LUMINYS

License Plate Recognition (LPR) Camera

User Manual

Rev. 1

Foreword

General

This manual provides an overview of the functions, configuration, general operation, and system maintenance of the LPR 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	May 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 or visit our official website. Minor differences may exist between electronic and paper versions.
- All designs and specifications are subject to change without notice. Product updates may lead to discrepancies between the manual and the actual product. Contact customer service for the latest information and documentation.
- There may be errors or inaccuracies in the descriptions of functions, operations, and technical data. We reserve the right of final interpretation in case of questions or disputes.
- If the manual cannot be opened, please update your reader software or try another compatible reader.
- All trademarks and company names mentioned are the properties of their respective owners.
- For assistance, visit our website or contact your supplier or customer service.
- We reserve the right of final interpretation in case of questions or disputes.

Safety Instructions

The following symbols might appear in the manual.

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

Symbol	Definition
ⓘ	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.
- 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

The camera uses advanced algorithms to recognize license plates, colors, and more. It is equipped with a durable housing, built-in illuminator, and high-definition camera to deliver high-resolution images, excellent low-light performance, high frame rates, and accurate color reproduction. The camera is best suited for use in locations such as community roads, parking areas, and other access-controlled environments.

Functions

Functions may vary based on device model.

Permission Management

- Each user group defines specific permissions; individual users cannot have permissions beyond those assigned to their group.
- Supports two user levels.
- Includes permissions for barrier control and blocklist alarm functions.
- Allows device configuration and permission management over Ethernet.

Storage

- Stores video data on the central server according to the configured settings.
- Allows video recording via the webpage, with recordings saved locally on your computer.
- Supports local hot-swapping of storage cards and continues recording during network outages. The system automatically overwrites old data when storage is full.
- Can store up to 1,024 log entries.
- Supports FTP storage and Automatic Network Replenishment (ANR).

Alarm

- The camera triggers network alarms when issues occur, such as memory card failures.
- Certain devices support real-time response to external alarm inputs by connecting to alarm peripherals within 200 ms. The system handles alarms based on predefined linkages and can play custom voice prompts uploaded in advance.

Network Monitoring

- Compresses and transmits video data from a channel to the network terminal.
- Decompresses data for viewing.
- Keeps latency under 500 ms if bandwidth conditions permit.
- Supports up to 10 concurrent users.
- Allows system access and device management via a web browser.
- Video data transmission supports HTTP, TCP, UDP, MULTICAST, and RTP/RTCP protocols.

Capture and Recognition

- Identifies vehicle details including license plate, color, logo, and model.

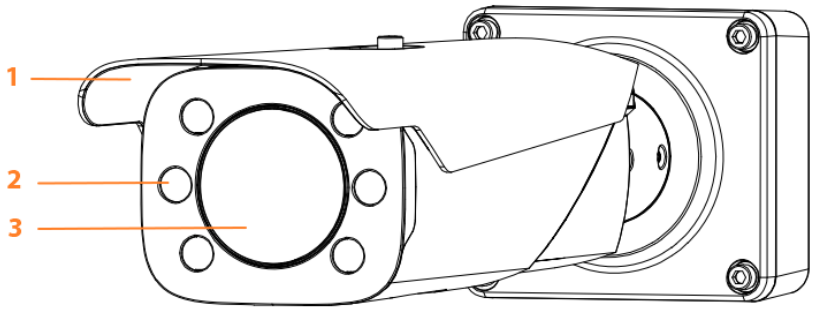
- Allows configuration of OSD (On-Screen Display) information.
- Supports video encoding, image snapshots, and watermark encryption to prevent tampering.

Peripheral Control

- Supports configuration of various peripheral control protocols and connection interfaces.
- Integrates with external devices such as vehicle detectors and signal detectors.

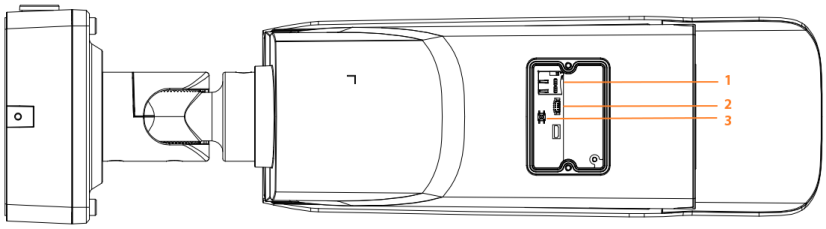
Structure

Appearance



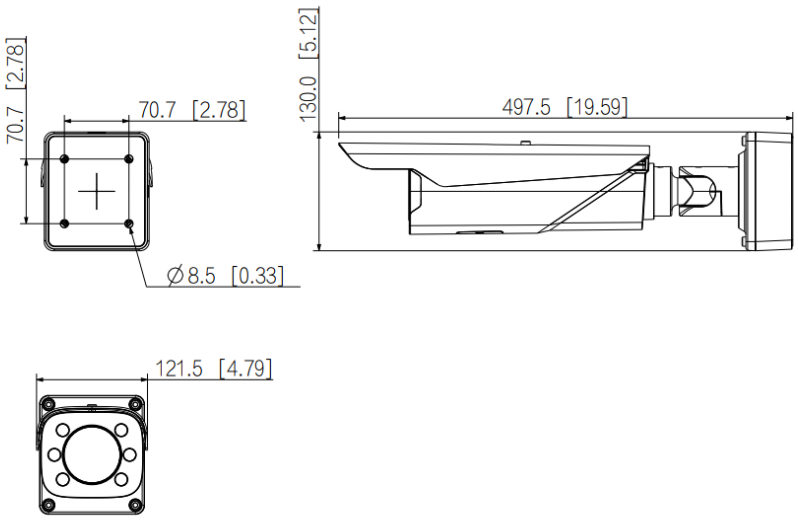
Number	Function
1	Protective Cover
2	Illuminator
3	Lens

Rear Panel

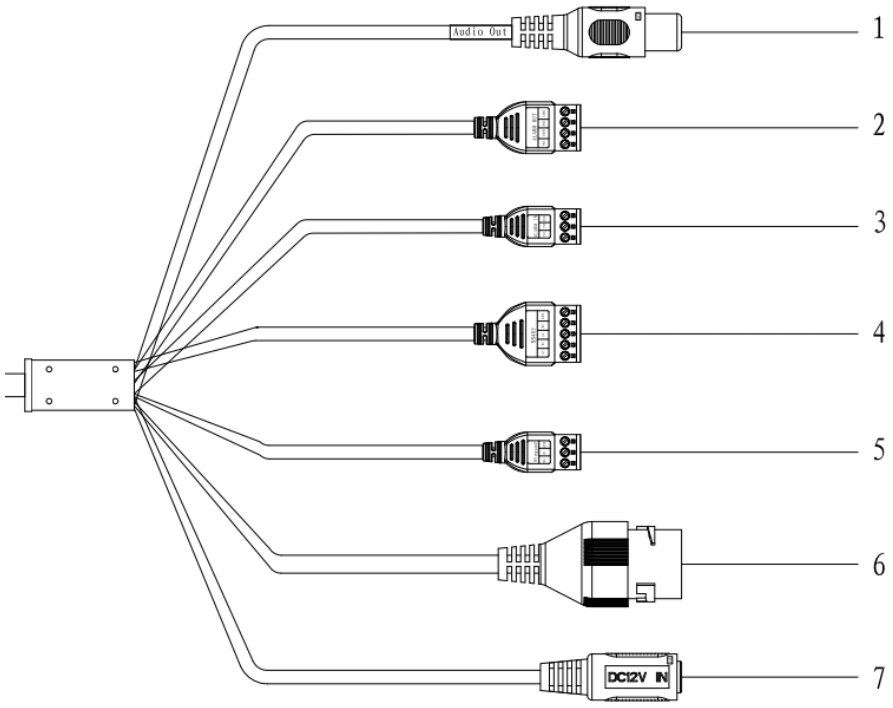


Number	Function
1	TC Card
2	Debugging Port
3	Hardware Reset Button

Dimensions (mm [in.])



Cable Connection



Number	Function	Description
1	Audio Out	Transmits audio output signals.
2	Alarm Out	Connects output and alarm devices.
3	Alarm In	Connects input devices such as vehicle detectors, IR detectors, and induction loops.
4	RS-485 Port	—

5	Wiegand Port	—
6	RJ-45 Port	—
7	12 VDC Input Port	—

Device Initialization

The camera is delivered uninitialized and must be initialized with a new password before use. Ensure the computer and camera IP addresses are on the same network segment; otherwise, the initialization page may not load.

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. Create and confirm a password. To change the password later, go to: **Setting → System → User Management → Account → User**.
3. Enter your email address.
4. Click **OK**.
5. Enter your username and password, then click **Login**. You will be automatically redirected to the Live View page.

Login

Log in to the Webpage

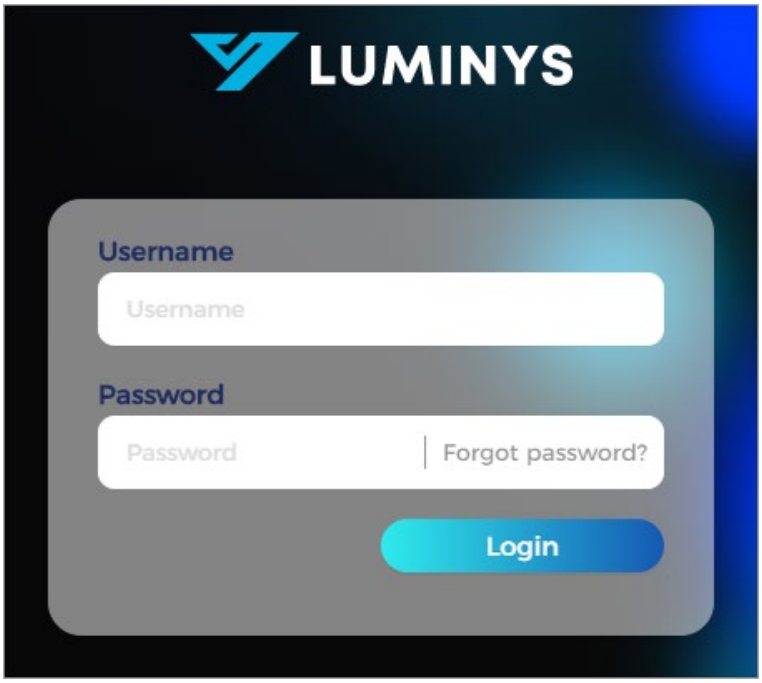
This section explains how to log in to the webpage, using Chrome as an example.

ⓘ

- 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**.

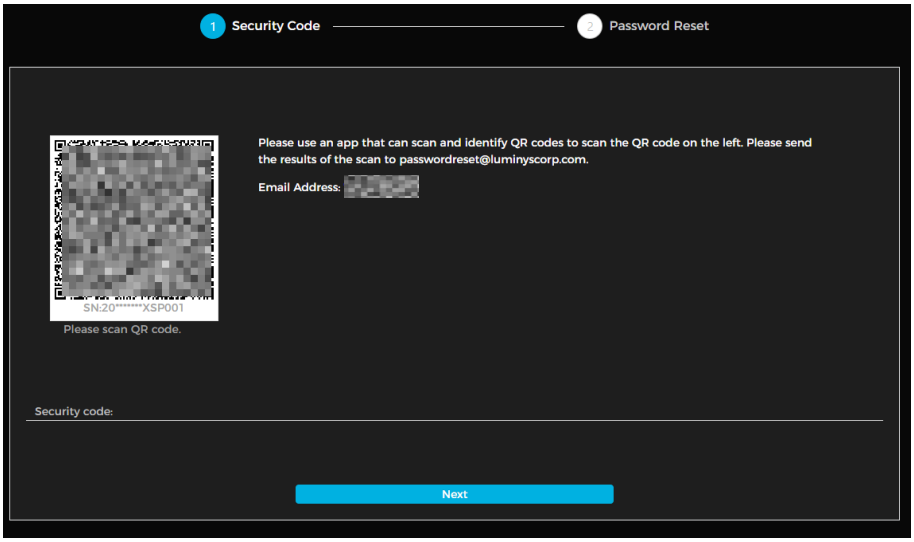
Password Reset

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.

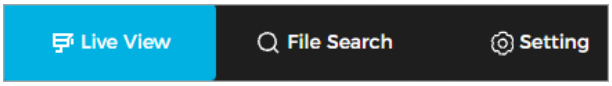


Password Reset

Web Client

Read the table to learn more about the functions of the web client.

Web Page Functions



Web Page Functions

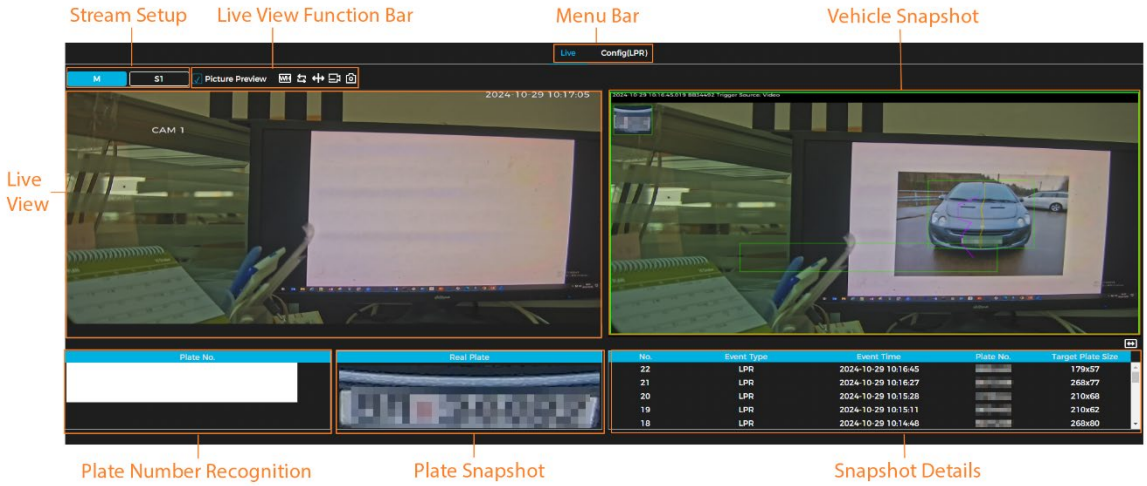
Function	Description
Live View	View live video in real time, take snapshots, record footage, adjust viewing window layouts, and configure image settings.
File Search	Search for images and videos, and set up watermark verification to ensure video authenticity.
Setting	Set up basic camera, network, storage, and system configurations, and view detailed system information.

Web Page Icons

Icon	Description
	Displays the device serial number and a QR code to download the LumiViewer mobile app.
	Log out of the current user account.
Default	Restore the default setting.
Refresh	Refresh settings.
Save	Save settings.

Live View

After logging in, you'll be directed to the Live View page, where you can view live videos, capture snapshots, check event details, and access other functions.



Live View

Set Up the Video Stream

Choose one of the following options to set up the video stream.

- Select **M (main stream)** when the network is stable and bandwidth is sufficient. It provides higher resolution and better image quality, ensuring critical details are captured clearly. You can configure the resolution for the main stream by going to **Setting → Video/Audio → Video → Video Stream**.
- Select **S1 (sub stream)** when bandwidth is limited. It offers lower resolution than the main stream, reducing bandwidth usage while maintaining smooth video playback.

Live View Function Bar

You can use the icons on the Live View function bar to configure related settings.

Live View Function Bar

Icon	Name	Description
Picture Preview	Picture Preview	When enabled, the camera automatically captures vehicle snapshots and detects event information, displaying both at the bottom of the page. Snapshots are stored in the path specified under **Setting → Storage → Storage Path**.
	W:H	Displays the live video either in its original size or scaled to fit the window automatically.
	Switch Window	Switches to full-screen view. Click again to exit full-screen mode.
	Target Box	Click to enable smart track detection. The video will display license plates, vehicle bounding boxes, and other tracking details.
	Full Screen	Click to enter full-screen display. Double-click or press **Esc** to exit full-screen mode.
	Video	Click to start or stop recording. The video will be saved to the local path. If the recording is not manually stopped, recording will continue until the web page is closed or the user logs out.

	Manual Snapshot	Click to take a snapshot. It is recommended to enable **Picture Preview** first.

Plate Number Recognition

Enable this function to display license plate numbers recognized by the camera in real time as a vehicle passes.

Plate Number Recognition Window

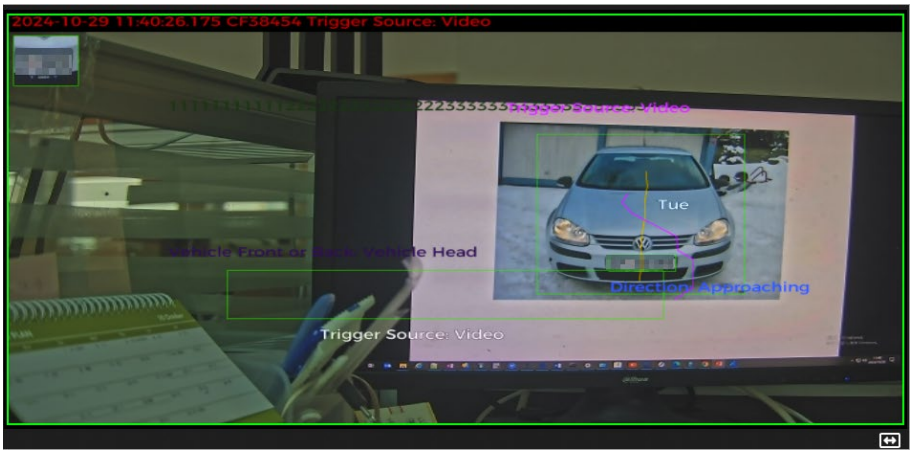
Plate Snapshot

Enable this function to display a snapshot of license plate numbers recognized by the camera in real time as a vehicle passes.

Plate Snapshot Window

Vehicle Snapshot

Select **Picture Preview** to display snapshots as vehicles pass. Click the icon to enter full-screen view. Click it again to exit full-screen mode.



