LUMINYS

# Network Camera

User Manual

Rev. 1

# Foreword

## General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the network 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 | March 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

- Adhere to local electrical safety codes and standards, verifying the correct power supply before operating the device.
- Ensure the power supply meets **ES1 in IEC 62368-1** standards and does not exceed PS2. Verify power requirements on the device label.
- It is recommended to use the power adapter provided with the device.
- Do not connect the device to multiple power sources unless explicitly stated, as this may cause damage.
- Install the device in a location accessible only to trained professionals to prevent potential injury to unauthorized individuals. Professionals must be fully aware of all safety precautions and warnings associated with the device.
- Avoid applying excessive pressure, exposing the device to strong vibrations, or submerging it in liquid during installation.
- Ensure an emergency disconnect device is installed in an easily accessible location to allow for immediate power shutoff when necessary
- For enhanced lightning protection, use the device with a lightning protection device. In outdoor environments, strictly follow lightning protection regulations.
- Ground the functional earthing section of the device to enhance reliability. As a Class I electrical appliance, ensure the device is connected to a power socket with protective grounding.

  ⓘ Some models may not have designated earthing holes
- The dome cover is an optical component; avoid direct contact or wiping the surface during installation to prevent damage.

## Operation Requirements

- Never open the device cover while the device is powered on.
- Avoid touching the heat dissipation components to prevent the risk of burns.
- Use the device within the specified humidity and temperature ranges.
- Do not aim the device at strong light sources (e.g., lamps, sunlight) when focusing, as this may shorten the lifespan of the CMOS sensor and cause overbrightness or flickering.
- Do not expose the device to laser radiation.
- Do not allow liquid to enter the device.
- Protect indoor devices from rain and moisture to reduce the risk of electric shock or fire.
- Do not obstruct the ventilation openings near the device to prevent heat buildup.

- Ensure that the power cord and wires are not subject to pressure or walking on, especially at plugs, power sockets, and exit points from the device.
- Avoid direct contact with the photosensitive CMOS sensor. Use an air blower to clean the lens from dust or dirt.
- The dome cover is an optical component; avoid direct contact or wiping its surface.
- There may be a risk of electrostatic discharge on the dome cover. Always power off the device when installing the cover after adjusting the camera. Avoid touching the cover and ensure that it is not exposed to other equipment or individuals.
- Enhance the protection of the network, device data, and personal information. Implement necessary security measures such as using strong passwords, regularly updating passwords, keeping firmware updated, and isolating computer networks. For some older IP Camera firmware versions, the ONVIF password may not synchronize automatically after the main system password is changed; you will need to update the firmware or manually change the password.

## Maintenance Requirements

- Always follow the provided instructions when disassembling the device. Non-professionals attempting to dismantle the device may cause water leakage or poor image quality. If the device requires disassembly before use, ensure that the seal ring is properly seated in the seal groove when reassembling the cover. If condensation appears on the lens or the desiccant turns green after disassembly, contact after-sales service for desiccant replacement. (Desiccants may not be provided for certain models.)
- Only use manufacturer-approved accessories.
- Only allowed qualified personnel to install, maintain, and operate the device.
- Never touch the photosensitive CMOS directly. Use an air blower to remove dust or dirt from the lens. If cleaning is necessary, slightly moisten a soft cloth with alcohol and gently wipe away dirt.
- Clean the device body with a soft, dry cloth. For stubborn stains, use a cloth lightly dampened with neutral detergent and wipe the surface dry. Avoid using volatile solvents (e.g., ethyl alcohol, benzene, or diluent) or abrasive detergents, as these may damage the coating and degrade the device's performance.
- The dome cover is an optical component. If it becomes dirty with dust, grease, or fingerprints, use degreasing cotton lightly moistened with ether or a clean, soft cloth dipped in water to gently clean it. An air blower is also effective for removing dust.
- Cameras made from stainless steel may develop rust when exposed to corrosive environments (e.g., near the seaside or in chemical plants). To remove rust, use an abrasive soft cloth moistened with a mild acid solution (vinegar is recommended) and gently wipe the rust away. Then, wipe the surface dry.

# Table of Contents

# Introduction

## About the Device

IP cameras (Internet Protocol cameras) are categorized as either single-channel or multi-channel, based on the number of video channels they support. For multi-channel IP cameras, users can independently configure the settings for each individual video channel.

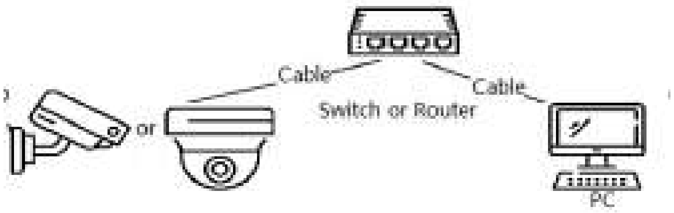
IP cameras are a type of digital video camera that transmits control data and image data over the internet. They are commonly used for surveillance, requiring only a local area network without the need for a local recording device.

## Unpacking

The equipment should be unpacked and handled carefully. If any item is found to be damaged, notify the shipper immediately. Ensure all parts are present; if anything is missing, contact Luminys customer service right away. The original packaging is the safest option for transporting the unit if it needs to be returned, so be sure to keep it for potential future use.

## Network Connection

Generally, an IP camera is connected to a PC through a network switch or router.



*General IP Camera Network Topology*

## Functions

Functions may vary based on device model.

### Basic Functions

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.

### Video Detection

- Includes motion detection, video tampering detection, and scene change detection.

- When an alarm is triggered, the system initiates linkages such as recording, alarm output, sending an email, PTZ operation, and snapshot.

## Exceptions

- Includes SD card error, network disconnection, illegal access, voltage detection, and security exceptions.
- When an SD card error or illegal access occurs, the system triggers alarm output and sends an email.
- When a network disconnection alarm is triggered, the system starts recording and activates alarm output.
- When the input voltage deviates from the rated voltage, an alarm is triggered, and the system sends an email.

## Alarm

- Set the alarm prompt mode and tone based on the type of alarm.
- View the alarm prompt messages.

## Record

- Automatically record according to the schedule.
- Playback recorded video and images as required.
- Download recorded video and images.
- Alarm-linked recording.

## 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

### VCA

- Line crossing, intrusion, abandoned object, moving object, fast moving, parking detection, people gathering, and loitering detection.
- When an alarm is triggered, the system performs actions such as recording, alarm output, sending an email, and taking a snapshot.

### Face Detection

- Detects faces and displays the related attributes.
- 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

- Captures people, non-motor vehicles, and vehicles, displaying the related information on the live page.
- The system links to alarm output when an alarm is triggered.

### People Counting

- Monitors the flow of people entering and exiting the detection area and generates a report.
- An alarm is triggered if the number of people or the duration of their stay exceeds the configured limit.

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

## Heat Map

- Measures the cumulative density of moving objects and displays the results using different colors.
- View the heat map report, which includes both the heat map and track map (track map is unavailable on budget fisheye cameras).

## LumiSearch

- Perform a fast and precise search on the selected NVR.

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

| 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 | |
| Reserved Email | 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. |

3. Click **OK**.

# Login

## Log in to the Webpage

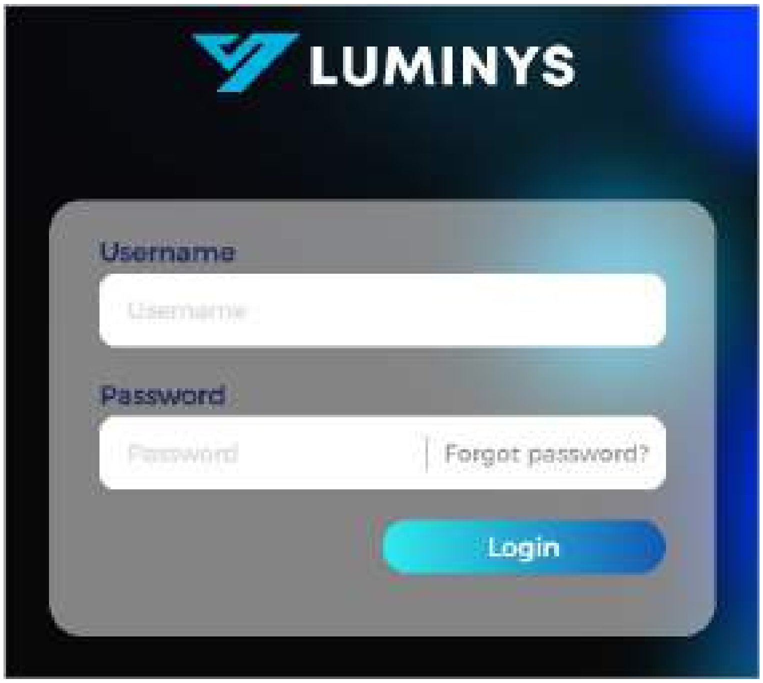
This section explains how to log in to the webpage, using Chrome as an example.

ⓘ

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

Follow the steps below to log in to the camera's web interface.

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



*Login Screen*

2. Enter the Device's login credentials. The default username is admin.
3. Hit **Login**.

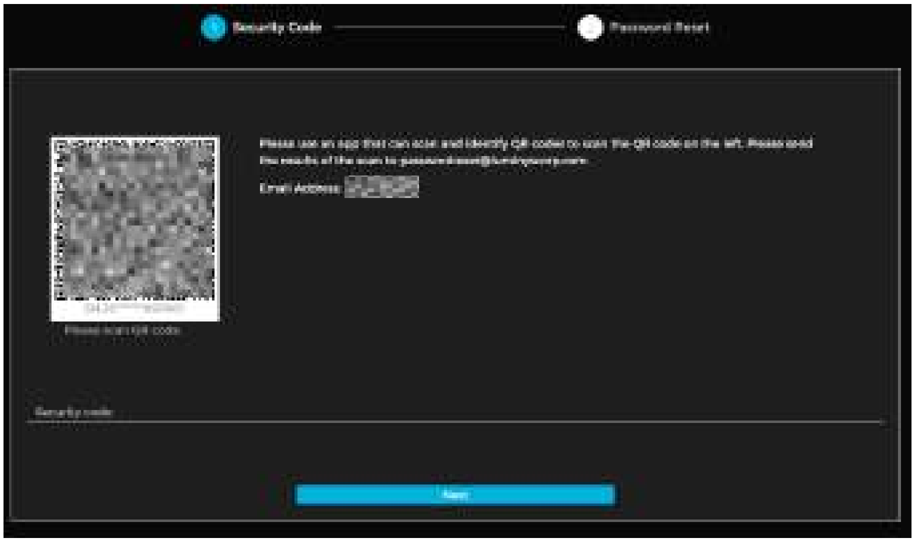
# Password Reset

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**.
4. Use an app with scanning and recognition functionality to 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.

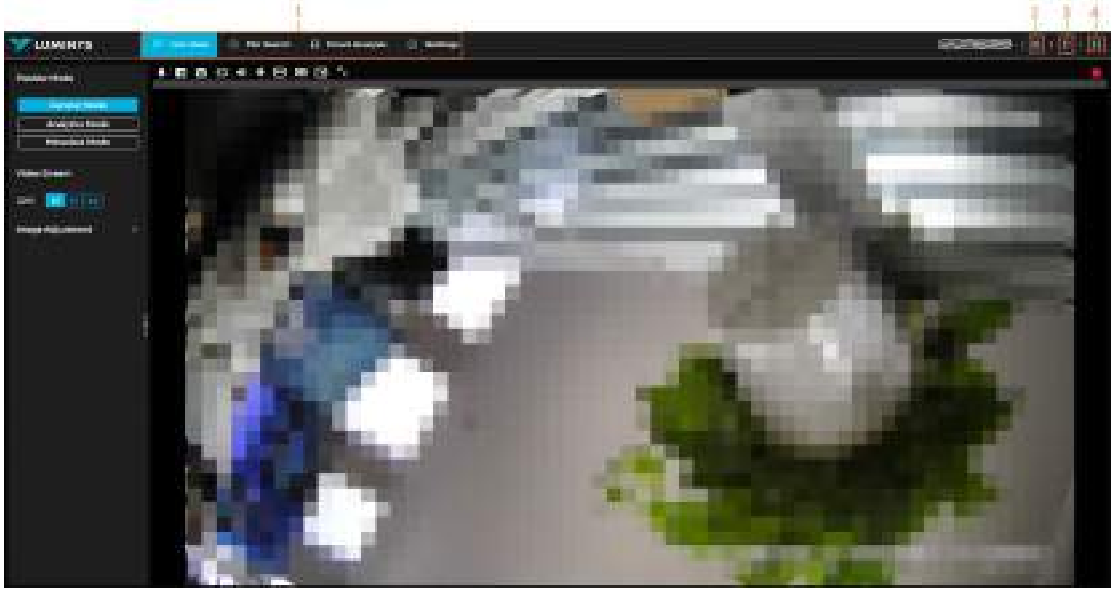


Please use an app that can scan and identify QR codes to scan the QR code on the left. Please send the results of the scan to passwordreset@luminyscorp.com

Email Address: [redacted]

*Password Reset*

# Homepage

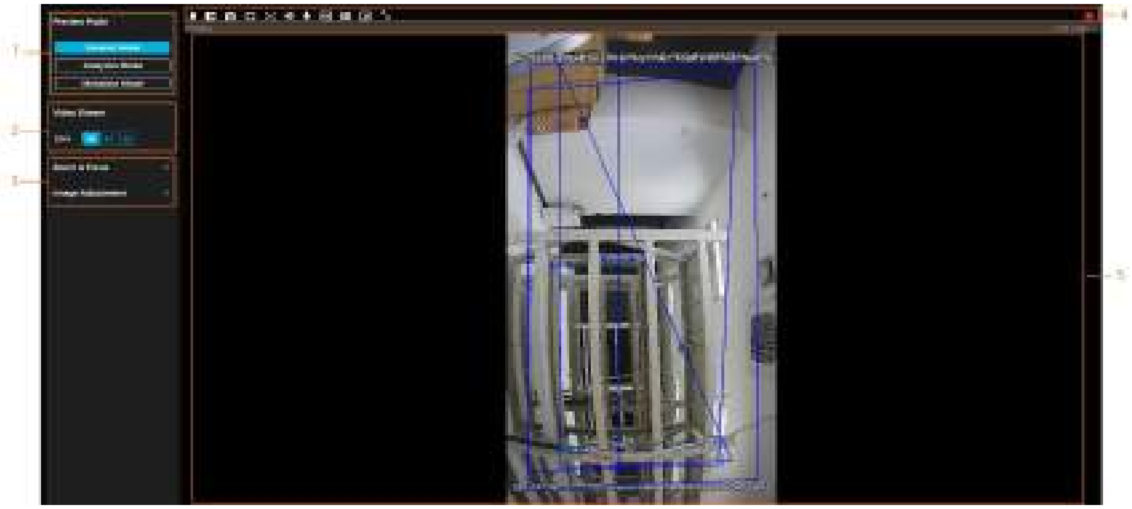


*LumiViewer Homepage*

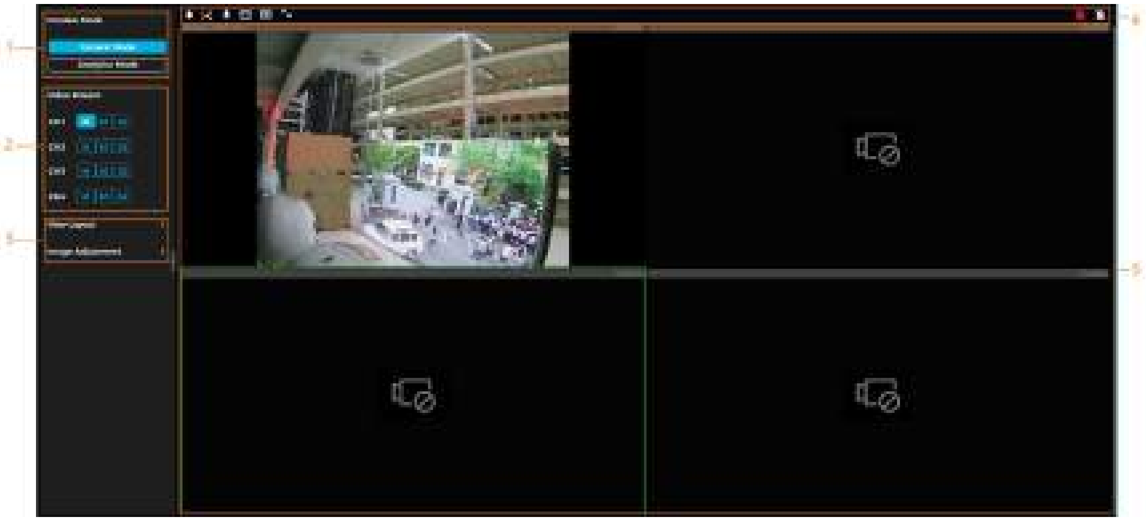
| Number | Function | Description |
|---|---|---|
| 1 | Function Tabs | • **Live View**: The Live View tab is displayed by default upon login. Options include General Mode, Analytics Mode, and Metadata Mode. Additionally, you can set the Video Stream and adjust your image for brightness and contrast.<br>• **File Search**: In the File Search tab you can configure Video Archive Search (Recording Settings, Storage, Schedule), Snapshot (Snapshot Archive Search, Snapshot Settings, Storage, Schedule and Network Destination), and Smart Report (Video Metadata, People Counting Report, and Heat Map).<br>• **Smart Analysis**: The File Search tab offers the ability to toggle ON or OFF for Face Detection, Heat Map, VCA, People Counting, Video Metadata, and Object Monitoring.<br>• **Settings**: In the Settings tab you can configure Local Settings, System, Network, Video/Audio/Image/LumiTracking, Event, and Storage. |
| 2 | QR Code | • Scan the **Mobile APP Download** QR code to download the LumiViewer APP.<br>• Scan the **Device SN** QR code with the LumiViewer APP to add the device to LumiViewer. |
| 3 | Restart and Logout | Click to log out or restart the device. |
| 4 | Full Screen | Click to display in full screen mode. |

# Live View

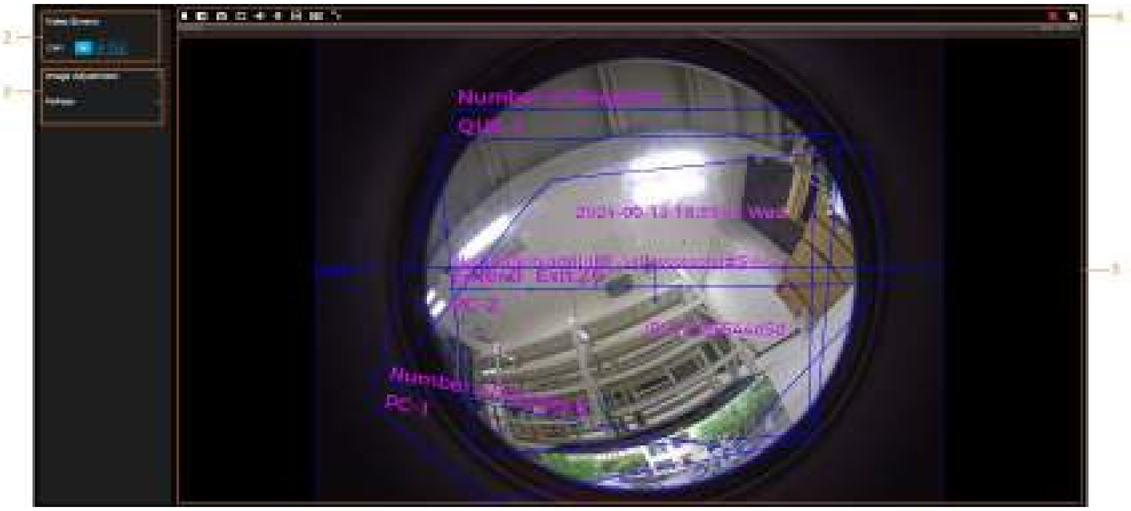
Real-time monitoring can be viewed from the Live View tab on the webpage.



*Single Channel Live View Mode*



*Multiple Channels Live View Mode*



*Live View (EPTZ)*

| Number | Function | Description |
|---|---|---|
| 1 | Display Mode | You can choose from the following display modes: General Mode, Analytics Mode, and Metadata Mode. |
| 2 | M (Main Stream) | A primary stream that provides high-quality video. High bit stream value and image with high resolution but requires large bandwidth. This option can be used for storage and monitoring. |
| | S1 (Sub Stream 1) | A secondary stream that provides low-quality video but is optimized for bandwidth efficiency. This option is normally used to replace the mainstream when there is not enough bandwidth |
| | S2 (Sub Stream 2) | |
| 3 | Image Adjustment | Adjustment operations for live viewing. |
| 4 | Live View Function Bar | Functions and operations for live viewing. |
| 5 | Live View | Shows real-time monitoring images. |

## Live View Function Bar Descriptions

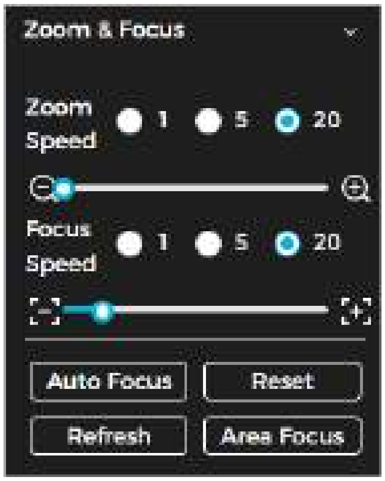
| Icon | Function | Description |
|---|---|---|
| 🔔 | Sound Alarm | Displays the status of the alarm sound. Click the icon to enable or disable the sound of the alarm. |
| ⊕ | Digital Zoom | There are two ways to zoom in on a selected area of a video image.<br>• Click the icon highlighted in the figure 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.<br>• Click the icon highlighted in the figure above. Next, scroll the mouse wheel in the video to zoom in or out. |
| 📷 | Snapshot | Click the icon to capture an image and save it to the configured storage path. |
| 🎥 | Record | Click the icon to start recording the video. It will be saved to the designated storage path. |
| 🔊 | Audio Output | Click the icon to enable or disable audio output. |
| 🎙 | Two-Way Talk | Click the icon to enable or disable the audio talk. |
| 💡 | Warning Light | Click the icon to enable or disable the warning light. |
| ⊕ | LumiTracking | Click the icon to enable or disable LumiTracking. |
| ↔ | W:H | Click the icon to restore the original ratio or adjust the ratio. |
| ▣ | AI Rule | Click the icon, then select Enable to display AI rules and the detection box. Select Disable to stop the display.<br>ⓘ It is enabled by default. |
| ▣ | Intelligence Area | Click the icon, then select Enable to display the intelligence area. Select Disable to stop the display. |

| | | |
|---|---|---|
| ⤢ | Full Screen | Click the icon to enter full-screen mode. Double-click or press Esc to exit. |
| 🚨 | Alarm Output | Click the icon to enable or disable the alarm output linkage. |

# Window Adjustment Bar

## Zoom and Focus

Click **Zoom & Focus** on the left side of the Live View page to adjust the focal length and zoom in or out of the video image. You can change image clarity or correct adjustment errors by manually or automatically adjusting the focus or focusing within a specific area. The focus will automatically adjust when zooming.



Zoom Speed ○ 1 ○ 5 ● 20

Focus Speed ○ 1 ○ 5 ● 20

*Zoom and Focus Parameters*

| Parameter | Description |
|---|---|
| Zoom Speed | Adjust the focal length of the camera to zoom in or out the image.<br>1. Set the speed value. Zoom Speed determines the adjustment range per click. A higher value will zoom in or out more with each click.<br>2. Click or hold the + or – button or drag the slider to adjust the zoom. |
| Focus Speed | Adjust the optical back focal length to improve image clarity.<br>1. Set the speed value. The Focus Speed determines the adjustment range per click. A higher value results in more adjustment per click.<br>2. Click or hold the + or – button, or drag the slider to adjust the focus. |
| Auto-Focus | Automatically adjusts the image clarity. During the auto-focus process, no other changes should be made. |
| Reset | Restores the focus to its default value and corrects any errors. You can restore the focus if the image appears unclear or if excessive zooming has occurred. |
| Refresh | Update the zoom setting of the camera to the latest setting. |
| Area Focus | Select the area to focus on by clicking Area Focus, and the camera will automatically adjust the focus in that selected region. |

## Image Adjustment

Click the Live View tab. Then, select Image Adjustment on the menu. To adjust the image parameters, (brightness, contrast, hue, and saturation), click the + or – button, or drag the slider bar. Press the Reset button to return to the factory default values.

The Image Adjustment display is only available through the web page and will not adjust the camera parameters.

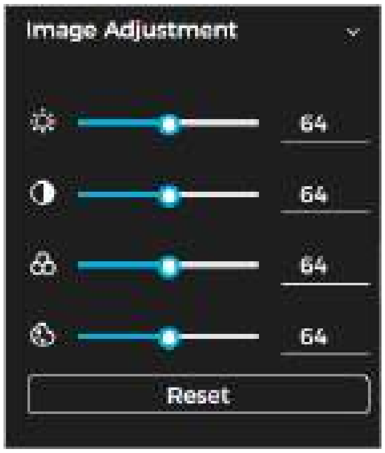


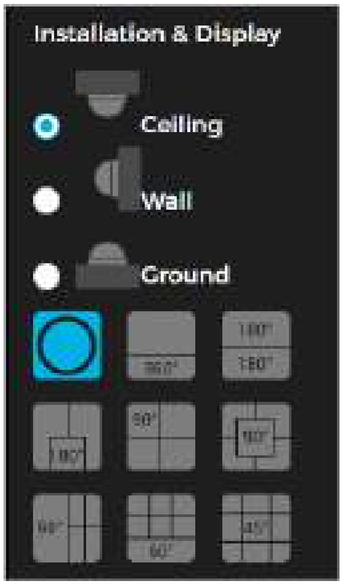
*Image Adjustment*

- ☼: The **Brightness** icon displays a slider bar to adjust the brightness of the image. There will be equal parts of bright and dark areas.
- ◐: The **Contrast** icon displays a slider bar to adjust the image brightness.
- ⊛: The **Saturation** icon displays a slider bar to adjust the image saturation. This does not change the brightness of the image.
- 🎨: The **Hue** icon displays a slider bar to adjust the colors. The default value is created based on the light sensor.
- Click the reset button to restore the default values.

## Fisheye

There are 3 mode options for fisheye devices: installation mode, display mode, and 3D mode.

- **Installation Mode**: Installation mode is recommended when setting up the camera and should be selected according to the user's requirements.
- **Display Mode**: For live viewing, select the display mode.



