

Smart Video Parking Detector

User Manual



V2.0.0

Foreword

General

This manual introduces the installation, functions and operations of the smart video parking detector (hereinafter referred to as "the Camera"). Read carefully before using the Camera, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.

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

Important Safeguards and Warnings

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

Transportation Requirements



Transport the Camera under allowed humidity and temperature conditions.

Storage Requirements



Store the Camera under allowed humidity and temperature conditions.

Installation Requirements



WARNING

- Do not connect the power adapter to the Camera while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Camera.
- Do not connect the Camera to two or more kinds of power supplies, to avoid damage to the Camera.



- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the Camera in a place exposed to sunlight or near heat sources.
- Keep the Camera away from dampness, dust, and soot.
- Put the Camera in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- 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 Camera label.
- the Camera is a class I electrical appliance. Make sure that the power supply of the Camera is connected to a power socket with protective earthing.
- An emergency disconnect device must be installed during installation and wiring at a readily accessible location for emergency power cut-off.
- Disconnect the Camera when installing and connecting the lens.

Operation Requirements



- Make sure that the power supply is correct before use.
- Do not unplug the power cord on the side of the Camera while the adapter is powered on.
- Operate the Camera within the rated range of power input and output.
- Use the Camera under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Camera, and make sure that there is no object filled with liquid on the Camera to prevent liquid from flowing into it.
- Do not disassemble the Camera.
- Do not aim the Camera at strong light sources (such as lamplight, and sunlight) when focusing it.
- Do not vibrate, squeeze or immerse the Camera in liquid during transportation, storage or installation.
- Do not block the ventilation near the Camera.
- We recommend you use the Camera 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 Camera (grounding cable or lightning surge protector) to improve its reliability. the Camera is a class I electrical appliance. Make sure that the power supply of the Camera is connected to a power socket with protective earthing.
- the Camera must be used with the protective cover for outdoor scenarios to avoid the risk of water damage to the Camera.
- 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 Camera.
- Modify the default password of the Camera after first-time login to prevent the Camera from being stolen.

Maintenance Requirements

- Pack the Camera with packaging provided by its manufacturer or packaging of the same quality before sending it back for repair.
- Please do not touch the photosensitive device with your hands. Use an air blower to clean off the dust and filth on the lens.
- Clean the surface of the Camera with a soft dry cloth or a clean soft cloth dipped in neutral detergent.
- Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Overview.....	1
1.2 Features.....	1
2 Structure.....	3
2.1 Appearance.....	3
2.2 Dimensions.....	3
2.3 Cable Connection.....	4
2.3.1 PoE Cable Connection.....	4
2.3.2 Cascading Power Supply.....	5
3 Installation.....	6
3.1 Power Supply.....	6
3.2 Installing the Camera.....	6
4 Device Initialization.....	8
5 Login.....	12
5.1 Device Login.....	12
5.2 Resetting Password.....	12
5.3 Changing IP Address.....	12
6 Home Page.....	14
7 Live.....	15
7.1 Live Page.....	15
7.2 Video Adjustment.....	16
7.3 Frequently Used Functions.....	16
7.3.1 Parking Space Status.....	16
7.3.2 Managing Parking Space.....	16
7.3.3 Device Test.....	17
7.3.4 PTZ Control.....	18
7.4 Live View Function Bar.....	18
8 Search.....	20
8.1 Parking Record Search.....	20
8.2 Picture Query.....	20
8.3 Playing Recordings.....	21
8.3.1 Record.....	21
8.3.2 Watermark.....	22
9 Setting.....	23
9.1 Local.....	23

9.2	ANPR.....	24
9.2.1	Parking Space Management.....	24
9.2.2	Image Config.....	26
9.2.3	Setting Allowlist for Vehicles.....	28
9.2.4	Indicator control.....	31
9.2.5	Configuring RS-485 Settings.....	34
9.2.6	Configuring Broadcast.....	35
9.2.7	Device Test.....	37
9.3	Camera.....	38
9.3.1	Setting Image Parameters.....	38
9.3.2	Setting Encode Parameters.....	41
9.4	Network.....	44
9.4.1	TCP/IP.....	44
9.4.2	Port.....	45
9.4.3	Auto Registration.....	47
9.4.4	Platform Access.....	47
9.4.5	Basic Services.....	49
9.5	Event.....	49
9.5.1	Setting Exception.....	49
9.5.2	Setting Video Detection.....	50
9.5.3	Subscribing Alarm.....	51
9.6	System.....	52
9.6.1	General Parameters.....	53
9.6.2	Account.....	54
9.7	Security.....	59
9.7.1	Security Status.....	59
9.7.2	System Service.....	60
9.7.3	Attack Defense.....	63
9.7.4	CA Certificate.....	64
9.7.5	A/V Encryption.....	68
9.7.6	Security Warning.....	69
9.8	Maintenance Center.....	69
9.8.1	One-click Diagnosis.....	70
9.8.2	System Information.....	70
9.8.3	Log.....	71
9.8.4	Manager.....	72
9.8.5	Update.....	74
9.8.6	Advanced Maintenance.....	74
Appendix 1	Security Recommendation.....	77

1 Introduction

1.1 Overview

This Camera is an intelligent parking space detector that can be used in the intelligent parking lot management system for parking guidance and reverse vehicle search in indoor parking lots.

- It detects and captures vehicles, recognizes license plates, detects parking space status (empty or occupied), and controls the indicator light of parking spaces.
- When connected to the parking management system, LED display, and reverse vehicle search device, it provides parking guidance for drivers and facilitates reverse vehicle search for an improved parking experience.

1.2 Features

Intelligent Recognition

- Supports drawing detection area to detect the status of parking spaces (empty or occupied), and automatically captures pictures.
- Recognizes license plates.
- Supports detecting vehicles without license plates, and the detection threshold can be set.
- OSD overlay on videos and snapshots.

Attractive Design

Attractive dome design, parking space indicator light, and ceiling installation allow the Camera to meet the needs of indoor parking lots.

Wide Dynamic Range (WDR)

WDR is available on select models, making these models work well in both dark and bright scenes.

Integration

- It has a dome design, parking space indicator light, and uses a ceiling mount, allowing it to meet the needs of the parking lots.
- Some models support wide dynamic mode, which can automatically adapt to brightly lit and poorly lit scenes.

Multi-color Indicator Light

- 7 colors are available for the indicator light, and the indicator light status can be adjusted as needed.
- The Camera detects vehicles by video detection and recognizes license plates. The indicator light displays the status of the parking space (empty or occupied) according to the detection results.
- Supports configuring the indicator color according to the network port status.

Multiple Parking Space Detection

- ITC214-PH5B-F series support detecting 2 parking spaces at the same time.
- ITC414-PH5B-F series support detecting 3 parking spaces at the same time.
- ITC414-PH5B-TF series support detecting 6 parking spaces at the same time.

Power Supply

Standard 48 VDC power supply. It can also adapt to 12–48 VDC voltage.

2 Structure

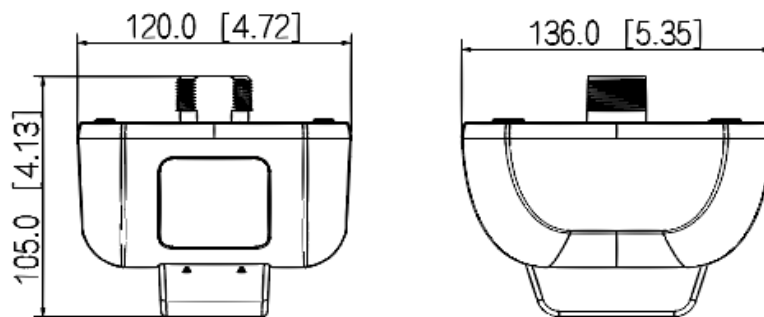
2.1 Appearance

Figure 2-1 Appearance



2.2 Dimensions

Figure 2-2 Dimensions (mm [inch])



2.3 Cable Connection

2.3.1 PoE Cable Connection

Figure 2-3 PoE

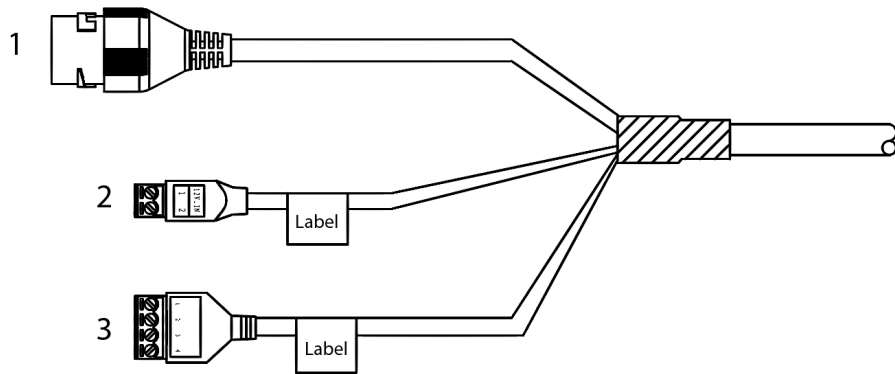


Table 2-1 PoE cable description

No.	Name	Description
1	Network port	Connect to standard Ethernet cable. PoE is supported.
2	Power	1: 12 VDC_IN. 2: GND_IN.
3	External light	1: 12V_OUT. 2: GND_OUT. 3: RS-485_A. 4: RS-485_B.

2.3.2 Cascading Power Supply

Figure 2-4 Network cable

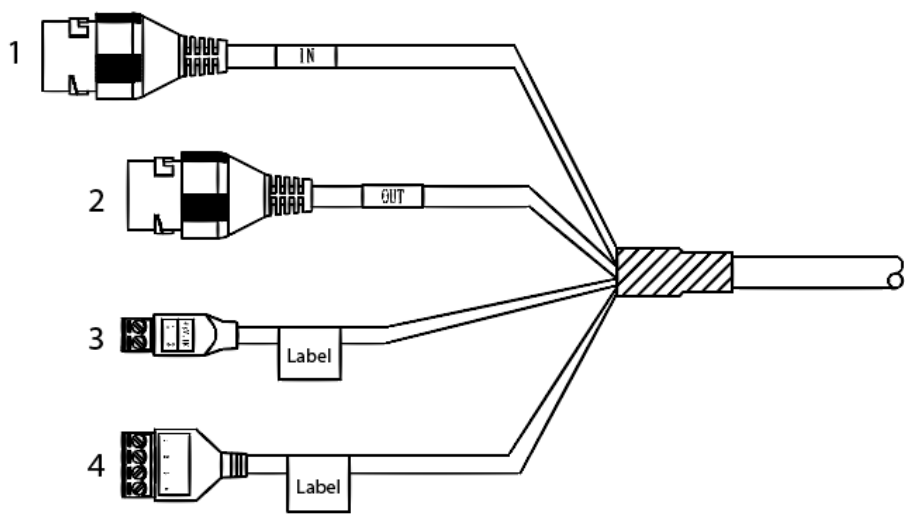


Table 2-2 Network cable description

No.	Name	Description
1	Network port (IN)	Network power input port.
2	Network port (OUT)	Network power output port.
3	Power	● 1: 48V_IN. ● 2: GND_IN.
4	External light	● 1: 12V_OUT. ● 2: GND_OUT. ● 3: RS-485_A. ● 4: RS-485_B.

3 Installation

3.1 Power Supply

- ITC214-PH5B-F3-POE, ITC414-PH5B-F2-POE and ITC414-PH5B-TF2-POE series devices are supplied with PoE.
- ITC214-PH5B-F3, ITC414-PH5B-F2 and ITC414-PH5B-TF2 series devices supports cascading with network cables to provide 48 V power supply. 4 dual-sensor cameras or 8 single-sensor cameras can be supplied at the same time.

3.2 Installing the Camera

Background Information



Mount the Camera to the ceiling mounting tray, and the installation surface must be able to bear at least 3 times the weight of the Camera.



- The stud diameter is 33 mm.
- The installation uses ITC214-PH5B-F3-POE as an example. The installation diagram is for reference only, and might differ from the actual device.