Vehicle Snapshot Window

Snapshot Details

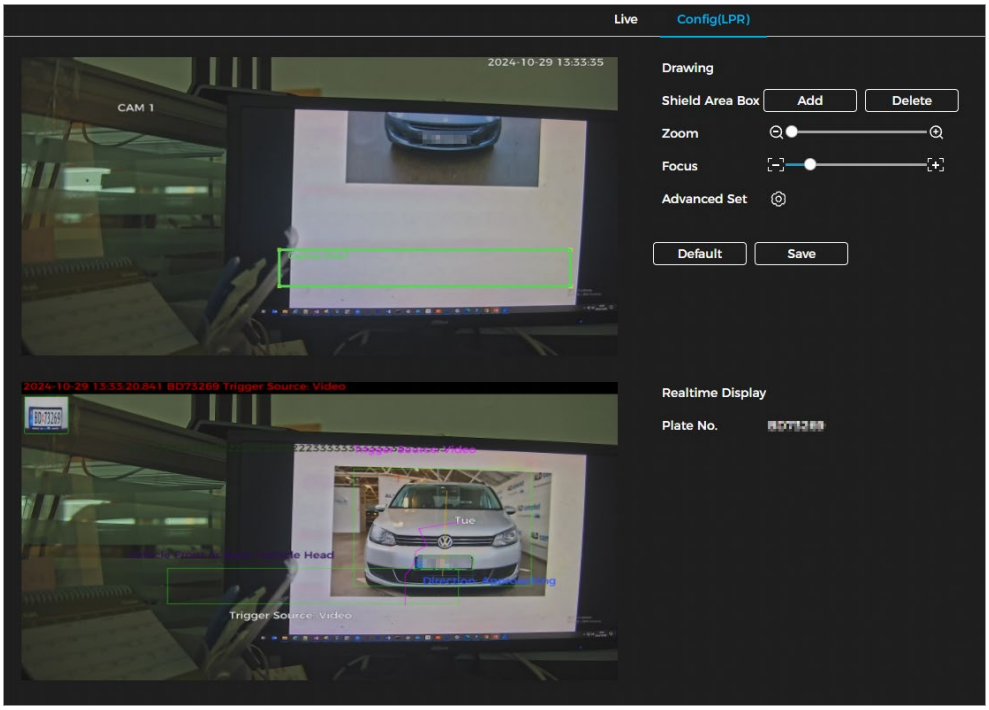
Select **Picture Preview** to display event details, including event number, type, time, plate number, and target plate size.

No.	Event Type	Event Time	Plate No.	Target Plate Size
5	LPR	2024-10-29 12:13:05		200x62
4	LPR	2024-10-29 12:12:48		262x83
3	LPR	2024-10-29 12:11:49		216x68
2	LPR	2024-10-29 12:11:32		204x63
1	LPR	2024-10-29 12:11:09		262x80

Snapshot Details Window

License Plate Recognition (LPR) Configuration

To ensure clear and accurate license plate capture, click **Config(LPR)** to adjust the camera settings for license plate recognition.



LPR Configuration Window

Capture Area and Shield Area

The **Capture Area** is the region where the camera captures images or video for license plate recognition. The **Shield Area** is a designated zone where detected plates are ignored and not processed.

- **Capture Area**: Customize the size, shape, and position by dragging the four corners and moving the entire area as needed.
- **Shield Area Box**: Add up to two shielded zones by clicking Add and adjusting the corners. Click **Delete** to remove a shield area.

It's recommended to test and fine-tune both areas to ensure effective license plate capture within the capture zone, while preventing recognition in the shielded zones.

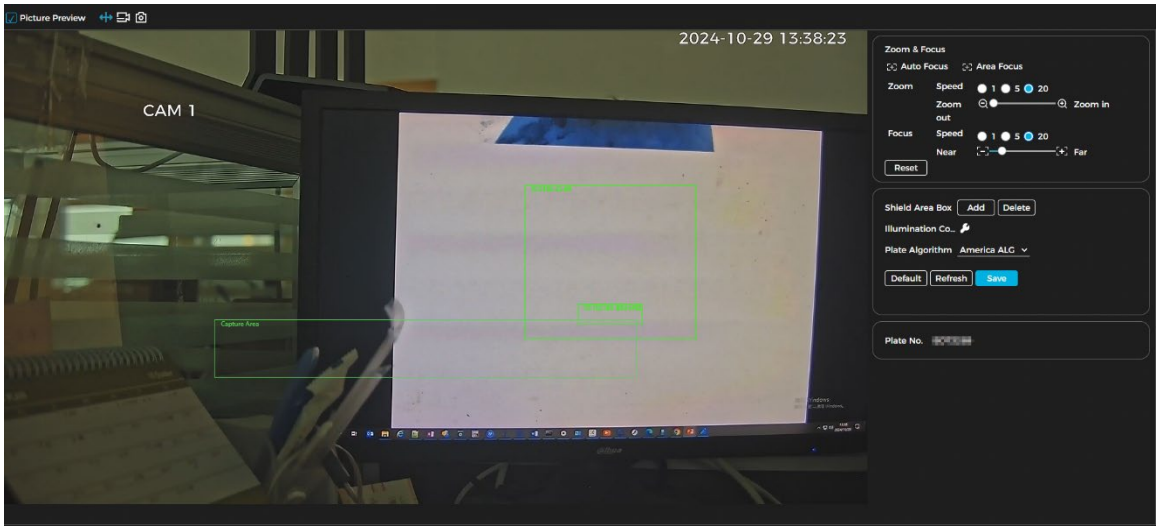
Zoom and Focus

The camera will automatically focus while zooming; however, zooming and focus can also be adjusted manually.

- **Zoom**: Changes the image size by adjusting the lens. Click or hold + or –, or drag the slider to zoom in or out.
- **Focus**: Adjusts the optical back focal length to sharpen the image. Click or hold + or –, or drag the slider to fine-tune focus.

For additional adjustments, click the icon next to **Advanced Set**.

Advanced Set



Advanced Set Window

Zoom and Focus

- **Auto Focus**: Click to let the camera automatically adjust focus. Other lens controls are disabled during this process
- **Area Focus**: Click to focus on a specific area, then drag over the desired region in the live view. This function is ideal for sharpening the license plate area while allowing other parts to blur.
- **Manually Adjust Zoom and Focus**: Adjust zoom and focus manually. Set the Speed value to control how much the camera adjusts with each click. A higher value results in greater adjustment per click.

Shield Area

Up to three (3) shield areas can be added.

Illumination Configuration

Click the icon to go to the **Display Settings** page. You can customize and optimize video display settings on this page.

Plate Algorithm

Plate algorithm enables the system to recognize license plates from specific regions. Selecting **America ALG** configures the system to detect U.S. and Canadian plates, including regional variations and designs. To return to the configuration page, click **Back** in the upper-right corner

File Search

Picture Query

Memory Card

Follow the steps below to search for and download images stored on the memory card.

ⓘ Ensure the memory card is properly inserted.

1. Navigate to File Search → Picture Query → Memory Card Image.
2. Set the parameters.

Parameter	Description
Start Time	Set the start and end times to define a search time range.
End Time	
Event Type	• **All Images**: Search for all stored snapshots. • **LPR**: Search for snapshots captured by the LPR camera during license plate recognition. • **Manual Snapshot**: Search for snapshots manually captured by the user.
Plate No.	Select the checkbox, then enter the plate number to search for images associated with that specific plate.

3. Hit **Search**.

Related Functions

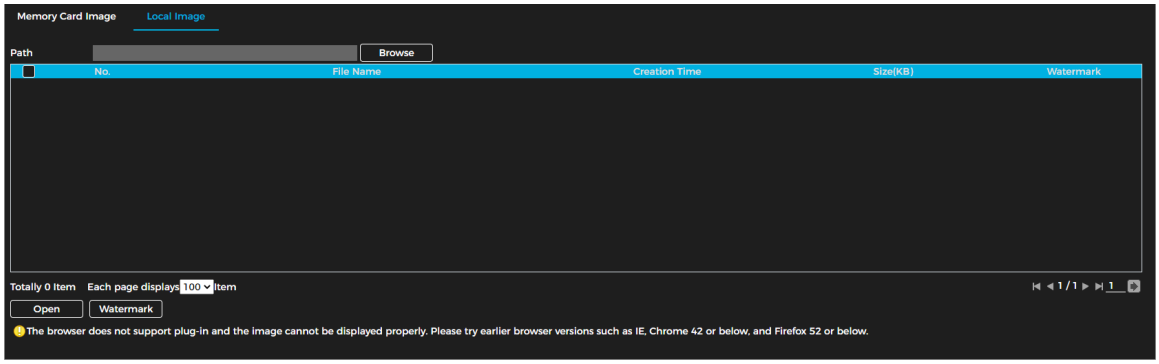
- Select a result from the list to view the plate image in the Real Plate Info section.
- Click **Open** to view the corresponding vehicle snapshot.
- To download images, select one or more, then click **Download by File** to save the selected images or **Download by Time** to save all images captured within a defined time range.
- To rename snapshots, click **Help** to view the naming rules, click **Reset** to enter a new name, and then click **OK** to apply.

View Local Image

Follow the steps below to view images saved on your computer and verify if any image tampering has occurred with a watermark.

ⓘ To view or configure the image save path on your computer, navigate to **Setting → Storage → Storage → Storage Path**.

1. Navigate to Search → Picture Query → Local Image.
2. Click **Browse**.
3. Select the images for verification.
4. Click **Watermark**. The results will display **Error** (tampering detected) or **Normal** (no tampering detected). Click **Open** or double-click the picture to preview it.



View Local Image Window

Video Search

You can search through video stored on your computer to find abnormal events.

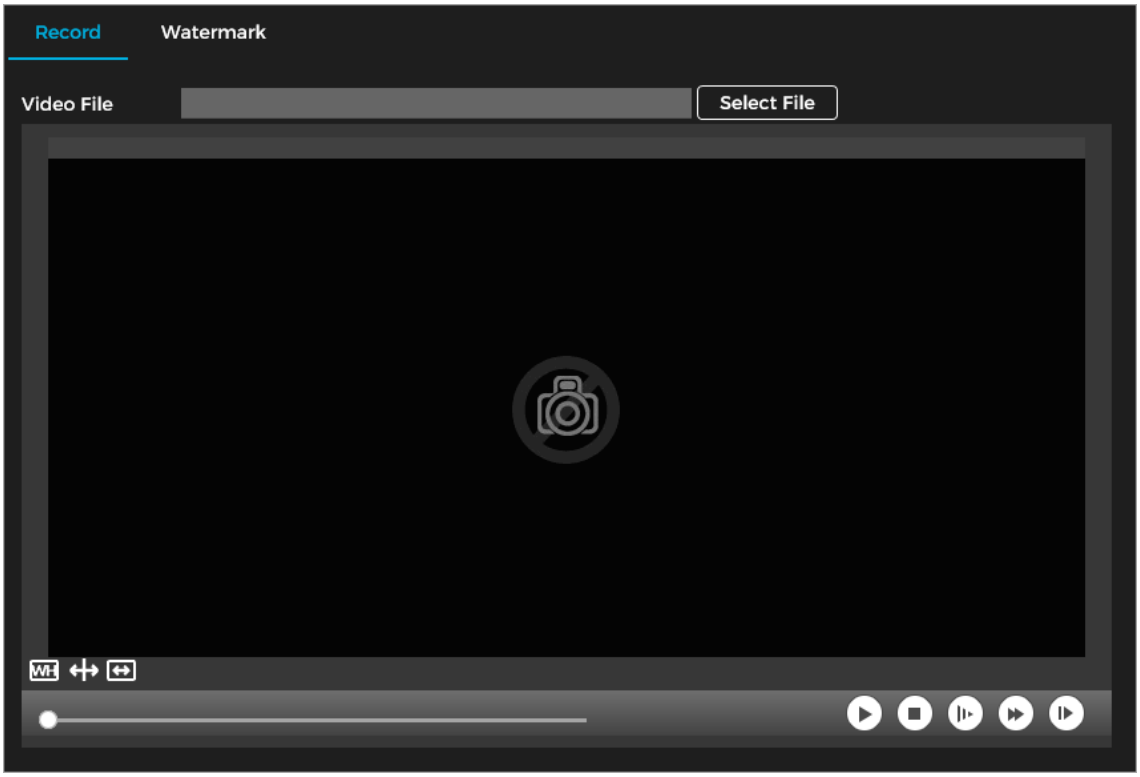
Record

Follow the steps below to search for and play back video stored on your computer.

ⓘ

- Click  on the **Live View** page to start recording.
- You can define the storage path by navigating to **Setting → Storage → Storage Path**.

1. Navigate to File Search → Search Video → Record.
2. Click Select File.
3. Choose the video you want to play back.



Playback Window

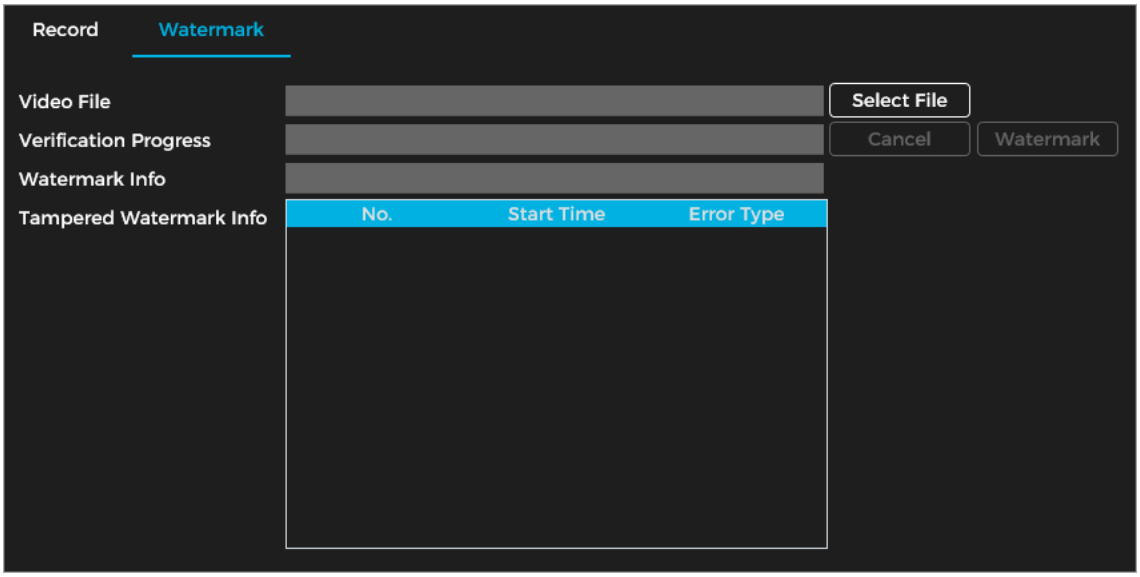
Icon	Description
	Displays the live video either in its original size or scaled to fit the window automatically.
	Click to enable smart track detection. The video will display license plates, vehicle bounding boxes, and other tracking details.
	Click to enter full-screen display. Double-click or press **Esc** to exit full-screen mode.
	Click to play back video.
	Click to stop playing the video.
	Click to slow the video down and play at half, quarter, or eighth speed. Click the play button to resume normal playback speed.
	Click to play the video at two times, four times, or eight times speed. Click the play button to resume normal playback speed.
	Click to play the next frame.

Watermark Verification

Follow the steps below to check if a video has been tampered with by checking the watermark.

ⓘ Only .lav files are supported.

1. Navigate to File Search → Search Video → Watermark.
2. Click Select File.
3. Choose the files for verification.
4. Click **Watermark**. If the video is verified as authentic, the configured watermark appears next to **Watermark Info**. If the video has been tampered with, details will be shown next to **Tampered Watermark Info**.



Watermark Verification Window

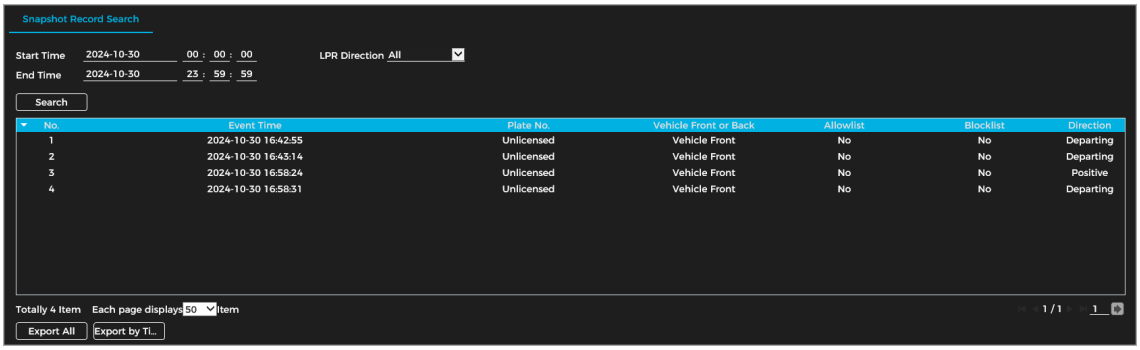
Snapshot Search

Follow the steps below to search for and download snapshots.

1. Navigate to File Search → Snapshot Record Search.
2. Set the parameters.

Parameter	Description
Start Time	Set the start and end times to define a search time range.
End Time	
LPR Direction	LPR direction defines the orientation in which the camera captures vehicles. Options include **All**, **Approaching**, **Departing**, and **Unknown**.

3. Click **Search**.



Snapshot Search Window

Related Operations

- Click **Export All** to export all records.
- Click **Export by Time** to save all images captured within a defined time range.

