



# **Network Camera Web 5.0**

## **Operation Manual**







# Foreword

## General

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

## Safety Instructions

The following signal words might appear in the manual.

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

## Revision History

Version	Revision Content	Release Date
V1.0.7	<ul style="list-style-type: none"> <li>Updated the description of people counting.</li> <li>Added the function of AcuPick and disarming.</li> </ul>	June 2023
V1.0.6	<ul style="list-style-type: none"> <li>Added smart object detection, power consumption mode, privacy detection and PPE detection.</li> <li>Updated the description of IVS.</li> </ul>	January 2023
V1.0.5	Added the description of splicing and panoramic linkage.	September 2022
V1.0.4	Added the description of EPTZ, AI SSA and AFSA.	April 2022
V1.0.3	Added parking space detection mode.	November 2021

Version	Revision Content	Release Date
V1.0.2	<ul style="list-style-type: none"> <li>• Added "6.2.2.2.14 Configuring Parking Space".</li> <li>• Added "8.6 Setting Vehicle Density".</li> <li>• Added "8.7 Setting Parking Space".</li> <li>• Added "12.1.4 Crowd Distribution".</li> <li>• Added "12.1.5 Vehicle Density".</li> <li>• Updated "8.13 Setting ANPR".</li> </ul>	July 2021
V1.0.1	<ul style="list-style-type: none"> <li>• Added "8.9 Setting People Counting" and "8.12 Setting Heat Map".</li> <li>• Added "6.2.1.11 Fisheye" and "7.4.4 Fisheye".</li> <li>• Updated "8.2 Setting Face Detection+".</li> <li>• Updated "12 Report".</li> </ul>	May 2021
V1.0.0	First release.	September 2020

## Privacy Protection Notice

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

## About the Manual

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

format) cannot be opened.

- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.



# Important Safeguards and Warnings

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

## Transportation Requirements



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

## Storage Requirements



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


## Installation Requirements



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



- Do not place heavy stress on the device, violently vibrate or immerse it in liquid during installation.

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

## Operation Requirements



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



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

password manually.

## Maintenance Requirements



- **Strictly follow the instructions to disassemble the device. Non-professionals dismantling the device can result in it leaking water or producing poor quality images. For a device that is required to be disassembled before use, make sure the seal ring is flat and in the seal groove when putting the cover back on. When you find condensed water forming on the lens or the desiccant becomes green after you disassembled the device, contact after-sales service to replace the desiccant. Desiccants might not be provided depending on the actual model.**
- **Use the accessories suggested by the manufacturer. Installation and maintenance must be performed by qualified professionals.**
- **Do not directly touch the photosensitive CMOS. Use an air blower to clean the dust or dirt on the lens. When it is necessary to clean the device, slightly wet a soft cloth with alcohol, and gently wipe away the dirt.**
- **Clean the device body with a soft dry cloth. If there are any stubborn stains, clean them away with a soft cloth dipped in a neutral detergent, and then wipe the surface dry. Do not use volatile solvents such as ethyl alcohol, benzene, diluent, or abrasive detergents on the device to avoid damaging the coating and degrading the performance of the device.**
- **The dome cover is an optical component. When it is contaminated with dust, grease, or fingerprints, use degreasing cotton moistened with a little ether or a clean soft cloth dipped in water to gently wipe it clean. An air gun is useful for blowing dust away.**
- **It is normal for a camera made of stainless steel to develop rust on its surface after being used in a strong corrosive environment (such as the seaside, and chemical plants). Use an abrasive soft cloth moistened with a little acid solution (vinegar is recommended) to gently wipe it away. Afterwards, wipe it dry.**

# Table of Contents

Foreword .....	I
Important Safeguards and Warnings.....	IV
1 Overview .....	1
1.1 Introduction.....	1
1.2 Network Connection.....	1
1.3 Functions.....	1
1.3.1 Basic Functions.....	1
1.3.2 Analytics+ Functions .....	2
2 Configuration Flow .....	5
3 Device Initialization.....	6
4 Login .....	10
4.1 Device Login .....	10
4.2 Resetting Password .....	11
5 Home Page.....	13
6 Setting .....	15
6.1 Local.....	15
6.2 Camera.....	16
6.2.1 Setting Image Parameters .....	16
6.2.1.1 Page Layout .....	16
6.2.1.2 AI SSA.....	18
6.2.1.3 Image .....	18
6.2.1.4 Exposure.....	19
6.2.1.5 Backlight.....	22
6.2.1.6 WB .....	23
6.2.1.7 Day/Night.....	23
6.2.1.8 Illuminator .....	24
6.2.1.9 Defog .....	26
6.2.1.10 AFSA.....	26
6.2.1.11 Fisheye.....	27
6.2.2 Setting Encode Parameters .....	28
6.2.2.1 Encode .....	28
6.2.2.2 Overlay .....	30
6.2.2.2.1 Configuring Privacy Masking .....	31
6.2.2.2.2 Configuring Channel Title.....	32
6.2.2.2.3 Configuring Time Title.....	32

---

6.2.2.2.4 Configuring Location .....	33
6.2.2.2.5 Configuring Font Properties .....	33
6.2.2.2.6 Configuring Picture Overlay .....	34
6.2.2.2.7 Configuring Custom Title .....	34
6.2.2.2.8 Configuring Target Statistics .....	35
6.2.2.2.9 Configuring ANPR .....	36
6.2.2.2.10 Configuring Face Detection .....	36
6.2.2.2.11 Configuring Face Detection+ .....	37
6.2.2.2.12 Configuring Face Statistics .....	38
6.2.2.2.13 Configure Face&Body Counting .....	38
6.2.2.2.14 Configuring Parking Space .....	39
6.2.2.2.15 Configuring People Counting .....	40
6.2.2.3 ROI .....	40
6.2.3 Splicing .....	41
6.2.4 Audio .....	42
6.2.4.1 Setting Audio Parameters .....	42
6.2.4.2 Setting Alarm Tone .....	43
6.3 Network .....	44
6.3.1 TCP/IP .....	44
6.3.2 Port .....	47
6.3.3 PPPoE .....	49
6.3.4 DDNS .....	49
6.3.5 Email .....	51
6.3.6 UPnP .....	52
6.3.7 SNMP .....	53
6.3.8 Bonjour .....	56
6.3.9 Multicast .....	56
6.3.10 Register .....	57
6.3.11 QoS .....	58
6.3.12 Platform Access .....	58
6.3.12.1 P2P .....	58
6.3.12.2 ONVIF .....	59
6.3.12.3 RTMP .....	60
6.3.13 Basic Service .....	61
6.4 EPTZ .....	62
6.5 Event .....	63
6.5.1 Setting Alarm Linkage .....	63

---

6.5.1.1 Setting Alarm-in .....	63
6.5.1.2 Alarm Linkage.....	64
6.5.1.2.1 Adding Schedule .....	65
6.5.1.2.2 Record Linkage .....	66
6.5.1.2.3 Snapshot Linkage.....	67
6.5.1.2.4 Alarm-out Linkage .....	67
6.5.1.2.5 Email Linkage.....	67
6.5.1.3 Subscribing Alarm.....	68
6.5.1.3.1 Alarm Types .....	68
6.5.1.3.2 Subscribing Alarm Information.....	68
6.5.2 Setting Exception.....	69
6.5.2.1 Setting SD Card Exception .....	70
6.5.2.2 Setting Network Exception.....	70
6.5.2.3 Setting Voltage Detection .....	71
6.5.3 Setting Video Detection.....	72
6.5.3.1 Setting Motion Detection.....	72
6.5.3.2 Setting Video Tampering.....	74
6.5.3.3 Setting Scene Changing .....	75
6.5.4 Setting Audio Detection.....	75
6.5.5 Setting Disarming .....	77
6.6 Storage .....	77
6.7 System .....	78
6.7.1 General .....	78
6.7.1.1 Basic .....	78
6.7.1.2 Date & Time.....	79
6.7.2 Power Consumption Mode .....	80
6.7.2.1 Setting Sleeping Mode .....	80
6.7.2.2 Setting General Mode.....	80
6.7.2.3 Setting Power Saving Mode .....	81
6.7.3 Account.....	81
6.7.3.1 User .....	81
6.7.3.1.1 Adding User .....	81
6.7.3.1.2 Resetting Password.....	84
6.7.3.2 Adding User Group .....	85
6.7.3.3 ONVIF User .....	86
6.7.4 Peripheral Management .....	87
6.7.4.1 Configuring Serial Port.....	87

---

6.7.4.2 Configuring External Light .....	88
6.7.4.3 Configuring Wiper.....	89
6.7.5 Manager .....	90
6.7.5.1 Requirements .....	90
6.7.5.2 Maintenance .....	90
6.7.5.3 Import/Export.....	91
6.7.5.4 Default .....	92
6.7.6 Upgrade.....	92
6.8 System Information .....	93
6.8.1 Version.....	93
6.8.2 Online User.....	93
6.9 Setting Log.....	93
6.9.1 Log.....	93
6.9.2 Remote Log .....	94
7 Live.....	96
7.1 Live Page .....	96
7.2 Setting Encode .....	97
7.3 Live View Function Bar.....	98
7.4 Window Adjustment Bar.....	99
7.4.1 Adjustment .....	99
7.4.2 Zoom and Focus .....	100
7.4.3 Image Adjustment .....	102
7.4.4 Fisheye.....	102
7.5 Display Mode.....	106
8 Analytics+ .....	110
8.1 Setting Crowd Distribution Map.....	110
8.1.1 Global Configuration .....	110
8.1.2 Rule Configuration.....	111
8.2 Setting Face Detection+.....	113
8.2.1 Enabling Face Detection+ .....	113
8.2.2 Setting Face Database.....	116
8.2.2.1 Creating Face Database.....	117
8.2.2.2 Adding Face Picture.....	118
8.2.2.2.1 Single Adding .....	119
8.2.2.2.2 Batch Importing.....	120
8.2.2.3 Managing Face Picture .....	122
8.2.2.3.1 Editing Face Information.....	122

---

---

8.2.2.3.2 Deleting Face Picture.....	123
8.2.2.4 Face Modeling .....	123
8.2.3 Setting Arm Alarm .....	124
8.2.4 Viewing Face Detection+ Result .....	127
8.3 Setting Face Detection .....	127
8.4 Setting IVS.....	130
8.4.1 Global Configuration .....	131
8.4.2 Rule Configuration.....	132
8.5 Setting Smart Object Detection .....	136
8.5.1 Global Configuration .....	137
8.5.2 Rule Configuration.....	137
8.6 Setting Vehicle Density .....	140
8.7 Setting Parking Space .....	142
8.7.1 Rule Configuration.....	142
8.7.1.1 For Parking Space Detection Fisheye WizMind Network Camera .....	142
8.7.1.2 For Other Cameras .....	144
8.7.2 Global Configuration .....	148
8.8 Setting Video Analytics.....	148
8.8.1 Global Configuration .....	148
8.8.2 Rule Configuration.....	150
8.8.3 Viewing Video Analytics Report.....	152
8.9 Setting People Counting.....	153
8.9.1 People Counting.....	153
8.9.2 Queuing .....	156
8.9.3 Abnormal Event Detection .....	158
8.9.4 Global Configuration .....	160
8.10 Face & Body Detection .....	161
8.10.1 Global Configuration.....	161
8.10.2 Rule Configuration .....	163
8.11 PPE Detection .....	164
8.11.1 Rule Configuration .....	165
8.11.2 Global Configuration.....	167
8.11.3 Setting Arming Database .....	167
8.12 Setting Heat Map .....	168
8.13 Setting ANPR .....	169
8.13.1 Lane Configuration.....	169
8.13.2 Rule Configuration .....	170



---

8.13.3 Picture .....	172
8.13.4 Allowlist.....	172
8.13.5 Blocklist .....	176
8.14 Setting Panoramic Linkage .....	176
8.14.1 Enabling Linkage Track.....	176
8.14.2 Configuring Calibration Parameter.....	177
8.15 Setting AcuPick .....	178
9 Security.....	180
9.1 Security Status.....	180
9.2 System Service.....	181
9.2.1 802.1x .....	181
9.2.2 HTTPS.....	182
9.3 Attack Defense .....	183
9.3.1 Firewall .....	183
9.3.2 Account Lockout .....	184
9.3.3 Anti-DoS Attack.....	185
9.4 CA Certificate.....	185
9.4.1 Installing Device Certificate.....	185
9.4.1.1 Creating Certificate.....	185
9.4.1.2 Applying for and Importing CA Certificate.....	186
9.4.1.3 Installing Existing Certificate .....	187
9.4.2 Installing Trusted CA Certificate .....	188
9.5 A/V Encryption .....	189
9.6 Security Warning.....	190
10 Record .....	191
10.1 Playback.....	191
10.1.1 Playing Back Video .....	191
10.1.2 Clipping Video.....	193
10.1.3 Downloading Video.....	194
10.2 Setting Record Control.....	195
10.3 Setting Record Plan .....	196
10.4 Storage .....	198
10.4.1 Local Storage .....	199
10.4.2 Network Storage .....	199
10.4.2.1 FTP .....	200
10.4.2.2 NAS.....	201
11 Picture .....	203

---

11.1 Playback.....	203
11.1.1 Playing Back Picture .....	203
11.1.2 Downloading Picture.....	204
11.2 Setting Snapshot Parameters .....	205
11.3 Setting Snapshot Plan.....	206
11.4 Storage .....	206
11.5 Setting Upload Method.....	206
12 Report.....	208
12.1 Viewing Report.....	208
12.1.1 Face Detection+ .....	208
12.1.2 Video Analytics.....	209
12.1.3 People Counting .....	210
12.1.4 Crowd Distribution .....	214
12.1.5 Vehicle Density.....	214
12.1.6 Heat Map .....	215
12.1.7 ANPR .....	217
12.2 Searching for Face Picture .....	218
12.3 Auto Upload .....	219
Appendix 1 Cybersecurity Recommendations .....	224

# 1 Overview

## 1.1 Introduction

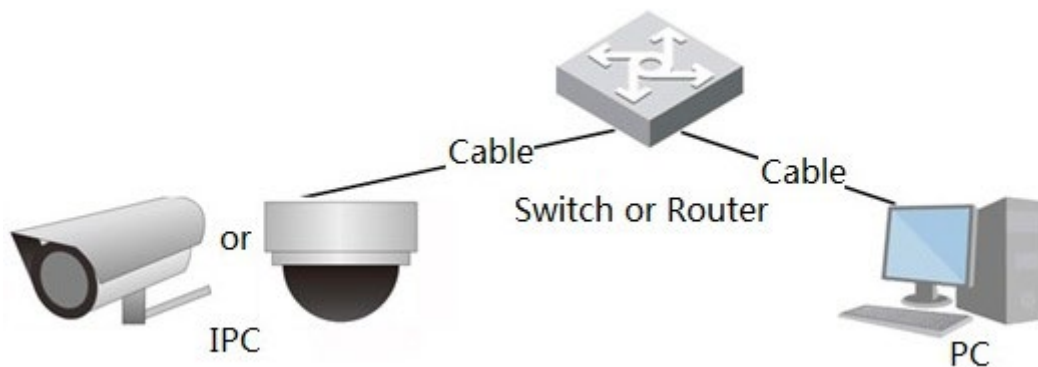
IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.

IP camera is divided into single-channel camera and multi-channel camera according to the channel quantity. For multi-channel camera, you can set the parameters for each channel.

## 1.2 Network Connection

In the general IPC network topology, IPC is connected to PC through network switch or router.

Figure 1-1 General IPC network



Get IP address by searching on ConfigTool, and then you can start accessing IPC through network.

## 1.3 Functions

Functions might vary with different devices.

### 1.3.1 Basic Functions

#### Real-time Monitoring

- Live view.
- When live viewing the image, you can enable audio, voice talk and connect monitoring center for quick processing on the abnormality.
- Adjust the image to the proper position by PTZ.

- Snapshot and triple snapshot abnormality of the monitoring image for subsequent view and processing.
- Record abnormality of monitoring image for subsequent view and processing.
- Configure coding parameters, and adjust live view image.

## Alarm

- Set alarm prompt mode and tone according to alarm type.
- View alarm prompt message.

## Exception

- SD card error, network disconnection, illegal access, voltage detection and security exception.
- When SD card error or illegal access is triggered, the system links alarm output and sending email.
- When network disconnection alarm is triggered, the system links recording and alarm output.
- When the input voltage is more or less than the rated voltage, the alarm is triggered and the system links sending email.

## Video Detection

- Motion detection, video tampering detection and scene changing detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Audio Detection

- Audio input abnormal detection and intensity change detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Record

- Auto record as schedule.
- Play back recorded video and picture as needed.
- Download recorded video and picture.
- Alarm linked recording.

## Account

- Add, edit and delete user group, and manage user authorities according to user group.
- Add, edit and delete user, and configure user authorities.
- Change user password.

