Outdoor Parking Space Detector

Web 5.0 Operation Manual

V1.0.0

Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of outdoor parking space detector (hereinafter referred to as "the Camera"). Read carefully before using the device, 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 Date
V1.0.0	First release.	January 2026

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 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 device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Transportation Requirements

- Transport the device under allowed humidity and temperature conditions.
- Pack the device with packaging provided by its manufacturer or packaging of the same quality before transporting it.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during transportation.

Storage Requirements

- Store the device under allowed humidity and temperature conditions.
- Do not place the device in a humid, dusty, extremely hot or cold site that has strong electromagnetic radiation or unstable illumination.
- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during storage.

Installation Requirements

WARNING

- Strictly comply with the local electrical safety code and standards, and check whether the power supply is correct before operating the device.
- Please follow the electrical requirements to power the device.
  - When selecting the power adapter, the power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
  - We recommend using the power adapter provided with the device.
- Do not connect the device to two or more kinds of power supplies, unless otherwise specified, to avoid damage to the device.
- The device must be installed in a location that only professionals can access, to avoid the risk of non-professionals becoming injured from accessing the area while the device is working. Professionals must have full knowledge of the safeguards and warnings of using the device.

- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.

- We recommend you use the device with a lightning protection device for stronger protection against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.
- Ground the function earthing portion ⏚ of the device to improve its reliability (certain models are not equipped with earthing holes). The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The dome cover is an optical component. Do not directly touch or wipe the surface of the cover during installation.

Operation Requirements

⚠ **WARNING**

- The cover must not be opened while the device is powered on.
- Do not touch the heat dissipation component of the device to avoid the risk of getting burnt.

⚠

- Use the device under allowed humidity and temperature conditions.
- Do not aim the device at strong light sources (such as lamplight, and sunlight) when focusing it, to avoid reducing the lifespan of the CMOS sensor, and causing overbrightness and flickering.
- When using a laser beam device, avoid exposing the device surface to laser beam radiation.
- Prevent liquid from flowing into the device to avoid damage to its internal components.
- Protect indoor devices from rain and dampness to avoid electric shocks and fires breaking out.
- Do not block the ventilation opening near the device to avoid heat accumulation.
- Protect the line cord and wires from being walked on or squeezed particularly at plugs, power sockets, and the point where they exit from the device.
- Do not directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens.
- The dome cover is an optical component. Do not directly touch or wipe the surface of the cover when using it.
- There might be a risk of electrostatic discharge on the dome cover. Power off the device when installing the cover after the camera finishes adjustment. Do not directly touch the cover and make sure the cover is not exposed to other equipment or human bodies
- Strengthen the protection of the network, device data and personal information. All necessary safety measures to ensure the network security of the device must be taken, such as using strong passwords, regularly changing your password, updating firmware to the latest version, and isolating computer networks. For the IPC firmware of some previous versions, the ONVIF password will not be automatically synchronized after the main password of the system has been changed. You need to update the firmware or change the password manually.

Maintenance Requirements

⚠

- Strictly follow the instructions to disassemble the device. Non-professionals dismantling the device can result in it leaking water or producing poor quality images. For a device that is required to be disassembled before use, make sure the seal ring is flat and in the seal groove when putting the cover back on. When you find condensed water forming on the lens or the desiccant becomes green after you disassembled the device, contact after-sales service to replace the desiccant. Desiccants might not be provided depending on the actual model.

- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.
- Do not directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens. When it is necessary to clean the device, slightly wet a soft cloth with alcohol, and gently wipe away the dirt.
- Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.
- The dome cover is an optical component. When it is contaminated with dust, grease, or fingerprints, use degreasing cotton moistened with a little ether or a clean soft cloth dipped in water to gently wipe it clean. An air gun is useful for blowing dust away.
- It is normal for a camera made of stainless steel to develop rust on its surface after being used in a strong corrosive environment (such as the seaside, and chemical plants). Use an abrasive soft cloth moistened with a little acid solution (vinegar is recommended) to gently wipe it away. Afterwards, wipe it dry.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Overview 1

1.1 Introduction 1

1.2 Features 1

2 Device Initialization 3

3 Login 6

3.1 Device Login 6

3.2 Resetting Password 6

4 Home Page 7

5 Configuration Wizard 9

6 Live 11

6.1 Live Page 11

6.2 Video Adjustment 12

6.3 Frequently Used Functions 12

6.3.1 Parking Space Status 12

6.3.2 Parking Space Management 12

6.3.3 Light 13

6.3.4 Device Test 14

6.3.5 Zoom and Focus 14

6.4 Live View Function Bar 15

7 ANPR 17

7.1 Parking Space Management 17

7.1.1 Configuring Scene Switch 17

7.1.2 Configuring Parking Space Management 17

7.1.3 Configuring Illegal Parking Area 18

7.2 Configuring AI Settings 19

7.3 Image Configuration 20

7.3.1 Original Picture OSD 20

7.3.2 Size 22

7.4 Configuring Allowlist 23

7.4.1 Fuzzy Matching 23

7.4.2 Allowlist 23

7.5 Configuring Warning Lights 25

7.6 Configuring Audio Broadcast 25

7.6.1 Event Broadcast 25

7.6.2 Volume/Encoding 26

7.6.3 Audio File 27
7.7 Setting Device Test 27
8 Picture 29
8.1 Image Search 29
8.2 Storage 30
8.2.1 Local 30
8.2.2 Network 30
8.3 Platform Server 32
9 Record 33
9.1 Video Search 33
9.2 Record Control 34
9.3 Time Plan 34
9.4 Storage 35
10 Search 37
10.1 Snapshot Records 37
10.2 Parking Record 37
10.2.1 Configuring Parking Records 37
10.2.2 Sending Email 38
10.3 Alarm Records 38
10.4 Picture Query 38
10.5 Searching Video 39
10.5.1 Record 39
10.5.2 Watermark 39
11 Camera 40
11.1 Setting Image Parameters 40
11.1.1 General Parameters 40
11.1.2 Shutter Parameters 42
11.2 Setting Encode Parameters 44
11.2.1 Video Stream 44
11.2.2 Video OSD 46
11.2.3 ROI 48
12 System 49
12.1 General Parameters 49
12.1.1 General 49
12.1.2 Date 49
12.2 Account 50
12.2.1 User 50
12.2.2 Adding a User Group 52
12.2.3 Adding an ONVIF User 53
13 Security 55

13.1 Security Status 55
13.2 System Service 56
13.2.1 802.1x 56
13.2.2 HTTPS 57
13.3 Attack Defense 58
13.3.1 Firewall 58
13.3.2 Account Lockout 59
13.3.3 Anti-DoS Attack 59
13.4 CA Certificate 60
13.4.1 Installing Device Certificate 60
13.4.2 Installing Trusted CA Certificate 62
13.5 A/V Encryption 63
13.6 Security Warning 64
13.6.1 Security Exception 64
13.6.2 Illegal Login 65
13.7 Security Authentication 65
14 Maintenance Center 66
14.1 One-Click Diagnosis 66
14.2 System Information 67
14.2.1 Version 67
14.2.2 Online User 67
14.2.3 Legal Info 67
14.3 Log 68
14.3.1 Searching for Logs 68
14.3.2 Obtaining Remote Logs 69
14.4 Maintenance Management 69
14.4.1 Maintenance 69
14.4.2 Import/Export 70
14.4.3 Default 70
14.5 Update 71
14.6 Advanced Maintenance 71
15 Setting 74
15.1 Local 74
15.2 Network 74
15.2.1 TCP/IP 75
15.2.2 Port 75
15.2.3 Auto Registration 77
15.2.4 SNMP 77
15.2.5 Email 79
15.2.6 Platform Access 80

15.2.7 Basic Services.....83
15.3 Event.....84
15.3.1 Setting Exception.....84
15.3.2 Video Detection.....85
15.4 Local Storage.....85
Appendix 1 Security Recommendation.....87

1 Overview

1.1 Introduction

The camera adopts intelligent deep learning algorithm. Supports vehicle detection, recognition of license plate, logo, model, and color, and encoding mode such as H.265.

The camera consists of a protective housing, illuminator, and intelligent HD camera. The intelligent HD camera adopts progressive scanning CMOS, which features high definition, low illuminance, high frame rate, and excellent color rendition.

1.2 Features

The features are available on select models, and might differ from the actual camera.

Permission Management

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

Storage

- Stores video data to the central server according to the configuration (such as alarm, and timing settings).
- Users can record videos on the webpage. The recorded video files will be stored on the computer where the client is located.
- Supports hot swapping of storage card, and storage when network is disconnected. It automatically overwrites pictures and videos when the memory is insufficient.
- Stores 1024 log records, and user permission control.
- Supports FTP storage, and ANR (automatic network replenishment).

Alarm

- Supports triggering alarms when exceptions occur, 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). It can deal with various alarms according to the linkage predefined by users, and generate voice prompts (users are allowed to record voice in advance).

Network Monitoring

- Keeps the video transmission delay within 500 ms when the bandwidth is sufficient.
- Supports up to 10 users online at the same time.
- Supports system access, and device management through the webpage of the device.
- Video data transmission adopts HTTP, TCP, UDP, MULTICAST, and RTP/RTCP.

Capture and Recognition

- Recognizes plate number, color, logo, model, and other features of vehicles.
- Supports setting OSD information, and configuring location of channel, and picture.
- Supports capturing and encoding images. Supports watermark encryption on images to prevent them from being tampered.
- The captured pictures contain the time, location, license plate, color, and more on the vehicle.

Peripheral Control

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

Auto Adjustment

- Auto iris: Automatically adjusts the iris opening to the changing light throughout the day.
- Auto white balance: Accurately displays the object color when light condition changes.
- Auto exposure: Automatically adjusts shutter speed according to the exposure value of the image, and the default values of the shutter and iris.
- Auto gain: Automatically increases camera sensitivity when illuminance is very low, enhancing image signal output so that the camera can acquire clear and bright images.

2 Device Initialization

Device initialization is required for the first-time use. This manual is based on the operation on the webpage. You can also initialize device through ConfigTool, NVR, or platform devices.

Table 2-1 Recommended requirements

Item	Recommended Requirements
Operating system	Windows 10 or later.
CPU	CPU Intel core i5 6500 or faster.
Graphics card	Intel HD Graphics or later.
Internal memory	16 GB or larger.
Monitor	The aspect ratio is 16:9 or 16:10, and the resolution is more than 720P.
Browser	Latest versions of Chrome and EDGE.

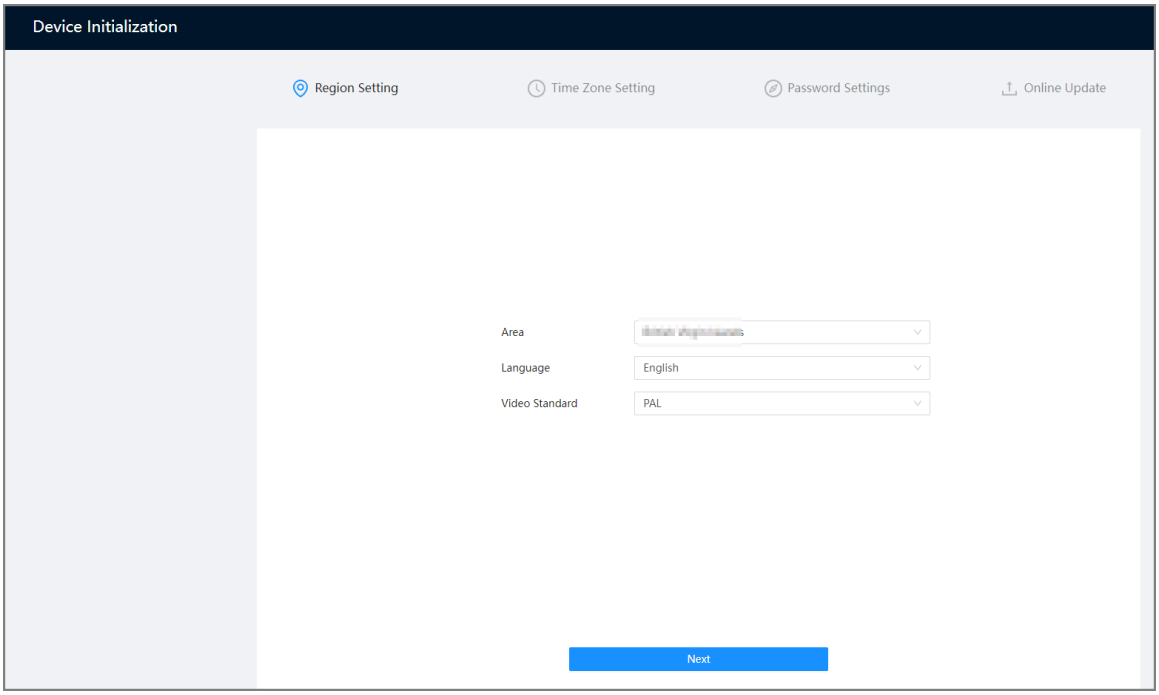
- The latest versions of Google Chrome and Microsoft browsers are supported. Most functions are available without a plug-in. A few functions require downloading a plug-in, but they still work with Google Chrome.
- Internet Explorer (IE) is not recommended. Before using it, clean up the web3.0 plug-in at C:\Program Files\webrec\ITCPlugin, and then you can use IE.
- To ensure the safety of the device, keep the password properly after initialization and change the password regularly.
- When initializing device, keep the IP addresses of the computer and device on the same network.

Procedure

Step 1 Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.

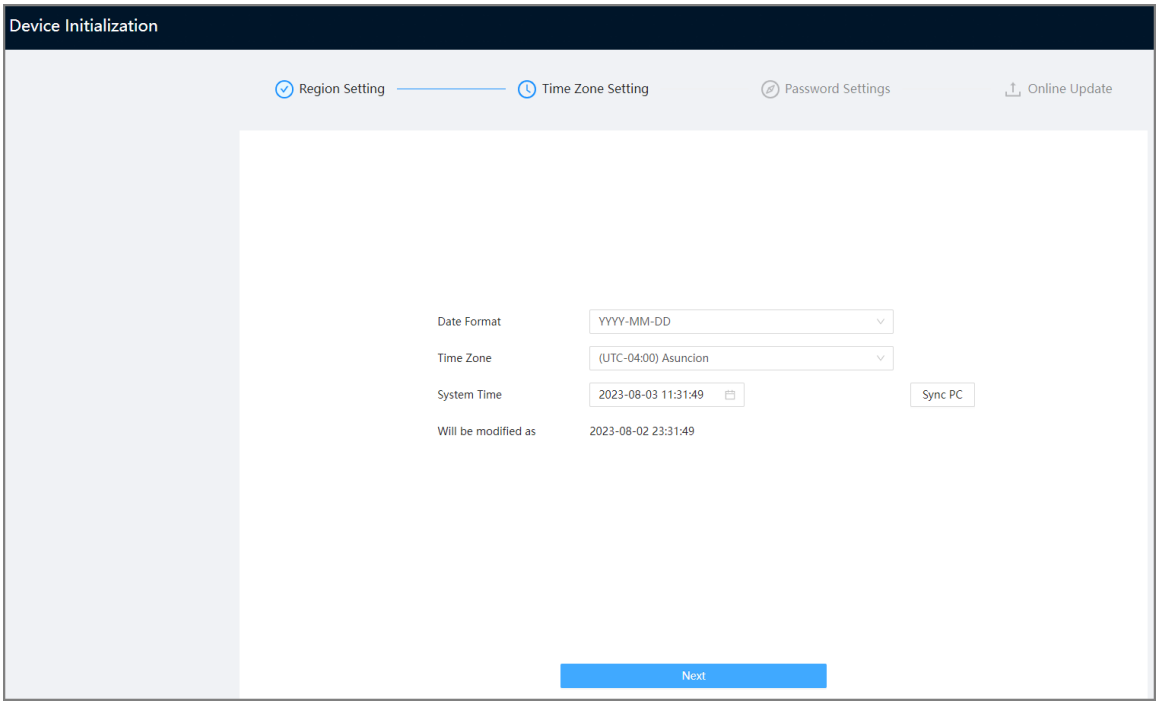
Step 2 Select the area, language, and video standard, and then click **Next**.

Figure 2-1 Region setting



Step 3 Configure the time parameters, and then click **Next**.

Figure 2-2 Time zone setting



Step 4 Set the password for admin account.

Figure 2-3 Password setting

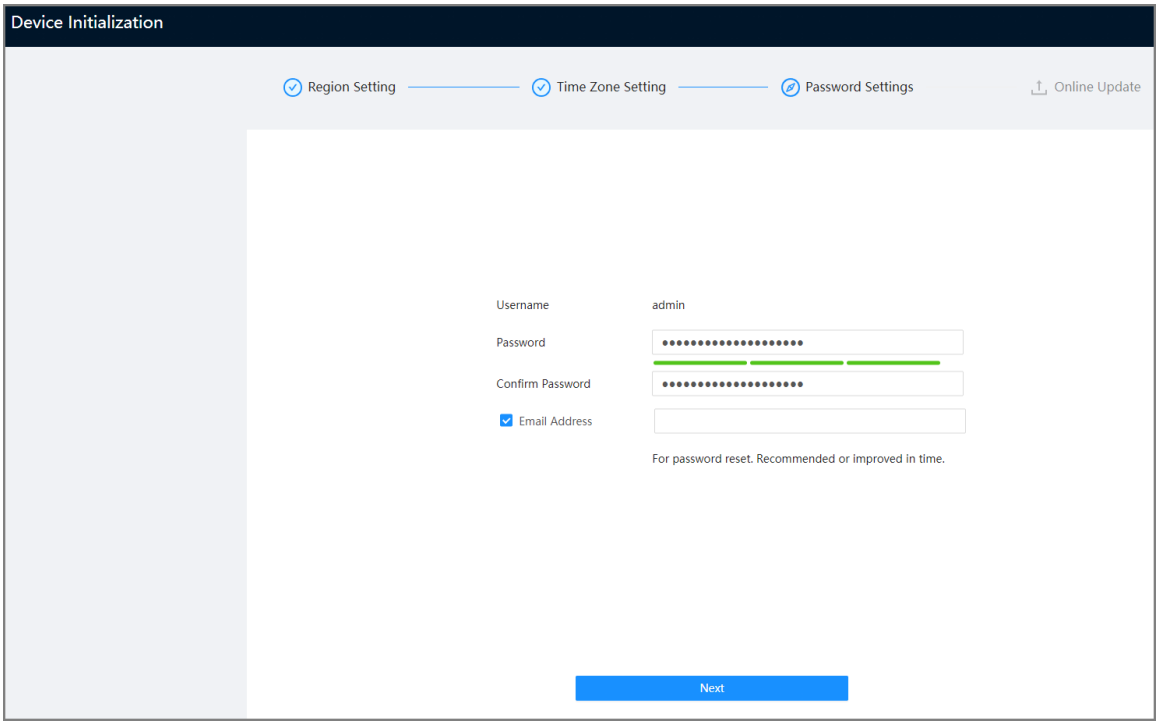


Table 2-2 Description of password configuration

Parameter	Description
Username	The default username is admin.
Password	The password must consist of 8 to 32 non-blank characters and contain at least 2 types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a high security level password according to the password security notice.
Confirm Password	
Email Address	Enter an email address for password resetting, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 5 Click **Next** , and then the **Online Update** page is displayed. Then, it automatically redirects to the login page. You can enter the new password to log in, and it goes to the **Live** page by default.

3 Login

3.1 Device Login

Introduces how to log in to the webpage. This section uses Chrome as an example.

- You need to initialize the camera before logging in to the webpage. For details, see "2 Device Initialization".
- When initializing the device, keep the IP addresses of the computer and device on the same network.
- Follow the instructions to download and install the plug-in for first-time login.

Procedure

Step 1 Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.

Step 2 Enter the username and password.

The username is admin by default.

Click **Forgot password?**, and you can reset the password through the email address that is set during the initialization. For details, see "12.2.1.2 Resetting Password".

Step 3 Click **Login**.

3.2 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 "12.2.1.2 Resetting Password".

Procedure

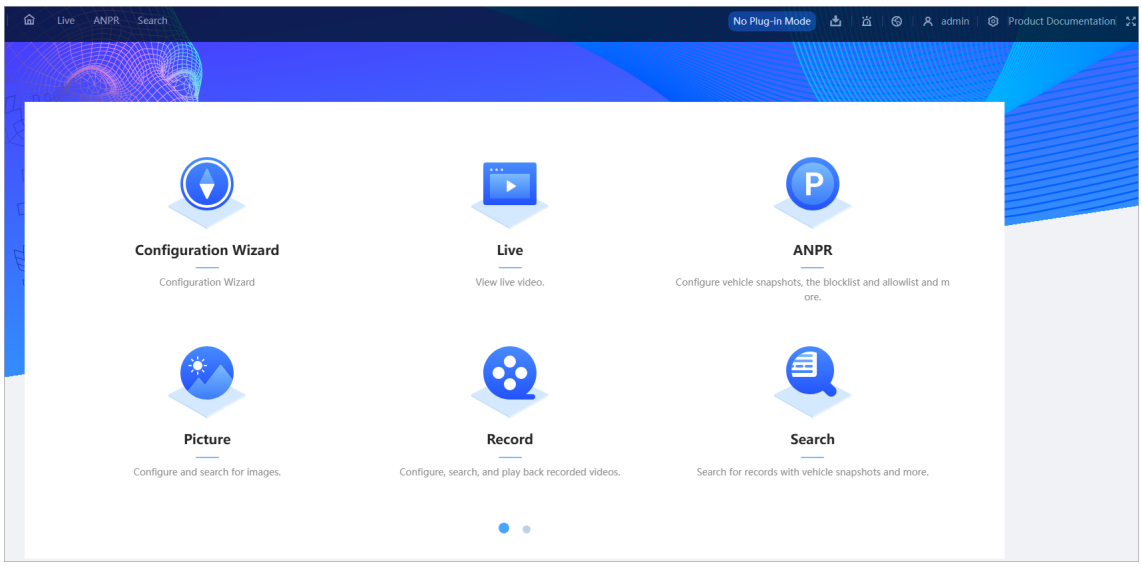
Step 1 Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.