Procedure

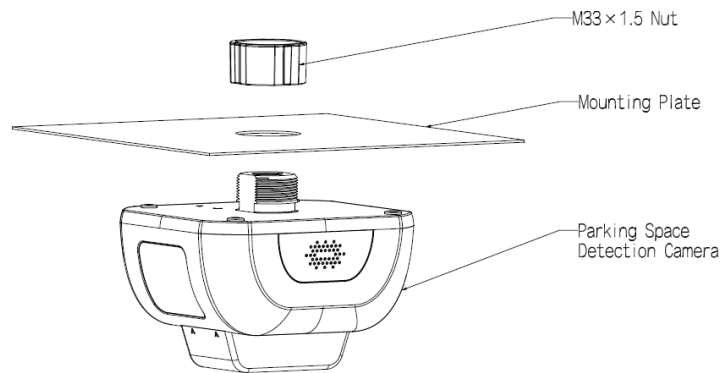
- Step 1 Use a hole saw to drill a hole with a diameter of 35 mm at the device mounting position.

Figure 3-1 Hole saw



- Step 2 Feed the cables of the Camera through the hole on the mounting plate.
- Step 3 Loosen the nut, feed the cable through the nut, and then fix the nut to the mounting plate.

Figure 3-2 Installation



- Step 4 Refer to "2.3 Cable Connection" to connect the cables.
- Step 5 Remove the cover, and adjust the monitoring view according to the position of the Camera.
- Step 6 Tighten the cover.

4 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 4-1 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.

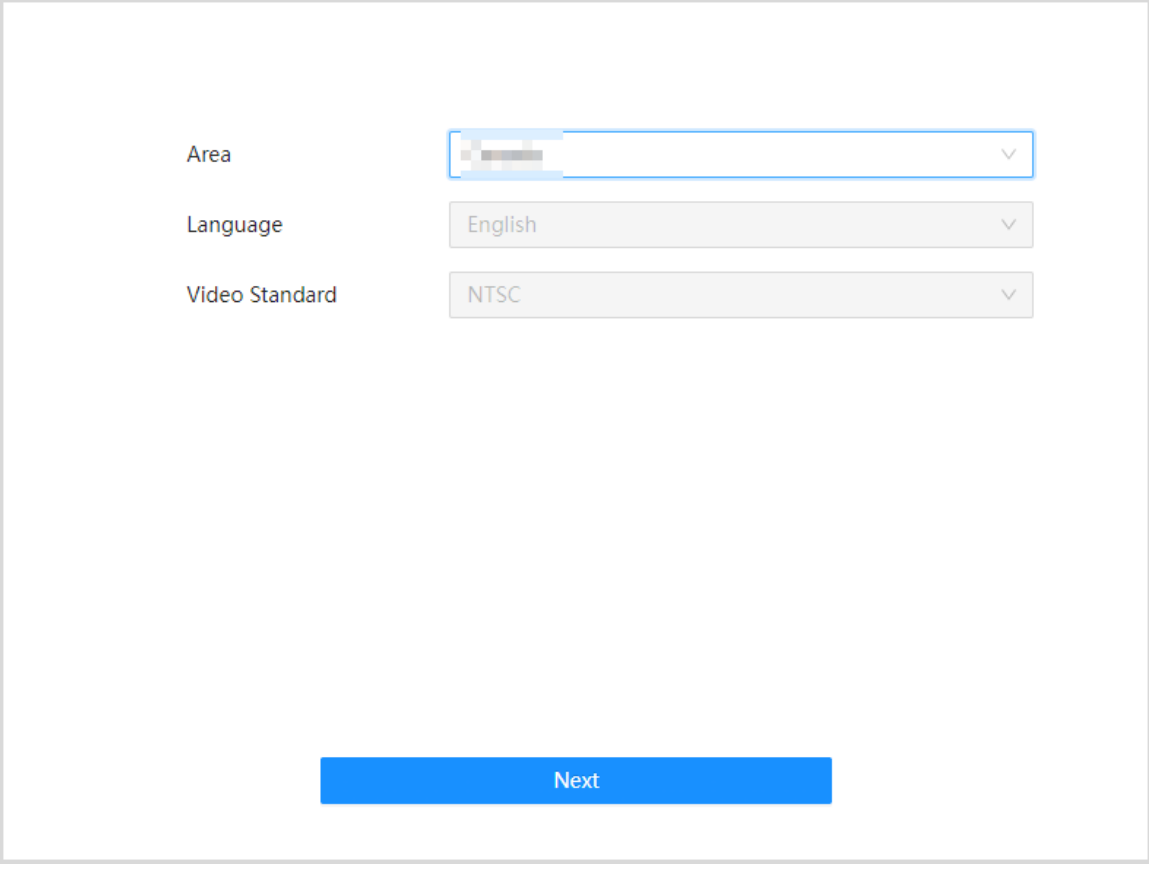


- The latest versions of Google Chrome and Microsoft browsers are supported. Most functions are available without a plug-in. A few functions require downloading a plug-in, but they still work with Google Chrome.
- Internet Explorer (IE) is not recommended. Before using it, clean up the web3.0 plug-in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

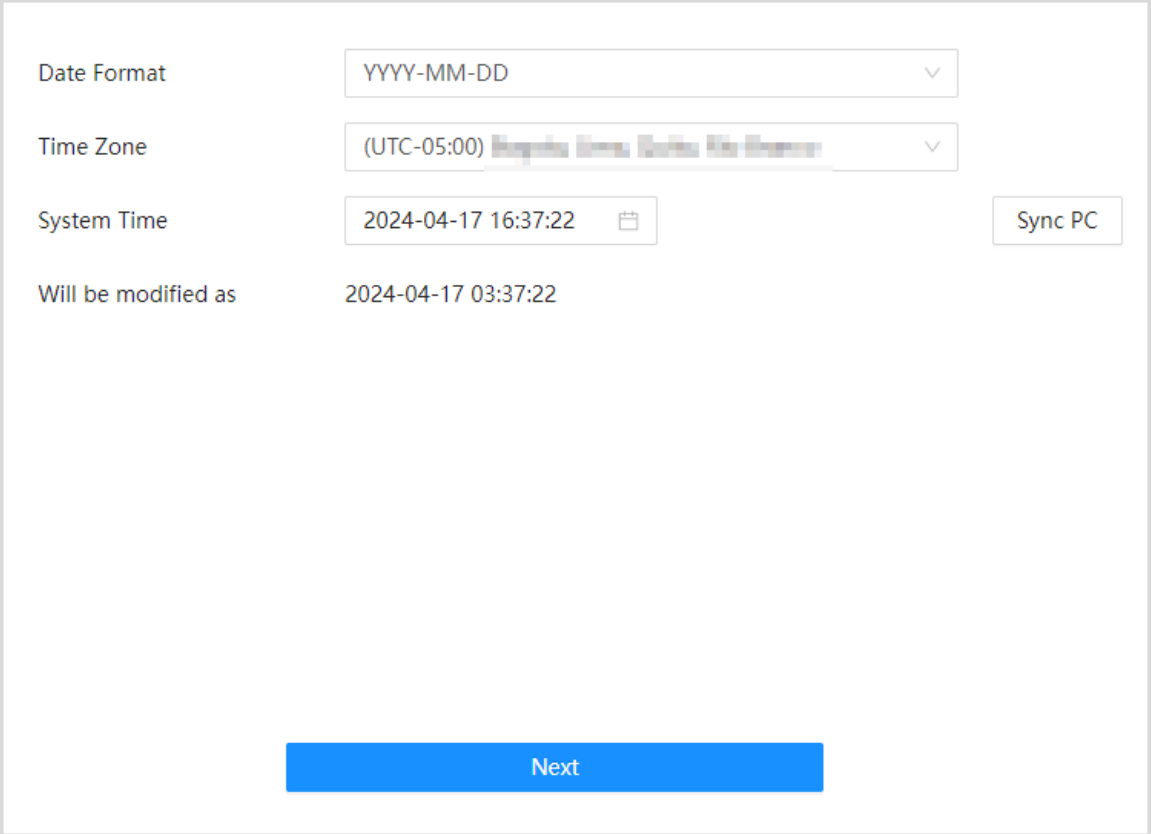
- Step 1 Open the browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar, and then press the Enter key.
- Step 2 Select the area, and then click **Next**.

Figure 4-1 Region setting

The image shows a region setting interface within a light gray rectangular frame. On the left side, there are three labels: 'Area', 'Language', and 'Video Standard'. To the right of 'Area' is a dropdown menu with a blue border and a small icon on the left. To the right of 'Language' is a dropdown menu with a light gray background and the text 'English'. To the right of 'Video Standard' is a dropdown menu with a light gray background and the text 'NTSC'. All three dropdown menus have a small downward arrow on the right side. At the bottom center of the frame is a blue rectangular button with the text 'Next' in white.

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

Figure 4-2 Time zone setting



The image shows a configuration window for time and date settings. It includes four rows of controls: 'Date Format' with a dropdown set to 'YYYY-MM-DD'; 'Time Zone' with a dropdown set to '(UTC-05:00)'; 'System Time' with a text field showing '2024-04-17 16:37:22' and a calendar icon, and a 'Sync PC' button; and 'Will be modified as' with a text field showing '2024-04-17 03:37:22'. A large blue 'Next' button is centered at the bottom.

Date Format	YYYY-MM-DD	▼
Time Zone	(UTC-05:00)	▼
System Time	2024-04-17 16:37:22	 Sync PC
Will be modified as	2024-04-17 03:37:22	

Next

Step 4 Set the password for admin account.

Figure 4-3 Password setting

The screenshot shows a password configuration form. The 'Username' field is labeled 'admin'. The 'Password' field is masked with dots and has a strength indicator bar below it, which is partially orange and partially blue. The 'Confirm Password' field is also masked with dots. The 'Email Address' field has a checked checkbox and is partially masked. Below the fields, there is a note: 'For password reset. Recommended or improved in time.' At the bottom, there is a blue 'Next' button.

Table 4-2 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	
Email Address	Enter an email address for password resetting, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 5 Click **Next**, and then the **Online Update** page is displayed. Then, it automatically redirects to the login page. Re-enter the password for the home page.

5 Login

Log in to the Camera web client through browser on the computer, and then you can configure, operate on, and manage the Camera.



The pages and settings are for reference only, and might differ from the actual page.

5.1 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 "4 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 "5.2 Resetting Password".

Step 3 Click **Login**.

5.2 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.

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.

5.3 Changing IP Address

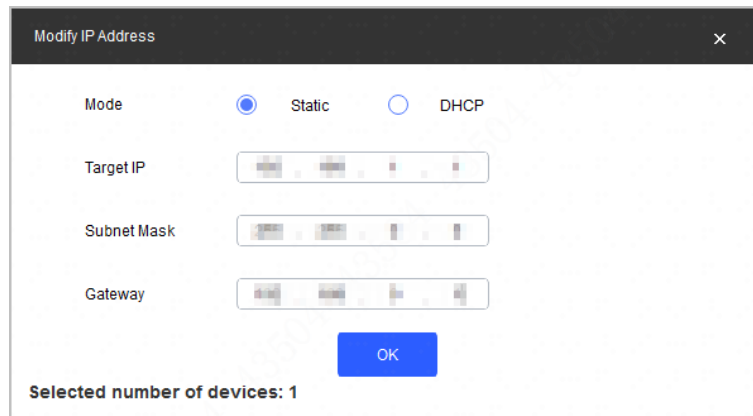
Background Information

You can acquire and change the IP address of devices accessed through wired network. This section uses changing IP address with ConfigTool as the example.

Procedure

- Step 1 Get ConfigTool from technical support and install it on your local computer.
- Step 2 Double-click .
- Step 3 Click **Modify IP** on the homepage.
- Step 4 Select the device(s) whose IP need(s) to be changed.
- Change one IP address: Click **Edit** corresponding to the device.
 - Change IP addresses in batches: Select the devices, and then click **Batch Modify IP**.
- Step 5 Set mode, IP, subnet mask and gateway.
- Step 6 Click **OK**.

