V1.0.0

License Plate Recognition Camera

User's Manual

Foreword

General

This manual introduces the structure, functions, and operations of the license plate recognition camera (hereinafter referred to as "the Camera"). Read carefully before using the Camera, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
⚠ DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
⚠ CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user’s manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates

might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.

- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Camera, hazard prevention, and prevention of property damage. Read carefully before using the Camera, and comply with the guidelines when using it.

Transportation Requirements

⚠

- Pack the Camera with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Avoid heavy stress, violent vibration, and immersion during transportation.
- Transport the Camera under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the transporting temperature and humidity of the Camera.

Storage Requirements

⚠

- Store the Camera under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the storing temperature and humidity of the Camera.
- Avoid heavy stress, violent vibration, and immersion during storage.

Installation Requirements

⚠ DANGER

- Make sure that the power is off when you connect the cables, install or disassemble the Camera.
- All installation and operations must conform to local electrical safety regulations.
- Use accessories suggested by the manufacturer, and installed by professionals.
- Do not block the ventilator of the Camera, and install the Camera in a well-ventilated place.
- Do not expose the Camera to heat sources or direct sunlight, such as radiator, heater, stove or other heating equipment, which is to avoid the risk of fire.
- Do not place the Camera in explosive, humid, dusty, extremely hot or cold sites with corrosive gas, strong electromagnetic radiation or unstable illumination.
- Avoid heavy stress, violent vibration, and immersion during installation.

⚠ WARNING

Safe and stable power supply is a prerequisite for proper operation of the Camera.

- Make sure that the ambient voltage is stable and meet the power supply requirements of the Camera.
- Prevent the power cord from being trampled or pressed, especially the plug, power socket and the junction from the Camera.
- Do not connect the Camera to two or more kinds of power supplies; otherwise, the Camera might be damaged.

⚠

It is recommended to use the Camera with a lightning protector for better lightning-proof effect.

Operation Requirements

⚠

A suitable operating environment is the foundation for the Camera to work properly. Confirm whether the following conditions have been met before use.

- Use the Camera under allowed humidity and temperature conditions. Refer to the technical parameters for requirements on the operating temperature and humidity of the Camera.
- Use the Camera on a stable base.
- Do not let any liquid flow into the Camera to avoid damage to internal components. When liquid flows into the Camera, immediately disconnect the power supply, unplug all cables connected to it, and contact after-sales service.
- Do not plug or unplug RS-232, RS-485 and other ports with the power on, otherwise, the ports will be easily damaged.
- Back up data in time during deployment and use, in an effort to avoid data loss caused by abnormal operation. The company is not liable for data security.
- The company is not responsible for damages to the Camera or other product problems caused by excessive use or other improper use.

Maintenance Requirements

⚠ WARNING

- Contact professionals for regular inspection and maintenance of the Camera. Do not disassemble or dismantle the Camera without a professional present.
- Use accessories suggested by the manufacturer, and maintain the Camera by professionals.

Table of Contents

1 Product Information

1.1 Overview

The Camera adopts intelligent deep learning algorithms and supports the recognition of license plates, logos, vehicle models, colors and mores.
It consists of a protective housing, illuminator and intelligent HD camera. The intelligent HD camera has progressive scan CMOS which supports high definition images, low illuminance, high frame rate and great color rendition.
The Camera is suitable for use in various scenes such as community roads, parking lots and places that need entrance and exit surveillance.

1.2 Functions

The functions are available on select models, and might differ depending on the model.

Permission Management

- Each user group has permissions. The permissions of a user cannot exceed the permissions of its group.
- 2 user levels.
- Permission to open the barrier and blocklist alarm function.
- Device configuration, and permission management through Ethernet.

Storage

- Stores video data on the central server based on the configuration.
- You can record videos on the webpage. The recorded videos will be stored on your computer.
- Supports local hot swapping of storage card, and storage when network is disconnected. The system automatically overwrites stored images and videos when the memory becomes insufficient.
- Stores up to 1,024 pieces of logs.
- Supports FTP storage and automatic network replenishment (ANR).

Alarm

- Alarms are triggered through the network when errors occur on the Camera, such as memory card damage.
- Some devices can connect to various alarm peripherals to respond to external alarm input in real time (within 200 ms). The system can deal with various alarms according to preset linkages and generate voice prompts (you can upload voice recordings in advance).

Network Monitoring

- Transmits compressed video data for a channel to the network terminal, and makes it reappear after decompression through the network. Keep latency within 500 ms when bandwidth is allowed.
- Up to 10 users can be online at the same time.
- Supports system access and device management through the webpage.
- Video data transmission adopts HTTP, TCP, UDP, MULTICAST, and RTP/RTCP.

Capture and Recognition

- Recognizes vehicle information such as the license plate, vehicle color, vehicle logo, and vehicle model.
- Supports setting OSD information.
- Supports encoding, taking snapshots, and image watermark encryption to prevent images from being tampered with.

Peripheral Control

- Peripheral control: Supports setting various peripheral control protocols and connection pages.
- Connects to external devices such as vehicle detectors and signal detectors.

2 Structure

2.1 Appearance

Figure 2-1 Appearance

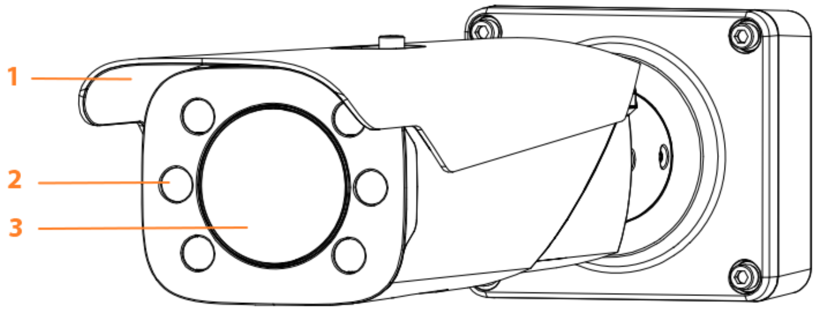


Table 2-1 Appearance description

No.	Description	No.	Description
1	Protective cover	3	Lens
2	Illuminator	–	

2.2 Rear Panel

Figure 2-2 Rear panel

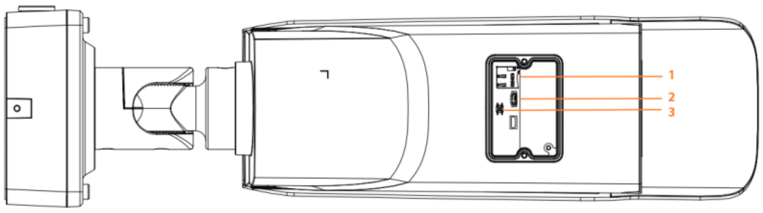
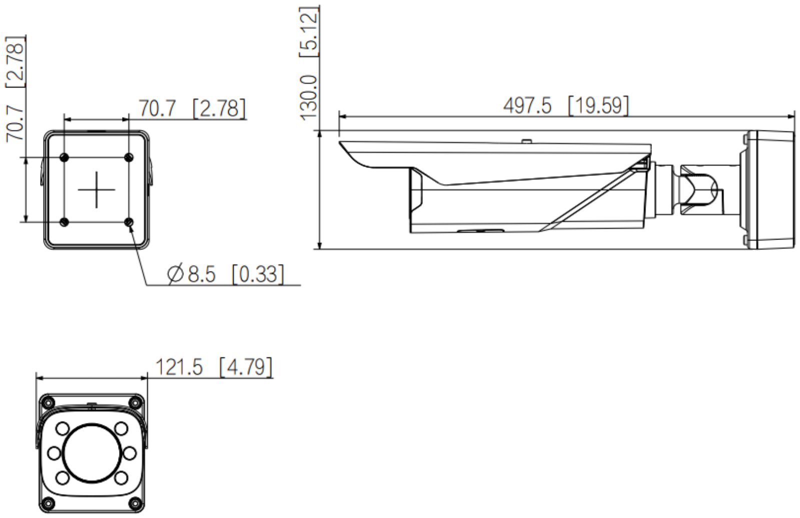


Table 2-2 Port description

No.	Description	No.	Description
1	TF card	3	Hardware reset
2	Debugging port	–	

2.3 Dimensions

Figure 2-3 Dimensions (mm [inch])



2.4 Cable Connection

Figure 2-4 Cable connection

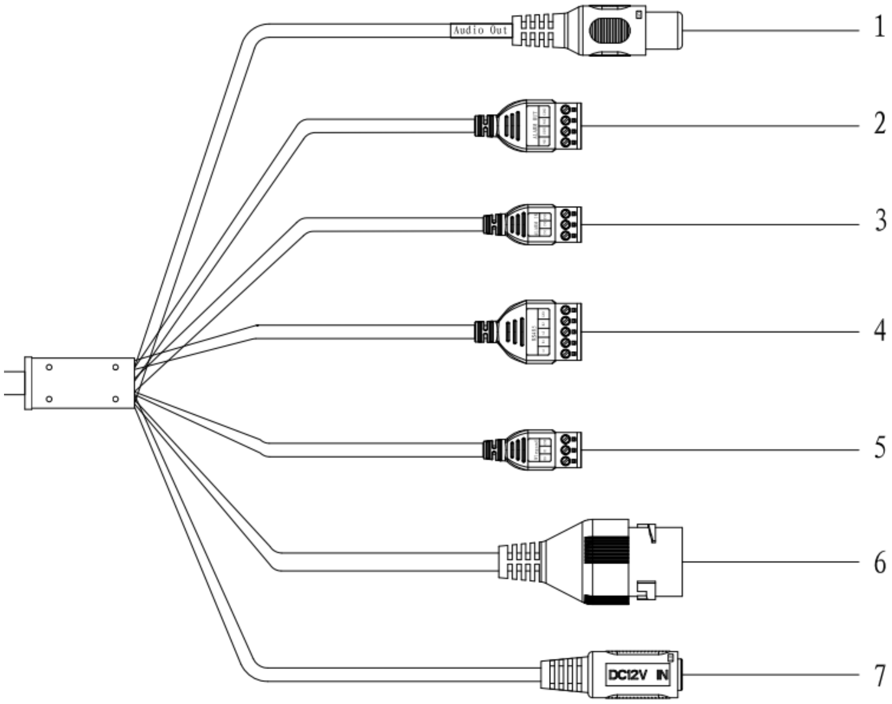


Table 2-3 Port description

No.	Name	Description
1	Audio out	Sends audio signals through this port.
2	Alarm out	Used to connect the barrier and alarm output devices such as alarm light.
3	Alarm in	Used to connect alarm input devices such as vehicles detectors, IR detectors and induction loops.
4	RS-485	The RS-485 port.
5	Wiegand	The wiegand port.
6	RJ-45	The RJ-45 port.
7	12 VDC	Inputs 12 VDC power.

3 Web Client

3.1 Webpage Introduction

Log in to the web client of the Camera through a browser, on which you can operate, configure and maintain the Camera.

3.1.1 Initializing Camera

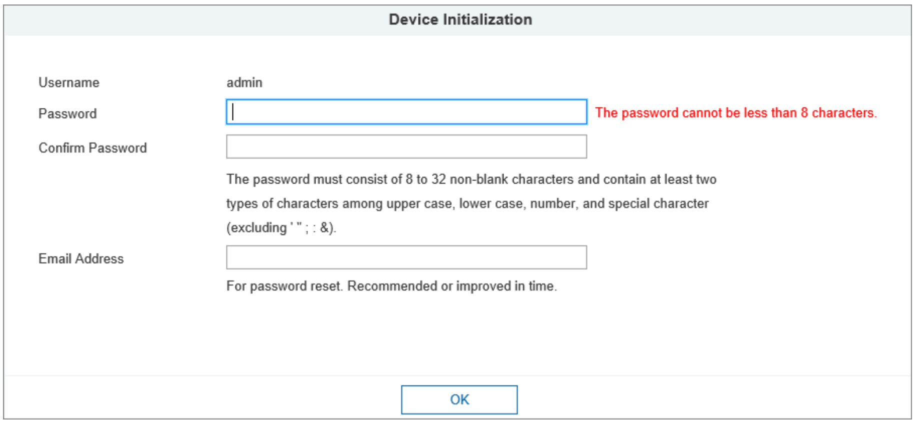
The Camera is delivered uninitialized. You need to initialize it, and change its password before performing operations with it.

Before initialization, make sure that computer IP and camera IP are on the same network segment. Otherwise, you might fail to open the initialization page.

Procedure

Step 1 Open a browser, enter the IP address of the Camera in the address bar, and then press the Enter key.

Figure 3-1 Device initialization



Device Initialization

Username: admin

Password: The password cannot be less than 8 characters.

Confirm Password:

The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

Email Address:

For password reset. Recommended or improved in time.

Step 2 Enter and confirm the password.

If you want to change the password again, go to **Setting** > **System** > **Account** > **Account** > **Username**.

Step 3 Enter your email address.

Step 4 Click **OK**.

Step 5 Enter the username and password, and then click **Login**. Then it automatically redirects to the **Live** page.

3.1.2 Device Login

Prerequisites

- You need to initialize the camera before logging in to the webpage. For details, see "3.1.1 Initializing Camera".
- Follow the instructions to download and install the plug-in for first-time login.

Procedure

Step 1 Open a browser, enter the IP address of the Camera in the address bar, and then press the Enter key.

Step 2 Enter the username and password.

The username is admin by default.

Click **Forget password?**, and then you can reset the password through the reserved email. For details, see "3.1.3 Resetting Password".

Step 3 Click **Login**.

3.1.3 Resetting Password

When you need to reset the password for the admin account, there will be a security code sent to the linked email address which can be used to reset the password.

Prerequisites

You have enabled password resetting service. For details, see "3.5.1.4.4 Resetting Password".

Procedure

Step 1 Open the browser, enter the IP address of the camera in the address bar, and then press the Enter key.

Step 2 Click **Forget password?**, and you can reset the password through the email address that is set during the initialization.

3.1.4 Webpage Functions

Figure 3-2 Functions

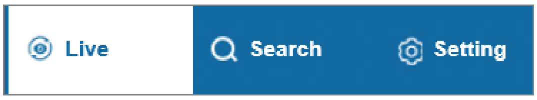


Table 3-1 Function description

Function	Description
Live	View live videos in real time, take snapshots, record videos, adjust the window display, and configure the image parameters.
Search	Search for images and videos, and configure watermark verification for videos.
Setting	Configure basic attributes of the camera, network, storage, and system settings, and view system information.

Function	Description
[→	Log out.

The common buttons on the webpage are as follows.

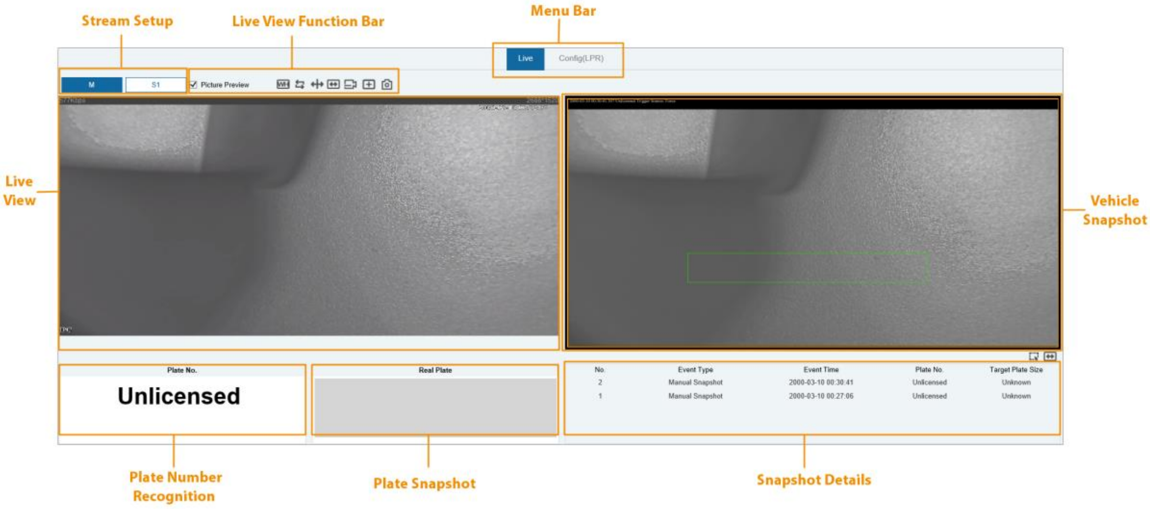
Table 3-2 Common buttons

Button	Description
Default	Restores the parameter to the default value.
Save	Saves current configurations.

3.2 Live Page

After successfully logging into the webpage, you will be directed to the **Live** page where you can access various features. This includes viewing the live video image, taking snapshots, viewing event details, and performing other operations.

Figure 3-3 Live page



No.	Event Type	Event Time	Plate No.	Target Plate Size
2	Manual Snapshot	2000-03-10 00:30:41	Unlicensed	Unknown
1	Manual Snapshot	2000-03-10 00:27:06	Unlicensed	Unknown

3.2.1 Stream Setup

Click M S1 to select the stream type.

- Select **M** (main stream) when you have stable network connectivity and sufficient bandwidth. It offers higher resolution and better image quality, ensuring that important details are captured accurately.

  You can configure main stream resolution in **Setting** > **Video/Audio** > **Video** > **Video Stream**.

- Select **S1** (sub stream) when you have limited bandwidth. It serves as a lower-resolution alternative to the main stream, which requires less bandwidth while still providing a smooth video play experience.

3.2.2 Live View

Displays the live video captured by the Camera. You can also click the icons to change the display mode of live view.

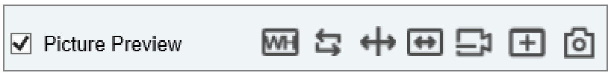
Table 3-3 Live view display adjustment

icon	name	description
WH	W:H	Displays the live video in its original size or in an adaptive window.
⇆	Switch Window	Switch to big window. Click it again to exit big window.
↔	Target Box	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed in the video image.
⇔	Full Screen	Click to full-screen display. Double-click or press the Esc button to exit full screen.

3.2.3 Live View Function Bar

Set functions on the **Live** page, and then the system will display the desired information on the **Live** page.

Figure 3-4 Function bar



☑ Picture Preview

Table 3-4 Function description of the Live page

Icon	Name	Description
☑ Picture Preview	Picture Preview	When selected, the camera automatically receives vehicle snapshots and detects event information, and displays snapshots and information at the lower part of the page. The snapshots are saved in the storage path defined by **Setting** > **Storage** > **Storage** > **Storage Path**.
📹	Video	Click to start recording. Click it again to stop recording and the recorded video will be saved to the set path. The Camera will keep recording until the webpage is closed or you log out if the recording is not manually stopped.

Icon	Name	Description
⊞	Digital Zoom	Select it, and place the cursor over the area in the live view image that you want to zoom in on. Click and then drag the mouse to draw a rectangle around the desired area. Adjust the area by dragging the mouse if needed. Right-click or click it again to restore the original size.
📷	Manual Snapshot	Click to take a snapshot. 🕮 Enable **Picture Preview** first.

3.2.4 Plate Number Recognition

Displays the plate number recognized by the Camera in real-time when a vehicle passes.

3.2.5 Plate Snapshot

Displays the snapshot of a license plate when a vehicle passes.

3.2.6 Vehicle Snapshot

Select **Picture Preview**, and then snapshots will be displayed when vehicles pass.

Click ⬚, and then draw a rectangle on the image to show the pixel size of that area.

Click ↔ to switch to a big window. Click it again to exit a big window.

Double click the image to full-screen display. Double-click or press the Esc button to exit full screen.

