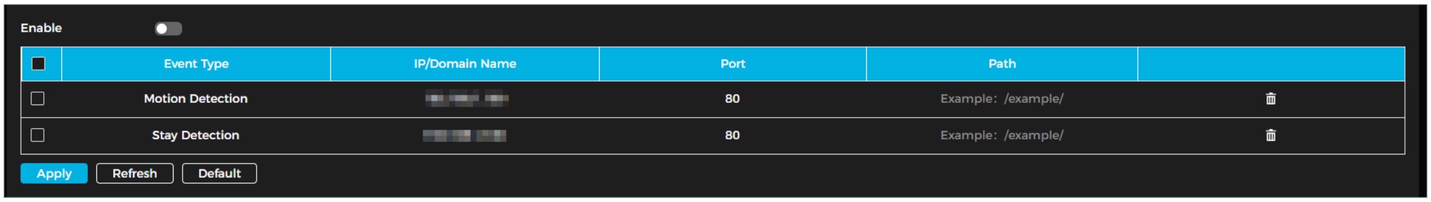
Snapshot by Location

How to Set a Network Destination

You can instruct the system to automatically transfer images to a specified server using the HTTP protocol. There is no need to set an upload period—images will be uploaded automatically when an alarm is triggered.

Follow the steps below to set a network destination to automatically receive images.

1. Navigate to **File Search → Snapshot → Network Destination**.
2. Enable the function.
3. Click +.
4. Configure the network destination parameters. You can add up to two servers. See the table below for more details.



Enable ○

■	Event Type	IP/Domain Name	Port	Path	
□	Motion Detection	[redacted]	80	Example: /example/	🗑
□	Stay Detection	[redacted]	80	Example: /example/	🗑

Network Destination

Parameter	Description
IP/Domain Name	Enter the IP address and port number of the server where the report will be uploaded.
Port	
Enable	Click ○ to enable the function.
Path	Refers to the storage path of the server.
Authentication	Enable this function and enter the correct username and password. The defined server will receive the images only if the credentials are correct.
Event Type	Select the event type from the drop-down list. You can choose multiple types simultaneously. The event types available in the drop-down list match those in snapshot playback.

5. Click **Apply**.

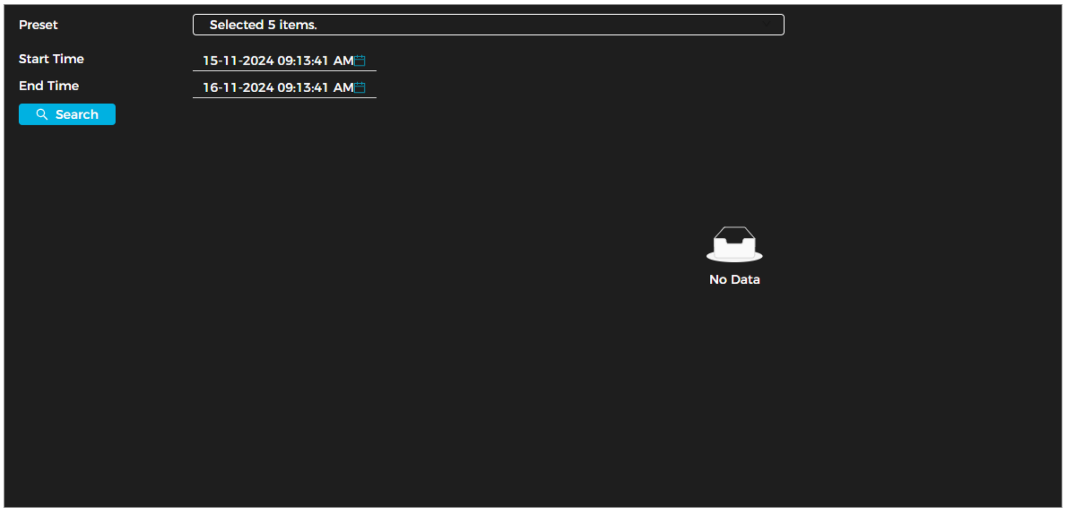
Smart Report

You can view AI function statistics by generating a smart report. The period for the report is from the past 24 hours by default. Click the 📅 to adjust the time period for the report.

Video Metadata Report

Follow the steps below to view a video metadata report.

1. Navigate to **File Search → Smart Report → Video Metadata**.
2. Specify the time period for the report. For multi-channel cameras, select the channel first.
3. Click **Search**.



Preset: Selected 5 items.

Start Time: 15-11-2024 09:13:41 AM

End Time: 16-11-2024 09:13:41 AM

Video Metadata Report

ⓘ

- You can select the desired statistics in the upper-right corner. Only selected statistics will be displayed.
- To export reports: Select the file format (.png or .csv). Click **Export**.

People Counting Report

The People Counting function accurately tracks and counts individuals as they enter or exit a designated area. To run a people counting report, do the following:

1. Ensure the people counting rule is configured before searching for the report.
2. Select **File Search → Smart Report → People Counting Report**.
3. Set search parameters. For multi-channel cameras, select the channel first. See the table below for more details.

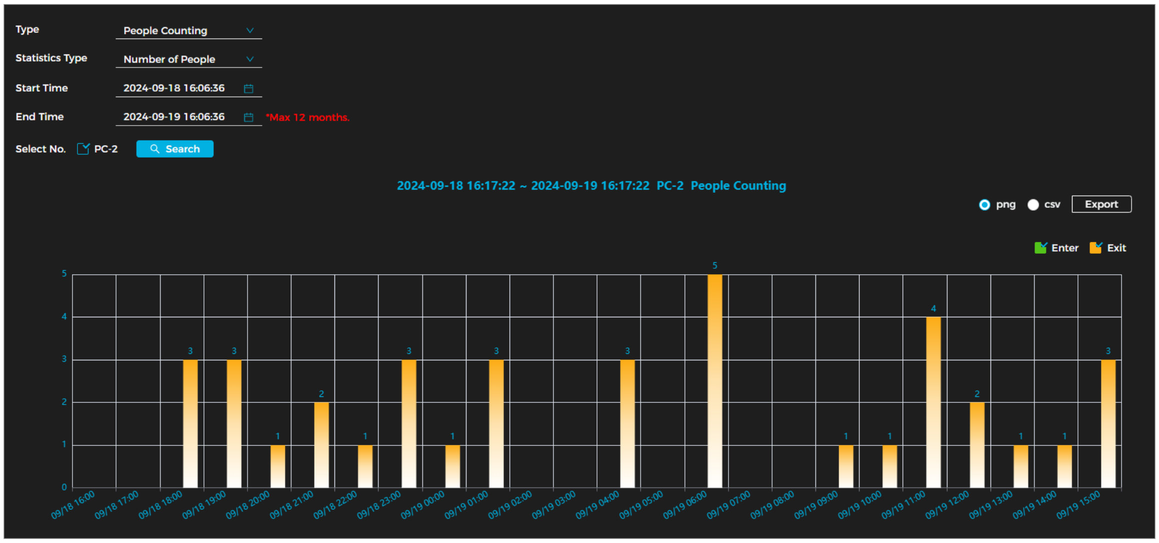
Parameter	Description
Type	Select the desired type, then choose the corresponding statistics type based on the selected option.
Statistics Type	• **Number of People**: Displays the report on the number of people who meet the specified conditions. • **Stay Time**: Shows the average duration people remain in the detection area within a specified period. This option is available when **Area People Counting** is selected.

Stay Time	When selecting **Area People Counting** as the rule and **Number of People** as the statistics type, Stay Time must be configured. The report shows the number of people whose stay time is less than or equal to or greater than the Stay Time threshold.
Queue Time	When selecting **Queuing** as the rule and **Number of People** as the statistics type, Queue Time must be configured. The report shows the number of people whose stay time is less than or equal to or greater than the Queuing Time threshold.
Start Time/End Time	Set the reporting period. • For **People Counting**, reports can be viewed daily, weekly, monthly, or yearly, with an option to customize the period. • For **Area People Counting** or **Queuing**, reports are available daily, weekly, or monthly, with an option to customize the period
Select No.	Select the event type from the drop-down list. You can choose multiple types simultaneously. The event types available in the drop-down list match those in snapshot playback.

4. Click **Search**.

ⓘ

- You can select the desired statistics in the upper-right corner. Only selected statistics will be displayed.
- To export reports: Select the file format (.png or .csv). Click **Export**.



Type: People Counting

Statistics Type: Number of People

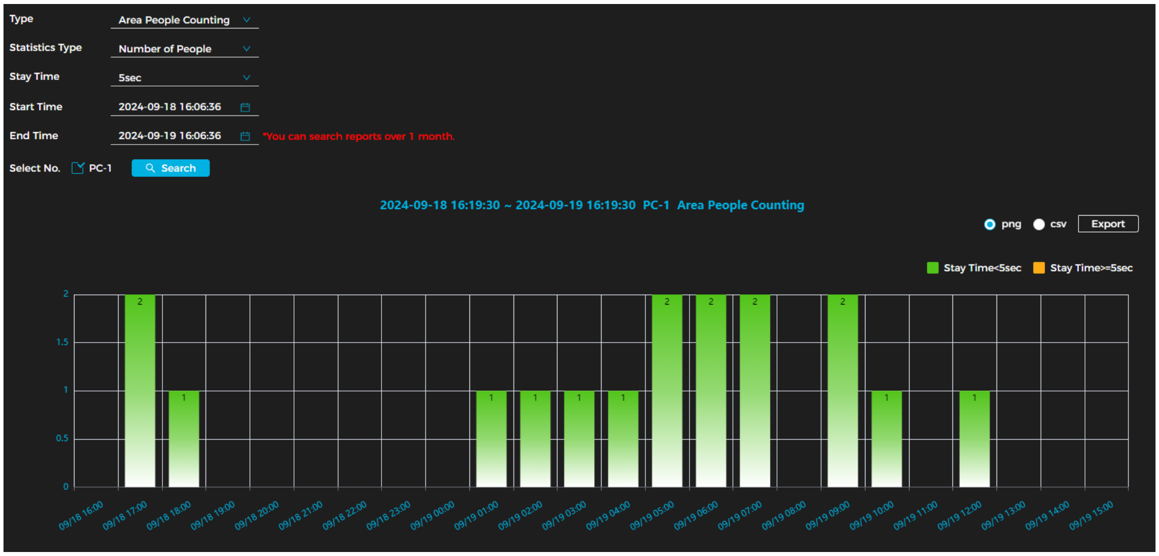
Start Time: 2024-09-18 16:06:36

End Time: 2024-09-19 16:06:36 *Max 12 months.

Select No. ☑ PC-2

2024-09-18 16:17:22 ~ 2024-09-19 16:17:22 PC-2 People Counting

People Counting Report



Type: Area People Counting

Statistics Type: Number of People

Stay Time: 5sec

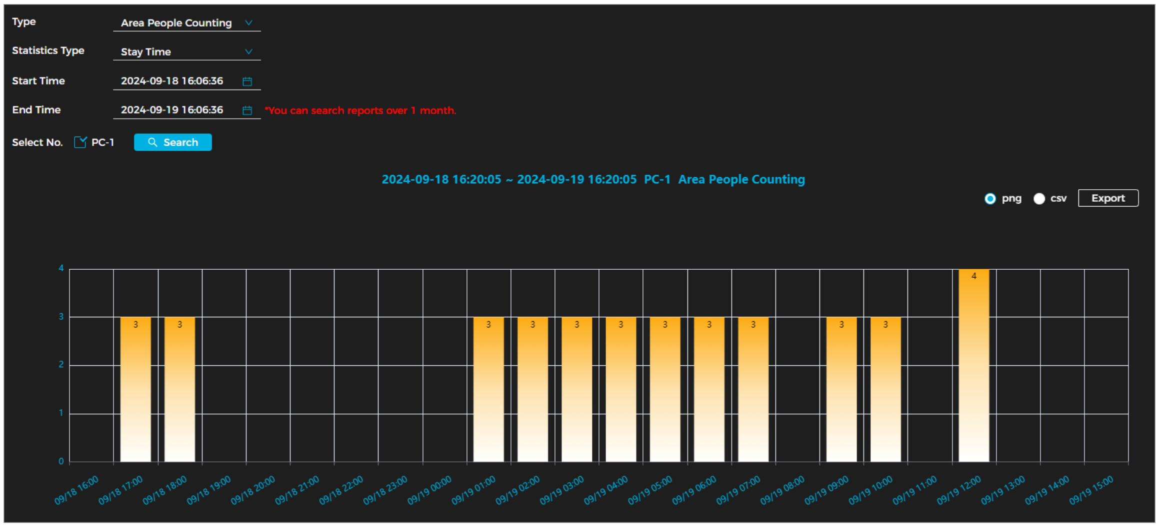
Start Time: 2024-09-18 16:06:36

End Time: 2024-09-19 16:06:36 *You can search reports over 1 month.

Select No. ☑ PC-1 Search

2024-09-18 16:19:30 ~ 2024-09-19 16:19:30 PC-1 Area People Counting

Area People Counting Report



Type: Area People Counting

Statistics Type: Stay Time

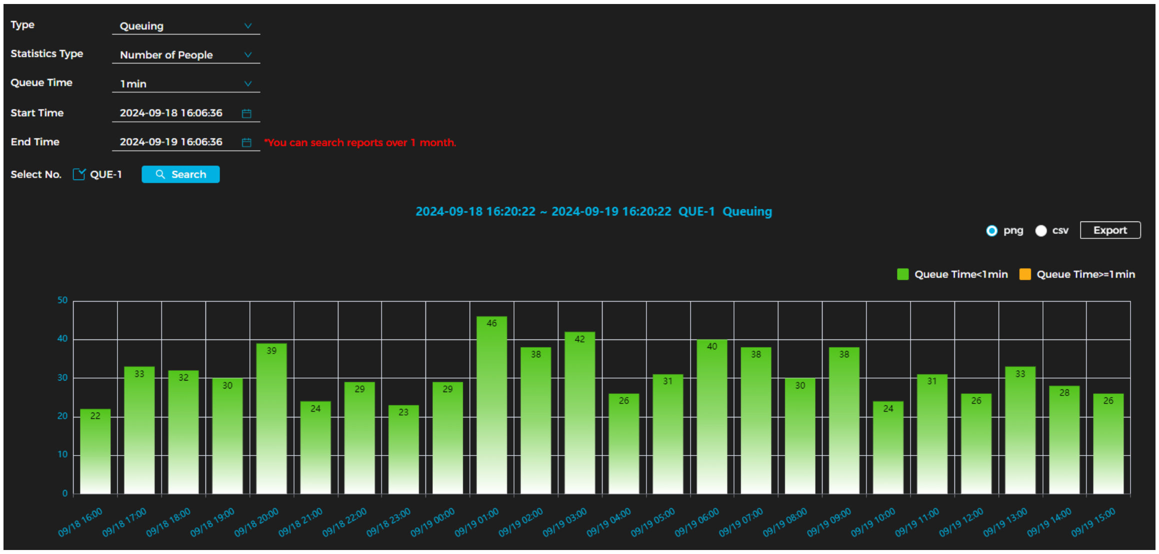
Start Time: 2024-09-18 16:06:36

End Time: 2024-09-19 16:06:36 *You can search reports over 1 month.

Select No. ☑ PC-1 Search

2024-09-18 16:20:05 ~ 2024-09-19 16:20:05 PC-1 Area People Counting

Stay Time Report



Type: Queuing

Statistics Type: Number of People

Queue Time: 1min

Start Time: 2024-09-18 16:06:36

End Time: 2024-09-19 16:06:36 *You can search reports over 1 month.

Select No. ☑ QUE-1 Search

2024-09-18 16:20:22 ~ 2024-09-19 16:20:22 QUE-1 Queuing

Queueing Report

Smart Analysis

The camera detects, recognizes, and tracks changes in the monitoring scene, analyzing target behavior as part of smart video monitoring.

When the intelligent function is enabled, configured rules and their effects are displayed on both the live video and the intelligent rule configuration page. If a target triggers an intelligent function, the rule lines flash red.

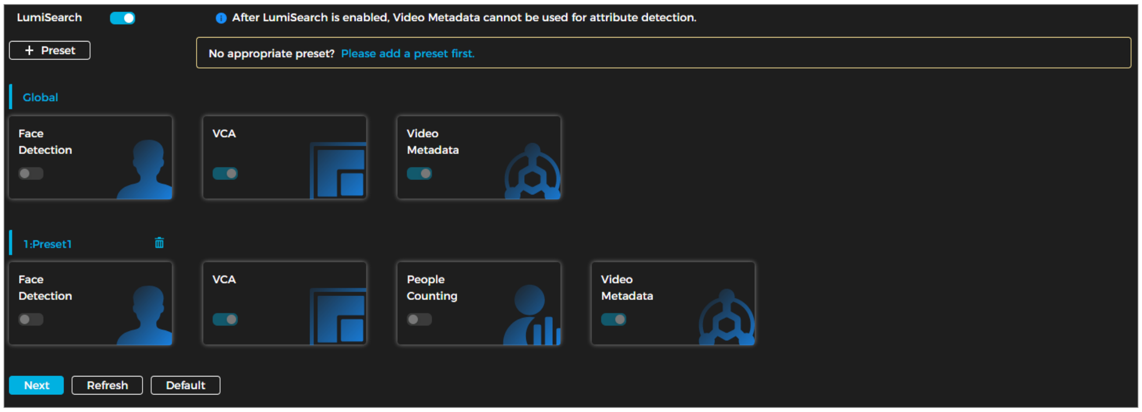
You can configure both global and preset intelligent modes in Smart Analysis. The global intelligent mode is displayed on the webpage by default. For the preset intelligent mode, ensure presets are added first, then click to select and display their intelligent modes on the webpage. For details on adding presets, see **PTZ Operation**.

How to Enable LumiSearch

LumiSearch allows you to quickly and accurately search for footage on a connected LumiSearch-enabled NVR. Follow the steps below to enable this feature.

ⓘ A Luminys NVR with LumiSearch capabilities must be used to enable LumiSearch.

1. Navigate to **Smart Analysis → Intelligent Mode**.
2. Click ○ next to LumiSearch to enable the function.



ⓘ After LumiSearch is enabled, Video Metadata cannot be used for attribute detection.

No appropriate preset? Please add a preset first.

Enable LumiSearch

3. (Optional) Click **Next** to configure other intelligent functions as required.

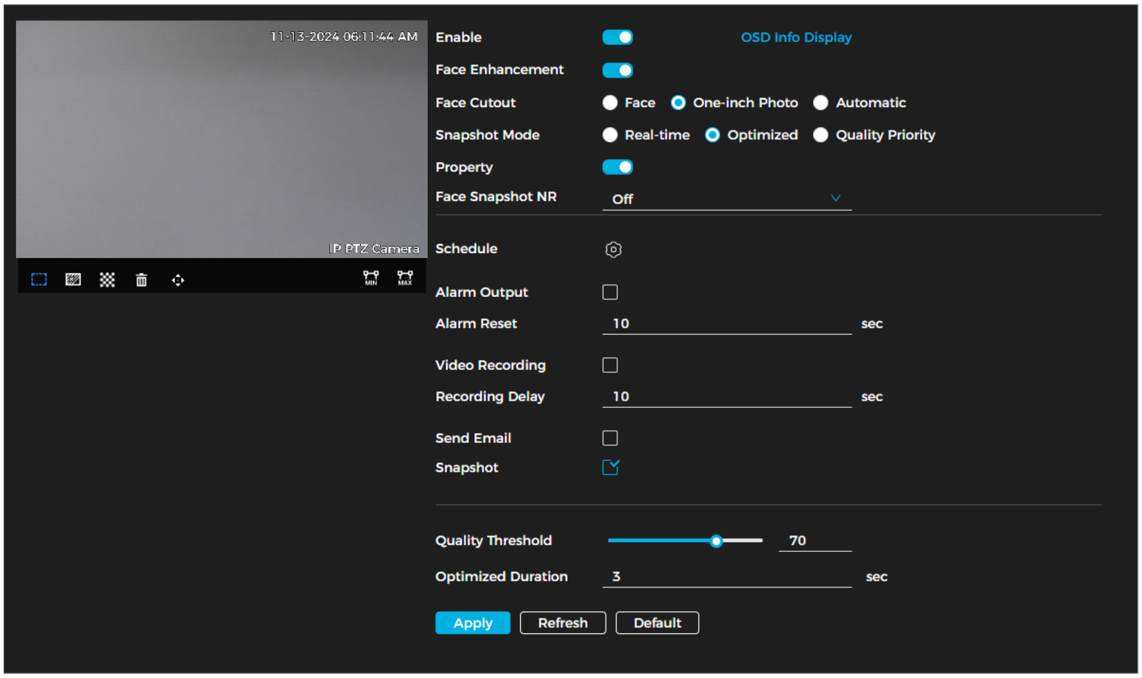
How to Set Up Face Detection

You can program the system to perform an alarm linkage action when a face is detected in a monitoring area. Follow the steps below to set up face detection.

1. Navigate to **Smart Analysis → Intelligent Mode**.
2. Click ○ next to Face Detection to enable the function on the corresponding channel.
3. Click **Next**.

ⓘ Pages and functions may vary based on device model.

4. Click ○ next to **Enable** to activate the face detection.
5. (Optional) Click the icons at the bottom of the image to configure the detection and exclusion area and target size. See the table for more details.



11-13-2024 06:11:44 AM

IP PTZ Camera

Enable: On — OSD Info Display

Face Enhancement: On

Face Cutout: ○ Face ● One-inch Photo ○ Automatic

Snapshot Mode: ○ Real-time ● Optimized ○ Quality Priority

Property: On

Face Snapshot NR: Off

Schedule ⚙

Alarm Output ☐

Alarm Reset: 10 sec

Video Recording ☐

Recording Delay: 10 sec

Send Email ☐

Snapshot ☑

Quality Threshold: 70

Optimized Duration: 3 sec

Face Detection

Icon	Description
⬚	Draw the detection area. By default, the whole image is the detection area.
▨	Draw the exclusion area.
MIN	Set the minimum size of the target. The target must be greater than or equal to the minimum size to trigger an alarm.
MAX	Set the maximum size of the target. The target must be less than or equal to the maximum size to trigger an alarm.
▦	To show pixel size, press and hold the left mouse to draw a rectangle.
🗑	Delete a detection line.

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

Parameter	Description
Face Enhancement	Click ○ to enable the function. If the bit stream is low, facial clarity will be given priority.
Non-Living Filtering	Filter non-living faces (i.e, picture of a face).
Target Box Overlay	Click ○ to enable the function. Add a bounding box to the face in the image to highlight it. The captured face will be saved to the SD card or storage path.
Remove Duplicate Faces	Removes duplicate faces for accurate counting. Click ⚙ to set the time and precision. • **Time**: Enable **Remove Duplicate Faces** in the configured time. • **Precision**: A higher level increases sensitivity, reducing duplicate faces.
Face Cutout	Set the range for matting face images, choosing from **Face**, **One-Inch Photo**, or **Automatic**. When selecting **Automatic**, click ⚙, configure the parameters on the prompt page, and then click **Apply**.

	- **Customized Width**: Set the snapshot width by entering a multiple of the original face width (range: 1 – 5). - **Customized Face Height**: Set the face height in the snapshot by entering a multiple of the original face height (range: 1 – 2). - **Customized Body Height**: Set the body height in the snapshot by entering a multiple of the original body height (range: 0 – 4). A value of 0 means only the face image will be cut out.
Snapshot Mode	- **Real-Time**: Captures the image immediately after the camera detects a face. - **Optimized**: Captures the clearest image within the set time after face detection. - **Quality Priority**: Continuously compares captured faces with those in the armed face database and captures the most similar image before sending the event. Recommended for access control scenarios.
Property	Click ○ to display properties.
Face Snapshot NR	Click ○ to enable the function. You can adjust the NR level manually.
Face Exposure	Click ○ to enable the function. When a face is detected, the camera can enhance its brightness to improve image clarity.
Face Target Brightness	Adjust the face target brightness. The default value is **50**.
Face Exposure Detection Interval	Set the face exposure detection interval to avoid image flickering due to continuous exposure adjustments. The default value is **5 seconds**.
Snapshot Angle Filter	Configure the snapshot angle to be filtered during face detection.
Snapshot Sensitivity	Adjust the snapshot sensitivity for face detection. Higher sensitivity improves face detection accuracy.
Quality Threshold	Adjust the quality threshold for face detection.
Optimized Duration	Configure the time period to capture the clearest image after face detection.

7. Configure the arming schedule and alarm linkage action(s). For more details, see the **Alarm Linkage** section of the manual.

8. Click **Apply**. The face detection results will appear on the live page. The pictures and their attribute information will be displayed. You can click a face picture in the display area to see details.

How to Configure Video Content Analytics (VCA)

This section explains the scene selection requirements and rule configuration for VCA.

Basic Scene Selection Requirements

The following are the basic requirements for scene selection:

- The target should not occupy more than 10% of the entire image.
- The target size should be at least 10 x 10 pixels. For abandoned objects, the minimum size should be 15 x 15 pixels (CIF image). The target's height and width should not exceed one-third of the image dimensions. The recommended target height is 10% of the image height.
- The brightness difference between the target and the background should be at least 10 gray levels.
- The target should remain in the image for at least two seconds, with a movement distance greater than its width and no less than 15 pixels (CIF image).

- Minimize the complexity of the surveillance scene. Intelligent analysis functions are not recommended for scenes with dense targets or frequent lighting changes.
- Avoid areas with glass, reflective surfaces, water, or interference from branches, shadows, or insects. Also, avoid backlit scenes and direct light exposure.

Rule Configuration

You can set the rules for VCA including cross fence detection, line crossing, intrusion, abandoned object, moving object, fast moving, parking detection, crowd gathering, and loitering detection.

See the table below for the functions and applications of the rules. Not all device models will support every function listed in the table.

Rule	Description	Applicable Scene
Line Crossing	When a target crosses the tripwire in the defined motion direction.	Suitable for scenes with sparse targets and no target occlusion.
Intrusion	When a target enters, exits, or appears in the detection area.	
Abandoned Object	When an object remains in the detection area beyond the configured time.	Suitable for scenes with sparse targets and minimal light changes. A simple detection area is recommended. • Missed alarms may increase in scenes with dense targets, frequent occlusion, or stationary individuals. • In complex foreground and background environments, false alarms may occur for abandoned or missing object
Missing Object	When an object is removed from the detection area for longer than the defined time.	Suitable for scenes with sparse targets and minimal light changes. A simple detection area is recommended. • Missed alarms may increase in scenes with dense targets, frequent occlusion, or stationary individuals • In complex foreground and background environments, false alarms may occur for abandoned or missing objects.
Parking Detection	When a target remains in the area beyond the configured time.	Ideal for road monitoring and traffic management.
Aggregate Detection	When a crowd gathers or reaches a higher density than the configured threshold.	Best for medium to long-distance scenes, such as outdoor plazas, government entrances, and station entry/exit points. Not recommended for short-distance analysis.
Loitering Detection	When a target loiters beyond the shortest alarm time, an alarm is triggered. If the target remains in the area within the alarm interval, the alarm will be triggered again.	Applicable to locations like parks and halls

Follow the steps below to configure VCA rules. Line crossing is used as an example.

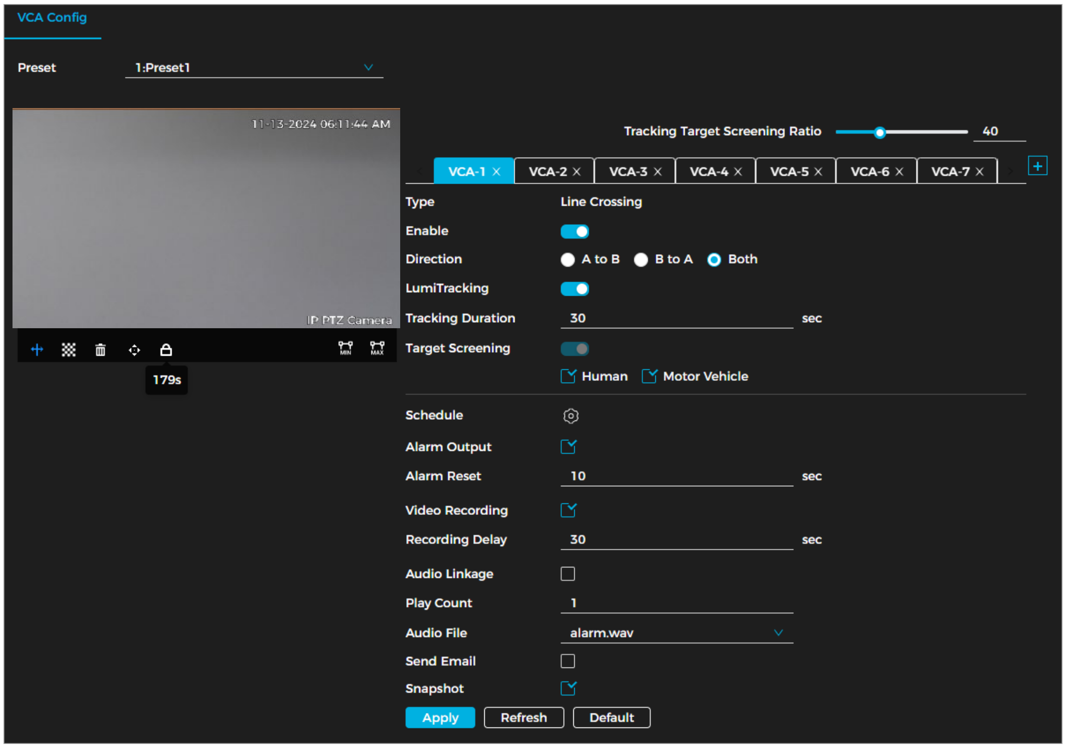
1. Navigate to **Smart Analysis → Intelligent Mode**.

2. Click ○ next to VCA to enable it for the corresponding channel.

3. Click **Next**.

4. Click + on the **VCA Config** page.

5. Select the desired VCA. **Line Crossing** is selected in this example.



VCA Config

Preset: 1:Preset1

11-13-2024 06:11:44 AM

IP PTZ Camera

179s

Tracking Target Screening Ratio: 40

VCA-1 × | VCA-2 × | VCA-3 × | VCA-4 × | VCA-5 × | VCA-6 × | VCA-7 ×

Type	Line Crossing
Enable	●
Direction	○ A to B ○ B to A ● Both
LumiTracking	●
Tracking Duration	30 sec
Target Screening	○
	☑ Human ☑ Motor Vehicle
Schedule	⚙
Alarm Output	☑
Alarm Reset	10 sec
Video Recording	☑
Recording Delay	30 sec
Audio Linkage	□
Play Count	1
Audio File	alarm.wav
Send Email	□
Snapshot	☑

Line Crossing VCA Configuration

6. Click ✛ to draw the rule lines on the image. Right click when done. Adjust the area range by dragging the corners of the detection area. See the table below for the drawing rules.

Rule	Description
Line Crossing	Draw the detection line.
Intrusion	Draw the detection area. • When detecting abandoned objects, an alarm may also be triggered if a pedestrian or vehicle remains in the area for an extended period. If the abandoned object is smaller than a pedestrian or vehicle, adjust the target size to filter out pedestrians and vehicles or extend the detection duration to prevent false alarms caused by brief stops. • When detecting crowd gatherings, false alarms may occur due to factors such as low camera installation height, a single person occupying a large portion of the image, significant target occlusion, continuous camera shaking, moving leaves or tree shadows, frequent opening or closing of retractable doors, or high-density traffic and pedestrian flow.
Abandoned Object	
Missing Object	
Parking Detection	
Aggregate Detection	
Loitering Detection	

7. (Optional) Click the icons to the right side of the image to add target filters. See the table below for more details.

Icon	Description
MIN	Set the minimum size of the target. The target must be greater than or equal to the minimum size to trigger an alarm.

MAX	Set the maximum size of the target. The target must be less than or equal to the maximum size to trigger an alarm.
▩	To show pixel size, press and hold the left mouse to draw a rectangle.
🗑	Delete a detection line.
✥	Adjust the live page through the PTZ control panel.
🔒	Lock PTZ functions while drawing rule lines. The maximum lock duration is 180 seconds.

8. Set the VCA rule parameters. See the table below for more details.

Parameter	Description
Direction	Configure the detection direction for rule settings. • For line crossing, choose A → B, B → A, or A ←→ B. • For intrusion, select Enter, Exit, or Both.
LumiTracking	Click ○ to enable **LumiTracking**, then set the Tracking Duration based on actual requirements. Once auto tracking is enabled, the camera follows and captures the target until the set duration expires. This function is supported only on certain devices.
Tracking Duration	
Target Filter	When **Target Filter** is enabled, the system will not trigger an alarm for selected targets only the selected targets. Available for line crossing, intrusion, and fast-moving rules. Human and vehicles are the targets selected by default.
Duration	• For **abandoned objects**, the duration represents the shortest time required to trigger an alarm after an object is left unattended. • For **missing objects**, the duration is the shortest time needed to trigger an alarm after an object disappears. • For **parking detection**, crowd gathering, or loitering detection, the duration is the minimum time required to trigger an alarm after an object appears in the designated area.
Sensitivity	Higher sensitivity increases detection accuracy but may also lead to more false detections.