Figure 5-1 Change IP addresses in batches



Modify IP Address

Mode ☒ Static ☐ DHCP

Target IP

Subnet Mask

Gateway

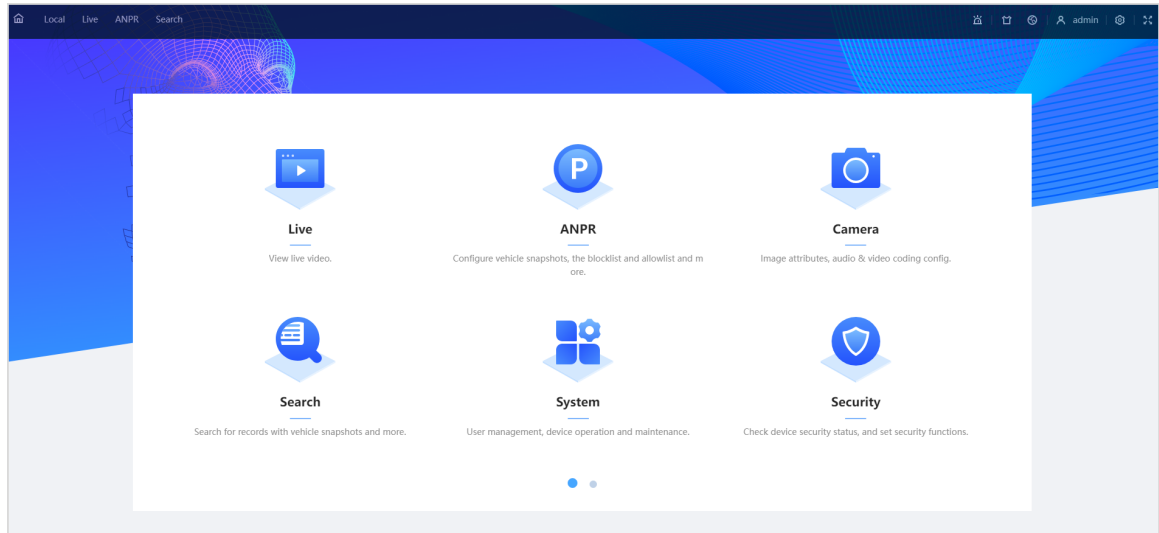
OK

Selected number of devices: 1

6 Home Page

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

Figure 6-1 Home page



- 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 **Restart**, 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.

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

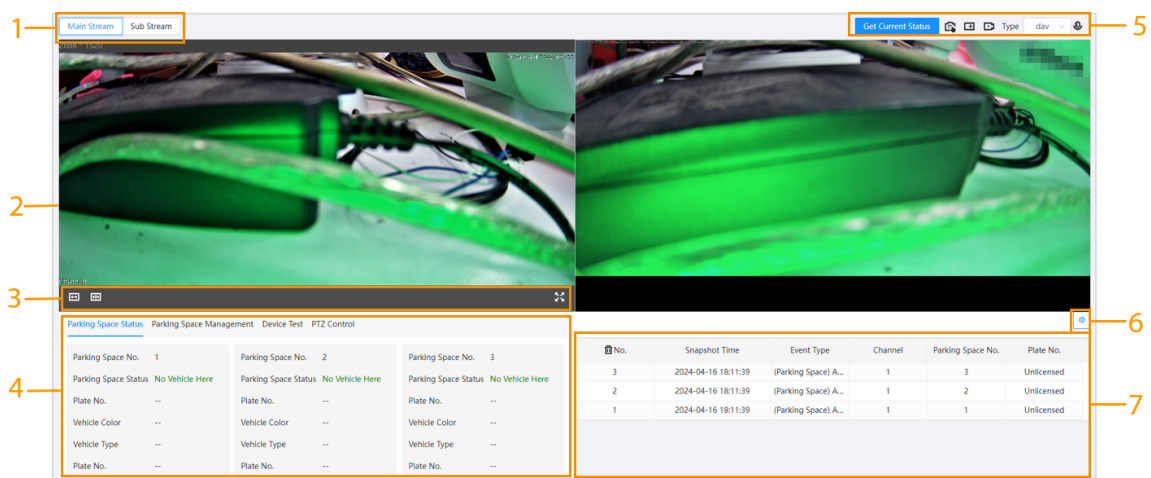


Table 7-1 Function description

No.	Function	Description
1	Stream Switch	Select a video stream based on your network bandwidth. ● Main stream: Displays video with high resolution, but requires large bandwidth. This option can be used for storage and monitoring. ● Sub stream: Displays the video in lower resolution but smoothly. It requires less bandwidth. This option is normally used to replace main stream when the network bandwidth is not enough.
2	Live view and snapshots	Displays real-time video and snapshots.
3	Video adjustment	Adjustment operations in live viewing.
4	Frequently used functions	You can view parking space status, manage parking space, test device and perform PTZ operations.
5	Live view function bar	Functions and operations in live viewing.
6	Filter	You can select different choices to filter the details of the capture that are displayed in the list.
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
	W:H	Adjust the display scale, that is, the ratio between the width and the height of the live video display. • Original: Restore to the original display size. • Adaptive: Maximize the video to the full-screen display.
	Smart track detection	Click the icon to enable intelligent trajectory.
	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 Parking Space Status

Click **Parking Space Status** to view the information of parking space and parked vehicles, including parking space number and number, plate number of the parked vehicles and vehicle property.

Figure 7-2 Parking space status

Parking Space Status Parking Space Management Device Test PTZ Control			
Parking Space No.	1	Parking Space No.	2
Parking Space Status	No Vehicle Here	Parking Space Status	No Vehicle Here
Plate No.	--	Plate No.	--
Vehicle Color	--	Vehicle Color	--
Vehicle Type	--	Vehicle Type	--
Plate No.	--	Plate No.	--
Parking Space No.	3	Parking Space No.	3
Parking Space Status	No Vehicle Here	Parking Space Status	No Vehicle Here
Plate No.	--	Plate No.	--
Vehicle Color	--	Vehicle Color	--
Vehicle Type	--	Vehicle Type	--
Plate No.	--	Plate No.	--

7.3.2 Managing Parking Space

Set a parking zone and parking spaces inside the zone, so the Camera can detect whether the specified parking space is occupied and recognize the vehicle.

Click **Parking Space Management** on the lower-left corner.

Add parking space and draw detection lines, and then click **Apply**.

Figure 7-3 Snapshot

Parking Space Status **Parking Space Management** Device Test PTZ Control

Parking Space No.	Large Vehicle	Motorcycle	Operation
1	☒	☐	
2	☒	☐	

[+ Add Parking Space](#)

Detection Line

Table 7-3 Parameter description

Parameter	Description
Add Parking Space	Click Add Parking Space to add parking space. You can add up to 3 parking spaces.
Detection Line	Click Add Detection Line , draw lines between parking spaces. The Camera detects when vehicles are parking over the line and trigger alarms based on the drawn lines. Click Delete to delete detection lines

7.3.3 Device Test

You can view and test parking event, voice broadcast, external light settings and status, and abnormal configuration. You can also export device information.

Enter a plate number and select events, and then click **(Parking Space) Occupied**. The Camera reports the corresponding event data to the third party platform. If no events are selected, only a record of parking space occupied by the set vehicle will be reported.



Click **(Parking Space) Available** to report on empty parking spaces to the platform.

Set a text, click **Test** next to **Voice Broadcast** to test the set text audio.

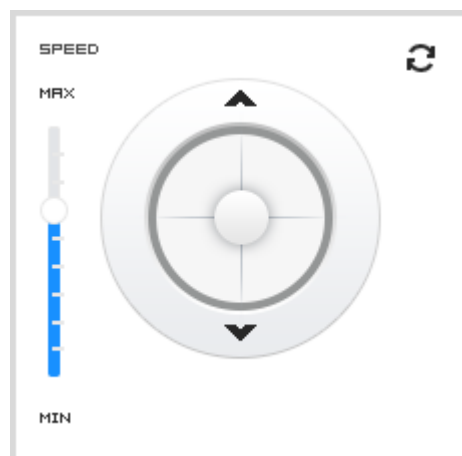
Figure 7-4 Device test

Test Event	(Parking Space) Occupied	(Parking Space) Available
Parking Space No.	1	AB12345
Event	☐ TrafficParkingSpaceOverLine ☐ Occupied by Non-allowlist Vehicle ☐ Small Vehicle Parked in Large Vehicle's Space	
Test Voice Broadcast	Test	Welcome

7.3.4 PTZ Control

Click **PTZ Control** to adjust the camera view. Make sure the target parking spaces are inside the Camera field of vie and are easy to recognize.

Figure 7-5 Peripheral



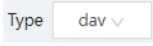
7.4 Live View Function Bar

Figure 7-6 Live view function bar



Table 7-4 Function description

Icon	Description
Get Current Status	View the newest snapshot of parking space status change.
	Click this icon and then the camera will take 1 snapshot.

Icon	Description
	Use this function to zoom in on any area of the video. Click this icon, and then click and hold to select an area on the video. The camera will zoom in on the area you selected.
	Click 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.

8 Search

Use this function to play local videos, and search for snapshots and parking records.

8.1 Parking Record Search

Search for the vehicle parking record within the defined period.

Procedure

Step 1 On the home page, click **Search**.

Step 2 Configure the search conditions such as time range, event type and plate number.

Figure 8-1 Parking record search

No.	Snapshot Time	CH	Parking Space No.	Event Type	Plate No.	Attribute	Trigger Source	Subscribed Platform IP
No data								

- **Parking Space No.** : Select parking spaces to view the corresponding records.
- **Event Type** : The status of the selected parking spaces during the set period.
- **Search Results** : Click **Export All** or **Export by Time** to export parking records of the defined period or all records to local computer.

Step 3 Click **Search**.

8.2 Picture Query

You can search for snapshots stored on the SD card.

Procedure

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

Figure 8-2 Memory card picture

No.	File Name	Creation Time	Size(KB)	Watermark
No data				

Supported image formats: jpg.

Step 2 Click **Browse**, and then select folder where the picture to be verified is located.

Step 3 Click the picture which needs to be verified.

Step 4 Click **Watermark**, and then view the results under **Watermark Verification**.

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



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

8.3 Playing Recordings

The Camera allows you to play local recordings, add watermarks to them and verify whether the video is tampered by using watermarks.

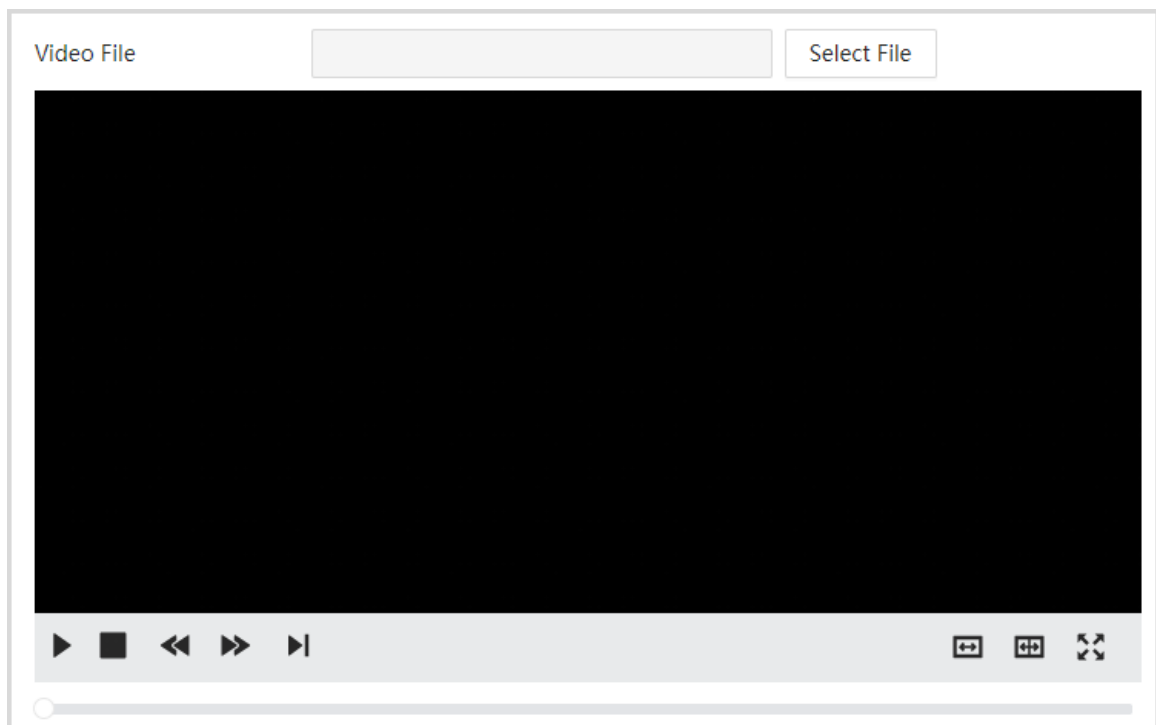
8.3.1 Record

You can play videos that are stored on your computer.

Procedure

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

Figure 8-3 Record



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

Functions, such as adjust image size, IVS and full screen are supported while you play the recording.

