Smart ANPR Camera

Web 5.0 Operation Manual



V1.2.0

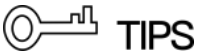
Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of smart ANPR camera. Read carefully before using the platform, and keep the manual safe for future reference.

Symbols

The following symbols might appear in the manual.

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

Revision History

Version	Revision Content	Release Date
V1.2.0	Updated snapshot settings, platform access, and more.	October 2026
V1.1.0	Added parking space management and illegal parking area, and updated IVS configuration.	November 2025
V1.0.3	Added images and videos sections.	October 2024
V1.0.2	Added maintenance center.	September 2023
V1.0.1	Updated the color theme of the webpage.	August 2023
V1.0.0	First release.	April 2023

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays,

potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

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. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- The power supply must meet the rated voltage requirements as indicated on the device label.
- If the device uses a power adapter, ensure it meets the following requirements:
  - If a power adapter was shipped with your device, we recommend you use it. If you need to buy a separate adapter, make sure it meets the following requirements.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.

- Do not connect the power adapter to the device while the adapter is powered on.

- 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 Configuration Flow 3
3 Device Initialization 4
4 Login 7
4.1 Device Login 7
4.2 Resetting Password 7
5 Home Page 8
6 Configuration Wizard 10
7 Live 12
7.1 Live Page 12
7.2 Video Adjustment 13
7.3 Frequently Used Functions 14
7.3.1 Zoom and Focus 14
7.3.2 Snapshot 15
7.3.3 Peripheral 16
7.3.4 Light 17
7.3.5 Device Test 19
7.4 Live View Function Bar 20
7.5 Display Mode 20
8 ANPR 22
8.1 Snapshot 22
8.1.1 Configuring Snapshot 22
8.1.2 Configuring Main and Sub Stream Snapshot Optimization 24
8.2 Configuring AI Setting 25
8.2.1 Intelligent Analysis 25
8.2.2 Smart Detection 25
8.3 Image Configuration 27
8.3.1 Original Picture OSD 27
8.3.2 Size 29
8.3.3 Cutout Configuration 30
8.4 Vehicle Blocklist and Allowlist 30
8.4.1 Fuzzy Match 30
8.4.2 Allowlist 31

8.4.3 Blocklist 33
8.5 Configuring Barrier Control 33
8.5.1 Barrier Control 33
8.5.2 Remote Control 34
8.6 Configuring RS-485 Settings 35
8.7 Configuring LED Screen 40
8.8 Configuring Broadcast 41
8.8.1 Event Broadcast 41
8.8.2 Passing Vehicles 42
8.8.3 Volume/Encoding 44
8.8.4 Audio File 44
8.9 Setting Device Test 45
8.9.1 Device Test 45
8.9.2 Capture Adjustment Information 46
8.9.3 Collection Log 46
8.10 Available Space Count 47
8.11 Configuring Wiegand 49
9 IVS 50
9.1 Configuring IVS 50
9.2 Parking Space Management 52
9.3 Illegal Parking Area 53
10 Picture 55
10.1 Image Search 55
10.2 Storage 56
10.2.1 Local 56
10.2.2 Network 56
10.3 Platform Server 58
11 Record 60
11.1 Video Search 60
11.2 Record Control 61
11.3 Time Plan 62
11.4 Storage 62
12 Search 64
12.1 Snapshot Records 64
12.1.1 Configuring Snapshot Records 64
12.1.2 Sending Email 64
12.2 Alarm-Out Port 65
12.3 Barrier Logs 65
12.4 Radar Logs 65
12.5 Parking Records 66

12.6 Passed Vehicles Records..... 66
12.7 Searching Images..... 66
12.8 Searching Video..... 67
12.8.1 Record..... 67
12.8.2 Watermark..... 67
13 Camera..... 68
13.1 Setting Image Parameters..... 68
13.1.1 General Parameters..... 68
13.1.2 Shutter Parameters..... 72
13.1.3 Metering Parameters..... 73
13.2 Setting Encode Parameters..... 74
13.2.1 Video Stream..... 74
13.2.2 Video OSD..... 76
13.2.3 ROI..... 80
14 System..... 81
14.1 General Parameters..... 81
14.1.1 General..... 81
14.1.2 Date..... 81
14.2 Account..... 82
14.2.1 User..... 83
14.2.2 Adding a User Group..... 85
14.2.3 Adding an ONVIF User..... 86
14.2.4 Clearing Users..... 87
15 Security..... 88
15.1 Security Status..... 88
15.2 System Service..... 89
15.2.1 802.1x..... 89
15.2.2 HTTPS..... 91
15.3 Attack Defense..... 92
15.3.1 Firewall..... 92
15.3.2 Account Lockout..... 93
15.3.3 Anti-DoS Attack..... 93
15.4 CA Certificate..... 94
15.4.1 Installing Device Certificate..... 94
15.4.2 Installing Trusted CA Certificate..... 96
15.5 A/V Encryption..... 97
15.6 Security Warning..... 99
15.6.1 Security Exception..... 99
15.6.2 Illegal Login..... 99
15.7 Security Authentication..... 100

16 Maintenance Center....101
16.1 One-Click Diagnosis....101
16.2 System Information....102
16.2.1 Version....102
16.2.2 Online User....102
16.2.3 Running Status....102
16.2.4 Legal Info....103
16.3 Log....103
16.3.1 Searching for Logs....103
16.3.2 Obtaining Remote Logs....104
16.4 Maintenance Management....104
16.4.1 Maintenance....105
16.4.2 Import/Export....105
16.4.3 Default....106
16.5 Update....106
16.6 Advanced Maintenance....107
17 Setting....109
17.1 Local....109
17.2 Network....109
17.2.1 TCP/IP....110
17.2.2 Port....111
17.2.3 DDNS....113
17.2.4 Auto Registration....114
17.2.5 Multicast....114
17.2.6 SNMP....115
17.2.7 Email....117
17.2.8 PPPoE....118
17.2.9 Platform Access....119
17.2.10 Basic Services....124
17.2.11 RTMP....125
17.3 Event....127
17.3.1 Setting Alarm....127
17.3.2 Setting Exception....128
17.3.3 Rule Configuration....130
17.3.4 Subscribing Alarm....130
17.4 Local Storage....132
Appendix 1 Security Recommendation....134

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 Configuration Flow

Figure 2-1 Configuration flow

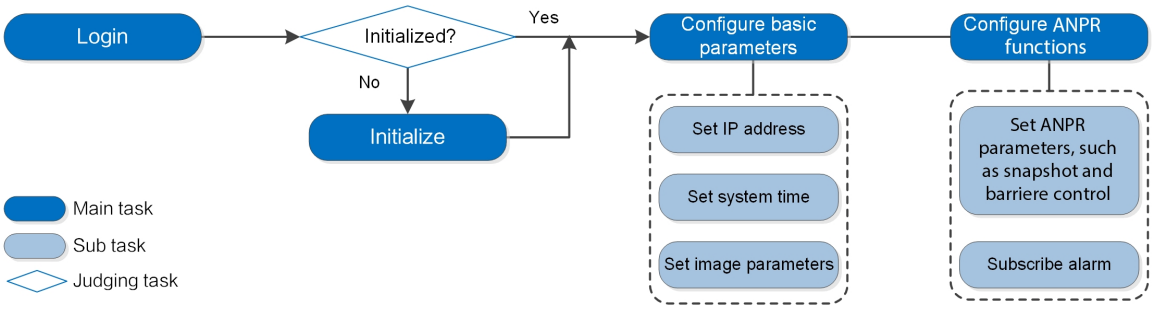


Table 2-1 Description of flow

Configuration		Description	Reference
Login		Open an internet browser and enter the IP address to log in to the webpage. The default IP address is 192.168.1.108.	"4.1 Device Login"
Initialization		Initialize the camera when you use it for the first time.	"3 Device Initialization"
Basic parameters	Camera parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	"13 Camera"
	Date & time	Set date and time to ensure the recording time is correct.	"14.1.2 Date"
	IP address	Change IP address according to network planning for the first use or during network adjustment.	"17.2.1 TCP/IP"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"17.3.4 Subscribing Alarm"
ANPR	ANPR parameters	Configure parameters for various ANPR functions, such as taking snapshots of vehicles.	"8 ANPR"

3 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 3-1 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.

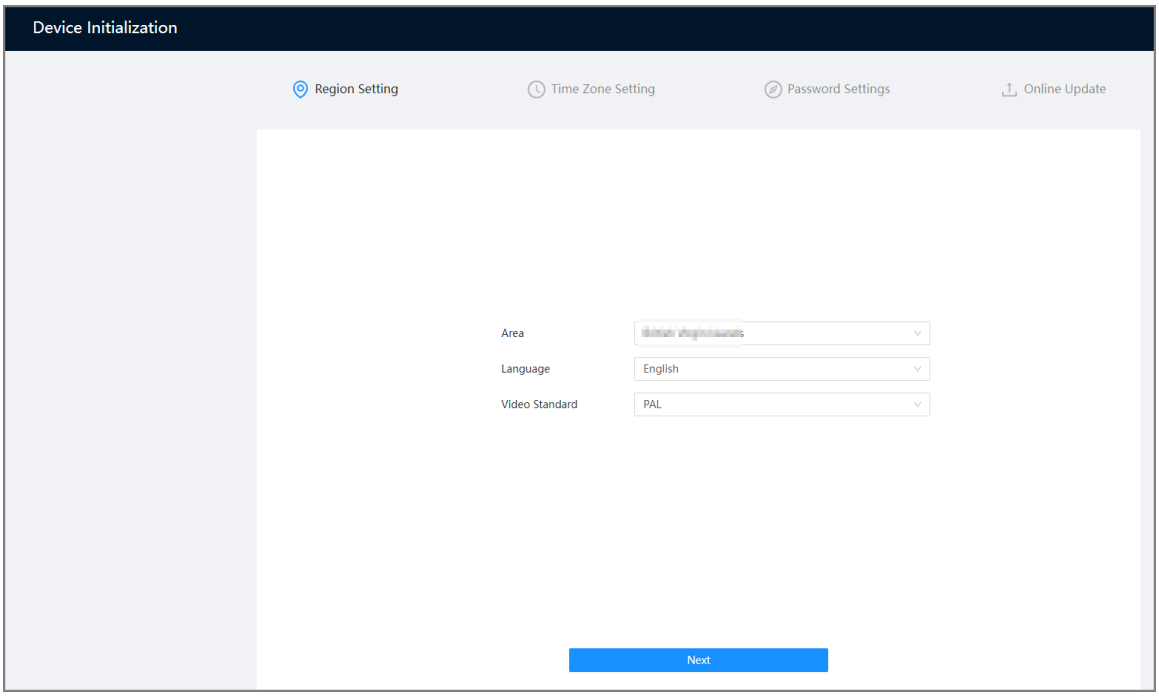
- The latest versions of Google Chrome and Microsoft browsers are supported. Most functions are available without a plug-in. A few functions require downloading a plug-in, but they still work with Google Chrome.
- Internet Explorer (IE) is not recommended. Before using it, clean up the web3.0 plug-in 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.

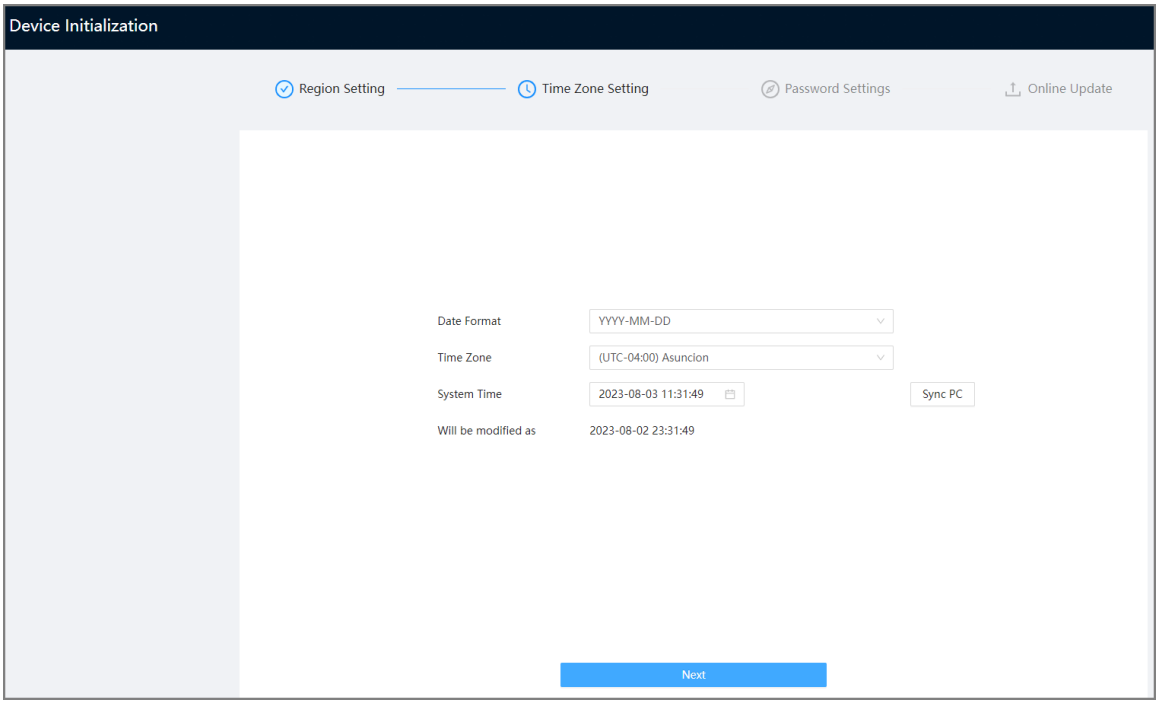
Step 2 Select the area, language, and video standard, and then click **Next**.

Figure 3-1 Region setting



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

Figure 3-2 Time zone setting



Step 4 Set the password for admin account.

Figure 3-3 Password setting

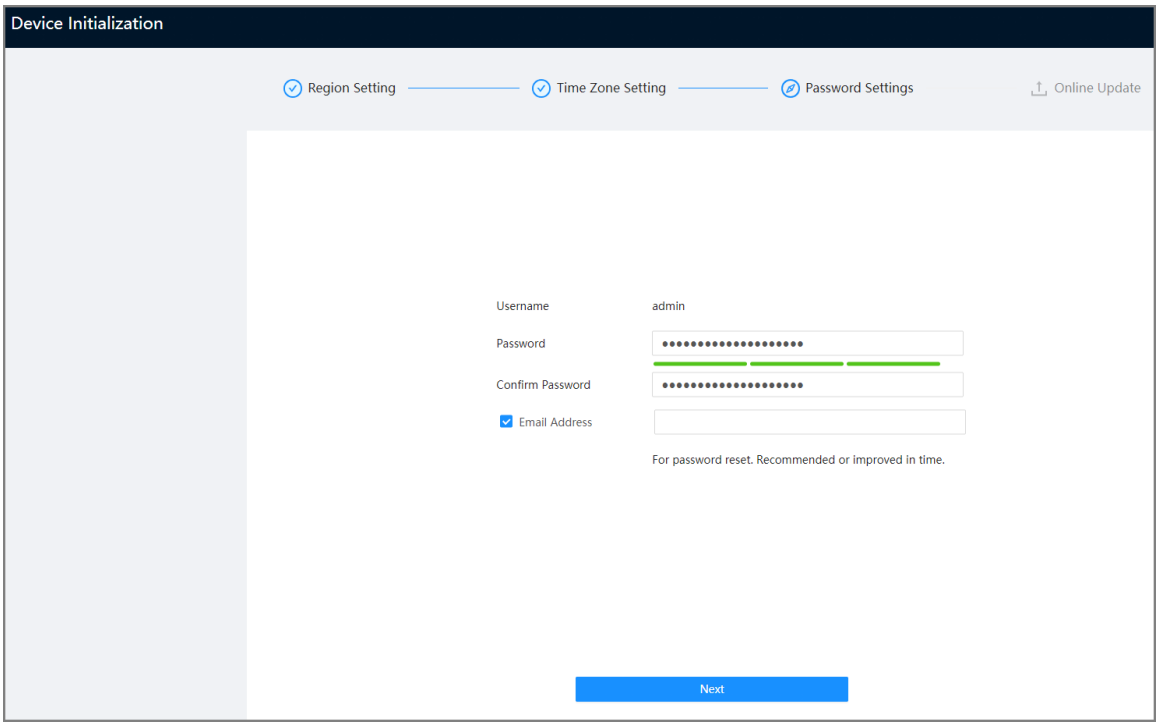


Table 3-2 Description of password configuration

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.

4 Login

4.1 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 "3 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 "4.2 Resetting Password".

Step 3 Click **Login**.

4.2 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 "14.2.1.2 Resetting Password".

Procedure

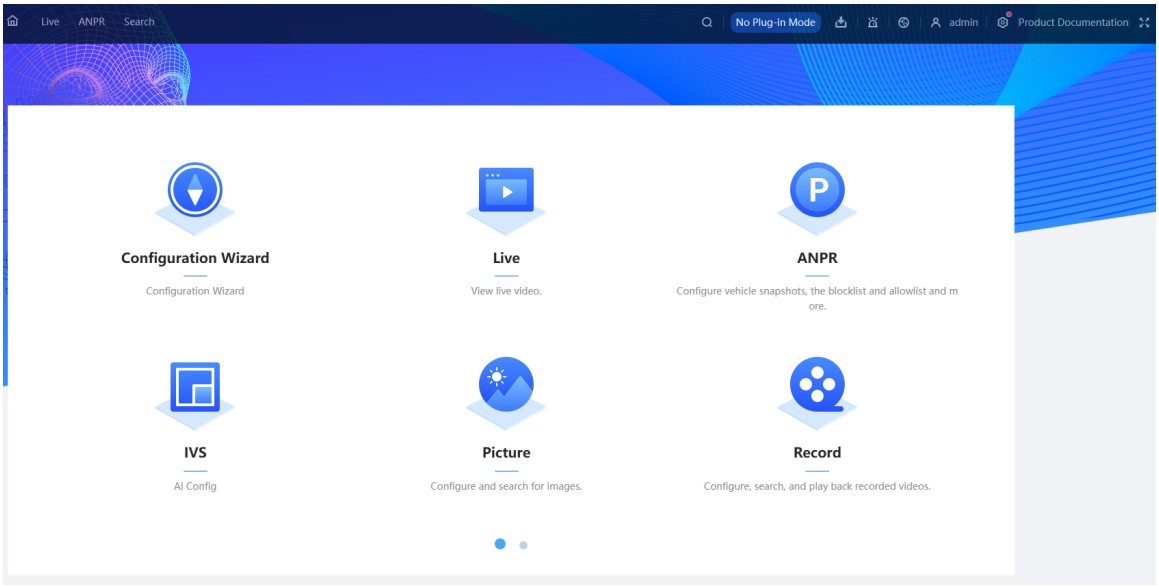
Step 1 Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.

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

5 Home Page

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

Figure 5-1 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.
- IVS: Configure AI functions related to parking management.
- 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.
- : Search and view the menu.
- : Download the plug-in.
- : Subscribe to various types of alarms.

- : Set the skin of the webpage.
- : Set the language of the webpage.
- Restart: Click admin at the upper-right corner of the page, select **Restart**, and the camera restarts.
- Logout: Click admin 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.

6 Configuration Wizard

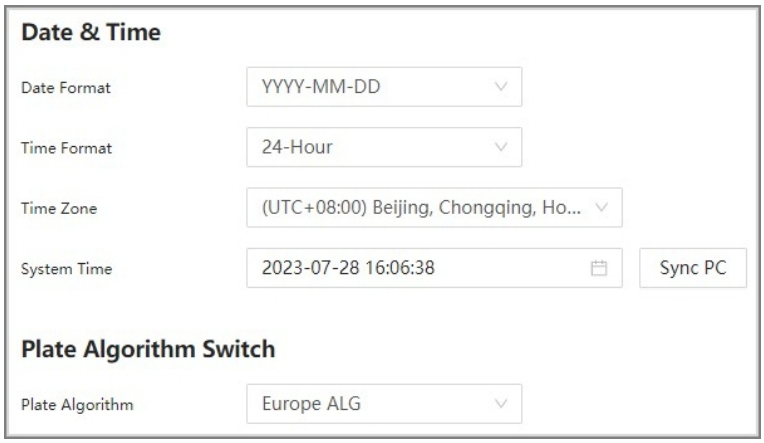
You can configure the scene for capture, and use various functions to help you with different installation scenarios.

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

Procedure

Step 1 Click **Configuration Wizard**.

Figure 6-1 Configuration wizard

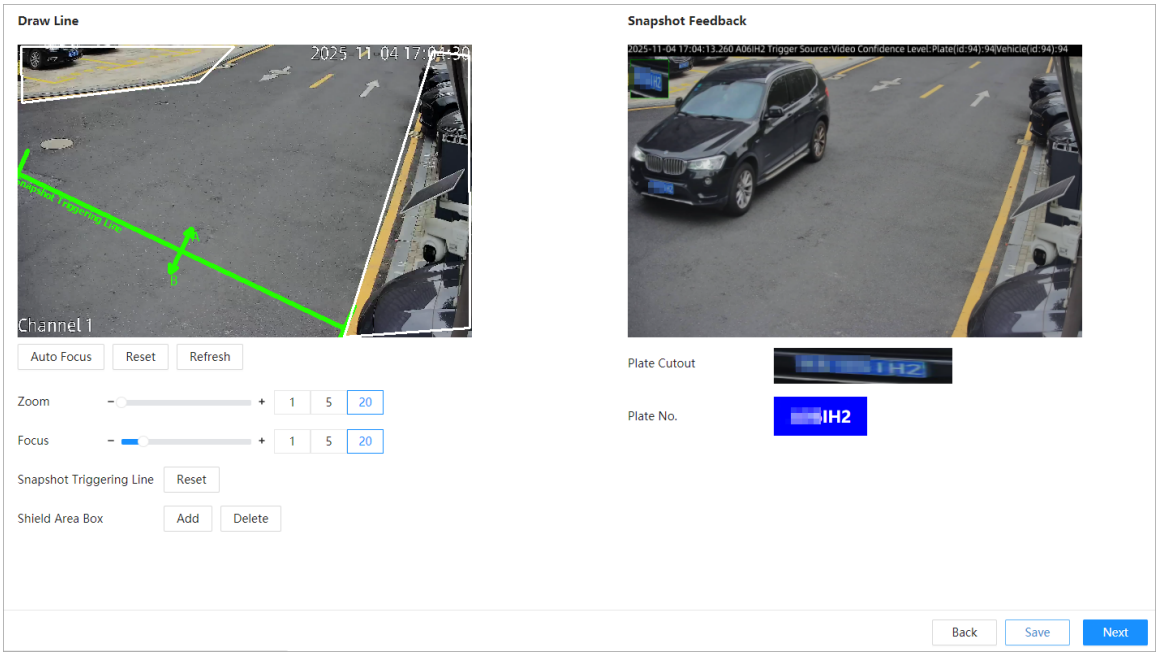


Step 2 Select the basic date and time format and system time of the camera, and then click **Next**.

- 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, refer to the datasheet of your device.

Step 3 Check whether the video image is properly zoomed, and focused by the plate pixel.

Figure 6-2 Adjust the video for recognition



1. Drag the zoom and focus bars to adjust the video image until the image is clear.
2. Follow the tips on the figure on the left side, and then draw an area for capturing vehicles that enter.
3. Click **Add** next to **Shield Area Box** to draw areas that the camera does not recognize.

   Click **Delete** to delete the area.
4. Drag the **Snapshot Triggering Line** to specify the location of taking the snapshots.
5. Click **Next**.

Step 4 Click **Go to Home Page**.

7 Live

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

7.1 Live Page

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

The pages might vary with different models.

