

Spotter Nano

Web Operation Manual



V1.0.0






Foreword

General

This manual introduces the web operations of the Spotter Nano (hereinafter referred to as the "Camera").

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.
 NOTE	Provides additional information as a supplement to the text.
 TIPS	Provides methods to help you solve a problem or save time.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2025

Privacy Protection Notice

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

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

Foreword.....	I
1 Webpage Introduction.....	1
1.1 Device Initialization.....	1
1.2 Device Login.....	3
1.3 Logout.....	5
1.4 Resetting Password.....	5
1.5 Functions.....	6
2 Local.....	9
3 Configuration Wizard.....	10
3.1 ANPR Mode (without Radar).....	10
3.2 ANPR Mode (with Radar).....	15
3.3 Road Monitoring Mode.....	18
4 Live.....	19
4.1 Live View.....	20
4.2 Frequently Used Functions.....	21
4.2.1 Zoom and Focus.....	21
4.2.2 AI Configuration.....	21
4.2.3 Illuminator Adjustment.....	21
4.2.4 Picture Parameter.....	22
4.3 Live View Function Bar.....	23
4.4 Plate Number Recognition.....	24
4.5 Vehicle Snapshot.....	24
4.6 Event List.....	24
5 Camera.....	25
5.1 Configuring Camera Attributes.....	25
5.1.1 Configuring General Parameters.....	25
5.1.2 Configuring Shutter.....	26
5.1.3 Configuring Metering Zone.....	28
5.1.4 Configuring Focus.....	28
5.1.5 Configuring LDC.....	29
5.2 Configuring Encode Parameters.....	30
5.2.1 Configuring Video Parameters.....	30
5.2.2 Configuring Video OSD.....	32
5.2.3 Configuring Interest Area.....	33
6 Radar.....	34
7 Playback.....	35
8 Search.....	36

8.1	Picture Query.....	36
8.1.1	Searching for SD Card Image.....	36
8.1.2	Local Image.....	37
8.2	Flow Query.....	38
8.3	Search Video.....	38
8.3.1	Recording.....	39
8.3.2	Watermark.....	40
9	ITC.....	41
9.1	Configuring Smart Plan.....	41
9.1.1	ANPR Mode.....	41
9.1.2	Road Monitoring Mode.....	47
9.2	Intelligent Analysis.....	49
9.2.1	Recognition.....	49
9.2.2	Advanced Settings.....	50
9.3	Configuring Image.....	50
9.3.1	Configuring Picture Parameter.....	50
9.3.2	Configuring Snapshot Composition.....	52
9.3.3	Configuring Cutout.....	53
9.4	Traffic Flow Statistics.....	53
9.4.1	Flow Data.....	54
9.4.2	Traffic Flow.....	54
9.4.3	Pedestrian Flow.....	54
9.4.4	Flow Control.....	54
9.5	Configuring OSD.....	55
9.5.1	Configuring Original Picture OSD.....	55
9.5.2	Configuring Combination Picture OSD.....	56
9.6	Configuring Blocklist and Allowlist.....	56
9.6.1	Allowlist.....	56
9.6.2	Blocklist Search.....	58
9.7	Smart Restore Factory Settings.....	58
10	Network Settings.....	59
10.1	TCP/IP.....	59
10.2	Port.....	60
10.2.1	Configuring Port.....	60
10.2.2	Configuring ONVIF.....	61
10.3	Auto Registration.....	62
10.4	Multicast.....	63
10.5	Email.....	63
10.6	Basic Services.....	65
10.7	ITSAPI.....	65

10.8 Network Proxy.....	67
11 Event.....	68
11.1 Alarm.....	68
11.1.1 Enabling Alarm-in and Alarm-out Ports.....	68
11.1.2 Alarm-out Ports.....	69
11.2 Exception.....	70
11.2.1 Setting SD Card Exception.....	70
11.2.2 Setting Network Exception.....	71
11.2.3 Setting Vehicle Blocklist.....	72
11.2.4 Setting Unlicensed Vehicle.....	73
11.2.5 Setting Intrusion.....	74
12 Report.....	75
13 Peripheral.....	76
14 Storage.....	80
14.1 Storage Spot Config.....	80
14.2 Local Storage.....	80
14.3 FTP.....	81
14.4 Platform Server.....	82
14.5 Record Control.....	83
15 System.....	85
15.1 General.....	85
15.1.1 General Settings.....	85
15.1.2 Date.....	86
15.2 Account.....	88
15.2.1 User.....	88
15.2.2 Adding User Groups.....	90
15.2.3 Clearing User.....	91
15.2.4 ONVIF User.....	91
16 Security.....	93
16.1 Security Status.....	93
16.2 System Service.....	94
16.2.1 802.1x.....	94
16.2.2 HTTPS.....	95
16.3 Attack Defense.....	96
16.3.1 Firewall.....	96
16.3.2 Account Lockout.....	97
16.3.3 Anti-DoS Attack.....	97
16.4 CA Certificate.....	98
16.4.1 Installing Device Certificate.....	98
16.4.2 Installing Trusted CA Certificate.....	100

16.5	A/V Encryption.....	101
16.6	Security Warning.....	102
16.6.1	Security Exception.....	102
16.6.2	Illegal Login.....	103
17	Maintenance Center.....	104
17.1	One-click Diagnosis.....	104
17.2	System Information.....	105
17.2.1	Version Information.....	105
17.2.2	Online User.....	105
17.2.3	Running Status.....	106
17.2.4	Legal Information.....	106
17.3	Log.....	106
17.3.1	System Log.....	106
17.3.2	Remote Log.....	107
17.4	Maintenance Management.....	107
17.4.1	Requirements.....	107
17.4.2	Maintenance.....	107
17.4.3	Import/Export.....	108
17.4.4	Default.....	109
17.5	Update.....	109
17.6	Advanced Maintenance.....	110
Appendix 1	Security Recommendation.....	112

1 Webpage Introduction

After mounting the Camera, power on the Camera, connect it to the network, and configure its settings. Then, you can obtain the desired detection results.



The actual page might vary depending on the model you purchased and the version of software. The figures in this manual are only for reference, and might differ from the actual page.

1.1 Device Initialization

The Camera is delivered in the uninitialized status. You need to initialize the Camera and change its default password before it can be used.

Procedure

Step 1 Connect the Camera to the network.

1. Connect the Camera to computer over the Ethernet cable.
2. Keep the IP address of the computer and the camera on the same network segment.

The network segment can be set to 192.168.1.X, but cannot be the same as the factory default IP of the Camera (192.168.1.108).

3. Execute ping `***.***.***.***` (device IP) command on computer to check the network connection.

Step 2 Enter the IP address of the Camera (192.168.1.108) in the browser address bar, and press the Enter key to log in to the webpage of the Camera.

Step 3 On the **Region Setting** page, configure **Language** and **Video Standard**. Then, click **Next**.

Figure 1-1 Region setting

The screenshot shows the 'Region Setting' page of a camera's web interface. At the top, there are four navigation links: 'Region Setting' (with a globe icon and highlighted), 'Time Zone Setting' (with a clock icon), 'Password Settings' (with a lock icon), and 'Online Update' (with an upload icon). The main content area is a white box containing three configuration items, each with a label and a dropdown menu: 'Language' is set to 'English', 'Video Standard' is set to 'PAL', and 'Plate Algorithm' is set to 'Oversea ALG'. At the bottom center of this white box is a prominent blue button labeled 'Next'.

Step 4 On the **Time Zone Setting** page, configure date & time parameters. Then, click **Next**.

Figure 1-2 Time zone setting

The screenshot shows the 'Time Zone Setting' page. At the top, there are navigation links: 'Region Setting', 'Time Zone Setting' (active), 'Password Settings', and 'Online Update'. The main content area contains the following settings:

- Date Format: YYYY-MM-DD
- Time Zone: (UTC+00:00) Dublin, Edinburgh, Lisbon, London
- System Time: 2023-08-28 11:25:34 (with a calendar icon and a 'Sync PC' button)
- Will be modified as: 2023-08-28 03:25:34

At the bottom, there are two buttons: 'Back' and 'Next'.

Step 5 On the **Password Settings** page, enter your new password.

Step 6 Select the **Email Address** checkbox, and then enter your email address. This helps you reset your password when your password is lost or forgotten.

Step 7 Click **Next**.

Figure 1-3 Password setting

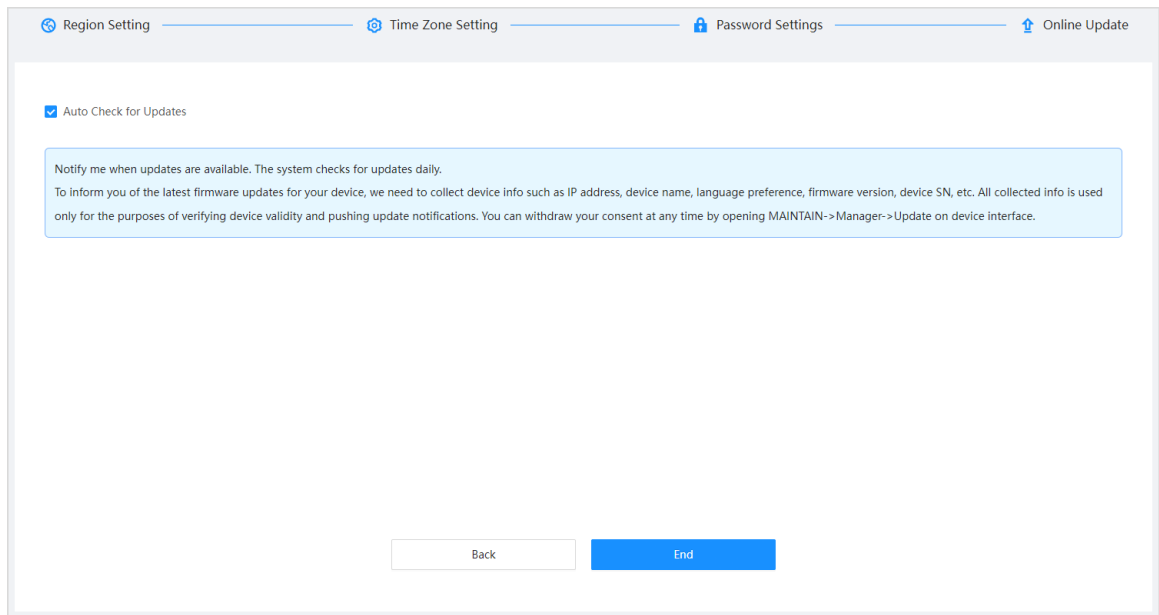
The screenshot shows the 'Password Settings' page. At the top, there are navigation links: 'Region Setting', 'Time Zone Setting', 'Password Settings' (active), and 'Online Update'. The main content area contains the following settings:

- Username: admin
- Password: [masked with dots]
- Confirm Password: [masked with dots]
- Email Address: [masked]@qq.com

At the bottom, there are two buttons: 'Back' and 'Next'.

Step 8 On the **Online Upgrade** page, select **Auto Check for Updates** and click **End**.

Figure 1-4 Online upgrade



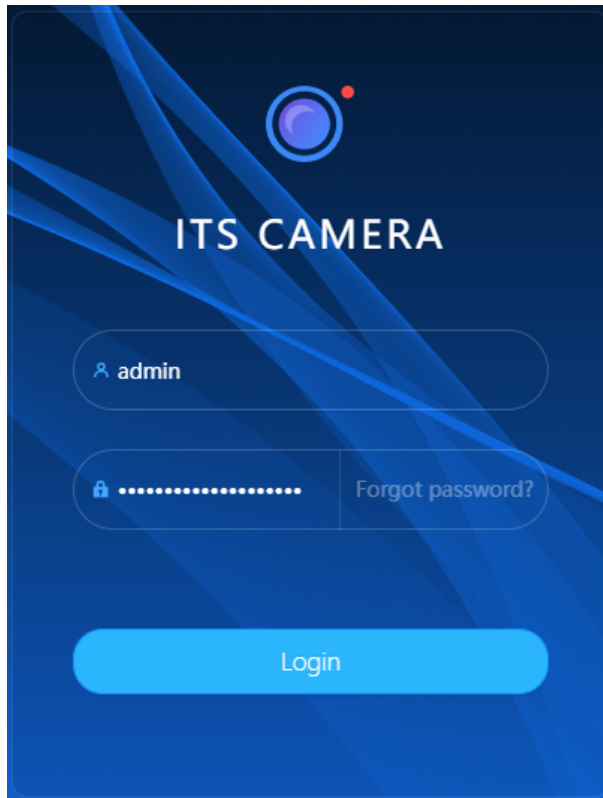
Step 9 On the **Login** page, enter the username (admin) and the password that you set, and then click **Login**.

1.2 Device Login

Procedure

- Step 1** Enter the IP address of the Camera in the browser address bar, and then press Enter.
- Step 2** Enter username and password on the login page, and then click **Login**.

Figure 1-5 Login



- A box pops up when the username or password is incorrect.
- If you enter an invalid username or password five times, the account will be locked for five minutes.

Figure 1-6 Home page

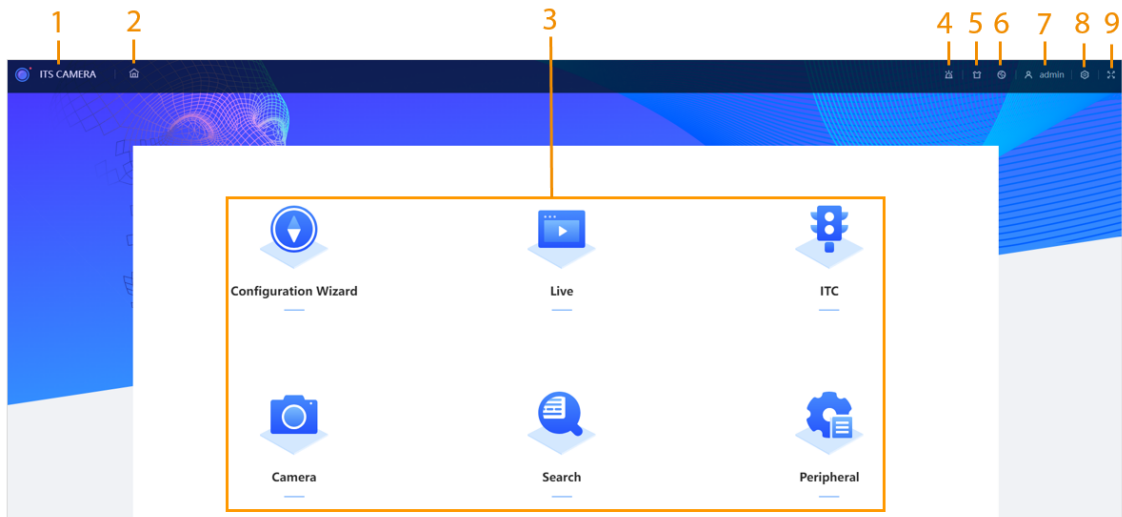


Table 1-1 Parameter description

No.	Description
1	The name of the device.

No.	Description
2	Home.
3	Functions module.
4	Alarm subscription. You can enable the alarm function, select events that trigger alarm, and set the alarm tone.
5	Theme.
6	Language. You can change the language of the webpage.
7	Account. You can restart the device and log out.
8	Functions. You can view all functions of the device.
9	Exit full screen mode.

Related Operations

If you forget password, click **Forgot password?**, and you can reset the password through the email address that is set during the initialization. For details, see "1.4 Resetting Password".

1.3 Logout

Click **Logout** at the upper-right corner of the webpage to log out.

You can enter the username and password to log in again.

1.4 Resetting Password

You can reset your password through email when it is lost or forgotten. Make sure that your email is correctly entered during initialization.

Procedure

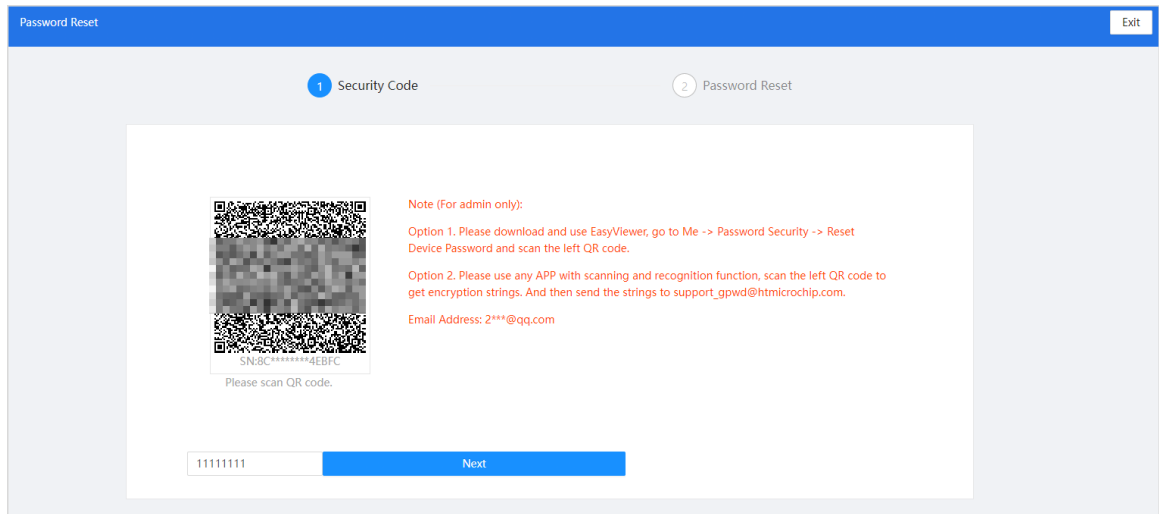
- Step 1 Enter the IP address of the Camera in the browser address bar, and then press Enter.
- Step 2 On the login page, click **Forgot password?**.
- Step 3 In the pop-up dialog box, click **OK**.
- Step 4 Scan the QR code according to the page prompt, and send the scanning result to the designated email to acquire security code.



Scan the actual QR code. Do not scan the QR code in this manual.

- Step 5 Enter the security code that you received in the text box of **Security code**.

Figure 1-7 Reset password



Step 6 Click **Next**.

Step 7 Configure **Password** , and then enter your new password again in **Confirm Password**.



- The new password must consist of 8–32 characters, and contain at least two types from upper cases, lower cases, numbers and special characters (excluding ' " ; : and &).
- The new password must be the same as the **Confirm Password**. Follow the password security notice to set a high-security password.

Step 8 Click **OK**.

1.5 Functions

You can view real-time video captured by the Camera, set detection rules of number plate recognition and traffic violations, and play back video recordings and snapshots to track back events (if any). This chapter introduces each function.

Figure 1-8 Navigation bar

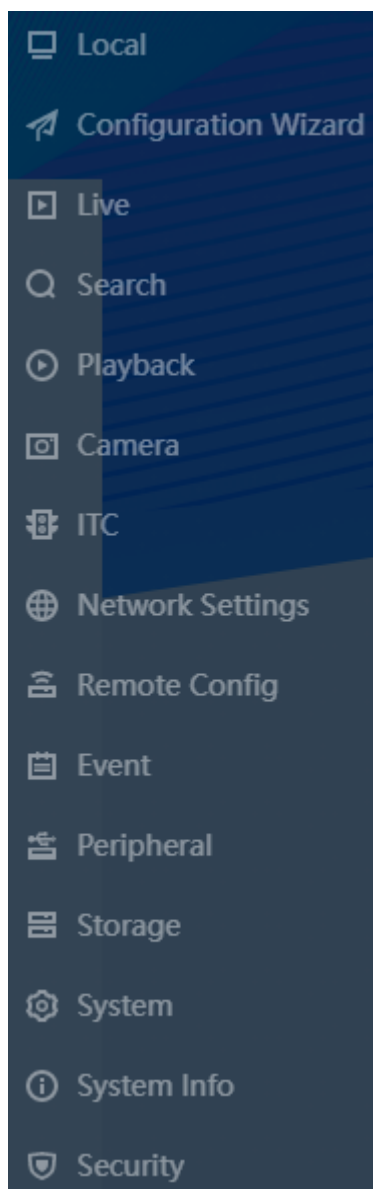


Table 1-2 Function introduction

Function	Description
Local	You can configure the naming format of picture and storage path.
Configuration Wizard	You can configure the scene for capture, and use various functions to help you with different installation scenarios.
Live	Displays real-time videos and images. You can record video and capture images, and configure video play and image settings.
Search	You can search for images, traffic flow information, pedestrian information, and records on this page.
Playback	You can play back manual video recordings and videos related to traffic violations to track back events (if any).
Camera	You can configure camera attributes such as brightness, contrast, shutter, metering zone, and focus.

Function	Description
ITC	You can configure smart plan, image, OSD, vehicle blocklist and allowlist, perform intelligent analysis, and more.
Network Settings	You can configure TCP/IP, port number, automatic registration, basic services and ITSAPI.
Remote Config	You can enable the remote device such as enforcement camera or IP camera to work with the Camera.
Event	You can enable how the Camera responds when alarms and exception occur.
Peripheral	You can add and configure external devices.
Storage	You can configure the storage path of snapshots and video records.
System	You can configure system information, add users, restore to factory settings, import and export system configuration files, and more.
System Info	You can view information such as version, log, online user, running status, device location and legal information.
Security	You can view security status and enable multiple system services to secure network safety.

2 Local

You can configure play protocol, and the names and storage path of snapshots and video recordings.

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**.

Figure 2-1 Local

Play Parameter	
Protocol	<input checked="" type="radio"/> TCP Port <input type="radio"/> UDP Port <input type="radio"/> Multicast

Picture and Storage Path Naming	
Naming Format	<input type="text" value="%y%M%d%h%m%s_%27_%09"/> <input type="button" value="Reset"/>
Name Preview	<input type="text" value="20130106152730_8_EUP5689"/> <input type="button" value="Help"/>

Record	
Live Record	<input type="text" value="C:\Users\... \WebDownload\LiveRecord"/> <input type="button" value="Browse"/>
Playback Download	<input type="text" value="C:\Users\... \WebDownload\PlaybackRecord"/> <input type="button" value="Browse"/>

Snapshot	
Live Snapshot	<input type="text" value="C:\Users\... \WebDownload\LiveSnapshot"/> <input type="button" value="Browse"/>

<input type="button" value="Apply"/>	<input type="button" value="Refresh"/>	<input type="button" value="Default"/>
--------------------------------------	--	--

Step 2 Select the play protocol.

Step 3 Name the snapshots in the **Naming Format** section. You can click **Help** to view the naming rules, or click **Reset** to restore the naming rule to the default.

Step 4 Click **Browse** to select the storage path of live rerecords, playback records, and live snapshots.

Step 5 Click **Apply**.

3 Configuration Wizard

The configuration wizard guides you to quickly configure the settings such as basic parameters, lens type, detection line, AI detection, and more.

3.1 ANPR Mode (without Radar)

You can upgrade software, configure scene for capture, lens type, detection line, AI detection, and more.

Procedure

- Step 1 Log in to the webpage.
- Step 2 Click **Configuration Wizard**.
- Step 3 (Optional) On the **Software Version** page, click **Import** to select upgrade file from local computer, and then click **Upgrade**. Click **Next**.



When the software version is not what you need but the device type is what you need, you can upgrade the software.

- Step 4 On the **Basic Settings** page, configure the date and time format, and system time of the Camera, and then click **Next**.

Figure 3-1 Configure basic parameters

The screenshot displays a configuration interface with the following parameters:

- Language: English
- Fill Light: IR Mode
- Plate Algorithm: Overseas ALG
- Date Format: YYYY-MM-DD
- Time Format: 24-Hour
- Time Zone: (UTC+08:00)
- System Time: 2025-05-21 15:58:36

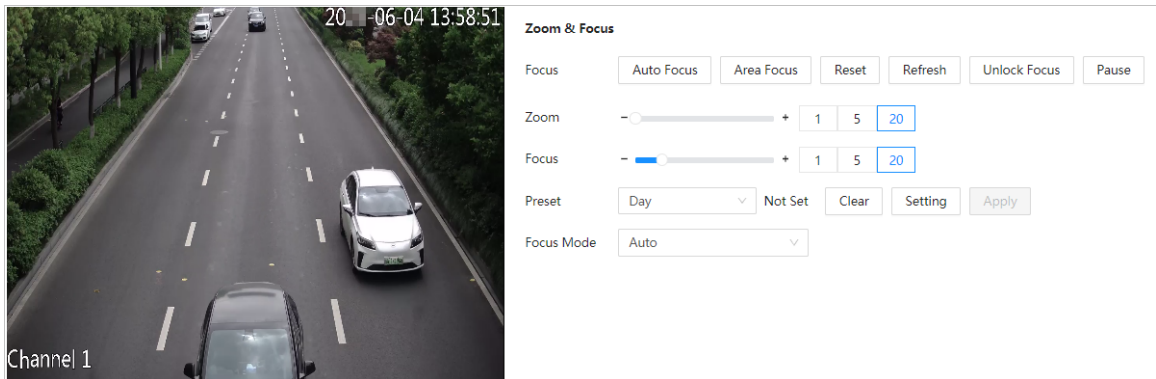
At the bottom, there are two buttons: "Back" and "Next".