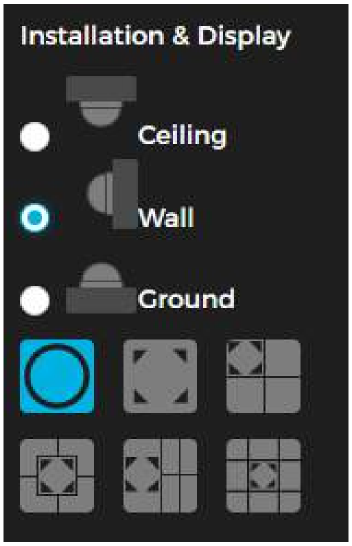
Installation & Display

● Ceiling

○ Wall

○ Ground

*Fisheye Options for Ceiling Mount*



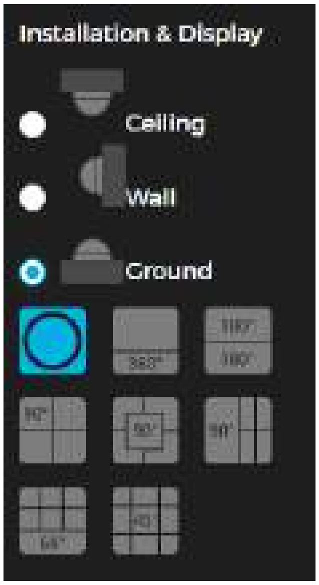
Installation & Display

○ Ceiling

● Wall

○ Ground

*Fisheye Options for Wall Mount*



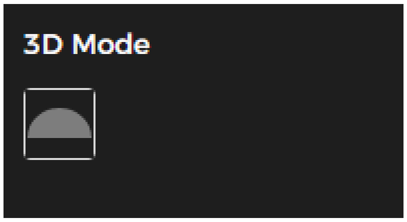
Installation & Display

○ Ceiling

○ Wall

● Ground

*Fisheye Options for Ground Mount*


3D Mode

*3D Mode*

| Parameter | Description | |
|---|---|---|
| Installation Mode | The installation mode offers 3 modes: ceiling, wall, and ground mount | |
| Display Mode | The display model of the current image varies depending on the installation mode. By default, the image will be shown at its original size when switched to installation mode.<br>• **Ceiling**: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8.<br>• **Wall**: 1P, 1P+3, 1P+4, 1P+8.<br>• **Ground**: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8. | |
| Ceiling/Wall/Ground Mount | ○ Original Image | Image before any correction. |
| Ceiling/Ground Mount | 360° 1P+1 | The 360° rectangular panoramic image screen features independent sub-screens.<br>You can zoom or drag the image across all screens.<br>You can move the starting point (left and right) on the rectangular panoramic image screen. |
| | 180° 180° 2P | Two connected 180° rectangular image screens form a 360° panoramic image, also known as a dual-panoramic image.<br>You can move the starting point (left and right) on both rectangular image screens, with the two screens linked together. |
| | 180° 1+2 | The original image screen with two independent sub-screens. This display mode is not supported for ground mounting.<br>You can zoom or drag the image on all screens.<br>You can rotate the image on the original image screen to adjust the starting point. |
| | 90° 1+3 | The original image screen with three independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can rotate the image on the original image screen to adjust the starting point. |

| | | |
|---|---|---|
| | 90°, 90° 1+4 | The original image screen with four independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can rotate the image on the original image screen to adjust the starting point. |
| | 60° 1P+6 | 360° rectangular panoramic screen with six independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can adjust the starting point (left and right) on the rectangular panoramic image screen. |
| | 45° 1P+8 | Original image screen with eight independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can rotate the image on the original image screen to adjust the starting point. |
| Wall Mount | 1P | 180° rectangular panoramic image screen (from left to right).<br>You can move the image on all screens (up and down) to adjust the vertical view. |
| | 1P+3 | 180° rectangular panoramic image screen + three independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can move the image on all screens (up and down) to adjust the vertical view. |
| | , 1P+4 | 180° rectangular panoramic image screen + four independent sub-screens.<br>You can zoom or drag the image on all screens.<br>You can move the image on all screens (up and down) to adjust the vertical view. |
| | 1P+8 | 180° rectangular panoramic image screen + eight independent sub-screens.<br>You can zoom or drag the image across all screens.<br>You can move the image on all screens (up and down) to adjust the vertical view. |
| 3D Mode | Semi Circle | You can drag the image in any direction (up, down, left, or right). Press I to display the panorama and O to restore the original size. |

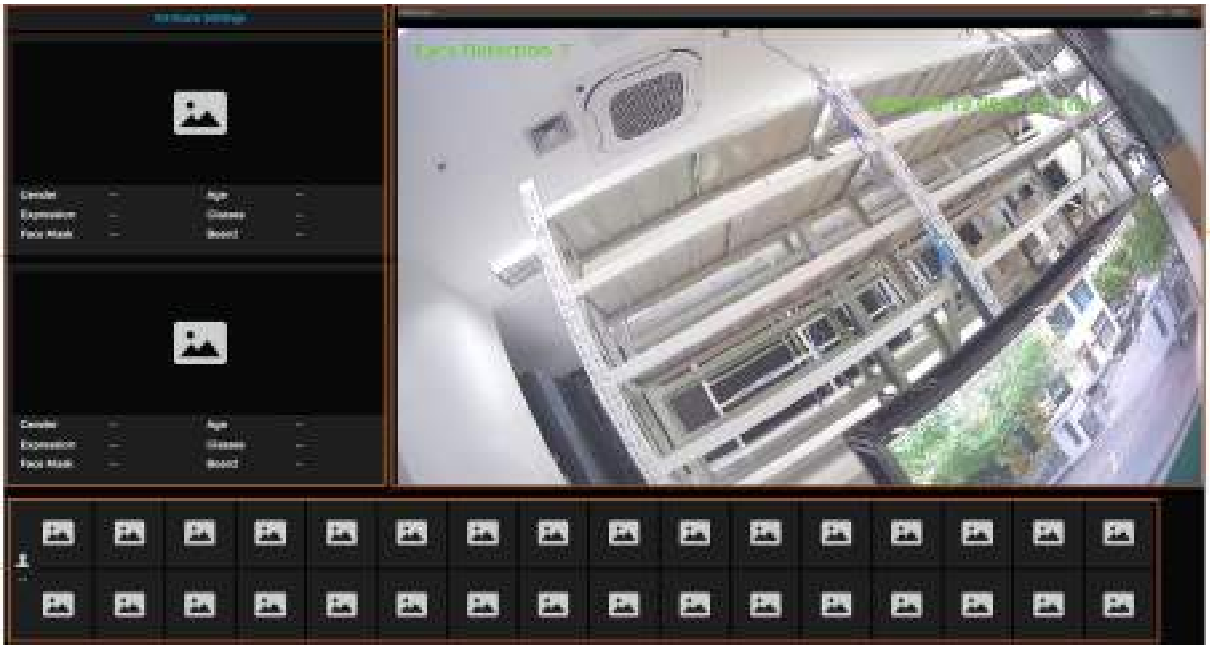
|  |  |  |
|---|---|---|
|  |  | Press S to rotate the image counterclockwise and E to stop the rotation.<br>Use the mouse wheel to zoom in or out. |

# Display Mode

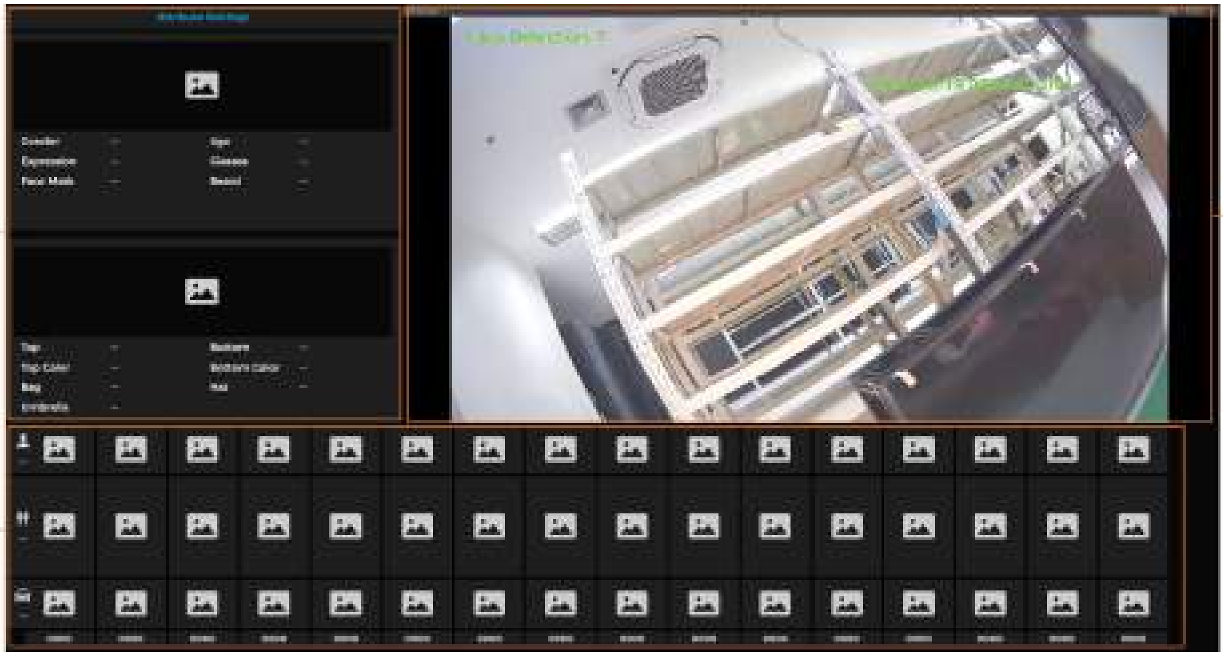
This section covers **Analytics Mode** and **Metadata Mode**.  Choose between General Mode, Analytics Mode, and Metadata Mode. For details on General Mode, refer to the Live View section of this manual.

ⓘ

- Pages may vary based on model.
- Ensure corresponding functions are enabled.



*Analytics Mode*



*Metadata Mode*

| Number | Function | Description |
|---|---|---|
| 1 | Details | Shows the captured image and its details. Click Attribute Settings to configure the displayed attributes. |
| 2 | Captured Image | Shows the captured images. Click a snapshot in the area to view its details. |
| 3 | Live View | Shows the real-time monitoring image. |

# 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.

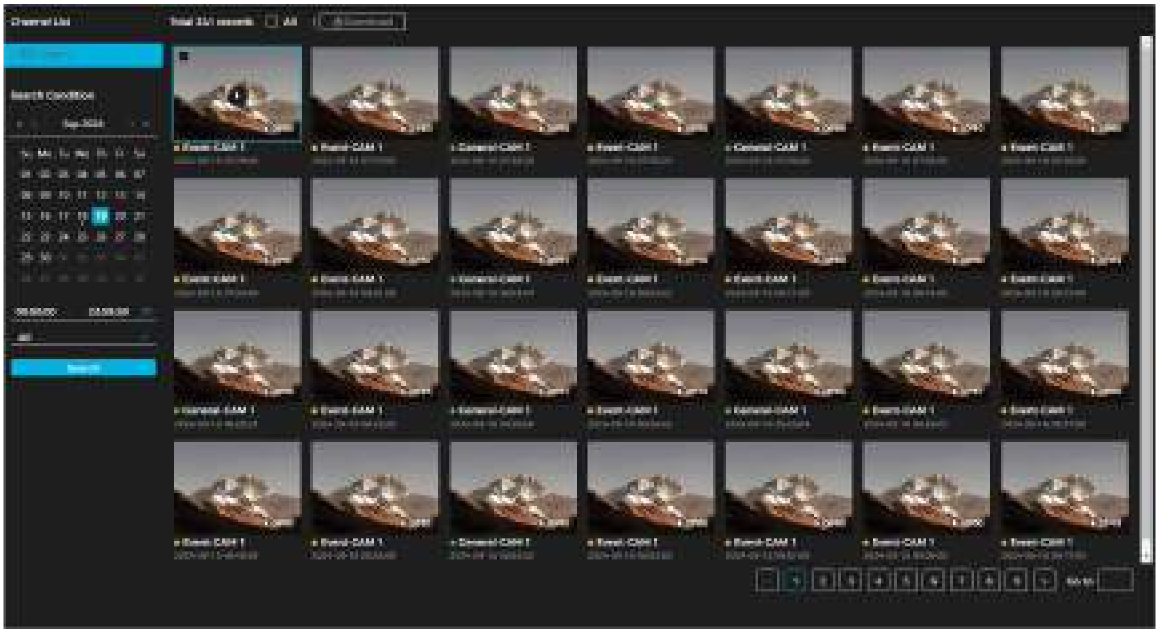
Follow the steps below to play back a video.

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

ⓘ

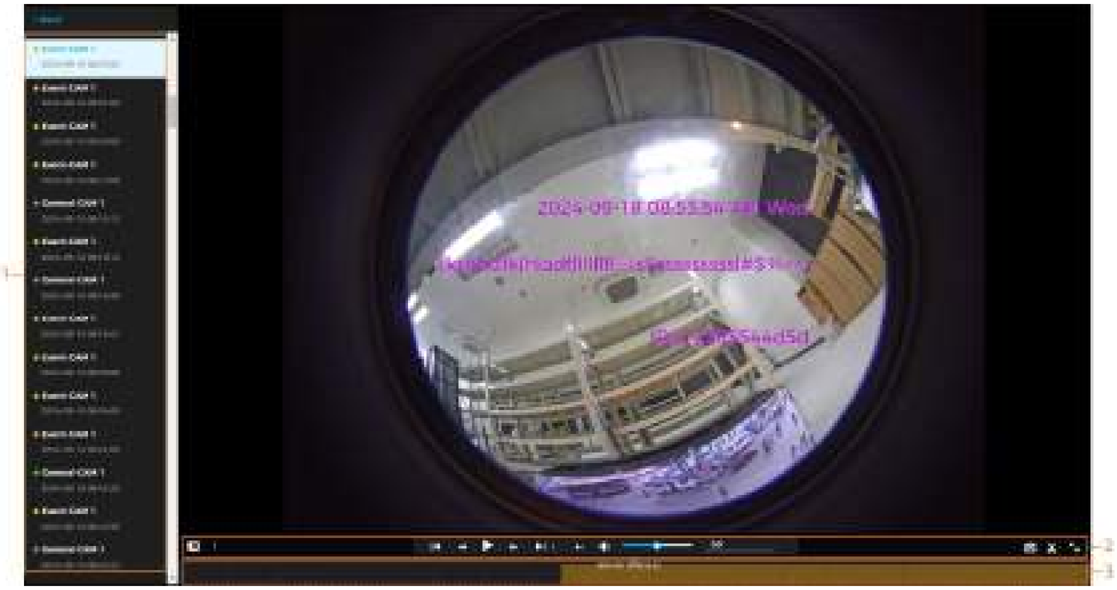
- When choosing Event as the record type, you can specify event types like Motion Detection, Video Tampering, and Scene Changing.
- Days with recorded video are marked with a green dot.

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*

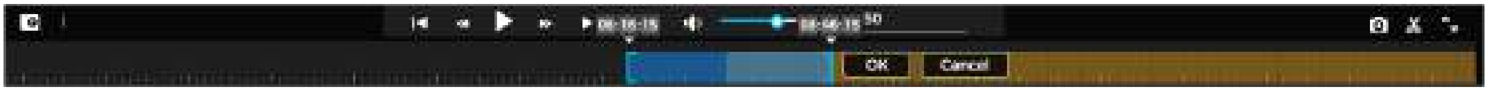
| Number | Function | | Description |
|---|---|---|---|
| 1 | Recorded Video List | | Displays all searched recorded video files. Click any file for playback. Click **Back** at the upper-left corner to go to the Video Archive Search page. |
| 2 | Digital Zoom | | There are two ways to zoom in on a selected area of a video image.<br>• 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.<br>• 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.<br>- Click any point in the colored area to start playback from that moment.<br>- Each recording type is represented by a specific color, which can be referenced in the Record Type bar. |

## How to Clip a Video

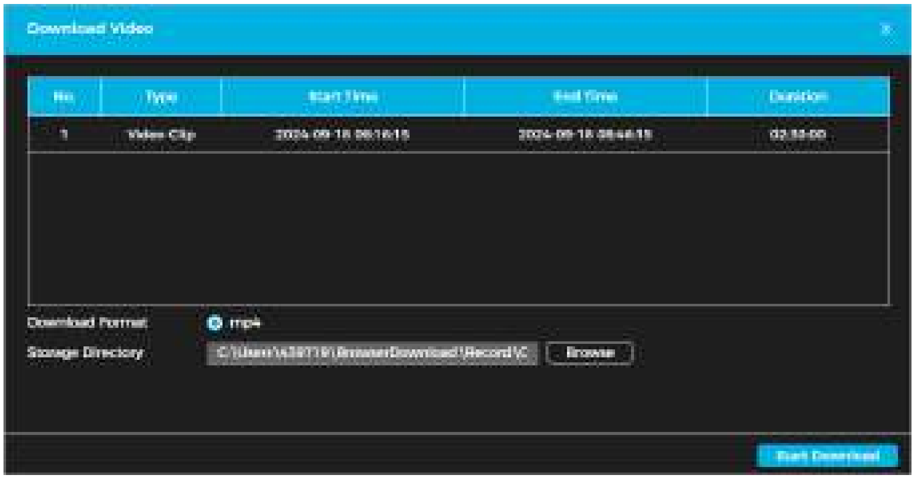
Follow the steps below to clip a video.

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 08:16:15 | 2024-09-18 08:46:15 | 02:30:00 |

Download Format ● mp4

Storage Directory C:\Users\638719\BrowserDownload\Record\C Browse

*Download Video Screen*

5. Click **Start Download**.

## How to Download a Video

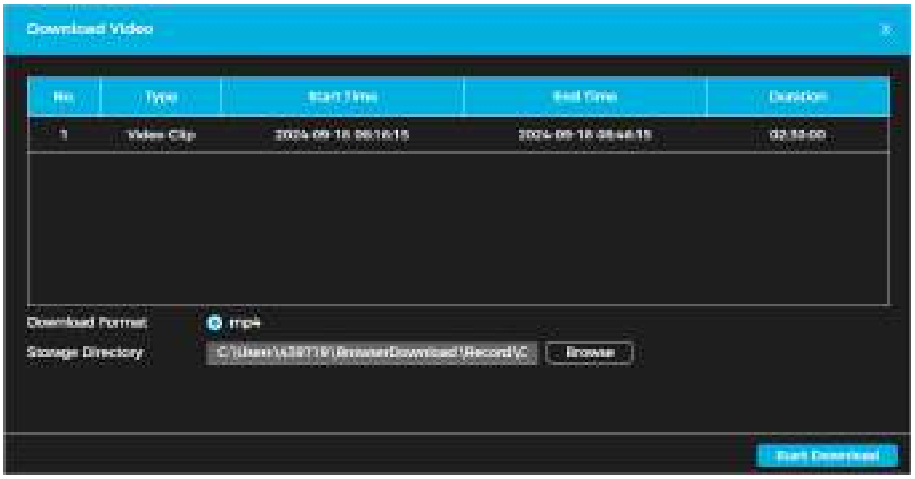
Videos can be downloaded individually or as a batch. Follow the steps below to download a video to a defined path.

ⓘ

- 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.
5. 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\[illegible]\BrowserDownload\Record\C

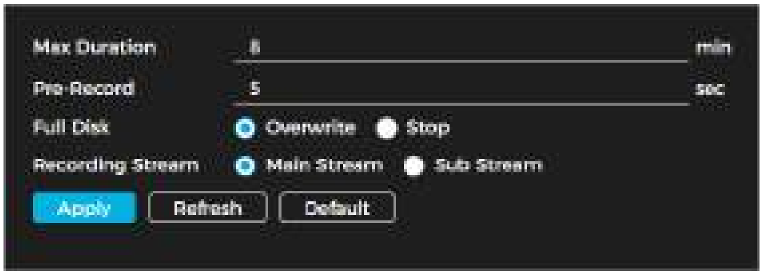
*Download Video Screen*

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.<br>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.<br>• **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**. |

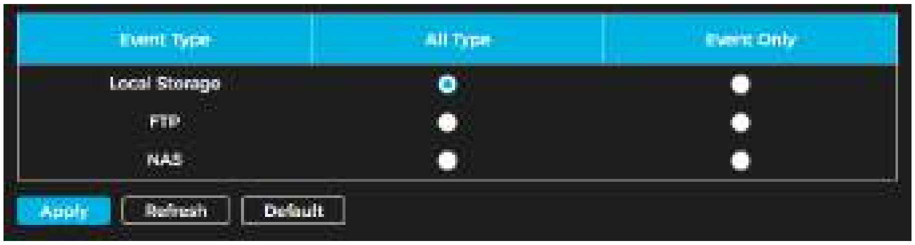
3. Click **Apply**.

# 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

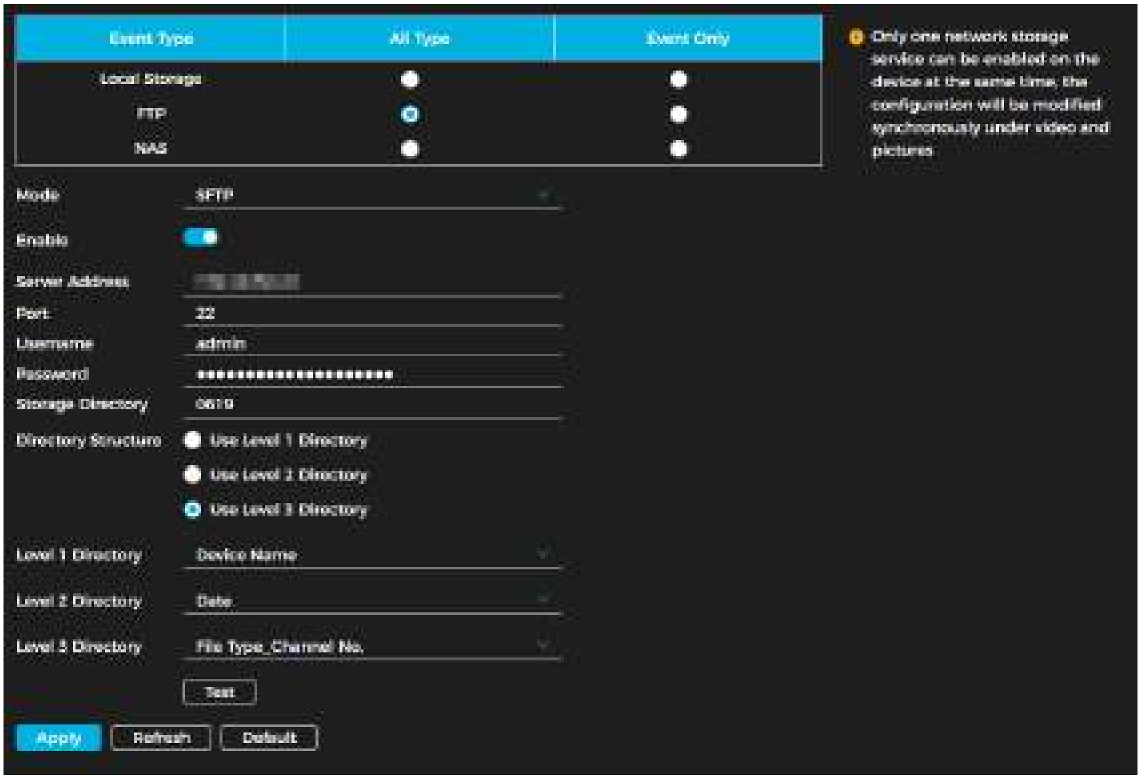
You can store videos on the network using an FTP or NAS server. In case of a network error, videos can be backed up using the internal SD card.

### 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 | [redacted] |
| Port | 22 |
| Username | admin |
| Password | •••••••••••••••••••• |
| Storage Directory | 0619 |
| Directory Structure | ○ Use Level 1 Directory<br>○ Use Level 2 Directory<br>◉ Use Level 3 Directory |
| Level 1 Directory | Device Name |
| Level 2 Directory | Date |
| Level 3 Directory | File Type_Channel No. |

*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. |
| Directory Structure | Configure the directory structure by selecting Use Level 1 Directory, Use Level 2 Directory, or Use Level 3 Directory. |
| Level 1 Directory | Set the Device Name, Device IP, or Automatic. If Automatic is selected, enter a custom directory name. |
| Level 2 Directory | Set the File Type, Channel No., Date, File Type_Channel No., or Automatic. If Automatic is selected, enter a custom directory name. |
| Level 3 Directory | |

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.

| Parameter | Description |
|---|---|
| Server Address | NAS server IP address. |
| Username | The username and pass required when using the SMB protocol. |
| Password | |
| Storage Directory | NAS server destination path. |

4. Click **Apply**.

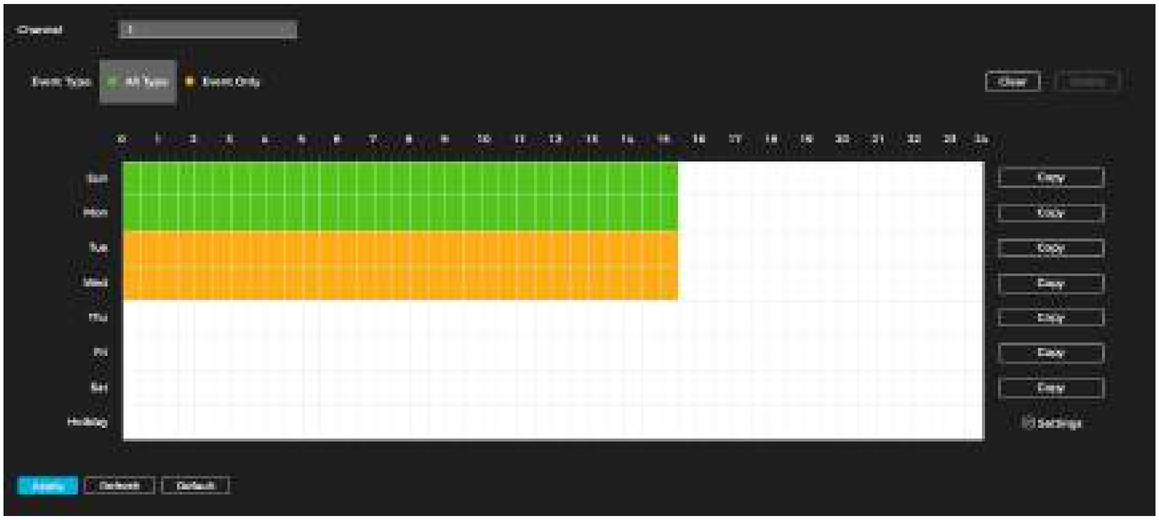
## How to Set the Recording Plan

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**.



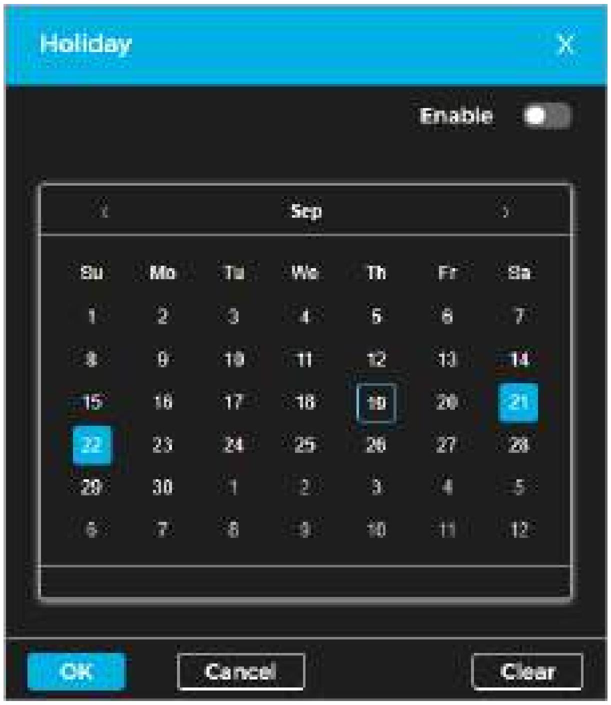
*Recording Plan Schedule*

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.

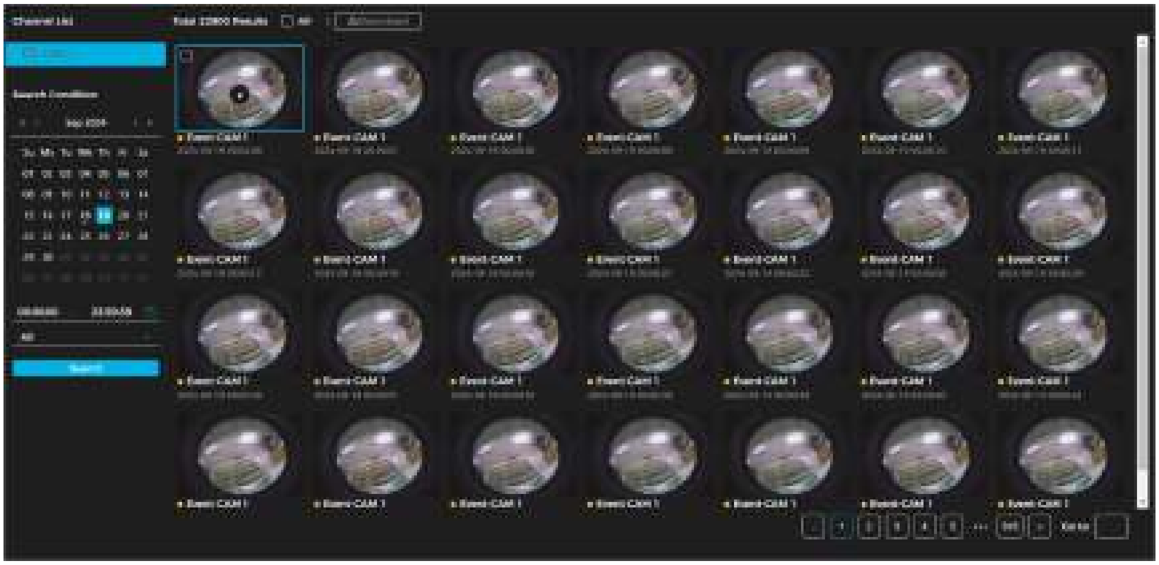
Follow the steps below to play back a snapshot.