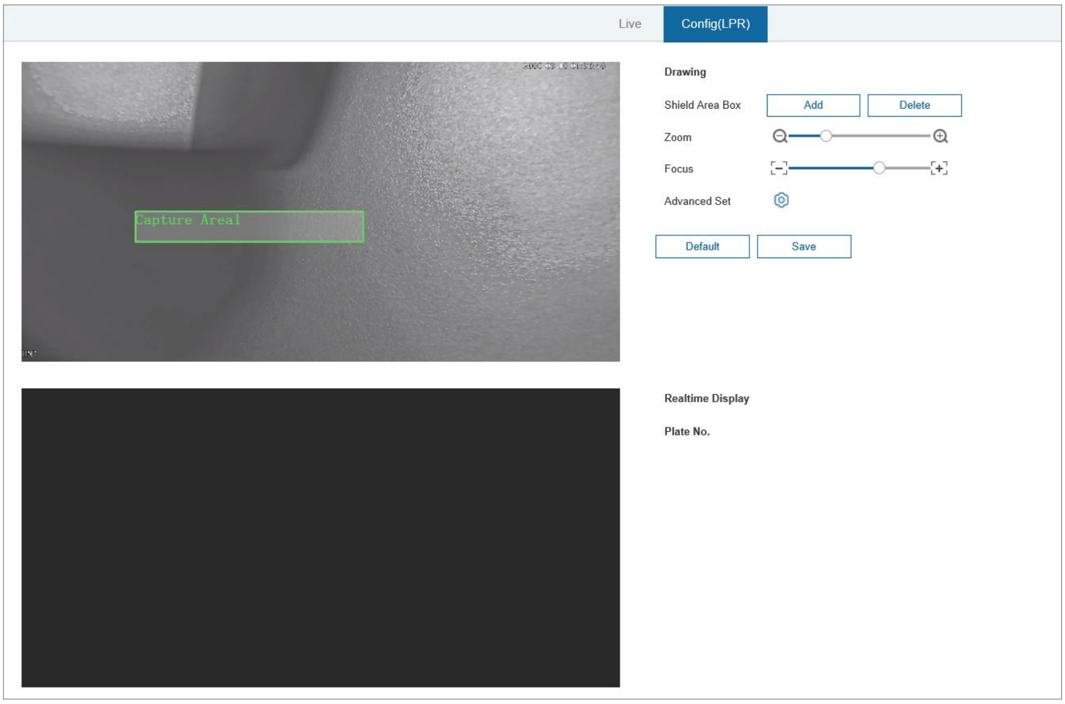
3.2.7 Snapshot Details

Select **Picture Preview**, and the event information will be displayed, including number, event types, capture time and target plate size.

3.3 LPR Config

To capture clear and accurate images of license plates, click **Config(LPR)** to configure the camera parameters for license plate recognition.

Figure 3-5 Drawing



- **Capture Area and Shield Area**

  Capture area refers to the region where the camera captures images or video footage for license plate recognition.

  Shield area refers to a specific region that is intended to be shielded from license plate recognition. The camera will ignore all the license plates detected in this area.

  - **Capture Area**: You can customize its size, shape and position. Drag the 4 vertexes to adjust its shape and drag the entire shape to adjust its position.
  - **Shield Area Box**: You can add up to 2 shielding areas by clicking **Add** and dragging the 4 vertexes to define its scope.

    Click **Delete** to delete the area.

  We recommend performing tests and adjustments to ensure that the capture area can be effectively used to take snapshots of license plates. Also, make sure that license plate recognition is not being performed in the shield area.

- **Zoom and Focus**

  Focus is triggered by zoom and is automatically adjusted. The focus can be adjusted manually as well.

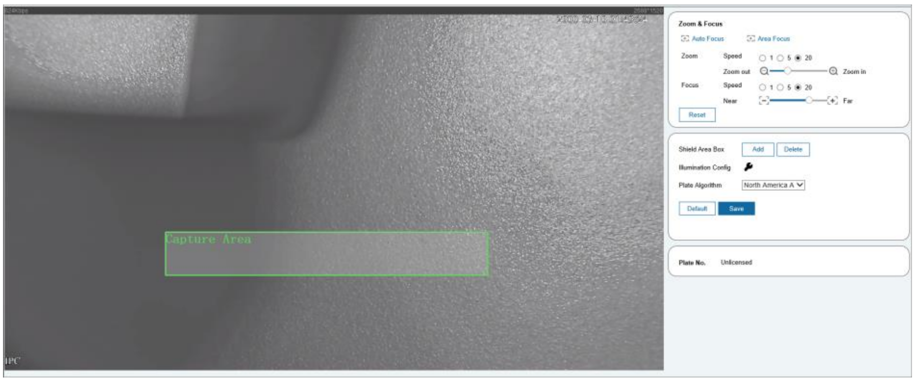
  - **Zoom**: Adjusts the lens to magnify or reduce the size of the image.

    Click or hold + or –, or drag the slider to zoom in or out.
  - **Focus**: Adjusts the optical back focal length to make the image sharper and clearer.

    Click or hold + or –, or drag the slider to adjust the focus.

If you want to further adjust the camera, click ⚙ next to **Advanced Set**.

Figure 3-6 Advanced set



Zoom Speed: ○ 1 ○ 5 ● 20

Focus Speed: ○ 1 ○ 5 ● 20

Shield Area Box

Illumination Config

Plate Algorithm: North America A

Plate No. Unlicensed

- **Zoom and Focus**
  - ◇ **Auto Focus**: Click to adjust the focus automatically.

    Other lens operations are not allowed during this process.
  - ◇ **Area Focus**: Click to concentrate the focus on the designated area.

    Click it and then drag over an area in the live view video.

    This is useful when you want to focus on the license plate area, and allow other areas in the image to become blurred.
  - ◇ Manually adjust zoom and focus.

    Adjust the speed to configure how much a camera focuses and zooms with each time it is clicked. The larger the value is, the more the camera will adjust its focus and zoom with each click.
- **Shield Area**

  Up to 3 areas can be added.
- **Illumination Config**

  Click , then it automatically redirects to the **Display Settings** page. You can customize and optimize how the video is displayed.
- **Plate Algorithm** allows the system to recognize license plates from specific regions. When it is set to North America ALG, the system will recognize North American license plates, and the various designs and versions that are local to the region.

You can click **Back** at the upper-right to the config page.

3.4 Query

You can search for snapshots, vehicle flow, and video recordings on the **Query** page.

3.4.1 Image Search

3.4.1.1 Memory Card Image

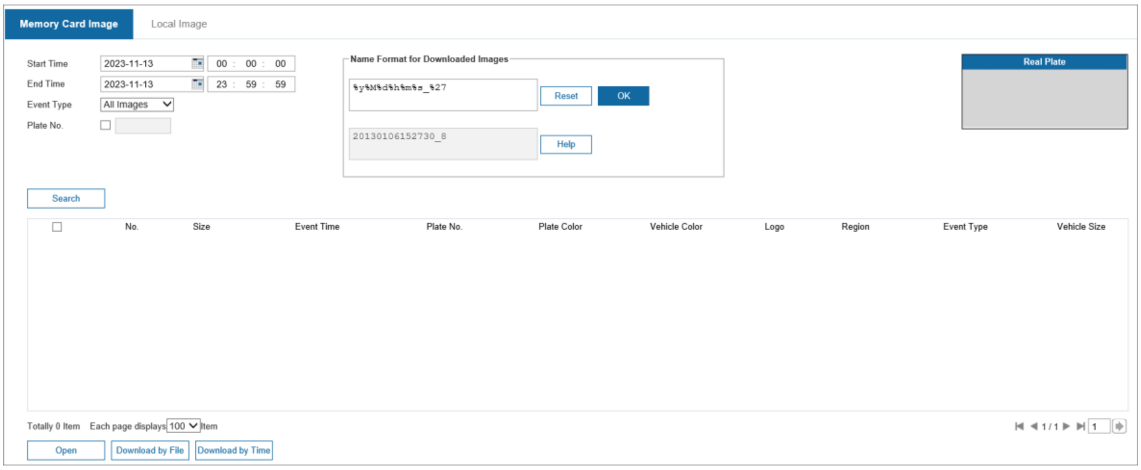
Search for and download the images stored in the memory card.

Make sure that the memory card is properly inserted; otherwise, there might be no results.

Procedure

Step 1 Select **Search** > **Picture Query** > **Memory Card Image**.

Figure 3-7 Memory card image



Start Time 2023-11-13 00 : 00 : 00

End Time 2023-11-13 23 : 59 : 59

Event Type All Images

Plate No. □

Name Format for Downloaded Images

%y%M%d%h%m%s_%27

20130106152730_8

□	No.	Size	Event Time	Plate No.	Plate Color	Vehicle Color	Logo	Region	Event Type	Vehicle Size

Totally 0 Item Each page displays 100 Item

Step 2 Configure the parameters, and then click **Search**.

Table 3-5 SD picture parameters

Parameter	Description
Start Time	Set the start time and the end time to define a period, and then you can search for images stored on the memory card within this period.
End Time	
Event Type	● **All Images**: Search for all snapshots. ● **LPR**: Snapshots captured by the LPR camera when it detects and recognizes license plates. ● **Manual Snapshot**: Search for snapshots that are captured manually by the user.
Plate No.	Select the checkbox, and then enter the plate number to search for images related to this plate.

Related Operations

- Select a search result from the result list. The **Real Plate Info** section displays the captured image of the plate.
- Select a search result from the result list, and then click **Open** to view the corresponding vehicle snapshot.
- Select one or more images that you want to download. Click **Download by File** to download the selected images to the defined path. Click **Download by Time** to download the images that were captured during the defined period to the defined path.
- Rename the snapshots. Click **Help** to view the naming rule. Click **Reset** to rename, and then click **OK**.

3.4.1.2 PC Picture

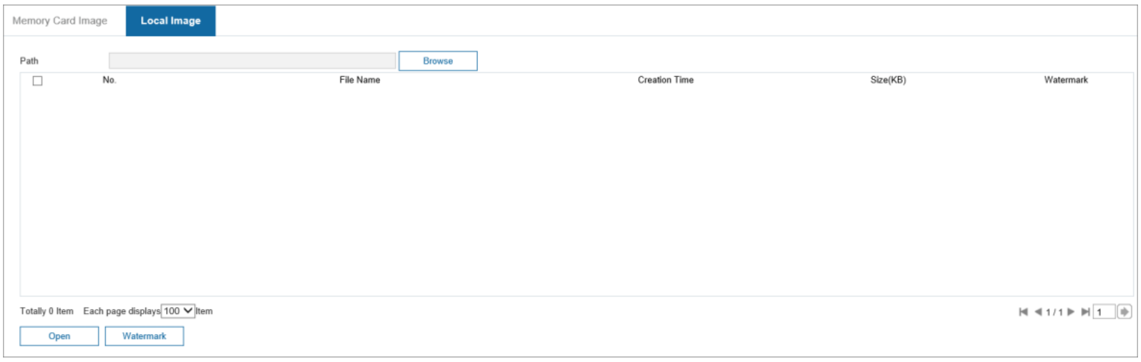
You can view images saved on your computer and verify whether the image was tampered with a watermark.

To view or set the save path of images on your computer, go to **Setting** > **Storage** > **Storage** > **Storage Path**.

Procedure

Step 1 Select **Search** > **Picture Query** > **Local Image**.

Figure 3-8 PC picture



Step 2 Click **Browse**, and then select the images that you want to verify.

Step 3 Click **Watermark**, and view the result under the **Watermark** column.

- When the result is **Error**, the picture is tampered.
- When the result is **Normal**, the picture is not tampered.

Click **Open** or double-click the picture if you need to preview the picture.

3.4.2 Recording Search

Search for the video recordings stored on your computer to trace back abnormal events (if any).

3.4.2.1 Recording

You can search for video recordings on your computer and play back the video.

Click on the **Live** page, and the Camera starts recording. The recorded video is saved to the path defined in **Setting** > **Storage** > **Storage** > **Storage Path**.

Procedure

Step 1 Select **Search** > **Search Video** > **Record**.

Step 2 Click **Select File** to select the recorded video on your computer, and then you can play back the video.

Figure 3-9 Record

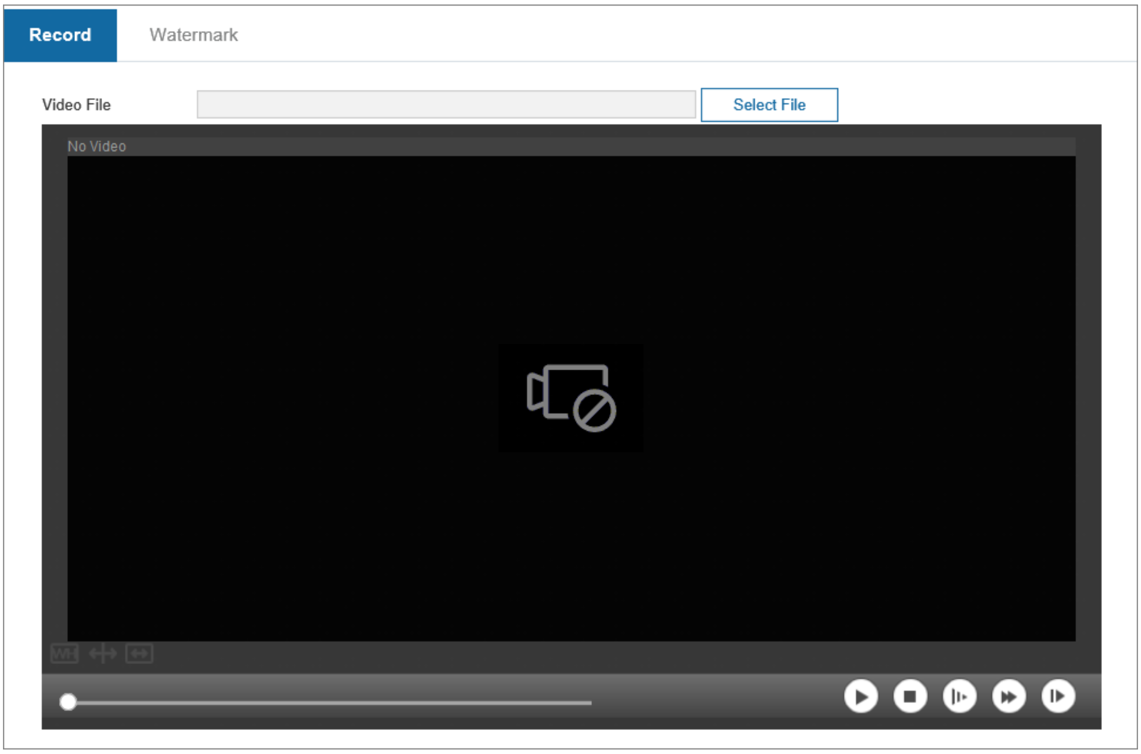


Table 3-6 Play parameters

Icon	Description
WH	Click it to display the video its original size or in an adaptive window.
↔	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed on the video image.
⇔	Click it or double-click the video image to enter full screen. Double-click or press Esc key to exit.
▶	Click it to play back the video. Click ■ to pause.
■	Click it to stop playing back the current video.
⏸▶	Click it to slow down the video to play at × (1/2), × (1/4) or × (1/8). Click ▶ to restore to normal playing speed.
⏩	Click it to speed up the video to play at × 2, × 4, or × 8. Click ▶ to restore to normal playing speed.
⏭	Click it to play back the next frame.

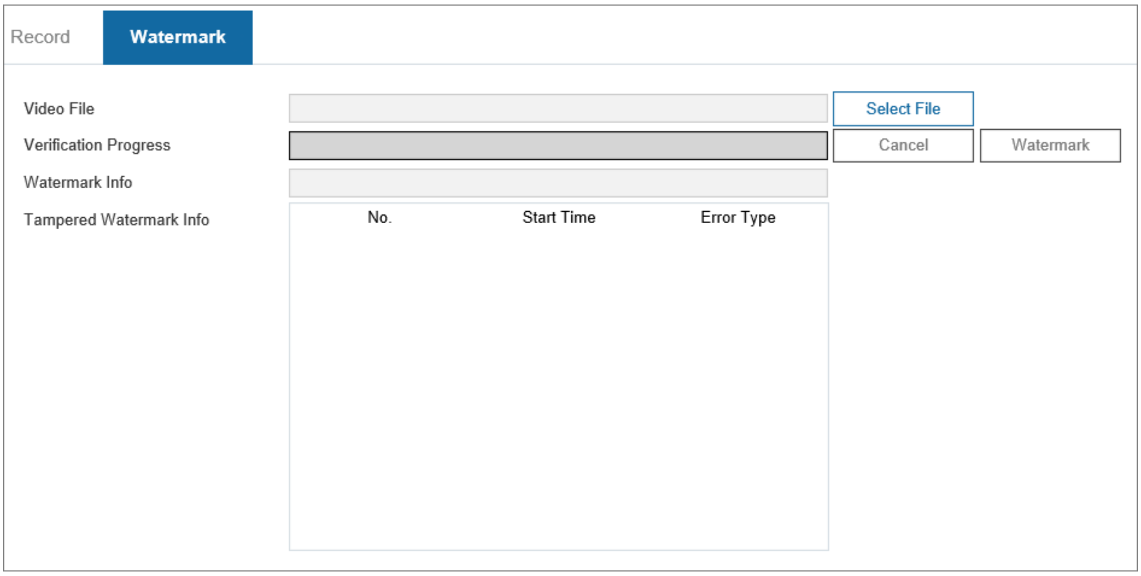
3.4.2.2 Watermark

Verify the watermark of selected video recordings to check whether the recording was tampered. Only .dav recording is supported.

Procedure

Step 1 Select **Search** > **Search Video** > **Watermark**.

Figure 3-10 Watermark



Step 2 Click **Select File** to select a recording.

Step 3 Click **Watermark**. The system will display the verification progress and normal watermark information.

- If the video is verified to be authentic, the watermark you set is displayed next to **Normal Watermark**.
- If the video is tampered, you can check the details next to **Tampered Watermark**.

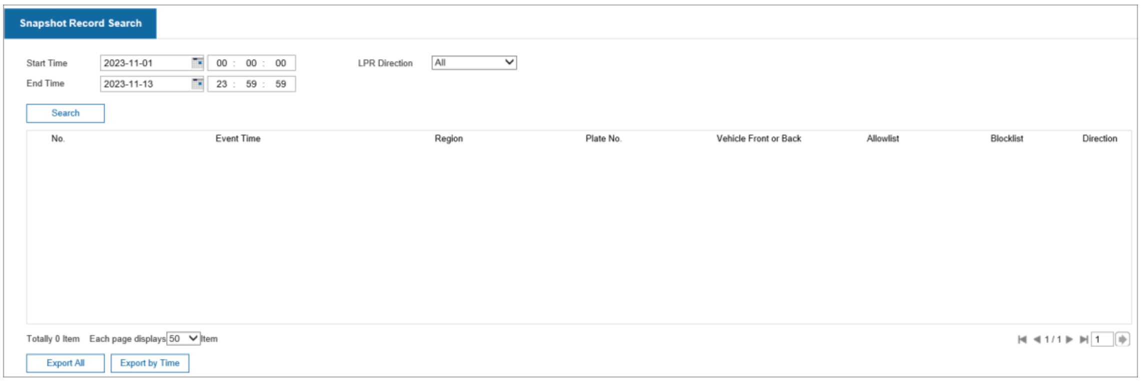
3.4.3 Snapshot Records Search

Search for and download the snapshot records.

Procedure

Step 1 Select **Search** > **Snapshot Record Search**.

Figure 3-11 Snapshot records



Start Time 2023-11-01 00 : 00 : 00

End Time 2023-11-13 23 : 59 : 59

LPR Direction All

Totally 0 Item Each page displays 50 Item

1 / 1

Step 2 Configure the parameters, and then click **Search**.

Table 3-7 Snapshot record parameters

Parameter	Description
Start Time	Set the start time and the end time to define a period, and then you can search for images stored on the memory card within this period.
End Time	

Parameter	Description
LPR Direction	The LPR direction refers to the direction in which the camera is configured to capture vehicles. You can select from **All**, **Positive**, **Departing** and **Unknown**.

Related Operations

Click **Export All** or **Export by Time** to export all records or the records that were searched for on your computer.

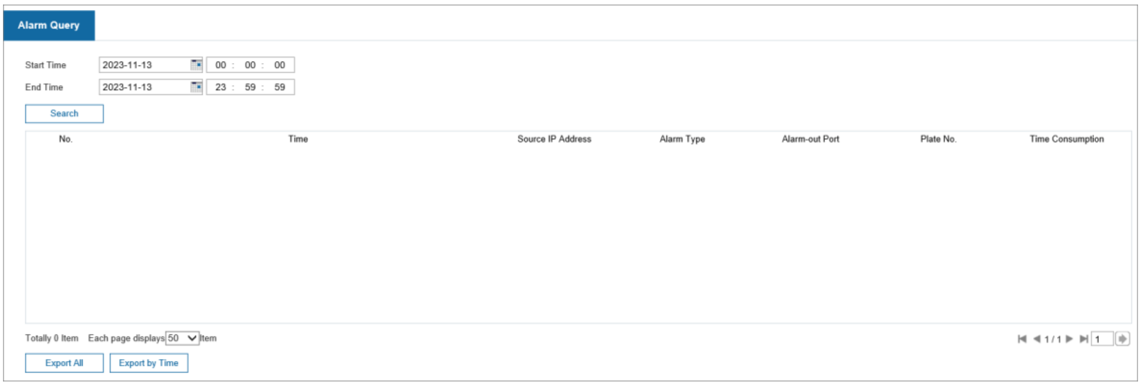
3.4.4 Alarm Query

Search for and export alarms.