9. Set the arming schedule and alarm linkage actions. For more details, see the **Alarm Linkage** section of this manual.

10. Click **Apply**.

How to Configure People Counting

You can configure people counting (including entry, exit, and area stay counts), queue counting, and view the results in report form. People counting data is periodically overwritten when storage reaches full capacity.

Global Configuration

Follow the steps below to set the sensitivity of people counting.

1. Navigate to **Smart Analysis → Intelligent Mode**.

2. Click ○ next to **People Counting** to enable the function on the corresponding preset.

3. Click **Next**.

4. Set **Sensitivity**. Higher sensitivity increases the likelihood of triggering an alarm.

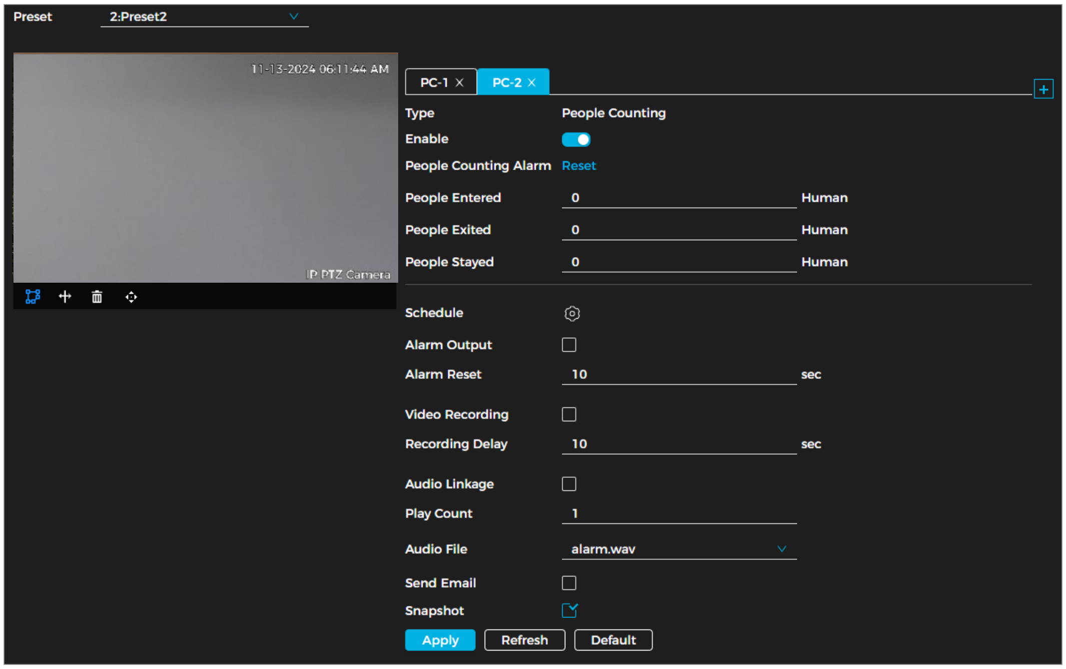
5. Click **Apply**.

People Counting

The system tracks the number of people entering and exiting the detection area. When the count exceeds the set threshold, an alarm is triggered, and the system executes the configured linkage action.

1. Navigate to **Smart Analysis → Intelligent Mode**.
2. Click ○ next to **People Counting**.
3. Click **Next**.
4. Click + to select the rules as needed. Choose between **Area People Counting** or **People Counting**.

- **People Counting:** Click ⛶. Drag any corner of the box to resize the detection area. Right-click and hold to move the box. Click ✛ to draw the direction line on the image. Refer to the on-screen prompts and diagram when drawing the detection area and direction line, then configure the people counting parameters.



Preset 2:Preset2

11-13-2024 06:11:44 AM

IP PTZ Camera

PC-1 × | PC-2 ×

Type People Counting

Enable ●

People Counting Alarm Reset

People Entered 0 Human

People Exited 0 Human

People Stayed 0 Human

Schedule

Alarm Output □

Alarm Reset 10 sec

Video Recording □

Recording Delay 10 sec

Audio Linkage □

Play Count 1

Audio File alarm.wav

Send Email □

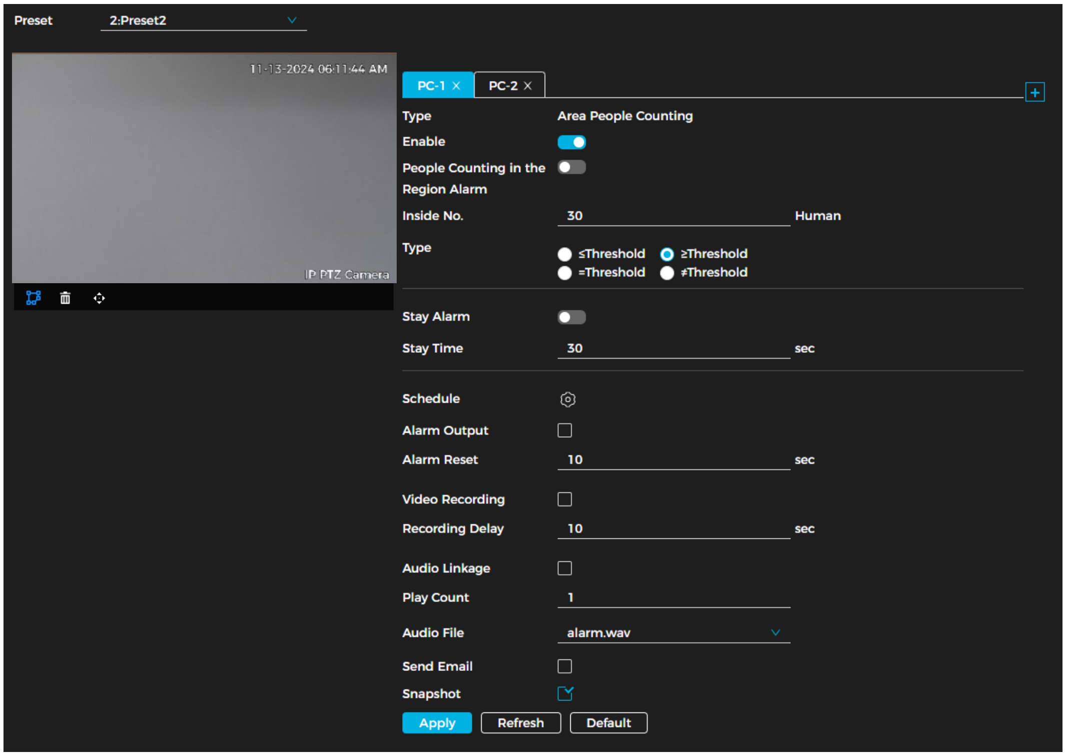
Snapshot ☑

Apply Refresh Default

People Counting Rule

Parameters	Description
People Counting Alarm	Click **Reset** to clear the current count results.
People Entered	Counts people moving from A → B; an alarm triggers when the count exceeds the set limit.
People Exited	Counts people moving from B → A; an alarm triggers when the count exceeds the set limit.
People Stayed	Calculates the difference between People Entered and People Exited; an alarm triggers when the value exceeds the set threshold.

- **Area People Counting**: The system measures the number of people and their dwell time within the detection area. When either count or duration exceeds the set threshold, an alarm is triggered, and the system executes the configured linkage action. This function is supported only by certain models.
    - Click ⛶. Drag any corner of the box to resize the detection area. Right-click and hold to move the box. Set the parameters.



Preset 2:Preset2

11-13-2024 06:11:44 AM

IP PTZ Camera

PC-1 × PC-2 ×

Type Area People Counting

Enable ●

People Counting in the Region Alarm ○

Inside No. 30 Human

Type ○ ≤Threshold ● ≥Threshold ○ =Threshold ○ ≠Threshold

Stay Alarm ○

Stay Time 30 sec

Schedule

Alarm Output □

Alarm Reset 10 sec

Video Recording □

Recording Delay 10 sec

Audio Linkage □

Play Count 1

Audio File alarm.wav

Send Email □

Snapshot ☑

Parameters	Description
People Counting in the Region Alarm	When the People Counting in Region Alarm function is enabled, alarm rules are generated based on Inside No. and Type. For example, if Inside No. is set to 8 and Type is > Threshold, an alarm triggers when the number of people in the detection area reaches 9. Click ○ next to People Counting in Region Alarm to enable the function. Set the number of people for the detection area. Choose the counting type from the following: • < Threshold • > Threshold • = Threshold • =/= Threshold
Inside No.	
Type	
Stay Alarm	Click ○ next to Stay Alarm to enable the function, then set the Stay Time. When a person's dwell time in the detection area exceeds the set value, an alarm is triggered.
Stay Time	

5. (Optional) Click 🗑 to delete the detection. Click ✥ to adjust the image through the PTZ control panel.

6. Set the arming schedule and alarm linkage actions.

7. Click **Apply**.

You can view the counting results on the Live View page. For **People Counting** rules, entry and exit counts are shown. For **Area People Counting** rules, the number of people within the detection area is shown.

Queue People Counting

The system monitors the number of people queuing within the detection area. When the queue count or wait time exceeds the configured threshold, an alarm is triggered, and the system executes the configured linkage action.

Follow the steps below to enable queue people counting.

1. Navigate to **Smart Analysis → Intelligent Mode**.

2. Click ○ next to **People Counting**.

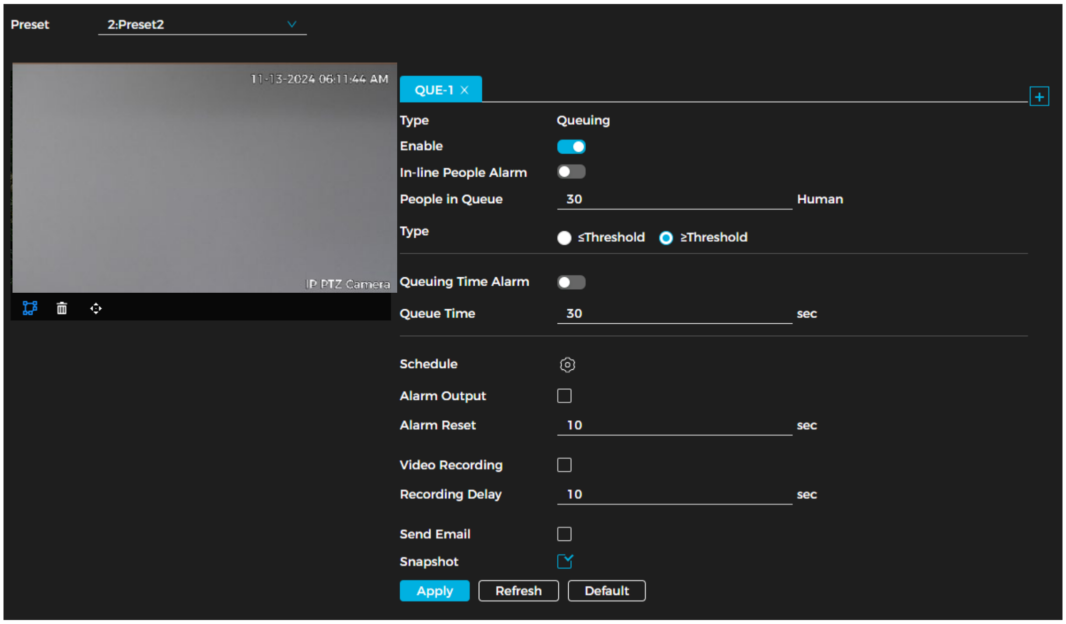
3. Click **Next**.

4. Click the **Queueing** tab. Select a preset from the dropdown list.

5. Click + to add rules as needed.

6. Click ⛶. Drag any corner of the box to resize the detection area. Right-click and hold to move the box.

7. Set the parameters.



Preset 2:Preset2

QUE-1 ×

Type Queuing

Enable ●

In-line People Alarm ○

People in Queue 30 Human

Type ○ ≤Threshold ● ≥Threshold

Queuing Time Alarm ○

Queue Time 30 sec

Schedule

Alarm Output □

Alarm Reset 10 sec

Video Recording □

Recording Delay 10 sec

Send Email □

Snapshot ☑

Apply Refresh Default

Parameters	Description
In-Line People Alarm	When the In-line People Alarm function is enabled, alarm rules are defined by People in Queue and Type.For example, if People in Queue is set to 8 and Type is ≥ Threshold, an alarm triggers when the queue count in the detection area reaches 9. Click ○ next to In-Line People Alarm to enable the function. Set the number of people for the detection area. Choose the counting type from the following: • ≤ Threshold • ≥ Threshold
People in Queue	
Type	
Queuing Time Alarm	Click ○ next to Queuing Time Alarm to enable the function, then set the Queuing Time. When a person's queue time in the detection area exceeds the set value, an alarm is triggered.
Queuing Time	

8. (Optional) Click 🗑 to delete the detection. Click ✥ to adjust the image through the PTZ control panel.

9. Set the arming schedule and alarm linkage actions.

10. Click **Apply**.

You can view the counting results on the Live View page. The page displays each target's queue count and waiting time.

How to Set Up Video Metadata

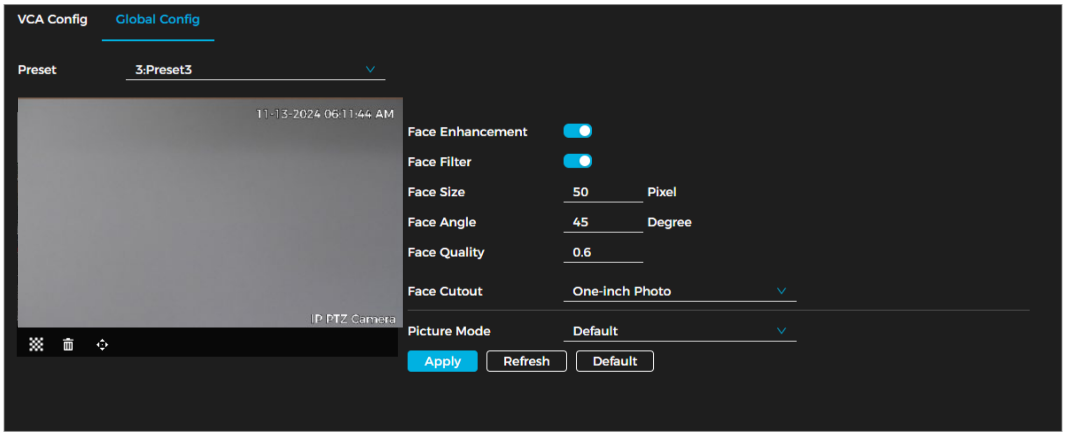
Classify people and motor vehicles in the captured video, displaying their relevant attributes on the live page.

Global Configuration

Follow the steps below to configure the global configuration of video metadata, including face parameter and scene parameter.

1. Navigate to **Smart Analysis → Intelligent Mode**.
2. Click ○ next to **Video Metadata** to enable the function on the corresponding channel.
3. Click **Next**.
4. Click the **Global Config** tab.
5. Configure the parameters. See the table below for more details.

ⓘ Pages and functions may vary based on device model.



Preset 3:Preset3

Face Enhancement ●

Face Filter ●

Face Size 50 Pixel

Face Angle 45 Degree

Face Quality 0.6

Face Cutout One-inch Photo

Picture Mode Default

Global Configuration of Video Metadata

Parameter	Description
Preset	If Video Metadata is enabled for multiple presets, you can select a preset from the drop-down list to configure its corresponding metadata.
Face Enhancement	Click ○ to enable face enhancement. Priority should be given to ensuring facial clarity when the bit stream is relatively low.
Face Cutout	Set the range for matting face images, choosing from **Face** or **One-Inch Photo**.
Face Filter	Click ○ to enable the function. You can adjust the face size, face angle and face quality level manually.
Picture Mode	• **Default**: Uses standard image parameters for capture. • **Number Plate Priority**: Applies image parameters optimized for license plate capture. • **Face Priority**: Applies image parameters optimized for face capture.

6. Click **Apply**.

Rule Configuration

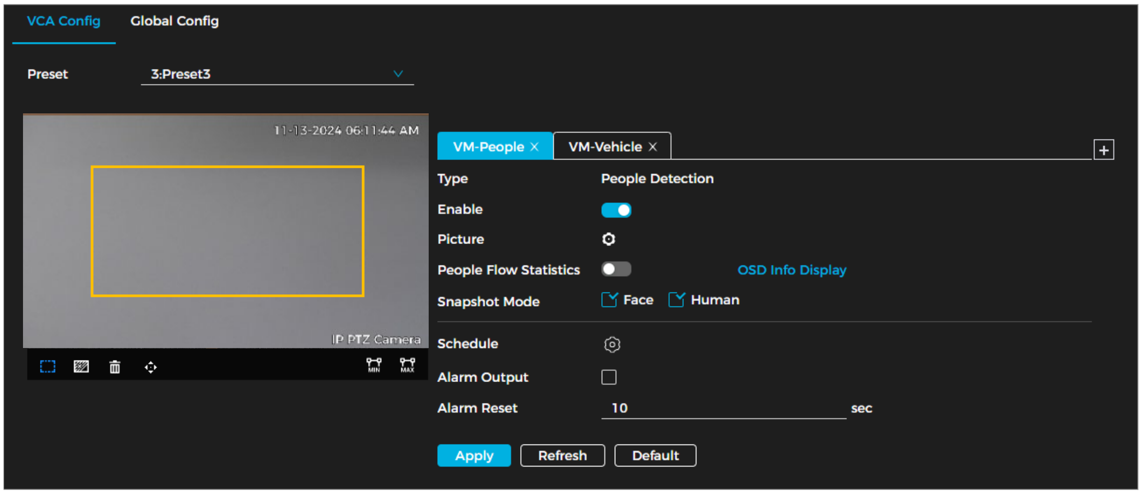
Prior to rule configuration, ensure the following prerequisites are met:

- Navigate to **Smart Analysis → Intelligent Mode**. Enable **Video Metadata**.
- Ensure the **Global Config** parameters are set.

Follow the steps below set the detection scene and rules.

1. Navigate to **Smart Analysis → Intelligent Mode**.
2. Click ○ next to **Video Metadata**.
3. Click **Next**.
4. Click the **VCA Config** tab.

5. Click + to select the rules.



VCA Config | Global Config

Preset: 3:Preset3

11-13-2024 06:11:44 AM

IP PTZ Camera

VM-People × | VM-Vehicle × | +

Type: People Detection

Enable: ●

Picture: ⚙

People Flow Statistics: ○ OSD Info Display

Snapshot Mode: ☑ Face ☑ Human

Schedule: ⚙

Alarm Output: □

Alarm Reset: 10 sec

Apply | Refresh | Default

Rule Configuration (Video Metadata)

6. Configure the picture by clicking ⚙.

7. Configure the overlay for motor vehicles and people and set the box position. This section uses motor vehicle overlay configuration as an example.

8. Click ○ to enable **Video OSD Show**. Configure the related information.

9. Select the type of overlay to be captured and adjust the position of the displayed information.

10. Choose the overlay image upload type(s).

11. Click **Apply**.

12. (Optional) Click the icons at the bottom of the image. See the table for more details.

Icon	Description
⬚	After enabling the rule, the detection area is displayed. Click the icon, then drag any corner of the box to adjust its size. Press and hold the left mouse button to move the box and change its position.
▨	Draw the exclusion area.
MIN	Set the minimum size of the target. The target must be greater than or equal to the minimum size to trigger an alarm.
MAX	Set the maximum size of the target. The target must be less than or equal to the maximum size to trigger an alarm.
✥	Adjust the live page through the PTZ control panel.
🗑	Delete a detection line.

13. Set the video metadata parameters. Click **Apply**.

Parameter	Description
People Flow Statistics	Count the number of people in the detection area.
Traffic Flow Statistics	Count the number of motor vehicles in the detection area.
Snapshot Mode	Choose a snapshot mode. - **Optimized**: Captures images until the vehicle exits the frame, then reports the clearest one.

	• **Line Crossing**: Captures images when a vehicle crosses the rule line in the configured direction. Choose the direction: A to B, B to A, or both, and adjust the rule line position as needed.
Vehicle Filter	Select **Unlicensed**, **Invalid Plate**, or both.

14. Set the arming schedule and alarm linkage actions. For more details, see the **Alarm Linkage** section of this manual.

15. Click **Apply**.

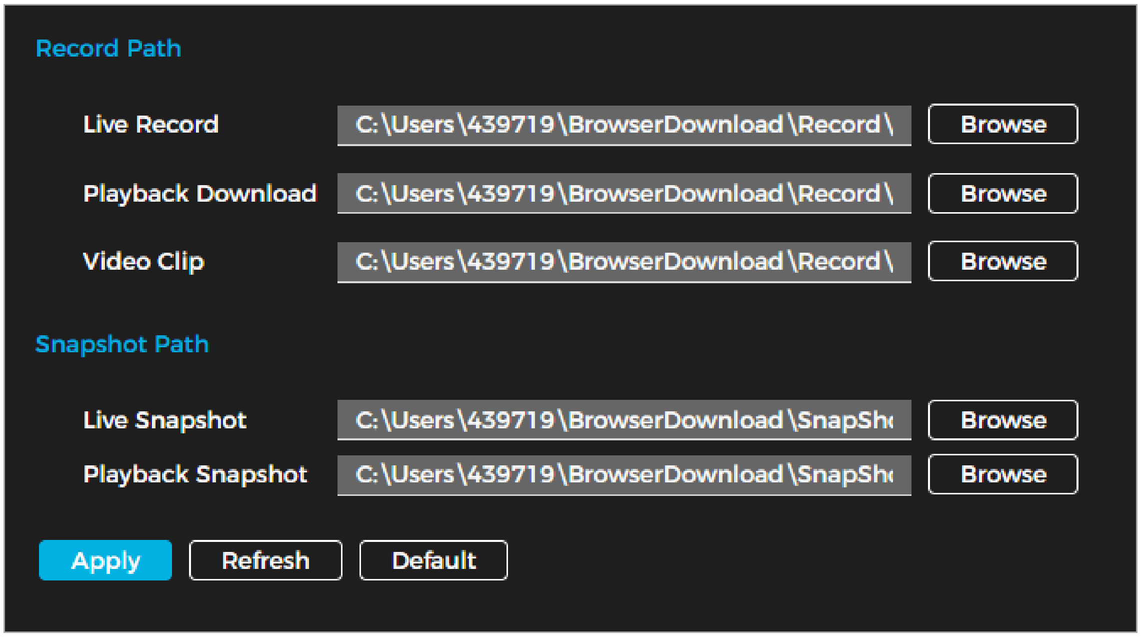
Settings

This section covers the basic camera settings, including the configuration of local settings, system, network, video/audio, image, event, and storage.

Local Settings

Follow the steps below to configure local settings.

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



Record Path

Live Record: C:\Users\439719\BrowserDownload\Record\

Playback Download: C:\Users\439719\BrowserDownload\Record\

Video Clip: C:\Users\439719\BrowserDownload\Record\

Snapshot Path

Live Snapshot: C:\Users\439719\BrowserDownload\SnapSh

Playback Snapshot: C:\Users\439719\BrowserDownload\SnapSh

Local Settings

2. Click **Browse** to select the storage path for live snapshot, live record, playback snapshot, playback download, and video clip. See the table below for more details.

Parameter	Description
Live Record	The recorded video of live page. The default path is C:\Users\admin\BrowserDownload\Record\Live.
Playback Download	The downloaded video of playback page. The default path is C:\Users\admin\BrowserDownload\Record\Playback.
Video Clip	The clipped video of playback page. The default path is C:\Users\admin\BrowserDownload\Record\Clips.
Live Snapshot	The snapshot of live page. The default path is C:\Users\admin\BrowserDownload\Snapshot\Live.
Playback Snapshot	The snapshot of playback page. The default path is C:\Users\admin\BrowserDownload\Snapshot\Playback.

ⓘ "Admin" in the path indicates the account currently in use.

3. Click **Apply**.

System

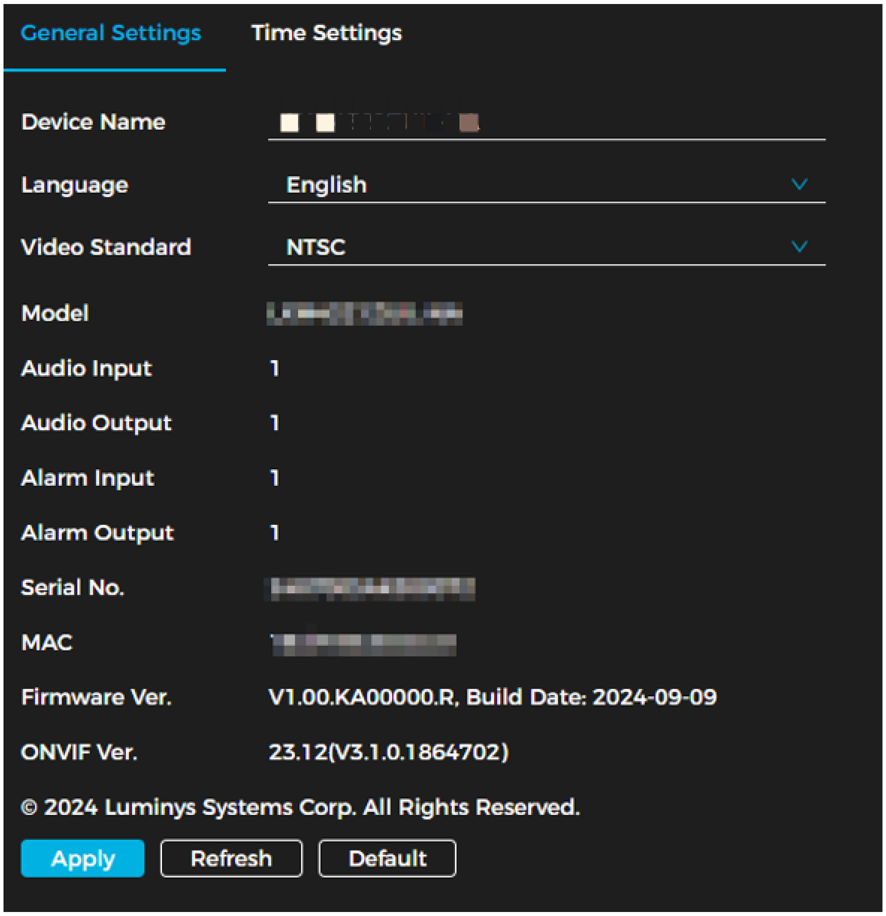
This section covers system configurations, including system settings, maintenance, security, user management, and legal information.

System Settings

General Settings

Follow the steps below to configure the device name, language, and video standard, and view device information such as model, serial number, MAC address, firmware version, and ONVIF version.

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



Device Name [redacted]

Language English

Video Standard NTSC

Model [redacted]

Audio Input 1

Audio Output 1

Alarm Input 1

Alarm Output 1

Serial No. [redacted]

MAC [redacted]

Firmware Ver. V1.00.KA00000.R, Build Date: 2024-09-09

ONVIF Ver. 23.12(V3.1.0.1864702)

© 2024 Luminys Systems Corp. All Rights Reserved.

General Settings

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

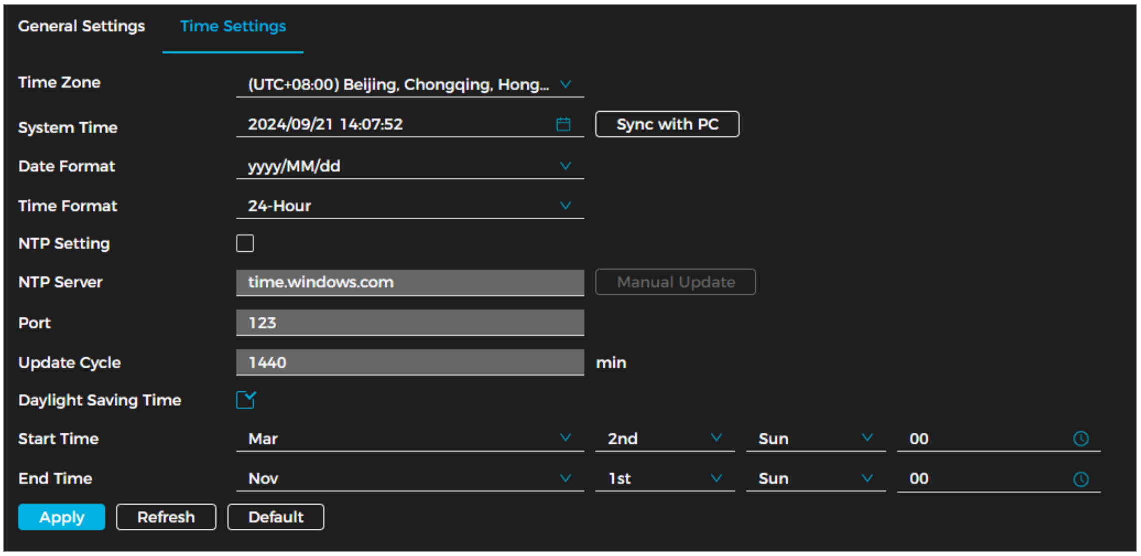
Parameter	Description
Device Name	Input the device name.
Language	Set the system language (English, Spanish, or French).
Video Standard	Choose **PAL** or **NTSC**.

3. Click **Apply**.

Time Settings

Follow the steps below to configure the date and time format, time zone, system time, daylight saving time or NTP server.

1. Navigate to **Settings → System → System Settings → Time Settings**.


General Settings | Time Settings

Time Zone: (UTC+08:00) Beijing, Chongqing, Hong...

System Time: 2024/09/21 14:07:52 | Sync with PC

Date Format: yyyy/MM/dd

Time Format: 24-Hour

NTP Setting: □

NTP Server: time.windows.com | Manual Update

Port: 123

Update Cycle: 1440 min

Daylight Saving Time: ☑

Start Time: Mar | 2nd | Sun | 00

End Time: Nov | 1st | Sun | 00

Apply | Refresh | Default

Time Settings

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

Parameter	Description
Time Zone	Select the time zone the camera is installed at.
System Time	Set the system time. Select **Sync with PC** to use the system time.
Date Format	Set the date format.
Time Format	Set the time format (12-Hour or 24-Hour).
NTP Setting	When selecting **NTP**, the system synchronizes time with an internet server in real time. You can also enter the NTP server port and set the update cycle for a PC running an NTP server to enable synchronization.
Daylight Saving Time	Enable DST as required. Select this option to activate the function and set the start time and end time for daylight saving time.

3. Click **Apply**.

Maintenance

This section goes over upgrades, maintenance, backup captured packets, and system logs.

Upgrades and Maintenance

You can configure auto reboot timing, device restore, reset to default settings, backup the configuration file, and upgrade the system version. Follow the steps in this section to learn how to perform these functions.

Requirements

Maintain the following requirements to ensure an operational system:

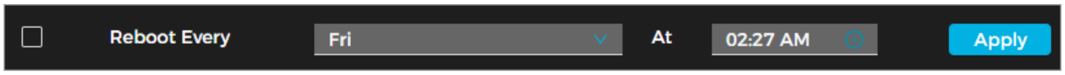
- Regularly check surveillance images.
- Remove unused user and user group information.
- Change the password every three months.
- Review and analyze system logs to address abnormalities promptly.
- Back up the system configuration periodically.
- Restart the device and delete old files regularly.

- Keep the firmware updated.

Auto-Reboot

Follow the steps below to configure auto-reboot.

1. Navigate to **Settings → System → Maintenance → Upgrade and Maintenance**.



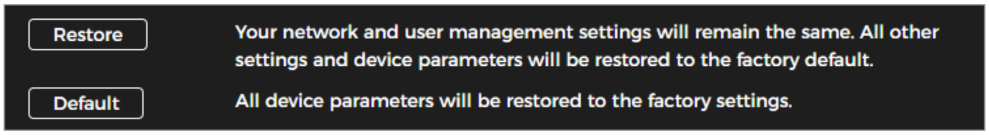
Auto-Reboot

2. Click ■ next to **Reboot Every**.
3. Set the reboot time.
4. Click **Apply**.

Restore and Default

Follow the steps below to restore the device to the default settings.

1. Navigate to **Settings → System → Maintenance → Upgrade and Maintenance**.
2. Select Restore or Default.


Restore — Your network and user management settings will remain the same. All other settings and device parameters will be restored to the factory default.

Default — All device parameters will be restored to the factory settings.

Restore and Default

Import and Export

You can export the system configuration to save as a backup. You can also import a system configuration file for quick configuration or system recovery.

⚠ Important an incompatible configuration file may result in device damage.

Follow the steps below to import or export a configuration file.

1. Navigate to **Settings → System → Maintenance → Upgrade and Maintenance**.
2. Import or export the configuration file.

- **To import a fil**e: Click **Browse**. Select the local configuration file. Click **Upload**.
- **To export a file**: Click Export.