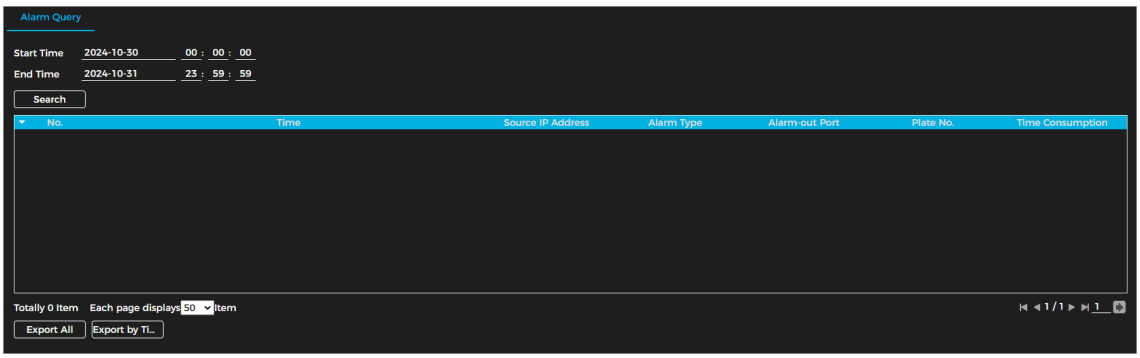
Alarm Query

Follow the steps below to search for and export alarms.

1. Navigate to File Search → Alarm Query.
2. Set the parameters.

Parameter	Description
Start Time	Set the start and end times to define a search time range.
End Time	

3. Click **Search**.



Alarm Query Window

Related Operations

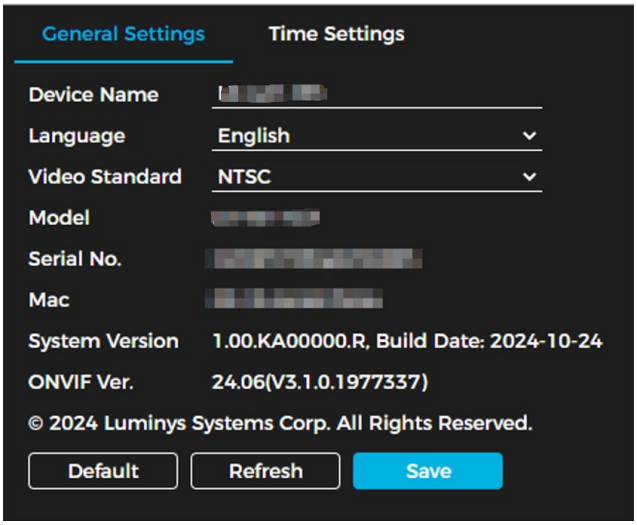
- Click **Export All** to export all records.
- Click **Export by Time** to save all images captured within a defined time range.

Settings

System Settings

General Settings

Navigate to **Setting → System → System Setting → General Settings** to configure the camera name, choose the system language and video standard, view the system version, and access other general settings.



General Settings Window

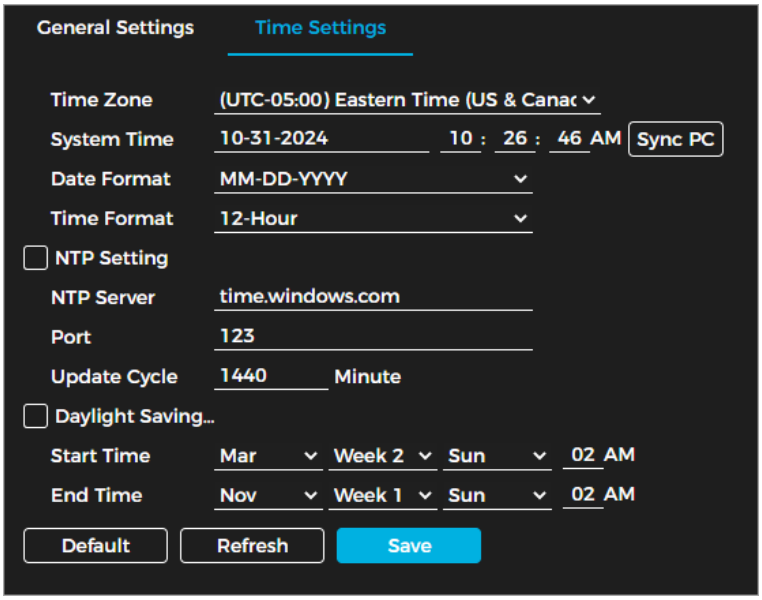
Time Settings

Follow the steps below to configure the time-related settings for the camera.

1. Navigating Setting → System → System Settings → Time Settings.
2. Set the parameters.

Parameter	Description
Time Zone	Set the time zone the camera is installed in.
System Time	Set the current time for the camera. You can click **Sync PC** to sync the camera's time to your PC.
Date Format	Set the date format.
Time Format	Choose between a 12-Hour or 24-Hour time format.
NTP Setting	Sync the camera's time with the configured server. • **NTP Server/Port**: Enter the IP address and port number of the time server the device will use for synchronization. • **Update Cycle**: Set how often the device will sync its time with the server.
Daylight Saving Time	Enable Daylight Saving Time (DST) by selecting the Daylight Saving Time checkbox, then set the Start Time and End Time as required.

3. Click **Save**.



Time Settings Window

Device Maintenance

Upgrade and Maintenance

Follow the steps below to schedule automatic reboots, restore the camera to default or factory settings, import or export configuration files, and update the system to the latest version to ensure proper operation.

1. Navigate to Setting → System → Device Maintenance → Upgrade and Maintenance.
2. Select the maintenance operations.

- **Reboot**: Click to restart the camera immediately.
- **Auto Restart**: Enable by selecting the checkbox, then set the desired restart time. The system will automatically reboot at the scheduled interval.

3. Choose the default settings.

- **Restore**: Click to reset all settings to default, excluding IP address, auto registration, port, HTTPS, and multicast configurations.
- **Default**: Restores all parameters to factory settings. Use this with caution as this setting will restart the camera and require re-initialization.

4. Select the import and export configurations. The system allows you to export configuration settings from the webpage to your local computer for backup and import them later for quick setup or recovery.

- **Export**: Save the current configuration on your local computer.
- **Import Config**: Load configuration files from a local backup.

5. Update the system via file upgrade or online upgrade.

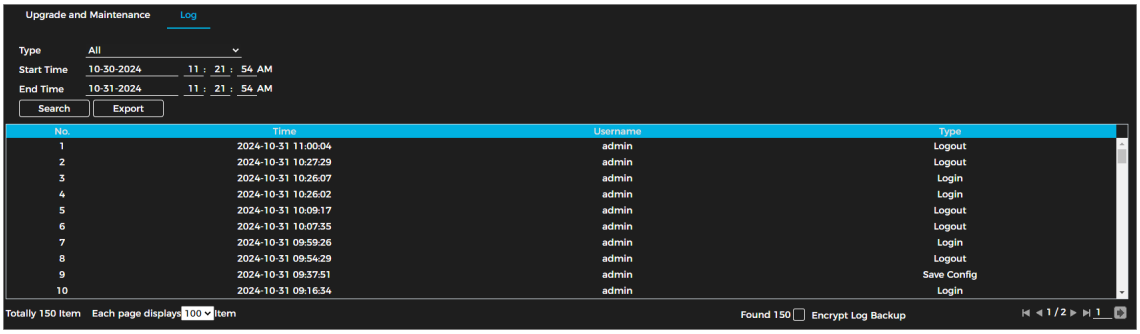
- **File Upgrade**: Click **Browse**, select the upgrade file, and then click **Upgrade**.
- **Online Upgrade**: Select **Automatic Detection**, and then click **OK**. Click **Manual Check** to verify the current system version.

6. Click **Save** to save all settings.

System Log

Follow the steps below to search for, view, and back up logs.

1. Navigate to Setting → System → Device Maintenance → Log.
2. Set the start and end time.
3. Select the log type.
4. Click **Search**. The results will be displayed in a list.
5. (Optional) Click **Export** to save the logs to your computer as a .txt file. Select **Encrypt Log Backup** to set a password for the log file.

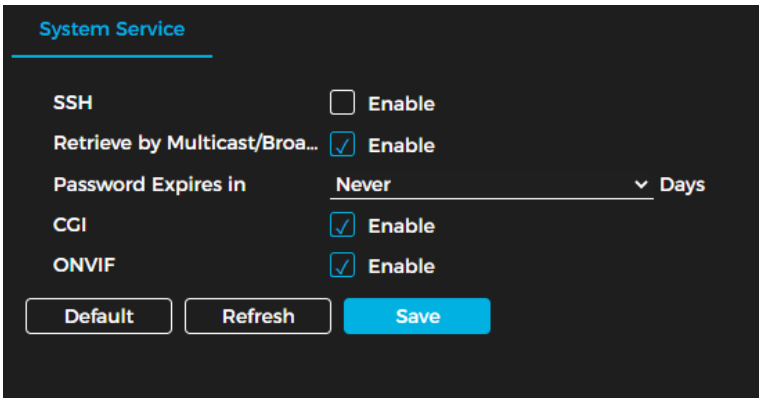


System Log Window

System Service

Follow the steps below to enable system services for network safety.

1. Navigate to Setting → System → Security → System Service.
2. Enable the services as needed.



System Service Window

Service	Description
SSH	Secure Shell (SSH) is a cryptographic protocol that enables secure remote login and access over unsecured networks. While it provides encrypted communication for managing network services, enabling SSH may introduce potential security risks and should be used with caution.
Retrieve by Multicast/Broadcast	Retrieve by Multicast/Broadcast allows messages to be sent across the network, enabling compatible software or devices to automatically detect and list the camera. This simplifies camera discovery and network integration but may introduce security vulnerabilities.

Password Expires in	Set how many days a password is valid before it needs to be reset.
CGI	Enable this function to allow other devices to access the camera through the service. It is enabled by default.
ONVIF	This service is enabled by default and allows network video devices from different manufacturers to communicate and operate together.

3. Click **Save**.

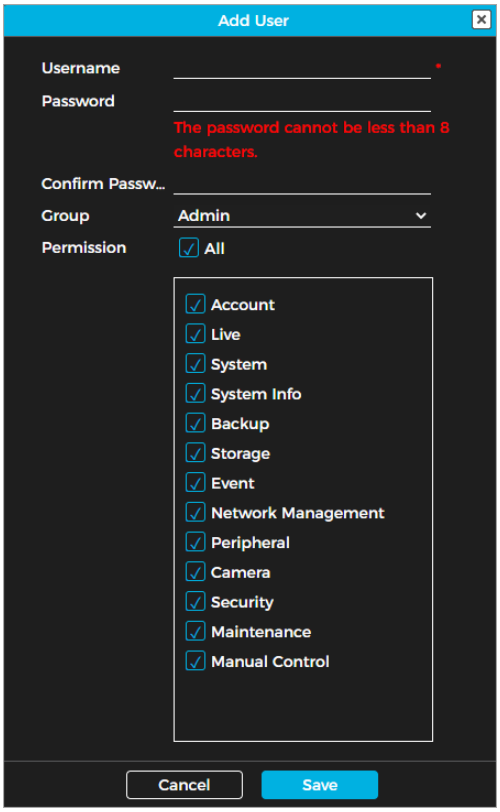
User Management

Follow the procedures below to add or delete users and user groups, assign specific permissions, change passwords, and manage all user accounts and groups.

Manage Users

You can manage users by viewing user information, adding or deleting users, changing passwords, assigning permissions, and performing other administrative tasks.

1. Navigate to Setting → System Setting → User Management → Account → User.
2. Click **Add User**. Set the username, password, group, and permissions.



Add User Window

Parameter	Description
Username	Each user must have a unique username that has not been used before. Usernames can be up to 31 characters long and may include uppercase letters, lowercase letters, numbers, "_", "@", and ".".
Password	Enter and confirm the password. It must be 8 to 32 non-blank characters and include at least two of the following: uppercase letters, lowercase letters, numbers, or special
Confirm Password	

	characters (excluding ' " ; : &). Follow the password strength prompt to ensure a secure password.
Group	Specifies the user group the user belongs to. Each group has its own set of permissions.
Permission	Choose what functionalities a user has access to.

3. Click **Save** when done.

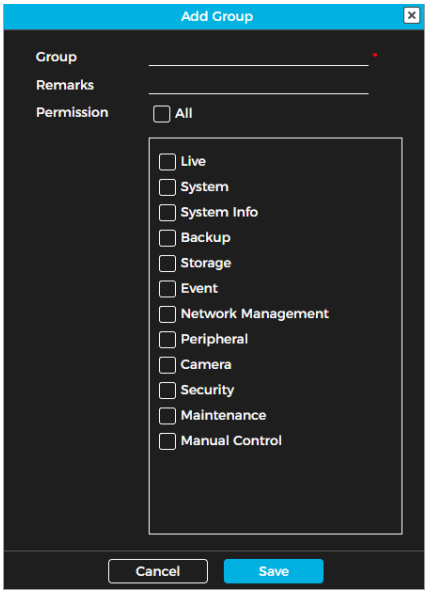
Related Operations

- Click to delete a user. Admin users cannot be deleted.
- Click to edit a user's information.

Manage User Groups

A group is a collection of permissions. Configure different groups to efficiently assign specific access rights to users.

1. Navigate to Setting → System Setting → User Management → Account → Edit Permission.
2. Click **Add Group**. Set the group name, any remarks or comments, and permissions.
3. Click **Save**.



Add User Group Window

Related Operations

- Click to delete a group.
- Click to edit the group's remarks and permissions.

View Online Users

Select **Setting → System Setting → User Management → Online User** to view user login information such as username, group, IP address, login time, and login type. This helps monitor potential unauthorized access or suspicious behavior.

Reset Your Password

Follow the steps below to enable the password reset function. If the function is not enabled, you will only be able to reset the password by performing a full reset of the camera.

1. Navigate to Setting → System Setting → User Management → Password Reset.
2. Check the box next to **Open**.
3. (Optional) Input your email address.
4. Click **Save**.

View Legal Information

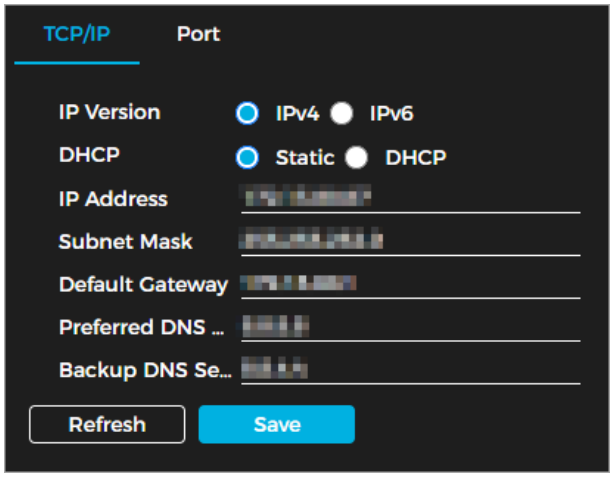
Navigate to **Setting → System → Legal Information** to view the software license agreement, privacy policy, and open-source software notice.

Network Settings

Configure TCP/IP

Follow the steps below to configure the IP address, DNS server, and other camera network connectivity parameters.

1. Navigate to Setting → Network →TCP/IP.
2. Set the parameters.



TCP/IP Settings Window

Parameter	Description
IP Version	Choose between IPv4 or IPv6.
DHCP	Choose a network mode. Select **Static** to manually assign a fixed IP address, subnet mask, and gateway. This ensures consistent and predictable access and is useful for specific port forwarding or network configuration needs. Select **DHCP** to automatically obtain the IP address, subnet mask, and gateway from a DHCP server. This simplifies network configuration and allows the camera to adjust to network changes. ⓘ If the DHCP server can update a DNS server, the camera can be accessed using its host name.
IP Address	Enter the camera's IP address.

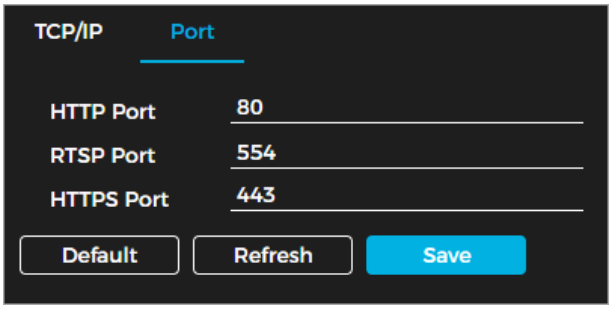
Subnet Mask	Specify the subnet mask for the network where the camera is located. The subnet prefix ranges from 1 to 255 and defines the network segment, typically following a hierarchical structure.
Default Gateway	Set a default gateway that is on the same network segment as the IP address if required.
Preferred DNS Server	Enter the IP address of the DNS.
Backup DNS Server	Enter the IP address of the backup DNS.

3. Click **Save**.

Configure Port Settings

Follow the steps below to configure the camera's port settings and enable data transfer between the camera and other devices on the same network.

1. Navigate to Setting → Network Settings → TCP/IP → Port.
2. Set the port parameters.



ⓘ

- Ports 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, and 42323 are reserved for specific uses.
- Avoid using values that are already assigned to other ports during port configuration.

Parameter	Description
HTTP Port	Hypertext Transfer Protocol Port. The default value is 80.
RTSP Port	• Real Time Streaming Protocol Port. The default value is 554. • This port is used for live view playback with applications such as Apple Safari, QuickTime, VLC, or BlackBerry smartphones. • If the URL format requires RTSP, include the channel number, bit stream type, and, if necessary, the username and password. • For playback on a BlackBerry smartphone, disable audio, set the codec mode to H.264B, and configure the resolution to CIF. **RTSP URL Example** URL = rtsp://**<ip address>**:**<port>**/video/livemedia?Ch=**<#>**&Streamtype=**<#>** • IP Address: The device IP address • Port: Optional. Omit if using the default port value of 554. • Ch: Channel number. Channels start from 1. For example, if using channel 2, the channel = 2.

	• Stream Type: The bit stream type. 0 = Main stream, 1 = sub stream. A completed example of a URL would be **rtsp://192.168.1.101:554/video/livemedia?Ch=2&Streamtype=1.**
HTTPS Port	HTTPS Communication Port. The default value is 443.