- Select fill light from **White Light** or **IR Mode** according to the type of illuminator that actually connected.
- You can manually enter the time, or click **Sync PC** to synchronize time from the server.
- Set **Plate Algorithm** to your country to get better results.

Step 5 Select **ANPR** (focuses on identifying vehicles by capturing and analyzing license plates), and then click **Next**.

Step 6 Check whether the video image is properly zoomed and focused by the plate pixel.

Figure 3-2 Adjust the video for recognition



1. Click **Unlock Focus**, and then configure the focus mode.

- **Auto Focus** : Adjusts video clarity automatically.
- **Area Focus** : Draw a detection zone and adjust the clarity of the detection zone.
- **Reset** : Reset all focus and zoom parameters to the default settings.
- **Refresh** : Update the page content.
- **Unlock Focus** : Unlock the focus setting.



The focus configuration will be locked without any operations within 60 s.

- **Pause /Play**: Click **Pause** to stop playing the live video, and then click **Play** to start playing the live video.

2. Drag the zoom and focus bars to adjust the video image until the image is clear.
3. Configure the presets.

You can select **Day** or **Night** presets.

4. Click **Setting** to configure presets, and then click **Apply**.
5. Click **Next**.

Step 7 Configure scene validation.

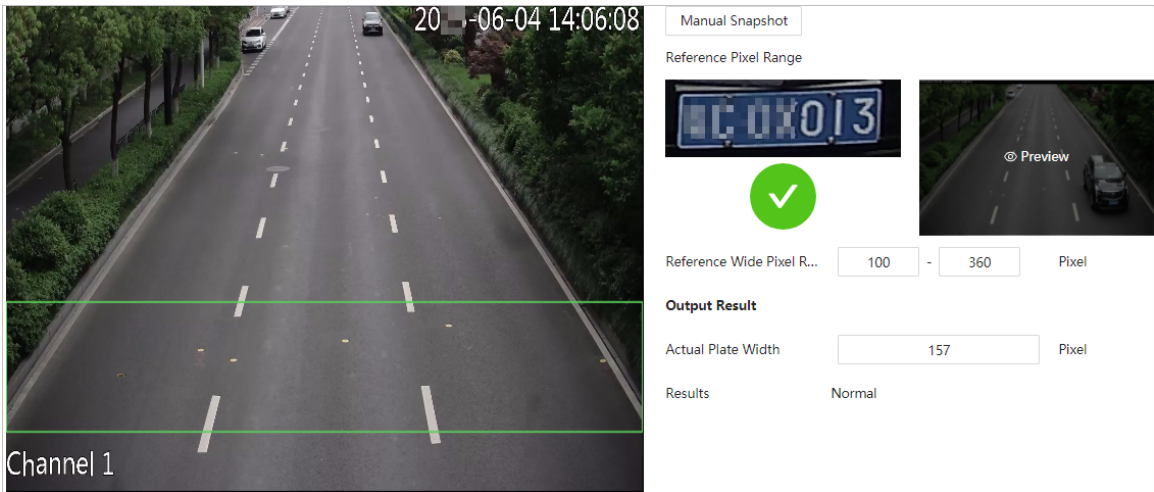


This function is only available for models that do not support radar.

1. When the target enters the green box, click **Manual Snapshot** to capture a picture of plate.
2. the Camera compares the pixel of the snapshots with the pixel range.

If the pixel of the snapshot is within the given pixel range, the results display **Normal** . Otherwise the results will display **Too Small**, and then you need to click **Back** to configure the parameter of zoom and focus again.

Figure 3-3 Scene validation

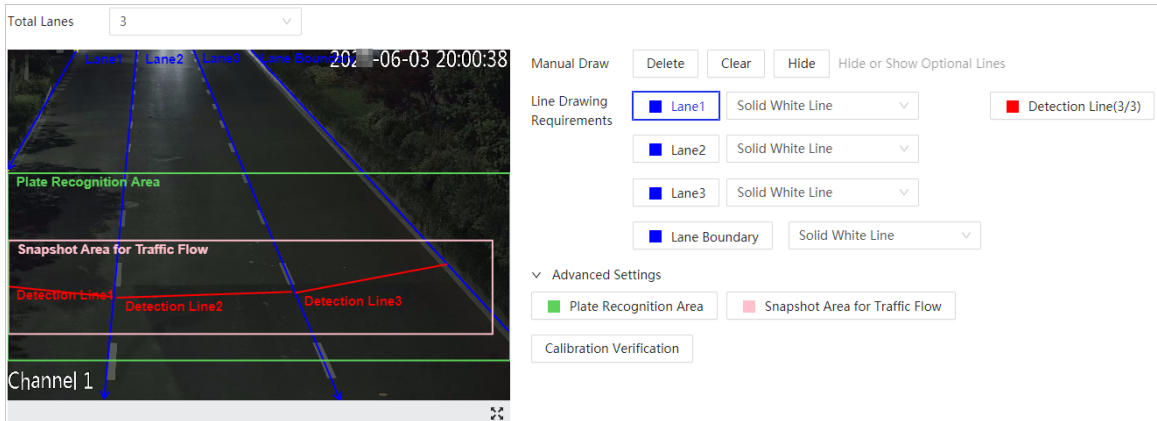


3. Click **Next**.

Step 8 Configure detection mode for lines.

1. Select trigger mode.
 - **Video** : Draw detection lines manually according to line drawing requirements.

Figure 3-4 Video



a. Configure the total lanes.



You need to draw lanes from left to right, beside you just need to draw the left lane lines.

- b. Draw lane lines and right lane boundary.
- c. (Optional) Configure advanced settings according to your needs.

- **Radar** : Click **+** to add a radar, and then configure the parameters.

Table 3-1 Radar parameters

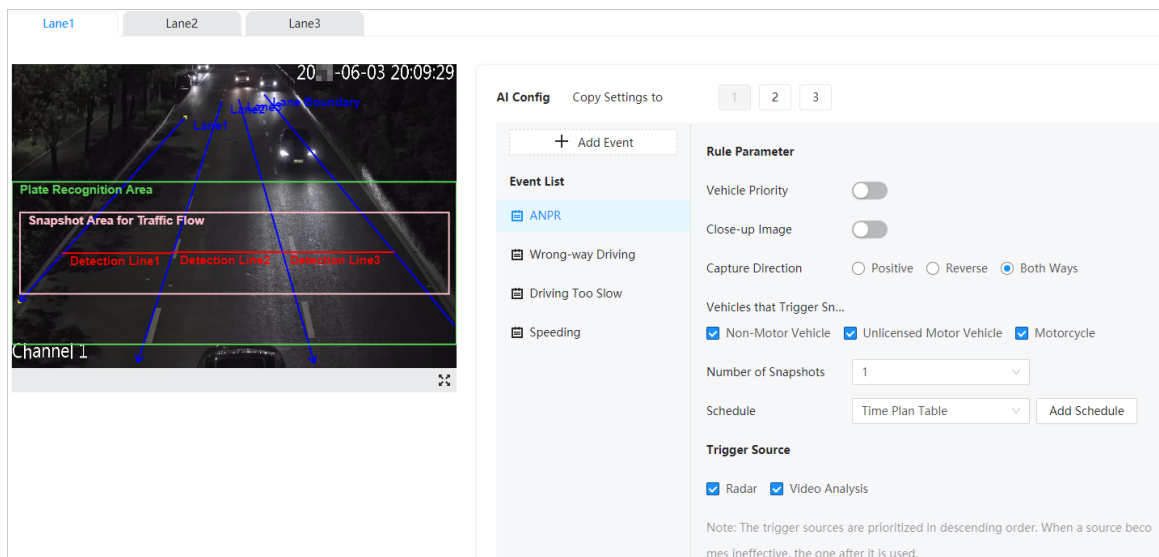
Parameter	Description
Protocol	The protocol of the radar.

Parameter	Description
Starts Monitoring from Lane	Set the lane No. as the starting lane at which the radar starts detecting, and the number of lanes detected by the radar.
Number of Lanes	For example, when setting Starts Monitoring from Lane to 3, and Number of Lanes to 2, the radar will detect lane 3–lane 5.
Wait Time Before Capture	You can set the duration between wait time before camera capturing and wait time after camera capturing.
Wait Time after Capture	<ul style="list-style-type: none"> ◇ If the radar detects the speed of a vehicle within the duration, the speed detected will be shown in the snapshot. ◇ If not, there will be no vehicle velocity shown in the snapshot.

2. Click **Next**.

Step 9 Configure AI detection for lanes.

Figure 3-5 AI configuration



1. Select a lane.

2. Click **Add Event** to select events to the lane.

Figure 3-6 Add event

Add Event

Select All

ANPR Wrong-way Dr... Driving Too Sl... Speeding

Illegal Lane Ch... Crossing Solid... Illegal Parking Traffic Conges...

Non-motor Ve... Not Wearing ... Occupying Lane

Cancel OK



Click **Select All** to select all events.

3. Click **OK**.
4. Configure the parameters of every event that you add.



Select **2** or **3** next to **Copy Settings to** to copy the settings of lane1 to lane2 and lane3.

Step 10 Click **Next**, and then it goes to the **Complete** page.

Step 11 Click **Go to Home Page**.

3.2 ANPR Mode (with Radar)

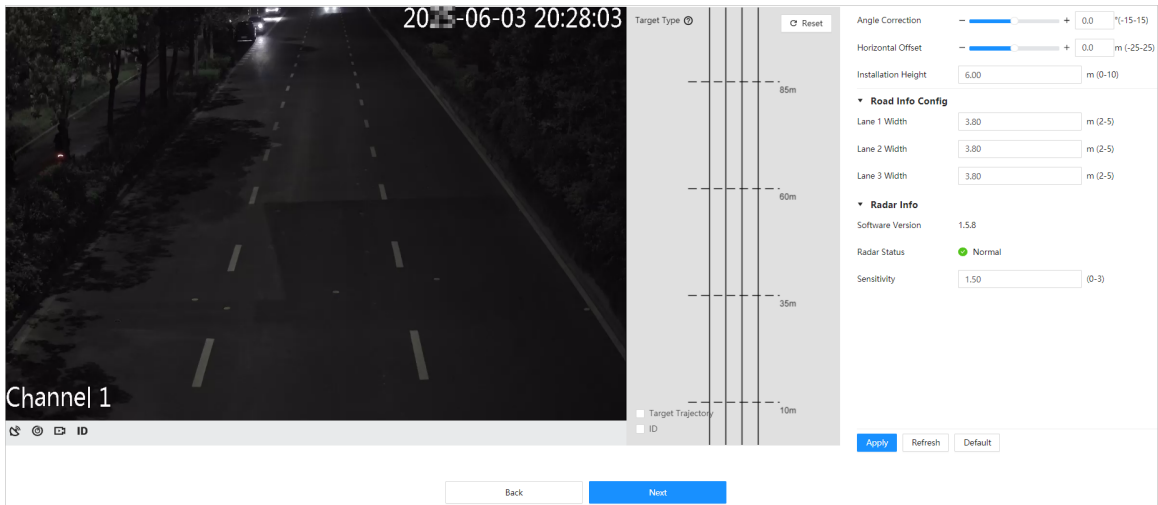
You can upgrade software, configure scene for capture, lens type, detection line, AI detection, and more.

Procedure

Step 1 Refer to Step 1–Step 4, Step 6–Step 7, and Step 9 in "3.1 ANPR Mode (without Radar)".

Step 2 On the **Radar Settings** page, configure the radar parameters, and then click **Next**.

Figure 3-7 Configure the radar



1. Configure angle correction and horizontal offset.



We recommend adjusting the angle correction first to ensure that radar trajectories are parallel to lane lines, and then adjusting the horizontal offset to accurately align the radar lane with the video lane.

- Angle correction
 - ◇ If the original vehicle trajectory is biased to the left of the center lane line, increase the angle correction.
 - ◇ If the original vehicle trajectory is biased to the right of the center lane line, decrease the angle correction.
- Horizontal offset
 - ◇ If the radar lane appears left of the video lane, increase the horizontal offset.
 - ◇ If the radar lane appears right of the video lane, decrease the horizontal offset.

2. Configure the parameters of road and radar information.


Table 3-2 Parameter description of radar

Module	Parameter	Description
Road Info Config	Lane X Width	Input the width value for each lane.
Radar Info	Software Version	The radar software version.
	Radar Status	Normal or abnormal.
	Sensitivity	It is recommended to leave the sensitivity as default to avoid false detections.

Step 3 On the **Calibrate by Radar & Video** page, configure online or manual calibration, and then click **Next**.

- Online calibration
 1. Select **Online Calibration** from the calibration mode.
 2. Click **Enable**, click **Pause** when vehicles pass, and then enter the video ID and radar ID.



- ◇ We recommend collecting at least 1 set of IDs for each lane.
- ◇ Click +/- to add or delete one set of ID. Supports adding up to 10 sets of IDs.
- ◇ Click  to view the radar ID.
- ◇ Click **ID** to view the video ID.


3. Click **Calibrate**.

The system calibrates based on the input data, and displays the calibration progress at the bottom of the page.

● Manual calibration

1. Select **Manual** from the calibration mode, and then adjust the calibration frame on the live view based on the on-site measurement.



- ◇ Click  to clear the current calibration frame.
- ◇ Click **Calibration Area**, and then click 4 points on the image to create a new frame. We recommend drawing the frame along the lane lines to form a trapezoid.

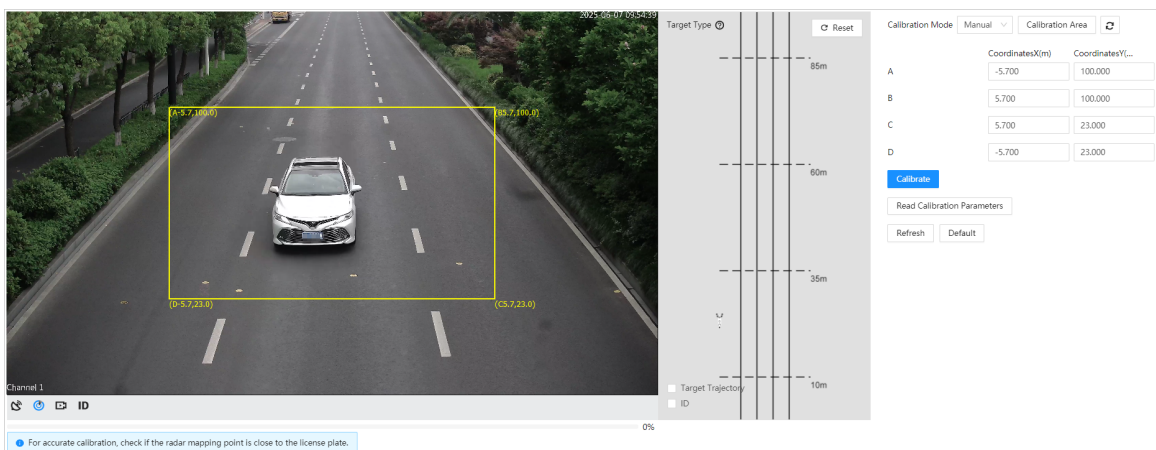
2. Click **Read Calibration Parameters**.

The coordinates of the calibration frame will be automatically synchronized to the right of the live view.

3. Click **Calibrate**.

The system calibrates based on the input data, and displays the calibration progress at the bottom of the monitoring screen. After the calibration is complete, the system prompts that the calibration is successful.

Figure 3-8 Manual calibration



Step 4 Click **Next**, and then it goes to the **Complete** page.

Step 5 Click **Go to Home Page**.

3.3 Road Monitoring Mode

You can upgrade software, configure scene for capture, lens type, detection line, AI detection, and more.

Procedure

- Step 1 Refer to Step 1 –Step 4 in "3.1 ANPR Mode (without Radar)".
- Step 2 Select **Road Monitoring** (suitable for traffic management such as tracking traffic flow), and then click **Next**.
- Step 3 Refer to Step 6 –Step 11 in "3.1 ANPR Mode (without Radar)".



For road monitoring mode, only **ANPR** is supported when adding an event on the **AI Config** page.

4 Live

The **Live** page is displayed after you successfully log in to the webpage. On this page, you can view the live video image and the captured number plate, take snapshots, view snapshot details, and perform other operations.

Figure 4-1 Live page

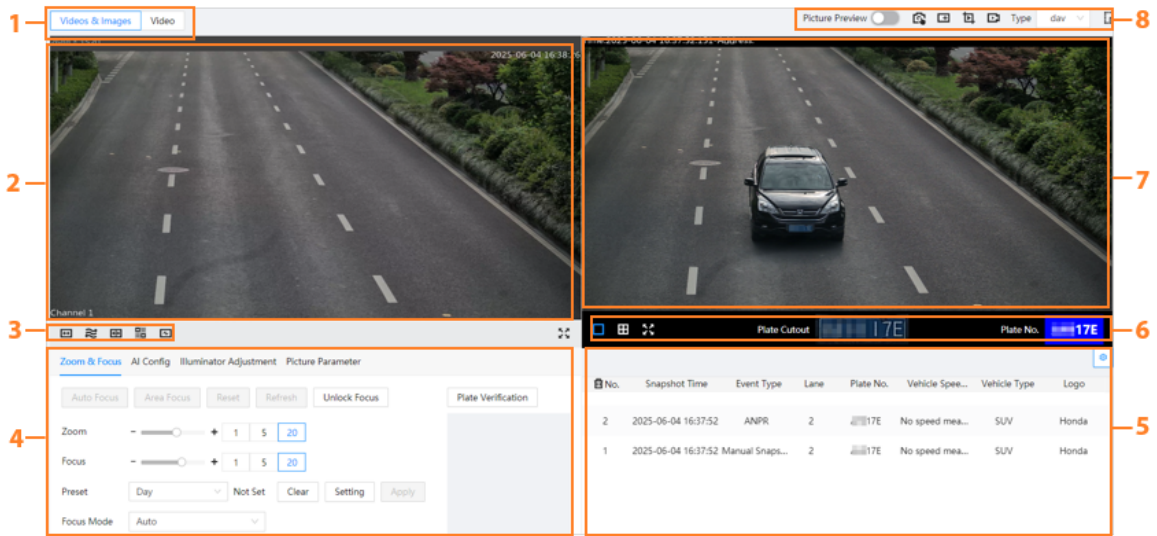


Table 4-1 Description of the live page

No.	Function	Description
1	Display mode	The display modes include Video & Image and Video mode.
2	Live view	Displays real-time video.
3	Video adjustment	Adjustment operations in live viewing.
4	Frequently used functions	These functions are frequently used when viewing live videos, such as adjusting the focus and zoom, AI detection, picture parameters, flash light, and more.
5	Snapshot details	Displays the details of the vehicle that is captured.
6	Plate snapshot and plate number	Displays plate snapshots and recognized plate number.
7	Snapshot	Displays license plate snapshots.
8	Live view function bar	Functions and operations in live viewing.

4.1 Live View

Displays the live video of the camera. You can click the icons to change the display mode of live view.

Figure 4-2 Live view

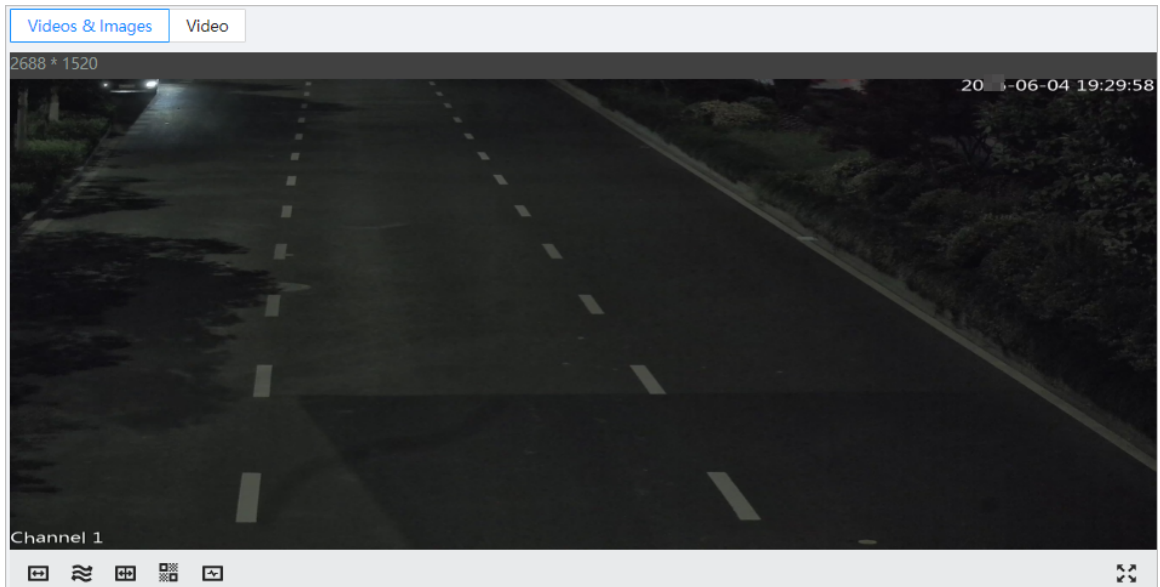









Table 4-2 Icon description of live view page

Icon	Function	Description
	W:H	Click the icon to select Original or Adaptive playback.
	Smoothness Adjustment	<p>Change the fluency of the video. Select one based on your network bandwidth.</p> <p></p> <p>Download and install the plug-in before using the function.</p> <ul style="list-style-type: none"> ● Realtime : Guarantees the real time of the video. When the network bandwidth is not enough, the video might not be smooth. ● General : It is between Realtime and Fluent. ● Fluent : Guarantees the fluency of the video but the video might not be real-time.
	AI Rule	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed on the video image.
	Pixel	Click it, and then draw a rectangular area on the image to show the pixel size of that area.

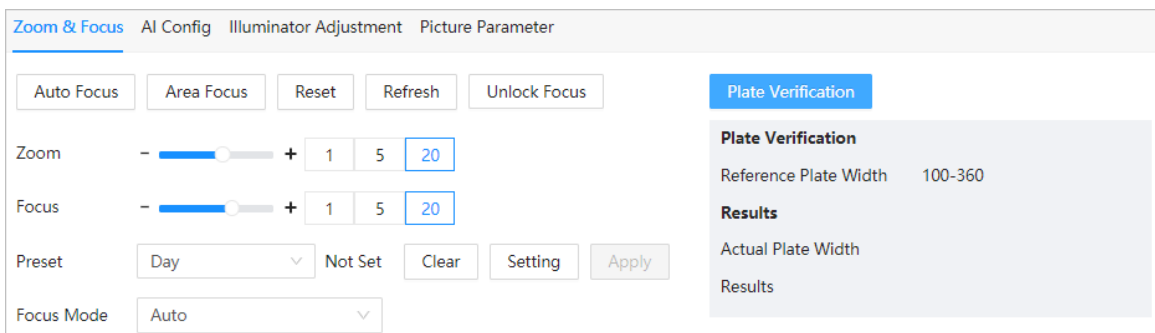
Icon	Function	Description
	Main Stream Sub Stream	<p>Click it to select a video stream based on your network bandwidth.</p> <ul style="list-style-type: none"> • Main stream: Displays video with high resolution, but requires large bandwidth. This option can be used for storage and monitoring. • Sub stream: Displays the video in lower resolution but smoothly. It requires less bandwidth. This option is normally used to replace main stream when the network bandwidth is not enough.
	Full Screen	Click it to go to full-screen display. In full-screen display, press Esc to exit full screen.

4.2 Frequently Used Functions

4.2.1 Zoom and Focus

Click **Zoom & Focus** to drag the slider to adjust the parameters. For details, see "3 Configuration Wizard".

Figure 4-3 Zoom and focus



4.2.2 AI Configuration

Draw detection lines for every lane, and then click **Save**. For details, see [Step 8](#) in "3.1 ANPR Mode (without Radar)".

4.2.3 Illuminator Adjustment

Click **Illuminator Adjustment** to configure the output mode, brightness, auto mode, ambient brightness of the illuminator.

Figure 4-4 Illuminator adjustment

Table 4-3 Parameter description of flash light

Parameter	Description
Fill Light	Select White Light or IR Mode according to the type of illuminator actually connected.
Output Mode	Selects the output mode of spotlight. <ul style="list-style-type: none"> ● Close : The spotlight is always off. ● Always : The spotlight is always on. ● Auto : The spotlight turns off according to the ambient brightness.
Brightness	Drag the slider to adjust the brightness of the light. Both the darker areas and the brighter areas will be changed together when adjusting the brightness. The image might become blurry when the value gets bigger.
Auto Mode	You can select Time or Brightness .
Ambient Brightness	You can adjust the ambient brightness.