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

ⓘ

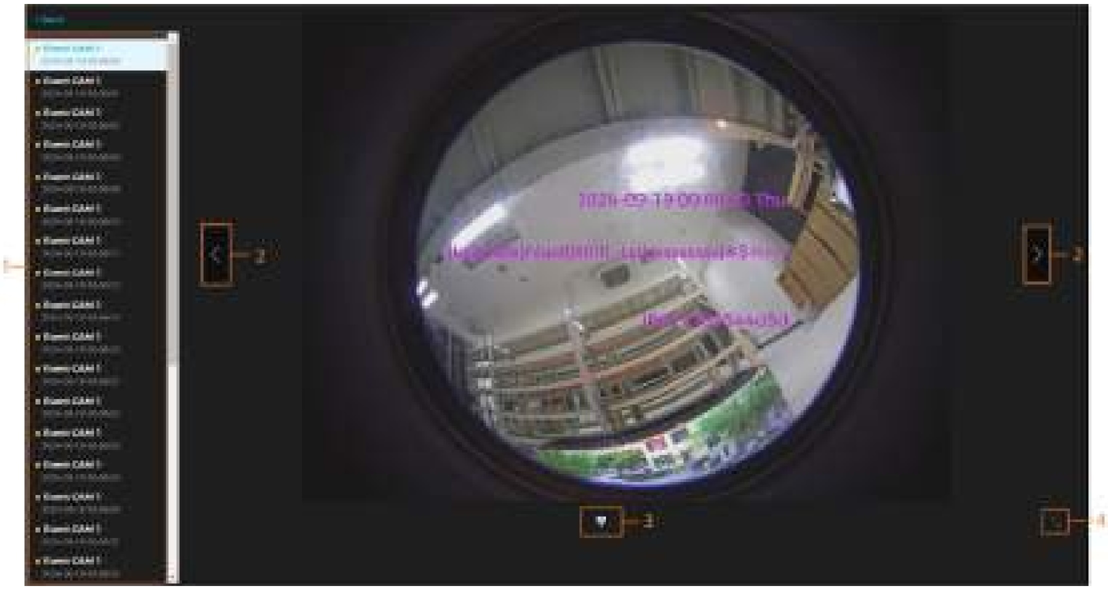
- When choosing Event as the record type, you can specify event types like Motion Detection, Video Tampering, and Scene Changing.
- Days with recorded video are marked with a green dot.

3. Click **Search**.



*Picture Search*

4. Click ▶ to play back the desired snapshot.



*Snapshot Playback*

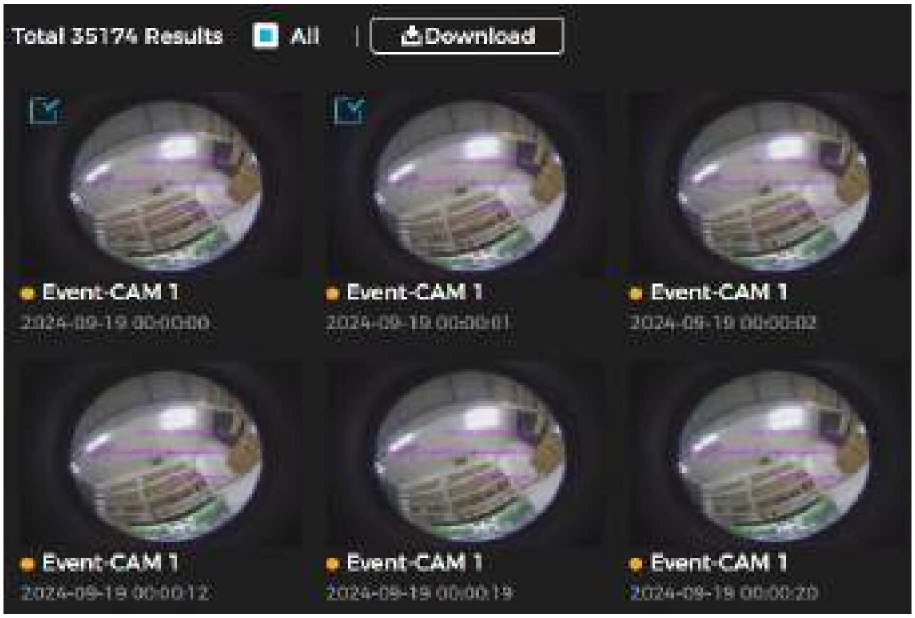
| Number | Function | Description |
|---|---|---|
| 1 | Snapshot List | Displays all the searched snapshots. Click on any file to play it back.<br>Click Back in the upper-left corner to return to the Snapshot Archive Search page. |
| 2 | Manual Display | ‹ displays the previous snapshot in the snapshot list.<br>› 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
2024-09-19 00:00:00

Event-CAM 1
2024-09-19 00:00:01

Event-CAM 1
2024-09-19 00:00:02

Event-CAM 1
2024-09-19 00:00:12

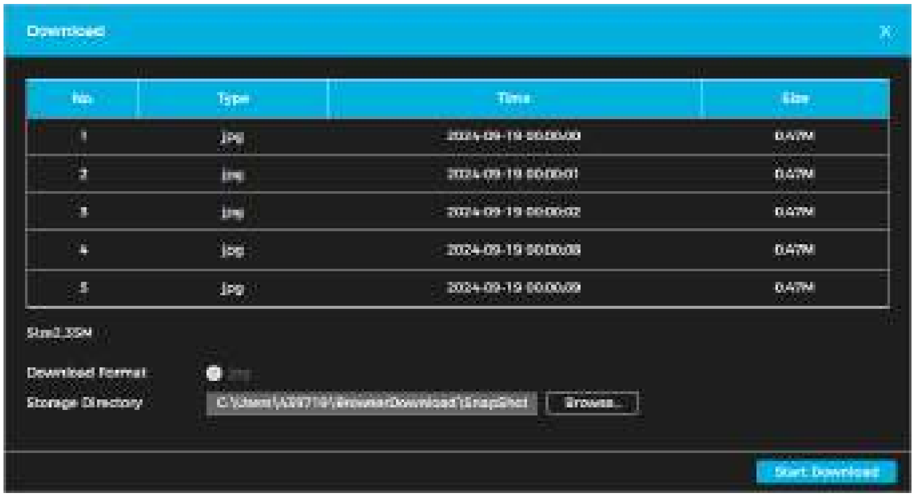
Event-CAM 1
2024-09-19 00:00:19

Event-CAM 1
2024-09-19 00:00:20

*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\A39719\BrowserDownload\SnapShot

*Download Snapshot Screen*

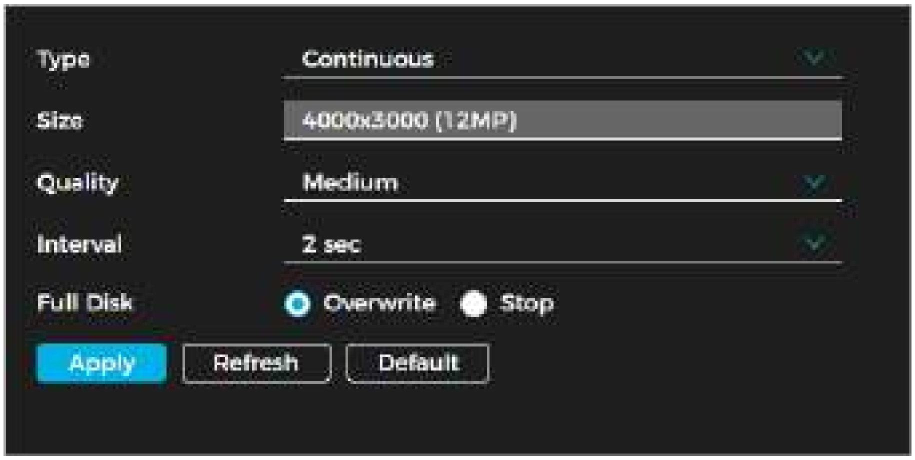
7. Click **Start Download**.

# 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**.<br>• **Continuous**: Captures images within the configured period.<br>• **Event**: Captures images when a configured event, such as Motion Detection, Video Tampering, or Scene Changing, is triggered.<br>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.<br>• **Stop**: When the disk is full, the recording is stopped, and no additional video can be recorded until space becomes available. |

3. Click **Apply**.

## Storage

Configure the snapshot storage method. 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**.

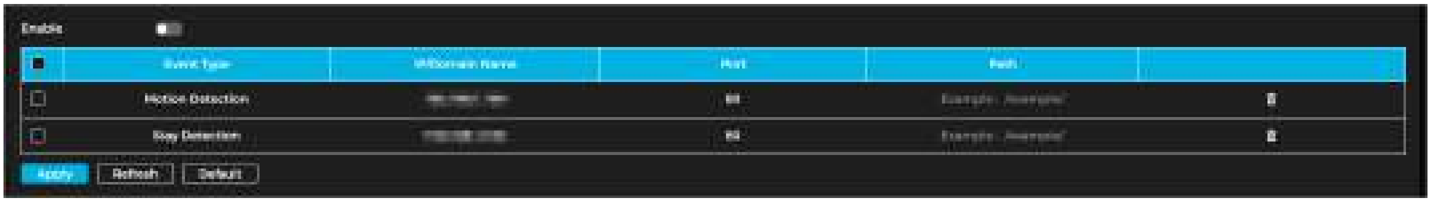
## How to Set a Network Destination

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*

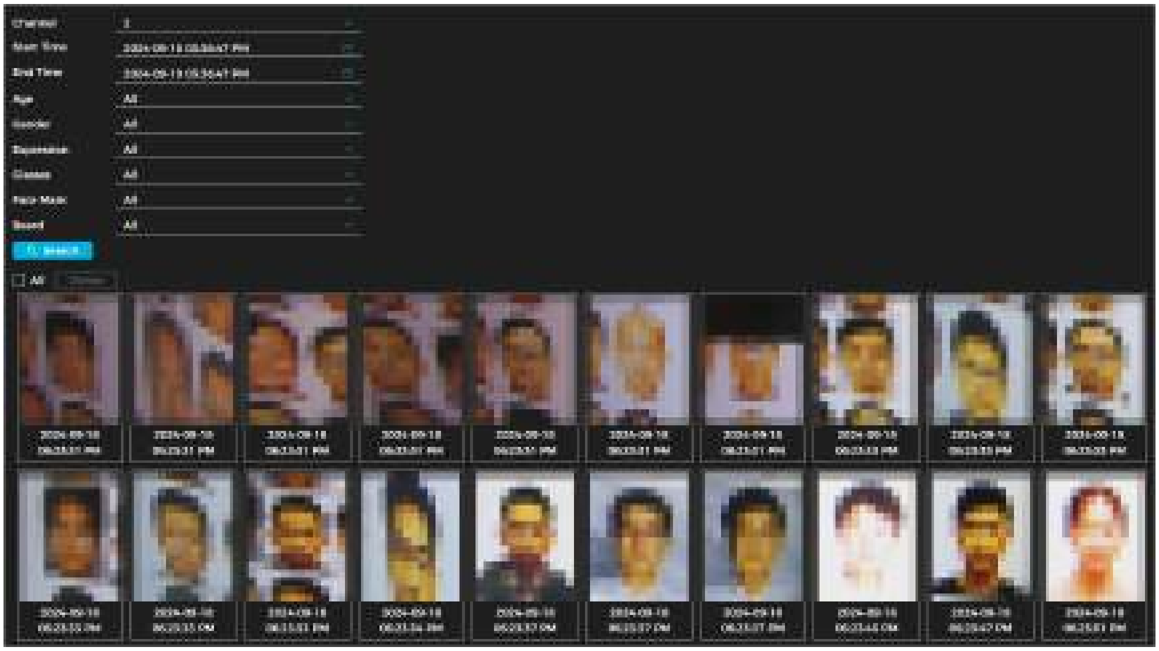
| Parameter | Description |
|---|---|
| IP/Domain Name | Enter the IP address and port number of the server where the report will be uploaded. |
| Port | |
| Enable | Click ○ to enable the function. |
| Path | Refers to the storage path of the server. |
| Authentication | Enable this function and enter 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 Search: Face Detection

Follow the steps below to search for face recognition or snapshot results using images. Ensure an SD card is installed prior to searching.

1. Navigate to **File Search → Smart Search → Face Detection Search**.
2. Select the channel and set the time for the report.
3. Set the face attributes (age, gender, expression, glasses, face mask, beard).
4. Click **Search**.
5. Select a picture to view the details.



Channel [illegible]
Start Time [illegible]
End Time [illegible]
Age All
Gender All
Expression All
Glasses All
Face Mask All
Beard All

*Face Detection Search*

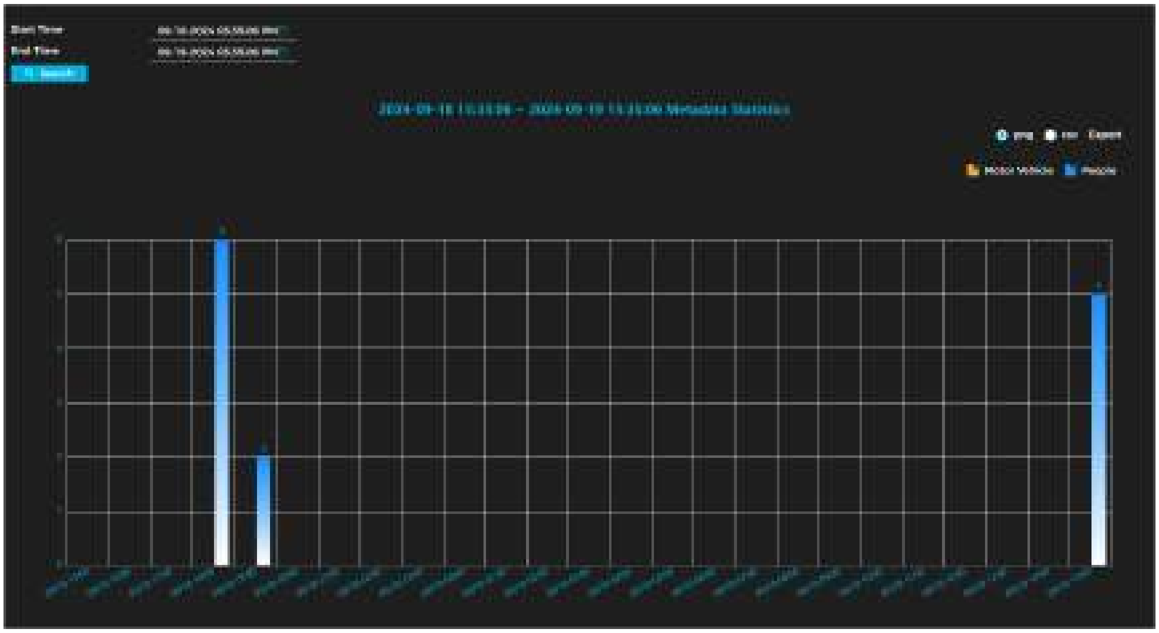
# Smart Report

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**.



*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.

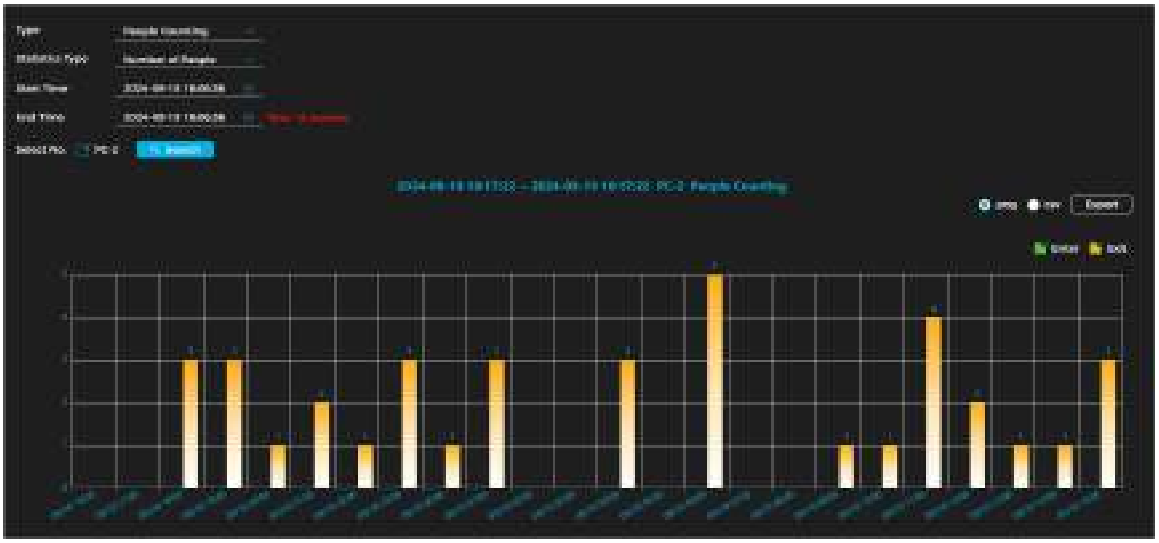
| Parameter | Description |
|---|---|
| Type | Select the desired type, then choose the corresponding statistics type based on the selected option. |

| | |
|---|---|
| Statistics Type | - **Number of People**: Displays the report on the number of people who meet the specified conditions.<br>- **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.<br>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.<br>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.<br>- For **People Counting**, reports can be viewed daily, weekly, monthly, or yearly, with an option to customize the period.<br>- 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

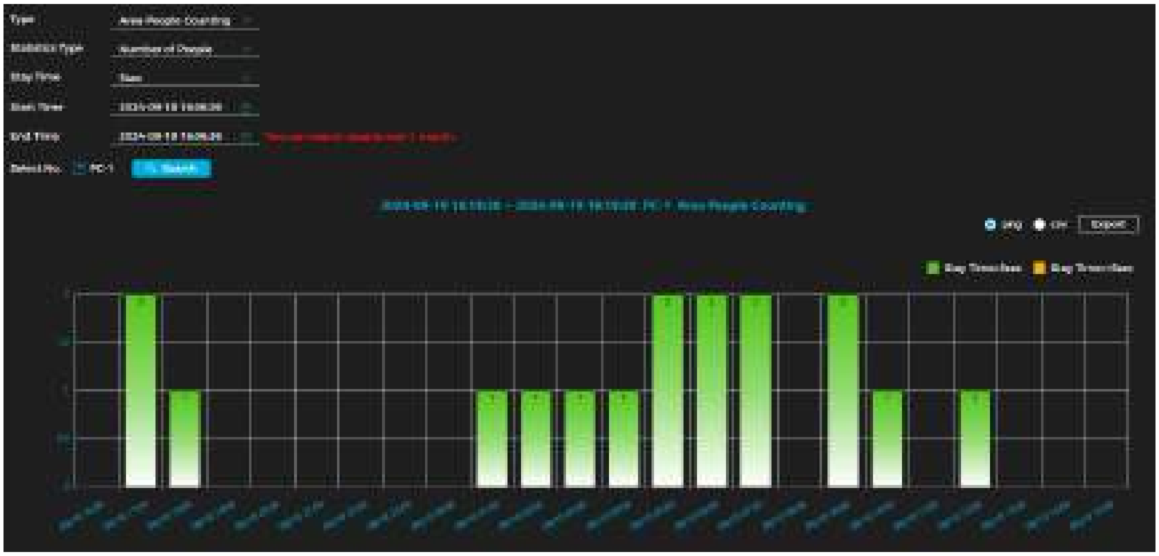
Statistics Type: Number of People

Start Time: [illegible]

End Time: [illegible]

Select No.: PC-2

*People Counting Report*



Type: Area People Counting

Statistics Type: Number of People

Stay Time: Sum

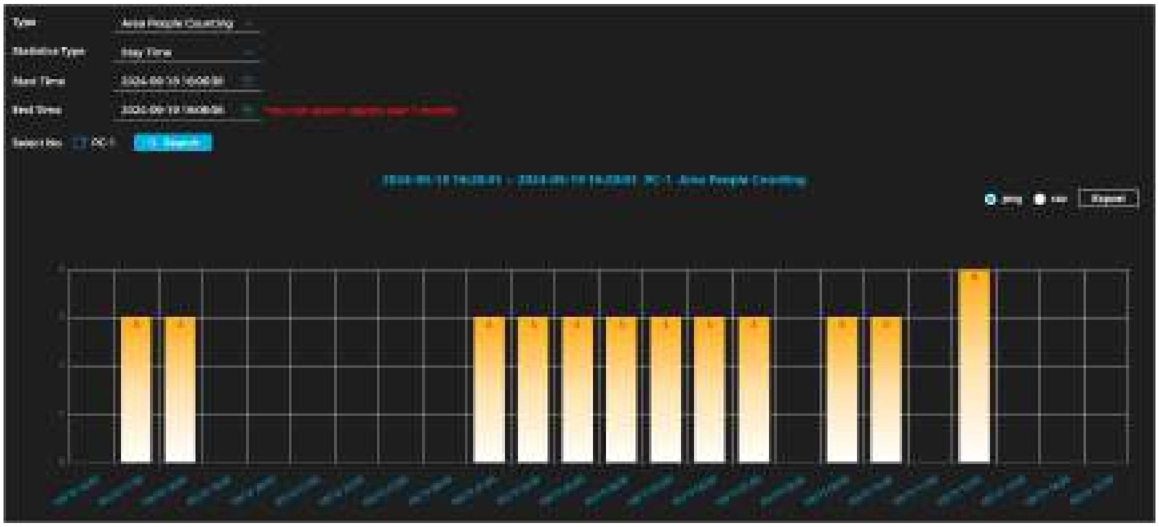
Start Time: 2024-09-18 16:06:26

End Time: 2024-09-19 16:06:26 [illegible]

Select No. □ PC-1 Search

2024-09-19 16:10:26 ~ 2024-09-19 16:10:26 PC-1 Area People Counting

*Area People Counting Report*



Type: Area People Counting

Statistics Type: Stay Time

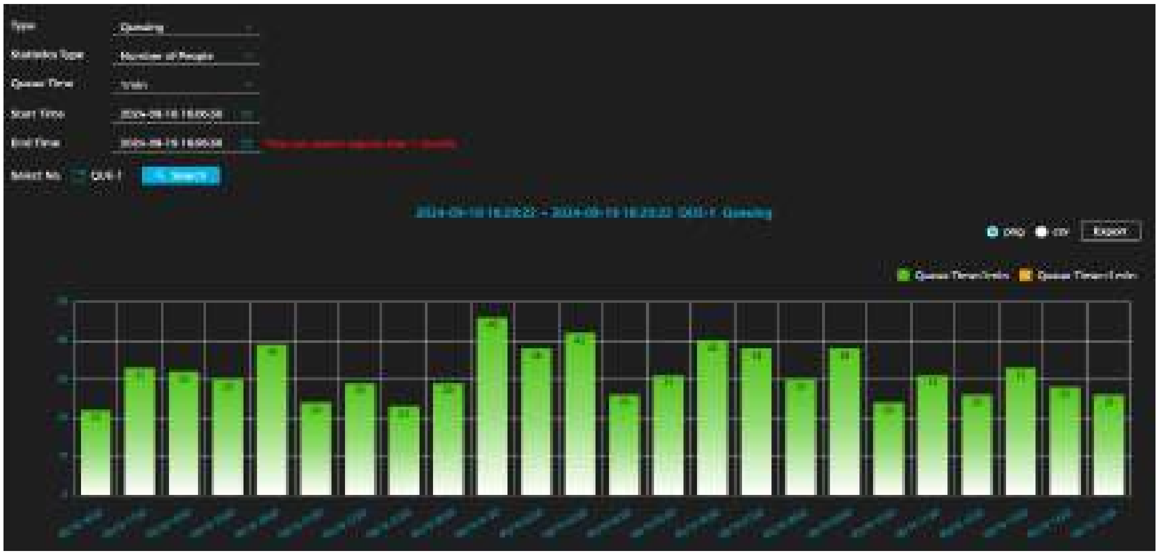
Start Time: 2024-09-18 16:06:56

End Time: 2024-09-19 16:06:56 [illegible]

Select No. □ PC-1 Search

2024-09-18 16:28:01 ~ 2024-09-19 16:28:01 PC-1 Area People Counting

*Stay Time Report*



Type: Queuing

Statistics Type: Number of People

Queue Time: 1min

Start Time: 2024-09-18 16:05:58

End Time: 2024-09-19 16:05:58 [illegible]

Select No. □ QUE-1 Search

2024-09-18 16:28:22 ~ 2024-09-19 16:28:22 QUE-1 Queuing

*Queueing Report*

## Heat Map

Heat Mapping provides a visual representation of movement patterns within the monitored area. Areas with high levels of activity are represented using warm colors such as red, orange, and yellow, while areas with little to no activity are depicted in cooler colors like blue and green.

Users can easily identify “hot spots” where people congregate or frequently pass through, as well as “cold spots” where there is minimal activity.

You can search the detection results by the number of people and stay time and then generate the heat map.

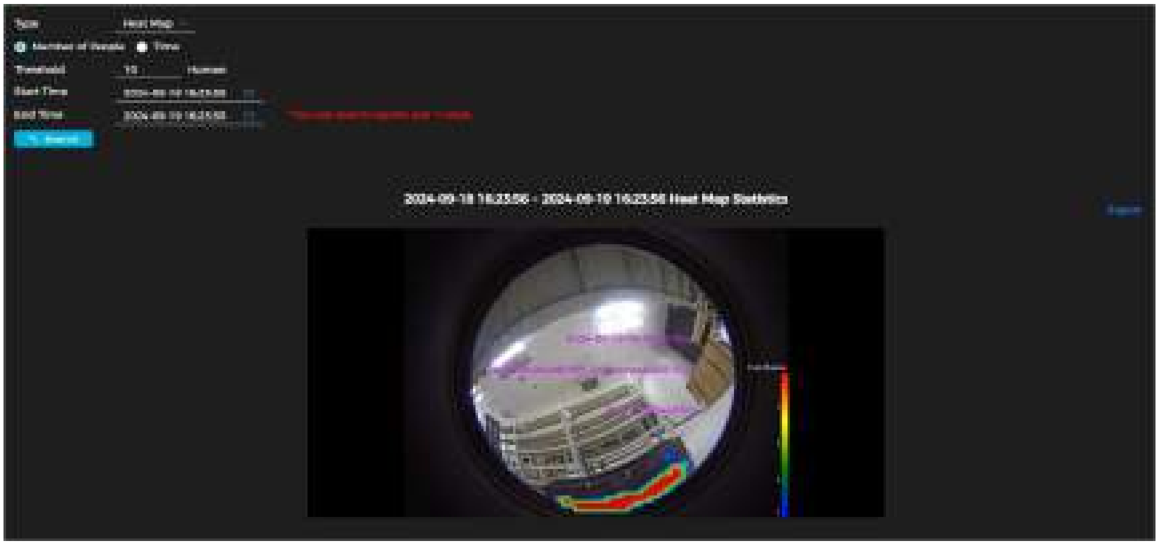
ⓘ Heat Map is not available on fisheye cameras.

To produce a Heat Map report, do the following:

1. Navigate to **File Search → Smart Report → Heat Map**.
2. Set the search parameters. See the table below for more details.

| Parameter | Description |
|---|---|
| Channel | For multi-channel cameras, select the channel first. |
| Type | Select the report type. |
| Number of People | When selecting **Heat Map** as the type, choose **Number of People** and set the threshold. The system will generate a heat map displaying people density. |
| Threshold | |
| Time | When selecting Heat Map as the type, choose Time and set the threshold. The system will generate a heat map based on stay duration. |
| Threshold | |
| Start Time/End Time | Set the reporting period |

3. Click **Search**.
4. (Optional) To save a report, click **Export** and select the storage path. The report will be in .bmp format.



Type: Heat Map

● Number of People ○ Time

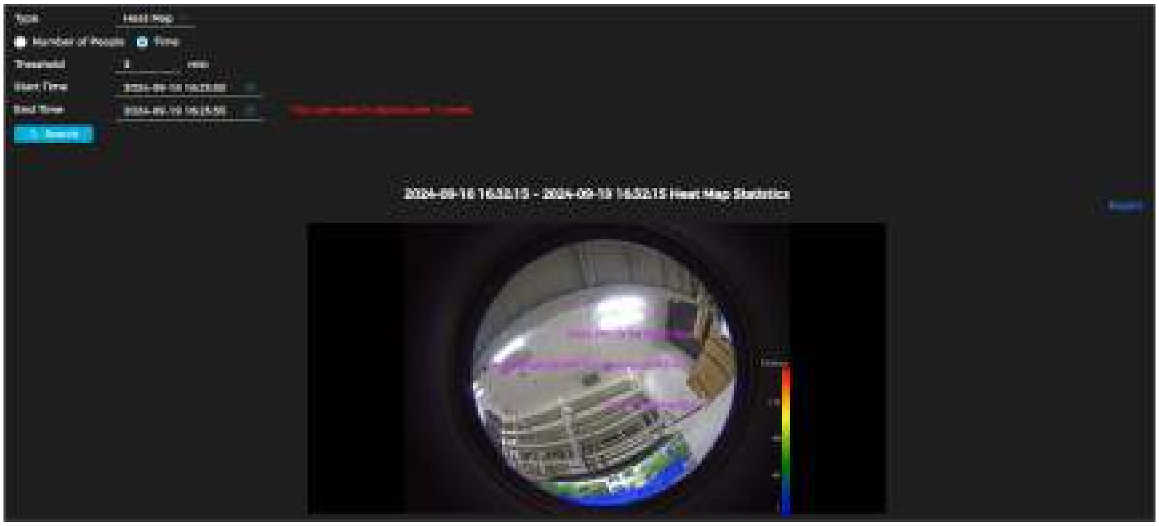
Threshold: 10 Human

Start Time: 2024-09-18 16:23:56

End Time: 2024-09-19 16:23:56

2024-09-18 16:23:56 - 2024-09-19 16:23:56 Heat Map Statistics

*Heat Map (Number of People)*



*Heat Map (Time)*

# How to Set a Network Destination

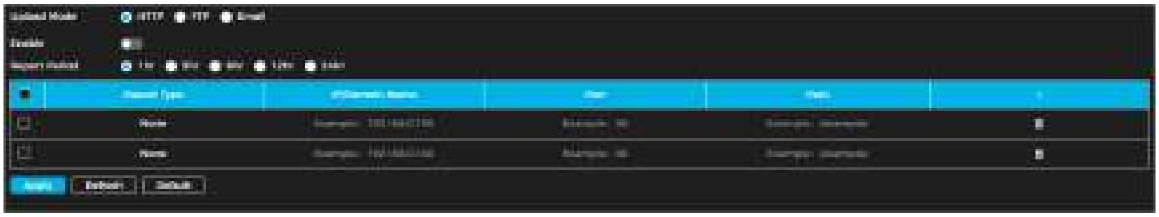
Select and enable the upload mode, then configure the parameters. The camera will periodically upload AI function reports to a designated server.

