



Smart ANPR Camera

Web 5.0 Operation Manual







Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

| Version | Revision Content | Release Date |
|---------|--|----------------|
| V1.0.2 | Add "Maintenance Center". | September 2023 |
| V1.0.1 | Update the color theme of the webpage. | August 2023 |
| V1.0.0 | First release. | April 2023 |

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between

the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the 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




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



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

against lightning. For outdoor scenarios, strictly comply with the lightning protection regulations.

- Ground the function earthing portion  of the device to improve its reliability (certain models are not equipped with earthing holes). The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.
- The dome cover is an optical component. Do not directly touch or wipe the surface of the cover during installation.

Operation Requirements



- 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 | 8 |
| 4.1 Device Login..... | 8 |
| 4.2 Resetting Password | 8 |
| 5 Home Page..... | 9 |
| 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..... | 17 |
| 7.4 Live View Function Bar..... | 18 |
| 7.5 Display Mode | 18 |
| 8 Search..... | 20 |
| 8.1 Picture Query..... | 20 |
| 8.1.1 Memory Card Image | 20 |
| 8.1.2 Local Image..... | 20 |
| 8.2 Playing Recordings | 21 |
| 8.2.1 Record..... | 21 |
| 8.2.2 Watermark | 21 |
| 8.3 Snapshot Records..... | 21 |
| 8.4 Alarm-out Port | 22 |
| 9 Setting..... | 23 |
| 9.1 Local | 23 |
| 9.2 ANPR | 24 |

| | |
|---|----|
| 9.2.1 Setting Snapshot..... | 24 |
| 9.2.2 Configuring AI Setting | 25 |
| 9.2.2.1 Intelligent Analysis | 25 |
| 9.2.2.2 Smart Detection..... | 26 |
| 9.2.3 Image Config..... | 27 |
| 9.2.3.1 Original Picture OSD | 27 |
| 9.2.3.2 Size..... | 29 |
| 9.2.3.3 Cutout..... | 30 |
| 9.2.4 Setting Blocklist and Allowlist for Vehicles..... | 30 |
| 9.2.4.1 Allowlist..... | 30 |
| 9.2.4.2 Fuzzy Match..... | 31 |
| 9.2.4.3 Blocklist | 32 |
| 9.2.5 Configuring Barrier Control | 32 |
| 9.2.6 Configuring RS-485 Settings..... | 33 |
| 9.2.7 Configuring LED Screen..... | 35 |
| 9.2.8 Configuring Broadcast..... | 36 |
| 9.2.8.1 Event Broadcast..... | 36 |
| 9.2.8.2 Passing Vehicles | 37 |
| 9.2.8.3 Volume/Encoding | 38 |
| 9.2.8.4 Audio File..... | 39 |
| 9.2.9 Setting Device Test | 39 |
| 9.2.9.1 Device Test..... | 39 |
| 9.2.9.2 Capture Adjustment Information..... | 40 |
| 9.2.9.3 Collection Log..... | 40 |
| 9.3 Camera..... | 41 |
| 9.3.1 Setting Image Parameters..... | 41 |
| 9.3.1.1 General Parameters..... | 41 |
| 9.3.1.2 Shutter Parameters..... | 43 |
| 9.3.1.3 Metering Parameters | 44 |
| 9.3.2 Setting Encode Parameters | 45 |
| 9.3.2.1 Video Stream..... | 45 |
| 9.3.2.2 Video OSD..... | 46 |
| 9.3.2.2.1 Configuring Channel Title | 47 |
| 9.3.2.2.2 Configuring Time Title | 47 |
| 9.3.2.2.3 AI Detection..... | 47 |
| 9.3.2.2.4 Configuring Privacy Masking..... | 47 |
| 9.3.2.2.5 Configuring Custom Title..... | 48 |

| | |
|---|-----------|
| 9.3.2.3 ROI | 48 |
| 9.4 Network | 48 |
| 9.4.1 TCP/IP | 49 |
| 9.4.2 Port | 49 |
| 9.4.3 DDNS | 51 |
| 9.4.4 Auto Registration | 52 |
| 9.4.5 Multicast | 52 |
| 9.4.6 SNMP | 53 |
| 9.4.7 Email | 56 |
| 9.4.8 PPPoE | 56 |
| 9.4.9 Platform Access | 57 |
| 9.4.9.1 P2P | 57 |
| 9.4.9.2 ONVIF | 58 |
| 9.4.9.3 ITSAPI | 58 |
| 9.4.10 Basic Services | 60 |
| 9.5 Event | 61 |
| 9.5.1 Setting Alarm | 61 |
| 9.5.1.1 Enabling Alarm-in and Alarm-out Ports | 61 |
| 9.5.1.2 Alarm-out Port | 62 |
| 9.5.2 Setting Exception | 62 |
| 9.5.2.1 Setting SD Card Exception | 62 |
| 9.5.2.2 Setting Network Exception | 63 |
| 9.5.3 Rule Config | 63 |
| 9.5.4 Subscribing Alarm | 65 |
| 9.5.4.1 Alarm Types | 65 |
| 9.5.4.2 Subscribing Alarm Information | 65 |
| 9.6 Storage | 66 |
| 9.6.1 Storage Spot Config | 66 |
| 9.6.2 Local Storage | 67 |
| 9.6.3 FTP | 67 |
| 9.6.4 Platform Server | 69 |
| 9.7 System | 69 |
| 9.7.1 General Parameters | 69 |
| 9.7.1.1 General | 69 |
| 9.7.1.2 Date | 70 |
| 9.7.2 Account | 70 |
| 9.7.2.1 User | 71 |

| | |
|---|----|
| 9.7.2.1.1 Adding User | 71 |
| 9.7.2.1.2 Resetting Password | 73 |
| 9.7.2.2 Adding User Group | 73 |
| 9.7.2.3 ONVIF User | 74 |
| 9.7.3 Manager | 75 |
| 9.7.3.1 Requirements | 75 |
| 9.7.3.2 Maintenance | 75 |
| 9.7.3.3 Import/Export | 76 |
| 9.7.3.4 Default | 76 |
| 9.7.4 Update | 77 |
| 9.8 System Information | 77 |
| 9.8.1 Version | 77 |
| 9.8.2 Log | 77 |
| 9.8.2.1 Searching for Logs | 77 |
| 9.8.2.2 Obtaining Remote Logs | 78 |
| 9.8.3 Online User | 79 |
| 9.8.4 Running Status | 79 |
| 9.8.5 Legal Info | 79 |
| 9.9 Security | 79 |
| 9.9.1 Security Status | 79 |
| 9.9.2 System Service | 80 |
| 9.9.2.1 802.1x | 80 |
| 9.9.2.2 HTTPS | 82 |
| 9.9.3 Attack Defense | 82 |
| 9.9.3.1 Firewall | 82 |
| 9.9.3.2 Account Lockout | 83 |
| 9.9.3.3 Anti-DoS Attack | 83 |
| 9.9.4 CA Certificate | 84 |
| 9.9.4.1 Installing Device Certificate | 84 |
| 9.9.4.1.1 Creating Certificate | 84 |
| 9.9.4.1.2 Applying for and Importing CA Certificate | 85 |
| 9.9.4.1.3 Installing Existing Certificate | 85 |
| 9.9.4.2 Installing Trusted CA Certificate | 86 |
| 9.9.5 A/V Encryption | 87 |
| 9.9.6 Security Warning | 88 |
| 9.9.6.1 Security Exception | 88 |
| 9.9.6.2 Illegal Login | 89 |

| | |
|---|----|
| 9.10 Maintenance Center | 89 |
| 9.10.1 One-click Diagnosis | 89 |
| 9.10.2 Advanced Maintenance | 90 |
| Appendix 1 Cybersecurity Recommendations | 93 |

1 Overview

1.1 Introduction

The camera adopts intelligent deep learning algorithm. It 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

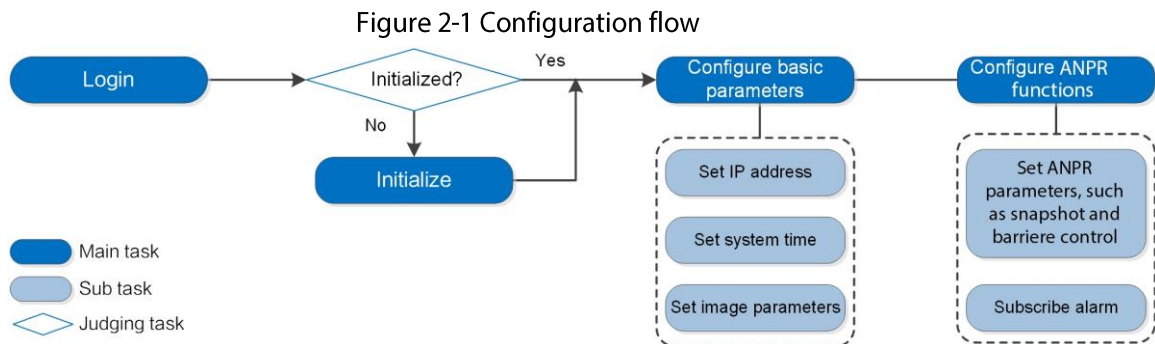


Table 2-1 Description of flow

| 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. | "9.3 Camera" |
| | Date & time | Set date and time to ensure the recording time is correct. | "9.7.1.2 Date" |
| | IP address | Change IP address according to network planning for the first use or during network adjustment. | "9.4.1 TCP/IP" |
| | Subscribe alarm | Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab. | "9.5.4 Subscribing Alarm" |
| ANPR | ANPR parameters | Configure parameters for various ANPR functions, such as taking snapshots of vehicles. | "9.2 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. |

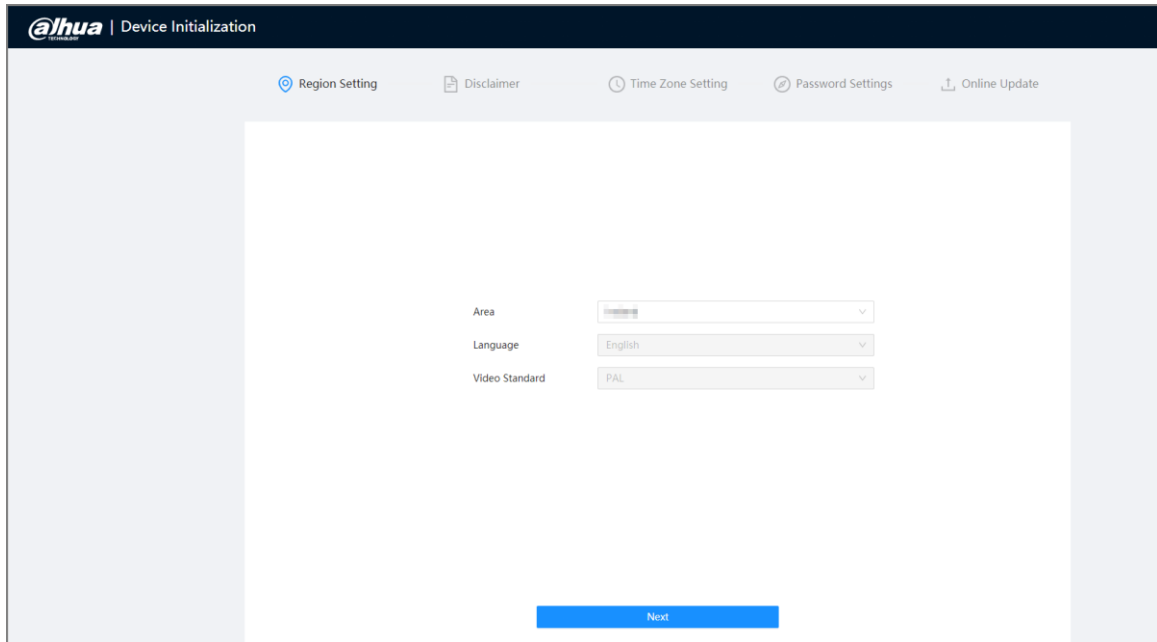


- The latest versions of Google Chrome and Microsoft browsers are supported. Most functions are available without a plug-in. A few functions require downloading a plug-in, but they still work with Google Chrome.
- Internet Explorer (IE) is not recommended. Before using it, clean up the web3.0 plug-in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

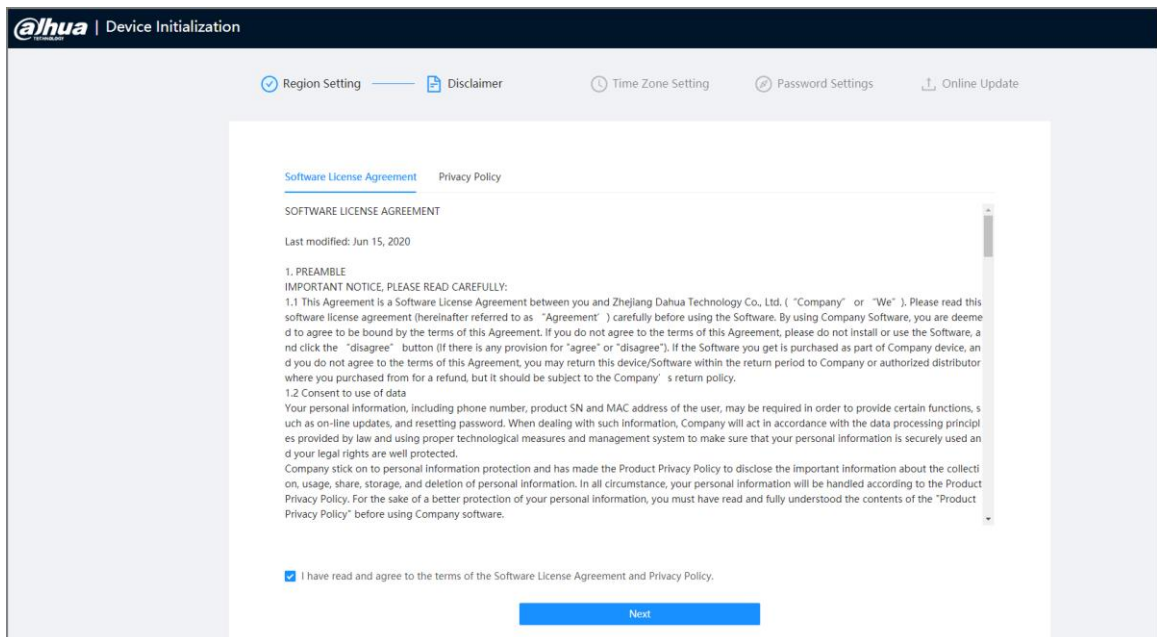
- Step 1** Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.
- Step 2** Select the area, language, and video standard, and then click **Next**.