Table 8-1 Play function description

Icon	Description
	Play
	Stop playing
	Slow down
	Speed up

Icon	Description
	Playing the next frame

8.3.2 Watermark

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

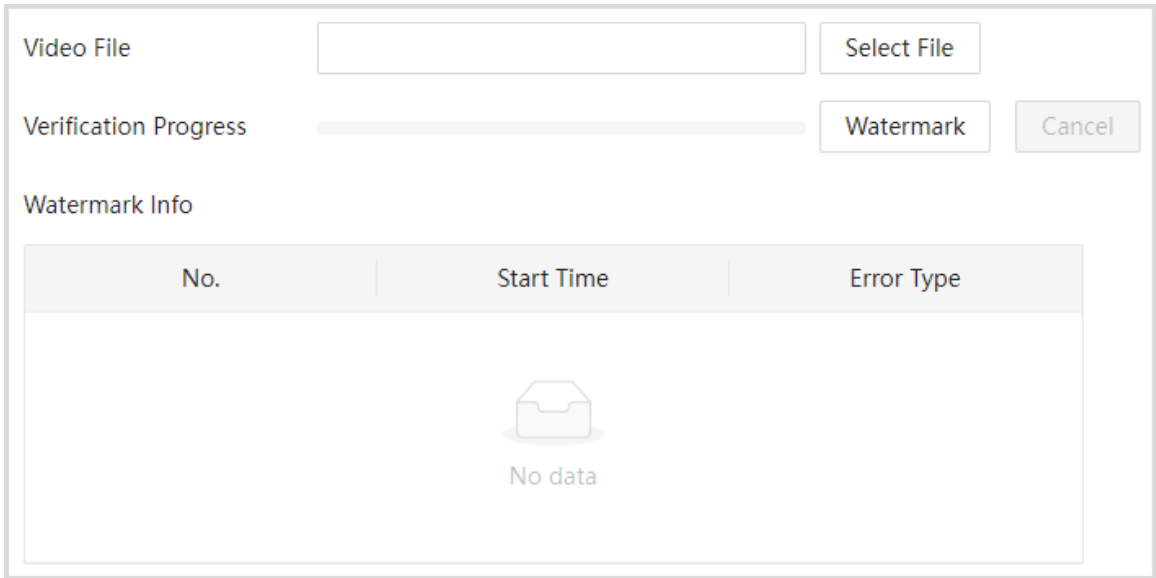
Prerequisites

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**.

Figure 8-4 Watermark



Video File

Verification Progress

Watermark Info

No.	Start Time	Error Type
 No data		

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

Step 3 Click **Watermark**, and the Camera displays the verification progress.

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

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.	
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 Parking Space Management

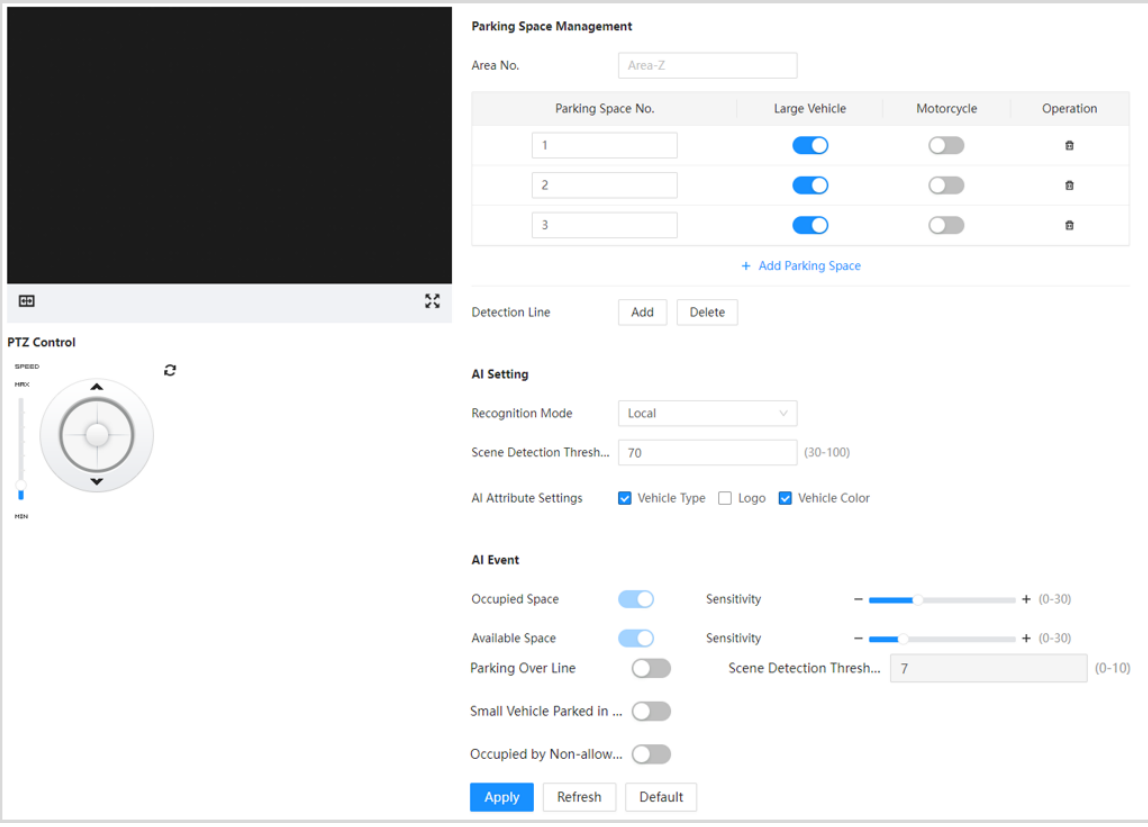
9.2.1.1 Configuring Parking Space

Configure a parking zone and parking spaces inside the zone, so the Camera can detect whether the specified parking space is occupied and recognize the vehicle.

Procedure

Step 1 Select  > **ANPR** > **Parking Space Management** > **Parking Space Management**.

Figure 9-1 Parking space management



Parking Space Management

Area No.

Parking Space No.	Large Vehicle	Motorcycle	Operation
1	☒	☐	
2	☒	☐	
3	☒	☐	

[+ Add Parking Space](#)

Detection Line

AI Setting

Recognition Mode

Scene Detection Thresh... (30-100)

AI Attribute Settings ☒ Vehicle Type ☐ Logo ☒ Vehicle Color

AI Event

Occupied Space ☒ Sensitivity (0-30)

Available Space ☒ Sensitivity (0-30)

Parking Over Line ☐ Scene Detection Thresh... (0-10)

Small Vehicle Parked in ... ☐

Occupied by Non-allow... ☐

Step 2 Add parking space and configure the parking space including parking area number and adding detection line.

- The Camera detects when vehicles are parking over the line and triggers alarms based on the drawn lines.
- The type and number must be filled in for each parking area.
- The number of parking spaces that can be detected varies depending on the model of the Camera.

Step 3 At the lower-left corner of the page, set **Speed** and click  or  to adjust the Camera view. Make sure the target parking spaces are inside the Camera field of view and are easy to recognize.



You can select **Local** or **Remote** as the recognition mode.

- **Local** : Video recordings are analyzed by the Camera to get information such as parking space number, status, plate number and vehicle model, and display on the **Live** page.
- **Remote** : The Camera only sends snapshots and video recordings to terminals such as a platform for analysis.

Step 4 Configure AI rules including recognition mode, scene detection threshold and AI attributes.

The Camera obtains the corresponding attributes and reports them to backend terminals such as a platform for analysis.

Step 5 Configure AI event, select AI events and set the corresponding sensitivity as needed, and then click **Apply**.

- **(Parking Space) Occupied /(Parking Space) Available**: Detects the parking space status. They are selected by default.
- **Vehicle Parking on Line** : Detects whether the vehicle is parked on the drawn detection lines.
- **Small Vehicle Parked in Large Vehicle's Space** : Select to enable the Camera to detect when a small vehicle is parked in a large vehicle space, and to report on these alarms to the third party platform.



To enable this function, make sure to select **Vehicle Type** when setting **AI Attribute Settings**.

- **Occupied by Non-allowlist Vehicle** : Detects and recognizes whether the specified parking space is occupied by a vehicle that is not on the allowlist.

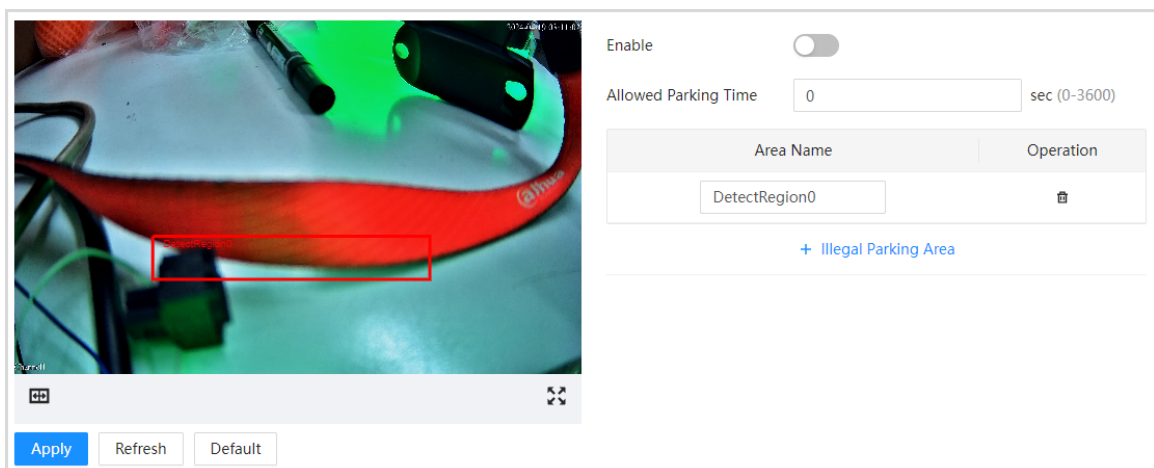
Step 6 Click **Apply**.

9.2.1.2 Configuring Illegal Parking Area

Procedure

Step 1 Select  > **ANPR** > **Parking Space Management** > **Illegal Parking Space**.

Figure 9-2 Illegal parking area



Area Name	Operation
DetectRegion0	

[+ Illegal Parking Area](#)

Apply **Refresh** **Default**

Step 2 Click  to enable illegal parking space function.

Step 3 Click **Illegal Parking Time**, and when detects illegal parking area is occupied and the duration exceeds the defined time, an alarm will be triggered.

Step 4 Click [+ Illegal Parking Area](#) to add illegal parking area.



You can add up to 2 illegal parking areas.

Step 5 Click **Apply**.

9.2.2 Image Config

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

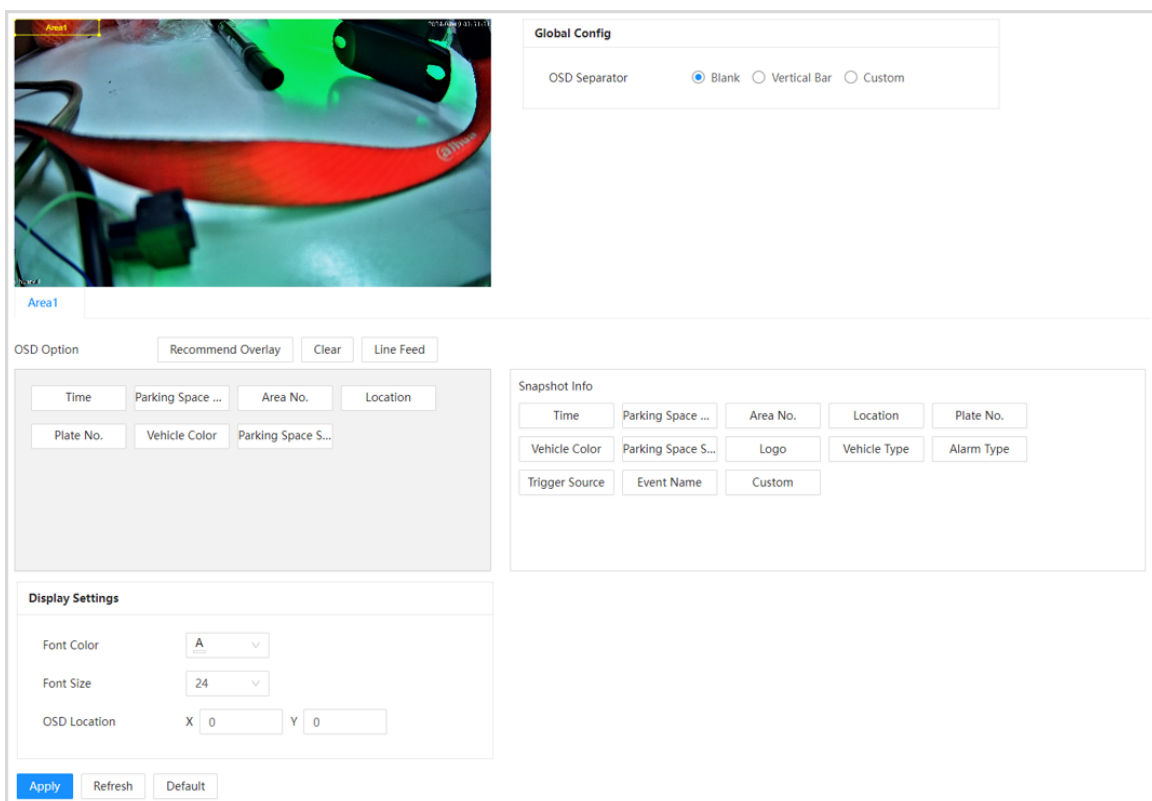
9.2.2.1 Original Picture OSD

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

Procedure

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

Figure 9-3 Original picture OSD



Step 2 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 "2024-04-19|A12345".