There are three upload methods:

- **HTTP**: Upload reports to a server using the HTTP protocol.
- **FTP**: Upload reports via FTP. Configure parameters such as server IP, username, password, and storage path.
- **Email**: Send reports to specified recipients via email. Set parameters including username, password, sender, and receiver details.

Follow the steps below to set a network destination to automatically upload AI reports to.

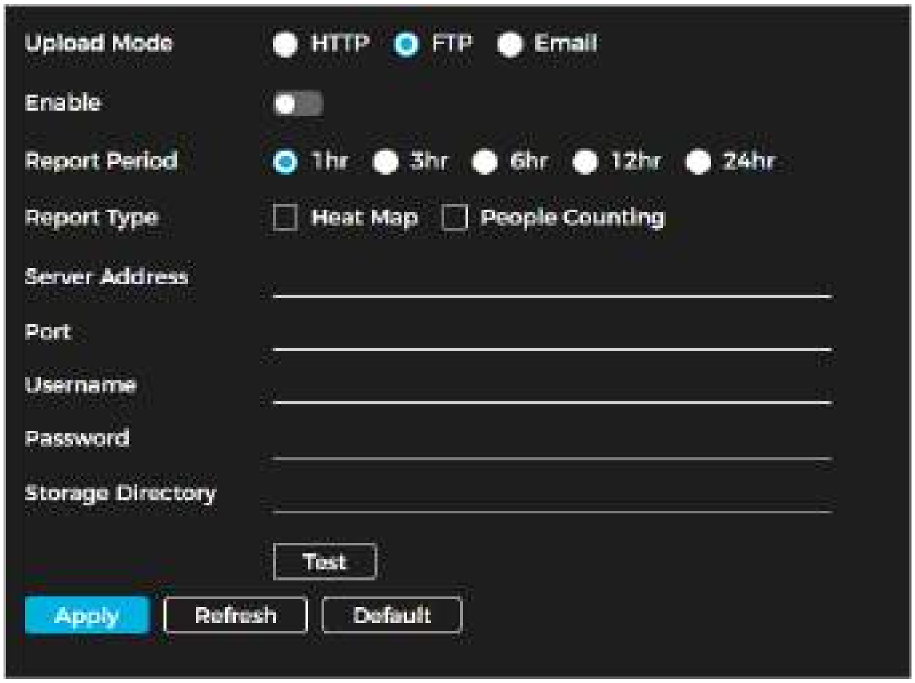
1. Navigate to **File Search → Smart Report → Network Destination**.
2. Select and enable the upload method.
3. Set the parameters. Each upload method has different parameters. See the tables below for more details.



*HTTP Upload Method*

| Parameter | Description |
|---|---|
| Report Period | Select the report period from the drop-down list. The default setting is one hour (report is uploaded every hour). |
| IP/Domain Name | Enter the IP address and port number of the server where the report will be uploaded. |
| Port | |
| HTTPS | Click ⚪ to enable the function. |
| Path | The storage path for the report. |

| | |
|---|---|
| Report Type | Select the report type from the drop-down list. You can choose multiple types simultaneously. The available report types correspond to the supported AI functions.<br>For example, if the camera supports People Counting, Heat Map, and Video Metadata, these options will appear in the drop-down list. |



Upload Mode ○ HTTP ● FTP ○ Email

Enable

Report Period ● 1hr ○ 3hr ○ 6hr ○ 12hr ○ 24hr

Report Type □ Heat Map □ People Counting

Server Address

Port

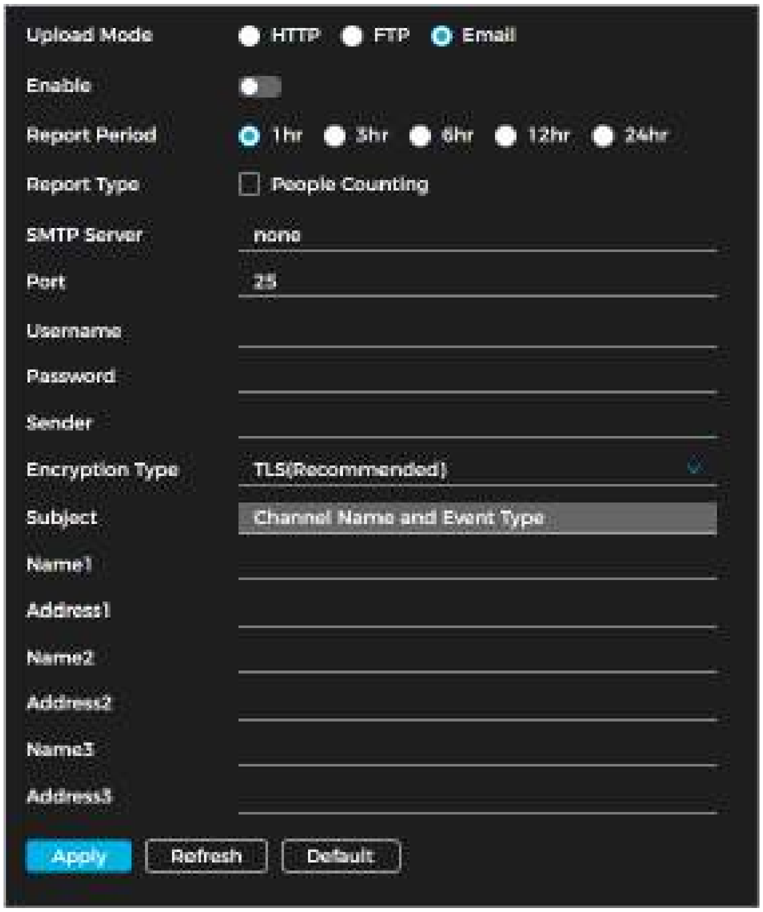
Username

Password

Storage Directory

*FTP Upload Method*

| Parameter | Description |
|---|---|
| Report Period | Select the report period from the drop-down list. The default setting is one hour (report is uploaded every hour). |
| Report Type | Select the report type from the drop-down list. You can choose multiple types simultaneously. The available report types correspond to the supported AI functions.<br>For example, if the camera supports People Counting, Heat Map, and Video Metadata, these options will appear in the drop-down list. |
| Server Address | The FTP server’s IP address and port number. |
| Port | |
| Username | Login credentials for the FTP server. |
| Password | |
| Storage Directory | The FTP server destination path. |
| Test | Check the network connection between the camera and server. |



Upload Mode ○ HTTP ○ FTP ● Email

Enable

Report Period ● 1hr ○ 3hr ○ 6hr ○ 12hr ○ 24hr

Report Type □ People Counting

SMTP Server: none

Port: 25

Username:

Password:

Sender:

Encryption Type: TLS(Recommended)

Subject: Channel Name and Event Type

Name1:

Address1:

Name2:

Address2:

Name3:

Address3:

*Email Upload Method*

| Parameter | Description |
|---|---|
| Report Period | Select the report period from the drop-down list. The default setting is one hour (report is uploaded every hour). |
| Report Type | Select the report type from the drop-down list. You can choose multiple types simultaneously. The available report types correspond to the supported AI functions.<br>For example, if the camera supports People Counting, Heat Map, and Video Metadata, these options will appear in the drop-down list. The heat map report will not be uploaded when the email upload method is selected, so it will not appear in the drop-down list. |
| SMTP Server | The SMTP server's IP address and port number. See the table below for more details. |
| Port | |
| Username | Login credentials for the server. See the table below for more details. |
| Password | |
| Sender | Email address of the sender. |
| Encryption Type | Choose the encryption type: **None**, **SSL (Secure Sockets Layer)**, and **TLS (Transport Layer Security)**. See the table below for more details. |
| Subject | Email subject line. This can be 120 characters in Chinese, English, or Arabic numerals. |
| Name/Address | Supports up to three receiving email addresses. |

## Major Mailbox Configuration

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

4. Click **Apply**.

# Smart Analysis

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

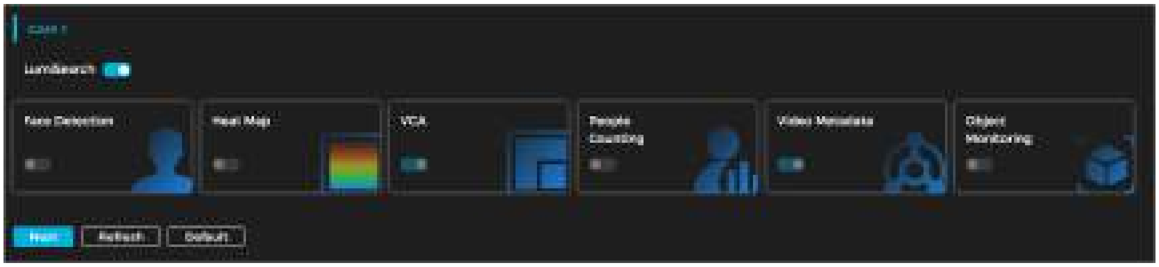
When the intelligent function is enabled, configured rules and their effects are displayed on both the live video and the intelligent rule configuration page. If a target triggers an intelligent function, the rule lines flash red.

## 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.



*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.

| 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.<br>• **Time**: Enable **Remove Duplicate Faces** in the configured time.<br>• **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**.<br>When selecting **Automatic**, click ⚙, configure the parameters on the prompt page, and then click **Apply**.<br>• **Customized Width**: Set the snapshot width by entering a multiple of the original face width (range: 1 – 5).<br>• **Customized Face Height**: Set the face height in the snapshot by entering a multiple of the original face height (range: 1 – 2).<br>• **Customized Body Height**: Set the body height in the snapshot by entering a multiple of the original body height (range: 0 – 4).<br>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.<br>• **Optimized**: Captures the clearest image within the set time after face detection.<br>• **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.

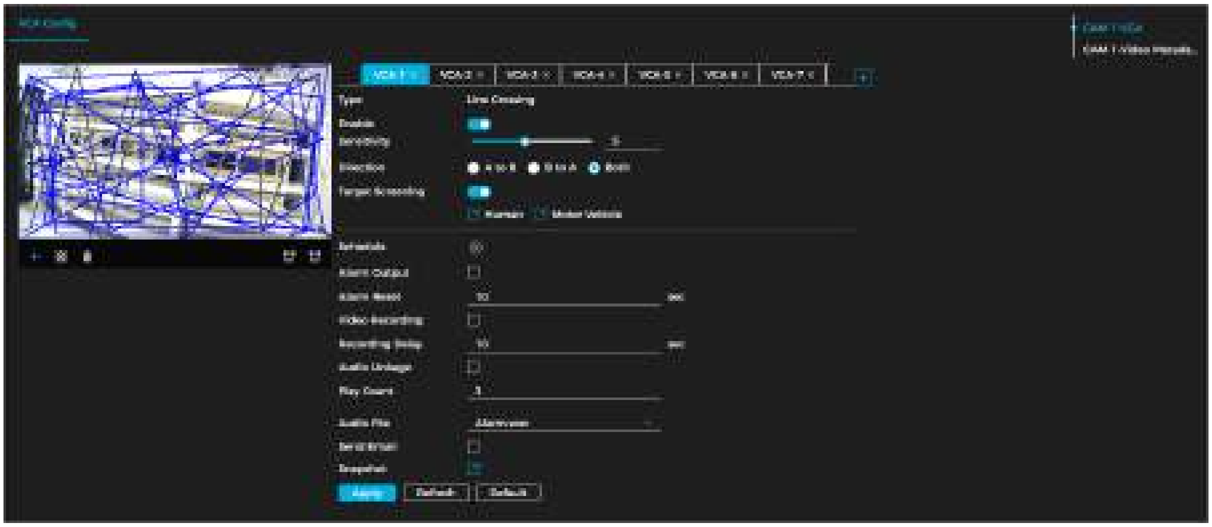
See the table below for the functions and applications of the rules. Not all device models will support every function listed in the table.

| 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. | |
| Object Placement | 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.<br>• Missed alarms may increase in scenes with dense targets, frequent occlusion, or stationary individuals.<br>• In complex foreground and background environments, false alarms may occur for abandoned or missing object |

| | | |
|---|---|---|
| Object Fetch | 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.<br>• Missed alarms may increase in scenes with dense targets, frequent occlusion, or stationary individuals<br>• In complex foreground and background environments, false alarms may occur for abandoned or missing objects. |
| Fast Moving | When the target speed exceeds the configured threshold. | Suitable for scenes with sparse targets and minimal occlusion. The camera should be installed directly above the monitoring area with light direction perpendicular to the motion direction. |
| Parking Detection | When a target remains in the area beyond the configured time. | Ideal for road monitoring and traffic management. |
| Crowd Gathering | 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.



Type: Line Crossing
Enable
Sensitivity: 5
Direction: ○ A to B ○ B to A ● Both
Target Screening
☑ Human ☑ Motor Vehicle
Schedule
Alarm Output □
Alarm Reset: 10 sec
Video Recording □
Recording Delay: 10 sec
Audio Linkage □
Play Count: 1
Audio File: Alarm...
Send Email □
Snapshot ☑
Apply Refresh Default

*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.<br>• 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.<br>• 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. |
| Object Placement | |
| Object Fetch | |
| Fast Moving | |
| Parking Detection | |
| Crowd Gathering | |
| 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. |

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

| Parameter | Description |
|---|---|
| Direction | Configure the detection direction for rule settings.<br>• For line crossing, choose A → B, B → A, or A ←→B.<br>• For intrusion, select Enter, Exit, or Both. |
| Action | When configuring intrusion actions, choose from **Appears**, **Cross**, or **Inside**.<br>**Inside** and **Appears/Cross** cannot be enabled simultaneously. |
| Target Screening | When **Target Screening** is enabled, the system detects only the selected targets. Only these targets can trigger alarm rules.<br>• **Target Screening** is available for line crossing, intrusion, and fast-moving rules.<br>• Human and Motor Vehicle are the targets selected by default.<br>• The algorithm mainly supports detecting cats and dogs in the animal category. It may detect other four-legged animals, but accuracy is not guaranteed. |
| Duration | • For **abandoned objects**, the duration represents the shortest time required to trigger an alarm after an object is left unattended.<br>• 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.<br>**Object Placement**, **Object Fetch**, and **Loitering Detection** do not support this function. |

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 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**.

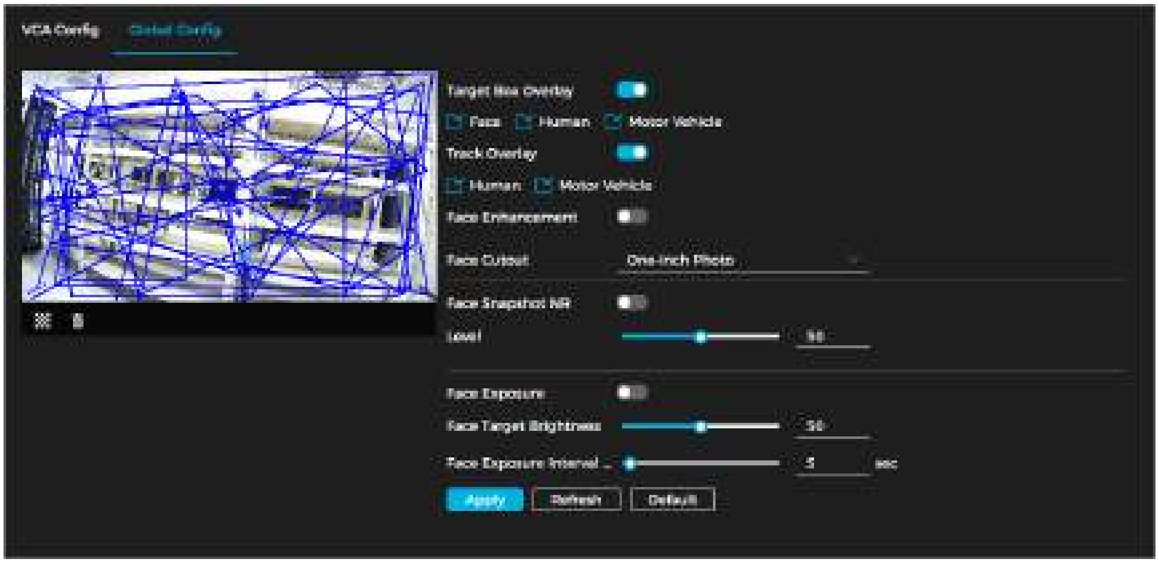
2. Click ○ next to **Video Metadata** to enable the function on the corresponding channel.

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.



Target Box Overlay ●
☑ Face ☑ Human ☑ Motor Vehicle
Track Overlay ●
☑ Human ☑ Motor Vehicle
Face Enhancement ○
Face Cutout One-inch Photo
Face Snapshot NR ○
Level 50
Face Exposure ○
Face Target Brightness 50
Face Exposure Interval 5 sec

*Global Configuration of Video Metadata*

| Parameter | Description |
|---|---|
| Target Box Overlay | Overlay a target box on captured images to indicate the target's position.<br>Three types of target boxes are available; select the appropriate one as needed.<br>Captured images are stored on the SD card or in the configured storage path. |
| Track Overlay | Overlay a track on captured images.<br>Two types of tracks are available; select the appropriate one as needed. |

| | |
|---|---|
| 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**, **One-Inch Photo**, or **Automatic**. |
| 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. |
| Target Face Brightness | Adjust the face target brightness. The default value is **50**. |
| Face Exposure Interval Detection Time | Set the face exposure detection interval to avoid image flickering due to continuous exposure adjustments. The default value is **5 seconds**. |

6. Click **Apply**.

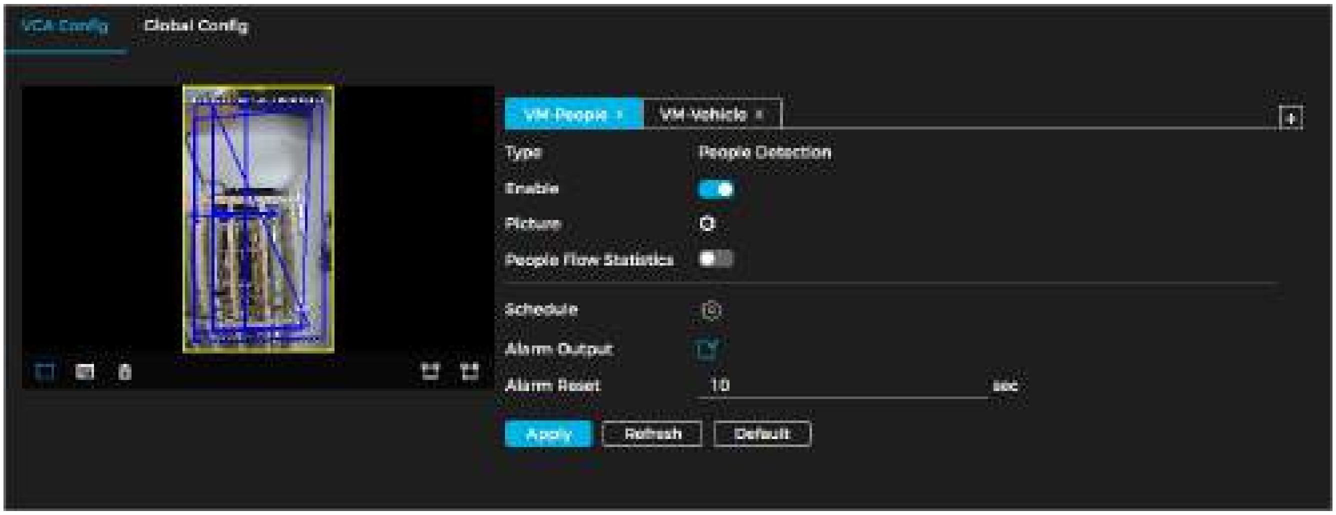
## Rule Configuration

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 + to select the rules.



Type People Detection

Enable

Picture

People Flow Statistics

Schedule

Alarm Output

Alarm Reset 10 sec

*Rule Configuration (Video Metadata)*

5. Configure the picture by clicking ⚙.
6. Configure the overlay for motor vehicles and people and set the box position. This section uses motor vehicle overlay configuration as an example.
7. Select the type of overlay to be captured and adjust the position of the displayed information.
8. Choose the overlay image upload type(s).
9. Click **Apply**.

10. (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. |
| ▦ | To show pixel size, press and hold the left mouse to draw a rectangle. |
| 🗑 | Delete a detection line. |

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

12. Click **Apply**.

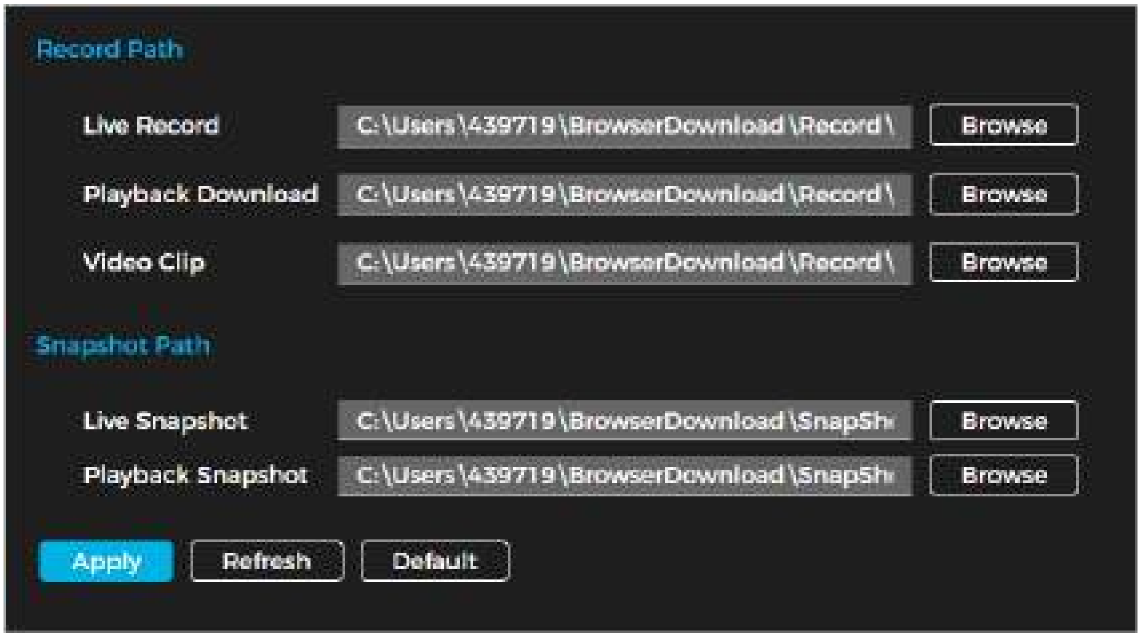
# Settings

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.<br>The default path is C:\Users\admin\BrowserDownload\Record\Live. |
| Playback Download | The downloaded video of playback page.<br>The default path is C:\Users\admin\BrowserDownload\Record\Playback. |
| Video Clip | The clipped video of playback page.<br>The default path is C:\Users\admin\BrowserDownload\Record\Clips. |
| Live Snapshot | The snapshot of live page.<br>The default path is C:\Users\admin\BrowserDownload\Snapshot\Live. |
| Playback Snapshot | The snapshot of playback page.<br>The default path is C:\Users\admin\BrowserDownload\Snapshot\Playback. |

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

3. Click **Apply**.

# System

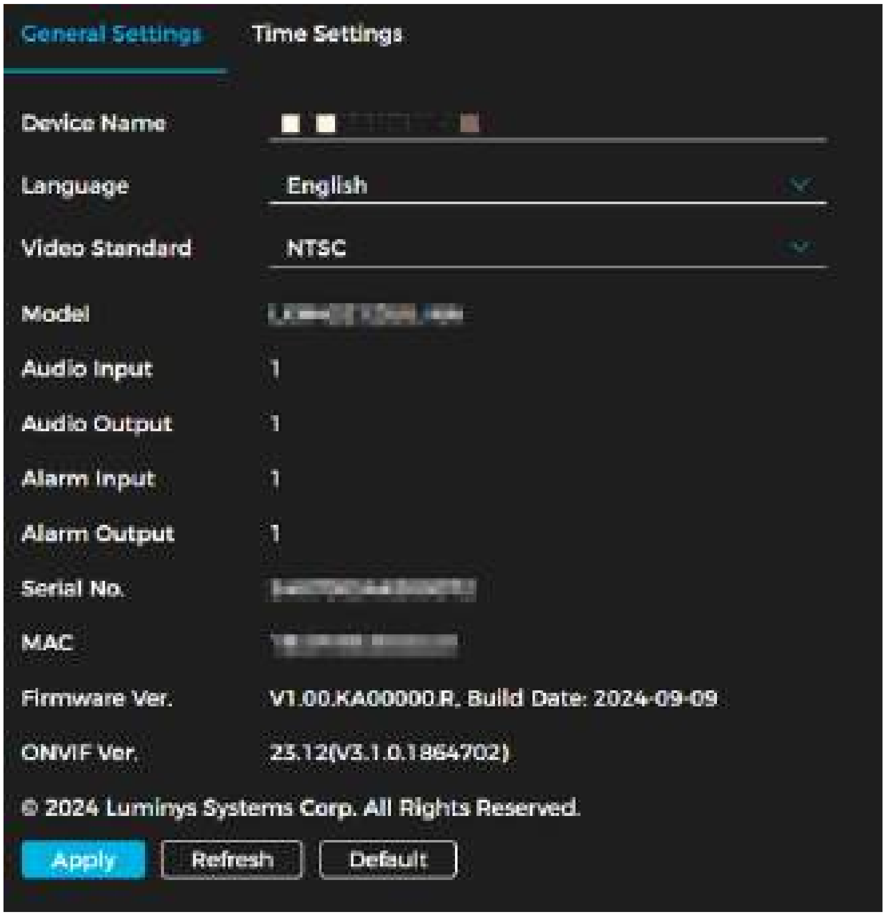
This section covers system configurations, including system settings, maintenance, security, user management, and legal information.

## 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**.



General Settings | Time 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.

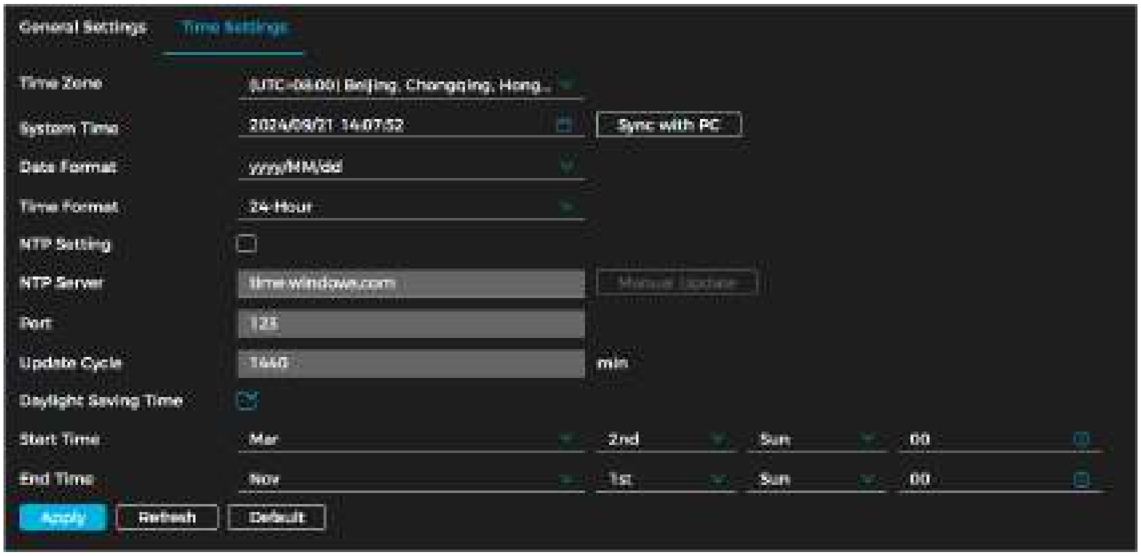
| Parameter | Description |
|---|---|
| Device Name | Input the device name. |
| Language | Set the system language (English, Spanish, or French). |
| Video Standard | Choose **PAL** or **NTSC**. |

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**.