4.2.4 Picture Parameter

You can adjust the picture parameters of the camera to obtain clear images.

Click **Picture Parameter** to configure the parameters of images.

Figure 4-5 Picture parameter of manual mode

Figure 4-6 Picture parameter of Auto mode

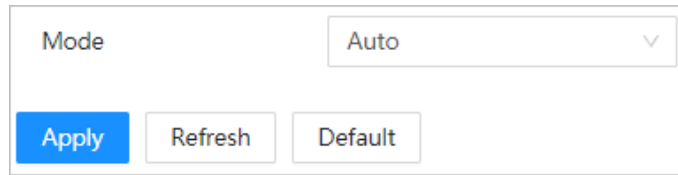




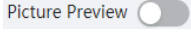


Table 4-4 Parameter description





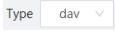

Parameter	Description
Mode	You can select Manual or Auto mode.
Shutter	<p>Shutter controls how long the sensor is exposed to light. Fast shutter (for example, 1/250) reduces motion blur but darkens the image. Slow shutter (for example, 1/25) brightens the image but risks motion blur.</p> <p>You can select the shutter value, or select Custom, and then set the shutter range.</p> <p></p> <p>You need to configure shutter when Shutter is set to Custom.</p>
Gain	<p>Gain amplifies the camera's sensor signal to brighten the image. Higher gain increases brightness but introduces noise, degrading detection accuracy.</p> <p></p> <p>You need to configure gain scope when Mode is set to Manual.</p>

4.3 Live View Function Bar

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

Table 4-5 Function description of the live page

Icon	Name	Description
	Picture Preview	<ul style="list-style-type: none"> Click  to enable the function, and then the Camera automatically receives vehicle snapshots and detects event information triggered by sources such as radar or video detection, and displays such snapshots and information in the window on the right. The snapshots are saved in the storage path. To change the storage path, go to the Storage page.
	Manual Snapshot	Enable Picture Preview , and then click the icon, the camera automatically takes a snapshot when a vehicle passes, and saves snapshots to the storage path.

Icon	Name	Description
	Digital Zoom	Use this function to zoom in on any area of the video. Click the icon and drag to select any area in the video, and then the camera will zoom in on the area you selected.
	Take Screenshot	Takes a snapshot of the current live video.
	Snapshot	Click the icon to take 1 snapshot from the video, and then you can acquire a snapshot of bmp format. You can check the quality of the video by viewing the snapshot.
	Record	Click the icon to start recording. Click again to save the recording to your local computer.
	Type	Select the format of the video recording (dav) by default.
	Aux Focus	Click the icon to start auto focus, local focus, and license plate check for the monitoring image.


4.4 Plate Number Recognition

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

4.5 Vehicle Snapshot

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

4.6 Event List

Click  to enable the **Picture Preview** function, and the event information will be displayed, including number, snapshot time, event type, lane, plate number, vehicle speed, vehicle type, and logo.




Click  to select the fields that you want to display.

Figure 4-7 Event list

No.	Snapshot Time	Event Type	Lane	Plate No.	Vehicle Speed (km...)	Vehicle Type	Logo
7	2025-06-04 19:52:34	ANPR	2	M■■■■39	No speed measurem...	SUV	Dodge
6	2025-06-04 19:52:29	ANPR	3	■■■■D	No speed measurem...	Large Bus	GAC Hino
5	2025-06-04 19:52:28	ANPR	2	■■■■77	No speed measurem...	Sedan	Jeep
4	2025-06-04 19:52:26	Manual Snapshot	2	U■■■■ed	No speed measurem...	Sedan	Unknown
3	2025-06-04 19:50:53	ANPR	3	■■■■3	No speed measurem...	Sedan	Unknown

5 Camera

You can configure camera attributes such as brightness, contrast, saturation, shutter, metering zone, and focus. Besides, you can also configure encoding parameters such as video stream, video OSD and ROI (region of interest).

5.1 Configuring Camera Attributes

After connecting the camera to the network and viewing the live video on its webpage, you can adjust the image parameters of the camera to obtain clear images.

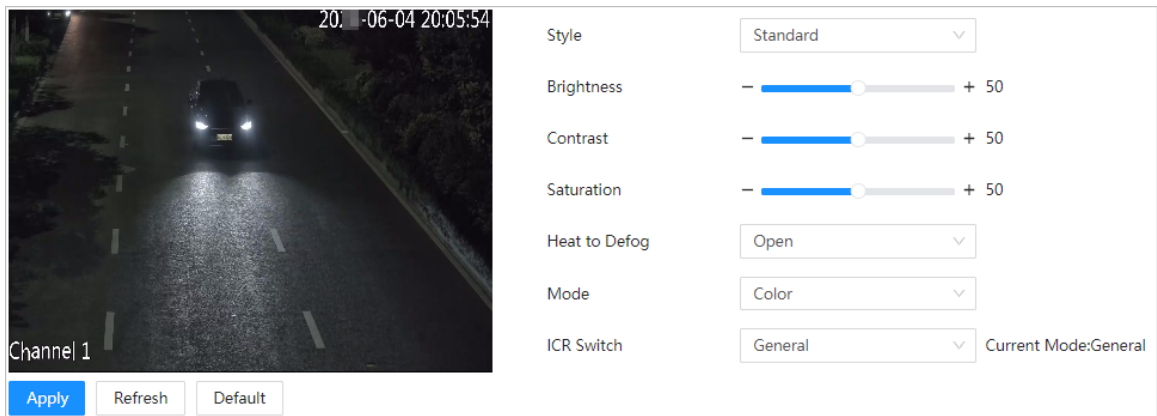
5.1.1 Configuring General Parameters

You can configure the brightness, contrast, saturation, mode, and other attributes of the camera.

Procedure

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

Figure 5-1 General



Step 2 Configure the parameters.

Table 5-1 Description of general parameters

Parameter	Description
Brightness	<ul style="list-style-type: none"> Both the darker areas and the brighter areas will be changed together when adjusting the brightness. The image might become blurry when the value gets bigger. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the brighter the image.
Contrast	<ul style="list-style-type: none"> The larger the value, the darker the dark area, and the more exposed the bright area. The image might become blurry when the value gets smaller. The recommended range is 40–60, and the available range is 0–100. It is 50 by default. The larger the value, the stronger the contrast.

Parameter	Description
Saturation	<ul style="list-style-type: none"> • The saturation value does not change the overall image brightness. • The larger the value, the more saturated the image. • It is 50 by default. The smaller the value, the more unsaturated the image. The recommended range is 40–60, and the available range is 0–100.
Heat to Defog	<ul style="list-style-type: none"> • Open : Enable the defog function. • Close : Not enable the defog function.
Mode	<ul style="list-style-type: none"> • Color : The image is always colored. • Auto : When the brightness is higher than the threshold, the image automatically changes to color. When it is below the threshold, the image changes to black and white. • B/W : The image is always black and white.
ICR Switch	<ul style="list-style-type: none"> • Auto : You need to pre-set the brightness in this mode. When the ambient brightness is higher than the pre-set value, the Polarizer will start to work. • Polarizer : The Polarizer is always running. Applicable to scenarios with high brightness. • IR : Applicable to scenarios with low brightness.
Ambient Brightness	The light adjusts its brightness according to the ambient brightness.

Step 3 Click **Apply**.

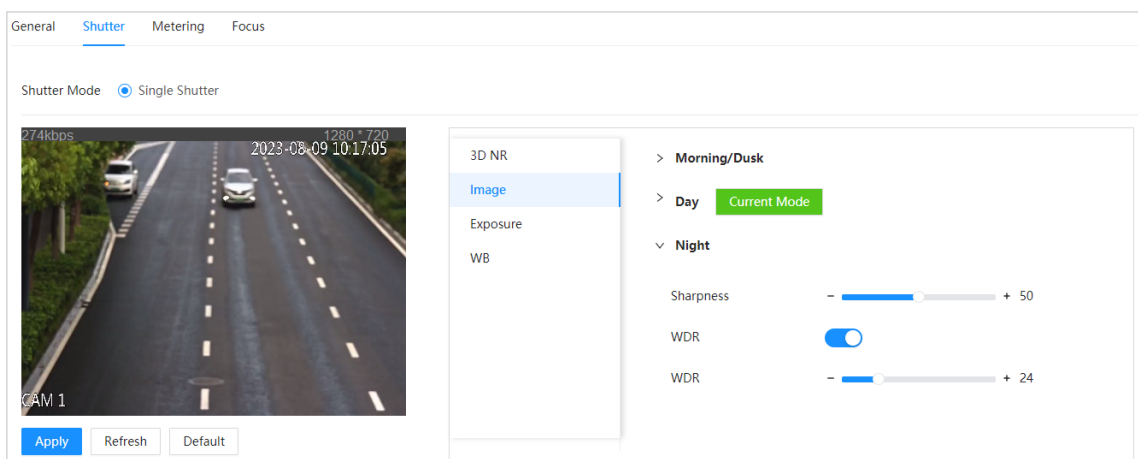
5.1.2 Configuring Shutter

You can configure shutter mode, exposure mode, and gain mode.

Procedure





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

Figure 5-2 Shutter



Step 2 Configure the parameters.

Table 5-2 Description of shutter parameters

Module	Parameter	Description
Shutter Mode	Single Shutter	Video and snapshot share the same exposure mode.
3D NR	Video/Image 3D NR	Click  , and then 3D NR is enabled to reduce noise of video/image. The higher the value, the less the noise.
Image	Scene	You can change the scene and adjust the sharpness of the corresponding scene. Available scenes include Morning/ Dusk , Day , and Night .
	Sharpness	You can set the sharpness of the corresponding scene. The higher the value, the clearer the image. But there will be noise if the sharpness is too high.
	WDR	Click  to enable WDR (wide dynamic range), which helps provide clear video images in bright and dark light.
Exposure	Iris	<ul style="list-style-type: none"> • In Auto mode, only Manual iris type is available. • In Force mode, several iris types are available, and you also need to configure Iris, which includes Auto and Manual. If Manual is selected, you can manually drag the slider to adjust the value.
	Mode	Select the way of adjusting exposure mode. You can select from Manual and Auto .
	Shutter	<p>Shutter controls how long the sensor is exposed to light. Fast shutter (for example, 1/2000) reduces motion blur but darkens the image. Slow shutter (for example, 1/25) brightens the image but risks motion blur.</p> <p>You can select the shutter value, or select Custom, and then set the shutter range.</p> <p></p> <p>You need to configure shutter when Shutter is set to Custom.</p>
	Gain	<p>Gain amplifies the camera's sensor signal to brighten the image. Higher gain increases brightness but introduces noise, degrading detection accuracy.</p> <p></p> <p>You need to configure gain scope when Mode is set to Manual.</p>
WB	Mode	Set scene mode to adjust the image to its best status.

Step 3 Click **Apply**.

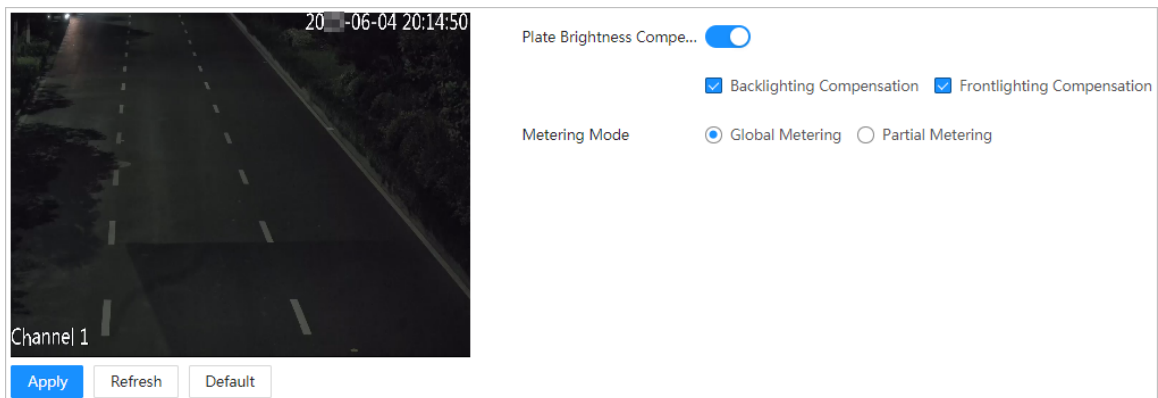
5.1.3 Configuring Metering Zone

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

Procedure

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

Figure 5-3 Metering



Step 2 Configure the parameters.

Table 5-3 Description of metering parameters

Parameter	Description
Plate Brightness Compensation	Click to enable this function, and then you can select Backlighting Compensation and Frontlighting Compensation according to scene requirements to improve the backlight and frontlight image brightness.
Metering Mode	<ul style="list-style-type: none"> ● Global Metering : Measure the brightness of the whole image area and intelligently adjust the overall image brightness. ● Partial Metering : Measure the brightness of sensitive areas and intelligently adjust the overall image brightness. If the measured area becomes bright, then the whole area becomes dark, and vice versa. Click Draw, and then drag the mouse to draw measured areas and yellow boxes display over the video image. <ul style="list-style-type: none"> ◇ Click Clear to redraw partial metering areas. ◇ Click to delete a partial metering area.

Step 3 Click **Apply**.

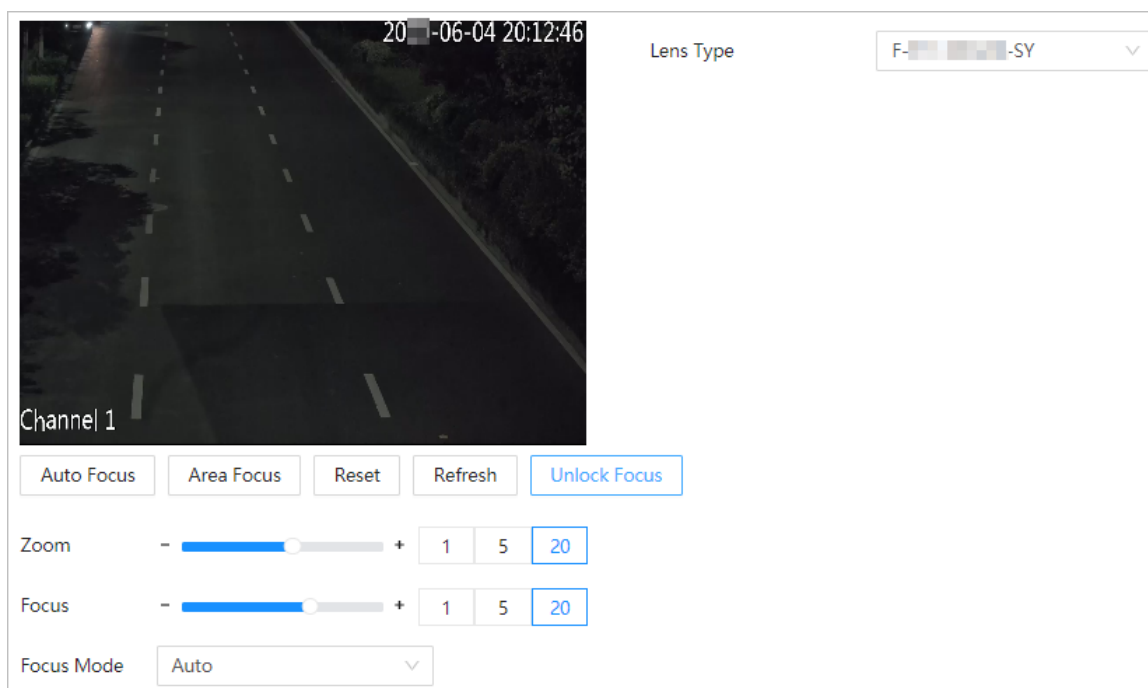
5.1.4 Configuring Focus

Adjust the focus of the Camera.

Procedure


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

Figure 5-4 Focus



Step 2 Click **Unlock Focus**, and then configure the parameters.

Table 5-4 Description of focus parameters

Parameter	Description
Lens Type	Keep it as default.
Zoom	Drag the slider to zoom in or out the video image at the selected speed.  Click Unlock Focus before configuring the parameters.
Focus	Drag the slider to adjust the camera focus.
Auto Focus	Automatically adjusts the camera focus to get clear images.
Area Focus	Function reserved.
Reset	Reset all focus and zoom parameters to the default settings.
Refresh	Update the page content.

Step 3 Click **Refresh**.

5.1.5 Configuring LDC

LDC (Low Distortion Control) is a feature that corrects optical distortions like barrel or pincushion effects. You can adjustable parameters that fine-tune how the distortion correction is applied.

Procedure

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

Step 2 Select type of lens that you want to correct distortions.

Step 3 Click  to enable LDC.

Step 4 Click **Apply**.

5.2 Configuring Encode Parameters

After connecting the camera to the network and viewing the live video on its webpage, you can configure encoding parameters when necessary to obtain clear and smooth video image.

5.2.1 Configuring Video Parameters

Configure the parameters of video streams.

Procedure

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

Figure 5-5 Video stream





The screenshot displays the 'Video Stream' configuration page, divided into two columns: 'Main Stream' and 'Sub Stream'. At the bottom, there are three buttons: 'Apply', 'Refresh', and 'Default'.

Parameter	Main Stream Value	Sub Stream Value
Encoding Mode	H.264H	H.264M
Resolution	2688*1520(2688x1520)	1280*720(720P)
Frame Rate (FPS)	25	25
Bit Rate Type	CBR	VBR
Bit Rate	4096 (Kb/S)	Custom (Kb/S)
I Frame Interval	50 (25-150)	50 (25-150)
Smooth Stream	Slider at 50 [Smooth <-> Clear]	Slider at 50 [Smooth <-> Clear]
Watermark	Enabled (Toggle)	Not applicable
Watermark String	DigitalCCTV	Not applicable

Step 2 Configure the parameters.

Table 5-5 Description of video stream parameters

Parameter	Description
Encoding Mode	<ul style="list-style-type: none"> ● H.264M: Balances quality and file size using inter-frame compression. Suitable for real-time video streaming such as surveillance, but it has lower compression efficiency compared to H.265. ● H.264H: Requires lower bit rate than H.264M at the same quality, but needs more processing power for encoding. ● MJPEG: Simple to encode and decode, and no motion blur, but poor for streaming due to high bandwidth requirements. ● H.265: Lower bit rate requirements and higher compression efficiency than H.264 at the same quality, but requires significant processing power.

Parameter	Description
Resolution	<p>The higher the value, the clearer the overall image. For each resolution, the recommended bit stream value is different.</p>  <p>The resolution of sub stream cannot be greater than that of main stream.</p>
Frame Rate (FPS)	<p>The higher the value, the smoother the video image. The frame rate might vary due to different resolutions.</p>
Bit Rate Type	<p>You can select from VBR (variable bitrate) and CBR (constant bitrate).</p> <ul style="list-style-type: none"> ● VBR : Gives the best balance between quality and file size as the bitrate can be altered depending on the video. ● CBR keeps the bitrate the same during encoding, and it is more advantageous to use when the network connection is limited to performing at, for example, 320 Kbps.
Quality	<p>6 quality levels are available. The higher the value, the better the quality.</p>  <p>You need to configure the image quality when VBR is set to Bit Rate Type.</p>
Bit Rate	<p>Higher bit rate signifies greater image or video quality, but also occupies more storage space.</p>  <p>You need to configure the bit rate when CBR is set to Bit Rate Type.</p>
Max Bit Rate	<p>It is the upper limit of stream in VBR. In CBR, the value is fixed.</p>
I Frame Interval	<p>The number of P-frame between two I-frames. The number varies according to the bit rate. The range is 25-150. We recommend configuring the value to be twice the amount of the bit rate.</p>
Smooth Stream	<p>The higher the value, the smoother the video and the less the clarity.</p>
Watermark	<p>You can verify the watermark to check whether the video has been tampered.</p>
Watermark String	<p>Select the Watermark checkbox to enable watermark verification. The watermark string is DigitalCCTV by default.</p> <p>Watermark string consists of up to 85 characters with numbers, letters and underlines.</p>
Sub Stream	<p>Click  to enable sub stream when your network bandwidth is insufficient or other conditions that influence the video smoothness in main stream.</p>

Step 3 Click **Apply**.

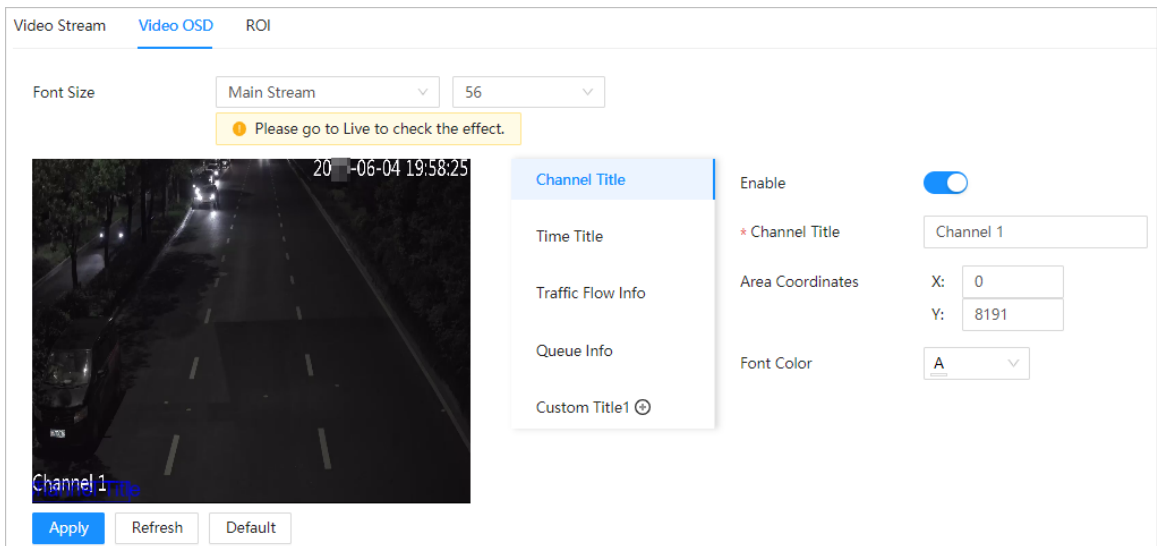
5.2.2 Configuring Video OSD

Configure the OSD information of videos.

Procedure



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


Figure 5-6 Video OSD



Step 2 Configure the parameters.

Table 5-6 Description of video OSD parameters

Parameter	Description
Font Size	Configure the font size of Main Stream or Sub Stream1 .
Channel Title	Click <input type="checkbox"/> to enable the function and configure the channel title, coordinates and font color (can be customized) of channel information OSD.
Time Title	Click <input type="checkbox"/> to enable the function and configure the coordinates and font color (can be customized) of time information OSD. You can click <input type="checkbox"/> to enable Week Display to display week information on the video image.
Traffic Flow Info	Click <input type="checkbox"/> to enable the function and configure the coordinates and font color (can be customized) of flow information OSD.  This function is not available for road monitoring mode.
Queue Info	Click <input type="checkbox"/> to enable the function and set the font color (can be customized) of queue information OSD.  This function is not available for road monitoring mode.

Parameter	Description
Custom Title	<p>Click <input type="checkbox"/> to enable the function and set the coordinates, custom title and font color (can be customized) of custom information OSD.</p> <p></p> <p>You can add up to 8 custom titles.</p>

Step 3 Click **Apply**.

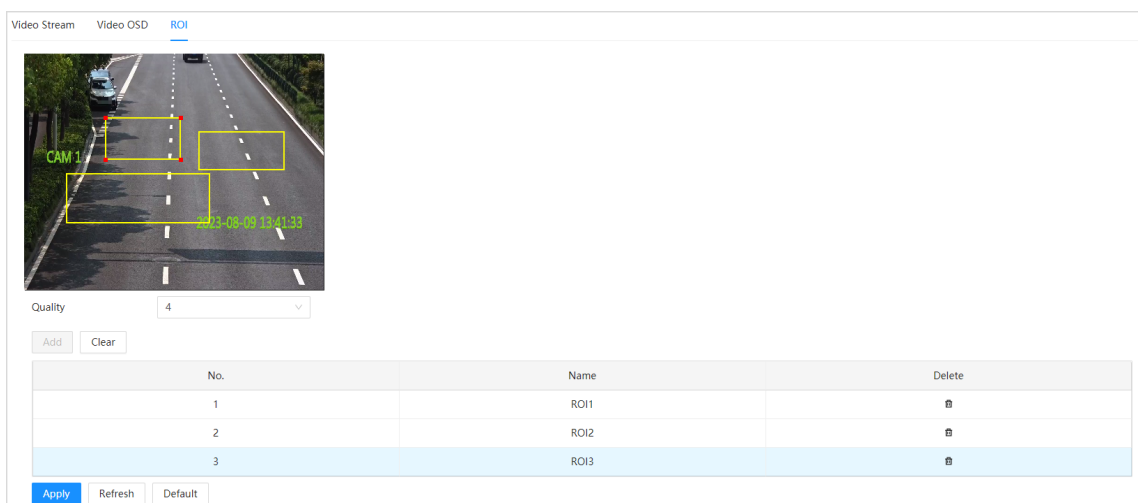
5.2.3 Configuring Interest Area

Configure the region of interest in the video image, and then the selected image will be displayed with the configured quality.