3. Click **Save**.

Configure P2P

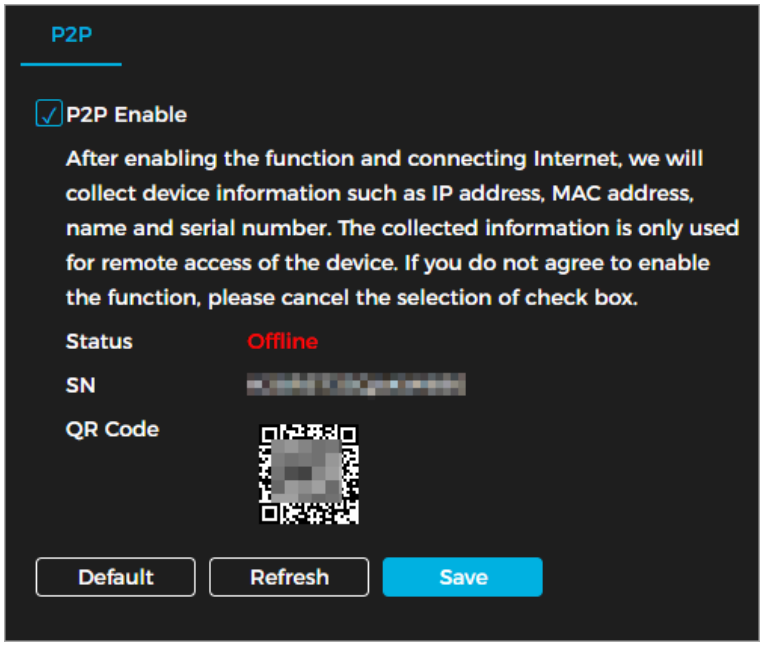
Follow the steps below to configure P2P and enable remote access to the camera for functions such as port forwarding.

1. Navigate to Setting → Network Settings → P2P.
2. Check the box to enable P2P.

ⓘ

- By enabling P2P, you consent to having certain user information collected.
- Scan the QR code to view the device serial number.

3. Click **Save**.



Enable P2P Window

Configure DDNS

Follow the steps below to properly configure DDNS. Once DDNS is correctly configured, the domain name on the DNS server will always match the current IP address of the camera. This mapping updates in real time, allowing you to access the camera using the same domain name, even if the IP address changes.

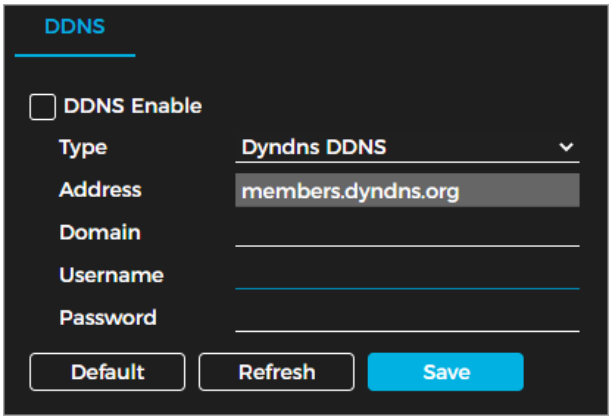
ⓘ Verify the type of DNS server supported by the camera prior to configuring.

1. Navigate to Setting → Network Settings → DDNS.
2. Check the box next to **DDNS Enable**.

ⓘ

- By enabling DDNS, certain user and device information may be collected by the third-party server.
- You can create an account with the DDNS website to register and view devices connected to your account.

3. Set the parameters.



DDNS Configuration Window

Parameter	Description
Type	The type of DDNS server.
Address	DDNS service provider's name and web address
Domain	Registered domain name on the DDNS website
Username	Username of the account associated with the DDNS server provider.
Password	Password of the account associated with the DDNS server provider.

4. Click **Save**.

Configure Register

Follow the steps below to configure the camera's register. When this function is enabled, the camera reports its current location to a designated server upon connecting to the Internet. This server acts as a relay, simplifying remote access via client software.

1. Navigate to Setting → Network Settings → Register.
2. Check the box next to **Enable**.
3. Enter the parameters.

Configure Register Window

Parameter	Description
IP Address	The server IP address or domain name.
Port	Registration port.
Sub-Device ID	The camera's custom ID.

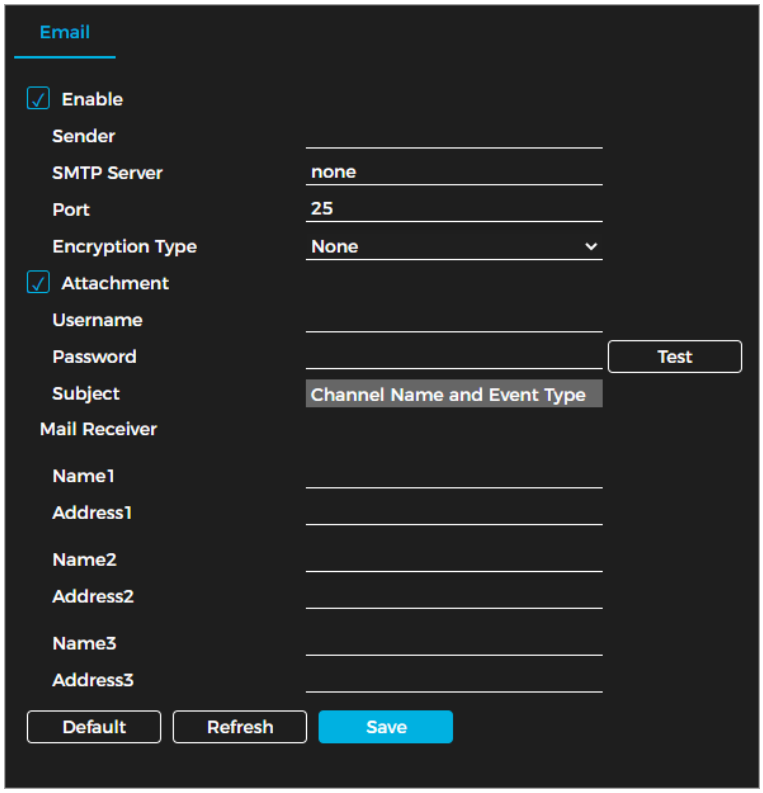
4. Click **Save**.

Configure Email

Follow the steps below to configure email alerts. When alarms or abnormal events occur, the system sends an email to the recipient via the SMTP server. The recipient can retrieve the email by logging into the incoming mail server.

⚠ When this function is enabled, the system transmits device data to the specified server. This may pose a risk of data leakage.

1. Navigate to Setting → Network Settings → Email.
2. Click the checkbox next to **Enable**.
3. Set the parameters.



Configure Email Window

Parameter	Description
Sender	The sender's email address.
SMTP Server	The IP address of the SMTP-compliant outgoing mail server.
Port	The port number of the SMTP-compliant outgoing mail server. The default value is 25.
Encryption Type	Choose between **None**, **SSL**, or **TLS** (recommended).
Attachment	Check this box to allow attachments to be sent with emails.
Username	Sender mailbox username.
Password	Sender mailbox password.
Mail Receiver	Receiver's email address. Up to three (3) can be added.
Test	Click to test if the email function to verify normal operation. If configured correctly, the recipient's email address will receive a test message. Be sure to save the email settings before testing.

4. Click **Save**.

Advanced Settings

Configure PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is used by the device to connect to the internet. After configuration, the camera will connect to the network via PPPoE and obtain a dynamic WAN IP address.

Prior to configuring PPPoE, the camera must be connected to the network, and UPnP should be disabled to avoid possible interference.

Follow the steps below to enable PPPoE.

ⓘ The device IP address cannot be modified through the web page after enabling PPPoE connection.

1. Navigate to Setting → Network Settings → Advanced → PPPoE.
2. Click the box next to **Enable** and enter the username and password. You can obtain this information through the internet service provider.
3. Click **Save**.

PPPoE Configuration Window

Configure SNMP

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

Prior to configuring SNMP, install an SNMP management software, ensure you have the correct MIB file, and connect to the camera via the management software.

Follow the steps below to configure SNMP settings.

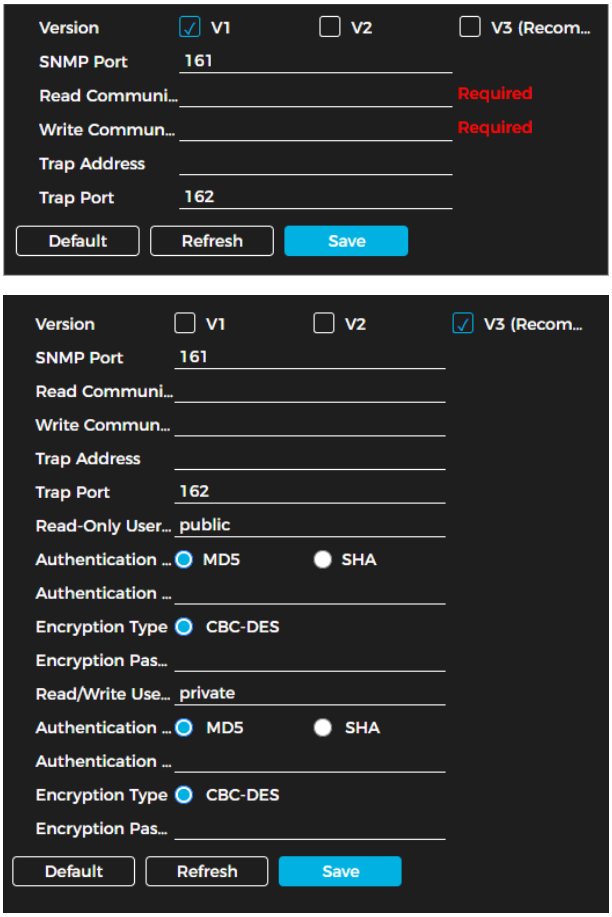
1. Navigate to Setting → Network Settings → Advanced → SNMP.
2. Select a version of SNMP to use: V1, V2, or **V3** (recommended).

ⓘ

- By selecting V1 or V2, the system will only be able to process information from the selected version.
- By selecting V3, V1 and V2 will become unavailable for use. You can configure the username, password, and authentication type. Accessing the device from the server requires matching the configured username, password, and authentication type.

⚠ V1 and V2 may cause data breaches.

3. Enter the IP address of the PC with the SNMP management software into the Trap Address section. Leave the other parameters as their defaults.



SNMP Parameters

Parameter	Description
SNMP Port	The listening port used by the software agent on the device.
Read Community	The read/write community string supported by the software agent. It can include numbers, letters, underscores, and dashes.
Write Community	
Trap Address	The target address where the software agent sends trap information.
Trap Port	The target port where the software agent sends trap information.
Read-Only Username	Set the read-only username for accessing the device. The default value is public. It can include numbers, letters, and underscores.
Authentication Type	Choose between **MD5** (default) and **SHA**.
Authentication Password	The password must have a minimum of eight (8) characters.
Encryption Type	The default is CBC-DES**.**
Encryption Password	The password must have a minimum of eight (8) characters.

4. Click **Save**.

How to View the Device Configuration through MIB Builder or MG-SOFT MIB Browser

Follow the steps below to view the device configuration using MIB builder of MG-SOFT MIB browser.

1. Launch 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 device's IP address in MG-SOFT MIB Browser, select the SNMP version, and start the search.
5. Expand all tree lists in MG-SOFT MIB Browser to view configuration information, including:

- Number of video channels
- Number of audio channels
- Software version

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

Configure Multicast

When multiple users are viewing the device's video simultaneously over the network, the connection may fail due to limited bandwidth. To resolve this, set a multicast IP address (range: 224.0.1.0–238.255.255.255) for the camera and enable the multicast protocol.

Follow the steps below to configure multicast.

1. Navigate to Setting → Network Settings → Advanced → Multicast.
2. Click the box next to **Enable**.
3. Set the parameters.

Multicast Parameters Window

4. Click **Save**.

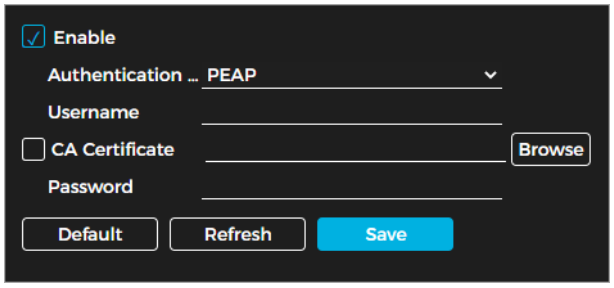
Configure 802.1x

802.1x is a port-based access control and authentication protocol that enhances network security by preventing unauthorized access and potential data breaches.

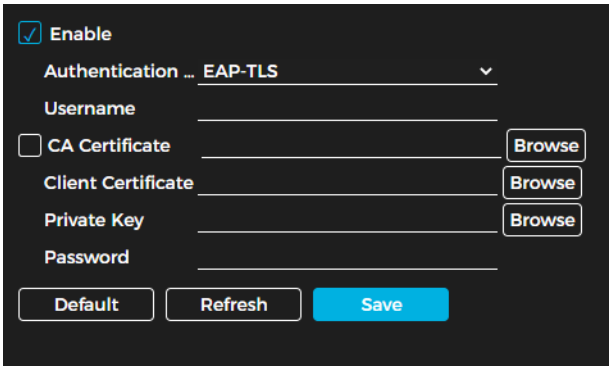
If the network switch is configured with 802.1x, the camera must also be configured accordingly or users will be unable to access the camera over the network.

Follow the steps below to configure 802.1x.

1. Navigate to Setting → Network Settings → Advanced → 802.1x.
2. Click the box next to **Enable**.
3. Set the parameters.



802.1x (PEAP)



802.1x (EAP-TLS)

Module	Parameter	Description
Common Parameter	Authentication Mode	• **PEAP**: Typically uses TLS to authenticate the server to the client. Only the server is required to have a public key certificate. • **EAP-TLS**: Provides mutual authentication between client and server. Both must have a digital certificate issued by a trusted Certificate Authority (CA).
	CA Certificate	Click **Browse** to import a CA certificate, then select the CA Certificate to verify its validity.
PEAP	Username	For the PEAP method, user authentication is performed using password-based credentials (username and password).
	Password	
EAP-TLS	Client Certificate	Click **Browse** to import a client certificate and a private key for authentication.
	Private Key	

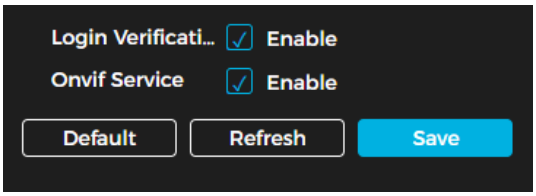
4. Click **Save**.

Configure ONVIF Protocols

ONVIF (Open Network Video Interface Forum) is a standard protocol that enables interoperability between devices from different manufacturers, such as video recorders and other recording equipment. This allows for seamless integration without compatibility concerns.

Follow the steps below to enable ONVIF.

1. Navigate to Setting → Network Settings → Advanced → ONVIF.
2. Enable the parameters as needed. Enabling login verification requires a username and password when logging in via ONVIF.



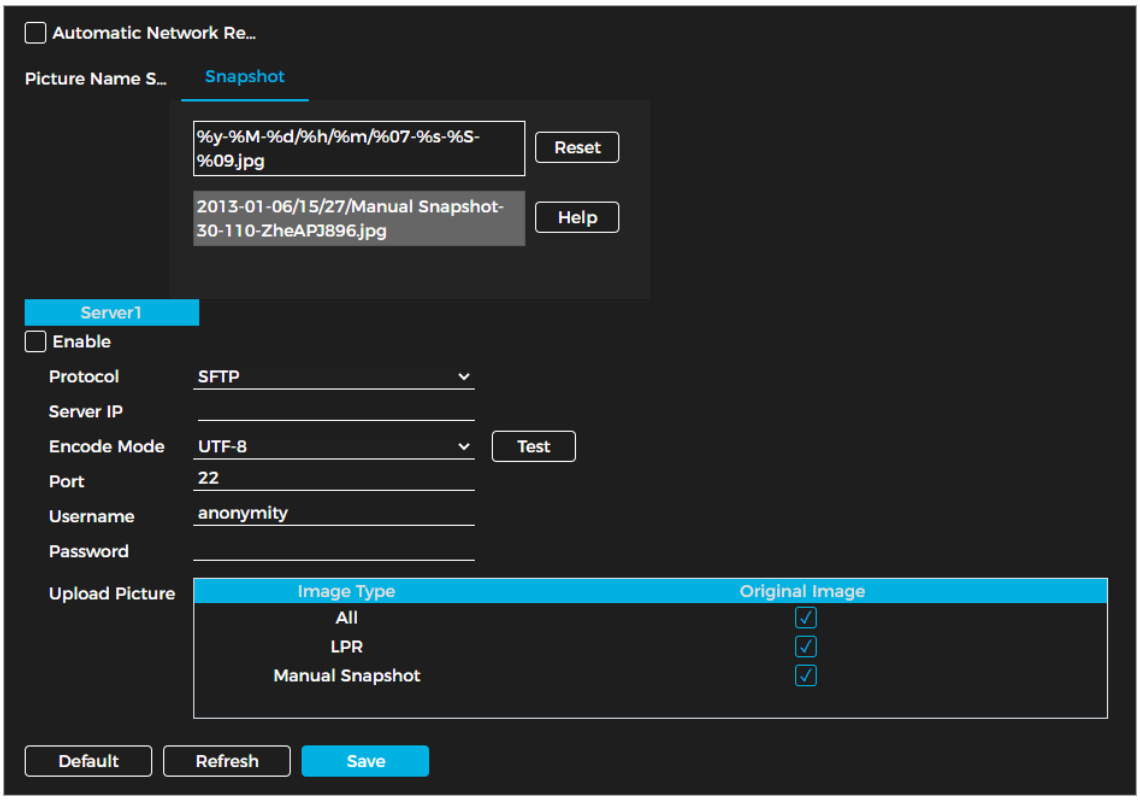
ONVIF Parameters

3. Click **Save**.

Configure FTP

Follow the steps below to enable FTP. FTP function can only be enabled when selected as the destination. If the network is down, all files can be saved to the internal memory card as a backup.