Time Zone: (UTC+08:00) Beijing, Chongqing, Hong...
System Time: 2024/09/21 14:07:52
Date Format: yyyy/MM/dd
Time Format: 24-Hour
NTP Setting: □
NTP Server: time.windows.com
Port: 123
Update Cycle: 1440 min
Daylight Saving Time: ☑
Start Time: Mar 2nd Sun 00
End Time: Nov 1st Sun 00

*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.<br>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:

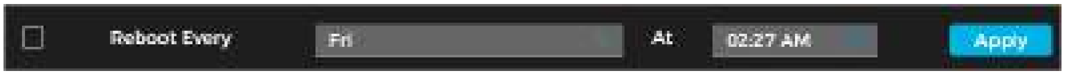
- Regularly check surveillance images.
- Remove unused user and user group information.
- Change the password every three months.
- Review and analyze system logs to address abnormalities promptly.
- Back up the system configuration periodically.
- Restart the device and delete old files regularly.

- Keep the firmware updated.

## Auto-Reboot

Follow the steps below to configure auto-reboot.

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



☐ Reboot Every Fri At 02:27 AM

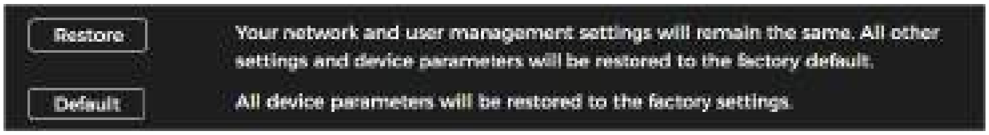
*Auto-Reboot*

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.

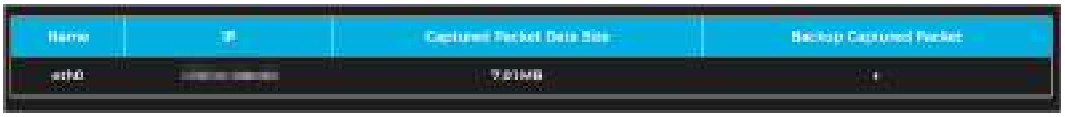
1. Navigate to **Settings → System → Maintenance → Upgrade and Maintenance**.
2. Choose to update the system using a **Firmware Upgrade** or an **Online Upgrade**.

- **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**.

### 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**.



*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**.

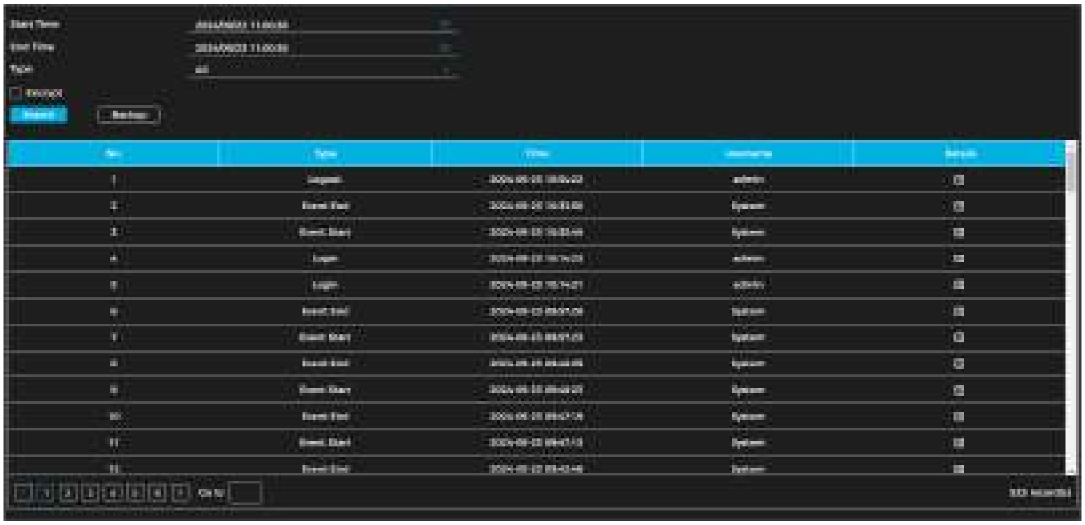
2. Set the Start Time and End Time.

3. Select the log type. 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.



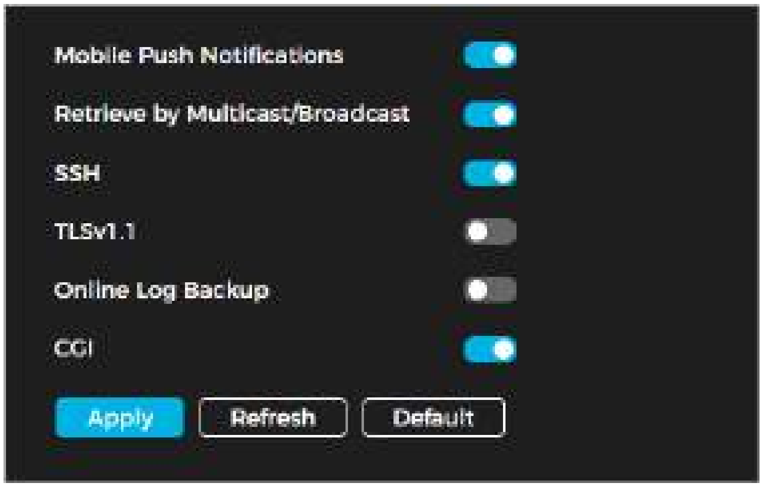
*System Logs*

# 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
Retrieve by Multicast/Broadcast
SSH
TLSv1.1
Online Log Backup
CGI

*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.<br>ⓘ<br>• Ensure that compatible devices or software support video decryption.<br>• It is recommended to enable this function to reduce the risk of data leakage. |
| Online Log Backup | File access, file access error, and file search |
| CGI | Enable this function to back up the online log. |
| Mobile Push Notification | Enable this function to allow access from other devices. This feature is enabled by default. |

3. Click **OK**.

## Unauthorized Access

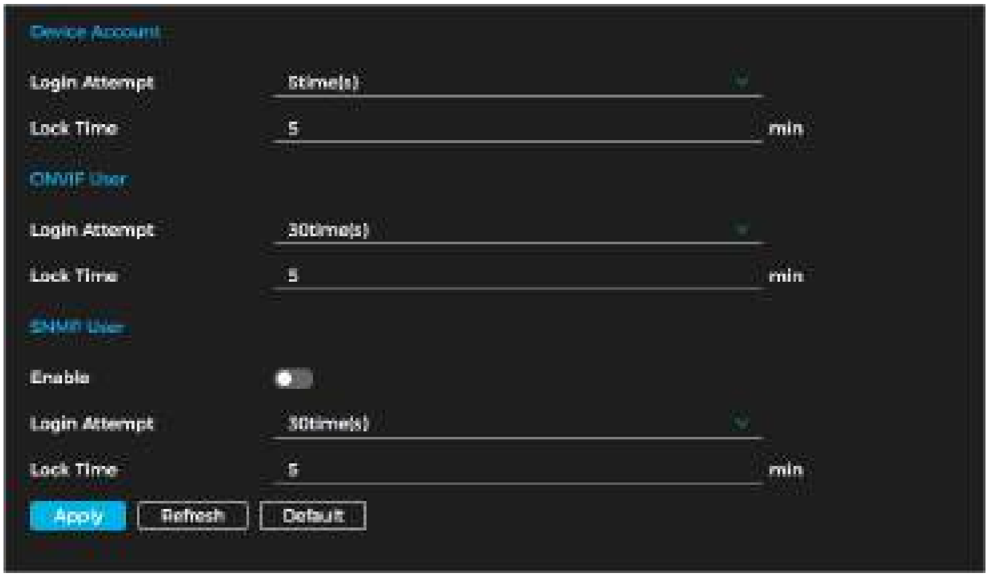
You can set the maximum number of unsuccessful login attempts before an account is locked to prevent unauthorized access. Follow the steps below to configure this setting.

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)

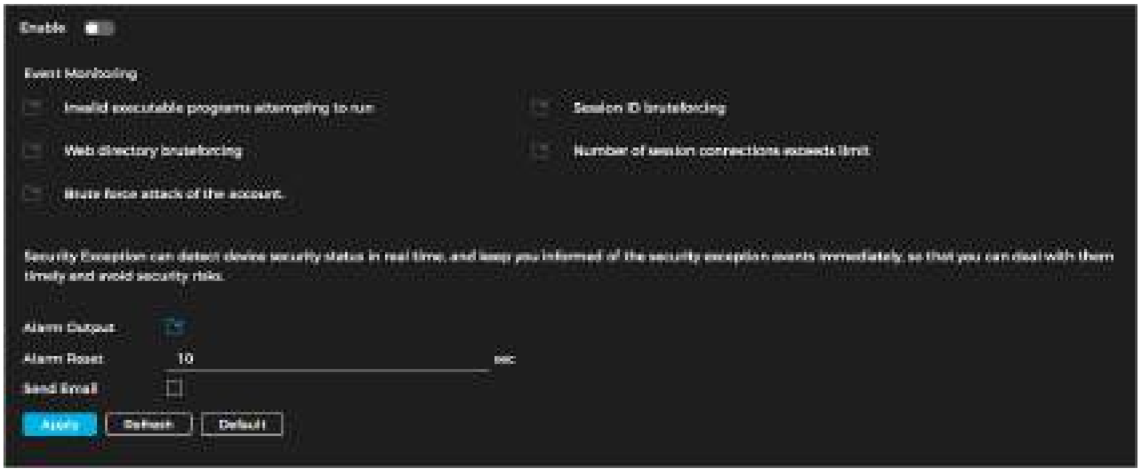
Lock Time: 5 min

*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: □

*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.

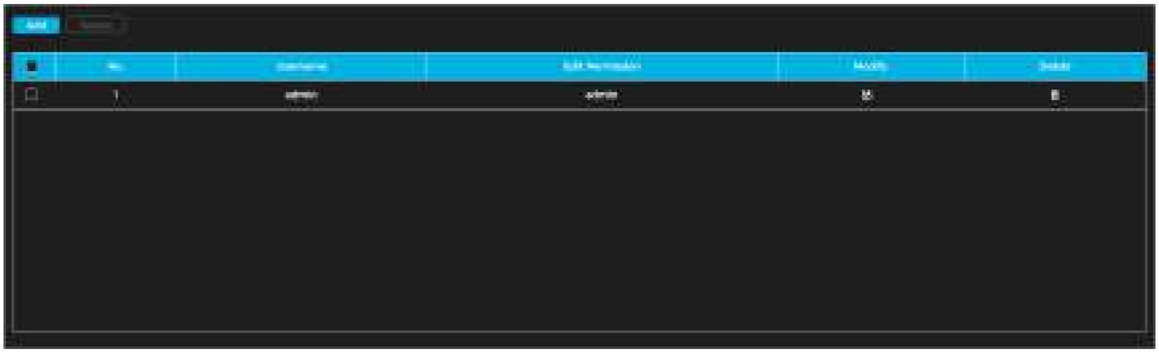
The following are user management rules and requirements:

- 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:

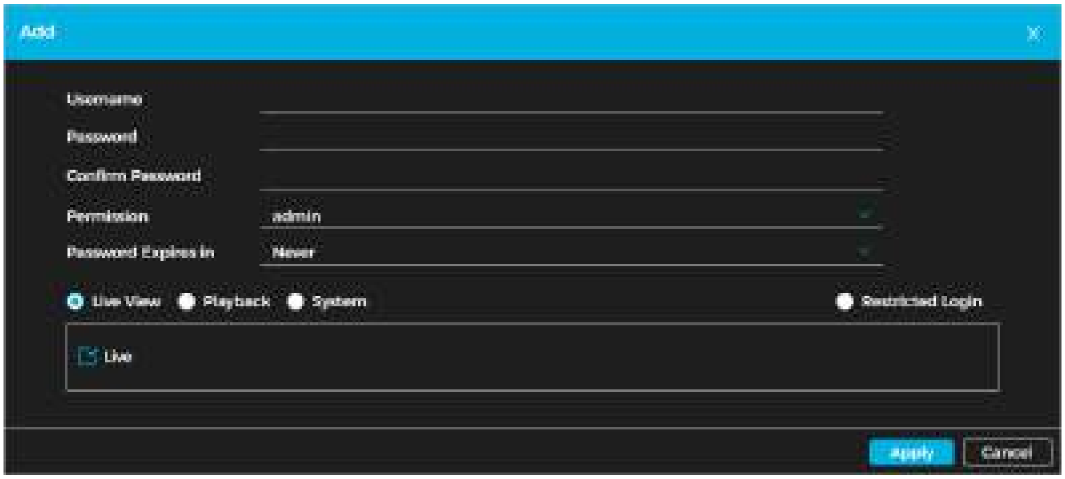
1. Navigate to **Settings → System → User Management → User**.



| ● | No. | Username | Edit Permission | Modify | Delete |
|---|---|---|---|---|---|
| □ | 1 | admin | admin | | |

*User Management*

2. Click **Add**.

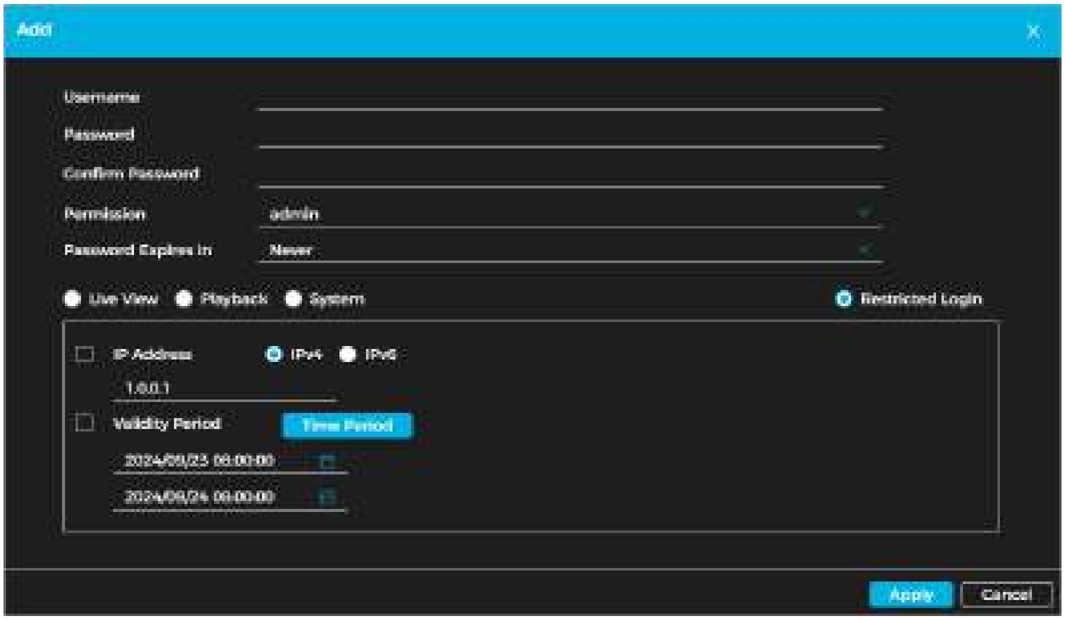


| | |
|---|---|
| Username | |
| Password | |
| Confirm Password | |
| Permission | admin |
| Password Expires in | Never |

● Live View ○ Playback ○ System ○ Restricted Login

□ Live

*Add a User (System)*



Add

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 00:00:00

2024/09/24 00:00:00

*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.<br>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.<br>• **IP Address**: Allows login only from the specified PC IP.<br>• **Validity Period**: Defines the time range when login is permitted.<br>• **Time Period**: Restricts login access to a specific timeframe within the validity period.<br>To set restricted login for the user, do the following:<br>1. Select the type and enter the IP address.<br>• **IP Address**: Input the specific host IP to be added.<br>• **IP Segment**: Enter the start and end IP addresses for a range of hosts.<br>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**.

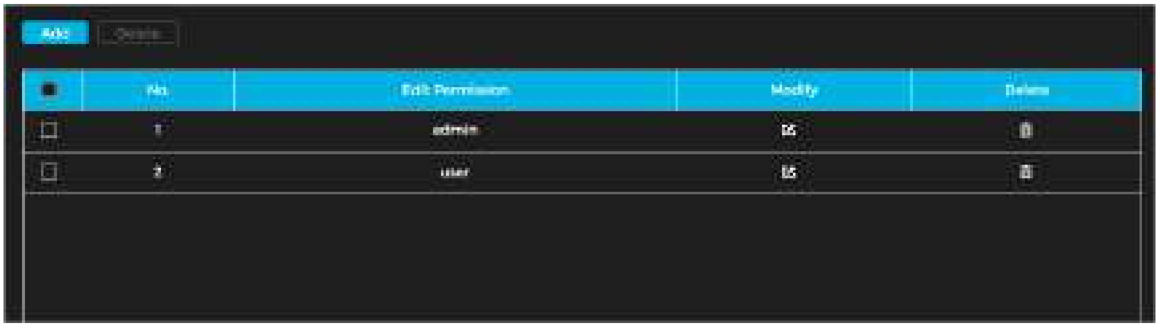
## Related Operations

- 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:

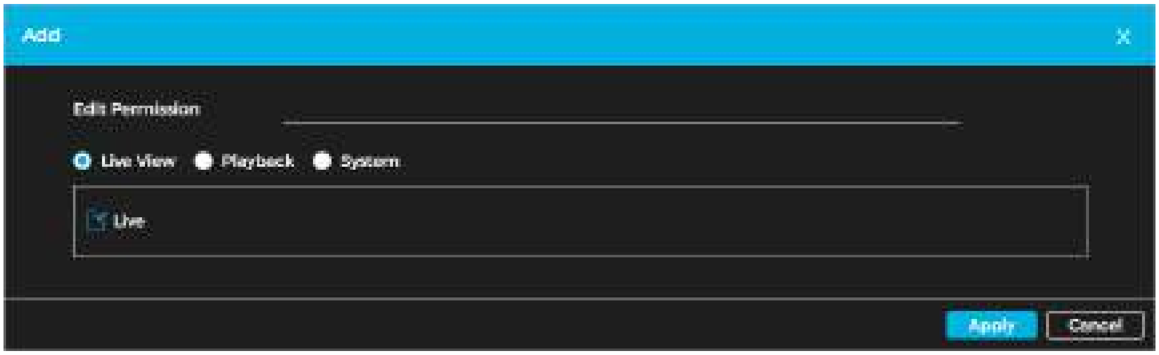
1. Navigate to **Settings → System → User Management → Edit Permission**.



| ● | No. | Edit Permission | Modify | Delete |
|---|---|---|---|---|
| □ | 1 | admin | ✎ | 🗑 |
| □ | 2 | user | ✎ | 🗑 |

*Permission Parameters*

2. Click **Add**.



Edit Permission

● Live View ● Playback ● System

☑ Live

*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.

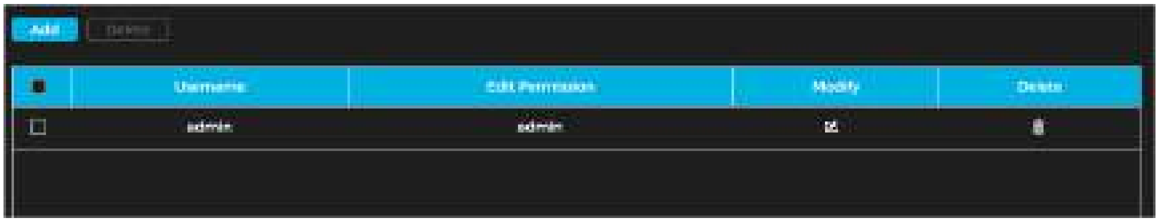
## Related Operations

- 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.

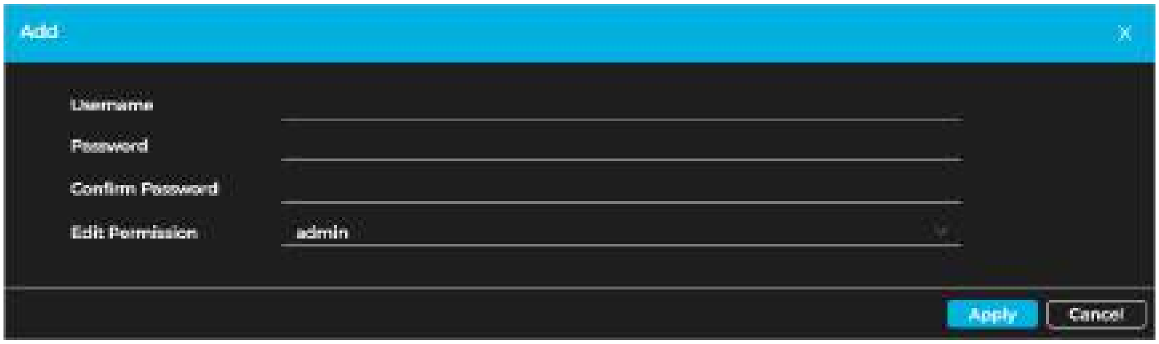
1. Navigate to **Settings → System → User Management → ONVIF User**.



| ■ | 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.<br>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. |

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.

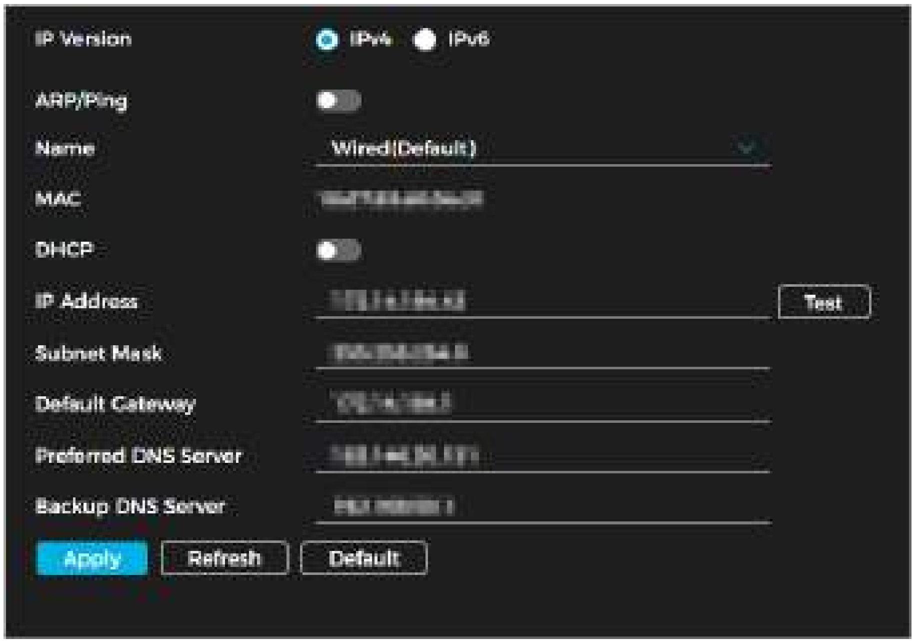
## Basic Network Configuration

### 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

ARP/Ping ○

Name Wired(Default)

MAC [redacted]

DHCP ○

IP Address [redacted]

Subnet Mask [redacted]

Default Gateway [redacted]

Preferred DNS Server [redacted]

Backup DNS Server [redacted]

*TCP/IP Parameters*

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

| Parameter | Description |
|---|---|
| IP Version | Choose IPv4 or IPv6. |
| ARP/Ping | Click ○ to enable ARP/Ping for setting the IP address. Retrieve the camera's MAC address, then use the ARP/Ping command to change and configure the device IP address.<br>This function is enabled by default. After a restart, you have up to 2 minutes to configure the IP address using a ping packet of a specific length. The service will automatically turn off after 2 minutes or immediately once the IP address is successfully configured.<br>If this function is disabled, the IP address cannot be configured using a ping packet<br>**Example of Configuring IP Address With ARP/Ping**<br>1. Ensure the camera to be configured and the PC are on the same local network, then obtain an available IP address.<br>2. Retrieve the MAC address of the camera from the device label.<br>3. Open the command prompt on the PC and enter the following command. |

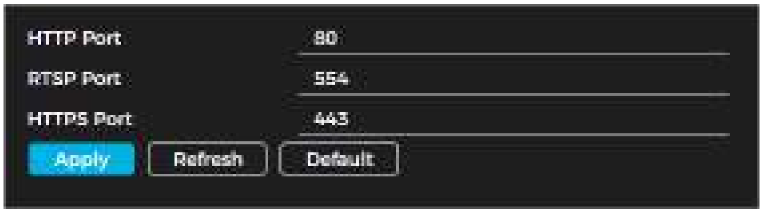
| | |
|---|---|
| | - **Windows Syntax**<br>arp -s <IP Address> <MAC><br>ping -l 480 -t <IP Address><br>- **UNIX/Linux/Mac Syntax**<br>arp -s <IP Address> <MAC><br>ping -s 480 <IP Address><br>4. Restart the camera.<br>5. Check the PC command line. If a message like "Reply from 192.168.1.101" appears, the configuration was successful, and you can close the command prompt.<br>6. Open your browser and enter http://(IP address) in the address bar to log in |
| 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.<br>ⓘ<br>- IPv6 does not use a subnet mask.<br>- 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 .<br>• When using RTSP, specify the channel number and bit stream type in the URL, along with username and password if required.<br>• On a BlackBerry smartphone, disable audio, set codec mode to H.264B, and set the resolution to CIF before playing the stream.<br>**Parameters**<br>• **IP**: The device IP address (e.g., 192.168.1.101).<br>• **Port**: Leave blank if using the default value (554).<br>• **Ch**: The channel number (starting from 1). If using channel 2, set Ch=2.<br>• **StreamType**: The bit stream type: 0 for the main stream (streamtype=0) and 1 for the sub stream (streamtype=1).<br>**Example**<br>• 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.
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:<br>• **NO-IP DDNS**: dynupdate.no-ip.com<br>• **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

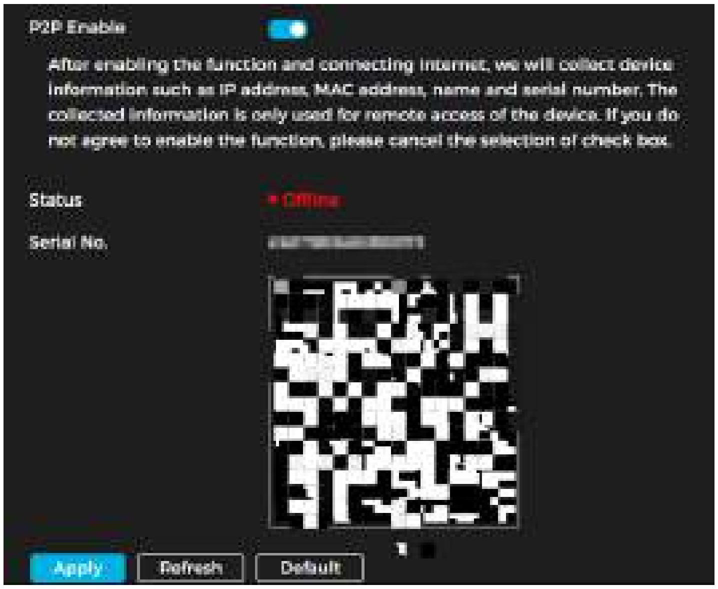
P2P (peer-to-peer) technology allows users to manage devices easily without the need for DDNS, port mapping, or a transit server. You can scan the device's QR code with your smartphone to add and manage more devices on the mobile app.