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

4 Home Page

Click at the upper-left corner of the page to display the home page.

Figure 4-1 Home page



- Configuration wizard: Provides guidance to configure basic settings before using the camera.
- Live: View the real-time monitoring image.
- ANPR: Configure AI functions related to vehicle detection and control.
- Picture: Supports viewing and searching pictures, as well as configuring the storage methods.
- Record: Supports playing back and searching recorded videos, as well as configuring the storage methods.
- Search: Search for recordings, images, and alarm output records.
- Camera: Configure camera parameters, including image parameters, encoder parameters, and audio parameters.
- System: Configure system parameters, including general parameters, date and time, and account.
- Security: Check the security status of the device and configure security parameters.
- Maintenance center: Check the running status of devices and perform maintenance, view system information and logs, update the device, import and export configurations, and more.
- : Download the plug-in.
- : Subscribe various types of alarms.
- : Set the language of the webpage.
- Restart: Click at the upper-right corner of the page, select **Restart**, and then the camera restarts.
- Logout: Click at the upper-right corner of the page, and then select **Logout** to go to the login page.

  The system will sleep automatically after idling for a period of time.
- Setting: Click at the upper-right corner of the page to set basic parameters.
- Product documentation: Click it, and then scan the QR code to get the user manual.

- Full screen: Click at the upper-right corner of the page to enter full screen mode; click it again to exit full screen mode.

5 Configuration Wizard

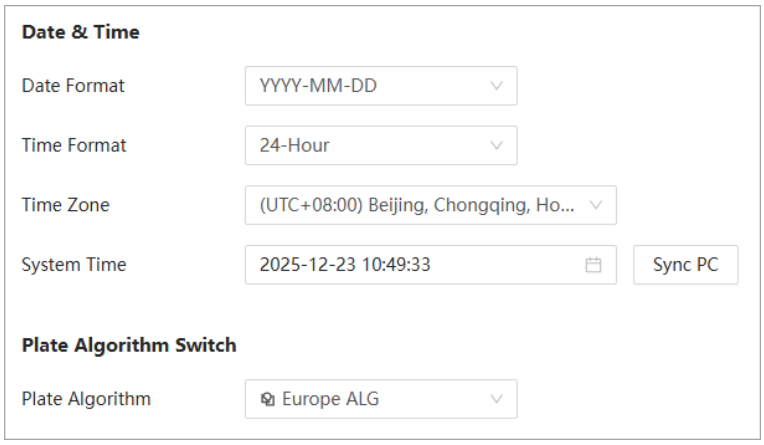
You can configure the scene for capture, and use various functions to help you with different installation scenarios.

You can click **Log out** at the upper-right corner to go back to the home page.

Procedure

Step 1 Click **Configuration Wizard**.

Figure 5-1 Configure wizard (1)



Step 2 Select the basic date and time format and system time of the camera, and then click **Next**.

- You can manually enter the time, or click **Sync PC** to synchronize time from the server.
- Select **Plate Algorithm** according to the region of your device. For the regions that are supported by each option, see the datasheet of your device.

Step 3 Click **Next** to configure the scene switch.

Figure 5-2 Configure wizard (2)

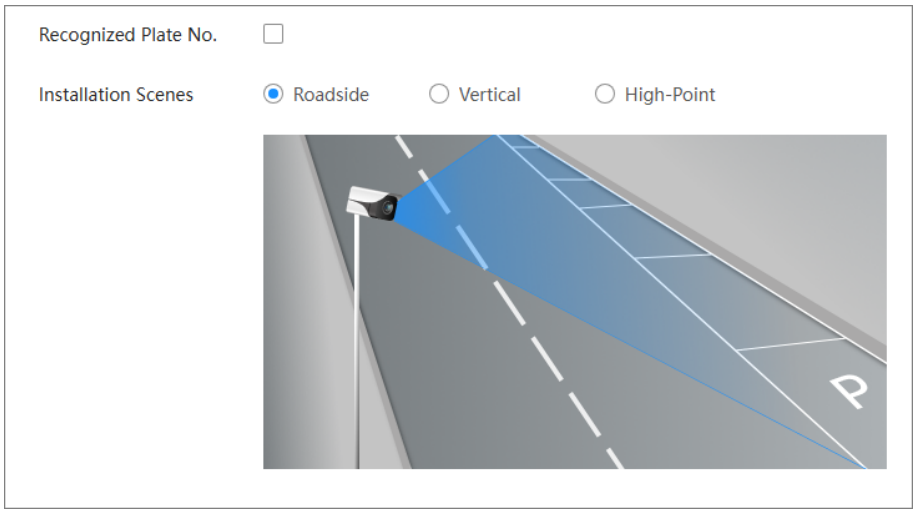


Table 5-1 Configure the scene switch

Parameter	Description
Recognized Plate No.	Select the **Recognized Plate No.** to recognize and detect the vehicle. The parking space mode is enabled by default.
Installation Scenes	• Roadside: Suitable for the parallel parking space. The camera is installed on the parallel or opposite side of the parking space. • Vertical: Suitable for monitoring large-scale parking space. The camera is installed above the front/rear of the vehicle. • High-Point: Suitable for vertical parking space or that with an inclination angle of less than 15°. The camera is installed on the front or rear side of the vehicle.

Step 4 Click **Next** , and then click **Go to Home Page**.

6 Live

This chapter introduces the layout of the page and function configuration.

6.1 Live Page

Log in to the device webpage, and then click **Live**.

The page might vary with different models.

Figure 6-1 Live Page

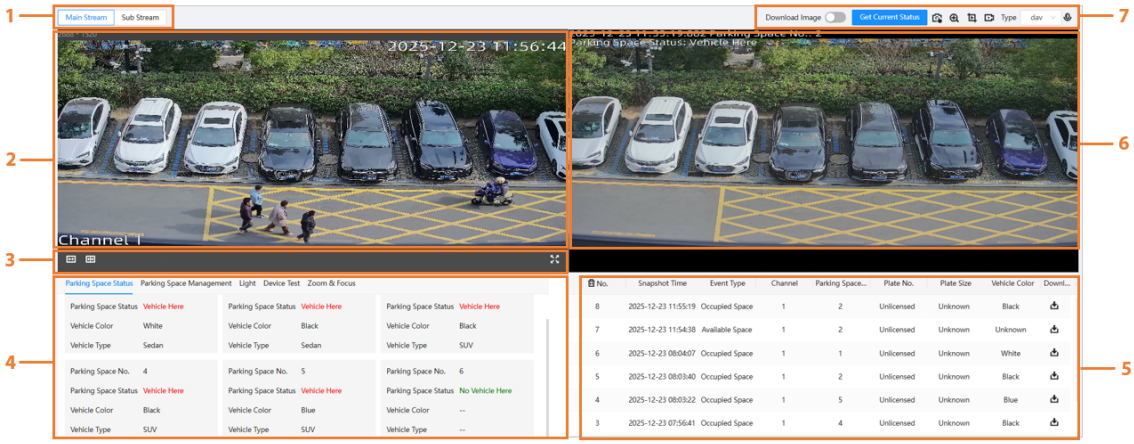


Table 6-1 Function description

No.	Function	Description
1	Display mode	The display modes include main stream and sub stream. You can select a video stream based on your network bandwidth. ● Main stream: Displays video with high resolution, but requires large bandwidth. This option can be used for storage and monitoring. ● Sub stream: Displays the video in lower resolution but smoothly. It requires less bandwidth. This option is normally used to replace main stream when the network bandwidth is not enough.
2	Live view	Displays real-time videos.
3	Video adjustment	Adjustment operations in live viewing.
4	Frequently used functions	It is a fast configuration page where you can properly configure the video image. These functions are frequently used when viewing live videos, such as adjusting the focus and zoom, and changing the configurations of license plate snapshots.
5	Snapshot details	Displays the details of the vehicle that is captured.
6	Snapshots	Displays vehicle snapshot, plate cutout, and plate number.

No.	Function	Description
7	Live view function bar	Displays functions and operations in live view.

6.2 Video Adjustment

Table 6-2 Description of adjustment bar

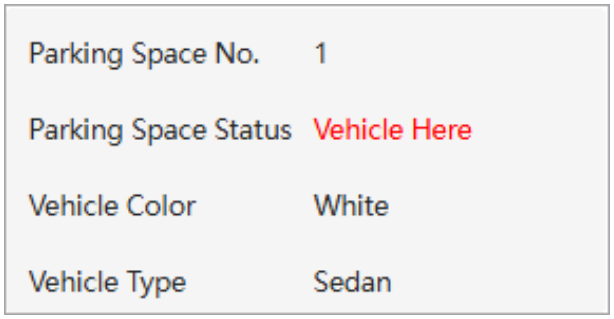
Icon	Function	Description
	W:H	Adjusts the display scale, that is, the ratio between the width and the height of the live video display. ● Original: Restores to the original display size. ● Adaptive: Maximizes the video to the full-screen display.
	Intelligent Track	Click the icon, and then the vehicle trajectory will be intelligently recognized and displayed.
	Full Screen	Displays the video in full-screen mode. Double-click or press **Esc** to exit full-screen mode.

6.3 Frequently Used Functions

6.3.1 Parking Space Status

Displays the parking space status, vehicle color, vehicle type, and more.

Figure 6-2 Parking Space Status



6.3.2 Parking Space Management

Supports adding parking spaces, detection lines, and more.

Procedure

Step 1 Click **Adding Parking Space**, and then the parking space will be displayed.

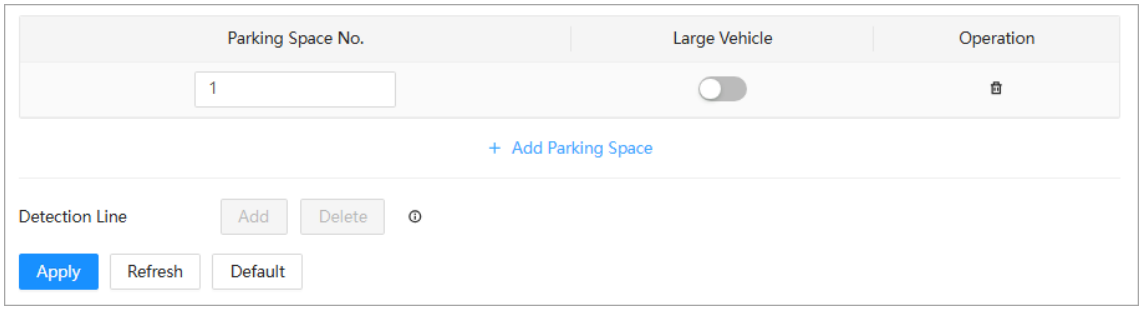
- Click to enable the large vehicle function.
- Click to delete the parking space added.

Step 2 Click **Add** or **Delete** to add or delete detection lines.

After **Parking Over Line** is enabled, you can add or delete the detection lines.

Step 3 Click **Apply**.

Figure 6-3 Parking space management



6.3.3 Light

Click **Light** to configure the working mode and brightness for the camera light.

Figure 6-4 Configure the light

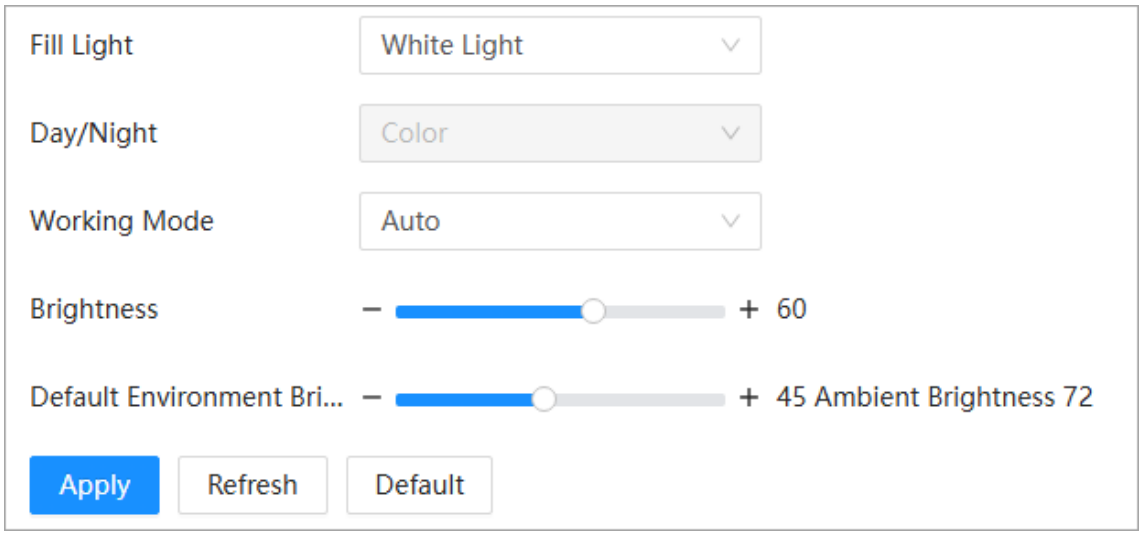


Table 6-3 Parameters description of the light

Parameter	Description
Fill Light	Select IR mode or white light as needed.
Day/Night	ICR Switch.
Working Mode	Select a working mode for the light as needed. ● **Always Off** : Select the mode when the device environment is relatively bright. ● **Always On** : Select the mode when the device environment is relatively dark. ● **Day/Night** : When you select the mode, the device will adjust the brightness based on the environment.

Parameter	Description
Brightness	The higher the value, the brighter the light.
Default Environment Brightness	Set a value for the brightness. When the environment brightness is higher or lower than the threshold, the ICR in the **Auto** mode will be automatically changed to the **Color** or **B/W** mode.

6.3.4 Device Test

Click **Device Test** to test if various functions of the camera are working properly, including capturing snapshots, screen display, and voice broadcast.

Figure 6-5 Configure the device test

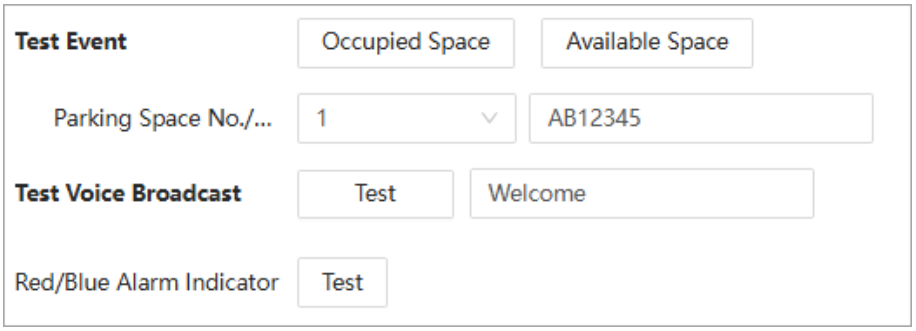


Table 6-4 Parameters description of device test

Parameter	Description
Test Event	Select the parking space No., enter a plate number, and then click **Occupied Space** or **Available Space** to test whether the camera responds correctly.
Test Voice Broadcast	Enter some information, and then click **Test** to check whether the device plays the sound normally.
Red/Blue Alarm Indicator	Click **Test** to check if the red/blue alarm indicator works normally.

6.3.5 Zoom and Focus

Click **Zoom & Focus** to adjust the focal length to zoom in or out on the video; by adjusting the focus manually or automatically or on an area, you can change the video clarity.

The focus will be adjusted automatically after you zoom in or out.

Figure 6-6 Zoom and focus

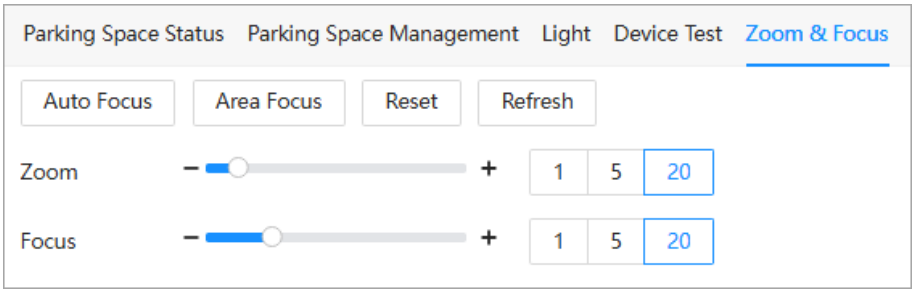


Table 6-5 Parameters description of zoom and focus

Parameter	Description
Auto Focus	Adjusts video clarity automatically. Do not make any other operation during auto focus process.
Area Focus	Click it to enable the function, and draw an area on the window. The area will then be focused automatically.
Reset	Reset all focus and zoom parameters to the default settings. You can reset the focus and zoom if the video is not clear or has been zoomed in or out too frequently.
Refresh	Update the page content.
Zoom	Zoom in or out on the video. 1. Select the speed. The larger the value is, the more the camera will zoom in or out on every click. 2. Click or hold + or –, or drag the slider to zoom in or out.
Focus	Adjusts the optical back focal length to make the image clearer. 1. Select the speed. The larger the value is, the more the camera will adjust the focus on every click. 2. Click or hold + or –, or drag the slider to adjust the focus.

6.4 Live View Function Bar

For the live view function bar, see Table 6-6 .

Table 6-6 Function description

Icon	Description
Download Image	When enabled, the snapshots will be automatically downloaded to the storage path defined in the browser. It is not enabled by default.
	Click it, and then the camera will take 1 snapshot.

Icon	Description
	Use this function to zoom in on any area of the video. Click this icon, and then click and hold to select an area on the video. The camera will zoom in on the area you selected.
	Click it to take 1 snapshot from the video, and then you can acquire a snapshot of bmp format. You can check the quality of the video by viewing the snapshot.
	Click it to start recording. Click it again to save the recording to your local computer.
Type dav	Select the format of the recording.
	Click it, and then you can talk to the people near the camera. Click it again to stop talking.

7 ANPR

7.1 Parking Space Management

Supports configuring scene switch, parking space management, and illegal parking area.

7.1.1 Configuring Scene Switch

Supports configuring recognition mode, installation scenes, and more. For details, see "5 Configuration Wizard".

7.1.2 Configuring Parking Space Management

Supports configuring rules for detecting occupied and available parking spaces.

Procedure

Step 1 On the home page, click **ANPR** > **Parking Space Management**, and then select **Parking Space Management**.

Step 2 Click **Add Parking Space**, and then it will display the parking space detection area on the video image automatically.

- In roadside or vertical installation scenes, you can draw up to 4 parking areas and 2 illegal parking areas, and add up to 6 parking spaces.
- In high-point installation scenes, you can draw up to 4 parking areas and 2 illegal parking areas, and add up to 50 parking spaces in total.
  - Select **Area** in the **Counting Mode** box, and then press and hold the left mouse button and drag the mouse pointer to draw the area.
  - Select **Parking Space** in the **Counting Mode** box, click the left mouse button to add the parking space.

Step 3 Configure the AI event.

After configuring the AI event, the camera will detect occupied or available parking space when the parking space is occupied or available after the defined check time.

Step 4 Click **Add** or **Delete** to add or delete detection lines.

Figure 7-1 Configure parking space management

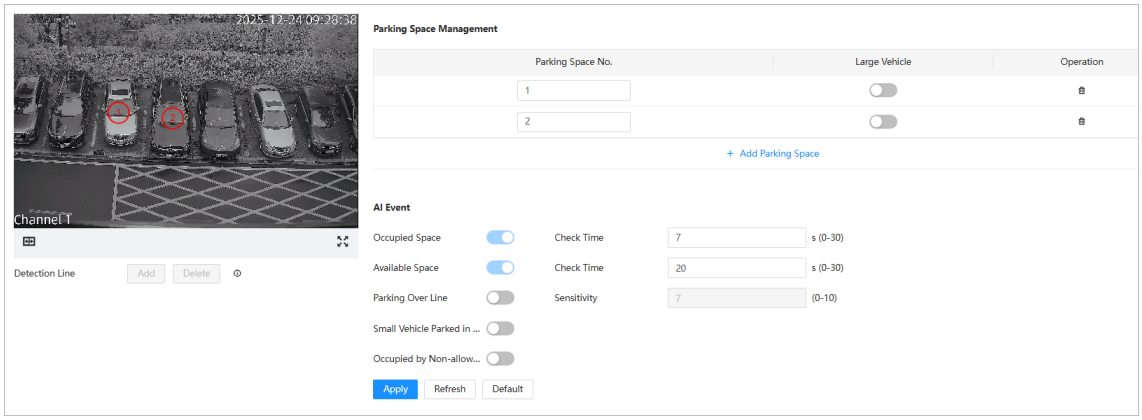


Table 7-1 Parameters description of the parking space management

Parameter	Description
Parking Space No.	The parking space number is filled in automatically after you add the parking space. You can also modify it as needed.
Large Vehicle	Enable the button, and then the camera will recognize the large vehicle entering the parking space.
Operation	Click to delete the parking space added.
Occupied Space	The function is enabled by default. You cannot turn off it. A snapshot is triggered when a vehicle is detected in the parking space.
Available Space	A snapshot is triggered when no vehicle is detected in the parking space.
Check Time	A snapshot is triggered at set time intervals.
Sensitivity	The higher the sensitivity value, the longer the detection snapshot time and the higher the detection stability.
Parking Over Line	Click to enable the function. A snapshot is triggered when a vehicle is detected over the parking line.
Small Vehicle Parked in Large Vehicle's Space	Click to enable the function. A snapshot is triggered when a small vehicle parking in large vehicle's space is detected.
Occupied by Non-allowlist Vehicle	Click to enable the function. A snapshot is triggered when a parking space is occupied by non-allowlist vehicle.
Detection Line	After **Parking Over Line** is enabled, you can add or delete the detection lines.