Step 3 Configure the OSD information to be displayed.

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



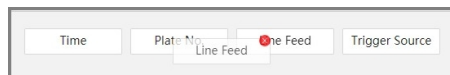
- Click **Recommend Overlay** and then the camera will automatically add various types of information.
- To delete any type of information, hover your mouse over it, and then click . Or you can click **Clear** to delete all the information that have been added.
- **Line Feed** is used to separate the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

Figure 9-4 Line feed

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

2. Drag to adjust the order of information.

Figure 9-5 Adjust the order



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

Table 9-2 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 4 Configure the font color and size.

Step 5 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 6 Click **Apply**.

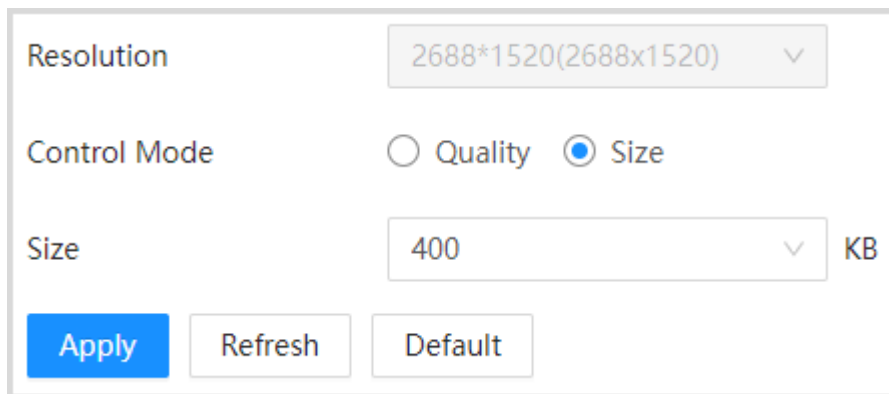
9.2.2.2 Size

Configure the quality of snapshots.

Procedure

Step 1 Select  > **ANPR** > **Image Config** > **Size**.

Figure 9-6 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 Setting Allowlist for Vehicles

9.2.3.1 Fuzzy Match

When comparing the actual plate numbers to those in the allowlist for barrier control, this function allows the camera to misread certain characters in the plate numbers so that a vehicle can still pass even if the camera is unable to recognize its plate number exactly.

Procedure

Step 1 Select  > **ANPR** > **Vehicle Blocklist/Allowlist** > **Fuzzy Matching**.

Figure 9-7 Fuzzy match

Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Table 9-3 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.
The system matches similar characters to be the same	This parameter allows the camera to misread certain characters as other ones. You can add up to 6 rules. For example, a 0<->D rule allows the barrier to open if the camera recognizes A0123 to AD123, or vice versa.

Step 4 Click **Apply**.

9.2.3.2 Allowlist

You can view allowlist vehicles, add a plate number to the allowlist and set a specific parking space for the vehicle.

Procedure

Step 1 Select  > **ANPR** > **Allowlist** > **Allowlist**.

Figure 9-8 Allowlsit

Add

Import

Export

Clear Expired Data

Clear

All x

All

Search for plate... Search

No.	Parking Space No.	Plate No.	Owner Name	Start Time	End Time	Status	Operation
No data							

Step 2 Add plates.

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

Figure 9-9 Add vehicles

Add

* Parking Space No.

All x

* Plate No.

A123456

Owner Name

3333

Start Time

2024-04-19 00:00:00

End Time

2024-04-19 23:59:59

☒ Add More

Cancel

OK

Table 9-4 Parameter description

Parameter	Description
Parking Space No.	(Required) Select a parking space.
Plate No.	(Required) Enter the plate number of the vehicle.
Owner Name	Enter the name of owner of the vehicle.
Card	(Optional) Enter the parking card number.
Start Time	Configure a valid period, within which the parking space is available.
End Time	

Parameter	Description
Add More	Select the checkbox, and then you can continue to add another parking space 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 parking space: Click  of a vehicle to edit its information.
- Delete parking space one by one: Click  of a vehicle to delete it from the allowlist.
- Delete vehicles in batches: Click **Clear** to delete all the parking space from the allowlist. Please be advised that this operation cannot be undone.
- Delete expired vehicles: parking spaces 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 Indicator control

9.2.4.1 Configuring Indicator Control

Configure the corresponding indicator color for different statuses of parking spaces, and then the corresponding light will turn on when the parking space status changes.

Procedure

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

Figure 9-10 Indicator control

Light Sensitivity
 Delay for Light on if Oc... sec (2-100)
 Delay for Light on if Av... sec (2-100)

Light Corresponding to Parking Space Status
 Parking Space Available Flicker ☐
 Occupied Space Flicker ☐

Event Alarm Corresponding Lights
 Parking Space Alarm
 Flicker sec (1-300)

Light Corresponding to Ethernet Port Status
 Single Abnormal Ethernet... Flicker ☐
 Double Abnormal Ethernet... Flicker ☐

Light Group	1	2	3
Built-in Light	☒	☒	☒
External Light1	☒	☐	☐
External Light2	☐	☒	☐
External Light3	☐	☐	☒

Step 2 Configure the parameters.

Table 9-5 Parameter description

Parameter		Description
Light Sensitivity Config	Delay for Light on if Occupied	Set the sensitivity that the indicator is to respond with when the status of a parking space changes between occupied, available and alarmed. The lower the value, the faster the indicator responds.
	Delay for Light on if Available	
Light Corresponding to Parking Spaces Status	Parking Space Available	Set the indicator to indicate when a parking space is empty (Parking Space Available), occupied (Occupied Space), and when an alarm is triggered (Parking Space Alarm).
	Occupied Space	
Event Alarm Corresponding Light	Parking Space Alarm	1. Select a light color for each status. You can also select Close to disable the indicator light. 2. Select Always On to set the indicator status when an alarm is triggered. 3. Select Customized (twinkle duration) to set the indicator status when an alarm is triggered.
	Flicker	
Light Corresponding to Ethernet Port Status	Single Net Exception	Set the indicator status when a network error is detected. Only available for models powered by cascading network cables. Double Net Exception is for dual-sensor models.
	Double Net Exception	
Light Corresponding to Parking Space Status	Single Abnormal Ethernet Port	Link the built-in indicator light of the Camera to parking spaces.
	Double Abnormal Ethernet Port	Link the external indicator light of the Camera to a parking space.

Step 3 Click **Apply**.

9.2.4.2 Adding Camera

Procedure

Step 1 Select  > **ANPR** > **Add Camera**.

Figure 9-11 Add camera

Controlled

Controlled Device IP

Controlled Lighting ☒ Built-in Light ☐ External Light1 ☐ External Light2 ☐ External Light3

Remote Control

▼ Remote Control 1

Enable ☐

Username

Password

IP Address

Step 2 Configure the parameters.

Table 9-6 Parameter description

Parameters		Description
Controlled	Controlled Device IP	Enter the IP address of camera in Controlled Device IP , and then all external lights connected to the camera can be remotely controlled by the current camera.
	Controlled Lightning	Select the built-in light or external light of the camera, and then the camera light will be linked to the parking space.

Parameters		Description
Remote Control	—	Click Add to add a remote control, and then click > to enter the username, password and IP address of another camera.  Click  to enable the corresponding remote control.

Step 3 Click **Apply**.

9.2.5 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

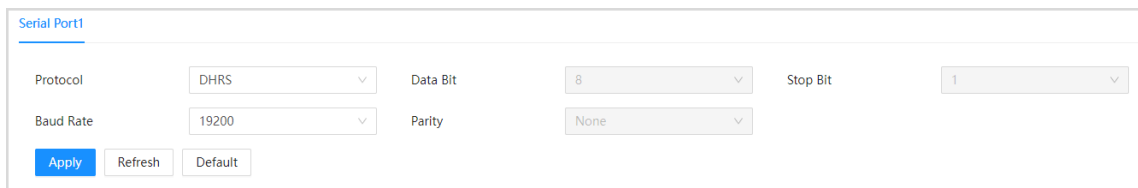
Step 1 Select  > **ANPR** > **RS-485 Settings**.

Step 2 Configure the parameters.

The camera supports multiple protocols.

- D HRS and DGRS

Figure 9-12 D HRS parameters



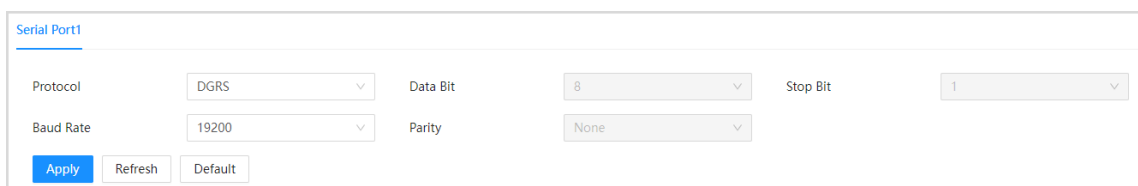
Serial Port1

Protocol: DHRS Data Bit: 8 Stop Bit: 1

Baud Rate: 19200 Parity: None

Apply Refresh Default

Figure 9-13 DGRS



Serial Port1

Protocol: DGRS Data Bit: 8 Stop Bit: 1

Baud Rate: 19200 Parity: None

Apply Refresh Default

- 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 9-14 RS-485 Transparent transmission

Step 3 Click **Apply**.

9.2.6 Configuring Broadcast

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

9.2.6.1 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 9-15 Broadcast content

Type	Enable	Play Mode	Audio Content	Interval sec (1-20)	Duration sec (1-3600)
Small Vehicle Parked in Large Vehi...		Text	Small Occupy Large	2	60
Occupied by Non-allowlist Vehicle		Text	Not Allow Occupy	2	60
Parking Over Line		Text	Over Line	2	60
Allowlist Vehicle		Text	Allow List In	2	60
Available Space		Text	no car	2	60
Occupied Space		Text	has car	2	60
Illegal Parking		Text	No parking area, please	2	60

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

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 "9.2.6.3 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**.

9.2.6.2 Volume/Encoding

Configure the volume for voice broadcast.

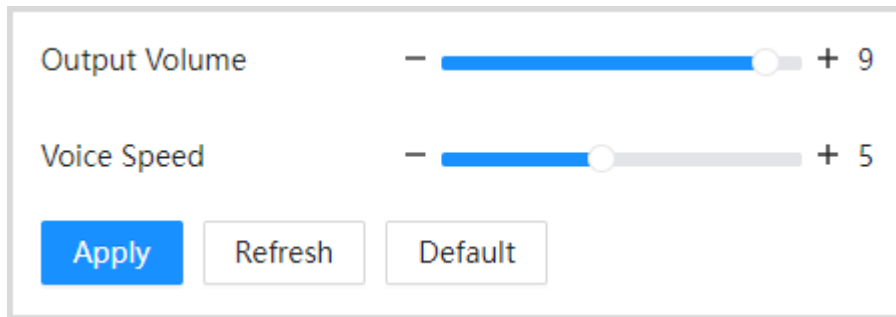


This function is only available for select models.

Procedure

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

Figure 9-16 Volume/Encoding Settings



Step 2 Configure the parameters.

Table 9-7 Parameter description

Parameter	Description
Audio Output Type	Two types are available, including camera audio output and camera speaker.
Voice Speed	The speed for the voice broadcast.

Step 3 Click **Apply**.

9.2.6.3 Audio File

Upload audio files for broadcast content.