1. Navigate to Setting → Network Settings → Advanced → FTP.
2. Set the parameters.



Parameter	Description
Automatic Network Recovery	When the network disconnects or fails, snapshots are stored on the memory card. Once the network is restored, the snapshots will be uploaded from the memory card to the FTP server or client. Ensure the memory card is properly inserted in the camera; otherwise, the offline transfer function cannot be enabled.
Picture Name Settings	Set the naming rule for snapshots saved on the FTP server. Click **Help** to view the naming rule or click **Reset** to restore the default rule.
Enable	Click the box to enable FTP server storage.
Protocol	• **SFTP (Secure File Transfer Protocol)**: A network protocol that enables secure file access and transfer over an encrypted data stream. • **FTP (File Transfer Protocol)**: A network protocol for exchanging files over a TCP/IP network; supports anonymous user access via an FTP server.
Server IP	FTP server's IP address.
Encode Mode	Two options are available: **UTF-8** and **GB2312**. After setting the Server IP and Port, click Test to verify the FTP server connection.
Port	FTP server port number.

Username	FTP server username.
Password	FTP server password.
Upload Picture	Choose the image files to upload to the FTP server.

3. Click **Save**.

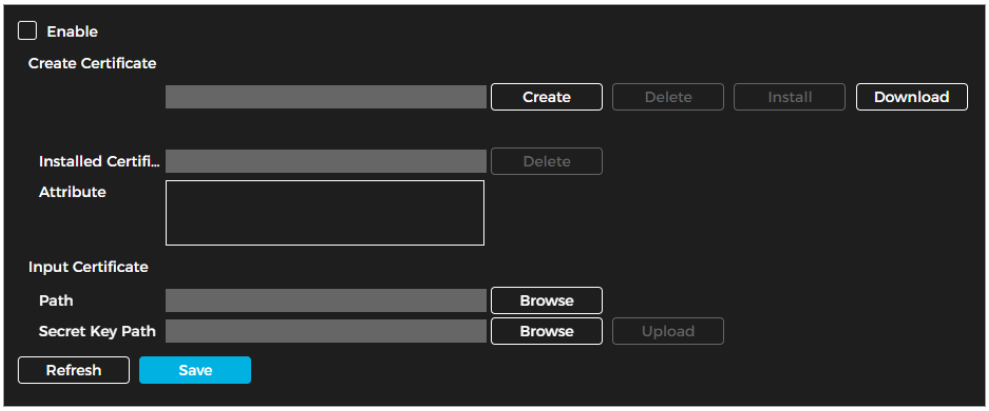
Configure HTTPS

You can log in via HTTPS by creating or uploading an authenticated certificate, ensuring secure communication and device safety through a reliable method.

For first-time HTTPS use or after changing the device IP, create a server certificate and install the root certificate. After creating and installing certificates, if accessing from a new computer, download and install the root certificate on that computer again.

Follow the steps below to configure HTTPS.

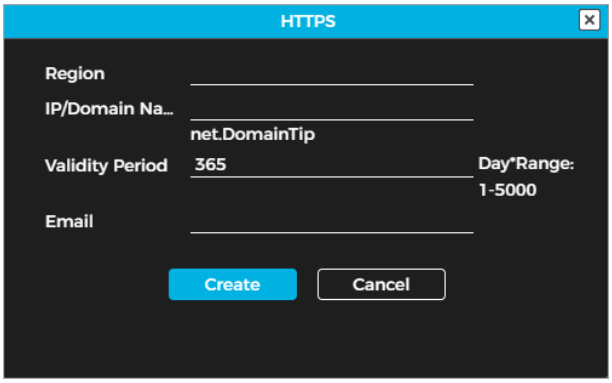
1. Navigate Setting → Network Settings → Advanced → HTTPS.



HTTPS Configuration Page

2. Create a certificate or upload an authenticated certificate.

- Create a Certificate



Creating a Certificate

- Click **Create**.
- Input the required information and click **Create**. Ensure the IP or domain name entered for the certificate matches the camera.
- Click **Install**. Download the root certificate.
- Double-click the RootCert.cer icon and install the certificate.

- Upload an Authenticated Certificate
- Click **Browse**. Choose the signed certificate and certificate key. Click **Upload**.
- Double-click the RootCert.cer icon and install the certificate.

3. Check the box next to **Enable**.
4. Click **Save**.

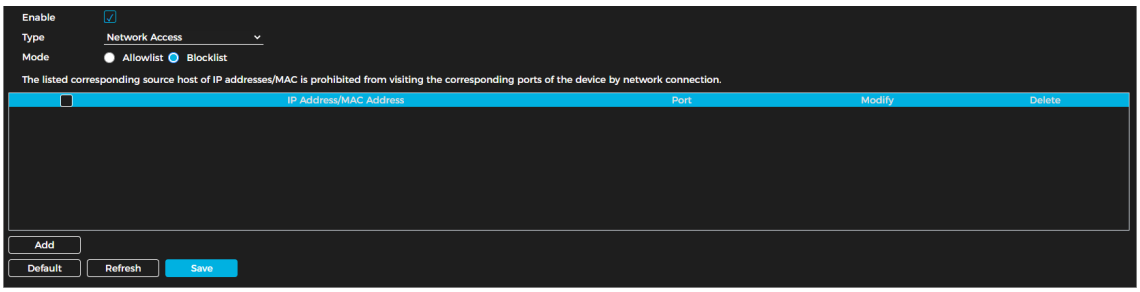
The configuration will be in effect until the camera is restarted. To use HTTPS to log in to the camera, go to https://<Camera IP Address> in your browser and enter the camera's login information.

Configure a Firewall

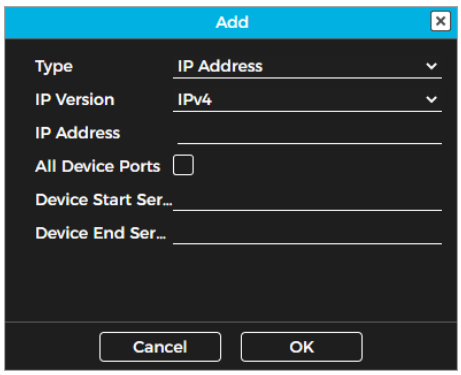
A firewall enhances network security by blocking unauthorized access and protecting against potential attacks. Follow the steps below to configure one.

1. Navigate to Setting → Network Settings → Advanced → Firewall.
2. Select **Type**.

- **Network Access:** Add IP/MAC addresses to an allowlist or blocklist to permit or restrict access to specific camera ports.



Network Access



Add IP/MAC Address

- **PING Prohibited**: Blocks ping requests to the camera's IP address to reduce exposure to unauthorized access attempts.
- **Anti Half Connection**: Prevents half-open SYN attacks by monitoring SYN packets and allowing only valid, complete connection requests

3. Click **Save**.

Related Operations

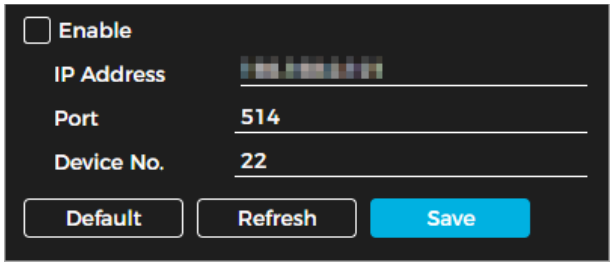
- Click to delete the information.
- Click to edit the information.

Configure Remote Logs

Remote logs can be saved to a designated log server to assist with tracing the source of security incidents. Follow the steps below to configure a remote log.

ⓘ Prior to configuration, the log server is pre-configured by technical support or a system administrator.

1. Navigate to Setting → Network Settings → Advanced → Remote Log.
2. Click the box to enable the function.
3. Set the IP address, port, and device number.
4. Click **Save**.



Enable Remote Logs

Configure LPRAPI

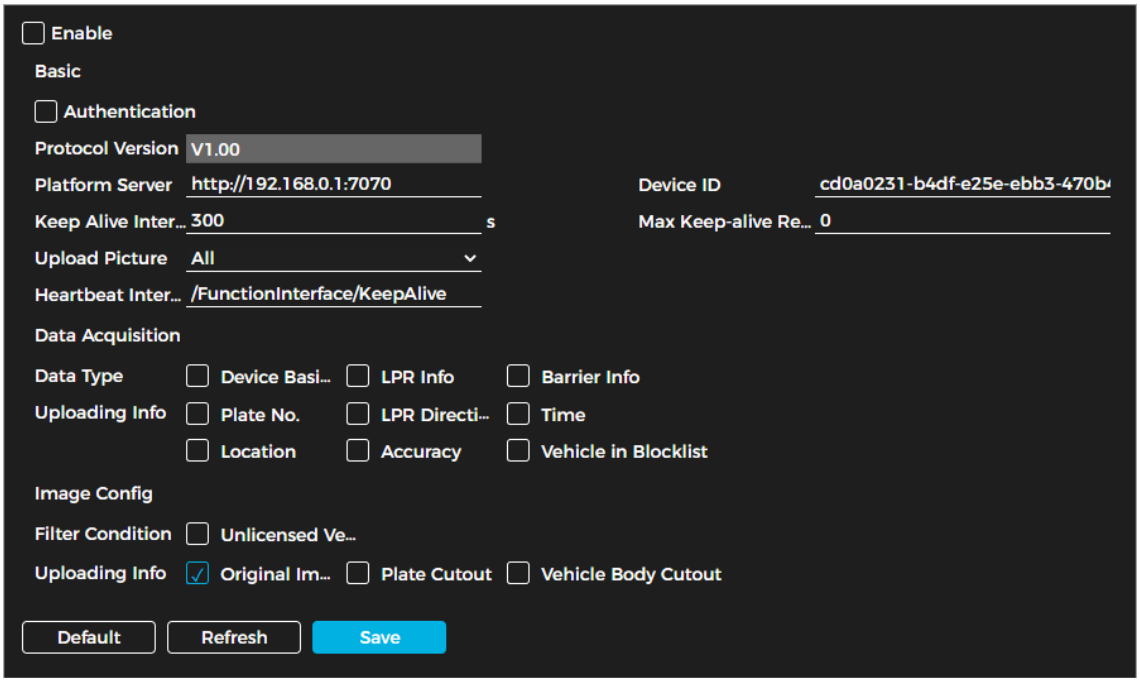
You can configure LPRAPI to push captured data to the server.

Prior to configuring LPRAPI, the following requirements must be met:

- All communication must use the HTTP protocol, comply with RFC2616 standards, and support Digest authentication.
- The server must support IO multiplexing.
- Business-related data must be in JSON format, with the HTTP header Content-Type: application/json;charset=UTF-8, indicating UTF-8 encoding.

Follow the steps below to configure LPRAPI.

1. Navigate to Setting → Network Settings → Advanced → LPRAPI.
2. Check the box next to **Enable**.
3. Set the parameters.



Module	Parameter	Description
Basic Configuration	Authentication	Enter the username and password when enabled.
	Keep Alive Interval	Set the connection time between the server and device.
	Max. Keep-Alive Request	Set the maximum number of heartbeats between the server and the device. If the defined limit is exceeded, the device is considered disconnected.
	Upload Picture	Choose images to be uploaded.
Data Acquisition	Data Type	Choose data to be uploaded.
	Uploading Info	Choose information to be uploaded.
Image Configuration	Filter Condition	Choose whether to upload the information of unlicensed information.
	Uploading Info	Choose the types of images to be uploaded.

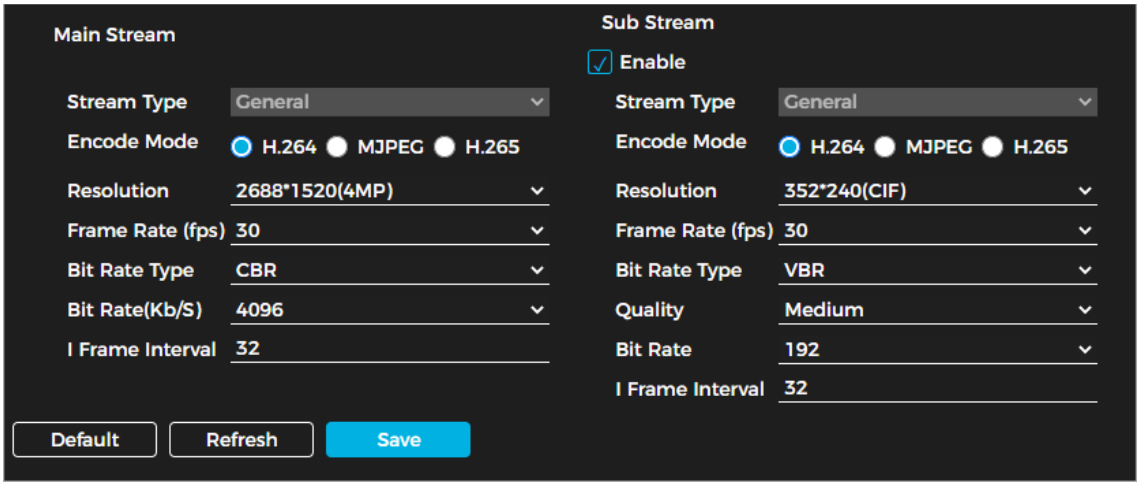
4. Click **Save**.

Video and Audio

Configure a Video Stream

Follow the steps below to set the parameters for a video stream.

1. Navigate to Setting → Video/Audio → Video → Video Stream.
2. Set the parameters.



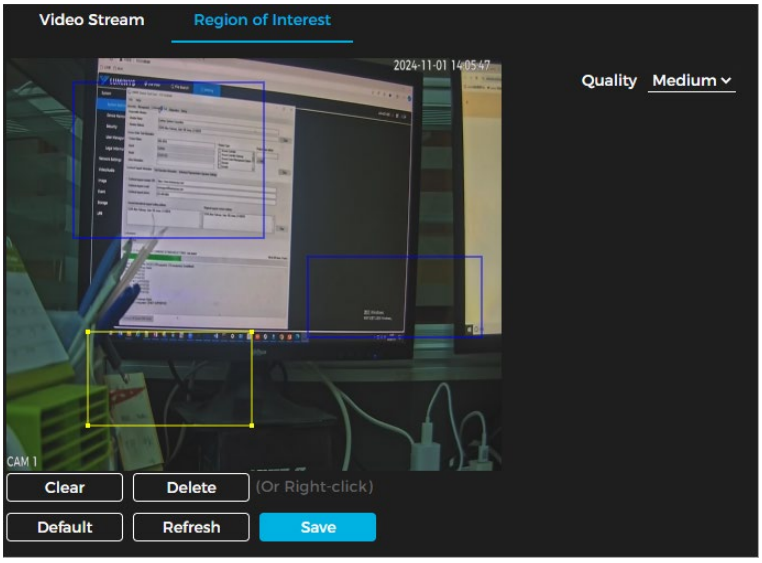
Parameter	Description
Encode Mode	Choose between **H.264**, **MJPEG**, or **H.265**.
Resolution	The higher the value, the clearer the overall image. Each resolution has a different recommended bit stream value. The resolution of the sub stream cannot exceed that of the main stream.
Frame Rate (fps)	The higher the value, the smoother the video playback. Frame rate may vary depending on the selected resolution.
Bit Rate Type	Choose between VBR or CBR. **VBR (variable bitrate)**: Bitrate adjusts according to scene complexity. Ideal for dynamic scenes, offering efficient compression while preserving quality. **CBR (constant bitrate)**: Maintains a fixed bitrate. Suitable for limited bandwidth environments (e.g., 320 Kbps), ensuring consistent video quality but possibly larger file sizes.
Quality	Six quality levels are available. A higher value indicates better image quality. Image quality must be configured when Bit Rate Type is set to VBR.
Bit Rate	A higher bitrate indicates a better image or video quality but consumes more storage space. Bitrate must be configured when Bit Rate Type is set to CBR.
I Frame Interval	Specifies the number of P-frames between two I-frames, ranging from 25 to 150. It is recommended to set the value to approximately twice the bit rate.
Enable	Enable the sub stream when the network bandwidth is limited or other conditions affect the smoothness of the main stream.

3. Click **Save**.

Configure a Region of Interest (ROI)

Follow the steps below to select one or more ROIs (regions of interest) on the video, configure their quality settings, and display the selected areas at their defined quality level.

1. Navigate to Setting → Video/Audio → Video → ROI.
2. Click and drag on the video image to draw the region of interest. You can create up to three regions. Click **Clear** to remove all areas. Click **Delete** or right-click to remove the most recently drawn area.



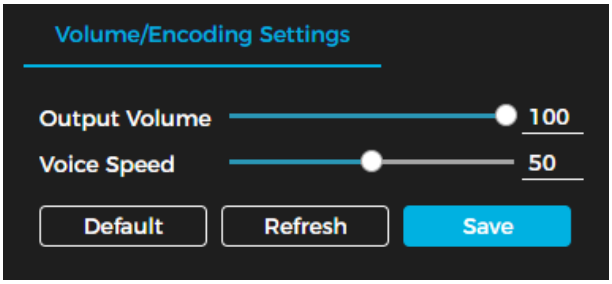
ROI Window

3. Set the image quality of the ROIs (Low, Medium, High).
4. Click **Save**.

Configure a Voice Broadcast (Volume/Encoding)

Follow the steps below to set the parameters for a voice broadcast.

1. Navigate to Setting → Video/Audio → Audio → Volume/Encoding Settings.
2. Set the volume and speed of the broadcast.
3. Click **Save**.