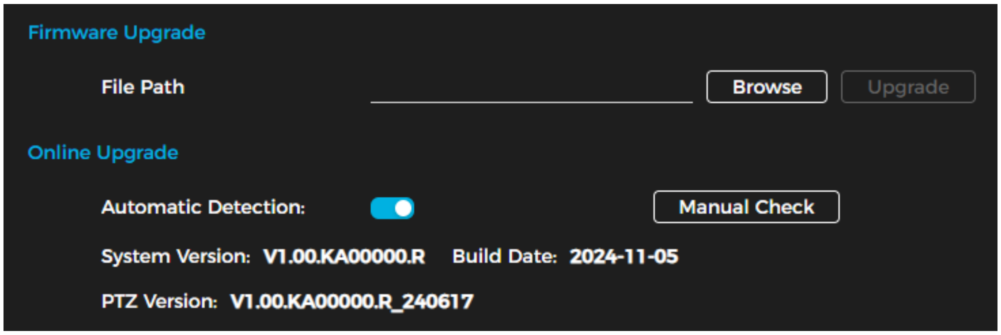
Upgrade the System

Upgrading the camera system ensures proper functionality and stability. Follow the steps below to upgrade the camera's system.

⚠ Using the wrong upgrade file may result in certain functions not working. Restart the device of the wrong file has been used.

1. Navigate to **Settings → System → Maintenance → Upgrade and Maintenance**.
2. Choose to update the system using a **Firmware Upgrade** or an **Online Upgrade**.

- **Firmware Upgrade**: Click **Browse**. Upload the upgrade file. Ensure the file is a .bin file.
- **Online Upgrade**: Click ○ next to **Automatic Detection** to allow the system to automatically check for updates. Click **Manual Check**. If there is a system upgrade available, click **Upgrade**.



Firmware Upgrade

File Path

Online Upgrade

Automatic Detection:

System Version: V1.00.KA00000.R Build Date: 2024-11-05

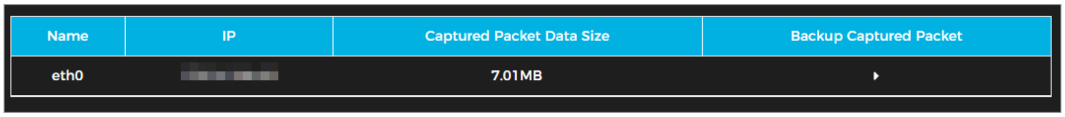
PTZ Version: V1.00.KA00000.R_240617

System Upgrade

Backup Packet Capture

You can retrieve network interaction data between the camera and a specified network card on the client and store it on your computer. Follow the steps below to set up backup packet capture.

1. Navigate to **Settings → System → Maintenance → Backup Packet Capture**.



Name	IP	Captured Packet Data Size	Backup Captured Packet
eth0	[redacted]	7.01MB	▶

Backup Packet Capture

2. Click ▶ to begin capturing. You can see the size of the packet under **Captured Packet Data Size**.
3. Click ⏸ to end capturing. The file will be saved on your local device.

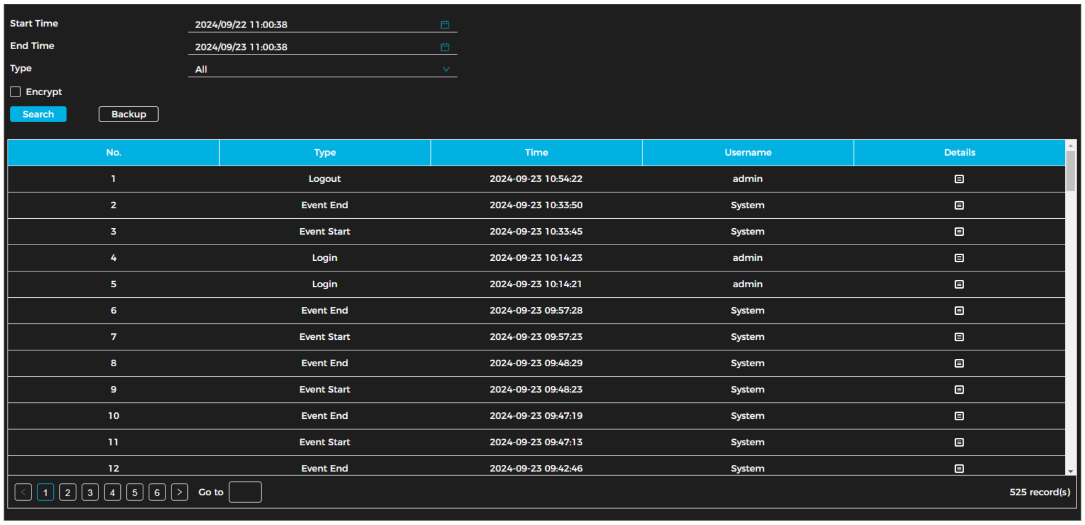
View and Back Up System Logs

Follow the steps below to view and back up system logs.

1. Navigate to **Settings → Maintenance → System Logs**.
2. Set the Start Time and End Time.
3. Select the log type. The log types include All, System, Config, Storage, Alarm Event, Record, User Management, Security, PTZ Operation and Clear Log. See the table below for more details.

Log Type	Information Included
System	Program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
Config	Saving configuration and deleting configuration file
Storage	Configuring disk type, clearing data, hot swap, FTP state, and record mode.
Alarm Event	Events such as video detection, smart plan, alarm and abnormality. Includes event start and event end.
Record	File access, file access error, and file search
User Management	Login, logout, adding user, deleting user, editing user, adding group, deleting group, and editing group.
Security	Password resetting and IP filter.

4. Click **Search**.
5. Click ☰ or a specific log to view detailed information. Click **Backup** to save all found logs to the local device.



Start Time 2024/09/22 11:00:38

End Time 2024/09/23 11:00:38

Type All

□ Encrypt

No.	Type	Time	Username	Details
1	Logout	2024-09-23 10:54:22	admin	▤
2	Event End	2024-09-23 10:33:50	System	▤
3	Event Start	2024-09-23 10:33:45	System	▤
4	Login	2024-09-23 10:14:23	admin	▤
5	Login	2024-09-23 10:14:21	admin	▤
6	Event End	2024-09-23 09:57:28	System	▤
7	Event Start	2024-09-23 09:57:23	System	▤
8	Event End	2024-09-23 09:48:29	System	▤
9	Event Start	2024-09-23 09:48:23	System	▤
10	Event End	2024-09-23 09:47:19	System	▤
11	Event Start	2024-09-23 09:47:13	System	▤
12	Event End	2024-09-23 09:42:46	System	▤

525 record(s)

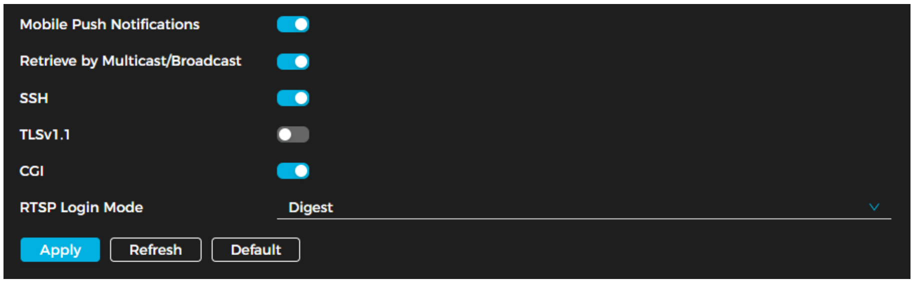
System Logs

Security

System Service

Follow the steps below to set up IP hosts (devices with specific IP addresses) that are permitted to access the device. Only hosts listed in the trusted sites can log in to the webpage, enhancing network and data security.

1. Navigate to **Settings → System → Security → System Service**.



Mobile Push Notifications: on

Retrieve by Multicast/Broadcast: on

SSH: on

TLSv1.1: off

CGI: on

RTSP Login Mode: Digest

System Service Parameters

2. Enable the system service as required. See the table below for more information.

Parameter	Description
Mobile Push Notification	Enable this function to automatically send snapshots to your phone when an alarm is triggered. This feature is enabled by default.
Retrieve by Multicast/Broadcast	Enable this function to allow multiple users to simultaneously view the device's video feed over the network using the multicast/broadcast protocol.
SSH	Enable SSH authentication to enhance security management.
TLSv1.1	Enable this function to encrypt transmitted data over standard protocols. ⓘ • Ensure that compatible devices or software support video decryption. • It is recommended to enable this function to reduce the risk of data leakage.
CGI	Enable this function to back up the online log.
RTSP Login Mode	Supports compatibility with the legacy platform login mode. Digest mode is used by default.

3. Click **Apply**.

Unauthorized Access

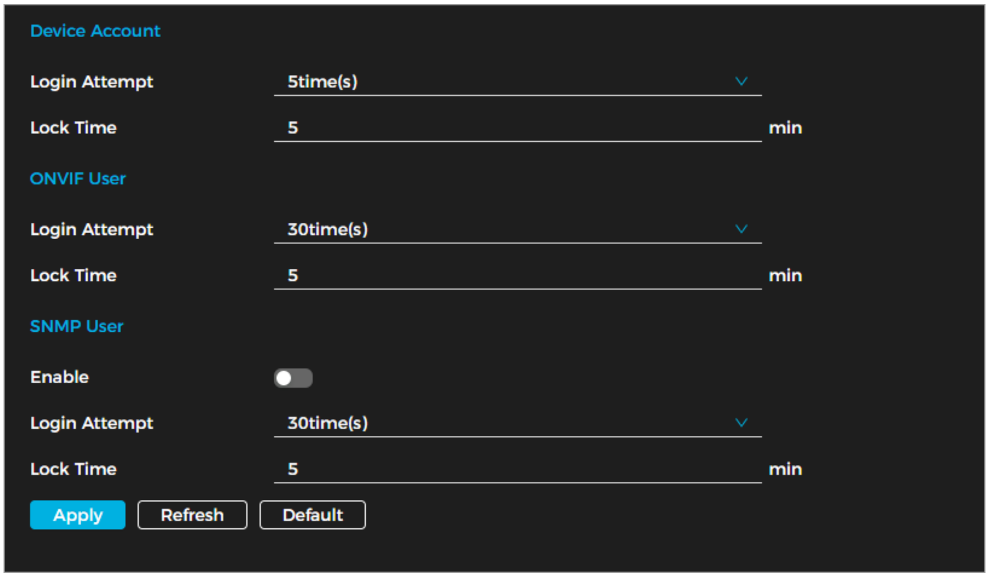
You can set the maximum number of unsuccessful login attempts before an account is locked to prevent unauthorized access. Follow the steps below to configure this setting.

1. Navigate to **Settings → System → Security → Unauthorized Access**.
2. Configure the login attempt limit and lock time for device accounts, ONVIF users, and SNMP users.

ⓘ

- **Login Attempt**: The number of times a user can input the incorrect credentials before the account is locked
- **Lock Time**: The amount of time a user cannot login in after the maximum number of login attempts is reached.

3. Click **Apply**.



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

ONVIF User

Login Attempt: 30time(s)

Lock Time: 5 min

SNMP User

Enable: ○

Login Attempt: 30time(s)

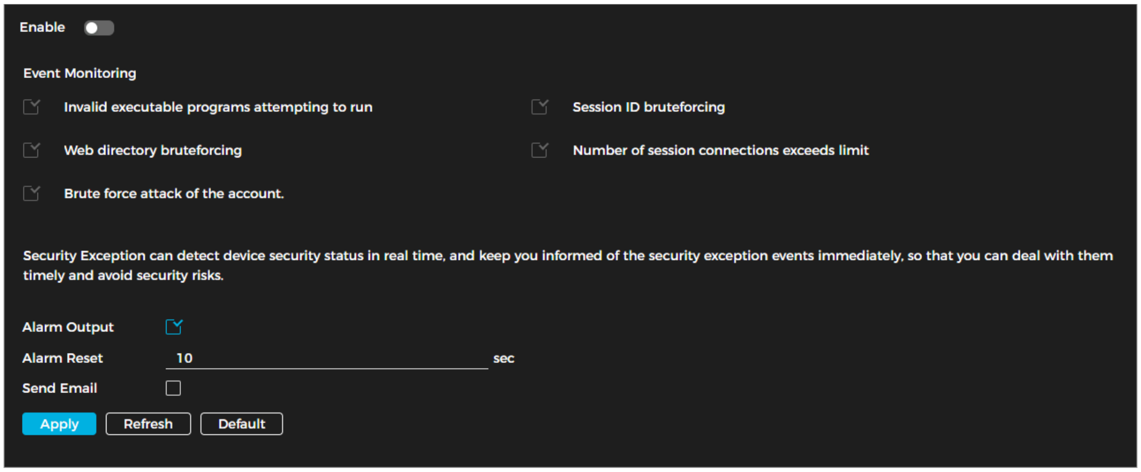
Lock Time: 5 min

Unauthorized Access Parameters

Security Exception

When a security exception occurs, such as an event is detected, the camera sends a warning reminder to avoid security risks. To set up security exception parameters, do the following:

1. Navigate to **Settings → System → Security Exception**.
2. Click ○ next to **Enable** to allow security exceptions.
3. Set the parameters and alarm linkage actions.
4. Click **Apply**.



Enable

Event Monitoring

☑ Invalid executable programs attempting to run ☑ Session ID bruteforcing

☑ Web directory bruteforcing ☑ Number of session connections exceeds limit

☑ Brute force attack of the account.

Security Exception can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

Alarm Output ☑

Alarm Reset 10 sec

Send Email □

Apply Refresh Default

Security Exception Prompt

User Management

Manage users by adding, deleting, or editing them. Users include admin, added users, ONVIF users, and online users. Only administrator users can manage users and edit permissions.

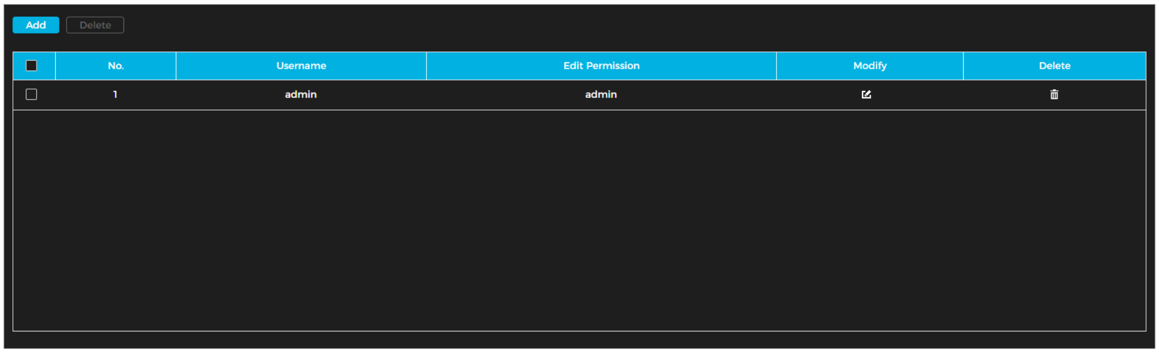
The following are user management rules and requirements:

- The maximum length for a user or group name is 31 characters, consisting of numbers, letters, underscores (_), dashes (-), dots (.), and the @ symbol.
- Passwords must be 8 to 32 non-blank characters long and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ‘ “ ; : &).
- A maximum of 18 users and 8 groups can be created.
- Users can be managed individually or through groups. Duplicate usernames or group names are not allowed. Each user can belong to only one group, and group members inherit permissions within the group’s authority range.
- Online users cannot edit their own permissions.
- One default admin user exists with the highest authority.

How to Add a User

You are an admin user by default. To add users and configure different permissions, do the following:

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

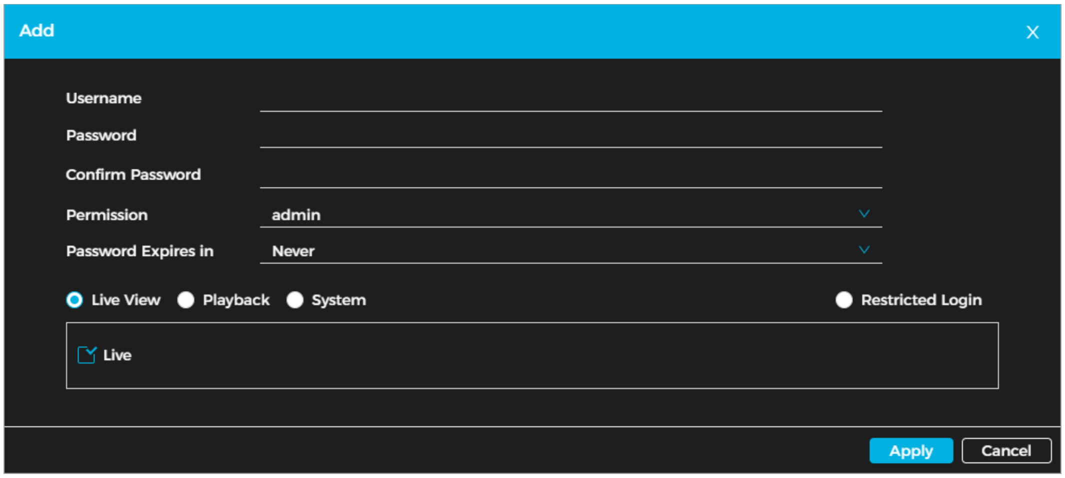


Add Delete

■	No.	Username	Edit Permission	Modify	Delete
□	1	admin	admin	✎	🗑

User Management

2. Click **Add**.



Username

Password

Confirm Password

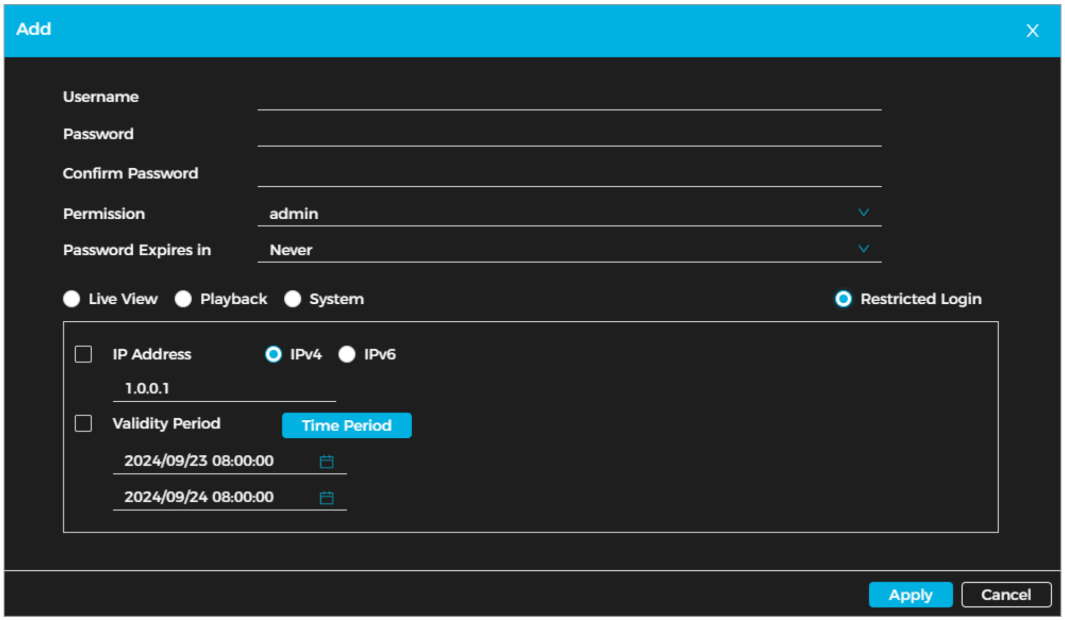
Permission: admin

Password Expires in: Never

● Live View ○ Playback ○ System ○ Restricted Login

☑ Live

Add a User (System)



Username

Password

Confirm Password

Permission: admin

Password Expires in: Never

○ Live View ○ Playback ○ System ● Restricted Login

□ IP Address ● IPv4 ○ IPv6

1.0.0.1

□ Validity Period

2024/09/23 08:00:00

2024/09/24 08:00:00

Add a User (Restricted Login)

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

Parameter	Description
Username	The user's unique ID. A username cannot be used twice.
Password	Input and confirm the user's password. Passwords must be 8 to 32 non-blank characters long and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).
Confirm Password	
Permission	Select the group the user belongs to. Each group will have different permissions.
Password Expires in	Set the automatic logout time for users. If a user remains inactive beyond the specified timeout period, the system will automatically log them out.
System	Select the user permissions as required. It is recommended to limit the number of permissions normal users have and reserve more permissions for premium or admin users.
Live View	Choose if the user has live view authority.
Playback	Choose if the user has playback authority.

Restricted Login	Configure the PC address, validity period, and time range for user login access to the camera. Users can only log in to the webpage from the specified IP address within the defined time range of the validity period. • **IP Address**: Allows login only from the specified PC IP. • **Validity Period**: Defines the time range when login is permitted. • **Time Period**: Restricts login access to a specific timeframe within the validity period. To set restricted login for the user, do the following: 1. Select the type and enter the IP address. • **IP Address**: Input the specific host IP to be added. • **IP Segment**: Enter the start and end IP addresses for a range of hosts. 2. Select the **Validity Period** and configure the start and end times. 3. Click **Time Period** to set the allowed login hours.

4. Click **Apply**.

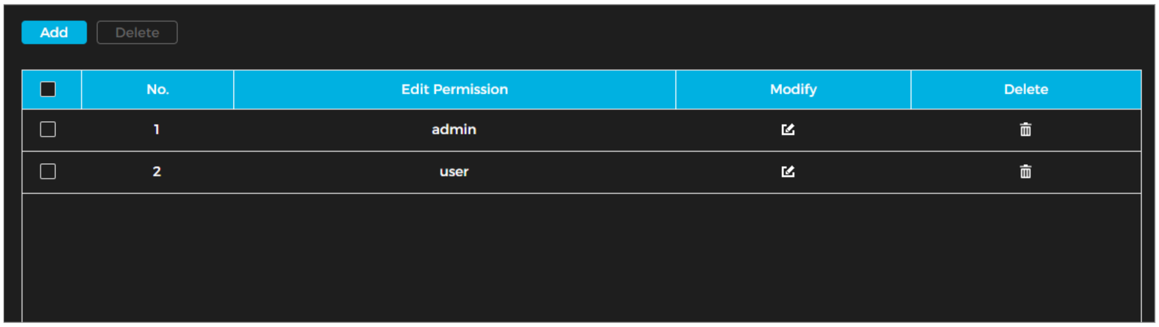
Related Operations

- Click ✎ to change a user's password, permissions, or authorities. Only admin accounts can change passwords.
- Click 🗑 to delete a user. The admin account cannot be deleted.

Editing Permissions

There are two default permission groups: admin and user. You can add a new group, delete a group that was added, or edit the authority of a group. To edit permission parameters, do the following:

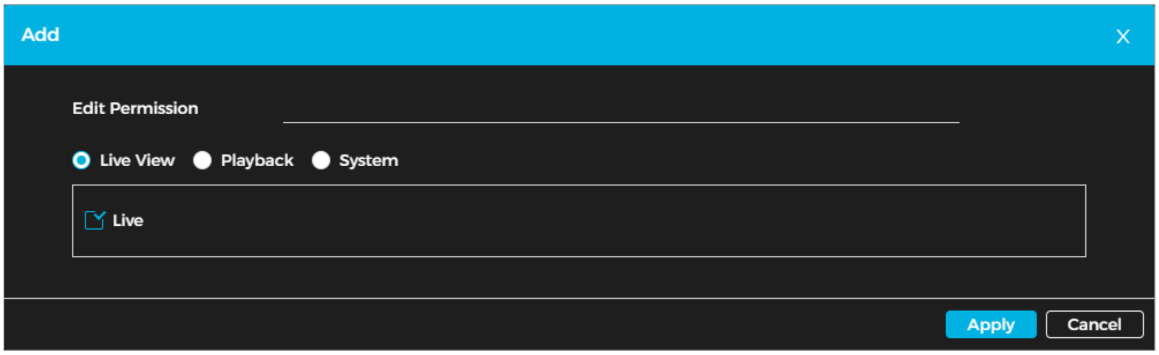
1. Navigate to **Settings → System → User Management → Edit Permission**.



■	No.	Edit Permission	Modify	Delete
□	1	admin	✎	🗑
□	2	user	✎	🗑

Permission Parameters

2. Click **Add**.



Add Permission Groups

3. Enter the name of the permission group. Select group authorities.

4. Click **Apply**. The added group is displayed in the group list.

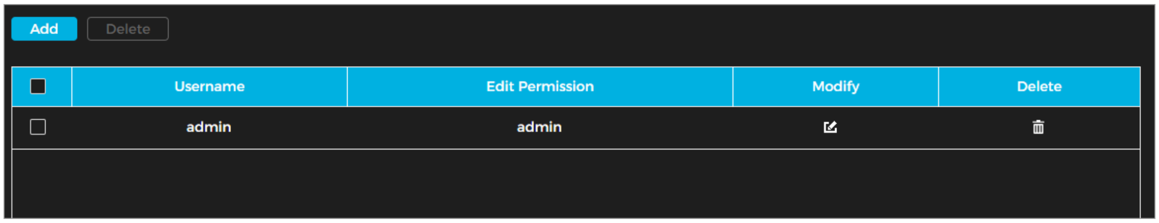
Related Operations

- Click ✎ to change a user's password, permissions, or authorities. Only admin accounts can change passwords.
- Click 🗑 to delete a user. The admin account and user group cannot be deleted.

How to Add an ONVIF User

Follow the steps below to add an ONVIF user.

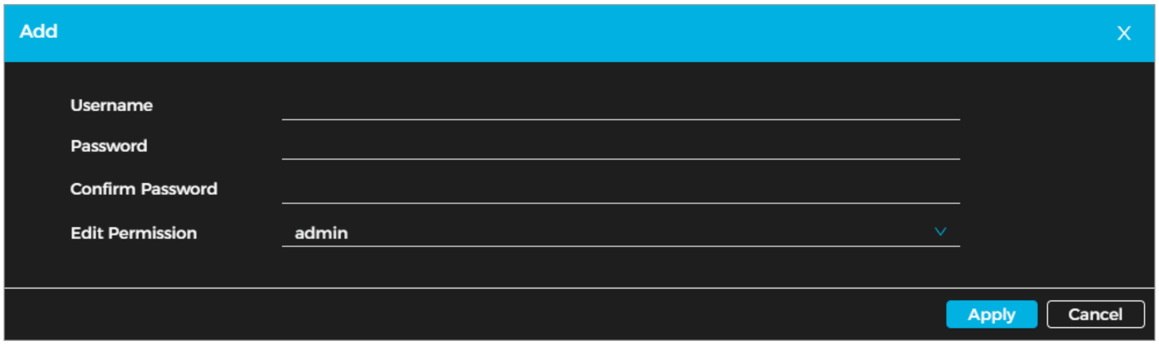
1. Navigate to **Settings → System → User Management → ONVIF User**.



☐	Username	Edit Permission	Modify	Delete
☐	admin	admin	✎	🗑

Add ONVIF User

2. Click **Add**.



Username

Password

Confirm Password

Edit Permission: admin

ONVIF User Parameters

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

Parameter	Description
Username	The user's unique ID. A username cannot be used twice.
Password	Input and confirm the user's password. Passwords must be 8 to 32 non-blank characters long and include at least two of the following: uppercase letters, lowercase letters, numbers, or special characters (excluding ' " ; : &).
Confirm Password	
Edit Permission	Select the group the user belongs to. Each group will have different permissions.

4. Click **Apply**.

Related Operations

- Click ✎ to change a user's password, permissions, or authorities. Only admin accounts can change passwords.
- Click 🗑 to delete a user. The admin account and user group cannot be deleted.

How to View Online Users

To see who has logged in to the camera, navigate to **Settings → System → User Management → Online User**.

How to Enable Password Reset

Follow the steps below to enable the password reset function.

⚠ If you do not enable the password reset function, you can only reset a user password by resetting the camera.

1. Navigate to **Settings → System → User Management → PW Reset**.
2. Click ○ next to **Enable**.
3. Enter the email address associated with the user.
4. Click **Apply**.

How to View Legal Information

To view legal information, navigate to **Settings → System → Legal Information.** View relevant information under different tabs, including the open-source software statement, software license agreement, and privacy policy.

Network Configuration

This section goes over network configuration.

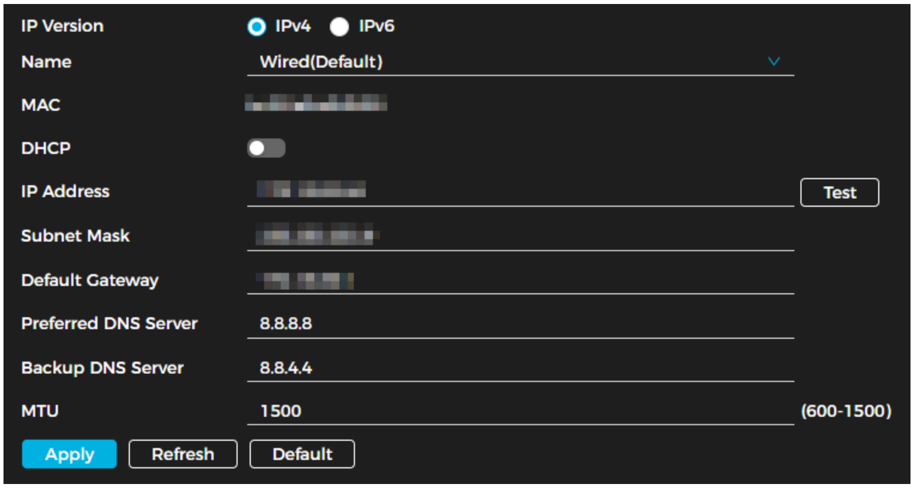
Basic Network Configuration

TCP/IP

Prior to configuring, ensure the camera is connected to the network.

Follow the steps below to configure the IP address, DNS (Domain Name System) server, and other network settings according to the network plan.

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



IP Version ● IPv4 ○ IPv6

Name: Wired(Default)

MAC: [redacted]

DHCP: ○

IP Address: [redacted] Test

Subnet Mask: [redacted]

Default Gateway: [redacted]

Preferred DNS Server: 8.8.8.8

Backup DNS Server: 8.8.4.4

MTU: 1500 (600-1500)

Apply Refresh Default

TCP/IP Parameters

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

Parameter	Description
IP Version	Choose IPv4 or IPv6.
Name	Select the Ethernet card to configure. The default option is **Wired**.
MAC	Shows host MAC address.
DHCP	Click ○ to enable DHCP. If a DHCP server is available on the network, selecting DHCP allows the camera to automatically obtain an IP address

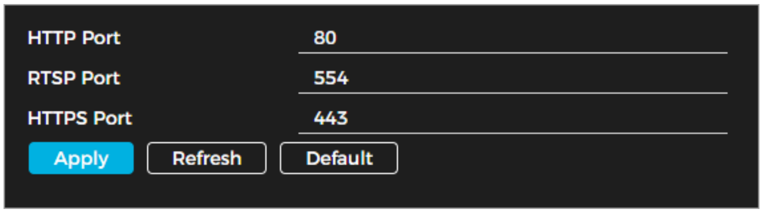
IP Address	When selecting Static in Mode, manually enter the required IP address and subnet mask. ⓘ • IPv6 does not use a subnet mask. • The default gateway must be on the same network segment as the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS Server	Preferred DNS's IP address.
Backup DNS Server	Alternate DNS's IP address.

3. Click **Apply**.

Port

Follow the steps below to set the port numbers and define the maximum number of users (including web, platform clients, and mobile app clients) that can connect to the device simultaneously.

1. Navigate **Settings → Network → Basic → Port**.



HTTP Port 80

RTSP Port 554

HTTPS Port 443

Port Parameters

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

ⓘ

- The following ports are reserved for specific uses: 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, and 42323.
- Ensure that no other port is assigned the same value during port configuration.

Parameter	Description
HTTP Port	Hypertext Transfer Protocol (**HTTP**) port. The default value is **80**.
RTSP Port	• Real-Time Streaming Protocol (RTSP) port with a default value of 554. If streaming live view via QuickTime, VLC, or a BlackBerry smartphone, use the following RTSP URL format: rtsp://ip:port/video/livemedia?Ch=1&Streamtype=0 . • When using RTSP, specify the channel number and bit stream type in the URL, along with username and password if required. • On a BlackBerry smartphone, disable audio, set codec mode to H.264B, and set the resolution to CIF before playing the stream. **Parameters** • **IP**: The device IP address (e.g., 192.168.1.101). • **Port**: Leave blank if using the default value (554). • **Ch**: The channel number (starting from 1). If using channel 2, set Ch=2. • **StreamType**: The bit stream type: 0 for the main stream (streamtype=0) and 1 for the sub stream (streamtype=1). **Example**

	- For sub stream on channel 2, the RTSP URL would be: rtsp://192.168.1.101:554/video/livemedia?Ch=2&Streamtype=1
HTTPS Port	HTTPS communication port. The default port is **443**.