Procedure

Step 1 Select **Camera > Encode > ROI**.

Figure 5-7 ROI



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




- You can add up to 3 regions of interest.
- The higher the value, the better the quality will be.
- Large regions may influence the smoothness of the video.

Step 3 Configure the image quality of the regions of interest.

6 quality levels are available. The higher the value, the better the quality.

Step 4 Click **Apply**.

Related Operations

- Click **Clear** to delete all the regions of interest.
- Click  to delete the corresponding area.

6 Radar

You need to configure radar settings, and radar & video calibration, to ensure the radar detection accuracy and performance. For details, see "3.2 ANPR Mode (with Radar)".



This function is available for devices with radar.

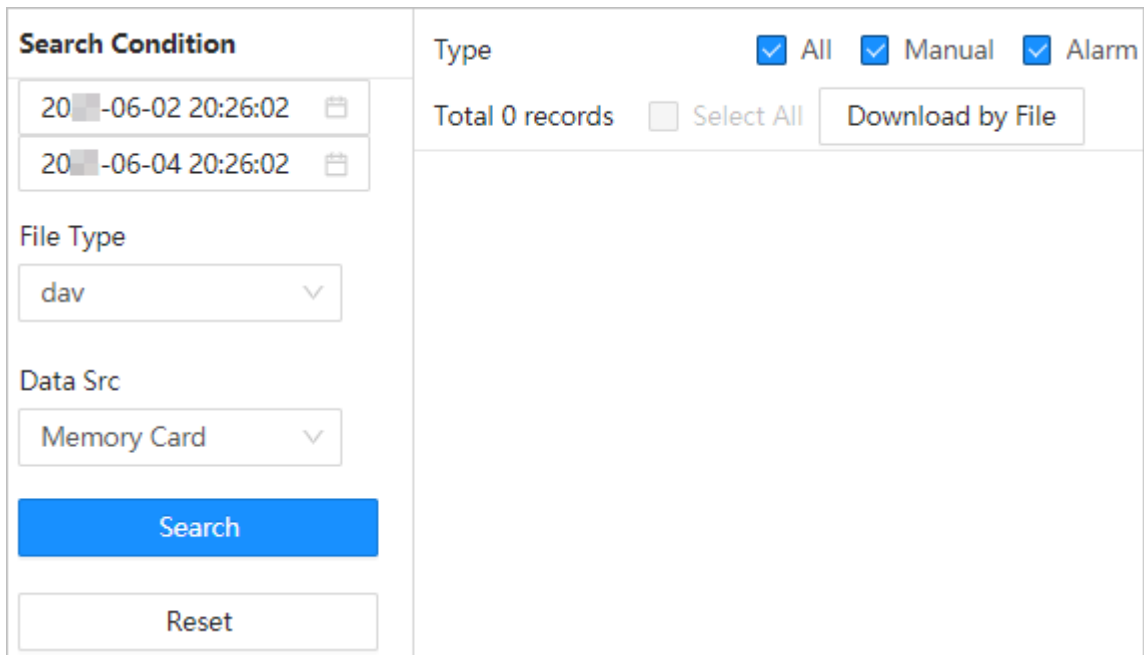
7 Playback

You can search for and download video recordings.

Procedure

Step 1 Select  > **Playback**.

Figure 7-1 Playback



Search Condition	Type
20-06-02 20:26:02	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Manual <input checked="" type="checkbox"/> Alarm
20-06-04 20:26:02	Total 0 records <input type="checkbox"/> Select All <input type="button" value="Download by File"/>
File Type: dav	
Data Src: Memory Card	
<input type="button" value="Search"/>	
<input type="button" value="Reset"/>	

Step 2 Select the record time, **File Type** and data source (**Data Src**).

The data source is **Memory Card** (here referred to as TF card) by default. No video will be played if there are no videos stored on the TF card.

Step 3 Select the type of the snapshot.

- **All** : Take the snapshot of vehicles and the vehicles that violate the rules.
- **Manual** : Take snapshots of vehicles that passed.
- **Alarm** : Take snapshots of vehicles that violates rules.

Step 4 (Optional) Click **Download by File** to download files to your local computer.

8 Search

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

8.1 Picture Query

8.1.1 Searching for SD Card Image

On the **Memory Card Image** page, you can search for and download the images stored in the TF card of the Camera.

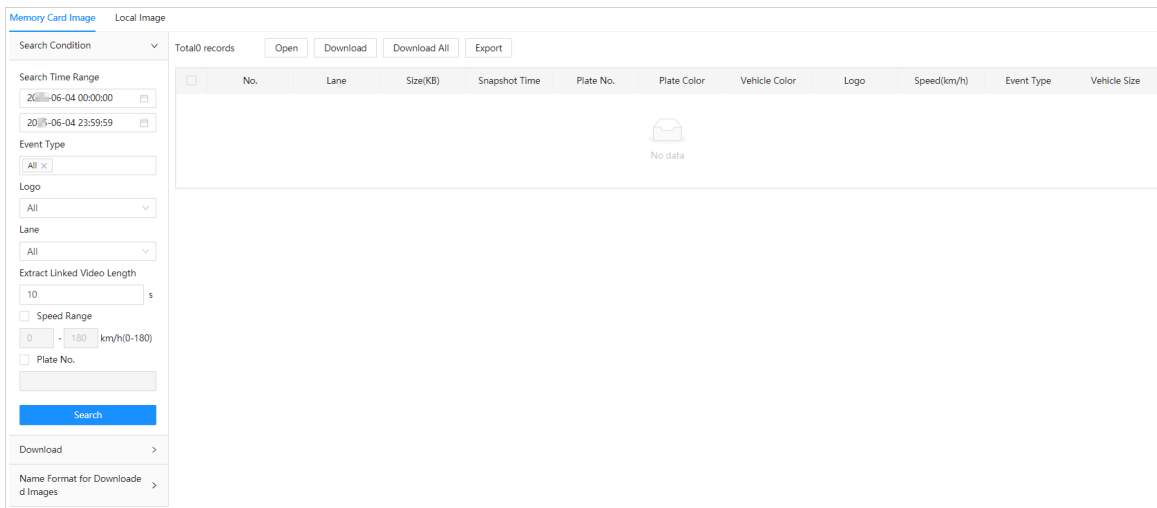


Make sure that the TF card is inserted into the Camera. Otherwise, there might be no results.

Procedure

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

Figure 8-1 Memory card image



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

Table 8-1 Parameter description

Parameter		Description
Search Condition	Search Time Range	Configure the start time and the end time to define a period, and then you can search for images stored on the TF card within this period.
	Event Type	<ul style="list-style-type: none"> ● All : Search for all snapshots. ● Search for snapshots related to events, which include but are not limited to ANPR , Cross Solid White Line, and Wrong-way Driving. <p>For road monitoring mode, only ANPR and manual snapshot events are supported.</p>

Parameter		Description
	Logo	Search for snapshots by the selected vehicle sign. You can select All , Unknown , or a specific vehicle sign.
	Lane	Select the capture lane.
	Extract Linked Video Length	The length of a recorded video associated with the snapshot that you want to save.
	Speed Range	Select the Speed Range checkbox, and set the speed range to search for images of vehicles within the defined speed range.
	Plate No.	Select the Plate No. checkbox, and then enter the plate number to search for images related to this plate.
Download	Download Image by	Select download images by creation time or snapshot time.
	Cutout Type	The type of cutout that you want to download, which includes plate cutout and vehicle body cutout.
	Path	Click Browse to select the path to save the downloaded images.
Name Format for Downloaded Images		Define the naming rules of the downloaded images.

Step 3 (Optional) Select the images that you need, and then click **Open** to view the images in photo viewer.



To open the image, you need to download and install the plug-in.

Step 4 (Optional) Click **Download All** to download all images, or you can select the images that you want to download, and then click **Download** to download the selected images.

Step 5 (Optional) Select the items, and then click **Export** to export the information on captured passed vehicles to your computer.

8.1.2 Local Image

You can view images saved on your and verify whether the image contains a watermark.

Prerequisites

To use the function, you need to download and install the plug-in first.

Procedure

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

Step 2 Click **Browse** to select an image in .jpg format.

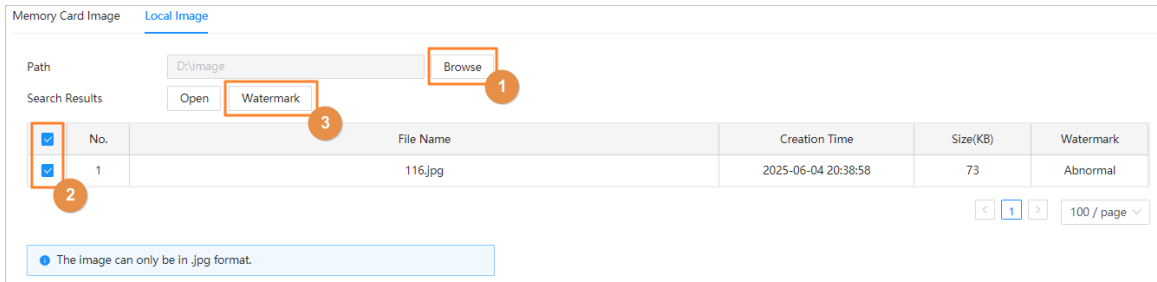
Step 3 Select the image, and then click **Watermark**. You can view the results under **Watermark**.

- When the result is **Abnormal**, the image is tampered.
- When the result is **Normal**, the image is not tampered.



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

Figure 8-2 Local images



8.2 Flow Query

Background Information

You can search for traffic flow and pedestrian flow within the defined period.



- This function is not available in road monitoring mode.
- The function is available on select models, and might differ from the actual product.
- This section uses **Traffic Flow** as an example.

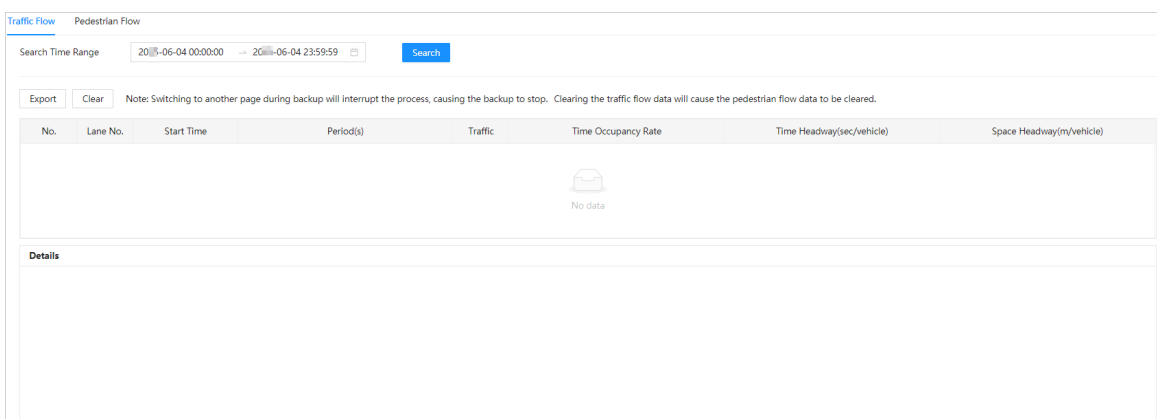
Procedure

- Step 1** Select **Search > Flow Query > Traffic Flow** (select **Pedestrian Flow** if you want to search for pedestrian flow).
- Step 2** Configure search time range.
- Step 3** Click **Search**.
- Step 4** (Optional) Click **Export** to save the results to your computer.



Click **Clear** to delete all results.

Figure 8-3 Traffic flow search



8.3 Search Video



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

8.3.1 Recording

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

Background Information



- Click  on the **Live** page, and the Camera starts recording. The recorded video is saved on the path defined in  > **Local** > **Record** > **Live Record**.
- The function is available on selected models, and might differ from the actual product.

Procedure

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

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

Figure 8-4 Record

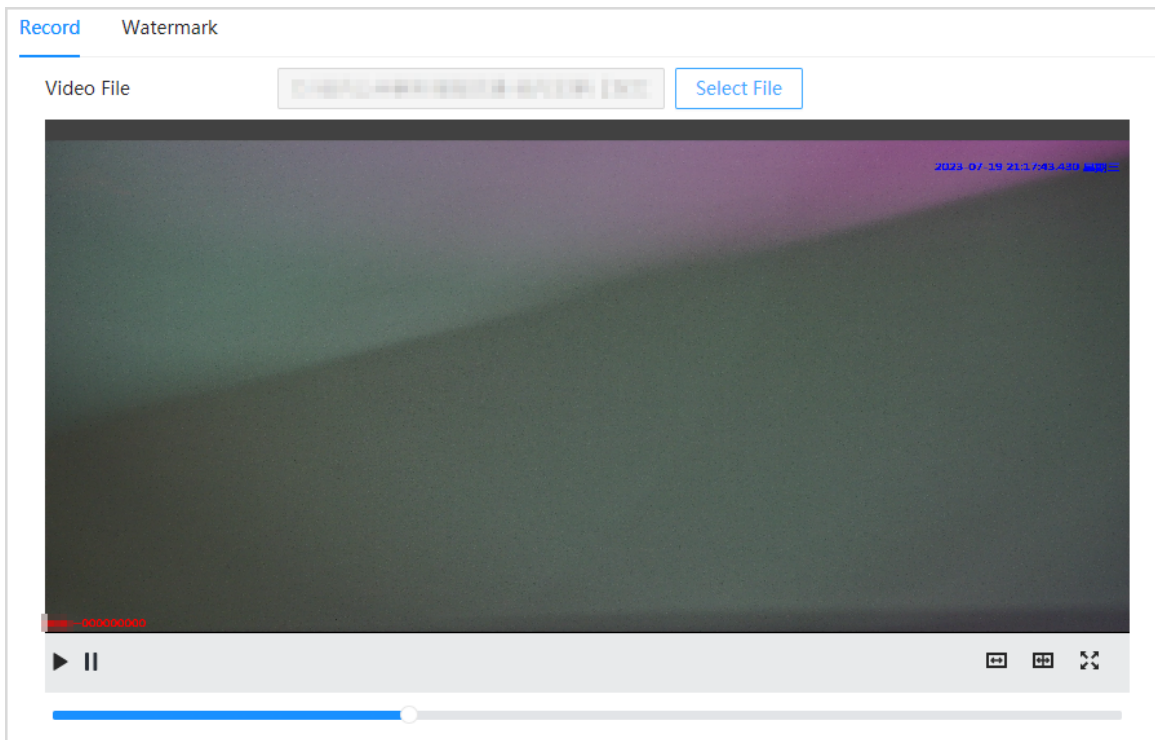







Table 8-2 Description of play parameters

Icon	Description
	Select Original or Adaptive playback.
	Click it to enable smart track detection. Number plate, vehicle bounding box, and other smart tracking information will be displayed on the video image.
	Full screen. Double-click the video image or press Esc to exit.
	Play back the video.
	Stop playing back the current video.

8.3.2 Watermark

Prerequisites

Before verifying the watermark, you need to select **Watermark** and configure **Watermark String** from **Camera > Encode > Video Stream > Main Stream**.



The watermark character is **DigitalCCTV** by default.

Procedure

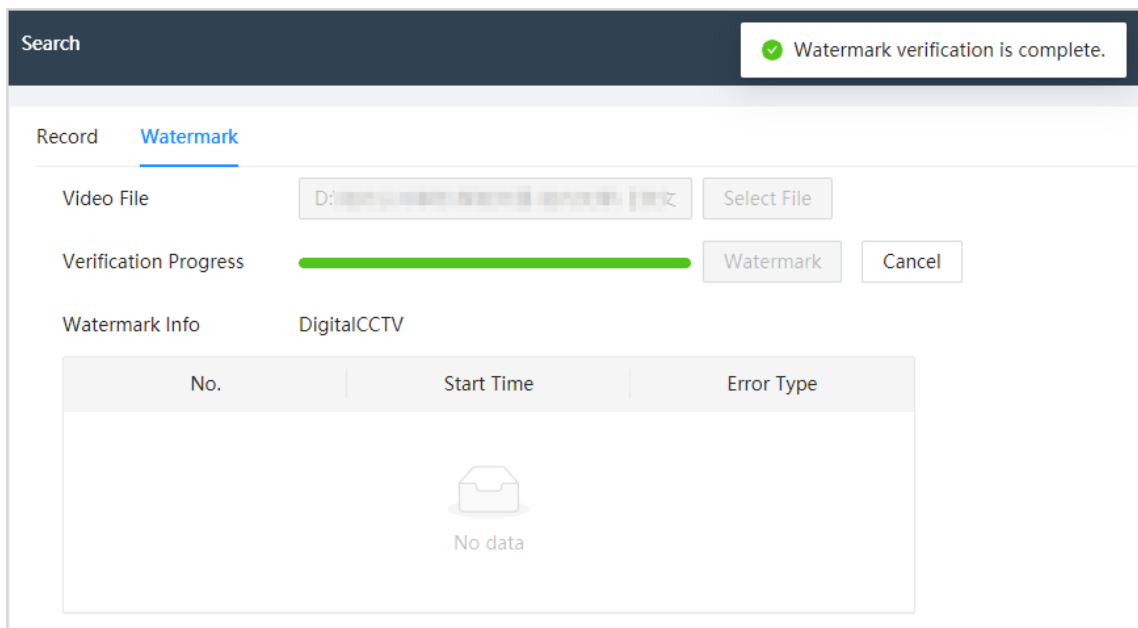
Step 1 Select **Search > Search Video > Watermark**.

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

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

If the video is verified to be authentic, the watermark you set is displayed next to **Watermark Info**.

Figure 8-5 Watermark



9 ITC

Configure smart plan, intelligent analysis, image, OSD, vehicle blocklist and allowlist, and view traffic flow statistics.

9.1 Configuring Smart Plan

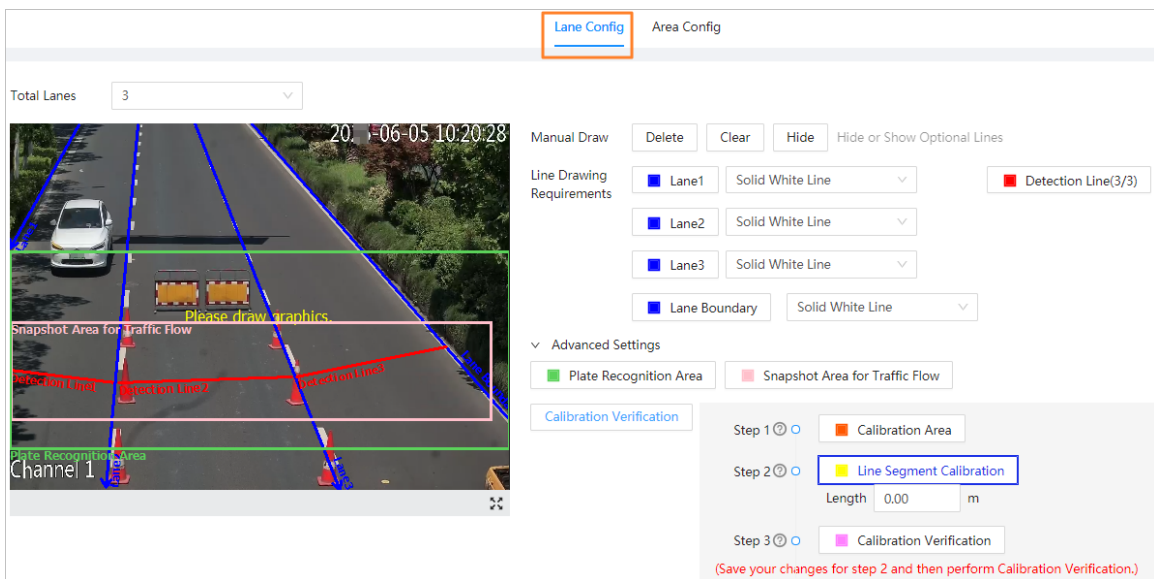
9.1.1 ANPR Mode

Configure lines and detection rules for lanes and intrusion rules.

Procedure

- Step 1 Select **ITC > Smart Plan**.
- Step 2 Select **ANPR** intelligent scheme, which mainly focuses on identifying vehicles by capturing and analyzing license plates.
- Step 3 Click **AI Config**, and then click the **Lane Config** tab to configure the lane parameters.


Figure 9-1 Configure the lines



1. Configure the lines for lanes.
 - **Manual Draw** : You can click **Delete** to delete the lines. You can also click **Clear** to clear all lines.
 - **Line Drawing Requirements** : You can draw lane line for lane1,2 and 3, and draw right lane boundary and detection line for lane1.
2. (Optional) Click **Advanced Settings** to **Plate Recognition Area**, **Snapshot Area for Traffic Flow**, and **Calibration Verification**.

Table 9-1 Parameter description

Parameter	Description
Plate Recognition Area	The area for recognizing the license plates of vehicles.
Snapshot Area for Traffic Flow	The area for capturing vehicles to make statistics of traffic flow.

Parameter	Description
Calibration Verification	Used to verify the accuracy of calibration results. Follow the onscreen steps to perform the verification. You can click  to view the instructions of each step.

3. Configure the parameters for lanes.

Figure 9-2 Configure the lane parameters

▼ Lane Configuration

Lane Direction: Vehicle Front Vehicle Back Lane Type:

Custom Lane No.: Distance between Stop ...: cm(-10000-8000)

Passing Direction: Lane Description:

Table 9-2 Parameter description

Parameter	Description
Lane Direction	Set the lane direction as Vehicle Front or Vehicle Back .
Lane Type	Set the lane type as General Lane , Motor Vehicle Lane , Non-Motor Vehicle and Bus Lane .
Custom Lane No.	Customize the lane number to differentiate it from others.
Distance between Stop Line and Image Bottom	Set the distance between the stop line and the bottom of the image.
Passing Direction	Configure the passing direction of the vehicle. You can select South to North , West to East , North to South , East to West or Custom .

4. Configure the speed limit for different types of vehicles.

Figure 9-3 Configure the speed of vehicles

Distinguish Speed Limit by Vehicle Type

Large Passenger Vehicle

Vehicle Min Speed Limit: km/h(0-180) - km/h(0-180) Large Passenger Vehicl...: km/h(0-180) + km/h(0-180)

Small Passenger Vehicle

Vehicle Min Speed Limit: km/h(0-180) - km/h(0-180) Small Passenger Vehicl...: km/h(0-180) + km/h(0-180)

Truck

Vehicle Min Speed Limit: km/h(0-180) - km/h(0-180) Truck of Highest Speed ...: km/h(0-180) + km/h(0-180)

Van

Vehicle Min Speed Limit: km/h(0-180) - km/h(0-180) Van of Highest Speed L...: km/h(0-180) + km/h(0-180)

- **Vehicle Min Speed Limit** : The low speed limit that when reached, causes a signal to be sent to the Camera to take snapshots.
- **Highest Speed Limit** : The high speed limit that when reached, causes a signal to be sent to the Camera to take snapshots.

5. Configure events for lanes.

- Select a lane.

- b. Click **Add Event**.
- c. Select the event that you want to configure, and then click **OK**.



Click **Select All** to select all events.

- d. Configure the parameters for every event that you add.