Figure 3-1 Region setting



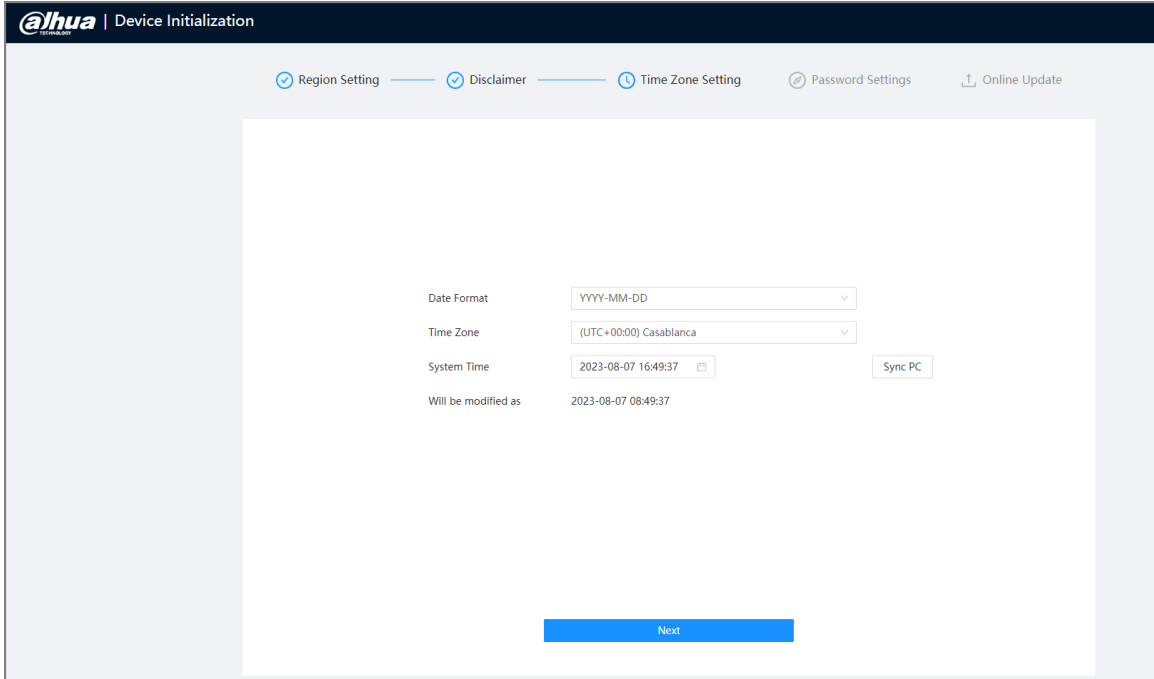
Step 3 Select the **I have read and agree to the terms of the Software License Agreement and Privacy Policy** checkbox, and then click **Next**.

Figure 3-2 Disclaimer



Step 4 Configure the time parameters, and then click **Next**.

Figure 3-3 Time zone setting



Step 5 Set the password for admin account.

Figure 3-4 Password setting

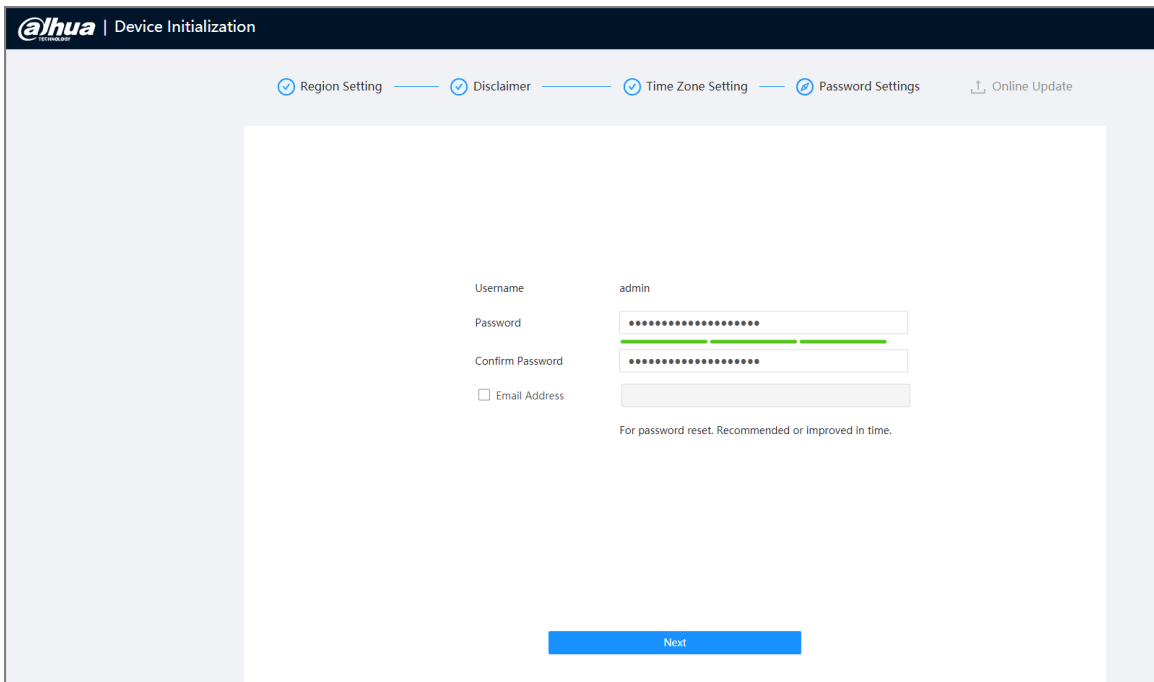


Table 3-2 Description of password configuration

| Parameter | Description |
|------------------|--|
| Username | The default username is admin. |
| Password | The password must consist of 8 to 32 non-blank characters and contain at least two 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 | |

| Parameter | Description |
|----------------|---|
| Reserved email | 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 6 Click **Next**, and then the **Online Update** page is displayed. Then, it automatically redirects to the login page. Re-enter the password for the home page.

4 Login

4.1 Device Login

This section 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 **Forget 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 "9.7.2.1.2 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 **Forget password?**, and you can reset the password through the email address that is set during the initialization.

5 Home Page


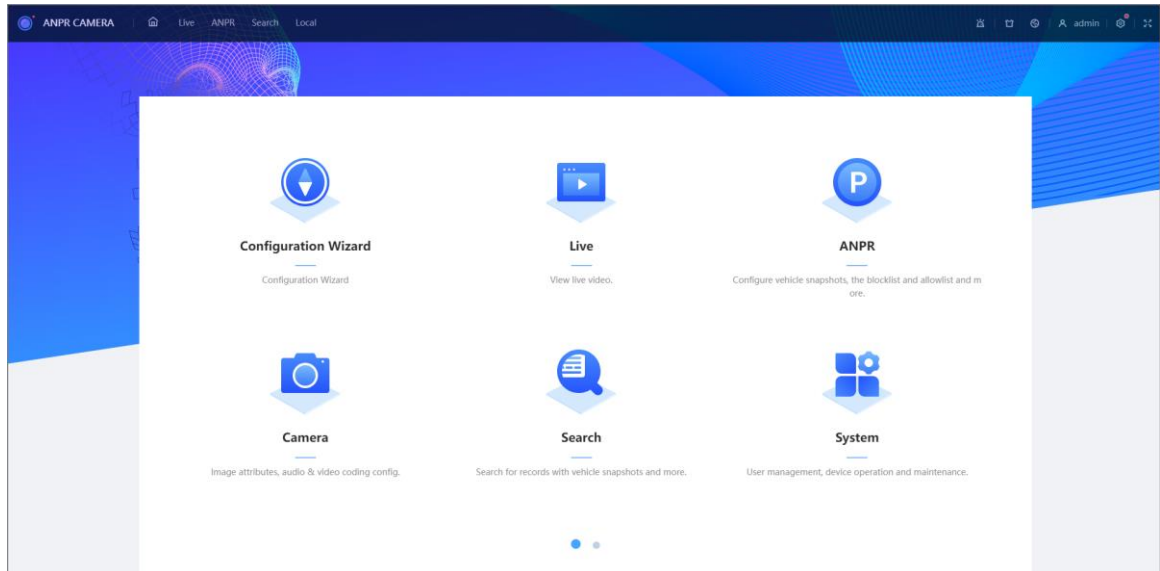







Click  at the upper-left corner of the page to display the home page.

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.
- Camera: Configure camera parameters, including image parameters, encoder parameters, and audio parameters.
- Search: Search for recordings, images, and alarm output records.
- System: Configure system parameters, including general parameters, date and time, account, safety, restoring to default settings, importing and exporting configurations, automatic maintenance and upgrade.
- Security: Check the security status of the device and configure security parameters.
- Maintenance center: Check the running status of devices and perform maintenance.
- : Subscribe 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 **Reboot**, and the camera restarts.
- Logout: Click  **admin** at the upper-right corner of the page, 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.
- 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** on the upper-right corner to go back to the home page.

Procedure

Step 1 Click **Configuration Wizard**.

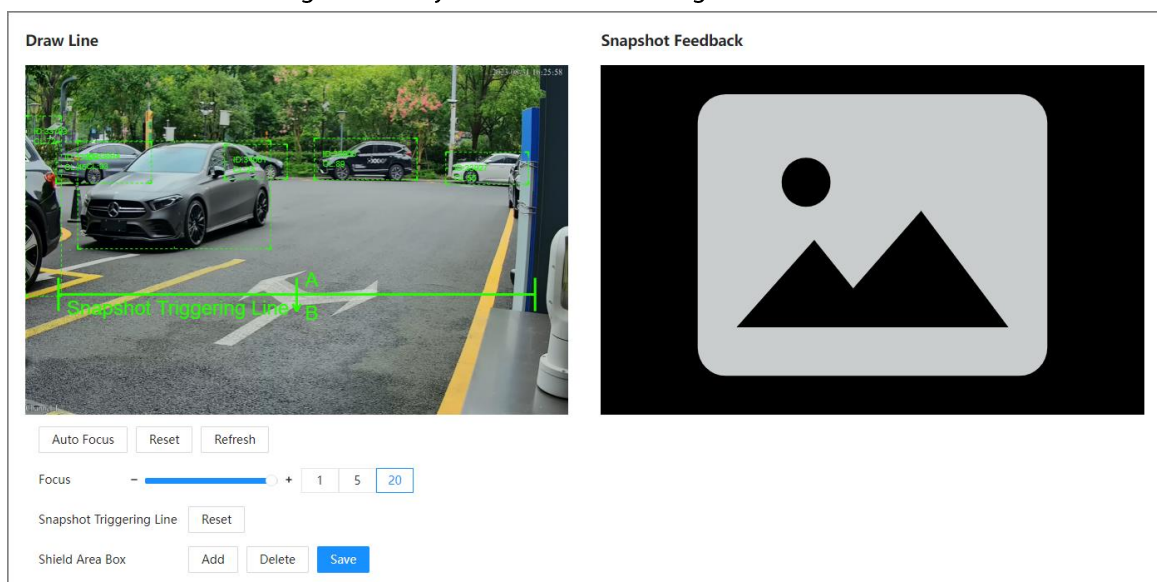
Figure 6-1 Configuration wizard

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 right side, and then draw an area for capturing vehicles that enter.
- 3) Click **Add** next to **Shield Area** to draw areas that the camera does not recognize. Click **Delete** to delete the area.

- 4) **Snapshot Triggering Line:** Drag this line to specify the location of taking the snapshots.
- 5) The **Real-time Display** window in the middle displays the plate recognition result cutout at the upper-left corner and vehicle image in real time.
- 6) 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

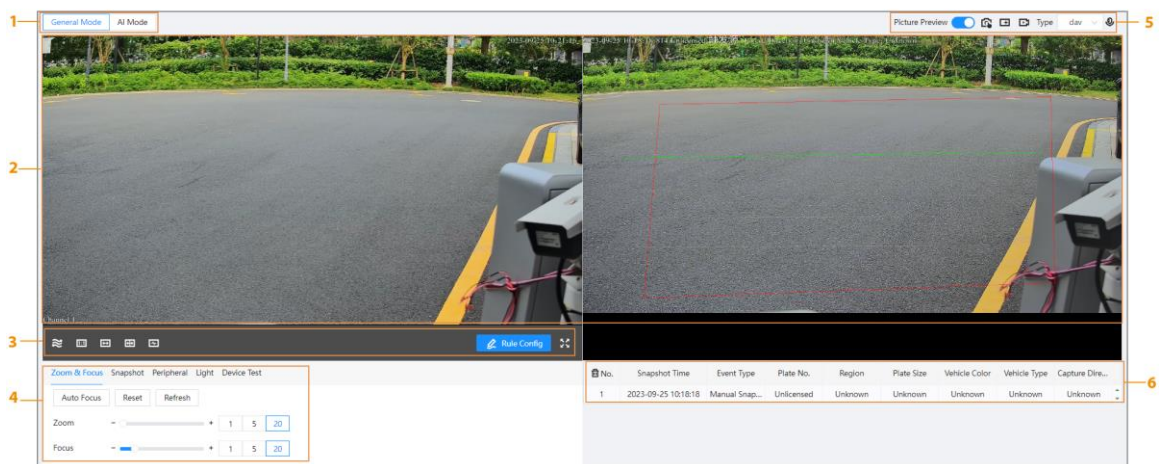









Table 7-1 Function description

| No. | Function | Description |
|-----|---------------------------|---|
| 1 | Display mode | The display modes include general mode and AI mode. For details, see "7.5 Display Mode". |
| 2 | Live view and snapshots | Displays real-time video and license plate snapshots. |
| 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 | Live view function bar | Functions and operations in live viewing. |
| 6 | Snapshot details | Displays the details of the vehicle that is captured. |

7.2 Video Adjustment

Table 7-2 Description of adjustment bar

| Icon | Function | Description |
|---|------------------------|---|
|  | Smoothness Adjustment | <p>Change the fluency of the video. Select one based on your network bandwidth.</p> <ul style="list-style-type: none"> • Realtime: Guarantees the real time of the video. When the network bandwidth is not enough, the video might not be smooth. • General: It is between Realtime and Fluent. • Fluent: Guarantees the fluency of the video but the video might not be real-time. |
|  | Original Size | Displays the video in its original size. |
|  | W:H | <p>Adjust the display scale, that is, the ratio between the width and the height of the live video display.</p> <ul style="list-style-type: none"> • 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 | <p>Select a video stream based on your network bandwidth.</p> <ul style="list-style-type: none"> • 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 |  <ul style="list-style-type: none"> • Drag the snapshot triggering line to specify the capture area. Only number plates in the area will be captured. • 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 **Installation and Adjustment** 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