3. Click **Apply**.

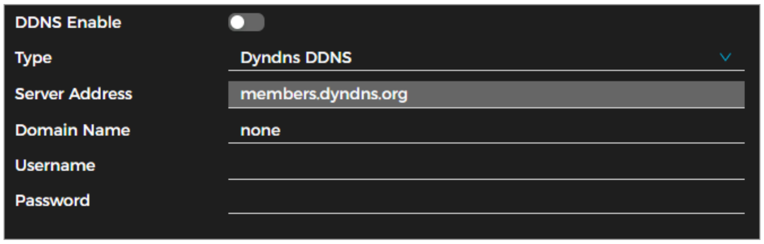
DDNS

Properly configure DDNS to ensure that the domain name on the DNS server continuously matches your IP address and updates in real time. This allows you to access the camera using the same domain name, even if the IP address changes.

Follow the steps below to configure DDNS. Prior to configuring, ensure the type of DNS server is supported by the camera.

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

2. Click ○ to enable the function.



DDNS Enable	○
Type	Dyndns DDNS
Server Address	members.dyndns.org
Domain Name	none
Username	
Password	

DDNS

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

Parameter	Description
Type	The name and web address of the DDNS service providers are as follows: - **NO-IP DDNS**: dynupdate.no-ip.com - **DynDNS DDNS**: members.dyndns.org
Server Address	
Domain Name	Domain name registered on the DDNS website.
Test	You can click Test to verify the domain name registration only when selecting the NO-IP DDNS type.
Username	Enter the username and password provided by the DDNS server provider. You must first register an account (including a username and password) on the provider's website.
Password	

4. Click **Apply**.

5. Open a browser on your PC, enter the domain name in the address bar, and press Enter to display the login page.

P2P

P2P (peer-to-peer) technology allows users to manage devices easily without the need for DDNS, port mapping, or a transit server. You can scan the device’s QR code with your smartphone to add and manage more devices on the mobile app.

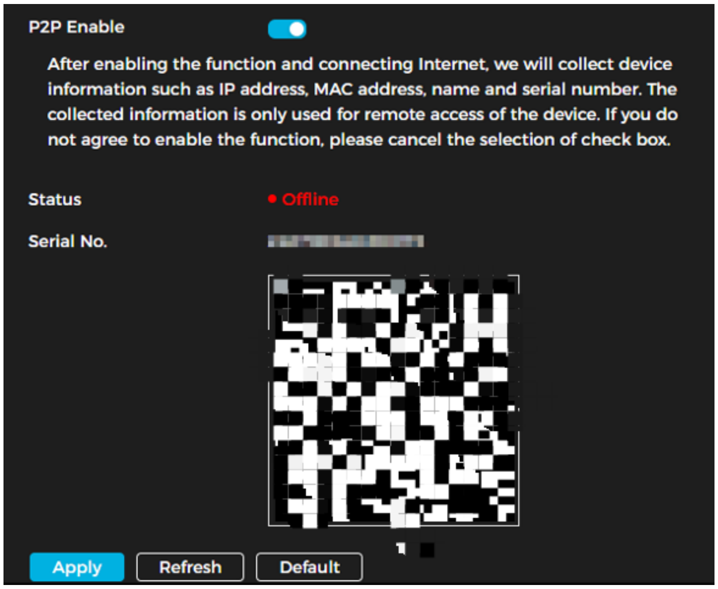
Follow the steps below to enable P2P functionality.

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

ⓘ

- Enabling P2P allows remote device management.

- When P2P is enabled and the device is connected to the network, its status appears as online. The system collects the device IP address, MAC address, name, and SN for remote access purposes only. You can disable P2P to prevent data collection.



P2P Enable: on

After enabling the function and connecting Internet, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access of the device. If you do not agree to enable the function, please cancel the selection of check box.

Status: ● Offline

Serial No.: [redacted]

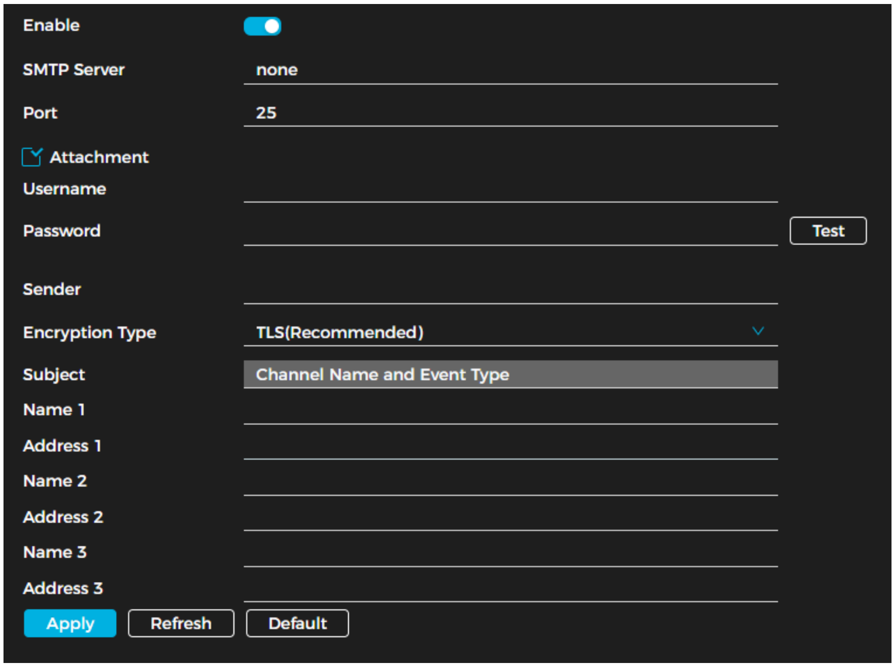
Enable P2P

2. Log in to the mobile client and tap **Device Management**.
3. Tap + in the upper-right corner.
4. Scan the QR code on the P2P page.
5. Follow the instructions to finish the setup.

Email

Follow the steps below to configure the email parameters and enable email linkage. When an alarm is triggered, the system sends an email to the specified address.

1. Navigate **Settings → Network → Basic → Email**.



Enable	on
SMTP Server	none
Port	25
☑ Attachment	
Username	
Password	
Sender	
Encryption Type	TLS(Recommended)
Subject	Channel Name and Event Type
Name 1	
Address 1	
Name 2	
Address 2	
Name 3	
Address 3	

Email Linkage

2. Click ○ to enable the function.

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

Parameter	Description
STMP Server	The server address.
Port	SMTP server port number.
Attachment	Check the box to allow for attachments to be sent with emails.
Username	SMTP server username.
Password	SMTP server password.
Sender	Sender's email address.
Encryption Type	Choose from **None**, **SSL**, and **TLS**.
Subject	Email subject line. Supports up to 63 characters in Chinese, English, and Arabic numerals. If attachments are enabled, the system will send one image to the receiving email address after an alarm is triggered by default. Up to three images can be sent. You may configure the interval (the frequency the system will send the image(s)) after an alarm is triggered.
Name and Address	You can set up to three names and email addresses to receive email alerts.

Major Mailbox Configuration

Mailbox	STMP	Authentication	Port	Description
Gmail	smtp.gmail.com	SSL	465	You must enable SMTP service.
		TLS	587	

4. Click **Apply**.

Network Access

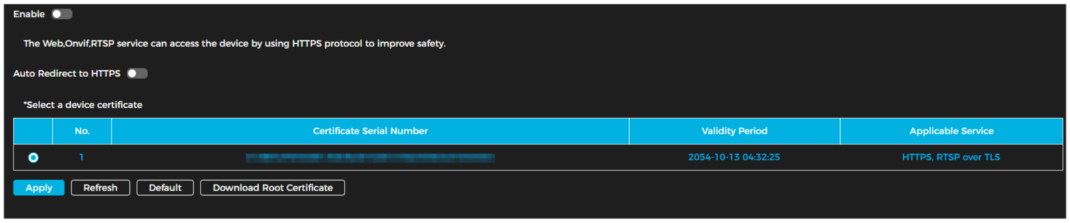
HTTPS

Follow the steps to create or upload an authenticated certificate to enable HTTPS login on your PC. HTTPS ensures page authenticity, secures accounts, and protects user communications, identity, and web browsing privacy.

1. Navigate to **Settings → Network → Network Access → HTTPS**.

2. Click ○ to enable the function.

3. Select the certificate. If no certificate is listed, click **Certificate Mana.** on the navigation bar to the right.



Enable ○

The Web,Onvif,RTSP service can access the device by using HTTPS protocol to improve safety.

Auto Redirect to HTTPS ○

*Select a device certificate

	No.	Certificate Serial Number	Validity Period	Applicable Service
●	1	[redacted]	2054-10-13 04:32:25	HTTPS, RTSP over TLS

HTTPS

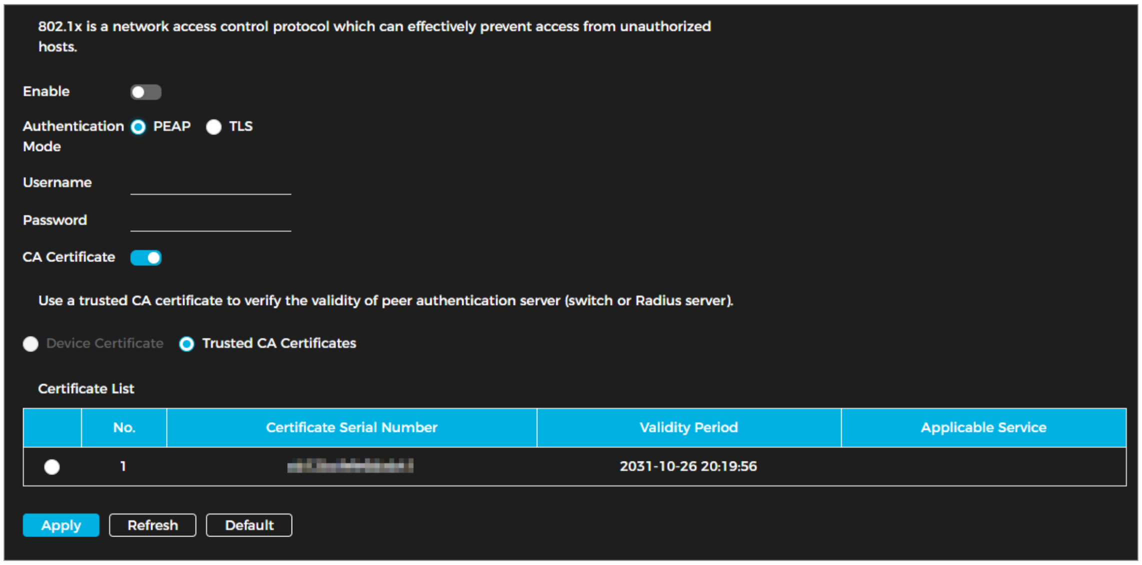
4. Click **Apply**.

802.1x

Cameras can connect to the LAN only after successfully passing 802.1x authentication. Follow the steps below to configure 802.1x authentication.

1. Navigate to **Settings → Network → Network Access → 802.1x**.
2. Click to enable the function.
3. Choose the authentication mode and set the parameters.

- **Protected EAP Protocol (PEAP)**
  - Select PEAP as the authentication mode.
  - Enter the server login credentials.
  - Click next to the CA certificate.
  - Select the trusted CA certificate from the list. If no certificate is listed, click **Certificate Mana.** on the navigation bar to the right.



802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

Enable

Authentication Mode [✓ PEAP] TLS

Username

Password

CA Certificate

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

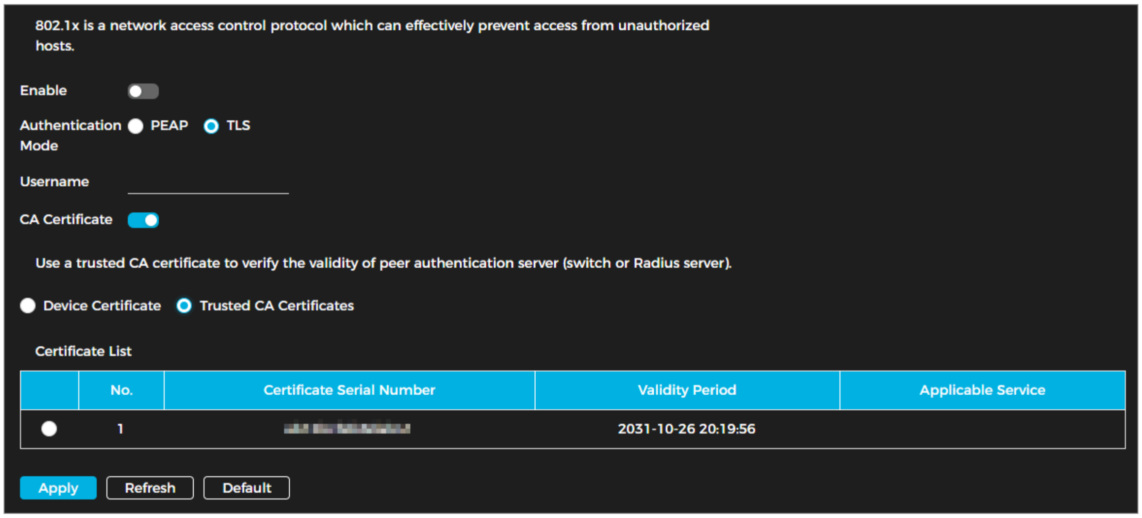
Device Certificate [✓ Trusted CA Certificates]

Certificate List

	No.	Certificate Serial Number	Validity Period	Applicable Service
○	1	[redacted]	2031-10-26 20:19:56	

802.1x (PEAP)

- **Transport Layer Security (TLS)**
  - Select TLS as the authentication mode.
  - Enter the username.
  - Click next to the CA certificate.
  - Select the trusted CA certificate from the list. If no certificate is listed, click **Certificate Mana.** on the navigation bar to the right.



802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

Enable

Authentication Mode PEAP [✓ TLS]

Username

CA Certificate

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

Device Certificate [✓ Trusted CA Certificates]

Certificate List

	No.	Certificate Serial Number	Validity Period	Applicable Service
○	1	[redacted]	2031-10-26 20:19:56	

802.1x (TLS)

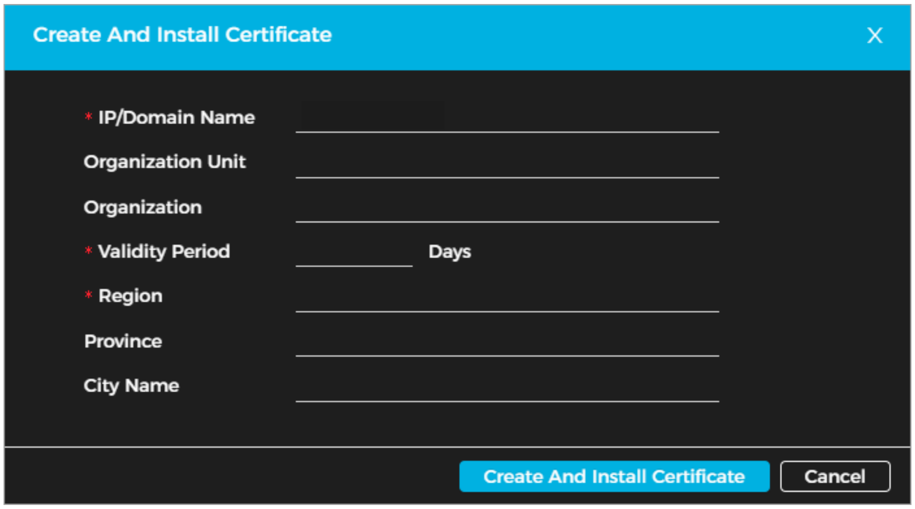
4. Click **Apply**.

Certificate Mana.

How to Install a Device Certificate

Follow the instructions to create a certificate to enable login via HTTPS on your PC.

1. Navigate to **Settings → Network → Network Access → Certificate Mana**.
2. Select Device Certificate.
3. Click Install Device Certificate.
4. Input the certificate information.
5. Click **Create and install certificate**. To view the certificate after it's been created, go to **Device Certificate**.



Create And Install Certificate

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days

* Region

Province

City Name

Create and Install a Device Certificate

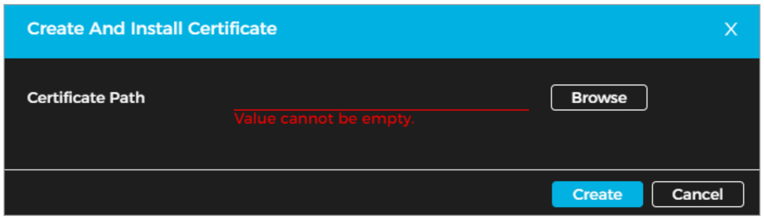
6. (Optional) Click ⭳ to download the certificate and 🗑 to delete it.

How to Install a Trusted CA Certificate

A CA certificate is a digital certificate that verifies the legal identity of the camera. For example, when the camera connects to a LAN via 802.1X authentication, a CA certificate is required.

Follow the steps below to install a trusted CA certificate.

1. Navigate to **Settings → Network → Network Access → Certificate Mana**.
2. Select Trusted CA Certificates.
3. Click Installing Trusted Certificate.
4. Click **Browse** to choose the certificate.



Create And Install Certificate

Certificate Path

Value cannot be empty.

Install Trusted Certificate

5. Click **Create**. To view the certificate, go to **Trusted CA Certificate**.

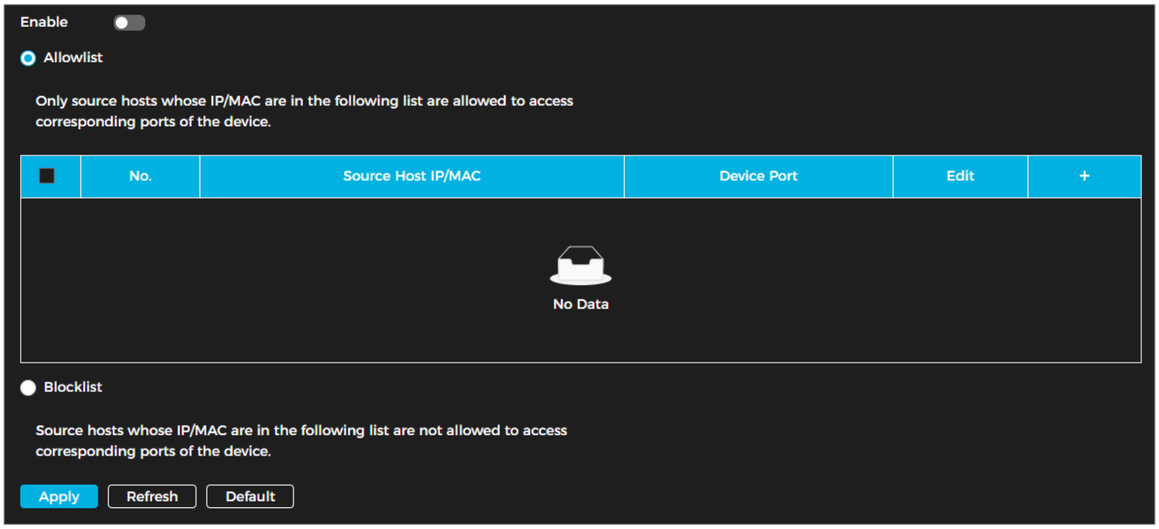
6. (Optional) Click ⬇ to download the certificate and 🗑 to delete it.

Advanced Network Configurations

Firewall

Follow the instructions to configure the firewall to limit access to the camera.

1. Navigate to **Settings → Network → Advanced → Firewall**.
2. Click ○ to enable the function.



Enable ○

● Allowlist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

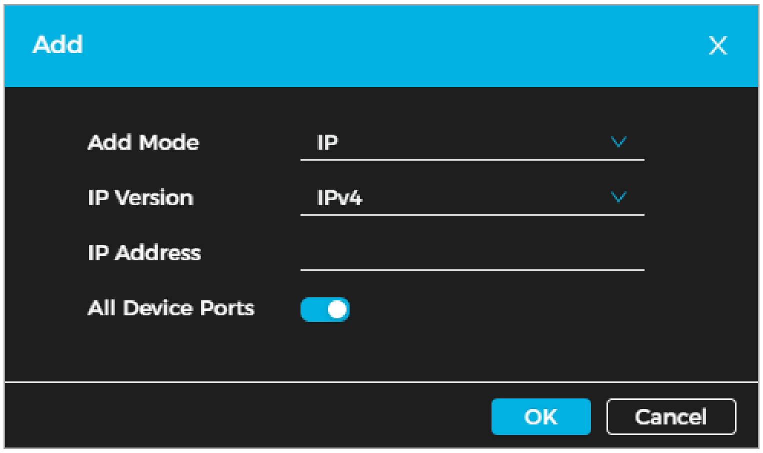
■	No.	Source Host IP/MAC	Device Port	Edit	+
		No Data			

○ Blocklist

Source hosts whose IP/MAC are in the following list are not allowed to access corresponding ports of the device.

Firewall

3. Choose a firewall mode: Allowlist (only hosts listed can access the device) or Blocklist (restricts hosts listed from accessing the device).
4. Click + to add the host IP/MAC address to the Allowlist or Blocklist.
5. Click **OK**.



Add

Add Mode: IP

IP Version: IPv4

IP Address:

All Device Ports: ●

Add a Host IP/MAC Address to the Firewall

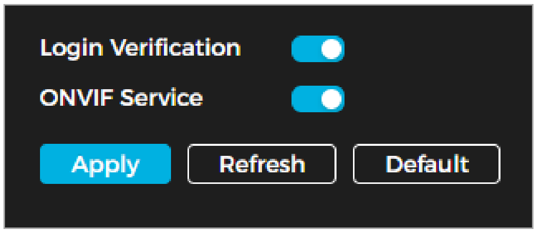
6. Click **Apply**.
7. (Optional) Click ✎ to edit host information and 🗑 to delete the host.

ONVIF

The ONVIF service is enabled by default, allowing network video products—including video recording devices and other recording equipment—from different manufacturers to connect to your device.

Follow the steps below to enable ONVIF manually.

1. Navigate to **Settings → Network → Advanced → ONVIF**.
2. Click ○ next to Login Verification and ONVIF Service.
3. Click **Apply**.



Login Verification: on

ONVIF Service: on

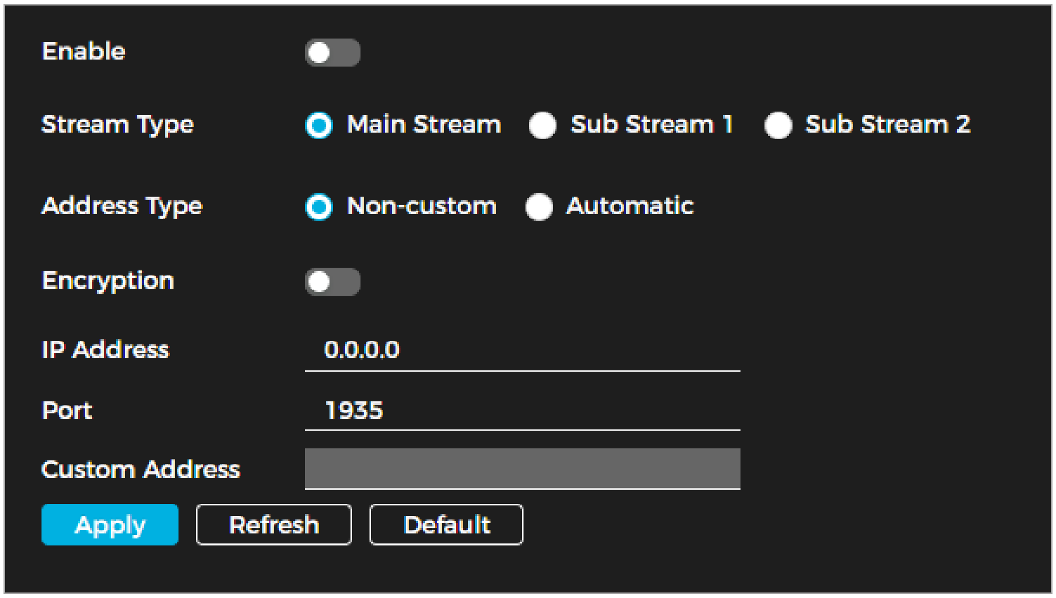
ONVIF Service

RTMP

Using RTMP, you can stream live video to third-party platforms such as Ali and YouTube. RTMP supports H.264, H.264 B, H.264H video formats and AAC audio format. Only the admin can configure RTMP settings.

Follow the steps below to configure RTMP settings.

1. Navigate to **Settings → Network → Advanced → RTMP**.



Enable: off

Stream Type: ◉ Main Stream ○ Sub Stream 1 ○ Sub Stream 2

Address Type: ◉ Non-custom ○ Automatic

Encryption: off

IP Address: 0.0.0.0

Port: 1935

Custom Address:

RTMP Parameters

2. Click ○ to enable the function.

⚠ Only enable RTMP with trusted IP addresses.

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

Parameter	Description
Stream Type	The stream used for live view must be in H.264, H.264 B, or H.264H video format and AAC audio format.
Address Type	There are two types of addresses: • **Non-Custom**: Input the server's IP address and domain name. • **Automatic**: Input the path given by the server.

Encryption	Click ○ when using a non-custom address.
IP Address	When using a non-custom address, enter the server IP address (IPv4 or domain name) and port (use default value).
Port	
Custom Address	Enter the path given by the server when selecting **Automatic**.

4. Click **Apply**.

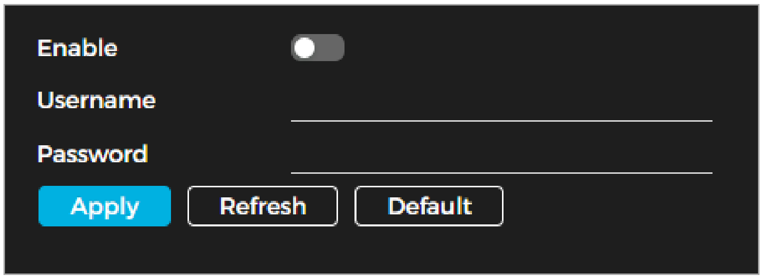
PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol used by the device to connect to the internet.

Prior to configuring PPPoE settings, you must obtain the PPPoE username and password from your Internet Service Provider (ISP) and configure the network connection using PPPoE. The camera will then acquire a dynamic WAN IP address.

Once the prerequisite information has been obtained, follow the steps below to enable PPPoE.

1. Navigate to **Settings → Network → Advanced → PPPoE Settings**.
2. Click ○.
3. Enter the login credentials.
4. Click **Apply**. Upon successful connection, a prompt box appears, displaying the real-time WAN IP address. You can now access the camera using this IP address.



PPPoE Settings

ⓘ

- Disable UPnP when using PPPoE to prevent potential conflict.
- Once PPPoE is connected, the device IP address cannot be modified through the web interface.

UPnP

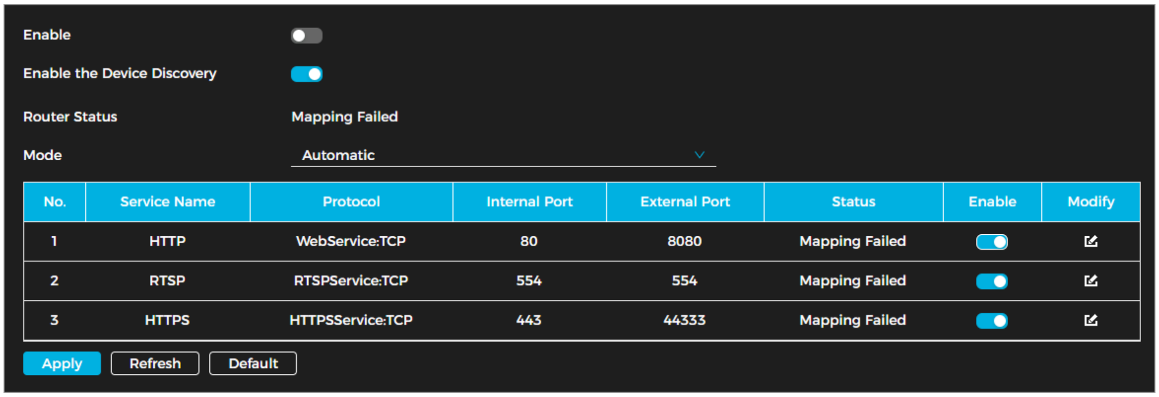
UPnP (Universal Plug and Play) is a protocol that creates a mapping between local area networks (LAN) and wide area networks (WAN). This function allows access to local devices using a wide area IP address.

Prior to enabling UPnP, ensure the following prerequisites are met:

- Ensure that the UPnP service is installed on the system.
- Log in to the router and configure the WAN IP address for internet access.
- Enable UPnP on the router.
- Connect the device to the LAN port of the router.
- Navigate to Settings > Network > Basic > TCP/IP, then either:
- Enter the local area IP address of the router
- Select DHCP to automatically obtain an IP address

Once the prerequisites have been met, follow the steps below to enable UPnP.

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



Enable	○
Enable the Device Discovery	●
Router Status	Mapping Failed
Mode	Automatic

No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify
1	HTTP	WebService:TCP	80	8080	Mapping Failed	●	✎
2	RTSP	RTSPService:TCP	554	554	Mapping Failed	●	✎
3	HTTPS	HTTPSService:TCP	443	44333	Mapping Failed	●	✎

UPnP

2. Click ○ to enable the function.

3. Choose a mapping mode: **Automatic** or **Default**.

ⓘ

- **Automatic**: Click ✎. Change the external port as needed.
- **Default**: The system will map the unoccupied port automatically. You cannot change mapping relationships using **Default**.

4. Click **Apply**.

5. Open a web browser on your PC, enter http://[wide area IP address]:[external port number], and access the local device through the corresponding port.

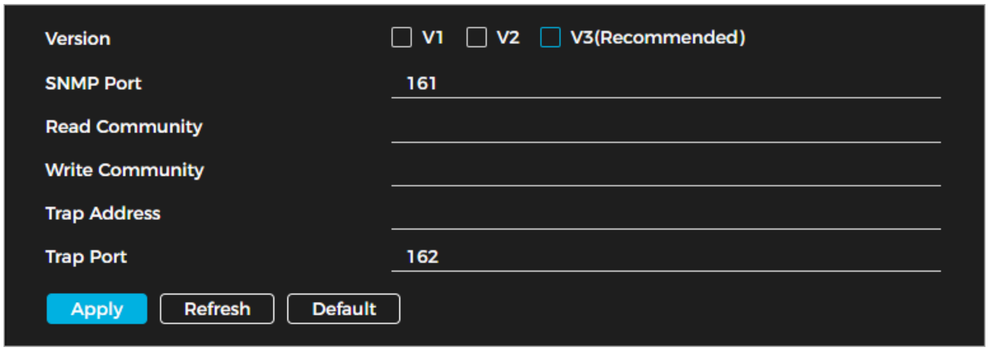
SNMP

SNMP (Simple Network Management Protocol) allows software such as MIB Builder and MG-SOFT MIB Browser to connect, manage, and monitor the camera.

Prior to enabling SNMP, ensure the following prerequisites are met:

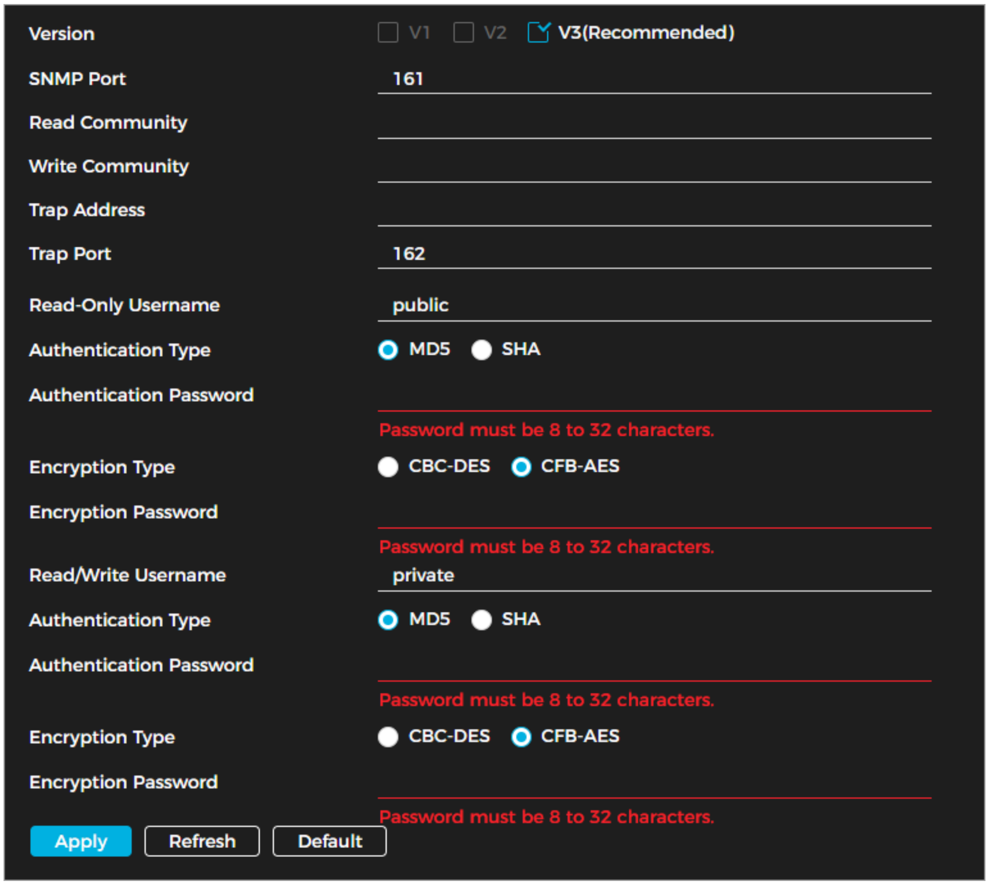
- Install SNMP monitoring and management tools such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the MIB file matching the device version from technical support.