Figure 9-4 Configure the parameter of ANPR

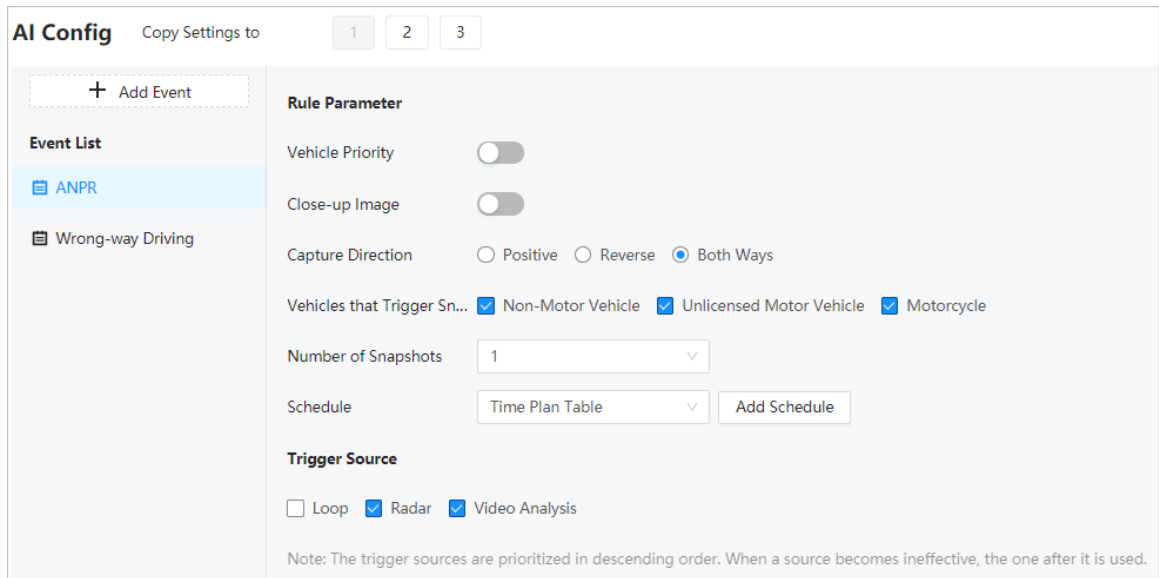




Table 9-3 Parameter description of ANPR

Parameter	Description
Copy Settings to	Copy settings of the current lane to another lane.
Vehicle Priority	Click  to enable the function. If vehicles enter the trigger line with plate obscured, the camera will not capture until the plate displays totally.
Close-up Image	The close-up of the offending vehicle.
Capture Direction	Vehicle driving direction to the camera.
Vehicle that Trigger Snapshots	Select the vehicle type to take snapshots.
Number of Snapshots	The number of snapshots.
Schedule	The period during which alarms will be triggered. To set a time, click Add Schedule , and then drag the slider over the time table to configure the time. If you want to add more schedules, click +Time Plan Table .  <ul style="list-style-type: none"> ● Click Clear to reset time. ● Click Copy to copy the defined time to other days, and then click Apply.


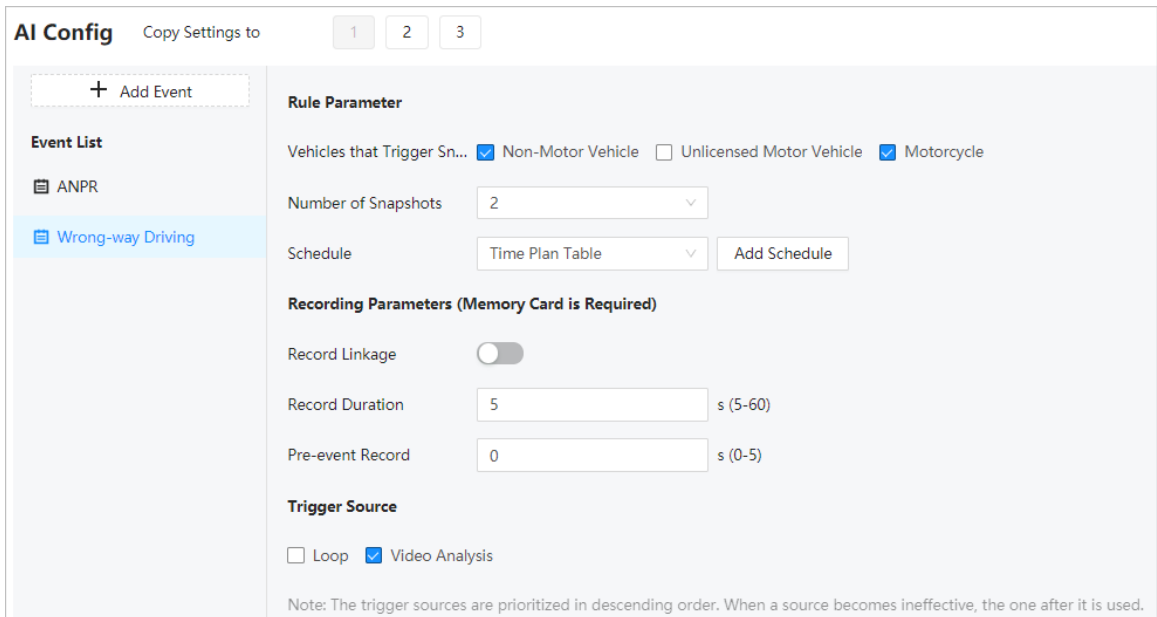
Parameter	Description
Trigger Source	Select trigger sources from Loop (only available for ANPR mode without radar), Radar and Video Analysis .  The trigger sources are prioritized in descending order. When a source becomes ineffective, the one after it is used.

Figure 9-5 Configure the parameters of wrong-way driving



AI Config Copy Settings to 1 2 3

Event List

- ANPR
- Wrong-way Driving**

Rule Parameter

Vehicles that Trigger Sn... Non-Motor Vehicle Unlicensed Motor Vehicle Motorcycle

Number of Snapshots: 2

Schedule: Time Plan Table

Recording Parameters (Memory Card is Required)

Record Linkage:

Record Duration: 5 s (5-60)



Pre-event Record: 0 s (0-5)

Trigger Source

Loop Video Analysis

Note: The trigger sources are prioritized in descending order. When a source becomes ineffective, the one after it is used.

Table 9-4 Parameter description of wrong-way driving

Parameter	Description
Rule Parameter	Refer to the table above.
Recording Parameters	<p>Record Linkage: Click  to enable the record linkage function. When the event is captured, the Camera will automatically record the corresponding videos according to the defined record duration and pre-event record (record made before the event occurs).</p>
Trigger Source	Select trigger sources from Loop (only available for ANPR mode without radar) and Video Analysis .  The trigger sources are prioritized in descending order. When a source becomes ineffective, the one after it is used.

e. (Optional) Configure global configurations for the Camera according to your needs.

Figure 9-6 Global configuration

Global Config

Measure Speed by Radar Only suitable for scenes where the target is recognized by a camera and the speed is measured by a radar.

Max Speed km/h (0-180)

Spacing between Vehicl... cm (0-25500)

Violation Priority

Capture Interval Mode (Supports checkpoint scene and loop mode)

I Frame Interval

Self-adaptive

0km/h ≤ Low Speed < ≤ Medium ≤ < High Speed ≤ 180km/h

Frame Interval for Low-...

Frame Interval for Medi...

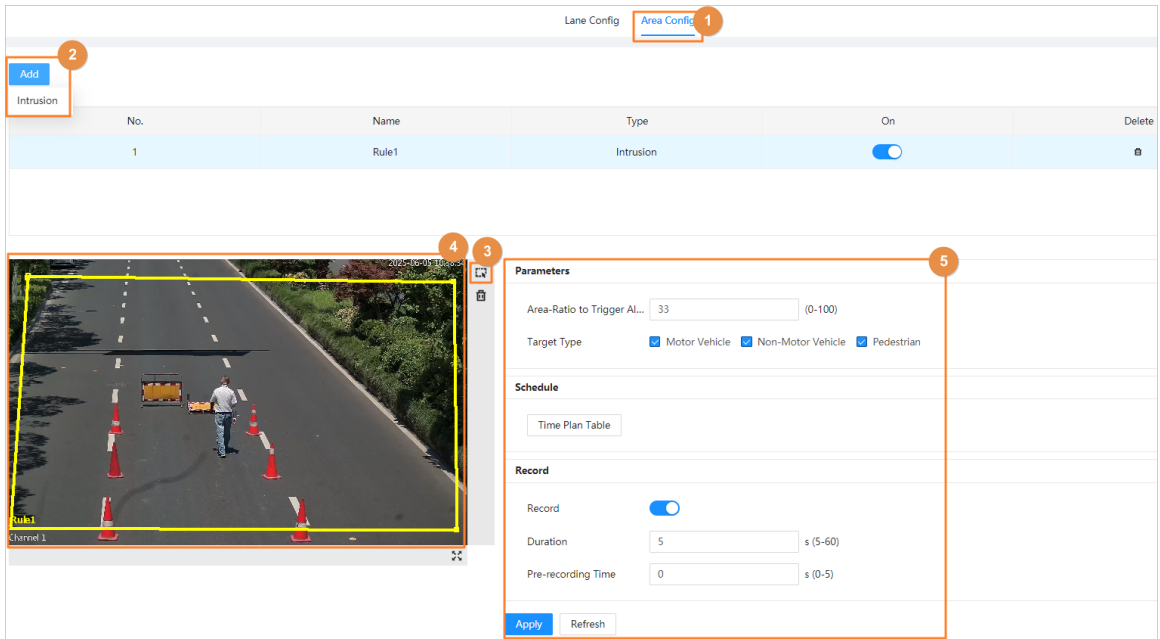
Frame Interval for High...

Table 9-5 Global configuration parameters

Parameter	Description
Max Speed	The maximum speed limit allowed. The radar measures the speed of a vehicle, and compares it to this limit to detect violations.
Spacing between Vehicles	The distance between 2 consecutive vehicles.
Violation Priority	The priority used to rank different traffic violations.
Capture Interval Mode	<ul style="list-style-type: none"> ● I frame interval: It sets a fixed time or frame count between successive I-frames. Shorter interval provides better quality but larger storage and bandwidth usage, while longer interval needs smaller file sizes but potential artifacts during fast motion or scene changes. ● Self-adaptive: You can define the range of low, medium, and high speeds, and set the frame interval for each speed level.

Step 4 Click the **Area Config**, and then you can configure the area and rules for intrusion. When the defined targets intrude the drawn area, the Camera will take snapshots and record videos according the defined parameters.

Figure 9-7 Area configuration











1. Click **Add** , and then select **Intrusion**.
2. Click  , and then draw an area on the video image for detection. Right click to finish drawing.

 Click  to detect the drawn area.
3. Configure the parameters.

Table 9-6 Parameter description

Parameter	Description
Area-Ratio to Trigger Alarm	The sensitivity of the detection.
Target Type	The type of targets that the intrusion rules work on.
Time Plan Table	<p>Set when the intrusion rules take effect.</p> <ol style="list-style-type: none"> a. Click Time Plan Table. b. Click the timeline, and then drag  to set the arming periods. Alarms will be triggered in the green period.  You can set 6 periods per day. c. Click Apply.  Click Copy next to a day, and then select the days that you want to copy to in the prompt page, you can copy the configurations to the selected days.

Parameter	Description
Record	 Click  to enable the record function. When the event is captured, the Camera will automatically record the corresponding videos according to the defined record duration and pre-recording time (record made before the event occurs).
Duration	
Pre-recording Time	

4. Click **Apply**.

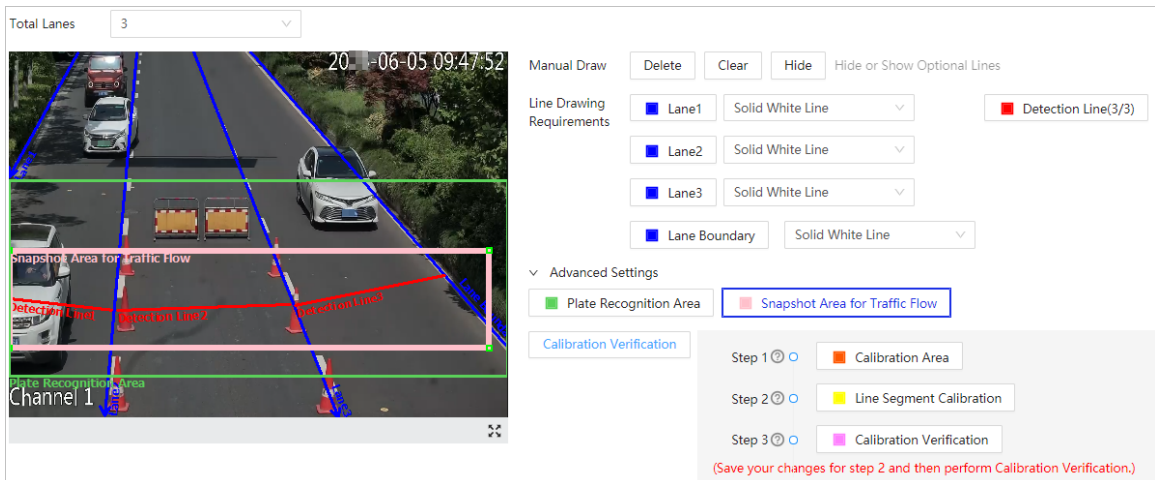
9.1.2 Road Monitoring Mode

Configure lines and detection rules for lanes.

Procedure

- Step 1** Select **ITC > Smart Plan**.
- Step 2** Select **Road Monitoring** intelligent scheme, which is suitable for traffic management such as tracking traffic flow.
- Step 3** Click **AI Config**, and then configure the lines for lanes. For details, see 1 and 2 in "9.1.1 ANPR Mode".

Figure 9-8 Configure the lines



- Step 4** Configure the parameters for lanes.

Figure 9-9 Configure the lane parameters

Lane Configuration	
Custom Lane No.	<input type="text" value="1"/>
Distance between Stop ...	<input type="text" value="0"/> cm(-10000-8000)
Passing Direction	<input type="text" value="South to North"/>
Lane Description	<input type="text"/>

Table 9-7 Parameter description

Parameter	Description
Custom Lane No.	Customize the lane number to differentiate it from others.


Parameter	Description
Distance between Stop Line and Image Bottom	Set the distance between the stop line and the bottom of the image.
Passing Direction	Configure the passing direction of the vehicle. You can select South to North , West to East , North to South , East to West or Custom .
Lane Description	Customize the description on the lane.

Step 5 Configure the ANPR event for lanes.

1. Click **Add Event**.
2. Select **ANPR** , and then click **OK**.
3. Configure the parameters.

Figure 9-10 Configure the parameter of ANPR

Table 9-8 Parameter description of ANPR

Parameter	Description
Quality	You can set the snapshot quality by either quality or size. <ul style="list-style-type: none"> ● Quality: 6 quality levels are available. The higher the value, the better the quality. ● Size: The size of a snapshot.
Size	
Number of Snapshots	The number of snapshots that will be taken when plate number is recognized.
Schedule	The period during which alarms will be triggered. To set a time, click Add Schedule , and then drag the slider over the time table to configure the time. If you want to add more schedules, click +Time Plan Table .  <ul style="list-style-type: none"> ● Click Clear to reset time. ● Click Copy to copy the defined time to other days, and then click Apply.

Step 6 Click **Apply**.

9.2 Intelligent Analysis

Configure the intelligent functions of the Camera.



This function is not available in road monitoring mode.



9.2.1 Recognition

Procedure

Step 1 Select **ITC > Intelligent Analysis > Recognition**.

Figure 9-11 Recognition

Table 9-9 Parameter description of recognition

Parameter	Description
Motor Vehicle	<p>Click  to enable metadata information of motor vehicle, including motor vehicle logo and vehicle type.</p> <p>Click  to view the detailed information of metadata information.</p>
Non-motor Vehicle	Identifies non-motor vehicle attributes such as type, helmet, and the number of passenger.
Other	<ul style="list-style-type: none"> ● License Plate Enhancement : Enhances number plate image effect (function reserved). ● Track Overlay : Enable track overlay, and then you can see each vehicle is covered by a green frame on Live page, which means each vehicle is tracked.

Step 2 Click **Apply**.

9.2.2 Advanced Settings


You can make a custom algorithm.

Procedure

Step 1 Select **ITC > Intelligent Analysis > Advanced Settings**.

Step 2 Configure a custom algorithm.



Click  to view the instructions on how to set custom algorithm expressions.

Step 3 Click **Apply**.

9.3 Configuring Image



This function is not available in road monitoring mode.

9.3.1 Configuring Picture Parameter

You can configure the parameter of the image of the captured vehicle.

Procedure

Step 1 Select **ITC > Image Config > Picture Parameter**.

Figure 9-12 Picture parameter

Picture Parameter
Snapshot Composition
Cutout Config

Original Image

Quality

6(Best) ▼

Size

1024

KB(200-2048)

Composite Picture

Image Resolution

Normal Proportion ▼

Quality

3 ▼

Size

5120

KB(1024-5120)

Close-up Image

Quality

6(Best) ▼

Size

2048

KB(200-2048)

Apply

Refresh

Default

Step 2 Configure the parameters of the picture.

Table 9-10 Parameter description of picture

Parameter	Description
Original Image	The original picture of the vehicle that is violating traffic rules.
Composite Picture	The compound picture of several sequential images of the vehicle violating the traffic rules.
Close-up Image	The close-up of the offending vehicle.
Quality	You can set the snapshot quality by either quality or size.
Size	<ul style="list-style-type: none"> ● Quality: 6 quality levels are available. The higher the value, the better the quality. ● Size: The size of a snapshot.

Step 3 Click **Apply**.

9.3.2 Configuring Snapshot Composition



Procedure

Step 1 Select **ITC > Image Config > Snapshot Composition**.

Figure 9-13 Snapshot composition

Step 2 Configure the parameters of snapshot composition.

Table 9-11 Parameter description of snapshot composition

Parameter	Description
Composite Picture	Click  to enable this function, and the select ANPR or Violation . The camera will upload original pictures and composite pictures of ANPR and other events.
Upload All	Click  to enable this function, and then you can upload original picture and composite pictures.
Combination Mode for Pictures	Select combination mode for different number of pictures.
Feature Picture No.	Configure the number of the picture, you can select Auto or a specific number.
Composite Sequence of One Picture	Select how the picture will be composed.
Feature Picture No.	Configure the number of the picture, you can select Auto or a specific number.
Close-up Area	Set the width and altitude of the area that a close-up image will be composed.

Step 3 Click **Apply**.

9.3.3 Configuring Cutout

The Camera can recognize and crop snapshots, and save the cutouts.

Procedure

Step 1 Select **ITC > Image Config > Cutout Config**.

Figure 9-14 Configure cutout

Step 2 Configure the parameters.

Table 9-12 Parameter description of cutouts

Parameter	Description
Cutout Config	Select cutout type for motor vehicles, non-motor vehicles, and pedestrians.
Target Box	Configure overlay track box on the driver of motor vehicles and non-motor vehicles.

Step 3 Click **Apply**.

9.4 Traffic Flow Statistics



This function is not available in road monitoring mode.

9.4.1 Flow Data

You can configure the lane and the period of traffic flow statistics, and then the flow data will be displayed in the **Traffic Flow** and **Pedestrian Flow**.

Procedure

Step 1 Select **ITC > Traffic Flow Statistics > Flow Data**.

Figure 9-15 Flow data



The screenshot shows a configuration panel for flow data. At the top, under 'Traffic Flow', there are four blue buttons labeled '1', '2', '3', and '4'. Below that, 'Pedestrian Flow' has a blue toggle switch that is currently turned on. The 'Statistical Cycle' is set to '60' with a unit of 's (1-15000)'. The 'Flow Upper Limit' is set to '10000' with a range of '(100-10000)'. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Step 2 Select the lanes that you want to make flow statistics.

Step 3 Select the **Pedestrian Flow** checkbox to enable statistics of pedestrian flow as needed.

Step 4 Configure the **Statistical Cycle** and **Flow Upper Limit** of making statistics.

Step 5 Click **Apply**.

9.4.2 Traffic Flow

After enabling traffic flow statistics, you can view the traffic flow data of the defined lane within the defined period by clicking the **Traffic Flow**. The flow data will automatically update when a period ends.

- Click **Clear** to clear flow information.
- Click **Export** to export the flow information to local computer.

9.4.3 Pedestrian Flow

After enabling pedestrian flow statistics, you can view the pedestrian flow data of the defined lane within the defined period by clicking the **Pedestrian Flow**. The flow data will automatically update when a period ends.


- Click **Clear** to clear the flow information.
- Click **Export** to export the flow information to local computer.

9.4.4 Flow Control

After enabling this function, the camera will transmit the captured traffic data to the traffic signal controller. You can configure the lane and the period of traffic flow statistics, and then the flow data will be displayed in the **Traffic Flow** and **Pedestrian Flow**.

Procedure

Step 1 Select **ITC > Traffic Flow Statistics > Flow Control**.

Step 2 Click  to enable the function.

Step 3 Set the loop length, which affects the coverage of the loop, and the number of loops, which affect the sensitivity of the loop.

Step 4 Click **Apply**.

9.5 Configuring OSD

Configure OSD content, style and position for captured image.

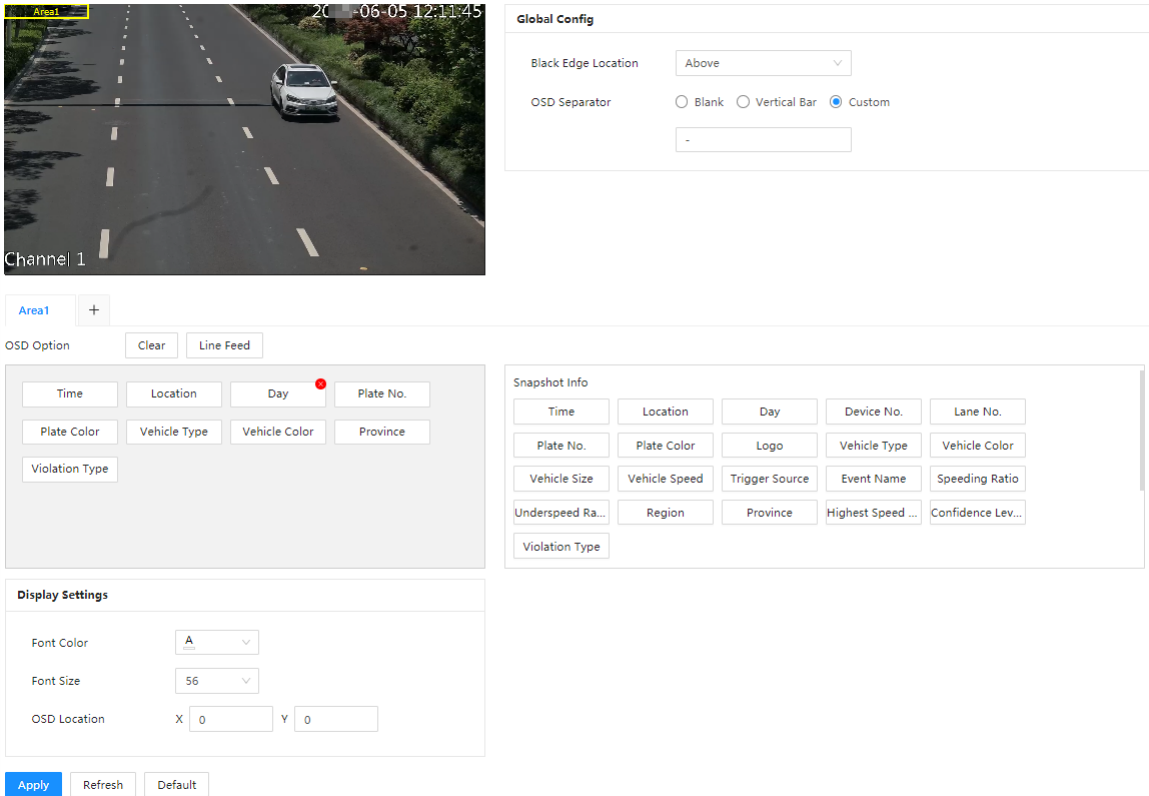
9.5.1 Configuring Original Picture OSD

Configure OSD information overlaid on original pictures.

Procedure


Step 1 Select **ITC > OSD Config > Original Picture OSD**.


Figure 9-16 Original picture OSD



Step 2 Configure OSD black edge position and OSD separator.

Step 3 Configure OSD parameters.

- Click a field (such as **Time**) in the **Snapshot Info** section to select an OSD option.
- **Line Feed**: To start a new line after a certain OSD option, click the OSD option, and then click **Line Feed**.
- **Clear**: Delete all the selected OSD options.
- Hover the mouse over the OSD options selected, and then click  to delete the option.

- Click a selected OSD option, and then configure the prefix, suffix and delimiter quantity of the OSD option.
- Click  to add a new area, and then configure the OSD.

Step 4 Configure the display settings, including the font color, font size, and display position of the OSD.

Step 5 Click **Apply**.

9.5.2 Configuring Combination Picture OSD

Configure OSD information overlaid on composite images.

Procedure

Step 1 Select **ITC > OSD Config > Combination Picture OSD**.

Step 2 Configure the parameters. For details, see "9.5.1 Configuring Original Picture OSD".

Step 3 Click **Apply**.

9.6 Configuring Blocklist and Allowlist

An alarm is triggered when a vehicle is detected in the blocklist. A vehicle in the allowlist will not be captured.

9.6.1 Allowlist

You can add plate numbers to the allowlist, search to check whether the plate number is in the allowlist, or export plate numbers.

Procedure

Step 1 Select **ITC > Vehicle Blocklist/Allowlist > Allowlist**.

Step 2 Click  to enable allowlist.

Step 3 Add a plate number.