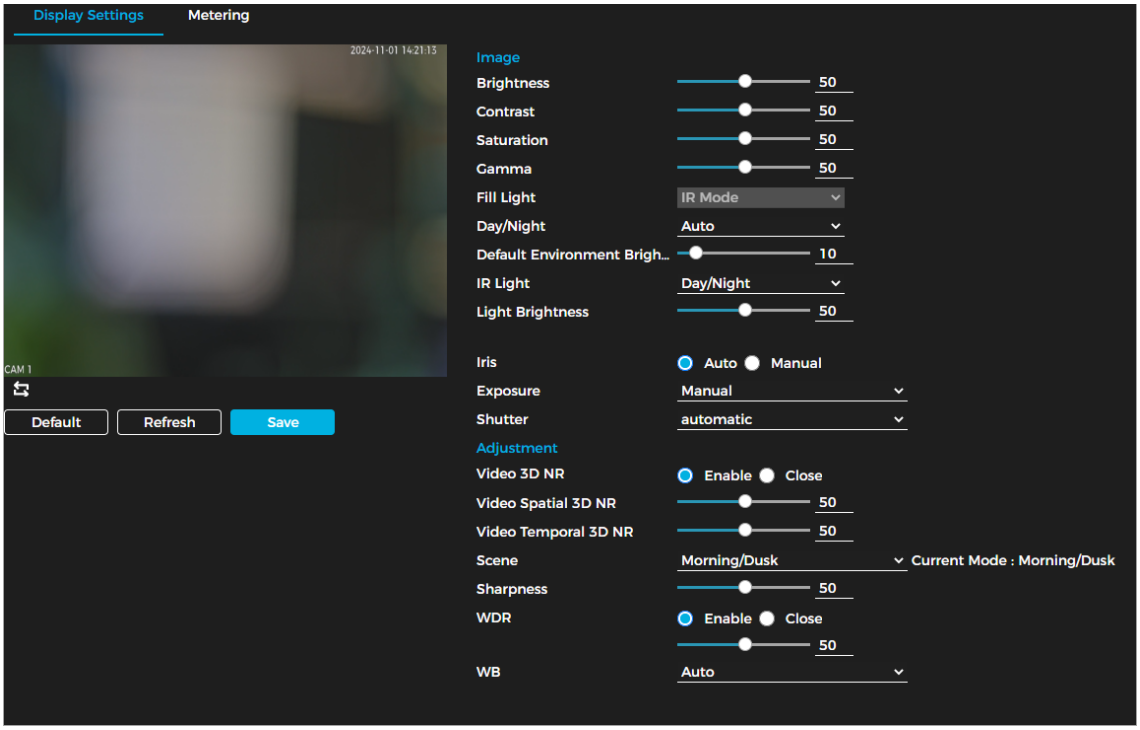
Volume/Encoding Settings

Images and Display

Configure Display Parameters

Follow the steps below to set the display parameters (brightness, contrast, saturation, mode, etc.).

1. Navigate to Setting → Image → Display Settings.
2. Set the parameters.



Display Settings Window

Parameter	Description
Brightness	Adjusting brightness affects both darker and brighter areas simultaneously. Increasing the value may cause the image to appear blurry. A higher value results in a brighter image. • Default Value: 50 • Recommended Range: 40–60 • Available Range: 0–100
Contrast	Adjusting contrast affects the darkness of dark areas and the exposure of bright areas. Reducing the value may cause the image to become blurry. A higher value increases contrast. • Default Value: 50 • Recommended Range: 40–60 • Available Range: 0–100
Saturation	Saturation affects the intensity of colors without altering the brightness of the overall image. A lower value results in a more desaturated (grayer) image. • Default Value: 50 • Recommended Range: 40–60 • Available Range: 0–100
Gamma	Adjust the image brightness level. A higher value results in a brighter image but may cause the image to appear blurrier.
Day/Night	• **Auto**: Automatically switches between color and black-and-white modes based on the set brightness threshold.

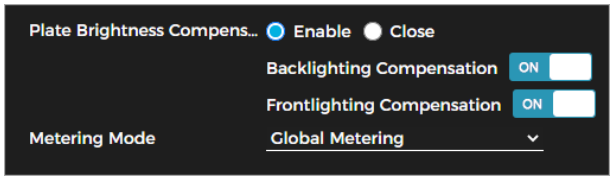
	• **Color**: Displays the image in color, suitable for daytime use. • **Black and White**: Displays the image in black and white, suitable for nighttime use.
IR Light	• **Always Off**: The IR light remains off at all times. • **Always On**: The IR light remains on at all times. • **Day/Night**: The IR light turns on or off automatically based on the selected Day/Night mode.
Light Brightness	Set the illumination intensity when no vehicles are passing. A higher value results in a brighter illumination.
Iris	Choose between **Auto** and **Manual**. When **Manual** is selected, adjust the iris value using the slider.
Exposure	Choose **Auto** or **Manual**. When **Manual** is selected, set the Shutter value.
Video 3D NR	Enables noise reduction. Choose between: • **Video Spatial 3D NR** reduces spatial noise; higher values mean less noise. • **Video Temporal 3D NR** reduces flicker noise over time; higher values mean less flicker.
Scene	Adjust the sharpness of corresponding scene by choosing one of the three options: **Morning/Dusk**, **Day**, and **Night**.
Sharpness	Set the sharpness of the corresponding scene. A higher value will result in a clearer image. If the sharpness value is set too high, there will be image noise.
WDR	Enables Wide Dynamic Range.
WB	Set the scene mode to adjust the image for the best clarity.

3. Click **Save**.

Configure the Metering Zone

Follow the steps below to configure the measuring mode for a metering zone.

1. Navigate to Setting → Image → Display Settings → Metering.
2. Set the parameters.

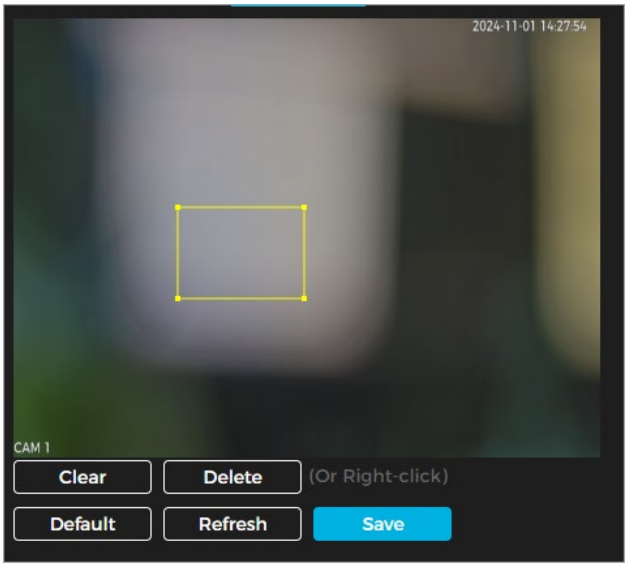


Metering Window

Parameter	Description
Plate Brightness Compensation	When enabled, you can turn **ON** or **OFF** backlighting and frontlighting compensation based on scene needs to enhance image brightness in backlit conditions.
Backlighting Compensation	
Frontlighting Compensation	

Metering Mode	• **Global Metering**: Measures brightness across the entire image and adjusts overall brightness intelligently. • **Partial Metering**: Measures brightness in selected areas and adjusts overall brightness accordingly; if the measured area brightens, the rest darkens, and vice versa.

3. When Metering Mode is set to Partial Metering, draw areas on the image by placing the cursor over the live view, then clicking and dragging to form a rectangle around the target area. Drag the vertices to resize the area and drag the edges to move its position. Right-click an area or select it and click **Delete** to remove the most recently drawn area. Click **Clear** to delete all areas. Up to five areas can be added.



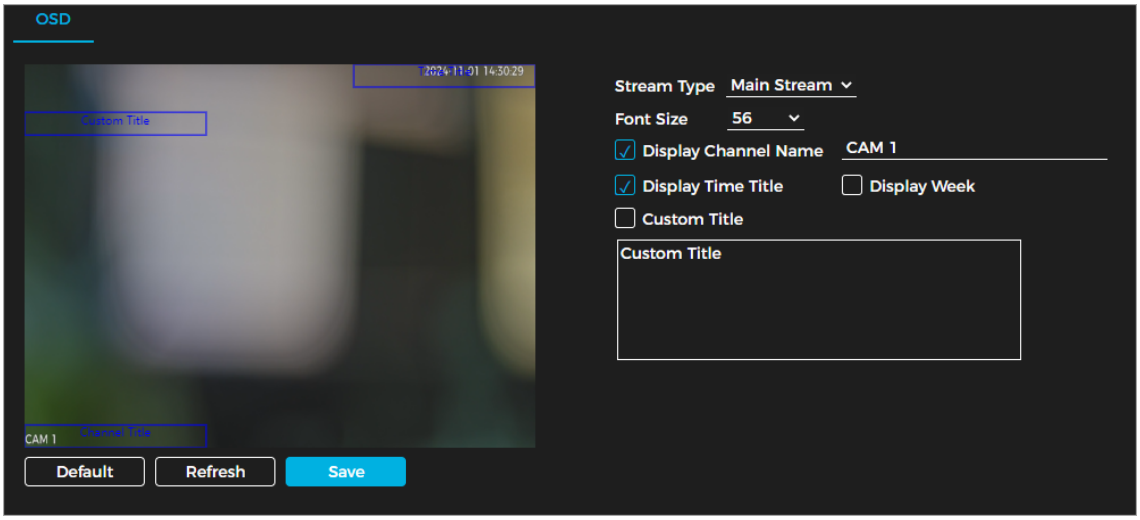
Partial Metering

4. Click **Save**.

Configure OSD

Follow the steps below to configure OSD information. This information will appear on the **Live** page.

1. Navigate to Setting → Image → OSD.
2. Set the parameters. Drag the yellow box on the live view image to adjust the OSD position.



Parameter	Description

Channel Name	Check to display and enter the channel title.
Time Title	Check to display; optionally select **Display Week** to show the weekday on the video.
Custom Title	Enter the text you want displayed.

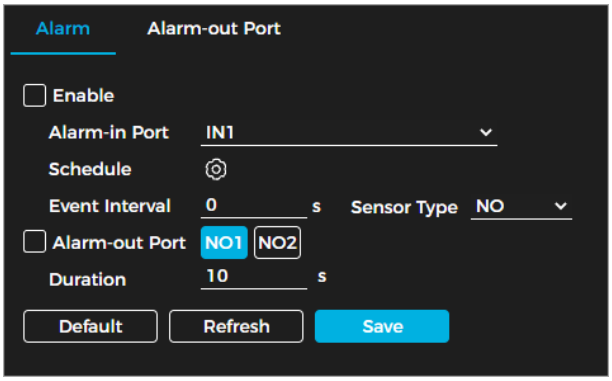
3. Click **Save**.

Event

Enable Alarm-In and Alarm-Out Ports

Follow the steps below to configure multiple parameters for alarm-in and alarm-out ports. When an alarm is triggered, the device sends a signal to activate external devices, such as a buzzer.

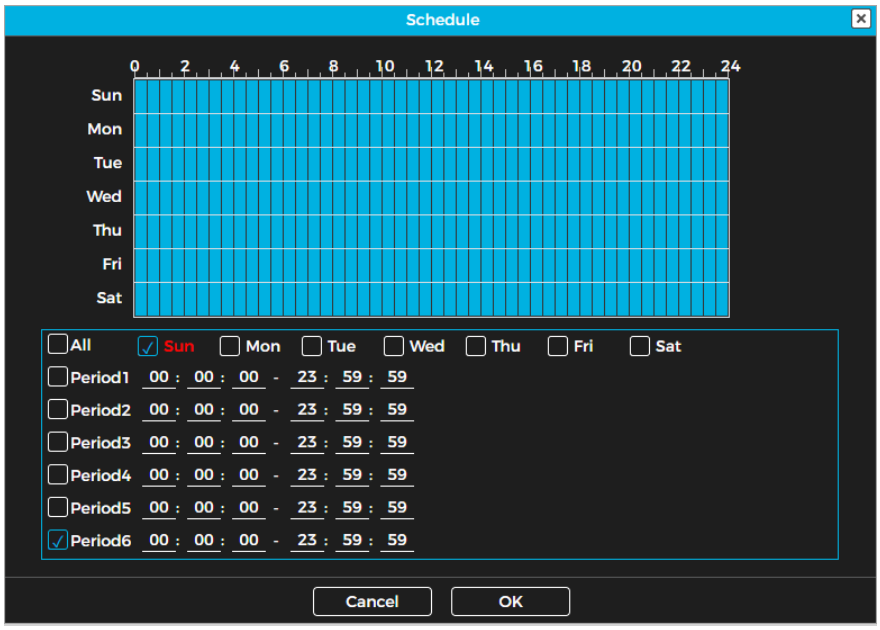
1. Navigate to Setting → Event → Alarm → Alarm.



Alarm Window

2. Click the box next to **Enable** to enable alarm input for the current channel.
3. Choose an alarm input channel.
4. Click  to set an alarm schedule or follow the steps to create a new one.

- Creating an Alarm Schedule



Create an Alarm Schedule

- Select one or more days by checking the box or clicking the specific day.

- Set the time: Click and hold the left mouse button on the chosen day, then drag to select the time period on the timeline. Alternatively, enter the specific time manually. You can set up to 6 time periods.
- Delete a time period: Click once to remove it.

5. Set the other parameters.

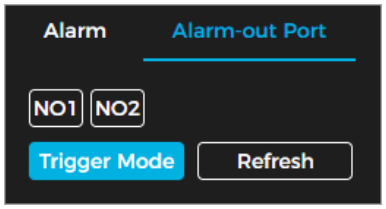
Parameter	Description
Event Interval	Enter the interval time (1–100 seconds). The system will record only one alarm if multiple alarms occur within this period.
Sensor Type	Select the relay-in type based on the connected alarm input device: • **NO**: Low level active • **NC**: High level active
Alarm-out Port	Check the box and select one or more alarm output channels. The corresponding devices will activate when alarms are triggered.
Alarm Channel	
Duration	When an alarm is triggered, it will last for the specified duration.

6. Click **Save**.

Check Alarm-Out Ports

Follow the steps below to check if the alarm-out ports are functioning properly.

1. Navigate to Setting → Event → Alarm → Alarm-out Port.



Alarm-Out Port

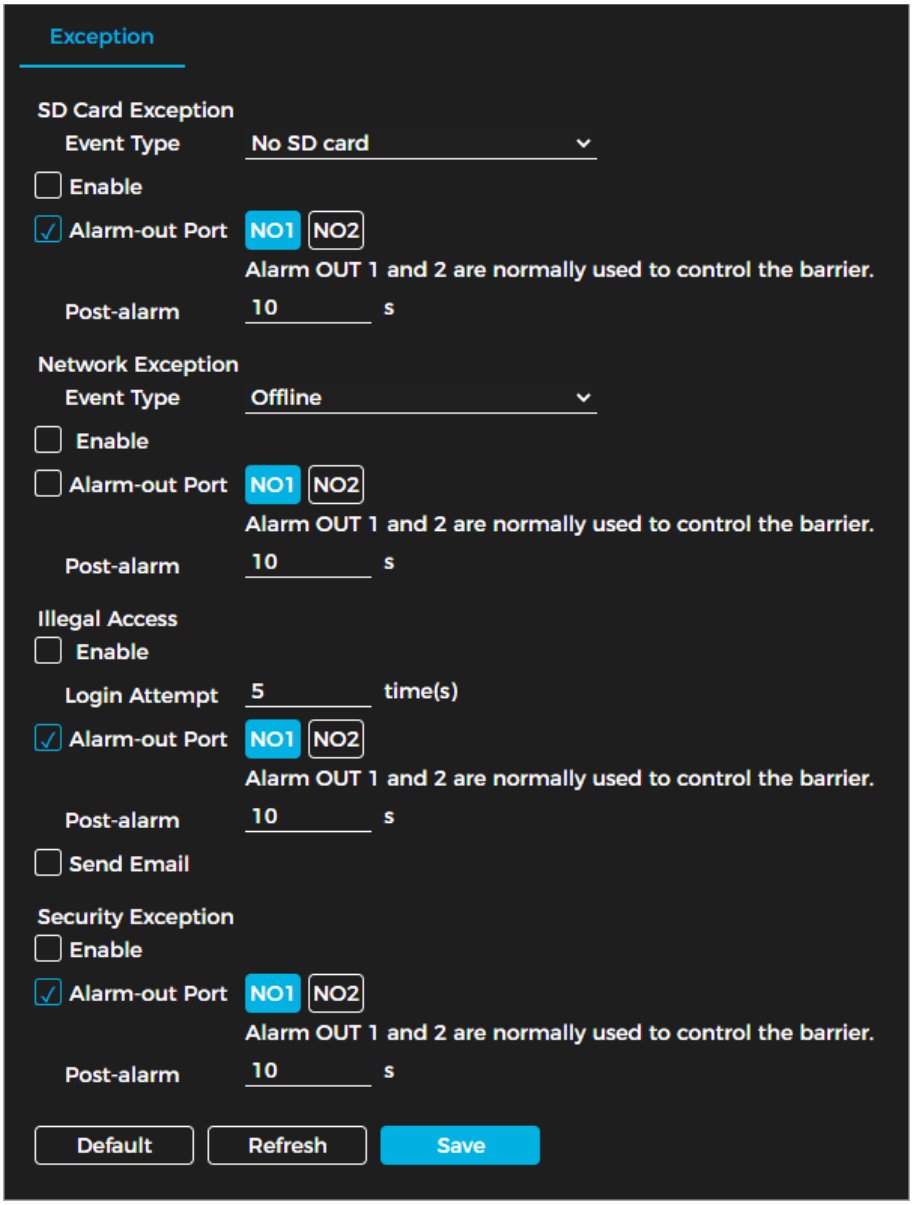
2. Choose one or more alarm channels.
3. Select **Trigger Mode** to send test alarm signals to the selected ports. Any output devices connected to the device should be triggered.

Configure Exception Alarms

Exception alarms are designed to detect and notify users of abnormal conditions. When such an event occurs, an alarm is triggered to help maintain the reliability and performance of your camera system.

Follow the steps below to configure exception alarms.

1. Navigate to Setting → Event → Exception.



Exception	Description
SD Card	An alarm will be triggered if there is no SD card, an SD card error, or insufficient storage space.
Network Error	An alarm will be triggered if the camera is offline or if there is an IP conflict.
Illegal Access	An alarm will be triggered when the system detects unauthorized access.
Security Exception	An alarm will be triggered when a security issue occurs.

2. Set the exception parameters. Some parameters on the table below may not be applicable to the specific exception. Refer to the exception page to view all the relevant parameters.

Parameter	Description
Enable	Enables exception alarms.
Free Space	When enabling Memory Insufficient, set a Free Space value. An alarm is triggered if the SD card's remaining space falls below this value.
Post-Alarm	When an alarm is triggered, it will remain active for the specified period after the event ends.