Figure 7-1 Live Page

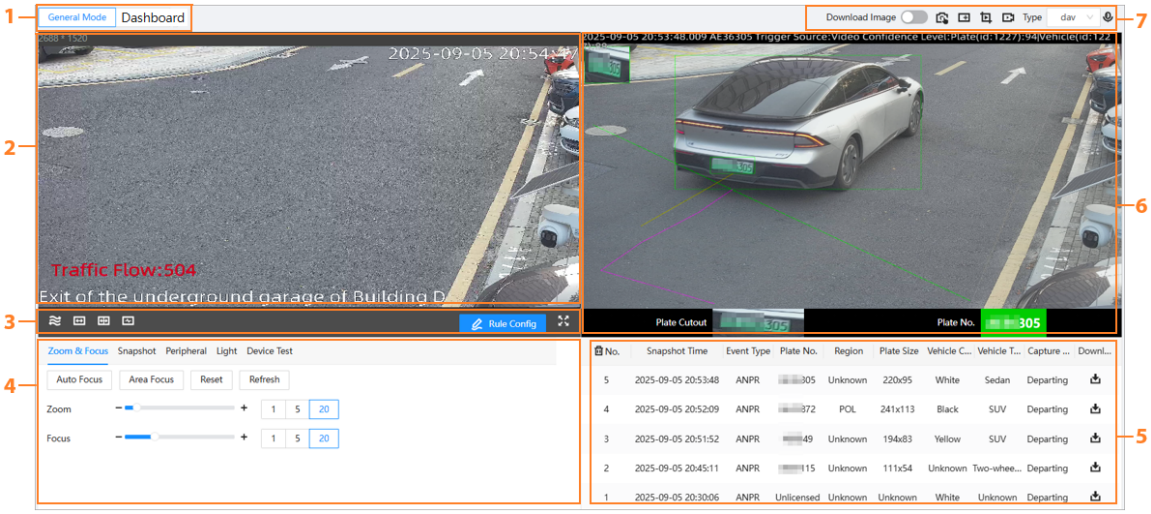


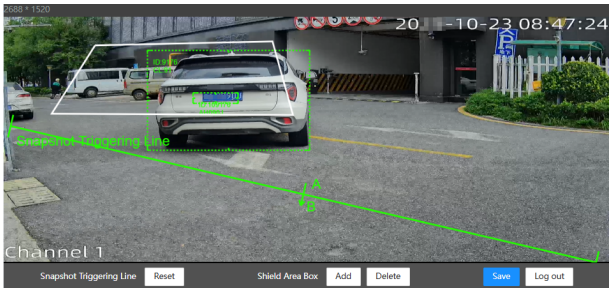
Table 7-1 Function description

No.	Function	Description
1	Display mode	The display modes include general mode and dashboard. For details, see "7.5 Display Mode".
2	Live view	Displays real-time video.
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	Display vehicle snapshot, plate cutout, and plate number.
7	Live view function bar	Functions and operations in live view.

7.2 Video Adjustment

Table 7-2 Description of adjustment bar

Icon	Function	Description
	Smoothness Adjustment	Change the fluency of the video. Select one based on your network bandwidth. • **Realtime** : Guarantees the real time of the video. When the network bandwidth is not enough, the video might not be smooth. • **General** : Strikes a balance between **Realtime** and **Fluent**. • **Fluent** : Guarantees the fluency of the video but the video might not be real-time.
	W:H	Adjust the display scale, that is, the ratio between the width and the height of the live video display. • Original: Restore to the original display size. • Adaptive: Maximize the video to the full-screen display.
	AI Rule	Click the icon, and then select **Enable** to display AI rules and detection box; select **Disable** to stop the display. It is enabled by default.
	Main Stream/Sub Stream	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.

Icon	Function	Description
Rule Config		 • Drag the snapshot triggering line to specify the capture location. Vehicles are captured when crossing the line. • If vehicles frequently appear near the capture area, use the shielding areas so that the camera will not detect vehicles in them. Drag the 4 corners of shield area boxes to delimit the scope. Up to 3 shielding areas can be added.
	Full Screen	Displays the video in full-screen mode. Double-click or press Esc to exit full-screen mode.

7.3 Frequently Used Functions

7.3.1 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 7-2 Zoom and focus

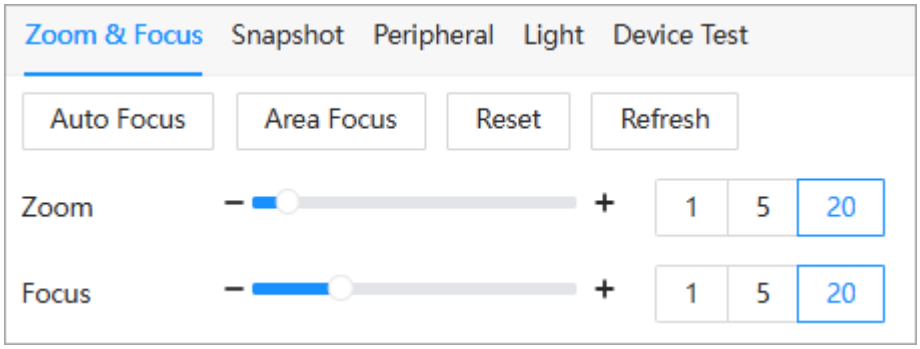


Table 7-3 Parameters description of zoom and focus

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.

7.3.2 Snapshot

Click **Snapshot** on the lower-left corner to configure parameters related to snapshots, and then click **Apply**.

Figure 7-3 Snapshot

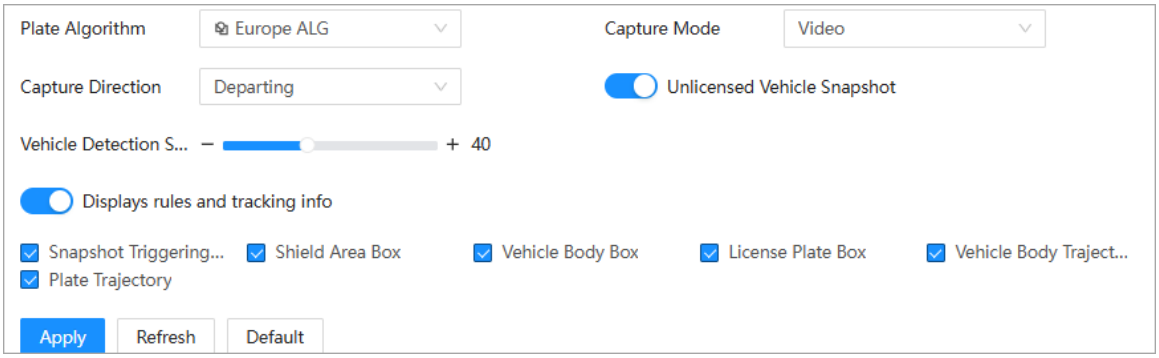


Table 7-4 Parameters description of snapshot

Parameter	Description
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.
Capture Mode	Select a mode to apply related parameters. For details on the parameters, see "8.1.1 Configuring Snapshot".
Capture Direction	• **Approaching** : Only captures vehicles that approach. • **Departing** : Only captures vehicles that depart. • **Both Ways** : Captures vehicles that approach or depart.
Vehicle Detection Sensitivity	The higher the value, the easier the vehicles will be detected.
Unlicensed Vehicle Snapshot	After it is enabled, the camera will take snapshots of vehicles with no license plates.
Displays rules and tracking info	Click to enable the function, and then select one or more types of information you want to display. When enabled, the selected information will be displayed on snapshots.

7.3.3 Peripheral

Click **Peripheral** to set the working mode of the LED screen and how the barrier will open, and then click **Apply**.

Figure 7-4 Peripheral

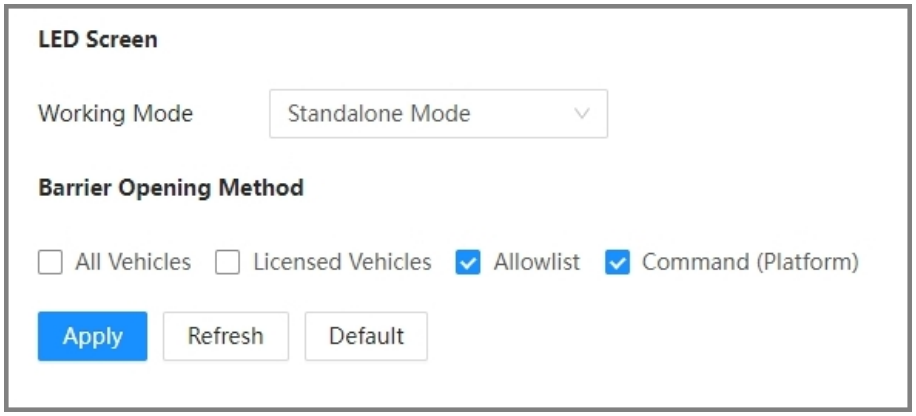


Table 7-5 Parameters description of peripheral

Parameter	Description
LED Screen	Set the working mode for the screen. • **Standalone Mode** : Display as configured, and not controlled by any platforms. • **Partially Managed Mode (Platform)** : Select this to allow the platform to control parts of the screen information. • **Managed Mode (Platform)** : Grant the platform complete control over the information on the screen.
Barrier Opening Method	Triggers alarm through different modes, and remotely controls the barrier opening and close. • **All Vehicles** : When the camera captures any vehicle, it outputs an open barrier signal. • **Licensed Vehicles** : When the camera captures any plate, it outputs an open barrier signal. • **Allowlist** : When the camera captures vehicles that are on the allowlist or conform to fuzzy matching, it outputs an open barrier signal. • **Command (Platform)** : The camera outputs an open barrier signal when it receives a command from the platform. You can set barrier opening control to **Allowlist** and **Command (Platform)** at the same time.

7.3.4 Light

Click **Light** to configure the working mode and brightness for the camera illuminator and RS-485 illuminator.

Figure 7-5 Light

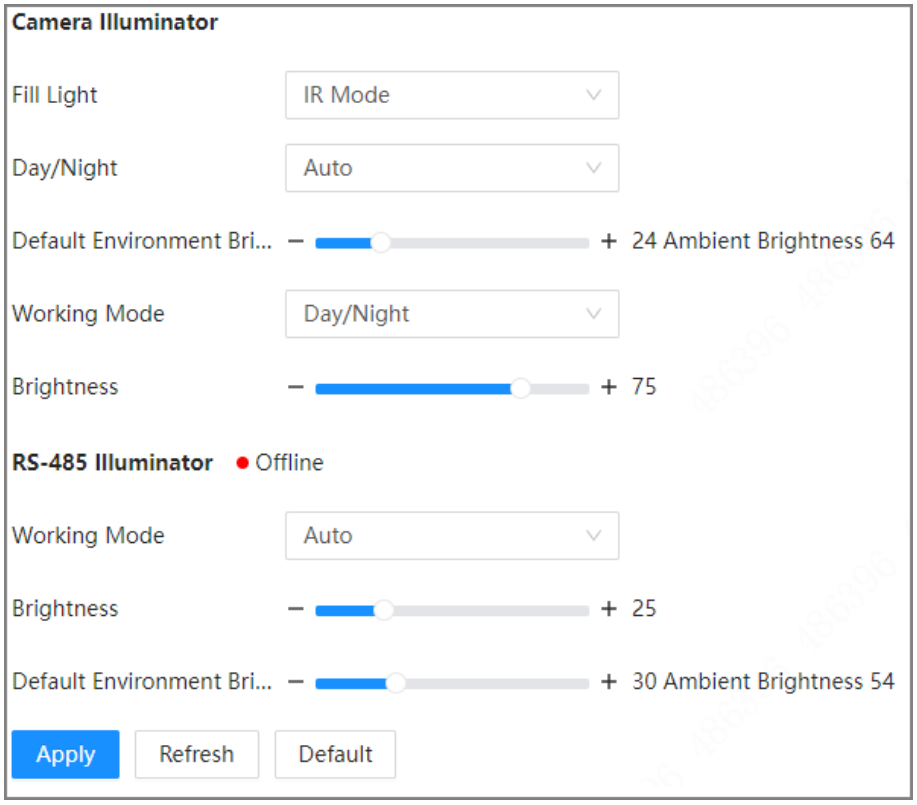


Table 7-6 Parameters description of light

Parameter	Description
Camera Illuminator	• **Fill Light** : IR Light/White Light. • **Day/Night** : ICR Switch. • **Working Mode** : Select a working mode for the light. If you select **By Time**, you must configure the time schedule. For details, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports". • **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.

Parameter	Description
RS-485 Illuminator	• **Working Mode** : Select a working mode for the light. If you select **By Time**, you must configure the time schedule. For details, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports". • **Brightness** : The higher the value, the brighter the light. • **Default Environment Brightness** : Set a default value for the environment brightness. ◇ When the **Ambient Brightness** is lower than the value, the RS-485 illuminator will be automatically turned on. ◇ When the **Ambient Brightness** is higher than the value, the RS-485 illuminator will be automatically turned off.

7.3.5 Device Test

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

Figure 7-6 Device test

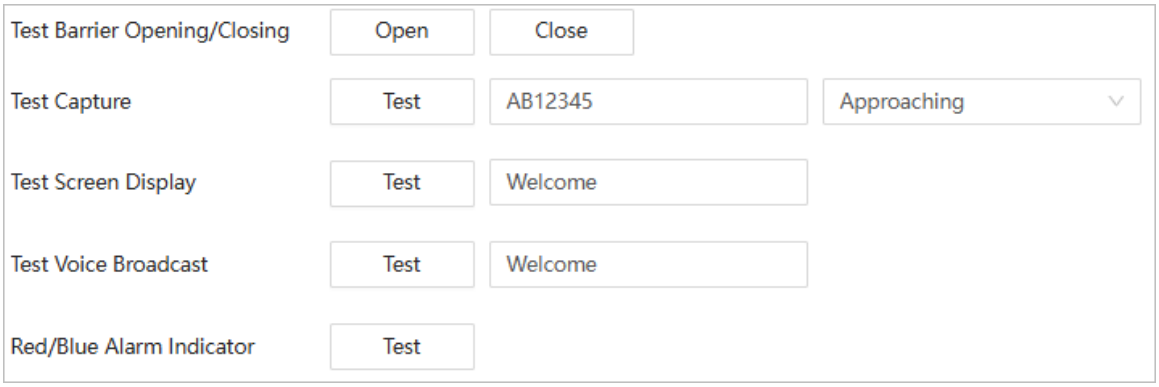


Table 7-7 Parameters description of device test

Parameter	Description
Test Barrier Opening/Closing	Click **Open** or **Close** to test whether the barrier responds correctly.
Test Capture	Enter a plate number, click **Test** to trigger capture, and then view the snapshot in the **Live** page.
Test Screen Display	Enter some information, click **Test**, and then view whether the information is correctly displayed on the LED screen.
Test Voice Broadcast	Enter some information, and then click **Test** to check whether the device plays the sound normally.
Red/Blue Alarm Indicator	Only available for the ITC413 series products. Click **Test** to check if the red/blue alarm indicator works normally.

7.4 Live View Function Bar

For the live view function bar, see Table 7-8 .

Table 7-8 Function description

Icon	Description
	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.
	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.
	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.

7.5 Display Mode

2 modes are available: **General Mode** and **Dashboard**.

- General mode is typically used for daily observation and installation assistance, which includes frequently used functions such as adjusting the zoom and focus and parameters related to snapshots.
- Dashboard supports displaying real-time snapshots, and the statistics on passed vehicles, barrier opening times, ANPR alarms, frequent visitors, and more.

Figure 7-7 General mode

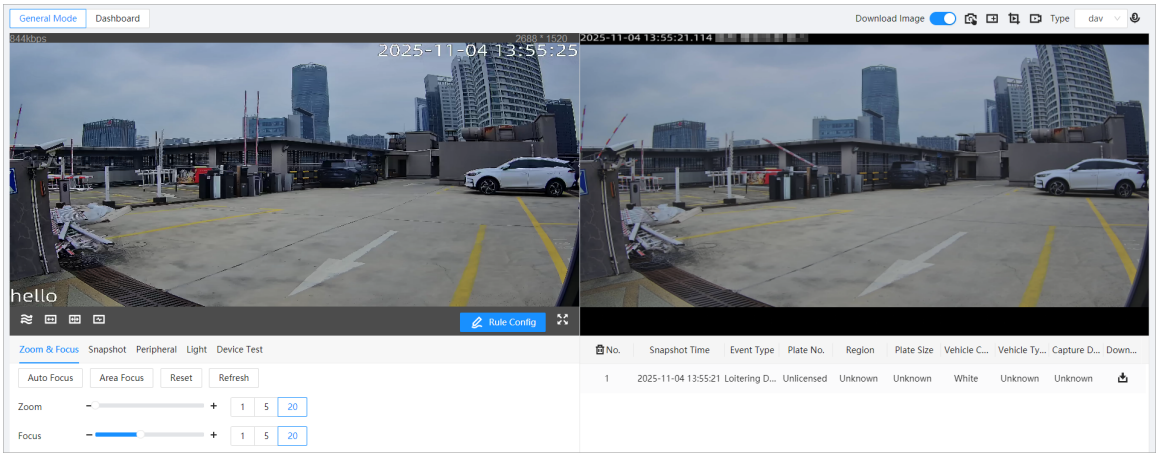
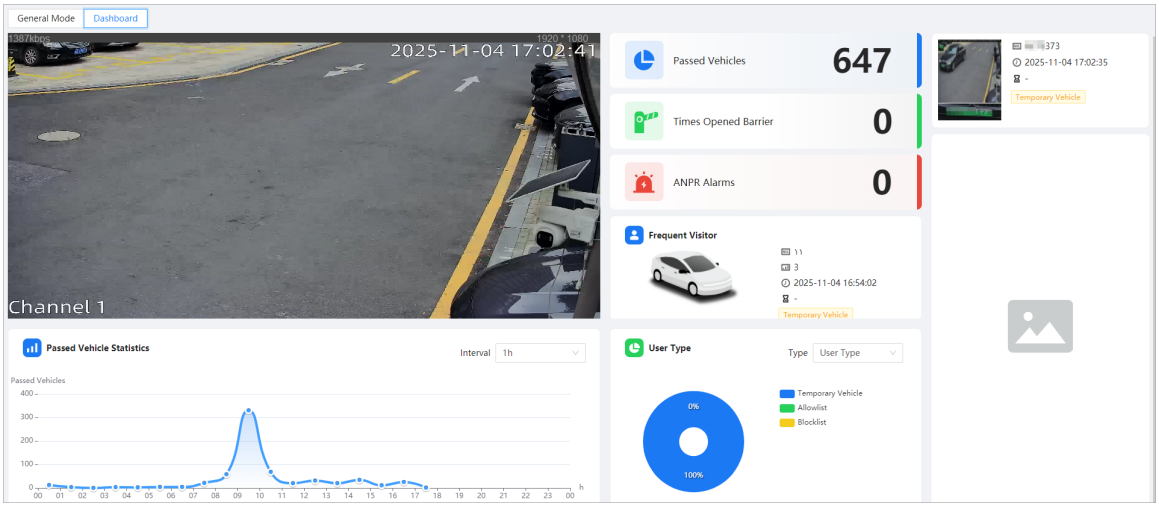


Figure 7-8 Dashboard



8 ANPR

8.1 Snapshot

Supports snapshot setting and main and sub stream snapshot optimization of the camera.

8.1.1 Configuring Snapshot

You can set snapshot rule of the camera.

Procedure

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

Step 2 Configure the parameters.

Table 8-1 Parameters description of snapshot

Type	Parameter	Description
General Parameters	Capture Mode	• **Loop** : Snapshots will be taken when targets enter a loop. • **Video** : Snapshots will be taken when video analyzes the targets. • **Mixed Mode** : Combine both loop and video for taking the snapshots.
	Capture Direction	• **Approaching** : Only captures vehicles that approach. • **Departing** : Only captures vehicles that depart. • **Both Ways** : Captures vehicles that approach or depart.
	Same Plate Capture Interval	Set the time interval during which one plate can only be captured once.
Video Mode Parameters Only available when the **Capture Mode** is set to **Video** or **Mixed Mode**.	Unlicensed Vehicle Snapshot	When it is enabled, vehicles without license plates will be captured.
	Sensitivity	Vehicle capture sensitivity. The higher the value, the easier vehicles will be captured. It is **High** by default.
	Filter Vehicle Back	Filters images that capture the vehicle back. Applicable only when **Capture Direction** is set to **Approaching**.

Type	Parameter	Description
Scheduled Snapshot	Enable	Enable scheduled snapshot, and set the interval and times. The camera will take snapshots of the defined times according to the defined interval.
	Interval	
	Times	
Loop Mode Parameters Only available when the **Capture Mode** is set to **Loop** or **Mixed Mode**.	Plan	Set the scheme of snapshots triggered by the loop. • **Single Loop** : A single loop is set. It will take a snapshot when the vehicle enters a loop. • **Dual Loop** : 2 single loops are placed several meters apart. It is used to determine the driving direction of the vehicle. The 1N1 signal is triggered firstly, then it will take a forward snapshot when the 1N2 signal is triggered.
	Loop1	Set the loop trigger mode. • **Do Not Trigger** : No capture is triggered. • **Rising Edge** : Capture is triggered when the vehicle enters loop. • **Falling Edge** : Capture is triggered when the vehicle exits the loop. When the scheme is **Single Loop**, then loop 2 cannot be set.
	Loop2	
	Max Vehicle Pass Time	In loop mode, when a vehicle passes the first loop, and within the defined maximum vehicle passing time (5 seconds by default), the vehicle passes the first loop again, the camera will not capture the vehicle. The helps reduce interference.

Step 3 Click **Apply**.

8.1.2 Configuring Main and Sub Stream Snapshot Optimization

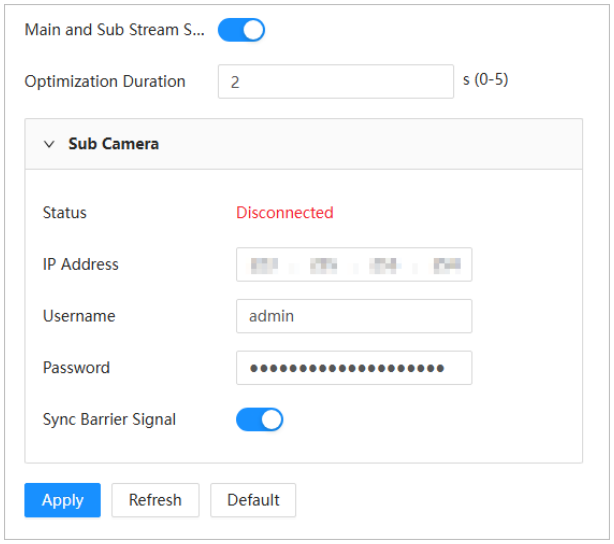
The main and sub optimization system scores the images captured based on license plate clarity, completeness, recognition confidence, and angle reasonableness, reporting the license plate image with higher accuracy.

Procedure

Step 1 On the home page, click **ANPR** > **Snapshot** > **Main and Sub Stream Snapshot Optimization**.

Step 2 Configure the parameters.

Figure 8-1 Configure main and sub stream snapshot optimization



1. Click to enable the main and sub stream snapshot optimization.
2. Set the optimization duration.

   In the set duration, the priority snapshot camera waits for capture data from the other camera. When the duration is exceeded, the data captured by the priority snapshot camera shall be deemed the preferred data for this main and sub snapshot.
3. Set the IP address, username, and password of the sub camera.
4. Click to enable sync barrier signal function.

Step 3 Click **Apply**.

8.2 Configuring AI Setting

8.2.1 Intelligent Analysis

You can set vehicle recognition parameters, recognition mode, and other functions.

Procedure

Step 1 On the home page, click **ANPR**, and then select **AI Settings** > **Intelligent Analysis**.

Step 2 Configure the parameters.

Table 8-2 Parameters description of intelligent analysis

Parameter	Description
Detection Type	Select the type of targets to be detected.
Vehicle Detection Sensitivity	Set the sensitivity of vehicle detection. The higher the value, the easier targets will be detected. It is 40 by default.
Motor Vehicle	Select parameters such as type, logo and color that can be recognized by the camera.
Two-wheeled and Three-wheeled Vehicles	Select the vehicle type that can be recognized by the camera.
Advanced Parameters	Configure advanced vehicle recognition function through algorithm. Click ⓘ to view the advanced algorithm formula.

Step 3 Click **Apply**.