1. Click **Add**.

Figure 9-17 Add

The 'Add' dialog box contains the following fields and options:

- * Plate No. (text input)
- Owner Name (text input)
- Plate Type (dropdown menu: Personal Vehicle)
- Plate Color (dropdown menu: Black)
- Vehicle Type (dropdown menu: Large-sized)
- Vehicle Color (dropdown menu: White)
- Start Time (date picker: 2025-06-05)
- End Time (date picker: 2025-06-05)
- Add More
- Buttons: Cancel, OK

2. Enter the entire plate number and owner name.
3. Select the plate type, plate color, vehicle type and vehicle color.
4. Configure the start time and end time to add the plate number to the allowlist. The plate number will be outside of the allowlist beyond this period of time.
5. Click **OK**.



To save and add more, select **Add More** before clicking **OK**.

Related Operations

- Search for a plate number: Enter the plate number (or part of it) that you want to search for, and then click **Search** to check whether it is in the allowlist.
- Delete a plate number: Click **Delete** to delete the corresponding plate number.
- Delete plate numbers in batches: Click **Clear**, and then click **OK** in the pop-up box to delete all the information in the allowlist.
- Import allowlist plates in batches: Click **Import**, and then download template. Fill in the template, and then click **Select File** to select the template to import the allowlist information to the system.
- Export allowlist plates in batches: Click **Export**, and then select the path to save the file to. Click **Export** to export the allowlist information to the system.



You can encrypt the file when importing and exporting the allowlist, depending on your actual needs.

9.6.2 Blocklist Search

An alarm will be triggered when a vehicle in the blocklist is detected.

Select **ITC > Vehicle Blocklist/Allowlist > Blocklist**, and then click to enable the blocklist function.

The adding, search, import, and export of blocklist are similar to that of allowlist. For details, see "9.6.1 Allowlist".

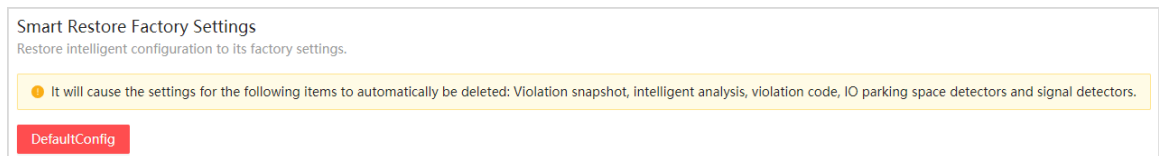
9.7 Smart Restore Factory Settings

Select **ITC > Smart Restore Factory Settings**, and then click **DefaultConfig** to restore configurations of the camera to default settings.



This function will cause violation, snapshot, intelligent analysis, violation code, IO parking space detectors and signal detectors to be deleted, please be advised.

Figure 9-18 Smart restore factory settings



10 Network Settings

You can configure network parameters such as TCP/IP, port, auto registration, basic services and ITSAPI.

10.1 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.

Background Information



Some models are designed with two network ports. Do not configure the ports to be on the same network segment. Otherwise, the network might fail.

Procedure

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

Figure 10-1 TCP/IP

* Host Name	ITC
* NIC	Wired(Default) ▾
* Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	e-11-22-33-44-55-5c
IP Version	IPv4 ▾
IP Address	192 . 168 . 129 . 23
Subnet Mask	255 . 255 . 255 . 0
Default Gateway	192 . 168 . 129 . 1
Preferred DNS	2 5
Alternate DNS	2 6
<input type="button" value="Apply"/> <input type="button" value="Refresh"/>	

Step 2 Configure the parameters.

Table 10-1 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.
NIC	Supports wired network only.
Mode	<p>The mode that the camera gets IP:</p> <ul style="list-style-type: none"> ● Static : Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Apply, the login page with the configured IP address is displayed. ● DHCP : The Camera automatically assigns IP addresses. In this case, the IP Address, Subnet Mask, and Default Gateway cannot be configured.
MAC Address	Displays host MAC address.
IP Version	IPv4 and IPv6 are available. Both IP version can be accessed.
IP Address	When you select Static in Mode , enter the IP address and subnet mask that you need.
Subnet Mask	
Default Gateway	<ul style="list-style-type: none"> ● IPv6 does not have subnet mask. ● The default gateway must be in the same network segment with the IP address.
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

Step 3 Click **Apply**.

10.2 Port

10.2.1 Configuring Port

You can set the port information. Then, you can access the Camera through different protocols or configuration tools.

Procedure

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

Figure 10-2 Port

Parameter	Value	Range
* Max Connection	10	(1-20)
* TCP Port	37777	(1025-65534)
* HTTP Port	80	(1025-65534)
* RTSP Port	554	(1025-65534)
* HTTPS Port	443	(1025-65534)
* SSH Port	22	(1025-65534)

Step 2 Configure port parameters.

Table 10-2 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. It is 10 by default.
TCP Port	TCP protocol communication port. It is 37777 by default.
HTTP Port	HTTP communication port. It is 80 by default.
RTSP Port	Media streaming control port. It is 554 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.
SSH Port	Secure remote access port. It is 22 by default.

Step 3 Click **Apply**.

10.2.2 Configuring ONVIF

Open Network Video Interface Forum (ONVIF) is an open industry forum with the goal of providing and promoting standardized pages for interoperability of physical IP-based security products, such as IP camera, and network recorder, and more.

Select  > **Network Settings** > **Port** > **ONVIF**.

Verification of username and password will be required for logging in to ONVIF when ONVIF authentication is turned on. If it is turned off, then no verification is required.

Figure 10-3 Configure ONVIF

10.3 Auto Registration

When the Camera is connected to the network, it will automatically report its location to the server specified by the user. This helps client software to access the Camera through the server for viewing and monitoring the live video.

Procedure

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

Figure 10-4 Auto registration

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

Table 10-3 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**.

10.4 Multicast

Multicast allows one sender transmits data to multiple recipients simultaneously over a network. Ideal for streaming media or distributing data to many devices without overloading the network.

Procedure

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

Step 2 Click to enable multicast of main stream and sub stream as needed.

Figure 10-5 Multicast

Main Stream	Sub Stream
Enable <input checked="" type="checkbox"/>	Enable <input checked="" type="checkbox"/> Sub Stream 1
Multicast Address <input type="text" value="224 . . . 4"/> (224.0.0.0-239.255.255.255)	Multicast Address <input type="text" value="224 . . . 4"/> (224.0.0.0-239.255.255.255)
Port <input type="text" value="10000"/> (1025-65534)	Port <input type="text" value="10016"/> (1025-65534)
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

Step 3 Configure the multicast address and port.

- Multicast address: The IP address that identifies a multicast group. Devices use this address to send or receive multicast traffic.
- Port: Used to direct traffic to the correct service on a device.

Step 4 Click **Apply**.

10.5 Email

You can configure the email server and the receiver, and the email content that will be sent to the receiver.

Procedure

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

Step 2 Click to enable the email function.

Step 3 Configure the parameters.



The events might vary depending on the actual product.

Parameter	Description
Health Mail	Send an mail at the defined interval to ensure that the email function works normally.
Sending Interval	
Image Config	Select the type of image that will be included in the email.
Event Config	Select the type of event that will be included in the email.

Step 4 Click **Apply**.

10.6 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 Settings** > **Basic Services**.

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

Table 10-5 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 (recommended) and Compatible Mode .
TLSv1.1	Enable this function so that you can access the webpage with TLSv1.1.  There might be security risks if you enable this function. Please be advised.
LLDP	LLDP (Link Layer Discovery Protocol) is a network protocol that allows network devices to share information about themselves with neighboring devices.

Step 3 Click **Apply**.

10.7 ITSAPI

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

Background Information

- 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 Settings** > **ITSAPI**.


Figure 10-7 ITSAPI

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

Step 3 Configure the parameters.

Table 10-6 Parameter description

Section	Parameter	Description
Basic	Authentication	Enable the function, and then you need to set the username and password for device authentication.
	Platform Server	The URL or IP address where the device sends data to.
	Device ID	A unique identifier to distinguish the device in the platform.
	Keep Alive Interval	Update interval of the connection between the server and the device.
	Authentication	Enable the function, and then you need to set the username and password for device authentication.
	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.
	Protocol Version	Setting is not supported and subject to actuality.

Section	Parameter	Description
	Heartbreak Interface	Set the interface according to the data type.
	Need Response	Select Yes or No . <ul style="list-style-type: none"> ● Yes: Suitable for scenarios that require real-time feedback. ● No: Suitable for scenarios that do not require real-time feedback.
	Function	Select the Basic Info , ANPR , or E-police be uploaded.  E-police is not available in road monitoring mode.
	Upload Info	Select the specific information to be uploaded.
	Type of Upload Content	The type of content that will be sent.
	Device ID	A unique identifier to distinguish the device in the platform.
	Image Config	Image Type
Filter Condition		Select whether to upload information of unlicensed vehicles.
Uploading Info		Select the specific information to be uploaded.
Encoding Format		Select the license plate encoding. <ul style="list-style-type: none"> ● UTF-8 supports many languages and it is selected by default. ● ASCII supports relatively few languages, generally only English and some symbols.


Step 4 Click **Apply**.

10.8 Network Proxy

A network proxy acts as an intermediary between your device and the internet. It helps hide your location, block dangerous websites, and more.

Procedure

Step 1 Select  > **Network Settings** > **Network Proxy**.

Step 2 Click  to enable network proxy.

Step 3 Click **Add**, configure local port, remote IP address, and remote port, and then click **OK**.

- Local port: The port on your local device where the proxy server listens.
- Remote IP address: The IP address of the destination server the proxy will forward traffic to.
- Remote port: The port on the destination server (remote IP) that the proxy connects to.

Step 4 Click **Apply**.

11 Event

You can configure how the Camera responds when alarms or abnormal events occur.

11.1 Alarm

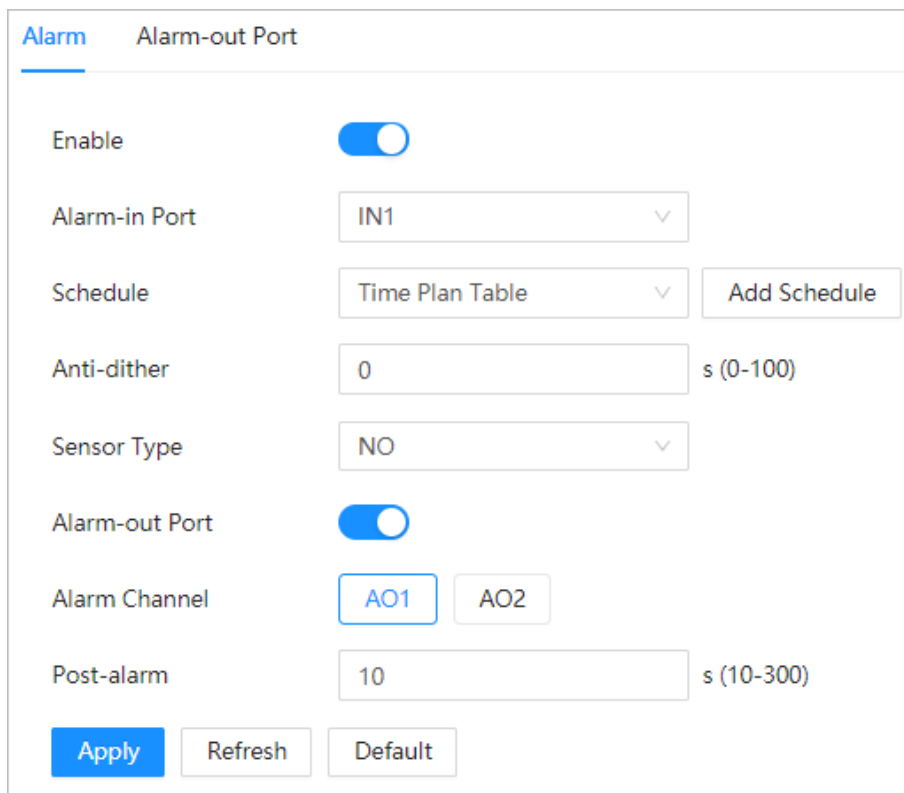
11.1.1 Enabling Alarm-in and Alarm-out Ports

You can connect the alarm output device to corresponding I/O port.

Procedure


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

Figure 11-1 Alarm



Enable	<input checked="" type="checkbox"/>
Alarm-in Port	IN1
Schedule	Time Plan Table ▼ Add Schedule
Anti-dither	0 s (0-100)
Sensor Type	NO
Alarm-out Port	<input checked="" type="checkbox"/>
Alarm Channel	AO1 AO2
Post-alarm	10 s (10-300)

Apply Refresh Default

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

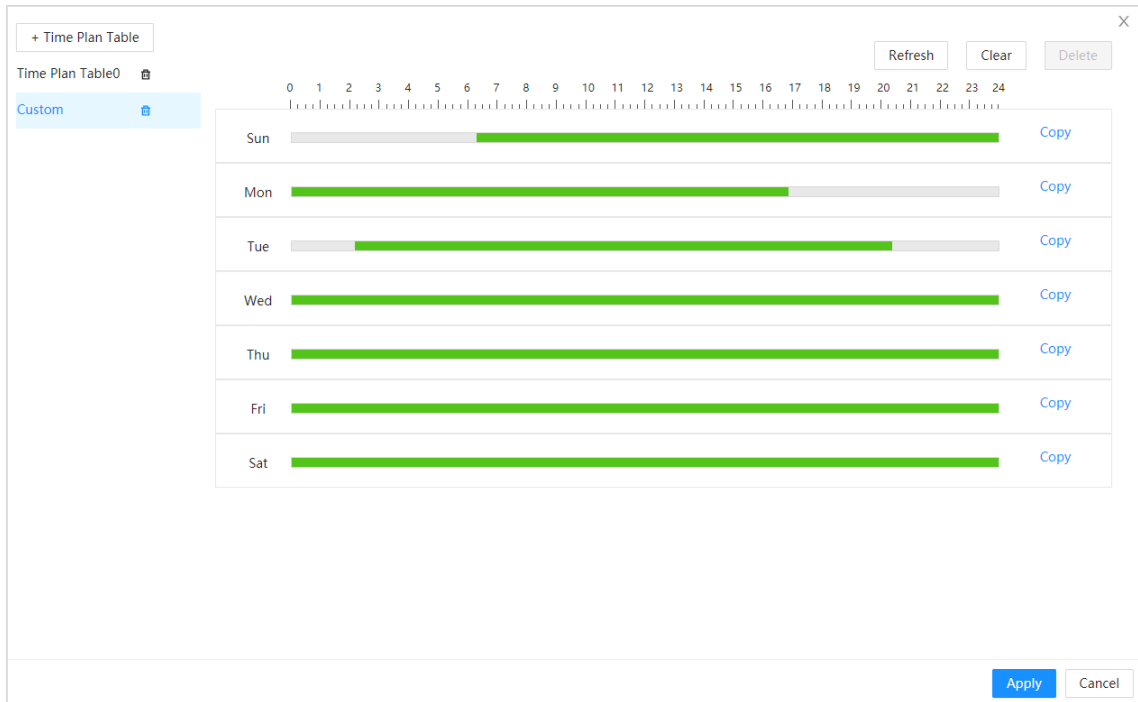
Step 3 Select an alarm input channel and schedule.



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

1. Click **Add Schedule**.
2. Drag on the timeline to set the arming periods. Alarms will be triggered in the green period.
3. Click + **Time Plan Mode** to add more schedules.
4. Click **Apply**.

Figure 11-2 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**.
- You can set 6 periods per day.

Step 4 Configure the parameters.

Table 11-1 Parameter description

Parameter	Description
Anti-dither	Enter anti-dither time (1 s–100 s). System will only record one when there are multiple alarms during the defined time.
Sensor Type	Select relay-in type according to the connected alarm input device. <ul style="list-style-type: none"> ● NO : Normally open. ● NC : Normally closed.
Alarm-out Port	Click <input type="checkbox"/> , and then select one or more alarm output channels. The corresponding device will be activated when alarms are triggered.
Alarm Channel	
Post-alarm	The alarm linkage keeps running for the defined time after alarm ends. The time range is 10 seconds–300 seconds.

Step 5 Click **Apply**.

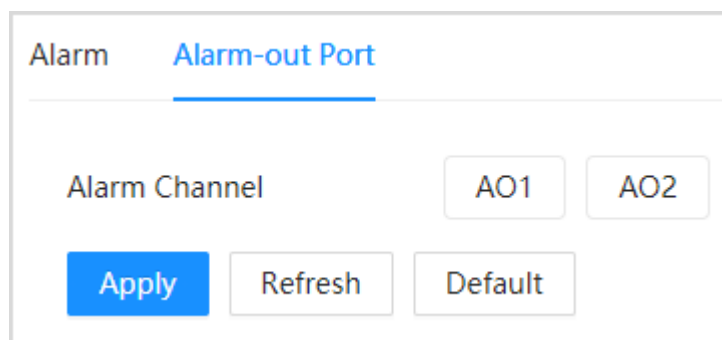
11.1.2 Alarm-out Ports

You can check whether alarm-out ports are working properly.

Procedure

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

Figure 11-3 Alarm-out port



Step 2 Select **AO1** or **AO2** to configure one-channel alarm output.

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

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

11.2 Exception

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

Prerequisites

Only the device with SD card has the anomaly functions, including no SD card, SD card error, and low SD card space.

Background Information

An alarm will be triggered when an abnormal event occurs. The event types are as follows.

- **SD Card Exception** : Alarm will be triggered when there is **No SD card, Low SD card space, or SD card error**.
- **Network Exception** : Alarm will be triggered when there is **Offline** (the Camera is offline) or **IP Conflict**.
- **Vehicle Blocklist** : Alarms will be triggered if vehicles in the blocklist are detected.
- **Unlicensed Vehicle** : Alarms will be triggered if unlicensed vehicles are detected.
- **Intrusion** : Alarms will be triggered when intrusions are detected.



This function is not available in road monitoring mode.



You can set the alarm tone by selecting  at the upper right of the Camera's webpage.

11.2.1 Setting SD Card Exception

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

Procedure

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

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

Figure 11-4 Enable events

The screenshot shows a configuration page for enabling events. It is divided into three main sections, each with a toggle switch and configuration options:

- No SD card:** The toggle is turned on. The 'Alarm Channel' is set to AO1. The 'Post-alarm' duration is 10 seconds.
- Low SD card space:** The toggle is turned on. The 'Free Space' threshold is set to 10%. The 'Alarm Channel' is set to AO1. The 'Post-alarm' duration is 10 seconds.
- SD card error:** The toggle is turned on. The 'Alarm Channel' is set to AO1. The 'Post-alarm' duration is 10 seconds.

At the bottom of the page, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Step 3 Configure the parameters.

Table 11-2 Parameter description

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

Step 4 Click **Apply**.

11.2.2 Setting Network Exception

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

Procedure

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



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

Figure 11-5 Enable events

The screenshot shows a configuration window with two main sections: 'Offline' and 'IP Conflict'. Each section contains a toggle switch to enable the event, an 'Alarm-out Port' toggle, an 'Alarm Channel' selector with buttons for 'AO1' and 'AO2', and a 'Post-alarm' duration input field set to '10' with a unit of 'sec (10-300)'. At the bottom of the window are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Step 3 Configure the parameters.

Table 11-3 Parameter description

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

Step 4 Click **Apply**.

11.2.3 Setting Vehicle Blocklist

An alarm will be triggered if a vehicle in the blocklist is detected.


Procedure

Step 1 Select  > **Event** > **Exception** > **Vehicle Blocklist**.

Figure 11-6 Enable events

Step 2 Configure the parameters.

Table 11-4 Parameter description

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

Step 3 Click **Apply**.

11.2.4 Setting Unlicensed Vehicle

An alarm will be triggered if an unlicensed vehicle is detected.

Procedure

Step 1 Select  > **Event** > **Exception** > **Unlicensed Vehicle**.


Step 2 Click  to enable detection of the event.

Figure 11-7 Enable events

Step 3 Configure the parameters. For details, see Table 11-4 .

Step 4 Click **Apply**.



11.2.5 Setting Intrusion

An alarm will be triggered when intrusion is detected.



This function is not available in road monitoring mode.

Procedure

- Step 1 Select  > **Event** > **Exception** > **Intrusion**.
- Step 2 Click  to enable detection of the event.
- Step 3 Configure the parameters. For details, see Table 11-4 .
- Step 4 Click **Apply**.

12 Report

You can search for traffic flow data according to the search conditions.

Prerequisites

Make sure that the Camera is inserted with TR card before you can search for the traffic flow data.



This function is available for ANPR mode.

Procedure

Step 1 Select **Report > Traffic Flow**.

Step 2 Set search conditions, including time (today, this week, this month, or this year), lane, vehicle type, and speed.



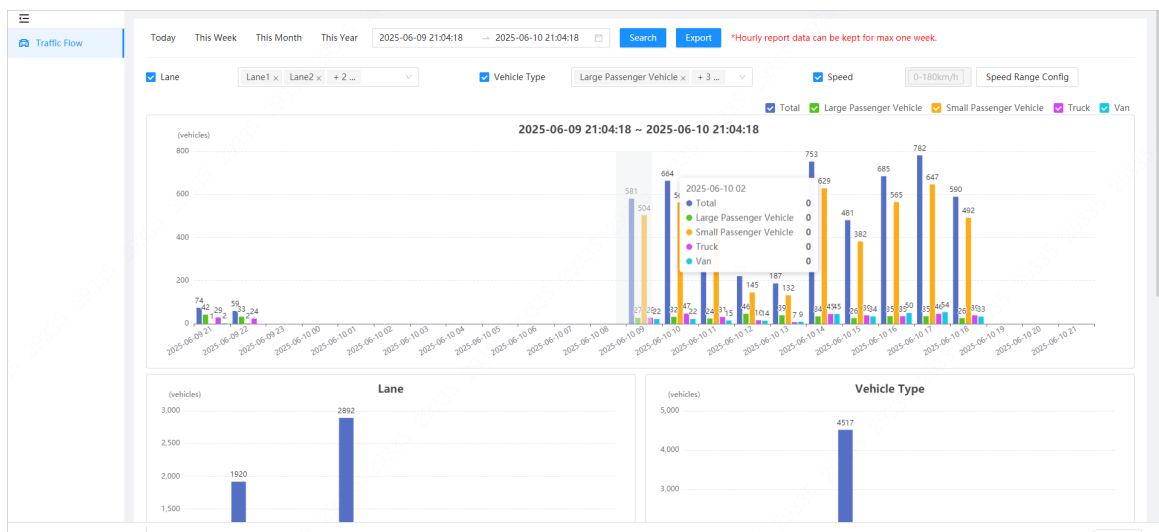
Click **Speed Range Config**, and then you can define the speed range that you want to search.

Step 3 Click **Search**.



Hourly report data can be kept for a maximum of one week.

Figure 12-1 Report



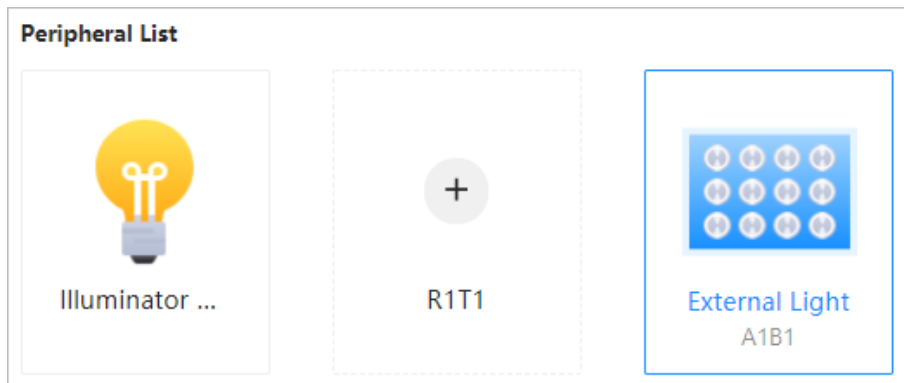
Step 4 (Optional) Hover over the graph, and then you can view the specific data, such as the data of different vehicle types.

13 Peripheral

You can view the status of the device, configure the work mode of the illuminator and the serial port of radar, external light and transparent.

Device Status

Figure 13-1 Status



Configuring the Parameters of Illuminator

Figure 13-2 Configuring the parameters of illuminator

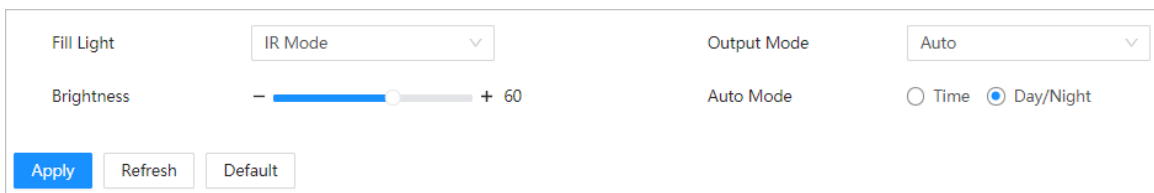


Table 13-1 Parameter description of illuminator

Parameter	Description
Fill Light	Select the type of the illuminator from IR Mode or White Light .
Output Mode	<ul style="list-style-type: none"> ● Always : The illuminator is always on. ● Close : The illuminator is always off. ● Auto : The illuminator turns on or off according to the ambient brightness.
Brightness	Both the darker areas and the brighter areas will be changed together when adjusting the brightness. The image might become blurry when the value gets bigger.
Auto Mode	You can set auto mode to Time or Day/Night . <ul style="list-style-type: none"> ● Time : Configure the time, and then the illuminator will on within the defined time. ● Day/Night : The illuminator will turns on or off according to the ambient brightness.