Procedure

Step 1 Select **Search** > **Alarm Query**.

Figure 3-12 Alarm query



Start Time 2023-11-13 00 : 00 : 00

End Time 2023-11-13 23 : 59 : 59

No.	Time	Source IP Address	Alarm Type	Alarm-out Port	Plate No.	Time Consumption

Totally 0 Item Each page displays 50 Item

1 / 1

Step 2 Configure the parameters, and then click **Search**.

Set the start time and the end time to define a period, and then you can search for alarms within this period.

Related Operations

Click **Export All** or **Export by Time** to export all records or the records that were searched for on your computer.

3.5 Setting

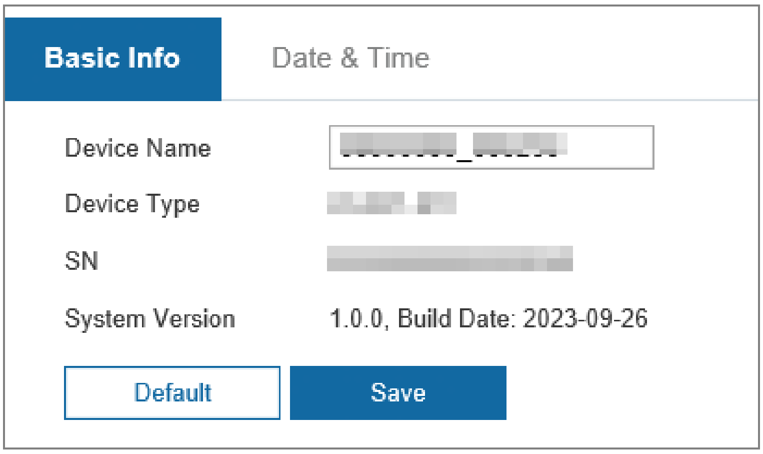
3.5.1 System

3.5.1.1 System Setting

3.5.1.1.1 Basic information

Select **Setting** > **System** > **System Setting** > **Basic Info** to configure the Camera name, view the system version and more.

Figure 3-13 Basic info



Device Name [redacted]

Device Type [redacted]

SN [redacted]

System Version 1.0.0, Build Date: 2023-09-26

3.5.1.1.2 Date & Time

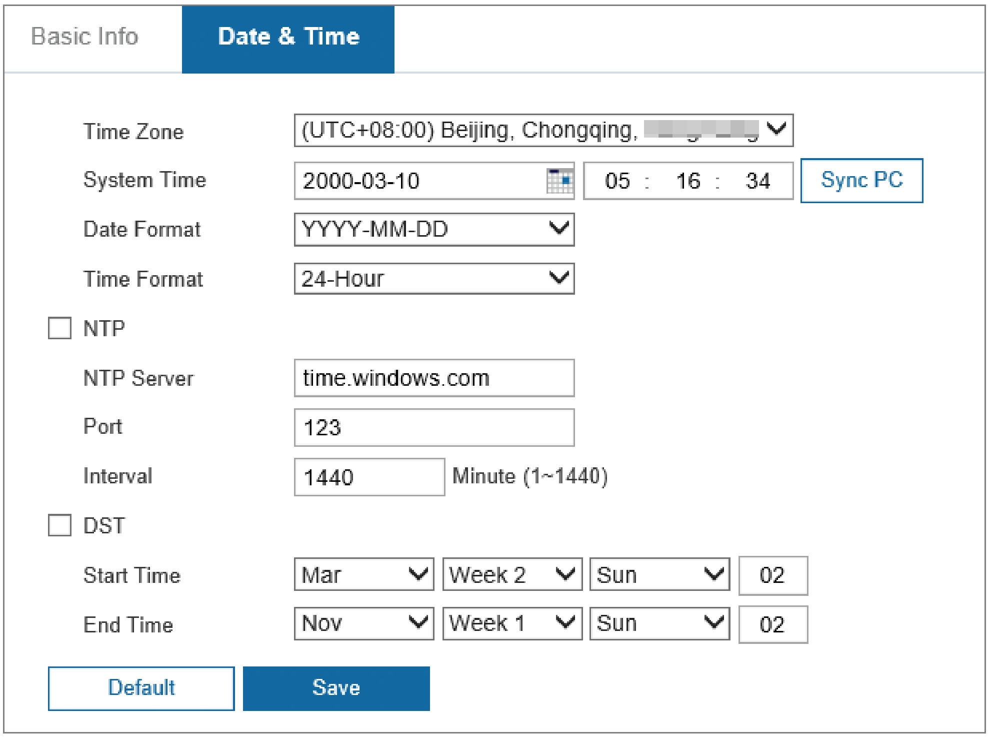
You can configure date, time, time zone, and more of the camera.

Procedure

Step 1 Select **Setting** > **System** > **System Settings** > **Date & Time**.

Step 2 Configure the parameters.

Figure 3-14 Date & time



Time Zone (UTC+08:00) Beijing, Chongqing, [redacted]

System Time 2000-03-10 05 : 16 : 34

Date Format YYYY-MM-DD

Time Format 24-Hour

□ NTP

NTP Server time.windows.com

Port 123

Interval 1440 Minute (1~1440)

□ DST

Start Time Mar Week 2 Sun 02

End Time Nov Week 1 Sun 02

Table 3-8 Date & time parameters

Parameter	Description
Time Zone	The time zone where the Camera locates.
System Time	The current time of the Camera. Click **Sync PC**, and the system time changes to the PC time.

Parameter	Description
Date Format	Select the date format. - DD - day number from 01-31. - MM - month number from 01-12. - YYYY - 4-digit year number.
Time Format	Configure the time format. You can select from **12-Hour** or **24-Hour**.
NTP	Synchronize its time with the server you configure. - **NTP Server/Port**: Enter the IP address and port number of the server that the device will synchronize time with. - **Interval**: Configure the frequency that the device will synchronize its time with the server.
DST	Enable DST as needed. Select the **DST** (Daylight Saving Time) checkbox, and then configure the **Start Time** and **End Time** of DST.

Step 3 Click **Save**.

3.5.1.2 Device Maintenance

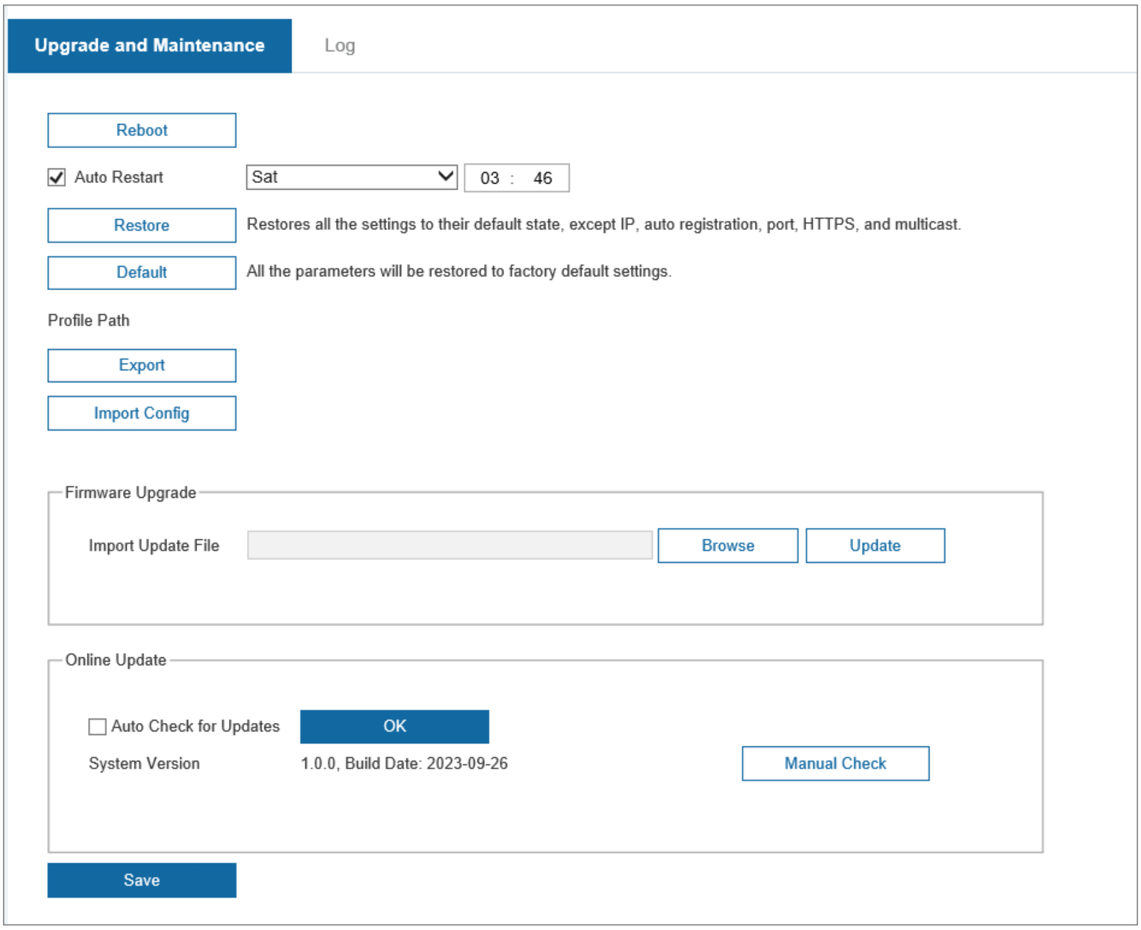
3.5.1.2.1 Upgrade and Maintenance

You can set the time of automatic reboot, restore the settings of the camera to default settings or factory settings, import or export configurations, and update the system to the latest version to make the camera run properly.

Procedure

Step 1 Select **Setting** > **System** > **Device Maintenance** > **Upgrade and Maintenance**.

Figure 3-15 Upgrade and maintenance



Upgrade and Maintenance | Log

Reboot

☑ Auto Restart   Sat   03 : 46

Restore   Restores all the settings to their default state, except IP, auto registration, port, HTTPS, and multicast.

Default   All the parameters will be restored to factory default settings.

Profile Path

Export

Import Config

Firmware Upgrade

Import Update File   Browse   Update

Online Update

□ Auto Check for Updates   OK

System Version   1.0.0, Build Date: 2023-09-26   Manual Check

Save

Step 2 Maintenance operations.

- **Reboot**: Click it to restart the camera immediately.
- **Auto Restart**: Select the checkbox to enable it, and then set the restart time.

  The system will automatically restart at the defined period and time.

Step 3 Default settings.

- **Restore**: Click it to restore all the settings to their default state, except for IP, auto registration, port, HTTPS, and multicast.
- **Default**: All the parameters will be restored to their default factory settings. Please be cautious. Also, the camera will restart and you will have to initialize it again.

Step 4 Import and export configurations.

The system supports exporting the configurations from the webpage to the local computer for backup, and importing the configuration files from local backup for quick configuration or restoration.

- **Export**: Export the configuration from the webpage to the local computer.
- **Import Config**: Import the configuration files to local backup.

  The imported and exported files should be in the format of .backup.

Step 5 Update the system through file upgrade or online upgrade.

- Firmware Upgrade
  - Click **Browse**, and then select the upgrade file in the pop-up dialog box.
  - Click **Upgrade** to start updating the system.
- Online Upgrade

- Select **Auto-check for updates**, and then click **OK**.

  The system starts to upgrade firmware.
- Click **Manual Check** to manually check the system version.

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

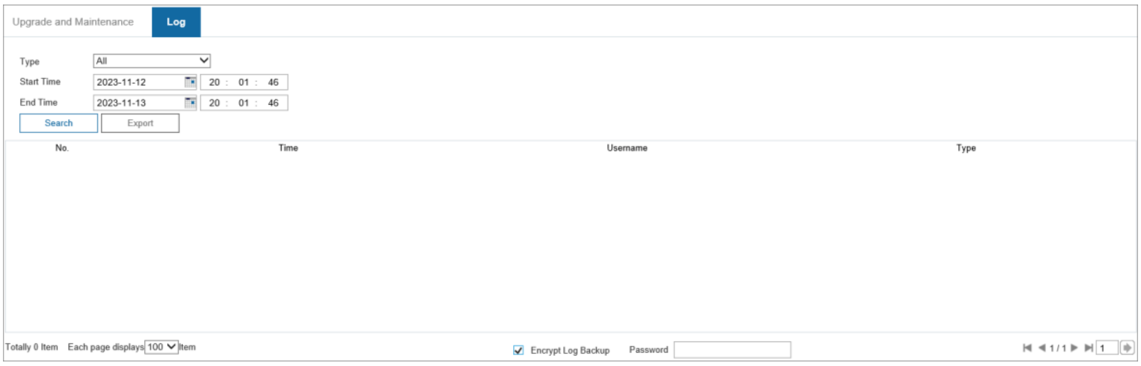
3.5.1.2.2 System Log

You can search for and view logs by time and type, and backup the logs.

Procedure

Step 1 Select **Setting** > **System** > **Device Maintenance** > **Log**.

Figure 3-16 System log



Type: All

Start Time: 2023-11-12 20 : 01 : 46

End Time: 2023-11-13 20 : 01 : 46

Totally 0 Item Each page displays 100 Item

☑ Encrypt Log Backup Password

1/1

Step 2 Set **Start Time** and **End Time**, and then select the log type.

Step 3 Click **Search**.

The matched log files will be displayed on the list.

Step 4 Click a log to view its details in the **Detailed Information** area.

Step 5 (Optional) Click **Backup** to back up the log to local computer in .txt format.

Select **Encrypt Log Backup** and set a password to protect the log file. The password must be used when accessing the log file.

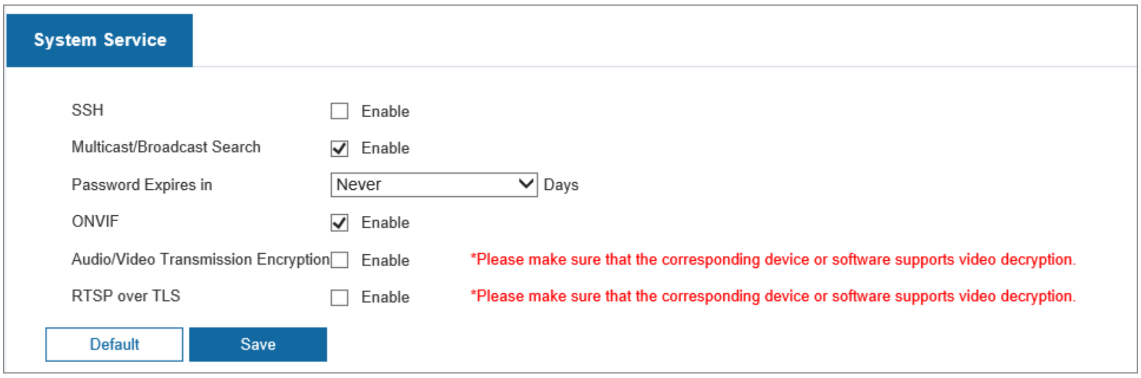
3.5.1.3 System Service

You can enable multiple system services to secure network safety.

Procedure

Step 1 Select **Setting** > **System** > **Security** > **System Service**.

Figure 3-17 System service



SSH ☐ Enable

Multicast/Broadcast Search ☑ Enable

Password Expires in Never Days

ONVIF ☑ Enable

Audio/Video Transmission Encryption ☐ Enable *Please make sure that the corresponding device or software supports video decryption.

RTSP over TLS ☐ Enable *Please make sure that the corresponding device or software supports video decryption.

Step 2 Enable the services as needed.

Table 3-9 Description of system service parameters

Parameter	Description
SSH	Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. It is a method for secure remote login, providing secure access for users. It's important to note that enabling it might have some security vulnerabilities.
Multicast/Broadcast Search	Multicast/Broadcast Search sends messages to all devices on the same network, enabling compatible software or devices to detect and list the camera as a network device. Enabling this feature can simplify the process of discovering and adding cameras to your network. But it should be done cautiously as it may pose security threats.
Password Expires in	Set the validity of the password.
ONVIF	The service is enabled by default. It allows network video products produced by different manufacturers to communicate with each other.
Audio/Video Transmission Encryption	Enable this function to encrypt stream transmitted through private protocol. 📖 ● Make sure that the matched device or software supports video decryption function; otherwise, do not enable it. ● We recommend enabling the encryption service to avoid data breach.
RTSP over TLS	Enable this function to encrypt stream transmitted through standard protocol. 📖 ● Make sure that the matched device or software supports video decryption function; otherwise, do not enable it. ● We recommend enabling it to avoid data breach.

Step 3 Click **Save**.

3.5.1.4 Account Management

You can add or delete users and user groups, assign permissions to new users and user groups, change password, and manage users and user groups.

3.5.1.4.1 Managing Users

You can view user information, add or delete user(s), change user password, assign user permissions, and more.

Procedure

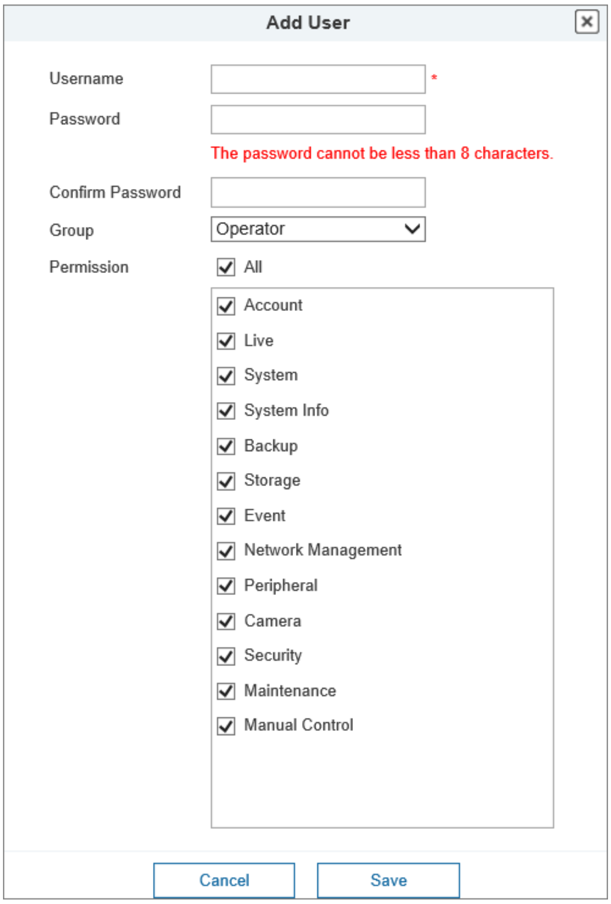
Step 1 Select **Setting** > **System** > **Account** > **Account** > **Username**.

Step 2 Click **Add User**.

1) Configure the general information.

- After the Camera is initialized, the admin user generated by default has the highest permission. The admin user cannot be deleted, and its permissions cannot be changed.
- Users with **Account** permission can change its own password, and change the password of other users.
- Users who have logged in cannot be deleted.
- We recommend you give fewer permissions to normal users than premium users to make user management convenient.

Figure 3-18 Add user



Add User

Username *

Password

The password cannot be less than 8 characters.

Confirm Password

Group: Operator

Permission: ☑ All

☑ Account
☑ Live
☑ System
☑ System Info
☑ Backup
☑ Storage
☑ Event
☑ Network Management
☑ Peripheral
☑ Camera
☑ Security
☑ Maintenance
☑ Manual Control

Table 3-10 Description of user parameters

Parameter	Description
Username	User’s unique identification. You cannot use existed username. It can contain a maximum of 31 characters, including only upper case, lower case, number, "_", "@", and ".".
Password	Enter password and confirm it again.
Confirm Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Follow the password security prompt to set a high security level password.
Group	The group that users belong to. Each group has different authorities.

Parameter	Description
Permission	The permissions that you want to grant to the user.

Step 3 Click **Save**.

Related Operations

- Click ⛔ to delete the corresponding user. Admin user cannot be deleted.
- Click ✏ to edit the information of the corresponding user. Click **Save** to save the settings.