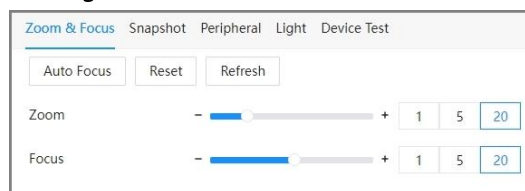




Table 7-3 Parameter description

| Parameter | Description |
|------------|---|
| Auto Focus | <p>Adjusts video clarity automatically.</p>  <p>Do not make any other operation during auto focus process.</p> |

| Parameter | Description |
|-----------|---|
| Reset | <p>Reset all focus and zoom parameters to the default settings.</p>  <p>You can reset the focus and zoom if the video is not clear or has been zoomed in or out too frequently.</p> |
| Refresh | Update the page content. |
| Zoom | <p>Zoom in or out on the video.</p> <ol style="list-style-type: none"> 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 | <p>Adjusts the optical back focal length to make the image clearer.</p> <ol style="list-style-type: none"> 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

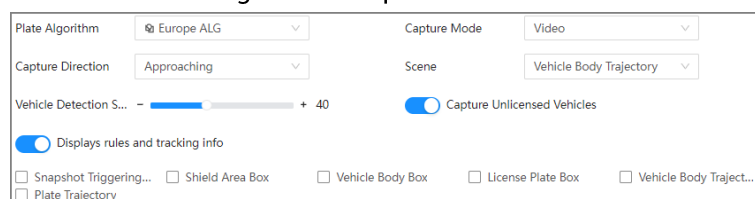


Table 7-4 Parameter description

| 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 "9.2.1 Setting Snapshot". |
| Capture Direction | <ul style="list-style-type: none"> • Positive: Only captures vehicles that approach. • Reverse: Only captures vehicles that depart. • Both Ways: Captures vehicles that approach or depart. |

| Parameter | Description |
|----------------------------------|--|
| Scene | This parameter is only available when the Capture Mode is set to Video or Mixed Mode . <ul style="list-style-type: none"> • Vehicle Body Trajectory: Applicable to scenes with large-sized vehicles. • Plate Trajectory: Applicable to scenes with small-sized vehicles. • Self-adaptive: The camera will automatically adapt to the scene. |
| Vehicle Detection Sensitivity | The higher the value, the easier vehicles will be detected. |
| Capture Unlicensed Vehicles | After it is enabled, the camera will take snapshots of vehicles with no license plates. |
| Displays rules and tracking info | Click <input type="checkbox"/> 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 Parameter description

| Parameter | Description |
|------------|--|
| LED Screen | Set the working mode for the screen. <ul style="list-style-type: none"> • 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. |

| Parameter | Description |
|------------------------|--|
| Barrier Opening Method | <p>Triggers alarm through different modes, and remotely controls the barrier opening and close.</p> <ul style="list-style-type: none"> • 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. <p> You can set barrier opening control to Allowlist and Command (Platform) at the same time.</p> |

7.3.4 Light

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

Figure 7-5 Light

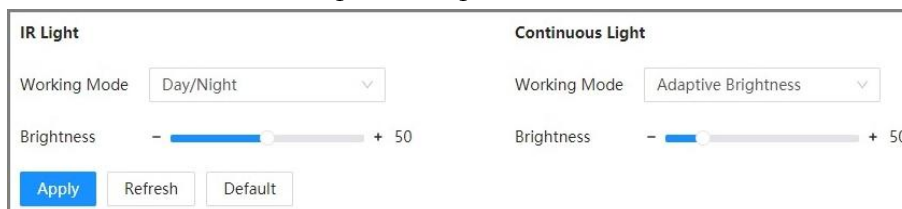


Table 7-6 Parameter description

| Parameter | Description |
|----------------------|--|
| IR Light/White Light | <ul style="list-style-type: none"> • Working Mode: Select a working mode for the light. If you select By Time, you need to configure the time schedule. For details, see "9.5.1.1 Enabling Alarm-in and Alarm-out Ports". • Brightness: The higher the value, the brighter the light. |
| Continuous Light | |

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

| | | |
|------------------------|-------------------------------------|--|
| Test Barrier Openin... | <input type="button" value="Open"/> | <input type="button" value="Close"/> |
| Test Capture | <input type="button" value="Test"/> | <input type="text" value="AB12345"/> <input type="text" value="Positive"/> |
| Test Screen Display | <input type="button" value="Test"/> | <input type="text" value="Welcome"/> |
| Test Voice Broadcast | <input type="button" value="Test"/> | <input type="text" value="Welcome"/> |

Table 7-7 Parameter description

| Parameter | Description |
|----------------------|--|
| Test Barrier Opening | 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. |

7.4 Live View Function Bar

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

Table 7-8 Function description

| Icon | Description |
|------|--|
| | Enable this function to preview the snapshots the camera takes or the ones you manually take. When a snapshot is taken, it will be displayed in the window on the right. |
| | Click this icon 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 this button to start recording. Click again to save the recording to your local computer. |
| | Select the format of the recording. |
| | Click this icon, and then you can talk to the people near the camera. Click it again to stop talking. |

7.5 Display Mode

There are 2 modes available, **General Mode** and **AI Mode**. General mode is typically used for daily observation and installation assistance, while AI mode is applicable for projection screen display, normally used in the exhibition hall.

The 2 modes have approximately the same functions, but they focus on slightly different

information. For example, there are frequently used functions available in **General Mode**, but not in **AI Mode**, such as adjusting the zoom and focus and parameters related to snapshots. As for snapshots, the 2 modes display different information. For details, see the following figures.

Figure 7-7 General mode

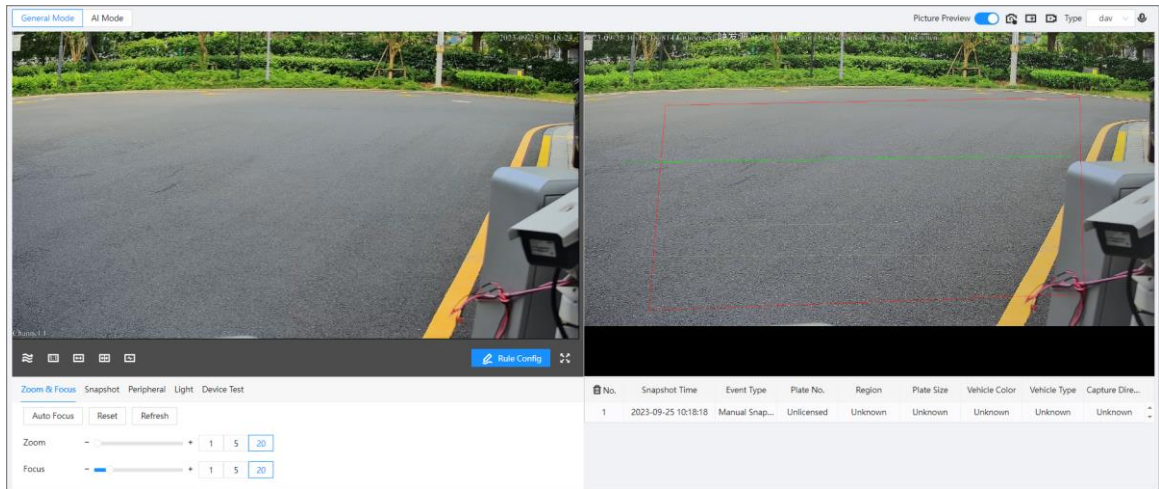
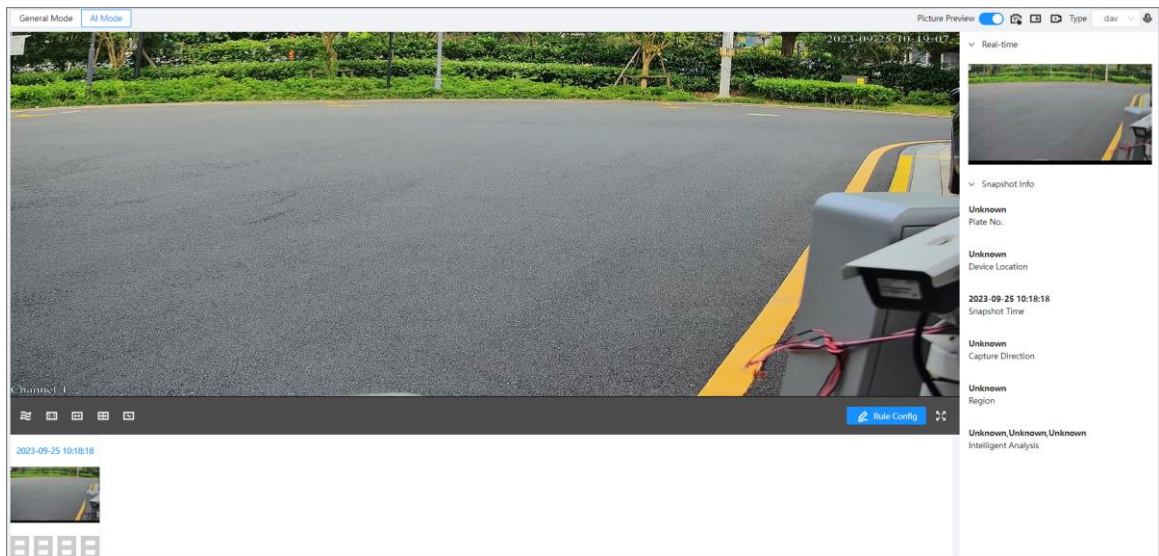


Figure 7-8 AI mode



8 Search

Use this function to play local videos, and search for snapshots, logs on snapshots, and alarm output logs.

8.1 Picture Query

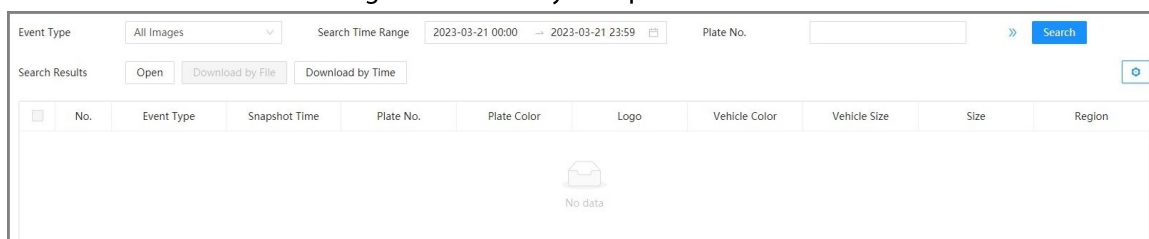
8.1.1 Memory Card Image

You can search for snapshots stored on the SD card.

Procedure

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

Figure 8-1 Memory card picture



| No. | Event Type | Snapshot Time | Plate No. | Plate Color | Logo | Vehicle Color | Vehicle Size | Size | Region |
|---------|------------|---------------|-----------|-------------|------|---------------|--------------|------|--------|
| No data | | | | | | | | | |

Step 2 Configure the search conditions.

- **Event Type:** Select an event type if you only want to search for snapshots related to that type.
- **Search Time Range:** The camera will only search for snapshots taken within this range.
- **Plate No.:** This is not a required option. If you enter a plate number, the camera will only search for snapshots related to this plate number.

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

Related Operations

- View a snapshot: Select a snapshot on the list, and then click **Open**.
- Download snapshots by file: Select one or more snapshots, and then click **Download by File** to download them to the defined path.
- Download snapshots by time: All snapshots searched for will be downloaded to the defined path.

8.1.2 Local Image

Use this function to verify if the watermarks on the snapshots stored on your computer are tampered.

Procedure

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

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**.

8.2 Playing Recordings

8.2.1 Record

You can play videos that are stored on your computer.

Procedure


Step 1 Select **Search > 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.

8.2.2 Watermark

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

Prerequisites

Go to  > **Camera > Encode > Video Stream**, enable **Watermark**, and then set the corresponding **Watermark String**. The default character is DigitalCCTV.

Procedure

Step 1 Select **Search > 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**.

8.3 Snapshot Records

Search for the snapshot records within the defined period. The camera can store up to 10,000 records when no memory card is installed.

Procedure

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

Step 2 Configure the search conditions.

- **Search Time Range:** The camera will only search for records taken within this range.
- **Plate No.:** This is not a required option. If you enter a plate number, the camera will only search for records related to this plate number.

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

8.4 Alarm-out Port

Set the search conditions to search alarm output.


Procedure

- Step 1 Select **Search > 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.

9 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.

9.1 Local

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

Prerequisites



To use the functions on this page, you must install the plugin first. Configure any parameter, and then a prompt will be displayed on the bottom of the page. Follow the instructions to install the plugin. If you do not install the plugin, images and videos will be stored to the default path set by your browser.

Procedure

Step 1 Select  > **Local**.

Step 2 Configure the parameters.

Table 9-1 Parameter description

| Parameter | Description | |
|---------------------------------|---|--|
| Protocol | You can select the network transmission protocol as needed, and the options are TCP Port , UDP Port and Multicast .  Before selecting Multicast , make sure that you have set the Multicast parameters. For details, see "9.4.5 Multicast". | |
| Picture and Storage Path Naming | You can reset the storage path by referring to the naming parameters. Click Help for more details. |  Admin in the path refers to the account being used. |
| Live Record | The recorded video of live page. The default path is C:\Users\admin\WebDownload\LiveRecord. | |
| Live Snapshot | The snapshot of live page. The default path is C:\Users\admin\WebDownload\LiveSnapshot. | |

Step 3 Click **Apply**.

9.2 ANPR

You can set intelligent parameters of the camera.

9.2.1 Setting Snapshot


You can set snapshot rule of the camera.





Procedure

Step 1 Select  > **ANPR** > **Snapshot**.

Step 2 Configure the parameters.

Table 9-2 Parameter description

| Type | Parameter | Description |
|---|--|--|
| General Parameters | Capture Mode | <ul style="list-style-type: none"> • Loop: Snapshots will be taken when targets enter a loop. • Video: Snapshots will be taken when video analyzes the targets. • Mix Mode: Combine both loop and video for taking the snapshots. |
| | Capture Direction | <ul style="list-style-type: none"> • Positive: Only captures vehicles that approach. • Reverse: 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 . | Scene | <ul style="list-style-type: none"> • Vehicle Body Trajectory: Applicable to scenes with large-sized vehicles. • Plate Trajectory: Applicable to scenes with small-sized vehicles. • Self-adaptive: The camera will automatically adapt to the scene. |
| | Unlicensed Vehicle Snapshot | Click to enable the capture towards unlicensed motor vehicles. |
| | Frames to Output Licensed Vehicle Snapshot | Configure the frame number of capturing licensed vehicle. 1 (default) means to capture when detecting one frame of licensed vehicle passing detection area. |
| | Frames to Output Unlicensed Vehicle Snapshot | Configure the frame number of capturing unlicensed vehicle. 10 (default) means to capture when detecting 10 frames of unlicensed vehicle passing detection area. |

| Type | Parameter | Description |
|---|-----------------------|---|
| 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 | Set a time period, during which a vehicle enters the first loop and triggers the second, the camera only takes snapshots for the first trigger.  Applicable for double loops. |
| | Max Vehicle Pass Time | Set a time period, during which a vehicle enters the first loop and triggers the second, the camera only takes snapshots for the first trigger.  Applicable for double loops. |

Step 3 Click **Apply**.