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

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. [illegible]

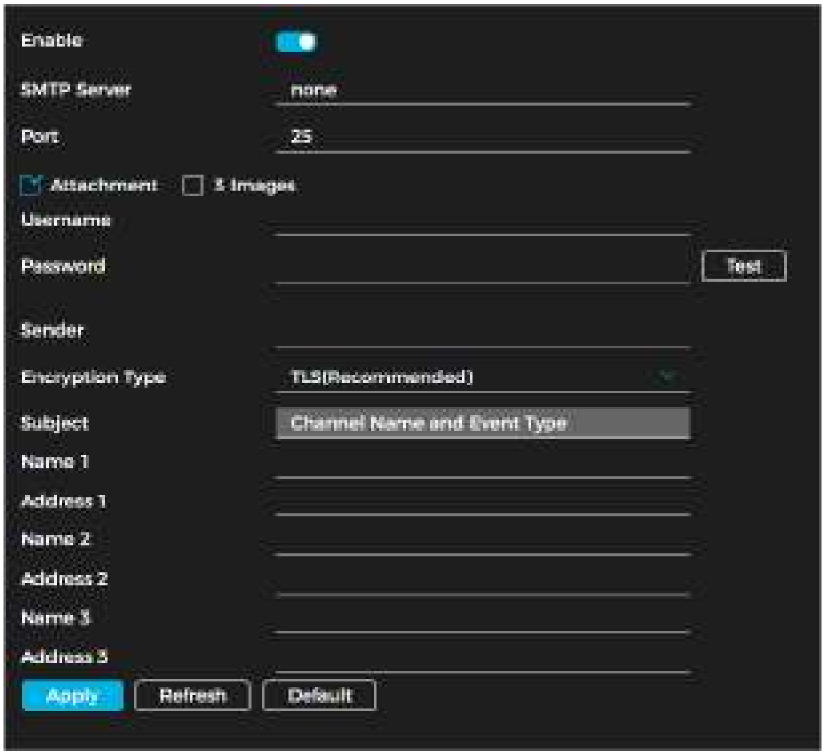
*Enable P2P*

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 ●

SMTP Server: none

Port: 25

☑ Attachment □ 3 Images

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. |

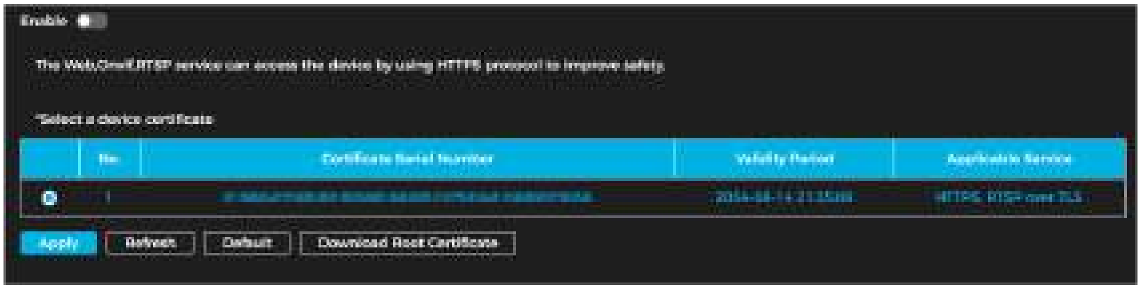
4. Click **Apply**.

## 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.

*Select a device certificate

| | No. | Certificate Serial Number | Validity Period | Applicable Service |
|---|---|---|---|---|
| ● | 1 | [illegible] | 2034-08-14 21:35:08 | HTTPS, RTSP over TLS |

*HTTPS*

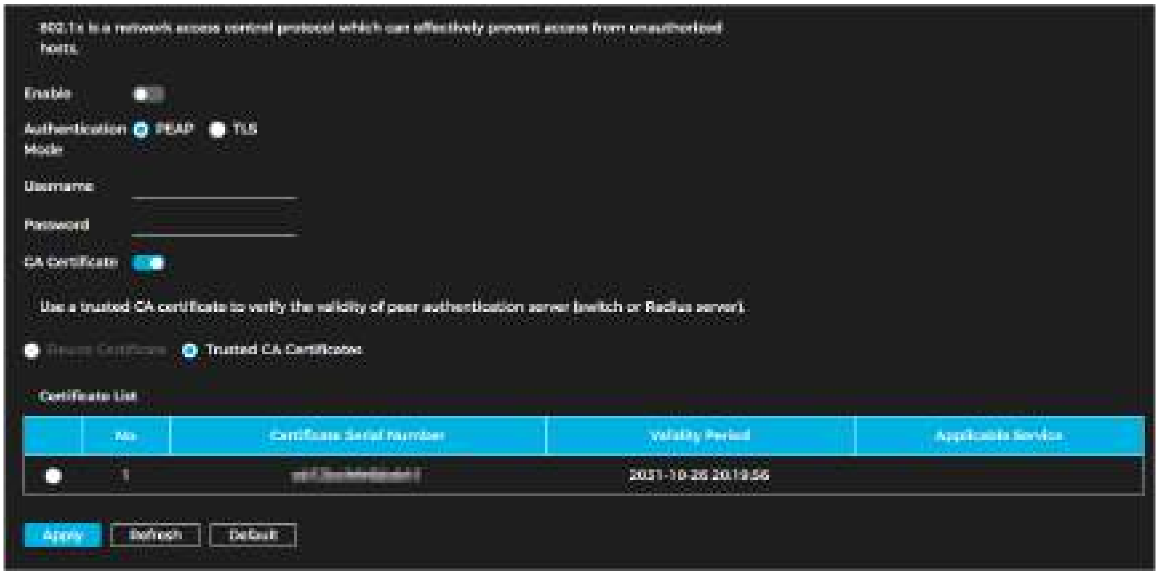
4. Click **Apply**.

## 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).

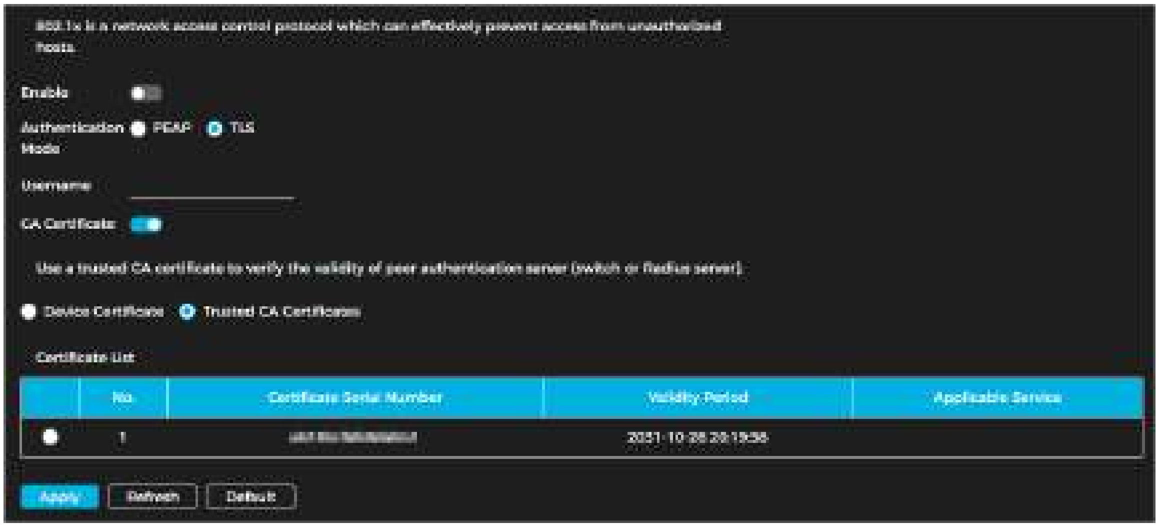
○ Device Certificate ● Trusted CA Certificates

Certificate List

| | No. | Certificate Serial Number | Validity Period | Applicable Service |
|---|---|---|---|---|
| ○ | 1 | [illegible] | 2031-10-28 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 Certificate

Certificate List

| | No. | Certificate Serial Number | Validity Period | Applicable Service |
|---|---|---|---|---|
| ○ | 1 | [illegible] | 2031-10-28 20:19:58 | |

*802.1x (TLS)*

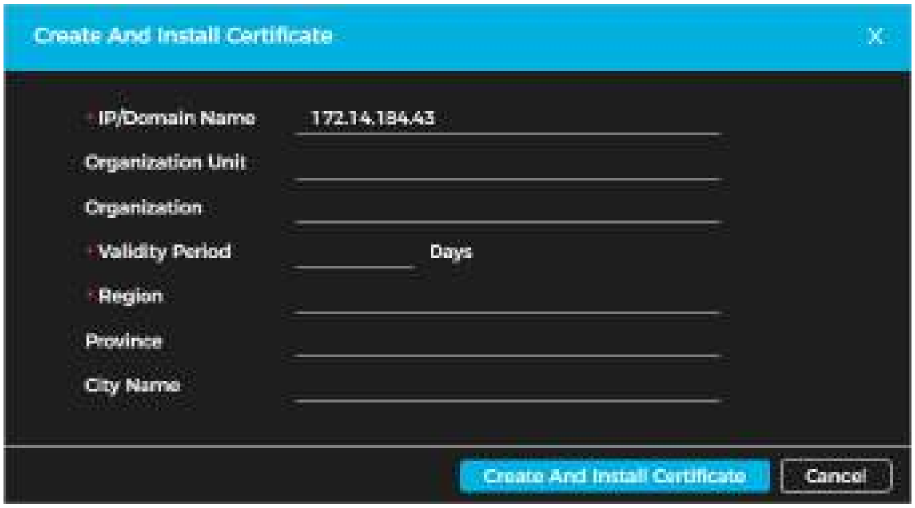
4. Click **Apply**.

## 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: 172.14.184.43

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.

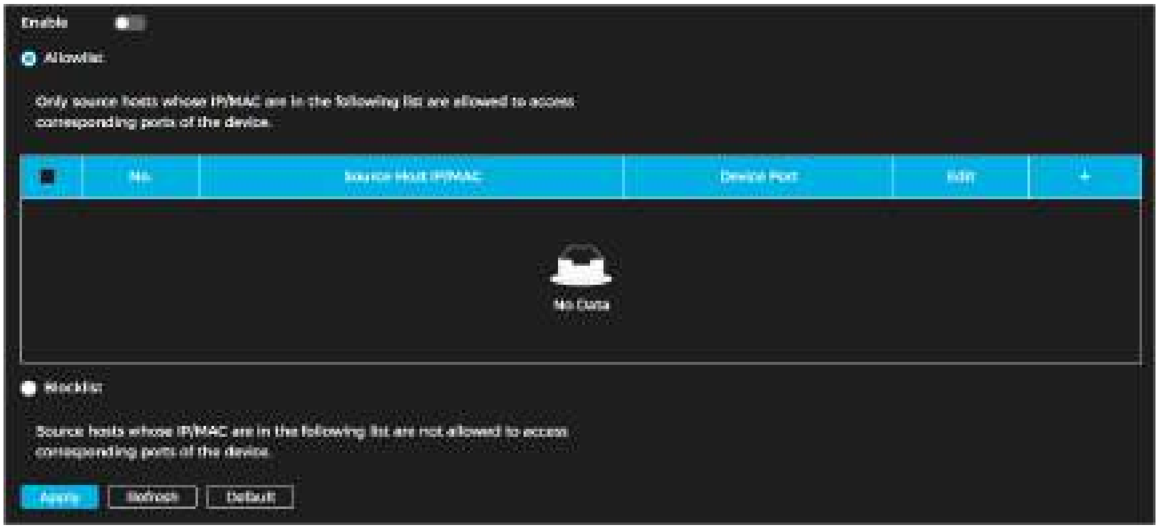
Follow the steps below to install a trusted CA certificate.

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.
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

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 | + |
|---|---|---|---|---|---|

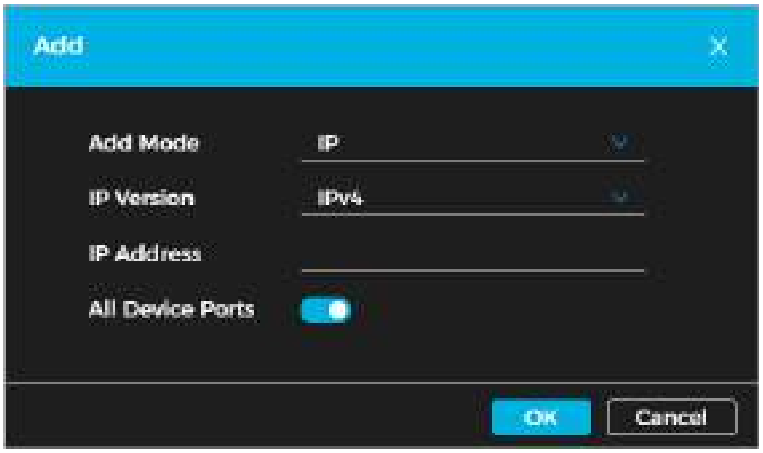
No Data

○ 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 Mode: IP

IP Version: IPv4

IP Address:

All Device Ports: ●

*Add a Host IP/MAC Address to the Firewall*

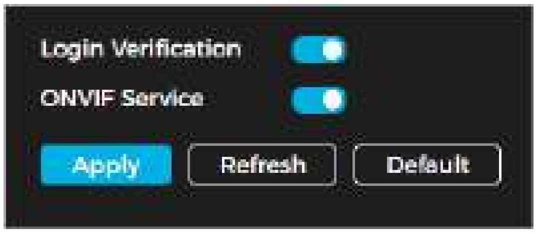
6. Click **Apply**.
7. (Optional) Click ✎ to edit host information and 🗑 to delete the host.

## 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: ●

ONVIF Service: ●

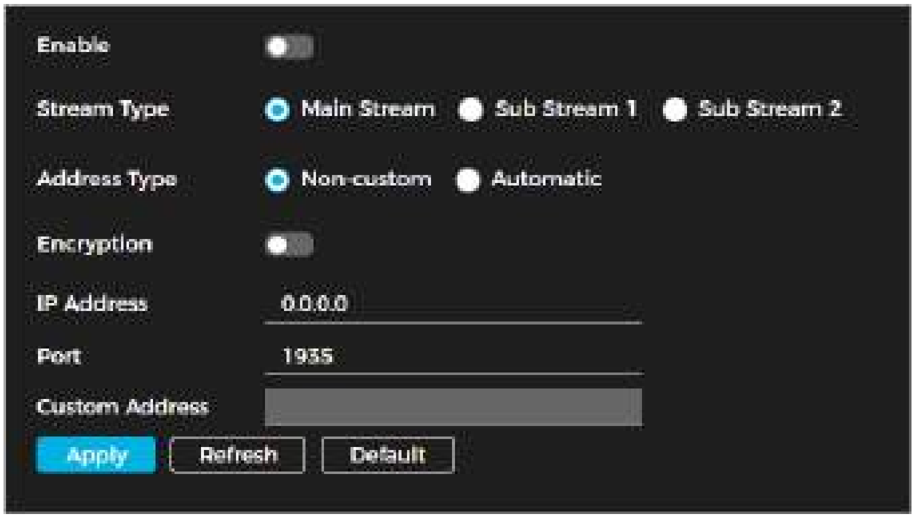
*ONVIF Service*

## 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 ○

Stream Type ● Main Stream ○ Sub Stream 1 ○ Sub Stream 2

Address Type ● Non-custom ○ Automatic

Encryption ○

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:<br>• **Non-Custom**: Input the server's IP address and domain name.<br>• **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**.

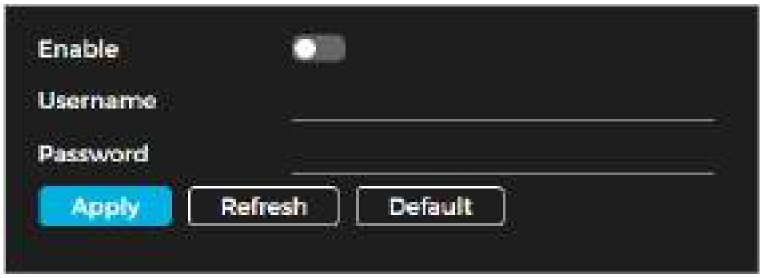
## PPPoE

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.



Enable

Username

Password

*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

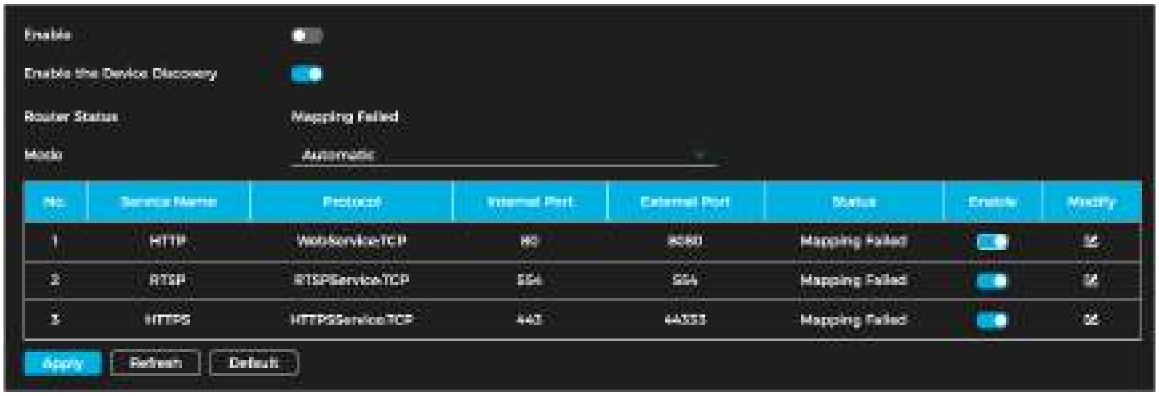
UPnP (Universal Plug and Play) is a protocol that creates a mapping between local area networks (LAN) and wide area networks (WAN). This function allows access to local devices using a wide area IP address.

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 | WebServiceTCP | 80 | 8080 | Mapping Failed | | |
| 2 | RTSP | RTSPServiceTCP | 554 | 554 | Mapping Failed | | |
| 3 | HTTPS | HTTPSServiceTCP | 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.

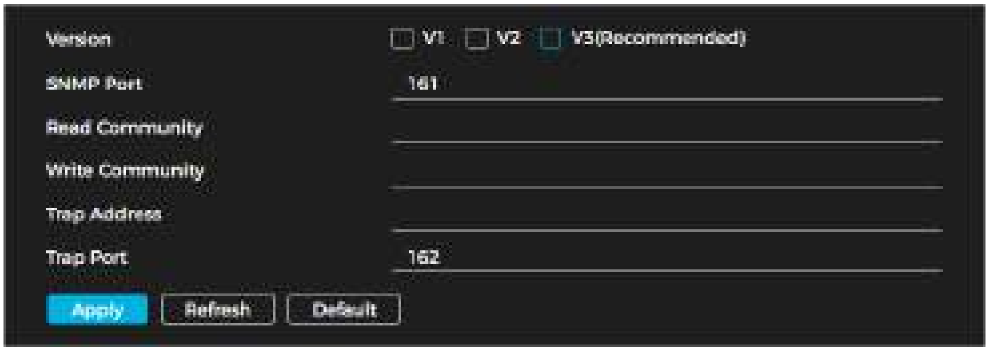
## SNMP

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:

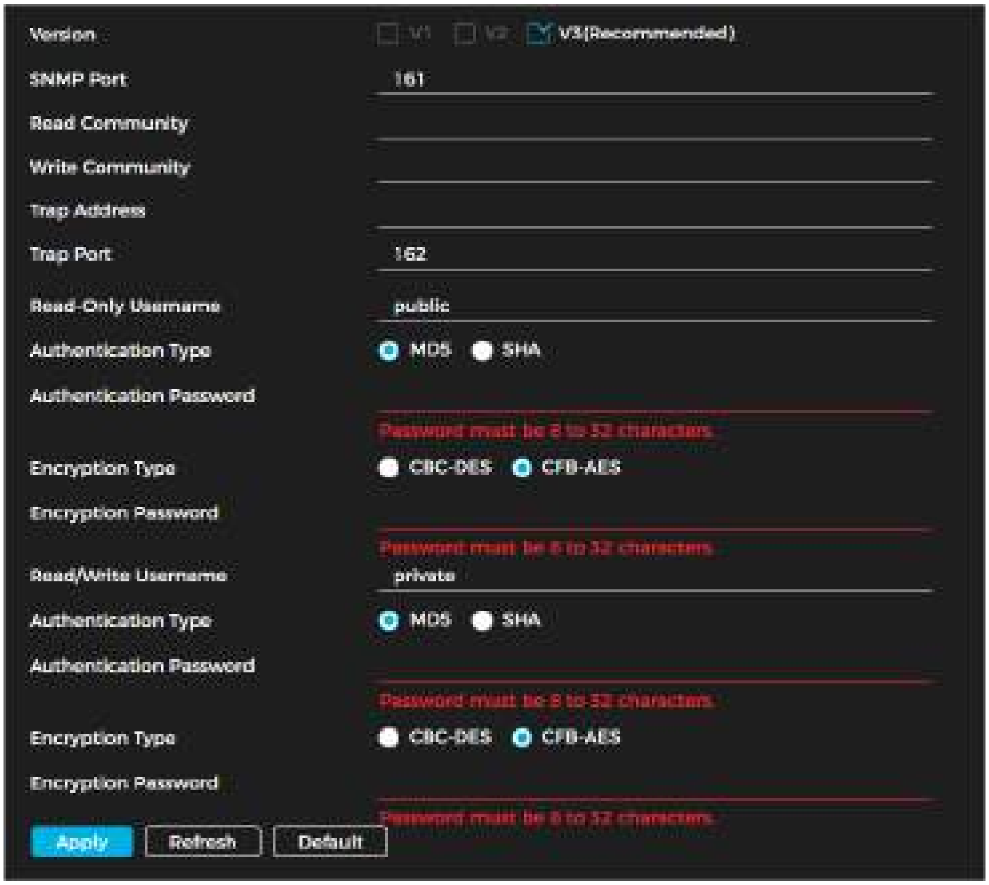
- Install SNMP monitoring and management tools such as MIB Builder and MG-SOFT MIB Browser.
- Obtain the MIB file matching the device version from technical support.

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.<br>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.<br>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.<br>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.

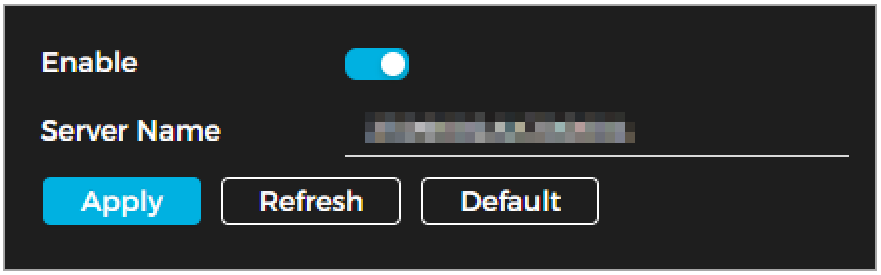
ⓘ Use a Windows PC and disable SNMP Trap service. MG-SOFT MIB Browser will display a prompt when an alarm is triggered.

### 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.

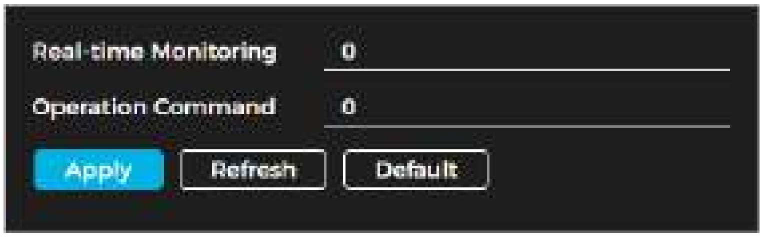
## QoS

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.

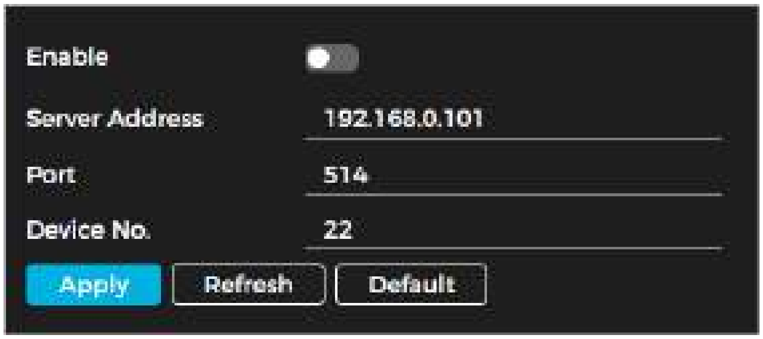
| Parameter | Description |
|---|---|
| Real-Time Monitor | Set the priority level for data packets used in network surveillance. The priority range is 0–63, with 0 being the lowest and 63 the highest. |
| Operation Command | Set the priority level for data packets used for configuration and status checks.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

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

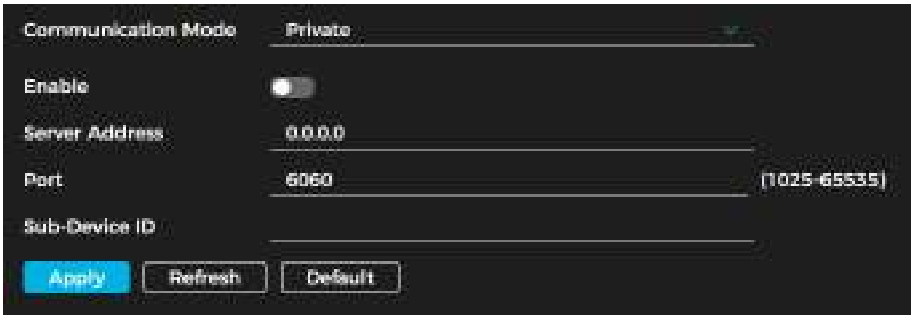
*Remote Log Parameters*

## 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

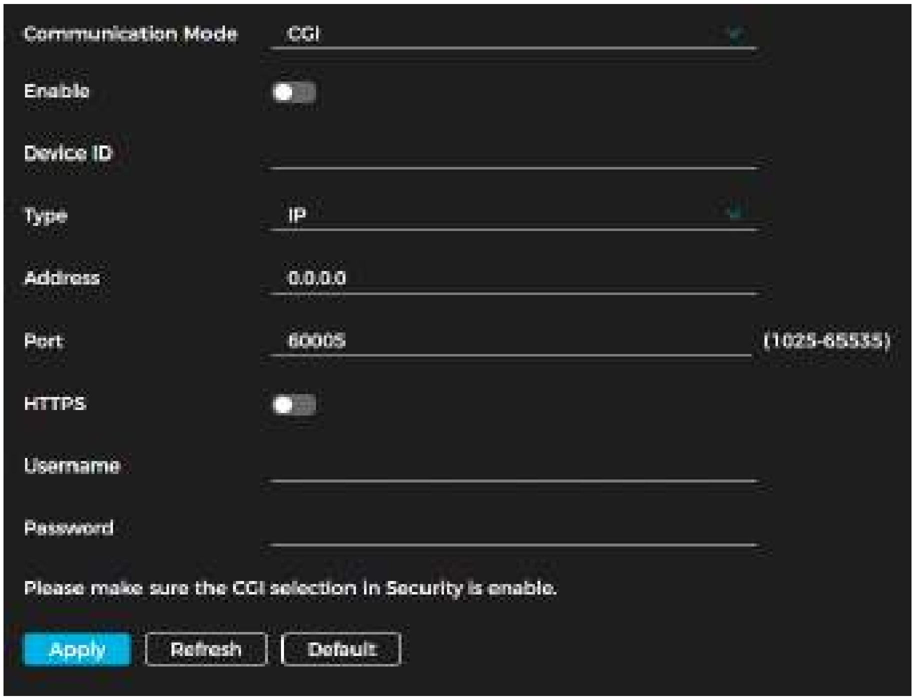
Enable ○

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. |
| Port | Registration port. |
| Sub-Device ID | Camera's custom ID. |
| Device ID | Camera's custom ID. |
| Type | Enter the IP address or domain name of the third-party platform. |
| IP | |
| Domain Name | |
| 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.