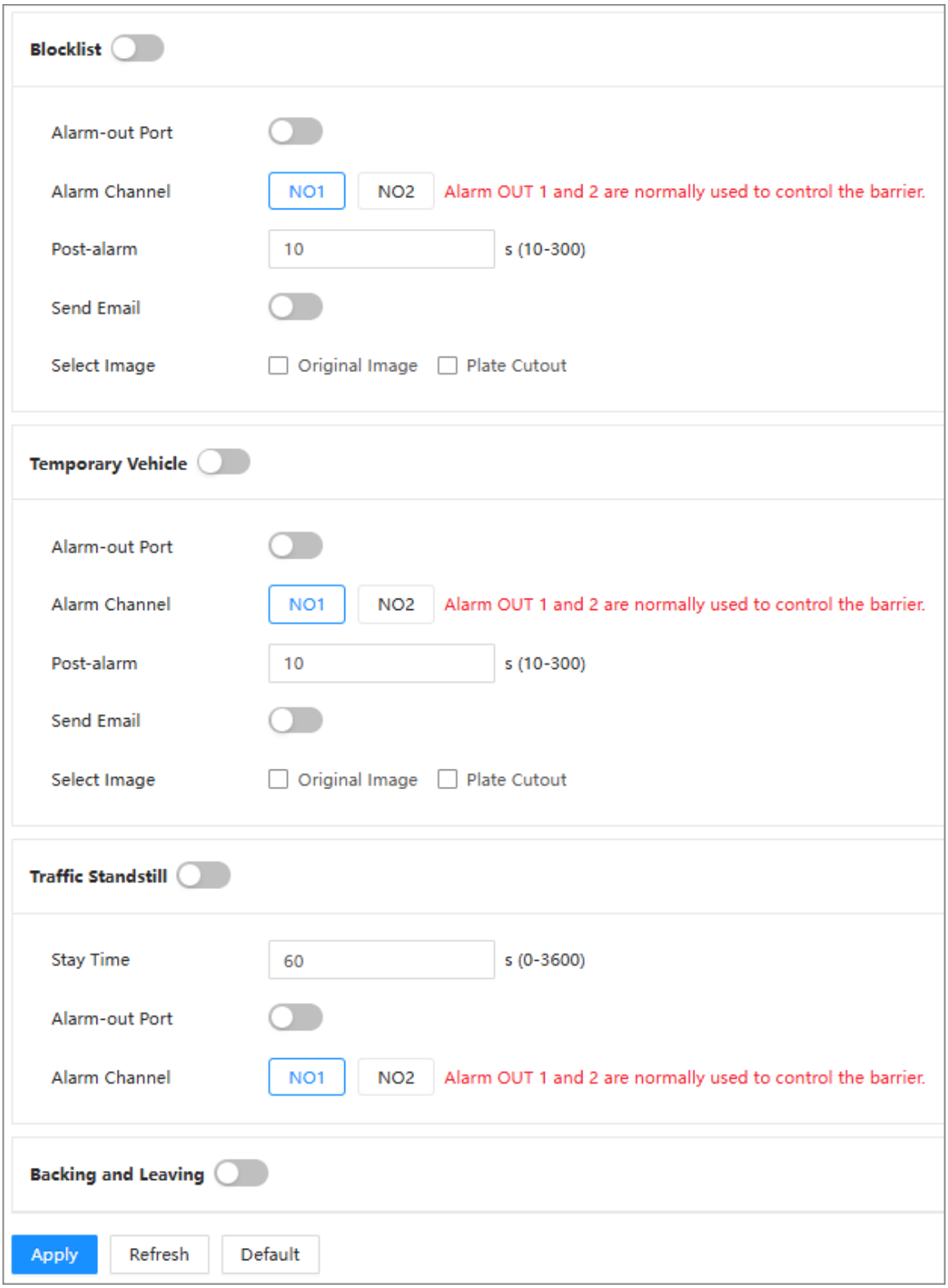
8.2.2 Smart Detection

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

Procedure

Step 1 On the home page, click **ANPR**, and then select **AI Settings** > **Smart Detection**.

Figure 8-2 Smart detection



Step 2 Configure the parameters.

Table 8-3 Parameters description of smart detection

Parameter	Description
Blocklist	Enable **Blocklist**, and then alarms will be triggered when vehicles in the blocklist are captured.
Alarm-out Port	Click to enable alarm-out ports, so that the camera sends alarm signals to the alarm channels that you select when an alarm is triggered.
Alarm Channel	Select one or more alarm channels to send alarm signals to.
Post-alarm	The camera will keep sending alarms signals for the defined period after the alarm ends.
Send Email	Click to enable the function so that the camera will send an email to the defined email address when an alarm is triggered. For how to configure the email address, see "17.2.7 Email".
Select Image	Select the type of image that the camera will capture when alarms are captured. • **Original Image** : The complete image taken by the camera. • **Plate Cutout** : A cutout image of the number plate.
Temporary Vehicle	Enable **Temporary Vehicle**, and then alarms will be triggered when temporary vehicles are captured.
Traffic Standstill	Click to enable the function, and then enter **Stay Time** on a scale from 0 to 3600 seconds. Vehicles that loiter in the area for an exceeded period of time will be captured.
Backing and Leaving	Click to enable the function, and then a vehicle that crosses the detection line is captured, and it will be captured again when it reverses.

Step 3 Click **Apply**.

8.3 Image Configuration

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

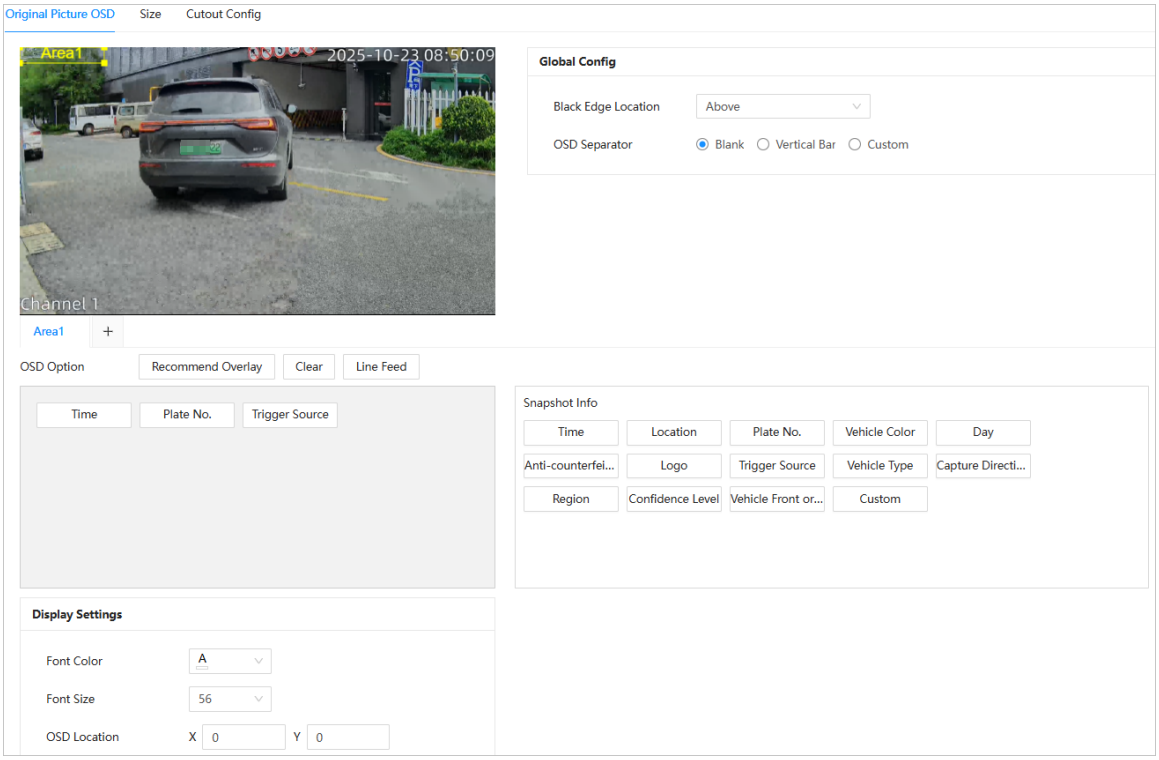
8.3.1 Original Picture OSD

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 8-3 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".

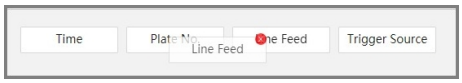
Step 4 Configure the OSD information to be displayed.

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 8-4 Adjust the order



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

Table 8-4 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**.

8.3.2 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**.

8.3.3 Cutout Configuration

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

Procedure

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

Step 2 Configure the parameters.

Table 8-5 Cutout parameter

Parameter	Description
Cutout Config	• **Plate No.** : The camera will cut out pictures of the plate number, and save them to the storage path. • **Vehicle Body Cutout** : The camera will cut out pictures of the vehicle bodies, and save them to the storage path. You can select both of the 2 options at the same time.
Plate Overlay	Click **Enable** corresponding to **Motor Vehicle** or **Two-wheeled and Three-wheeled Vehicles**, and then the camera will add a picture of the plate number of the vehicle to the snapshot. You can select the position and size of the plate number from the **Overlay Position** and **Overlay Size** drop-down lists.

Step 3 Click **Apply**.

8.4 Vehicle Blocklist and Allowlist

8.4.1 Fuzzy Match

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 **Vehicle Blocklist/Allowlist** > **Fuzzy Matching**.

Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 8-6 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**.

8.4.2 Allowlist

If the barrier control is set to **Open barrier by allowlist**, only vehicles on the allowlist can pass. You can add up to 110,000 records.

Procedure

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

Step 2 (Optional) Enable **Verify Vehicle Color** if you want to verify the vehicle by both vehicle license plate and vehicle color.

After it is enabled, the vehicle color verification will take effect only when the camera is in **Color** mode and the ambient brightness exceeds 47. When the camera is in **B/W** mode or the ambient brightness is lower than 47, the vehicle color verification does not take effect.

In the dual-factor verification mode (license plate and vehicle color verification), the camera will verify both of them only when license plate and vehicle body color are configured when adding the vehicle to the allowlist. If license plate is configured, but no vehicle color is configured, only the license plate will be verified.

Step 3 Add vehicles.

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

Figure 8-5 Add a vehicle to the allowlist

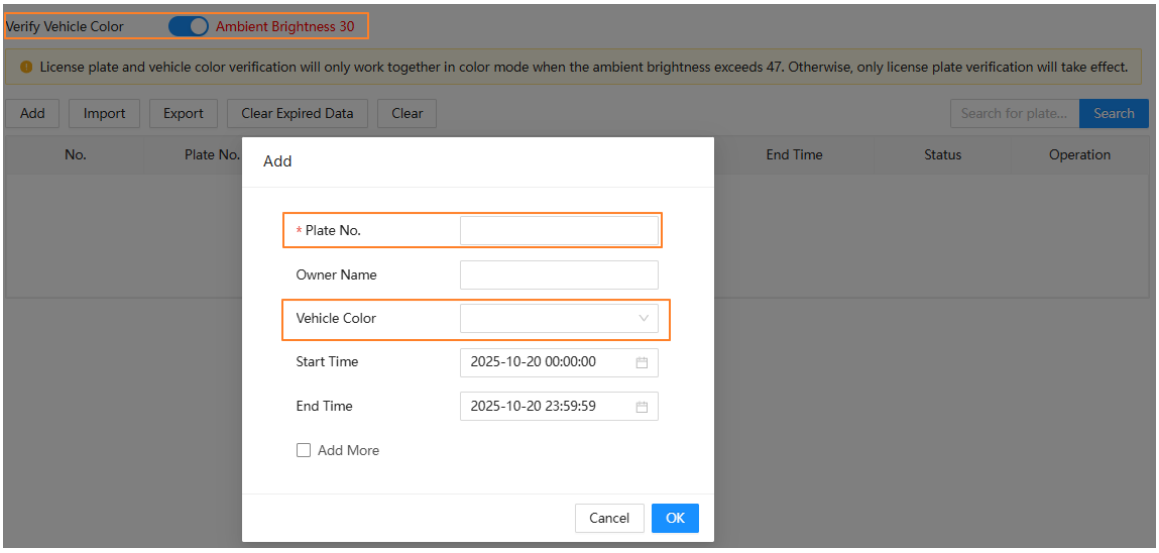


Table 8-7 Parameters description of allowlist

Parameter	Description
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.

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.

8.4.3 Blocklist

A vehicle in the blocklist cannot pass the barrier. You can add up to 110,000 records.

On the home page, click **ANPR**, and then select **Vehicle Blocklist/Allowlist** > **Blocklist**. The configurations are similar to those of allowlist. For details, see "8.4.2 Allowlist".

8.5 Configuring Barrier Control

8.5.1 Barrier Control

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

Procedure

Step 1 On the home page, click **ANPR**, and then select **Barrier Control** > **Barrier Control**.

Step 2 Configure the parameters.

Table 8-8 Parameters description of barrier control

Parameter	Description
Scheduled Barrier Always Open	Click to enable this function, and then click **Time Plan Table** to set the period for which the barrier remains open. For details on setting the time plan, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports".

Parameter	Description
Scheduled Barrier Always Closed	Click to enable this function, and then click **Time Plan Table** to set the period for which the barrier keeps normally closed when no barrier opening signals are triggered from the camera. For details on setting the time plan, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports".
Barrier Control Mode	Triggers alarm through different modes, and remotely controls the barrier opening and closing. • **All Vehicles** : When the camera captures any vehicle, it outputs an open barrier signal. • **Licensed Vehicles** : When the camera captures any plate, it outputs an open barrier signal. • **Allowlist** : When the camera captures vehicles that are on the allowlist or conform to fuzzy matching, it outputs an open barrier signal. • **Custom Plate** : Supports customizing the license plate prefix/suffix characters (up to 3 characters). Once a matching license plate is recognized, the barrier gate will open automatically. You can add up to 5 release rules. • **Command (Platform)** : The camera outputs an open barrier signal when it receives a command from the platform. If you only enable **Command (Platform)**, you can specify the control mode if the platform is offline. You can set barrier opening control to **Allowlist** and **Command (Platform)** at the same time.
Barrier Opening	• **Alarm Channel** : Alarm linkage output port. Select the corresponding channel for alarm signal output according to the field connection. • **Duration** : The duration that the barrier opening or closing signal lasts.
Barrier Closing	

Step 3 Click **Apply**.

8.5.2 Remote Control

Remote control for barrier opening is supported on ITC413 series products. You can configure it as needed.

Procedure

Step 1 On the home page, click **ANPR**, and then select **Barrier Control** > **Remote Control**.

Step 2 Configure the parameters.

Table 8-9 Parameter description of remote control

Parameter	Description
Warning Light	Click to enable the function. After it is enabled, the light flashes when the camera receives remote control signals.
Duration	You can configure the flashing duration of the warning light. The default setting is 10 seconds. The range is 10 seconds–3,600 seconds.
Connect	• Click **Connect**, press and hold the learning button on the remote control for 10 seconds, and then the remote control will connect to the camera. • Click **Disconnect** to disconnect the remote control and the camera.
Disconnect	

Step 3 Click **Apply**.

8.6 Configuring RS-485 Settings

You can configure RS-485 serial protocol of external devices. After configuration, you can set related parameters of the device on the webpage of the camera.

Background Information

- Serial port 1: Connects to external devices such as illuminator and LED screen.
- Serial port 2: Connects to barrier and anti-smashing radar.

Procedure

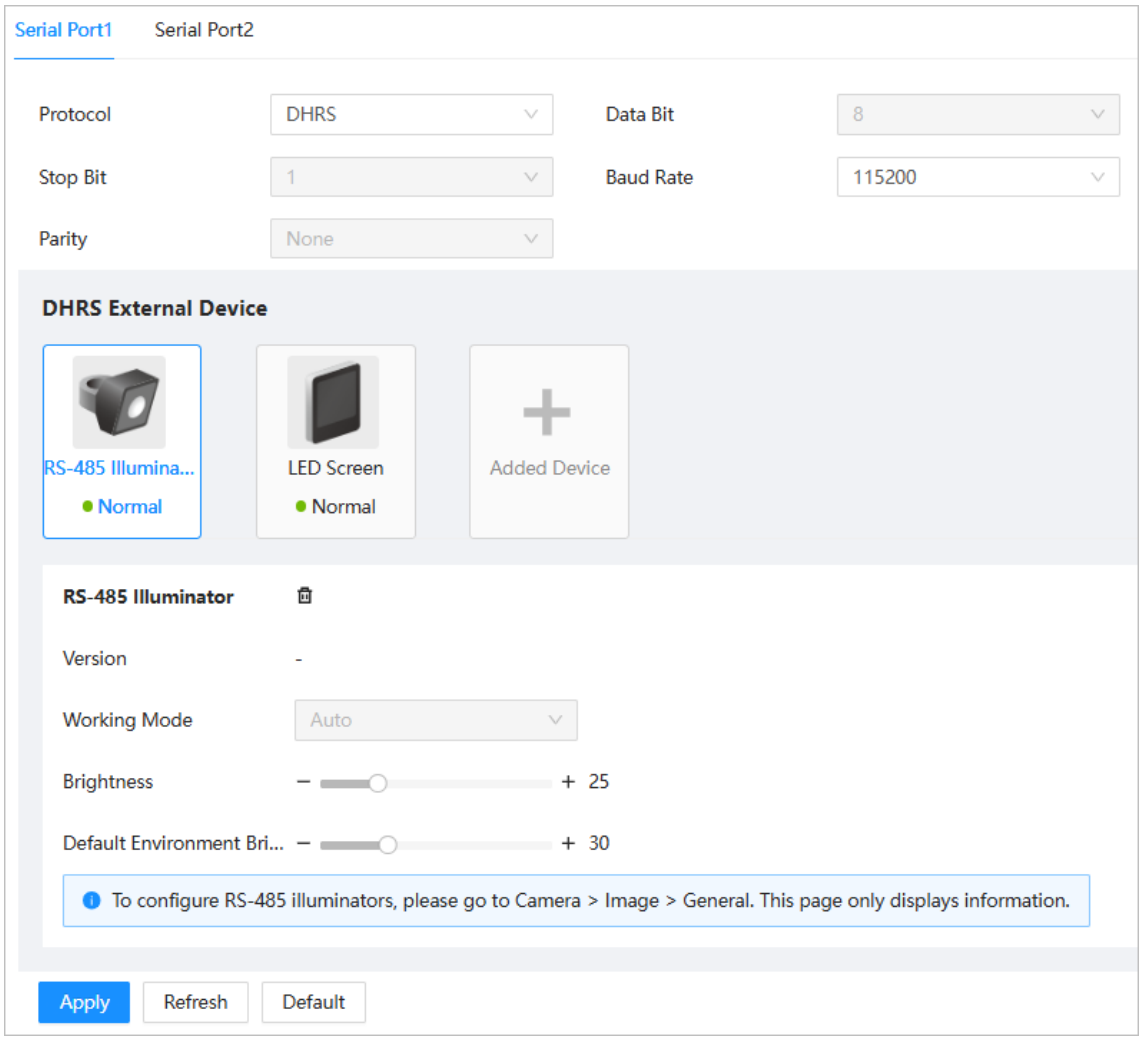
Step 1 On the home page, click **ANPR** , and then select **RS-485 Settings**.

Step 2 Configure the parameters.

- DHRS

  Click the **Serial Port 1** tab, and then you can view the information of RS-485 illuminator. To configure the RS-485 illuminator, go to **Camera** > **Image** > **General**. For details, "13.1.1 General Parameters".

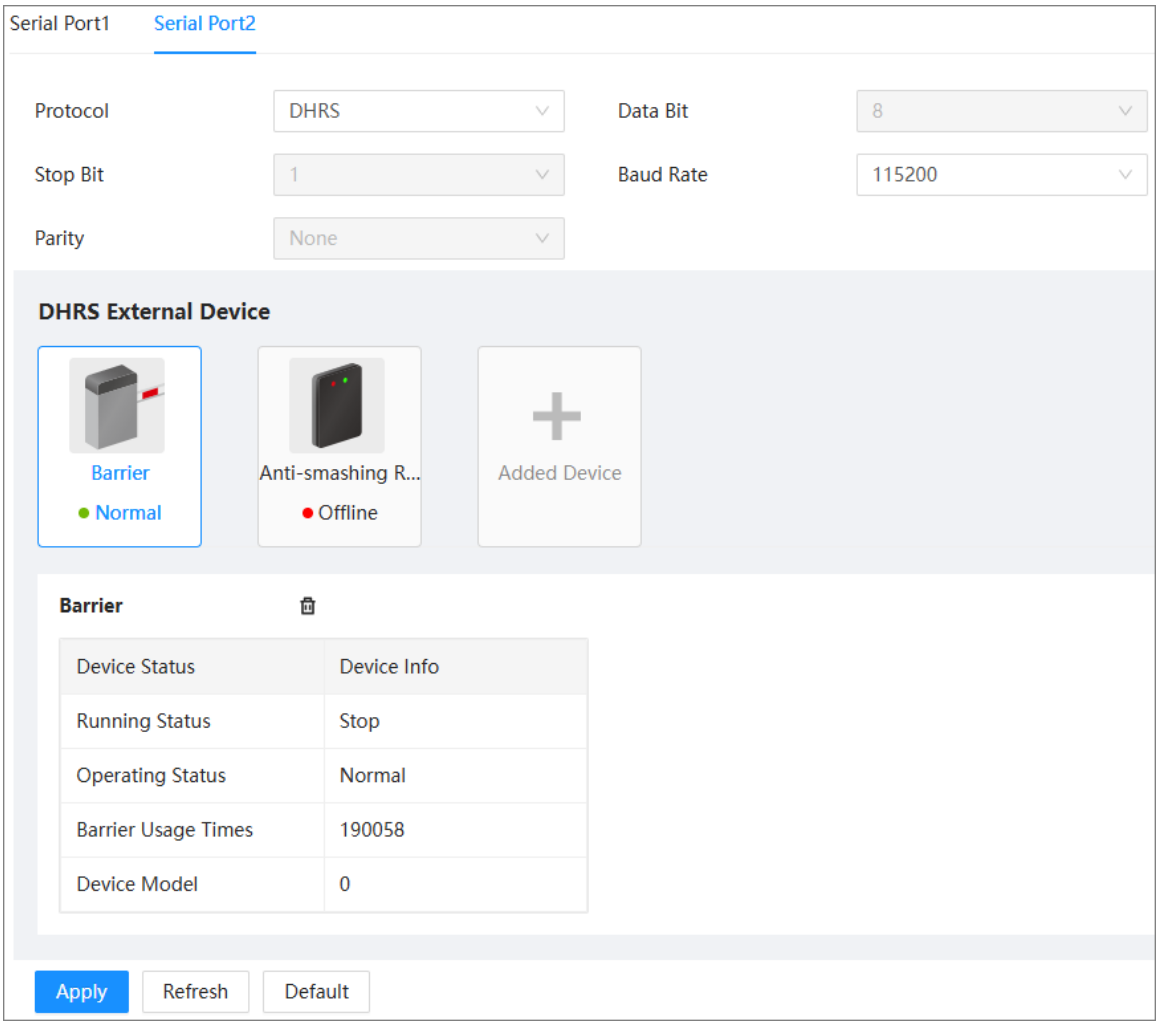
Figure 8-6 DHRS parameters (serial port 1)



Click the **Serial Port 2** tab, and then you can view the information of the barrier and the anti-smashing radar, including running status, operating status, barrier usage times (for the radar) or relay usage times (for the anti-smashing radar), and device model.

- Running status: The working status of the device. For example, for the barrier, the status includes stop, open, close, and unknown.
- Operating status: The online and offline status of the device.
- Barrier usage times, relay usage times: The times that the barrier or the anti-smashing barrier has worked.

Figure 8-7 DHRS parameters (serial port 2)

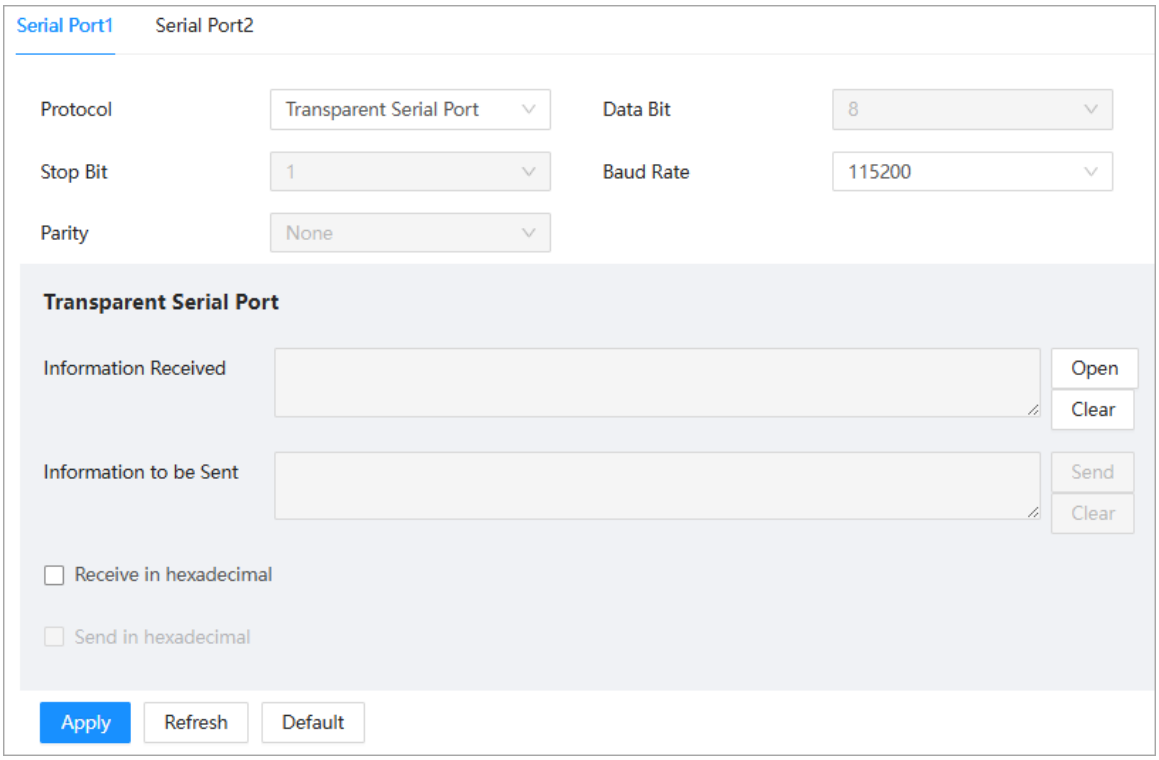


- Transparent Serial Port

  The third-party platform can control the RS-485 output of the camera through RS-485 transparent transmission, and then you can connect external devices.