3.5.1.4.2 Managing User Groups

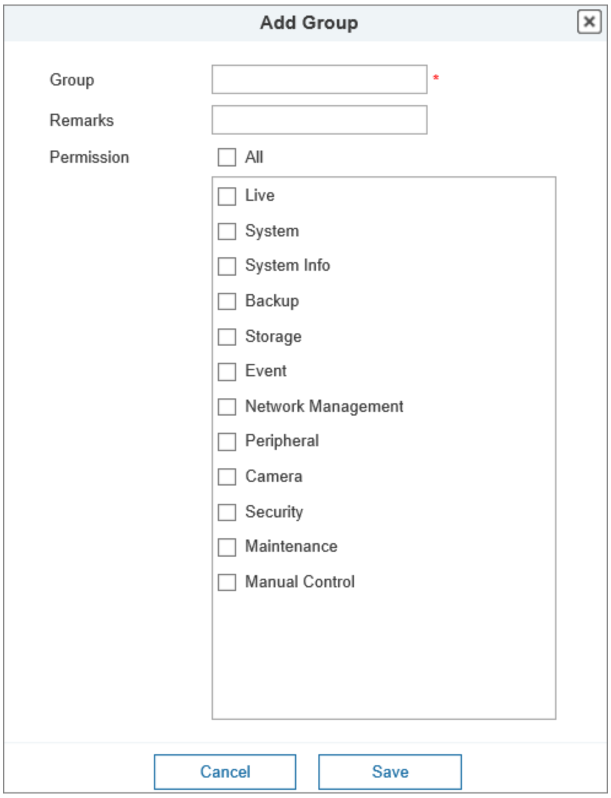
A group is a set of permissions. You can configure different groups to quickly assign permissions to different users.

Procedure

Step 1 Select **Setting** > **System** > **Account** > **Account** > **Edit Permission**.

Step 2 Click **Add Group**.

Figure 3-19 Add user group



Add Group

Group *

Remarks

Permission □ All

□ Live
□ System
□ System Info
□ Backup
□ Storage
□ Event
□ Network Management
□ Peripheral
□ Camera
□ Security
□ Maintenance
□ Manual Control

Step 3 Enter the group name and remarks, and then select permissions.

Step 4 Click **Save**.

Related Operations

- Click ✏ to edit the remarks and permissions.
- Click ⛔ to delete a group.

3.5.1.4.3 Viewing Online User

Select **Setting** > **System** > **Account** > **Online User** to view the login information of users, including name, group, IP address, login time and login type. This allows you to monitor any unauthorized access attempts or suspicious activity. Pay attention to unsuccessful login attempts, multiple login sessions, or login records from unfamiliar IP addresses.

3.5.1.4.4 Resetting Password

Enable the function, and you can reset password when you forget it by clicking **Forget password?** on the login page.

Procedure

Step 1 Select **Setting** > **System** > **Account** > **Password Reset**.

Step 2 Select the checkbox next to **Open**.

If the function is not enabled, you can only reset the password by resetting the camera.

Step 3 (Optional) You can change the email address.

Step 4 Click **Save**.

You can now reset the password of users on the login page by clicking **Forgot password?**.

3.5.2 Network Settings

You can set the network parameters of the Camera.

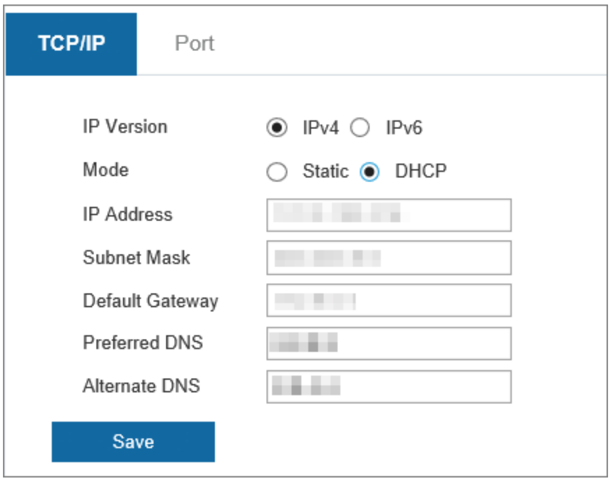
3.5.2.1 Configuring TCP/IP

Set the IP address, DNS server and other parameters of the Camera to make sure that the Camera can connect to other devices on the network.

Procedure

Step 1 Select **Setting** > **Network** > **TCP/IP**.

Figure 3-20 TCP/IP



IP Version	● IPv4 ○ IPv6
Mode	○ Static ● DHCP
IP Address	[redacted]
Subnet Mask	[redacted]
Default Gateway	[redacted]
Preferred DNS	[redacted]
Alternate DNS	[redacted]

Step 2 Configure the parameters.

Table 3-11 TCP/IP parameters

Parameter	Description
IP Version	IPv4 and IPv6 are supported.
Mode	Select a network mode. ● **Static**: Manually assign a fixed IP address, subnet mask and gateway. It provides consistent and predictable access. This option is useful if you have specific requirements for port forwarding or network settings. ● **DHCP**: Automatically obtains the IP address, subnet mask and gateway from a DHCP server. This simplifies network setup and eliminates the need for manual configuration. It allows the camera to adapt to changes in the network, such as IP conflicts or changes in the DHCP server. 📖 If your DHCP server can update a DNS server, you can access the camera by host name.
IP Address	Enter IP address.
Subnet Mask	Specify the mask for the subnet that the camera is located on. The subnet prefix is a number in the range from 1 to 255. The subnet prefix identifies a specific network link and usually contains a hierarchical structure.
Default Gateway	Set a default gateway on the same network segment as the IP address as needed.
Preferred DNS	IP address of DNS.
Alternate DNS	IP address of the alternate DNS.

Step 3 Click **Save**.

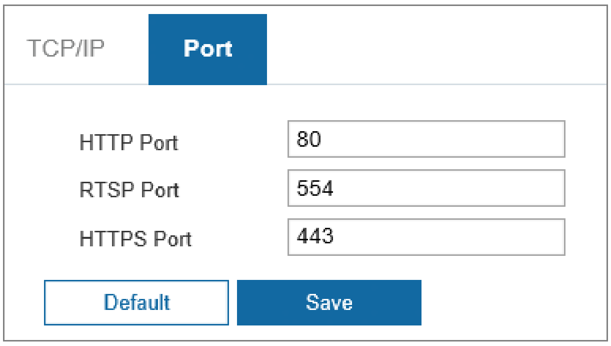
3.5.2.2 Configuring Port

Configuring the port settings allows the camera to establish network connections and transfer data between the camera and other devices on the network.

Procedure

Step 1 Select **Setting** > **Network Settings** > **TCP/IP** > **Port**.

Figure 3-21 Port



HTTP Port 80

RTSP Port 554

HTTPS Port 443

Step 2 Configure port parameters.

📖

- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- Do not use the same value of any other port during port configuration.

Table 3-12 Description of port parameters

Parameter	Description
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	● Real time streaming protocol port, and the value is 554 by default. If you play live view with Apple Safari, QuickTime, VLC or Blackberry smart phone, the following URL format is available. ● When the URL format requires RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. ● When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Among that: ● Username: The username, such as admin. ● Password: The password, such as admin. ● IP: The device IP, such as 192.168.1.112. ● Port: Leave it if the value is 554 by default. ● Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. ● Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@192.168.1.112:554/cam/realmonitor?channel=2&subtype=1 If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Save**.

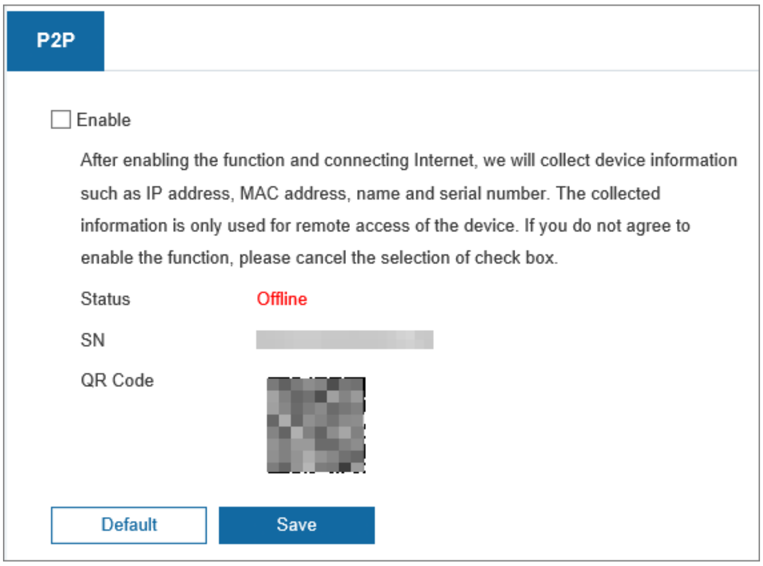
3.5.2.3 Configuring P2P

P2P allows remote access to the camera without complex configurations, such as port forwarding.

Procedure

Step 1 Select **Setting** > **Network Settings** > **P2P**.

Figure 3-22 P2P



□ Enable

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

Status Offline

SN [redacted]

QR Code [redacted]

After enabling P2P, the camera will collect and process user information. Please be advised.

Step 2 Select the checkbox to enable the function.

Scan the QR code to check the serial number of the device.

Step 3 Click **Save**.

3.5.2.4 Configuring DDNS

Properly configure DDNS, and then the domain name on the DNS server matches your IP address and the matching relation refreshes in real time. You can always visit the camera with the same domain name no matter how the IP address changes.

Prerequisites

Check the type of DNS server supported by the camera.

Procedure

Step 1 Select **Setting** > **Network Settings** > **DDNS**.

- Third party server might collect your device information after DDNS is enabled.
- Register and log in to the DDNS website, and then you can view the information of all the connected devices in your account.

Step 2 Select the checkbox to enable the function.

Step 3 Configure the parameters.

Table 3-13 Parameter description

Parameter	**Description**
Type	The name and web address of the DDNS service provider.
Address	
Domain	The domain name you registered on the DDNS website.

Parameter	Description
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the website of the DDS server provider.
Password	

Step 4 Click **Save**.

Result

Go to the domain name in the browser, and then the login page is displayed.

3.5.2.5 Configuring Email

Configure the email. When alarms or abnormal events occur, an email will be sent to the recipient server through SMTP server. The recipient can log in to the incoming mail server to receive emails.

⚠

After you enable this function, the system will send device data to the given server. There is data leakage risk.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Email**.

Step 2 Select the checkbox next to **Enable** to enable the function.

Step 3 Configure the parameters.

Table 3-14 Parameter description

Parameter	Description
Sender	The email address of the sender.
SMTP Server	The IP address of the outgoing mail server that complies with SMTP protocol.
Port	The port number of the outgoing mail server that complies with SMTP protocol. It is 25 by default.
Attachment	Select the checkbox to support attachment in the email.
Username	The username of sender mailbox.
Password	The password of sender mailbox.
Encryption Type	Select encryption type from **None**, **SSL**, and **TLS(Recommended)**.
Mail Receiver	The email address of the receiver. Supports 3 addresses at most.
Test	Test whether the email function is normal. If the configuration is correct, the email address of the receiver will receive the test email. Save the email configuration before running a test.

Step 4 Click **Save**.

3.5.2.6 Advanced

3.5.2.6.1 PPPoE

Point-to-Point Protocol over Ethernet is one of the protocols that device uses to connect to the internet. Get the PPPoE username and password from the internet service provider, and then set up network connection through PPPoE, the camera will acquire a WAN dynamic IP address.

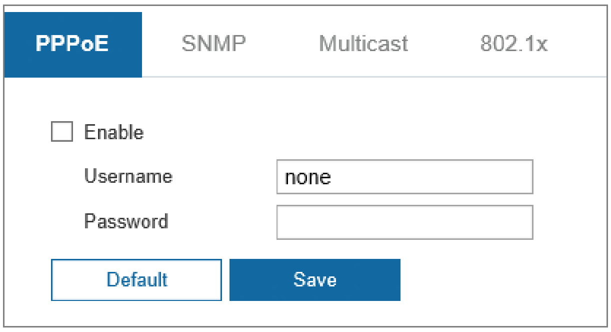
Prerequisites

- The camera has connected to the network.
- You have gotten the account and password from an internet service provider.
- Disable UPnP while using PPPoE to avoid possible influence.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **PPPoE**.

Figure 3-23 PPPoE



PPPoE | SNMP | Multicast | 802.1x

□ Enable

Username: none

Password:

Default | Save

Step 2 Select the checkbox to enable it, and then enter username and password.

After making PPPoE connection, the device IP address cannot be modified through webpage.

Step 3 Click **Save**.

3.5.2.6.2 SNMP

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

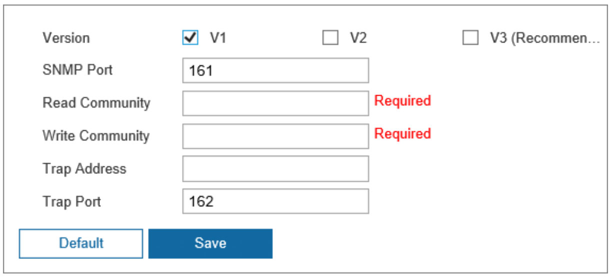
Prerequisites

- Install the toll software for monitoring and managing SNMP (Simple Network Management Protocol) device.
- Get the corresponding version of MIB file from technical support.
- Set SNMP and connect to the Camera through tool such as MIB Builder and MG-SOFT MIB Browser.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **SNMP**.

Figure 3-24 SNMP (1)



Version: ☑ V1 □ V2 □ V3 (Recommen...

SNMP Port: 161

Read Community: Required

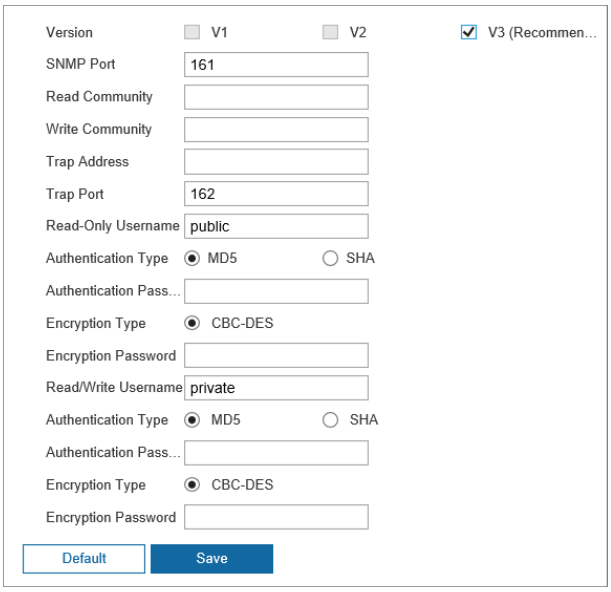
Write Community: Required

Trap Address:

Trap Port: 162

Default | Save

Figure 3-25 SNMP (2)



Version □ V1 □ V2 ☑ V3 (Recommen...

SNMP Port: 161

Read Community:

Write Community:

Trap Address:

Trap Port: 162

Read-Only Username: public

Authentication Type: ● MD5 ○ SHA

Authentication Pass...:

Encryption Type: ● CBC-DES

Encryption Password:

Read/Write Username: private

Authentication Type: ● MD5 ○ SHA

Authentication Pass...:

Encryption Type: ● CBC-DES

Encryption Password:

Step 2 Select an SNMP version to enable this function.

- Select **V1**, and the system can only process information of version V1.
- Select **V2**, and the system can only process information of version V2.
- Select **V3**, and then **V1** and **V2** become unavailable. You can configure username, password and authentication type. It requires corresponding username, password and authentication type to visit your device from the server.

⚠

Using **V1** and **V2** might cause data leakage, and **V3** is recommended.

Step 3 In **Trap Address**, enter the IP address of the PC that has MIB Builder and MG-SOFT MIB Browser installed, and leave other parameters as default.

Table 3-15 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports. 📖 You can enter number, letter, underline and dash to form the name.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.

Parameter	Description
Read-only Username	Set the read-only username accessing device, and it is **public** by default. You can enter number, letter, and underline to form the name.
Authentication Type	You can select from **MD5** and **SHA**. The default type is **MD5**.
Authentication Password	It should be no less than 8 characters.
Encryption Type	The default is CBC-DES.
Encryption Password	It should be no less than 8 characters.

Step 4 Click **Save**.

Result

View device configuration through MIB Builder or MG-SOFT MIB Browser.

1. Run MIB Builder and MG-SOFT MIB Browser.
2. Compile the two MIB files with MIB Builder.
3. Load the generated modules with MG-SOFT MIB Browser.
4. Enter the IP address of the device you need to manage in the MG-SOFT MIB Browser, and then select version to search.
5. Unfold all the tree lists displayed in the MG-SOFT MIB Browser, and then you can view the configuration information, video channel amount, audio channel amount, and software version.

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

3.5.2.6.3 Multicast

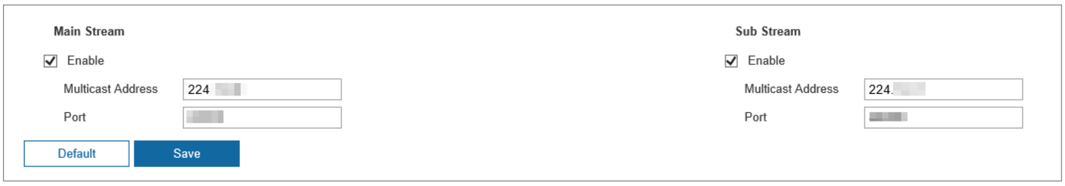
When multiple users are viewing the device video image simultaneously through network, it might fail due to limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.1.0–238.255.255.255) for the camera and adopt the multicast protocol.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **Multicast**.

Step 2 Select the checkbox to enable the function, and then configure the parameters.

Figure 3-26 Multicast



Main Stream

☑ Enable

Multicast Address: 224

Port:

Sub Stream

☑ Enable

Multicast Address: 224.

Port:

Step 3 Click **Save**.

3.5.2.6.4 802.1x

802.1X is a port-based access control and authentication protocol designed to enhance network security. It helps prevent unauthorized access attempts and potential data breaches. When the network switch is configured with 802.1x, the Camera also needs to be set to 802.1x, otherwise users cannot access the Camera through the network.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **802.1x**.

Step 2 Select the checkbox to enable 802.1x, and then configure the parameters.

Table 3-16 802.1x parameters

Module	Parameter	Description
Common Parameter	Authentication Mode	- **PEAP**: Ordinarily uses TLS only to authenticate the server to the client, and only the sever is required to have a public key certificate. - **EAP-TLS**: Provides mutual authentication of client to server, and server to client. Both the client, and the server must be assigned a digital certificate signed by a CA (Certificate Authority) that they both trust.
	CA Certificate	Click **Browse** to import a CA certificate and then select the **CA Certificate** to verify whether the certificate is valid.
PEAP	Username	For PEAP method, user authentication is performed by 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	

Step 3 Click **Save**.

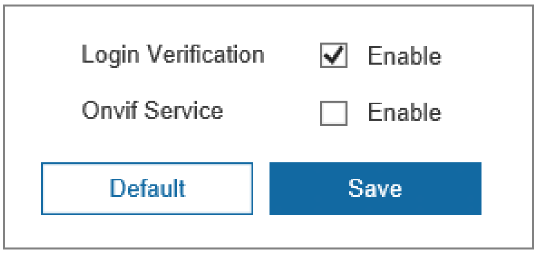
3.5.2.6.5 ONVIF

ONVIF, short for Open Network Video Interface Forum, is a standard protocol that allows for interoperability between devices from different manufacturers, including video recording device and other recording devices. This enables integration of devices without concerns about compatibility issues.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **ONVIF**.

Figure 3-27 ONVIF



Login Verification ☑ Enable

Onvif Service □ Enable

Step 2 Select the checkbox as needed.

By enabling login verification, login username and password are required when logging in through ONVIF.

Step 3 Click **Save**.