ⓘ

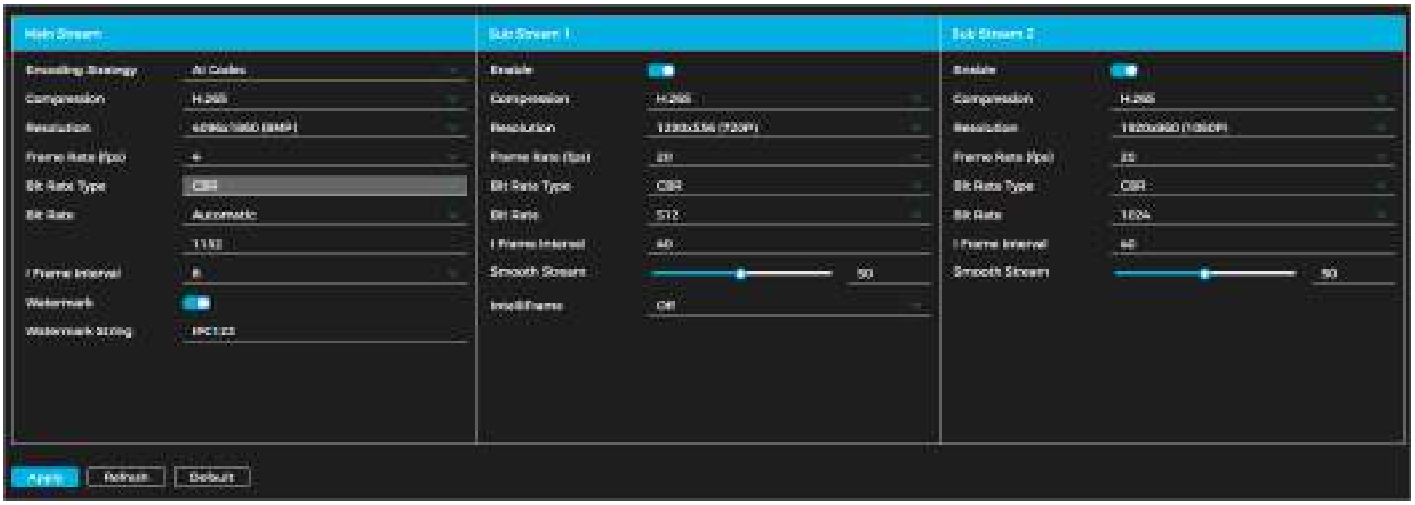
- Click **Default** to restore the device to its default configuration.

- 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: AI Codec<br>
Compression: H.265<br>
Resolution: 4096x1800 (8MP)<br>
Frame Rate (fps): 4<br>
Bit Rate Type: CBR<br>
Bit Rate: Automatic<br>
1152<br>
I Frame Interval: 8<br>
Watermark: ●<br>
Watermark String: IPC123

Sub Stream 1

Enable: ●<br>
Compression: H.265<br>
Resolution: 1280x536 (720P)<br>
Frame Rate (fps): 20<br>
Bit Rate Type: CBR<br>
Bit Rate: 512<br>
I Frame Interval: 40<br>
Smooth Stream: 50<br>
IntelliFrame: Off

Sub Stream 2

Enable: ●<br>
Compression: H.265<br>
Resolution: 1920x800 (1080P)<br>
Frame Rate (fps): 25<br>
Bit Rate Type: CBR<br>
Bit Rate: 1024<br>
I Frame Interval: 40<br>
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.<br>• **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:<br>• **CBR (Constant Bit Rate)**: The bit rate remains stable and stays close to the defined value.<br>• **VBR (Variable Bit Rate)**: The bit rate adjusts based on changes in the monitoring scene.<br>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.<br>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.<br>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 four.

## 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**.
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.

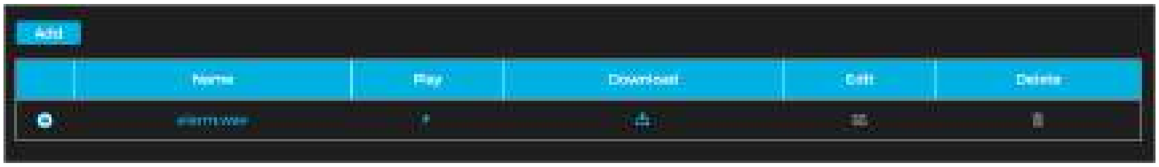
| Parameter | Description |
|---|---|
| Encoding Mode | Choose the audio encoding mode from PCM, G.711A, G.711Mu, or AAC.<br>The selected audio encoding mode applies to both audio recording and intercom. Using the default setting is recommended. |
| Sampling Rate | The sampling rate represents the number of audio samples taken per second. A higher sampling frequency results in more samples, leading to a more accurate restored signal.<br>Select an audio sampling rate from 8000, 16000, 32000, 48000, or 64000. |
| Audio Input Type | • **LineIn:** Requires an external audio device.<br>• **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

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**.



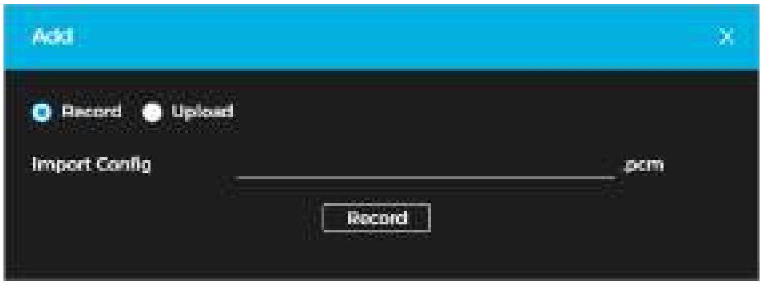
Add

| | 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.



Add ✕

● Record ○ Upload

Import Config ______ .pcm

Record

*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.

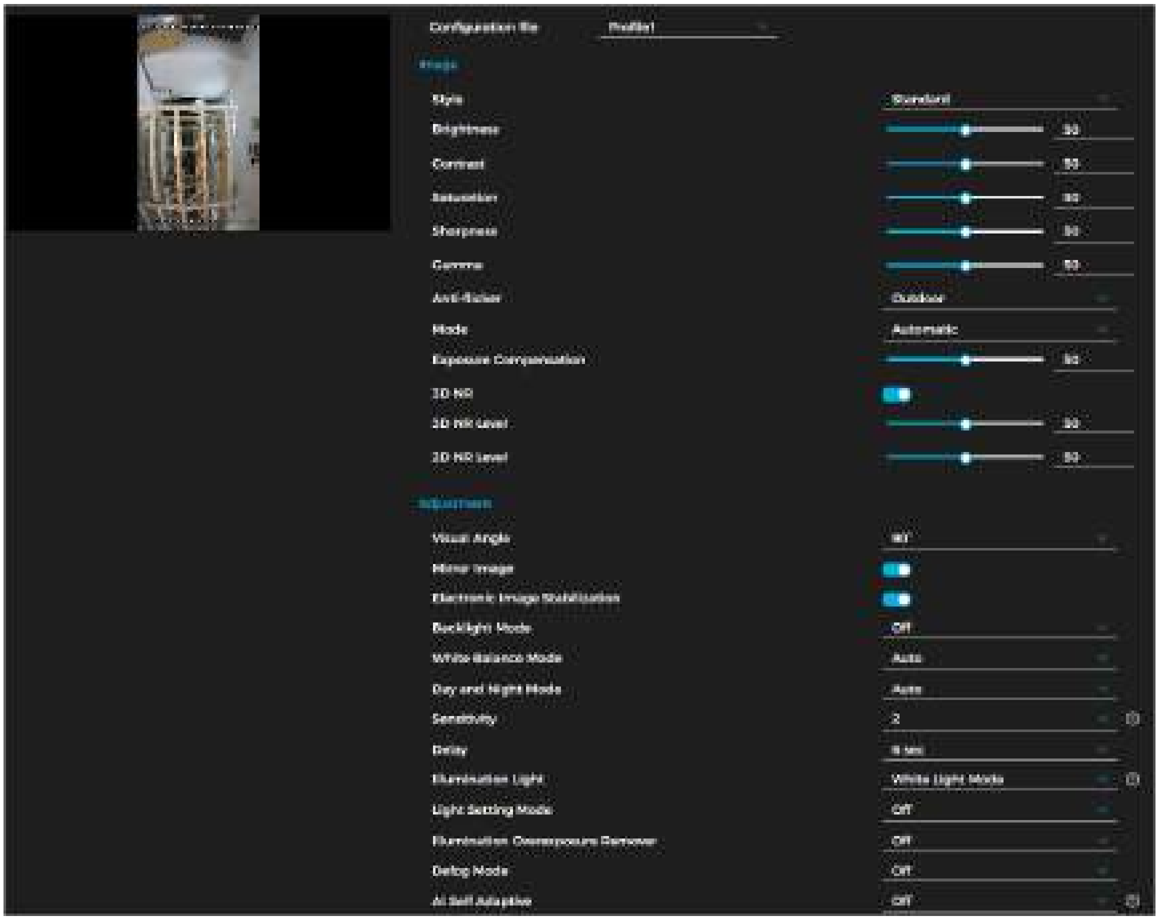
ⓘ Parameters may vary depending on device model.

## Display

### Display Settings

Follow the steps below to configure the display parameters.

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



Configuration file: Profile1

Image

Style: Standard

Brightness: 50

Contrast: 50

Saturation: 50

Sharpness: 50

Gamma: 50

Anti-flicker: Outdoor

Mode: Automatic

Exposure Compensation: 50

3D NR

3D NR Level: 50

2D NR Level: 50

Adjustment

Visual Angle: 90°

Mirror Image

Electronic Image Stabilization

Backlight Mode: Off

White Balance Mode: Auto

Day and Night Mode: Auto

Sensitivity: 2

Delay: 5 sec

Illumination Light: White Light Mode

Light Setting Mode: Off

Illumination Overexposure Remover: Off

Defog Mode: Off

AI Self Adaptive: 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:<br>• **Standard**: Default image style. Displays colors as they appear naturally.<br>• **Soft**: Reduces hue intensity and contrast. Images appear lighter.<br>• **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. |

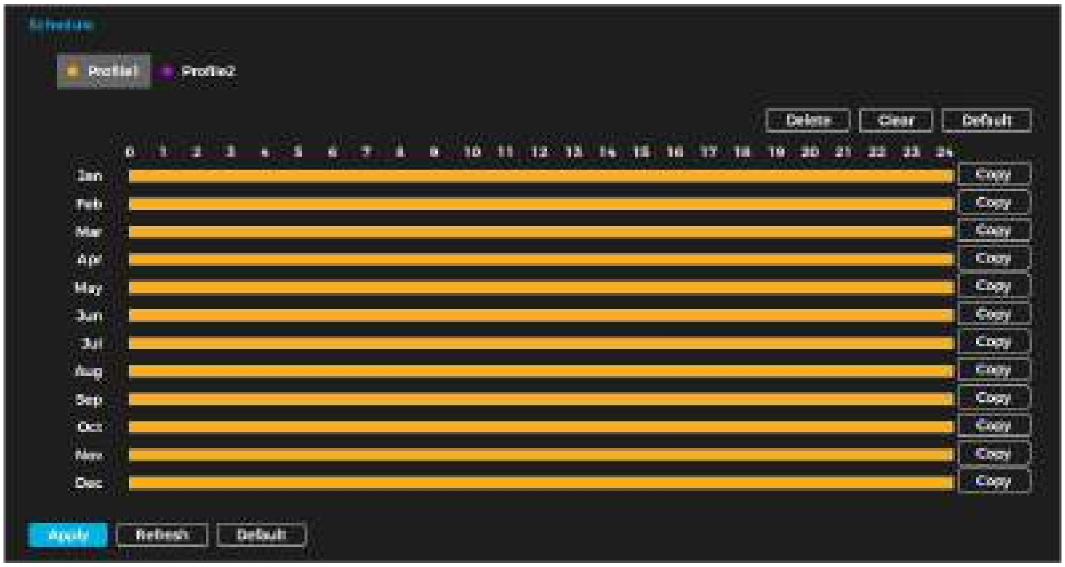
| | |
|---|---|
| Sharpness | Adjust the sharpness to control the clarity of picture edges. A higher value makes edges sharper and more defined. A lower value results in softer edges, reducing sharpness. If set too high, image noise may become more noticeable. |
| Gamma | Adjust the brightness and enhance 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:<br>• **50 Hz**: Adjusts exposure based on ambient light when the power supply is 50 Hz, preventing flickering or stripes.<br>• **60 Hz**: Adjusts exposure based on ambient light when the power supply is 60 Hz, preventing flickering or stripes.<br>• **Outdoor**: Allows selection of any exposure mode based on requirements. |
| Mode | Refers to device exposure modes. Choose between:<br>• **Automatic**: Automatically adjusts image brightness based on real-time conditions.<br>• **Manual**: Allows manual configuration of gain and shutter value to control image brightness |
| Shutter | Set the effective exposure time. A smaller value results in a shorter exposure time. |
| Gain | When 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. |
| 3D NR | Uses multi-frame processing (at least 2 frames) to reduce noise by analyzing frame information from both previous and subsequent frames. |
| 3D NR Level | This configuration is available only when 3D NR (Noise Reduction) is enabled.<br>A higher level provides better noise reduction results |
| 2D NR Level | |
| Visual Angle | Adjust the image display direction as needed. |
| Mirror Image | Click ○ to enable the function, flipping the image horizontally so that the left and right sides are reversed. |
| Electronic Image Stabilization | Click ○ to enable the function. |
| Backlight Mode | Adjust the backlight compensation mode for the monitoring screen.<br>• **Off**: Disables backlight compensation.<br>• **BLC (Backlight Compensation)**: Balances areas with extreme brightness or darkness to maintain a normal exposure for the main subject.<br>• **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.<br>• **WDR (Wide Dynamic Range)**: Reduces overexposure in bright areas and enhances details in dark areas for improved clarity.<br>• **Scene-Adaptive**: Automatically adjusts image brightness based on ambient lighting conditions to optimize 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.<br>• **Natural**: Optimizes white balance for environments without artificial light to maintain color accuracy.<br>• **Streetlamp**: Adjusts white balance for outdoor night scenes, ensuring correct color representation.<br>• **Outdoor**: Automatically balances white in most outdoor environments, whether under natural or artificial light.<br>• **Manual**: Allows manual adjustment of red and blue gain, while the system compensates based on color temperature.<br>• **Custom Area**: Applies white balance correction only to a specific area, ensuring color accuracy based on color temperature in that region |
| Day and Night Mode | Configure the image display mode based on lighting conditions:<br>• **Auto**: Automatically switches between color and black-and-white based on ambient lighting.<br>• **Color**: Displays the image in full color mode.<br>• **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.<br>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.<br>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. |
| Illumination Light | Configure the illumination mode by selecting one of the following options:<br>• **IR Mode**: Uses infrared light for night vision in low-light conditions.<br>• **White Light Mode**: Uses visible white light to enhance image clarity.<br>• **LumiLuxSmart**: Automatically adjusts IR and white light based on the scene for optimal illumination. |
| Light Setting Mode | You can choose from Manual, Auto, or Off modes.<br>• **Manual**: Allows manual adjustment of brightness based on actual needs.<br>• **Auto**: Automatically adjusts brightness according to ambient lighting conditions.<br>• **Off**: Disables illumination. |
| Illumination Overexposure Remover | Configure illumination overexposure removal by selecting one of the following options: **Off** or **General**.<br>This function is supported only in specific fill light modes. |
| Defog Mode | In foggy or hazy environments, the defog function enhances image clarity.<br>• **Manual**: Manually configure function intensity and atmospheric light mode to improve clarity. The atmospheric light mode can be set to automatic or manual.<br>• **Auto**: The system automatically adjusts image clarity based on real-time conditions.<br>• **Off**: Disables the defog function. |

| | |
|---|---|
| AI Self-Adaptive | Select On to enable this function. The camera will automatically adjust the image based on the environment. |

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.



*Profile Schedule Setting*

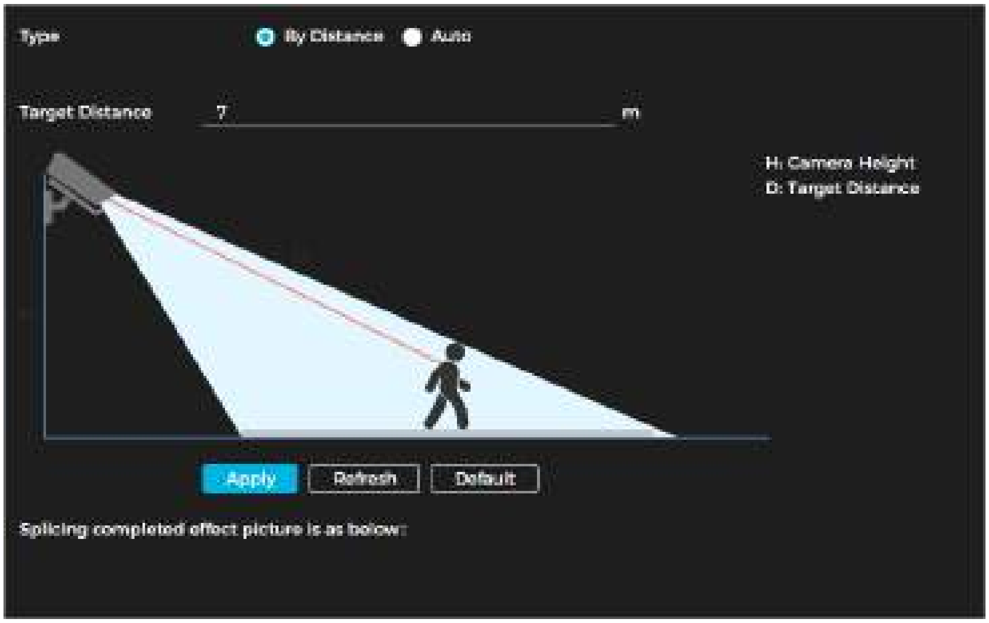
6. Click **Apply**.

## Splicing

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

2. Select the type of splicing: **By Distance** or **Auto**.

- **By Distance**: Set the splicing distance for the detected object, then click **Apply**. The system will automatically display the corresponding splicing result.



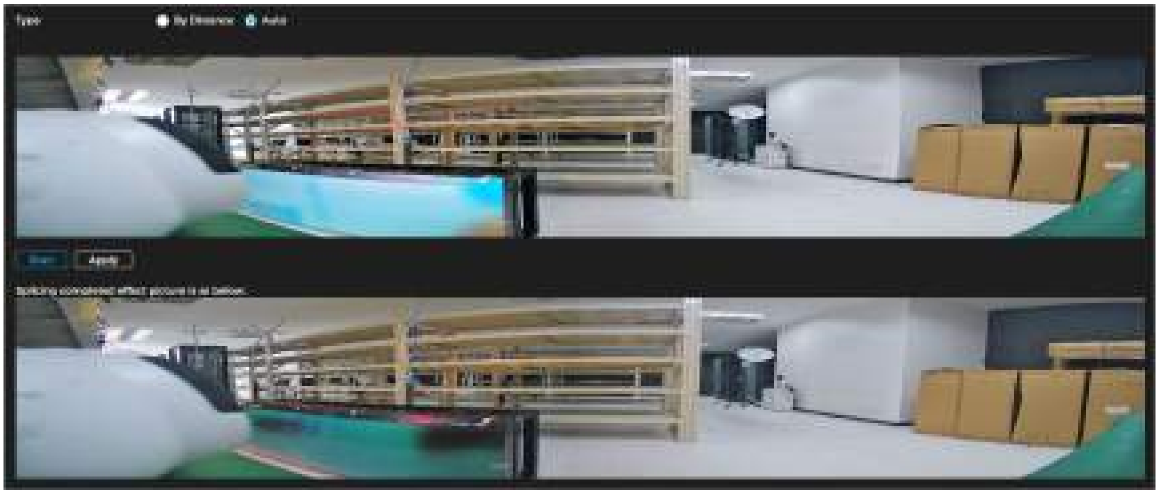
Type ● By Distance ○ Auto

Target Distance 7 m

Splicing completed effect picture is as below:

*Splice by Distance*

- **Auto**: Click **Start**. Wait three minutes. The system will display the results after the splicing is complete. Review the results and click **Apply**.

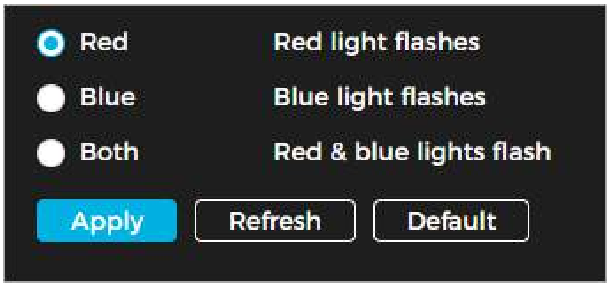


*Auto Splicing*

## Warning Light

Follow the steps below to configure the warning light for the camera.

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



● Red Red light flashes
○ Blue Blue light flashes
○ Both Red & blue lights flash

*Warning Light Parameters*

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

| Parameter | Description |
|---|---|
| Red | Set the warning light to flash red. |
| Blue | Set the warning light to flash blue. |
| Both | Set the warning light to flash both red and blue. |

3. Click **Apply**.

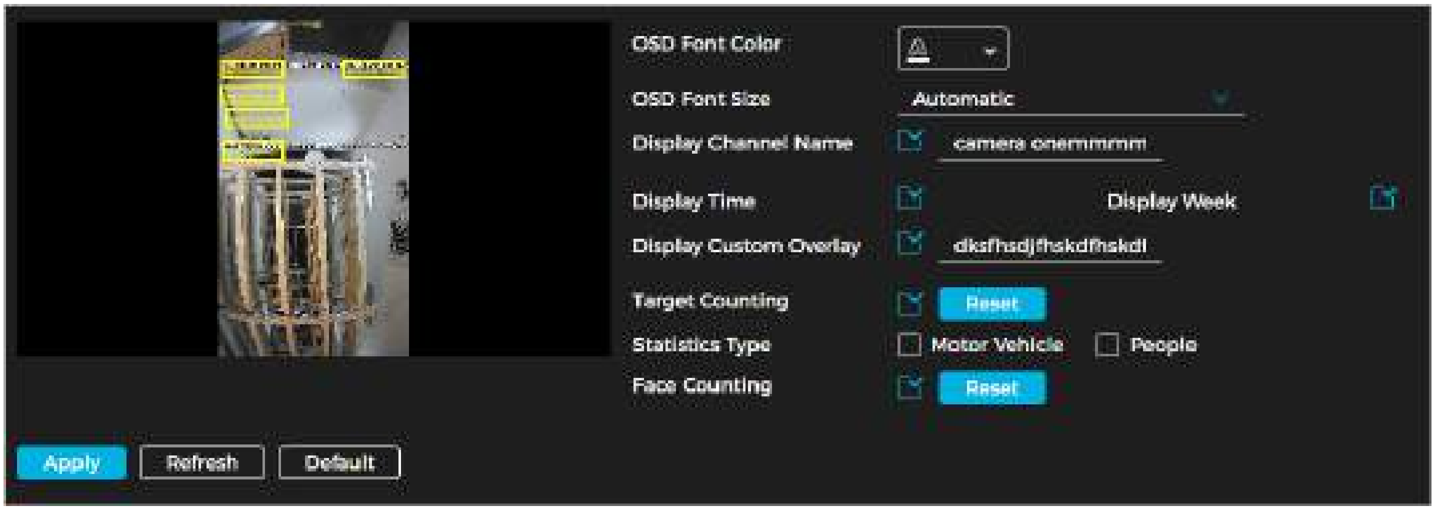
# OSD

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

1. Navigate **Settings → Images → OSD**.
2. Specify the color and size of the OSD information as required.

ⓘ Parameters may vary depending on device model.

3. Set the display information.
4. Click **Apply**.



OSD Font Color ☐
OSD Font Size Automatic
Display Channel Name ☑ camera onemmmmm
Display Time ☑ Display Week ☑
Display Custom Overlay ☑ dksfhsdjfhskdfhskdl
Target Counting ☑ Reset
Statistics Type ☐ Motor Vehicle ☐ People
Face Counting ☑ Reset

*OSD*

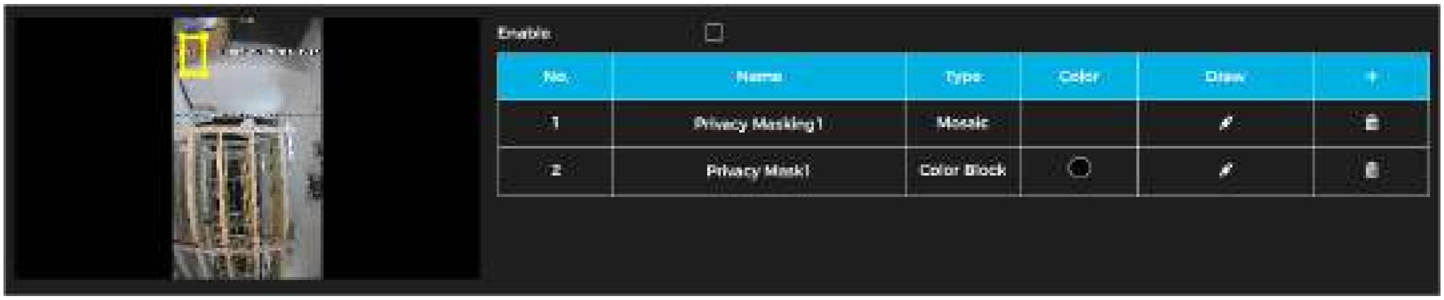
## Privacy Mask

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 | Draw | + |
|---|---|---|---|---|---|
| 1 | Privacy Masking1 | Mosaic | | ✎ | 🗑 |
| 2 | Privacy Mask1 | Color Block | ● | ✎ | 🗑 |

*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 🗑.

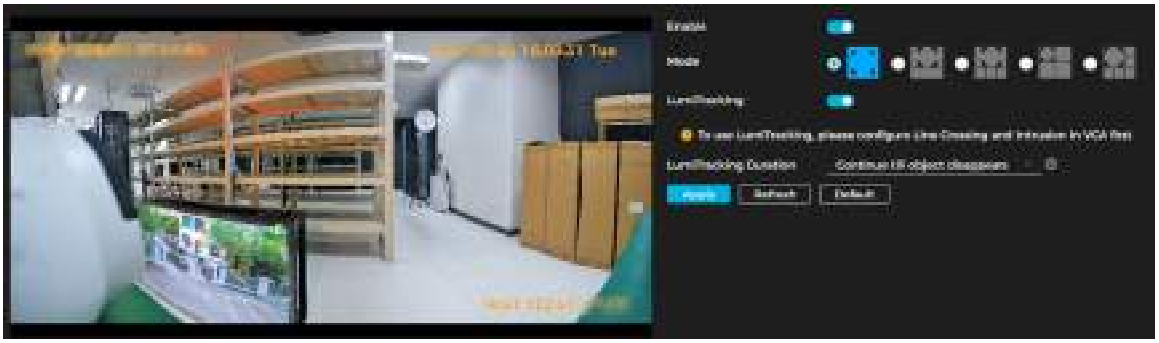
# LumiTracking

The LumiTracking function allows simultaneous zooming and tracking of multiple humans and vehicles that trigger alarms. It provides both detailed close-ups and a panoramic view.

ⓘ LumiTracking is only available on select devices.

Follow the steps below to enable this function.

1. Navigate to **Settings → LumiTracking**.



Enable ●

Mode ● ⛶ ○ ○ ○ ○

LumiTracking ●

To use LumiTracking, please configure Line Crossing and Intrusion in VCA first

LumiTracking Duration: Continue till object disappears

*LumiTracking*

2. Click ○ to enable the function.
3. Select the display mode. See the table below for more details.

| Mode | Description |
|---|---|
| ⛶ | Displays original screen. |
| ⛶<br>▭ | Displays the original screen and one sub-screen. |
| ⛶<br>▭▭▭ | Displays the original screen and three sub-screens. |
| ⊞ | |
| ⛶⊟<br>▭▭▭ | Displays the original screen and five sub-screens. |

ⓘ You can zoom in or drag the sub-screen images within the original screen.

4. (Optional) Enable the LumiTracking checkbox and select the LumiTracking duration mode (**Automatic** or **Continue till Object Disappears**).

ⓘ

- **Automatic**: Manually set the tracking duration. For example, if the duration is set between 30 to 60 seconds, the camera will track Object A for at least 30 seconds. If Object B appears, the camera will switch to track Object B. If no other object appears, the camera will stop tracking Object A after 60 seconds.
- **Continue till Object Disappears**: The camera will track the detected object until it completely disappears from the image.