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



Version	□ V1 □ V2 □ V3(Recommended)
SNMP Port	161
Read Community	
Write Community	
Trap Address	
Trap Port	162

SNMP Parameters (1)



Version: □ V1 □ V2 ☑ V3(Recommended)

SNMP Port: 161

Read Community:

Write Community:

Trap Address:

Trap Port: 162

Read-Only Username: public

Authentication Type: ● MD5 ○ SHA

Authentication Password:

Password must be 8 to 32 characters.

Encryption Type: ○ CBC-DES ● CFB-AES

Encryption Password:

Password must be 8 to 32 characters.

Read/Write Username: private

Authentication Type: ● MD5 ○ SHA

Authentication Password:

Password must be 8 to 32 characters.

Encryption Type: ○ CBC-DES ● CFB-AES

Encryption Password:

Password must be 8 to 32 characters.

SNMP Parameters (2)

2. Select the SNMP version.

ⓘ

- **V1**: Selecting V1 allows the system to process only SNMP V1 information.
- **V2**: Selecting V2 allows the system to process only SNMP V2 information.
- **V3**: Selecting V3 disables V1 and V2. You can configure the username, password, and authentication type. Accessing the device from the server requires the corresponding credentials and authentication settings.

⚠ V1 and V2 may cause data leakage. V3 is the recommended SNMP version.

3. In Trap Address, enter the IP address of the PC where MIB Builder and MG-SOFT MIB Browser are installed, and keep the other parameters at their default settings. See the table below for more details.

Parameter	Description
SNMP Port	Listening port of the software agent.
Read Community, Write Community	The read and write community string supported by the software agent. You can use numbers, letters, underscores (_), and dashes (-) to create the name
Trap Address	The target address where the Trap information is sent by the software agent in the device.
Trap Port	The target port used for sending Trap information from the software agent in the device.
Read-Only Username	Set the read-only username for accessing the device. It is public by default. You can use numbers, letters, and underscores (_) to create the name
Read/Write Username	Set the read/write username for accessing the device. It is private by default.

	You can use numbers, letters, and underscores (_) to create the name
Authentication Type	Choose **MD5** (default) or **SHA**.
Authentication Password	Must be between 8 and 32 characters.
Encryption Type	The default type is CBC-DES.
Encryption Password	Must be between 8 and 32 characters.

4. Click **Apply**.

How to View the Device Configuration via MIB builder or MG-SOFT MIB Browser

Once SNMP is configured, follow the steps below to view the device configuration through the MIB builder or MG-SOFT MIB Browser:

1. Open MIB Builder and MG-SOFT MIB Browser.
2. Compile the two MIB files using MIB Builder.
3. Load the generated modules into MG-SOFT MIB Browser.
4. Enter the IP address of the device to be managed in MG-SOFT MIB Browser, then select the SNMP version to search.
5. Expand all tree lists in MG-SOFT MIB Browser to view configuration details, including video channels, audio channels, and software version.

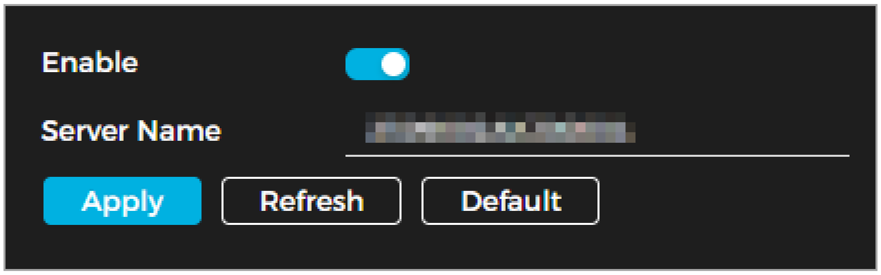
ⓘ Use a Windows PC and disable SNMP Trap service. MG-SOFT MIB Browser will display a prompt when an alarm is triggered.

Bonjour

This function allows OS and clients that support Bonjour to automatically detect the camera. You can quickly access the camera using the Safari browser. This function is enabled by default.

Follow the steps below to enable Bonjour manually.

1. Navigate to **Settings → Network → Advanced → Bonjour**.
2. Click ○ to enable the function.
3. Input the server name.
4. Click **Apply**.



Enable ●

Server Name [redacted]

Bonjour

How to Access the Camera Using Safari

Once Bonjour is enabled, follow the steps below to use Safari to access the camera:

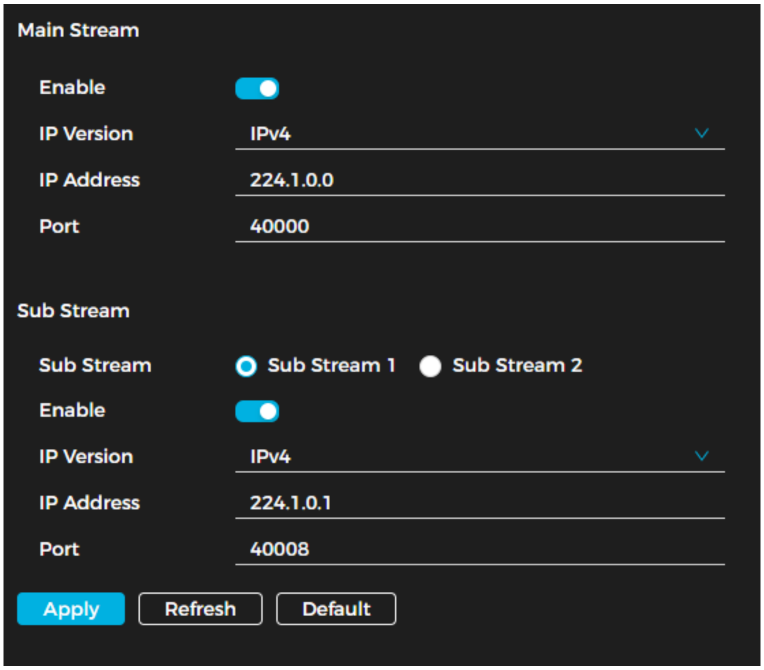
1. Open Safari.
2. Click Show All Bookmarks.
3. Enable **Bonjour**. The OS or client will automatically detect any Bonjour-enabled network cameras in the LAN.

4. Select the camera to access.

Multicast

When multiple users access the video stream over the network, playback may fail due to limited bandwidth. To resolve this, configure a multicast IP address (224.0.0.0–239.255.255.255) for the camera and enable the multicast protocol.

1. Navigate to **Settings → Network → Advanced → Multicast**.



Main Stream

Enable: on
IP Version: IPv4
IP Address: 224.1.0.0
Port: 40000

Sub Stream

Sub Stream: ● Sub Stream 1 ○ Sub Stream 2
Enable: on
IP Version: IPv4
IP Address: 224.1.0.1
Port: 40008

2. Click ◯ to enable the function.
3. Enter the IP address and port number.

Parameter	Description
IP Version	Choose between IPv4 and IPv6.
Multicast Address	The default multicast IP address for the Main Stream and Sub Stream is 224.1.2.4, with a valid range of 224.0.0.0–239.255.255.255.
Port	The multicast port range is 1025–65500. For single-channel devices, the default multicast ports are: • Main Stream: 40000 • Sub Stream 1: 40008 • Sub Stream 2: 40016

4. Click **Apply.**

Click Live View on the main page to monitor the video stream using multicast mode on the Live View page.

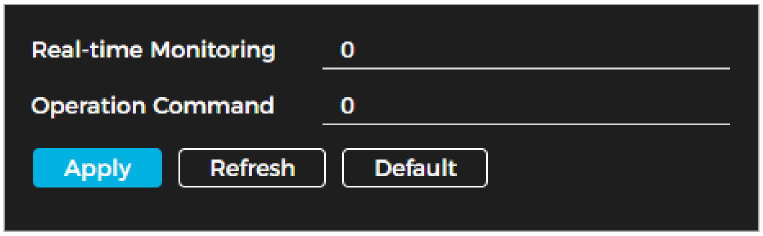
QoS

This function helps address issues like network delay and congestion by optimizing bandwidth allocation, reducing transmission delays, minimizing packet loss, and stabilizing delay jitter for a better experience.

The priority range is 0–63, where 0 represents the lowest priority and 63 the highest.

Follow the steps below to enable QoS.

1. Navigate to **Settings → Network → Advanced → QoS**.


Real-time Monitoring: 0

Operation Command: 0

QoS Parameters

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

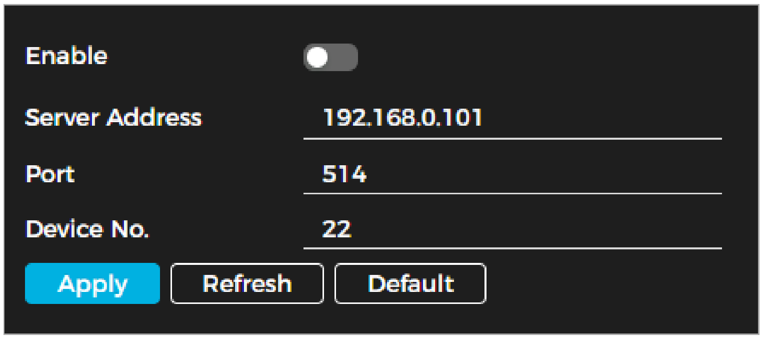
Parameter	Description
Real-Time Monitor	Set the priority level for data packets used in network surveillance. The priority range is 0–63, with 0 being the lowest and 63 the highest.
Operation Command	Set the priority level for data packets used for configuration and status checks.

3. Click **Apply**.

Remote Log Records

Follow the steps below to receive logs when accessing a set address.

1. Navigate **Settings → Network → Advanced → Remote Log Records**.
2. Click ○ to enable the function.
3. Set the address, port, and device number.
4. Click **Apply**.


Enable ○

Server Address: 192.168.0.101

Port: 514

Device No.: 22

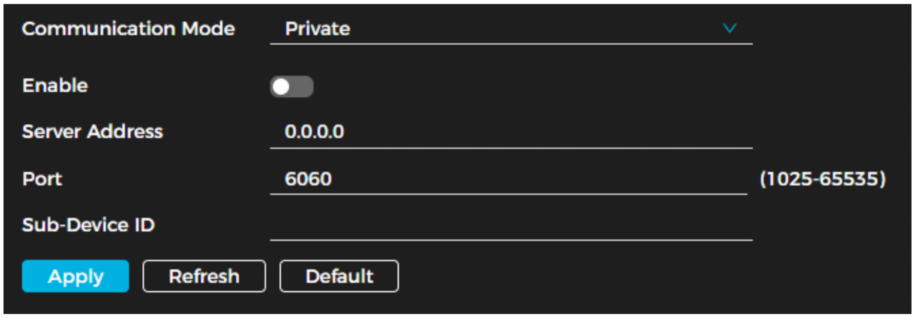
Remote Log Parameters

Auto-Registration

When this function is enabled, the camera reports its current location to a specified server upon connecting to the Internet. The server acts as a transit point, making it easier for client software to access the camera.

Follow the steps below to configure auto-registration.

1. Navigate to **Settings → Network → Auto Registration**.
2. Choose the communication mode: **Private** or **CGI**.



Communication Mode: Private

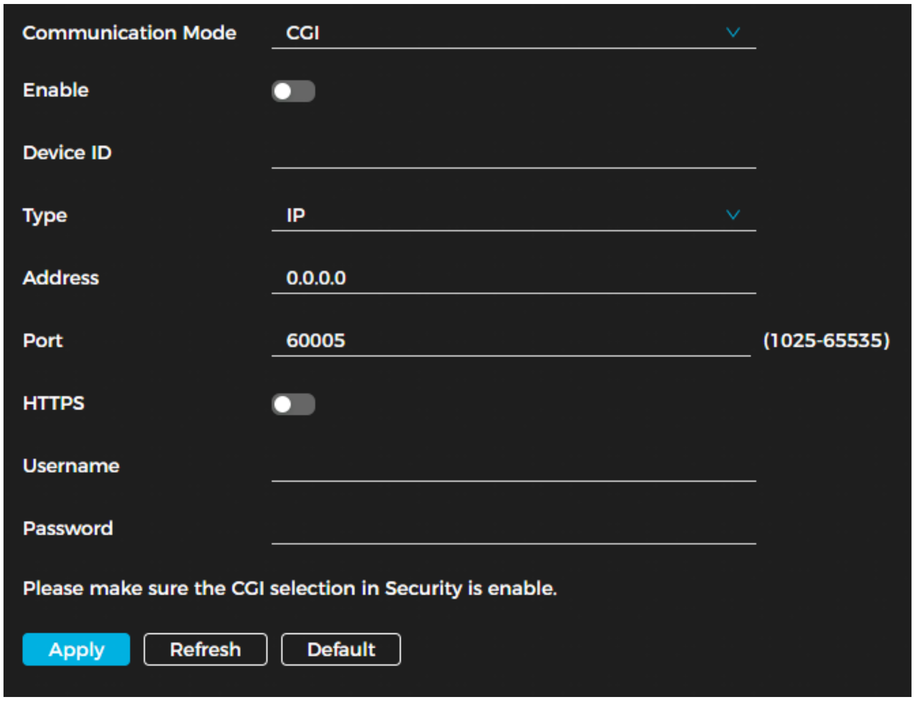
Enable: ○

Server Address: 0.0.0.0

Port: 6060 (1025-65535)

Sub-Device ID:

Auto-Registration (Private)



Communication Mode: CGI

Enable: ○

Device ID:

Type: IP

Address: 0.0.0.0

Port: 60005 (1025-65535)

HTTPS: ○

Username:

Password:

Please make sure the CGI selection in Security is enable.

Auto-Registration (CGI)

3. Click ○ to enable the function.
4. Set the parameters. See the table below for more details.

Parameter	Description
Server Address	IP address or domain name of server.
Address	
Domain Name	
Port	Registration port.
Sub-Device ID	Camera’s custom ID.
Device ID	
Type	Select from **IP** or **Domain**.
Port	Enter a number between 1025 and 65535.
HTTPS	Access the third-party platform via HTTPS. HTTPS provides secure communication over the network.
Username/Password	Device username and password.

5. Click **Apply**.

Video and Audio

This section goes over how to set the video and audio parameters on the camera.

ⓘ Parameters may vary based on device.

How to Set Video Parameters

This section covers video parameters, including video stream and region of interest settings.

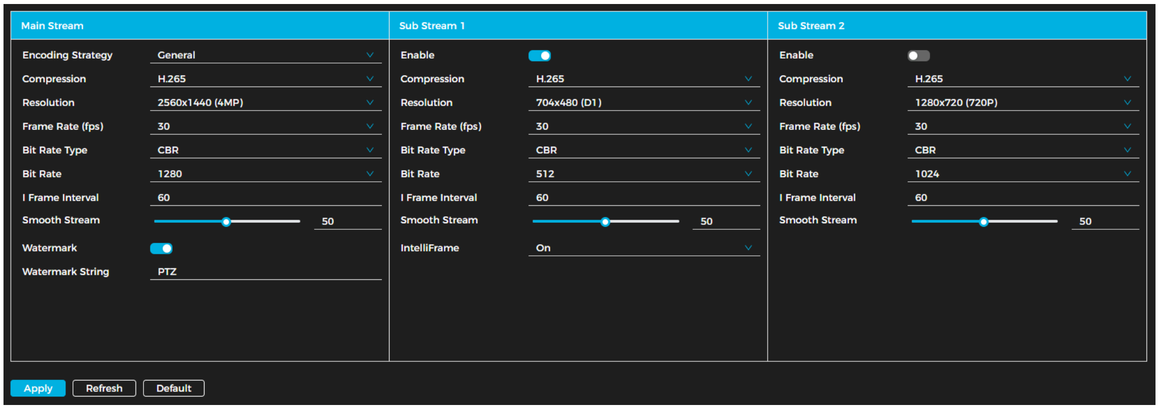
ⓘ

- Click **Default** to restore the device to its default configuration.
- Click **Refresh** to display the latest configuration.

Video Stream

Follow the steps below to configure video stream parameters.

1. Navigate to **Settings → Video/Audio → Video → Video Stream**.



Main Stream

- Encoding Strategy: General
- Compression: H.265
- Resolution: 2560x1440 (4MP)
- Frame Rate (fps): 30
- Bit Rate Type: CBR
- Bit Rate: 1280
- I Frame Interval: 60
- Smooth Stream: 50
- Watermark: ●
- Watermark String: PTZ

Sub Stream 1

- Enable: ●
- Compression: H.265
- Resolution: 704x480 (D1)
- Frame Rate (fps): 30
- Bit Rate Type: CBR
- Bit Rate: 512
- I Frame Interval: 60
- Smooth Stream: 50
- IntelliFrame: On

Sub Stream 2

- Enable: ○
- Compression: H.265
- Resolution: 1280x720 (720P)
- Frame Rate (fps): 30
- Bit Rate Type: CBR
- Bit Rate: 1024
- I Frame Interval: 60
- Smooth Stream: 50

Video Stream Parameters

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

Parameter	Description
Sub Stream	Click ○ to enable the substream. Substreams are enabled by default. You can enable multiple substreams simultaneously.
Encoding Strategy	Choose between **General, Smart Encoding,** or **AI Codec**.
Compression	• **H.264**: Main profile encoding mode. Requires less bandwidth compared to H.264B. • **H.265**: Main profile encoding mode. Requires less bandwidth compared to H.264H.
Resolution	The video resolution determines image clarity. Higher resolution provides a clearer image but requires more bandwidth.
Frame Rate (FPS)	The frame rate refers to the number of frames per second in a video. A higher frame rate results in a smoother and clearer video
Bit Rate Type	The bit rate control type determines how video data is transmitted. Choose from the following options: • **CBR (Constant Bit Rate)**: The bit rate remains stable and stays close to the defined value. • **VBR (Variable Bit Rate)**: The bit rate adjusts based on changes in the monitoring scene.

	When Encoding Strategy is set to AI Codec, the Bit Rate Type can only be set to CBR.
Quality	This parameter is configurable only when the Bit Rate Type is set to VBR. Higher video quality improves clarity but requires more bandwidth.
Bit Rate	This parameter is configurable only when the Bit Rate Type is set to CBR. Supports custom bit rate selection. Choose a bit rate value based on actual conditions.
I Frame Interval	The I Frame Interval defines the number of P frames between two I frames. The available range adjusts based on the FPS (frames per second) setting. It is recommended to set the I Frame Interval to twice the FPS value for optimal performance.
Watermark	Enable watermark verification to detect any tampering in the video.
Watermark String	

3. Click **Apply**.

Region of Interest (RoI)

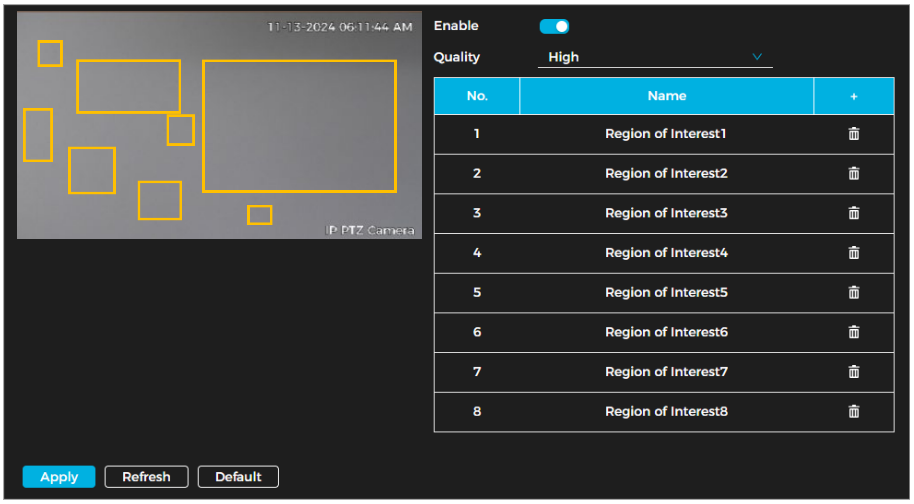
Follow the steps below to select a RoI and configure its image quality.

1. Navigate to **Settings → Video/Audio → Video → Region of Interest**.
2. Click ○ next to **Enable.**
3. Draw the RoI area on the image.
4. Configure the RoI image quality.

ⓘ

- A higher image quality value will result in a clearer image.
- Click 🗑 to delete a box.

5. Click **Apply**.
6. Click + to add more regions. You can add up to eight.



Enable ●

Quality High

No.	Name	+
1	Region of Interest1	🗑
2	Region of Interest2	🗑
3	Region of Interest3	🗑
4	Region of Interest4	🗑
5	Region of Interest5	🗑
6	Region of Interest6	🗑
7	Region of Interest7	🗑
8	Region of Interest8	🗑

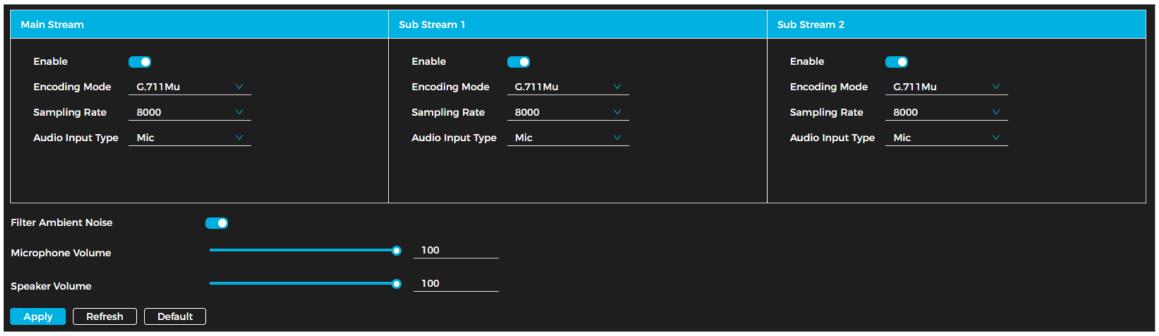
How to Set Audio Parameters and Alarm Audio

This section goes over how to configure audio parameters and alarm audio.

Audio Parameters

Follow the steps below to set the camera’s audio parameters.

1. Navigate to **Settings → Video/Audio → Audio**.



	Main Stream	Sub Stream 1	Sub Stream 2
Enable	●	●	●
Encoding Mode	G.711Mu	G.711Mu	G.711Mu
Sampling Rate	8000	8000	8000
Audio Input Type	Mic	Mic	Mic

Filter Ambient Noise ●

Microphone Volume 100

Speaker Volume 100

Audio Parameters

2. Click ○ next to **Enable** for the **Main Stream** and **Sub Stream(s)**. For cameras with multiple channels, select the channel number.

⚠ Ensure the audio acquisition function is activated or deactivate per the scene requirements.

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

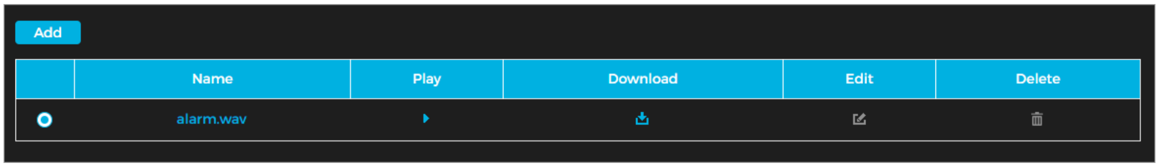
Parameter	Description
Encoding Mode	Choose the audio encoding mode from PCM, G.711A, G.711Mu, or AAC. The selected audio encoding mode applies to both audio recording and intercom. Using the default setting is recommended.
Sampling Rate	The sampling rate represents the number of audio samples taken per second. A higher sampling frequency results in more samples, leading to a more accurate restored signal. Select an audio sampling rate from 8000, 16000, 32000, 48000, or 64000.
Audio Input Type	• **LineIn:** Requires an external audio device. • **Mic:** Does not require an external audio device.
Filter Ambient Noise	The system will automatically filter ambient noise if this function is enabled.
Microphone Volume	Controls microphone volume.
Speaker Volume	Controls speaker volume.

4. Click **Apply**.

Alarm Audio Files

Follow the steps below to record and upload an alarm audio file. The file will be played when the alarm is triggered.

1. Navigate to **Settings → Video/Audio → Audio → Alarm Audio Files**.



	Name	Play	Download	Edit	Delete
○	alarm.wav	▶	⤓	✎	🗑

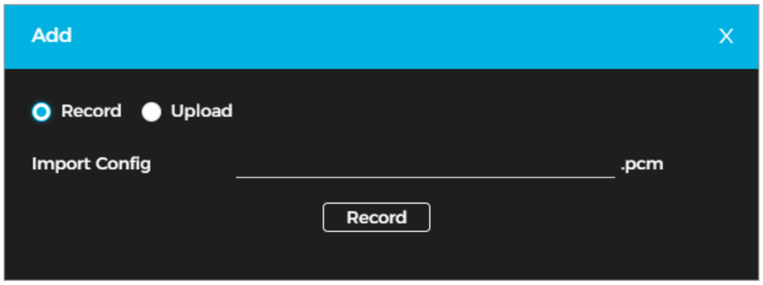
Alarm Audio Files

2. Click **Add**.

3. Select **Record** or **Upload**.

- If you select **Record**, input the audio name and then click **Record**. Recordings are in .pcm format only. Only select device models support audio recordings.

- If you select **Upload**, click **Browse** and select the file to be uploaded. Click **Upload**. You can upload .pcm, .wav2, .mp3, or .aac files.



◉ Record ○ Upload

Record or Upload Alarm Audio

Related Operations

- **To edit an audio file**: Click ✎.
- **To delete an audio file**: Click 🗑.
- **To play an audio file**: Click ▶.
- **To download an audio file**: Click ⤓.

Image

This section goes over how to configure image parameters.

ⓘ Parameters may vary depending on device model.

Display

Display Settings

Follow the steps below to configure the display parameters.

1. Navigate to **Settings → Image → Display Settings**.

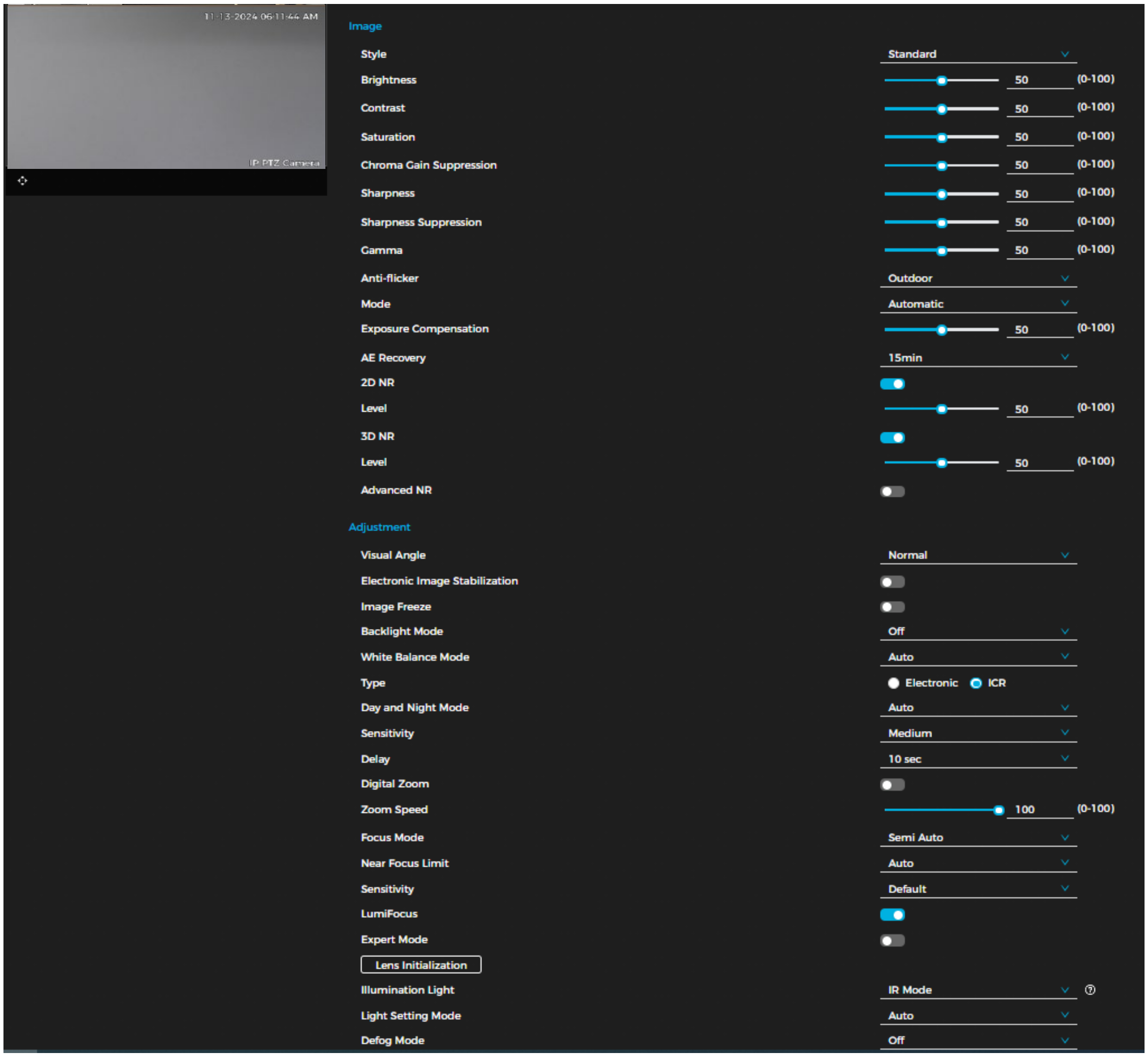


Image		
Style	Standard	
Brightness	50	(0-100)
Contrast	50	(0-100)
Saturation	50	(0-100)
Chroma Gain Suppression	50	(0-100)
Sharpness	50	(0-100)
Sharpness Suppression	50	(0-100)
Gamma	50	(0-100)
Anti-flicker	Outdoor	
Mode	Automatic	
Exposure Compensation	50	(0-100)
AE Recovery	15min	
2D NR	☑	
Level	50	(0-100)
3D NR	☑	
Level	50	(0-100)
Advanced NR	☐	
Adjustment		
Visual Angle	Normal	
Electronic Image Stabilization	☐	
Image Freeze	☐	
Backlight Mode	Off	
White Balance Mode	Auto	
Type	○ Electronic ● ICR	
Day and Night Mode	Auto	
Sensitivity	Medium	
Delay	10 sec	
Digital Zoom	☐	
Zoom Speed	100	(0-100)
Focus Mode	Semi Auto	
Near Focus Limit	Auto	
Sensitivity	Default	
LumiFocus	☑	
Expert Mode	☐	
Lens Initialization		
Illumination Light	IR Mode	
Light Setting Mode	Auto	
Defog Mode	Off	

Display Settings

2. Select the configuration file: **Profile1** (Daytime) or **Profile2** (Nighttime).

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

Parameter	Description
Style	Choose a picture style: • **Standard**: Default image style. Displays colors as they appear naturally. • **Soft**: Reduces hue intensity and contrast. Images appear lighter. • **Vivid**: Enhances colors for a more vibrant appearance.
Brightness	Adjust the brightness value to control the image's brightness. A higher value makes the image brighter, while a lower value makes it darker. Setting the value too high may cause the image to appear hazy.
Contrast	Adjust the contrast to control the difference between bright and dark areas in the image. A higher value increases contrast, making bright areas brighter and dark areas darker. Excessively high contrast may cause overexposure in bright areas and loss of detail in dark areas. A lower value reduces contrast, making the image appear flatter. If set too low, the image may become hazy.