Configuring the Serial Port and Parameters of Radar

Figure 13-3 Configure the serial port of radar

Serial Port			
Type	RS-232	Protocol	ITARD-024SA-I ▼
Data Bit	8	Stop Bit	1
Baud Rate	9600	Verification Type	None

Table 13-2 Parameter description

Parameter	Description
Type	<p>RS-232 and RS-485 ports are supported.</p> <ul style="list-style-type: none"> RS-232 port can enable radar for single lane, and RS-485 enables radar for multiple lanes. You cannot enable single lane and multiple lanes at the same time. Only one external device can be enabled for one port at the same time. One serial port can only enable one external device.
Protocol	Keep it as default.

Figure 13-4 Configuring the parameters of radar

Device Config			
Enabled Lanes	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input type="checkbox"/> 4	Working Mode	Send Beams by Vehicle ▼
		Starts Monitoring from ...	1 (1-5)
Detection Direction	Approaching ▼	Distinguish Target Inter...	200 ms(0-65535)
Angle	20 °(0-45)	Sensitivity	3 ▼
Wait Time Before Captu...	3000 (0-10000)	Wait Time After Capture	1000 (0-10000)

Table 13-3 Parameter description


Parameter	Description
Enabled Lanes	The number of lanes on which the radar has been enabled.
Starts Monitoring from Lane	The lane number on which the radar starts detecting.
Number of Lanes	Number of radar lanes.
Wait Time Before Capture	During the speed wait, if the Camera reads the speed from the radar, it is the vehicle speed; Otherwise, the displayed vehicle speed is a random value within the speed limit.
Wait Time After Capture	

Configuring Transparent

- Click , and then select **Transparent** from **Device Type**.

2. Click **OK**.




You can hover over the peripheral icon, and then click  to delete the peripheral.

3. Configure the parameters.

Figure 13-5 Configuring the parameters of transparent

Serial Port			
Type	RS-232	Protocol	Transparent
Data Bit	8	Stop Bit	1
Baud Rate	9600	Verification Type	None
Transparent Serial Port ...	<input type="checkbox"/> Enable	Port ...	6001 (6001-6010)


Table 13-4 Parameter description of transparent

Parameter	Description
Type	RS-232 and RS-485 ports are supported. <ul style="list-style-type: none"> You cannot enable single lane and multiple lanes at the same time. One serial port can only enable one external device.
Protocol	Keep it as default.
Baud Rate	Keep it as default.
Transparent Serial Port Service	Click  to enable the function, and then you can configure the serial port from 6001 to 6010.

Configuring External Light

1. Click , and then select **External Light** from **Device Type**.
2. Click **OK**.




You can hover over the peripheral icon, and then click  to delete the peripheral.

3. Configure the parameters.

Figure 13-6 Configuring the parameters of external light

Serial Port		Device Config	
Type	RS-485	Select Device No.	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 Auto Address Assignment
Protocol	Continuous Light	1	
Data Bit	8	Address	<input type="text" value="2"/> (2-32)
Stop Bit	1	Detect Status	<input type="radio"/> Yes <input checked="" type="radio"/> No
Baud Rate	9600	Device Status	-
Verification Type	None	Working Mode	<input type="text" value="Auto"/>
		Auto Mode	<input type="radio"/> Time <input checked="" type="radio"/> Brightness
		Default Environment Bri...	<input type="text" value="30"/> (0-100)
		Light Brightness	<input type="text" value="20"/> (0-20)
		Connected Device Qua...	<input type="text" value="2"/> (1-8)
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>			

Table 13-5 Parameter description of external light

Parameter	Description
Type	RS-232 and RS-485 ports are supported. <ul style="list-style-type: none"> You cannot enable single lane and multiple lanes at the same time. One serial port can only enable one external device.
Select Device No.	Select device number as needed.  Click Auto Address Assignment to assign addresses to the device automatically.
Detect Status	Select Yes to enable external light status check.
Working Mode	Select the work mode of the external light from Close , Enable and Auto .
Auto Mode	<ul style="list-style-type: none"> Time: The external light will on within the defined time. Brightness: Configure the value of the ambient brightness, and then the flashlight will off when the ambient brightness is higher than the pre-defined value.
Default Environment Brightness	Configure the default environment brightness and light brightness. The higher the value, the brighter the environment and the light.
Light Brightness	
Connected Device Quantity	The number of device connected.

14 Storage

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

14.1 Storage Spot Config

Configure the storage path of snapshots and video recordings.

Procedure


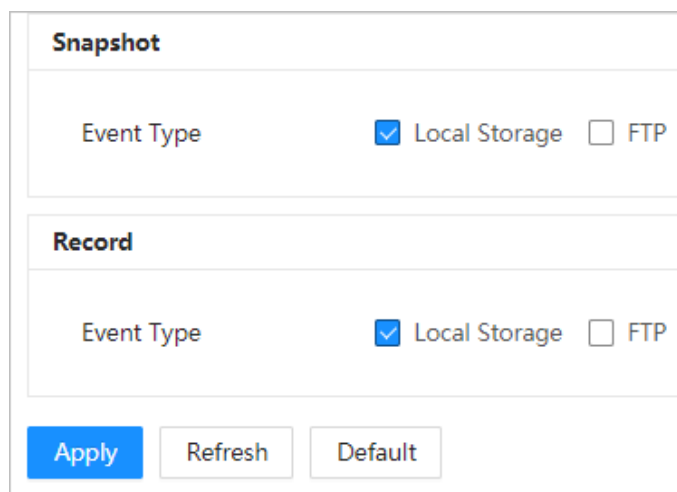
Step 1 Select  > **Storage** > **Storage** > **Storage Spot Config**.

Figure 14-1 Storage spot config



Snapshot	
Event Type	<input checked="" type="checkbox"/> Local Storage <input type="checkbox"/> FTP

Record	
Event Type	<input checked="" type="checkbox"/> Local Storage <input type="checkbox"/> FTP


Apply Refresh Default

Step 2 Select storage path as needed.

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

Step 3 Click **Apply**.

14.2 Local Storage

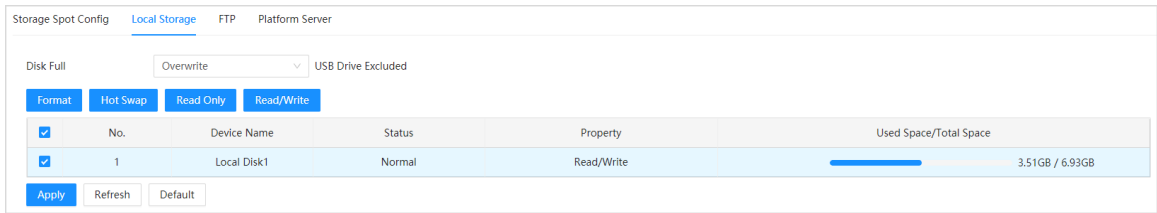
Select  > **Storage** > **Storage** > **Local Storage**, and the page displays the information of the TF card.

You can **Format** or **Hot Swap** the TF card, or select to **Overwrite** or **Stop** storage when the disk is full. Click **Save** after these operations.



Make sure that a TF card is inserted. Otherwise, no card information will be displayed on the **Local Storage** page.

Figure 14-2 Local storage



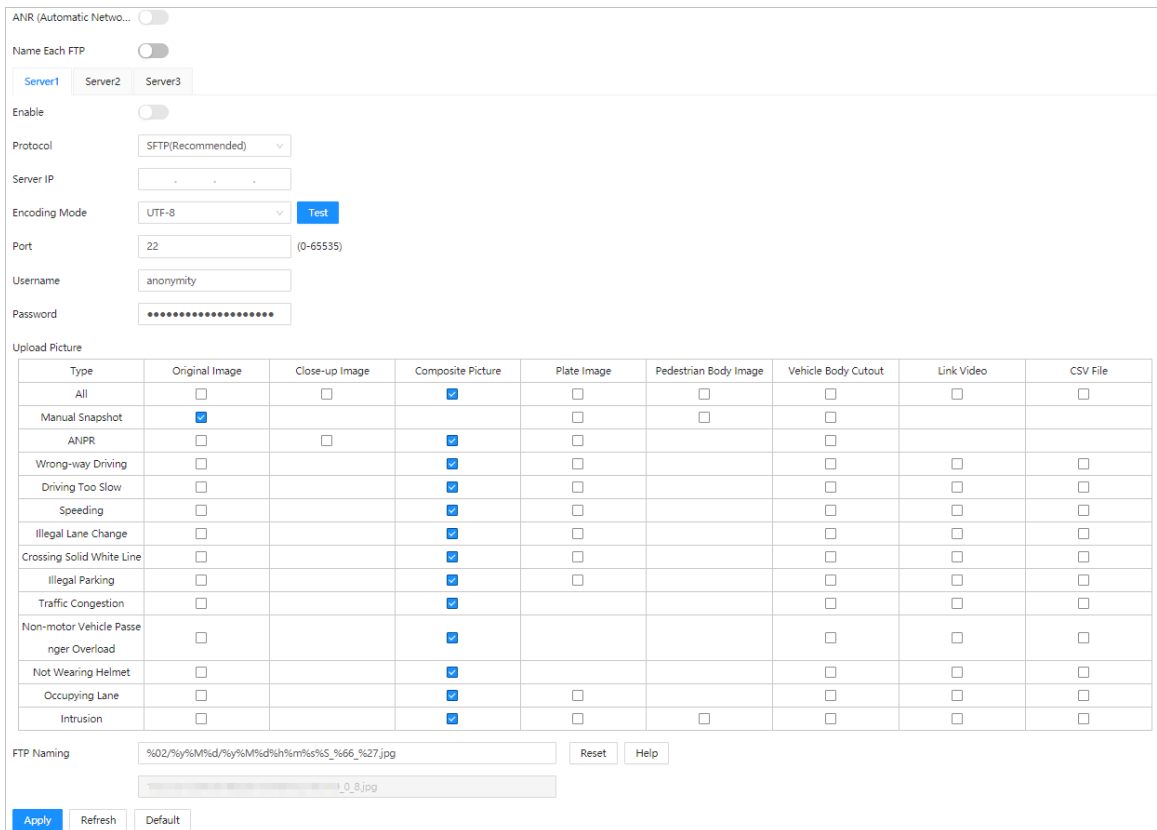
14.3 FTP

FTP function can be enabled only when TF card is inserted and FTP server is enabled. Only snapshots can be saved to the FTP server.

Procedure


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

Figure 14-3 FTP



Step 2 Configure the parameters.

Table 14-1 FTP parameters

Parameter	Description
ANR	When the network disconnects or fails, snapshots will be stored in TF card. After the network is restored, the snapshots will be uploaded from the TF card to FTP or client. Make sure that TF card is inserted in the Camera; otherwise, the offline transfer function cannot be enabled.
Name Each FTP	Click  to enable this function, and then the parameters of FTP Naming can be different.
Server1, Server2, Server3	Supports uploading to multiple servers. You can save different types of snapshots to different servers. Select the snapshot types from Upload Picture .
Enable	Enable FTP server storage.
Protocol	<ul style="list-style-type: none"> ● SFTP(Recommended) : Secure File Transfer Protocol, a network protocol allows file access, and transfer over a secure data stream. ● FTP : File Transfer Protocol, a network protocol implemented to exchange files over a TCP/IP network. Anonymous user access is also available through an FTP server.
Server IP	The IP address of FTP server.
Encoding Mode	Refers to the encode mode of Chinese characters when naming images. Only UTF-8 is supported. After configuring Server IP and Port , click Test to check whether the FTP server works.
Port	The port number of FTP server.
Password	The username and password of FTP server.
Username	
Upload Picture	Select event(s) and picture type(s) to be uploaded to each FTP server. Different modes support different events, and might differ from the actual page.
FTP Naming	Configure the naming rule of snapshots to be saved in FTP server. You can click Help to view the naming rule, or click Reset to restore the default naming rule.

Step 3 Click **Apply**.

14.4 Platform Server

You can set the parameters of storing to the client, which generally refers to the platform.

Prerequisites

You need to install and log in to platform first before you can store snapshots to platform server.

Procedure

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

Figure 14-4 Platform server

Step 2 Configure the parameters.

Table 14-2 Parameter description

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

Step 3 Click **Apply**.

14.5 Record Control

You can set how to record the videos and the stream for recording the videos.

Procedure

Step 1 Select > **Storage** > **Record**.

Figure 14-5 Record

Record Mode Enable Auto Manual

Record Stream Main Stream ▾

Apply Refresh Default

Step 2 Select the checkbox to next to **Enable** to enable the record mode.

- **Auto** : Record videos only when a traffic violation event is detected.
- **Manual** : Record videos continuously.

Step 3 Select the record stream. You can select from **Main Stream** and **Sub Stream**.

Step 4 Click **Apply**.

15 System

You can configure system information, add users, restore to factory settings, import and export system configuration files, and more.

15.1 General

You can configure display language, video standard, and also set the time and time zone of the Camera.

15.1.1 General Settings

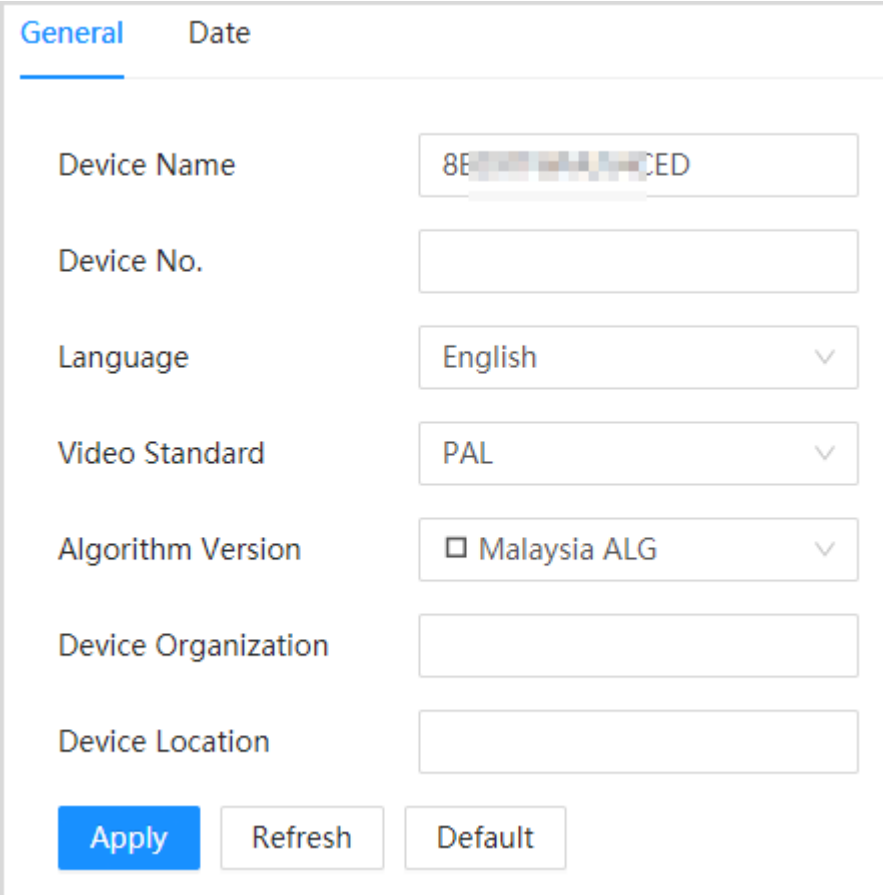
You can configure the device code, system, video standard, and more.

Procedure

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

Step 2 Configure the parameters.

Figure 15-1 General



General	Date
Device Name	8E...CED
Device No.	
Language	English
Video Standard	PAL
Algorithm Version	<input type="checkbox"/> Malaysia ALG
Device Organization	
Device Location	
<input type="button" value="Apply"/>	<input type="button" value="Refresh"/> <input type="button" value="Default"/>

Table 15-1 General parameters

Parameter	Description
Device Name	The device serial number consisting of letters, numbers, underlines and strikethroughs.
Device No.	No. of the Camera. The device code cannot be overlaid with OSD information.
Language	Language of web browser page. You need to log in again when switching to another language.
Video Standard	<p>PAL and NTSC are available.</p> <ul style="list-style-type: none"> ● PAL : Much more common around the world, and can be found in most of Western Europe, Australia, China, and elsewhere. ● NTSC : Mostly limited to North America, parts of South America, Japan, the Philippines and more.
Device Organization	The group or entity that uses the Camera.
Device Location	The locations where snapshots were taken by the Camera.

Step 3 Click **Apply**.

15.1.2 Date

You can configure date, time, time zone, and more for the Camera.

Procedure

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

Step 2 Configure the parameters.

Figure 15-2 Date

Time and Time Zone

Date Format ▼

Time Format ▼

Time Zone ▼

System Time 📅 Sync PC

DST

Enable

Type Date Week

Start Time 📅

End Time 📅

Time Synchronization NTP

NTP Server

Port (1-65535)

Interval min (1-30)



Sync Time-Allowlist

Enable

Apply
Refresh
Default

Table 15-2 Date & time parameters

Parameter	Description
Date Format	Select the date format. Three formats are available: YYYY-MM-DD , MM-DD-YYYY and DD-MM-YYYY .
Time Format	Select the time format. Two formats are available: 24-Hour and 12-Hour .
Time Zone	The time zone where the Camera is located.

Parameter	Description
System Time	The current time of the Camera. Click Sync PC to synchronize the time of the Camera to that of the computer.
DST	Click  to enable the DST (means daylight saving time) function, set the Type by Date or by Week , and then configure the Start Time and End Time of DST.
Time Synchronization	Time synchronization mode. You can select NTP (network time protocol).
NTP Server	The IP address and the port number of NTP server.
Port	
Interval	The time synchronization interval of the Camera and the NTP.
Sync Time-Allowlist	Click  to enable it, and then only the added IP and devices can synchronize the time with the computer.

Step 3 Click **Apply**.

15.2 Account

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

15.2.1 User

15.2.1.1 Adding Users

You can view the information of a user or user group, add or delete users or user groups, change user password, assign user permissions, restrict user login, and more.

Procedure


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

Step 2 Click **Add**.

Figure 15-3 Add user

Step 3 Configure the parameters.

Table 15-3 Description of 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 permissions of each function as needed.  We recommend you give fewer permissions to normal users than premium users.
Live	Select the live view permissions for the user to be added.
Playback	Select the video playback permissions for the user to be added.

Parameter	Description
Restricted Login	<p>Set the computer address that allows the defined user to log in to the Camera and the validity period and time range. You can log in to the webpage with the defined IP in the defined time range of validity period.</p> <ul style="list-style-type: none"> ● IP address: You can log in to web through the PC with the defined IP or one within the set IP segment. ● Validity period: You can log in to webpage within the defined validity period. ● Period: You can log in to webpage within the defined time range.

Step 4 Click **Apply**.


The user is displayed in the username list.

Related Operations

- Click  to edit password, remarks, 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.

15.2.1.2 Resetting Password

Enable the function, and you can reset password by clicking **Forget Password?** on the login page. For details, see "1.4 Resetting Password".

Procedure

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

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



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

Step 3 Configure the validity period of the password.

Step 4 Click **Apply**.

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

15.2.2 Adding User Groups

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 15-4 Add group



The screenshot shows a dialog box titled "Add" with a close button "X" in the top right corner. It contains two input fields: "Group" with the value "564" and "Remarks" with the value "11111". Below these fields are three tabs: "System" (selected), "Live", and "Playback". Under the "System" tab, there are several checked checkboxes: "All", "System", "Storage", "Peripheral", "Maintenance", "System Info", "Event", "Camera", "Manual Control", "File Backup", "Network", "Security", and "Sub Device Management". At the bottom right, there are "Apply" and "Cancel" buttons.

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.

15.2.3 Clearing User

Procedure

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

Step 2 Click **Clear User**, and then enter the password on the dialogue box to clear all information on custom users.



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

15.2.4 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 15-5 Add user

Step 3 Configure the parameters.


Table 15-4 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 uppercase, lowercase, number, and special character (excluding ' " ; : &).
Group	The group that users belong to. Each group has different authorities.

Step 4 Click **Apply**.

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.

16 Security

16.1 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.

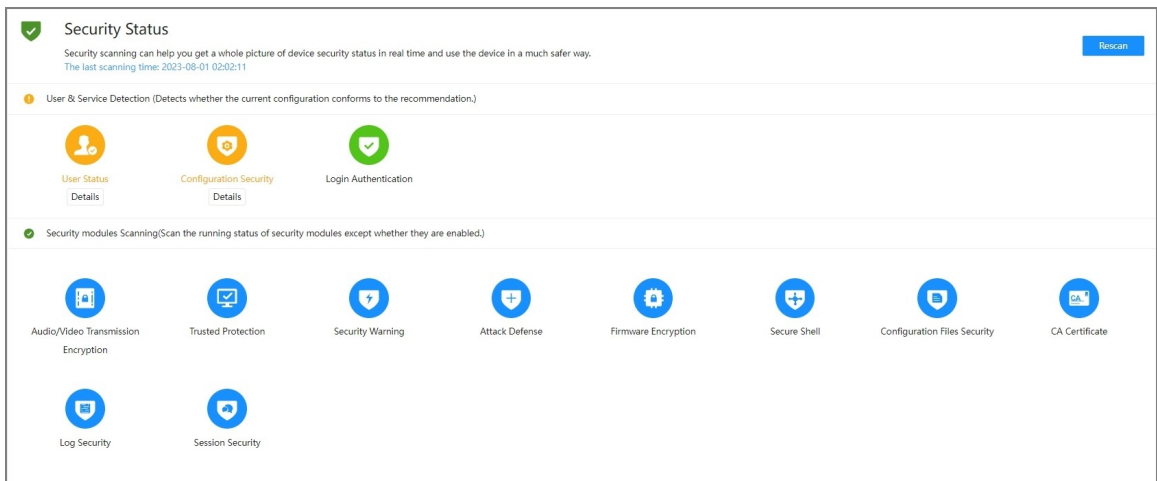
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing 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 16-1 Security status




Related Operations

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

1. Click **Details** to view the details of the scanning result.
2. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.
Click **Rejoin Detection**, and the exception will be scanned in next scanning.
3. Click **Optimize**, and the corresponding page will be displayed, and you can edit the configuration to clear the exception.

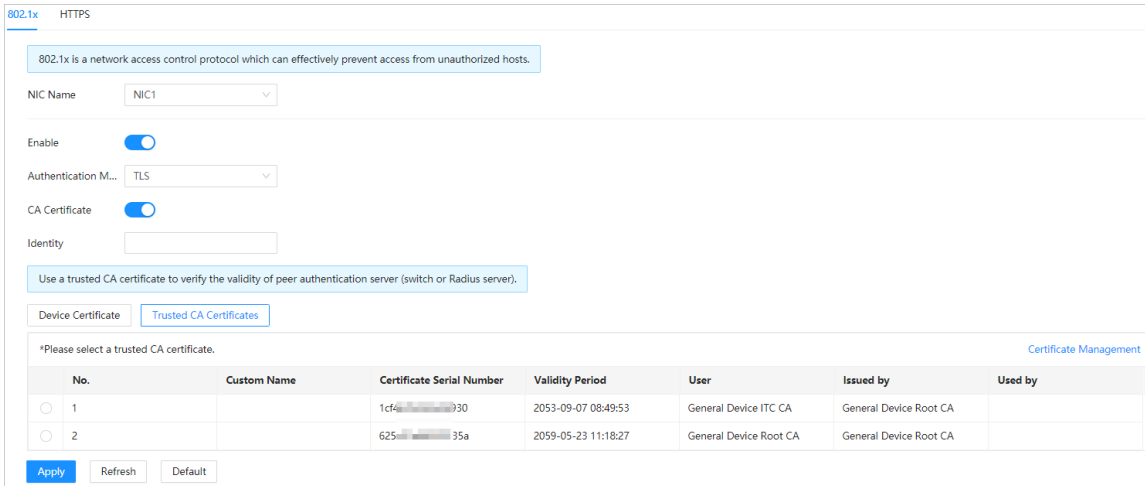
- **TLS: Transport Layer Security.** It is applied in two communication application programs to guarantee the security and integrity of the data.