## 1.3.2 Analytics+ Functions

### IVS

- Tripwire, intrusion, abandoned object, moving object, fast moving, parking detection, people gathering, and loitering detection.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

## Face Detection

- Detects face and display the related attributes on the live page.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Face Detection+

- Displays the recognition result on the live view page
- In general mode, makes comparison between the detected face with the faces in face database after detecting face. You can set the alarm mode and reporting mode for each face database separately, and set linkages for each reporting mode.
- In counting mode, does precise face counting after detecting face.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Crowd Distribution Map

- View crowd distribution in real time for the timely arm to avoid accidents such as stampede.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Video Analytics

- Captures people, non-motor vehicle and vehicle, and displays the related information on the live page.
- When an alarm is triggered, the system links alarm output.

## People Counting

- Counts the people flow in/out the detection area, and generates report.
- When the number of counted number of people in the detection area or the stay duration exceeds the configured value, an alarm will be triggered.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

## Heat Map

- Counts cumulative density of moving objects, and displays the result in different colors.
- View report of heat map, which includes heat map and track map (track map is not available on economic fisheye cameras).

## ANPR

- Recognizes plate number in detection area, and displays the related information on live

page.

- When an alarm is triggered, the system links alarm output and snapshot.

## Face & Body Detection

- Detects faces and human body separately, and then correlates the face and the body.
- When select compliant mode, the camera can detect attributes including face masks, helmets, glasses, safety vests, top color, and bottom color, and determine whether PPE requirements are met. PPE compliance or non-compliance alarms can be triggered according to the alarm settings.
- When an alarm is triggered, the system links alarm output and snapshot.

## Parking Space

- Supports planned parking space and open parking space.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, and snapshot.

## Vehicle Density

- Includes road congestion and parking limit, and supports to view vehicle statistics through the live page.
- When the counted vehicle exceeds the configured vehicle number and the congestion time exceeds the configured time, an alarm will be triggered.
- When an alarm is triggered, the system performs linkages such as recording, alarm output and sending email.

## PPE Detection

- When the target attributes are inconsistent with the configured attributes, the alarm is triggered.
- When an alarm is triggered, the system performs linkages such as recording, sending emails and alarm output.

## Privacy Protection

The target objects will be blurred by mosaic or color blocks when they are detected.

## Smart Object Detection

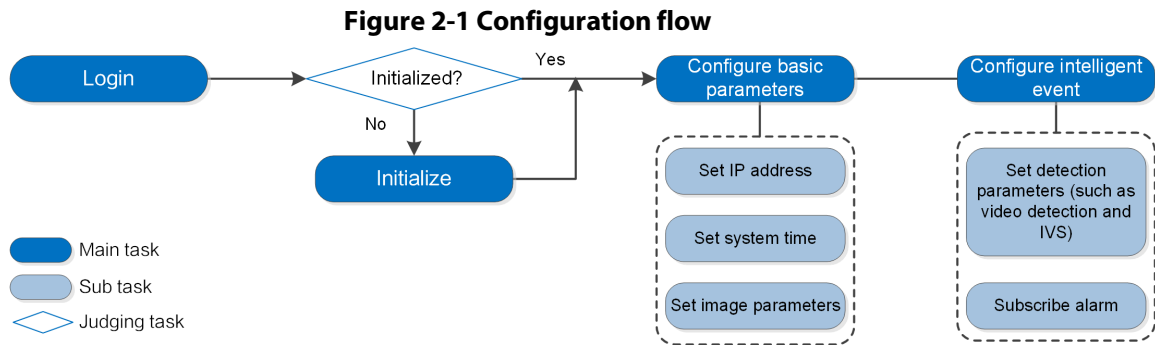
- Supports smart abandoned object and smart missing object detection.
- When an alarm is triggered, the system performs linkage such as recording, alarm output, sending email and snapshot.

## AcuPick

Achieve accurate and quick search on the connected NVR.

## 2 Configuration Flow

For the device configuration flow, see Figure 2-1. For details, see Table 2-1. Configure the device according to the actual situation.



**Table 2-1 Description of flow**

Configuration		Description	Reference
Login		Open IE browser and enter IP address to log in to the web page, The camera IP address is 192.168.1.108 by default.	"4 Login"
Initialization		Initialize the camera when you use it for the first time.	"3 Device Initialization"
Basic parameters	Camera parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	"6.2 Camera"
	Date & time	Set date and time to ensure the recording time is correct.	"6.7.1.2 Date & Time"
	IP address	Change IP address according to network planning for the first use or during network adjustment.	"6.3.1 TCP/IP"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"6.5.1.3 Subscribing Alarm"
Analytics+	Analytics+ rules	Configure the necessary detection rules, such as face detection and IVS.	"8 Analytics+"

# 3 Device Initialization

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



- **To ensure the device safety, keep the password properly after initialization and change the password regularly.**
- **When initializing device, keep the PC IP and device IP in the same network.**

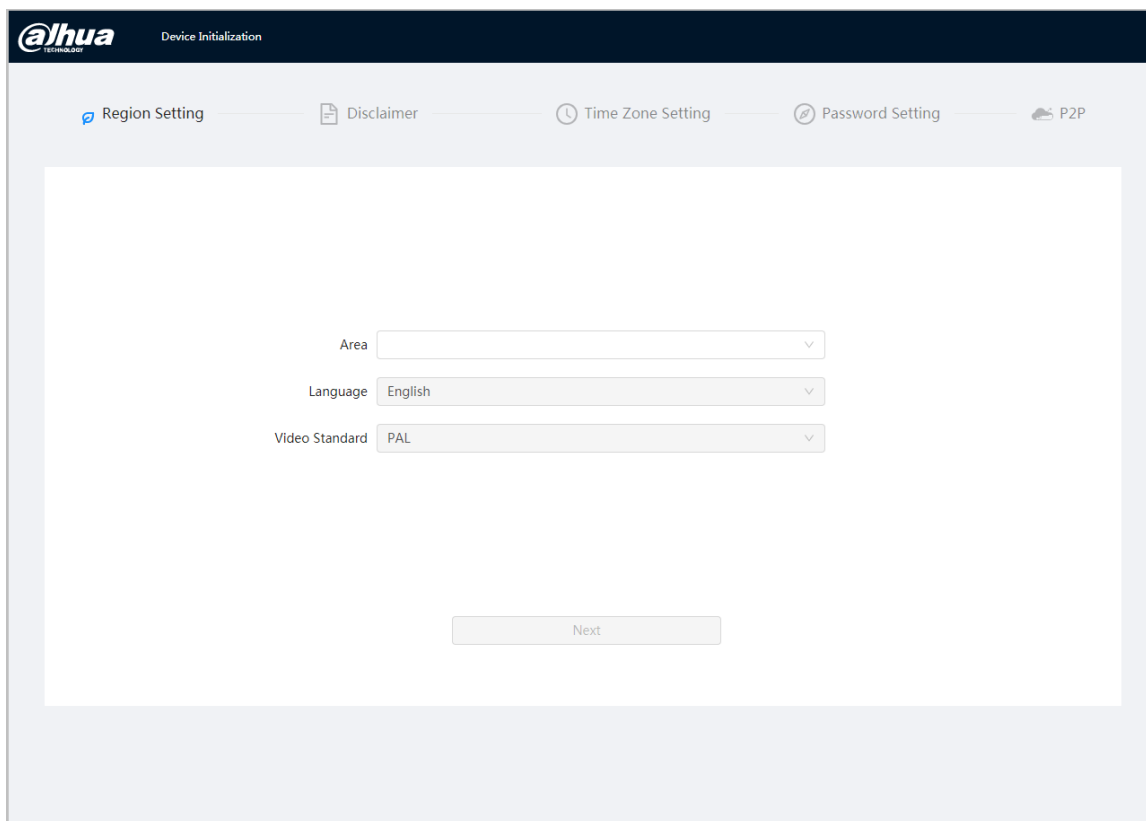
## Procedure

**Step 1** Open IE browser, enter the IP address of the device in the address bar, and then press the Enter key.



**The IP is 192.168.1.108 by default.**

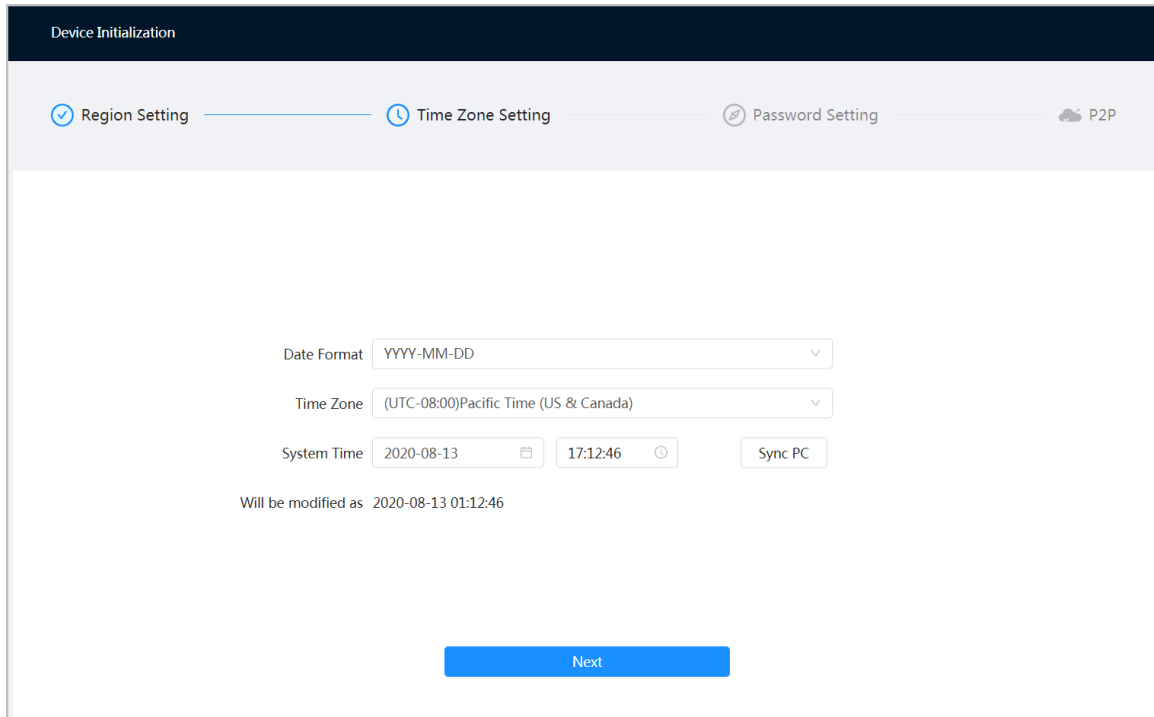
Figure 3-1 Region setting



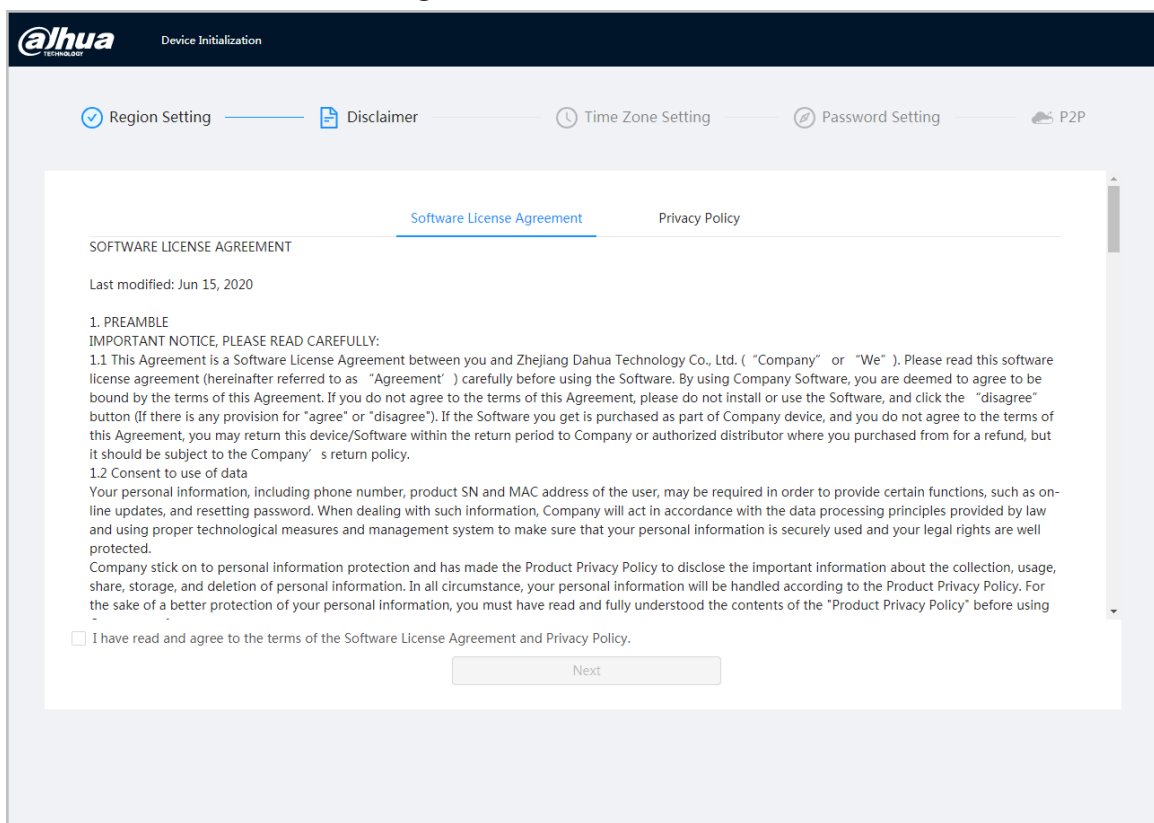
**Step 2** Select the area, language, and video standard according to the actual situation, and then click Next.