9.2.2 Configuring AI Setting

9.2.2.1 Intelligent Analysis

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

Procedure

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

Step 2 Configure the parameters.

Table 9-3 Parameter description

| Parameter | Description |
|-------------------------------|---|
| Detection Type | Select the type of target to be detected. Motor vehicles are selected by default. |
| Vehicle Detection Sensitivity | Set the sensitivity of vehicle detection. The higher the value, the easier targets will be detected. |
| AI Attribute Settings | Select parameters such as type, logo and color that can be recognized by the camera. |
| Advanced | Configure advanced vehicle recognition function through algorithm. Click to view the advanced algorithm formula. |

Step 3 Click **Apply**.

9.2.2.2 Smart Detection

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

Procedure


Step 1 Select **Setting > ANPR > AI Setting > Smart Detection**.

Figure 9-1 Smart detection

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

Table 9-4 Parameter description

| Parameter | Description |
|----------------|--|
| Alarm-out Port | Click to enable alarm-out ports so that the camera sends alarm signals to the alarm channels you select when an alarm is triggered. |
| Alarm Channel | Select one or more alarm channels to send alarm signals to. |

| Parameter | Description |
|--------------------|--|
| Post-alarm | The camera will keep sending alarms signals for the defined period after the alarm ends. |
| Send Email | Click <input type="checkbox"/> 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 "9.4.7 Email". |
| Select Image | Select the type of image the camera will send to the email address. If you want to use this function, you must enable the Send Email function. <ul style="list-style-type: none"> • Original Image: The complete image taken by the camera. • Plate Cutout: A cutout image of the number plate. |
| Traffic Standstill | Click <input type="checkbox"/> to enable the function. 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. |

Step 3 Click **Apply**.

9.2.3 Image Config

Set the overlapping OSD (On-screen Display) information on video and image.

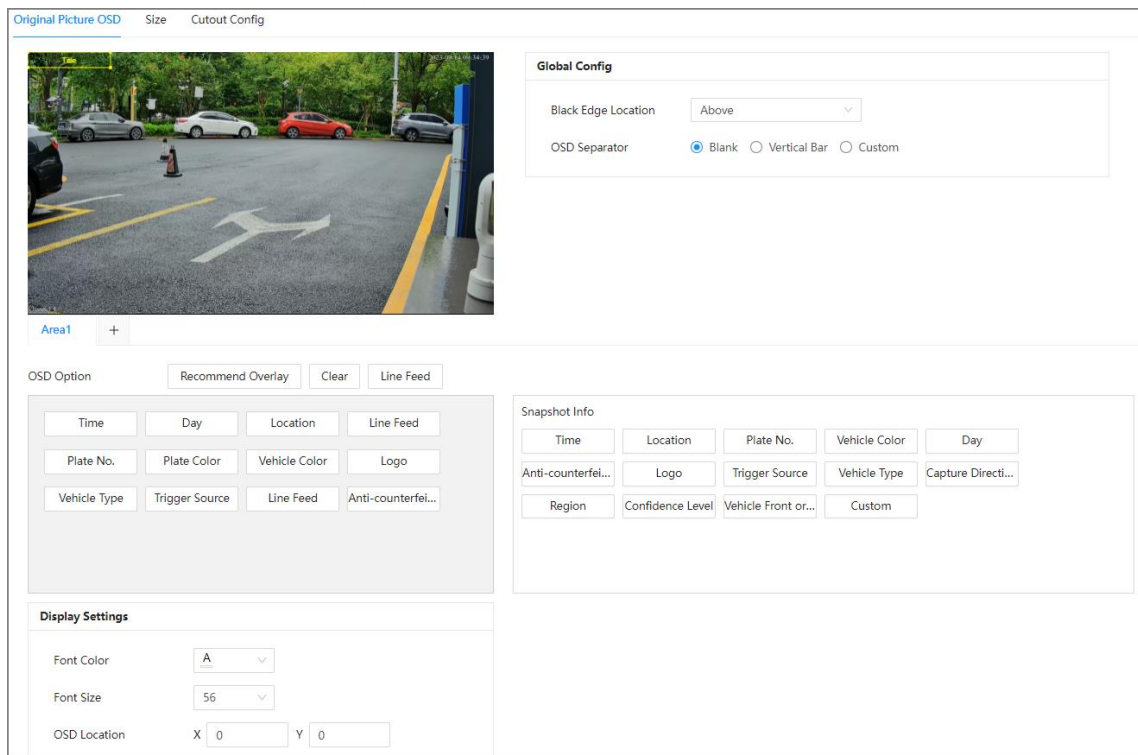
9.2.3.1 Original Picture OSD

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

Procedure

Step 1 Select  > **ANPR** > **Image Config** > **Original Picture OSD**.

Figure 9-2 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 "2023-02-22|A12345".

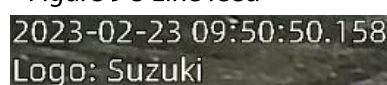
Step 4 Configure the OSD information to be displayed.

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



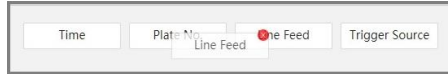
- Click **Recommend Overlay** and then the camera will automatically add various types of information.
- To delete any type of information, hover your mouse over it, and then click . Or you can click **Clear** to delete all the information that have been added.
- **Line Feed** is used to separate the information into different lines. See the example below for reference.

Figure 9-3 Line feed



2) Drag to adjust the order of information.

Figure 9-4 Adjust the order



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

Table 9-5 Parameter description

| Parameter | Description |
|--------------------|--|
| With ms | Select whether to display millisecond. This parameter is only available for Time . |
| Prefix | The information to be displayed before the type of information you are configuring. For example, a prefix "Time of trigger:" for Time can be "Time of trigger: 2023-02-23 09:58:41". |
| Suffix | The information to be displayed before the type of information you are configuring. For example, a prefix "Time of trigger:" for Time can be "Time of trigger: 2023-02-23 09:58:41". |
| Contents | Enter the fixed content that will be displayed the same on each snapshot. This parameter is only available for Location and Custom . |
| Delimiter Quantity | Select the number of separators to separate the information you are configuring with other types. For example, select the quantity to 5 when the OSD separator is set to Blank : 2023-02-23 09:35:06.840 AB12345 Vehicle |

Step 5 Configure the font color and size.

Step 6 Adjust the position where you want to display 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**.

9.2.3.2 Size

Configure the quality of snapshots.

Procedure

Step 1 Select  > **ANPR** > **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 better quality the snapshots will be.

Step 3 Click **Apply**.

9.2.3.3 Cutout

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

Procedure

- Step 1 Select  > **ANPR** > **Image Config** > **Cutout Config**.
- Step 2 Configure the parameters.
- **Plate No.** and **Vehicle Body Cutout**: The camera will cut out pictures of the plate numbers and bodies of vehicles and save them to the storage path. These 2 options can be selected at the same time.
 - **Motor Vehicle**: Enable this function and the camera will add a picture of the plate number of the vehicle to the snapshot. Select the position and size of the plate number on the snapshot.
- Step 3 Click **Apply**.

9.2.4 Setting Blocklist and Allowlist for Vehicles

9.2.4.1 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 Select  > **ANPR** > **Vehicle Blocklist/Allowlist** > **Allowlist**.
- Step 2 Add vehicles.
- Add them one by one.
 1. Click **Add**.
 2. Configure the information of the vehicle, and then click **OK**.



Table 9-6 Parameter description

| Parameter | Description |
|------------|--|
| Plate No. | (Required) Enter the plate number of the vehicle. |
| Owner Name | (Optional) Enter the name of owner of the vehicle. |
| Card | (Optional) Enter the parking card number. |
| Start Time | Configure a period for this vehicle to pass the barrier. |
| End Time | <ul style="list-style-type: none"> • 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. |
| 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

- Import information of vehicles on the allowlist: Click **Import**, and then upload a file of vehicle information.
- Export information of vehicles on the allowlist: Click **Export**, and then select to enable or disable encryption.
- Edit the information of a vehicle: Click  of a vehicle to edit its information.
- Delete vehicles one by one: Click  of a vehicle to delete it from the allowlist. If barrier control by allowlist is enabled, this vehicle will not be able to pass.
- Delete 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.

9.2.4.2 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 Select  > **ANPR** > **Vehicle Blocklist/Allowlist** > **Fuzzy Matching**.
- Step 2 Click to enable the function.
- Step 3 Configure the parameters.

Table 9-7 Parameter description

| Parameter | Description |
|--|---|
| The snapshot is missing the first or last character of the plate | You can enable one or both of these 2 options. |
| The snapshot has 1 character added to either end of the plate | |
| 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. |
| Number of characters allowed to be misread | 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**.

9.2.4.3 Blocklist

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

Select **Setting > ANPR > Vehicle Blocklist/Allowlist > Blocklist**. The configuration procedures are similar to those of allowlist. For details, see "9.2.4.1 Allowlist".

9.2.5 Configuring Barrier Control


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

Procedure

Step 1 Select  > **ANPR > Barrier Control**.

Step 2 Configure the parameters.

Table 9-8 Parameter description

| Parameter | Description |
|-------------------------------|--|
| Scheduled Barrier Always Open | Select it, and enable the function of barrier always open. Configure the period of barrier always open. The barrier will not close during the defined period. For details, see "9.5.1.1 Enabling Alarm-in and Alarm-out Ports". |
| Barrier Control Mode | <p>Triggers alarm through different modes, and remotely controls the barrier opening and close.</p> <ul style="list-style-type: none"> • 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. If you only enable Command (Platform), you can specify the control mode if the platform is offline. <p> You can set barrier opening control to Allowlist and Command (Platform) at the same time.</p> |
| Barrier Opening | <ul style="list-style-type: none"> • Alarm Channel: Alarm linkage output port. Select the corresponding one according to the field connection. • Duration: The duration that the barrier opening or closing signal lasts. • Vehicle Queuing Mode: When enabled, the system will identify a vehicle queuing before an authorized vehicle and sends alarm. You can enter the duration for alarm output, with a scale from 1 to 10 seconds. |
| Barrier Closing | |

Step 3 Click **Apply**.

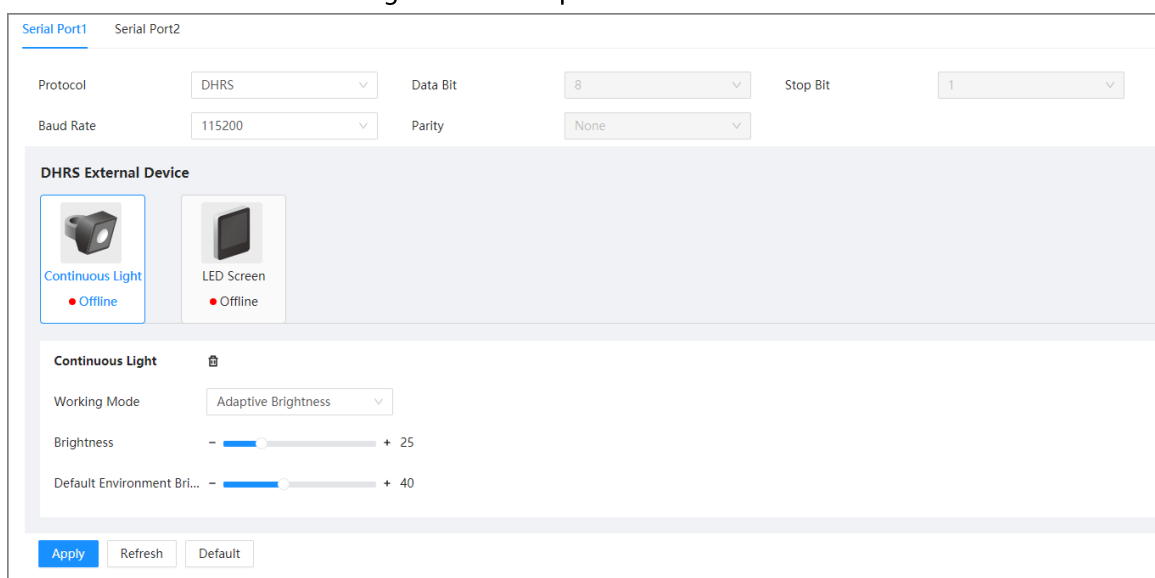
9.2.6 Configuring RS-485 Settings

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

Procedure

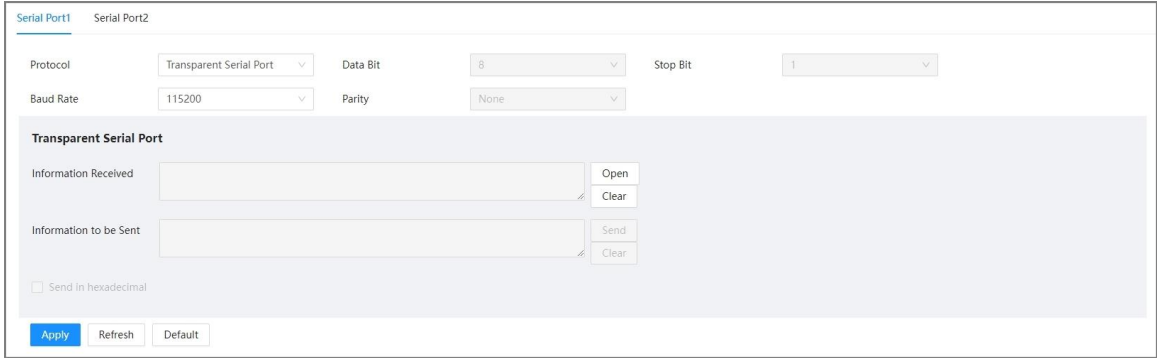
- Step 1 Select > **ANPR** > **RS-485 Settings**.
- Step 2 Configure the parameters.
The camera supports multiple protocols.
- DHRS

Figure 9-5 DHRS parameters



- ◇ **Working Mode:** Select a working mode for the light. If you select **By Time**, you need to configure the time schedule. For details, see "9.5.1.1 Enabling Alarm-in and Alarm-out Ports".
 - ◇ **Brightness:** The higher the value, the brighter the video.
 - ◇ **Default Environment Brightness:** Set a threshold for the automatic switch of continuous light. You can drag the slider to adjust the value. If the current environment brightness is lower than the threshold, the continuous light is on. Otherwise, the continuous light is off.
- RS-485 Transparent Transmission
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 9-6 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 two ports, serial port push protocol is only available for serial port 2.