Procedure

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

Figure 9-17 Audio file

Requirement for uploading audio:

1. Size does not exceed 1024k.
2. Audio Channel: Mono; Bit Depth: 16 bit; Sample Rate: 8KHZ/16KHZ/32KHZ/48KHZ/64KHZ
3. Audio format can only be wav.

No.	Name	Size(KB)	Play	Download	Delete
1	alarm.wav(Default)	107			

< 1 >
100 / page

Step 2 Click **Upload** 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.

9.2.7 Device Test

You can view and test parking event, voice broadcast, external light settings and status, and abnormal configuration. You can also export device information.

Procedure

Step 1 Select > **ANPR** > **Device Test** > **Device Test**.

Figure 9-18 Device test

Test Event

Parking Space No.

Occupied Space ☐ Parking Over Line ☐ Occupied by Non-allowlist Vehicle ☐ Small Vehicle Parked in Large Vehicle's Space

Available Space

Test Voice Broadcast

Built-in Light

External Light

Light Status

No.	Light Type	Color	Action	Source IP Address
1	Built-in Light	Green	Always On	
2	External Light1	Green	Always On	
3	External Light2	Green	Always On	
4	External Light3	Green	Always On	

Check for Abnormal Co...

Export Device Info

Export ☐ Encrypt Log Backup

Step 2 Test if different functions are working normally.

Table 9-8 Parameter description

Parameter	Description
Parking Space No.	Select the parking space that need to be tested.
Occupied Space	Enter a plate number, click Test to trigger capture, and you can view the snapshot. You can also select the event from Parking Over Line, Occupied by Non-allowlist Vehicle or Small Vehicle Parked in Large Vehicle's Space .
Available Space	Click Test to report in empty parking spaces to the platform.
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.
Built-in Light	Configure the light color and status, and then click Test to test the control of lights.
External Light	
Light Status	Light Status refreshes every time you test the light. Source IP is the IP address which sends out the test command.
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.

9.3 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 brightness, contrast, saturation, and more.

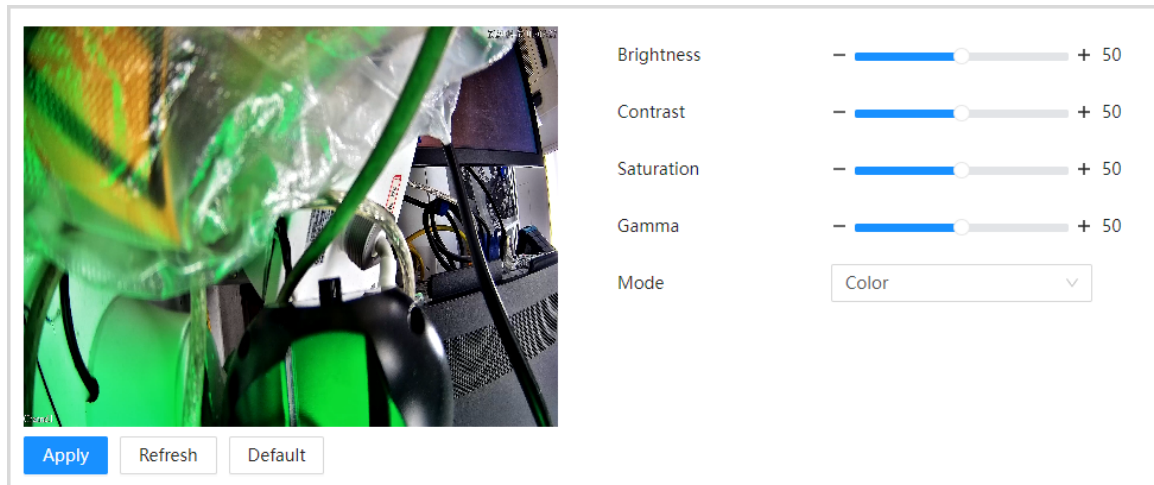
9.3.1.1 General Parameters

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

Procedure

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

Figure 9-19 General



Step 2 Configure the parameters.

Table 9-9 Parameter description

Parameter	Description
Brightness	Adjust the overall image brightness. Change the value when the image is too bright or too dark. The bright and dark areas will have equal changes. The image becomes blurry when the value is too high. The recommended value is from 40 to 60. The range is from 0 to 100. It is 50 by default. The higher the value is, the brighter the image becomes.
Contrast	Change the value when the image brightness is proper but contrast is not enough. • If the value is too big, the dark area is likely to become darker, and the bright area is likely to be overexposed. • The picture might be blurry if the value is set too small. The recommended value is from 40 to 60, and the range is from 0 to 100. It is 50 by default. The higher the value is, the more obvious the contrast between the bright area and dark area will become.
Saturation	Adjust the color vividness, and will not influence the image overall brightness. • The image becomes too flamboyant if the value is too big. • The image is not flamboyant enough if the value is too small. The recommended value is from 40 to 60, and the range is from 0 to 100. It is 50 by default. The higher the value is, the more flamboyant the image becomes.
Gamma	Adjust the image brightness level. The higher the value is, the brighter and blurrier the image becomes.
Mode	Select image display mode. The image changes to colorful when the ambient brightness is higher than the preset value, and changes to black and white when lower if you select B/W.

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 9-10 Parameter description

Parameter	Description
3D NR	
3D NR	Click  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 Settings	Select from WDR , BLC , HLC and SSA to adjust the picture effect.
WDR	Drag the slider to adjust WDR (wide dynamic range) value, which helps provide clear video images in bright and dark light.
Exposure	
Mode	Select the way of adjusting exposure mode. You can select from Manual , and Auto .
Exposure Compensation	You can drag the slider to adjust the exposure compensation to improve the image brightness in backlighting situations.
Shutter	You can select the shutter value, or select Custom , and then set the shutter range.  You need to set shutter when setting Mode to Manual .
Shutter Range	Set the time range for shutter.  You need to set shutter range when setting Custom to Shutter .
Gain	Set the value range for gain.  You need to set gain scope when setting Mode to Manual .

Parameter	Description
WB	
Mode	Set a scene mode to adjust the image to its best status.

Step 3 Click **Apply**.

9.3.2 Setting Encode Parameters

This section introduces video parameters, such as video stream, video OSD, and 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**.

Figure 9-20 Video stream

Main Stream	Sub Stream
Encoding Mode: H.264M	Enable: ☒
Resolution: 2688*1520(2688x1520)	Encoding Mode: H.264M
Frame Rate (FPS): 20	Resolution: 704*480(D1)
Bit Rate Type: CBR	Frame Rate (FPS): 20
Reference Bit Rate: 1743-13946(Kb/S)	Bit Rate Type: VBR
Bit Rate: 2048 (Kb/S)	Quality: 5
I Frame Interval: 40 (20-150)	Reference Bit Rate: 144-1153(Kb/S)
SVC: 1(off)	Max Bit Rate: 768 (Kb/S)
Smooth Stream: <input type="range"/> 100 [Clear<->Smooth]	I Frame Interval: 40 (20-150)
Watermark: ☒	SVC: 1(off)
Watermark String: DigitalCCTV	Smooth Stream: <input type="range"/> 100 [Clear<->Smooth]
Apply Refresh Default	

Step 2 Configure the parameters.

Table 9-11 Parameters description

Parameter	Description
Encode Mode	Currently it only supports H.264B, H.264M, H.264H, H.265, and MJPEG.

Parameter	Description
Resolution	Select the video resolution.  The resolution of sub stream cannot be greater than that of the main stream.
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	We recommend that you use VBR in constantly changing scenes, and CBR in stable scenes. ● VBR : Variable bitrate. The bitrate automatically adjusts with changes in scene complexity. This is useful for providing clear video when the scene is complex, and saving the bandwidth when the scene is simple. ● CBR : Constant bitrate. The bitrate barely changes with the scene complexity. When the scene is complex, the video might not be clear enough. When the scene is simple, more unnecessary bandwidth might be consumed.  Image quality can only be set in VBR mode.
Quality	This parameter can be configured only when the Bit Rate Type is set as VBR. The better the quality is, but the bigger the required bandwidth will be.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the Bit Rate Type is set to VBR. You can select the value of the Max Bit Rate according to the Reference Bit Rate value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
I Frame Interval	Frame or time interval between two I frames. The bigger the interval, the smaller space taken by the decompressed video. The system default is set twice as big as frame rate.
SVC	Scalable video codec (SVC) contains 3 layers providing different frame rates. The higher the layer, the greater the video quality.
Smooth Stream	It is designed for fluid viewing of live video. The higher the value, the smoother the video.
Watermark	Set the watermarks, which will be added into videos of the camera. ● Select Watermark to enable the watermark adding. ● Watermark String is DigitalCCTV by default. ● The watermark character can only consist of number, letter, underline, and maximum length contains 85 characters.

Step 3 Click **Apply**.

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 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.

9.3.2.2.4 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 Select the font color according to your needs.
- Step 5 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 9-12 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: ● 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	
	● 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 9-13 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.
HTTP Port	Hypertext transfer protocol port. The value is 80 by default.
RTSP Port	- Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. - When the URL format requires RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. - When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: <pre>rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</pre> Among that: - Username: The username, such as admin. - Password: The password, such as admin. - IP: The device IP, such as 192.168.1.112. - Port: Leave it if the value is 554 by default. - Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. - Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: <pre>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&subtype=1</pre> If username and password are not needed, then the URL can be: <pre>rtsp://ip:port/cam/realmonitor?channel=1&subtype=0</pre>
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 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 9-14 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**.

9.4.4 Platform Access

9.4.4.1 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**.

9.4.4.2 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 9-21 ITSAPI

Step 3 Configure the parameters.

Table 9-15 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. • 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**.

9.4.5 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 9-16 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 Exception

Abnormality includes IP conflict and Offline.

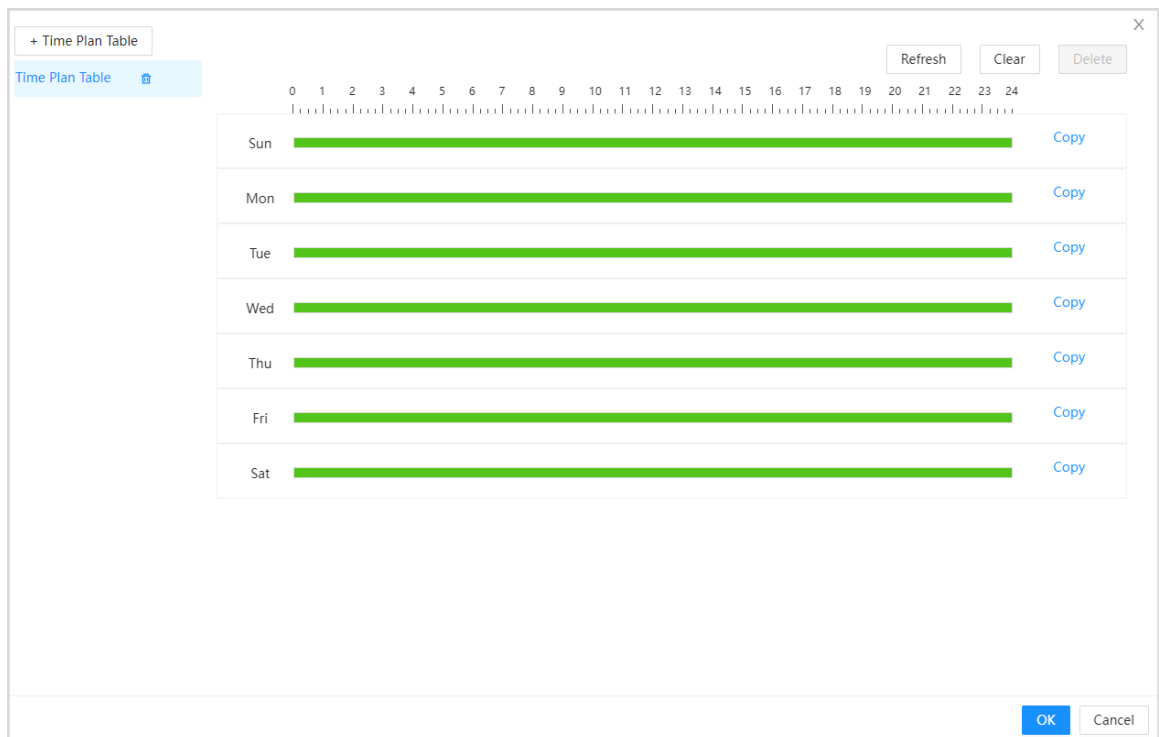
Select  > **Event** > **Exception**. Click  to enable detection of offline or IP conflict, and then click **Apply**.