Login Attempt	Set the allowed number of login errors, ranging from 3 to 10. This setting applies only to Illegal Access events.
Send Email	The system sends an email to the specified address when an alarm is triggered. To configure the email address, go to **Setting → Network Settings → Email**. This parameter applies only to Illegal Access events.

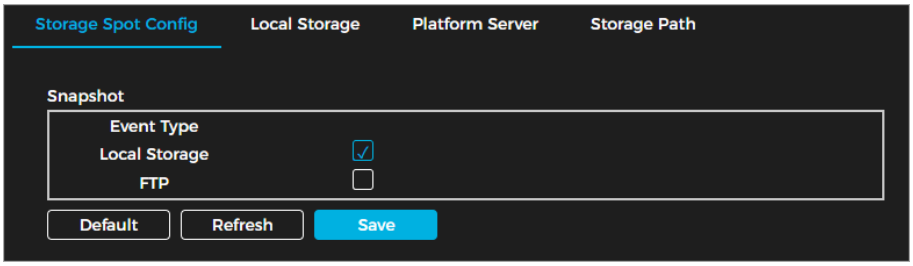
3. Click **Save**.

Storage

Configure Storage Spot

Follow the steps below to configure the storage path for snapshots.

1. Navigate Setting → Storage → Storage → Storage Spot Config.



Storage Spot Config

2. Choose the storage path (Local, FTP). Selecting both will save a copy of each snapshot to both locations.

- **Local Storage**: Saves to the memory card, which has limited capacity but provides continuous access even during network failure.
- **FTP**: Saves to the FTP server, which offers larger capacity but stops storing if the network fails.

3. Click **Save**.

Configure Local Storage

Follow the steps below to display information on the local memory card. Ensure the memory card is properly inserted before configuring. Newly installed memory cards may need to be formatted manually prior to use.

1. Navigate to Setting → Storage → Local Storage.
2. Set the parameters.

Parameter	Description
Disk Full Options	Choose **Overwrite** to replace old recordings with new ones or **Stop** to halt recording when the memory card is full.
Storage Info	Check the current usage and capacity of the memory card.
Format	Click **Format** to erase all data and reinitialize the memory card.

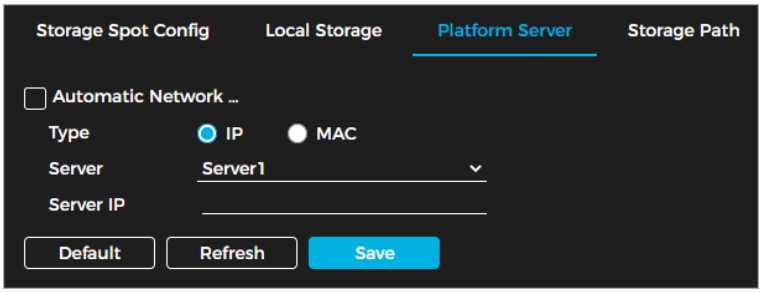
3. Click **Save**.

Configure the Platform Server

Follow the steps below to configure storage parameters for saving snapshots to the platform server. Ensure the platform software is installed and that you're logged in before enabling this function. Snapshots will only be saved to the platform server once a successful connection is established.

1. Navigate to Setting → Storage → Platform Server.

2. Set the parameters.



Platform Server

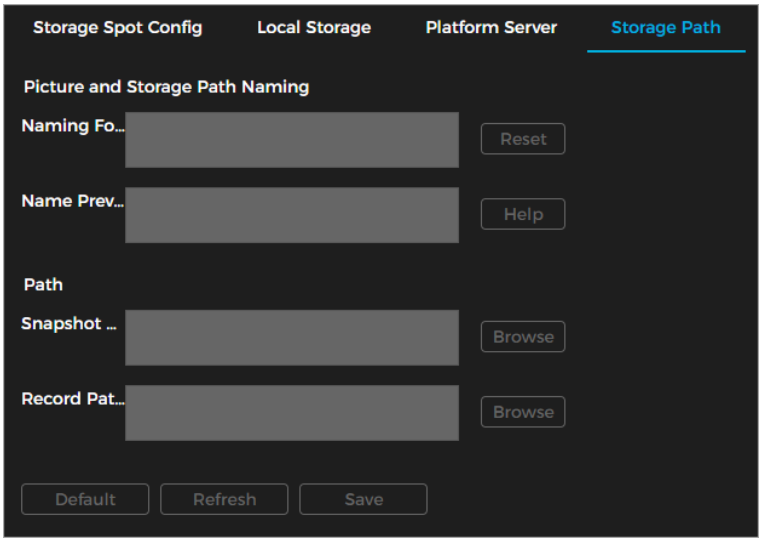
Parameter	Description
Automatic Network Recovery	When the network is disconnected or fails, images will be temporarily stored on the local storage card. Once the network connection is restored, the system will automatically upload the stored images to the platform server.
Type	Select whether to connect to the platform server using an IP address or a MAC address.
Server IP/MAC Address	Set the platform server IP or MAC address.

3. Click **Save**.

Configure the Storage Path

Follow the steps below to configure the names and storage paths of snapshots and video recordings.

1. Navigate to Setting → Storage → Storage Path.



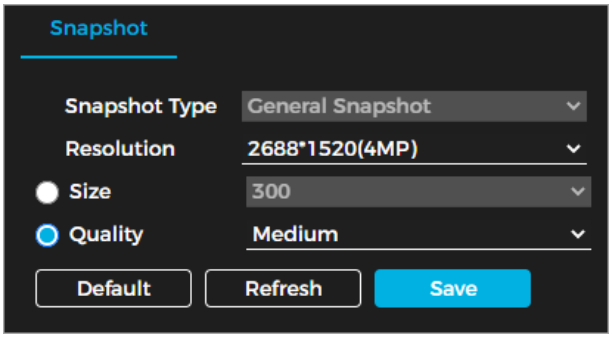
Storage Path Window

2. Set the snapshot naming rule in the Naming Format section. Click **Help** for guidance or **Reset** to restore defaults. A preview of the name appears in the Name Preview section.
3. Click **Browse** to set separate save paths for snapshots and video recordings.
4. Click **Save**.

Configure Snapshot Parameters

Follow the steps below to configure snapshot parameters.

1. Navigate to Setting → Storage → Snapshot.
2. Set the parameters.



Parameter	Description
Snapshot Type	Only General Snapshot can be selected.
Resolution	Choose the resolution to save snapshots.
Size	Choose the size of the snapshots. You can select from eight (8) preset options or select custom to manually define the size (50–1024).
Quality	Choose the quality to save the snapshots (Low, Medium, High).

3. Click **Save**.

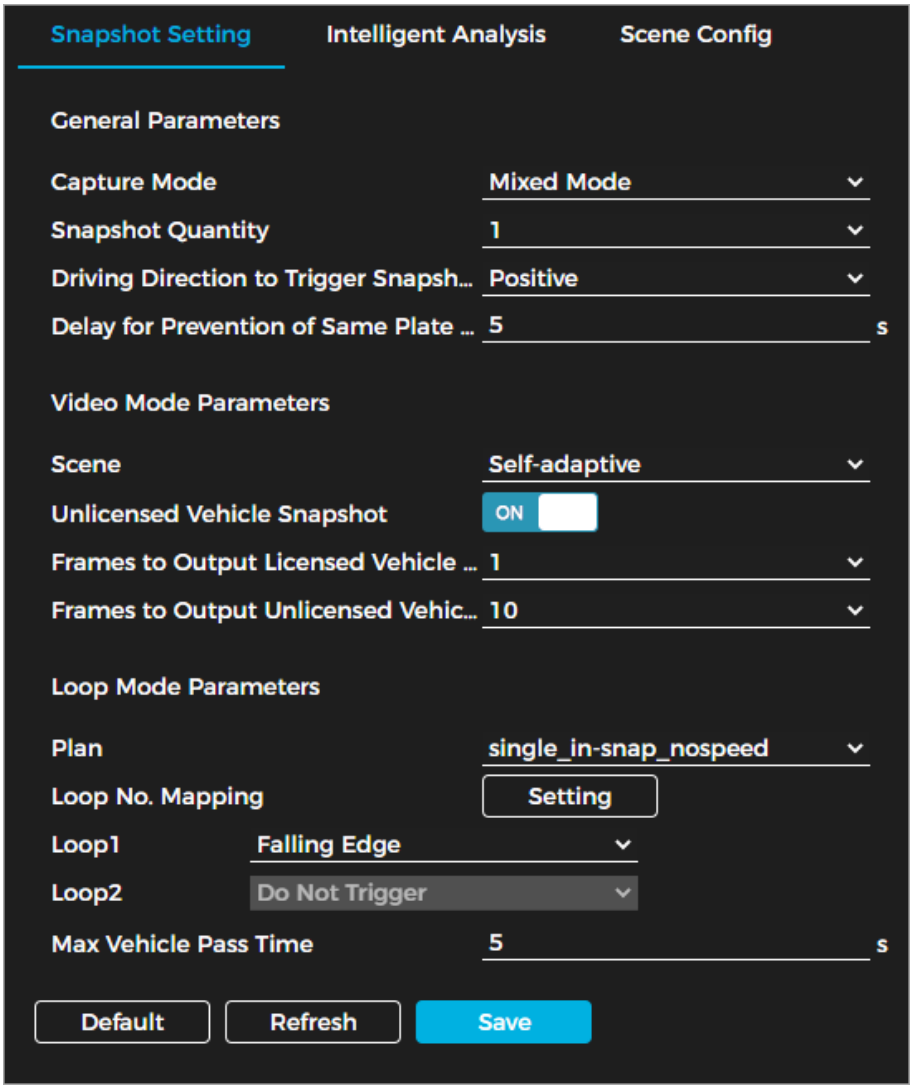
LPR

AI Settings

Configure Snapshot Rules

Follow the steps below to configure the snapshot rules of the camera.

1. Navigate to Setting → LPR → AI Setting → Snapshot Setting.
2. Set the parameters.



Type	Parameter	Description
General Parameters	Capture Mode	• **Loop**: Captures snapshots when targets enter a detection loop. • **Video**: Captures snapshots based on video analysis. • **Mixed Mode**: Captures snapshots using both loop detection and video analysis.
	Snapshot Quantity	Choose to take one (1) or two (2) snapshots at a time.
	Driving Direction to Trigger Snapshot	• **Positive**: Captures only approaching vehicles. • **Departing**: Captures only departing vehicles. • **Both Ways**: Captures vehicles moving in either direction.
	Delay for Prevention of Same Plate Capture	Set the time interval to ensure each plate is captured only once within that period.
Video Mode Parameters (These settings are only available	Scene	• Vehicle Body Trajectory: For large vehicles. • **Plate Trajectory**: For small vehicles. • **Self-Adaptive**: Automatically adjusts to the scene.

when the **Capture Mode** is set to **Video** or **Mixed Mode**).	Unlicensed Vehicle Snapshot	Click to enable capture of unlicensed motor vehicles.
	Frames to Output Licensed Vehicle Snapshot	Set the number of frames to capture a licensed vehicle. The default value 1 means capturing a snapshot upon detecting one frame of the vehicle in the detection area.
	Frames to Output Unlicensed Vehicle Snapshot	Set the number of frames to capture an unlicensed vehicle. The default value 10 means capturing a snapshot after detecting 10 frames of the vehicle in the detection area.
Loop Mode Parameters (These settings are only available when the **Capture Mode** is set to **Loop** or **Mixed Mode**).	Plan	• **single_in-snap_nospeed**: Single loop; snapshot taken when vehicle reaches the loop. • **double_in1-snap_nospeed**: Double loops; snapshot taken when vehicle reaches the first loop. • **double_in2-snap_speed**: Double loops; snapshot taken when vehicle reaches the second loop.
	Loop No. Mapping	Click **Setting** to set the map between logical loops and physical loops.
	Loop1	Set the loop trigger mode. • **Do Not Trigger**: No capture triggered. • **Rising Edge**: Capture triggered when vehicle enters loop. • **Falling Edge**: Capture triggered when vehicle exits loop. ⓘ For single_in-snap_nospeed scheme, loop 2 cannot be set.
	Loop2	

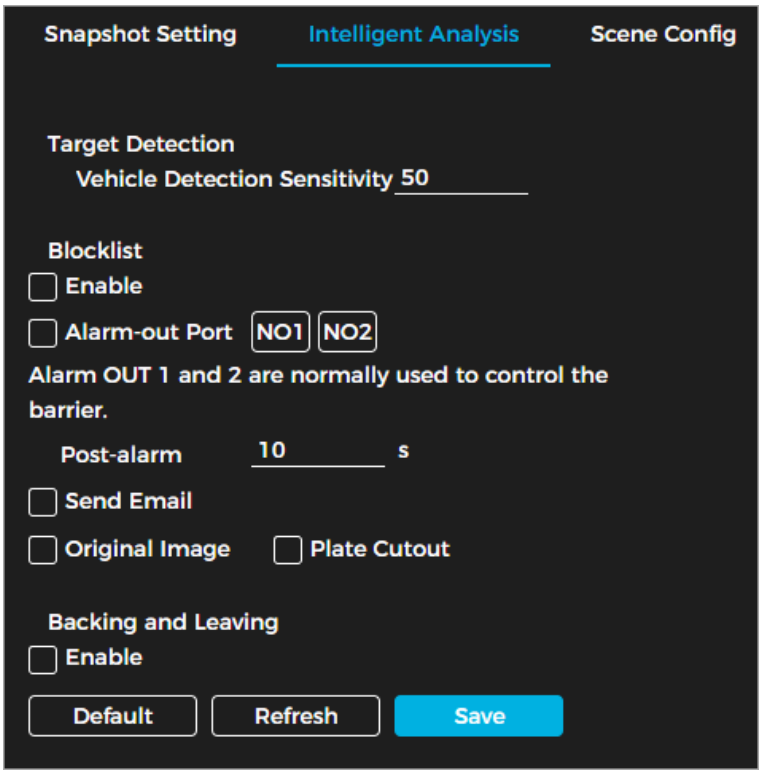
3. Click **Save**.

Configure Intelligent Analysis

The camera triggers blocklist alarms when vehicles on the blocklist are detected. Upon alarm, it activates selected alarm channels and executes specified actions. For backing and leaving events, it captures snapshots of the vehicles.

Follow the steps below to configure intelligent analysis.

1. Navigate to Setting → LPR → AI Setting → Intelligent Analysis.
2. Set the parameters.



Intelligent Analysis

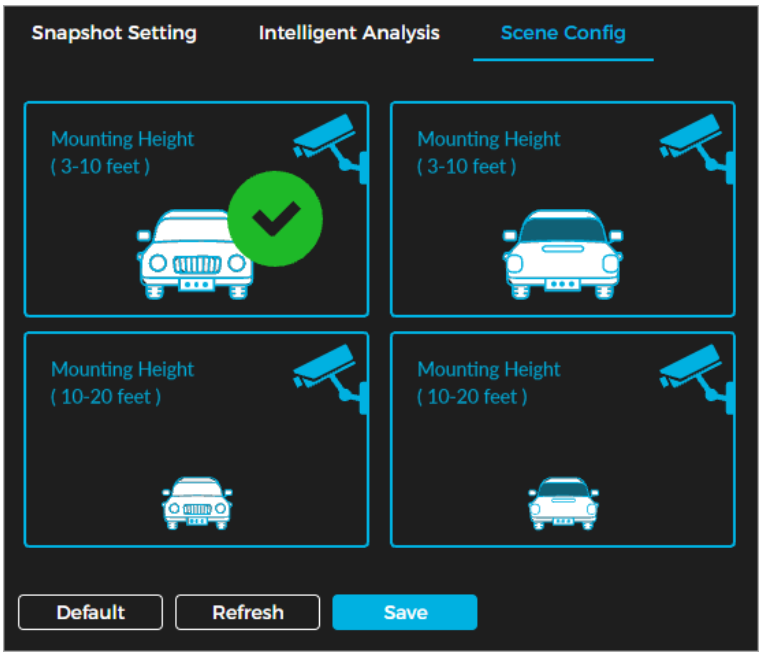
Parameter	Description
Vehicle Detection Sensitivity	Adjust vehicle detection sensitivity—the higher the value, the more easily targets are detected.
Enable	Select the checkbox to enable the blocklist.
Alarm-out Port	Select the Alarm-out port and set the post-alarm duration. Alarm out 1 and 2 are typically used to control barriers.
Send Email	Check the box to enable sending an email when intelligent detection is triggered.
Select Image	Choose the image type generated when a blocklist vehicle is detected: • **Original Image**: Full camera image • **Plate Cutout**: Cropped number plate image
Backing and Leaving	Check the box to enable alarms for backing and leaving events.

3. Click **Save**.

Scene Configuration

Follow the steps below to configure the advanced LPR functions and customize special functions.

1. Navigate Setting → LPR → AI Setting → Scene Config.
2. Choose a detection scene.



Scene Configuration

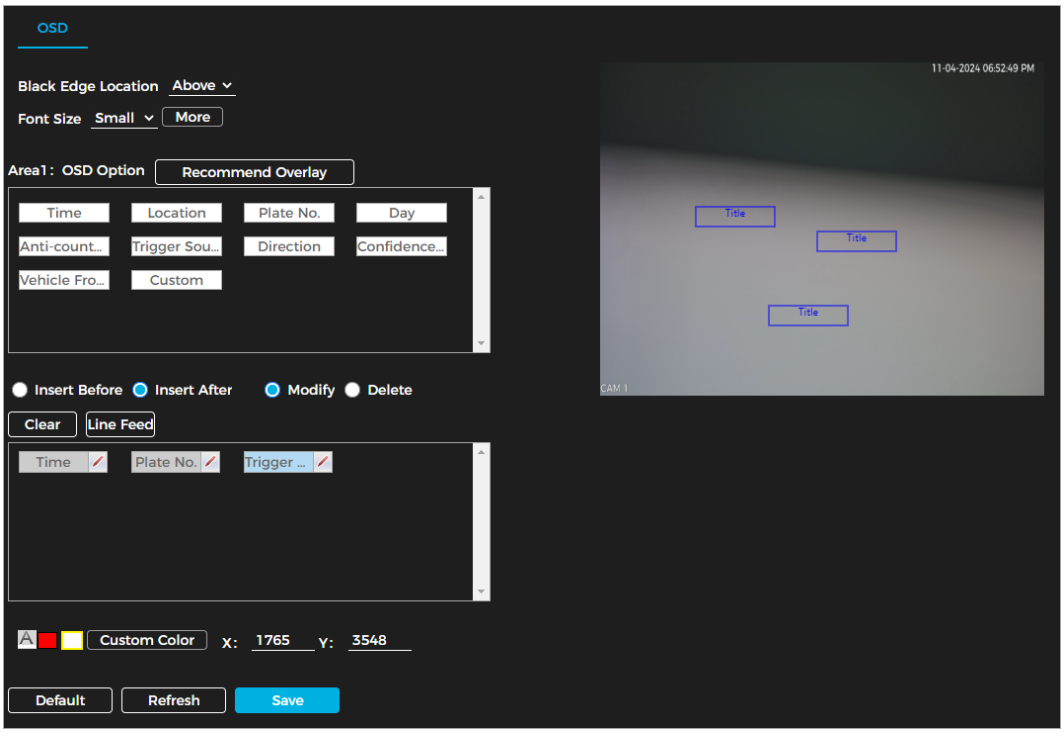
Parameter	Description
Head First	More sensitive to front plates.
Tail First	More sensitive to rear plates.
Mounting Height	Increased sensitivity when the camera is mounted higher.