Figure 9-7 Push data through serial port

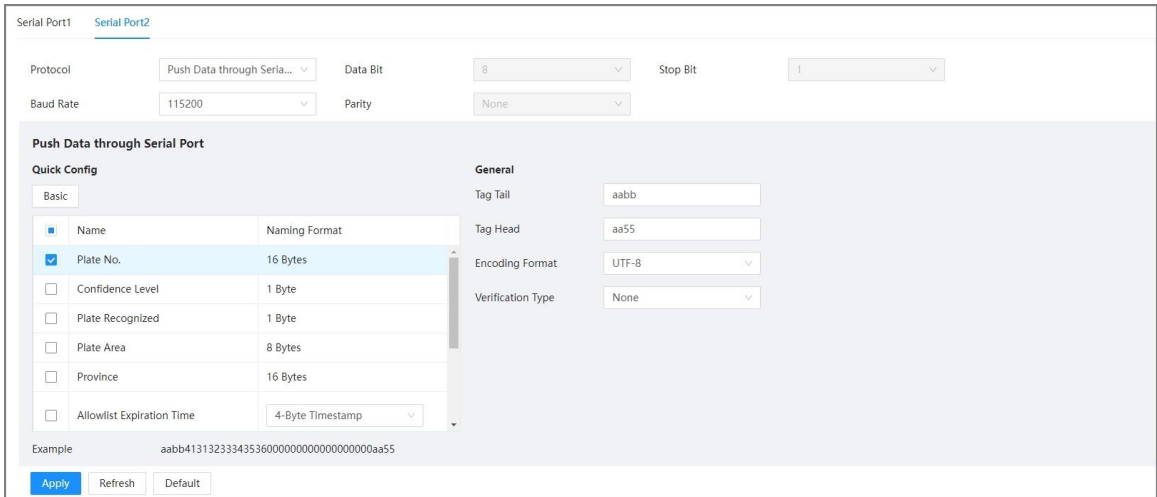


Table 9-9 Parameter description

| 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. |

| Parameter | | Description |
|----------------|-------------------|---|
| | Move Up/Down | Click all and then hold one item to move it up or down. |
| General Config | 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 Space , SUM Check and BCC Check . |

Step 3 Click **Apply**.

9.2.7 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 Select  > **ANPR** > **LED Screen**.

Figure 9-8 LED screen

Working Mode (Control settings will also be applied to Voice Broadcast function)

Standalone Mode
 Partially Managed Mode (Platform)
 Managed Mode (Platform)

Screen Control

Normal | **Vehicle Passing**

| No. | Type | Contents | Text Color | Text Effect | Effect |
|-----|-------------|----------|------------|---------------|-------------|
| 1 | Plate No. | | Red | Self-adaptive | Scroll Left |
| 2 | User Type | | Red | Self-adaptive | Scroll Left |
| 3 | Date | | Red | Self-adaptive | Scroll Left |
| 4 | System Time | | Red | Self-adaptive | Scroll Left |

Full Screen

Scrolling Speed: 4

Passing Info Appears O...: 30

Brightness Adjustment: Auto

Augment Brightness: - [slider] + 5

Self Check: Never

Step 2 Configure the parameters.

Table 9-10 Parameter description

| Parameter | | Description |
|----------------|------------------------------------|---|
| Working Mode | | Set the working mode for the screen. <ul style="list-style-type: none"> • 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. |
| Screen Control | | Set the color and action of display information when vehicles pass under 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 and Manual are available. <ul style="list-style-type: none"> • Auto: The display brightness will be automatically adjusted based on the current lighting conditions. • Manual: The display brightness will be manually adjusted. |
| | Augment Brightness | You can drag the slider for increased brightness. The higher the value, the brighter the screen. |
| | Intensity | You can manually drag the slider to fine-tune the brightness level. The higher the value, the brighter the screen. |
| | 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**.

9.2.8 Configuring Broadcast

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

9.2.8.1 Event Broadcast

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

Procedure

Step 1 Select > **ANPR** > **Audio Broadcast** > **Event Broadcast Settings**.

Step 2 Click to enable the function.

Figure 9-9 Broadcast content

| Type | Enable | Play Mode | Audio Content | Interval sec (1-20) | Duration sec (10-3600) |
|-------------------------|-------------------------------------|-----------|----------------------|---------------------|------------------------|
| Intrusion | <input checked="" type="checkbox"/> | Text | Invade | 2 | 60 |
| Loitering Detection | <input checked="" type="checkbox"/> | Text | Loitering | 2 | 60 |
| Barrier Opening Warning | <input checked="" type="checkbox"/> | Text | Please Leave Quickly | 2 | 60 |

Notes on special characters: "[plate]" means insert the real plate number. ";" means the audio will pause for 0.5 s.

Buttons: Apply, Refresh, Default

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 more details, see "9.2.8.4 Audio File".

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

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

Step 6 Click **Apply**.

9.2.8.2 Passing Vehicles

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



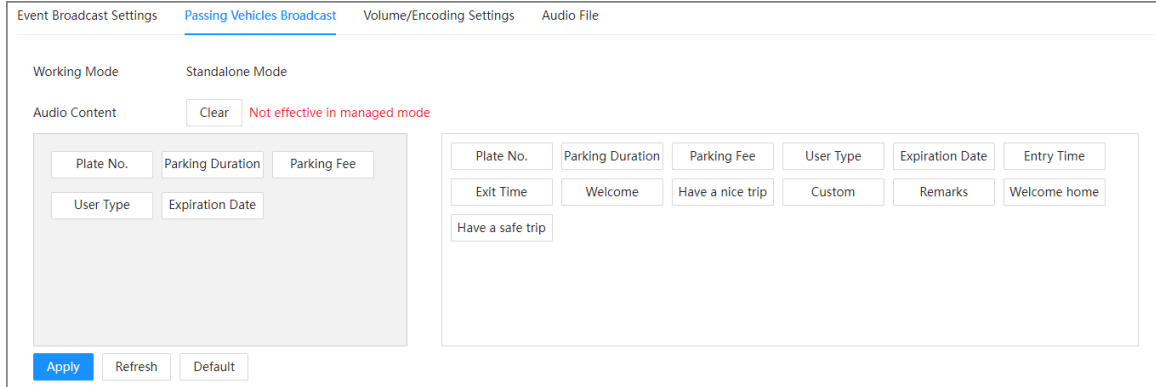
Only certain devices support this function.

Procedure

Step 1 Select > **ANPR** > **Audio Broadcast** > **Passing Vehicles Broadcast**.

Step 2 Enable one or more options.

Figure 9-10 Broadcast content



Step 3 Configure the content to be broadcasted.

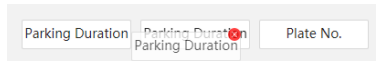
- 1) Click an item on the right to add it to the content.



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 9-11 Adjust the order



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

Step 4 Click **Apply**.

9.2.8.3 Volume/Encoding

Configure the volume for voice broadcast.



This function is only available for select models.

Procedure

Step 1 Select > **ANPR** > **Audio Broadcast** > **Volume/Encoding Settings**.

Step 2 Configure the parameters.

Table 9-11 Parameter description


| 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 3 Click **Apply**.

9.2.8.4 Audio File

Upload audio files for broadcast content.

Procedure

Step 1 Select  > **ANPR > Audio Broadcast > Audio File.**




Step 2 Click **Add Audio File** to upload files.



Requirements:

Maximum file size limit: 1024 k; Supported audio format: WAV; Audio channel: Mono; Bit depth: 16 bit; Sample rate: 8KHZ/16KHZ/32KHZ/48KHZ/64KHZ

Related Operations

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

9.2.9 Setting Device Test

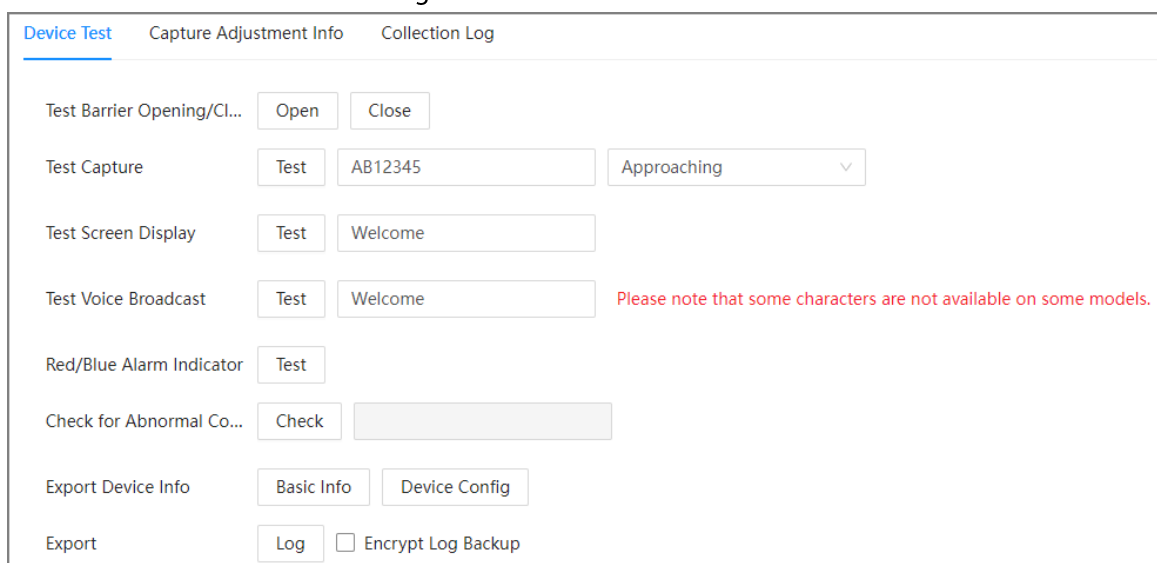
9.2.9.1 Device Test

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 Select  > **ANPR > Device Test > Device Test.**

Figure 9-12 Device test



Step 2 Test if different functions are working normally.



Table 9-12 Parameter description

| 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. |
| 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. |

9.2.9.2 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 Select  > **ANPR** > **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 you selected. If they do not meet your requirements, you can adjust them by repeating the steps above.

9.2.9.3 Collection Log

The camera supports collecting operation logs to track errors.

Procedure

- Step 1 Select  > **ANPR** > **Device Test** > **Collection Log**.
- Step 2 Turn on the toggle next to **Enable** to enable the function.

Figure 9-13 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**.

9.3 Camera

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



The parameters might vary with different models.

9.3.1 Setting Image Parameters

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

9.3.1.1 General Parameters

This section provides guidance on configuring parameters such as image brightness, contrast, saturation, and hue.



Procedure


Step 1 Select > **Camera** > **Image** > **General**.

Step 2 Configure the parameters.

Table 9-13 Parameter description

| Parameter | Description |
|------------|--|
| Brightness | <p>Adjust the overall image brightness. Change the value when the image is too bright or too dark.</p> <p>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.</p> <p>It is 50 by default. The higher the value is, the brighter the image becomes.</p> |

| Parameter | Description |
|--------------------------------|--|
| Contrast | <p>Change the value when the image brightness is proper but contrast is not enough.</p> <ul style="list-style-type: none"> 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. <p>It is 50 by default. The higher the value is, the more obvious the contrast between the bright area and dark area will become.</p> |
| Saturation | <p>Adjust the color vividness, and will not influence the image overall brightness.</p> <ul style="list-style-type: none"> 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. <p>It is 50 by default. The higher the value is, the more flamboyant the image becomes.</p> |
| Gamma | <p>Adjust the image brightness level. The higher the value is, the brighter and blurrier the image becomes.</p> |
| Fill Light | <p>Select IR or white light mode. This option might not be configurable because certain models only provide 1 mode.</p> |
| Day/Night | <ul style="list-style-type: none"> 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 "9.5.1.1 Enabling Alarm-in and Alarm-out Ports". <p> This parameter is only configurable when Fill Light is set to IR Mode.</p> |
| Default Environment Brightness | <p>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.</p> |
| IR Light | <ul style="list-style-type: none"> Always Off: Set the IR light to always on. Always On: Set the IR light to always off. Day/Night: Automatically turn on or off the IR light according to the configured Day/Night mode. <p> Only applicable when Fill Light is set to IR Mode.</p> |

| Parameter | Description |
|------------------|---|
| White Light | <ul style="list-style-type: none"> • Always Off: Set the white light to always on. • Always On: Set the white light to always off. • 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 how to configure the periods, see "9.5.1.1 Enabling Alarm-in and Alarm-out Ports".  <p>Only applicable when Fill Light is set to White Light.</p> |
| Light Brightness | Set the illumination intensity when there are no vehicles passing. The higher the value is, the brighter it will be. |

Step 3 Click **Apply**.

9.3.1.2 Shutter Parameters

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




Procedure

Step 1 Select  > **Camera** > **Image** > **Shutter**.

Step 2 Configure the parameters.

Table 9-14 Parameter description

| Parameter | Description |
|-------------|---|
| 3D NR | |
| 3D NR | Select Enable to enable the function. |
| 2D NR Level | Spatial video denoising. The higher the value, the fewer the noise. |
| 3D NR Level | 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 adjust mode from Auto , and Close . |
| Mode | Select the way of adjusting exposure mode. You can select from Manual , and Auto . |

| Parameter | Description |
|---------------|---|
| 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 . |
| 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 its best status. |

Step 3 Click **Apply**.

9.3.1.3 Metering Parameters

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

Procedure

Step 1 Select  > **Camera** > **Image** > **Metering**.

Step 2 Configure the parameters.

Table 9-15 Parameter description

| Parameter | Description |
|-------------------------------|--|
| Plate Brightness Compensation | When selecting Enable , you can turn ON or OFF backlighting compensation, and frontlighting compensation according to scene requirements, and then improve the image brightness in backlighting situations. |
| Backlighting Compensation | |
| Frontlighting Compensation | |
| Metering Mode | <ul style="list-style-type: none"> • 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**.

9.3.2 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.

9.3.2.1 Video Stream


You can set the video stream information.


Procedure

Step 1 Select  > **Camera** > **Encode** > **Video Stream**.

Step 2 Configure the parameters.

Table 9-16 Parameters description

| Parameter | Description |
|------------------|---|
| Encode Mode | Currently it only supports H.264M, H.264H, H.265, and MJPEG. |
| 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 | <p>We recommend that you use VBR in constantly changing scenes, and CBR in stable scenes.</p> <ul style="list-style-type: none"> • 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. <p> Image quality can only be set in VBR mode.</p> |
| Quality | <p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>The better the quality is, but the bigger the required bandwidth will be.</p> |
| Reference Bit Rate | <p>The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.</p> |
| Max Bit Rate | <p>This parameter can be configured only when the Bit Rate Type is set to VBR.</p> <p>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.</p> |
| I Frame Interval | <p>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.</p> |
| SVC | <p>Scalable video codec (SVC) contains 3 layers providing different frame rates. The higher the layer, the greater the video quality.</p> |
| Smooth Stream | <p>It is designed for fluid viewing of live video. The higher the value, the smoother the video.</p> |
| Watermark | <p>Set the watermarks, which will be added into videos of the camera.</p> <ul style="list-style-type: none"> • 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**.


9.3.2.2 Video OSD

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

9.3.2.2.1 Configuring Channel Title

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


Procedure

- Step 1 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**.