Step 5 Click **Apply**.

7.1.3 Configuring Illegal Parking Area

Supports configuring rules for detecting illegal parking, and the alarm linkage actions when illegal parking is detected.

Procedure

Step 1 On the home page, click **ANPR** > **Parking Space Management**, and then select **Illegal Parking Area**.

Step 2 Click to enable the function.

Step 3 Click **Illegal Parking Area**, and then draw the area that detects illegal parking on the video image (right-click to finish drawing).

The area name is filled in automatically. You can also modify it as needed.

You can draw up to 2 illegal parking areas.

Step 4 Configure the parameters.

Figure 7-2 Configure illegal parking area

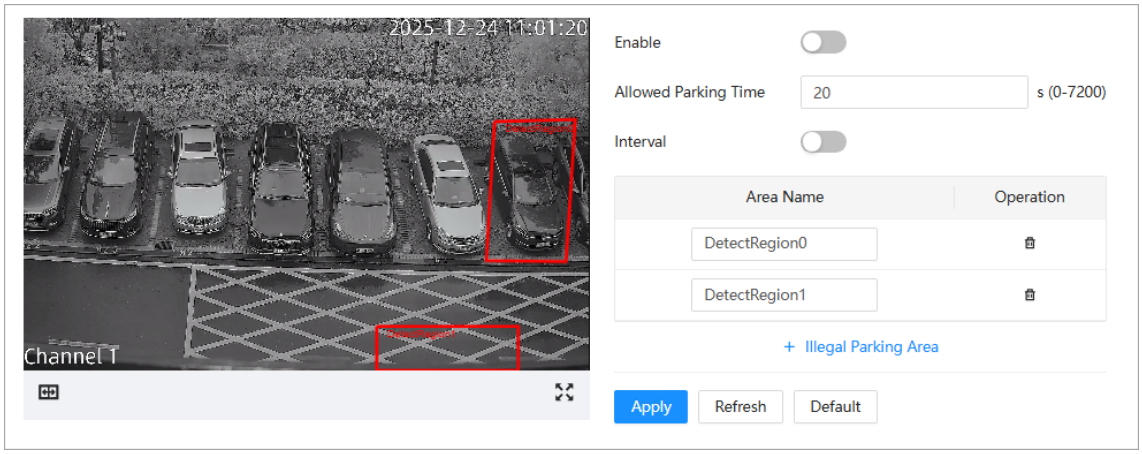


Table 7-2 Parameters description of Illegal parking area

Parameter	Description
Allowed Parking Time	Vehicles will not be detected as illegal parking within the allowed parking time.
Interval	Click to enable the function, and then set the time interval.
Area Name	Supports customizing and the area name

Step 5 Click **Apply**.

7.2 Configuring AI Settings

Supports configuring scene detection threshold, AI attribute settings, and more.

Procedure

Step 1 On the home page, click **ANPR** > **AI Settings**.

Step 2 Configure the parameters.

Figure 7-3 Configure AI Settings

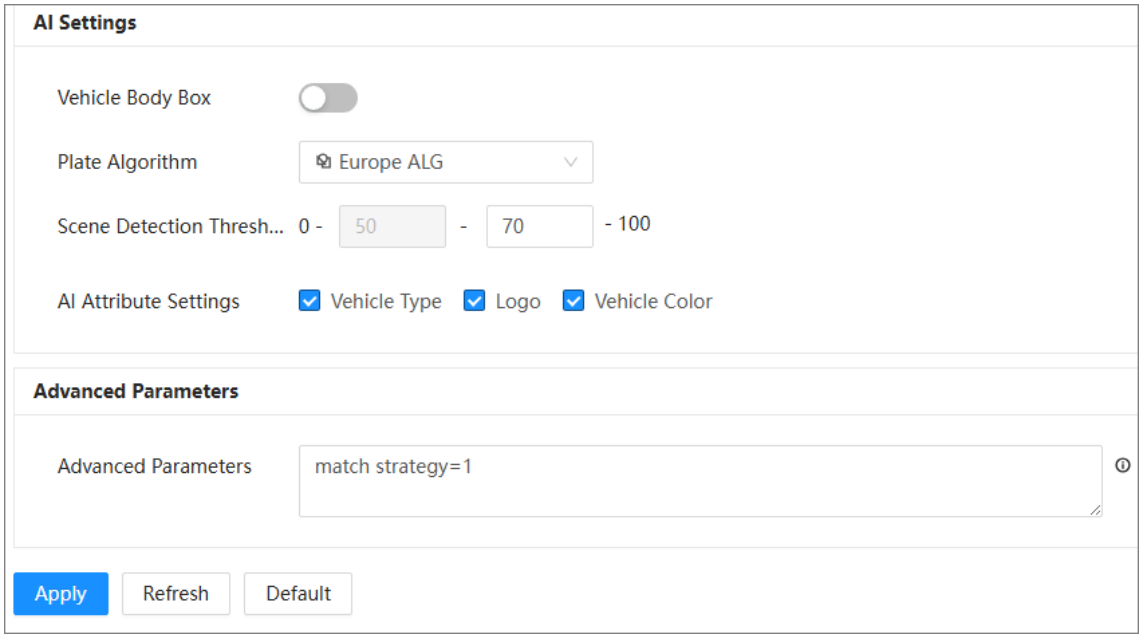


Table 7-3 Parameter description of the AI settings

Parameter	Description
Vehicle Body Box	Enable the function to mark the vehicle body.
Plate Algorithm	Select an algorithm according to your location. It can be divided into two categories: a collection of algorithms that includes multiple regions, such as the Middle East collection, and a country-specific algorithm that specifically recognizes certain countries, like Indonesia.
Scene Detection Threshold	Set the confidence level conditions for vehicle detection. The higher the value, the higher the detection sensitivity. You can set the minimum value to 50.
AI Attribute Settings	Select vehicle type, logo, and vehicle color as needed. A snapshot is triggered based on the AI attribute settings.
Advanced Parameters	Configure advanced vehicle recognition function through algorithm. Click ⓘ to view the advanced algorithm formula.

Step 3 Click **Apply**.

7.3 Image Configuration

Set the overlapping OSD (On-screen Display) information on images.

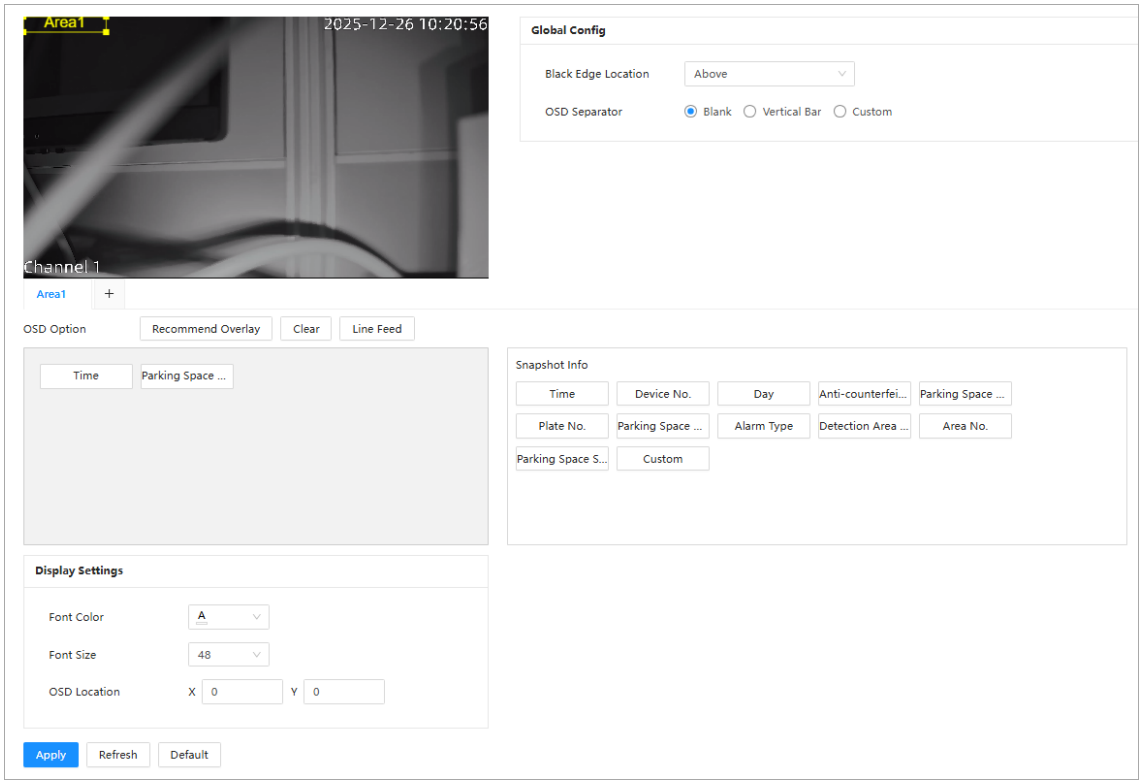
7.3.1 Original Picture OSD

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

Procedure

Step 1 On the home page, click **ANPR**, and then select **Image Config** > **Original Picture OSD**.

Figure 7-4 Original picture OSD



Step 2 Select the location of the black edge.

You can put the OSD information on the black bar to display it clearly.

- **Above** : A black bar will be generated on the top on snapshots.
- **Below** : A black bar will be generated on the bottom on snapshots.
- **None** : There will be no black bar on snapshots.

Step 3 Configure the 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 "2025-09-22|A12345".

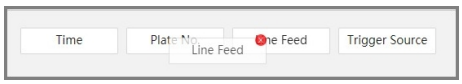
Step 4 Configure the OSD information to be displayed.

1. Click a type of information in **Snapshot Info** to add it to the **OSD Option** section.

   - Click **Recommend Overlay** and then the camera will automatically add various types of information.
   - To delete any type of information, 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.

2. Drag to adjust the order of information.

Figure 7-5 Adjust the order



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

Table 7-4 Parameters description of original picture OSD

Parameter	Description
With ms	Select whether to display millisecond. This parameter is only available for **Time**.
Prefix	The information to be overlaid before the type of information that you are configuring. For example, a prefix "Time of trigger:" for **Time** can be "Time of trigger: 2025-09-23 09:58:41".
Suffix	The information to be displayed after the type of information that you are configuring. For example, a suffix "Time of trigger" for **Time** can be "2025-09-23 09:58:41 Time of trigger".
Contents	Enter the fixed content that will be overlaid on each snapshot. This parameter is only available for **Location** and **Custom**.
Delimiter Quantity	Select the number of separators to separate the information that you are configuring with other types. For example, select the quantity to 5 when the OSD separator is set to **Blank** : 2025-09-23 09:35:06.840 AB12345 Vehicle.

Step 5 Configure the font color and size.

Step 6 Adjust the position where you want to overlay the OSD information by entering the coordinates next to **OSD Location** or dragging it on the video.

If you have configured the black bar, adjust the position so that the OSD information will be displayed on the black bar to display it clearly.

Step 7 Click **Apply**.

7.3.2 Size

Configure the quality of snapshots.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Image Config** > **Size**.

Step 2 Configure the parameters.

- **Resolution** : This parameter cannot be configured.
- **Control Mode** : Select a mode to control the quality of snapshots.
- **Quality** : When setting the control mode to **Quality**, configure the quality of snapshots. The higher the value, the better quality the snapshots will be.
- **Size** : When setting the control mode to **Size**, configure the size of snapshots. The higher the value, the larger the snapshots will be.

Step 3 Click **Apply**.

7.4 Configuring Allowlist

7.4.1 Fuzzy Matching

When comparing the actual plate numbers to those in the allowlist for barrier control, this function 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 On the home page, click **ANPR**, and then select **Allowlist** > **Fuzzy Matching**.

Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 7-5 Parameters description of fuzzy match

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	
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, with **Number of characters allowed to be misread** also being not enabled.
The system matches similar characters to be the same	This parameter allows the camera to misread certain characters as other ones. You can add up to 6 rules. For example, a 0<->D rule allows the barrier to open if the camera recognizes A0123 to AD123, or vice versa.

Step 4 Click **Apply**.

7.4.2 Allowlist

Supports searching for and exporting the allowlist, and adding vehicles.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Vehicle Blocklist/Allowlist** > **Allowlist**.

Step 2 Add vehicles.

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

Figure 7-6 Add a vehicle to the allowlist

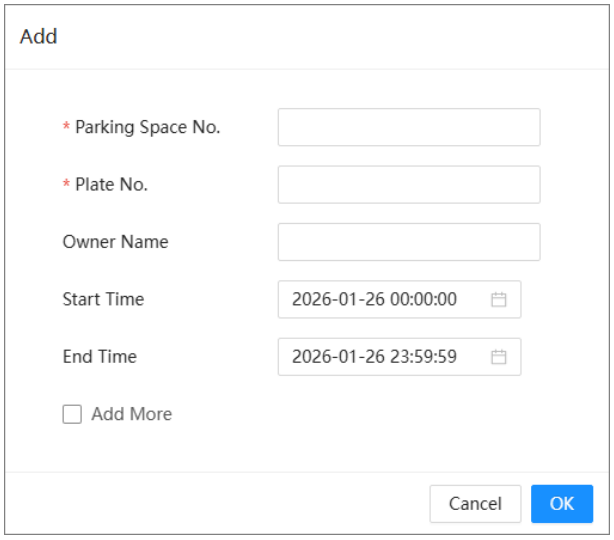


Table 7-6 Parameters description of allowlist

Parameter	Description
Parking Space No.	Select the parking space number.
Plate No.	Enter the plate number of the vehicle.
Owner Name	Enter the name of owner of the vehicle.
Vehicle Color	Select the vehicle color.
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	
Add More	Select the checkbox, and then you can continue add another vehicle after you click **OK**.

- Add them in batches.
  1. Click **Import**.
  2. Click **Download Template**, and then save the template to your computer.
  3. Enter the information of the vehicles in the template.
  4. Click **Select File** , select the template, and then click **Open**.

     All the vehicles are imported to the allowlist.

Step 3 (Optional) Search the allowlist.

1. Select the parking space no. and the status of the allowlist.
2. Enter the plate number.
3. Click **Search**, and then the allowlist will be displayed.

Related Operations

- Export information of vehicles on the allowlist: Click **Export** , select enabling or disabling encryption, and then click **OK**.
- 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 vehicles in batches: Click **Clear** to delete all the vehicles from the allowlist. Please be advised that this operation cannot be undone.
- 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.

7.5 Configuring Warning Lights

Supports configuring the events including parking over line, occupied by non-allowlist vehicle, and more.

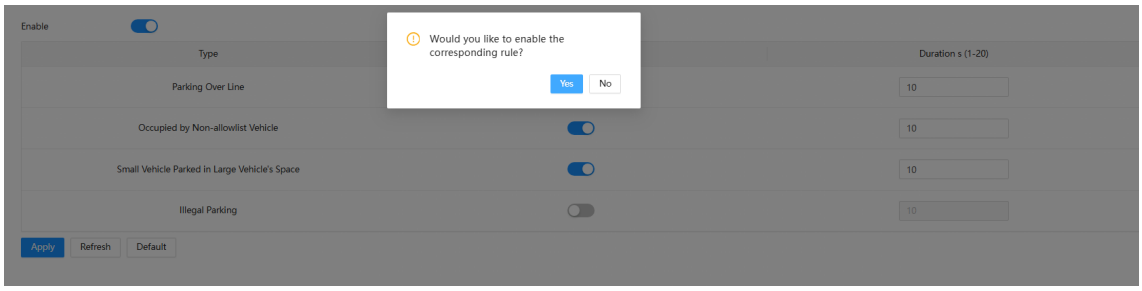
Procedure

Step 1 Click to enable the function.

Step 2 Enable the event type as needed, and then click **Yes** in the pop-up dialog.

Step 3 Set the duration for the event type.

Figure 7-7 Configure warning lights



Step 4 Click **Apply**.

7.6 Configuring Audio Broadcast

You can configure the broadcast content for when vehicles pass, and the volume and video encoding settings for the broadcast.

7.6.1 Event Broadcast

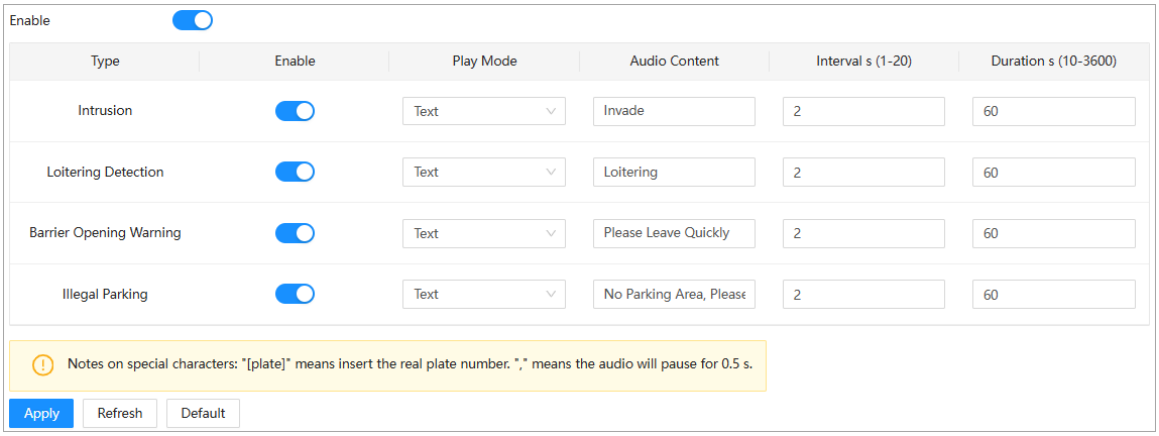
Configure the event broadcast settings. The camera will broadcast the customized content when specific events occur.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Audio Broadcast** > **Event Broadcast Settings**.

Step 2 Click to enable the function.

Figure 7-8 Broadcast content



Step 3 Click to enable the event types.

Step 4 Configure the play mode, including **Text** and **File**.

- **Text**: You can customize the audio content by entering text in **Audio Content**.
- **File**: The audio files uploaded will be played.

Select **ANPR** > **Audio Broadcast** > **Audio File** to upload audio files. For details, see "7.6.3 Audio File".

Step 5 Configure the play time, including **Interval s** and **Duration s**.

- **Intervals**: Set an interval at which an audio should be played, with a scale from 1 to 20 seconds.
- **Durations**: Enter the audio playback time, with a scale from 10 to 3600 seconds.

Step 6 Click **Apply**.

7.6.2 Volume/Encoding

Configure the volume for voice broadcast.

This function is only available on select models.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Audio Broadcast** > **Volume/Encoding Settings**.

Step 2 Configure the parameters.

Table 7-7 Parameters description of volume/encoding

Parameter	Description
Input Volume	The volume of the sound received by the camera.
Output Volume	The volume of the voice broadcast.
Voice Speed	The speed for the voice broadcast. You can select the speed from fast, medium, and low as needed.

Step 3 Click **Apply**.

7.6.3 Audio File

Upload audio files for broadcast content.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Audio Broadcast** > **Audio File**.

Step 2 Click **Upload** to upload files according to the on-screen requirements.

Related Operations

- Click to play the audio.
- Click to download the audio.
- Click to delete the audio file. Default files cannot be deleted.

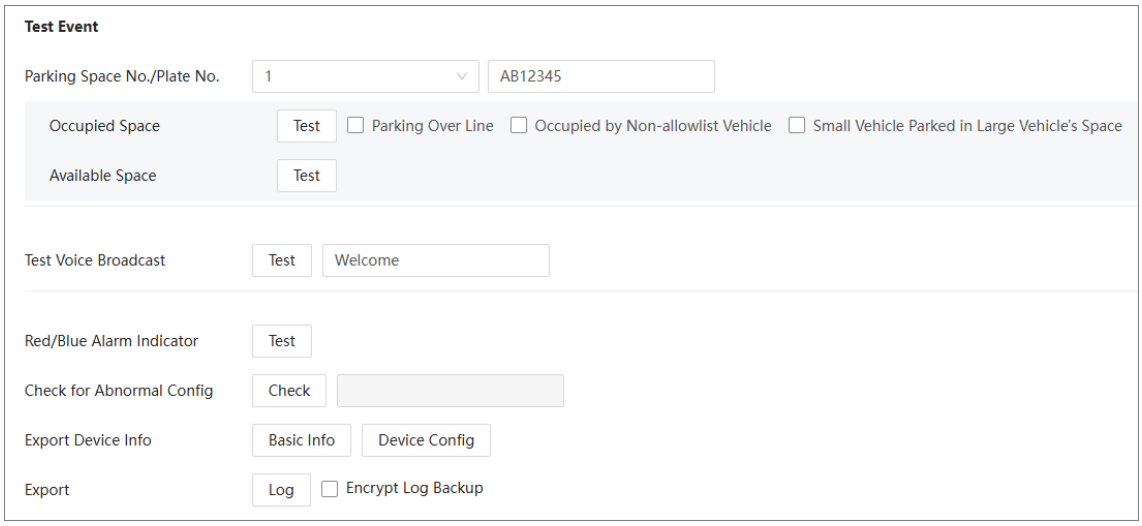
7.7 Setting Device Test

You can test the capture mode, voice broadcast, and abnormal configuration modules to see if they work as configured. You can also export related device information.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Device Test** .

Figure 7-9 Device test



Step 2 Test if different functions are working normally.