  Trigger capture through transmitting capture command. To test the RS-485 transparent transmission sending and receiving conditions, select **Send in hexadecimal** , and then click **Open** on the right side of the **Information Received** section.

Figure 8-8 RS-485 Transparent transmission



- Push Data through Serial Port

  You can configure the serial port push information. The camera pushes the snapshots to the third serial collection device through RS-485.

  When there are 2 ports, serial port push protocol is only available for serial port 2.

Figure 8-9 Push data through serial port

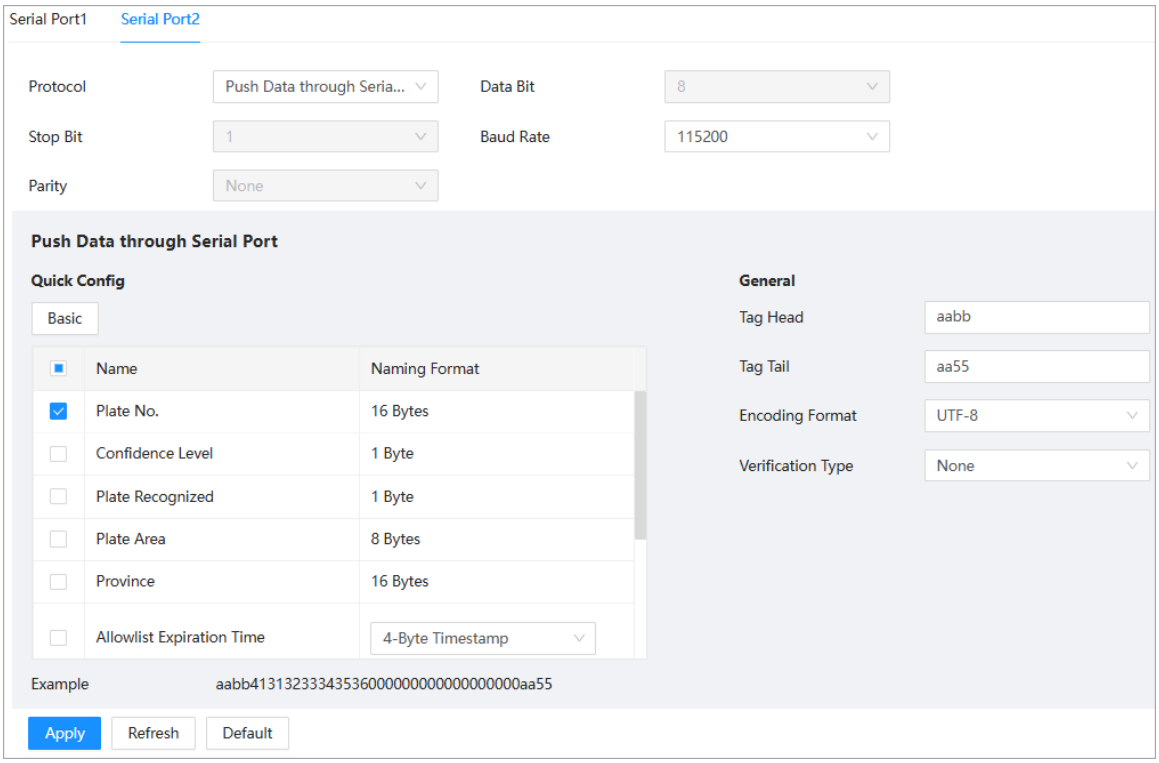


Table 8-10 Parameters description of RS-485

Parameter		Description
Quick Config	Message Type	Select one or more items to be sent to the third serial collection device. Hover your mouse over the items to see their explanations.
	Example	The format of the data based on the items you select.
	Basic	The camera will automatically select certain items by default.
General	Tag Tail	The tag tail of data package. It is **aabb** by default.
	Tag Head	The tag head of data package. It is **aa55** by default.
	Encoding Format	Select encode type from **UTF-8** (default) and **GB2312**.
	Verification Type	Select check mode from **None** , **Sum Check** and **BCC Check**.

Step 3 Click **Apply**.

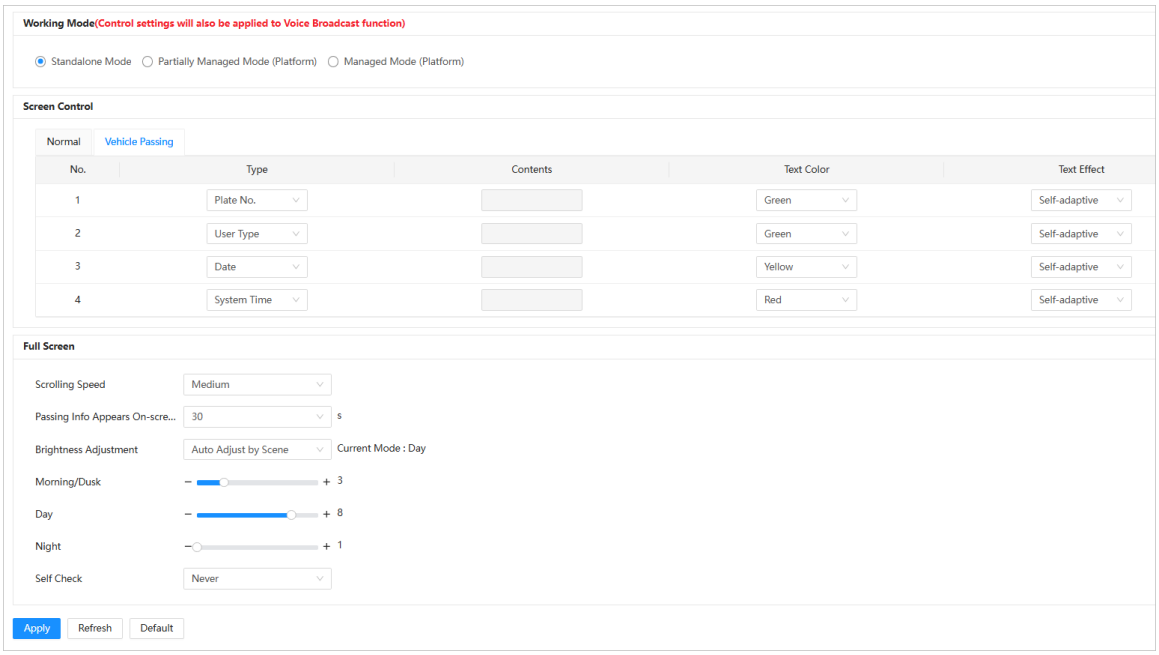
8.7 Configuring LED Screen

Connect the LED display with the camera through RS-485, and then you can configure the status, display type, display color, action, speed, and more parameters of the LED.

Procedure

Step 1 On the home page, click **ANPR** , and then select **LED Screen**.

Figure 8-10 LED screen



Step 2 Configure the parameters.

Table 8-11 Parameters description of LED screen

Parameter	Description
Working Mode	Set the working mode for the screen. • **Standalone Mode** : Display as configured, and not controlled by any platforms. • **Partially Managed Mode (Platform)** : Select this to allow the platform to control part of the screen information. • **Managed Mode (Platform)** : Grant the platform complete control over the display information on the screen. In this mode, the settings from **ANPR** > **Audio Broadcast** do not take effect.

Parameter		Description
Screen Control		Set the type, contents, text color, and text effect of display information when vehicles pass and normal state. The screen will display information as configured during the period for either status.
Full Screen	Scrolling Speed	The rolling speed of the information on the screen.
	Passing Info Appears On-screen for	The display duration of the passing vehicle information on the screen.
	Brightness Adjustment	The display brightness of the screen. • **Auto Adjust by Scene** : The display brightness will be automatically adjusted based on the current lighting conditions. • **Manual** : The display brightness will be manually adjusted.
	Morning/Dusk	You can drag the slider for increased brightness. The higher the value, the brighter the screen.
	Day	
	Night	
	Self Check	Test the screen for defects. **Never** and **Auto** are available. When **Auto** is selected, you can configure the time for self-test.

Step 3 Click **Apply**.

8.8 Configuring Broadcast

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

8.8.1 Event Broadcast

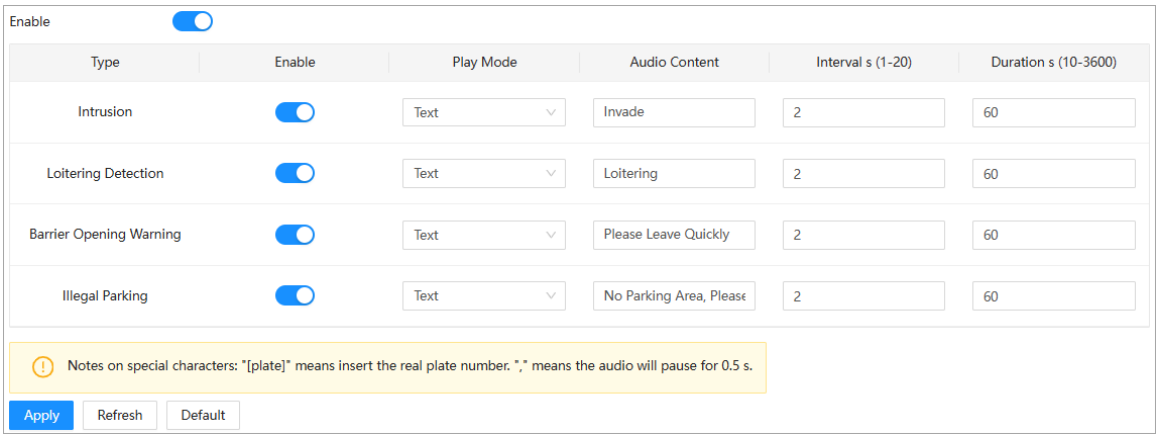
Configure the event broadcast settings. The camera will broadcast the customized content when specific events occur.

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 8-11 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 "8.8.4 Audio File".

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

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

Step 6 Click **Apply**.

8.8.2 Passing Vehicles

Configure the broadcast content, and the camera will broadcast the content when vehicles pass.

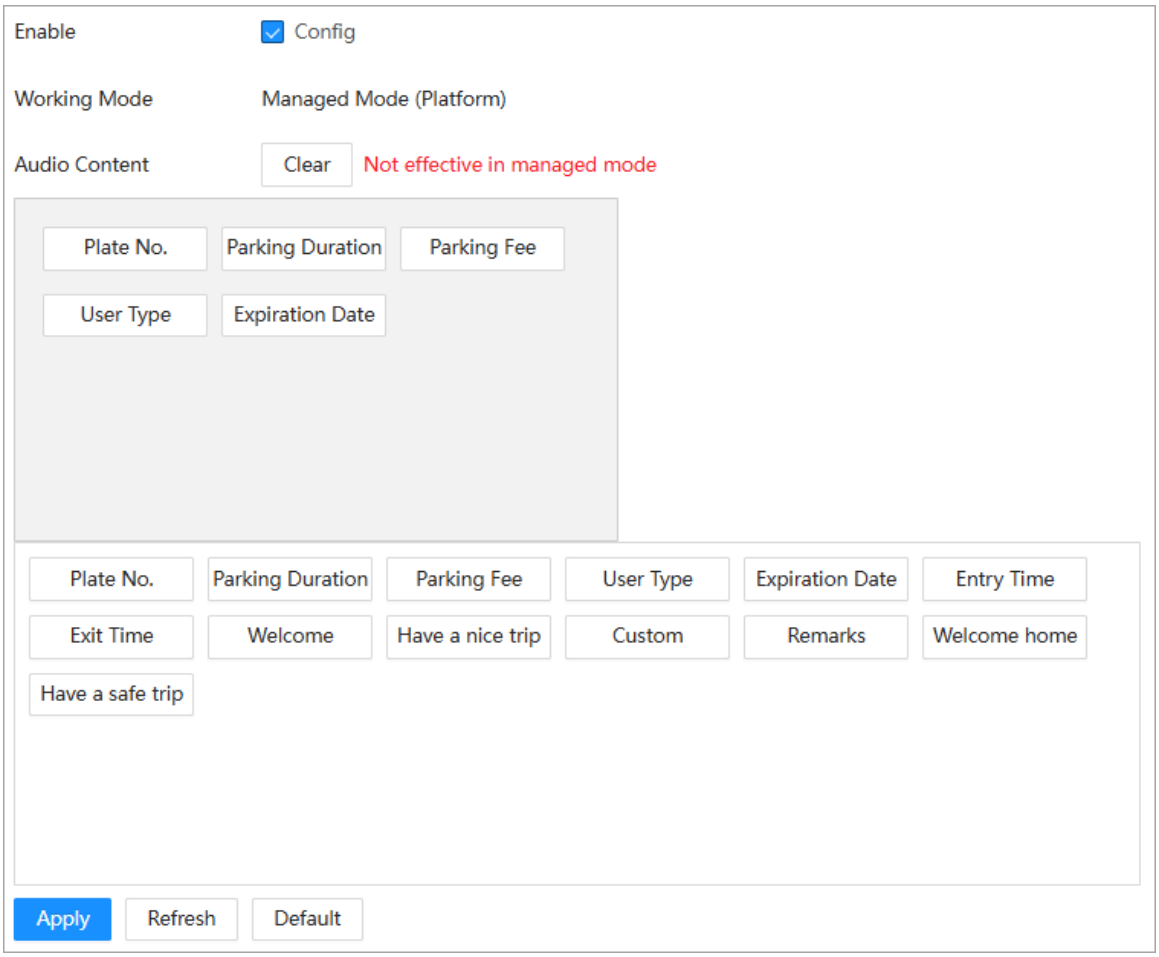
Only certain devices support this function.

Procedure

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

Step 2 Enable one or more options.

Figure 8-12 Passing vehicles broadcast



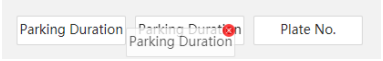
Step 3 Configure the broadcast content.

1. Click an item on the right to add it to the content.

   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.

2. Drag to adjust the order of information.

   Figure 8-13 Adjust the order

3. Click a type of information, and then configure the prefix and suffix content.

Step 4 Click **Apply**.

8.8.3 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 Click to enable the voice function.

Step 3 Configure the parameters.

Table 8-12 Description of volume/encoding parameters

Parameter	Description
Input Volume	The volume of the sound received by the camera.
Audio Output Type	Two types are available, including camera audio output and camera speaker.
Output Volume	The volume of the voice broadcast.
Voice Speed	The speed for the voice broadcast.

Step 4 Click **Apply**.

8.8.4 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.

8.9 Setting Device Test

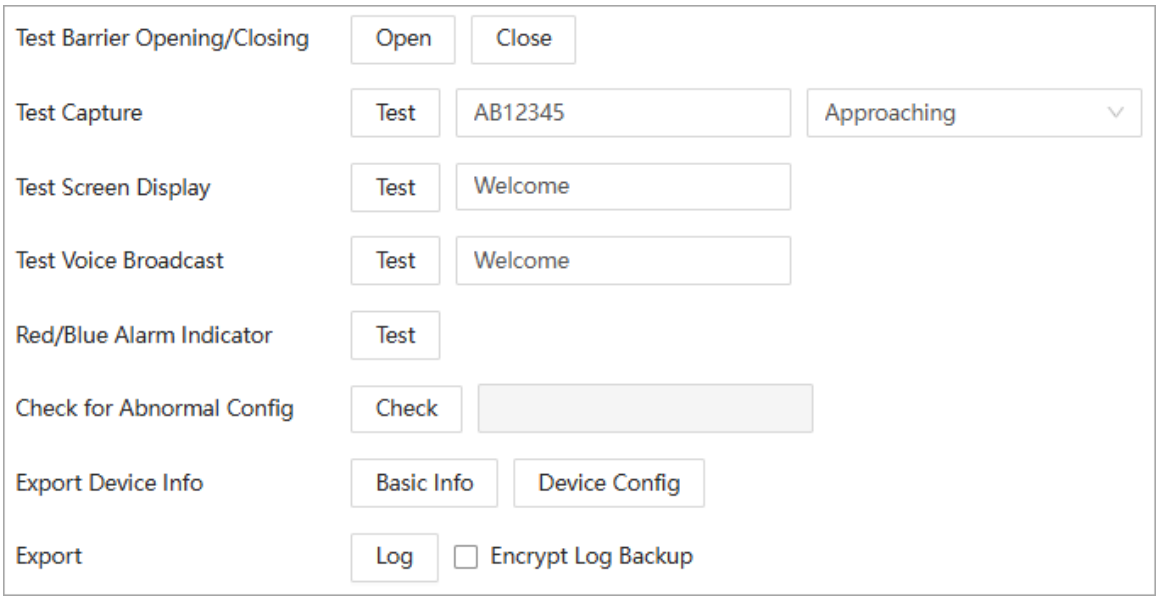
8.9.1 Device Test

You can test the barrier opening and closing, capture, display content, 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** > **Device Test**.

Figure 8-14 Device test



Step 2 Test if different functions are working normally.

Table 8-13 Parameters description of device test

Parameter	Description
Test Barrier Opening/ Closing	Click **Open** or **Close** to test whether the barrier responds correctly.
Test Capture	Enter a plate number, click **Test** to trigger capture, and view the snapshot in the **Live** page.
Test Screen Display	Enter some information, click **Test**, and view whether the information is correctly displayed on the LED screen.
Test Voice Broadcast	Enter some information, click **Test** to check whether the device plays the sound normally. Voice broadcast is only available on select models.

Parameter	Description
Red/Blue Alarm Indicator	Click **Test** to check whether the red/blue alarm indicator performs normally.
Check for Abnormal Config	Click **Check**, and system checks abnormality automatically.
Export Device Info	Select the information of the device, and export it in batches.
Export	Export logs to your computer. Select **Encrypt Log Backup** and configure the password to secure the logs. You need the password to access the logs.

8.9.2 Capture Adjustment Information

You can overlay shield area box, vehicle body box, license plate box, vehicle body trajectory, plate trajectory, and capture area on the snapshots to assist you in checking whether the snapshots are taken as you require.

Procedure

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

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

Step 3 Click **Apply**.

Step 4 Go to the **Live** page, and then click  to manually capture a license plate. On the snapshot, you can see the rules and tracking information that you have selected. If they do not meet your requirements, you can adjust them by repeating the steps above.

8.9.3 Collection Log

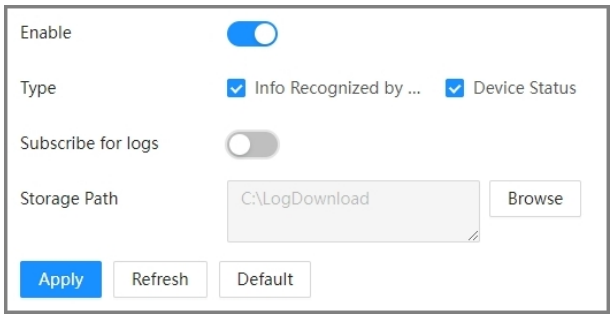
The camera supports collecting operation logs to track errors.

Procedure

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

Step 2 Turn on the toggle next to **Enable** to enable the function.

Figure 8-15 Collection log



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

Step 4 Click **Browse** to select a path to save the logs, and then turn on the toggle next to **Enable** to enable **Subscribe for logs**.

Step 5 Click **Apply**.

8.10 Available Space Count

In a one-way traffic environment with a dedicated entry and exit point, you can configure entrance and exit cameras to manage the remaining parking spaces.

Procedure

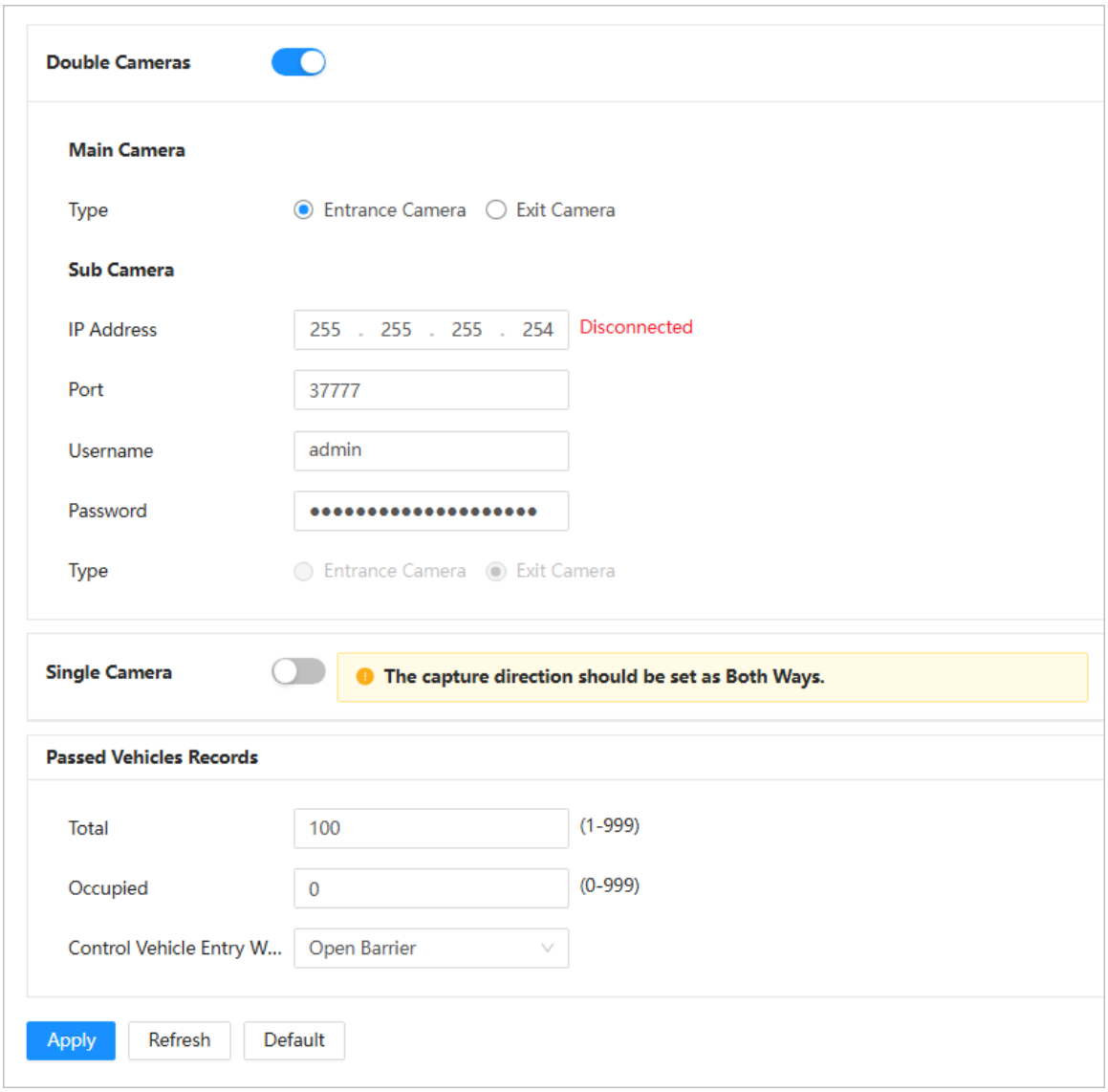
Step 1 On the home page, click **ANPR** , and then select **Available Space Count**.

Step 2 Enable either **Double Cameras** or **Single Camera** as needed.

- **Double Cameras** : Parking space counting with 2 cameras. This mode is applicable to the scene where 2 cameras manage the entry and exit of vehicles respectively, and the cameras are linked with barriers for the entrance and the exit. The main camera manages the available parking spaces in the parking lot according to the number of barrier opening times sent by the cameras.
- **Single Camera** : Parking space counting with 1 camera. This mode is applicable to the scene where a single camera manages the entry and exit of vehicles at the same time, and the camera is not linked to the barrier. The camera manages the available parking spaces in the parking lot according to the driving direction of the captured vehicles.

Step 3 Configure the parameters.

Figure 8-16 Available space count



Main camera and sub camera are only available for the **Double Cameras** mode.

Table 8-14 Parameter description

Parameter		Description
Main Camera	Type	Select the main camera as either an entrance camera or an exit camera based on its installation location.
Sub Camera	IP Address	The IP address for logging in to the sub camera.
	Port	The port for logging in to the sub camera.
	Username	The user name for logging in to the sub camera.
	Password	The password for logging in to the sub camera.

Parameter		Description
	Type	The type of the sub camera. If the main camera is an entrance camera, then the sub camera is automatically set as an exit camera. Vice versa.
Passed Vehicles Records	Total	The total parking spaces.
	Used	The occupied parking spaces.
	Control Vehicle Entry When Lot is Full	Supports customizing the vehicle entry manner including **Open Barrier** and **Do Not Open Barrier** when the lot is full.

Step 4 Click **Apply**.