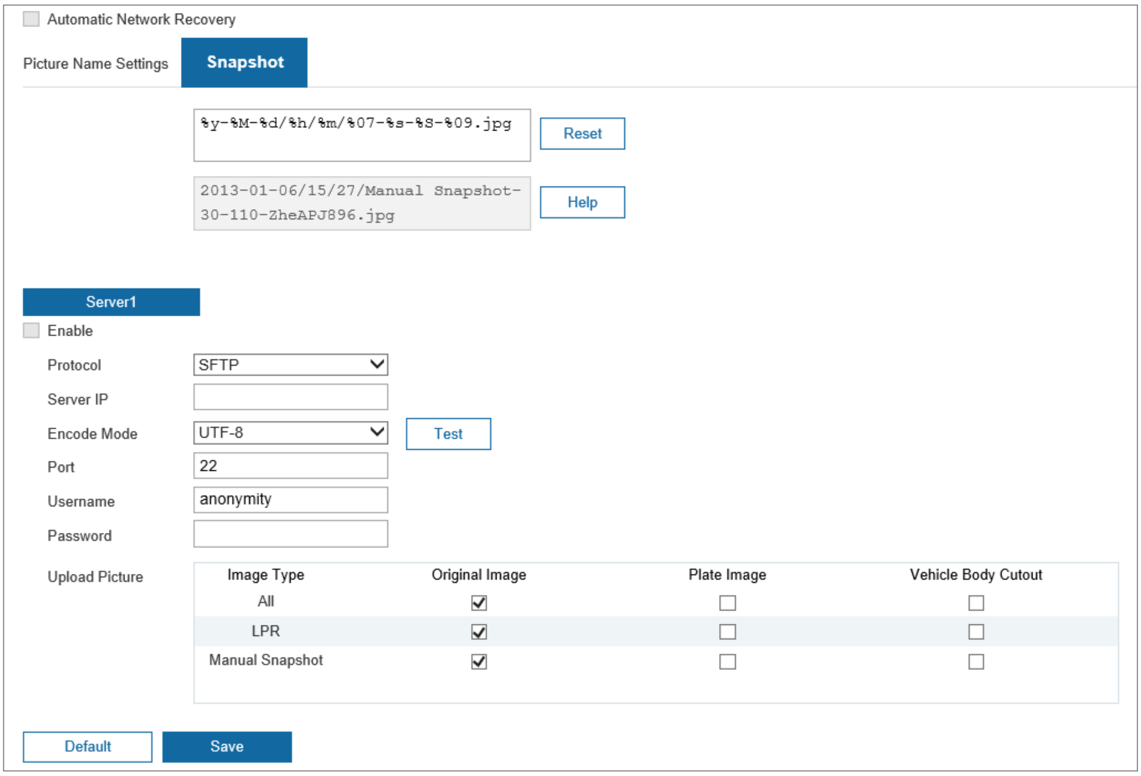
3.5.2.6.6 FTP

FTP function can be enabled only when it is selected as destination. When the network does not work, you can save all the files to the internal memory card for emergency.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **FTP**.

Figure 3-28 FTP



□ Automatic Network Recovery

Picture Name Settings: Snapshot

%y-%M-%d/%h/%m/%07-%s-%S-%09.jpg

2013-01-06/15/27/Manual Snapshot-30-110-ZheAPJ896.jpg

Server1

□ Enable

Protocol: SFTP

Server IP:

Encode Mode: UTF-8

Port: 22

Username: anonymity

Password:

Upload Picture

Image Type	Original Image	Plate Image	Vehicle Body Cutout
All	☑	□	□
LPR	☑	□	□
Manual Snapshot	☑	□	□

Step 2 Configure the parameters.

Table 3-17 Parameter description

Parameter	Description
Automatic Network Recovery	When the network disconnects or fails, snapshots will be stored in memory card. After the network is restored, the snapshots will be uploaded from the memory card to FTP or client. Make sure that memory card is properly inserted in the camera; otherwise, the offline transfer function cannot be enabled.
Picture Name Settings	Set the naming rule of snapshots to be saved in FTP server. You can click **Help** to view the naming rule, or click **Reset** to restore the default naming rule.
Enable	Enable FTP server storage.
Protocol	● **SFTP**: Secure File Transfer Protocol, a network protocol allows file access, and transfer over a secure data stream. ● **FTP**: File Transfer Protocol, a network protocol implemented to exchange files over a TCP/IP network. Anonymous user access is also available through an FTP server.
Server IP	The IP address of FTP server.

Parameter	Description
Encode Mode	Refers to the encode mode of Chinese characters when naming pictures. Two modes are available: **UTF-8**, and **GB2312**. After configuring **Server IP**, and **Port**, click **Test** to check whether the FTP server works.
Port	The port number of FTP server.
Username	The username and password of FTP server.
Password	
Upload Picture	Select the types of pictures to be uploaded to the FTP server.

Step 3 Click **Save**.

3.5.2.6.7 HTTPS

You can log in through HTTPS by creating certificate or uploading authenticated certificate. It can ensure communication data security, and device safety through reliable and stable technical approach.

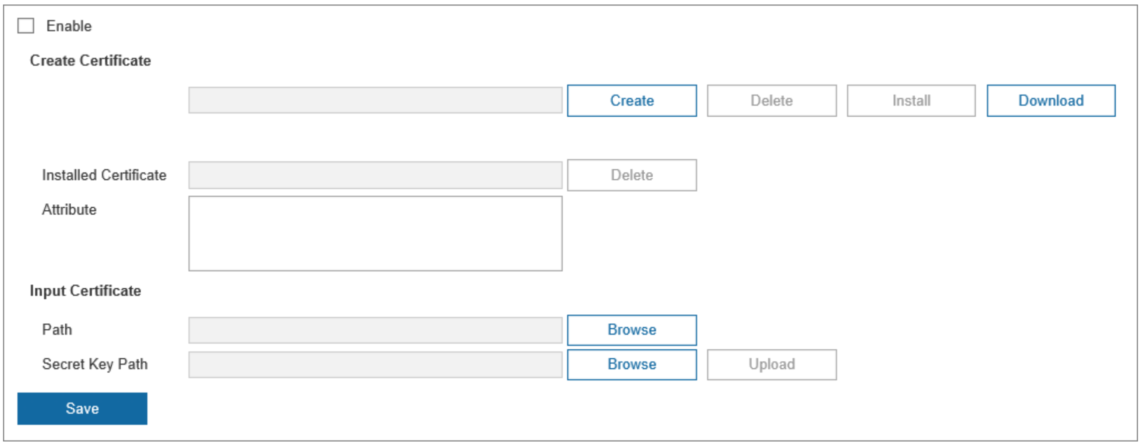
Prerequisites

- For first-time use of HTTPS or after changing device IP address, you need to create server certificate, and install root certificate.
- After creating server certificate, and installing root certificate, if you change a computer to log in to the web client, then you need to download and install the root certificate again on the new computer or copy the downloaded root certificate on the new computer, and install it.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **HTTPS**.

Figure 3-29 HTTPS

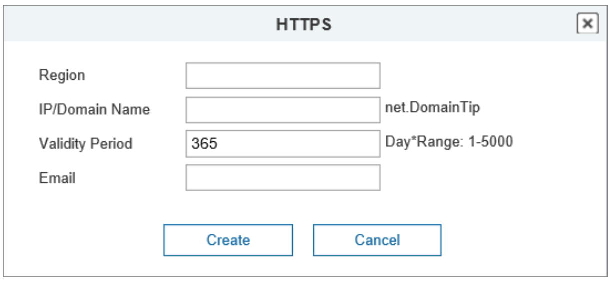


Step 2 Create certificate or upload the authenticated certificate.

- Create a certificate.

  1. Click **Create**.

Figure 3-30 Create certificate



HTTPS

Region

IP/Domain Name net.DomainTip

Validity Period 365 Day*Range: 1-5000

Email

2. Enter the required information such as region, IP or domain name, validity period and email, and then click **Create**.

The entered **IP or Domain name** must be the same as the IP or domain name of the Camera.

3. Click **Install**, and then click **Download** to download root certificate.

   Select the storage path, and then click **Save**.

4. Double-click the RootCert.cer icon and install the certificate.

- Install a signed certificate.
  1. Click **Browse** to upload the signed certificate, and certificate key, and then click **Upload**.
  2. Double-click the RootCert.cer icon and install the certificate.

Step 3 Select the checkbox to enable HTTPS, and click **Save**.

The configuration takes effect until the Camera restarts.

Step 4 Use HTTPS to log in to the Camera.

1. Enter https://*xx.xx.xx.xx* in the browser.

xx.xx.xx.xx is the Camera IP address or domain name.

2. Enter the username, and password to log in to the Camera.

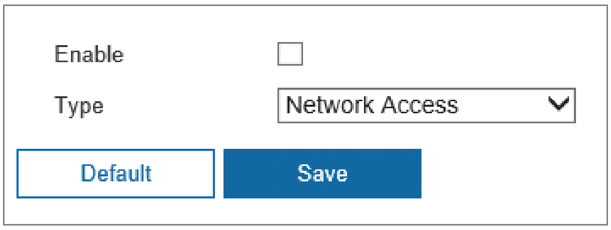
3.5.2.6.8 Firewall

The firewall plays a crucial role in enhancing the security of your network by preventing various types of unauthorized access and potential attacks.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **Firewall**.

Figure 3-31 Firewall



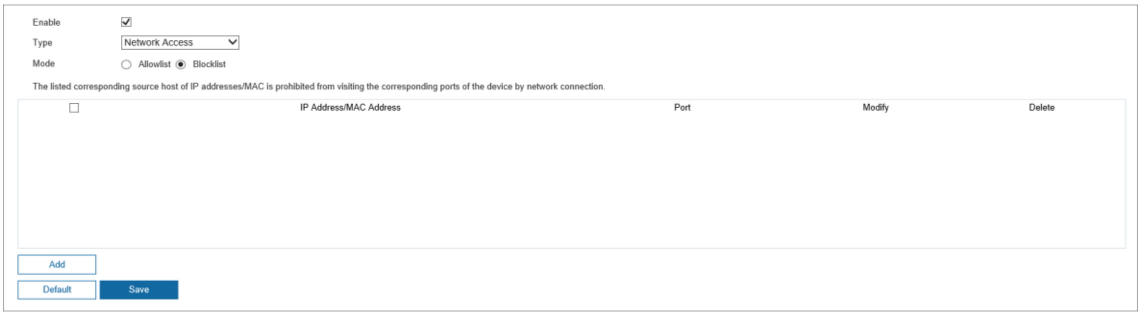
Enable □

Type Network Access

Step 2 Select **Type**.

- **Network Access**: Add the IP address to allowlist or blocklist to allow or restrict it to access corresponding ports of the Camera.

Figure 3-32 Network access



Enable ☑

Type: Network Access

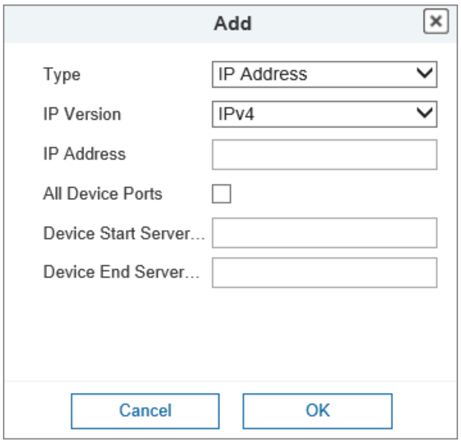
Mode: ○ Allowlist ● Blocklist

The listed corresponding source host of IP addresses/MAC is prohibited from visiting the corresponding ports of the device by network connection.

□	IP Address/MAC Address	Port	Modify	Delete

1. Select the mode: **Allowlist** and **Blocklist**.
   - ◇ **Allowlist**: Only when the IP/MAC of your PC in the allowlist, can you access the camera. Ports are the same.
   - ◇ **Blocklist**: When the IP/MAC of your PC is in the blocklist, you cannot access the camera. Ports are the same.
2. Click **Add IP/MAC** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 3-33 Add IP/MAC



Add

Type: IP Address

IP Version: IPv4

IP Address:

All Device Ports □

Device Start Server...:

Device End Server...:

- **PING Prohibited**: Your camera's IP address has been configured to prohibit ping requests. This helps prevent unauthorized access attempts.
- **Anti Half Connection**: Prevents half-open SYN attacks. When selected, your camera's software actively monitors the incoming SYN packets and ensures that only valid and complete connection requests are established.

Step 3 Click **Save**.

Related Operations

- Modify: Click ✎ to edit the information.
- Delete: Click ⊖ to delete the information.

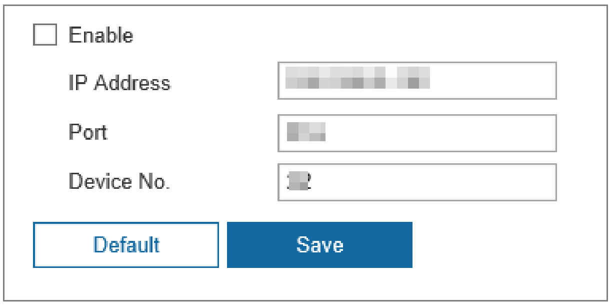
3.5.2.6.9 Remote Log

Critical logs can be saved to log server. This helps provide important clues to the source of security incidents. Log server needs to be deployed in advance by technical supports or system administrator.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **Remote Log**.

Figure 3-34 Remote log



Step 2 Select the checkbox to enable the function.

Step 3 Configure the IP address, port and device number.

Step 4 Click **Save**.

3.5.2.6.10 ITSAPI

You can configure this function to push the captured information to the server.

- All communications must be based on the HTTP protocol, conform to RFC2616 standards, and support Digest authentication.

  IO multiplexing must be available on the server.

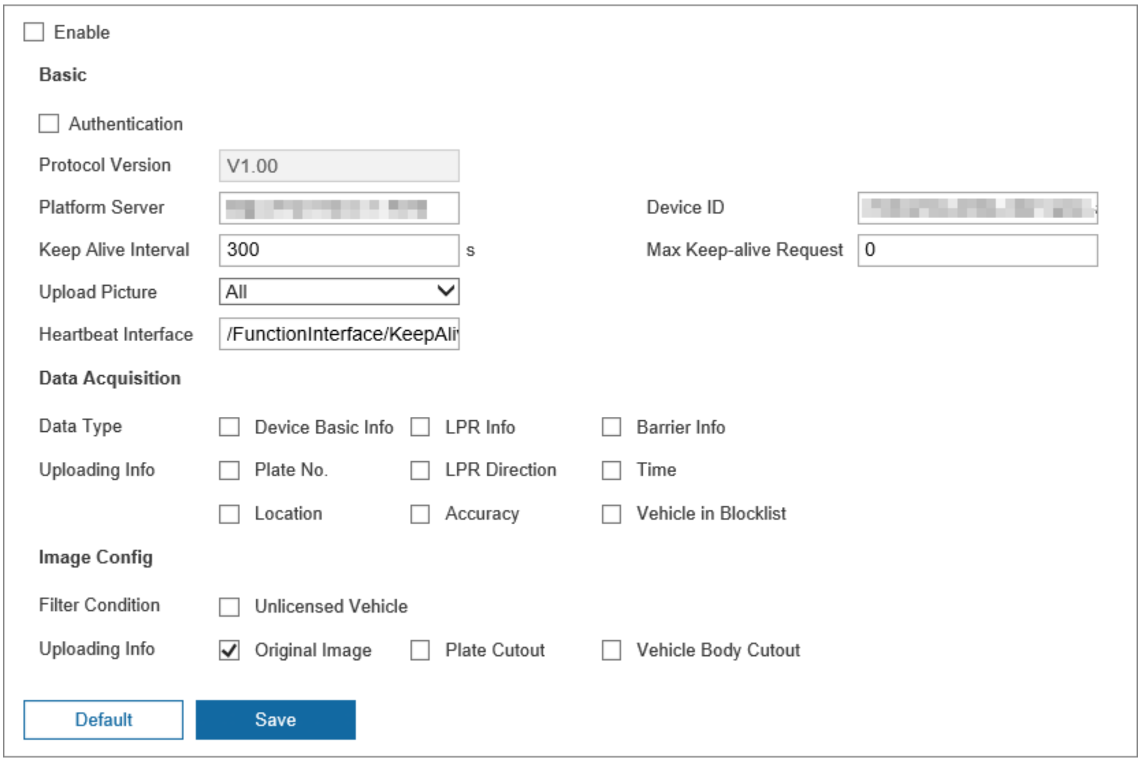
- Related business data must be in JSON format with ContentType: application/json;charset=UTF-8 as HTTP headers, which means the encoding method is UTF-8.

Procedure

Step 1 Select **Setting** > **Network Settings** > **Advanced** > **ITSAPI**.

Step 2 Select the checkbox next to **Enable** to enable the function.

Figure 3-35 ITSAPI



□ Enable

Basic

□ Authentication

Protocol Version: V1.00

Platform Server:

Device ID:

Keep Alive Interval: 300 s

Max Keep-alive Request: 0

Upload Picture: All

Heartbeat Interface: /FunctionInterface/KeepAli

Data Acquisition

Data Type: □ Device Basic Info □ LPR Info □ Barrier Info

Uploading Info: □ Plate No. □ LPR Direction □ Time □ Location □ Accuracy □ Vehicle in Blocklist

Image Config

Filter Condition: □ Unlicensed Vehicle

Uploading Info: ☑ Original Image □ Plate Cutout □ Vehicle Body Cutout

Step 3 Configure the parameters.

Table 3-18 Parameter description

Section	Parameter	Description
Basic Configuration	Authentication	When enabled, enter the username and password.
	Keep Alive Interval	Update interval of the connection between the server and the device.
	Max Keep-alive Request	Set the maximum number of heartbeats of the connection between the server and the device. When the defined number is exceeded, the device has disconnected.
	Upload Picture	Select the types to be uploaded.
Data Acquisition	Data Type	Select the data type to be uploaded.
	Uploading Info	Select the specific information to be uploaded.
Image Configuration	Filter Condition	Select whether to upload information of unlicensed vehicles.
	Uploading Info	Select the type of images to be uploaded.

Step 4 Click **Save**.

3.5.3 Video/Audio

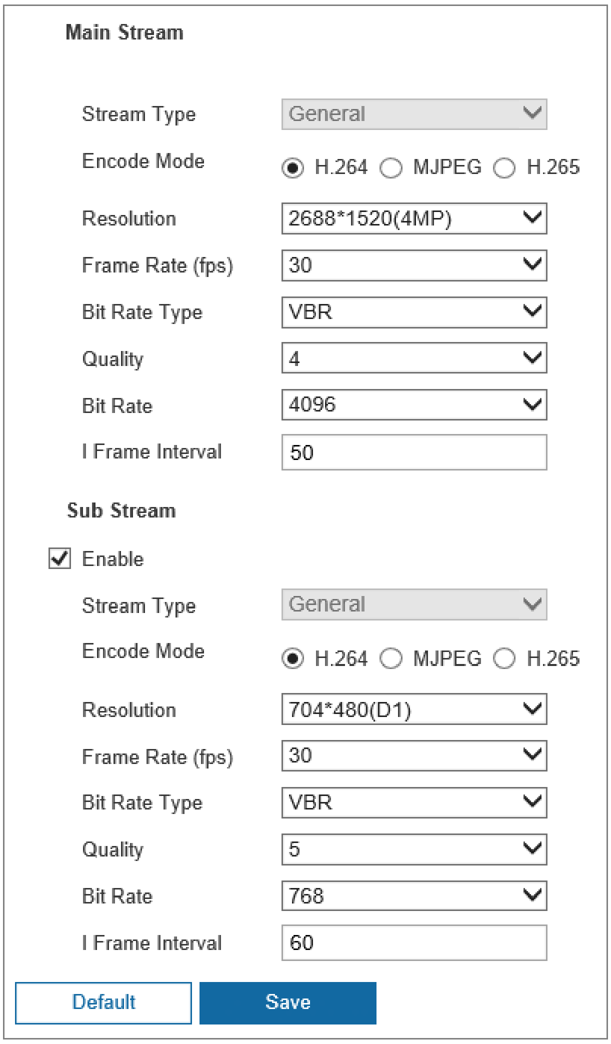
3.5.3.1 Configuring Video Stream

Configure the parameters of video stream.

Procedure

Step 1 Select **Setting** > **Video/Audio** > **Video** > **Video Stream**.

Figure 3-36 Video stream



Main Stream

Stream Type: General

Encode Mode: ● H.264 ○ MJPEG ○ H.265

Resolution: 2688*1520(4MP)

Frame Rate (fps): 30

Bit Rate Type: VBR

Quality: 4

Bit Rate: 4096

I Frame Interval: 50

Sub Stream

☑ Enable

Stream Type: General

Encode Mode: ● H.264 ○ MJPEG ○ H.265

Resolution: 704*480(D1)

Frame Rate (fps): 30

Bit Rate Type: VBR

Quality: 5

Bit Rate: 768

I Frame Interval: 60

Step 2 Configure the parameters.

Table 3-19 Video stream parameter

Parameter	**Description**
Encode Mode	Modes of H.264, MJPEG, and H.265 can be selected.
Resolution	The higher the value, the clearer the overall image. For each resolution, the recommended bit stream value is different. 📖 The resolution of sub stream cannot be greater than that of main stream.
Frame Rate (fps)	The higher the value, the smoother the video image. The frame rate might vary due to different resolutions.