Table 7-8 Parameters description of device test

Parameter	Description
Parking Space No./Plate No.	Select the parking space number and then enter the plate number.
Occupied Space	Click **Test** to detect the occupied space. Supports the events of parking over line, occupied by non-allowlist vehicle, and small vehicle parked in large vehicle's space.
Available Space	Click **Test** to detect the available space.

Parameter	Description
Test Voice Broadcast	Enter some information as needed, and then click **Test** to check whether the device plays the sound normally. Voice broadcast is only available on select models.
Red/Blue Alarm Indicator	Click **Test** to check whether the red/blue alarm indicator performs normally.
Check for Abnormal Config	Click **Check**, and then the system will check abnormality automatically.
Export Device Info	Select the information of the device, and then export it in batches.
Export	Export logs to your computer. Select **Encrypt Log Backup**, and then configure the password to secure the logs. You need the password to access the logs.

8 Picture

You can search for snapshots, select the storage method, and then configure the parameters of uploading.

8.1 Image Search

Prerequisites

Insert the SD card and complete the initialization.

Procedure

Step 1 On the home page, click **Picture** , and then select **Memory Card Image**.

Step 2 Configure the parameters.

Figure 8-1 Picture search

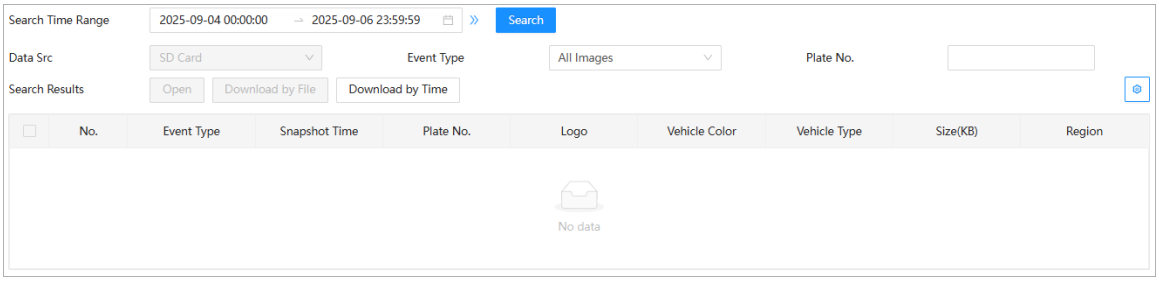


Table 8-1 Parameter descriptions of picture search

Parameter	Description
Search Time Range	Set the start time and end time for image search.
Event Type	Select the event type that you want to search for. The default setting is **All Images.**
Plate No.	Enter the plate number to search for images as required. Supports fuzzy search by entering keywords of the plate number.

Step 3 Click **Apply**.

The search results will be displayed.

Related Operations

Function	Operation
Open the picture	Select the picture that you want to open from the search results, and then click **Open** or double-click the selected picture. You can select multiple pictures, and then click **Open** to open all of them.

Function	Operation
Download by File	Select one or multiple results from the list, click **Download by File** , and then click **Browse** to select the save path. The system will download the selected results to your local computer.
Download by Time	Set the start time and end time, click **Download by Time** , and then click **Browse** to select the save path. The system will download all pictures during the set period to your local computer.

8.2 Storage

Configure the storage method of pictures, including local storage and network storage.

8.2.1 Local

Configure local storage parameters.

Procedure

Step 1 On the home page, click **Picture** , and then select **Storage**.

Step 2 Set the following operations for **Disk Full**.

- **Overwrite** (default): When the disk is full, the earliest local storage information will be overwritten.
- **Stop** : When the disk is full, local storage will be halted.

Step 3 Select **Local Storage** from **Storage Method**.

Step 4 Click **Apply**.

8.2.2 Network

When there is a network disconnection or failure, all snapshots can be automatically stored to the local SD card.

When testing the FTP, do not use the login IP address as the FTP address if there is no available plug-in.

Procedure

Step 1 On the home page, click **Picture** , and then select **Storage**.

Step 2 Select **Network Storage** from **Storage Method**.

Step 3 Configure the parameters.

Figure 8-2 Configure network storage

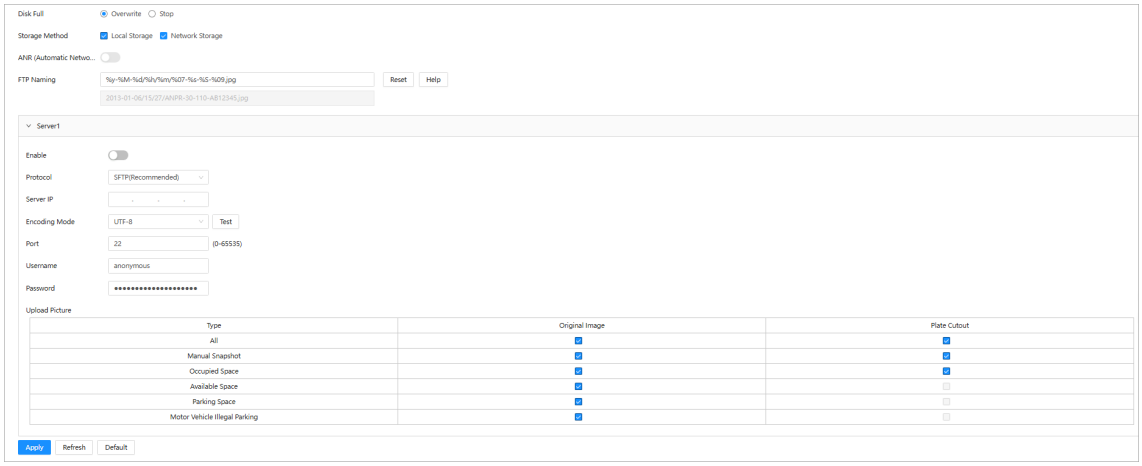


Table 8-2 Parameters description of FTP

Parameter		Description
ANR (Automatic Network Recovery)		Click to enable the function. After it is enabled, snapshots can be automatically stored to the local SD card when network disconnection or failure occur, and automatically stored to the FTP server when the network is recovered. You must enable the FTP first; otherwise, the ANR cannot be enabled.
FTP Naming		Set a name for the picture. ● Click **Reset** to rename the picture. ● Click **Help** to check for the naming rule.
Server	Enable	Click to enable the FTP. Enabling the FTP might involve risks; please be advised. We recommend selecting SFTP for data security.
	Protocol	Select the type of protocol, including **FTP** and **SFTP**. SFTP is recommended.
	Server IP	The IP address of the server.
	Encoding Mode	The default setting is UTF-8.
	Port	The port of the server.
	Username	The user name and password of the server.
	Password	
	Upload Picture	Upload pictures with different event types to the FTP server.

Step 4 Click **Apply**.

8.3 Platform Server

You can configure the parameters to automatically or manually upload snapshots in the local SD card to the platform server.

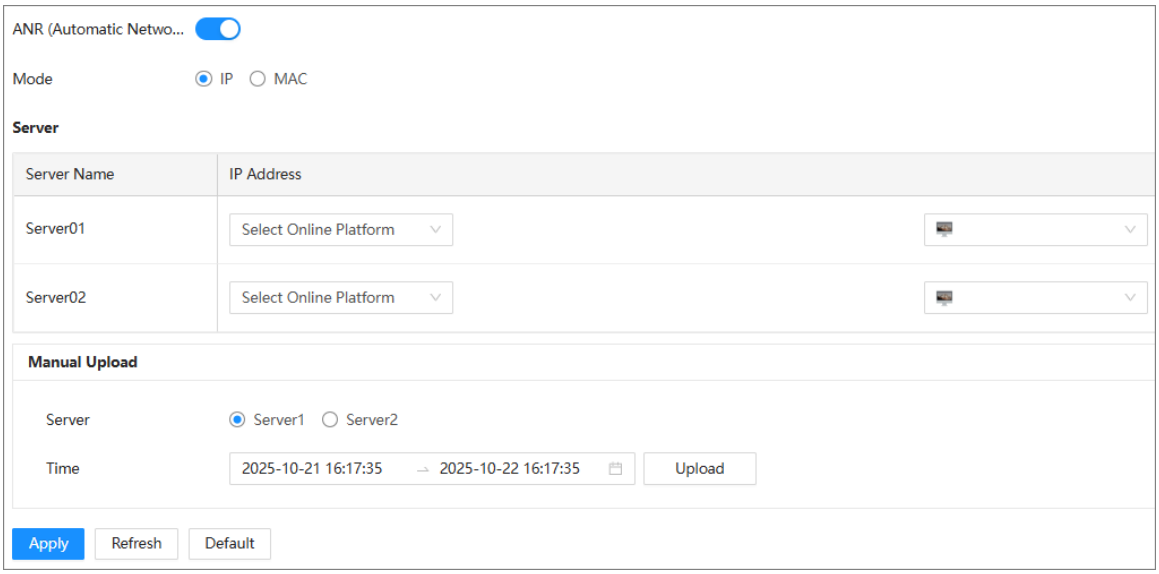
Procedure

Step 1 On the home page, click **Picture** , and then select **Platform Server**.

Step 2 Click to enable the ANR function.

Step 3 Upload snapshots automatically or manually.

Figure 8-3 Configure platform server



- Automatically
  1. Select **IP** or **MAC** as required.
  2. Select a server. You can click **Select Online Platform** , and then select a server, or click **Manually Enter**, and then enter the IP address or MAC address of the server.
  3. Click **Apply**.
- Manually
  1. Select a server for snapshots uploading.
  2. Set the start time and end time.
  3. Click **Upload** to upload snapshots during the defined time period.
  4. Click **Apply**.

9 Record

You can search and play back recorded videos, set recording schedule, and select recording strategy and storage method.

9.1 Video Search

You can search for the information of recordings and plate number in the SD card.

Prerequisites

Insert and initialize the SD card.

Procedure

Step 1 On the home page, click **Record** , and then select **Search Video**.

Step 2 Configure the parameters.

Figure 9-1 Configure video

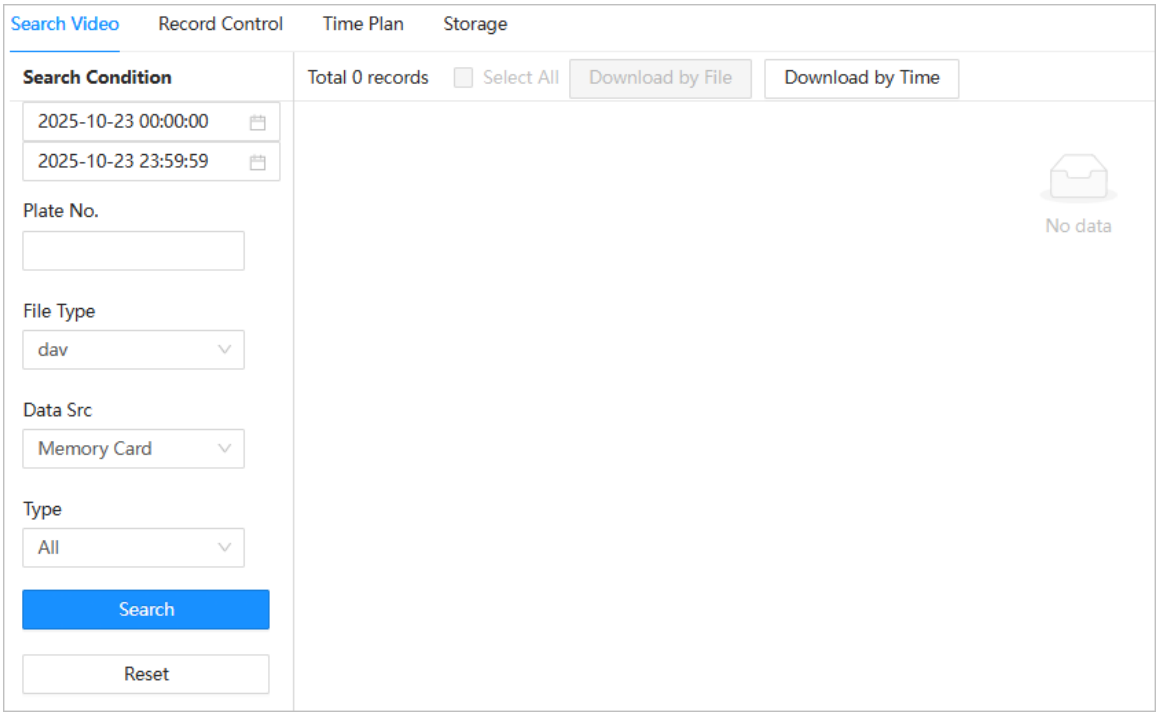


Table 9-1 Parameters description of video

Parameter	Description
Search Condition	Set the start time and end time for video recordings search.
Plate No.	Enter the plate number to search for videos as required. Supports fuzzy search by entering keywords of the plate number.
File Type	It is .dav by default, and cannot be modified.
Data Src	It is memory card by default, and cannot be modified.

Parameter	Description
Type	• **ALL** : Search for all recordings. • **Event** : Search for recordings triggered by specific events • **Alarm** : Search for recordings triggered by alarms. • **Manual** : Search for recordings within the time set by the user.

Step 3 Click **Search** to search for all recordings that meet the search conditions.

Related Operations

Download by Time : Select a file from the list, click **Download by Time**, and then click **Browser** to select the save path.

9.2 Record Control

You can set max duration, pre-record time, record mode, and record stream.

Prerequisites

Make sure that the SD card is authenticated prior to use

Procedure

Step 1 On the home page, click **Record** , and then select **Record Control**.

Step 2 Configure the parameters.

Table 9-2 Parameters description of record control

Parameter	Description
Max Duration	The duration of the recording file.
Pre-Record	When an alarm occurs, the system saves recordings between the set time and the alarm to the recording file. If the value is set to 5 seconds, recordings of 5 seconds before the alarm will be stored in the recording file.
Record Mode	• **Auto** : The system records during the set recording time. • **Manual** : The system starts to record following the configuration. • **Close** : No recording action.
Record Stream	The stream for recording, including main stream and sub stream.

Step 3 Click **Apply**.

9.3 Time Plan

Set the time plan of event recording and alarm recording.

Background Information

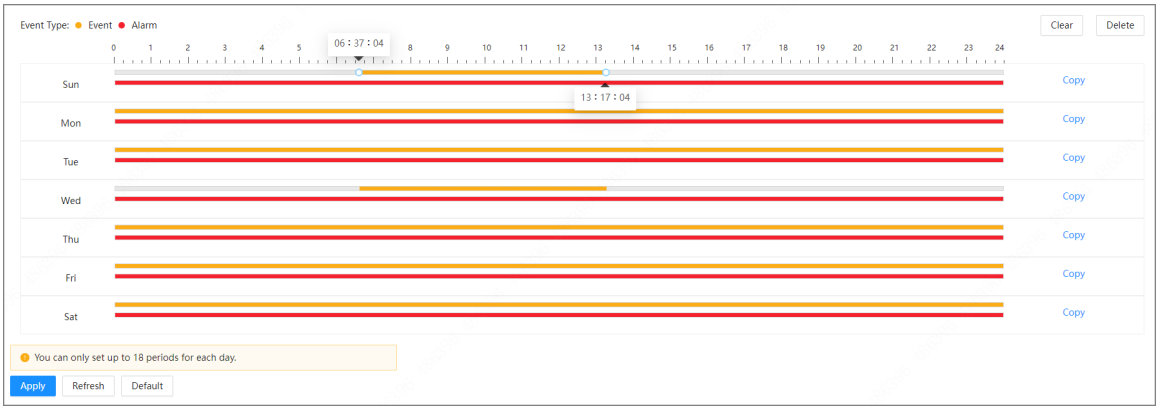
The system starts recording when an event or alarm is triggered within the scheduled time; and do not record beyond the schedule no matter what happens.

Procedure

Step 1 On the home page, click **Record** , and then select **Time Plan**.

Step 2 Set the time plan for recording.

Figure 9-2 Configure time plan



1. Click and drag the timeline to adjust the time period.
   - Yellow: event recording.
   - Red: alarm recording.
2. Enter the start time and end time in the text box.
3. Click **Copy** , select a day, and then click **Apply** to copy the current schedule to the selected day.

Related Operations

- Click **Clear** to delete all time plans.
- Click **Refresh** to restore the default time plan.
- Click a time line, and then click **Delete** to delete it.

9.4 Storage

Set the recording strategy and storage method for alarms and events when the disk is full.

Procedure

Step 1 On the home page, click **Record** , and then select **Storage**.

Step 2 Configure the parameters.

Figure 9-3 Storage

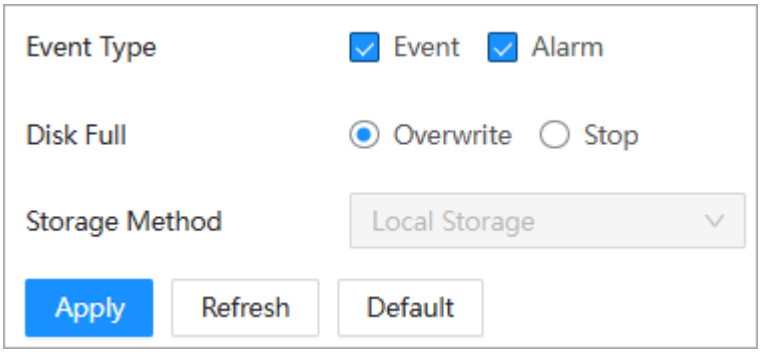


Table 9-3 Parameters description of storage

Parameter	Description
Event Type	Includes **Event** and **Alarm**.

Parameter	Description
Disk Full	The recording strategy when the disk is full. ● **Overwrite** : Cover the early recording file when the disk if full. ● **Stop** : Stop recording when the disk is full.
Storage Method	**Local Storage** is set by default and cannot be changed.

Step 3 Click **Apply**.

10 Search

You can search for snapshots, logs on snapshots, and alarm output logs.

10.1 Snapshot Records

Search for the snapshot records within the defined period. The camera can store up to 110,000 records when no memory card is installed.

Procedure

Step 1 On the home page, click **Search**, and then select **Snapshot Records** .

Step 2 Configure the search conditions.

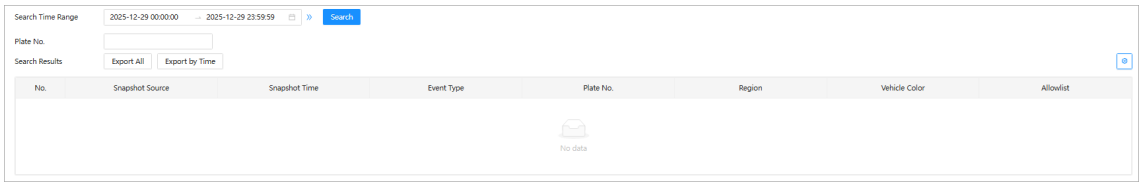
- **Search Time Range** : The camera will only search for records taken within this range.
- (Optional) **Plate No.** : If you enter a plate number, the camera will only search for records related to this plate number.

Step 3 Click **Search**, and then camera displays the results.

There are 3 types of reports: **Passed Vehicles Report** , **Report for Passed Vehicles in Allowlist**, and **Approaching and Departing Vehicles Report**.

Step 4 (Optional) Click **Export All** or **Export by Time** to export all results or the searched results based on the conditions to your computer.

Figure 10-1 Configure network storage



10.2 Parking Record

Set the search conditions to search for parking records.

10.2.1 Configuring Parking Records

Procedure

Step 1 On the home page, click **Search** , and then select **Parking Records**.

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

- **Search Time Range** : The camera will only search for records taken within this range.
- **Parking Space No.** : You can search the parking record through the parking number. The default setting is **All**.
- **Event Type** : You can search the parking records thought the event type. The default setting is **All**.

Step 3 (Optional) Click **Export All** or **Export by Time** to export all results or the searched results based on the conditions to your computer.

10.2.2 Sending Email

The scheduled email notification is supported when there is a parking record. You can configure the parameters to enable this function as required.

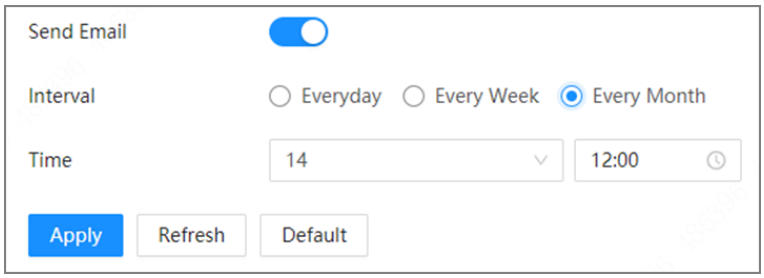
Procedure

Step 1 On the home page, click **Search**, and then select **Parking Records** .

Step 2 Enable **Send Email**, and then configure the parameters.

- **Interval** : The interval of email notification, including everyday, every week, and every month.
- **Time** : The specific time of email notification.

Figure 10-2 Email configuration



Step 3 Click **Apply**.

10.3 Alarm Records

Set the search conditions to search for alarm output.

Procedure

Step 1 On the home page, click **Search** , and then select **Alarm Records**.

Step 2 Configure the time range, and then click **Search**.

- **Search Time Range** : The camera will only search for records taken within this range.
- **Parking Space No.** : You can search the parking record through the parking number. The default setting is **All**.
- **Event Type** : You can search the parking records thought the event type. The default setting is **All**.

Step 3 (Optional) Click **Export All** or **Export by Time** to export all results or the searched results based on the conditions to your computer.

10.4 Picture Query

Verify if the watermarks on the snapshots stored on your computer are tampered.

Background Information

The image can only be in .jpg format.

Procedure

Step 1 On the home page, click **Search** , and then select **Picture Query**.

Step 2 Click **Browse**, and select the folder where the snapshots are stored.

Step 3 Select a snapshot which needs to be verified, and then click **Open**.