**Figure 3-2 Time zone setting**

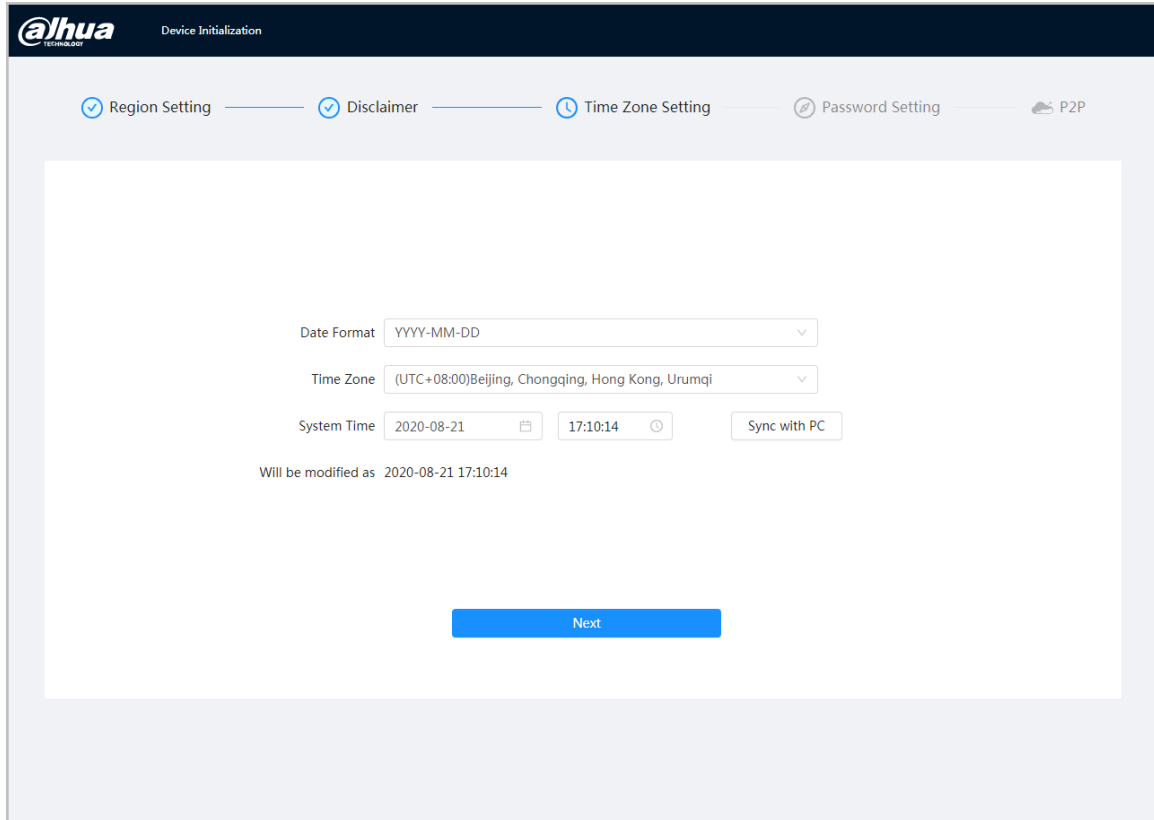


**Figure 3-3 Disclaimer**



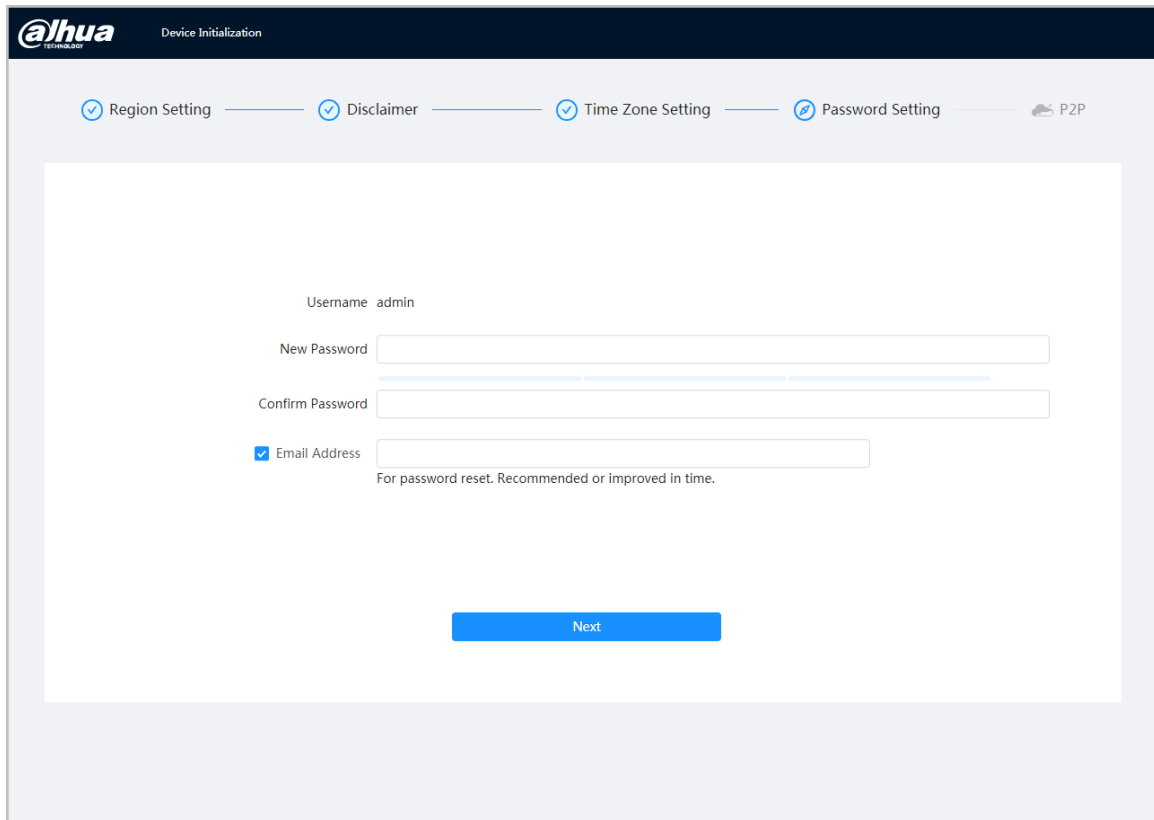
**Step 3** Select the I have read and agree to the terms of the Software License Agreement and Privacy Policy checkbox, and then click Next.

**Figure 3-4 Time zone setting**



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

**Figure 3-5 Password setting**



**Step 5** Set the password for admin account.

Table 3-1 Description of password configuration

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

**Step 6** Click Next, and then P2P page is displayed.

## 4 Login

### 4.1 Device Login

This section introduces how to log in to the webpage. This section takes Chrome as an example.



- You need to initialize the camera before logging in to the web page. For details, see "3 Device Initialization".
- When initializing the camera, keep the PC IP and device IP in the same network.
- Follow the instruction to download and install the plug-in for the first login.

#### Procedure

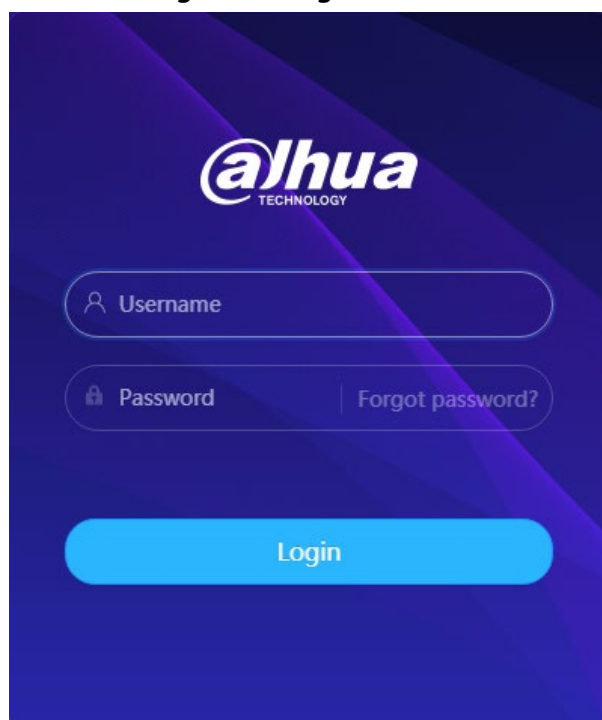
**Step 1** Open IE browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar and press Enter.

**Step 2** Enter the username and password.  
The username is admin by default.



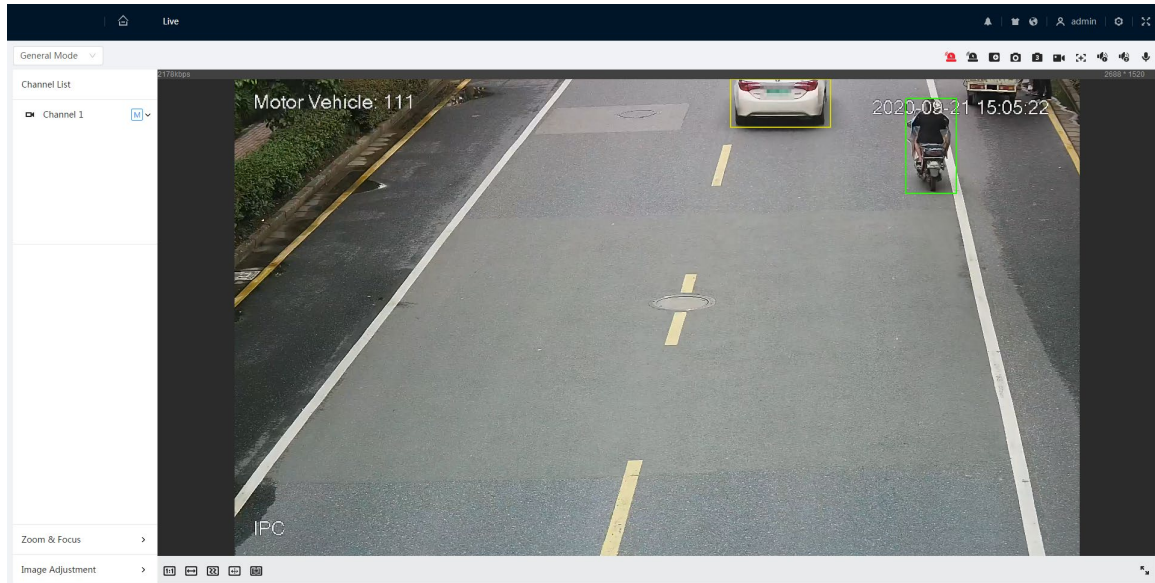
Click **Forgot password?**, and you can reset the password through the email address that is set during the initialization. For details, see "4.2 Resetting Password".

Figure 4-1 Login



**Step 3** Click Login.

Figure 4-2 Live page



## 4.2 Resetting Password

When you need to reset the password for the admin account, there will be a security code sent to the entered email address which can be used to reset the password.

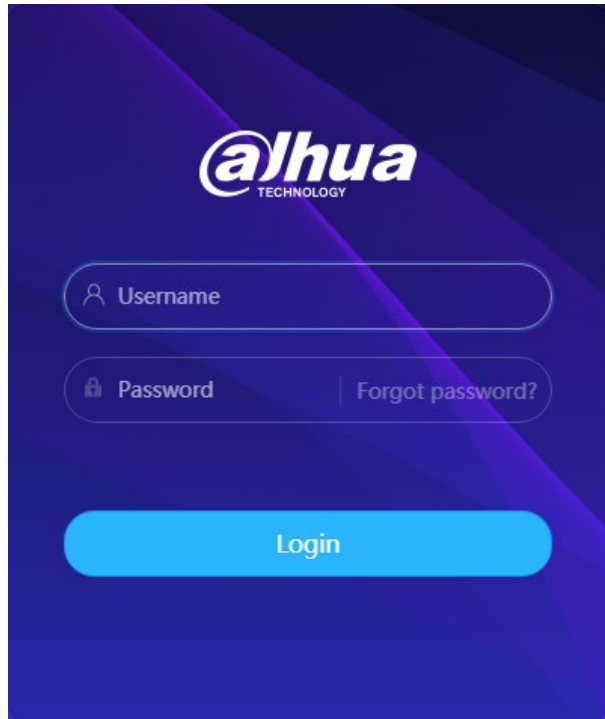
### Prerequisites

You have enabled password resetting service. For details, see "6.7.3.1.2 Resetting Password".

### Procedure

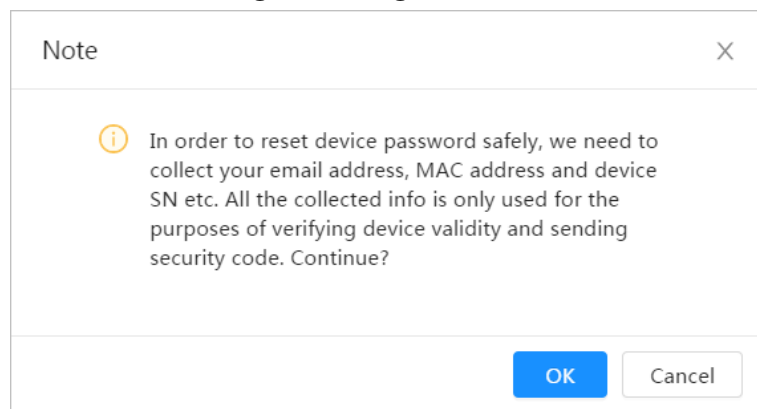
**Step 1** Open IE browser, enter the IP address of the device in the address bar and press Enter.

Figure 4-3 Login



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

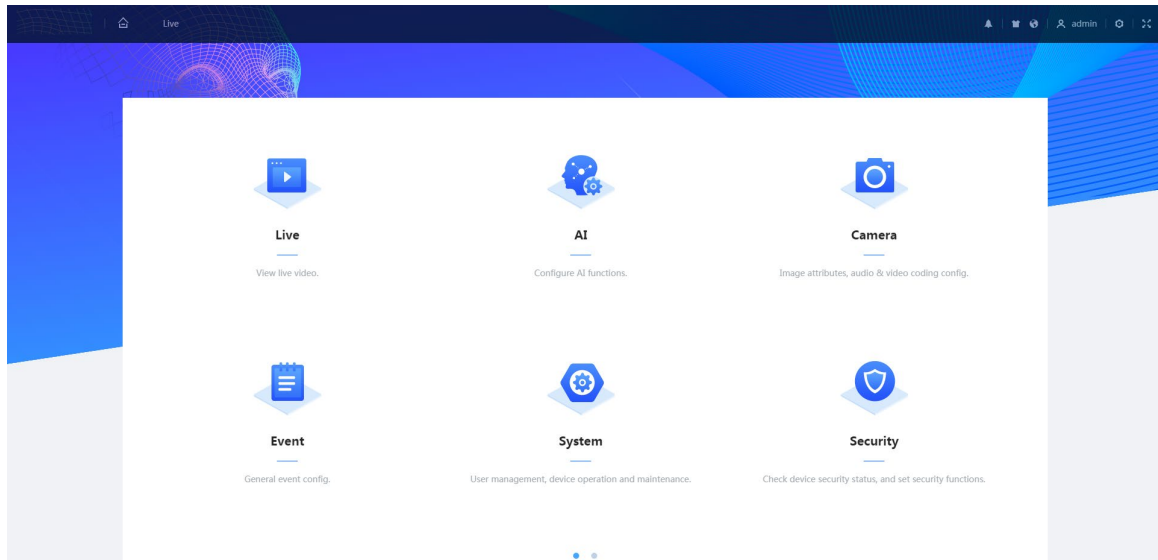
Figure 4-4 Login







## 5 Home Page

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

Figure 5-1 Home page



- **Live:** View the real-time monitoring image.
- **Analytics+:** Configure Analytics+ functions of the camera.
- **Camera:** Configure camera parameters, including image parameters, encoder parameters, and audio parameters.
- **PTZ:** Configure PTZ settings.
- **Event:** Configure general events, including alarm linkage exception, video detection, and audio detection.
- **System:** Configure system parameters, including general, date & time, account, safety, default, import/export, remote, auto maintain and upgrade.
- **Security:** Check the device security status and set security functions.
- **Record:** Play back or download recorded video.
- **Picture:** Play back or download image files.
- For the camera with multiple channels, through selecting channel numbers, you can set the parameters of the channels.
- **Report:** Search the Analytics+ event report and system report.
- **Alarm subscription:** Subscribe alarm.
- **Skin setting:** Set the skin.
- **Language setting:** Set the language.
- **Restart:** Click  **admin** at the upper-right corner of the page, select Reboot, and the camera restarts.
- **Logout:** Click  **admin** at the upper-right corner of the page, select Logout to go to the login page.  
The system will sleep automatically after idling for a period of time.
- **Setting:** Click  at the upper-right corner of the page to set the basic parameters.
- **Full screen:** Click  at the upper-right corner of the page to enter full screen mode; click

 to exit full screen mode.



# 6 Setting

This section introduces the basic setting of the camera, including the configuration of local, camera, network, event, storage, system, system information and log.

For Camera, Event and System, you can go to the configuration page through two methods.

This section takes method 1 as an example.

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

## 6.1 Local

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

### Procedure

**Step 1** Select  > Local.

Figure 6-1 Local


The screenshot shows a configuration page with three main sections:


- Play Parameter:** Contains a 'Protocol' field with three radio button options: 'TCP Port' (selected), 'UDP Port', and 'Multicast'.
- Record Path:** Contains three rows, each with a label, a text input field, and a 'Browse' button:
  - Live Record: C:\Users\... \WebDownload\LiveRecord
  - Playback Download: C:\Users\... \WebDownload\PlaybackRecord
  - Video Clip: C:\Users\... \WebDownload\VideoClips
- Snapshot Path:** Contains two rows, each with a label, a text input field, and a 'Browse' button:
  - Live Snapshot: C:\Users\... \WebDownload\LiveSnapShot
  - Playback Snapshot: C:\Users\... \WebDownload\PlaybackSnapshot

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

**Step 2** Click Browse to select the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.

Table 6-1 Description of local parameter

Parameter	Description
Protocol	<p>You can select the network transmission protocol as needed, and the options are TCP, UDP and Multicast.</p>  <p>Before selecting Multicast, make sure that you have set the Multicast parameters.</p>
Live Record	<p>The recorded video of live page. The default path is C:\Users\admin\WebDownload\LiveRecord.</p>
Playback Download	<p>The downloaded video of playback page. The default path is C:\Users\admin\WebDownload\PlaybackRecord.</p>
Video Clips	<p>The clipped video of playback page. C:\Users\admin\WebDownload\VideoClips.</p>
Live Snapshot	<p>The snapshot of live page. The default path is C:\Users\admin\WebDownload\LiveSnapshot.</p>
Playback Snapshot	<p>The snapshot of playback page. The default path is C:\Users\admin\WebDownload\PlaybackSnapshot.</p>



Admin in the path refers to the account being used.

**Step 3** Click Apply.

## 6.2 Camera

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



Camera parameters of different devices might vary.