Saturation	Adjust the saturation to make colors deeper or lighter without affecting image brightness. A higher value enhances color intensity, making the image more vibrant. A lower value reduces color intensity, making the image appear more muted or desaturated.
Chroma Gain Suppression	Reduces image color intensity to prevent oversaturation. A higher value produces a stronger effect. This setting is effective only in low-light environments.
Sharpness	Adjust the sharpness to control the clarity of picture edges. A higher value makes edges sharper and more defined. A lower value results in softer edges, reducing sharpness. If set too high, image noise may become more noticeable.
Sharpness Suppression	Adjusts the camera's sharpness NCT level. A higher value increases image sharpness CNT. This setting is effective only in low-light conditions.
Gamma	Adjust the brightness and enhance the dynamic range of the image in a non-linear manner. A higher value increases brightness. A lower value darkens the image.
Anti-Flicker	Choose one: • **50 Hz**: Adjusts exposure based on ambient light when the power supply is 50 Hz, preventing flickering or stripes. • **60 Hz**: Adjusts exposure based on ambient light when the power supply is 60 Hz, preventing flickering or stripes. • **Outdoor**: Allows selection of any exposure mode based on requirements.
Mode	Refers to device exposure modes. Choose between: • **Automatic**: Automatically adjusts image brightness based on real-time conditions. • **Manual**: Allows manual configuration of gain and shutter value to control image brightness. • **Iris Priority**: Sets the iris to a fixed value, allowing the camera to automatically adjust the shutter. If brightness remains insufficient and the shutter reaches its limit, the system increases gain to maintain proper exposure. • **Shutter Priority**: Allows custom shutter range; the camera automatically adjusts aperture and gain based on scene brightness. • **Gain Priority**: Enables manual adjustment of gain and exposure compensation.
Shutter	Set the effective exposure time. A smaller value results in a shorter exposure time.
Gain	When Gain Priority or Manual mode is selected, you can adjust Gain. With minimum illumination, the camera automatically increases Gain to enhance image clarity.
Exposure Compensation	Set the gain value within the range of 0 to 100. A higher value increases brightness, making the image clearer in low-light conditions.
AE Recovery	Automatic exposure adjusts the aperture and shutter speed based on ambient lighting conditions for both images and video. When an AE Recovery Time is set, the exposure mode automatically returns to its previous state after the iris is adjusted. Available options: Off, 5 min, 15 min, 1 hour, and 2 hours.
3D NR	Uses multi-frame processing (at least 2 frames) to reduce noise by analyzing frame information from both previous and subsequent frames.
2D NR	Averages pixels within a single frame to reduce image noise. Higher levels produce less noise but result in a softer image.
Level	Noise reduction level ranges from 0 to 100. Higher values provide stronger noise reduction.

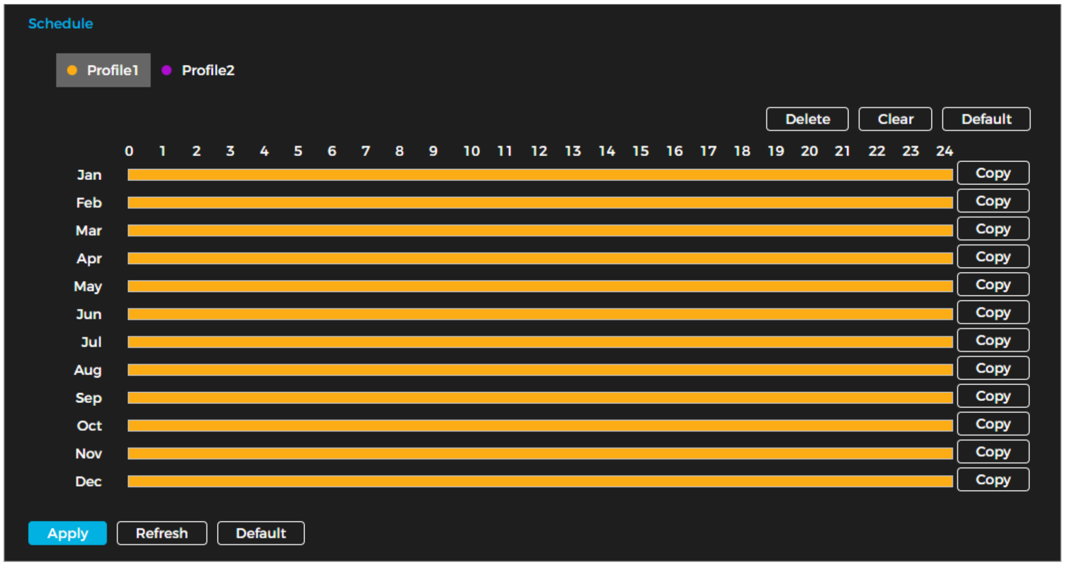
Visual Angle	Adjust the image display direction as needed.
Electronic Image Stabilization	Electronic Image Stabilization (EIS) reduces image shake to deliver clearer video. It is disabled by default. This setting is effective only in low-light environments. This feature is supported on select models. EIS and Optical Image Stabilization cannot be enabled simultaneously.
Image Freeze	When this function is enabled, only the image at the selected preset is displayed during a preset or tour call; no images are shown while the camera rotates.
Backlight Mode	Adjust the backlight compensation mode for the monitoring screen. • **Off**: Disables backlight compensation. • **BLC (Backlight Compensation)**: Balances areas with extreme brightness or darkness to maintain a normal exposure for the main subject. • **HLC (Highlight Compensation)**: Dims strong light sources, improving visibility of faces and license plates in extreme lighting conditions—ideal for toll stations and parking lot entrances/exits. • **WDR (Wide Dynamic Range)**: Reduces overexposure in bright areas and enhances details in dark areas for improved clarity.
White Balance Mode	The White Balance function ensures accurate color representation by keeping white objects truly white in different lighting conditions. • **Auto**: Adjusts white balance based on color temperature for accurate color display. • **Indoor**: Adjusts white balance for typical indoor lighting conditions to maintain accurate color representation. • **ATW**: During tracking, the system automatically adjusts white balance to maintain accurate color. • **Natural**: Optimizes white balance for environments without artificial light to maintain color accuracy. • **Streetlamp**: Adjusts white balance for outdoor night scenes, ensuring correct color representation. • **Outdoor**: Automatically balances white in most outdoor environments, whether under natural or artificial light. • **Manual**: Allows manual adjustment of red and blue gain, while the system compensates based on color temperature. • **Sodium Lamp**: Compensates white balance to sodium lamp to ensure color precision.
Day and Night Mode	Configure the image display mode based on lighting conditions: • **Auto**: Automatically switches between color and black-and-white based on ambient lighting. • **Color**: Displays the image in full color mode. • **B/W (Black-and-White)**: Displays the image in black-and-white mode.
Sensitivity	This configuration is available only when Auto is selected in Day and Night Mode. You can adjust the camera sensitivity for switching between color and black-and-white modes based on lighting conditions.
Delay	This configuration is available only when Auto is selected in Day and Night Mode.

	You can set the delay time for switching between color and black-and-white modes. A lower value results in a faster switch between modes.
Digital Zoom	Click ○ to enable digital zoom. This allows further zooming even after the optical zoom reaches its maximum limit.
Zoom Speed	Adjusts the camera's zoom speed. Higher values result in faster zooming.
Focus Mode	Choose the focus mode. • **Auto**: The camera refocuses automatically when motion or scene changes cause the image to blur. • **Semi-Auto**: The camera focuses automatically when you click Focus or Zoom, or when a preset change or PTZ movement is detected. • **Manual**: Focus must be adjusted manually; the camera does not autofocus.
Near Focus Limit	Set the camera's near focus limit. If the limit is too short, the camera may focus on its dome. Adjusting this limit also affects focus speed.
Sensitivity	Sets the camera's focus trigger sensitivity. Higher sensitivity allows focus to activate more easily.
LumiFocus	When the target moves, the camera automatically refocuses to maintain clarity.
Expert Mode	Trains the camera to rotate and focus along a defined path.
Lens Initialization	Click the button to automatically initialize the lens. The lens extends to calibrate zoom and focus.
Light Setting Mode	You can choose from Manual, Auto, Zoom Priority, or Off modes. • **Manual**: Manually adjust the illuminator brightness; the system adjusts image illumination accordingly. • **Auto**: The system automatically adjusts illuminator brightness based on ambient lighting. Some models allow setting the maximum brightness and sensitivity. ○ **Sensitivity**: Higher sensitivity increases illuminator brightness sooner as lighting decreases, and delays dimming when lighting improves. ○ **Brightness Upper Limit**: Prevents overexposure at the image center when illumination is too strong. Adjust according to the scene. Range: 0 – 100 (default 100). • **Zoom Priority**: The system automatically adjusts illuminator brightness with ambient light changes. You can fine-tune brightness through manual compensation. ○ In low light, the system activates low beams first, then high beams if brightness remains insufficient. ○ As light increases, high beams dim and turn off before low beams. ○ When zoomed out to a wide angle, high beams remain off to prevent close-range overexposure. • **Off**: Disables the illuminator.
Defog Mode	In foggy or hazy environments, the defog function enhances image clarity. • **Manual**: Manually configure function intensity and atmospheric light mode to improve clarity. The atmospheric light mode can be set to automatic or manual. • **Auto**: The system automatically adjusts image clarity based on real-time conditions.

	• **Off**: Disables the defog function.

4. Configure the schedule by clicking **Schedule** to open the profile schedule settings.

5. Slide the bar to set the time periods for daytime and night accordingly.



Schedule

● Profile1 ● Profile2

Delete Clear Default

	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	
Jan		Copy
Feb		Copy
Mar		Copy
Apr		Copy
May		Copy
Jun		Copy
Jul		Copy
Aug		Copy
Sep		Copy
Oct		Copy
Nov		Copy
Dec		Copy

Apply Refresh Default

Profile Schedule Setting

6. Click **Apply**.

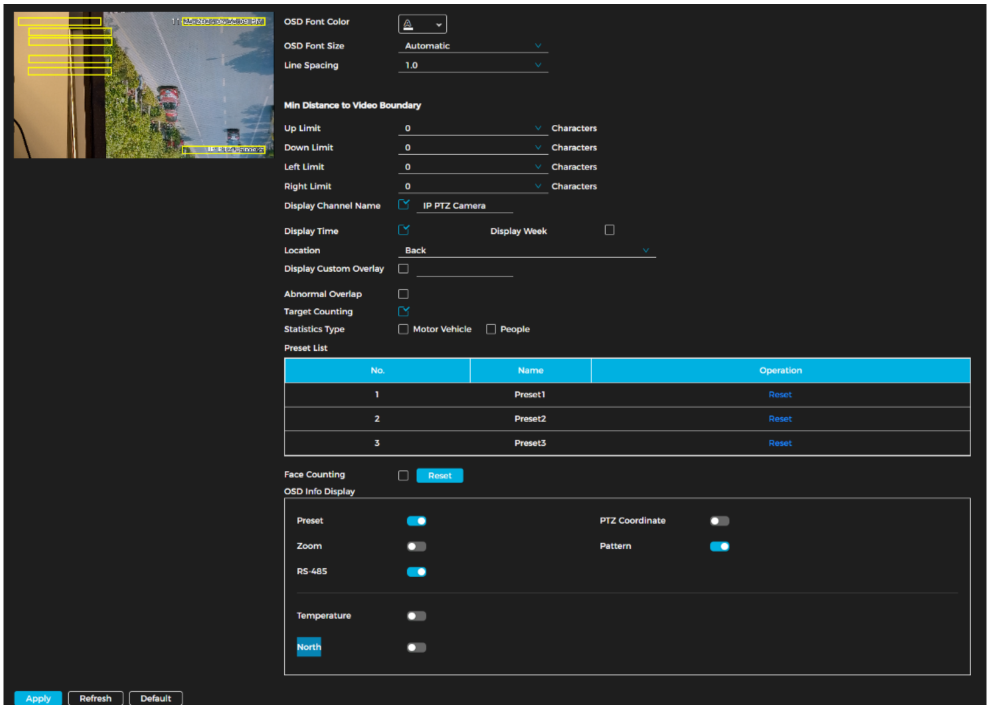
OSD

Follow the steps below to enable the OSD function and display the selected information on the image.

1. Navigate **Settings → Images → OSD**.

2. Set the OSD information as required.

ⓘ Parameters may vary depending on device model.



OSD Font Color

OSD Font Size: Automatic

Line Spacing: 1.0

Min Distance to Video Boundary

Up Limit: 0 Characters

Down Limit: 0 Characters

Left Limit: 0 Characters

Right Limit: 0 Characters

Display Channel Name ☑ IP PTZ Camera

Display Time ☑ Display Week □

Location: Back

Display Custom Overlay □

Abnormal Overlap □

Target Counting ☑

Statistics Type □ Motor Vehicle □ People

Preset List

No.	Name	Operation
1	Preset1	Reset
2	Preset2	Reset
3	Preset3	Reset

Face Counting □ Reset

OSD Info Display

Preset	●	PTZ Coordinate	○
Zoom	○	Pattern	●
RS-485	●		
Temperature	○		
North	○		

Apply Refresh Default

OSD

Parameter	Description
OSD Font Color	Configure OSD text properties, including color, size, and line spacing.
OSD Font Size	
Line Spacing	
Min Distance to Video Boundary	Set the minimum distance from the video edge. Available values: 0, 1, or 2.
Display Channel Name	Enter the channel name, then click to show it on the video image.
Display Time	Check to display time information on the image.
Display Week	Check to display the day of the week.
Location	Set the display position for time and week information.
Display Custom Overlay	Enter custom text, then click to show it on the image.
Abnormal Overlap	Check to overlay abnormal status information on the image.
Target Counting	Check to show target statistics on the image.
Statistics Type	Select the statistics type: Motor Vehicle or People.
Preset List	Display the preset list.
Face Counting	Check to show face statistics on the image. Click Reset to clear all statistical data.
OSD Info Display	• **Presets**: When enabled, the preset name appears on the image as the camera moves to that preset and disappears after 3 seconds. • **PTZ Coordinate**: When enabled, PTZ coordinate information is shown on the image. • **Zoom**: When enabled, zoom level information is displayed on the image. • **Pattern**: When enabled, pattern information is displayed on the image. • **RS-485**: When enabled, RS-485 communication information is shown on the image. • **Temperature**: When enabled, temperature information is displayed on the image. • **North**: When enabled, the north direction appears on the image. Enabling the true north function prompts a PTZ restart.

3. Click **Apply**.

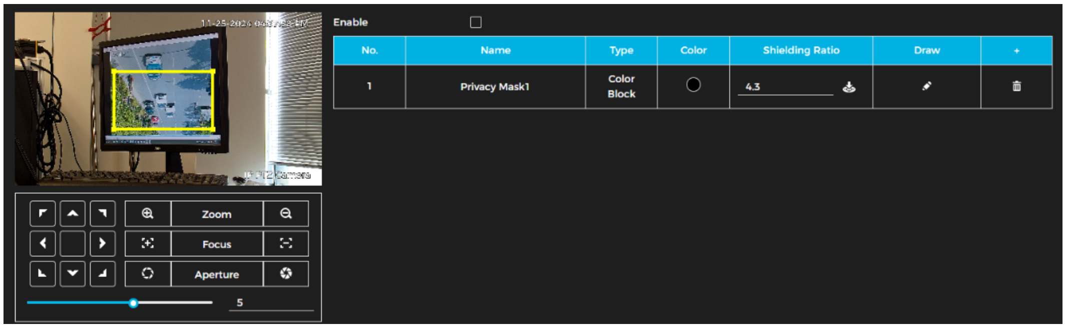
Privacy Mask

Enable this function to protect privacy by masking specific areas in the video image. You can choose from the following masking types:

- **Color Block**: Draw triangles and convex quadrilaterals as black blocks. Supports up to 8 blocks.
- **Mosaic**: Draw rectangular blocks with a mosaic effect. Supports up to 4 blocks.
- **Color Block + Mosaic**: Allows a combination of both types, supporting up to 8 blocks in total.

Follow the steps below to enable privacy masking.

1. Navigate to **Settings → Image → Privacy Mask**.
2. Click ■ next to **Enable**.
3. Click +. Drag the block to the area you would like to mask.
4. Adjust the size of the area.



Enable □

No.	Name	Type	Color	Shielding Ratio	Draw	+
1	Privacy Mask1	Color Block	●	4.3	✎	🗑

Privacy Masking

Related Operations

- **To view and edit a block**: Select the masking rule name from the list. The block will be highlighted and can be edited.
- **To edit a block name**: Double click the block's name.
- **To delete a block**: Click 🗑.

PTZ

This section describes how to configure PTZ parameters, including basic settings, PTZ operation, and scheduled tasks.

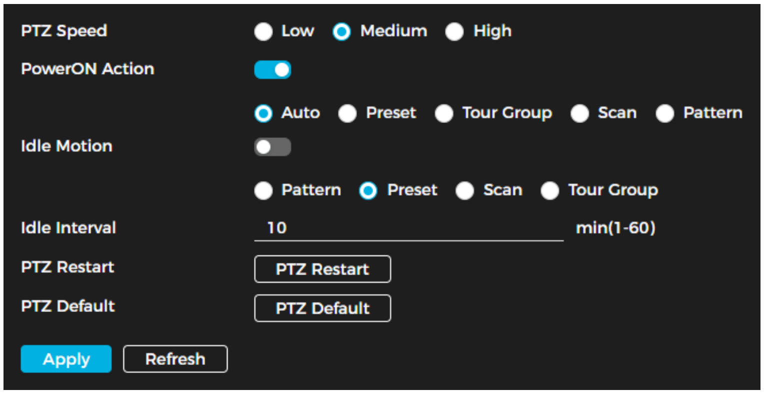
ⓘ

- The PTZ and detail camera channels support different functions, which may vary from the actual interface.
- Some PTZ camera models do not support focus, zoom, or iris adjustments, and the options may differ from the displayed page.

Basic Settings

Follow the steps below to configure the basic PTZ settings.

1. Navigate to **Settings → Image → PTZ → Basic Settings**.
2. Set the parameters. See the table for more details.



PTZ Speed ○ Low ● Medium ○ High

PowerON Action (on)

● Auto ○ Preset ○ Tour Group ○ Scan ○ Pattern

Idle Motion (off)

○ Pattern ● Preset ○ Scan ○ Tour Group

Idle Interval 10 min(1-60)

PTZ Restart [PTZ Restart]

PTZ Default [PTZ Default]

PTZ Parameters

Parameter	Description
PTZ Speed	
PowerON Action	Click to enable the function, then select the PowerON type. After configuration, the camera automatically performs the specified motion when powered on. Selecting **Auto** will repeat the last action performed for more than 20 seconds before shutdown.

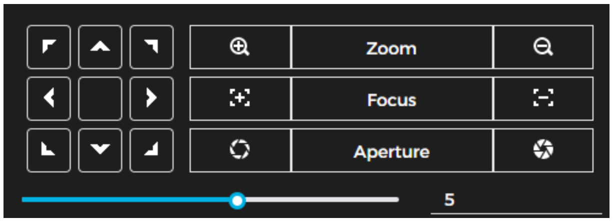
Idle Motion	Click to enable idle motion, set the idle interval time, and select the desired idle motion type.
Idle Interval	
PTZ Restart	Reboot the PTZ.
PTZ Default	Restore the PTZ to default settings.

PTZ Operations

How to Configure Presets

The camera stores parameters such as PTZ pan/tilt position and focus status, allowing quick recall to restore the PTZ to the saved position. Follow the steps below to configure.

1. Navigate to **Settings → Image → PTZ → PTZ Operation**.
2. Set the step length and use the direction buttons to adjust the PTZ position.
3. Adjust zoom, focus, and iris to position the camera.



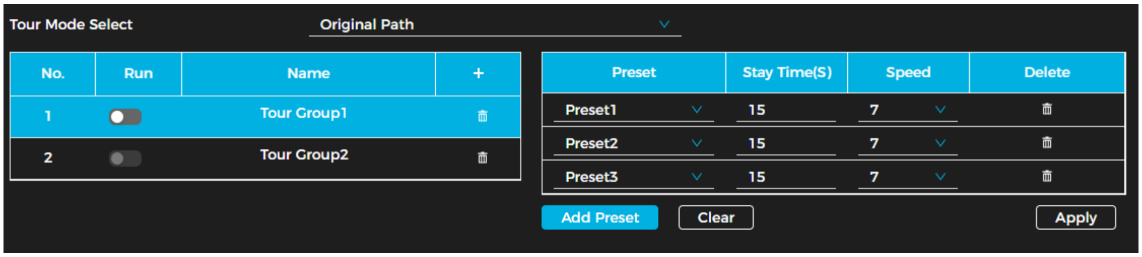
PTZ Control Pan

4. Click + to add a preset or add the current position as a preset.
5. Change the name of the preset by clicking on the name of it.
6. Click 💾 to save the preset or 🗑 to delete the preset.

How to Configure a Tour Group

Configure a tour group to make the PTZ camera automatically cycle through the preset points after setup. Preset points must be created in advance.

1. Navigate to **Settings → Image → PTZ → PTZ Operation → Tour Group**.
2. Click + and then **Name** to change the name of the tour group.
3. Select a tour group, click Add Preset, then choose presets from the Preset Point drop-down list on the left. Repeat this process to add multiple presets to the tour group.
4. Set **Stay Time(S)** and **Speed** to define how long the camera remains at each preset and how fast it rotates between points. Stay time can be set from 15 to 3600 seconds.



Tour Mode Select: Original Path

No.	Run	Name	+
1	○	Tour Group1	🗑
2	○	Tour Group2	🗑

Preset	Stay Time(S)	Speed	Delete
Preset1	15	7	🗑
Preset2	15	7	🗑
Preset3	15	7	🗑

Tour Group

5. Select the tour mode: Original (camera moves through the preset points in the selected order) or Shortest Path (camera rearranges the preset points by distance and moves along the shortest route).

ⓘ This function is only available on select models.

6. Click **Apply** and then ○ to start the tour. The tour will stop if the PTZ is commanded to perform an operation or by clicking ●.

7. To delete a tour group, click 🗑. To clear all tour groups, click **Clear**.

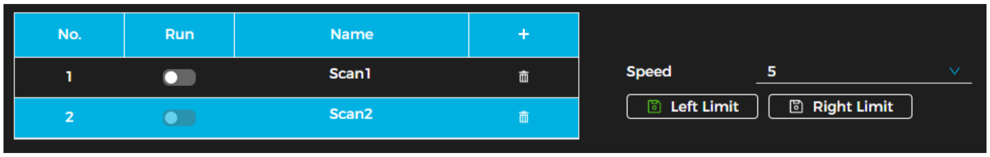
How to Configure Scan

Scan allows the camera to pan horizontally at a set speed between defined left and right boundaries.

1. Navigate to **Settings → Image → PTZ → PTZ Operation → Scan**.

2. Click + and then **Name** to change the name of the scan.

3. Set the left and right limit of the camera.



No.	Run	Name	+
1	○	Scan1	🗑
2	○	Scan2	🗑

Speed 5

Scan

4. Click ○ to start scanning. Click ● to stop scanning.

5. To delete a scan, click 🗑.

How to Configure Patterns

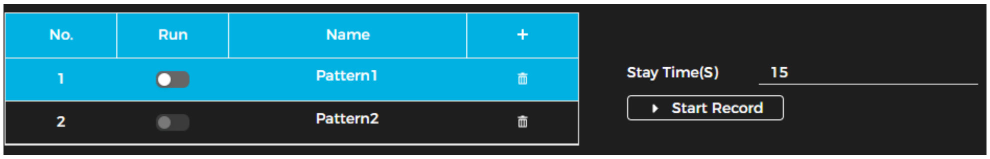
Pattern records a series of camera actions, including pan, tilt, zoom, and preset calls. After recording and saving, the camera can automatically repeat the same movement path.

1. Navigate to **Settings → Image → PTZ → PTZ Operation → Pattern**.

2. Click + and then **Name** to change the name of the pattern.

3. Click ▶ Start Record to change the direction, focus, zoom, and other settings as required.

4. Click II Stop Record to complete records.



No.	Run	Name	+
1	○	Pattern1	🗑
2	○	Pattern2	🗑

Stay Time(S) 15

Pattern

5. Click ○ to start the pattern. Click ● to stop the pattern.

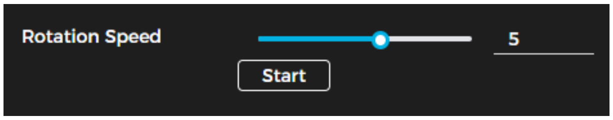
6. To delete a pattern, click 🗑.

How to Configure Pan

Pan allows the camera to rotate continuously 360° horizontally at a set speed.

1. Navigate to **Settings → Image → PTZ → PTZ Operation → Pan**.

2. Set the rotation speed and click **Start**.



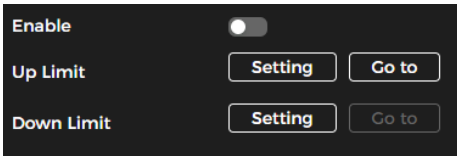
Rotation Speed 5

Pan

How to Configure PTZ Rotation Limit

Set PTZ rotation limits to restrict camera movement within a defined area, ensuring rotation stays within range during functions such as tour or pan.

1. Navigate to **Settings → Image → PTZ → PTZ Operation → PTZ Rotation**.
2. Move the camera to the desired upper position, then click Up Limit Setting to save it as the upper limit.
3. Move the camera to the desired lower position, then click Down Limit Setting to save it as the lower limit.
4. Click **Go To** to preview the configured up and down limits.



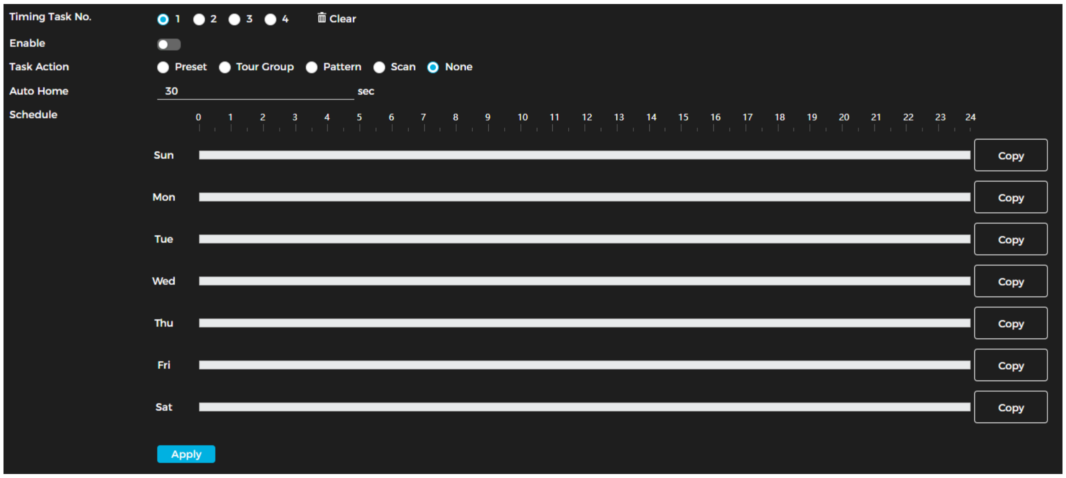
PTZ Rotation Limit

5. Select a value from the Max Elevation Angle drop-down list. This function is only available on select models.
6. Click ○ to enable the function.

How to Schedule a Task

After scheduling a task, the camera performs the specified PTZ actions during the configured time period. PTZ motions such as preset, tour, scan, or pattern must be configured in advance.

1. Navigate to **Settings → Image → PTZ → Schedule Task**.
2. Select a Timing Task No. You can configure up to four timing tasks.
3. Select the Task Action. Some actions require selecting a corresponding action number.
4. Set the Auto Home time. If the scheduled task is interrupted by manual PTZ control, the device automatically resumes the task after the specified Auto Home time.
5. Configure the task schedule.



Timing Task No. ● 1 ○ 2 ○ 3 ○ 4 Clear

Enable ○

Task Action ○ Preset ○ Tour Group ○ Pattern ○ Scan ● None

Auto Home 30 sec

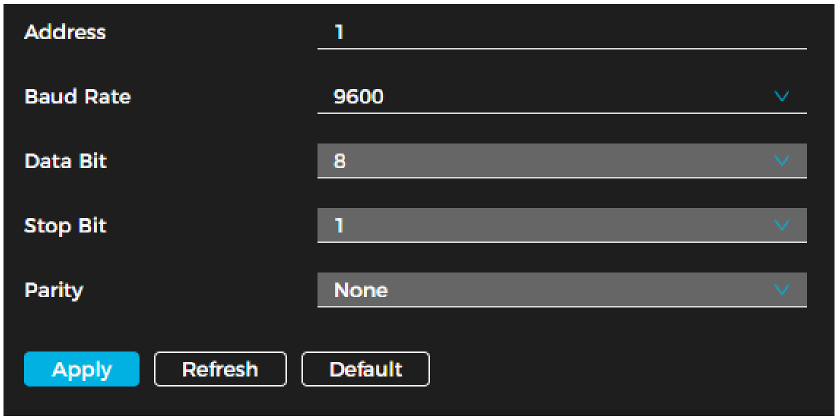
Scheduled Task

6. Click ● to enable the task schedule.
7. Click **Apply**.

How to Configure RS-485

Follow the steps below to configure the parameters for RS-485.

1. Navigate to **Settings → Image → PTZ → RS-485**.



Address: 1

Baud Rate: 9600

Data Bit: 8

Stop Bit: 1

Parity: None

RS-485 Parameters

2. Click **Apply**.

Events

General Settings

The system analyzes video images to detect significant changes. When changes occur—such as motion or image blur—an alarm is triggered and the configured linkage action is executed.

How to Configure Motion Detection Events

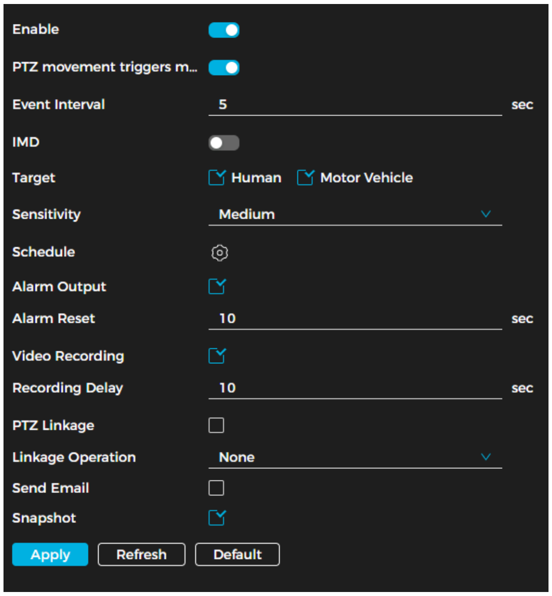
The system triggers an alarm linkage when motion is detected and the object's speed meets the configured sensitivity level.

If both Motion Detection and Smart Motion Detection are enabled with linkage actions configured, the linkages function as follows:

- When Motion Detection is triggered, the camera records and captures snapshots, but other linkages such as email alerts or PTZ actions will not activate.
- When Smart Motion Detection is triggered, all configured linkages are executed.

If only Motion Detection is enabled, all configured linkages activate when motion is detected.

1. Navigate to **Settings → Event → General Settings → Motion Detection**.



Enable: ●

PTZ movement triggers m...: ●

Event Interval: 5 sec

IMD: ○

Target: ☑ Human ☑ Motor Vehicle

Sensitivity: Medium

Schedule: ⚙

Alarm Output: ☑

Alarm Reset: 10 sec

Video Recording: ☑

Recording Delay: 10 sec

PTZ Linkage: □

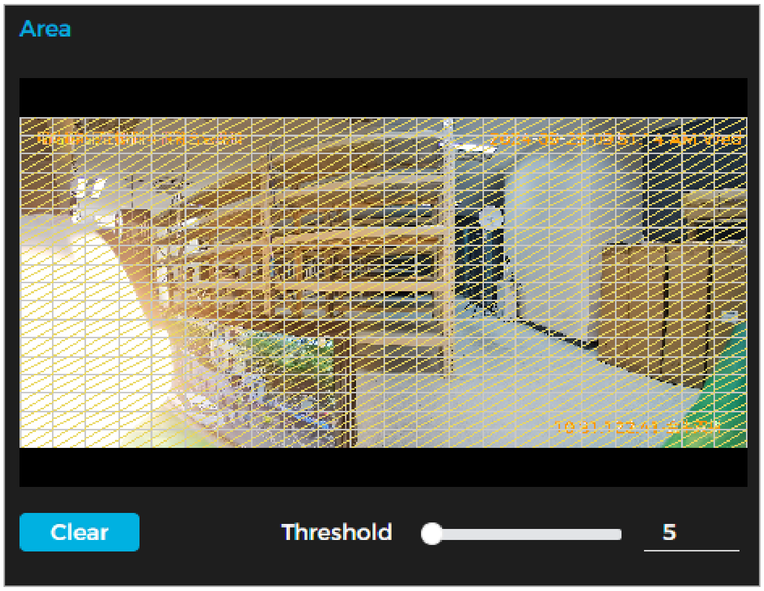
Linkage Operation: None

Send Email: □

Snapshot: ☑

Motion Detection

2. Click ○ to enable motion detection.
3. (Optional) Click ○ next to **PTZ movement triggers motion detection** to enable this feature.
4. Define the motion detection area. Click and drag the mouse to draw the area. Irregular and non-continuous regions are supported.