8.11 Configuring Wiegand

Supports Wiegand bit format selection, including Wiegand 26/34/48/64/72. After Wiegand digit is selected, the data captured by access ANPR cameras can be converted into Wiegand protocol communication format.

Procedure

Step 1 On the home page, click **ANPR** > **Wiegand**, and then select transmission mode.

Step 2 Click **Apply**.

9 IVS

You can configure the IVS rules for intrusion and loitering detection, parking space detection, and illegal parking detection.



The IVS module is only available on ITC413 series cameras. The functions of parking space management and illegal parking area are quite different from ANPR functions. We do not recommend enabling these functions at the same time.

9.1 Configuring IVS

Configure rules and alarm linkage actions for detecting intrusion and loitering. Alarms will be triggered, and the linked action will be performed when intrusion or loitering events are detected.

Procedure

Step 1 On the home page, click **IVS**, and then select **Rule Config** > **IVS**.

Step 2 Click **Add**, and then you can add up to 4 rules of either **Intrusion** or **Loitering Detection**.

Step 3 Configure the parameters.

Figure 9-1 IVS

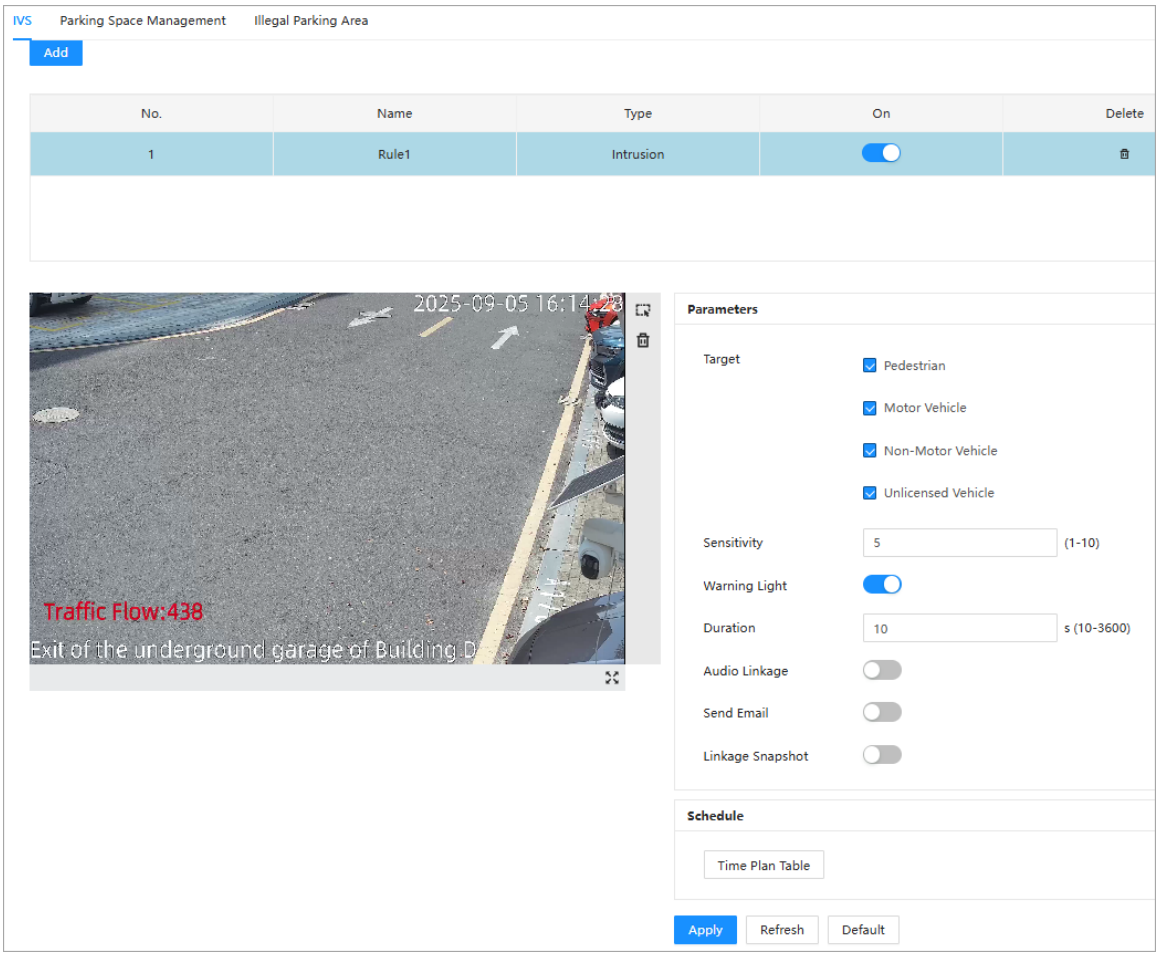


Table 9-1 IVS parameter description

Parameter	Description
Target	4 detection target types are available, which include pedestrian, motor vehicle, non-motor vehicle, and unlicensed vehicle. When selected, the camera will detect their behaviors.
Sensitivity	It determines how many changes in pixels or amount of an object will trigger an event. The higher the value, the easier targets will be detected. This parameter is only available for **Intrusion**.
Warning Light	After it is enabled, the light flashes when the camera detects specific events.
Duration	Enter the duration of flashing warning light, with a scale from 10 to 3,600 seconds.
Audio Linkage	After it is enabled, the camera broadcasts when it detects specific events.

Parameter	Description
Send Email	After it is enabled, the camera sends emails when it detects specific events.
Linkage Snapshot	After it is enabled, the camera takes snapshots when it detects specific events.
Interval	Only 1 alarm will be triggered within the configured interval. For example, if you configure the interval to be 300 seconds and 2 alarms are triggered in 290 seconds, only 1 alarm will be reported.
Loitering Duration	Enter the maximum time the target can loiter in the area, with a scale from 1 to 50 seconds. Once the target stays for an exceeded time, an alarm is triggered. This parameter is only available for **Loitering Detection**.
Time Plan Table	Click **Time Plan Table** to set the period that the rules take effect. 1. Click and drag the timeline to adjust the time period. 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.

Step 4 Configure the detection area.

Click , and then click and drag on the video image to draw the detection area (right-click to finish drawing). Only 1 area can be added to each detection rule.

Click to delete the detection area.

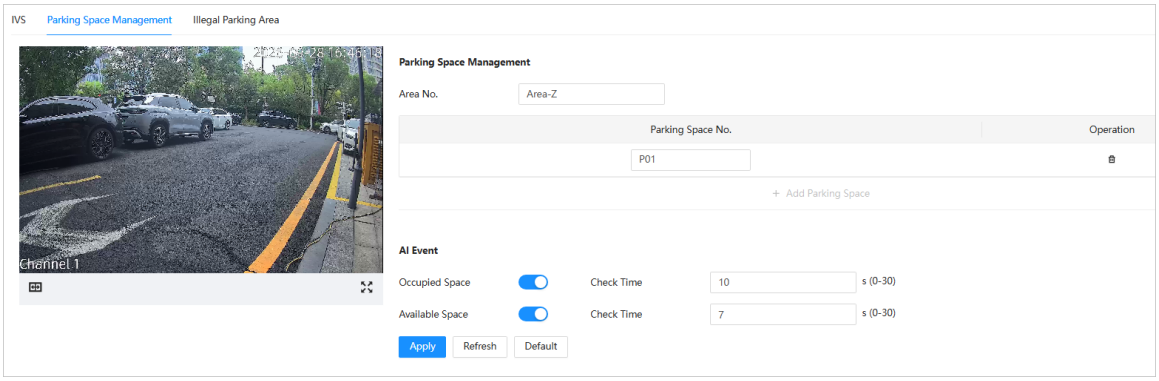
9.2 Parking Space Management

Configure rules for detecting occupied and available parking spaces.

Procedure

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

Figure 9-2 Parking space management



Step 2 Click **Add Parking Space**, and then draw the parking space detection area on the video image (right-click to finish drawing).

The parking space number is filled in automatically. You can also modify it as needed.

Step 3 Enable **Occupied Space** and **Available Space** as needed.

After enabling the function and setting the check time, 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 **Apply**.

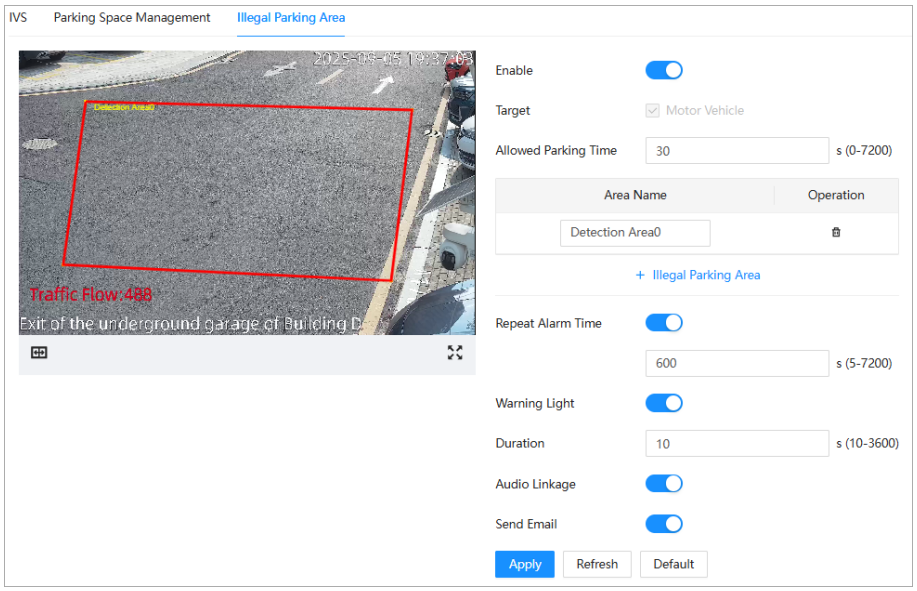
9.3 Illegal Parking Area

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

Procedure

Step 1 On the home page, click **IVS**, and then select **Rule Config** > **Illegal Parking Area**.

Figure 9-3 Illegal parking area



Step 2 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.

Step 4 Configure the parameters.

Table 9-2 Illegal parking area parameter description

Parameter	Description
Target	Motor vehicle by default, and cannot be edited.
Allowed Parking Time	Vehicles will not be detected as illegal parking within the allowed parking time.
Repeat Alarm Time	Enable the function, and then set the time. No repeat alarm will be triggered within the defined time.
Warning Light	After it is enabled, the light flashes when the camera detects illegal parking event.
Duration	Enter the duration of flashing warning light, with a scale from 10 to 3,600 seconds.
Audio Linkage	After it is enabled, the camera broadcasts when it detects specific events.
Send Email	After it is enabled, the camera sends emails when it detects specific events.

Step 5 Click **Apply**.

10 Picture

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

10.1 Image Search

Prerequisites

Insert the SD card and complete the initialization.

Procedure

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

Step 2 Configure the parameters.

Figure 10-1 Picture search

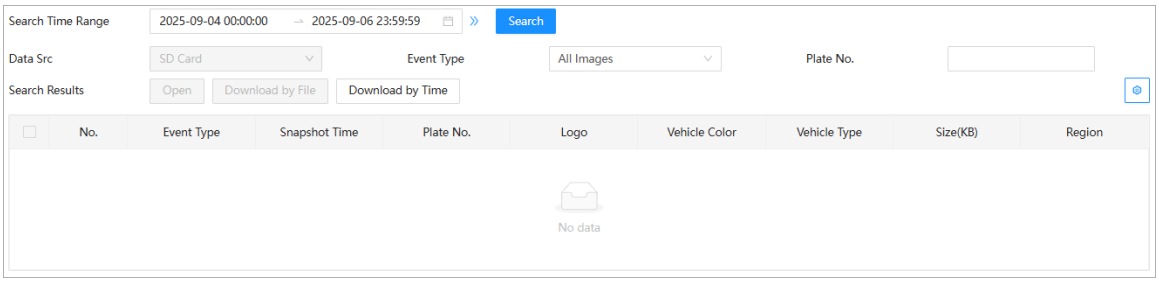


Table 10-1 Parameter descriptions of picture search

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.

10.2 Storage

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

10.2.1 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**.

10.2.2 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 10-2 Configure network storage

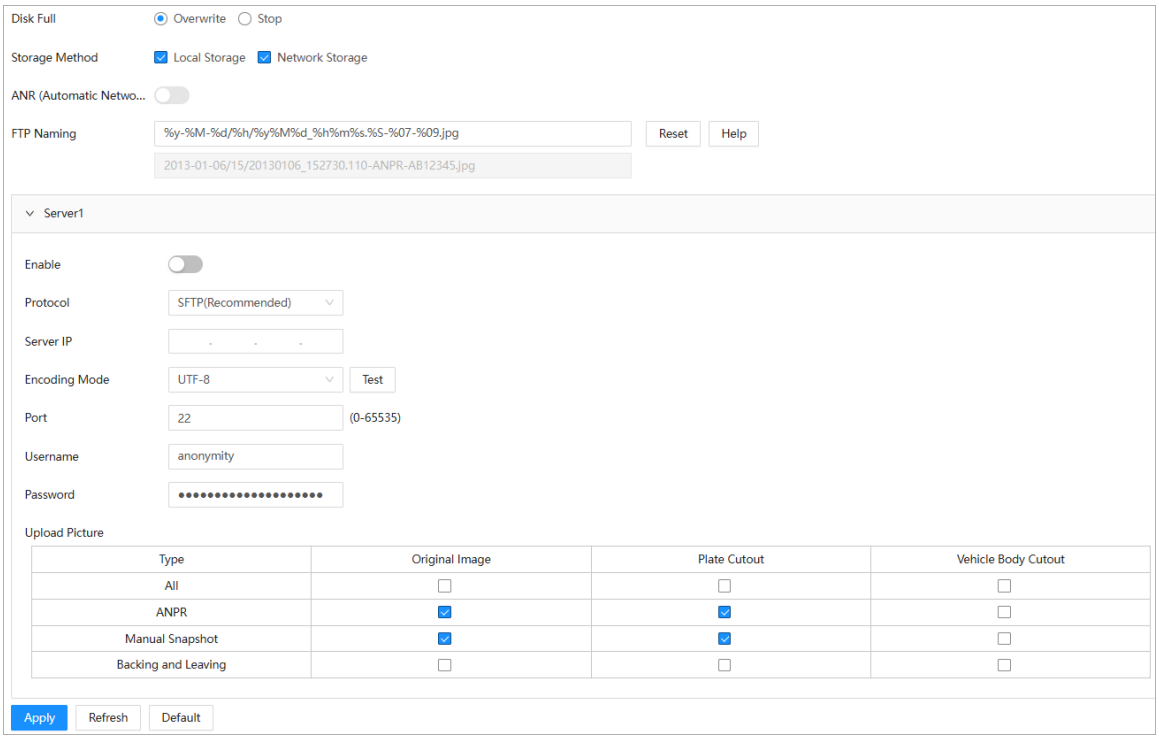


Table 10-2 Parameters description of FTP

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.

Parameter		Description
	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**.

10.3 Platform Server

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

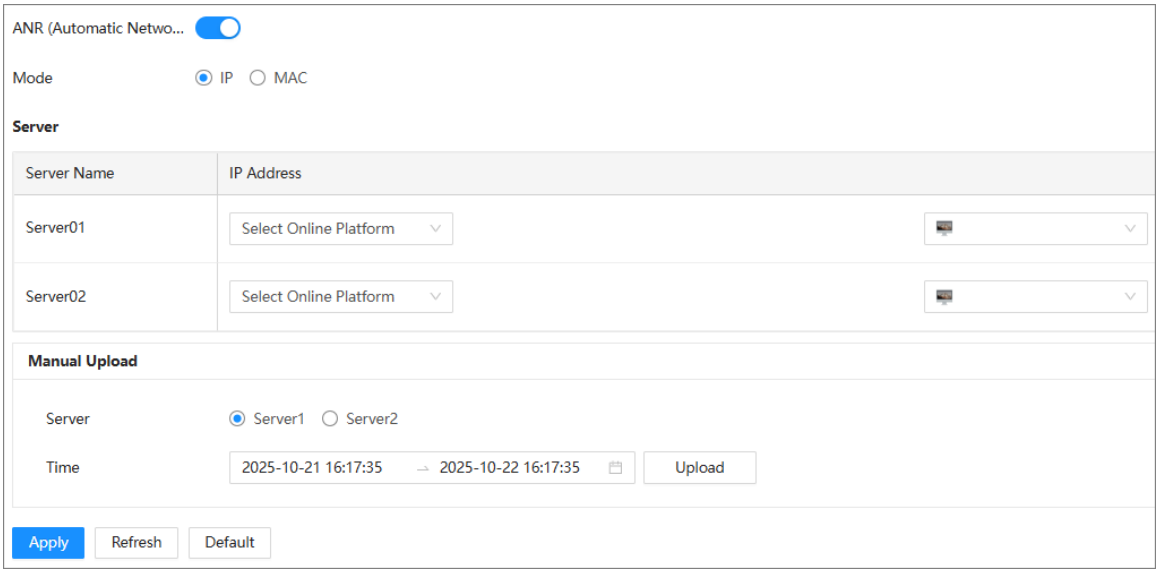
Procedure

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 10-3 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**.

11 Record

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

11.1 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 11-1 Configure video

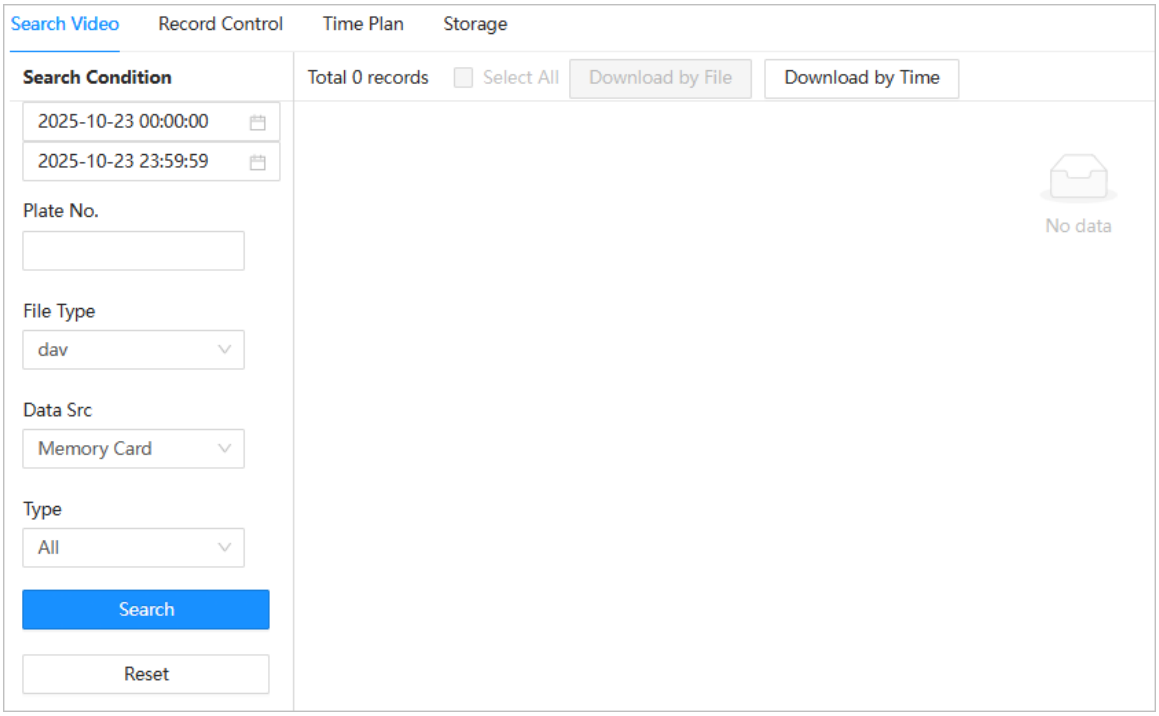


Table 11-1 Parameters description of video

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.

Parameter	Description
Data Src	It is memory card by default, and cannot be modified.
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.

11.2 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 11-2 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**.

11.3 Time Plan

Set the time plan of event recording and alarm recording.

Background Information

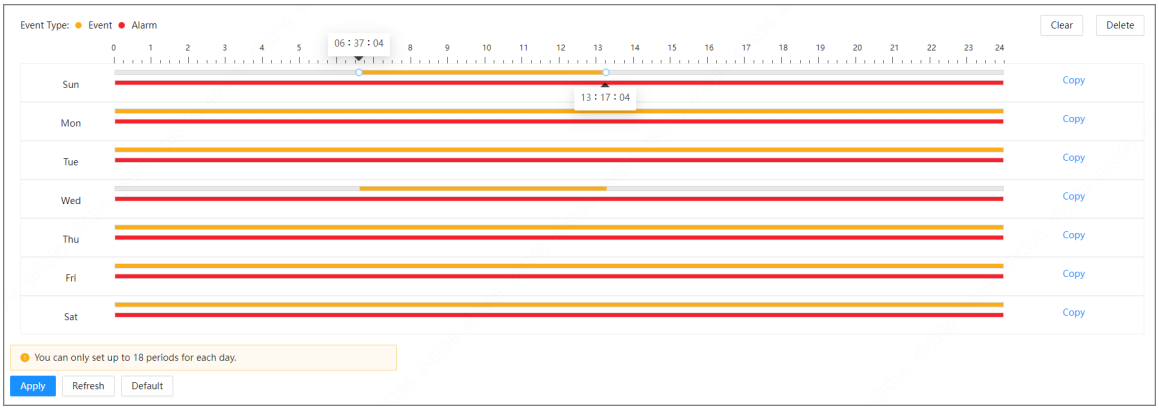
The system starts recording when an event or alarm is triggered within the scheduled time; and do not record beyond the schedule no matter what happens.

Procedure

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

Step 2 Set the time plan for recording.

Figure 11-2 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.

11.4 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 11-3 Storage

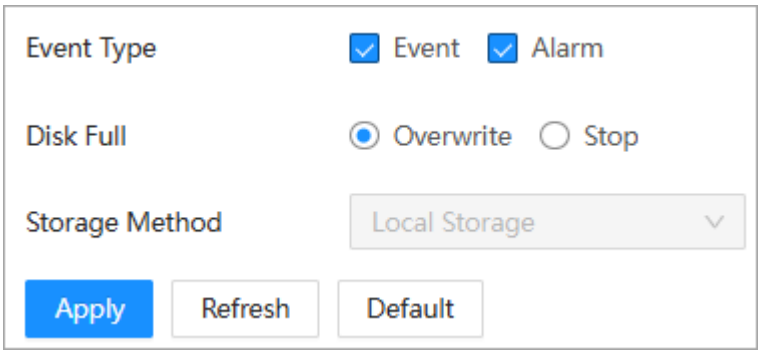


Table 11-3 Parameters description of storage

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

12 Search

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

12.1 Snapshot Records

12.1.1 Configuring Snapshot Records

Search for the snapshot records within the defined period. The camera can store up to 100,000 records when no memory card is installed.

Procedure

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

Step 2 Configure the search conditions.

- **Search Time Range** : The camera will only search for records taken within this range.
- **Event Type** : You can select different types of events from the checkbox. The default event type is **All**.
- **Capture Direction** : The direction of captured vehicles, including approaching and departing. Both directions are captured by default.
- (Optional) **Plate No.** : If you enter a plate number, the camera will only search for records related to this plate number.
- **Mode** : Displays the search results by table or chart.

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.

12.1.2 Sending Email

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

Procedure

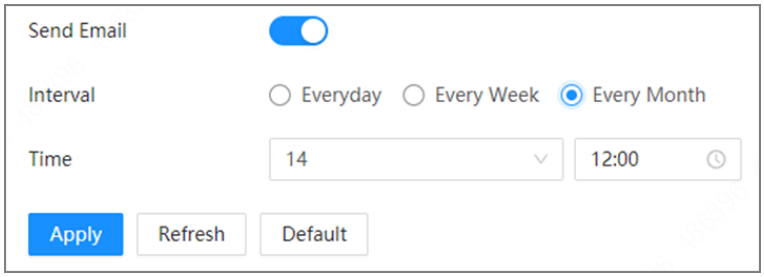
Step 1 On the home page, click **Search**, and then select **Snapshot Records** > **Send Email**.

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 12-1 Email configuration



12.2 Alarm-Out Port

Set the search conditions to search for alarm output.

Procedure

Step 1 On the home page, click **Search** , and then select **Alarm-out Port**.

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

The camera displays the results.

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.

12.3 Barrier Logs

Set the search conditions to search for barrier logs.

Procedure

Step 1 On the home page, click **Search** , and then select **Barrier Logs**.

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

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.

12.4 Radar Logs

Set the search conditions to search for radar logs.

Procedure

Step 1 On the home page, click **Search** , and then select **Radar Logs**.

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

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.

12.5 Parking Records

Set the search conditions to search for parking records.

Procedure

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

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.

12.6 Passed Vehicles Records

Set the search conditions to search passed vehicles records.

Procedure

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

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

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

12.7 Searching Images

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**.