### 6.2.1 Setting Image Parameters

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

#### 6.2.1.1 Page Layout

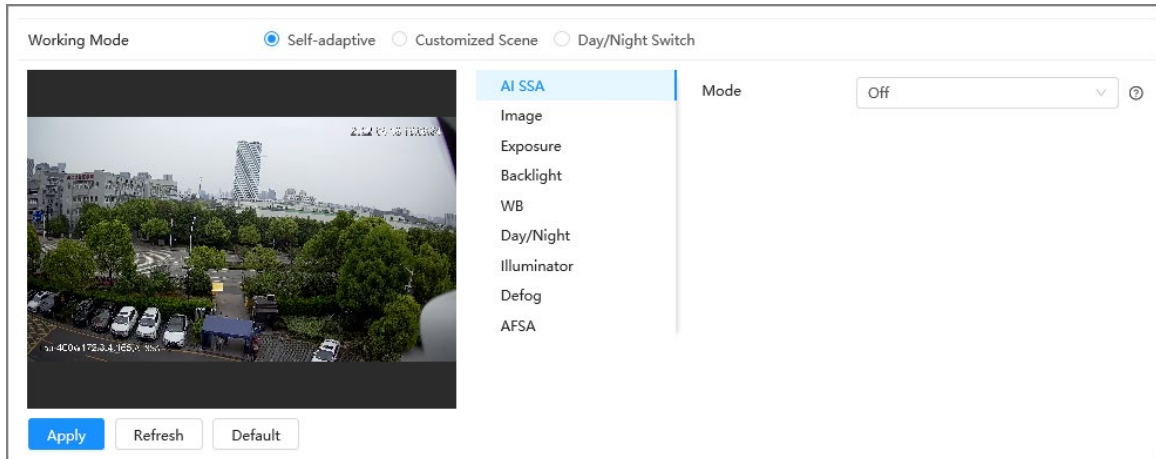
Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly.

You can select normal mode, day mode, or night mode to view the configuration and the effect of the selected mode, such as picture, exposure, and backlight.

Select the working mode as needed.

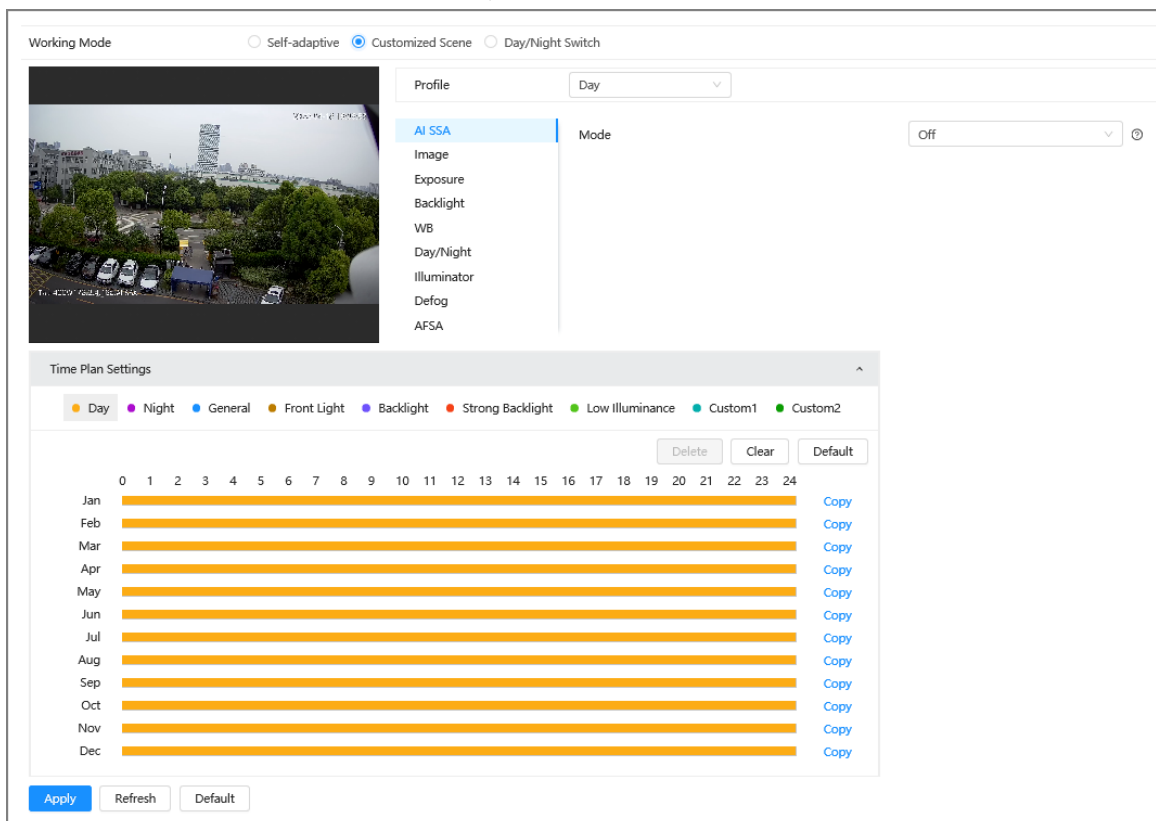
- **Self-adaptive:** The camera will adjust the image according to the environment.

**Figure 6-2 Page layout (self-adaptive)**



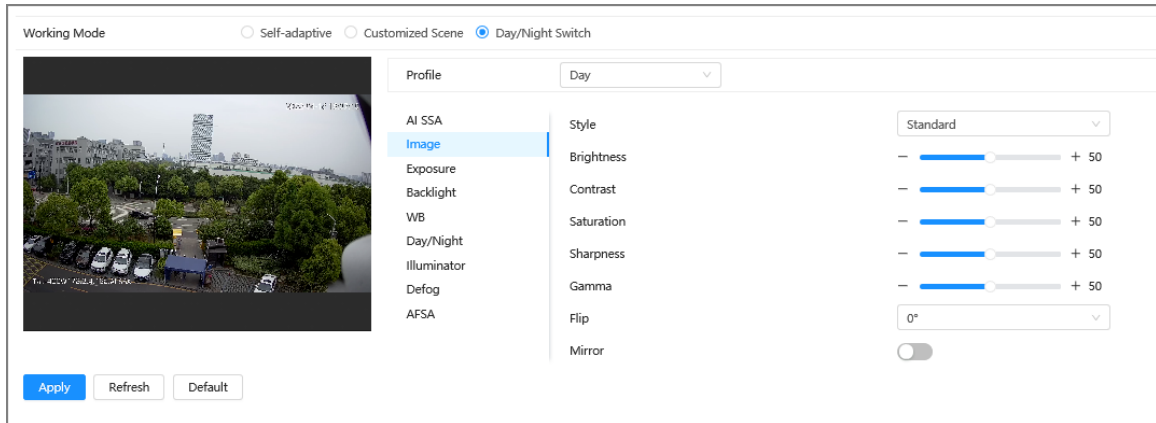
- **Customized scene:** You can select the profile as needed. Select the profile in Time Plan Setting and drag the slide block to set certain time as the selected profile. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night.

**Figure 6-3 Page layout (customized scene)**



- **Day/night switch:** You can select Day or night in Profile and the surveillance system works under Day/Night.

Figure 6-4 Page layout (day/night switch)



### 6.2.1.2 AI SSA

By enabling AI SSA (Analytics+ Scene Self-adaptation), the camera could detect environmental conditions, such as rain, fog, backlight, low light and flicker, to adjust the parameters of the image to suit the conditions, ensuring that clear images are always produced.

#### Procedure

**Step 1** Select > Camera > Image > AI SSA.

**Step 2** Select On in the dropdown list.



After you enable AI SSA, some other functions such as exposure, backlight, defog and AFSA will be disabled by default.

**Step 3** Click Apply.

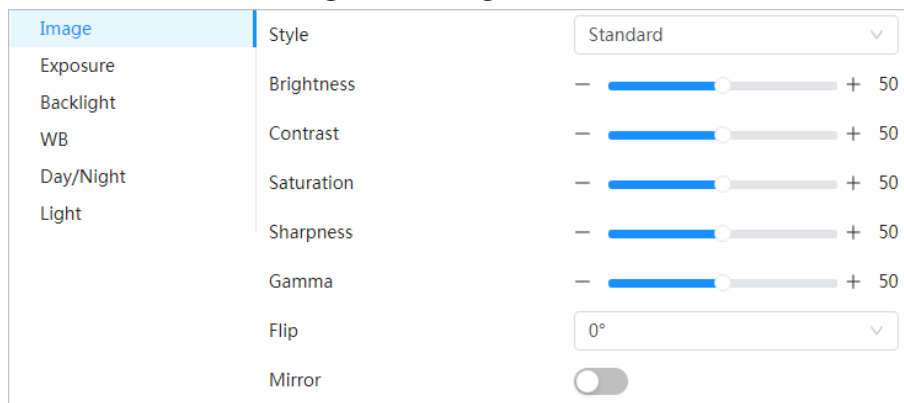
### 6.2.1.3 Image

You can configure picture parameters as needed.

#### Procedure


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

Figure 6-5 Image



**Step 2** Configure picture parameters.

Table 6-2 Description of picture parameters

Parameter	Description
Style	<p>Select the picture style from soft, standard and vivid.</p> <ul style="list-style-type: none"> <li>• <b>Soft:</b> Default image style, displays the actual color of the image.</li> <li>• <b>Standard:</b> The hue of the image is weaker than the actual one, and contrast is smaller.</li> <li>• <b>Vivid:</b> The image is more vivid than the actual one.</li> </ul>
Brightness	<p>Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.</p>
Contrast	<p>Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.</p>
Saturation	<p>Makes the color deeper or lighter. The higher the value is, the deeper the color will be, and the lower the lighter. Saturation value does not change image brightness.</p>
Sharpness	<p>Changes the sharpness of picture edges. The higher the value is, the clearer the picture edges will be, and if the value is set too big, picture noises are more likely to appear.</p>
Gamma	<p>Changes the picture brightness and improves the picture dynamic range in a non-linear way. The higher the value is, the brighter the picture will be, and the smaller the darker.</p>
Flip	<p>Changes the display direction of the picture, see the options below.</p> <ul style="list-style-type: none"> <li>• 0°: Normal display.</li> <li>• 90°: The picture rotates 90° clockwise.</li> <li>• 180°: The picture rotates 90° counterclockwise.</li> <li>• 270°: The picture flips upside down.</li> </ul> <p></p> <p>For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "6.2.2 Setting Encode Parameters".</p>
Mirror	<p>Click <input type="checkbox"/>, and the picture will display with left and right side reversed.</p>

**Step 3** Click Apply.

### 6.2.1.4 Exposure

Configure iris and shutter to improve image clarity.

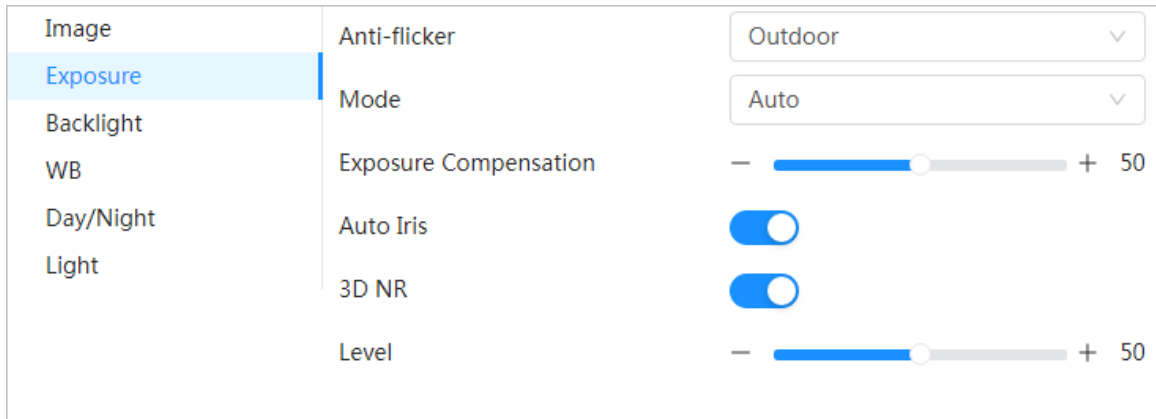


**Cameras with true WDR do not support long exposure when WDR is enabled in Backlight.**

**Procedure**

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


**Figure 6-6 Exposure**



**Step 2** Configure exposure parameters.

**Table 6-3 Description of exposure parameters**

Parameter	Description
Anti-flicker	<p>You can select from 50 Hz, 60 Hz and Outdoor.</p> <ul style="list-style-type: none"> <li>• <b>50 Hz:</b> When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that no stripe appears.</li> <li>• <b>60 Hz:</b> When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that no stripe appears.</li> <li>• <b>Outdoor:</b> You can select any exposure mode as needed.</li> </ul>

Parameter	Description
Mode	<p>Device exposure modes.</p> <ul style="list-style-type: none"> <li>• <b>Auto:</b> Adjusts the image brightness according to the actual condition automatically.</li> <li>• <b>Gain Priority:</b> When the exposure range is normal, the system prefers the configured gain range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the gain has reached upper or lower limit, the system adjusts shutter value automatically to ensure the image at ideal brightness. You can configure gain range to adjust gain level when using gain priority mode.</li> <li>• <b>Shutter priority:</b> When the exposure range is normal, the system prefers the configured shutter range when auto adjusting according to the ambient lighting condition. If the image brightness is not enough and the shutter value has reached upper or lower limit, the system adjusts gain value automatically to ensure the image at ideal brightness.</li> <li>• <b>Manual:</b> Configure gain and shutter value manually to adjust image brightness.</li> </ul> <p> <b>When the Anti-flicker is set to Outdoor, you can select Auto, Gain priority, Shutter priority or Manual in the Mode list.</b></p>
Exposure Compensation	Sets the value, and it ranges from 0 to 50. The higher the value is, the brighter the image will be.
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposure time will be.
Gain	When selecting Gain Priority or Manual in Mode, you can set Gain. With minimum illumination, the camera increases Gain automatically to get clearer images.
Auto Iris	<p>This configuration is available only when the camera is equipped with auto-iris lens.</p> <ul style="list-style-type: none"> <li>• When auto iris is enabled, the iris size changes automatically according to the ambient lighting condition, and the image brightness changes accordingly.</li> <li>• When auto iris is disabled, the iris stays at full size and does not change no matter how ambient lighting condition changes.</li> </ul>
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames.
Level	This configuration is available only when the 3D NR is enabled. The higher the level is, the better the result will be.

**Step 3** Click Apply.

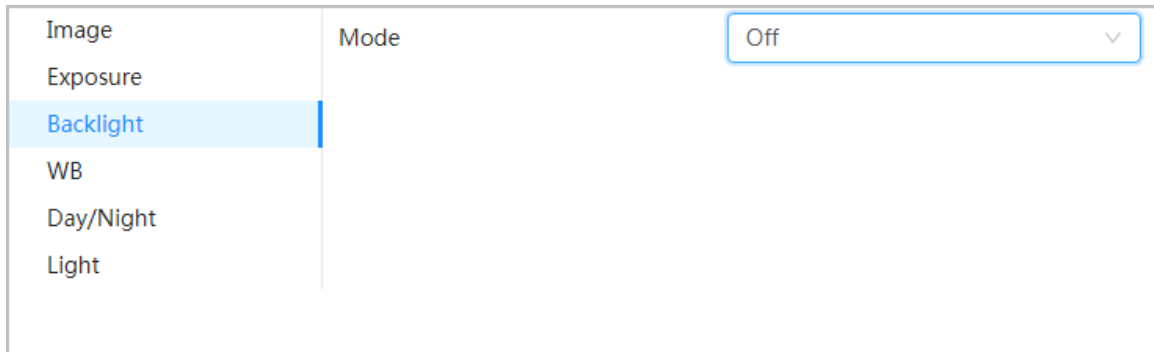
### 6.2.1.5 Backlight

You can select backlight mode from Auto, BLC, WDR, and HLC.

#### Procedure

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

Figure 6-7 Backlight



**Step 2** Configure backlight parameters.

Table 6-4 Description of backlight parameters

Backlight mode	Description
BLC	<p>Enable BLC, the camera can get clearer image of the dark areas on the target when shooting against light. You can enable or disable Customized mode.</p> <ul style="list-style-type: none"> <li>When you enable Customized mode, the system auto adjusts exposure only to the set area according to ambient lighting condition to ensure the image of the set area at ideal brightness.</li> <li>When you disable Default mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area.</li> </ul>
WDR	<p>The system dims bright areas and compensates dark areas to ensure the clarity of all the area. The higher the value is, the brighter the dark will be, but the more the noise will be.</p> <p> There might be a few seconds of video loss when the device is switching to WDR mode from other mode.</p>
HLC	<p>Enable HLC when extreme strong light is in the environment (such as toll station or parking lot), the camera will dim strong light, and reduce the size of Halo zone to lower the brightness of the whole image, so that the camera can capture human face or car plate detail clearly. The higher the value is, the more obvious the HLC effect will be.</p>
SSA	<p>Enable SSA, the system automatically adjusts the image brightness according to the environment to make the objects in the image clearer.</p>

**Step 3** Click Apply.



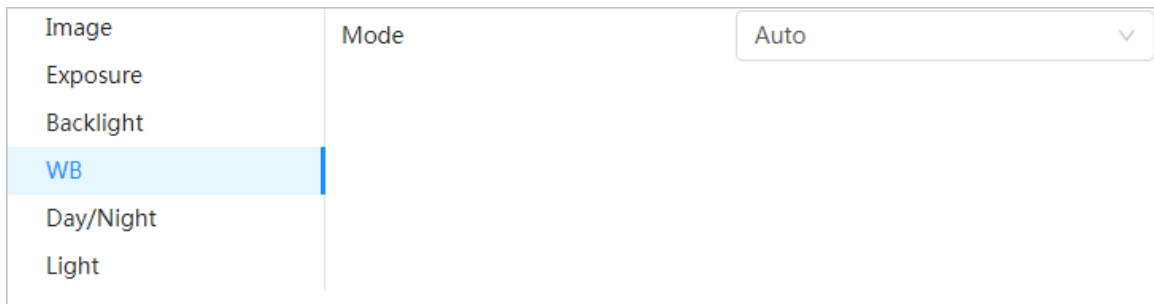
### 6.2.1.6 WB

WB function makes the image color display precisely as it is. When in WB mode, white objects would always display white color in different environments.