5. Click **Apply**.

# 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

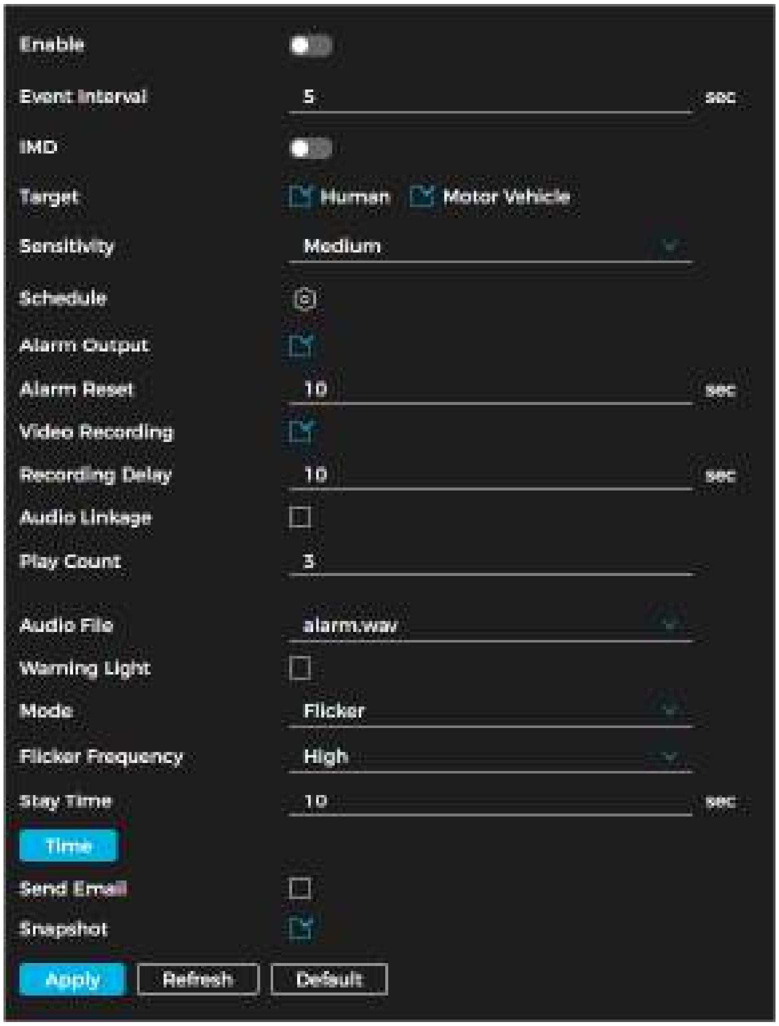
If motion detection is configured, the system performs any assigned alarm linkage actions when a moving object appears in the image and its speed exceeds the configured sensitivity threshold.

ⓘ

- 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 | ○ | |
| Event Interval | 5 | sec |
| IMD | ○ | |
| Target | ☑ Human ☑ Motor Vehicle | |
| Sensitivity | Medium | |
| Schedule | ⚙ | |
| Alarm Output | ☑ | |
| Alarm Reset | 10 | sec |
| Video Recording | ☑ | |
| Recording Delay | 10 | sec |
| Audio Linkage | □ | |
| Play Count | 3 | |
| Audio File | alarm.wav | |
| Warning Light | □ | |
| Mode | Flicker | |
| Flicker Frequency | High | |
| Stay Time | 10 | sec |
| Send Email | □ | |
| Snapshot | ☑ | |

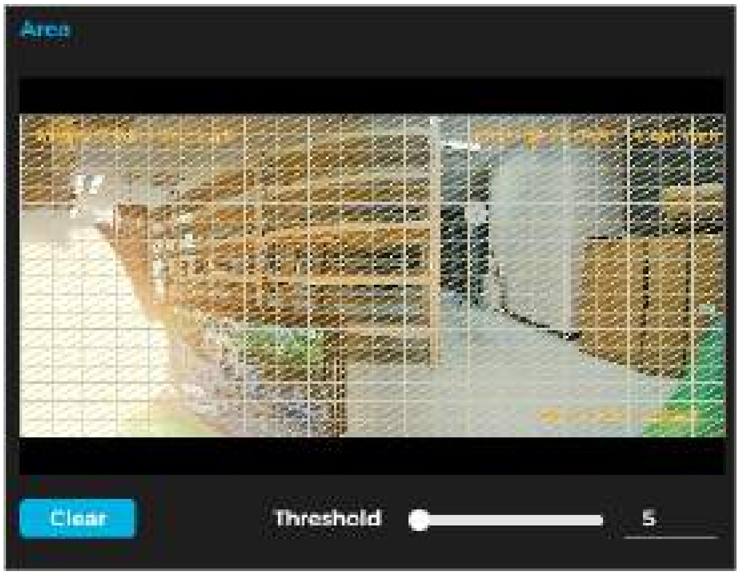
*Motion Detection*

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*

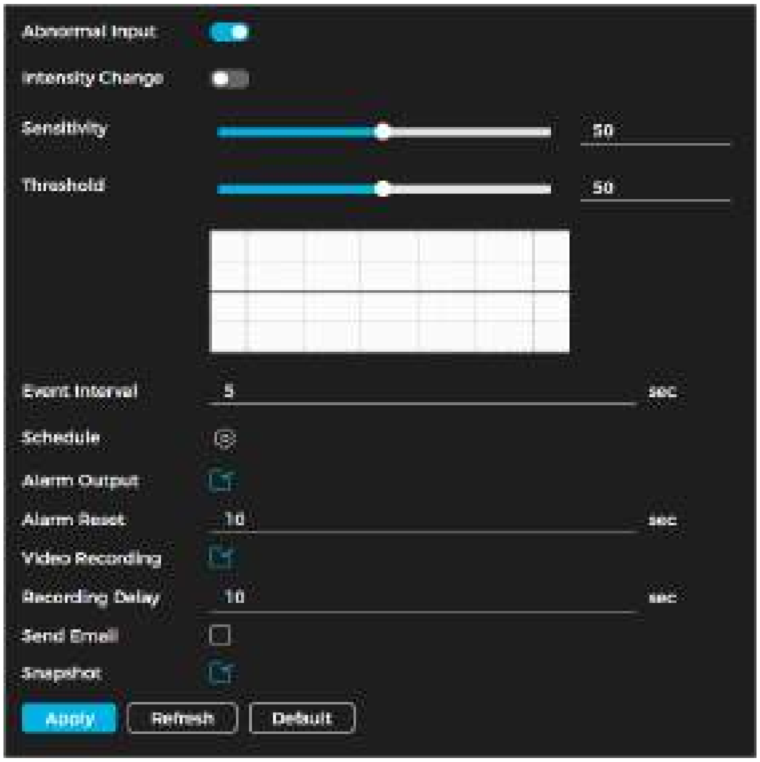
4. (Option) Click ○ next to IMD to enable the function. Select the target type and alarm sensitivity.
5. Set the arming schedule and alarm linkage actions. See the **Alarm Linkage** section of this manual for more information.
6. Click **Apply**.

## 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.<br>ⓘ<br>• A higher sensitivity or smaller threshold makes it easier to trigger an alarm. In noisy environments, set a higher threshold to reduce false alarms.<br>• 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

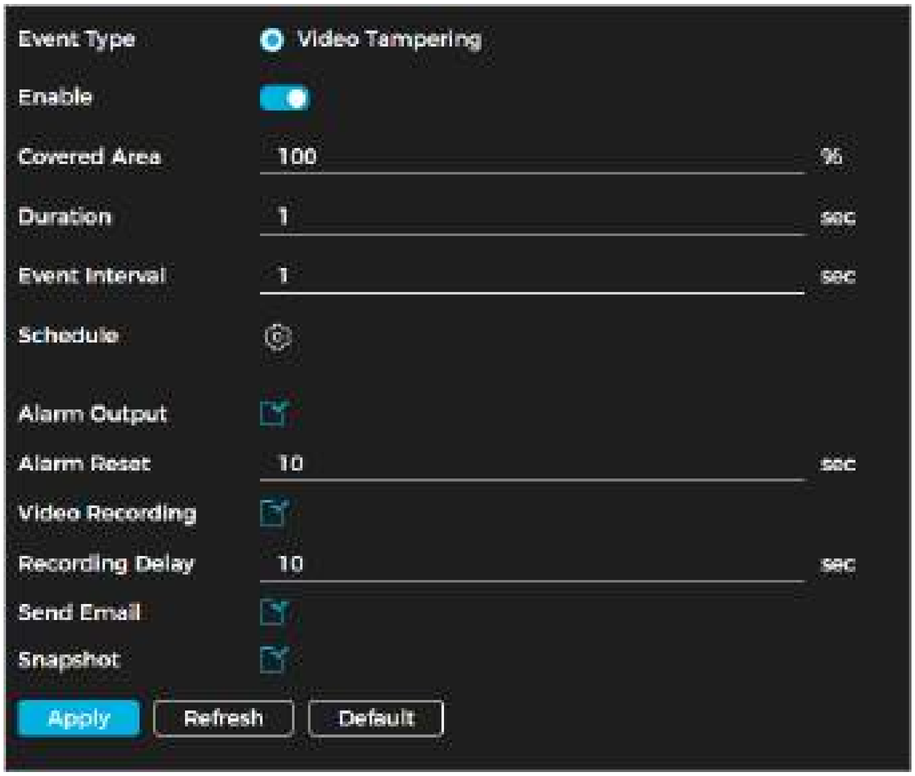
If video tampering is configured, the system performs any assigned alarm linkage actions when the lens is obscured, or the video color output is monochrome due to light or other reasons.

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 or Defocus Detection.

ⓘ

- **Video Tampering**: Triggers an alarm when the tampered image percentage and duration exceed the configured thresholds.
- **Defocus Detection**: Triggers an alarm when the image becomes blurred. This function is available on select models.



Event Type ● Video Tampering

Enable

Covered Area 100 %

Duration 1 sec

Event Interval 1 sec

Schedule

Alarm Output ☑

Alarm Reset 10 sec

Video Recording ☑

Recording Delay 10 sec

Send Email ☑

Snapshot ☑

| Parameter | Description |
|---|---|
| Covered Area | An alarm is triggered when the tampered image percentage and duration exceed the configured thresholds. |
| Duration | |
| Event Interval | Records only one alarm event within the configured event interval period. |

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

4. Click **Apply**.

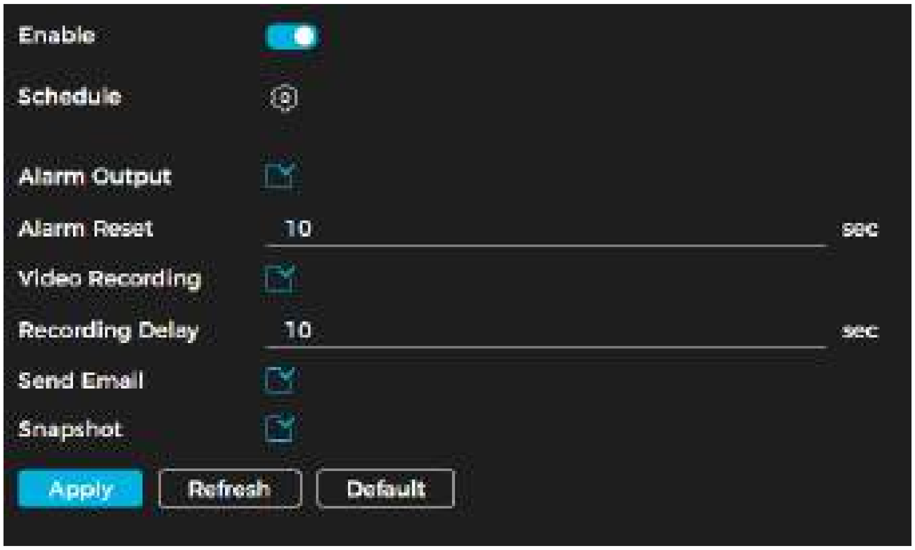
## How to Set a Scene Changing Alarm

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

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**.

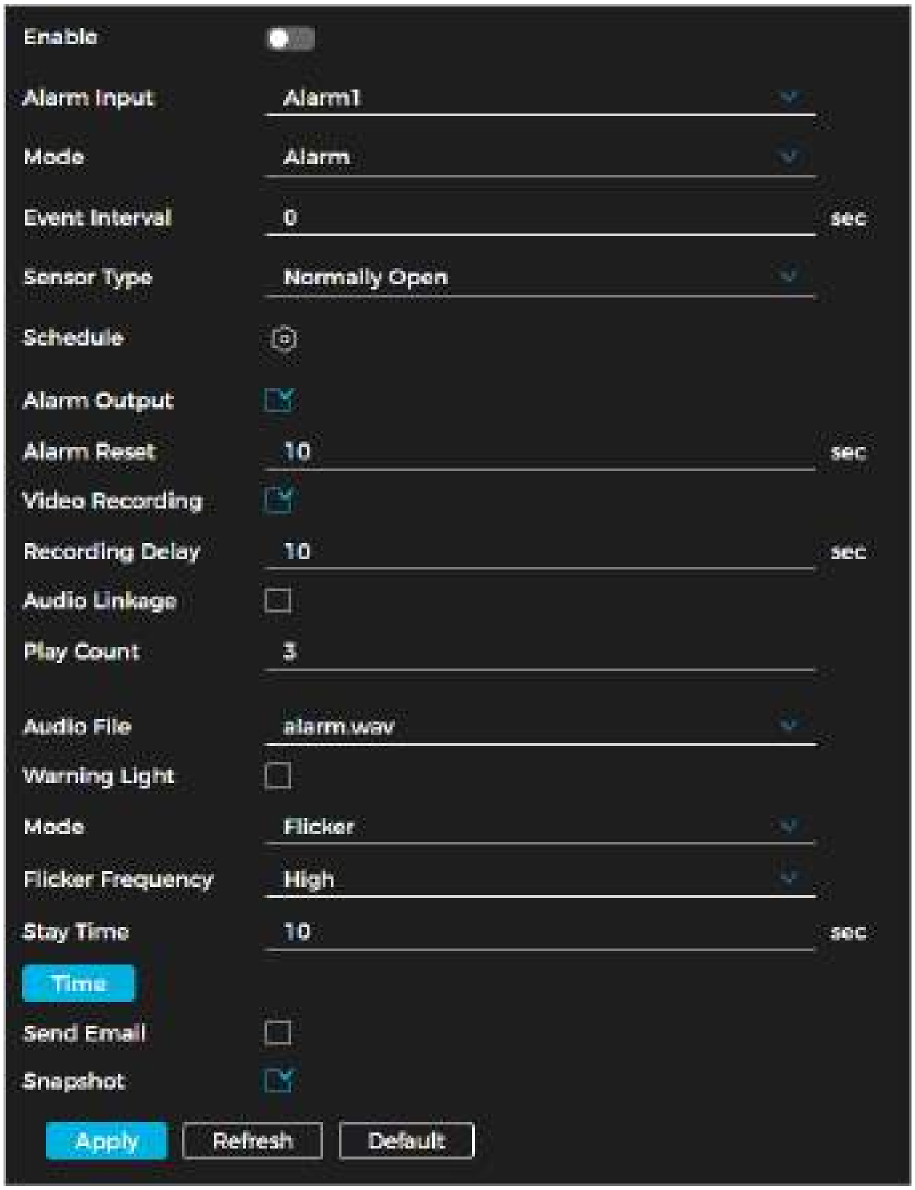
### Alarm Linkage

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 Linkage.
2. Click ○ to enable the function.
3. Choose the alarm input.
4. Select the mode.

- **Alarm**: When an alarm is triggered by a device connected to the alarm-in port, the system executes the configured alarm linkage actions.
    - Configure the sensor time (normally open or normally closed).
    - Configure the event interval. Only one alarm event can be recorded during the interval period.
    - Select the schedule and alarm linkage actions.



Enable ○

Alarm Input: Alarm1

Mode: Alarm

Event Interval: 0 sec

Sensor Type: Normally Open

Schedule

Alarm Output ☑

Alarm Reset: 10 sec

Video Recording ☑

Recording Delay: 10 sec

Audio Linkage □

Play Count: 3

Audio File: alarm.wav

Warning Light □

Mode: Flicker

Flicker Frequency: High

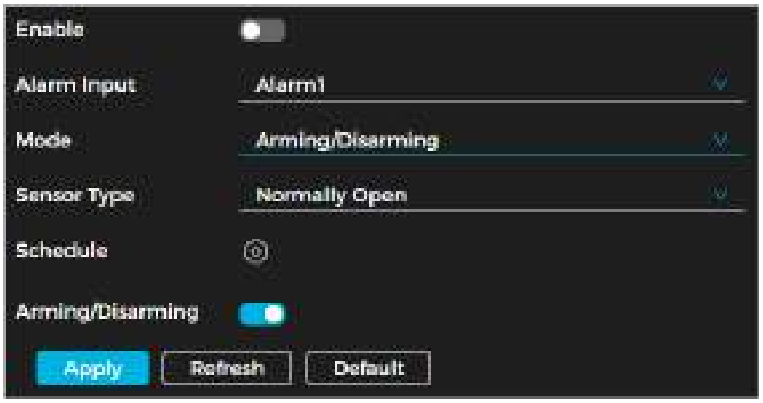
Stay Time: 10 sec

Send Email □

Snapshot ☑

*Mode (Alarm)*

- **Arming/Disarming**: Enable or disable the arming functions of the alarm input device.



Enable ○

Alarm Input: Alarm1

Mode: Arming/Disarming

Sensor Type: Normally Open

Schedule

Arming/Disarming ●

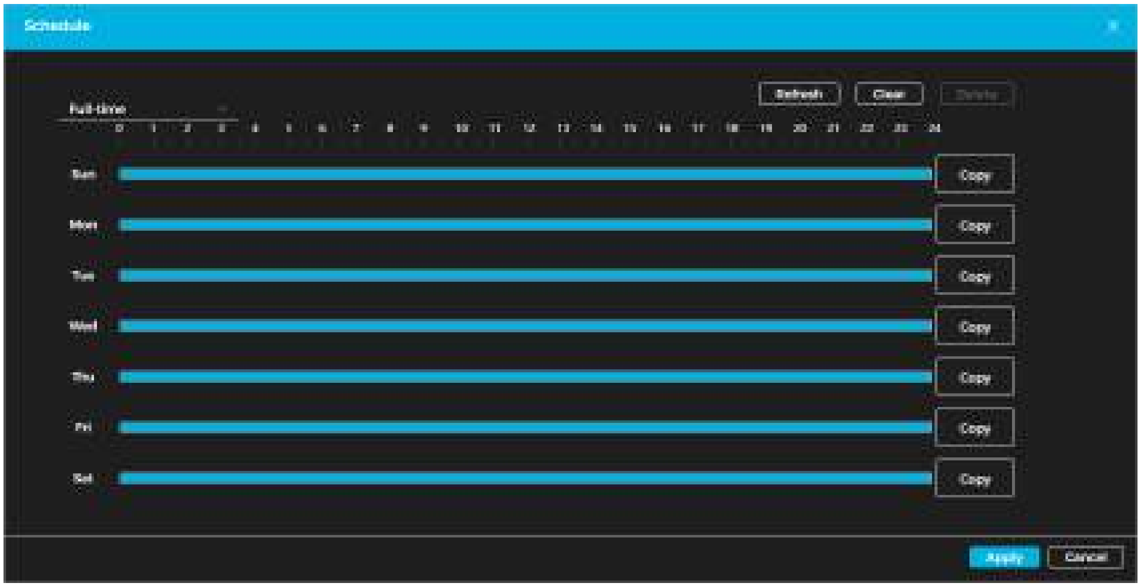
*Mode (Arming/Disarming)*

5. 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*

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.

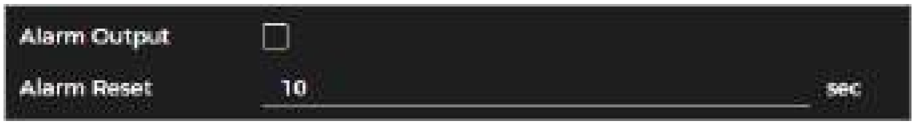
3. Click **Apply**.
4. (Optional) Click ⌄ and then **+ Schedule** to add a new table.
5. (Optional) Click 🗑 to delete tables as required.

## 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 □

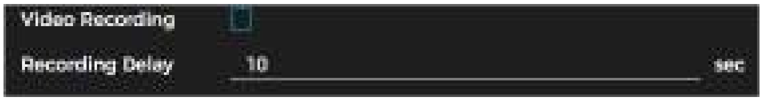
Alarm Reset 10 sec

*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 □

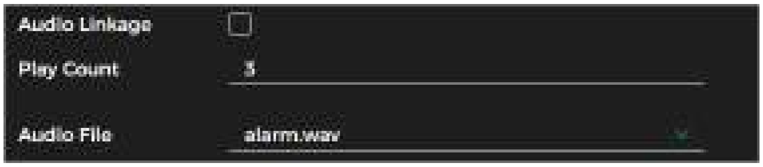
Recording Delay 10 sec

*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

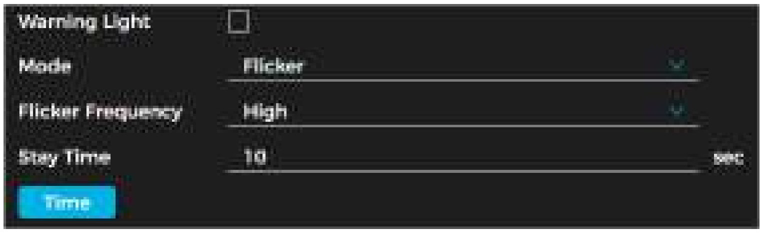
Audio File alarm.wav

*Audio Linkage*

## Warning Light Linkage

The system can link to a warning light with an alarm event occurs. Follow the steps below to enable this functionality.

1. Navigate to the **Alarm Linkage** page.
2. Click ■ to enable warning light linkage.
3. Select the mode.
4. Set the frequency.
5. Set the stay time.



Warning Light □

Mode Flicker

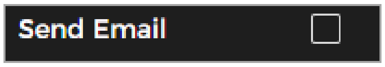
Flicker Frequency High

Stay Time 10 sec

*Warning Light 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.



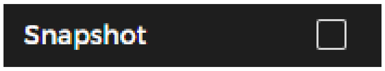
Send Email □

*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

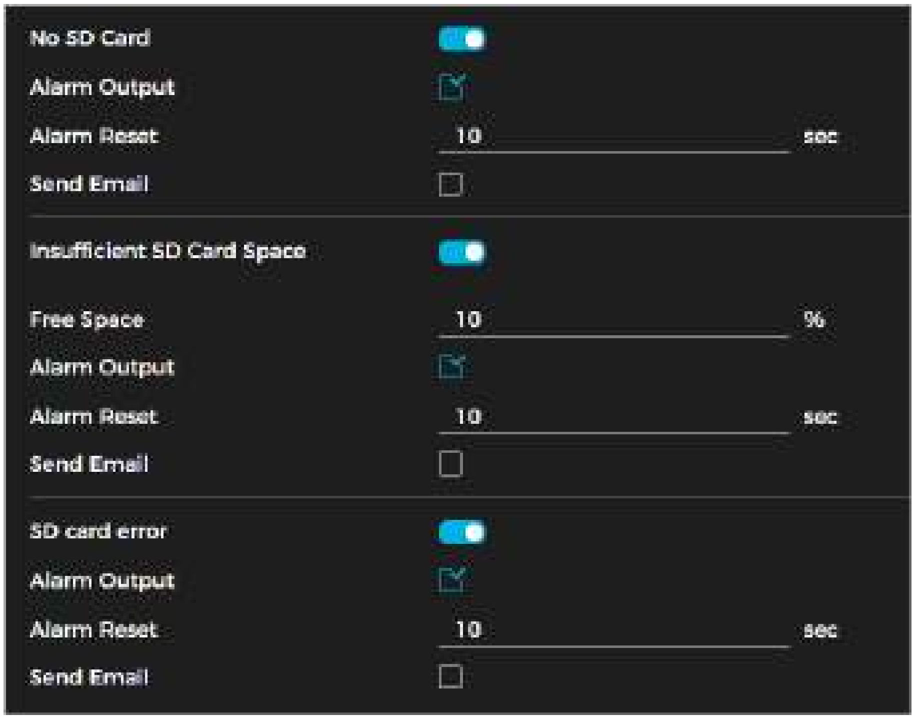
You can set up the system to inform you of exceptions and abnormalities. Abnormalities include issues related to the SD card, network, illegal access, voltage detection, and security exceptions.

## 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*

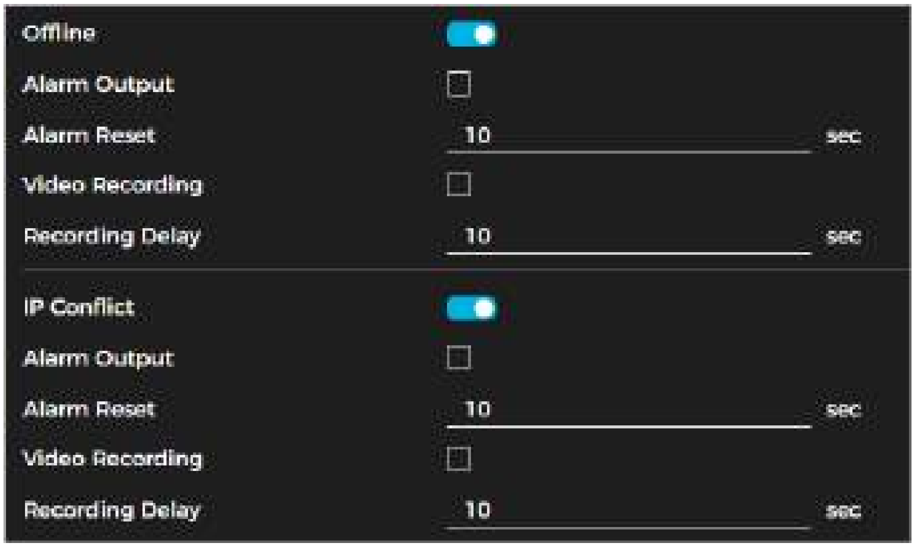
3. Set alarm linkage actions. See the **Alarm Linkage** portion of this manual for more information.
4. Click **Apply**.

## 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 Voltage Detection

The system can perform alarm linkage events if the input voltage is higher or lower than the rated value of the device. Follow the steps below to have the system to inform you of a voltage exception.

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

2. Click ○ to enable voltage detection functions. The alarm icon will appear as an overlay on the screen when an alarm is triggered if OSD is enabled.

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 **Disarming** (stop triggering alarm linkage actions entirely) or **Disarm by Period** (stop triggering alarm linkage actions during specific times).

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 |
| Voltage Detection | Triggered when the device detects abnormal voltage. | Voltage detection |

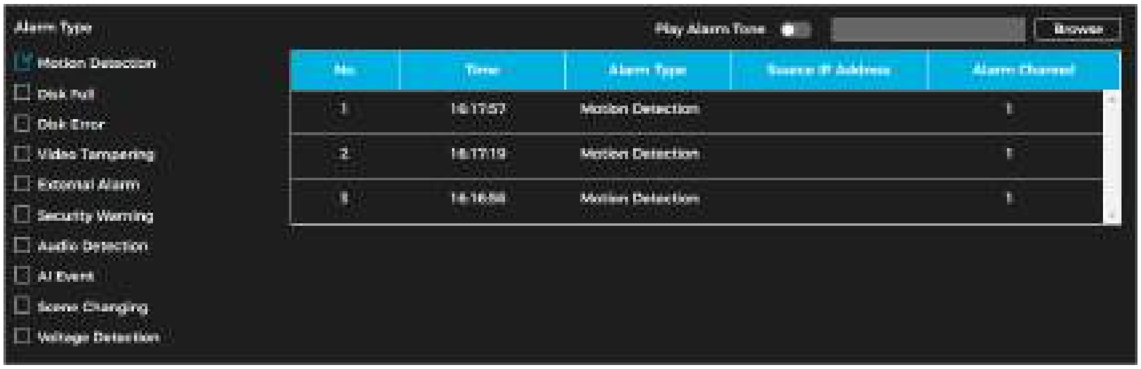
## Subscribing Alarm Information

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.



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

| No. | Time | Alarm Type | Source IP Address | Alarm Channel |
|---|---|---|---|---|
| 1 | 16:17:57 | Motion Detection | | 1 |
| 2 | 16:17:19 | Motion Detection | | 1 |
| 3 | 16:16:58 | Motion Detection | | 1 |

*Subscribing to an Alarm*

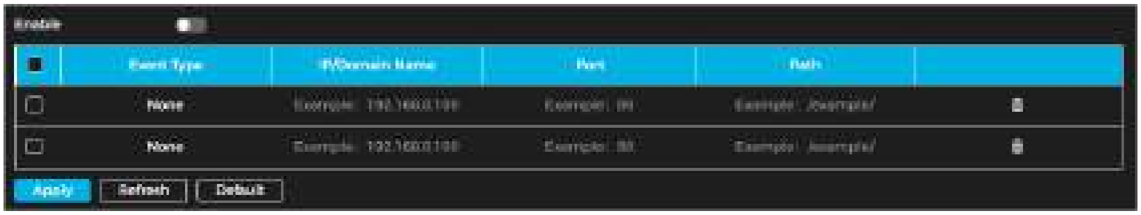
# How to Set Up a Network Destination

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**.



| ☐ | 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/ | |

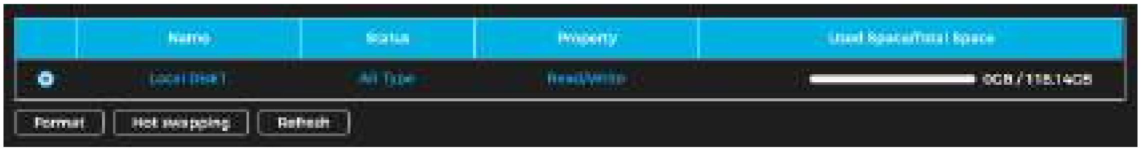
*Set Up a Network Destination*

# 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 Disk 1 | 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).