Double-click a snapshot to view it.

Step 4 Click **Watermark** . The camera starts verifying whether the snapshot has watermark and displays the results on the list under **Watermark**.

10.5 Searching Video

10.5.1 Record

You can play videos that are stored on your computer.

Procedure

Step 1 On the home page, click **Search**, and then select **Search Video** > **Record**.

Step 2 Click **Select File**, and then open a video stored on your computer.

You can now play the video directly on this page.

10.5.2 Watermark

You can verify whether the watermarks of local recordings are tampered.

Prerequisites

On the home page, click **Camera** , and then select **Encode** > **Video Stream**, enable **Watermark**, and then set the corresponding **Watermark String**. The default character is DigitalCCTV.

Procedure

Step 1 On the home page, click **Search**, and then select **Search Video** > **Watermark**.

Step 2 Click **Select File**, and then open a file that you want to verify.

Step 3 Click **Watermark**.

The camera displays the result under **Watermark Info**.

11 Camera

This section introduces the camera setting, including image and encoder parameters.

The parameters might vary with different models.

11.1 Setting Image Parameters

Configure image parameters according to the actual situation, including image, exposure, backlight, white balance, day/night, and light.

11.1.1 General Parameters

Supports configuring parameters such as image brightness, contrast, saturation, and hue.

Procedure

Step 1 On the home page, click **Camera**, and then select **Image** > **General**.

You can also select > **Camera** > **Image** > **General**.

Step 2 Configure the parameters.

Figure 11-1 Configure General

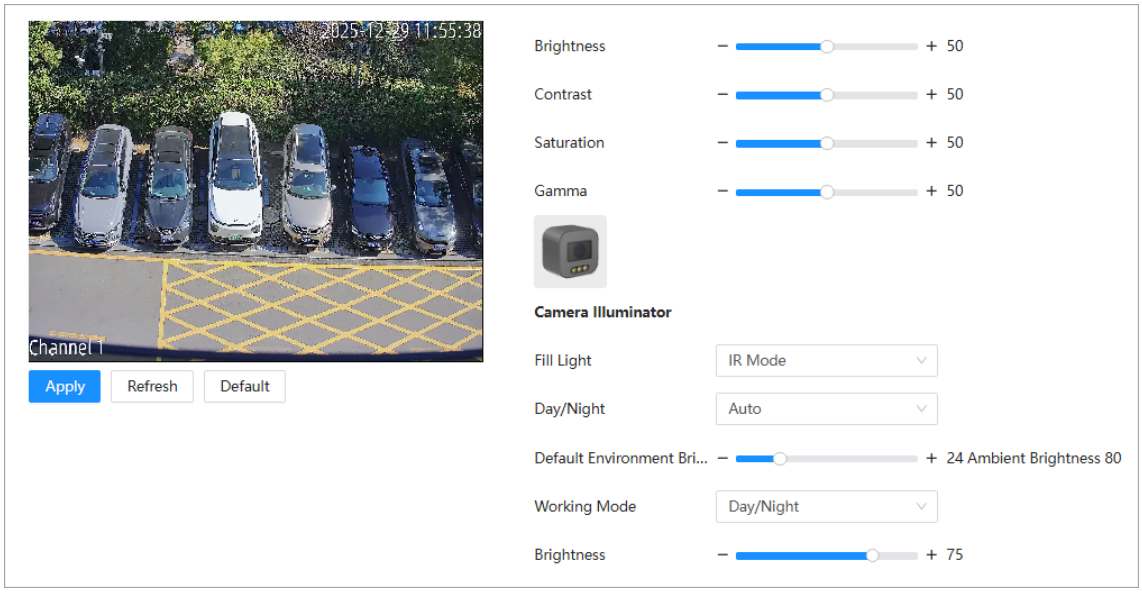


Table 11-1 Parameters description of general

Parameter		Description
Brightness		Adjust the overall image brightness. Change the value when the image is too bright or too dark. The bright and dark areas will have equal changes. The image becomes blurry when the value is too high. The recommended value is from 40 to 60. The range is from 0 to 100. It is 50 by default. The higher the value is, the brighter the image becomes.
Contrast		Change the value when the image brightness is proper but contrast is not enough. ● If the value is too high, the dark area is likely to become darker, and the bright area is likely to be overexposed. ● The picture might be blurry if the value is set too low. The recommended value is from 40 to 60, and the range is from 0 to 100. It is 50 by default. The higher the value is, the more obvious the contrast between the bright area and dark area will become.
Saturation		Adjust the color vividness, and will not influence the image overall brightness. ● The image becomes too flamboyant if the value is too high. ● The image is not flamboyant enough if the value is low. The recommended value is from 40 to 60, and the range is from 0 to 100. It is 50 by default. The higher the value is, the more flamboyant the image becomes.
Gamma		Adjust the image brightness level. The higher the value is, the brighter and blurrier the image becomes.
Camera Illuminator	Fill Light	Includes **IR Mode** or **White Light**. This option might not be configurable because certain models only provide 1 mode.

Parameter		Description
	Day/Night	• **Color** : Applicable during the day. The image is shown in colors. • **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. • **B/W** : Applicable during nights. The image is black and white. • **By Time** : The IR light will only be turned on during the periods you defined. When the IR light is on, the video will be brighter. This parameter is only configurable when **Fill Light** is set to **IR Mode**.
	Default Environment Brightness	Set a threshold for the automatic switch of fill light. You can drag the slider to adjust the value. If the current environment brightness is lower than the threshold, the fill light is on. Otherwise, the fill light is off.
	Working Mode	• **Always Off** : Set the IR light to always off. • **Always On** : Set the IR light to always on. • **Day/Night** : Automatically turn on or off the IR light according to the configured **Day/Night** mode. Only applicable when **Fill Light** is set to **IR Mode**.
		• **Always Off** : Set the white light to always off. • **Always On** : Set the white light to always on. • **Day/Night** : Automatically turn on or off the white light according to the defined default environment brightness. • **By Time** : The white light will only be turned on during the periods you defined. Only applicable when **Fill Light** is set to **White Light**.
	Brightness	Set the illumination intensity when there are no vehicles passing. The higher the value is, the brighter it will be.

Step 3 Click **Apply**.

11.1.2 Shutter Parameters

This section provides guidance on configuring camera shutter, including shutter mode, exposure mode, gain mode, and scene mode.

Procedure

Step 1 On the home page, click **Camera**, and then select **Image** > **Shutter**.

You can also select > **Camera** > **Image** > **Shutter**.

Step 2 Configure the parameters.

Figure 11-2 Configure Shutter

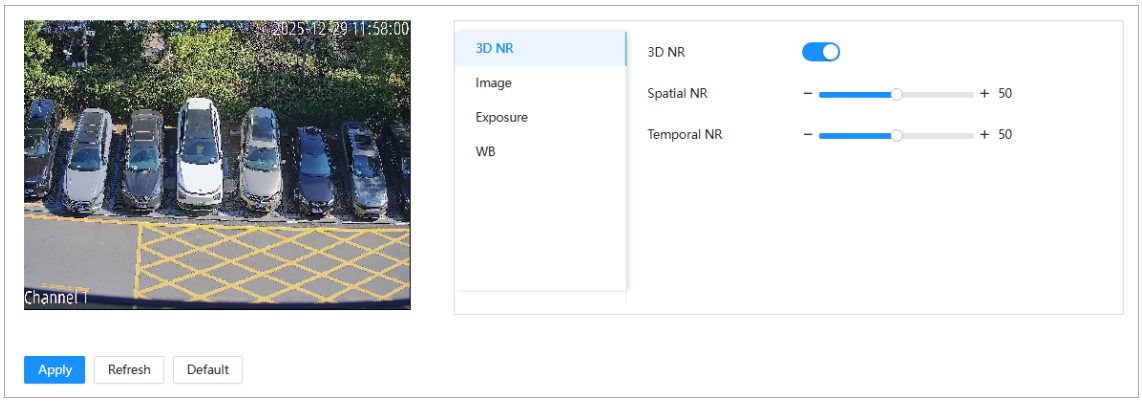


Table 11-2 Parameters description of shutter

Parameter	Description	
3D NR	3D NR	Select **Enable** to enable the function.
	Spatial NR	Spatial video denoising. The higher the value, the fewer the noise.
	Temporal NR	Temporal video denoising. The higher the value, the fewer the flicker noise.
Image	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	Select **On** to enable WDR (wide dynamic range), which helps provide clear video images in bright and dark light.
Exposure	Iris	Select the iris mode from **Auto** and **Manual**.
	Mode	Select the way of adjusting exposure mode. You can select from **Manual** , and **Auto**.
	Exposure Compensation	Sets the value, and it ranges from 0 to 50. The higher the value is, the brighter the image will be.
	Shutter	You can select the shutter value, or select **Custom**, and then set the shutter range. You need to set shutter when setting **Mode** to **Manual**.

Parameter	Description	
	Shutter Range	Set the time range for shutter. You need to set shutter range when setting **Customized** to **Shutter**.
	Gain	Set the value range for gain. You need to set gain scope when setting **Mode** to **Manual**.
WB	Mode	Set a scene mode to adjust the image to better status.

Step 3 Click **Apply**.

11.2 Setting Encode Parameters

This section introduces video parameters, such as video, snapshot, overlay, ROI (region of interest), and path.

Click **Default** , and the device is restored to default configuration. Click **Refresh** to view the latest configuration.

11.2.1 Video Stream

You can set the video stream information.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video Stream**.

You can also select > **Camera** > **Encode** > **Video Stream**.

Step 2 Configure the parameters.

Figure 11-3 Configure Shutter

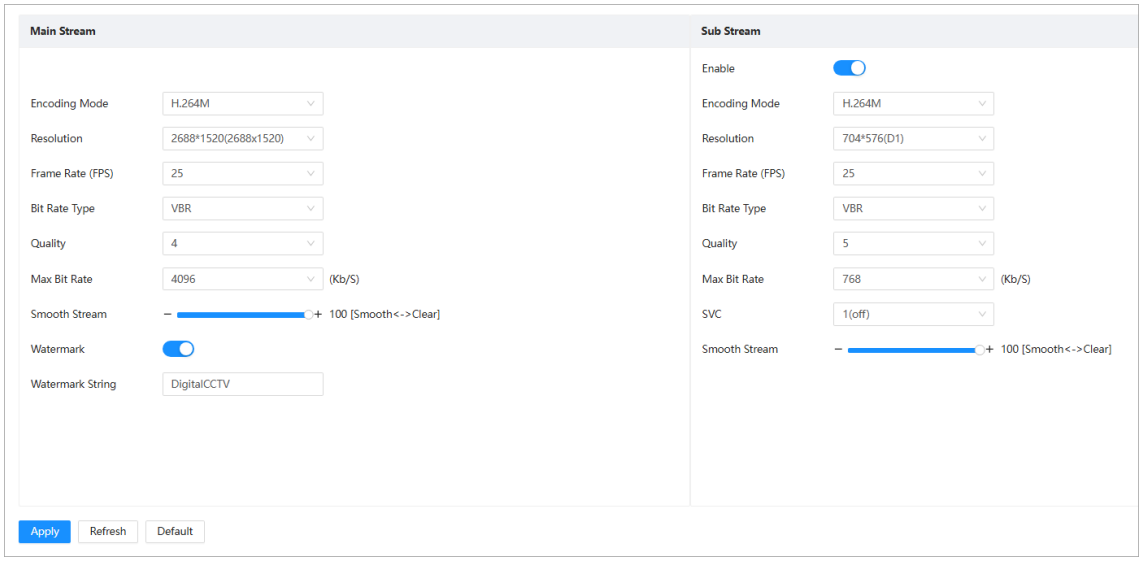


Table 11-3 Parameters description of video stream

Parameter	Description
Encoding Mode	Currently it only supports H.264M, H.264H, H.265, and MJPEG.
Smart Codec	Click to enable smart codec to improve video compressibility and save storage space. After smart codec is enabled, ROI, SVC, and smooth stream will not be displayed.
Resolution	Select the video resolution. The resolution of sub stream cannot be greater than that of the main stream.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	We recommend that you use VBR in constantly changing scenes, and CBR in stable scenes. ● **VBR** : Variable bitrate. The bitrate automatically adjusts with changes in scene complexity. This is useful for providing clear video when the scene is complex, and saving the bandwidth when the scene is simple. ● **CBR** : Constant bitrate. The bitrate barely changes with the scene complexity. When the scene is complex, the video might not be clear enough. When the scene is simple, more unnecessary bandwidth might be consumed. Image quality can only be set in VBR mode.

Parameter	Description
Quality	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. The better the quality is, but the bigger the required bandwidth will be.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set to **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
I Frame Interval	Frame or time interval between two I frames. The bigger the interval, the smaller space taken by the decompressed video. The system default is set twice as big as frame rate.
SVC	Scalable video codec (SVC) contains 3 layers providing different frame rates. The higher the layer, the greater the video quality.
Smooth Stream	It is designed for fluid viewing of live video. The higher the value, the smoother the video.
Watermark	Set the watermarks, which will be added into videos of the camera. • Select **Watermark** to enable the watermark adding. • **Watermark String** is DigitalCCTV by default. • The watermark character can only consist of number, letter, underline, and maximum length contains 85 characters.

Step 3 Click **Apply**.

11.2.2 Video OSD

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

11.2.2.1 Configuring Channel Title

You can enable this function when you need to display a channel title on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Channel Title**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Channel Title**.

Step 2 Click to enable the function.

Step 3 Enter a name for the title, and then adjust its position by entering the coordinates or dragging it on the video.

Step 4 Configure a color for the font.

Step 5 Click **Apply**.

11.2.2.2 Configuring Time Title

You can enable this function when you need to display time in the video image.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Time Title**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Time Title**.

Step 2 Click next to **Enable** to enable the function.

Step 3 Click next to **Week Display** to display the day of the week.

Step 4 Adjust the position of the title by entering the coordinates or dragging it on the video.

Step 5 Configure a color for the font.

Step 6 Click **Apply**.

11.2.2.3 AI Detection

When the camera detects a blocklist or traffic standstill event, information of the event will be displayed on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **AI Detection**.

You can also select > **Camera** > **Encode** > **Video OSD** > **AI Detection**.

Step 2 Click next to **Enable** to enable the function.

Step 3 Adjust the position of the title by entering the coordinates or dragging it on the video.

Step 4 Configure a color for the font.

Step 5 Click **Apply**.

11.2.2.4 Configuring Privacy Masking

You can enable this function when you need to protect the privacy of certain areas on the video.

You can draw rectangles as blocks. You can drag 4 blocks at most, and the color is black.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Privacy Mask**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Privacy Mask**.

Step 2 Configure privacy masking.

1. Click next to **Enable**.
2. Click **Add**, and then drag the block to the area that you need to cover.
3. Adjust the size of the rectangle to protect the privacy.
4. Click **Apply**.

Related Operations

- View and edit the block

Select the privacy masking rule to be edited on the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.

- Edit the block name

  Double-click the name in **Name** to edit the block name.
- Delete the block

  - Click to delete blocks one by one.
  - Click **Clear** to delete all blocks.

11.2.2.5 Configuring Custom Title

You can enable this function if you need to display custom information on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Custom Title**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Custom Title**.

Step 2 Click next to **Enable** to enable the function.

Step 3 Enter the text that you want to display, and then adjust its position by entering the coordinates or dragging it on the video.

Step 4 Click **Apply**.

11.2.3 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 > **Camera** > **Encode** > **ROI**.

Step 2 Click **Add**, adjust the area by the corners and drag it to a position, and then select its quality.

- You can add up to 3 areas.
- The higher the value is, the better the quality will be.
- Click or **Clear** to delete the area one by one or all areas.

Step 3 Click **Apply**.

12 System

This section introduces system configurations, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.

12.1 General Parameters

12.1.1 General

You can configure device name and number, language, video standard, device organization, and device location.

Procedure

Step 1 On the home page, click **System**, and then select **General** > **General**.

You can also select > **System** > **General** > **General**.

Step 2 Configure the parameters.

Table 12-1 Parameters description of general settings

Parameter	Description
Device Name	Enter the name and number of the device.
Device No.	
Language	Select a language to display the webpage.
Video Standard	Select video standard from **PAL** and **NTSC**.
Device Organization	Enter the organization and location of the device.
Device Location	

Step 3 Click **Apply**.

12.1.2 Date

You can configure date and time format, time zone, current time, DST (Daylight Saving Time) or NTP server.

Procedure

Step 1 On the home page, click **System**, and then select **General** > **Date**.

You can also select > **System** > **General** > **Date**.

Step 2 Configure the parameters.

Table 12-2 Parameters description of date

Parameter	Description
Date Format	Configure the date format.

Parameter	Description
Time Format	Configure the time format. You can select from **12-Hour** or **24-Hour**.
Time Zone	Configure the time zone that the camera is at.
System Time	Configure system time. Click **Sync PC**, and the system time changes to the PC time.
DST	Enable DST as needed. Click , and configure start time and end time of DST with **Date** or **Week**.
Time Synchronization	Select checkbox of **NTP** so that the device can synchronize its time with the server you configure.
Server	Enter the IP address and port number of the server that the device will synchronize time with.
Port	
Interval	Configure the frequency that the device will synchronize its time with the server.

Step 3 Click **Apply**.

12.2 Account

You can manage users, such as add, delete, or edit them. Users include admin, added users and ONVIF users.

Managing users and groups are only available for administrator users.

- The max length of the user or group name is 31 characters which consists of number, letter, underline, dash, dot and @.
- 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 ' " ; : &).
- You can have 18 users and 8 groups at most.
- You can manage users through single user or group, and duplicate user names or group names are not allowed. A user can only be in one group at a time, and the group users can own permissions within group permission range.
- Online users cannot edit their own permissions.
- There is one admin by default which has highest permission.
- Select **Anonymous Login** , and then log in with only IP address instead of user name and password. Anonymous users only have preview permissions. During anonymous login, click **Logout**, and then you can log in with other user name.

12.2.1 User

12.2.1.1 Adding a User

You are admin user by default. You can add users, and configure different permissions.

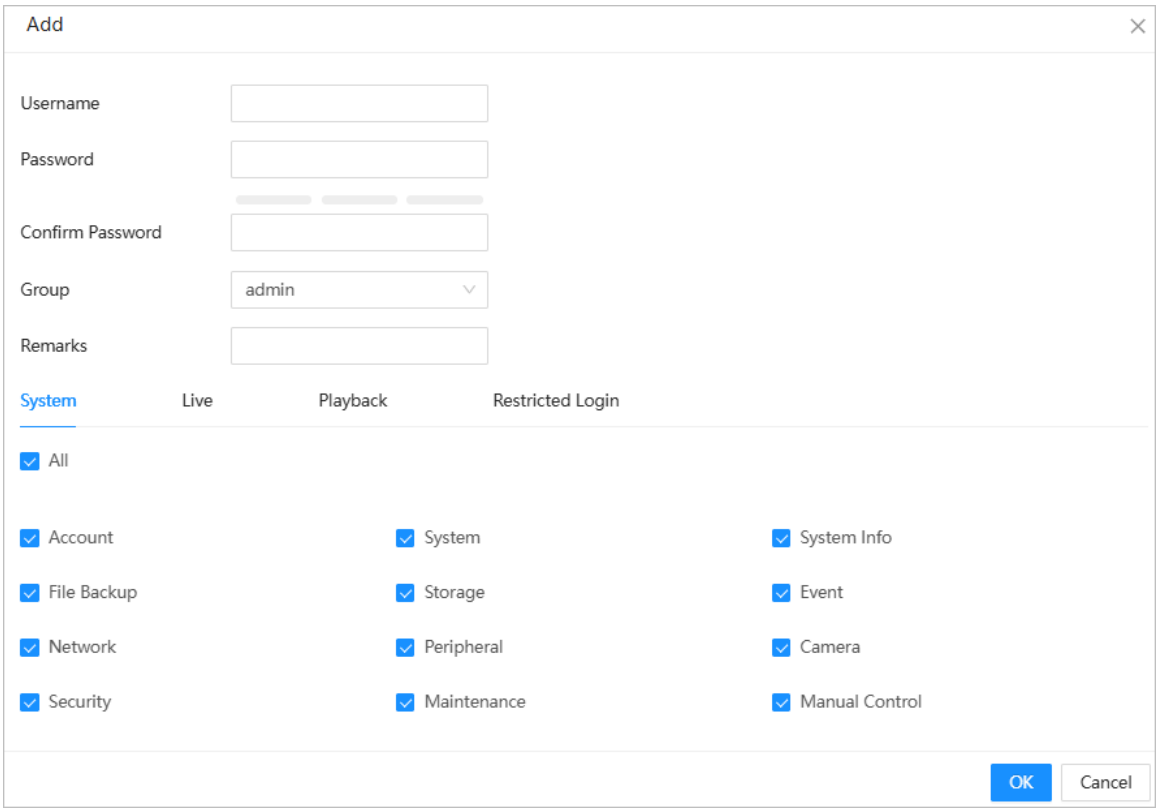
Procedure

Step 1 On the home page, click **System**, and then select **Account** > **User**.

You can also select > **System** > **Account** > **User**.

Step 2 Click **Add**.

Figure 12-1 Add user



Step 3 Configure the parameters.

Table 12-3 Parameters description of adding user

Parameter	Description
Username	The name that identifies the user.
Password	Enter password and confirm it again. 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 ' " ; : &).
Confirm Password	
Group	The group that users belong to. Each group has different permissions.
Remarks	Describe the user.
System	Select permissions as needed. We recommend you give fewer permissions to normal users than premium users.
Live	Select the live view permission for the user to be added.
Playback	Select the playback permission for the user to be added.