#### Procedure

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

Figure 6-8 WB



**Step 2** Configure WB parameters.

Table 6-5 Description of WB parameters

WB Mode	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Natural	The system auto compensates WB to environments without artificial light to ensure color precision.
Street Lamp	The system compensates WB to outdoor night scene to ensure color precision.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
Manual	Configure red and blue gain manually; the system auto compensates WB according to color temperature.
Custom Area	The system compensates WB only to the set area according to color temperature to ensure color precision.

**Step 3** Click Apply.

### 6.2.1.7 Day/Night

Configure the display mode of the image. The system switches between color and black-and-white mode according to the actual condition.

#### Procedure


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

Figure 6-9 Day/night

Image	Mode	Auto
Exposure	Sensitivity	Medium
Backlight	Delay	6sec.
WB		
Day/Night		
Light		

**Step 2** Configure day and night parameters.

Table 6-6 Description of day and night parameters

Parameter	Description
Mode	<p>You can select device display mode from Color, Auto, and B/W.</p>  <p><b>Day/Night configuration is independent from profile management configuration.</b></p> <ul style="list-style-type: none"> <li>• <b>Color:</b> The system displays color image.</li> <li>• <b>Auto:</b> The system switches between color and black-and-white display according to the actual condition.</li> <li>• <b>B/W:</b> The system displays black-and-white image.</li> </ul>
Sensitivity	<p>This configuration is available only when you set Auto in Mode. You can configure camera sensitivity when switching between color and black-and-white mode.</p>
Delay	<p>This configuration is available only when you set Auto in Mode. You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.</p>

**Step 3** Click Apply.

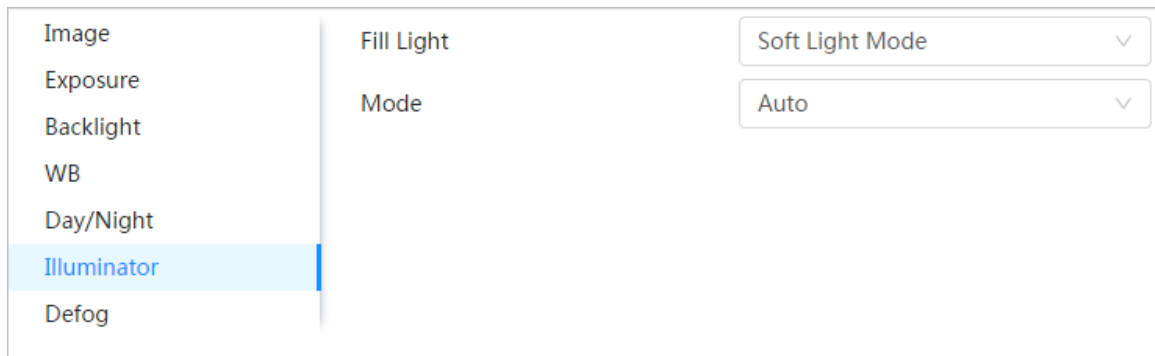
### 6.2.1.8 Illuminator

This configuration is available only when the device is equipped with illuminator.

#### Procedure

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

Figure 6-10 Light



**Step 2** Configure illuminator parameters.

Table 6-7 Description of illuminator parameters

Parameter	Description	
Fill Light	<p>Set Fill Light for sound and siren cameras.</p> <ul style="list-style-type: none"> <li>• <b>IR Mode:</b> Enable the IR illuminator, and the white light is disabled. When an alarm is triggered, the system will link white light.</li> <li>• <b>White Light:</b> Enable the white light, and the IR illuminator is disabled. When an alarm is triggered, the system will link white light.</li> <li>• <b>Soft Light Mode:</b> Enable IR illuminator and white light at the same time, and adjust the brightness of the two illuminators to get clear images.</li> </ul>	
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.
	Auto	The system adjusts the illuminator intensity according to the ambient lighting condition.
	Zoom Priority	<p>The system adjusts the illuminator intensity automatically according to the change of the ambient light.</p> <ul style="list-style-type: none"> <li>• When the ambient light turns darker, the system turns on the low beam lights first, if the brightness is still not enough, it turns on the high beam lights then.</li> <li>• When the ambient light turns brighter, the system dims high beam lights until they are off, and then the low beam lights.</li> <li>• When the focus reaches certain wide angle, the system will not turn on high beam light in order to avoid over-exposure in short distance. In the meantime, you can configure light compensation manually to fine-tune IR light intensity.</li> </ul>
	Off	Illuminator is off.

**Step 3** Click Apply.

### 6.2.1.9 Defog

The image quality is compromised in foggy or hazy environment, and defog can be used to improve image clarity.

#### Procedure

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

Figure 6-11 Light



**Step 2** Configure defog parameters.

Table 6-8 Description of defog parameters

Defog	Description
Manual	Configure function intensity and atmospheric light mode manually, and then the system adjusts image clarity accordingly. Atmospheric light mode can be adjusted automatically or manually.
Auto	The system adjusts image clarity according to the actual condition.
Off	Defog function is disabled.

**Step 3** Click Apply.

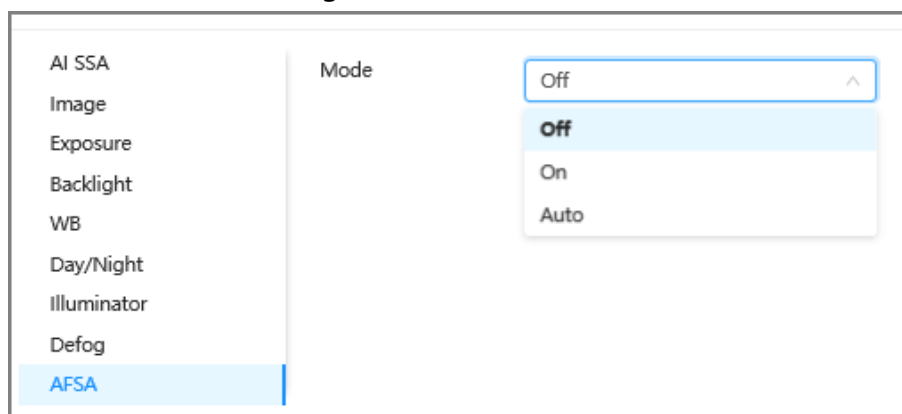
### 6.2.1.10 AFSA

You can enable AFSA (Anti-flicker Self-adaption) to prevent image flickering.

#### Procedure

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

Figure 6-12 AFSA



**Step 2** Select On or Auto in the dropdown list.



**When you select Auto, AFSA function will be enabled when the camera detects flicker and disabled when there is no flicker.**

**Step 3** Click Apply.

### 6.2.1.11 Fisheye

Select installation mode and record mode according to the actual installation scene. When the camera accesses the platform with corrective stream, the platform displays the corrective image.

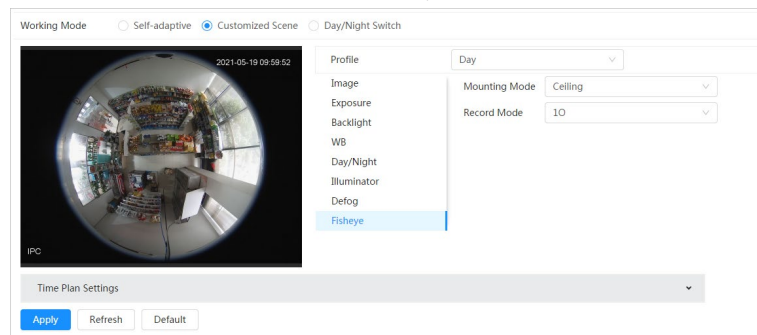


**This function is only available on fisheye device.**

#### Procedure

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

**Figure 6-13 Fisheye**



**Step 2** Set installation mode and record mode.

**Table 6-9 Description of fisheye parameters**

Parameter	Description
installation Mode	You can select Ceiling, Wall, or Ground.

Parameter	Description
Record Mode	<ul style="list-style-type: none"> <li>• 1O: The original image before correction.</li> <li>• 1P: 360° rectangular panoramic image.</li> <li>• 2P: When the installation mode is Ceiling or Ground, you can set this mode. Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image.</li> <li>• 1R: Original image screen + independent sub-screen. You can zoom or drag the image in all the screens.</li> <li>• 2R: Original image screen + two independent sub-screens. You can zoom or drag the image in all the screens.</li> <li>• 4R: Original image screen + four independent sub-screens. You can zoom or drag the image in all the screens.</li> <li>• 1O + 3R: Original image screen + three independent sub-screens. You can zoom or drag the image in original image screen, and move the image (upper and lower) in sub-screens to adjust the vertical view.</li> </ul>

**Step 3** Click Apply.

## 6.2.2 Setting Encode Parameters

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



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

### 6.2.2.1 Encode

Configure video stream parameters, such as compression, resolution, frame rate, bit rate type, bit rate, I frame interval, SVC, and watermark.

#### Procedure

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

Figure 6-14 Encode


The screenshot shows the 'Encode' configuration page with the following settings:

- Channel:** CAM 1
- Main Stream:**
  - Compression: H.264H
  - Smart Codec:
  - Resolution: 2592\*1944(2592x1944)
  - Frame Rate (FPS): 25
  - Bit Rate Type: CBR
  - Reference Bit Rate: 3329-16093 (Kb/s)
  - Bit Rate: 6144 (Kb/s)
  - I Frame Interval: 50 (25-150)
  - SVC: 1(off)
- Sub Stream:**
  - Sub Stream: Sub Stream 1
  - Compression: H.264H
  - Resolution: 704\*576(D1)
  - Frame Rate (FPS): 25
  - Bit Rate Type: CBR
  - Reference Bit Rate: 256-2304 (Kb/s)
  - Bit Rate: 512 (Kb/s)
  - I Frame Interval: 50 (25-150)
  - SVC: 1(off)
- Watermark:**  DigitalCCTV
- Buttons:** Apply, Refresh, Default

**Step 2** Configure encode parameters.

Table 6-10 Description of encode parameters

Parameter	Description
Sub Stream	<p>Click <input checked="" type="checkbox"/> to enable sub stream, it is enabled by default.</p> <p> You can enable multiple sub streams simultaneously.</p>
Compression	<p>Select encode mode.</p> <ul style="list-style-type: none"> <li>• <b>H.264:</b> Main profile encode mode. Compared with H.264B, it requires smaller bandwidth.</li> <li>• <b>H.264H:</b> High profile encode mode. Compared with H.264, it requires smaller bandwidth.</li> <li>• <b>H.264B:</b> Baseline profile encode mode. It requires smaller bandwidth.</li> <li>• <b>H.265:</b> Main profile encode mode. Compared with H.264, it requires smaller bandwidth.</li> <li>• <b>MJPEG:</b> When under this mode, the image requires high bit rate value to ensure clarity, you are recommended to set the Bit Rate value to the biggest value in the Reference Bit Rate.</li> </ul>
Smart Codec	<p>Click <input type="checkbox"/> to enable smart codec to improve video compressibility and save storage space.</p> <p> After smart codec is enabled, the device would stop supporting the third bit stream, ROI, and smart event detection.</p>
Output Mode	You can select from Single Stream or Flex Stream.
Resolution	The resolution of the video. The higher the value is, the clearer the image will be, but the bigger the required bandwidth will be.

Parameter	Description
Frame Rate (FPS)	The number of frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	<p>The bit rate control type during video data transmission. You can select bit rate type from:</p> <ul style="list-style-type: none"> <li>• CBR (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value.</li> <li>• VBR (Variable Bit Rate): The bit rate changes as monitoring scene changes.</li> </ul> <p> The Bit Rate Type can only be set as CBR when Encode Mode is set as MJPEG.</p>
Quality	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>The better the quality is, but the bigger the required bandwidth will be.</p>
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.
Max Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>You can select the value of the Max Bit Rate according to the Reference Bit Rate value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.</p>
Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as CBR.</p> <p>Select bit rate value in the list according to actual condition.</p>
I Frame Interval	<p>The number of P frames between two I frames, and the I Frame Interval range changes as FPS changes.</p> <p>It is recommended to set I Frame Interval twice as big as FPS.</p>
SVC	<p>Scaled video coding, is able to encode a high quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of related lays according to the network status.</p> <ul style="list-style-type: none"> <li>• 1: The default value, which means that there is no layered coding.</li> <li>• 2, 3 and 4: The lay number that the video stream is packed.</li> </ul>
Watermark	You can verify the watermark to check if the video has been tampered.
Watermark String	

**Step 3** Click Apply.

### 6.2.2.2 Overlay

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



### 6.2.2.2.1 Configuring Privacy Masking

You can enable this function when you need to protect the privacy of some area on the video image.

#### Background Information

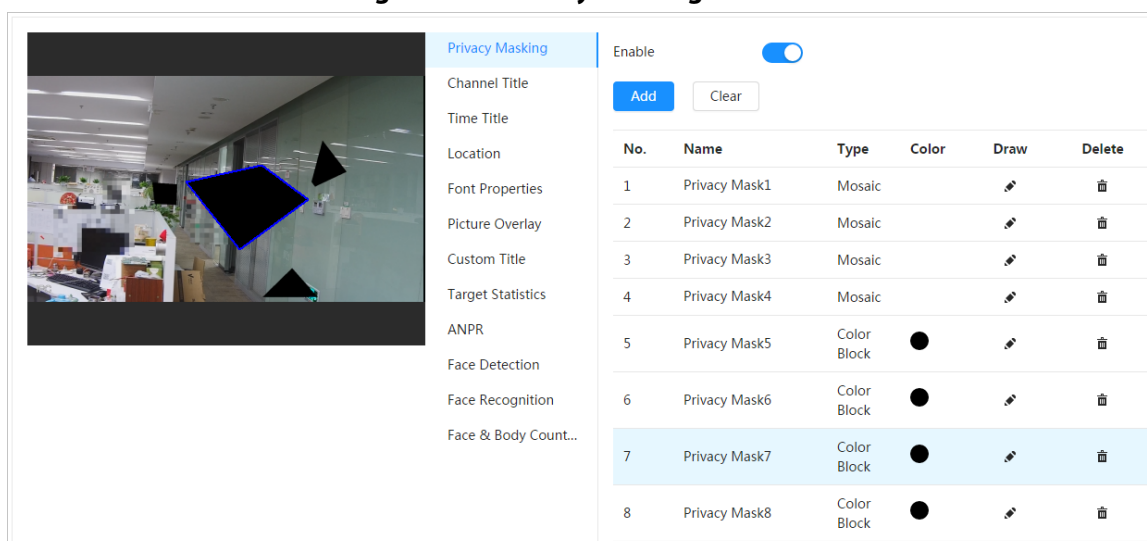
You can select the type of the masking from Color Block and Mosaic.

- When selecting Color Block only, you can draw triangles and convex quadrilaterals as blocks. You can drag 8 blocks at most, and the color is black.
- When selecting Mosaic, you can draw rectangles as blocks with mosaic. You can draw 4 blocks at most.
- Color Block + Mosaic: You can draw 8 blocks at most.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Privacy Masking.

Figure 6-15 Privacy masking



**Step 2** Configure privacy masking.

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

#### Related Operations

- View and edit the block  
Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- Edit the block name  
Double-click the name in Name to edit the block name.
- Delete the block
  - ◇ Click to delete blocks one by one.
  - ◇ Click Clear to delete all blocks.

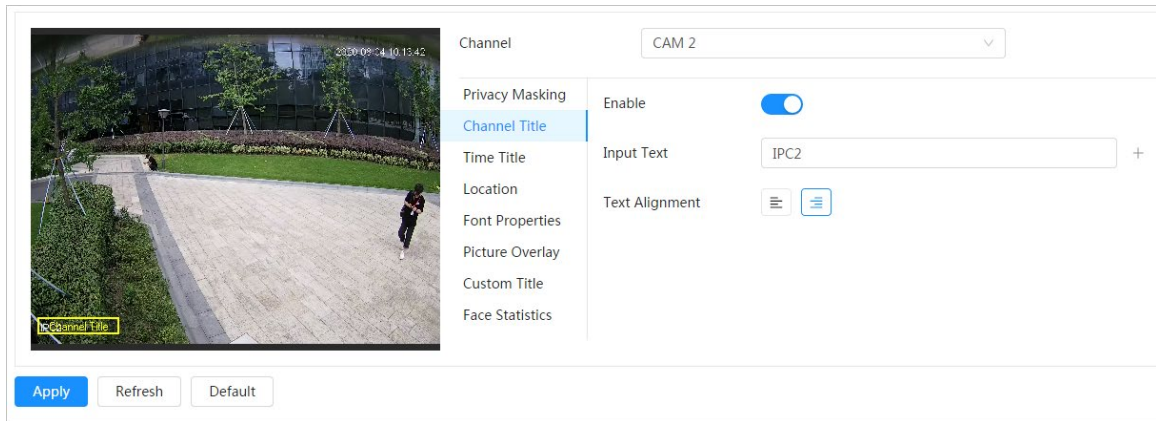
### 6.2.2.2.2 Configuring Channel Title

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

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Channel Title.