9.5.2 Setting Video Detection

Procedure

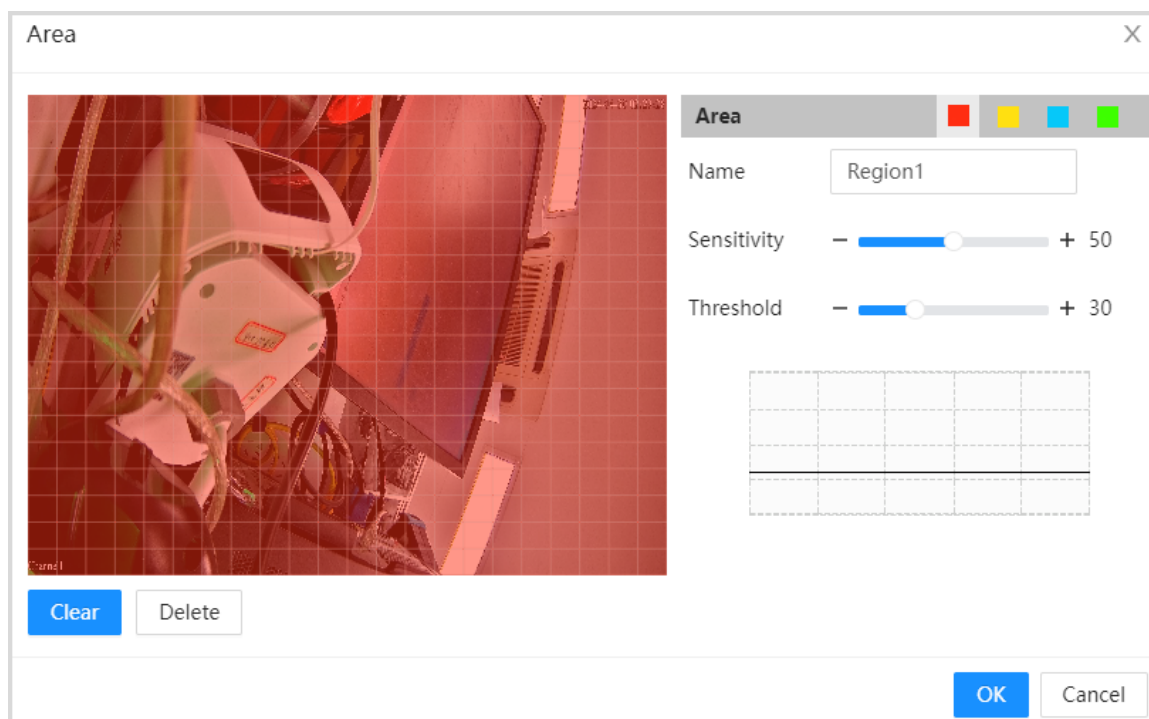
- Step 1 Select  > **Event** > **Exception**.
- Step 2 Click  next to **Enable** to enable video detection function.
- Step 3 Set anti-dither time and schedule.
1. Click **Add Schedule**.
 2. Drag on the timeline to set the arming periods. Alarms will be triggered in the green period.

Figure 9-22 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 Click **Setting** to set the video detection area.

Figure 9-23 Set video detection area



Step 5 Click ☐ to enable linkage snapshot, and then you can view the capture on the **Live** page.

Step 6 Click **Apply**.

9.5.3 Subscribing Alarm

9.5.3.1 Alarm Types

Table 9-17 Description of alarm types

Alarm Type	Description	Preparation
Motion Detection	An alarm is triggered when the device detects motion.	-
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.
Security Exception	An alarm is triggered when the device detects malicious attacks.	The security exception is enabled. For details.
Illegal Parking	An alarm is triggered when the device detects illegal parking	-

9.5.3.2 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 9-24 Subscribe to alarms

Alarm 

Subscribe Alarm 

☐ All Types

☐ Invalid Access ☐ Security Excep... ☐ Motion Detect... ☐ Illegal Parking

Play Alarm Tone 

No.	Time	Alarm Type	Alarm Channel	Source IP Address
 No data				

Clear

Step 2 Click  next to **Alarm**.

Step 3 Select one or more 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 System

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

9.6.1 General Parameters

9.6.1.1 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 9-18 Parameter description

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

Step 3 Click **Apply**.

9.6.1.2 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 9-19 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 .

Parameter	Description
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**.

9.6.2 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.

9.6.2.1 User

9.6.2.1.1 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 9-25 Add user (system)

Add

X

Username

Password

Confirm Password

Group

admin

▼

Remarks

System

Live

Restricted Login

☒ All

☒ Account

☒ File Backup

☒ Network

☒ Security

☒ System

☒ Storage

☒ Peripheral

☒ Maintenance

☒ System Info

☒ Event

☒ Camera

☒ Manual Control

Apply

Cancel

Figure 9-26 Add user (restricted login)

Step 3 Configure the parameters.

Table 9-20 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	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. ● 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.

9.6.2.1.2 Resetting Password

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

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?**

9.6.2.2 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 9-27 Add group

The 'Add' dialog box contains the following elements:

- Group:** A text input field.
- Remarks:** A text input field.
- Tabs:** 'System' (selected) and 'Live'.
- Permissions:** A list of checkboxes under the 'System' tab:
 - ☒ All
 - ☒ System
 - ☒ Storage
 - ☒ Peripheral
 - ☒ Maintenance
 - ☒ System Info
 - ☒ Event
 - ☒ Camera
 - ☒ Manual Control
 - ☒ File Backup
 - ☒ Network
 - ☒ Security
- Buttons:** 'Apply' and 'Cancel' at the bottom right.

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.

9.6.2.3 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 9-28 Add ONVIF user

The 'Add' dialog box contains the following elements:

- Username:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Group:** A dropdown menu with 'admin' selected.
- Buttons:** 'OK' and 'Cancel' at the bottom right.

Step 3 Configure the parameters.

Table 9-21 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 Security

9.7.1 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.

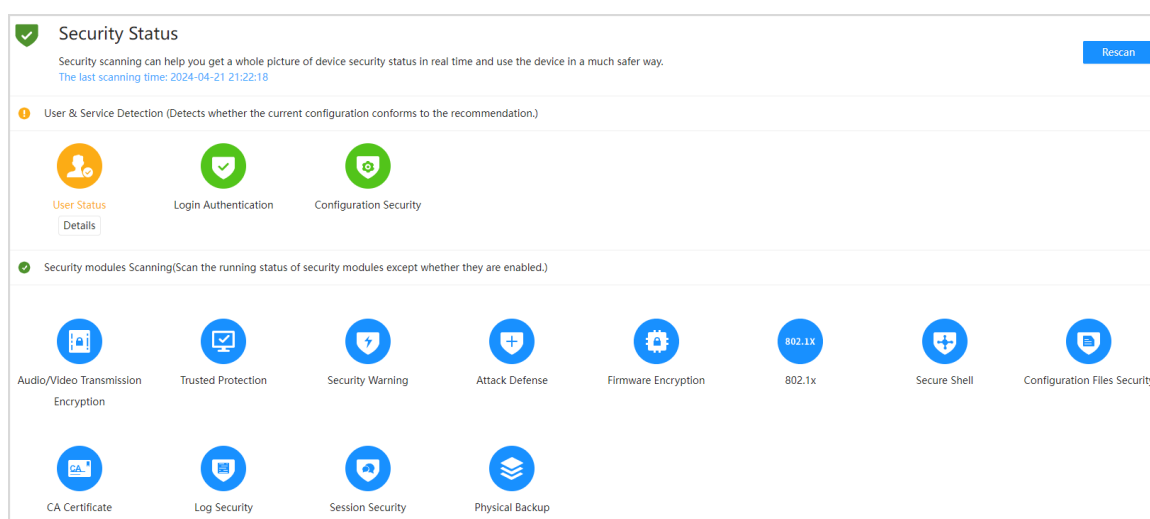
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing 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

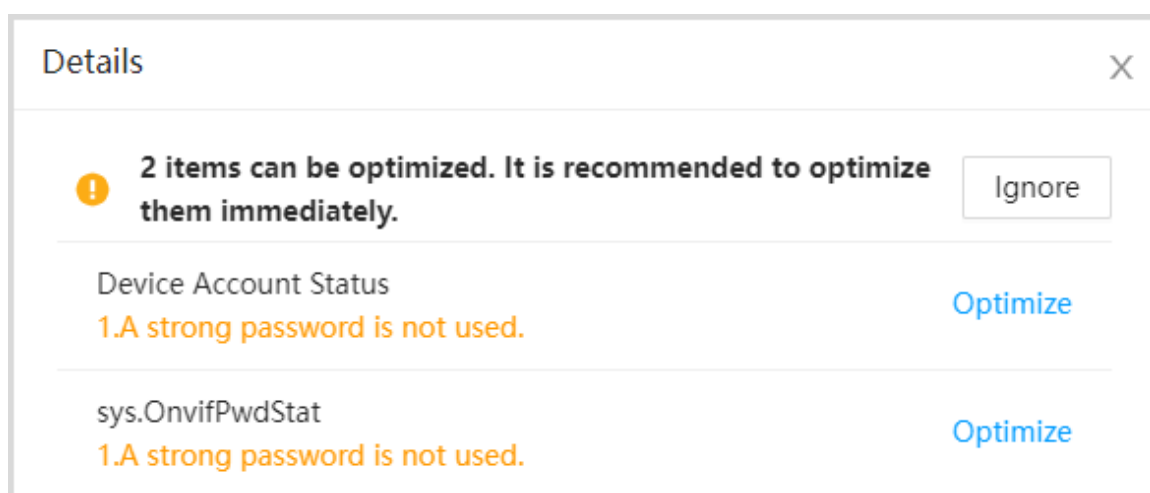
After scanning, different results will be displayed in different colors. Yellow indicates that the security modules are abnormal, and Green indicates that the security modules are normal.

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



9.7.2 System Service

9.7.2.1 802.1x

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

NIC Name

NIC1

Enable



Authentication M...

PEAP

CA Certificate



Username

none

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
☐ 1			2053-09-07 08:49:53	General Device ITC CA	General Device Root CA	
☐ 2			2059-05-23 11:18:27	General Device Root CA	General Device Root CA	

Apply

Refresh

Default

- 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 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.

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☐ 1			2053-09-07 08:49:53	General Device ITC CA	General Device Root CA	
☐ 2			2059-05-23 11:18:27	General Device Root CA	General Device Root CA	

[Certificate Management](#)

Step 4 Click **Apply**.

9.7.2.2 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.

Figure 9-33 HTTPS

Enable: ☒

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Auto Redirect to ...: ☐

*Select a device certificate

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
☒ 1			2054-04-09 18:11:11	47	General Device ITC CA	HTTPS, RTSP over TLS

[Certificate Management](#)

Step 4 Click **Apply**.

9.7.3 Attack Defense

9.7.3.1 Firewall

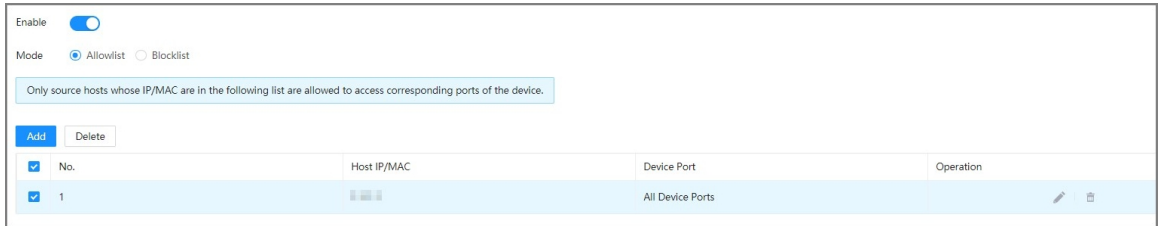
Configure the firewall to limit access to the camera.

Procedure

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

Step 2 Click  to enable the function.

Figure 9-34 Firewall



Enable ☒

Mode ☒ Allowlist ☐ Blocklist

Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

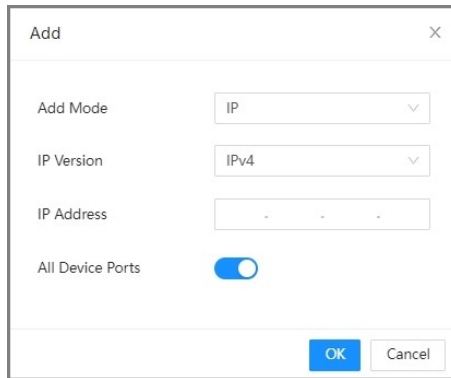
No.	Host IP/MAC	Device Port	Operation
1		All Device Ports	 

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



Add

Add Mode

IP Version

IP Address

All Device Ports ☒

Step 5 Click **Apply**.