Parameter	Description
Restricted Login	Set the IP address that allows the defined user to log in to the camera and the validity period and time range. You can log in to the webpage with the defined IP in the defined time range of validity period. ● IP address: You can log in to web through the computer with the defined IP or one within the defined IP segment. ● Validity period: You can log in to webpage in the defined validity period. ● Period: You can log in to webpage in the defined time range.

Step 4 Click **OK**.

The user is displayed in the user name list.

Related Operations

- Click to edit password, group, memo or permissions.

  For admin account, you can only edit the password.

- Click to delete the added users. Admin user cannot be deleted.

  The admin account cannot be deleted.

12.2.1.2 Resetting Password

Enable the function, and you can reset password by clicking **Forget password?** on the login page. For details, see "3.2 Resetting Password".

Procedure

Step 1 On the home page, click **System**, and then select **Account** > **User**.

You can also select > **System** > **Account** > **User**.

Step 2 Click next to **Password Reset**.

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

Step 3 Click **Apply**.

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

12.2.2 Adding a User Group

A group is a set of permissions. You can configure different groups to quickly assign permissions to different users. There are 2 groups named admin and user by default.

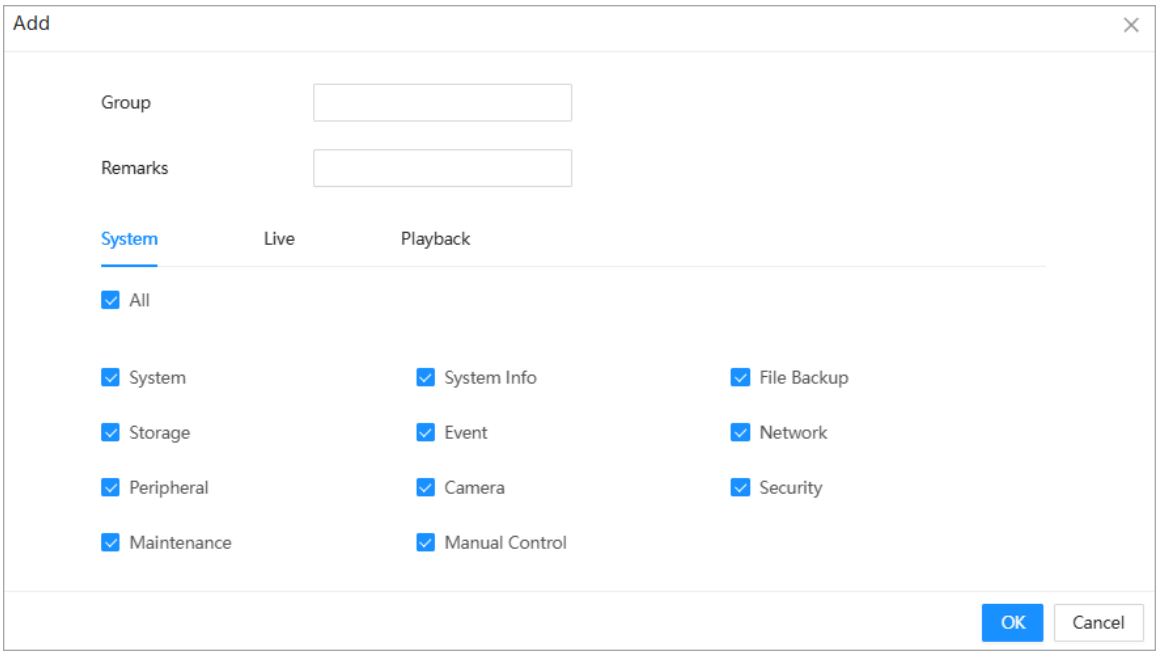
Procedure

Step 1 On the home page, click **System**, and then select **Account** > **Group**.

You can also select > **System** > **Account** > **Group**.

Step 2 Click **Add**.

Figure 12-2 Add group



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

Step 4 Click **OK**.

The group is displayed in the list.

Related Operations

- Click to edit the remarks and permissions.
- Click to delete a group. The admin and user groups cannot be deleted.

12.2.3 Adding an ONVIF User

You can add, delete ONVIF users, and change their passwords.

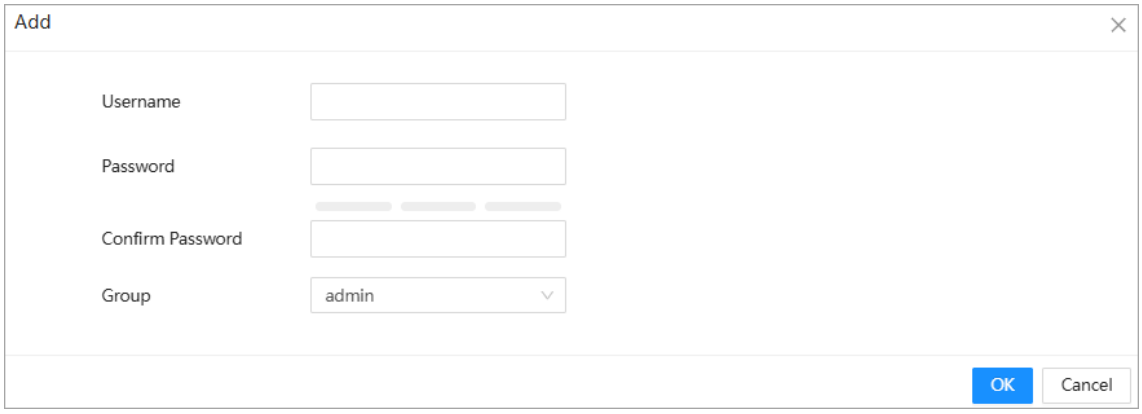
Procedure

Step 1 On the home page, click **System**, and then select **Account** > **ONVIF User**.

You can also select > **System** > **Account** > **ONVIF User**.

Step 2 Click **Add**.

Figure 12-3 Add ONVIF user



Step 3 Configure the parameters.

Table 12-4 Parameters description of ONVIF user

Parameter	Description
Username	The name that identifies the user.
Password	Enter password and confirm it again. 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 ' " ; : &).
Confirm Password	
Group Name	The group that users belong to. Each group has different permissions.

Step 4 Click **OK**.

The user is displayed in the list.

Related Operations

- Click to edit password, group, memo or permissions.

  For admin account, you can only change the password.

- Click to delete the added user.

  The admin account cannot be deleted.

13 Security

13.1 Security Status

Detects the user and service, and scans the security modules to check the security status of the camera, so that when abnormality appears, you can process it timely.

- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing warning and attack defense, not detect whether they are enabled.

Procedure

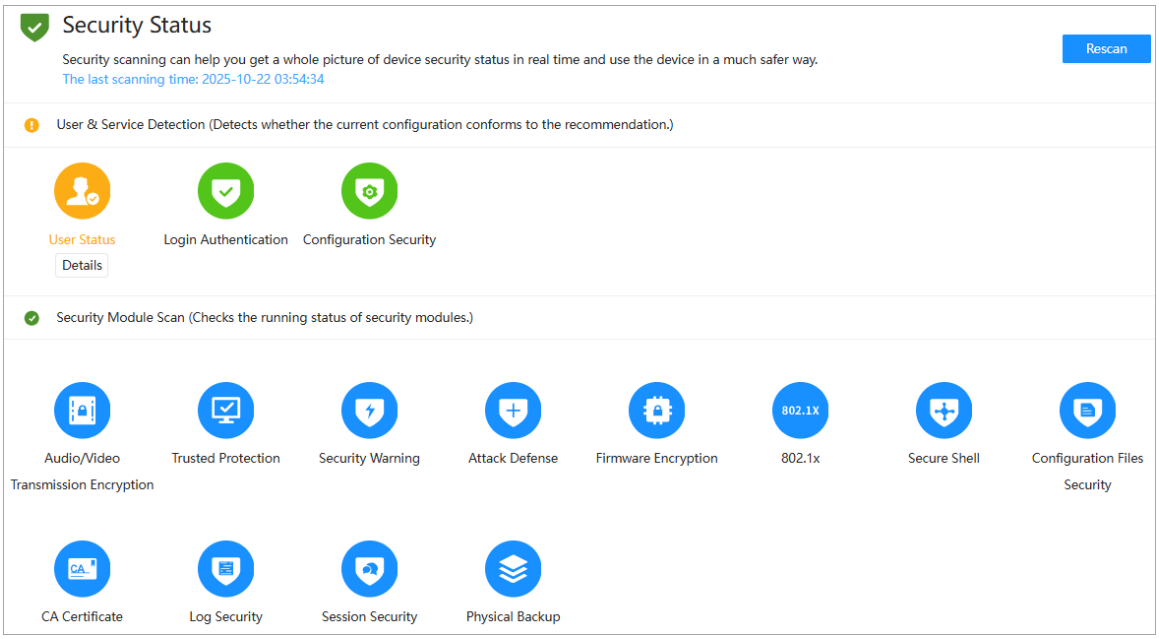
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Security Status**.

Step 3 Click **Scan** to scan the security status of the camera.

Click **Rescan** if it is not your first-time scanning.

Figure 13-1 Security status



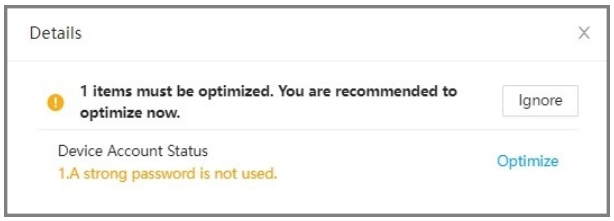
Related Operations

After scanning, different results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and Green indicates that the security modules are normal.

1. Click **Details** to view the details of the scanning result.
2. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.

   Click **Rejoin Detection**, and the exception will be scanned in next scanning.
3. Click **Optimize**, and the corresponding page will be displayed, and you can edit the configuration to clear the exception.

Figure 13-2 Security Status



13.2 System Service

13.2.1 802.1x

The camera can connect to LAN after passing 802.1x authentication.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **System Service** > **802.1x**.

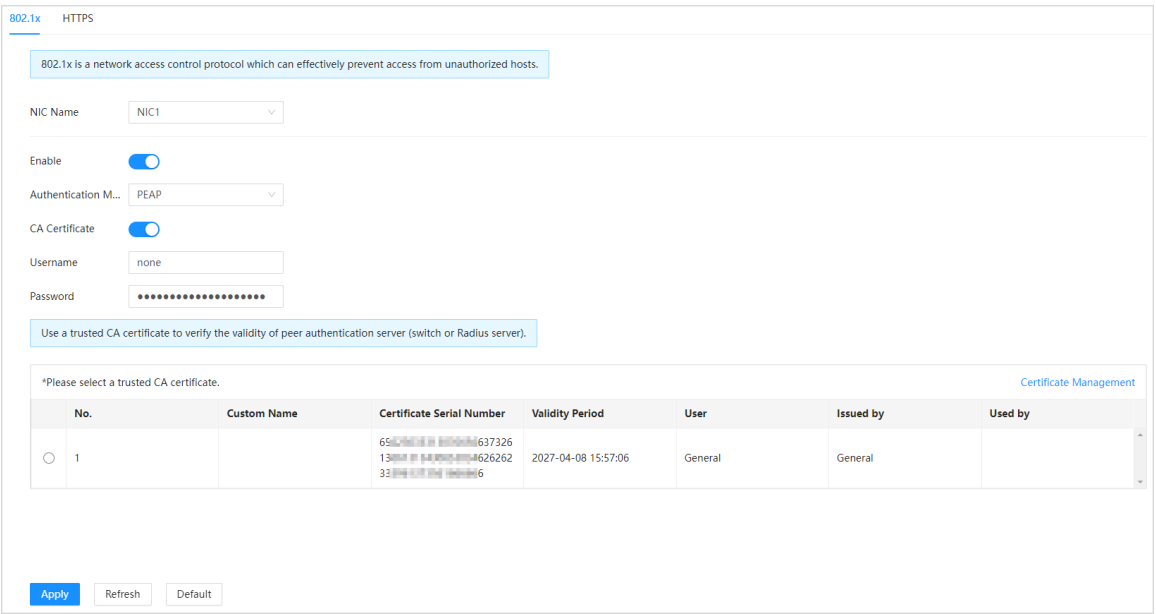
Step 3 Select the NIC name as needed, and click to enable it.

Step 4 Select the authentication mode, and then configure parameters.

- PEAP: Protected EAP protocol.
  1. Select PEAP as the authentication mode.
  2. Enter the username and password that has been authenticated on the server.
  3. Click next to CA certificate, and select the trusted CA certificate in list.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar.

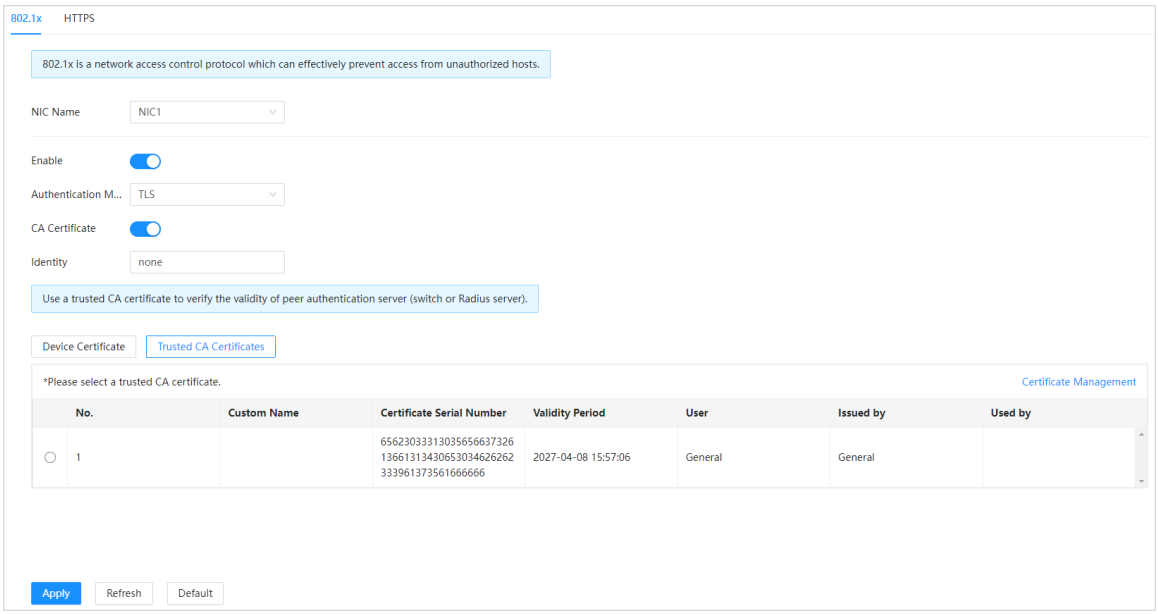
Figure 13-3 802.1x (PEAP)



- TLS: Transport Layer Security. It is applied in two communication application programs to guarantee the security and integrity of the data.
  1. Select TLS as the authentication mode.
  2. Enter the username.
  3. Click next to CA certificate, and select the trusted CA certificate in list.

     If there is no certificate in the list, click **Certificate Management** at the left navigation bar.

Figure 13-4 802.1x (TLS)



Step 5 Click **Apply**.

13.2.2 HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your computer. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **System Service** > **HTTPS**.

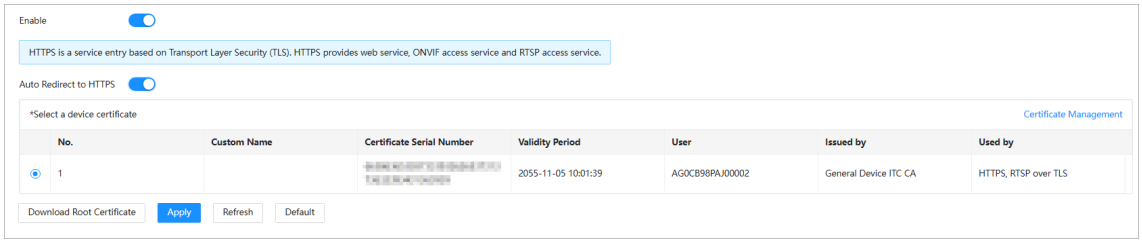
Step 3 Click to enable the function. After it is enabled, you can log in to the camera through HTTP or HTTPS.

By enabling **Auto Redirect to HTTPS**, the system will automatically load over HTTPS instead of unsecured HTTP.

Step 4 Select the certificate.

If there is no certificate in the list, click **Certificate Management** to configure one. For details, see "13.4.2 Installing Trusted CA Certificate".

Figure 13-5 HTTPS



Step 5 Click **Apply**.

13.3 Attack Defense

13.3.1 Firewall

Configure the firewall to limit access to the camera.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Attack Defense** > **Firewall**.

Step 3 Click to enable the function.

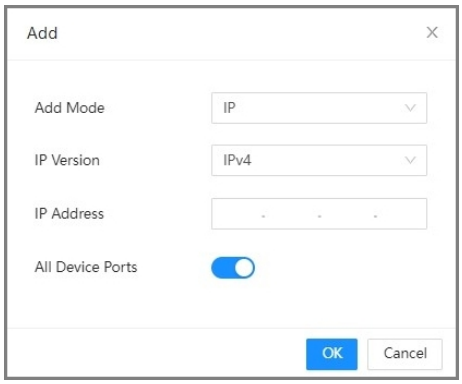
Figure 13-6 Firewall

Step 4 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist** : Only when the IP or MAC of your computer is in the allowlist, can you access the camera. Ports are the same.
- **Blocklist** : When the IP or MAC of your computer is in the blocklist, you cannot access the camera. Ports are the same.

Step 5 Click **Add** to add the host IP or MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 13-7 Firewall



Step 6 Click **Apply**.

Related Operations

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

13.3.2 Account Lockout

If you use a wrong password to log in for more than the configured value, the account will be locked.

Procedure

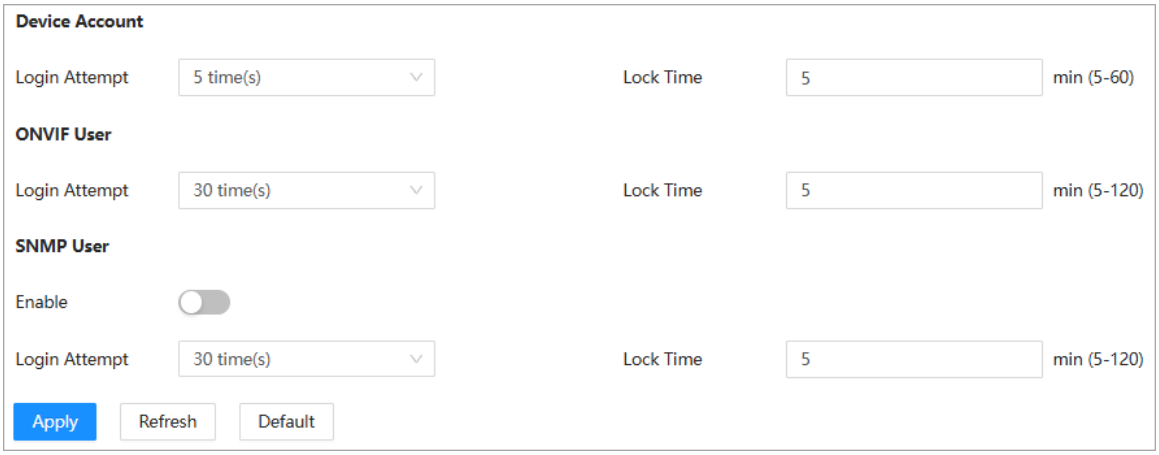
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Attack Defense** > **Account Lockout**.

Step 3 Configure the login attempt and lock time for device account, ONVIF user, and SNMP user.

- Login attempt: Upper limit of login attempts. If you consecutively enter a wrong password more than the configured value, the account will be locked.
- Lock time: The period during which you cannot log in after the login attempts reaches the upper limit.

Figure 13-8 Account lockout



Step 4 Click **Apply**.

13.3.3 Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against DoS attack.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Attack Defense** > **Anti-DoS Attack**.

Step 3 Click to enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

Step 4 Click **Apply**.

13.4 CA Certificate

13.4.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your computer.

13.4.1.1 Creating Certificate

Create certificate in the device.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

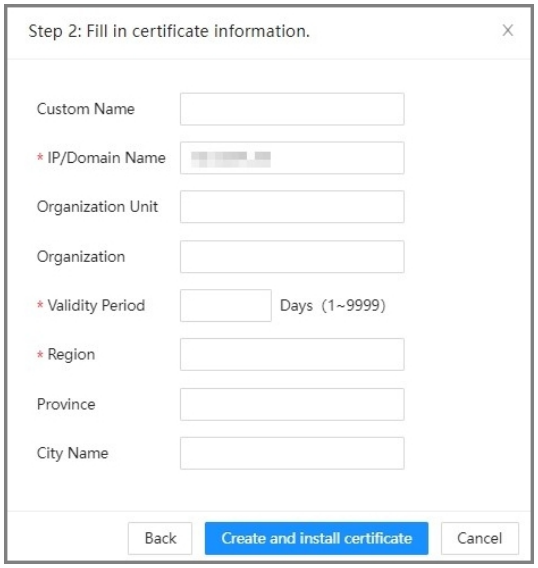
Step 2 Select **CA Certificate** > **Device Certificate**.

Step 3 Click **Install Device Certificate**.

Step 4 Select **Create Certificate** , and click **Next**.

Step 5 Enter the certificate information.