Figure 6-16 Channel title



**Step 2** Click  next to Enable, enter the channel title, and select the text alignment.



Click **+** to add the channel title, and you can add 1 line at most.

**Step 3** Move the title box to the position that you want in the image.

**Step 4** Click Apply.

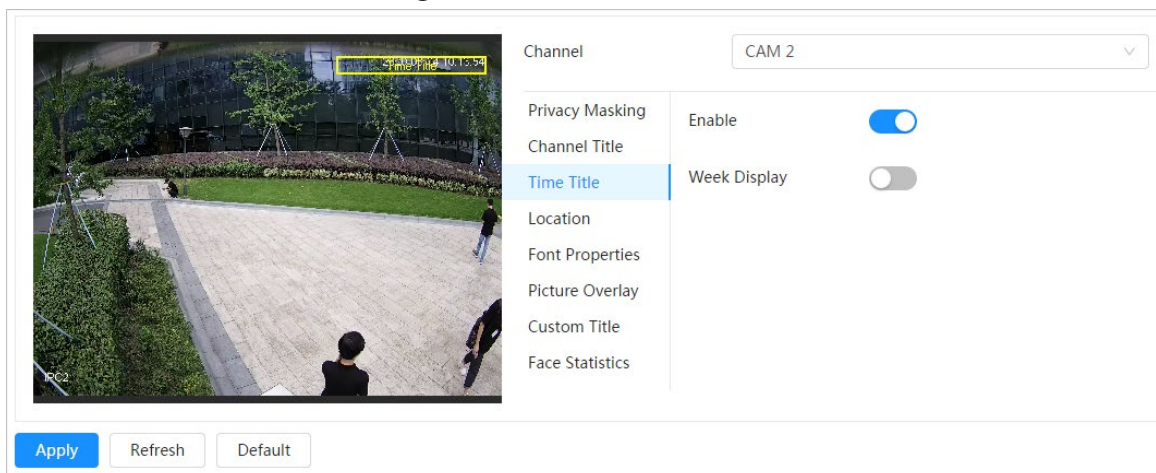
### 6.2.2.2.3 Configuring Time Title

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

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Time Title.

Figure 6-17 Time title



**Step 2** Click  next to Enable.

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

**Step 4** Move the time box to the position that you want in the image.

**Step 5** Click Apply.

### 6.2.2.2.4 Configuring Location

You can enable this function if you need to display text in the video image.

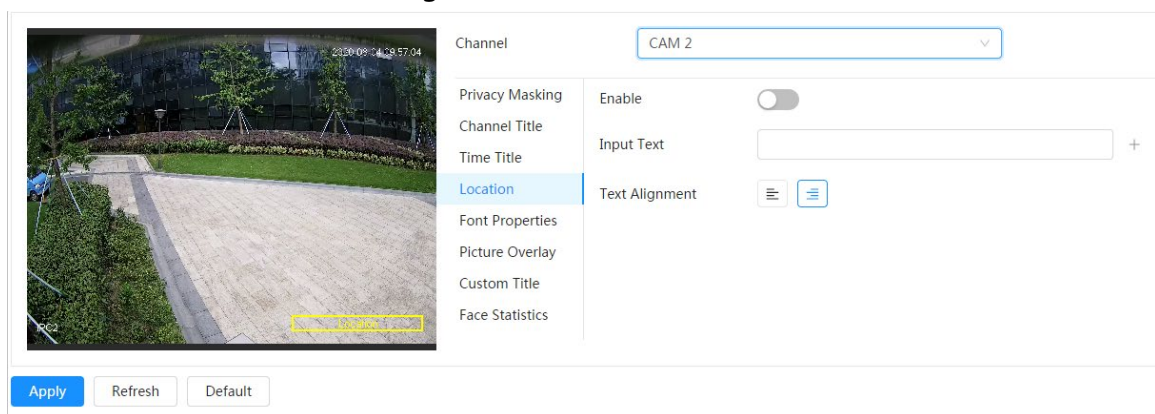


**Text overlay and picture overlay cannot work at the same time, and the IPC that connects to mobile NVR with private protocol would display GPS information as priority.**

### Procedure

**Step 1** Select > Camera > Encode > Overlay > Location.

**Figure 6-18 Location**



**Step 2** Click  next to Enable, enter the location information, and then select alignment. The text is displayed in the video image.



**Click + to add the text overlay, and you can add 13 lines at most.**

**Step 3** Move the text box to the position that you want in the image.

**Step 4** Click Apply.

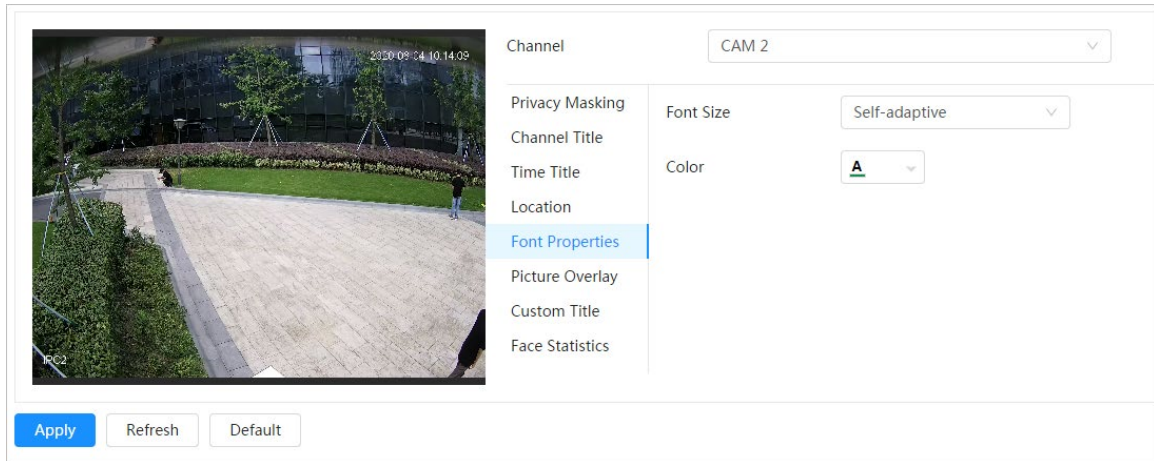
### 6.2.2.2.5 Configuring Font Properties

You can enable this function if you need to adjust the font size in the video image.

### Procedure

**Step 1** Select > Camera > Encode > Overlay > Font Properties.

Figure 6-19 Font properties



**Step 2** Select the font color and size.

You can set the RGB value to customize the font color.

**Step 3** Click Apply.

### 6.2.2.2.6 Configuring Picture Overlay

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

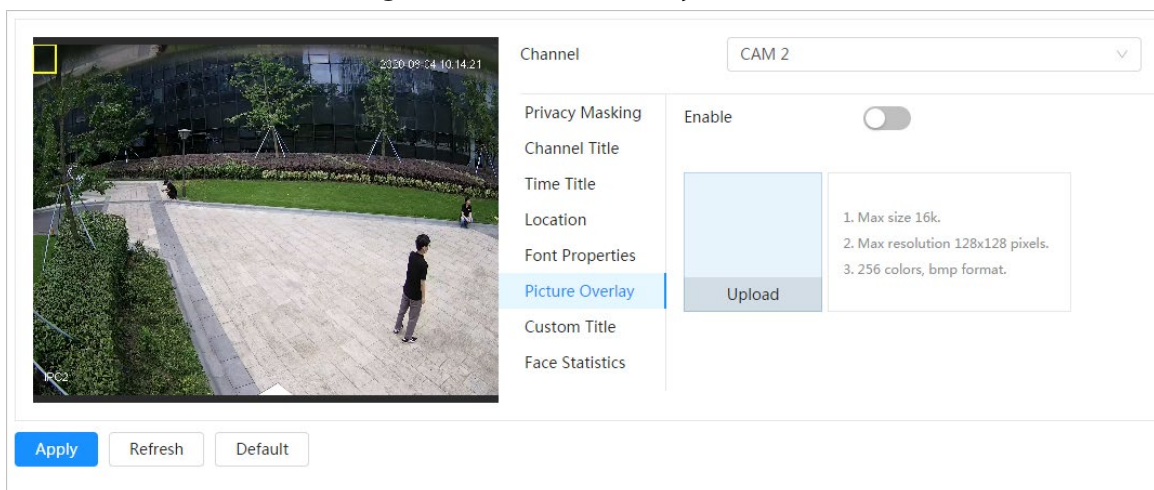


**Text overlay and picture overlay cannot work at the same time.**

### Procedure

**Step 1** Select > Camera > Encode > Overlay > Picture Overlay.

Figure 6-20 Picture overlay



**Step 2** Click next to Enable, click Upload, and then select the picture to be overlaid. The picture is displayed on the video image.

**Step 3** Move the overlaid picture to the position that you want in the image.

**Step 4** Click Apply.

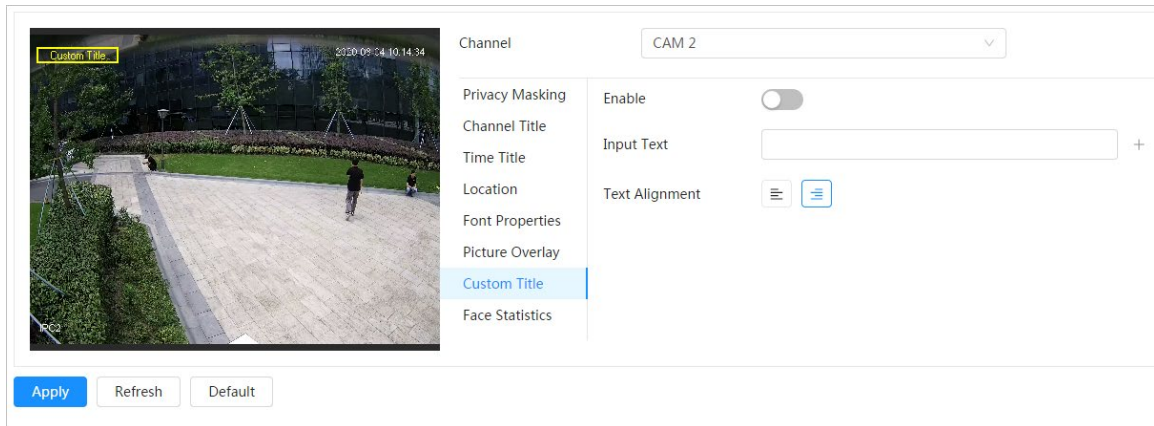
### 6.2.2.2.7 Configuring Custom Title

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

## Procedure

**Step 1** Select  > Camera > Encode > Overlay > Custom Title

**Figure 6-21 Custom title**



**Step 2** Click  next to Enable, enter the text that you want to display, and then select the text alignment.



Click **+** to add the text overlay, and you can add 1 line at most.

**Step 3** Move the custom box to the position that you want in the image.

**Step 4** Click Apply.

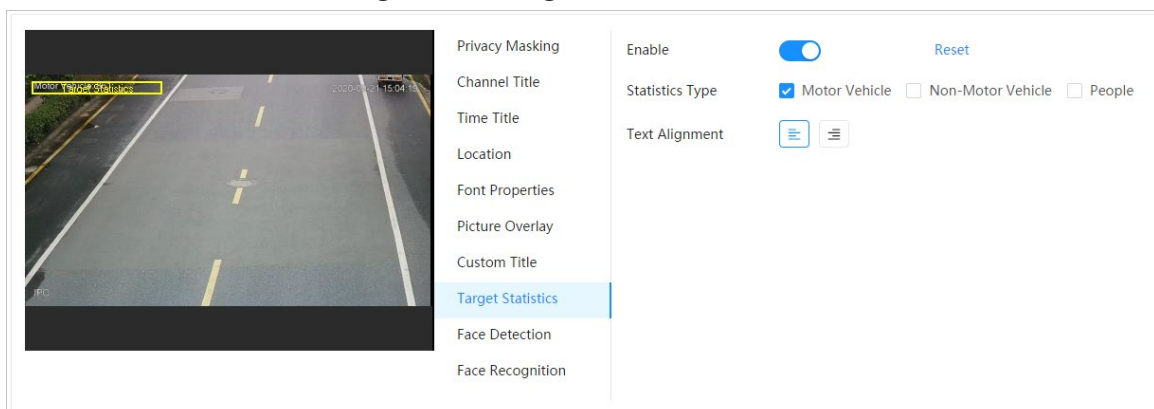
### 6.2.2.2.8 Configuring Target Statistics

After configuring the target statistics, the number of target statistics will be displayed on the image.

## Procedure

**Step 1** Select  > Camera > Encode > Overlay > Target Statistics.

**Figure 6-22 Target statistics**



**Step 2** Click  next to Enable, select the statistics type, and then select the text alignment.



Click **Reset** to clear the statistics data.

**Step 3** Move the custom box to the position that you want in the image.



**Step 4** Click Apply.

The overlaid information will be displayed after enabling video Analytics function.

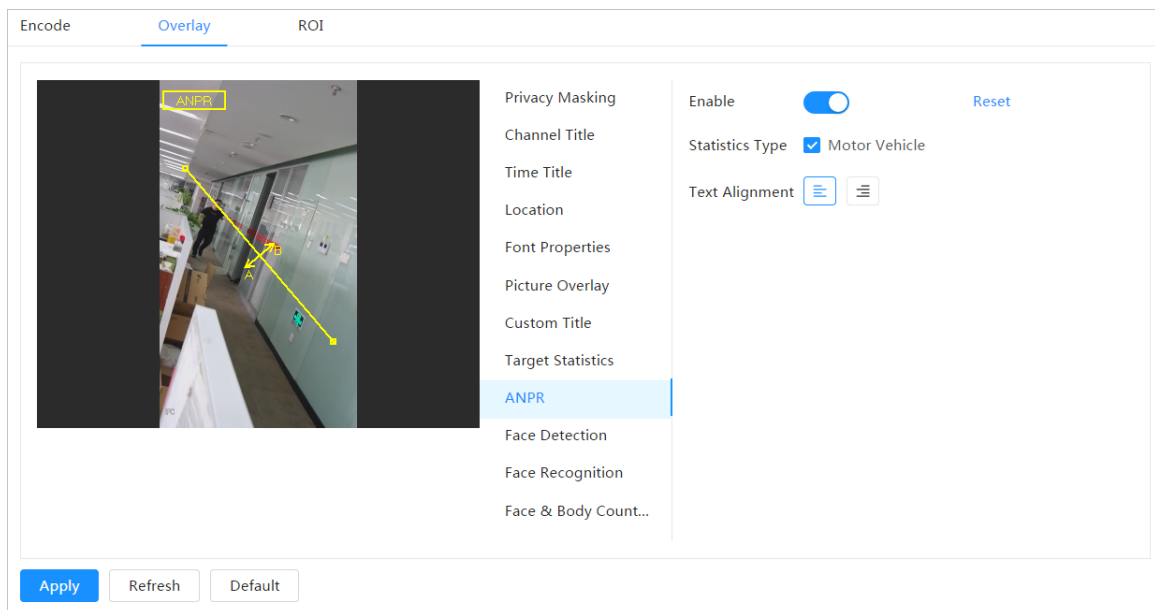
### 6.2.2.2.9 Configuring ANPR

After enabling this function, ANPR statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > ANPR.

Figure 6-23 ANPR



**Step 2** Select the Enable check box, select the statistics type, and then select text alignment.



Click Reset to clear the statistics data.