Threshold 5

Area

ⓘ

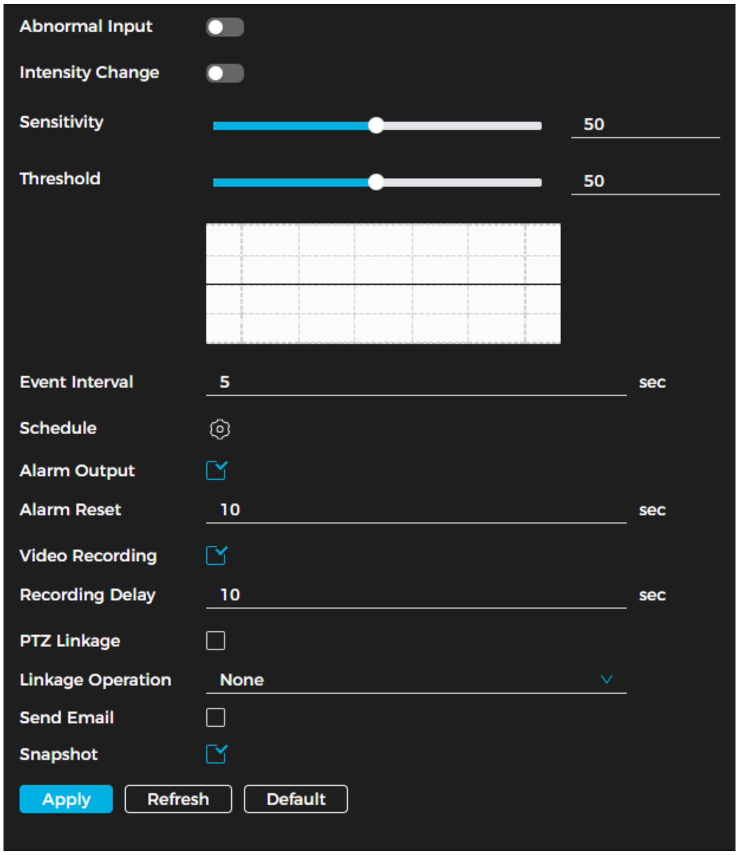
- **Threshold**: Defines the effective area sensitivity for motion detection. A lower value makes alarms trigger more easily.
- By default, the entire video image is used as the motion detection area.
- Click **Clear** to remove all defined detection areas.

5. (Optional) Click ○ next to iMD to enable the function, then set the target type and sensitivity. The device can detect humans, motor vehicles, or both as required.
6. Set arming schedule and alarm linkage action(s).
7. Click **Apply**.

How to Configure Audio Detection Events

Follow the steps below to have the system trigger an alarm linkage action when it detects unclear sounds, tone variations, or sudden changes in sound intensity.

1. Navigate to **Settings** → **Event** → **General Settings** → **Audio Detection**.



Abnormal Input ○
Intensity Change ○
Sensitivity 50
Threshold 50
Event Interval 5 sec
Schedule
Alarm Output ☑
Alarm Reset 10 sec
Video Recording ☑
Recording Delay 10 sec
PTZ Linkage □
Linkage Operation None
Send Email □
Snapshot ☑

Audio Detection

2. Set the parameters.

Mode	Description
Abnormal Input	An alarm is triggered when the system detects abnormal audio input.
Intensity Change	Set Sensitivity and Threshold. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold. ⓘ • Higher sensitivity or a lower threshold makes the alarm easier to trigger. Use a higher threshold in noisy environments. • In the waveform, a red line indicates audio detection is triggered, while a green line indicates no detection. Adjust sensitivity and threshold based on the waveform display.

3. Set arming schedule and alarm linkage action(s).

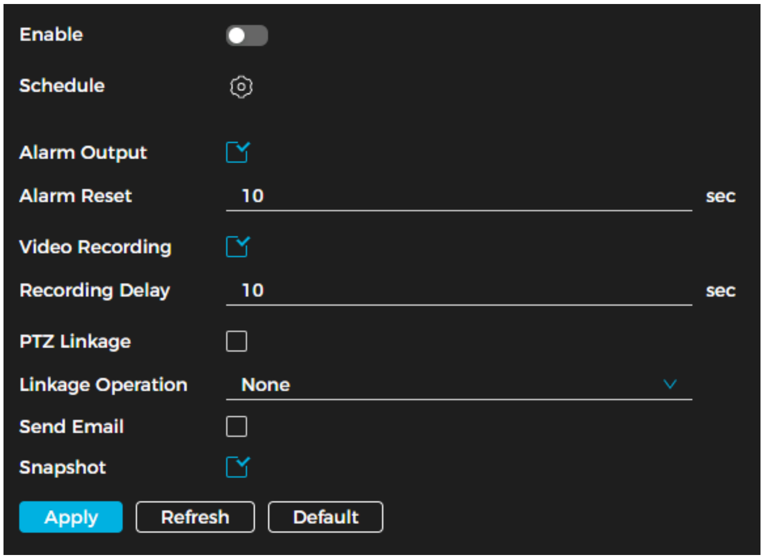
4. Click **Apply**.

How to Configure Video Tampering Events

Follow the steps below to have the system trigger an alarm linkage action when the lens is blocked or the video output turns into a monochrome screen due to lighting or other factors.

1. Navigate to **Settings → Event → General Settings → Video Tampering**.

2. Click ○ to enable the function.



Enable

Schedule

Alarm Output ☑

Alarm Reset 10 sec

Video Recording ☑

Recording Delay 10 sec

PTZ Linkage □

Linkage Operation None

Send Email □

Snapshot ☑

Video Tampering

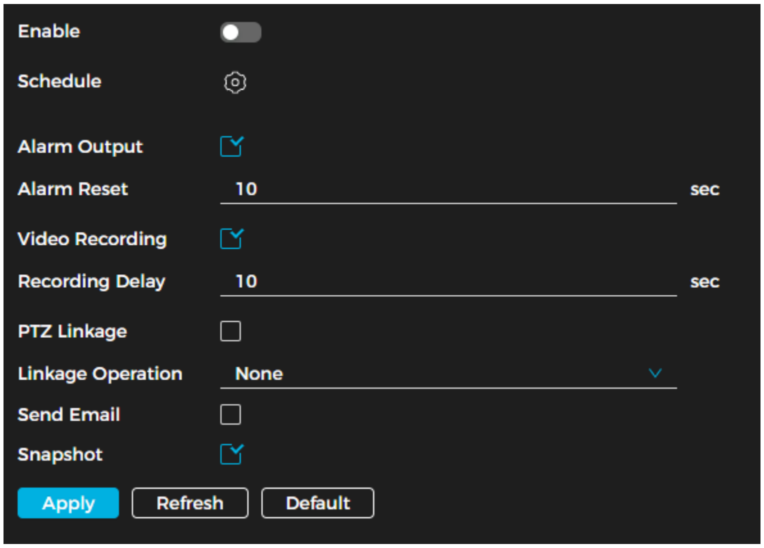
3. Set the arming schedule and linkage action(s).

4. Click **Apply**.

How to Configure Scene Changing Events

Follow the steps below to have the system trigger an alarm linkage action when the image switches from the current scene to another one.

1. Navigate to **Settings** → **Event** → **Video Detection** → **Scene Changing**.



Enable

Schedule

Alarm Output ☑

Alarm Reset 10 sec

Video Recording ☑

Recording Delay 10 sec

PTZ Linkage □

Linkage Operation None

Send Email □

Snapshot ☑

Scene Changing

2. Set the arming schedule and linkage action(s).

3. Click **Apply**.

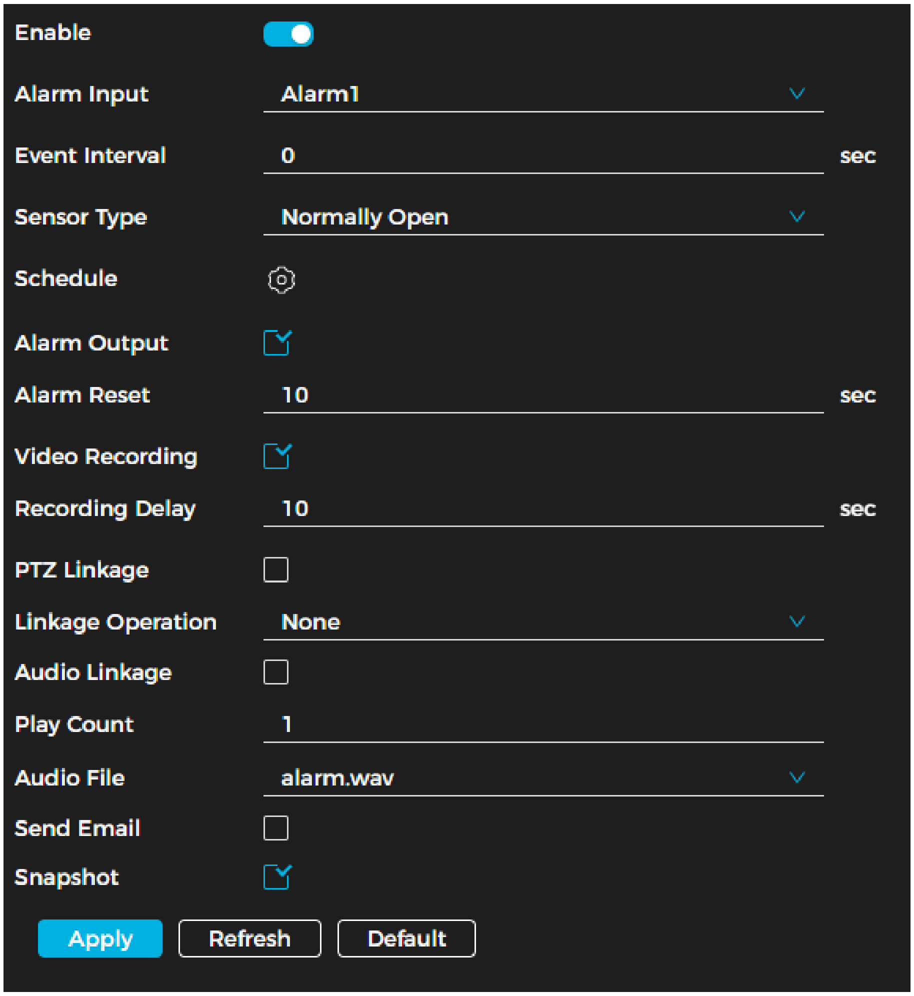
How to Configure Alarm Linkage Actions

When setting alarm events, choose the desired alarm linkage actions (such as recording or snapshot). The system triggers the alarm during the configured arming period when the specified event occurs.

How to Set the Alarm Input

1. Navigate to **Settings** → **Event** → **General Settings**→ **Alarm Configuration**.

2. Click ○ to enable the function.
3. Set the alarm input. When a device connected to the alarm-in port triggers an alarm, the system executes the configured alarm linkage.
4. Click **Apply**.



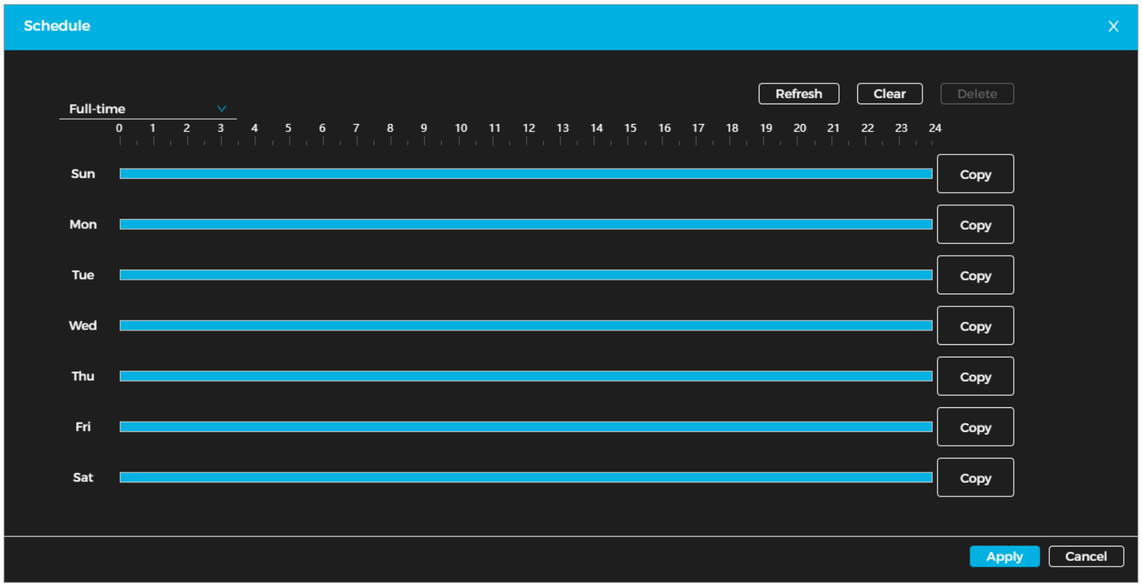
Enable	●	
Alarm Input	Alarm1	
Event Interval	0	sec
Sensor Type	Normally Open	
Schedule	⚙	
Alarm Output	☑	
Alarm Reset	10	sec
Video Recording	☑	
Recording Delay	10	sec
PTZ Linkage	□	
Linkage Operation	None	
Audio Linkage	□	
Play Count	1	
Audio File	alarm.wav	
Send Email	□	
Snapshot	☑	

Alarm Input

How to Set the Arming Schedule

Follow the steps below to have the system perform corresponding linkage actions only during a configured period.

1. Click ⚙ next to **Schedule**.



Arming Schedule

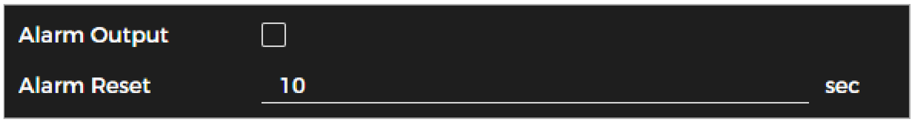
2. Press and drag the left mouse button on the timeline to define up to six (6) arming periods. Alarms are active during the blue segments on the timeline. Click **Copy** next to a day, then choose the days to apply the same configuration. Select the Select All checkbox to copy to all days.

3. Click **Apply**.

4. (Optional) Click ⌄ and then + Schedule to add a new schedule. Click 🗑 to delete a schedule as needed.

How to Configure Alarm Output Linkage

When an alarm is triggered, the system can automatically activate the connected alarm-out device. On the **Alarm Linkage** page, check the box to enable alarm output linkage, select the desired channel, and configure **Alarm Reset**. When Alarm Reset is enabled, the alarm output remains active for a set period after the alarm event ends.



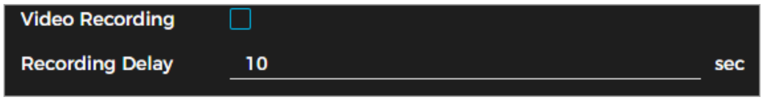
Alarm Output □

Alarm Reset 10 sec

Alarm Output Linkage

How to Configure Record Linkage

Select the checkbox to enable record linkage, then set **Recording Delay** to define the alarm recording duration. When Recording Delay is configured, recording continues for a set time after the alarm event ends.



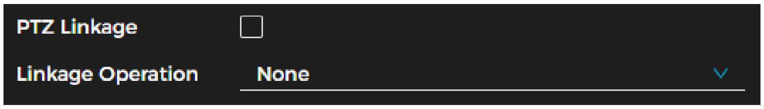
Video Recording □

Recording Delay 10 sec

Record Linkage

How to Configure PTZ Linkage

Select the checkbox to enable PTZ linkage. Select **Linkage Operation** from the following options: none, preset, tour, group, and pattern.



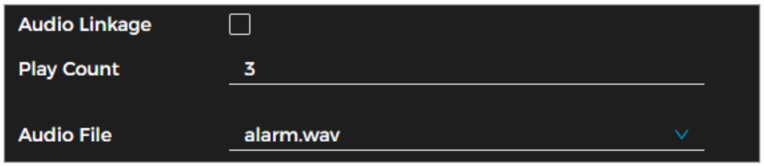
PTZ Linkage □

Linkage Operation None ⌄

Audio Linkage

How to Configure Audio Linkage

The system can trigger an audio channel when an alarm event occurs. On the Alarm Linkage page, check the box to enable audio linkage, set the play count, and select the desired audio file.



Audio Linkage □

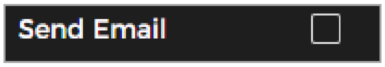
Play Count 3

Audio File alarm.wav

Audio Linkage

How to Configure Email Linkage

When an alarm is triggered, the system automatically sends an email notification to users. Email linkage is active only after SMTP is properly configured.



Send Email □

Email Linkage

How to Configure Snapshot Linkage

When an alarm is triggered, the system automatically triggers an alarm and captures snapshots when an alarm occurs. On the Alarm Linkage page, select the checkbox to enable snapshot linkage.

Snapshot □

Email Linkage

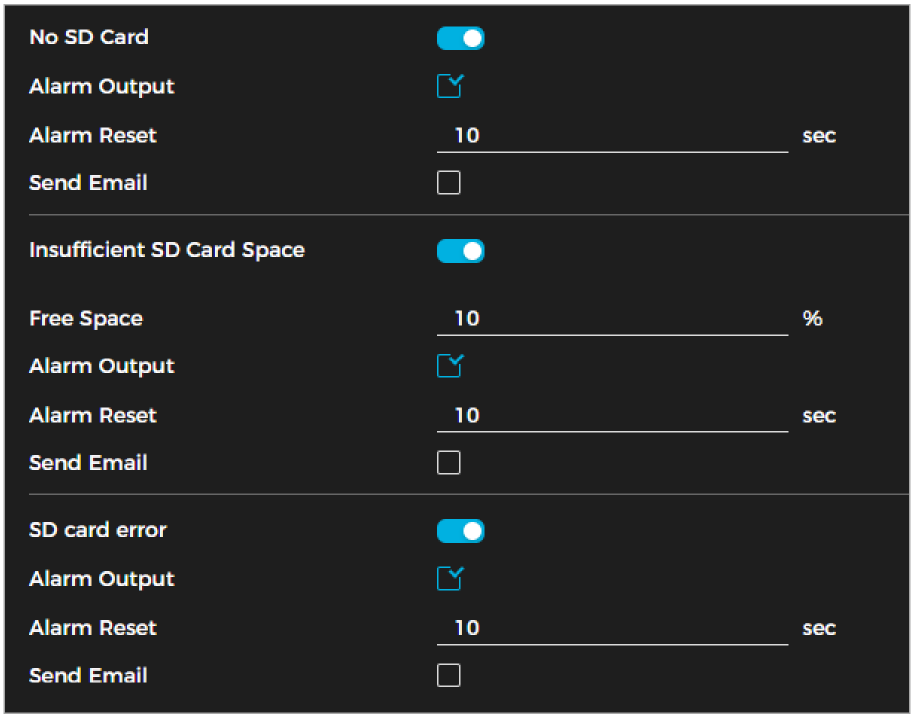
How to Configure Exception Events

Abnormalities include SD card issues and network exceptions. Only devices equipped with an SD card support abnormality detection functions such as No SD Card, SD Card Error, and Insufficient SD Card Space.

How to Configure an SD Card Exception Event

When an SD card exception occurs, the system triggers an alarm linkage. Event types include No SD Card, Insufficient SD Card Space, and SD Card Error. Supported functions may vary by model.

1. Navigate **Settings → Event → Exception**.



No SD Card ●

Alarm Output ☑

Alarm Reset 10 sec

Send Email □

Insufficient SD Card Space ●

Free Space 10 %

Alarm Output ☑

Alarm Reset 10 sec

Send Email □

SD card error ●

Alarm Output ☑

Alarm Reset 10 sec

Send Email □

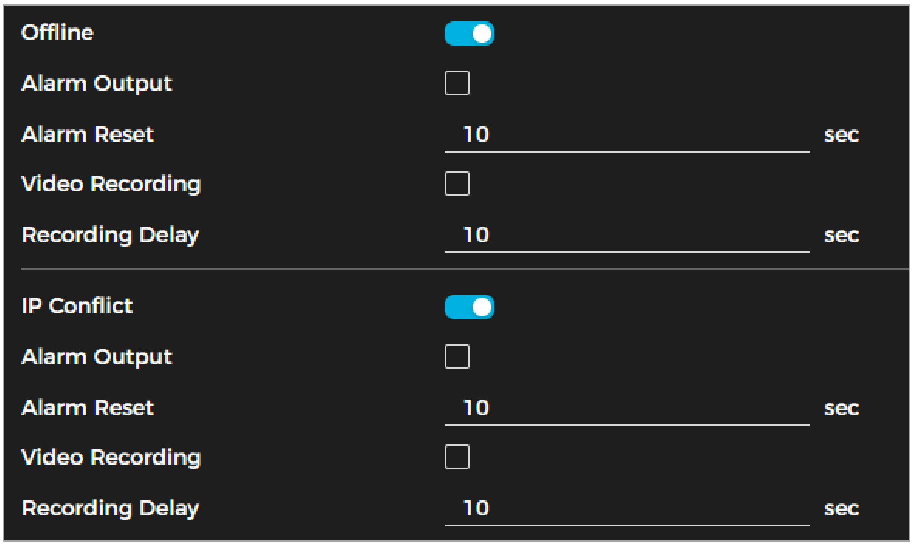
SD Card Exception

2. Click ○ to enable the SD card detection functions. When enabling Insufficient SD Card Space, configure the Free Space value. An alarm is triggered when the remaining SD card space falls below this threshold.
3. Set the arming schedule and linkage action(s).
4. Click **Apply**.

How to Configure a Network Exception Event

When a network abnormality occurs, the system triggers an alarm linkage. Event types include Offline and IP Conflict.

1. Navigate **Settings → Event → Exception**.



Offline ●

Alarm Output □

Alarm Reset 10 sec

Video Recording □

Recording Delay 10 sec

IP Conflict ●

Alarm Output □

Alarm Reset 10 sec

Video Recording □

Recording Delay 10 sec

Network Exception

2. Click ○ to enable the SD card detection functions. When enabling Insufficient SD Card Space, configure the Free Space value. An alarm is triggered when the remaining SD card space falls below this threshold.
3. Set the arming schedule and linkage action(s).

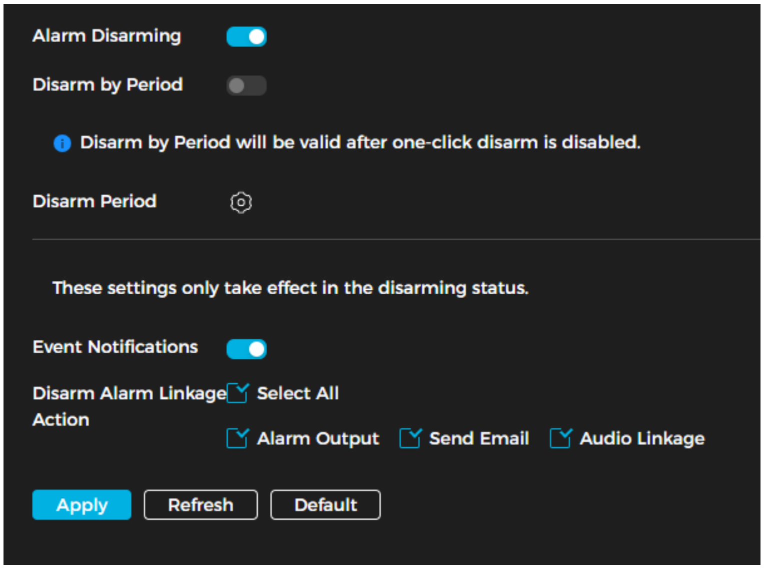
4. Click **Apply**.

How to Configure Alarms

How to Set Disarm Alarm Linkage Actions

The camera supports one-click control to disarm alarm linkage actions. When **Event Notification** is enabled, only the selected alarm linkage actions are triggered.

1. Navigate to **Settings → Event → Alarm → Alarm Disarming**.
2. Enable **Alarm Disarming** (system continuously disables all alarm linkage actions) or **Disarm by Period** (system disables alarm linkage actions only during the specified time period) as required.



Alarm Disarming ●

Disarm by Period ○

Disarm by Period will be valid after one-click disarm is disabled.

Disarm Period

These settings only take effect in the disarming status.

Event Notifications ●

Disarm Alarm Linkage Action ☑ Select All

☑ Alarm Output ☑ Send Email ☑ Audio Linkage

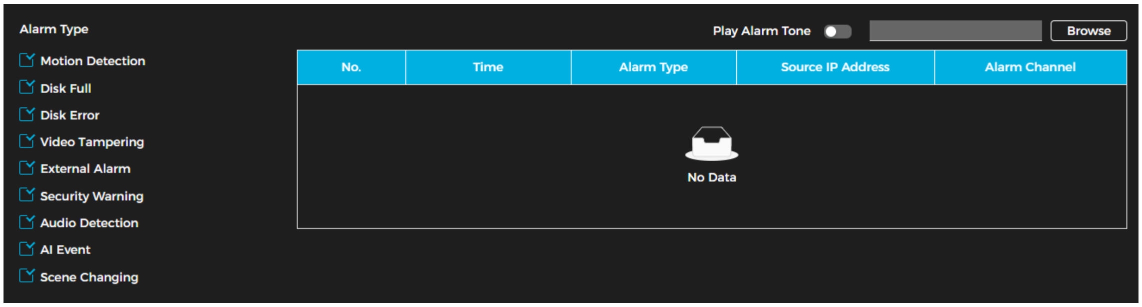
Disarming

3. Enable Event Notification, then select the desired Disarm Alarm Linkage Actions. Supported disarm linkage types may vary by device.
4. Click **Apply**.

How to Subscribe to Alarm Events

You can subscribe to alarm events. When a subscribed event occurs, the system logs detailed alarm data on the right panel.

1. Navigate to **Settings → Event → Alarm → Subscribe Alarm**.



Alarm Type

☑ Motion Detection
☑ Disk Full
☑ Disk Error
☑ Video Tampering
☑ External Alarm
☑ Security Warning
☑ Audio Detection
☑ AI Event
☑ Scene Changing

Play Alarm Tone ○

No.	Time	Alarm Type	Source IP Address	Alarm Channel

No Data

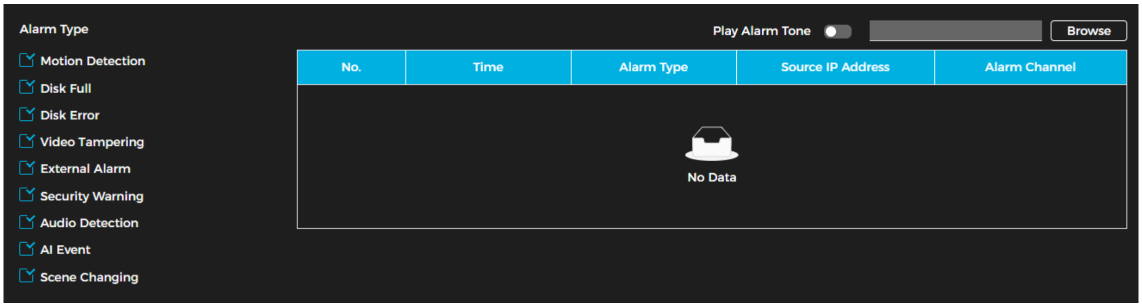
Subscribe to an Alarm

2. Choose an event alarm type.
3. Click ○ next to **Play Alarm Tone**, and choose an audio file. The system will play the file when the selected alarm is triggered.

How to Set the Network Destination

Follow the steps to choose the network destination, activate it, and set the parameters. The camera periodically sends AI function reports to the specified server.

1. Navigate to **Settings → Event → Network Destination**.



Alarm Type

- ☑ Motion Detection
- ☑ Disk Full
- ☑ Disk Error
- ☑ Video Tampering
- ☑ External Alarm
- ☑ Security Warning
- ☑ Audio Detection
- ☑ AI Event
- ☑ Scene Changing

Play Alarm Tone ○ Browse

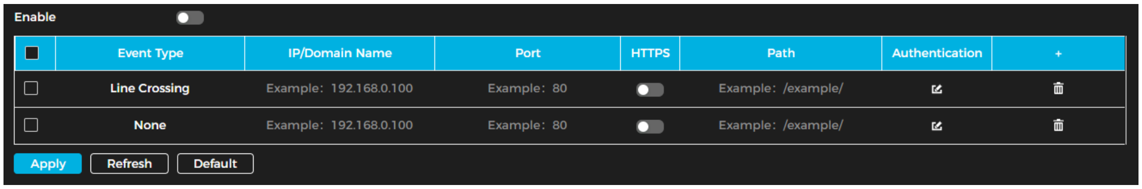
No.	Time	Alarm Type	Source IP Address	Alarm Channel

No Data

Subscribe to an Alarm

2. Enable the function.

3. Click **+**. Set the parameters.



Enable ○

□	Event Type	IP/Domain Name	Port	HTTPS	Path	Authentication	+
□	Line Crossing	Example: 192.168.0.100	Example: 80	○	Example: /example/	✎	🗑
□	None	Example: 192.168.0.100	Example: 80	○	Example: /example/	✎	🗑

Apply Refresh Default

Mode	Description
Event Type	Choose the event type from the drop-down list. Multiple types can be selected simultaneously. The available event types match those in picture playback.
IP/Domain Name	The server's IP address and port number where the report is sent.
Port	
HTTPS	When HTTPS is enabled, download the CA certificate and upload it to the server.
Path	The server's storage path for the report.

4. Click **Apply**.

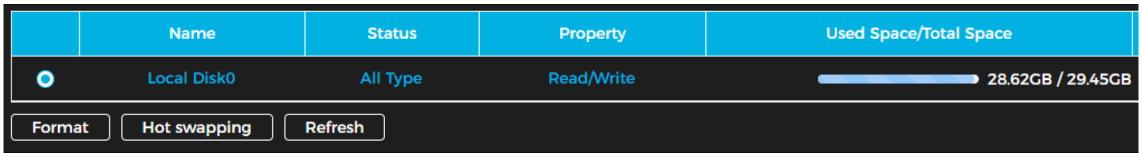
Related Operations

- Click ✎ to set up server authentication.
- Click 🗑 to delete the server information.

Local Storage

Follow the steps below to show the local SD card information and format it. Functions may differ by model.

1. Navigate to **Settings → Storage → Local Storage**.
2. Click **Format** to erase the SD card.
3. Click **Hot Swapping** to enable SD card replacement while powered on.



	Name	Status	Property	Used Space/Total Space
◉	Local Disk0	All Type	Read/Write	28.62GB / 29.45GB

Local Storage

Event

General Settings

Analyze video images to detect significant changes in the scene. If notable changes occur, such as a moving object or a blurry image, the system will trigger an alarm linkage.

How to Set Up a Motion Detection Alarm

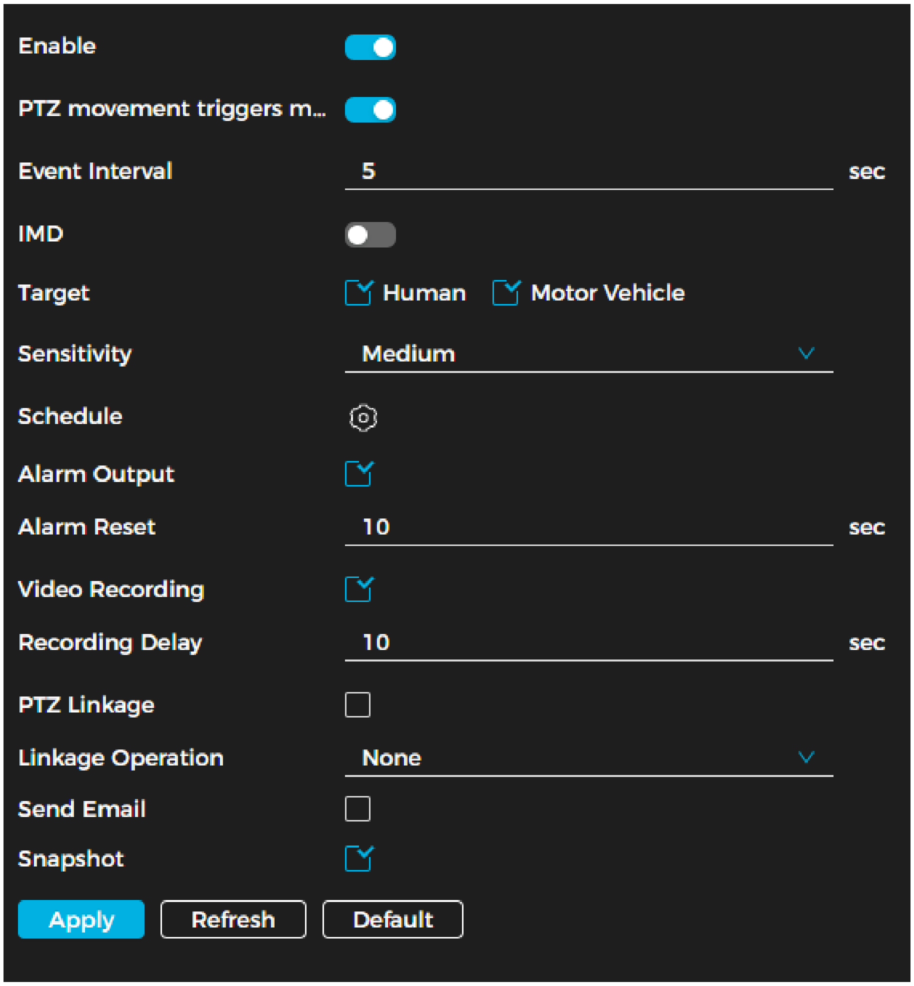
If motion detection is configured, the system performs any assigned alarm linkage actions when a moving object appears in the image and its speed exceeds the configured sensitivity threshold.