Parameter	Description
Bit Rate Type	You can select from **VBR** (variable bitrate) and **CBR** (constant bitrate). ● **VBR**: The bit rate varies based on the complexity of the content being recorded. If the recording contains a lot of dynamic and complex scenes, using VBR might offer better compression and efficiency while maintaining the desired quality. ● **CBR**: Maintains a specific bitrate during encoding. It is advantageous to use CBR when the network has limited bandwidth, for instance, at 320 Kbps. This ensures a consistent level of video quality throughout the recording, but it can result in larger file sizes compared to VBR.
Quality	6 quality levels are available. The higher the value, the better the quality. 📖 You need to configure the image quality when **VBR** is set to **Bit Rate Type**.
Bit Rate	Higher bit rate signifies greater image or video quality, but also occupies more storage space. 📖 You need to configure the bit rate when **CBR** is set to **Bit Rate Type**.
I Frame Interval	The number of P-frame between two I-frames. The number varies according to the bit rate. The range is 25–150. We recommend configuring the value to be twice the amount of the bit rate.
Enable	Enable sub stream when your network bandwidth is insufficient or other conditions that influence the video smoothness in main stream.

Step 3 Click **Save**.

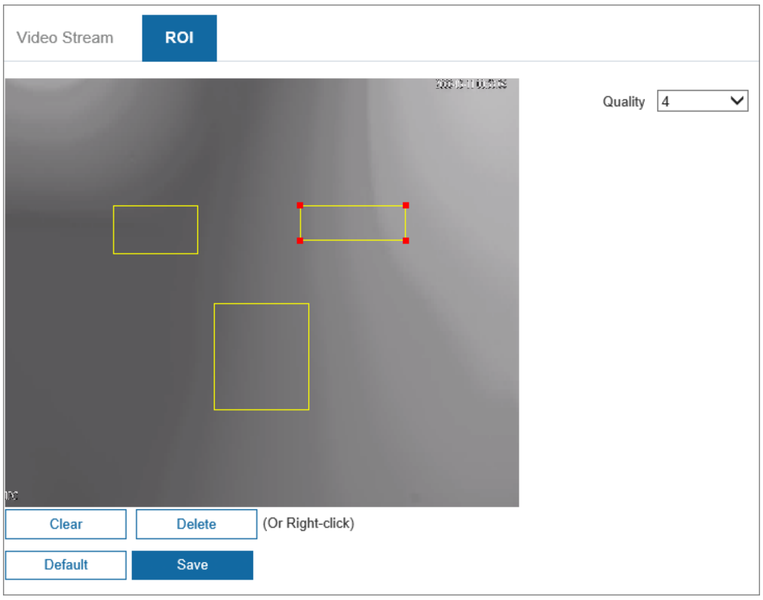
3.5.3.2 ROI

Select one or more ROI (region of interest) on the video, configure the quality of these areas, and then the areas on the video will be displayed at the defined quality.

Procedure

Step 1 Select **Setting** > **Video/Audio** > **Video** > **ROI**.

Figure 3-37 ROI



Step 2 Drag anywhere in the video image to draw the region of interest. You can draw more than one region when necessary. Up to 3 areas can be added.

Click **Clear** to delete all the areas; click **Delete** or right click to delete the most recently drawn area.

Step 3 Set the image quality of the regions of interest. 6 quality levels are available. The higher the value, the better the quality.

Step 4 Click **Save**.

3.5.3.3 Volume/Encoding

Configure the parameters for voice broadcast.

Procedure

Step 1 Select **Setting** > **Video/Audio** > **Audio** > **Volume/Encoding Settings**.

Step 2 Configure the volume and speed of the voice broadcast as needed.

Step 3 Click **Save**.

3.5.4 Image

3.5.4.1 Setting Display Parameters

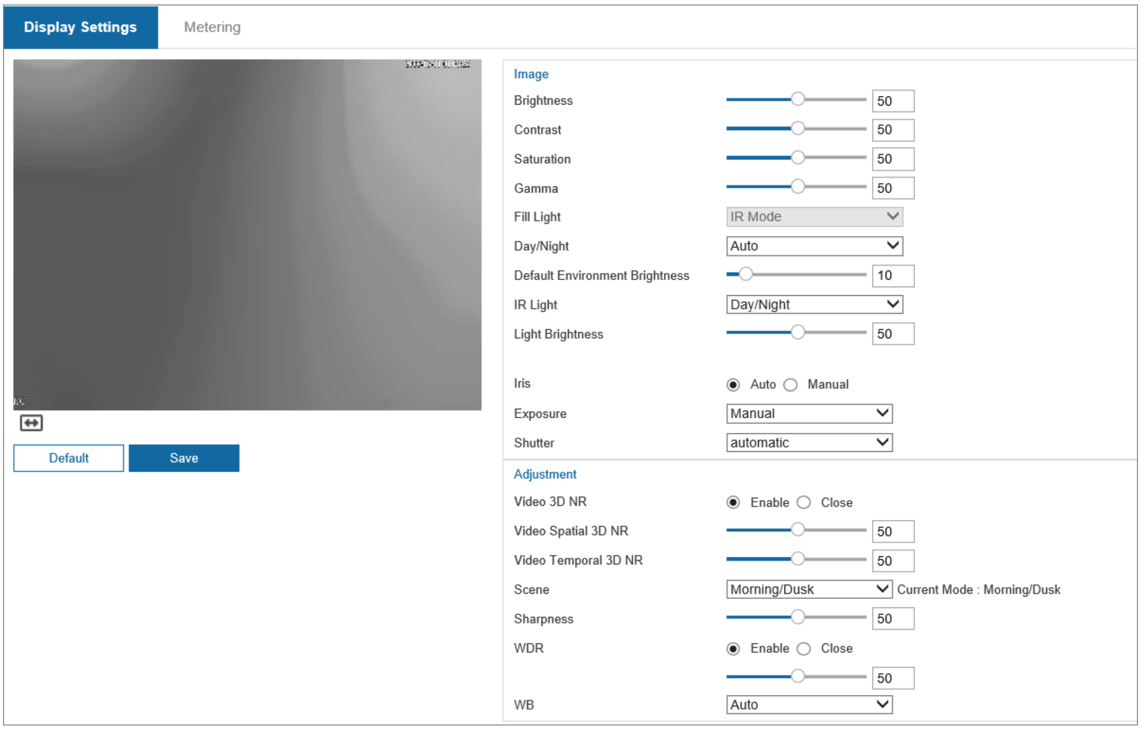
You can configure the brightness, contrast, saturation, mode, and other properties.

Procedure

Step 1 Select **Setting** > **Image** > **Display Settings** > **Display Settings**.

Step 2 Configure the corresponding parameters.

Figure 3-38 General



Image

Brightness 50

Contrast 50

Saturation 50

Gamma 50

Fill Light IR Mode

Day/Night Auto

Default Environment Brightness 10

IR Light Day/Night

Light Brightness 50

Iris ● Auto ○ Manual

Exposure Manual

Shutter automatic

Adjustment

Video 3D NR ● Enable ○ Close

Video Spatial 3D NR 50

Video Temporal 3D NR 50

Scene Morning/Dusk Current Mode : Morning/Dusk

Sharpness 50

WDR ● Enable ○ Close

50

WB Auto

Table 3-20 General parameters

Parameter	**Description**
Image	
Brightness	Both the darker areas and the brighter areas will be changed together when adjusting the brightness. The image might become blurry when the value gets bigger. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the brighter the image.
Contrast	The larger the value, the darker the dark area, and the more exposed the bright area. The image might become blurry when the value gets smaller. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the stronger the contrast.
Saturation	Saturation value does not change the overall image brightness. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The smaller the value, the more unsaturated the image.
Gamma	Adjust the image brightness level. The higher the value is, the brighter and blurrier the image becomes.
Day/Night	● **Auto**: Set a value for brightness. When the brightness is higher or lower than the value, the image shows in colors or black and white respectively. ● **Color**: Applicable during the day. The image is shown in colors. ● **B/W**: Applicable during nights. The image is black and white.
IR Light	● **Always Off**: Set the IR light to always on. ● **Always On**: Set the IR light to always off. ● **Day/Night**: Automatically turn on or off the IR light according to the configured Day/Night mode.
Light Brightness	Set the illumination intensity when there are no vehicles passing. The higher the value is, the brighter it will be.

Parameter	Description
Iris	Select from **Auto**, and **Manual**. When it is selected as **Manual**, drag the slider to adjust the iris value.
Exposure	Select from **Auto**, and **Manual**. When it is selected as **Manual**, choose the **Shutter** value.
Adjustment	
Video 3D NR	Enabling the function to reduce noise. ● Video Spatial 3D NR: Spatial video denoising. The higher the value, the fewer the noise. ● Video Temporal 3D NR: Temporal video denoising. The higher the value, the fewer the flicker noise.
Scene	You can change the scene, and adjust the sharpness of corresponding scene. Scenes available: **Morning/Dusk**, **Day**, and **Night**.
Sharpness	You can set the sharpness of corresponding scene. The higher the value, the clearer the image. But there will be noise if sharpness is too high.
WDR	Enabling WDR (wide dynamic range) helps provide clear video images in bright and dark light.
WB	Set a scene mode to adjust the image to its best status.

Step 3 Click **Save**.

3.5.4.2 Setting Metering Zone

This section provides guidance on setting the measure mode of metering zone.

Procedure

Step 1 Select **Setting** > **Image** > **Display Settings** > **Metering**.

Step 2 Configure the parameters.

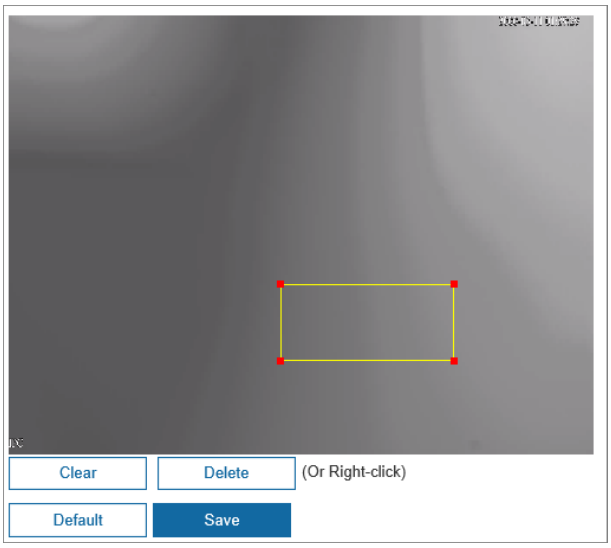
Table 3-21 Parameter description

Parameter	Description
Plate Brightness Compensation	When selecting **Enable**, you can turn **ON** or **OFF** backlighting compensation, and frontlighting compensation according to scene requirements, and then improve the image brightness in backlighting situations.
Backlighting Compensation	
Frontlighting Compensation	
Metering Mode	● **Global Metering**: Measure the brightness of the whole image area, and intelligently adjust the overall image brightness. ● **Partial Metering**: Measure the brightness of sensitive area, and intelligently adjust the overall image brightness. If the measured area becomes bright, then the whole area becomes dark, and vice versa.

Step 3 When setting **Metering Mode** to **Partial Metering**, draw areas on the image.

Place the cursor over the area in the live view image. Click and then drag the mouse to draw a rectangle around the desired area.

Figure 3-39 Partial metering



- Drag the vertexes to adjust its size and drag the lines to adjust its position.
- Up to 5 areas can be added.
- Right-click an area or select it and then click **Delete** to delete the most recently drawn area. Click **Clear** to delete all areas.

Step 4 Click **Save**.

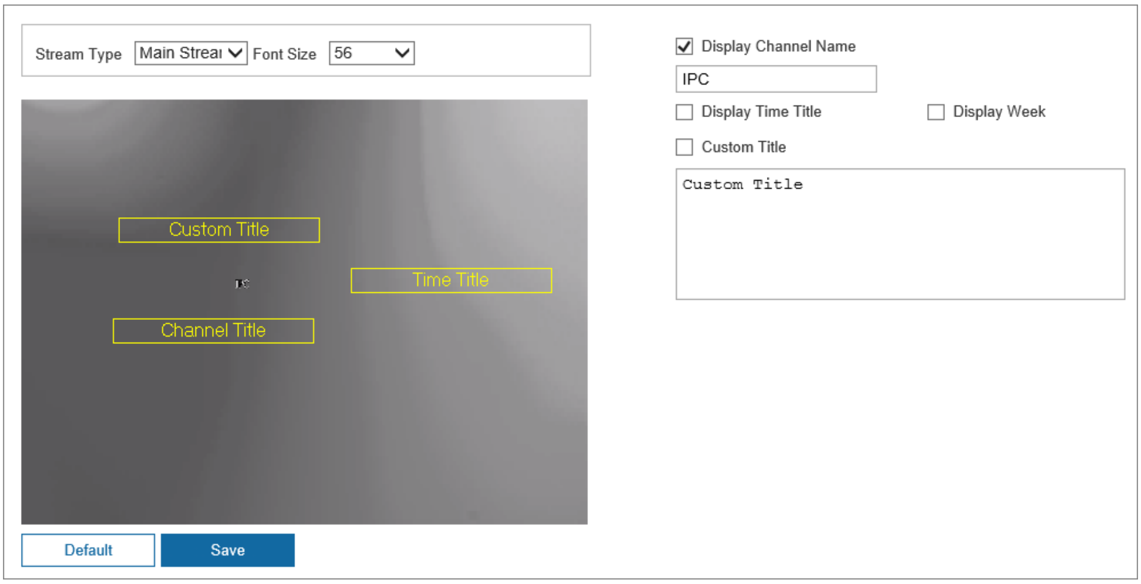
3.5.4.3 Configuring OSD

Configure the OSD information, and it will be displayed on the **Live** page.

Procedure

Step 1 Select **Setting** > **Image** > **OSD** > **OSD**.

Figure 3-40 OSD


Stream Type: Main Strea

Font Size: 56

☑ Display Channel Name

IPC

□ Display Time Title □ Display Week

□ Custom Title

Custom Title

Step 2 Configure the parameters.

- **Channel Name**: Select the checkbox to display it and enter the channel title.
- **Time Title**: Select the checkbox to display it. You can select **Display Week** to display

week information on the video image.

- **Custom Title**: Enter the text that you want to display.

Drag the yellow box on the live view image to adjust the OSD positions.

Step 3 Click **Save**.

3.5.5 Event

3.5.5.1 Alarm

3.5.5.1.1 Enabling Alarm-in and Alarm-out Ports

You can set several parameters of alarm-in and alarm-out ports. When an alarm is triggered, the device sends a signal to trigger, for example, a buzz on external devices.

Procedure

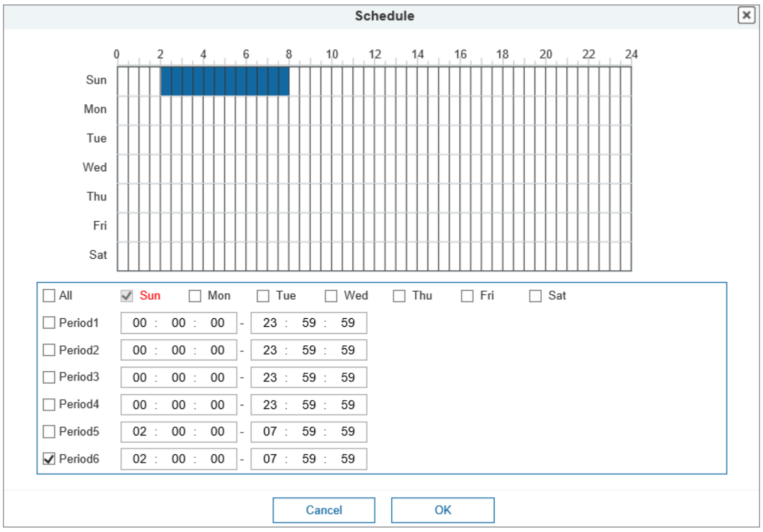
Step 1 Select **Setting** > **Event** > **Alarm** > **Alarm**.

Step 2 Select the checkbox next to **Enable** to enable alarm input for the current channel.

Step 3 Select an alarm input channel and click **Setting** to set a schedule.

If there are no suitable schedules, you can follow the steps below to add a new one.

Figure 3-41 Drag to set periods



☐ All ☑ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

☐ Period1 00 : 00 : 00 - 23 : 59 : 59

☐ Period2 00 : 00 : 00 - 23 : 59 : 59

☐ Period3 00 : 00 : 00 - 23 : 59 : 59

☐ Period4 00 : 00 : 00 - 23 : 59 : 59

☐ Period5 02 : 00 : 00 - 07 : 59 : 59

☑ Period6 02 : 00 : 00 - 07 : 59 : 59

- Choose a day/days: Select the checkbox or just click the specific day.
- Configure the time: Press and hold the left mouse button on the chosen day, and directly drag to set the period on the timeline. Or you can enter the specific time. Up to 6 time periods can be set.
- Delete the time: Click once to delete it.

Step 4 Configure other parameters.

Table 3-22 Parameter description

Parameter	Description
Event Interval	Enter the interval time (1 s–100 s). System will only record one when there are multiple alarms during the defined time.
Sensor Type	Select relay-in type according to the connected alarm input device. ● **NO**: Low level valid. ● **NC**: High level valid.
Alarm-out Port	Select the checkbox, and then select one or more alarm output channels. The corresponding device will be activated when alarms are triggered.
Alarm Channel	
Duration	When an alarm is triggered, it will continue for the defined period.

Step 5 Click **Save**.

3.5.5.1.2 Alarm-out Port

This function is used to check if alarm-out ports are working properly.

Procedure

Step 1 Select **Setting** > **Event** > **Alarm** > **Alarm-out Port**.

Step 2 Select one or more alarm channels.

Step 3 Click **Trigger Mode** to send alarm signals to the selected ports.

For example, if the camera is connected to a buzzer, the buzzer will produce a sound. This means the alarm-out port is working properly.

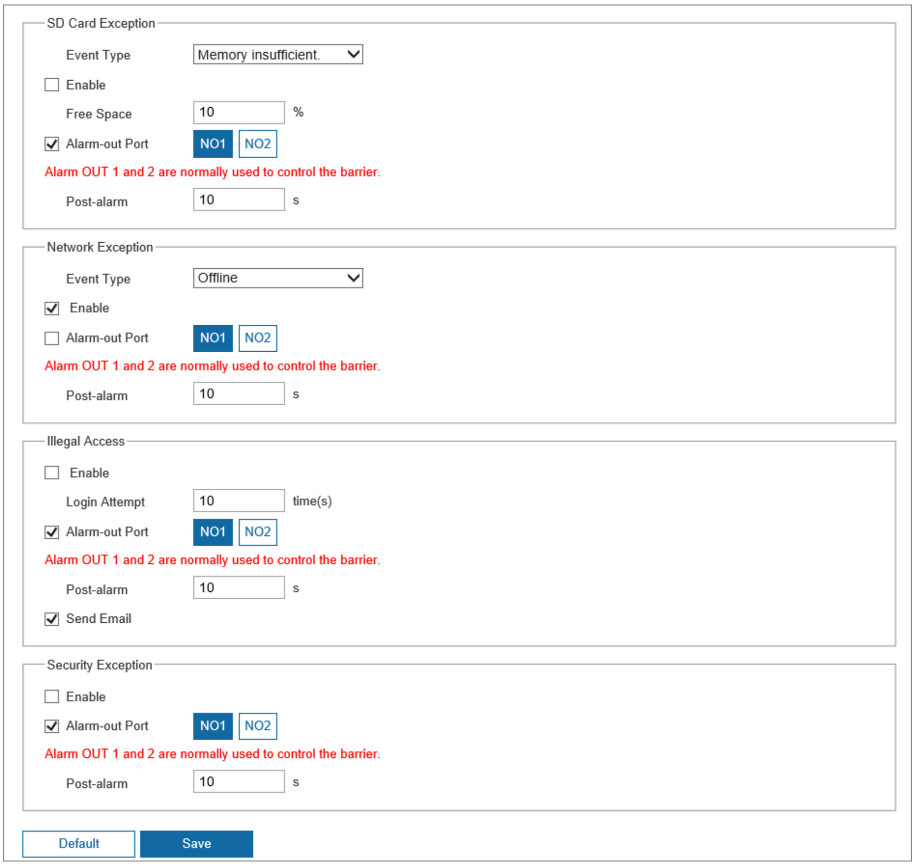
3.5.5.2 Exception

It is designed to detect and alert users to any abnormal conditions. An alarm will be triggered when an abnormal event occurs, which helps maintain the reliability and performance of your camera system.

Procedure

Step 1 Select **Setting** > **Event** > **Exception** > **Exception**.

Figure 3-42 Exception



SD Card Exception

Event Type: Memory insufficient.

□ Enable

Free Space: 10 %

☑ Alarm-out Port: NO1 NO2

Alarm OUT 1 and 2 are normally used to control the barrier.