9.3.2.2.2 Configuring Time Title

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


Procedure

- Step 1 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**.

9.3.2.2.3 AI Detection

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


Procedure

- Step 1 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**.

9.3.2.2.4 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 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.

9.3.2.2.5 Configuring Custom Title

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




Procedure

- Step 1 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**.

9.3.2.3 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.
- 
- The higher the value, the better the quality will be.
 - Click **Clear** to delete all the areas; click  to delete an area.
- Step 3 (Optional) Click **Add** to add more areas.
You can add up to 4 areas.
- Step 4 Click **Apply**.

9.4 Network

This section introduces network configuration.

9.4.1 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 9-17 Description of TCP/IP parameters

| 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: <ul style="list-style-type: none"> • 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. |
| Subnet Mask | |
| Default Gateway |  <ul style="list-style-type: none"> • IPv6 does not have subnet mask. • The default gateway must be in the same network segment with the IP address. |
| Preferred DNS | IP address of the preferred DNS. |
| Alternate DNS | IP address of the alternate DNS. |

Step 3 Click **Apply**.

9.4.2 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** > **TCP/IP**.

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 9-18 Description of port parameters

| 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. |
| UDP Port | User datagram protocol port. The value is 37778 by default. |
| HTTP Port | Hyper text transfer protocol port. The value is 80 by default. |
| RTSP Port | <ul style="list-style-type: none"> • 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. <p>URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</p> <p>Among that:</p> <ul style="list-style-type: none"> • 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). <p>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</p> <p>If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</p> |
| 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.

9.4.3 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 9-19 Parameter description

| Parameter | Description |
|-----------|---|
| Type | The name and web address of the DDNS service provider. |
| Address | CN99 DDNS web address: www.3322.org |
| 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**.

Result

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

9.4.4 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 9-20 Parameter description


| 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**.

9.4.5 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 9-21 Parameter description

| Parameter | Description |
|-------------------|--|
| Multicast Address | The multicast IP address of Main Stream/Sub Stream is 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**.

Result

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

9.4.6 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.

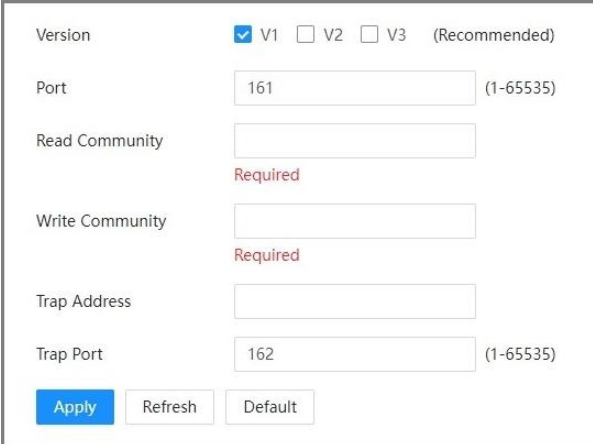
Prerequisites

- 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 9-14 SNMP (1)



The figure shows a web-based configuration form for SNMP. It includes the following fields and options:

- Version:** Radio buttons for V1 (checked), V2, and V3 (Recommended).
- Port:** Text input field containing '161' with a range '(1-65535)' to its right.
- Read Community:** Text input field with a red 'Required' label below it.
- Write Community:** Text input field with a red 'Required' label below it.
- Trap Address:** Text input field.
- Trap Port:** Text input field containing '162' with a range '(1-65535)' to its right.
- Buttons:** 'Apply' (blue), 'Refresh', and 'Default' (grey).

Figure 9-15 SNMP (2)

| | |
|--|--|
| Version | <input type="checkbox"/> V1 <input type="checkbox"/> V2 <input checked="" type="checkbox"/> V3 (Recommended) |
| Port | <input type="text" value="161"/> (1-65535) |
| Read Community | <input type="text"/> |
| Write Community | <input type="text"/> |
| Trap Address | <input type="text"/> |
| Trap Port | <input type="text" value="162"/> (1-65535) |
| * Read-Only Username | <input type="text" value="private"/> |
| Authentication Type | <input type="text" value="MD5"/> |
| Authentication Password | <input type="password"/> |
| Encryption Type | <input type="text" value="CBC-DES"/> |
| Encryption Password | <input type="password"/> |
| * Read/Write Username | <input type="text" value="public"/> |
| Authentication Type | <input type="text" value="MD5"/> |
| Authentication Password | <input type="password"/> |
| Encryption Type | <input type="text" value="CBC-DES"/> |
| Encryption Password | <input type="password"/> |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/> | |

Step 2 Select an SNMP version to enable this function.

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






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

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

Table 9-22 Description of SNMP parameters

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

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

Result

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

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



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

9.4.7 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 9-23 Parameter description


| Parameter | Description |
|-----------------|---|
| SMTP Server | SMTP server address |
| Port | The port number of the SMTP server. |
| Username | The account of SMTP server. |
| Password | The password of SMTP server. |
| Anonymous | Click <input type="checkbox"/> , 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 9-24. |
| Subject | Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click  to select title type, including Device Name , Device ID , and Event Type , and you can set maximum 2 titles. |
| Attachment | Select the checkbox to support attachment in the email. |
| Receiver | <ul style="list-style-type: none"> 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 9-24 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**.

9.4.8 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.

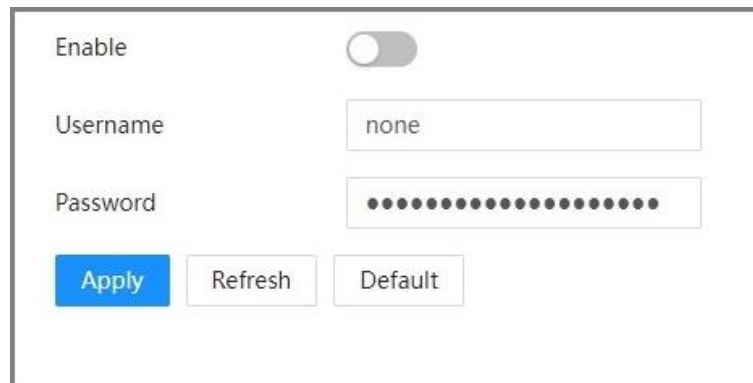
Prerequisites


- 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 9-16 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.


9.4.9 Platform Access

9.4.9.1 P2P

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

Procedure

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

Step 2 Click  to enable the function.

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

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

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

Step 6 Follow the instructions to finish the settings.

9.4.9.2 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 Click  next to **ONVIF Verification** to enable the function.
- Step 3 Click **Apply**.

9.4.9.3 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 9-17 ITSAPI

Step 3 Configure the parameters.

Table 9-25 Parameter description

| Section | Parameter | Description |
|---------------------|------------------------|--|
| Basic Configuration | Keep Alive Interval | Update interval of the connection between the server and the device. |
| | Max Keep-alive Request | Set the maximum number of heartbeats of the connection between the server and the device. When the defined number is exceeded, the device has disconnected. |
| Data Acquisition | Data Type | Select the data type to be uploaded. |
| | Uploading Info | Select the specific information to be uploaded. |
| Image Configuration | Filter Condition | Select whether to upload information of unlicensed vehicles. |
| | Upload Type | Select the type of images to be uploaded. |
| | Encoding Format | Select the license plate encoding. <ul style="list-style-type: none"> 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**.

9.4.10 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 9-26 Description of basic service parameters

| 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. |

Step 3 Click **Apply**.

9.5 Event

9.5.1 Setting Alarm

9.5.1.1 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

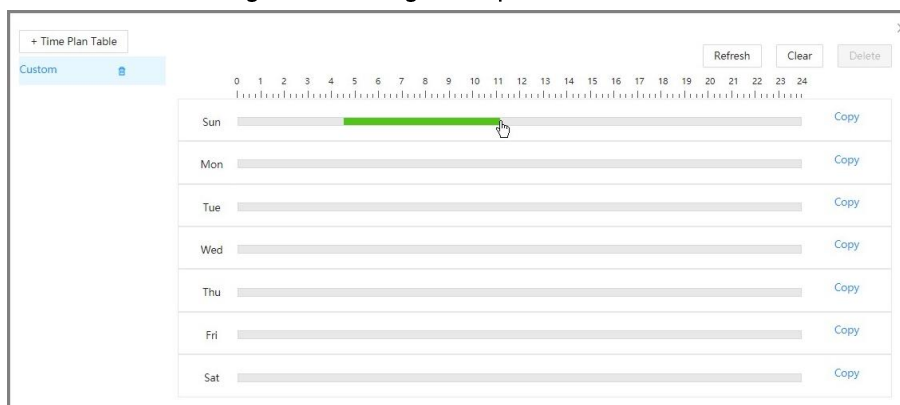
- Step 1** Select > **Event** > **Alarm** > **Alarm**.
- Step 2** Click next to **Enable** to enable alarm input for the current channel.
- Step 3** Select an alarm input channel and schedule.



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 9-18 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 9-27 Parameter description

| Parameter | Description |
|-------------|---|
| Anti-dither | Enter anti-dither time (1 s–100 s). System will only record one when there are multiple alarms during the defined time. |

| Parameter | Description |
|----------------|---|
| Sensor Type | Select relay-in type according to the connected alarm input device. <ul style="list-style-type: none"> • NO: Low level valid. • NC: High level valid. |
| Alarm-out Port | Click <input type="checkbox"/> , 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**.

9.5.1.2 Alarm-out Port

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

Procedure

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

Step 2 Select one or more alarm channels.

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

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

9.5.2 Setting Exception

Abnormality includes SD card, network, illegal access, voltage detection, and security exception.



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

9.5.2.1 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 9-28 Parameter description

| Parameter | Description |
|----------------|---|
| Alarm-out Port | Click <input type="checkbox"/> , and then select an alarm output channel. The corresponding device will be activated when alarms are triggered. |
| Alarm Channel | |

| Parameter | Description |
|------------|--|
| 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**.

9.5.2.2 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 9-29 Parameter description

| 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**.

9.5.3 Rule Config

You can configure the IVS rules for intrusion and loitering detection.

Procedure

Step 1 Select  > **Event** > **Rule Config**.

Step 2 Click **Add Rule**, then you can add up to 3 rules of either **Intrusion** or **Loitering Detection**.

Step 3 Configure the parameters.

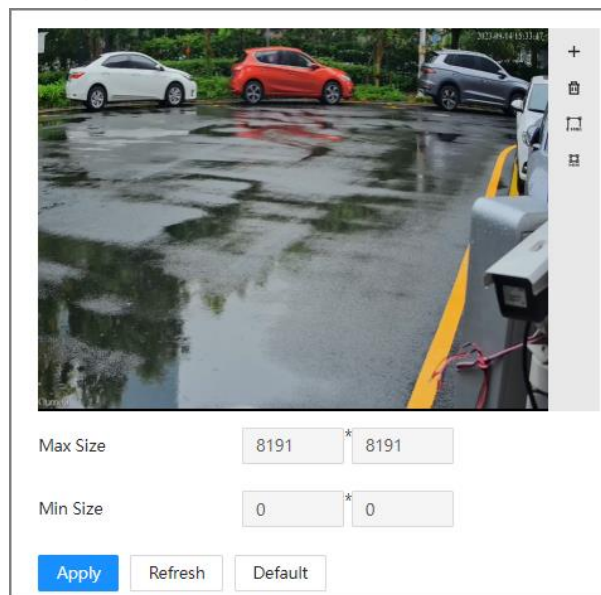
Table 9-30 Parameters

| Alarm Type | Description |
|-------------|---|
| Target | 4 detection target types are available. 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. |
| Interval | Only one 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 one alarm will be reported. |

| Alarm Type | Description |
|--------------------|---|
| 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. |
| Warning Light | Click <input type="checkbox"/> to enable the function. Once the camera detects specific events, the light flashes. |
| Duration | Enter the duration of flashing warning light, with a scale from 10 to 3,600 seconds. |
| Audio Linkage | Click <input type="checkbox"/> to enable the function. The camera will broadcast when it detects specific events. |
| Send Email | Click <input type="checkbox"/> to enable the function. The camera will send emails when it detects specific events. |
| Linkage Snapshot | Click <input type="checkbox"/> to enable the function. The camera will take snapshots when it detects specific events. |

Step 4 Configure the detection areas and targets.

Figure 9-19 Detection parameters



- 1) Click to specify the detection area. Drag the line to draw a polygon, and right click to finish. Only 1 area can be added to each detection rules.
Click to delete the detection area.
- 2) Click to set the maximum size of the target.
Click to set the minimum size of the target.



An alarm will not be triggered if the target size exceeds the max one or smaller than the min one.

9.5.4 Subscribing Alarm

9.5.4.1 Alarm Types

Table 9-31 Description of alarm types

| Alarm Type | Description | Preparation |
|--------------------|---|---|
| Disk Full | An alarm is triggered when the free space of SD card is less than the configured value. | The low SD card space function is enabled. For details, see "9.5.2.1 Setting SD Card Exception". |
| Disk Error | An alarm is triggered when there is failure or malfunction in the SD card. | SD card error detection is enabled. For details, see "9.5.2.1 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 "9.5.1.1 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 function is enabled. For details, see "9.5.2.1 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 "9.2.2.2 Smart Detection". |
| 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 "9.9.6.2 Illegal Login". |
| Security Exception | An alarm is triggered when the device detects malicious attacks. | The security exception is enabled. For details, see "9.9.6.1 Security Exception". |
| Traffic Standstill | An alarm is triggered when the device detects traffic standstill. | The traffic standstill is enabled. For details, see "9.2.2.2 Smart Detection". |
| IVS | An alarm is triggered when the device detects events like intrusion and loitering. | The IVS is enabled. For details, see "9.5.3 Rule Config". |

9.5.4.2 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 9-20 Subscribe to alarms

Step 2 Click next to **Alarm**.

Step 3 Select one or more alarm types. For details on each alarm, see "9.5.4.1 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.

9.6 Storage

This section provides guidance on setting associated information of storage, and record control.

9.6.1 Storage Spot Config

Set the locations for storing snapshots.

Procedure

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

Step 2 Select a location to store snapshots.

- **Local Storage:** Stores the snapshots on the memory card.
- **FTP:** Stores the snapshots on the FTP server.



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

Step 3 Click **Apply**.

9.6.2 Local Storage

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



Format the SD card before use.

Procedure

- Step 1 Select > **Storage** > **Local Storage**.
- Select **Overwrite** or **Stop** from **Disk Full**, meaning overwrite the records or stop storing new pictures or videos respectively when disk is full.
 - View the storage information of the card.
 - Click **Hot Swap**, and then you can pull out the SD card.
 - Click **Format**, and then you can format the SD card.
 - **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 9-21 Local configuration parameter description

| No. | Device Name |
|-----|-------------|
| | |

- Step 2 Click **Apply**.

9.6.3 FTP

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



You can set picture name, and storage path. Click **Help...** to view the naming rule.

Procedure

- Step 1 Select > **Storage** > **FTP**.