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 16-4 802.1x (TLS)



No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
<input type="radio"/> 1		1cf4...930	2053-09-07 08:49:53	General Device ITC CA	General Device Root CA	
<input type="radio"/> 2		625...35a	2059-05-23 11:18:27	General Device Root CA	General Device Root CA	

Step 4 Click **Apply**.

16.2.2 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**.

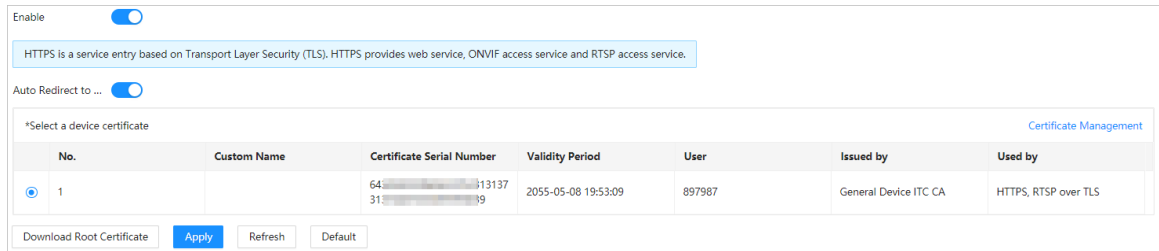
Step 2 Click  to enable the function.

Step 3 Select the certificate.



- Enable **Auto Redirect to HTTPS**, and the system will automatically load over HTTPS instead of unsecured HTTP.
- If there is no certificate in the list, click **Certificate Management** to configure one.

Figure 16-5 HTTPS



Step 4 Click **Apply**.

16.3 Attack Defense

16.3.1 Firewall

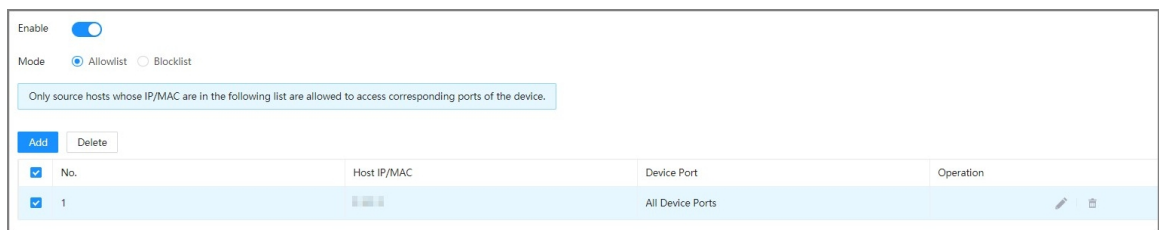
Configure the firewall to limit access to the camera.

Procedure

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

Step 2 Click  to enable the function.

Figure 16-6 Firewall

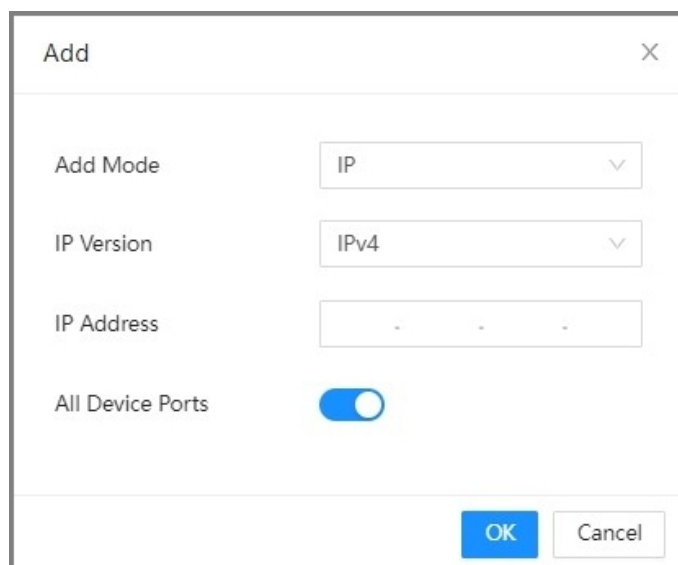


Step 3 Select the mode: **Allowlist** and **Blocklist**.

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



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

Figure 16-7 Firewall



Step 5 Click **Apply**.


Related Operations

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

16.3.2 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**.

16.3.3 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**.

16.4 CA Certificate

16.4.1 Installing Device Certificate

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

16.4.1.1 Creating Certificate

Create certificate in the device.

Procedure


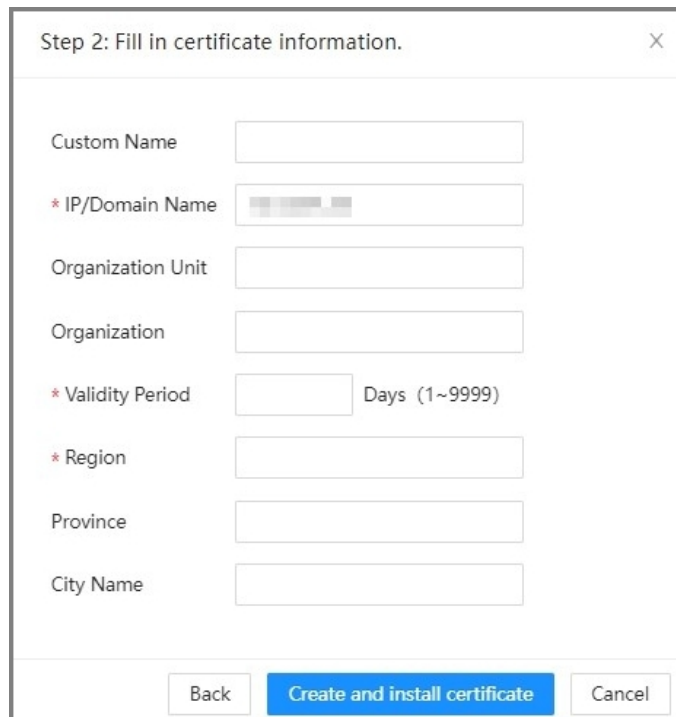
- Step 1 Select  > **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Create Certificate**, and click **Next**.
- Step 4 Enter the certificate information.

Figure 16-8 Certificate information (1)



Step 2: Fill in certificate information. [X]

Custom Name

* IP/Domain Name

Organization Unit

Organization

* Validity Period Days (1~9999)

* Region

Province



City Name

Back **Create and install certificate** Cancel

- 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.

16.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure


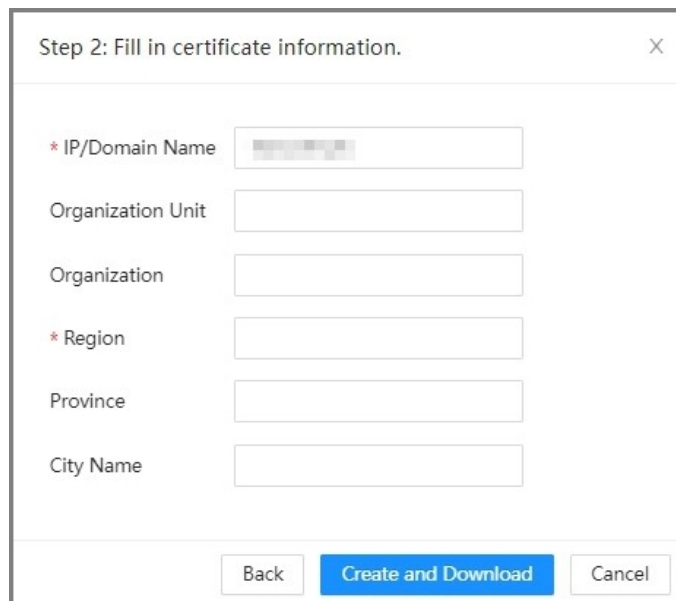
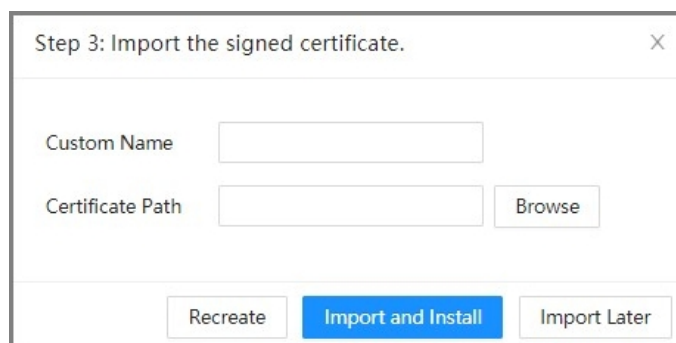
- Step 1 Select  > **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Click **Install Device Certificate**.
- Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
- Step 4 Enter the certificate information.

Figure 16-9 Certificate information (2)





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

Figure 16-10 Import a CA certificate



- Step 8 Click **Import and Install**.

Related Operations

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

16.4.1.3 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


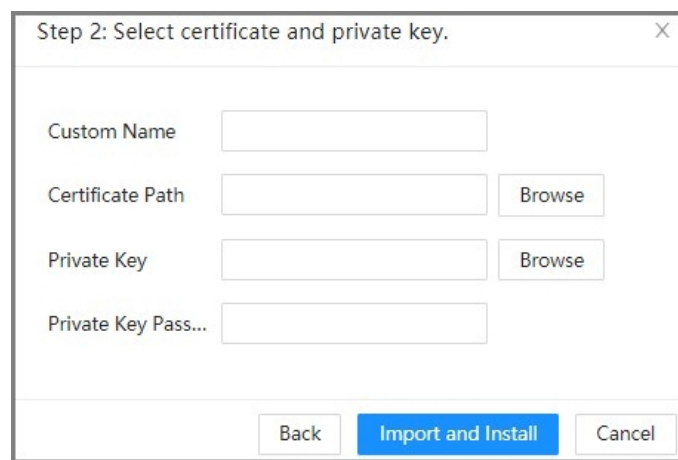
- Step 1 Select  > **Security** > **CA Certificate** > **Device Certificate**.
- Step 2 Select **Install Device Certificate**.
- Step 3 Select **Install Existing Certificate**, and then click **Next**.
- Step 4 Click **Browse** to open the CA certificate and private key, and enter the private key password.



Figure 16-11 Certificate and private key



- Step 5 Click **Import and Install**.

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

Related Operations

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

16.4.2 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


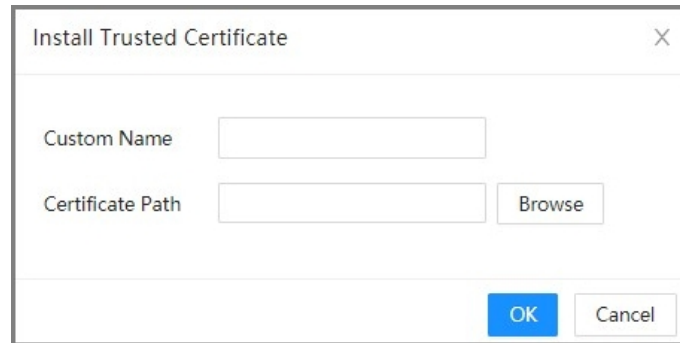
- Step 1 Select  > **Security** > **CA Certificate** > **Trusted CA Certificates**.
- Step 2 Select **Install Trusted Certificate**.
- Step 3 Click **Browse** to open the certificate.



Figure 16-12 Installing trusted certificate



Step 4 Click **OK**.

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

Related Operations

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

16.5 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 16-13 A/V encryption

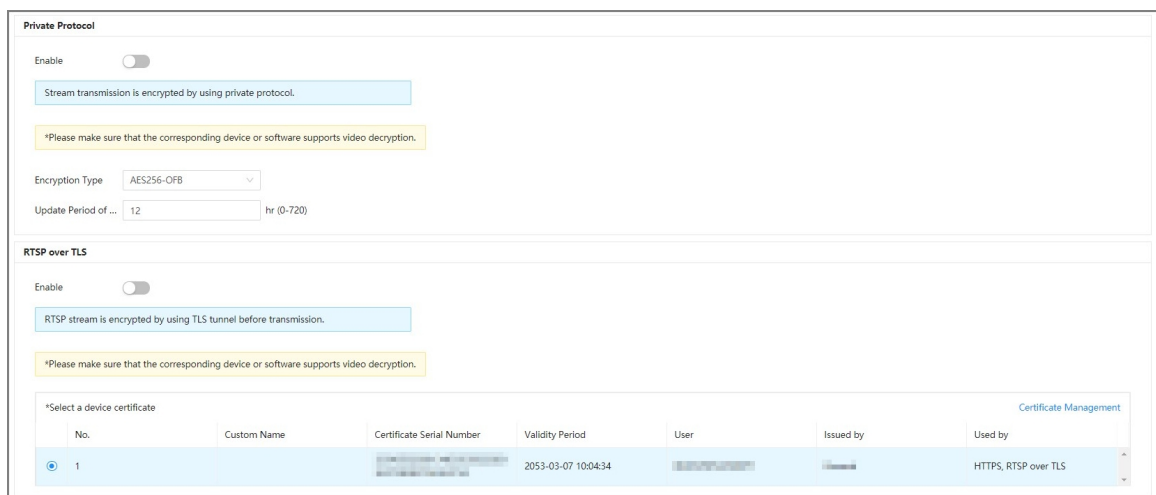




Table 16-1 Parameter description

Parameter		Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol.  There might be safety risk if this service is not enabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There might be safety risk if this service is not enabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "16.4 CA Certificate".

Step 3 Click **Apply**.

16.6 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.

16.6.1 Security Exception

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

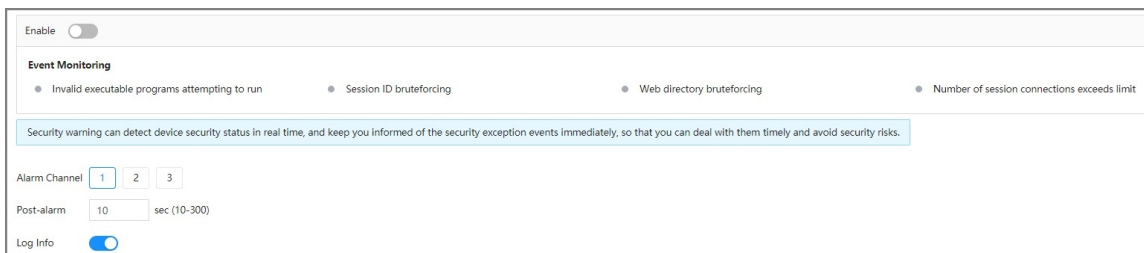
Procedure

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

Step 2 Click  to enable the function.

Step 3 Configure the parameters.

Figure 16-14 Security warning



- **Alarm Channel** : Select an alarm output channel. The corresponding device will be activated when an event is detected.

- **Post-alarm** : When an alarm is triggered, it will continue for the defined period after it ends.
- **Log Info** : After it is enabled, the camera will generate a log when an event occurs.


Step 4 Click **Apply**.

16.6.2 Illegal Login

The camera triggers a warning when illegal login is detected.

Procedure

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

Step 2 Click  to enable the function.

Step 3 Configure the parameters.

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

Step 4 Click **Apply**.

17 Maintenance Center

17.1 One-click Diagnosis

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

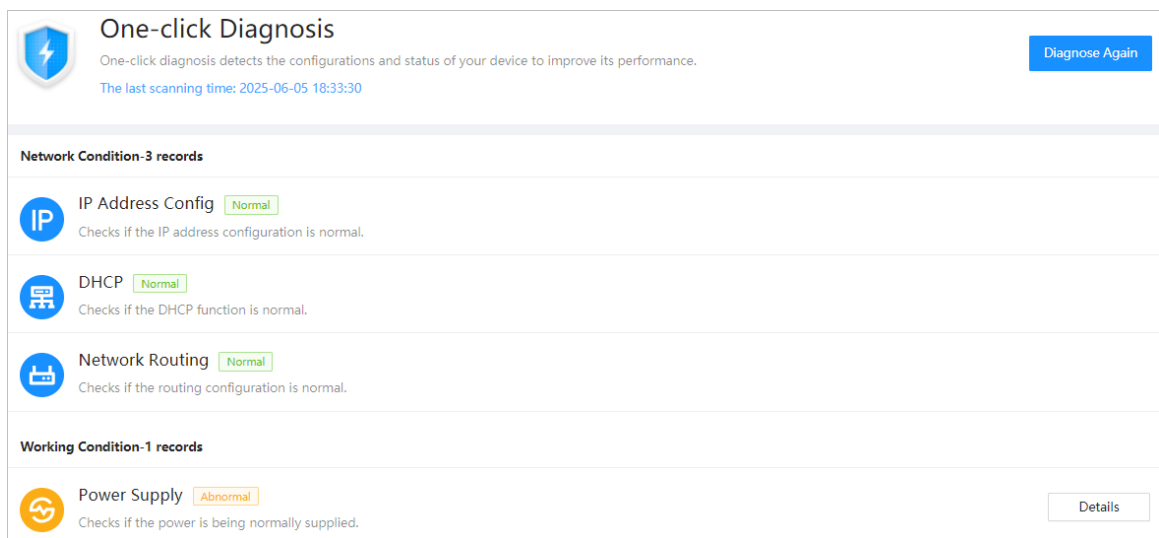
Procedure

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

Step 2 Click **Diagnose**.

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

Figure 17-1 One-click diagnosis



Related Operations

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

Click **Details** to view the details of the diagnosis results.

- Click **Ignore** to ignore the abnormality, and it will not be detected in next diagnosis.
- Click **Processed**, and the system will diagnose the abnormal item again, to check whether it is normal.

Figure 17-2 Details

Details
✕

The power supply of the device might behave abnormally. Please check if it is stable. Ignore


No.	Contents	Time Error Occurred	End Time
1	Power off and exit.	2025-05-29 10:27:39	2025-05-29 11:05:21
2	Power off and exit.	2025-05-15 11:53:13	2025-05-15 11:58:53
3	Power off and exit.	2025-05-15 06:53:38	2025-05-15 11:52:56
4	Power off and exit.	2025-05-07 05:49:11	2025-05-07 05:54:25
5	Power off and exit.	2025-05-07 01:15:13	2025-05-07 01:46:22
6	Power off and exit.	2025-05-06 14:12:03	2025-05-06 06:15:38

Processed

17.2 System Information

You can view information such as version, log, online user, and work status.

17.2.1 Version Information

Select  > **Maintenance Center** > **System Info** > **Version**, and then you can view the version information of the device (such as device model, and the version of the hardware, system, and software) and the peripheral (such as radar and illuminator).



Version might differ depending on the device model.

17.2.2 Online User

Select  > **Maintenance Center** > **System Info** > **Online User**, and then you can view online users' information, including username, user local group, IP address, user login time, and login type.

Figure 17-3 Online user

Refresh

No.	Username	Group	IP Address	User Login Time	Login Type
1	admin	admin	172.16.1.5	2025-06-05 17:23:03	DVRIP
2	admin	admin	172.16.1.61	2025-06-05 17:23:10	DVRIP
3	admin	admin	10.5.1.70	2025-06-05 17:23:23	DVRIP
4	admin	admin	10.5.1.70	2025-06-05 17:23:26	DVRIP
5	admin	admin	10.5.1.69	2025-06-05 18:27:14	Web3.0
6	admin	admin	10.5.1.69	2025-06-05 18:27:16	DVRIP



Click **Refresh** to refresh the page.

17.2.3 Running Status

Select > **Maintenance Center** > **System Info** > **Running Status**, and then you can view device work status, including CPU, memory and temperature.

17.2.4 Legal Information

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

17.3 Log

17.3.1 System Log

You can search for and view logs by the time and type, and backup the logs. The log type includes **All**, **System**, **Config**, **Storage**, **Event Operation**, **Record**, **Account**, and **Security**.

Procedure

- Step 1** Select > **Maintenance Center** > **Log** > **Log**.
- Step 2** Configure **Search Time Range**, and then select log type.
- Step 3** Click **Search**.
- Step 4** View the search results.

You can click **Back Up** to save the search results to your computer in a .txt file.

Figure 17-4 Log

Search Time Range: 2023-06-04 20:10:29 --> 2023-06-05 20:10:29

Type: All [Search]

Backup Encrypt Log Backup

No.	Time	Username	Type	Details
1	2023-06-05 19:47:49	admin	Logout	
2	2023-06-05 19:47:49	admin	Logout	
3	2023-06-05 19:40:26	admin	Login	
4	2023-06-05 19:40:24	admin	Login	
5	2023-06-05 19:09:55	admin	Save Config	
6	2023-06-05 19:09:53	admin	Save Config	
7	2023-06-05 19:07:38	admin	Logout	
8	2023-06-05 19:07:28	admin	Login	
9	2023-06-05 19:06:53	admin	Save Config	
10	2023-06-05 19:01:59	admin	Set System Time	
11	2023-06-05 18:46:24	admin	Login	
12	2023-06-05 18:46:23	admin	Login	
13	2023-06-05 18:46:19	admin	Login	
14	2023-06-05 18:46:19	admin	Login	

110 record(s) [1] [2] [100 / page] Go to Page


Related Operations

Click to view the details.

17.3.2 Remote Log

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

Procedure

- Step 1 Select  > **Maintenance Center** > **Log** > **Remote Log**.
- Step 2 Click to enable the function.
- Step 3 Configure the IP address, port and device number.
- Step 4 (Optional) Click to enable TLS, so that it will encrypt data transmission using TLS tunnel.
- Step 5 Click **Apply**.

17.4 Maintenance Management

17.4.1 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 anomaly in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

17.4.2 Maintenance

Procedure




- Step 1 Select  > **Maintenance Center** > **Maintenance Management** > **Maintenance**.

Figure 17-5 Maintenance


The screenshot shows a web interface for maintenance settings. It is divided into three main sections: 'Restart System', 'Delete Old Files', and 'Emergency Maintenance'.
1. 'Restart System': Contains a toggle for 'Auto Restart' (which is turned on), a dropdown menu for 'Restart Time' set to 'Tue', and a time selector set to '02:00'.
2. 'Delete Old Files': Contains a toggle for 'Auto Delete' (which is turned on) and a text input for 'Delete File' set to '1' day(s) ago.
3. 'Emergency Maintenance': Contains a toggle for 'Enable' (which is turned on) and a blue informational message: 'For easy access to our after-sales service, enable this function. If the device has any trouble performing functions, such as updating, the system will automatically enable this function.'
At the bottom of the interface are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

Step 2 Configure the parameters.

- Click  next to **Auto Restart** and configure the restart time. The device will automatically restart at the defined time every week.
- Click  next to **Auto Delete** and set the time. The device will automatically delete old files earlier than the defined time. The time range is 1 to 31 days.



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

- Click  next to **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**.

17.4.3 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  > **Maintenance Center** > **Maintenance Management** > **Import/Export**.

Figure 17-6 Import/Export

The screenshot shows a web interface for Import/Export configuration. It is divided into two main sections: 'Import' and 'Export'.
In the 'Import' section, there is a text input field labeled 'File'. To its right is a dashed box containing the text 'Please select file.' and a button labeled 'Import File'. Below this is a blue notification box with an information icon and the text 'Imported configuration will overwrite previous configuration.'
In the 'Export' section, there are two radio buttons under the label 'Export Method'. The first is 'Export All' with a selected radio button. The second is 'Export Some' with an unselected radio button. Below these is a button labeled 'Export Configuration File'.

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.

Step 3 Select the path of the file to import, or the path of the file to export.

17.4.4 Default

Restore all settings of the Camera to the default status.

Select  > **Maintenance Center** > **Maintenance Management** > **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.

17.5 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  > **Maintenance Center** > **Update**.

Step 2 Update the camera in the following ways.

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



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

3. Click **Update**.

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

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

17.6 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 17-7 Packet capture


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

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

Figure 17-8 Network test results

The screenshot displays the 'Network Test' interface. It includes input fields for 'Destination Address' and 'Data Packet Size' (set to 64). A 'Test' button is visible. The 'Test Result' section shows a successful ping: 'PING [IP] 64(92) bytes of data.' followed by two lines of results: '72 bytes from [IP]: icmp_seq = 1 ttl = 255 time < 1 ms' and '72 bytes from [IP]: icmp_seq = 2 ttl = 255 time < 1 ms'. A 'Copy' button is next to the results. Below the results, a summary box shows 'Data Packet: Sent = 2, Received = 2, Lost = 0 (0.00% Loss Rate)'. At the bottom, it states '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 lockout function

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

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

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

Service Configuration

1. Enable HTTPS

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

2. Encrypted transmission of audio and video

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

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

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

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

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

4. Change HTTP and other default service ports

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

Network Configuration

1. **Enable Allowlist**

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

2. **MAC address binding**

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

3. **Build a secure network environment**

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

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

Security Auditing

1. **Check online users**

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

2. **Check device log**

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

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

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

2. **Update client software in time**

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

Physical Protection

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

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