Post-alarm: 10 s

Network Exception

Event Type: Offline

☑ Enable

□ Alarm-out Port: NO1 NO2

Alarm OUT 1 and 2 are normally used to control the barrier.

Post-alarm: 10 s

Illegal Access

□ Enable

Login Attempt: 10 time(s)

☑ Alarm-out Port: NO1 NO2

Alarm OUT 1 and 2 are normally used to control the barrier.

Post-alarm: 10 s

☑ Send Email

Security Exception

□ Enable

☑ Alarm-out Port: NO1 NO2

Alarm OUT 1 and 2 are normally used to control the barrier.

Post-alarm: 10 s

- **SD Card**: Alarm will be triggered when there is **No SD Card**, **SD Card Error**, or **Memory Insufficient** (no enough storage space).
- **Network Error**: Alarm will be triggered when there is **Off-line** (the Camera is offline) or **IP Conflict**.
- **Illegal Access**: Alarm will be triggered when unauthorized access is detected by the system.
- **Security Exception**: Alarm will be triggered when security problem occurs.

Step 2 Configure the parameters.

Refer to the actual page to view the parameters that you need to configure for each exception.

Table 3-23 Parameters of abnormality

Parameter	**Description**
Enable	Select it to enable alarm of abnormal events.
Free Space	When enabling **Memory Insufficient**, set a value for **Free Space**. When the remaining space of SD card is less than this value, an alarm is triggered.
Post-alarm	When an alarm is triggered, it will continue for the defined period after it ends.

Parameter	Description
Login Attempt	Configure the number of login errors allowed. The range is 3 to 10 times. 📖 The parameter is available only in **Illegal Access**.
Send Email	The system sends an email to the defined email address when an alarm is triggered. To set the email address, go to **Setting** > **Network Settings** > **Email**. 📖 This parameter is available only in **Illegal Access**.

Step 3 Click **Save**.

3.5.6 Storage

You can configure the storage path of snapshots and video records.

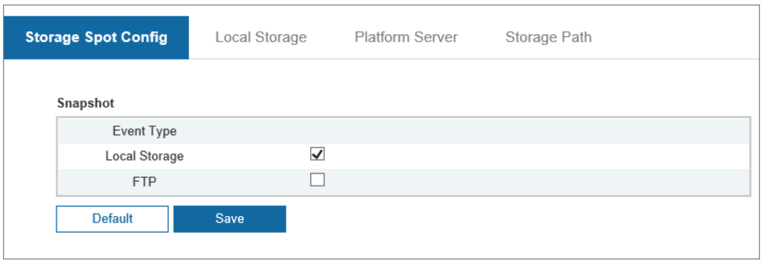
3.5.6.1 Storage Spot Config

Set the storage path of snapshots.

Procedure

Step 1 Select **Setting** > **Storage** > **Storage** > **Storage Spot Config**.

Figure 3-43 Storage spot config



Snapshot

Event Type	
Local Storage	☑
FTP	□

Step 2 Select storage path as needed.

- **Local Storage**: Store in the memory card, which has a limited capacity but offers continuous access to its storage, even during network failure.
- **FTP**: Store in the FTP server, which offers a greater capacity but it will stop storing when the network fails.

📖

If you select both locations, a copy of each snapshot will be stored on both of them.

Step 3 Click **Save**.

3.5.6.2 Local Storage

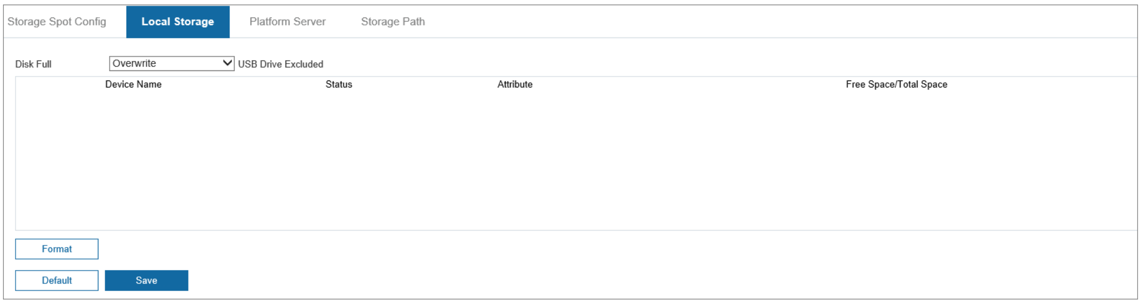
Display the information on the local memory card.

- Make sure that a memory card is properly inserted; otherwise, no card information will be displayed on the **Local Storage** page.
- For the newly installed storage card, you need to format it manually before using it normally.

Procedure

Step 1 Select **Setting** > **Storage** > **Storage** > **Local Storage**.

Figure 3-44 Local configuration



Disk Full: Overwrite, USB Drive Excluded

Device Name	Status	Attribute	Free Space/Total Space

- Select **Overwrite** or **Stop** from **Disk Full**, meaning overwrite the records or stop storing new pictures or videos respectively when the disk is full.
- View the storage information of the card.
- Click **Format**, and then you can format the memory card.

Step 2 Click **Save**.

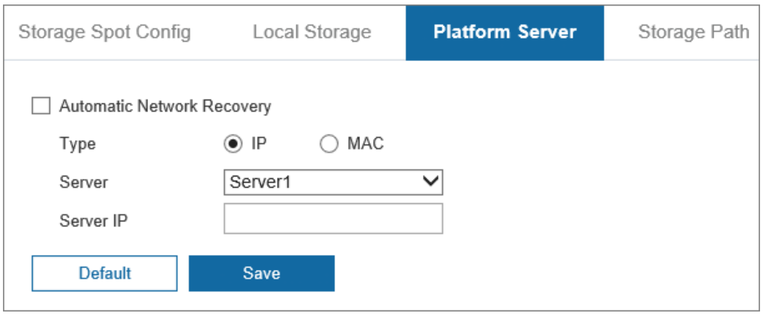
3.5.6.3 Platform Server

You can set the parameters of storing to the platform. You need to install and log in to platform first before you can store snapshots to platform server.

Procedure

Step 1 Select **Setting** > **Storage** > **Storage** > **Platform Server**.

Figure 3-45 Platform server



□ Automatic Network Recovery

Type ● IP ○ MAC

Server: Server1

Server IP:

Step 2 Configure the parameters.

Table 3-24 Platform server parameters

Parameter	Description
Automatic Network Recovery	When network is disconnected or failed, you can store the image into local storage card, and it will automatically upload to platform server after network resumes.
Type	Select connect to platform server through an IP address or a MAC address.

Parameter	Description
Server IP/MAC Address	Configure the IP address or MAC address of the platform server.

Step 3 Click **Save**.

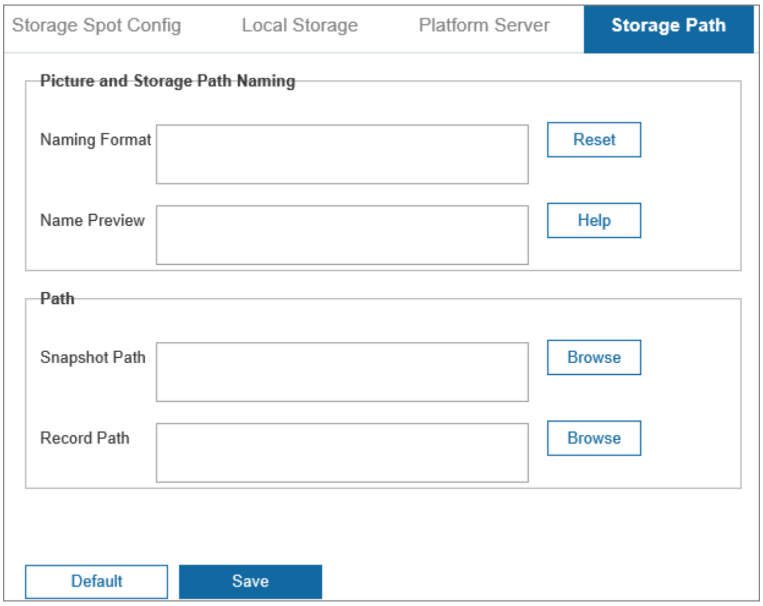
3.5.6.4 Storage Path

You can configure the names and storage paths of snapshots and video recordings.

Procedure

Step 1 Select **Setting** > **Storage** > **Storage** > **Storage Path**.

Figure 3-46 Save path



Step 2 Name the snapshots in the **Name Format** section. You can click **Help** to view the **Picture Naming Help**, or click **Reset** to restore the naming rule to the default.

After setting the naming rule, you can preview an example of the name in the **Name Preview** section.

Step 3 Click **Browse** to set the save paths of snapshots and video recordings respectively.

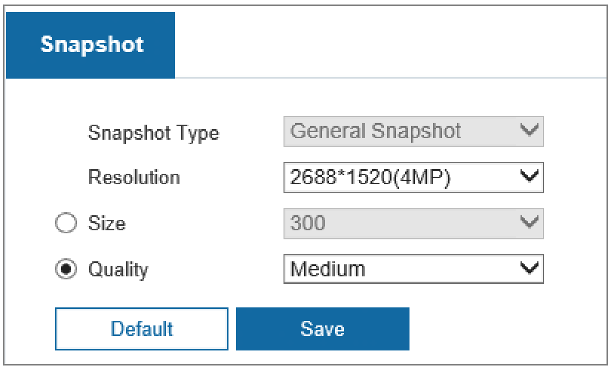
Step 4 Click **Save**.

3.5.6.5 Setting Snapshot Parameters

Procedure

Step 1 Select **Setting** > **Storage** > **Snapshot** > **Snapshot**

Figure 3-47 Snapshot



Snapshot

Snapshot Type	General Snapshot
Resolution	2688*1520(4MP)
○ Size	300
● Quality	Medium

Step 2 Set the parameters.

Table 3-25 Description of snapshot parameters

Parameter	Description
Snapshot Type	Only **General Snapshot** is supported.
Resolution	The resolution of snapshots.
Image Size	Select from 8 options, or select **Custom** to define the size (50–1024).
Quality	The quality of snapshots, including 3 levels.

Step 3 Click **Confirm**.

3.5.7 LPR

3.5.7.1 AI Setting

3.5.7.1.1 Setting Snapshot

You can set snapshot rules of the camera.

Procedure

Step 1 Select **Setting** > **LPR** > **AI Setting** > **Snapshot Setting**.

Step 2 Configure the parameters.

Table 3-26 Parameter description

Type	Parameter	Description
General Parameters	Capture Mode	● **Loop**: Snapshots will be taken when targets enter a loop. ● **Video**: Snapshots will be taken when video analyzes the targets. ● **Mix Mode**: Captures vehicles based on both induction loop and video detection.
	Snapshot Quantity	Takes 1 or 2 snapshots at a time.

Type	Parameter	Description
	Driving Direction to Trigger Snapshot	● **Positive**: Only captures vehicles that approach. ● **Departing**: Only captures vehicles that depart. ● **Both Ways**: Captures vehicles that approach or depart.
	Delay for Prevention of Same Plate Capture	Set the time interval during which one plate can only be captured once.
Video Mode Parameters Only available when the **Capture Mode** is set to **Video** or **Mixed Mode**.	Scene	● **Vehicle Body Trajectory**: Applicable to scenes with large-sized vehicles. ● **Plate Trajectory**: Applicable to scenes with small-sized vehicles. ● **Self-adaptive**: The camera will automatically adapt to the scene.
	Unlicensed Vehicle Snapshot	Click to enable the capture towards unlicensed motor vehicles.
	Frames to Output Licensed Vehicle Snapshot	Configure the frame number of capturing licensed vehicle. **1** (default) means to capture when detecting one frame of licensed vehicle passing detection area.
	Frames to Output Unlicensed Vehicle Snapshot	Configure the frame number of capturing unlicensed vehicle. **10** (default) means to capture when detecting 10 frames of unlicensed vehicle passing detection area.
Loop Mode Parameters Only available when the **Capture Mode** is set to **Loop** or **Mixed Mode**.	Plan	● **single_in-snap_nospeed**: Lay single loop, and the Camera takes a snapshot when a vehicle reaches the loop. ● **double_in1-snap_nospeed**: Lay double loops, and the Camera takes a snapshot when a vehicle reaches the first loop. ● **double_in2-snap_speed**: Lay double loops, and the Camera takes a snapshot when a vehicle reaches the second loop.
	Loop No. Mapping	Click **Setting** to set the mapping between logical loops and physical loops.
	Loop1	Set the loop trigger mode.

Type	Parameter	Description
	Loop2	- **Do Not Trigger**: No capture is triggered. - **Rising Edge**: Capture is triggered when the vehicle enters loop. - **Falling Edge**: Capture is triggered when the vehicle exits the loop. 📖 When the scheme is **single_in-snap_nospeed**, then loop 2 cannot be set.
	Max Vehicle Pass Time	Set a time period, during which a vehicle enters the first loop and triggers the second, the camera only takes snapshots for the first trigger. 📖 Applicable for double loops.

Step 3 Click **Save**.

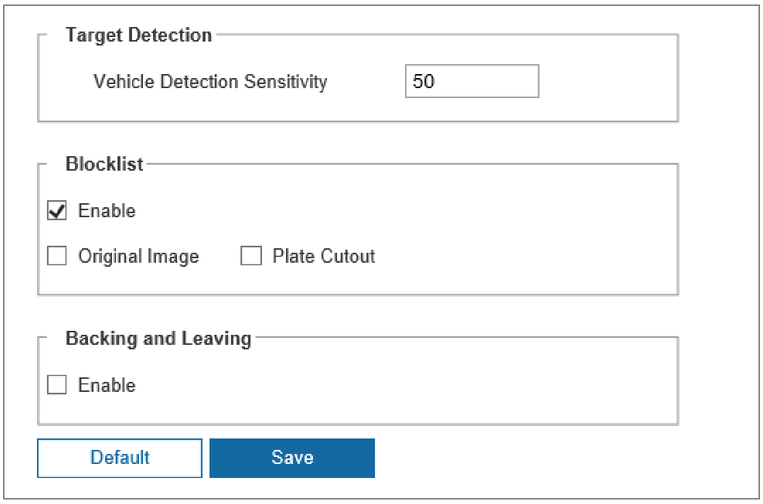
3.5.7.1.2 Configuring Intelligent Analysis

The camera can trigger blocklist alarms when vehicles in the blocklist are detected. When a blocklist alarm is triggered, the camera will link the alarm channels you select and perform the functions you specify. For backing and leaving events, the camera will take snapshots of the vehicles.

Procedure

Step 1 Select **Setting** > **LPR** > **AI Setting** > **Intelligent Analysis**.

Figure 3-48 Intelligent analysis



Target Detection

Vehicle Detection Sensitivity: 50

Blocklist

☑ Enable

□ Original Image □ Plate Cutout

Backing and Leaving

□ Enable

Step 2 Configure the parameters.

Table 3-27 Parameter description

Parameter	Description
Target Detection	

Parameter	Description
Vehicle Detection Sensitivity	Set the sensitivity of vehicle detection. The higher the value, the easier targets will be detected.
Blocklist	
Enable	Select the checkbox to enable blocklist.
Select Image	Select the image type to be generated when a vehicle in a blocklist is detected. ● **Original Image**: The complete image taken by the camera. ● **Plate Cutout**: A cutout image of the number plate.
Backing and Leaving	Select the checkbox to enable it, then the camera can trigger alarms when backing and leaving events are detected.

Step 3 Click **Save**.

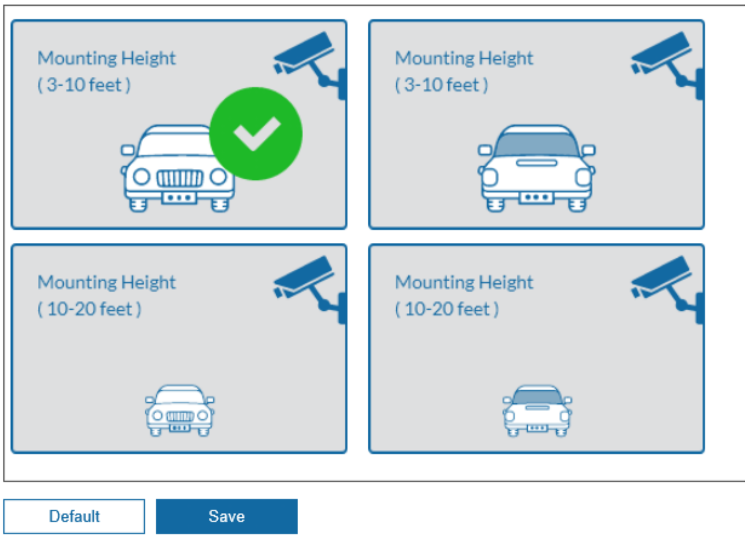
3.5.7.1.3 Selecting Scene

Configure the advanced functions of plate recognition, and customize special functions.

Procedure

Step 1 Select **Setting** > **LPR** > **AI Setting** > **Scene Config**.

Figure 3-49 Scene



Step 2 Select a detection scene as needed.

- Head first: Higher recognition sensitivity for the front plate.
- Tail first: Higher recognition sensitivity for the back plate.
- Mounting height: Higher recognition sensitivity when the Camera is installed in a higher place.

Step 3 Click **Save**.

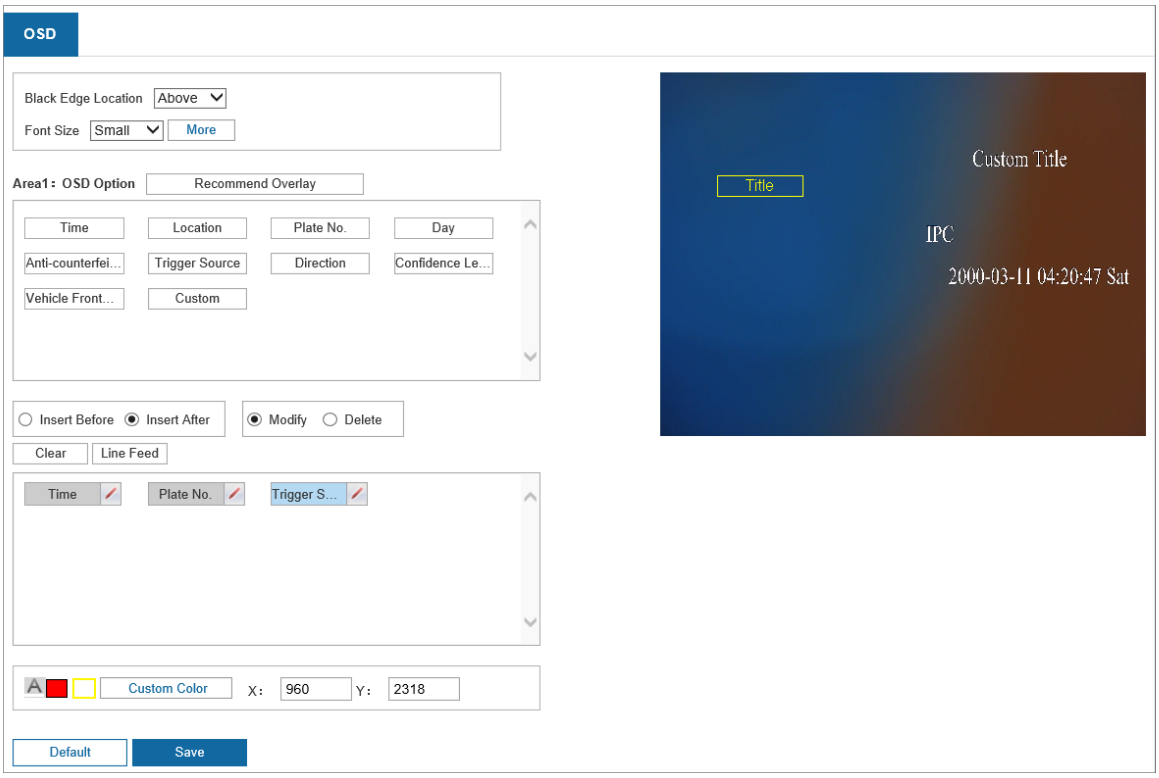
3.5.7.2 Picture OSD

You can set the extra information you want to display on snapshots.

Procedure

Step 1 Select **Setting** > **LPR** > **AI Setting** > **OSD**.

Figure 3-50 OSD



OSD

Black Edge Location: Above

Font Size: Small

Area1：OSD Option

X：960 Y：2318

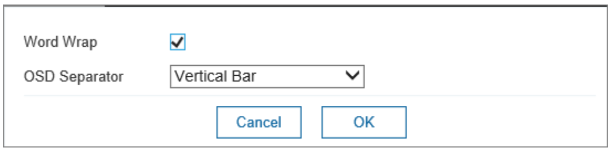
Step 2 Select the location of the black edge and font size.