12.8 Searching Video

12.8.1 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.

12.8.2 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**.

13 Camera

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

The parameters might vary with different models.

13.1 Setting Image Parameters

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

13.1.1 General Parameters

This section provides guidance on 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.

Table 13-1 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.

Parameter		Description
Contrast		Change the value when the image brightness is proper but contrast is not enough. • If the value is too big, 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 small. 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 big. • The image is not flamboyant enough if the value is too small. 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. For how to configure the periods, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports". 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**.

Parameter		Description
		• **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. For information on configuring the periods, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports". 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.
RS-485 Illuminator	Working Mode	• **Auto** : The RS-485 illuminator will be automatically turned on or off according to the current ambient brightness. • **Always Off** : Set the RS-485 Illuminator to always off. • **Always On** : Set the RS-485 Illuminator to always on. • **By Time** : The RS-485 illuminator will only be turned on during the periods you defined. For information on configuring the periods, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports".
	Brightness	Set the illumination intensity of the RS-485 illuminator when there are no vehicles passing. The higher the value is, the brighter it will be.
	Default Environment Brightness	Set a value for the automatic switch of RS-485 illuminator. When the current ambient brightness is lower than the value, the RS-485 Illuminator is on; otherwise, the RS-485 illuminator is off.

Step 3 Click **Apply**.

13.1.2 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.

Table 13-2 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 **Close**.
	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 **Customized**, 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**.

13.1.3 Metering Parameters

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

Procedure

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

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

Step 2 Configure the parameters.

Table 13-3 Parameters description of metering

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

Step 3 Drag to select the measured area, and the system displays a yellow box. Drag the box to a proper location.

Only need to draw measuring areas when setting **Metering Mode** to **Partial Metering**.

Step 4 Click **Apply**.

13.2 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.

13.2.1 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.

Table 13-4 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.

Parameter	Description
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.
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**.

13.2.2 Video OSD

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

13.2.2.1 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**.

13.2.2.2 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**.

13.2.2.3 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**.

13.2.2.4 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.

13.2.2.5 Abnormal Event Alarm

You can enable this function if you need to display **Abnormal Event Alarm** on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Abnormal Event Alarm**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Abnormal Event Alarm**.

Step 2 Click to enable this function.

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

Step 4 Select the font color.

Step 5 Click **Apply**.

13.2.2.6 Parking Space

You can enable this function if you need to display parking space management on the video.

Procedure

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

You can also select > **Camera** > **Encode** > **Video OSD** > **Parking Space**.

Step 2 Click to enable this function.

You can enable only one of the 3 OSD features: **Parking Space** , **Traffic Flow Info** or **Available Space Count**.

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

Step 4 Select the font color.

Step 5 Click **Apply**.

13.2.2.7 Traffic Flow Information

You can enable this function if you need to display daily traffic flow on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Traffic Flow Info**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Traffic Flow Info**.

Step 2 Click to enable this function.

You can enable only one of the 3 OSD features: **Parking Space** , **Traffic Flow Info** or **Available Space Count**.

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

Step 4 Select the font color.

Step 5 Click **Apply**.

13.2.2.8 Available Space Count

You can enable this function if you need to display available space count on the video.

Procedure

Step 1 On the home page, click **Camera**, and then select **Encode** > **Video OSD** > **Available Space Count**.

You can also select > **Camera** > **Encode** > **Video OSD** > **Available Space Count**.

Step 2 Click to enable this function.

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

Step 4 Select the font color.

Step 5 Click **Apply**.

- Use this feature with the **Linked Camera Settings**.
- You can enable only one of the 3 OSD features: **Parking Space** , **Traffic Flow Info** or **Available Space Count**.

13.2.2.9 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**.

13.2.3 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 4 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**.

14 System

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

14.1 General Parameters

14.1.1 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 14-1 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**.

14.1.2 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 14-2 Parameters description of date

Parameter	Description
Date Format	Configure the date format.
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**.

14.2 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.

14.2.1 User

14.2.1.1 Adding a User

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

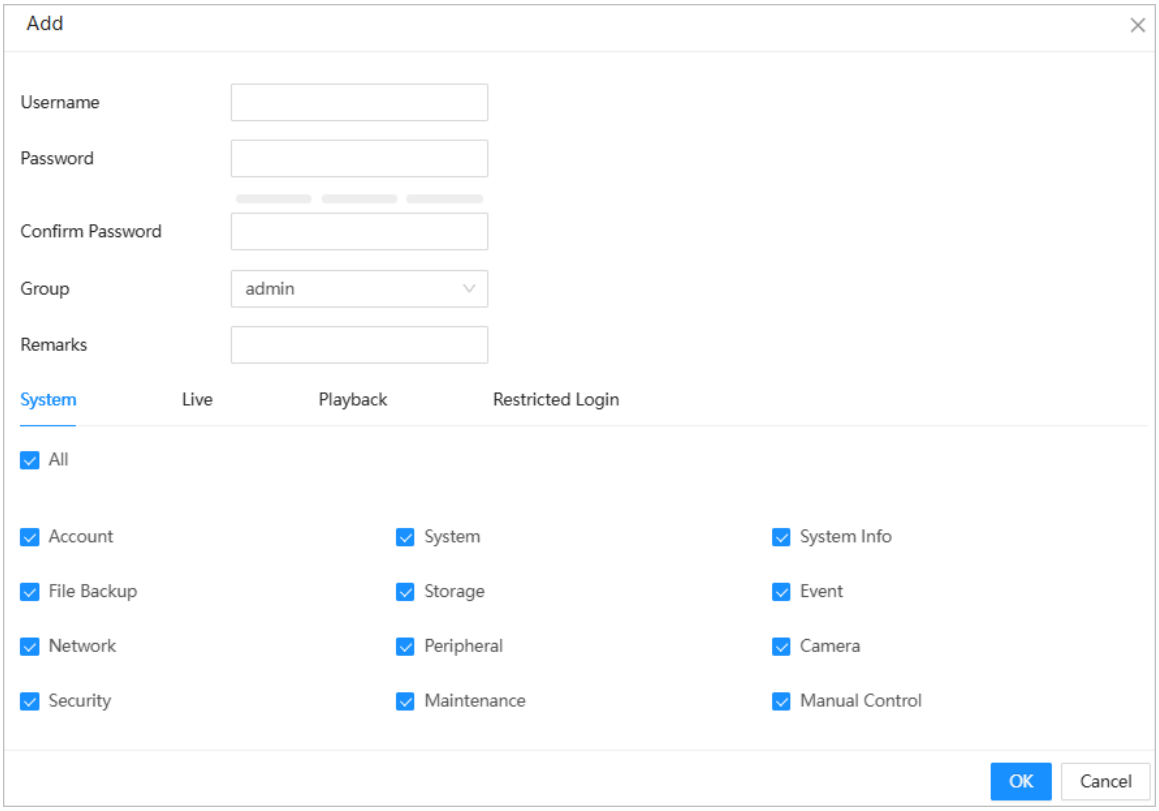
Procedure

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 14-1 Add user



Step 3 Configure the parameters.

Table 14-3 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	

Parameter	Description
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.
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.

14.2.1.2 Resetting Password

Enable the function, and you can reset password by clicking **Forgot password?** on the login page. For details, see "4.2 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?**.

14.2.2 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.

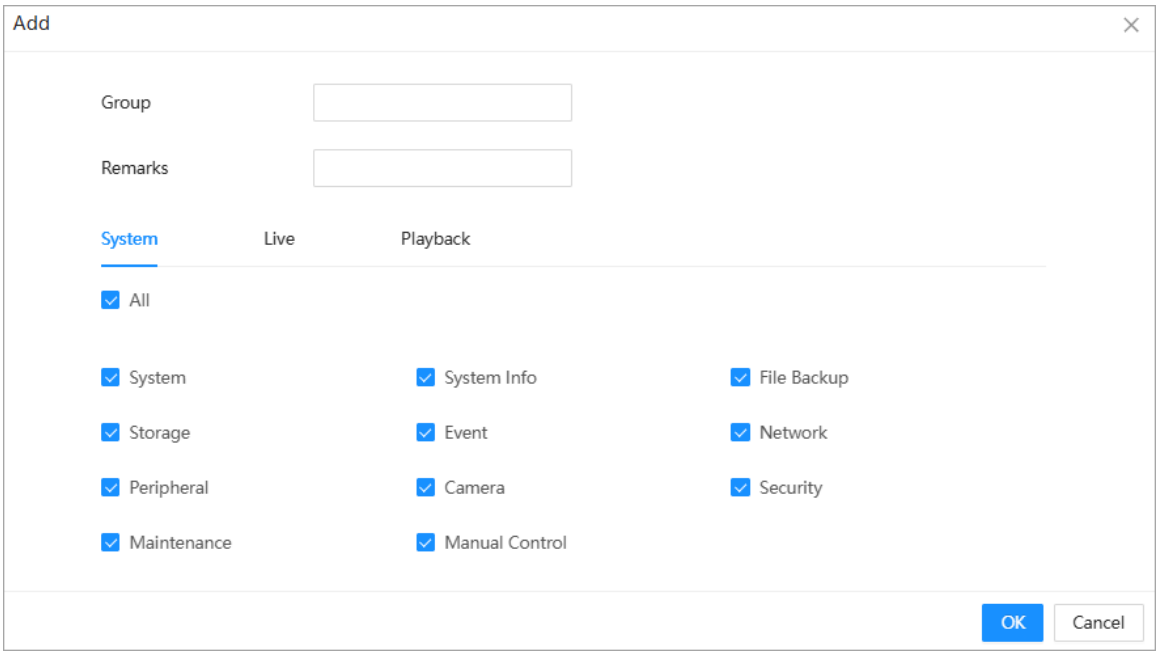
Procedure

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 14-2 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.

14.2.3 Adding an ONVIF User

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

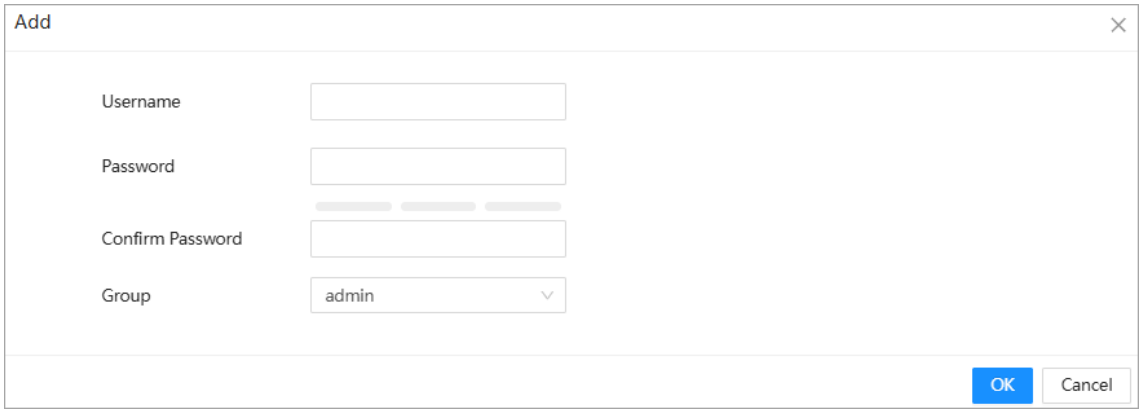
Procedure

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 14-3 Add ONVIF user



Step 3 Configure the parameters.

Table 14-4 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.

14.2.4 Clearing Users

You can clear the added users with one click.

Clearing users will clear all information on custom users and restart the device. Please be advised.

Procedure

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

Step 2 Click **Clear User**, and then enter the login password.

Step 3 Click **OK**.

15 Security

15.1 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

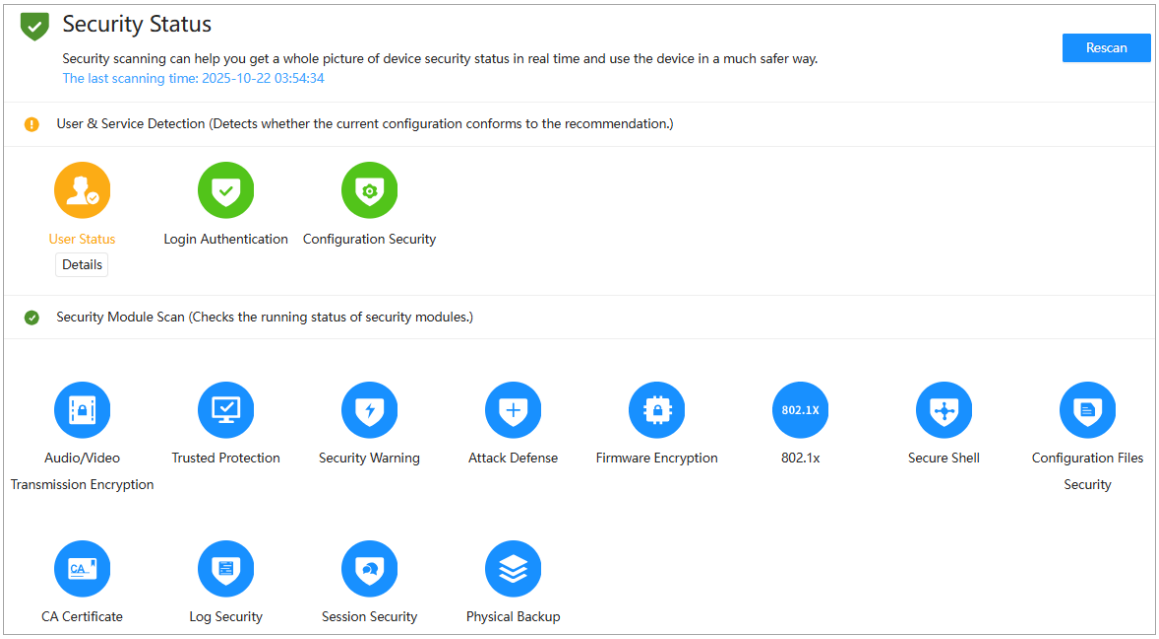
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

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 15-1 Security status



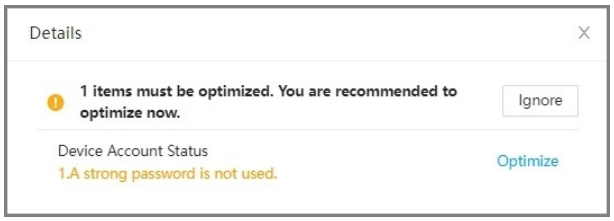
Related Operations

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 15-2 Security Status



15.2 System Service

15.2.1 802.1x

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**.

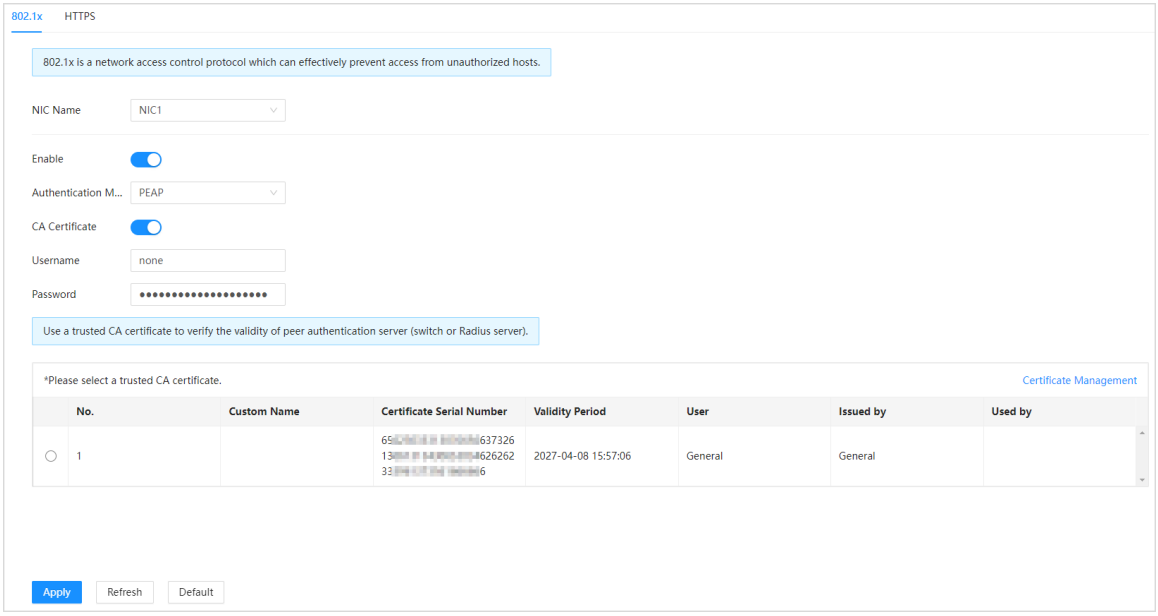
Step 3 Select the NIC name as needed, and click to enable it.

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.

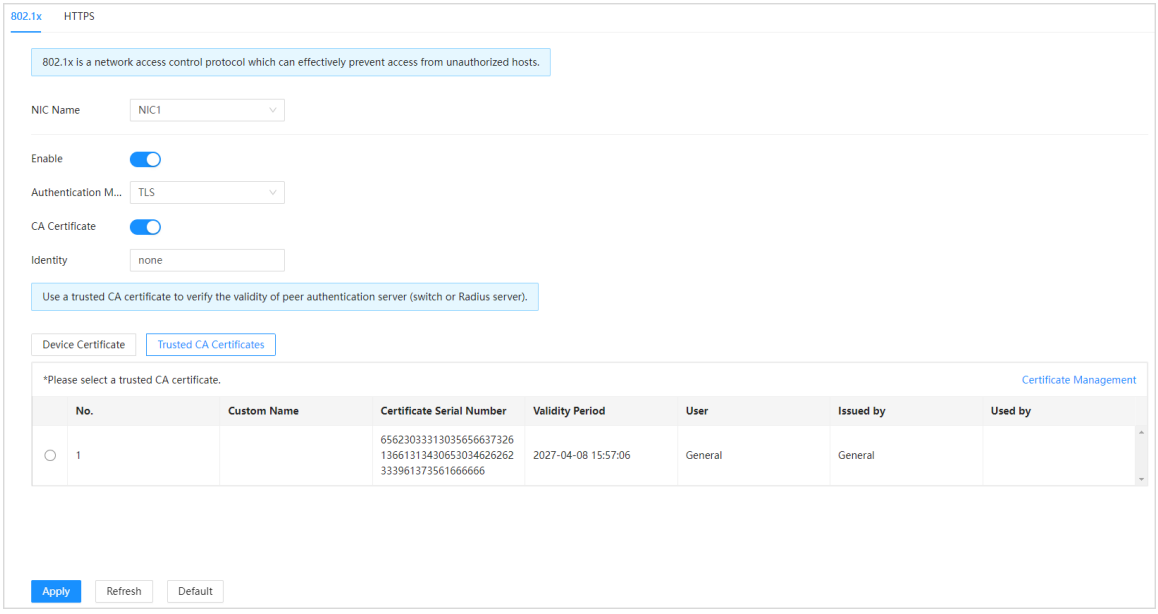
Figure 15-3 802.1x (PEAP)



- 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 15-4 802.1x (TLS)



Step 5 Click **Apply**.

15.2.2 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**.

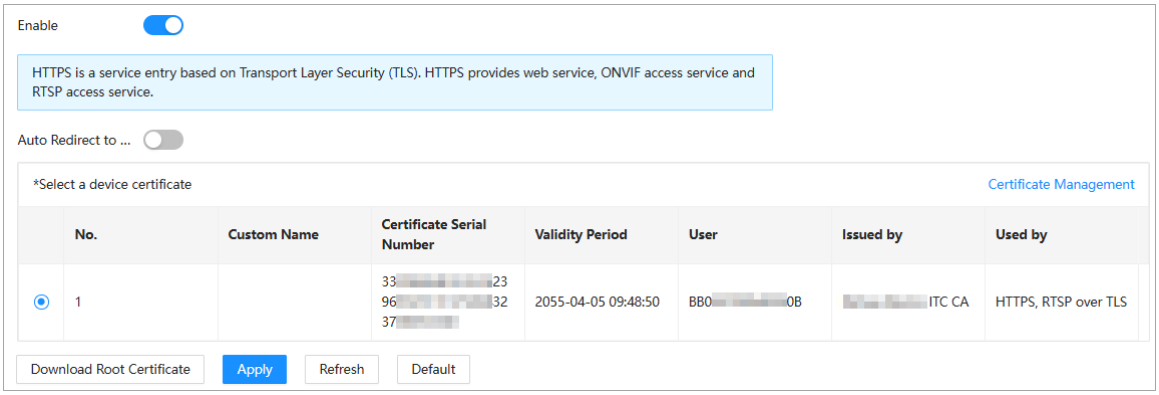
Step 3 Click to enable the function. After it is enabled, you can log in to the camera through HTTP or HTTPS.

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 "15.4.2 Installing Trusted CA Certificate".

Figure 15-5 HTTPS



Step 5 Click **Apply**.

15.3 Attack Defense

15.3.1 Firewall

Configure the firewall to limit access to the camera.

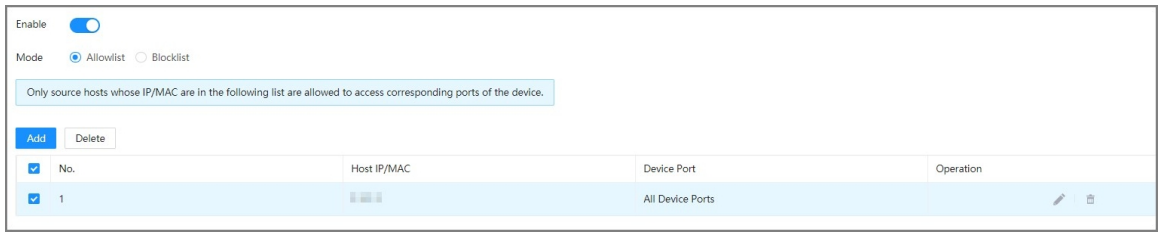
Procedure

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 15-6 Firewall

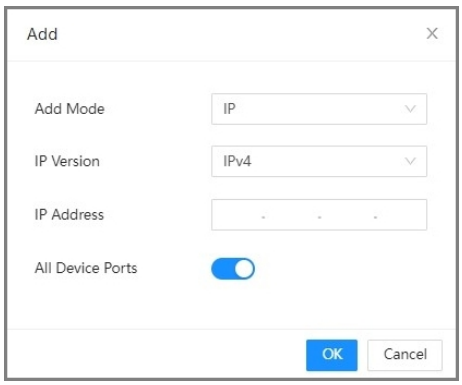


Step 4 Select the mode: **Allowlist** and **Blocklist**.

- **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 15-7 Firewall



Step 6 Click **Apply**.

Related Operations

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

15.3.2 Account Lockout

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

Procedure

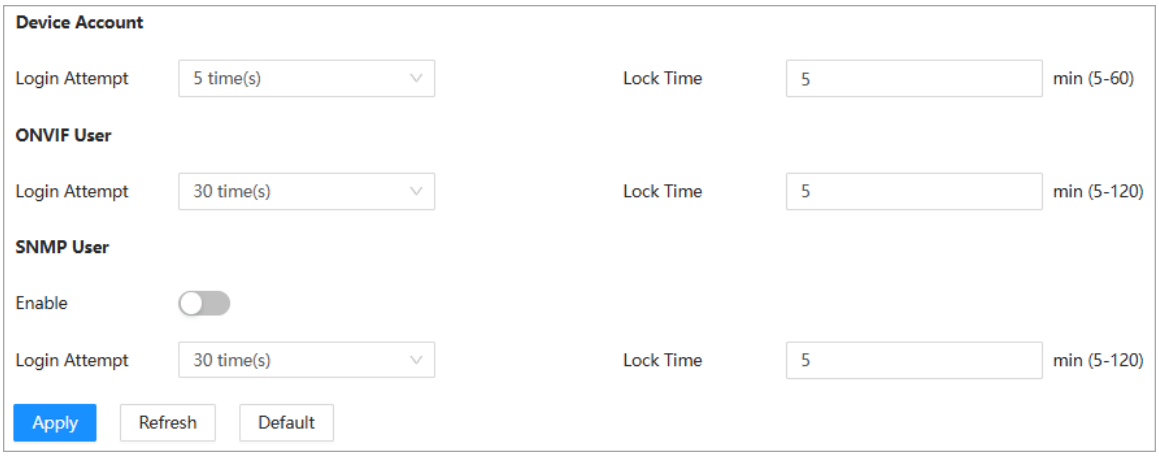
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

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 15-8 Account lockout



Step 4 Click **Apply**.

15.3.3 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**.

15.4 CA Certificate

15.4.1 Installing Device Certificate

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

15.4.1.1 Creating Certificate

Create certificate in the device.