Figure 13-9 Certificate information (1)



Step 6 Click **Create and install certificate**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

13.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

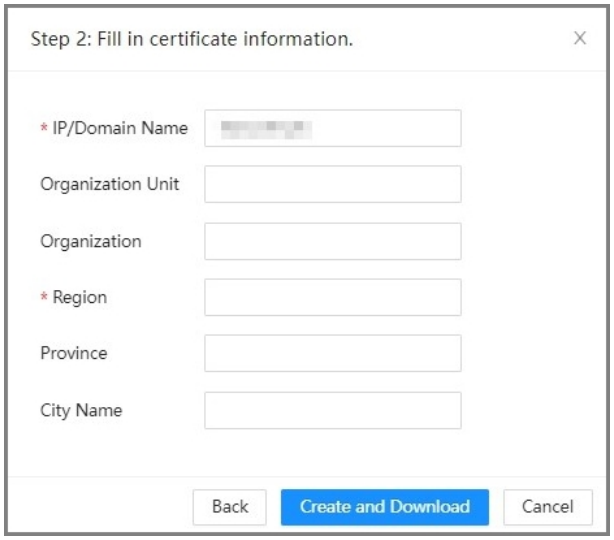
Step 2 Select **CA Certificate** > **Device Certificate**.

Step 3 Click **Install Device Certificate**.

Step 4 Select **Apply for CA Certificate and Import (Recommended)** , and then click **Next**.

Step 5 Enter the certificate information.

Figure 13-10 Certificate information (2)

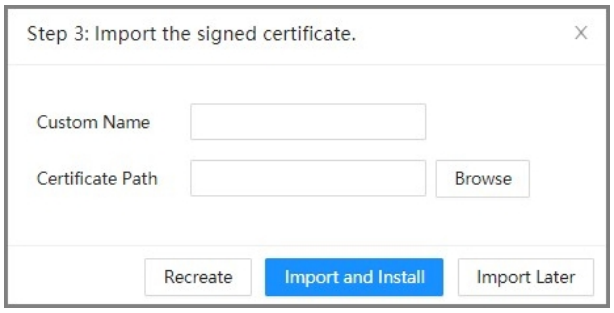


Step 6 Click **Create and Download** and save the request file to your computer.

Step 7 Use the request file to apply for a CA certificate with a third-party certificate authority.

Step 8 Click **Browse**, and then open the CA certificate.

Figure 13-11 Import a CA certificate



Step 9 Click **Import and Install**.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

13.4.1.3 Installing Existing Certificate

Import the existing third-party certificate to the camera. When applying for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

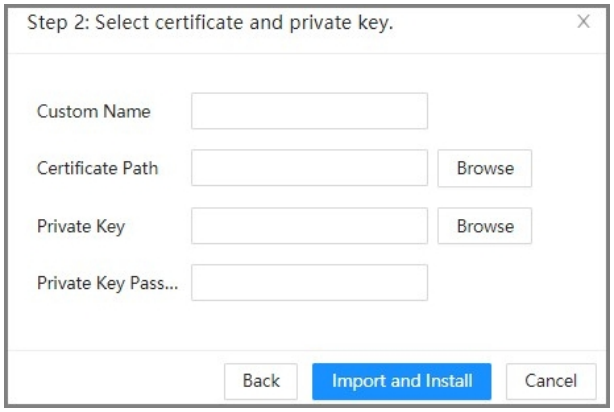
Step 2 Select **CA Certificate** > **Device Certificate**.

Step 3 Select **Install Device Certificate**.

Step 4 Select **Install Existing Certificate** , and then click **Next**.

Step 5 Click **Browse** to open the CA certificate and private key, and enter the private key password.

Figure 13-12 Certificate and private key



Step 6 Click **Import and Install**.

After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- Click **Enter Edit Mode** to edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

13.4.2 Installing Trusted CA Certificate

A CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

Procedure

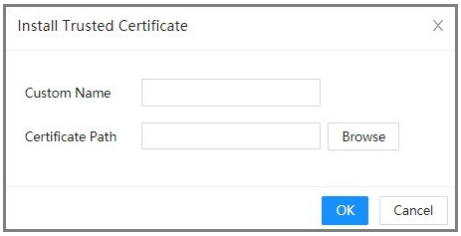
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **CA Certificate** > **Trusted CA Certificates**.

Step 3 Select **Install Trusted Certificate**.

Step 4 Click **Browse** to open the certificate.

Figure 13-13 Installing trusted certificate



Step 5 Click **OK**.

After the certificate is created successfully, you can view the created certificate on the **Trusted CA Certificate** page.

Related Operations

- Click **Enter Edit Mode**, you can edit the custom name of the certificate.
- Click to download the certificate.
- Click to delete the certificate.

13.5 A/V Encryption

The device supports encrypting data during audio and video transmission.

We recommend enabling the A/V Encryption function. Otherwise there might be safety risks.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **A/V Encryption**.

Step 3 Configure the parameters.

Figure 13-14 A/V encryption

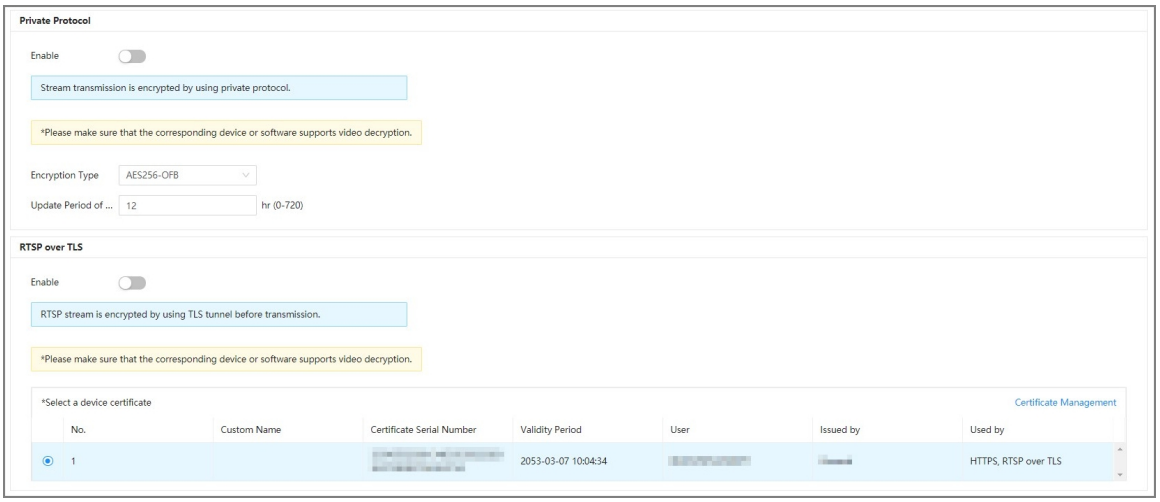


Table 13-1 Parameters description of A/V encryption

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is not enabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is not enabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "13.4 CA Certificate".

Step 4 Click **Apply**.

13.6 Security Warning

When a security exception event or illegal login is detected, the camera sends a warning to remind you to process it timely to avoid security risks.

13.6.1 Security Exception

The camera monitors exceptions and triggers a warning when one occurs.

Procedure

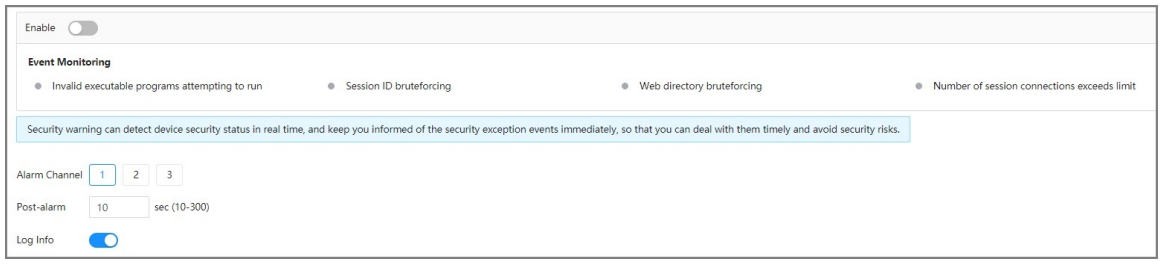
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Security Warning** > **Security Exception**.

Step 3 Click to enable the function.

Step 4 Configure the parameters.

Figure 13-15 Security warning



- **Alarm Channel** : Select an alarm output channel. The corresponding device will be activated when an event is detected.
- **Post-alarm** : When an alarm is triggered, it will continue for the defined period after it ends.
- **Log Info** : After it is enabled, the camera will generate a log when an event occurs. For how to search for the log, see "14.3.1 Searching for Logs".

Step 5 Click **Apply**.

13.6.2 Illegal Login

The camera triggers a warning when illegal login is detected.

Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Security Warning** > **Illegal Login**.

Step 3 Click to enable the function.

Step 4 Configure the parameters.

- **Alarm Channel** : Select an alarm output channel. The corresponding device will be activated when an event is detected.
- **Post-alarm** : When an alarm is triggered, it will continue for the defined period after it ends.
- **Log Info** : After it is enabled, the camera will generate a log when an event occurs. For how to search for the log, see "14.3.1 Searching for Logs".

Step 5 Click **Apply**.

13.7 Security Authentication

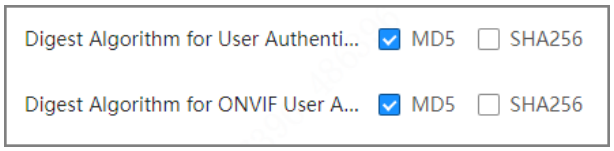
Procedure

Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

Step 2 Select **Security Authentication**.

Step 3 Configure the parameters.

Figure 13-16 Security Authentication



- **Digest Algorithm for User Authentication**

  The user can select **MD5** or **SHA256** for data encryption when logging in via WEB, ConfigTool or other methods.
- **Digest Algorithm for ONVIF Authentication**

  The user can select **MD5** or **SHA256** for data encryption when logging in with the ONVIF protocol.

Step 4 Click **Apply**.

14 Maintenance Center

The maintenance center supports one-click diagnosis of the device status, so that technical support can easily track and troubleshoot device issues.

14.1 One-Click Diagnosis

One-click diagnosis detects the configurations and status of your device to improve its performance.

Procedure

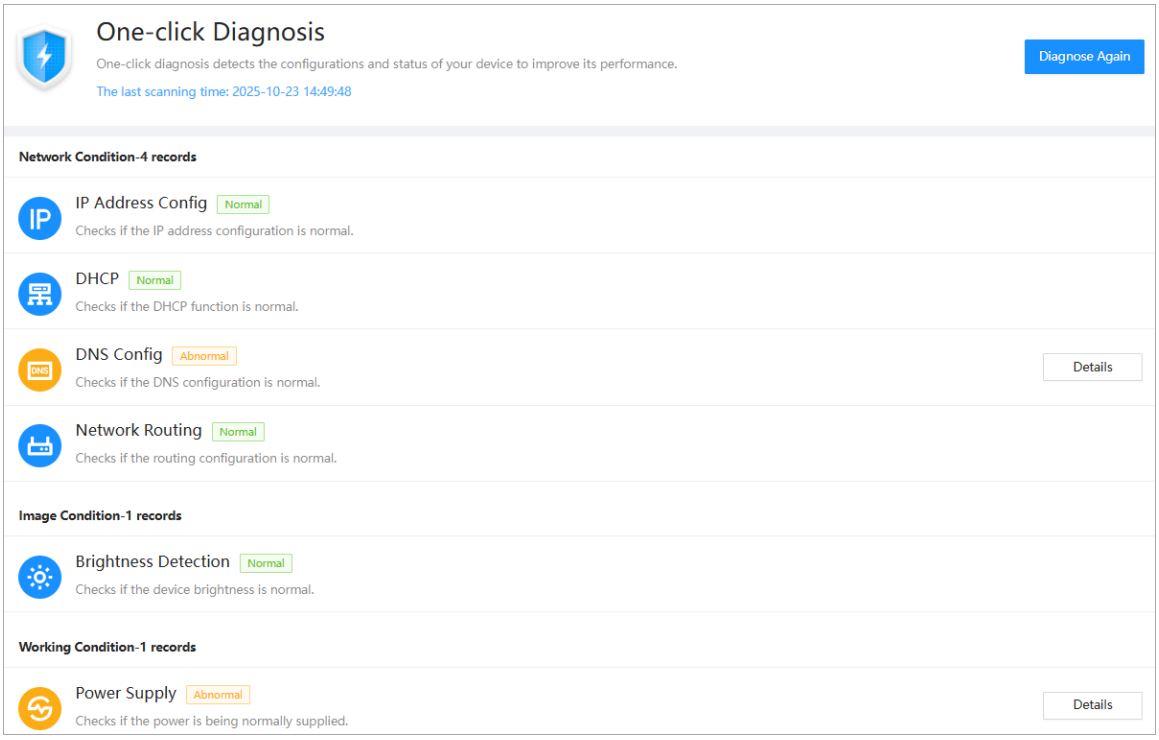
Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **One-click Diagnosis**.

Step 3 Click **Diagnose**.

If you need to re-diagnose the device, click **Diagnose Again**.

Figure 14-1 One-click diagnosis



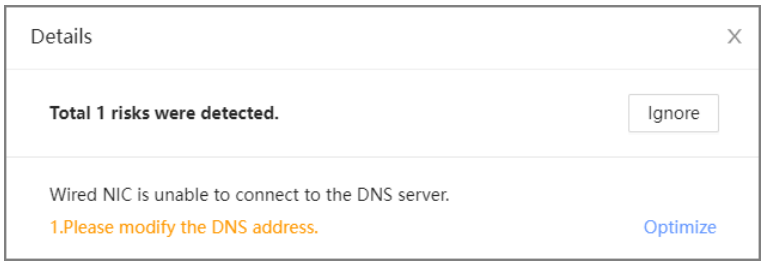
Related Operations

After the diagnosis completes, the page displays the diagnosis results. Yellow indicates that the condition is abnormal, and Green indicates that the condition is normal.

- Click **Details** to view the details of the diagnosis result.
- Click **Ignore** to ignore the abnormality, and it will not be detected in next diagnosis.

  Click **Rejoin Detection**, and the abnormality will be detected in next diagnosis.
- Click **Optimize**, and the corresponding page will be displayed, and you can edit the configuration to clear the abnormality.

Figure 14-2 Details



14.2 System Information

You can view various information of the camera, including version, logs and online users, running status, and legal information.

14.2.1 Version

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 View system information.

- Select **System Info** > **Version**, and then you can view different information of the camera, including device type, hardware version, algorithm version, system version, software version, system version, web version, serial number, and security baseline version.
- Select **System Info** > **Peripheral Version**, and then you can view the Wiegand firmware version.

14.2.2 Online User

On the home page, select **Maintenance Center** > **System Info** > **Online User** , or select > **Maintenance Center** > **System Info** > **Online User** at the upper right, and then you can view all the online users logging in to the webpage.

14.2.3 Legal Info

On the home page, select **Maintenance Center** > **System Info** > **Legal Info** , or select > **Maintenance Center** > **System Info** > **Legal Info** at the upper right, and then you can view the open source software notice.

14.3 Log

You can search for and back up logs on the camera, and obtain logs from a remote location.

14.3.1 Searching for Logs

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Log** > **Log**.

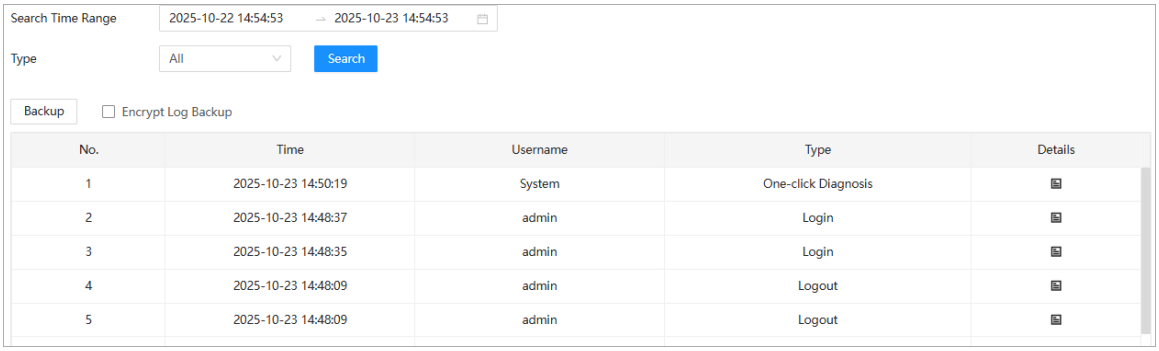
Step 3 Configure the search time range, and then select the log type.

- **All** : All types of logs.
- **System** : Includes program start, abnormal close, close, program reboot, device shutdown, device reboot, system reboot, and system upgrade.
- **Config** : Includes saving configuration and deleting configuration file.
- **Storage** : Includes configuring disk type, clearing data, hot swap, and FTP state.
- **Event Operation** : Includes the start time and end time of events.
- **Record** : Includes file access, file access error, and file search.
- **Account** : Includes login, logout, adding a user, deleting a user, editing a user, adding a group, deleting a group, and editing a group.
- **Security** : Includes password resetting and IP filter.

Step 4 Click **Search**.

Search results are displayed.

Figure 14-3 Log



Step 5 Click or click a log, and then you can view the detailed information in **Details** area.

Step 6 (Optional) Click **Backup**, and then you can back up all the logs that are searched for to your computer.

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

14.3.2 Obtaining Remote Logs

Critical logs can be saved to the log server. They can provide important clues to the source of security incidents. The log server needs to be deployed in advance by a professional or system administrator.

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Log** > **Remote Log**.

Step 3 Click to enable the function.

Step 4 Configure the IP address, port and device number.

Step 5 (Optional) Enable TLS as needed. After enabling it, the system will encrypt data transmission using TLS tunnel.

Step 6 Click **Apply**.

14.4 Maintenance Management

Prerequisites

To make sure the system runs normally, maintain it as the following requirements:

- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Change the password every three months. For details, see "12.2 Account".
- View system logs and analyze them, and process the abnormity in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

14.4.1 Maintenance

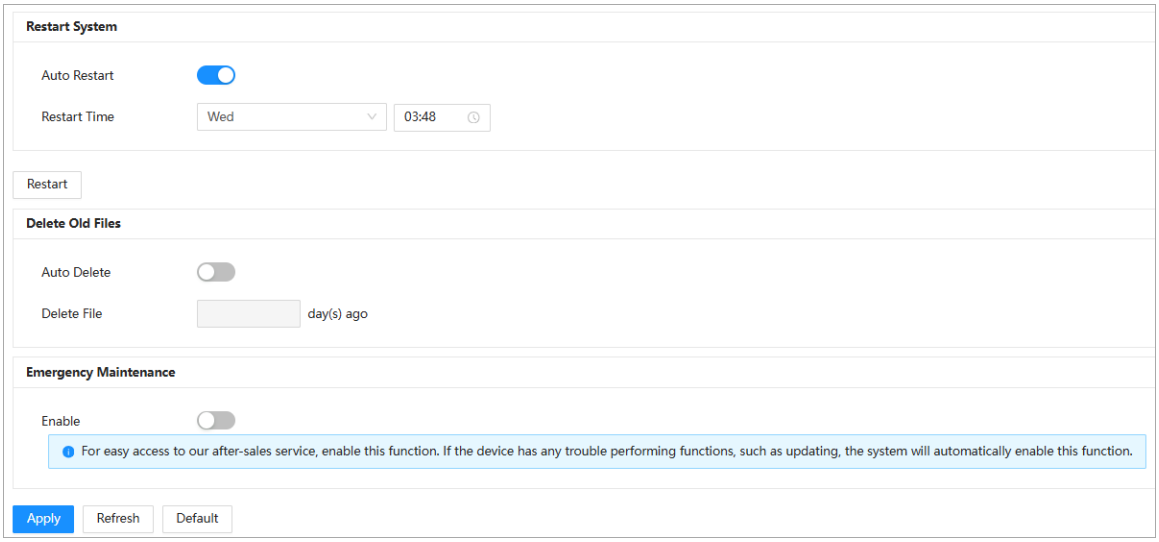
You can restart the system manually, and set the time of automatic restart and deleting old files. This function is not enabled by default.

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Maintenance**.

Figure 14-4 Maintenance



Step 3 Configure the parameters.

- Click next to **Auto Restart** and set the restart time. The device will automatically restart at the defined time every week.
- Click next to **Auto Delete** and set the time. The device will automatically delete old files at the defined time. The time range is 1 to 31 days.
- Enable **Emergency Maintenance** so that when the device cannot start properly, maintenance tools can be used to access the device for troubleshooting.

When you enable and confirm the **Auto Delete** function, the deleted files cannot be restored. Please be advised.

Step 4 Click **Apply**.

14.4.2 Import/Export

- Export the configuration of the camera in a file to your computer for backup.
- Import a configuration file to quickly configure the camera.

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Import/Export**.

Step 3 Import or export the file.

- Import: Select the configuration file on your computer, and then click **Import File** to import it to the camera.
- Export: Click **Export Configuration File** to export the configuration of the camera in a file to your computer.

14.4.3 Default

Restore all settings of the camera to the default status.

On the home page, select **Maintenance Center** > **Maintenance Management** > **Default** , or select > **Maintenance Center** > **Maintenance Management** > **Default** at the upper right.

- Click **Default**, and then all the configurations, except IP address, automatic registration, port numbers, HTTPS, and multicast, are reset to the default status.
- Click **Factory Default**, and then all the configurations, including IP address, automatic registration, port numbers, HTTPS, and multicast, are reset to factory settings.

14.5 Update

Update the camera to the latest version to improve its stability and functions. If wrong update file has been used, restart the device; otherwise some functions might not work properly.

Procedure

Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Update**.

Step 3 Update the camera in the following ways.

- Use an update file.
  1. Click **Browse**.
  2. Select the update file in .bin format.

     If you use an incorrect update file and the update is in progress, restart the device manually. Otherwise, certain functions might not work properly.
  3. Click **Update**.
- Update online.

  Click next to **Auto Check for Updates** to enable the function. The camera will regularly check for updates, and automatically update when available.