Related Operations

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

9.7.3.2 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**.

9.7.3.3 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**.

9.7.4 CA Certificate

9.7.4.1 Installing Device Certificate

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

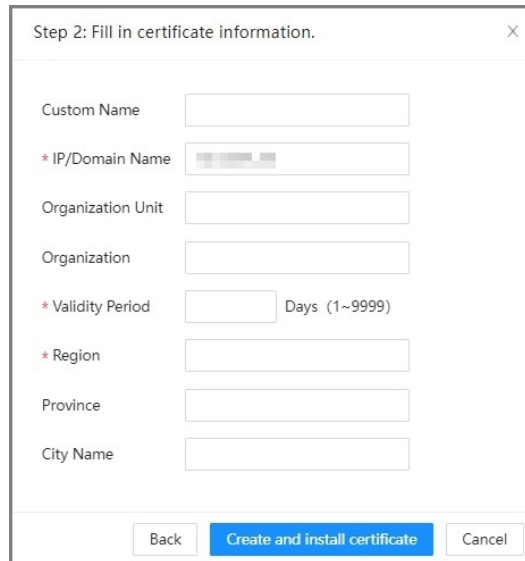
9.7.4.1.1 Creating Certificate

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.

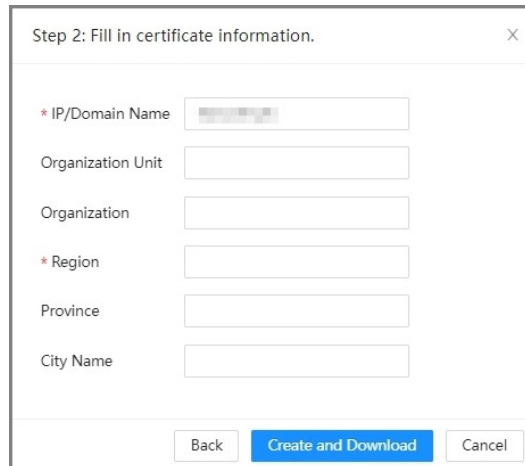
9.7.4.1.2 Applying for and Importing CA Certificate

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)

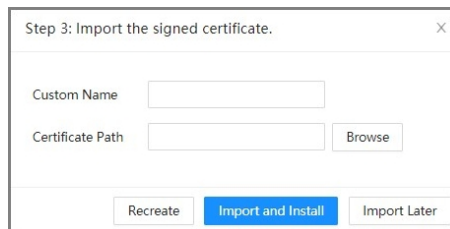
A dialog box titled "Step 2: Fill in certificate information." with a close button (X) in the top right corner. It contains several text input fields: "* IP/Domain Name", "Organization Unit", "Organization", "* Region", "Province", and "City Name". The fields for "* IP/Domain Name" and "* Region" have a small lock icon on the left. At the bottom, there are three buttons: "Back", "Create and Download" (highlighted in blue), and "Cancel".

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

A dialog box titled "Step 3: Import the signed certificate." with a close button (X) in the top right corner. It contains two text input fields: "Custom Name" and "Certificate Path". To the right of the "Certificate Path" field is a "Browse" button. At the bottom, there are three buttons: "Recreate", "Import and Install" (highlighted in blue), and "Import Later".

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.

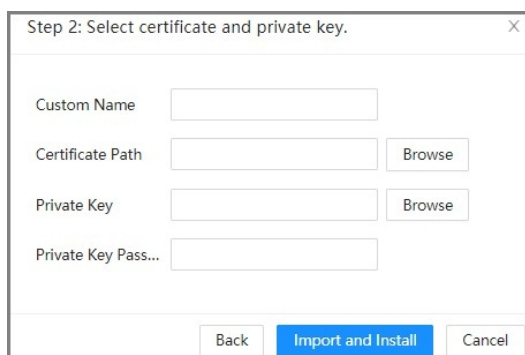
9.7.4.1.3 Installing Existing Certificate

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

A dialog box titled "Step 2: Select certificate and private key." with a close button (X) in the top right corner. It contains four input fields: "Custom Name", "Certificate Path", "Private Key", and "Private Key Pass...". The "Certificate Path" and "Private Key" fields have "Browse" buttons next to them. At the bottom, there are three buttons: "Back", "Import and Install" (highlighted in blue), and "Cancel".

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.

9.7.4.2 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.

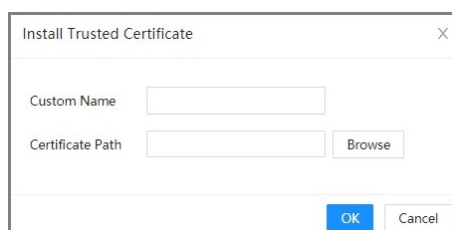
Procedure

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

A dialog box titled "Install Trusted Certificate" with a close button (X) in the top right corner. It contains two input fields: "Custom Name" and "Certificate Path". The "Certificate Path" field has a "Browse" button next to it. At the bottom, there are two buttons: "OK" (highlighted in blue) and "Cancel".

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.

9.7.5 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 9-22 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.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There might be safety risk if this service is not enabled.

Area	Parameter	Description
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "9.7.4 CA Certificate".

Step 3 Click **Apply**.

9.7.6 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.

9.7.6.1 Security Exception

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

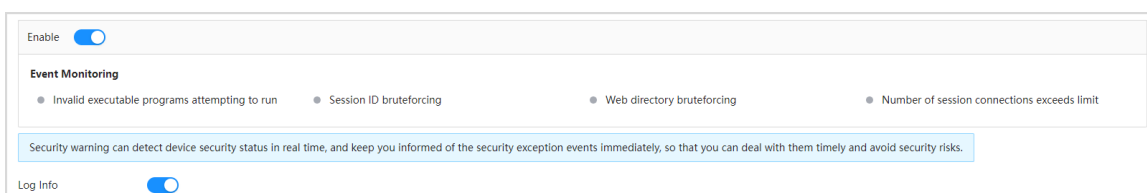
Procedure

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



Log Info : After it is enabled, the camera will generate a log when an event occurs.

Step 4 Click **Apply**.

9.7.6.2 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.

Log Info : After it is enabled, the camera will generate a log when an event occurs.

Step 4 Click **Apply**.

9.8 Maintenance Center

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

9.8.1 One-click Diagnosis

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

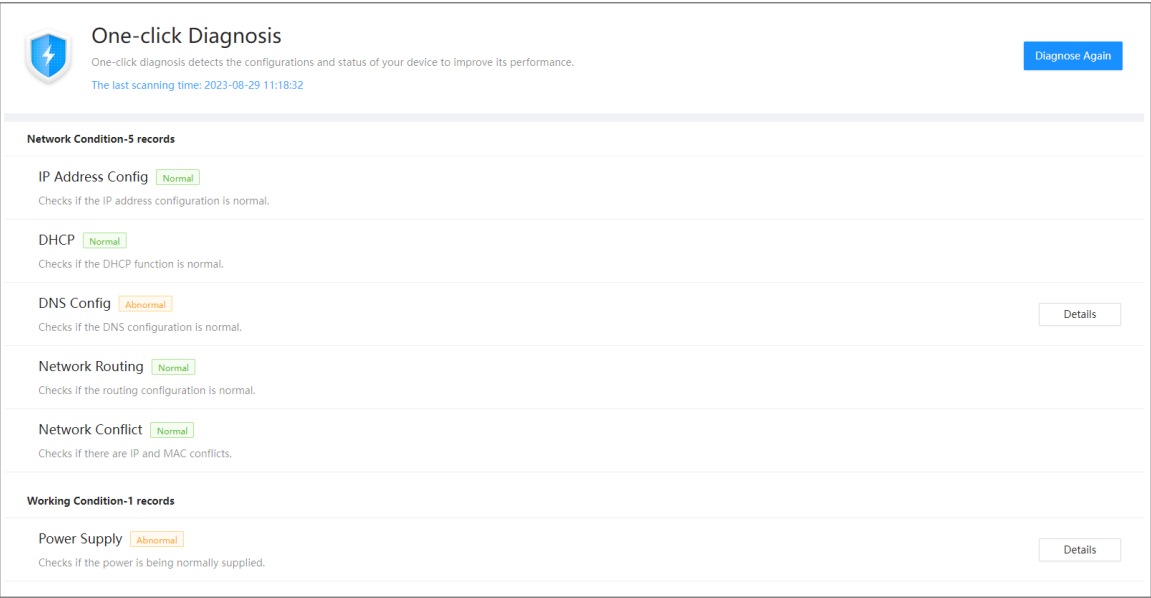
Procedure

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

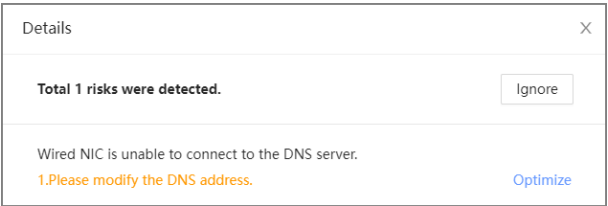


Related Operations

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



9.8.2 System Information

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

9.8.2.1 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.

9.8.2.2 Online User

Select  > **System Info** > **Online User** to view all the online users logging in to the webpage.
Click **Refresh** to get the latest status.

9.8.2.3 Legal Info

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

9.8.3 Log

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

9.8.3.1 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.
 - **Event Operation** : Includes the start time and end time of events.
 - **Record** : Includes file access, file access error, and file search.
 - **Account** : Includes login, logout, adding a user, deleting a user, editing a user, adding a group, deleting a group, and editing a group.
 - **Security** : Includes password resetting and IP filter.
- Step 3 Click **Search**.
- Search results are displayed.

Figure 9-45 Log

Search Time Range

2023-03-13 10:28:29

→ 2023-03-14 10:28:29

⊞

Type

All

▼

Search

Backup

☐ Encrypt Log Backup

Found253record(s) Time 2023-03-13 10:28:29--2023-03-14 10:28:29

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	⊞

<

1

2

3

>

100 / page ▼

Go to

Page

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.

9.8.3.2 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**.

9.8.4 Manager

9.8.4.1 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.
- 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.

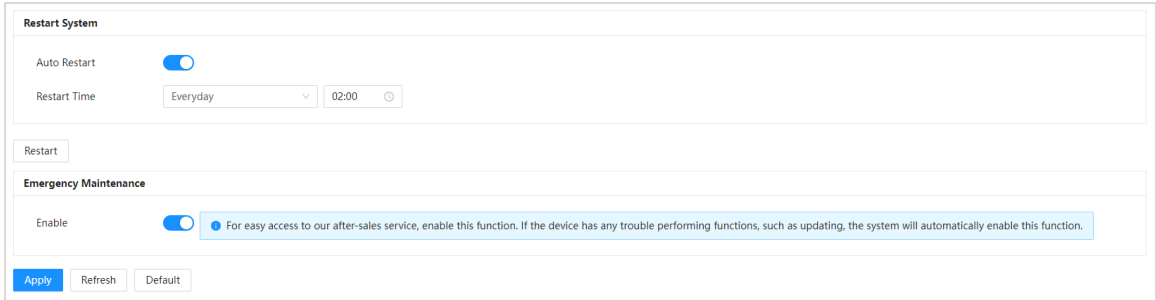
9.8.4.2 Maintenance

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 9-46 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.
- Enable **Emergency Maintenance** so that when the device cannot start properly, maintenance tools can be used to access the device for troubleshooting.

Step 3 Click **Apply**.

9.8.4.3 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.

9.8.4.4 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.

9.8.5 Update

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

Procedure

- Step 1 Select  > **System** > **Update**.
- Step 2 Update the camera in the following ways.

- Use an update file.
 1. Click **Import**.
 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.

9.8.6 Advanced Maintenance

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



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

Procedure

- Step 1 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 9-47 Packet capture

Packet Capture

NIC	Device Address	IP 1: Port 1	IP 2: Port 2	Packet Sn...	Packet Sn...
eth0		Optional	Optional	Optional	Optional

0.00MB

Network Test

Destination Address: **Test**

Data Packet Size: Byte (64-4096)

Test Result: **Copy**

- ◇ **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 9-48 Network test results

Network Test

Destination Address: **Test**

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 ---

Copy

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 Security Recommendation

Account Management

1. Use complex passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters: upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

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

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. **Enable Allowlist**

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

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

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