3. Click **Save**.

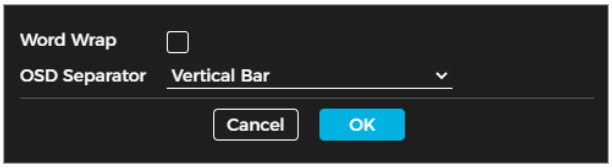
Configure Picture OSD

Follow the steps below to set the extra information displayed on snapshots.

1. Navigate to Setting → LPR → AI Setting → OSD.



2. Choose the black bar position for OSD info: Above, Below, or None (no bar).
3. Select font size and set font color.
4. Click More to adjust OSD Separator and enable or disable Word Wrap.



ⓘ

- **Word Wrap**: When enabled, OSD info moves to the next line at snapshot edges.
- **OSD Separator**: Choose how to separate info types (e.g., time and plate).
- **Example**: Vertical Bar results in "2024-11-04|A12345".

5. Set the OSD position (Title box) in the live view.

- Adjust position: Drag the yellow box or enter coordinates at the page's lower-left corner.
- Add title box: Click to get a crosshair cursor, drag to create a new box (up to 8), each showing different OSD info.
- Delete title box: Right-click the latest box to delete it.
- Configure OSD info: Click a title box to select it (area number shows), then set OSD options, font size, and color.

6. Configure the OSD information to display. Click an info type under OSD Option.

ⓘ

- Click Recommend Overlay to auto-add various info types.
- Select an existing OSD option, then Insert Before or After to add new options accordingly.
- To edit an OSD option, select Modify, then click to change prefix, suffix, content, or separator.
- To delete info, select Delete, hover, then click the delete icon; or click Clear to remove all.
- Use Line Feed to separate info into different lines.

7. Configure the information details.

Parameter	Description
With ms	Choose whether to show milliseconds. This option applies only to Time.
Prefix	Text displayed before the configured information type. For example, the prefix "Time of trigger:" for Time will show as "Time of trigger: 2024-11-04 09:58:41".
Suffix	Text shown after the configured information. For example, a suffix "Time of trigger:" for Time appears as "2024-11-04 09:58:41: Time of trigger".
Contents	Enter fixed text to display identically on each snapshot. This applies only to Location and Custom fields.
Delimiter Quantity	Choose how many separators to place between this information and other types.

8. Click **Save**.

Cutouts

Configuring Cutouts

Follow the steps below to have the camera crop plate number images from snapshots and save them to the storage path.

1. Navigate to Setting → LPR → Cutout Config.

Cutout Config Window

2. Enable this function and configure the parameters. The camera will crop and save images of vehicle plate numbers and bodies to the storage path. Both options can be selected simultaneously.
3. Click **Save**.

Configure Plate Overlays

Follow the steps below to set whether to overlay the plate image on the snapshot and adjust its position and size.

4. Navigate to Setting → LPR → Cutout Config. → Plate Overlay.

Plate Overlay Window

5. Set the overlay position and size.
6. Click **Save**.

Blocklist and Allowlist

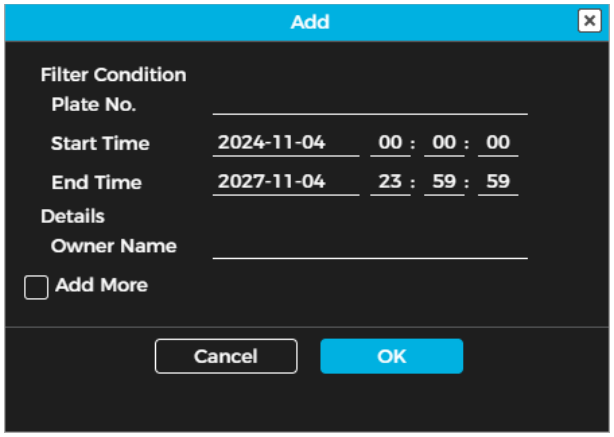
Configure the Allowlist

If the barrier control is set to Open barrier by allowlist, only vehicles on the allowlist can pass. Fuzzy match can be enabled to allow the camera to tolerate some plate character misreads, letting vehicles pass even without exact plate recognition.

Follow the steps below to configure the allowlist.

1. Navigate to **Setting → LPR → Vehicle Blocklist/Allowlist → Allowlist**.
2. Click **Search** without entering a plate number to display all vehicles in the allowlist or enter the plate number and click **Search** to check if the vehicle is in the allowlist. If found, its details will be shown.
3. Add vehicles individually or in batches.

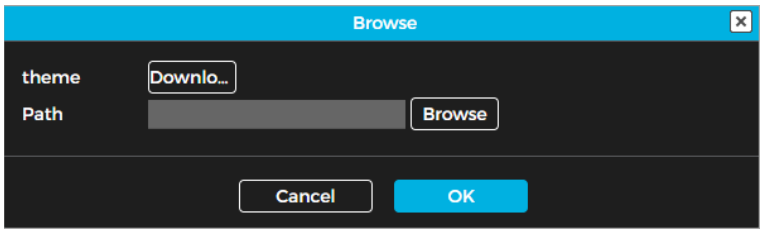
- **Add Vehicles Individually:** Click add, set the parameters, and then hit **OK**.



Add Vehicles Individually

Parameter	Description
Plate No.	Vehicle license plate number. This information is required.
Star Time End Time	Set a time period for the vehicle to pass the barrier. During this period, the vehicle's status is **Active**, allowing passage. Outside this period, the status is **Expired**, blocking passage.
Owner Name	Vehicle owner's name. This information is optional.
Add More	Check the box to continue adding another vehicle after clicking OK.

- **Add Vehicles in Batches**: Click **Browse** and then **Download** to save the template to your computer. Fill in the template, then click **Browse** to upload it. All the vehicles in the template will be imported to the allow list.



Download Template

  - To export allowlist info: Click **Export**, then choose whether to encrypt.
  - To edit a vehicle: Click the icon.
  - To delete a vehicle: Click the icon. If allowlist control is enabled, the vehicle won't pass.
  - To remove expired vehicles: Click **Clear Expired Data**.
  - To delete all vehicles: Click **Clear**. This cannot be undone.

4. Select **Fuzzy Matching**, then choose the options to define the fuzzy match rules.

Parameter	Description
The snapshot is missing the first or last character of the plate	Choose to enable one or both functions.
The snapshot has 1 character added to either end of the plate	

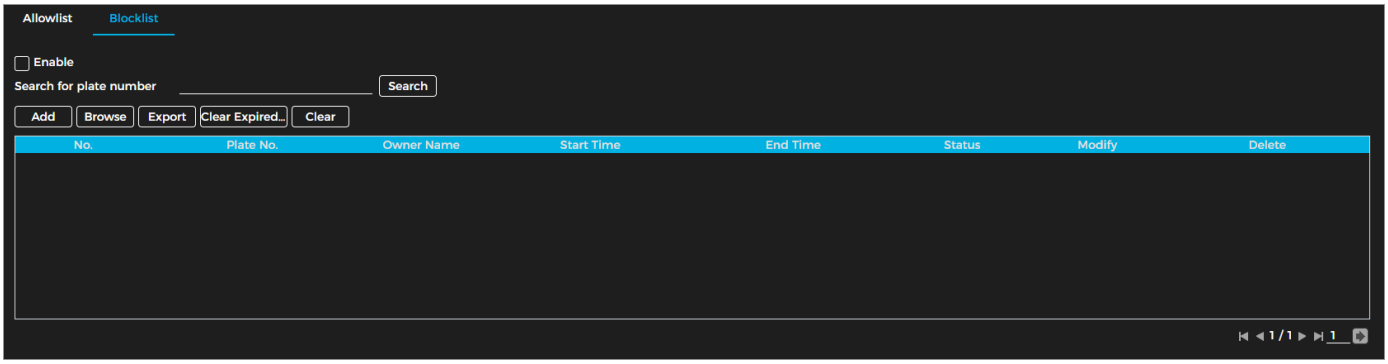
Allow the system to misread some of the characters on the plate	Select how many characters the camera can misread in a plate number. If set to 0, this setting will be automatically disabled.
Number of characters allowed to be misread	This setting lets the camera treat specific characters as interchangeable. You can define up to 10 rules. For example, a rule like 0<->D allows A0123 and AD123 to be recognized as the same, enabling the barrier to open for either.

5. Click **Save**.

Configure the Blocklist

Vehicles on the blocklist are denied access through the barrier.

Go to **Setting → LPR → Vehicle Blocklist/Allowlist → Blocklist** to configure. The steps are similar to configuring the allowlist.

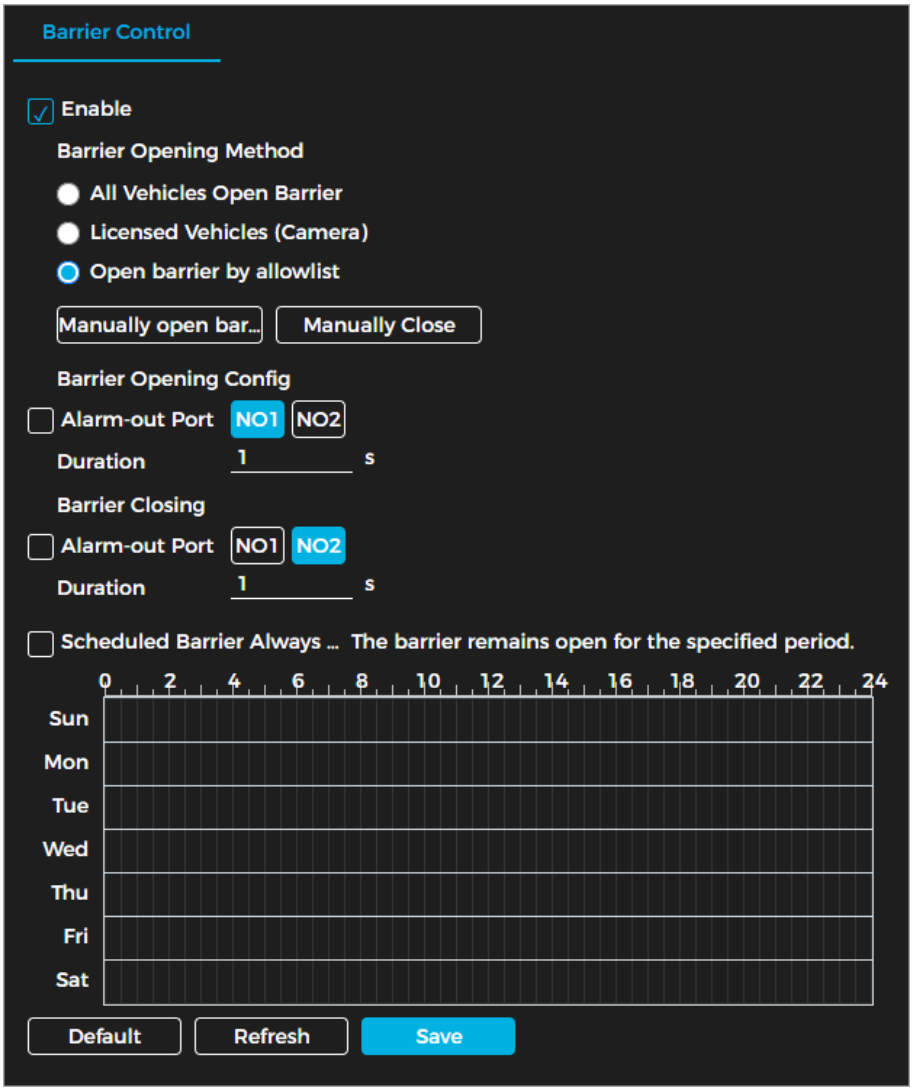


Blocklist

Configure Barrier Control

Follow the steps below to configure the barrier control mode and information about opening and closing the barrier.

1. Navigate to **Setting → LPR → Barrier Control**.
2. Set the parameters.



Barrier Control Configuration Window

Parameter	Description
Barrier Opening Method	Trigger alarms and control the barrier remotely using the following modes: • **All Vehicles Open Barrier**: Opens the barrier when any vehicle is detected. • **Licensed Vehicles (Camera)**: Opens the barrier when a license plate is detected. • **Open Barrier by Allowlist**: Opens the barrier for vehicles on the allowlist or matching fuzzy rules. • **Manual Control**: Click Manually Open Barrier or Manually Close to operate the barrier manually.
Barrier Opening Config Barrier Closing	• **Alarm-out Port**: Select the appropriate alarm output port based on your field connection. • **Duration**: Set how long the barrier open/close signal remains active.
Scheduled Barrier Always Open	Enable the **Barrier Always Open** function and set the time period during which the barrier remains open and does not close.

	Click a specific day, then drag on the timeline to define the period. Click once on the timeline to delete a set period.

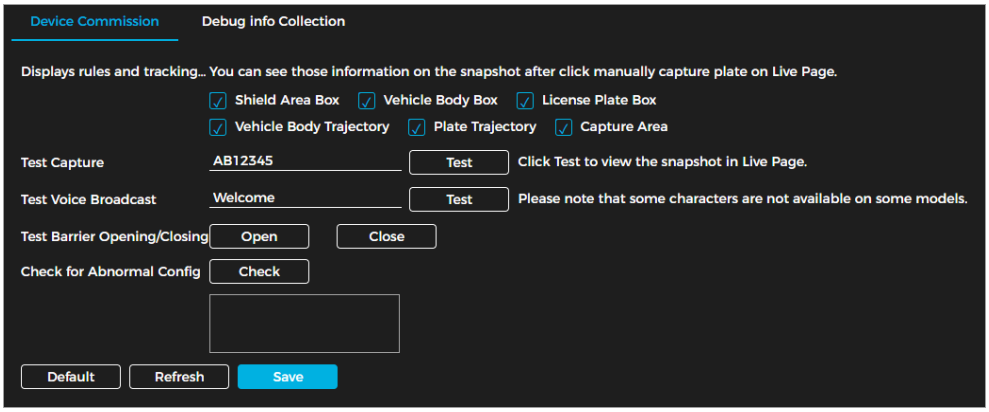
3. Click **Save**.

Device Commission

Configure Device Commissioning

Follow the steps below to overlay information on snapshots to verify if they meet your requirements. You can also test various functions to ensure they work as configured.

1. Navigate to **Setting → LPR → Device Commission → Device Commission**.



Device Commission Window

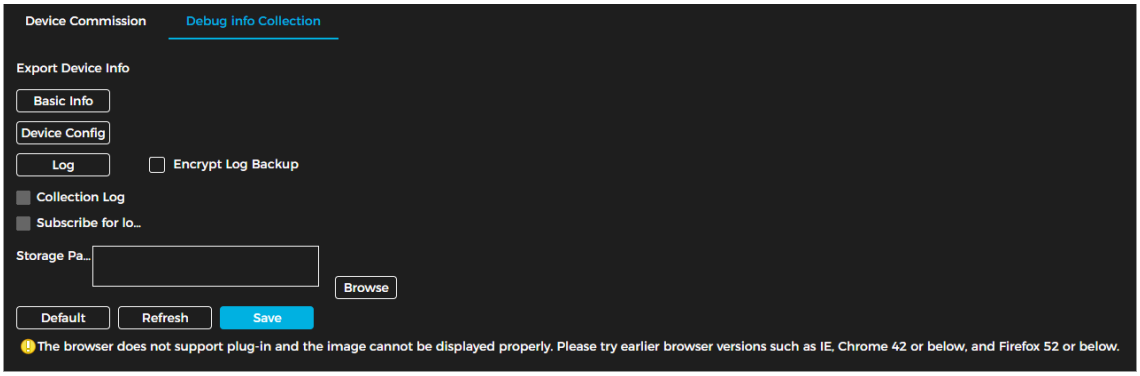
2. In Display Rules and Tracking Info, select the information to be shown. Click **Save** and check overlays on the **Live** page. Click the camera icon to manually capture a license plate for review. Adjust and repeat this step if needed.
3. Test the other functions to ensure proper functionality.

Parameter	Description
Test Capture	Enter a plate number, click **Test** to capture, and view the snapshot on the Live page.
Test Voice Broadcast	Enter information and click **Test** to check if the device plays the sound correctly. Some characters may not be supported on certain models.
Test Barrier Opening/Closing	Click **Open** or **Close** to test the barrier response.
Check for Abnormal Config	Click **Check** to let the system automatically detect abnormalities.

Collect Debug Information

Follow the steps below to collect operation logs to track errors.

1. Navigate to **Setting → LPR → Device Commission → Debug Info Collection**.
2. Export device info by selecting types and storage path. For logs, check **Encrypt Log Backup** to encrypt.
3. Choose one or more log types to collect.
4. Select **Subscribe for logs** (log path can't be changed).
5. Clear **Subscribe Log**, then click **Browse** to set operation log save path.
6. Click **Save**.



Collection Log

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).