Procedure

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

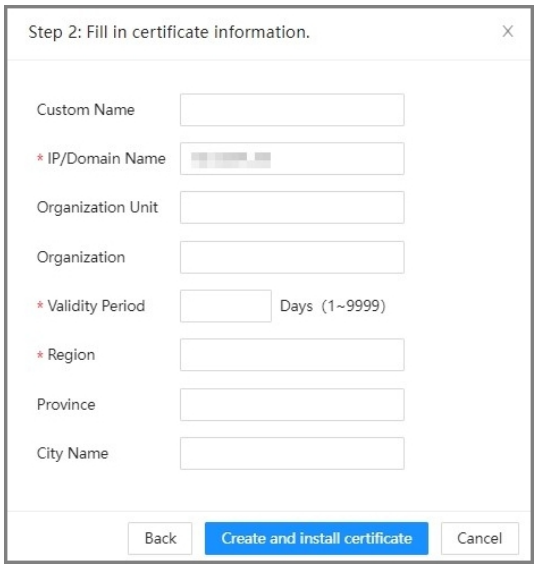
Step 2 Select **CA Certificate** > **Device Certificate**.

Step 3 Click **Install Device Certificate**.

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

Step 5 Enter the certificate information.

Figure 15-9 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.

15.4.1.2 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.

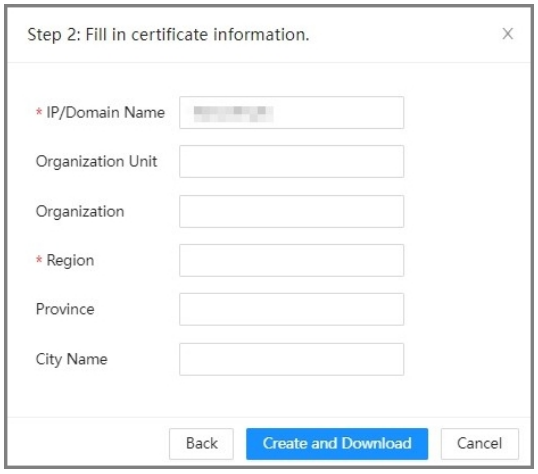
Step 2 Select **CA Certificate** > **Device Certificate**.

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 15-10 Certificate information (2)

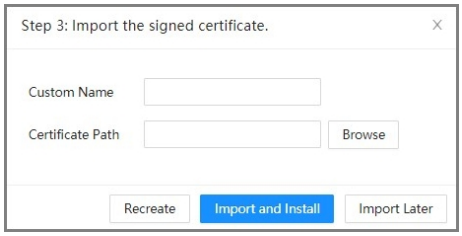


Step 6 Click **Create and Download** and save the request file to your computer.

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 15-11 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.

15.4.1.3 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.

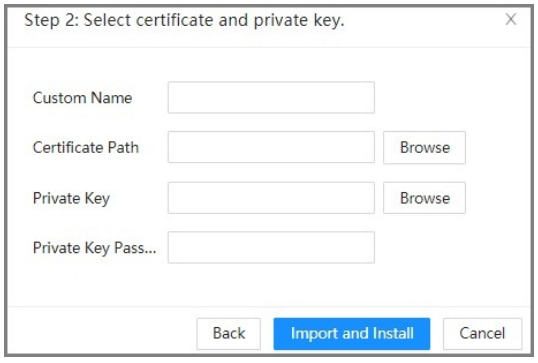
Step 2 Select **CA Certificate** > **Device Certificate**.

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 15-12 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.

15.4.2 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

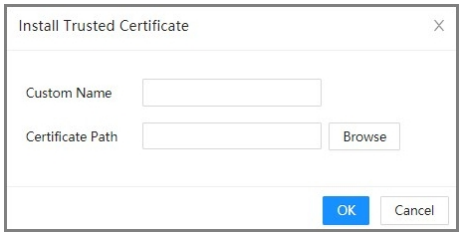
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

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

Step 3 Select **Install Trusted Certificate**.

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

Figure 15-13 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.

15.5 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 15-14 A/V encryption

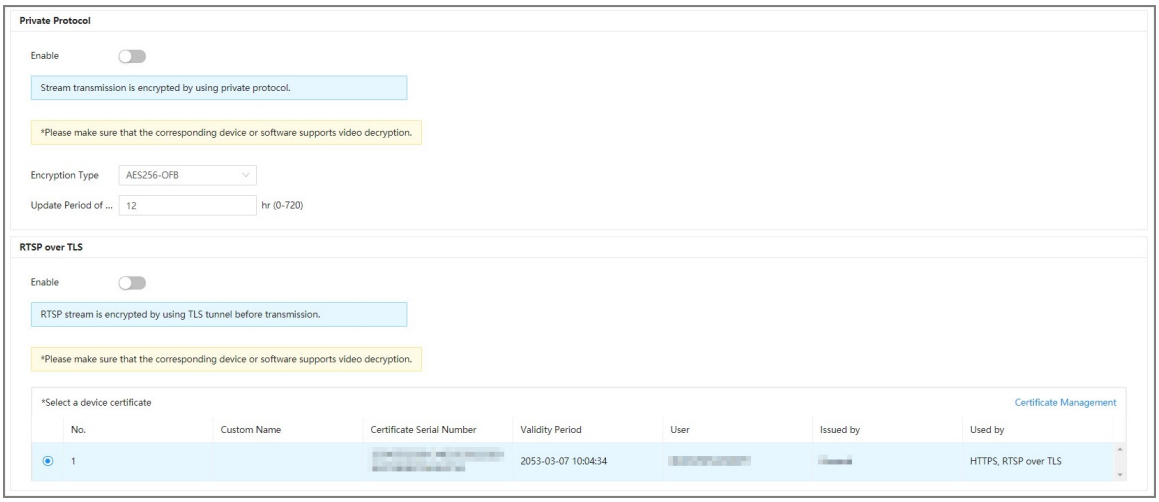


Table 15-1 Parameters description of A/V encryption

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 "15.4 CA Certificate".

Step 4 Click **Apply**.

15.6 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.

15.6.1 Security Exception

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

Procedure

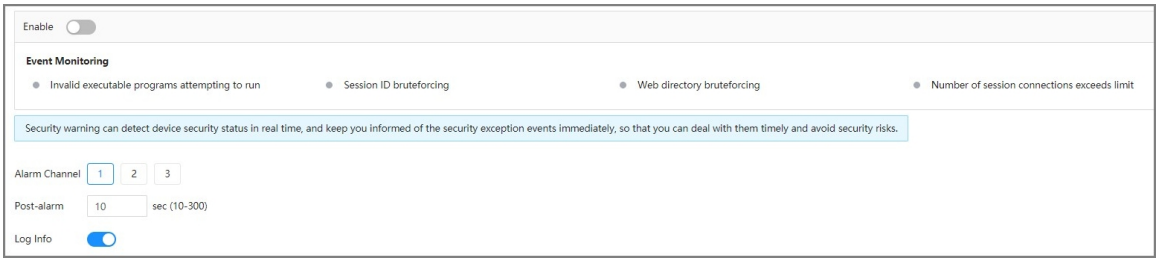
Step 1 On the home page, click **Security**, or select > **Security** at the upper-right corner.

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

Step 3 Click to enable the function.

Step 4 Configure the parameters.

Figure 15-15 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 "16.3.1 Searching for Logs".

Step 5 Click **Apply**.

15.6.2 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 "16.3.1 Searching for Logs".

Step 5 Click **Apply**.

15.7 Security Authentication

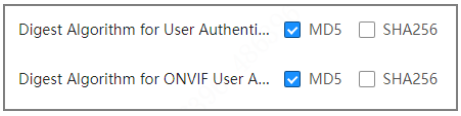
Procedure

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 15-16 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**.

16 Maintenance Center

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

16.1 One-Click Diagnosis

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

Procedure

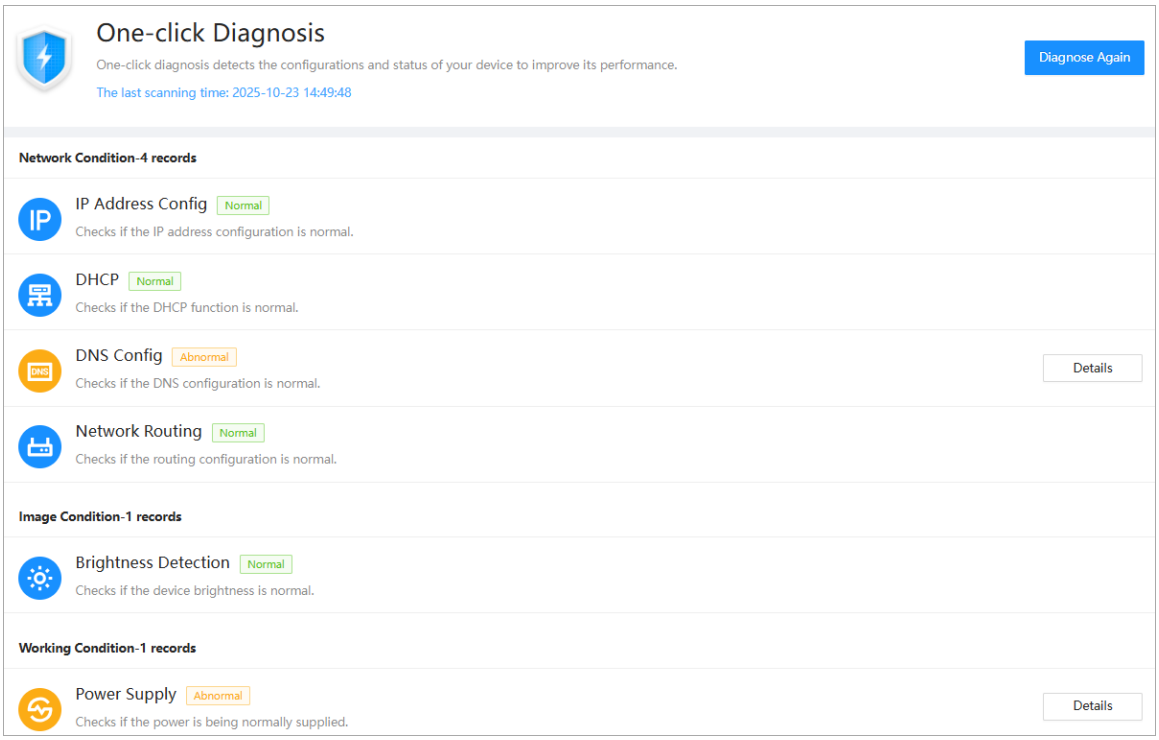
Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

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

Step 3 Click **Diagnose**.

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

Figure 16-1 One-click diagnosis



Related Operations

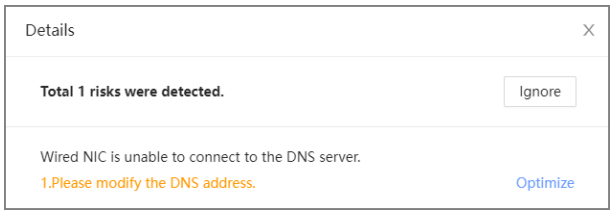
After the diagnosis completes, the page displays the diagnosis results. Yellow indicates that the condition is abnormal, and Green indicates that the condition is normal.

- 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 16-2 Details



16.2 System Information

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

16.2.1 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.

16.2.2 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.

16.2.3 Running Status

On the home page, select **Maintenance Center** > **System Info** > **Running Status** , or select > **Maintenance Center** > **System Info** > **Running Status** at the upper right, and then you can view the running status of the camera.

Click **Refresh** to get the latest status.

16.2.4 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.

16.3 Log

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

16.3.1 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**.

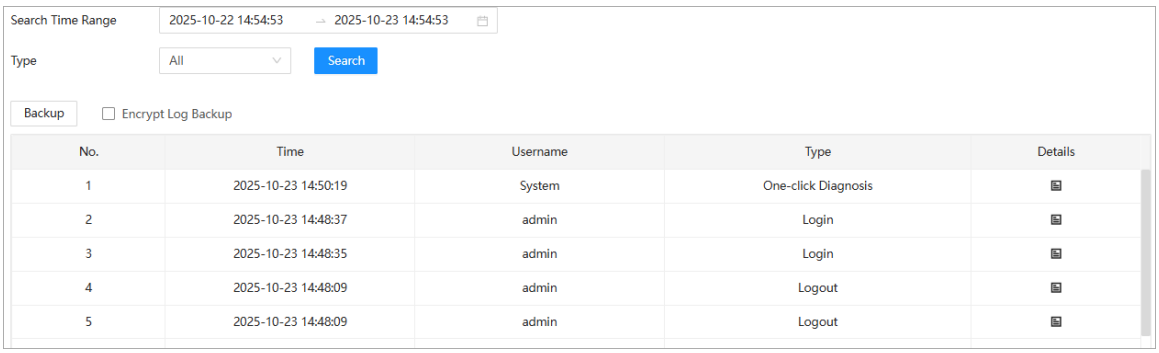
Step 3 Configure the search time range, and then select the log type.

- **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 16-3 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.

16.3.2 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**.

16.4 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 "14.2 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.

16.4.1 Maintenance

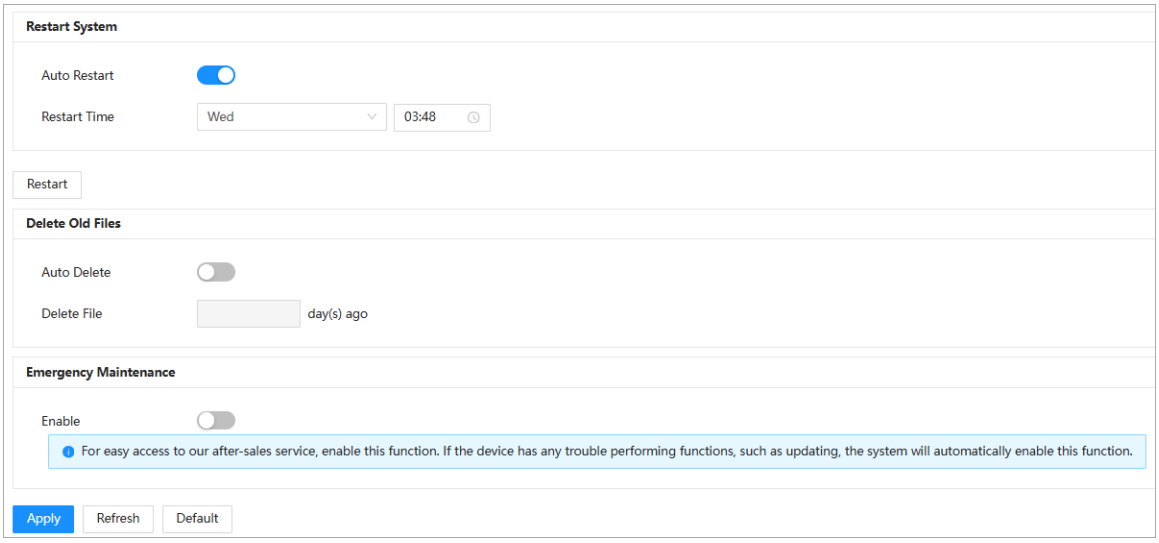
You can restart the system manually, and set the time of automatic restart and deleting old files. This function is not enabled by default.

Procedure

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

Step 2 Select **Maintenance**.

Figure 16-4 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**.

16.4.2 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.

16.4.3 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.

16.5 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.

16.6 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

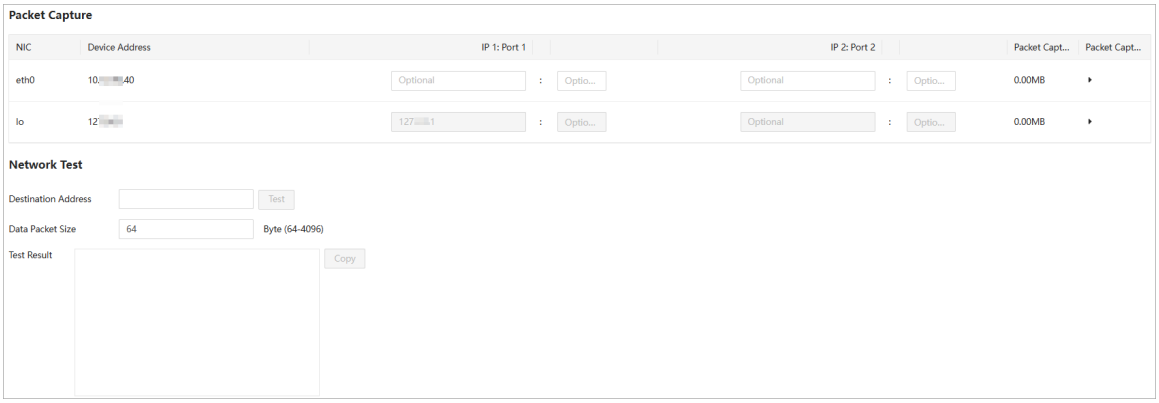
Step 1 On the home page, click **Maintenance Center**, or select > **Maintenance Center** at the upper right.

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 16-5 Packet capture

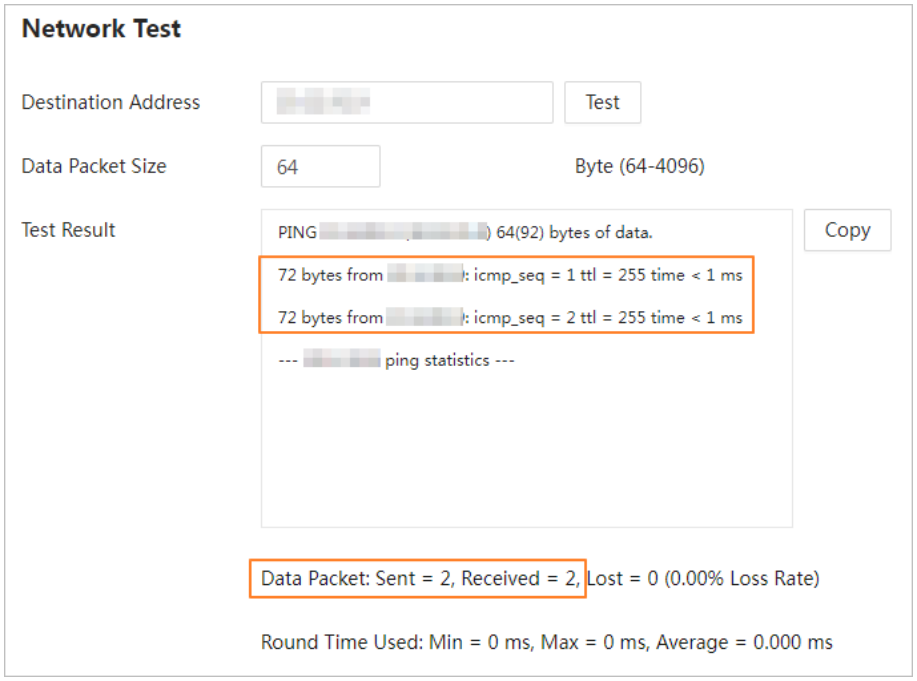


- ◇ **Packet Capture**: It examines network traffic by capturing IP packets to investigate network issues and detect security threats.
  1. (Optional) Enter the specified IP and port.
  2. Click to perform a packet capture. A packet sniffer backup will be uploaded automatically after you click to end 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 16-6 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.

17 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.

17.1 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 17-1 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**.

17.2 Network

This section introduces network configuration.

17.2.1 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 17-2 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**.

17.2.2 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 17-3 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.

Parameter	Description
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.

17.2.3 DDNS

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

Prerequisites

Check the type of DNS server supported by the camera.

Procedure

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

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

Step 2 Click to enable the function.

Step 3 Configure the parameters.

Table 17-4 Parameters description of DDNS

Parameter	Description
Type	The name and web address of the DDNS service provider. CN99 DDNS web address: www.3322.org
Address	
Domain	The domain name you registered on the DDNS website.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the website of the DDS server provider.
Password	
Interval	The update cycle of the connection between the device and the server, and the time is 10 minutes by default.

Step 4 Click **Apply**.

Results

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

17.2.4 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 17-5 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**.

17.2.5 Multicast

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

Procedure

Step 1 Select > **Network** > **Multicast**.

Step 2 Click , and then configure the parameters.

Table 17-6 Parameters description of multicast

Parameter	Description
Multicast Address	The multicast IP addresses of **Main Stream** and **Sub Stream** are 224.1.2.4 by default, and the range is 224.0.0.0–239.255.255.255.
Port	The multicast port of corresponding stream: **Main Stream** : 40000; **Sub Stream1**: 40016; **Sub Stream2**: 40032, and all the range is 1025–65500.

Step 3 Click **Apply**.

Results

On the **Live** page, select **RTSP** in **Multicast**, and then you can view the video image with multicast protocol.

17.2.6 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.

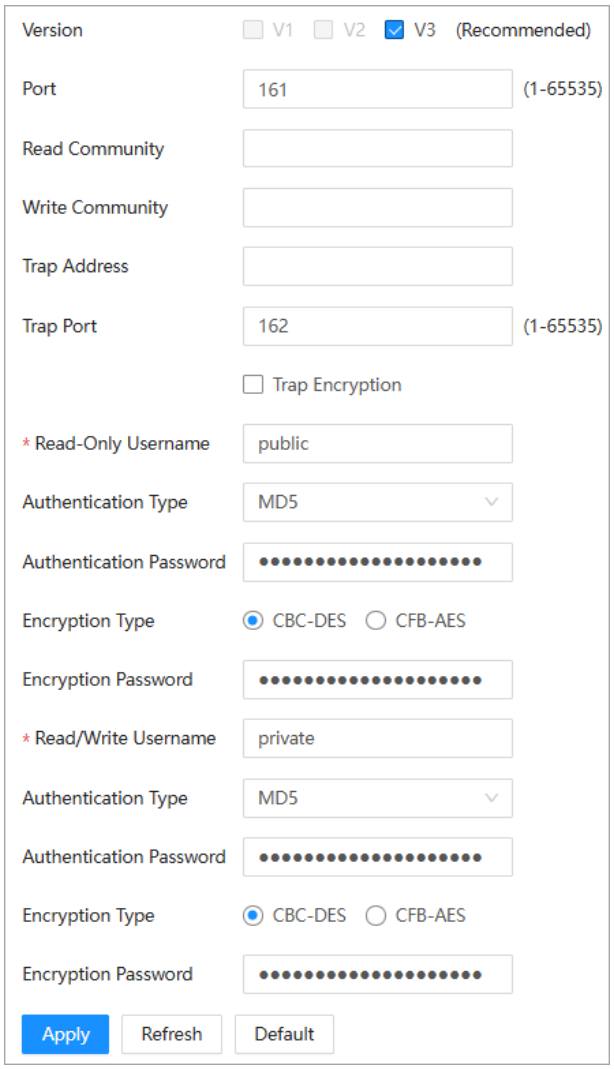
Prerequisites

- 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 17-1 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 17-7 Parameters description of SNMP

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

17.2.7 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 17-8 Parameters description of email

Parameter	Description	
SMTP Server	SMTP server address.	For details, see Table 17-9 .
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 17-9 .	
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.	

Parameter	Description
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 17-9 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**.

17.2.8 PPPoE

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

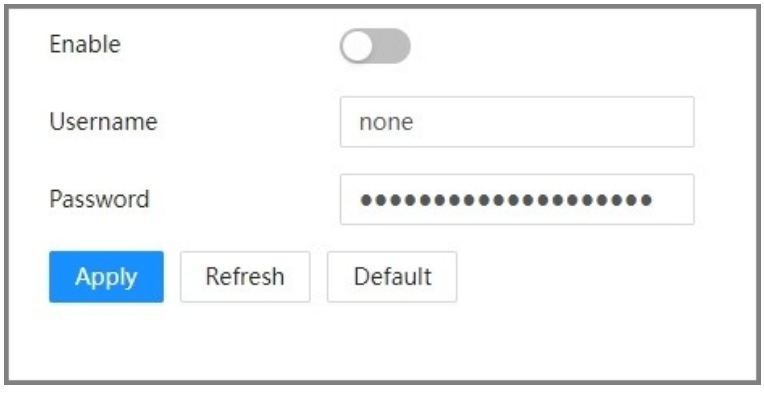
Prerequisites

- The camera has connected to the network.
- You have gotten the account and password from an internet service provider.

Procedure

Step 1 Select > **Network** > **PPPoE**.

Figure 17-2 PPPoE



Step 2 Click , and then enter username and password.

- Disable UPnP while using PPPoE to avoid possible influence.

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

Step 3 Click **Apply**.

The success prompt box is displayed, and then the real-time WAN IP address is displayed. You can access camera through the IP address.

17.2.9 Platform Access

17.2.9.1 DoLynk Cloud

You can easily manage devices with the DMSS app.