Figure 9-22 FTP

Step 2 Configure the parameters.

Table 9-32 Parameter description

| Parameter | Description |
|----------------|--|
| ANR | <p>When the network disconnects or fails, snapshots will be stored in TF card. After the network is restored, the snapshots will be uploaded from the TF card to FTP or client.</p> <p>Make sure that TF card is inserted in the camera; otherwise, the offline transfer function cannot be enabled.</p> |
| FTP Naming | <p>Set the naming rule of snapshots to be saved in FTP server. You can click Help... to view the naming rule, or click Reset to restore the default naming rule.</p> |
| Enable | <p>Enable FTP server storage.</p> |
| Protocol | <ul style="list-style-type: none"> ● SFTP (Recommended): Secure File Transfer Protocol, a network protocol allows file access, and transfer over a secure data stream. ● FTP: File Transfer Protocol, a network protocol implemented to exchange files over a TCP/IP network. Anonymous user access is also available through an FTP server. |
| Server IP | <p>The IP address of FTP server.</p> |
| Encode Mode | <p>Refers to the encode mode of Chinese characters when naming pictures. Two modes are available: UTF-8, and GB2312. After configuring Server IP, and Port, click test to check whether the FTP server works.</p> |
| Port | <p>The port number of FTP server.</p> |
| Username | <p>The username and password of FTP server.</p> |
| Password | |
| Upload Picture | <p>Select the types of pictures to be uploaded to the FTP server.</p> |

Step 3 Click **Apply**.

9.6.4 Platform Server

You can set the parameters of storing images to a platform.

Procedure

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

Step 2 Configure the parameters.

Table 9-33 Parameter description

| Parameter | Description |
|---------------|---|
| ANR | When network is disconnected or failed, you can store the picture into local storage card, and it will automatically upload to platform server after network resumes. |
| Mode | Select how the camera will connect to the platform. <ul style="list-style-type: none"> • IP: Connect to platform server through an IP address. • MAC: Connect to platform server through a MAC address. |
| Server | Configure the IP address or MAC address of the platform server. |
| Manual Upload | You can manually upload images within the specified period to the server. Select a server you want to upload images to, configure the time, and then click Upload . |

Step 3 Click **Apply**.

9.7 System

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

9.7.1 General Parameters

9.7.1.1 General

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

Procedure

Step 1 Select  > **System** > **General** > **General**.

Step 2 Configure the parameters.

Table 9-34 Parameter description

| Parameter | Description |
|-------------|--|
| Device Name | Enter the name and number of the device. |
| Device No. | |

| Parameter | Description |
|---------------------|---|
| 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**.

9.7.1.2 Date


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

Procedure

Step 1 Select  > **System** > **General** > **Date**.

Step 2 Configure the parameters.

Table 9-35 Parameter description

| 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**.

9.7.2 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 usernames or group names are not allowed. A user can only be in one group at a time, and the group users can own authorities within group authority range.
- Online users cannot edit their own authority.
- There is one admin by default which has highest authority.
- Select **Anonymous Login**, and then log in with only IP address instead of username and password. Anonymous users only have preview authorities. During anonymous login, click **Logout**, and then you can log in with other username.

9.7.2.1 User

9.7.2.1.1 Adding User

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

Procedure

Step 1 Select  > **System** > **Account** > **User**.


Step 2 Click **Add**.

Figure 9-23 Add user (system)

Figure 9-24 Add user (restricted login)

Step 3 Configure the parameters.

Table 9-36 Description of user parameters

| Parameter | Description |
|------------------|---|
| Username | User's unique identification. You cannot use existed username. |
| Password | Enter password and confirm it again. |
| Confirm Password | The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). |
| Group | The group that users belong to. Each group has different authorities. |
| Remarks | Describe the user. |
| System | Select authorities as needed.  We recommend you give fewer permissions to normal users than premium users. |
| Live | Select the live view authority for the user to be added. |

| Parameter | Description |
|------------------|---|
| Restricted Login | <p>Set the PC 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.</p> <ul style="list-style-type: none"> • IP address: You can log in to web through the PC with the set IP or one within the set IP segment. • Validity period: You can log in to web in the set validity period. • Period: You can log in to web in the set time range. |

Step 4 Click **Apply**.

The user is displayed in the username list.

Related Operations

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



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.

9.7.2.1.2 Resetting Password

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

Procedure

Step 1 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?**

9.7.2.2 Adding 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 Select  > **System** > **Account** > **Group**.

Step 2 Click **Add**.

Figure 9-25 Add group

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

Step 4 Click **Apply**.

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.

9.7.2.3 ONVIF User

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

Procedure

Step 1 Select > **System** > **Account** > **ONVIF User**.

Step 2 Click **Add**.

Figure 9-26 Add ONVIF user

Step 3 Configure the parameters.


Table 9-37 Parameter description

| Parameter | Description |
|------------------|---|
| Username | User's unique identification. You cannot use existed username. |
| Password | Enter password and confirm it again. |
| Confirm Password | The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). |
| Group Name | The group that users belong to. Each group has different authorities. |

Step 4 Click **OK**.

The user is displayed in the list.

Related Operations

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



For admin account, you can only change the password.

- Click  to delete the added user.



The admin account cannot be deleted.

9.7.3 Manager

9.7.3.1 Requirements

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 "9.7.2 Account".
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

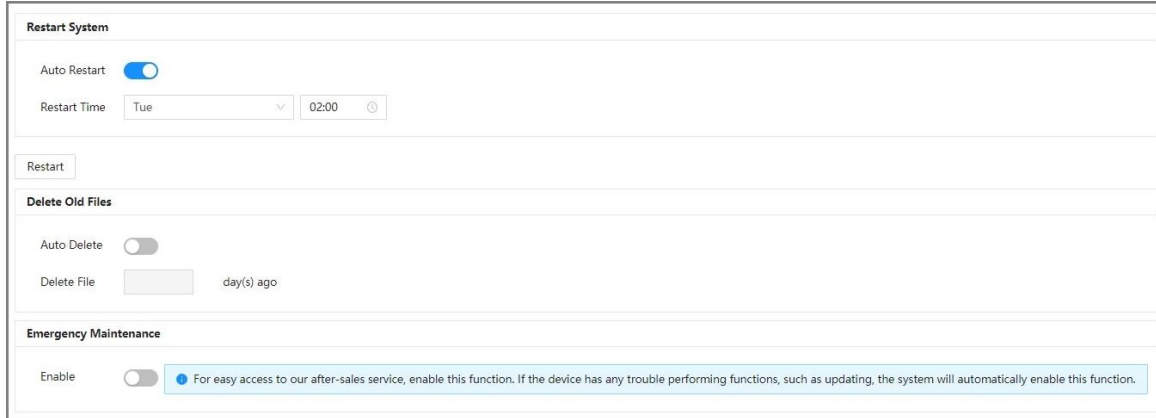
9.7.3.2 Maintenance

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 Select  > **System > Manager > Maintenance**.

Figure 9-27 Maintenance



Step 2 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 3 Click **Apply**.

9.7.3.3 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 Select > **System > Manager > Import/Export**.

Step 2 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.

9.7.3.4 Default

Restore all settings of the camera to the default status.

Select > **System > Manager > Default**.

- 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.

9.7.4 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 Select  > **System** > **Update**.

Step 2 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 manually.
 1. Click **Manual Check**, and then the camera will search for new version.
 2. If there is a new version available, follow the on-screen instructions to finish the process.
 - 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.

9.8 System Information

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

9.8.1 Version

Select  > **System Info** > **Version** to 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.

9.8.2 Log

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

9.8.2.1 Searching for Logs

Procedure

Step 1 Select  > **System Info** > **Log** > **Log**.

- Step 2** Configure the **Start Time** and **End Time**, and then select the log type.
- **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.
 - **Alarm Event:** 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.
 - **Clear Log:** Records the operation of clearing the logs.

Step 3 Click **Search**.
Search results are displayed.

Figure 9-28 Log

| No. | Time | Username | Type | Details |
|-----|---------------------|----------|------------------------|---------|
| 1 | 2023-03-14 10:26:49 | admin | Save Config | |
| 2 | 2023-03-14 10:26:45 | admin | Save Config | |
| 3 | 2023-03-14 10:26:43 | admin | Login | |
| 4 | 2023-03-14 10:26:33 | admin | Set System Time | |
| 5 | 2023-03-14 10:26:32 | admin | Login | |
| 6 | 2023-03-14 10:26:32 | System | Device Initialization | |
| 7 | 2023-03-14 10:26:32 | System | Add | |
| 8 | 2023-03-14 10:26:32 | System | Add | |
| 9 | 2023-03-14 10:21:04 | System | Save Config | |
| 10 | 2023-03-14 10:20:53 | System | Save Config | |
| 11 | 2023-03-14 10:20:53 | System | Certificate Management | |
| 12 | 2023-03-14 10:20:53 | System | Certificate Management | |
| 13 | 2023-03-14 10:20:53 | System | Certificate Management | |
| 14 | 2023-03-14 10:20:53 | System | Certificate Management | |
| 15 | 2023-03-14 10:20:53 | System | Certificate Management | |

Step 4 Click or click a log, and then you can view the detailed information in **Details** area.

Step 5 (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.

9.8.2.2 Obtaining Remote Logs

Procedure

- Step 1** Select > **System Info** > **Log** > **Remote Log**.
- Step 2** Click to enable the function.
- Step 3** Configure the IP address, port and device number.
- Step 4** Click **Apply**.

9.8.3 Online User

Select > **System Info** > **Online User** to view all the online users logging in to the webpage.

9.8.4 Running Status

Select > **System Info** > **Running Status** to view the running status of the camera.
Click **Refresh** to get the latest status.

9.8.5 Legal Info

Select > **System Info** > **Legal Info** to view the open source software notice.

9.9 Security

9.9.1 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.

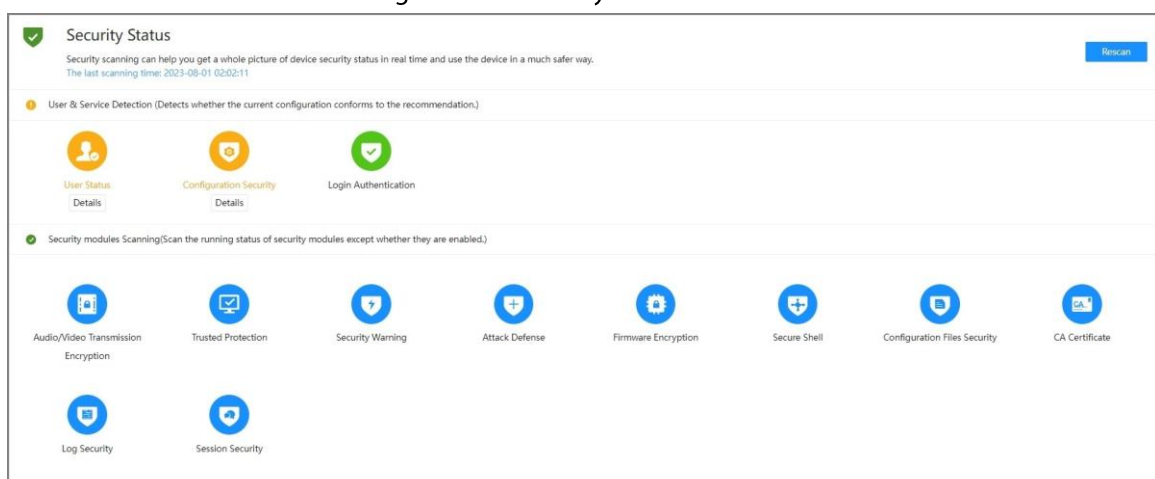
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing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

Procedure

Step 1 Select > **Security** > **Security Status**.

Step 2 Click **Rescan** to scan the security status of the camera.

Figure 9-29 Security status

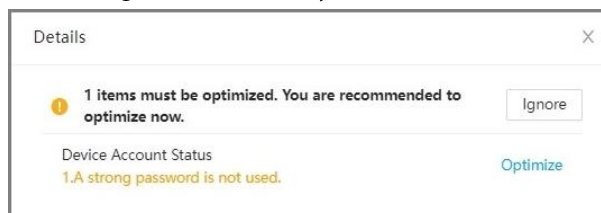


Related Operations

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 9-30 Security Status




9.9.2 System Service

9.9.2.1 802.1x

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

Procedure

- Step 1** Select  > **Security** > **System Service** > **802.1x**.
- Step 2** Select the NIC name as needed, and click to enable it.
- Step 3** 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 9-31 802.1x (PEAP)

802.1x HTTPS

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name:

Enable:

Authentication M...:

CA Certificate:

Username:

Password:

Use a trusted CA certificate to verify the validity of peer authentication server (switch or RADIUS server).

*Please select a trusted CA certificate. Certificate Management

| No. | Custom Name | Certificate Serial Number | Validity Period | User | Issued by | Used by |
|-------------------------|-------------|--|---------------------|---------|-----------|---------|
| <input type="radio"/> 1 | | 65623033313035656637326 13661313430653034626262 333961373561666666 | 2027-04-08 15:57:06 | General | General | |

- 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 9-32 802.1x (TLS)

802.1x HTTPS

802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name:

Enable:

Authentication M...:

CA Certificate:

Identity:

Use a trusted CA certificate to verify the validity of peer authentication server (switch or RADIUS server).

Device Certificate:

*Please select a trusted CA certificate. Certificate Management

| No. | Custom Name | Certificate Serial Number | Validity Period | User | Issued by | Used by |
|-------------------------|-------------|--|---------------------|---------|-----------|---------|
| <input type="radio"/> 1 | | 65623033313035656637326 13661313430653034626262 333961373561666666 | 2027-04-08 15:57:06 | General | General | |

Step 4 Click **Apply**.

9.9.2.2 HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC. 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 Select > **Security** > **System Service** > **HTTPS**.

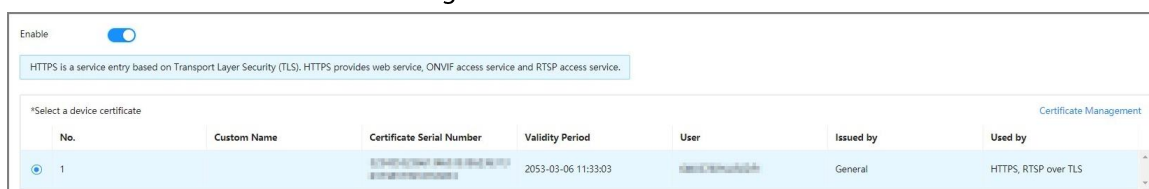
Step 2 Click to enable the function.

Step 3 Select the certificate.



If there is no certificate in the list, click **Certificate Management** to configure one. For details, see "9.9.4.2 Installing Trusted CA Certificate".

Figure 9-33 HTTPS



Step 4 Click **Apply**.