ⓘ

- If Motion Detection and Smart Motion Detection are both enabled with linked activities configured, the following applies:
- When Motion Detection is triggered, the camera will record and capture snapshots, but other configured actions (e.g., sending emails, PTZ operations) will not take effect.
- When Smart Motion Detection is triggered, all configured linkages will take effect.
- If only Motion Detection is enabled, all configured linkages will activate when motion is detected.

Follow the steps below to set up motion detection.

1. Navigate to **Settings → Event → General Settings → Motion Detection**.



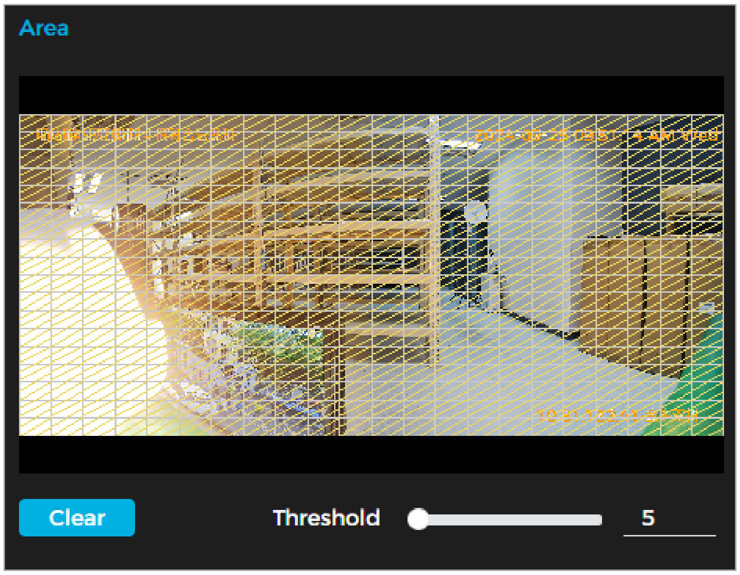
Enable	☑	
PTZ movement triggers m...	☑	
Event Interval	5	sec
IMD	□	
Target	☑ Human ☑ Motor Vehicle	
Sensitivity	Medium	
Schedule	⚙	
Alarm Output	☑	
Alarm Reset	10	sec
Video Recording	☑	
Recording Delay	10	sec
PTZ Linkage	□	
Linkage Operation	None	
Send Email	□	
Snapshot	☑	

Motion Detection

2. Click ○ to enable the function.
3. Select the monitoring area by clicking and dragging the mouse around the area. The area can be irregular and discontinuous.

ⓘ

- **Threshold**: Defines the effective area threshold for motion detection. A smaller threshold increases sensitivity, making alarms easier to trigger.
- By default, the entire video image serves as the motion detection area.
- Click Clear to remove all defined motion detection areas.



Threshold 5

Motion Detection Area

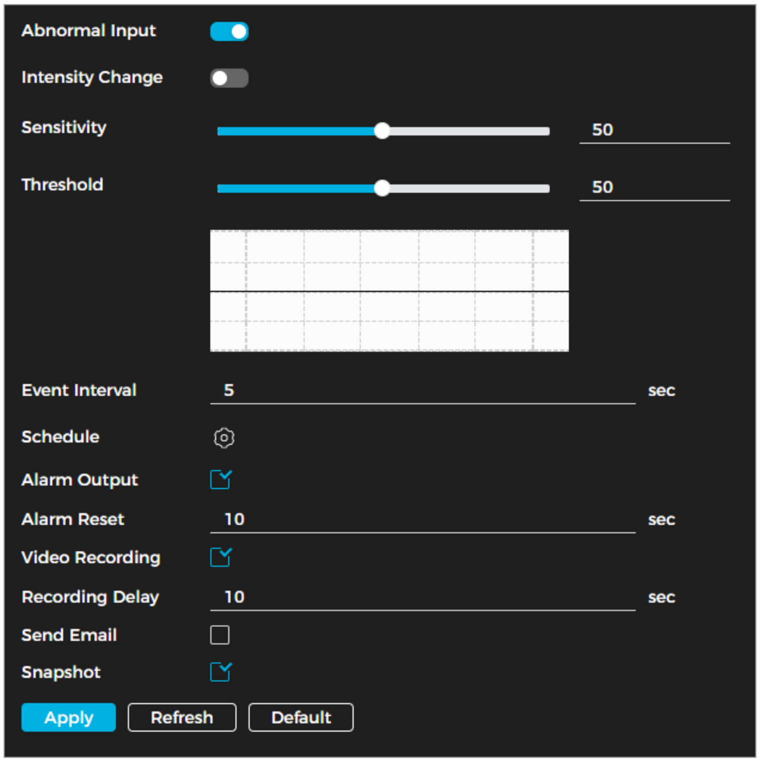
4. (Option) Click next to IMD to enable the function. Select the target type and alarm sensitivity.
5. Set the arming schedule and alarm linkage actions. See the **Alarm Linkage** section of this manual for more information.
6. Click **Apply**.

How to Set Up an Audio Detection Alarm

If audio detection is configured, the system performs any assigned alarm linkage actions when an unknown voice, tone change, or rapid change in sound intensity is detected.

Follow the steps below to enable audio detection.

1. Navigate to **Settings → Event → General Settings → Audio Detection**.



Abnormal Input ●
Intensity Change ○
Sensitivity 50
Threshold 50
Event Interval 5 sec
Schedule
Alarm Output ☑
Alarm Reset 10 sec
Video Recording ☑
Recording Delay 10 sec
Send Email □
Snapshot ☑

Audio Detection Parameters

2. Set the parameters.

Parameter	Description
Abnormal Input	Click to enable the function. An alarm will be triggered if the system detects abnormal sound input.
Intensity Change	Click to enable the function. Set the sensitivity and threshold. An alarm will be triggered if it detects sound intensity that exceeds the threshold. ⓘ • A higher sensitivity or smaller threshold makes it easier to trigger an alarm. In noisy environments, set a higher threshold to reduce false alarms. • The red line in the waveform indicates that audio detection is triggered. The green line indicates that no audio detection has occurred. Adjust sensitivity and threshold based on the waveform analysis.

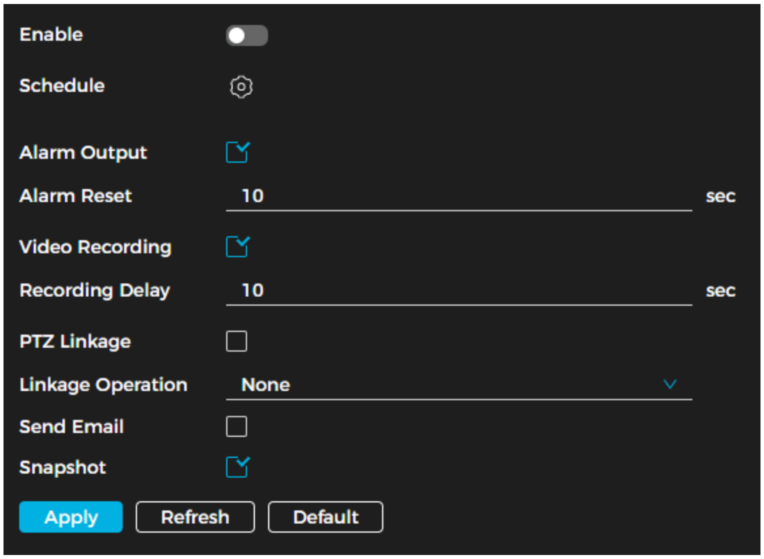
3. Set the arming schedule and alarm linkage actions. For more details, see the **Alarm Linkage** section of this manual.
4. Click **Apply**.

How to Set a Video Tampering Alarm

If video tampering is configured, the system performs any assigned alarm linkage actions when the lens is obscured, or the video color output is monochrome due to light or other reasons.

Follow the steps below to set a video tampering alarm.

1. Navigate to **Settings → Event → General Settings → Video Tampering**.
2. Select the event type: Video Tampering.



Enable ○
Schedule
Alarm Output ☑
Alarm Reset 10 sec
Video Recording ☑
Recording Delay 10 sec
PTZ Linkage □
Linkage Operation None
Send Email □
Snapshot ☑

Video Tampering

3. Set the arming schedule and alarm linkage actions. For more details, see the **Alarm Linkage** section of this manual.
4. Click **Apply**.

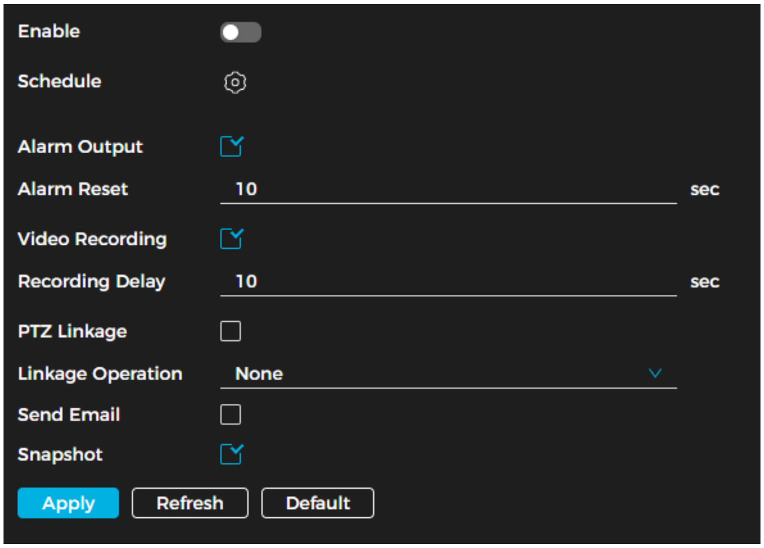
How to Set a Scene Changing Alarm

If scene changing is configured, the system performs any assigned alarm linkage actions when the image changes from the current scene to another one.

Follow the steps below to set a scene changing alarm.

1. Navigate to **Settings → Event → Video Detection → Scene Changing**.

2. Click ○ to enable the function.



Enable ○

Schedule

Alarm Output ☑

Alarm Reset 10 sec

Video Recording ☑

Recording Delay 10 sec

PTZ Linkage □

Linkage Operation None

Send Email □

Snapshot ☑

Scene Changing Alarm Parameters

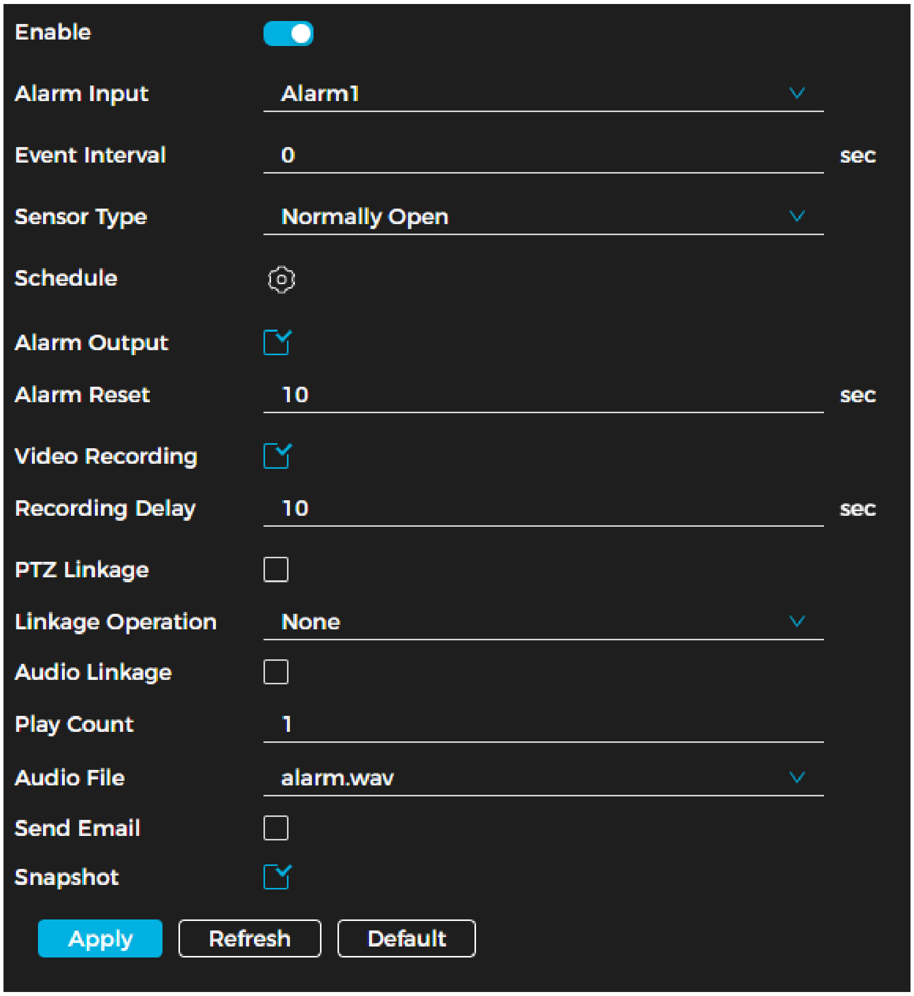
3. Set the arming schedule and alarm linkage actions. For more details, see the **Alarm Linkage** section of this manual.
4. Click **Apply**.

Alarm Linkage

When configuring alarm events, select alarm linkages such as recording or snapshot capture. When an alarm is triggered during the configured arming period, the system will activate the selected alarm response.

How to Set Alarm Input

1. Navigate to **Settings → Event → General Settings → Alarm Configuration**.
2. Click ○ to enable the function.
3. Choose the alarm input. When an alarm is triggered by a device connected to the alarm-in port, the system executes the configured alarm linkage actions.



Enable: ●

Alarm Input: Alarm1

Event Interval: 0 sec

Sensor Type: Normally Open

Schedule: ⚙

Alarm Output: ☑

Alarm Reset: 10 sec

Video Recording: ☑

Recording Delay: 10 sec

PTZ Linkage: □

Linkage Operation: None

Audio Linkage: □

Play Count: 1

Audio File: alarm.wav

Send Email: □

Snapshot: ☑

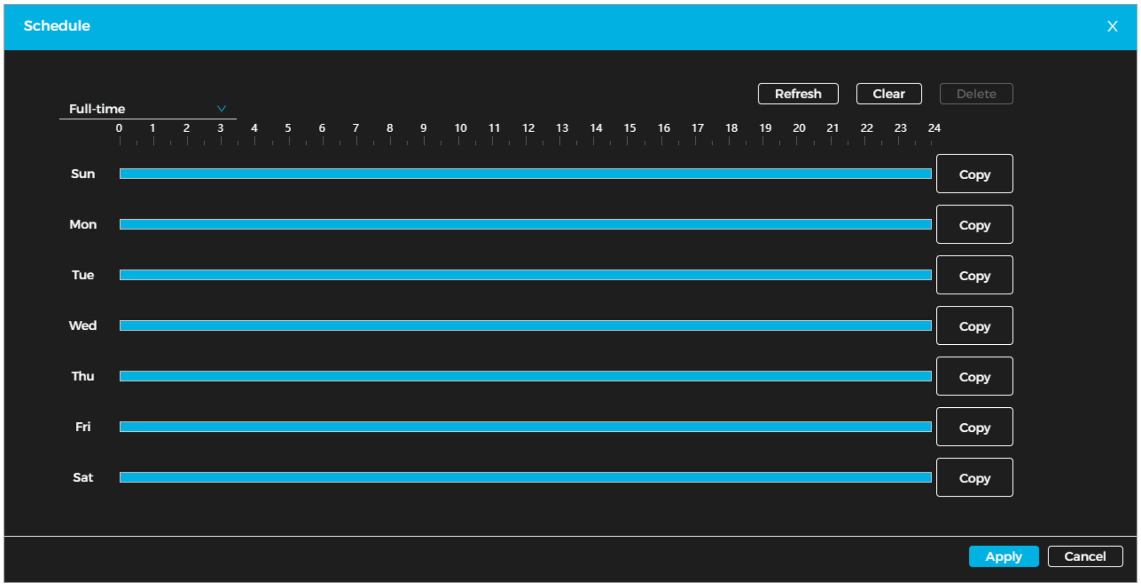
Alarm Input

4. Click **Apply**.

How to Add a Schedule

Follow the steps below to set the arming schedule so that the system executes alarm linkage actions only during the configured period.

1. Click ⚙ next to **Schedule**.



Schedule: Full-time

Schedule

2. Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered during the blue-marked periods on the timeline.

ⓘ

- Click **Copy** next to a day, then select the days to apply the same configuration. To copy a schedule to all days, check **Select All**.
- You can configure up to 6 arming periods per day.

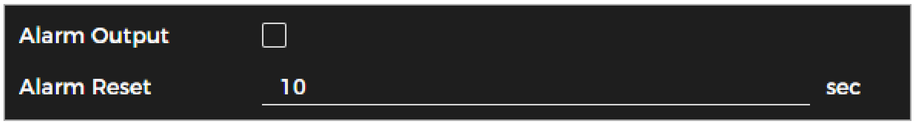
3. Click **Apply**.
4. (Optional) Click ∨ and then **+ Schedule** to add a new table.
5. (Optional) Click 🗑 to delete tables as required.

Alarm Output Linkage

When an alarm is triggered, the system can automatically link to alarm-out device. Follow the steps below to enable this functionality.

1. Navigate to the **Alarm Linkage** page.
2. Click ■ to enable alarm output linkage.
3. Select the desired channel.
4. Configure Alarm Reset.

When Alarm Reset is configured, the alarm will continue for an extended period after the initial alarm ends.



Alarm Output ☐

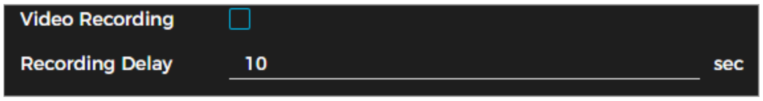
Alarm Reset 10 sec

Alarm Output Linkage

Record Linkage

The system can link to a recording channel when an alarm event occurs. After the alarm ends, recording stops for an extended period based on the Recording Delay setting. Follow the steps below to enable this functionality.

1. Navigate to the **Alarm Linkage** page.
2. Click ■ to enable record linkage.
3. Select the desired channel.
4. Set Recording Delay.



Video Recording ☐

Recording Delay 10 sec

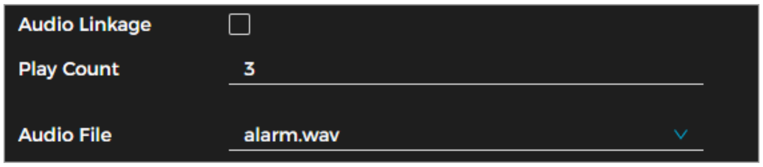
Record Linkage

Audio Linkage

The system can link to an audio channel with an alarm event occurs.

1. Navigate to the **Alarm Linkage** page.
2. Click ■ to enable audio linkage.
3. Select the play count.

4. Select the audio file.

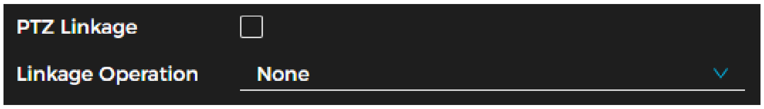


Audio Linkage □
Play Count 3
Audio File alarm.wav

Audio Linkage

PTZ Linkage

The system can trigger PTZ actions when an alarm occurs. To set PTZ linkage, click to enable it, then choose a linkage mode: None, Preset, Tour Group, or Pattern.

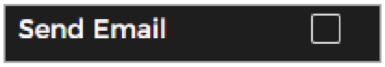


PTZ Linkage □
Linkage Operation None

PTZ Linkage

Email Linkage

The system can automatically send an email to users when an alarm event occurs. SMTP must be configured enable this feature. See the **SMTP** portion of this manual for more information.



Send Email □

Email Linkage

Snapshot Linkage

The system can automatically take snapshots when an alarm event occurs. Follow the steps below to enable this functionality.

1. Navigate to the **Alarm Linkage** page.

2. Click ■ to enable snapshot linkage.

Snapshot □

Snapshot Linkage

Setting Up Exceptions

You can set up the system to inform you of exceptions and abnormalities. Abnormalities include issues related to the SD card, network, illegal access, voltage detection, and security exceptions.

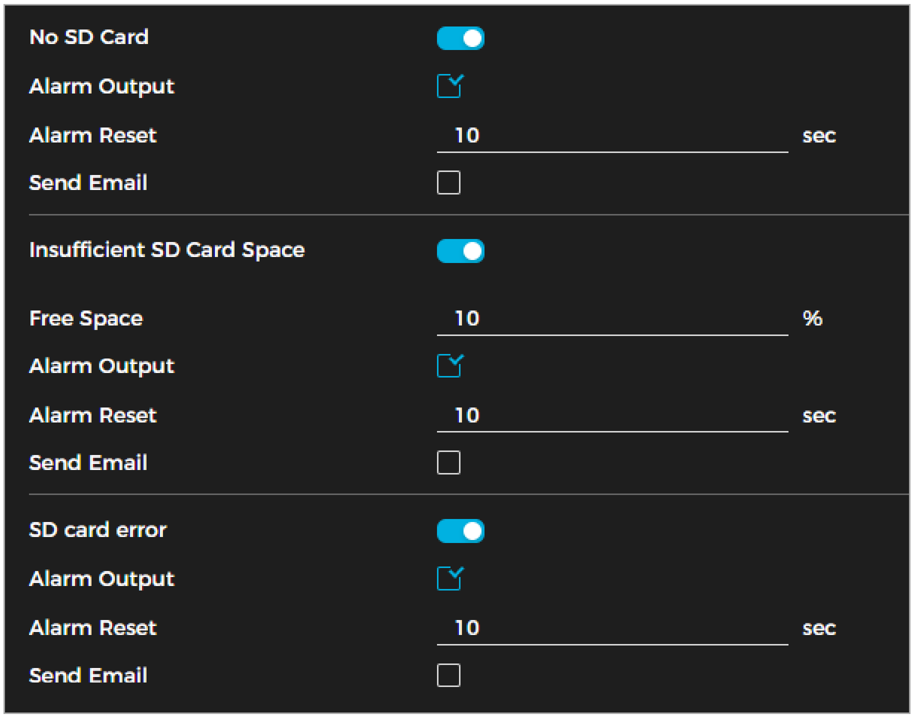
Setting Up an SD Card Exception

The system can perform alarm linkage events in the event of an SD card exception. Follow the steps below to have the system to inform you of an SD card exception.

ⓘ Functionality may vary depending on device model.

1. Navigate **Settings → Event → Exception**.

2. Click ○ to enable SD card detection functions. When enabling Insufficient SD Card Space, set the Free Space. When the remaining space on the SD card is less than this value, an alarm will trigger.



No SD Card ●
Alarm Output ☑
Alarm Reset 10 sec
Send Email □

Insufficient SD Card Space ●
Free Space 10 %
Alarm Output ☑
Alarm Reset 10 sec
Send Email □

SD card error ●
Alarm Output ☑
Alarm Reset 10 sec
Send Email □

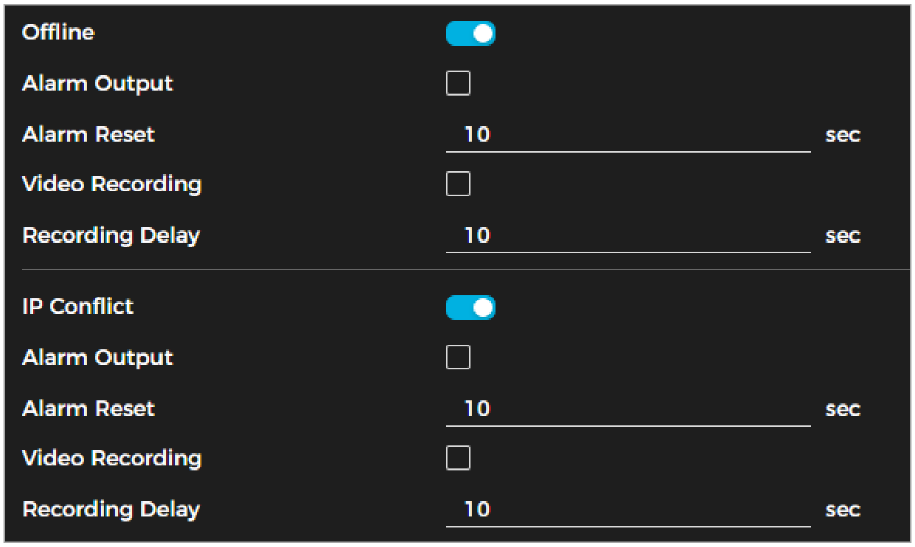
SD Card Exception

3. Set alarm linkage actions. See the **Alarm Linkage** portion of this manual for more information.
4. Click **Apply**.

Setting Up a Network Exception

The system can perform alarm linkage events in the event of a network exception (Network Offline and IP Conflict). Follow the steps below to have the system to inform you of a network exception.

1. Navigate to **Settings → Event → Exception**.
2. Click ○ to enable network detection functions.



Offline ●
Alarm Output □
Alarm Reset 10 sec
Video Recording □
Recording Delay 10 sec

IP Conflict ●
Alarm Output □
Alarm Reset 10 sec
Video Recording □
Recording Delay 10 sec

Network Exceptions

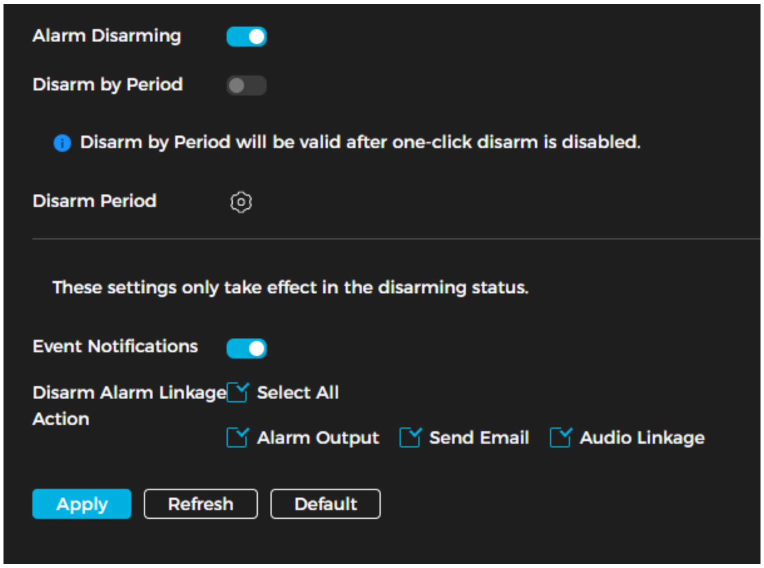
3. Set alarm linkage actions. See the **Alarm Linkage** portion of this manual for more information.
4. Click **Apply**.

Setting Up Alarms

Setting Up Disarming

The system allows you to disarm alarm linkage actions with one-click. By enabling **Event Notifications**, an alarm will only trigger based on the selected alarm linkage actions.

1. Navigate to **Settings → Event → Alarm → Disarming.**
2. Choose **Alarm Disarming** (stop triggering alarm linkage actions entirely) or **Disarm by Period** (stop triggering alarm linkage actions during specific times).



Alarm Disarming: on

Disarm by Period: off

Disarm by Period will be valid after one-click disarm is disabled.

Disarm Period

These settings only take effect in the disarming status.

Event Notifications: on

Disarm Alarm Linkage Action: ☑ Select All ☑ Alarm Output ☑ Send Email ☑ Audio Linkage

Disarming

3. Enable **Event Notifications**. Select **Disarm Alarm Linkage Action** as required.

ⓘ The disarm alarm linkage actions may vary by device. Currently, the supported actions include Alarm-out Port, Send Email, Audio Linkage, and Warning Light.

4. Click **Apply**.

Subscribing Alarms

Alarm Types

Alarm Type	Description	Function Enabled
Motion Detection	Triggered when a moving object is detected.	Motion detection
Disk Full	Triggered when percentage of SD card space free is less than the specified value.	SD card no space
Disk Error	Triggered when there is an SD card failure or malfunction.	SD card failure
Video Tampering	Triggered when the camera lens is obscured or out of focus.	Video tampering
External Alarm	Triggered when there is external alarm input.	Alarm input port and external alarm function
Audio Detection	Triggered when there is an audio input issue.	Abnormal audio detection

AI Event	Triggered when an intelligent rule is violated.	AI event, crowd map, face detection or people counting, and other intelligent functions
Scene Changing	Triggered when the monitoring scene changes.	Scene changing detection
Security Warning	Triggered when there is a security warning.	AI event, crowd map, face detection or people counting, and other intelligent functions

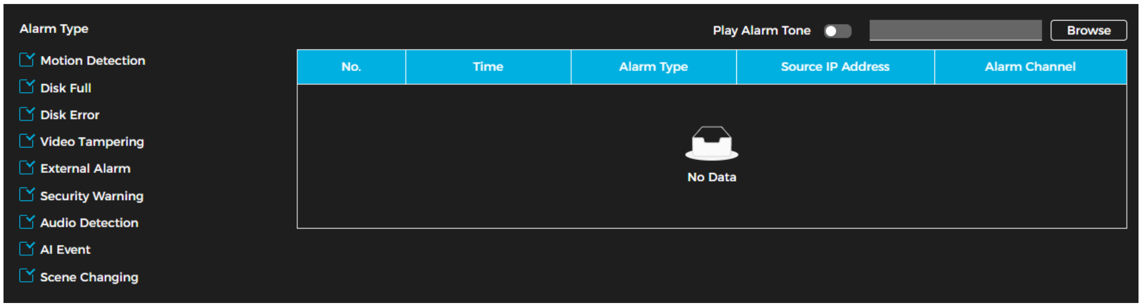
Subscribing Alarm Information

You can subscribe to alarm events. When a subscribed alarm event is triggered, the system logs detailed alarm information on the right side of the page.

ⓘ Functionality may vary depending on device model.

Follow the steps below to subscribe to an alarm event.

1. Navigate to **Settings → Event → Alarm → Subscribe Alarm.**
2. Choose an alarm type. See **Alarm Types** for more information.
3. Click ○ next to **Play Alarm Tone**.
4. Select the tone path. The system will play the selected audio file when the alarm is triggered.



Alarm Type

☑ Motion Detection
☑ Disk Full
☑ Disk Error
☑ Video Tampering
☑ External Alarm
☑ Security Warning
☑ Audio Detection
☑ AI Event
☑ Scene Changing

Play Alarm Tone ○ Browse

No.	Time	Alarm Type	Source IP Address	Alarm Channel

No Data

Subscribing to an Alarm

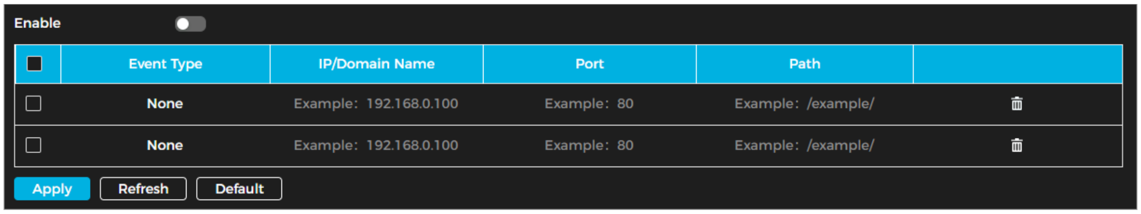
How to Set Up a Network Destination

You can select, enable, and configure a network destination to have the camera automatically upload AI function reports periodically. Follow the steps below to set up a network destination.

1. Navigate to **Settings → Event → Network Destination**.
2. Click ○ to enable the function.
3. Click + .
4. Set the parameters. You can add up to two network destinations. See the table below for more details.

Parameter	Description
IP/Domain Name	Enter the IP address and port number of the server where the report will be uploaded.
Port	
Path	Refers to the storage path of the server.
Event Type	Select the event type from the drop-down list. You can choose multiple types simultaneously. The event types available in the drop-down list match those in snapshot playback.

5. Click **Apply**.



Enable

□	Event Type	IP/Domain Name	Port	Path	
□	None	Example: 192.168.0.100	Example: 80	Example: /example/	🗑
□	None	Example: 192.168.0.100	Example: 80	Example: /example/	🗑

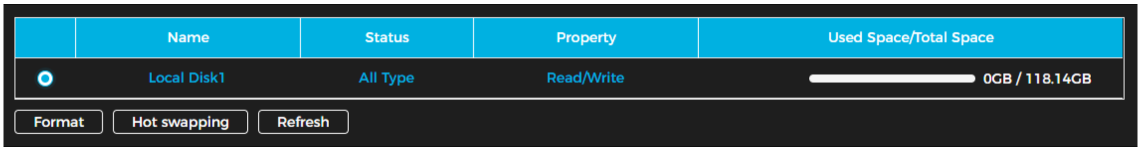
Set Up a Network Destination

Local Storage

Follow the steps below to display the information of the local SD card and format it.

ⓘ Functionality may vary depending on device model.

1. Navigate to **Settings → Storage → Local Storage.**
2. Click **Format**.
3. Click **Hot Swapping** to enable the functionality.



	Name	Status	Property	Used Space/Total Space
●	Local Disk1	All Type	Read/Write	0GB / 118.14GB

Local Storage

Appendix: 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).