**Step 3** Move the ANPR box to the position that you want in the image.

**Step 4** Click Apply.

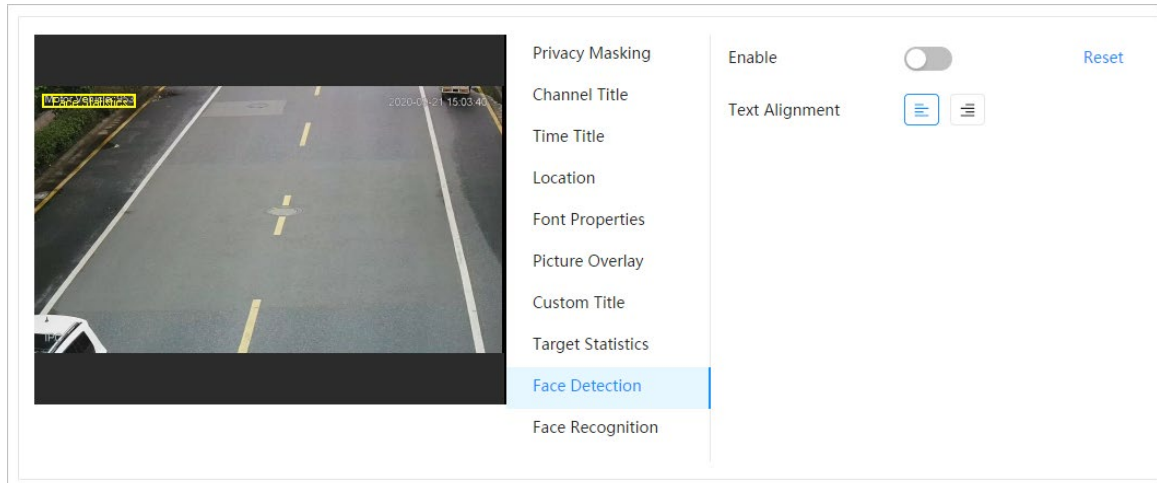
### 6.2.2.2.10 Configuring Face Detection

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Face Detection.

**Figure 6-24 Face detection**



**Step 2** Click  next to Enable, and select the text alignment.



Click Reset to clear the statistics data.

**Step 3** Move the statistics box to the position that you want in the image.

**Step 4** Click Apply.

The information will be displayed on the image after the face detection function is enabled.

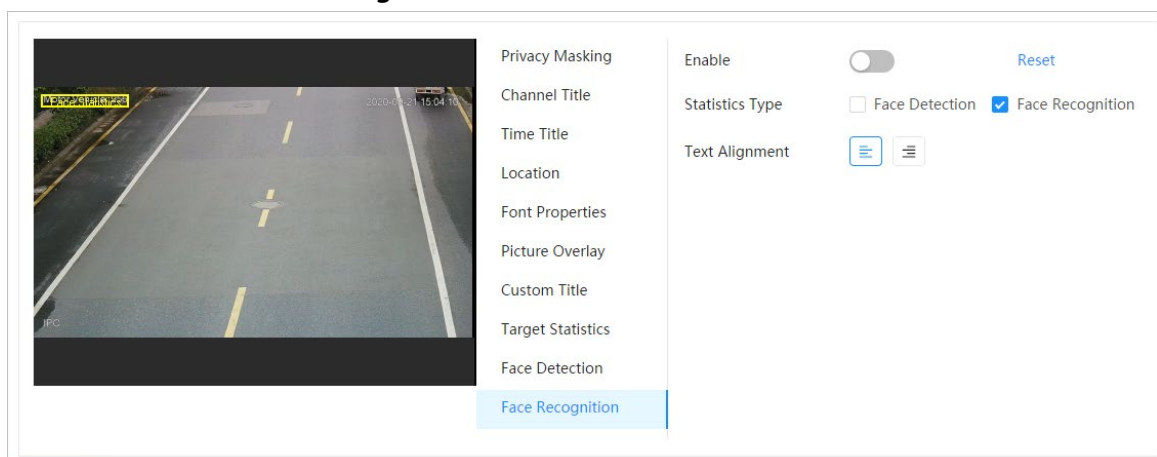
### 6.2.2.2.11 Configuring Face Detection+

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Face Detection+.

**Figure 6-25 Face Detection+**



**Step 2** Click  next to Enable, select the statistics type, and then select the text alignment.



**Click Reset to clear the statistics data.**

**Step 3** Move the statistics box to the position that you want in the image.

**Step 4** Click Apply.

The information will be displayed on the image after the Face Detection+ function is enabled.

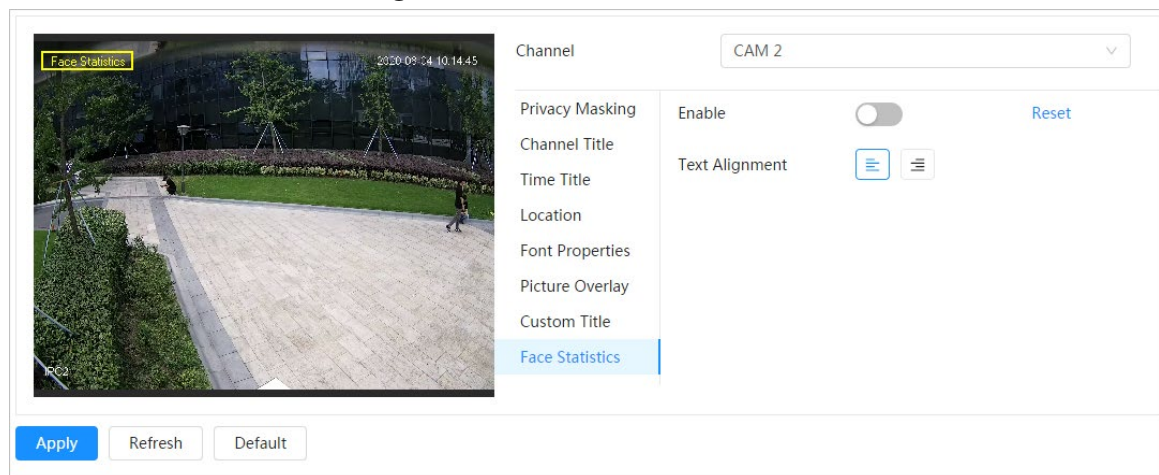
### 6.2.2.2.12 Configuring Face Statistics

After enabling this function, face statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Face Statistics.

Figure 6-26 Face statistics



**Step 2** Click  next to Enable, and select the text alignment.



**Click Reset to clear the statistics data.**

**Step 3** Move the statistics box to the position that you want in the image.

**Step 4** Click Apply.

### 6.2.2.2.13 Configure Face&Body Counting

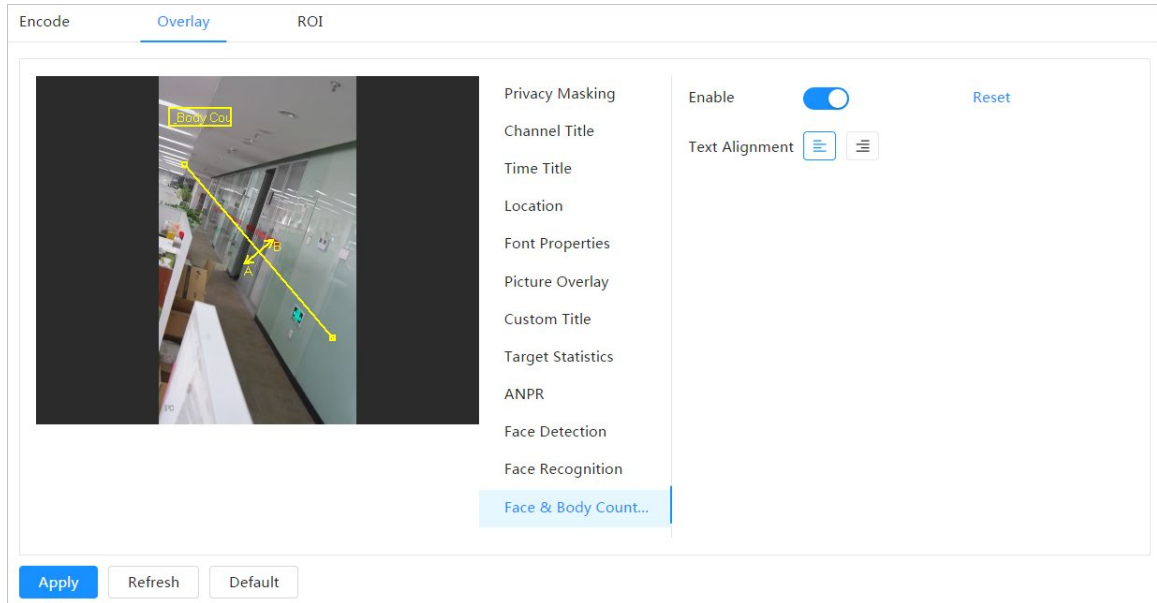
After enabling this function, face&body counting information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select > Camera > Encode > Overlay > Face&Body Counting.



**Figure 6-27 Face&body counting**



**Step 2** Select the Enable check box, and then select text alignment.



Click Reset to clear the statistics data.

**Step 3** Move the face&body counting box to the position that you want in the image.

**Step 4** Click Apply.

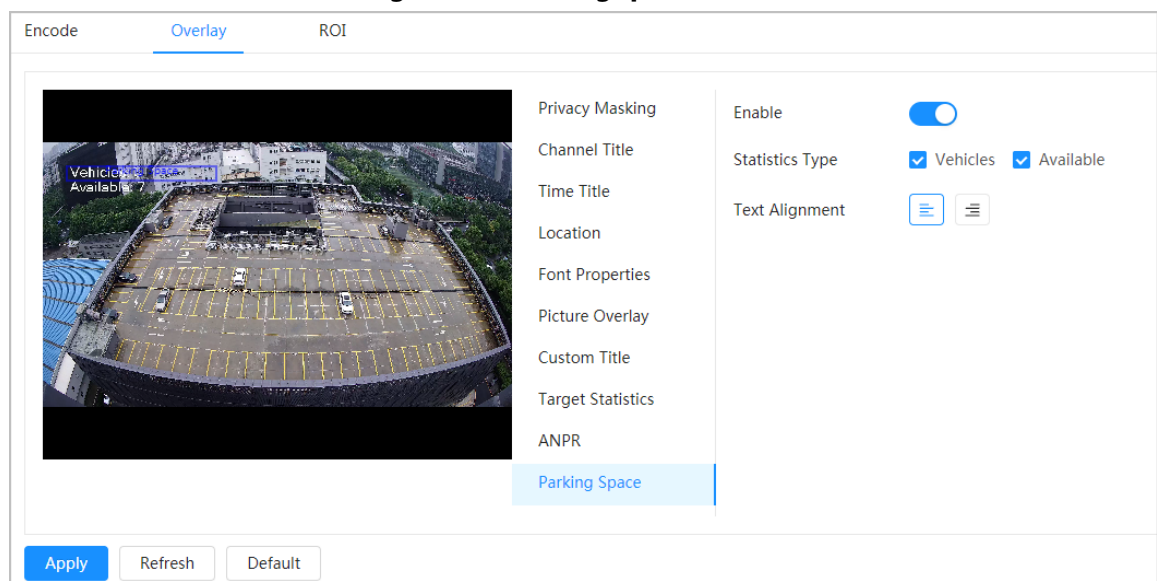
#### 6.2.2.2.14 Configuring Parking Space

After enabling this function, parking space information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

**Step 1** Select  > Camera > Encode > Overlay > Parking Space.

**Figure 6-28 Parking space**



- Step 2** Select the Enable check box.
- Step 3** Select statistic type and text alignment.
- Step 4** Click Apply.

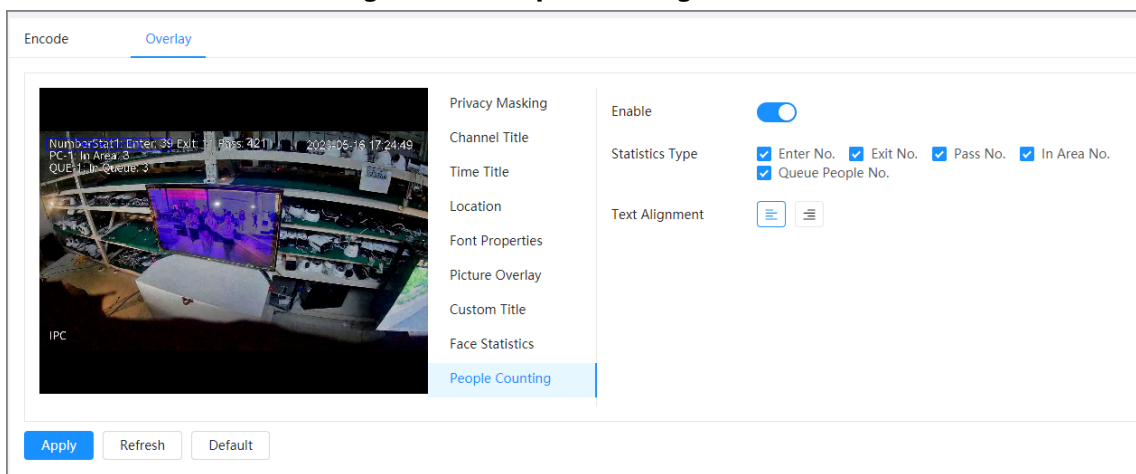
### 6.2.2.2.15 Configuring People Counting

After enabling this function, people counting information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is enabled simultaneously.

#### Procedure

- Step 1** Select  > Camera > Encode > Overlay > People Counting.

Figure 6-29 People counting



- Step 2** Click  next to Enable, select the statistics type, and then select the text alignment.
- Step 3** Move the custom box to the position that you want in the image.
- Step 4** Click Apply.

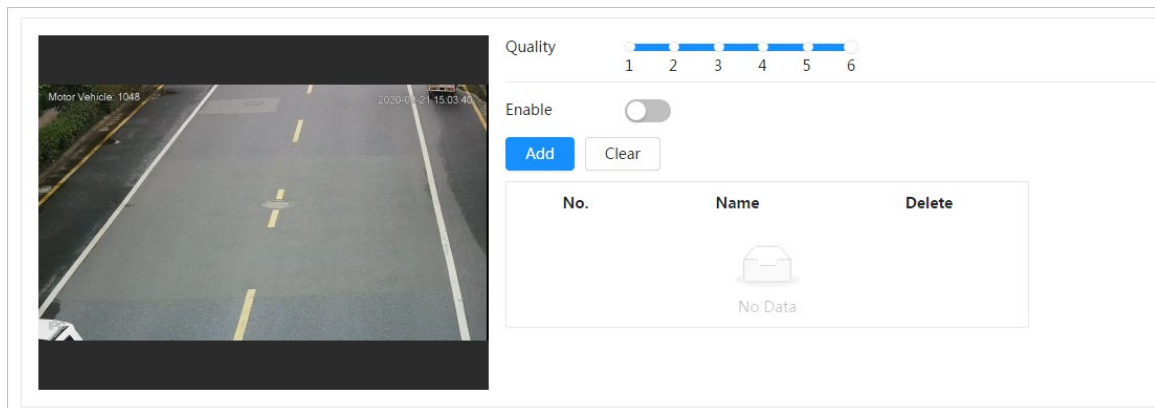
### 6.2.2.3 ROI

Select ROI (region of interest) on the image and configure the image quality of ROI, and then the selected image is display at defined quality.

#### Procedure

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

Figure 6-30 ROI



**Step 2** Click  next to Enable, draw an area on the image, and then configure the image quality of ROI.



- The higher the image quality value is, the better the quality will be.
- Click Clear to delete all the area boxes; select one box, and then click to delete it.

**Step 3** Click Apply.

**Step 4** Click Add to add more ROI. You can draw 4 area boxes at most.

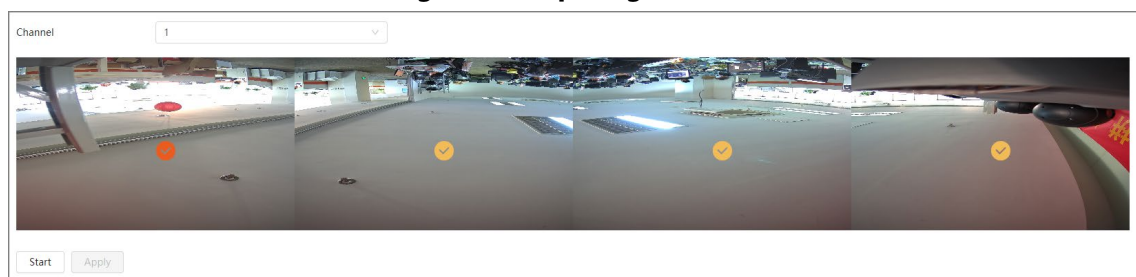
## 6.2.3 Splicing

When the panorama contains multiple images captured by different lenses, enable this function. Before splicing, make sure that the surveillance scene is large and there are no objects blocking the camera from taking a clear picture, otherwise, the splicing might fail.

### Procedure

**Step 1** Select > Camera > Splicing.

Figure 6-31 Splicing



**Step 2** Select the lenses that need to be spliced.

When splicing the image through selecting lenses, you need to select the continuous splicing screens. The screen with the icon (deeper color) is the first screen of the splicing. You can select any screen as the first one, and then select the following screens continuously. The system supports the splicing of 2 lenses to 8 lenses.



- This function is available on select models. And it is all sensors splicing by default.

- For Multi-Sensor Panoramic + PTZ Camera, the 4-sensor device supports 2 to 4 lenses splicing; the 6-sensor device supports 2 to 6 lenses splicing; the 8-sensor device supports 2-8 lenses splicing.