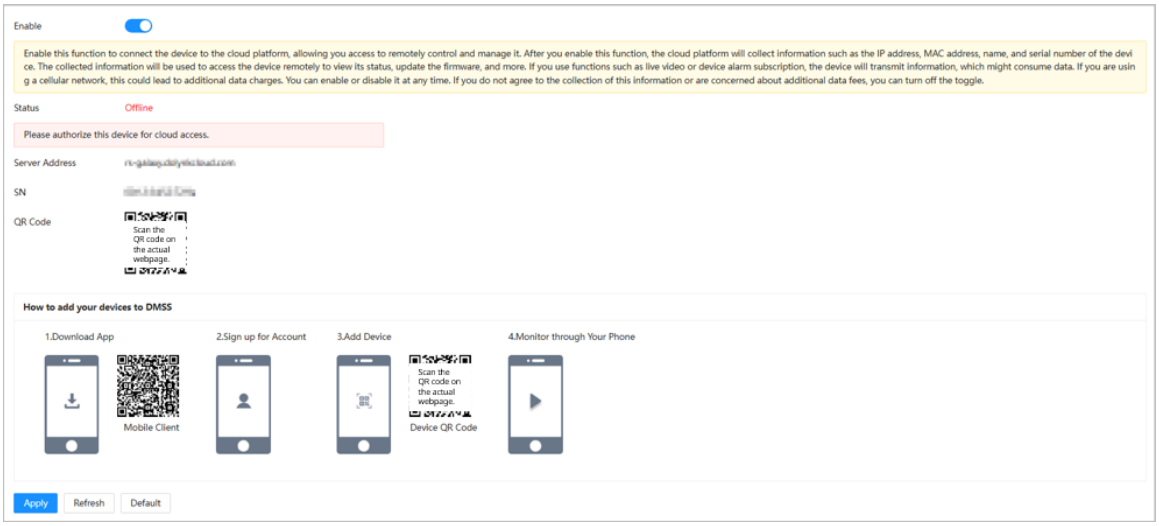
Procedure

Step 1 Enable the **DoLynk Cloud** function.

1. Select > **Network** > **Platform Access** > **Dolynk Cloud**.
2. Click to enable the function.
3. Click **Apply**.

- When **DoLynk Cloud** is enabled, remote management on device is supported.
- When **DoLynk Cloud** is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You can cancel **Enable** selection to reject the collection.

Figure 17-3 DoLynk Cloud



Step 2 Scan the **Mobile Client** QR code to install the DMSS app.

Step 3 Add and manage devices with the DMSS app.

1. Log in to DMSS app and tap **Device management**.
2. Tap **+** at the upper-right corner.

3. Scan the **Device QR code** to add the device.
4. Follow the instructions to finish the settings.

17.2.9.2 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**.

17.2.9.3 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.

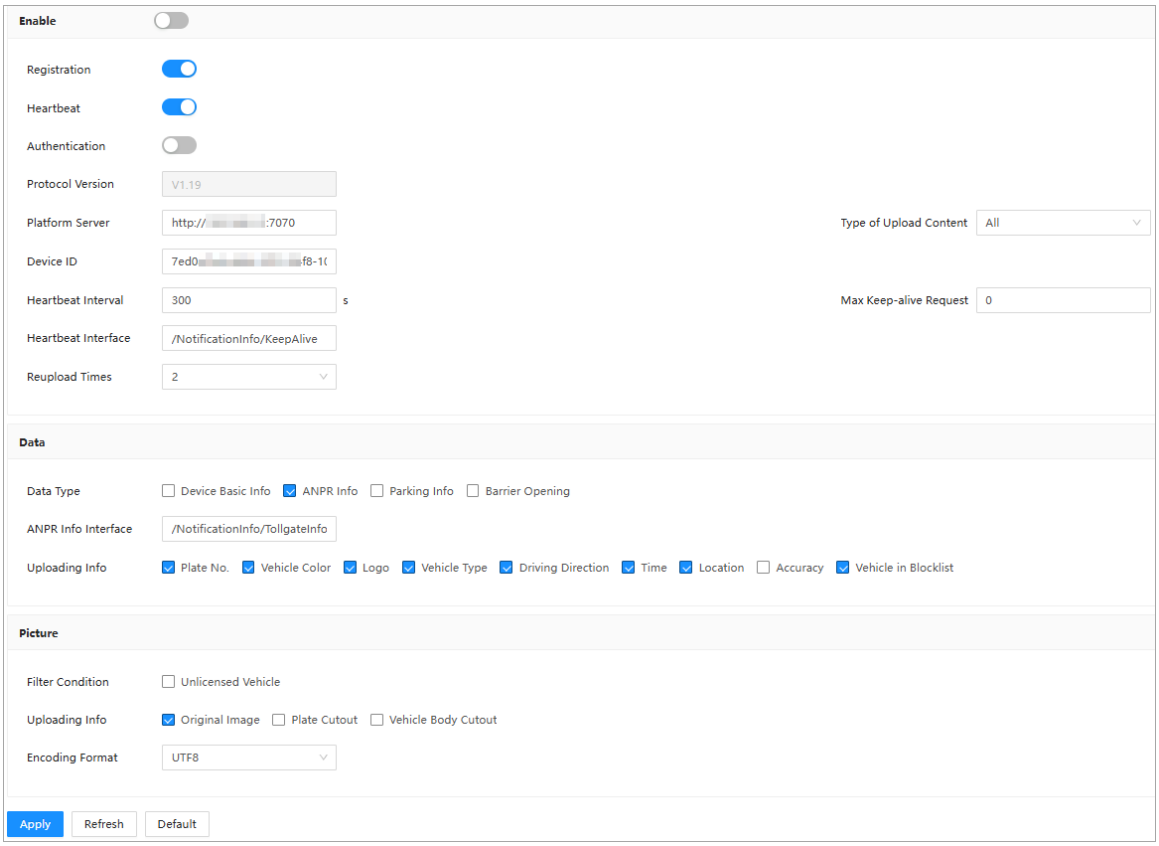
- Related business data must be in JSON format with ContentType: application/json;charset=UTF-8 as HTTP headers, which means the encoding method is UTF-8.

Procedure

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

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

Figure 17-4 ITSAPI



Step 3 Configure the parameters.

Table 17-10 Parameters description of ITSAPI

Section	Parameter	Description
Basic Configuration	Registration	After it is enabled (enabled by default), the device automatically requests registration from the platform server.
	Heartbeat	After it is enabled (enabled by default), the device automatically sends a heartbeat packet to the platform, and then the platform will determine whether the device is offline according the heartbeat.
	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**.

Section	Parameter	Description
	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.
	Reupload Times	Set the times of re-uploading the images when the upload fails. • 1–98: Uploads the next image after the defined times of failed response. • **Unlimited Reupload Times** : Uploads the image again after a failed response until the upload succeeds. • **Do Not Reupload** : Uploads the next image when it fails to upload an image.
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.
	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**.

17.2.9.4 Parking MQTT

Procedure

Step 1 On the upper right of the home page, select > **Network Settings** > **Platform Access** > **Parking MQTT**.

Step 2 Click to enable the function. After the function is enabled, the device will be connected to the MQTT platform.

Step 3 Configure the parameters.

Figure 17-5 Parking MQTT (1)

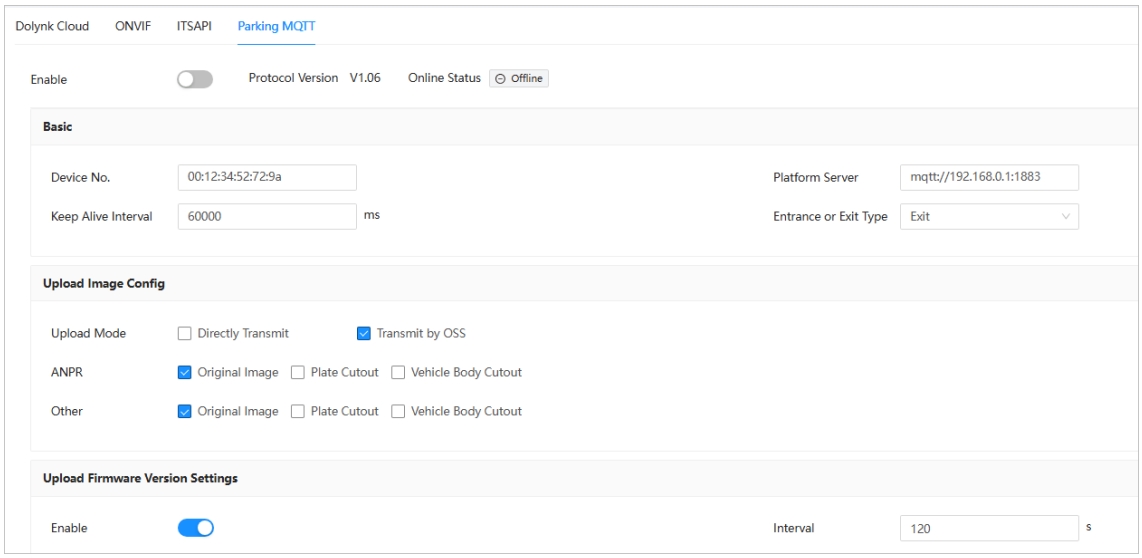


Figure 17-6 Parking MQTT (2)

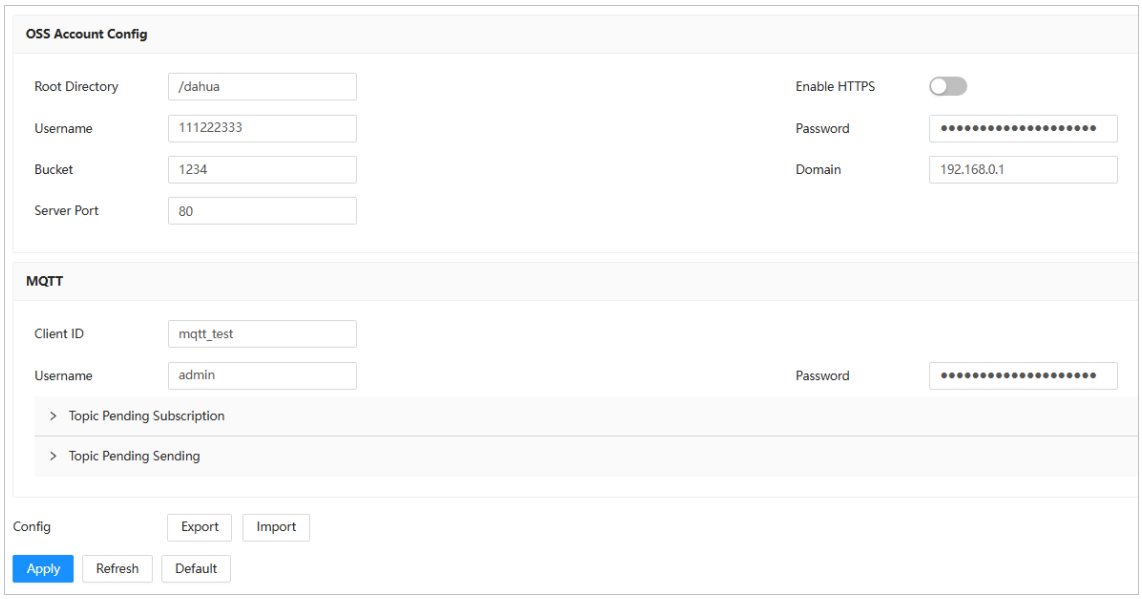


Table 17-11 Description of the parking MQTT parameters

Parameter		Description
Basic	Device No.	Enter the unique identification number of the device.
	Keep Alive Interval	Set the interval (unit: ms) for which the device sends the heartbeat to the platform.
	Platform Server	Enter MQTT server address.
	Entrance or Exit Type	Select the entrance or exit type.

Parameter		Description
Upload Image Config	Upload Mode	Select the mode for uploading images. Supports direct transmission and transmission by OSS.
	ANPR	Select the image type to be uploaded, including original image, plate cutout, and vehicle body cutout.
	Other	
Upload Firmware Version Settings	Enable	Click to enable the function of uploading the firmware version.
	Interval	Set the interval (unit: s) for uploading the firmware version.
OSS Account Config	Root Directory	Set the root directory of the OSS account.
	Enable HTTPS	Click to enable HTTPS.
	Username	Enter the username of the OSS account.
	Password	Enter the password of the OSS account.
	Bucket	Enter the name of the OSS bucket.
	Domain	Enter the domain of the OSS account.
	Server Port	Set the server port of the OSS account.
MQTT	Client ID	Enter the unique identification number of the MQTT.
	Username	Enter the username of MQTT.
	Password	Enter the password of MQTT.
	Topic Pending Subscription	The message topic to be subscribed for configuring MQTT.
	Topic Pending Sending	The message topic to be sent for configuring MQTT.

Step 4 Click **Apply**.

17.2.10 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 17-12 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**.

17.2.11 RTMP

Through RTMP, you can access a third-party platform (such as Ali and YouTube) to realize video live view.

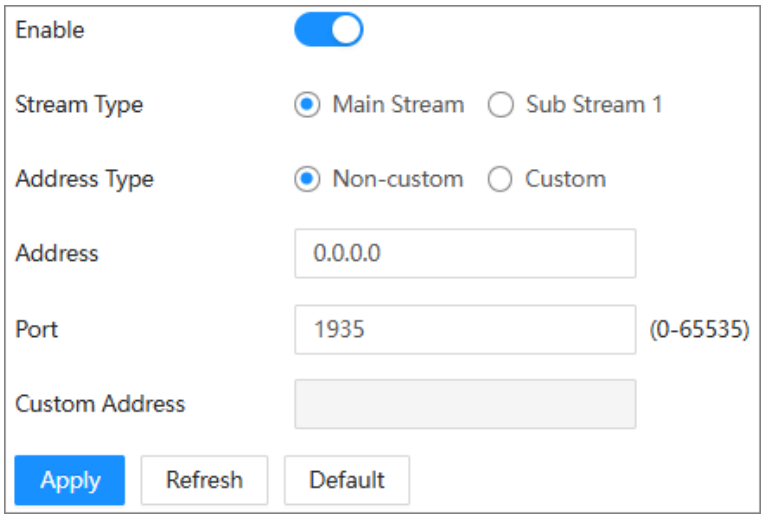
Background Information

- RTMP can be configured by admin only.
- RTMP supports the H.264, H.264 B and H.264H video formats, and the AAC audio format only.

Procedure

Step 1 Select > **Network** > **RTMP**.

Figure 17-7 RTMP



Step 2 Click .

Make sure that the IP address is trustable when enabling RTMP.

Step 3 Configure RTMP parameters.

Table 17-13 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	• **Non-custom** : Enter the server IP and domain name. • **Custom** : Enter the path allocated by the server.
IP Address	When selecting **Non-custom**, you need to enter server IP address and port. • **IP address** : Support IPv4 or domain name. • **Port** : Keep the default value.
Port	
Custom Address	When selecting **Custom**, you need to enter the path allocated by the server.

Step 4 Click **Apply**.

17.3 Event

17.3.1 Setting Alarm

17.3.1.1 Enabling Alarm-in and Alarm-out Ports

You can set several parameters of relay activation such as relay-in, period, anti-dither, and sensor type. When an alarm is triggered, the device sends a signal to trigger, for example, a buzz on external devices.

Procedure

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

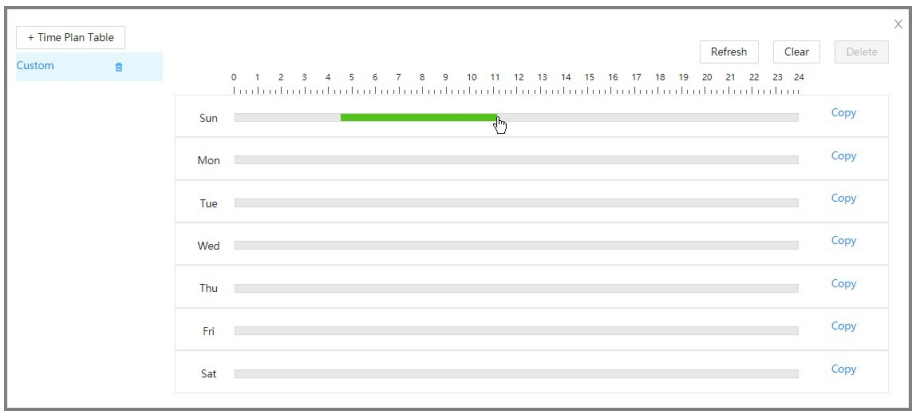
Step 2 Click next to **Enable** to enable alarm input for the current channel.

Step 3 Select an alarm input channel and schedule.

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

1. Click **Add Schedule**.
2. Drag on the timeline to set the arming periods. Alarms will be triggered in the green period.

Figure 17-8 Drag to set periods



- Click **Copy** next to a day, and select the days that you want to copy to in the prompt page, you can copy the configuration to the selected days. Select the **Select All** checkbox to select all days to copy the configuration.
- You can set 6 periods per day.

3. (Optional) Click **+ Time Plan Table** to add more schedules.
4. Click **Apply**.

Step 4 Configure other parameters.

Table 17-14 Parameters description of alarm-in and alarm-out ports

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

Step 5 Click **Apply**.

17.3.1.2 Alarm-out Port

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

Procedure

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

Step 2 Select one or more alarm channels.

Step 3 Click **Apply** to send alarm signals to the selected channel.

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

It is disabled by default to prevent the selected channels from keeping the barrier open by sending continuous signals.

17.3.2 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**.

17.3.2.1 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 17-15 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**.

17.3.2.2 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 17-16 Parameters description of exception

Parameter	Description
Alarm-out Port	Click , and then select an alarm output channel. The corresponding device will be activated when alarms are triggered.
Alarm Channel	
Post-alarm	When an alarm is triggered, it will continue for the defined period after it ends.

Step 4 Click **Apply**.

17.3.2.3 Setting Defocus Detection

In case of defocus is detected, for example, the image is blurred, an alarm will be triggered.

Procedure

Step 1 Select > **Event** > **Exception** > **Defocus Detection**.

Step 2 Click to enable defocus detection.

Step 3 Click **Apply**.

17.3.3 Rule Configuration

You can configure the IVS rules for intrusion and loitering detection, parking space detection, and illegal parking detection. For details, see "9 IVS".

17.3.4 Subscribing Alarm

17.3.4.1 Alarm Types

Click at the right-upper corner of the main page, and then you will see the alarm types that are supported.

Table 17-17 Parameters description of alarm types

Alarm Type	Description	Preparation
Low SD card space	An alarm is triggered when the free space of SD card is less than the configured value.	Low SD card space detection is enabled. For details, see "17.3.2.1 Setting SD Card Exception".
SD card error	An alarm is triggered when there is failure or malfunction in the SD card.	SD card error detection is enabled. For details, see "17.3.2.1 Setting SD Card Exception".
External alarm	An alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see "17.3.1.1 Enabling Alarm-in and Alarm-out Ports".
No SD card	An alarm is triggered when there is no SD card installed on the camera.	The no SD card detection function is enabled. For details, see "17.3.2.1 Setting SD Card Exception".
Vehicle blocklist	An alarm is triggered when a vehicle in the blocklist is detected.	The blocklist alarm is enabled. For details, see "8.2.2 Smart Detection".

Alarm Type	Description	Preparation
Invalid access	An alarm is triggered when number of login attempts to the webpage of the camera exceeds the defined value.	The illegal login function is enabled. For details, see "15.6.2 Illegal Login".
Security exception	An alarm is triggered when the device detects malicious attacks.	Security exception detection is enabled. For details, see "15.6.1 Security Exception".
Temporary vehicle	An alarm is triggered when the device detects temporary vehicles.	Temporary vehicle detection is enabled. For details, see "8.2.2 Smart Detection".
Traffic standstill	An alarm is triggered when the device detects traffic standstill.	Traffic standstill detection is enabled. For details, see "8.2.2 Smart Detection".
Illegal parking	An alarm is triggered when the device detects illegal parking.	Rules for detecting illegal parking are configured. For details, see "9.3 Illegal Parking Area".
IVS	An alarm is triggered when the device detects intrusion and loitering, parking space, .	IVS is enabled. For details, see "17.3.3 Rule Configuration".
Backing and leaving	A vehicle that crosses the detection line is captured, and it will be captured again when it reverses.	Backing and leaving detection is enabled. For details, see "8.2.2 Smart Detection".

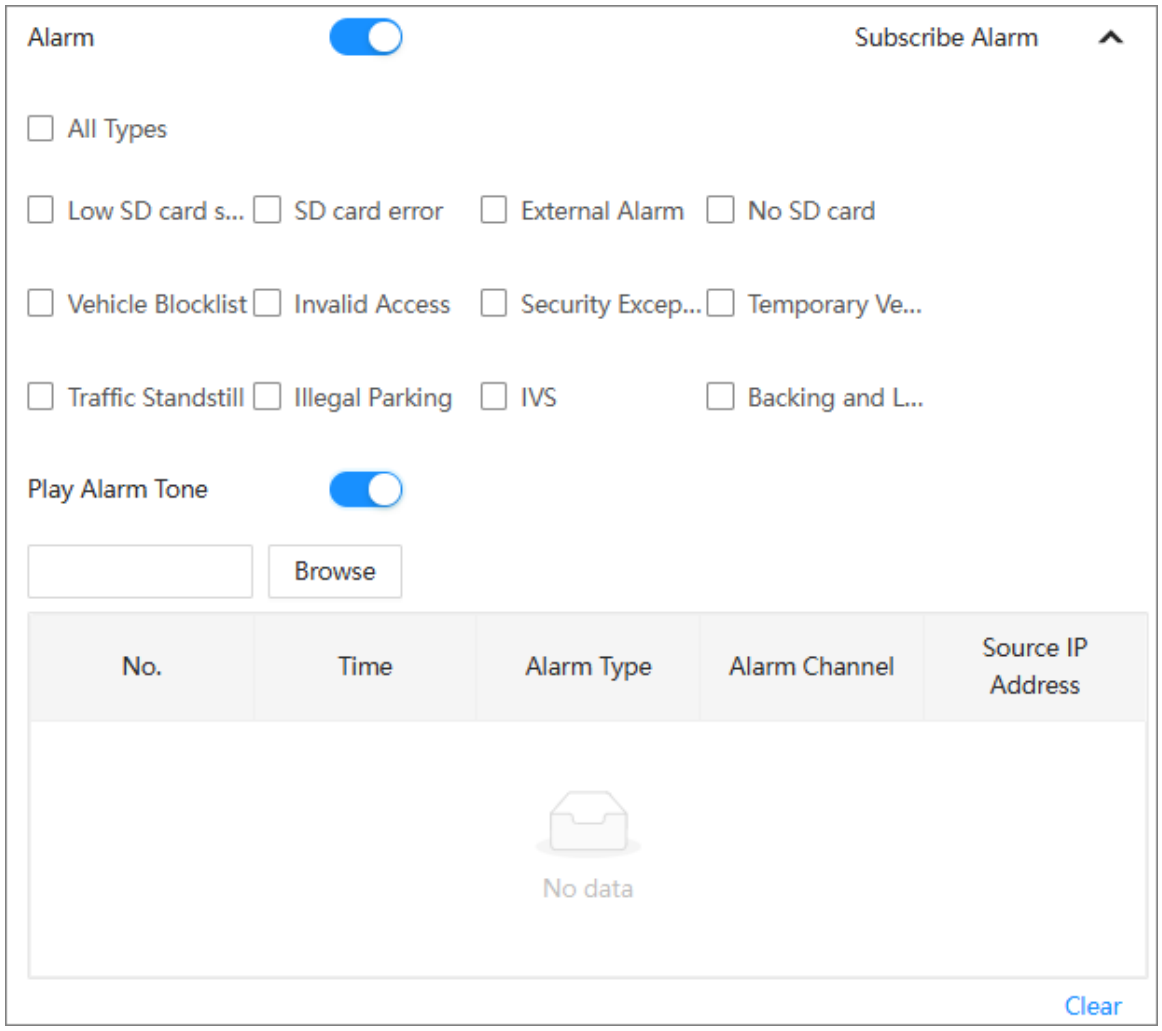
17.3.4.2 Subscribing Alarm Information

When a subscribed alarm is triggered, the camera records and displays detailed information of the alarm on the right of the page.

Procedure

Step 1 Click  at the right-upper corner of the main page.

Figure 17-9 Subscribe to alarms



Step 2 Click next to **Alarm**.

Step 3 Select one or more alarm types. For details on each alarm, see "17.3.4.1 Alarm Types".

Click **Clear** to clear all the alarms that are displayed.

Step 4 Click next to **Play Alarm Tone** , and then click **Browse** to select an alarm sound file.

The camera will play the file when a subscribed alarm is triggered.

17.4 Local Storage

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

Procedure

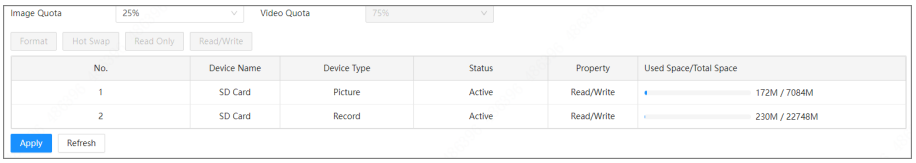
Step 1 Select > **Storage** > **Local Storage**.

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 17-10 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;
   - Establish 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).