14.6 Advanced Maintenance

It provides maintenance services for tracking and troubleshooting of network connection issues.

It is mainly used by technical support engineers for troubleshooting and other tech support.

Procedure

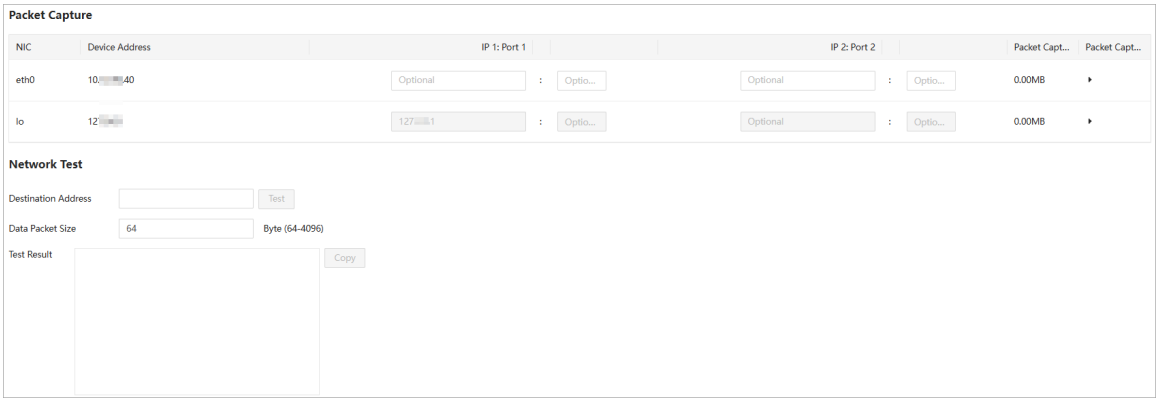
Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

Step 2 Select **Advanced Maintenance**.

Step 3 You can export device information, test packet capture and network, and view logs.

- Export device information: Click the **Export** tab, and then click **Export** to export the serial number, firmware version, device operation logs and configuration information if necessary.
- Packet capture: Click the **Packet Capture** tab, and then you can examine network traffic and test the network.

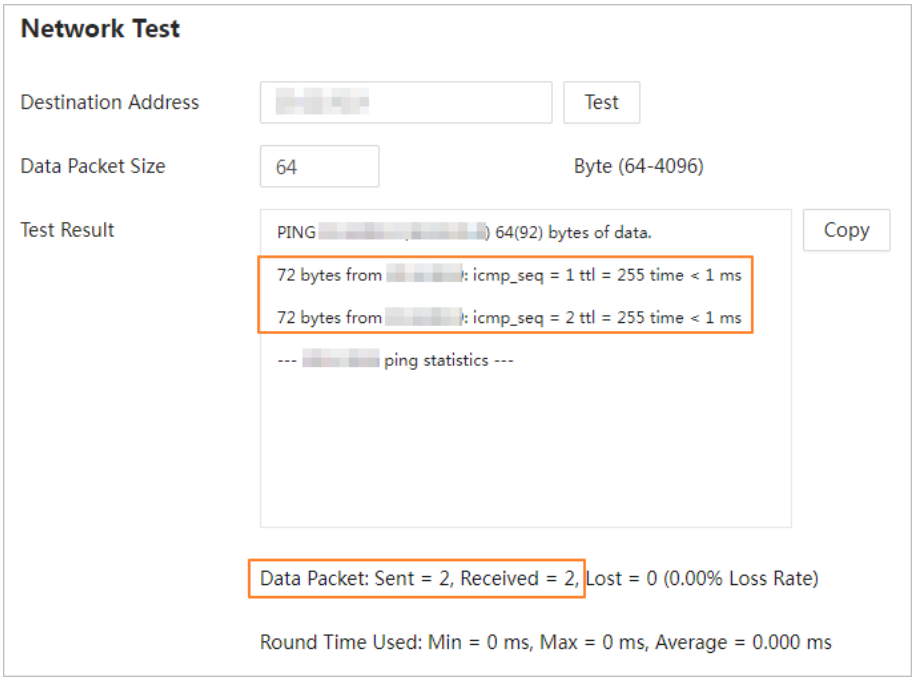
Figure 14-5 Packet capture



- **Packet Capture**: It examines network traffic by capturing IP packets to investigate network issues and detect security threats.
  1. (Optional) Enter the specified IP and port.
  2. Click ▶ to perform a packet capture. A packet sniffer backup will be uploaded automatically after you click ⏸ to end the capture.
- **Network Test**: Test whether the network can be accessed.
  1. Enter the destination address, that is, the address to which a packet of data is sent over a network.
  2. Click **Test** to perform the network test.

     Click **Stop**, and then the data packet and round time used will be displayed.
  3. Check the test results in **Test Result** . The following figure shows that the network is normal; if it shows **timeout**, means that the network cannot be accessed.

Figure 14-6 Network test results



- Click the **Running Logs** tab to view the logs of device abnormality and maintenance.

You can click to download a log, or select multiple logs, and then click **Export** to export them in batches.

15 Setting

This section introduces the basic setting of the camera, including the configuration of Local, Camera, Network, Event, Storage, System, System Information and Log.

For **Camera** and **System**, you can go to the configuration page through two methods. This section uses method 1 as an example.

- Method 1: Click , and then select the corresponding item.
- Method 2: Click the corresponding icon on the home page.

15.1 Local

You can select a protocol and configure the storage paths for live snapshot, live record, playback snapshot, playback download, and video clips.

Prerequisites

You must install the plug-in first. Configure any parameter, and then a prompt will be displayed on the bottom of the page. You can follow the instructions to install the plug-in.

If you do not install the plug-in, images and videos will be stored to the default path set on the browser.

Procedure

Step 1 Select > **Local**.

Step 2 Configure the parameters.

Table 15-1 Parameters description local

Parameter	Description	
Naming Format	You can reset the storage path by referring to the naming format. Click **Help** for more details.	**Admin** in the path refers to the account being used.
Name Preview		
Live Record	The recorded video of live page. The default storage path is C:\RecordDownload.	

Step 3 Click **Apply**.

15.2 Network

This section introduces network configuration.

15.2.1 TCP/IP

You can configure IP address and DNS (Domain Name System) server and so on according to network planning.

Prerequisites

The camera has connected to the network.

Procedure

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

Step 2 Configure TCP/IP parameters.

Table 15-2 Parameters description of TCP/IP

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.
NIC	Select the Ethernet card that needs to be configured, and the default one is **Wire**.
Mode	The mode that the camera gets IP: ● **Static** : Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login page with the configured IP address is displayed. ● **DHCP** : When there is DHCP server on the network, select **DHCP**, and the camera acquires IP address automatically.
MAC Address	Displays host MAC address.
IP Version	Select **IPv4** or **IPv6**.
IP Address	When you select **Static** in **Mode**, enter the IP address and subnet mask that you need. ● IPv6 does not have subnet mask. ● The default gateway must be in the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

Step 3 Click **Apply**.

15.2.2 Port

Configure the port numbers and the maximum number of users that can connect to the device simultaneously, including from the web client, platform client, and mobile phone client.

Procedure

Step 1 Select > **Network** > **Port**.

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 15-3 Parameters description of port

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
HTTP Port	Hypertext 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 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@10.12.4.84:554/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 **Apply**.

The configuration of **Max Connection** takes effect immediately, and others will take effect after reboot.

15.2.3 Auto Registration

After you enable this function, when the camera is connected to the Internet, it will report the current location to the specified server which acts as the transit to make it easier for the client software to access the camera.

Procedure

Step 1 Select > **Network** > **Auto Registration**.

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

Table 15-4 Parameters description of auto registration

Parameter	Description
Address	The IP address or domain name of the server to be registered.
Port	The port for registration.
Sub-Device ID	The custom ID for the camera.

Step 3 Click **Apply**.

15.2.4 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.

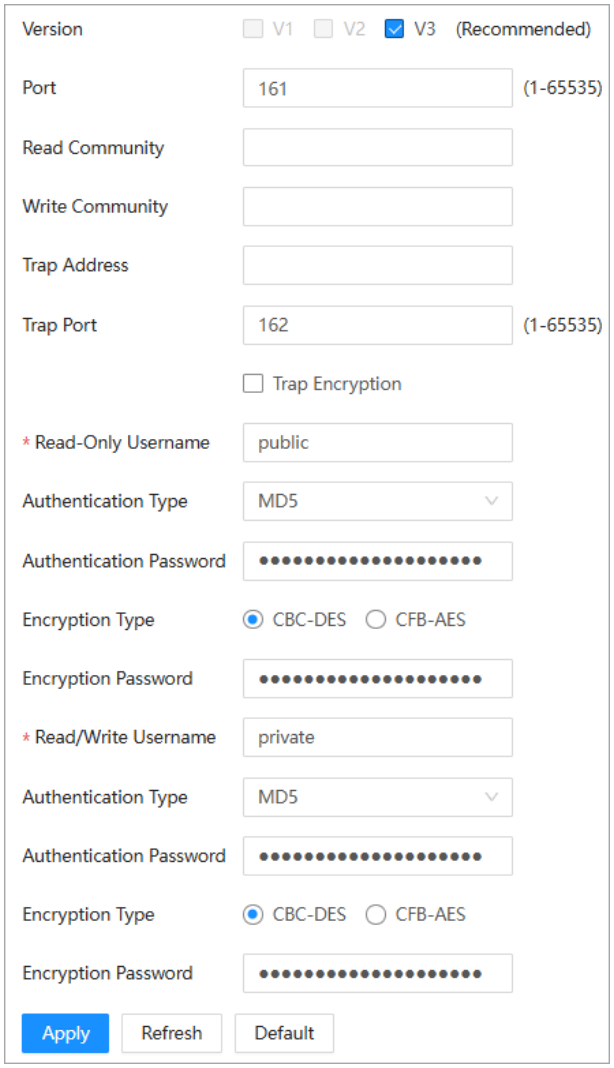
Prerequisites

- Install SNMP monitoring and managing tools such as MIB Builder and MG-SOFT MIB Browser.
- Get the MIB file of the matched version from technical support.

Procedure

Step 1 Select > **Network** > **SNMP**.

Figure 15-1 SNMP



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 user name, password and authentication type. It requires corresponding user name, 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 15-5 Parameters description of SNMP

Parameter	Description
Port	The listening port of the software agent in the device.

Parameter	Description
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.
Read-only Username	Set the read-only user name accessing device, and it is **public** by default. You can enter number, letter, and underline to form the name.
Read/Write Username	Set the read/write user name access device, and it is **private** 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 **Apply**.

Results

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.

15.2.5 Email

Configure email parameter and enable email linkage. The system sends email to the defined address when the corresponding alarm is triggered.

Procedure

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

Step 2 Click next to **Enable** to enable the function.

Step 3 Configure the parameters.

Table 15-6 Parameters description of email

Parameter	Description	
SMTP Server	SMTP server address	For details, see Table 15-7 .
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymous	Click , and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select from **None** , **SSL** and **TLS**. For details, see Table 15-7 .	
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click + to select title type, including **Device Name** , **Device ID**, and **Event Type**, and you can set maximum 2 titles.	
Attachment	Select the checkbox to support attachment in the email.	
Receiver	• Receiver's email address. Supports 3 addresses at most. • After entering the receiver's email address, the **Test** button is displayed. Click **Test** to test whether the emails can be sent and received successfully.	

Table 15-7 Description of major mailbox configuration

Mailbox	SMTP server	Authentication	Port	Description
Gmail	smtp.gmail.com	SSL	465	You need to enable SMTP service in your mailbox.
		TLS	587	

Step 4 Click **Apply**.

15.2.6 Platform Access

15.2.6.1 P2P

P2P (peer-to-peer) technology enables users to manage devices easily without requiring DDNS, port mapping or transiting server. Scan the QR code with your smartphone, and then you can add and manage more devices on the mobile phone client.

Procedure

Step 1 Select > **Network** > **Platform Access** > **P2P**.

Step 2 Click to enable the function.

Step 3 Log in to mobile phone client and tap **Device management**.

Step 4 Tap **+** on the upper-right corner.

Step 5 Scan the QR code on the **P2P** page.

Step 6 Follow the instructions to finish the settings.

15.2.6.2 ONVIF

The ONVIF verification is enabled by default, which allows the network video products (including video recording device and other recording devices) from other manufacturers to connect to your device.

ONVIF is enabled by default.

Procedure

Step 1 Select > **Network** > **Platform Access** > **ONVIF**.

Step 2 Select **Open** from **Login Verification** to enable the function.

Step 3 Click **Apply**.

15.2.6.3 ITSAPI

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

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

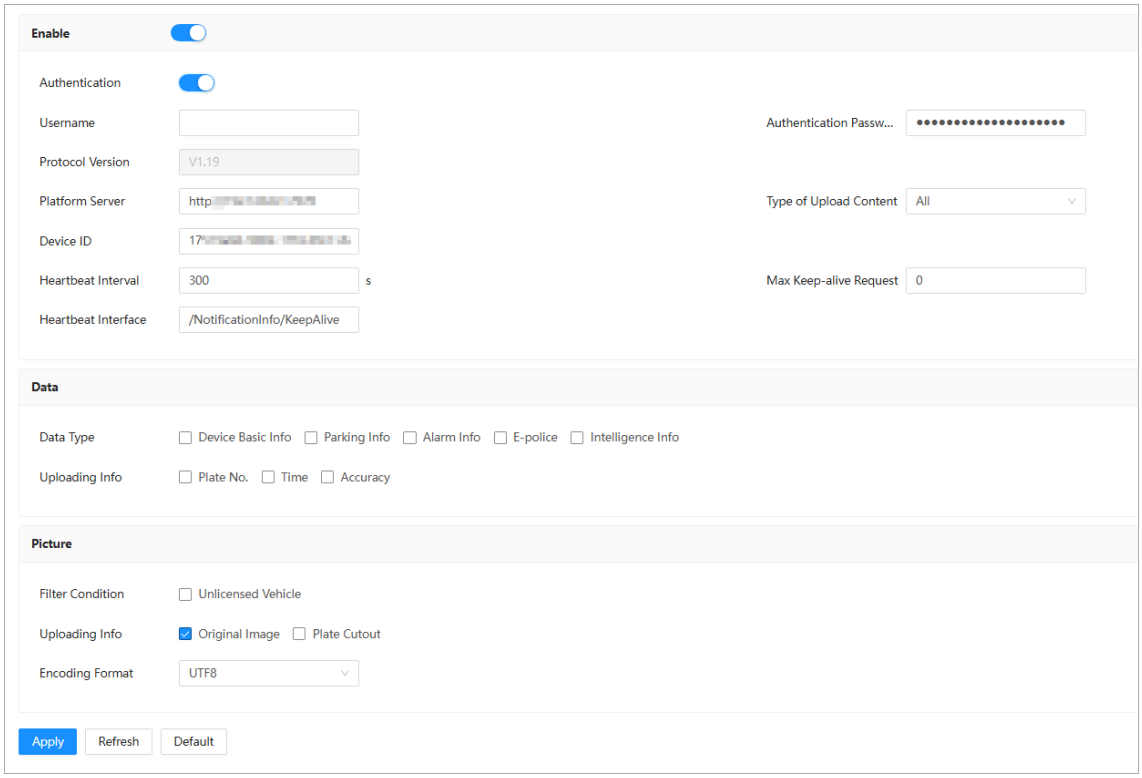
  IO multiplexing must be available on the server.
- Related business data must be in JSON format with ContentType: application/ json;charset=UTF-8 as HTTP headers, which means the encoding method is UTF-8.

Procedure

Step 1 Select > **Network** > **Platform Access** > **ITSAPI**.

Step 2 Click next to **Enable** to enable the function.

Figure 15-2 ITSAPI



Step 3 Configure the parameters.

Table 15-8 Parameters description of ITSAPI

Section	Parameter	Description
Basic Configuration	Authentication	Click to enable the function, and then enter the user name and authentication password.
	Protocol Version	Setting is not supported and subject to actuality.
	Platform Server	Enter the platform server address.
	Type of Upload Content	Select the upload type, including **ALL** , **Data** and **Picture**.
	Device ID	Enter the device ID.
	Heartbreak Interval	The heartbreak time between the device and the platform server.
	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.
	Heartbreak Interface	Set the interface according to the data type.
Data	Data Type	Select the data type to be uploaded.
	Uploading Info	Select the specific information to be uploaded.
Picture	Filter Condition	Select whether to upload information of unlicensed vehicles.
	Uploading Info	Select the type of images to be uploaded.

Section	Parameter	Description
	Encoding Format	Select the license plate encoding format. ● **UTF-8** supports many languages and it is selected by default. ● **ASCII** supports relatively few languages, generally only English and some symbols.

Step 4 Click **Apply**.

15.2.7 Basic Services

Configure the IP hosts (devices with IP address) that are allowed to visit the device. Only the hosts in the trusted sites list can log in to the webpage. This is to enhance network and data security.

Procedure

Step 1 Select > **Network** > **Basic Services**.

Step 2 Enable the basic service according to the actual needs.

Table 15-9 Parameters description of basic service

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Enable this function, and then when multiple users are viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
CGI	CGI is the port between external application program and web server.
ONVIF	Realizes network video framework agreement to make different network video products interconnected.
Private Protocol	Enable this function to transmit data through private protocols.
Private Protocol Authentication Mode	Select the authentication mode from **Security Mode** and **Compatible Mode**. Security mode is recommended.
TLSv1.1	Enable this function so that you can access the webpage with TLSv1.1. There might be security risks if you enable this function. Please be advised.
LLDP	Enable this function, and then the camera can exchange connection information with network devices (such as switches).

Step 3 Click **Apply**.

15.3 Event

15.3.1 Setting Exception

Exceptions include SD card, network, and defocus detection.

Only the device with SD card has the abnormality functions, including **No SD card** , **SD card error**, and **Low SD card space**.

15.3.1.1 Setting SD Card Exception

In case of SD card exception, the system performs alarm linkage. The event types include **No SD card** , **Low SD card space**, and **SD card error**. Functions might vary with different models.

Procedure

Step 1 Select > **Event** > **Exception** > **SD Card Exception**.

Step 2 Click to enable detection of one or more events.

Step 3 Configure the parameters.

Table 15-10 Parameters description of SD card exception

Parameter	Description
Alarm Channel	Click , and then select an alarm output channel. The corresponding device will be activated when alarms are triggered.
Post-alarm	When an alarm is triggered, it will continue for the defined period after it ends.
Free Space	When enabling **Low SD card space** , set a value for **Free Space**. When the remaining space of SD card is less than this value, an alarm is triggered.

Step 4 Click **Apply**.

15.3.1.2 Setting Network Exception

In case of network abnormality, the system performs alarm linkage. The event types include **Offline** and **IP Conflict**.

Procedure

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

Step 2 Click to enable detection of one or more events.

Step 3 Configure the parameters.

Table 15-11 Parameters description of exception

Parameter	Description
Offline	Click to enable the function. When the network is detected offline, it will trigger an alarm.

Parameter	Description
IP Conflict	Click to enable the function. When there is an IP conflict, it will trigger an alarm.

Step 4 Click **Apply**.

15.3.2 Video Detection

Procedure

Step 1 Click to enable the function.

Step 2 Configure the parameters.

Figure 15-3 Configure the video detection

Table 15-12 Parameters description of exception

Parameter	Description
Detection Sensitivity	The higher the value, the easier the vehicles will be detected.
Anti-dither	Enter anti-dither time (1–100 seconds). System will only record one when there are multiple alarms during the defined time.

15.4 Local Storage

Display the information on the local SD card. You can set hot swap, and format SD card.

Procedure

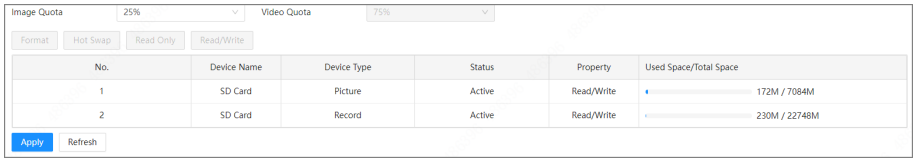
Step 1 Select > **Storage** > **Local Storage**.

Step 2 Configure the hot swap and format the SD card.

- Click **Hot Swap** before you pull out the SD card to prevent data loss.
- Click **Format**, and then you can format the SD card.

  The data will be cleared after the SD card is formatted. Please be cautious.
- **Read Only** : The camera can only read file on the SD card.
- **Read/Write** : The camera can read files on and write data to the SD card.

Figure 15-4 Local storage configuration



Step 3 Click **Apply**.

Appendix 1 Security Recommendation

Account Management

1. **Use complex passwords**

   Please refer to the following suggestions to set passwords:

   - The length should not be less than 8 characters;
   - Include at least two types of characters: 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 123, abc, etc.;
   - Do not use repeating characters, such as 111, aaa, etc.
2. **Change passwords periodically**

   It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.
3. **Allocate accounts and permissions appropriately**

   Appropriately add users based on service and management requirements and assign minimum permission sets to users.
4. **Enable account lockout function**

   The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.
5. **Set and update password reset information in a timely manner**

   The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

   It is recommended that you enable HTTPS to access web services through secure channels.
2. **Encrypted transmission of audio and video**

   If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.
3. **Turn off non-essential services and use safe mode**

   If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

   If necessary, it is highly recommended to choose safe modes, including but not limited to the following services:

   - SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up complex passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.
4. **Change HTTP and other default service ports**

   It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

   It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.
2. **MAC address binding**

   It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.
3. **Build a secure network environment**

   In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

   - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
   - According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
   - Stablish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

   It is recommended to check online users regularly to identify illegal users.
2. **Check device log**

   By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.
3. **Configure network log**

   Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

   According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.
2. **Update client software in time**

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

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).