1) You can put the OSD information on the black bar to display it clearly.
You can choose from **Above**/**Below**, then a black bar will be generated on the top/bottom on snapshots. When it is selected as **None**, there will be no black bar on snapshots.

2) Select a font size from the list. And you can set a font color in A🟥□ Custom Color.

3) Click **More** to configure **OSD Separator** and choose whether to enable **Word Wrap**.

Figure 3-51 More



Word Wrap ☑

OSD Separator: Vertical Bar

- **Word Wrap**: After it is enabled, the OSD information will automatically move to the next line when it reaches the edge of the snapshot.
- **OSD Separator**: Different types of information will be separated by the separator you select. For example, the OSD information includes time and plate number. If you select the OSD separator to be **Vertical Bar**, then the OSD information will be "2023-02-22|A12345".

Step 3 Set the OSD position, which is called the **Title** box in the live view image.

1) Adjust the position: Drag the yellow title box to the desired location or manually enter the coordinates at the lower-left corner of the page.

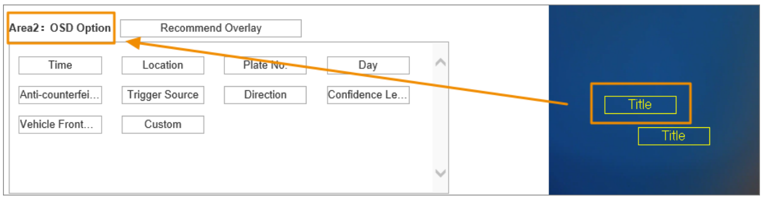
2) Add a title box: Click until a crosshair cursor appears, and then drag the crosshair for a new one. You can add up to 8 title boxes, each of which can display different OSD information.

3) Delete the title box: Right click to delete the recently added box.

4) Configure the OSD information: To configure the OSD information within a specific title box, click on the desired box, and the area will turn to the corresponding number, like area 2.

Once selected, you can set the OSD options, font size and color. See the image below.

Figure 3-52 Area

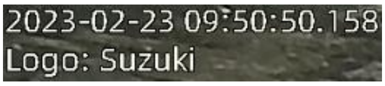


Step 4 Configure the OSD information to be displayed.

1) Click a type of information in the box under **OSD Option**.

- Click **Recommend Overlay** and then the camera will automatically add various types of information.
- Select an already-added OSD option, click **Insert Before** or **Insert After**, and then select new OSD options. The newly-added OSD options will be displayed before/after the original OSD option.
- To edit the OSD option, select **Modify**, and then click ✎ to modify the prefix, suffix, content, and separator of the corresponding OSD option.
- To delete any type of information, select **Delete**, hover your mouse over it, and then click ✕. Or you can click **Clear** to delete all the information that have been added.
- **Line Feed** is used to separate the information into different lines. See the example below for reference.

Figure 3-53 Line feed



2023-02-23 09:50:50.158
Logo: Suzuki

2) Click a type of information, and then configure its details.

Table 3-28 Parameter description

Parameter	Description
With ms	Select whether to display millisecond. This parameter is only available for **Time**.
Prefix	The information to be displayed before the type of information you are configuring. For example, a prefix "Time of trigger:" for **Time** can be "Time of trigger: 2023-02-23 09:58:41".

Parameter	Description
Suffix	The information to be displayed before the type of information you are configuring. For example, a prefix "Time of trigger:" for **Time** can be "Time of trigger: 2023-02-23 09:58:41".
Contents	Enter the fixed content that will be displayed the same on each snapshot. This parameter is only available for **Location** and **Custom**.
Delimiter Quantity	Select the number of separators to separate the information you are configuring with other types.

Step 5 Click **Save**.

3.5.7.3 Cutout

3.5.7.3.1 Configuring Cutout

Enable this function and the camera will cut out a picture of the plate numbers in snapshots, and then save them to the storage path.

Procedure

Step 1 Select **Setting** > **LPR** > **Cutout Config** > **Cutout Config**.

Step 2 Enable this function and configure the parameters.
The camera will cut out pictures of the plate numbers and bodies of vehicles and save them to the storage path. These 2 options can be selected at the same time.

Step 3 Click **Save**.

3.5.7.3.2 Configuring Plate Overlay

Set whether to overlay the plate image on the snapshot, and set its location and size.

Procedure

Step 1 Select **Setting** > **LPR** > **Cutout Config** > **Plate Overlay**.

Step 2 Set the overlay position and size.

Step 3 Click **Save**.

3.5.7.4 Blocklist and Allowlist

3.5.7.4.1 Setting Allowlist

If the barrier control is set to **Open barrier by allowlist**, only vehicles on the allowlist can pass. You can also configure fuzzy match, which allows the camera to misread certain characters in the plate numbers so that a vehicle can still pass even if the camera is unable to recognize its plate number exactly.

Procedure

Step 1 Select **Setting** > **LPR** > **Vehicle Blocklist/Allowlist** > **Allowlist**.

Step 2 Search for plate number.

- Enter the plate number, and click **Search** to determine whether a vehicle is in the allowlist.

  If the plate number is in the allowlist, its details will be displayed.
- Click **Search** without entering a plate number, and the information of all vehicles included in the allowlist will be displayed.

Step 3 Add vehicles.

- Add them one by one.
  1. Click **Add**.
  2. Configure the information of the vehicle, and then click **OK**.

Table 3-29 Parameter description

Parameter	Description
Plate No.	(Required) Enter the plate number of the vehicle.
Start Time	Configure a period for this vehicle to pass the barrier. ● Within the period, the status of the vehicle will be **Active**, and the vehicle can pass the barrier. ● Outside this period, the status of the vehicle will be **Expired**, and the vehicle cannot pass the barrier.
End Time	
Owner Name	(Optional) Enter the name of owner of the vehicle.
Add More	Select the checkbox, and then you can continue add another vehicle after you click **OK**.

- Add them in batches.
  1. Click **Browse**.
  2. Click **Download**, and then save the template to your computer.
  3. Fill in the template, click **Browse** to upload the template, and then click **OK**.

     All the vehicles are imported to the allowlist.
- Export information of vehicles on the allowlist: Click **Export**, and then select to enable or disable encryption.
- Edit the information of a vehicle: Click ✎ of a vehicle to edit its information.
- Delete vehicles one by one: Click ⊖ of a vehicle to delete it from the allowlist. If barrier control by allowlist is enabled, this vehicle will not be able to pass.
- Delete expired vehicles: Vehicles that are expired will not be able to pass the barrier. You can click **Clear Expired Data** to delete them from the allowlist.
- Delete vehicles in batches: Click **Clear** to delete all the vehicles from the allowlist. Please be advised that this operation cannot be undone.

Step 4 Select **Fuzzy Matching**, and then select options to define the rules of fuzzy match.

Table 3-30 Parameter description

Parameter	Description
The snapshot is missing the first or last character of the plate	You can enable one or both of these 2 options.
The snapshot has 1 character added to either end of the plate	

Parameter	Description
Allow the system to misread some of the characters on the plate	Select the number of characters the camera is allowed to misread on a plate number. If you select 0, this parameter will be automatically not enabled.
Number of characters allowed to be misread	This parameter allows the camera to misread certain characters as other ones. You can add up to 10 rules. For example, a 0<->D rule allows the barrier to open if the camera recognizes A0123 to AD123, or vice versa.

Step 5 Click **Save**.

3.5.7.4.2 Setting Blocklist

A vehicle in the blocklist is not able to pass the barrier.

Select **Setting** > **LPR** > **Vehicle Blocklist/Allowlist** > **Blocklist**. The configuration procedures are similar to those of allowlist. For details, see "3.5.7.4.1 Setting Allowlist".

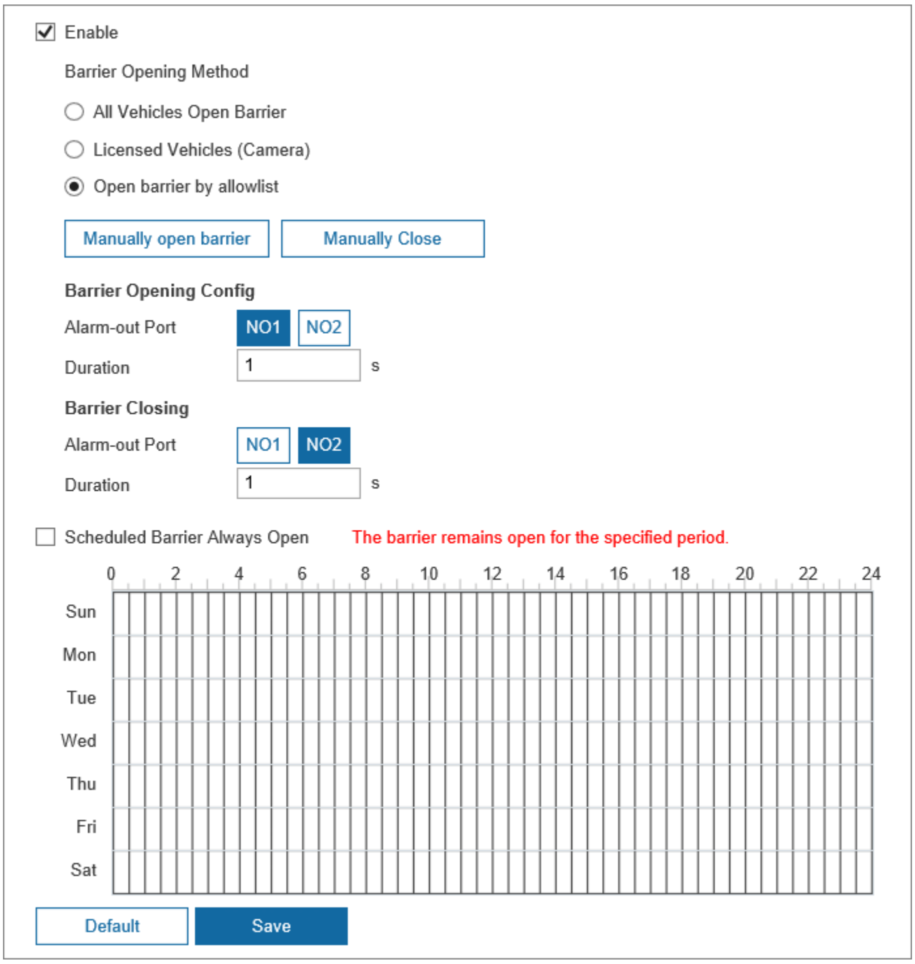
3.5.7.5 Barrier Control

You can set the barrier control mode, and configure information of opening, and closing barrier.

Procedure

Step 1 Select **Setting** > **LPR** > **Barrier Control** > **Barrier Control**.

Figure 3-54 Barrier control



☑ Enable

Barrier Opening Method

○ All Vehicles Open Barrier

○ Licensed Vehicles (Camera)

● Open barrier by allowlist

Barrier Opening Config

Alarm-out Port: NO1 (selected), NO2

Duration: 1 s

Barrier Closing

Alarm-out Port: NO1, NO2 (selected)

Duration: 1 s

□ Scheduled Barrier Always Open   The barrier remains open for the specified period.

Step 2 Configure the parameters.

Table 3-31 Parameter description

Parameter	Description
Barrier Opening Method	Triggers alarm through different modes, and remotely controls the barrier opening and close. ● **All Vehicles Open Barrier**: When the camera captures any vehicle, it outputs an open barrier signal. ● **Licensed Vehicles (Camera)**: When the camera captures any plate, it outputs an open barrier signal. ● **Open barrier by allowlist**: When the camera captures vehicles that are on the allowlist or conform to fuzzy matching, it outputs an open barrier signal. ● Click **Manually open barrier** or **Manually Close** to manually control the barrier.
Barrier Opening Config	● **Alarm-out Port**: Alarm linkage output port. Select the corresponding one according to the field connection. ● **Duration**: The duration that the barrier opening or closing signal lasts.
Barrier Closing	
Scheduled Barrier Always Open	Select it, and enable the function of barrier always open. Configure the period of barrier always open. The barrier will not close during the defined period. Click the chosen day, and directly drag to set the period on the timeline. Click once to delete it.

Step 3 Click **Save**.

3.5.7.6 Device Commission

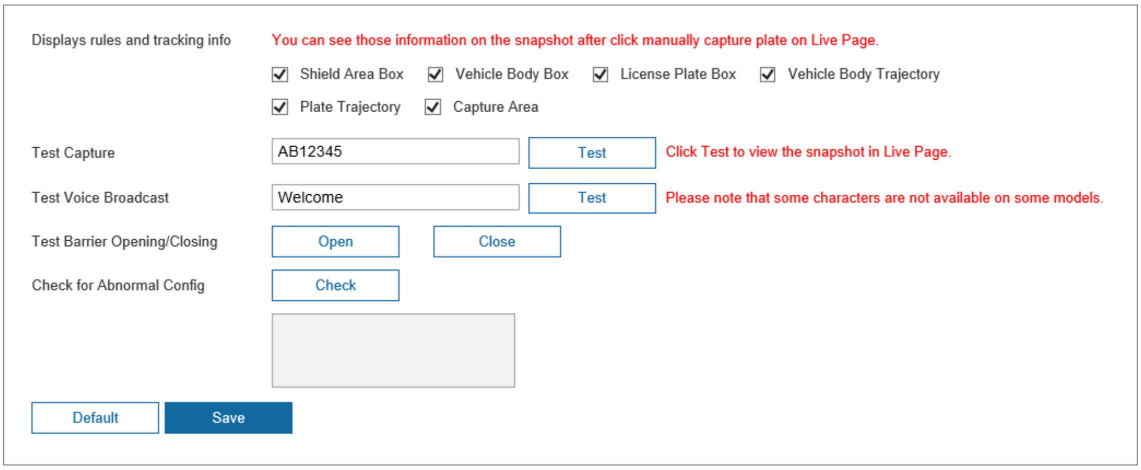
3.5.7.6.1 Device Commissioning

You can overlay some information on the snapshots to assist you in checking whether the snapshots are taken as you require. And you can test different functions to see if they work as configured.

Procedure

Step 1 Select **Setting** > **LPR** > **Device Commission** > **Device Commission**.

Figure 3-55 Device commission



Displays rules and tracking info — You can see those information on the snapshot after click manually capture plate on Live Page.

☑ Shield Area Box ☑ Vehicle Body Box ☑ License Plate Box ☑ Vehicle Body Trajectory

☑ Plate Trajectory ☑ Capture Area

Test Capture: AB12345 — Test — Click Test to view the snapshot in Live Page.

Test Voice Broadcast: Welcome — Test — Please note that some characters are not available on some models.

Test Barrier Opening/Closing: Open Close

Check for Abnormal Config: Check

Step 2 In **Displays rules and tracking info** session, select the types of information to be displayed.

Click **Save** and check the overlay effects in the **Live** page. Click 📷 to manually capture a license plate. On the snapshot, you can see the rules and tracking information you selected. If they do not meet your requirements, you can adjust them by repeating the steps above.

Step 3 Test if different functions are working normally.

Table 3-32 Parameter description

Parameter	Description
Test Capture	Enter a plate number, click **Test** to trigger capture, and view the snapshot in the **Live** page.
Test Voice Broadcast	Enter some information, click **Test** to check whether the device plays the sound normally. Some characters are not available on some models.
Test Barrier Opening/Closing	Click **Open** or **Close** to test whether the barrier responds correctly.
Check for Abnormal Config	Click **Check**, and system checks abnormality automatically.

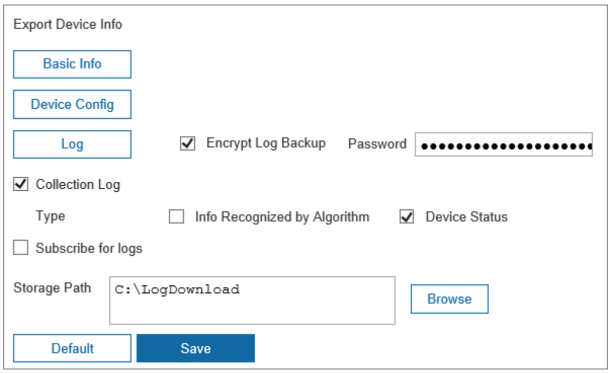
3.5.7.6.2 Collecting Debug Info

The camera supports collecting operation logs to track errors.

Procedure

Step 1 Select **Setting** > **LPR** > **Device Commission** > **Debug Info Collection**.

Figure 3-56 Collection log



Export Device Info

☑ Encrypt Log Backup Password ••••••••••••••••••••

☑ Collection Log

Type ☐ Info Recognized by Algorithm ☑ Device Status

☐ Subscribe for logs

Storage Path C:\LogDownload

Step 2 Export the device information. Click the types to be exported, and then choose the storage path.

For **Log**, you can select the checkbox next to **Encrypt Log Backup** to encrypt the logs.

Step 3 Select one or more types of log to collect.

Step 4 Select **Subscribe for logs**. You will not be able to change the log saving path.

Step 5 Clear **Subscribe Log**, and then click **Browse** to select the path where the operation logs are saved.

Step 6 Click **Save**.

Appendix 1 Cybersecurity Recommendations

Compulsory measures to ensure the basic device network security:

- Timely Update Firmware and Client Software
  - ◇ Keep the device (such as video recorder and IP camera) firmware up-to-date based on standard procedure in the tech-industry to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
  - ◇ Download and use the latest version of client software.
- Use Complex Passwords with Combination of Characters, Numbers and Symbols

  Please refer to the following suggestions to set passwords:
  - ◇ The length should not be less than 8 characters;
  - ◇ Combine at least two types of characters in a password among upper and lower case letters, numbers and symbols;
  - ◇ Do not contain the account name or the account name in reverse order;
  - ◇ Do not use continuous characters, such as abcdefgh and 12345678;
  - ◇ Do not use overlapped characters, such as aaaaaaaa and 11111111.

Constructive suggestions on improving device network security:

- Change Passwords Regularly

  We recommend that you change passwords regularly to reduce the risk of being guessed or cracked.
- Configure and Update Password Reset Information in Time

  Password reset function is supported by the device. Please configure related information for password reset in time, including the end user's email address and password protection questions. Please update the information accordingly in time if it changes. Please do not use simple questions whose answers can be easily obtained when setting password protection questions.
- Enable Account Lock

  The account lock is enabled by default. We recommend you keep it on to ensure the account security. A number of failed login attempts will lead the corresponding account and the source IP address to be locked.
- Physical Protection

  Physical protection is recommended on the device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement strict access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware and unauthorized connection of removable device (for example, USB flash drive and serial port).
- Reset Default HTTP and Other Service Ports

  Changing the default HTTP and other service ports is recommended. We recommend you change them into any set of numbers between 1024–65535 to reduce the risk of exposing ports in use to outsiders.
- Enable HTTPS

  HTTPS is recommended to be enabled so that you can obtain the web service through a secure communication channel.

- Bind IP and MAC Address to Device
  To reduce the risk of ARP spoofing, we recommend you bind the IP and MAC address of the gateway to the device.
- Assign Accounts and Privileges Reasonably
  Based on business requirements and management requirements, prudently add user accounts and assign a minimum set of permissions to them.
- Disable Unnecessary Services and Apply Secure Modes
  If not needed, we recommend you turn off some services such as SNMP, SMTP, and UPnP to reduce risks.
  If necessary, we recommend using security modes, including but not limited to the following services:
  - ◇ SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
  - ◇ SMTP: Choose TLS to access mailbox server.
  - ◇ FTP: Choose SFTP, and set up strong passwords.
  - ◇ AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
- Audio and Video Encrypted Transmission
  To reduce the risk of losing data during transmission, encrypted transmission is recommended for very important and sensitive audio and video data.
  *Reminder: Encrypted transmission might decrease the transmission efficiency.
- Establish a Secure Network Environment
  The following actions are highly recommended to ensure device security and to reduce potential cyber risks:
  - ◇ Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
  - ◇ Partition and isolate the network according to the actual network needs. If there are no communication requirements between two sub networks, we recommend you adopt network isolation through VLAN, network GAP and other technologies.
  - ◇ Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
  - ◇ Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.
- Security Auditing
  - ◇ Check online users: Check online users regularly to prevent unauthorized login.
  - ◇ Check device log: Obtain the IP addresses that were used to log in to the device and their key operations with help of the logs.
- Network Log
  The stored log is not saved in full due to the limited storage capacity. If you need to save the log for a long time, we recommend you enable the network log function to make sure that the critical logs are synchronized to the network log server for tracing.