9.9.3 Attack Defense

9.9.3.1 Firewall

Configure the firewall to limit access to the camera.

Procedure

Step 1 Select > **Security** > **Attack Defense** > **Firewall**.

Step 2 Click to enable the function.

Figure 9-34 Firewall



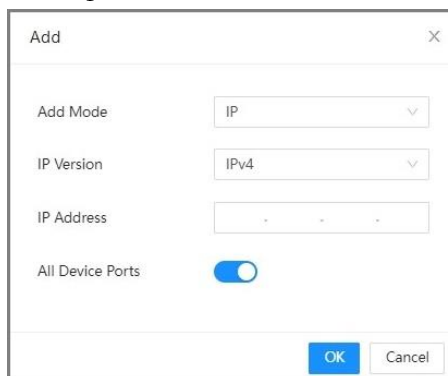
Step 3 Select the mode: **Allowlist** and **Blocklist**.

- **Allowlist:** Only when the IP/MAC of your PC in the allow list, can you access the camera. Ports are the same.
- **Blocklist:** When the IP/MAC of your PC is in the block list, you cannot access the camera.

Ports are the same.



Step 4 Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 9-35 Firewall



Step 5 Click **Apply**.

Related Operations

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

9.9.3.2 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 Select  > **Security** > **Attack Defense** > **Account Lockout**.

Step 2 Configure the login attempt and lock time for device account and ONVIF 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.

Step 3 Click **Apply**.

9.9.3.3 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 Select  > **Security** > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Click  to enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense**.

Step 3 Click **Apply**.

9.9.4 CA Certificate

9.9.4.1 Installing Device Certificate

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

9.9.4.1.1 Creating Certificate

Create certificate in the device.

Procedure


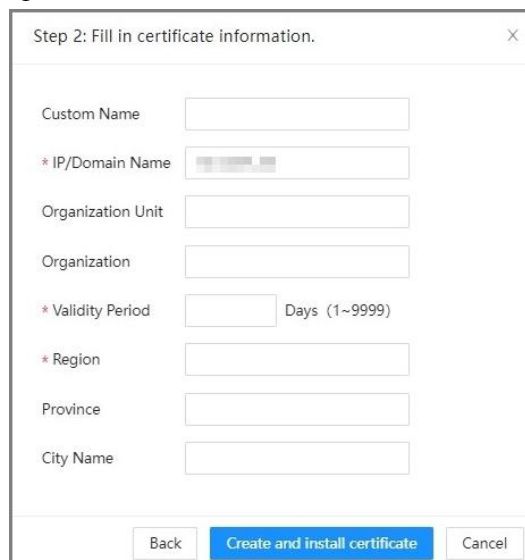
- Step 1 Select  > **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.



Figure 9-36 Certificate information (1)



- Step 5 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.

9.9.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure


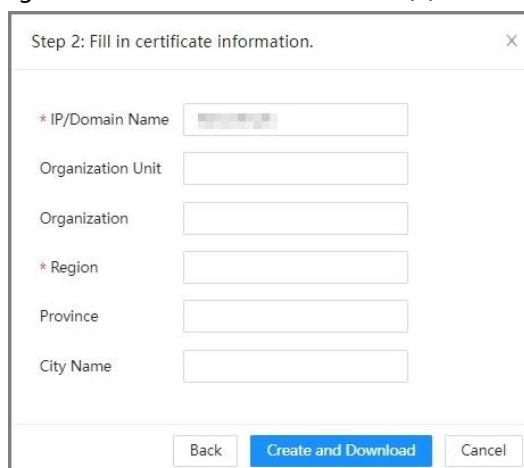
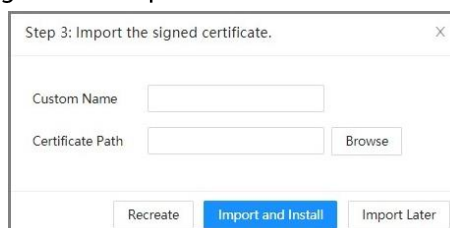
- Step 1** Select  > **Security** > **CA Certificate** > **Device Certificate**.
- Step 2** Click **Install Device Certificate**.
- Step 3** Select **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
- Step 4** Enter the certificate information.

Figure 9-37 Certificate information (2)





- Step 5** Click **Create and Download** and save the request file to your computer.
- Step 6** Use the request file to apply for a CA certificate with a third-party certificate authority.
- Step 7** Click **Browse**, and then open the CA certificate.

Figure 9-38 Import a CA certificate



- Step 8** 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.

9.9.4.1.3 Installing Existing Certificate

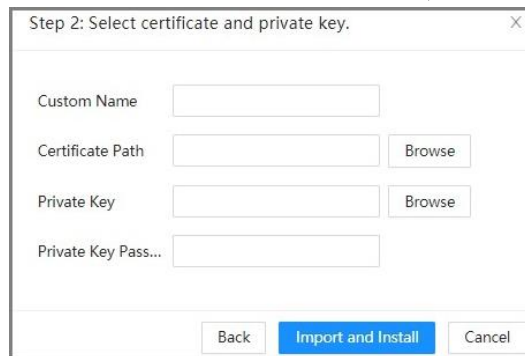
Import the existing third-party certificate to the camera. When applying for the third-party certificate, you also need to apply for the private key file and private key password.

Procedure

- Step 1** Select  > **Security** > **CA Certificate** > **Device Certificate**.



- Step 2 Select **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and then click **Next**.
- Step 4 Click **Browse** to open the CA certificate and private key, and enter the private key password.

Figure 9-39 Certificate and private key



- Step 5 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.

9.9.4.2 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


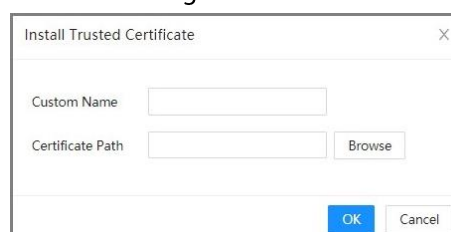
- Step 1 Select  > **Security** > **CA Certificate** > **Trusted CA Certificates**.
- Step 2 Select **Install Trusted Certificate**.
- Step 3 Click **Browse** to open the certificate.

Figure 9-40 Installing trusted certificate



- Step 4 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.

9.9.5 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** Select > **Security** > **A/V Encryption**.
- Step 2** Configure the parameters.

Figure 9-41 A/V encryption

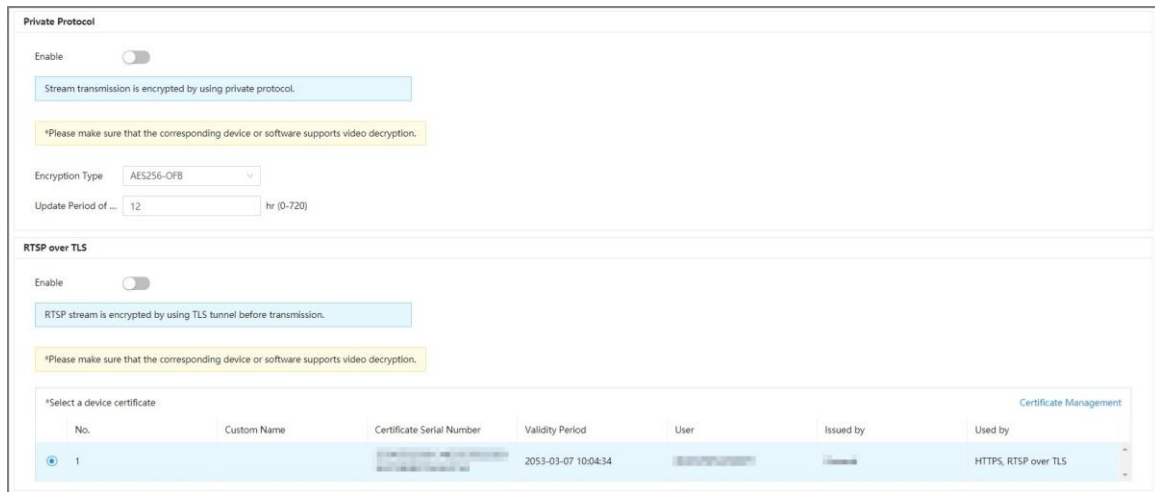



Table 9-38 Parameter description

| 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. |

| Area | Parameter | Description |
|---------------|-----------------------------|---|
| 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 "9.9.4 CA Certificate". |

Step 3 Click **Apply**.

9.9.6 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.

9.9.6.1 Security Exception

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

Procedure

Step 1 Select  > **Security** > **Security Warning** > **Security Exception**.

Step 2 Click to enable the function.

Step 3 Configure the parameters.

Figure 9-42 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 "9.8.2.1 Searching for Logs".

Step 4 Click **Apply**.

9.9.6.2 Illegal Login

The camera triggers a warning when illegal login is detected.

Procedure

Step 1 Select  > **Security** > **Security Warning** > **Illegal Login**.

Step 2 Click  to enable the function.

Step 3 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 "9.8.2.1 Searching for Logs".

Step 4 Click **Apply**.

9.10 Maintenance Center

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

9.10.1 One-click Diagnosis

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

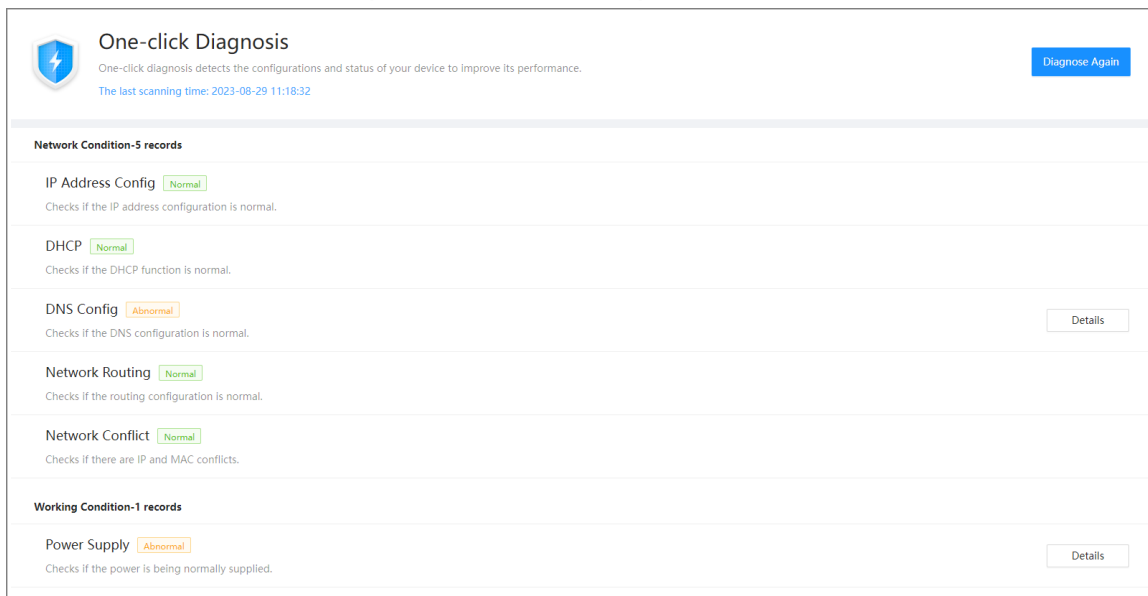
Procedure

Step 1 Select  > **Maintenance Center** > **One-click Diagnosis**.

Step 2 Click **Diagnose**.

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

Figure 9-43 One-click diagnosis

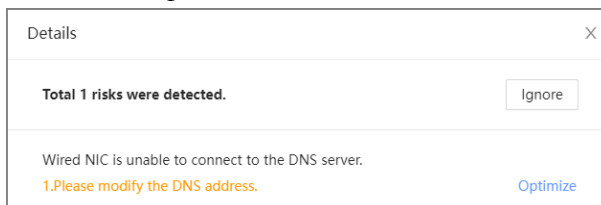


Related Operations

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 9-44 Details



9.10.2 Advanced Maintenance

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



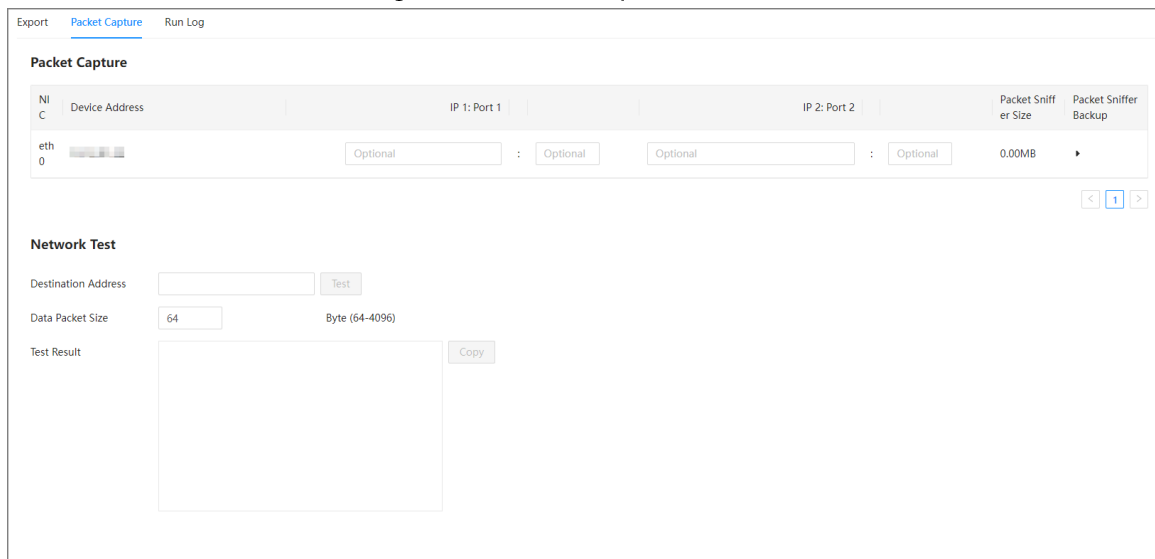
It is mainly used by technical support engineers for troubleshooting and other tech support.

Procedure

- Step 1 Select > **Maintenance Center** > **Advanced Maintenance**.
- Step 2 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 9-45 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 9-46 Network test results

Network Test

Destination Address

Data Packet Size Byte (64-4096)

Test Result

PING ... 64(92) bytes of data.


72 bytes from ...: icmp_seq = 1 ttl = 255 time < 1 ms

72 bytes from ...: icmp_seq = 2 ttl = 255 time < 1 ms

--- ... ping statistics ---

Data Packet: Sent = 2, Received = 2, Lost = 0 (0.00% Loss Rate)

Round Time Used: Min = 0 ms, Max = 0 ms, Average = 0.000 ms

- Click the **Run Log** 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.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong 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; character types include 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 overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. **MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. **Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. **Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

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

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. **Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. **Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. **Network Log**

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

13. **Construct a Safe Network Environment**

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the

device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188