**Step 3** Click Start.

The system starts to splice the image.

- Some cameras restart automatically after splicing is complete, you can view the results of the splicing in the Live window.
- Some cameras display splicing live window after splicing is complete. Click OK, and then the default window appears. Click OK and the splicing will take effect.

## 6.2.4 Audio

You can configure audio parameters and alarm audio.

### 6.2.4.1 Setting Audio Parameters

This section introduces audio parameters, including encode mode, sampling frequency, audio in type, and noise filter.

#### Procedure

**Step 1** Select > Camera > Audio.

Figure 6-32 Audio

**Step 2** Click  next to Enable in Main Stream or Sub Stream.

For the camera with multiple channels, select the channel number.



Please carefully activate the audio acquisition function according to the actual requirements of the application scenario.

**Step 3** Configure audio parameters.

Table 6-11 Description of audio parameters

Parameter	Description
Compression	You can select audio Encode Mode from PCM, G.711A, G.711Mu, G.726, AAC, G.723. The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accuracy the restored signal will be. You can select audio Sampling Frequency from 8000, 16000, 32000, 48000, 64000.
Audio Input Type	You can select audio input type from: <ul style="list-style-type: none"> <li>• LineIn: Requires external audio device.</li> <li>• Mic: Not require external audio device.</li> </ul>
Noise Filter	Enable this function, and the system auto filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

**Step 4** Click Apply.

### 6.2.4.2 Setting Alarm Tone

You can record or upload alarm audio file. The audio file will be played when the alarm is triggered.

#### Procedure

**Step 1** Select > Camera > Audio Tone.

Figure 6-33 Audio tone

**Step 2** Click Add.

**Step 3** Configure the audio file.

- Select Record, enter the audio name in the input box, and then click Record.
- Select Upload, click Browse to select the audio file to be uploaded, and then click Upload.



- The camera supports recording audio file in .pcm format only. Recording is only supported by select models.
- You can upload audio files in .pcm, .wav2, .mp3, or .aac format.

Figure 6-34 Add alarm tone

**Step 4** Select the file that you need.

## Related Operations

- **Edit audio file**  
Click to edit the file name.
- **Delete audio file**  
Click to delete the file name.
- **Play audio file**  
Click to play the file name.
- **Download audio file**  
Click to download the file name.

## 6.3 Network

This section introduces network configuration.

### 6.3.1 TCP/IP

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

#### Prerequisites

The camera has connected to the network.

#### Procedure

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


Figure 6-35 TCP/IP

The screenshot shows a configuration panel for TCP/IP settings. The 'Host Name' field contains 'IPC'. The 'ARP/Ping' toggle is turned on. The 'NIC' dropdown is set to 'Wired(Default)'. The 'Mode' section has 'Static' selected with a radio button. The 'MAC Address' field is empty. The 'IP Version' dropdown is set to 'IPv4'. The 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS' fields are all empty. At the bottom, there are three buttons: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.


**Step 2** Configure TCP/IP parameters.

Table 6-12 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter the host name, and the maximum length is 15 characters.

Parameter	Description
<p><b>ARP/Ping</b></p>	<p>Click  to enable ARP/Ping to set IP address service. Get the camera MAC address, and then you can change and configure the device IP address with ARP/ping command.</p> <p>This is enabled by default. During restart, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configured with ping packet.</p> <p><b>A demonstration of configuring IP address with ARP/Ping.</b></p> <ol style="list-style-type: none"> <li>1. Keep the camera that needs to be configured and the PC within the same local network, and then get a usable IP address.</li> <li>2. Get the MAC address of the camera from device label.</li> <li>3. Open command editor on the PC and enter the following command.</li> </ol> <div data-bbox="675 884 1350 1449" style="border: 1px solid black; padding: 5px;"> <pre>Windows syntax^v arp -s &lt;IP Address&gt; &lt;MAC&gt; ^v ping -l 480 -t &lt;IP Address&gt; ^v  Windows example^v arp -s 192.168.0.125 11-40-8c-18-10-11^v ping -l 480 -t 192.168.0.125^v  UNIX/Linux/Mac syntax^v arp -s &lt;IP Address&gt; &lt;MAC&gt; ^v ping -s 480 &lt;IP Address&gt; ^v  UNIX/Linux/Mac example^v arp -s 192.168.0.125 11-40-8c-18-10-11^v ping -s 480 192.168.0.125^v</pre> </div> <ol style="list-style-type: none"> <li>4. Restart the camera.</li> <li>5. Check the PC command line, if information such as Reply from 192.168.0.125...is displayed, the configuration succeeds, and you can turn it off then.</li> <li>6. Enter http://(IP address) in the browser address bar to log in.</li> </ol>
<p><b>NIC</b></p>	<p>Select the Ethernet card that need to be configured, and the default one is Wire.</p>
<p><b>Mode</b></p>	<p>The mode that the camera gets IP:</p> <ul style="list-style-type: none"> <li>• <b>Static:</b> Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Save, the login page with the configured IP address is displayed.</li> <li>• <b>DHCP:</b> When there is DHCP server in the network, select DHCP, and the camera acquires IP address automatically.</li> </ul>
<p><b>MAC Address</b></p>	<p>Displays host MAC address.</p>



Parameter	Description
IP Version	Select IPv4 or IPv6.
IP Address	When you select Static in Mode, enter the IP address and subnet mask that you need.
Subnet Mask	
Default Gateway	 <ul style="list-style-type: none"> <li>IPv6 does not have subnet mask.</li> <li>The default gateway must be on the same network segment with the IP address.</li> </ul>
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

**Step 3** Click Apply.

### 6.3.2 Port

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

#### Procedure

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

Figure 6-36 Port

The screenshot shows a configuration page for network ports. It contains the following fields and values:

- Max Connection: 10 (range 1-20)
- TCP Port: 37777 (range 1025-65534)
- UDP Port: 37778 (range 1025-65534)
- HTTP Port: 80
- RTSP Port: 554
- RTMP Port: 1935 (range 1025-65534)
- HTTPS Port: 443

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

**Step 2** Configure port parameters.



- 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 are occupied for specific uses.
- Do not use the same value of any other port during port configuration.

Table 6-13 Description of port parameters

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	<ul style="list-style-type: none"> <li>Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available.</li> <li>When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed.</li> <li>When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF.</li> </ul> <p>URL format example:  <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&amp;subtype=0</code></p> <p>Among that:</p> <ul style="list-style-type: none"> <li>Username: The username, such as admin.</li> <li>Password: The password, such as admin.</li> <li>IP: The device IP, such as 192.168.1.112.</li> <li>Port: Leave it if the value is 554 by default.</li> <li>Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2.</li> <li>Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1).</li> </ul> <p>Example: If you require the sub stream of channel 2 from a certain device, then the URL should be:  <code>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&amp;subtype=1</code></p> <p>If username and password are not needed, then the URL can be:  <code>rtsp://ip:port/cam/realmonitor?channel=1&amp;subtype=0</code></p>
RTMP Port	Real Time Messaging Protocol. The port that RTMP provides service. It is 1935 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

**Step 3** Click Apply.



The configuration of Max Connection takes effect immediately, and others will take

effect after reboot.

### 6.3.3 PPPoE

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

#### Prerequisites

- The camera has connected to the network.
- You have gotten the account and password from Internet Service Provider.

#### Procedure

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

Figure 6-37 PPPoE

**Step 2** Click , and then enter username and password.



- **Disable UPnP while using PPPoE to avoid possible influence.**
- **After making PPPoE connection, the device IP address cannot be modified through web page.**

**Step 3** Click Apply.

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

### 6.3.4 DDNS

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

#### Prerequisites

Check the type of DNS server supported by the camera.

#### Procedure

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



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

Figure 6-38 DDNS

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

**Step 3** Configure DDNS parameters.

Table 6-14 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below: <ul style="list-style-type: none"> <li>• CN99 DDNS web address: <a href="http://www.3322.org">www.3322.org</a></li> <li>• NO-IP DDNS web address: <a href="http://dynupdate.no-ip.com">dynupdate.no-ip.com</a></li> <li>• Dyndns DDNS web address: <a href="http://members.dyndns.org">members.dyndns.org</a></li> </ul>
Server Address	
Domain Name	The domain name you registered on the DDNS website.
Test	Only when selecting NO-IP DDNS type, you can click Test to check whether the domain name registration is successful.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the DDNS server provider's website.
Password	
Interval	The update cycle of the connection between the device and the server, and the time is 10 minutes by default.

**Step 4** Click Apply.

## Result

Open the browser on PC, then enter domain name at the address bar and press Enter, the login page is displayed.

### 6.3.5 Email

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

#### Procedure

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

Figure 6-39 Email

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

**Step 3** Configure email parameters.

Table 6-15 Description of email parameters

Parameter	Description	
SMTP Server	SMTP server address	For details, see Table 6-16.
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymous	Click , and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select from None, SSL and TLS. For details, see Table 6-16.	

Parameter	Description
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click + to select title type, including Device Name, Device ID, and Event Type, and you can set maximum 2 titles.
Attachment	Select the check box to support attachment in the email.
Receiver	<ul style="list-style-type: none"> <li>Receiver's email address. Supports 3 addresses at most.</li> <li>After entering the receiver's email address, the Test button is display. Click Test to test whether the emails can be sent and received successfully.</li> </ul>
Health Mail	The system sends test mail to check if the connection is successfully configured. Click <input type="checkbox"/> and configure the Sending Interval, and then the system sends test mail as the set interval.

Table 6-16 Description of major mailbox configuration


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

**Step 4** Click Apply.

## 6.3.6 UPnP

UPnP (Universal Plug and Play) is a protocol that establishes mapping relation between local area and wide area networks. This function enables you to access local area device through wide area IP address.

### Prerequisites

- Make sure the UPnP service is installed in the system.
- Log in the router, and configure WAN IP address to set up internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.
- Select  > Network > TCP/IP, in IP Address, enter the local area IP address of the router or select DHCP and acquires IP address automatically.

### Procedure

**Step 1** Select  > Network > UPnP.

Figure 6-40 UPnP

Enable

Enable Device Di...

---

Router Status Mapping Failed

Mode

No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify
1	HTTP	WebService:TCP	80	8080	Mapping Failed	<input checked="" type="checkbox"/>	<a href="#">✎</a>
2	TCP	PrivService:TCP	37777	37777	Mapping Failed	<input checked="" type="checkbox"/>	<a href="#">✎</a>
3	UDP	PrivService:UDP	37778	37778	Mapping Failed	<input checked="" type="checkbox"/>	<a href="#">✎</a>
4	RTSP	RTSPService:TCP	554	554	Mapping Failed	<input checked="" type="checkbox"/>	<a href="#">✎</a>
5	HTTPS	HTTPSService:TCP	443	44333	Mapping Failed	<input checked="" type="checkbox"/>	<a href="#">✎</a>

**Step 2** Click  next to Enable, and there are two mapping modes: Custom and Default.

- Select Custom, click [✎](#) and then you can change external port as needed.
- Select Default, and then the system finishes mapping with unoccupied port automatically, and you cannot edit mapping relation.

**Step 3** Click Apply.

Open web browser on PC, enter `http:// wide area IP address: external port number`, and then you can visit the local area device with corresponding port.

## 6.3.7 SNMP

SNMP (Simple Network Management Protocol), which can be used to enable software such as MIB Builder and MG-SOFT MIB Browser to connect to the camera and manage and monitor the camera.

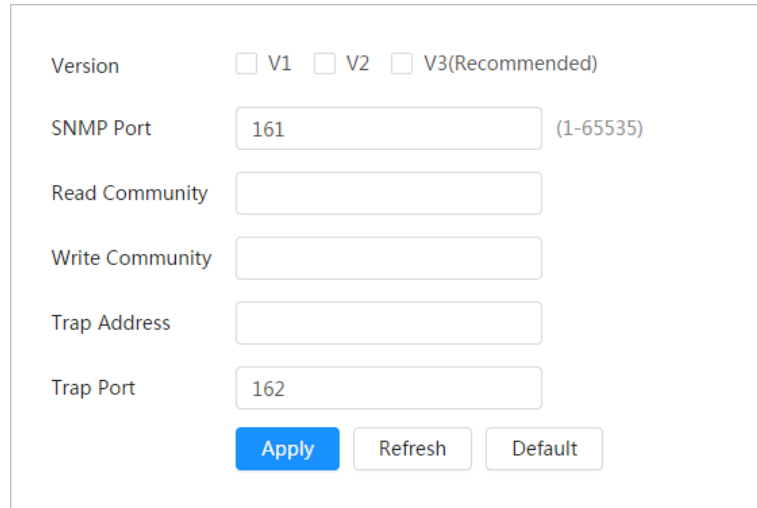
### Prerequisites

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

### Procedure

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

**Figure 6-41 SNMP (1)**



Version  V1  V2  V3(Recommended)

SNMP Port  (1-65535)

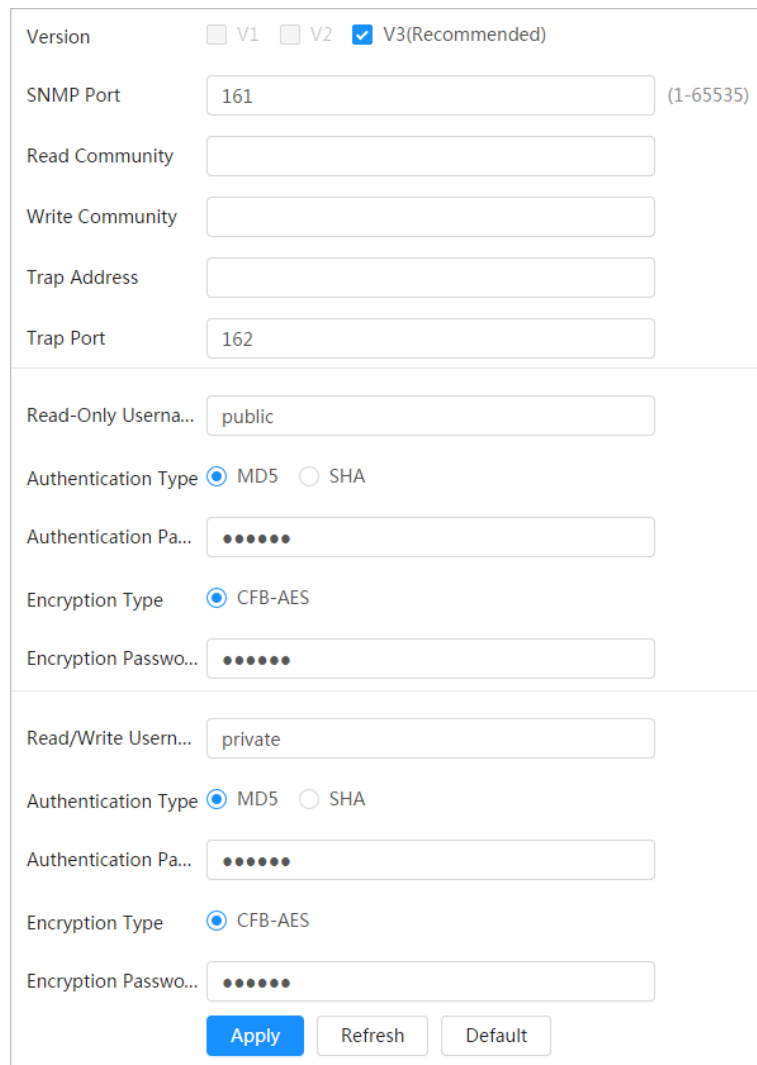
Read Community

Write Community

Trap Address

Trap Port

**Figure 6-42 SNMP (2)**



Version  V1  V2  V3(Recommended)

SNMP Port  (1-65535)

Read Community

Write Community

Trap Address

Trap Port

---

Read-Only Userna...

Authentication Type  MD5  SHA

Authentication Pa...

Encryption Type  CFB-AES

Encryption Passwo...

---

Read/Write Userm...

Authentication Type  MD5  SHA

Authentication Pa...

Encryption Type  CFB-AES

Encryption Passwo...

**Step 2** Select SNMP version to enable SNMP.

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






password and authentication type to visit your device from the server.



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

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

Table 6-17 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports.  You can enter number, letter, underline and dash to form the name.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.
Read-only Username	Set the read-only username accessing device, and it is public by default.  You can enter number, letter, and underline to form the name.
Read/Write Username	Set the read/write username access device, and it is private by default.  You can enter number, letter, and underline to form the name.
Authentication Type	You can select from MD5 and SHA. The default type is MD5.
Authentication Password	It should be no less than 8 digits.
Encryption Type	The default is CBC-DES.
Encryption Password	It should be no less than 8 digits.

**Step 4** Click Apply.

## Result

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

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

configuration information, video channel amount, audio channel amount, and software version.



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

### 6.3.8 Bonjour

Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser.

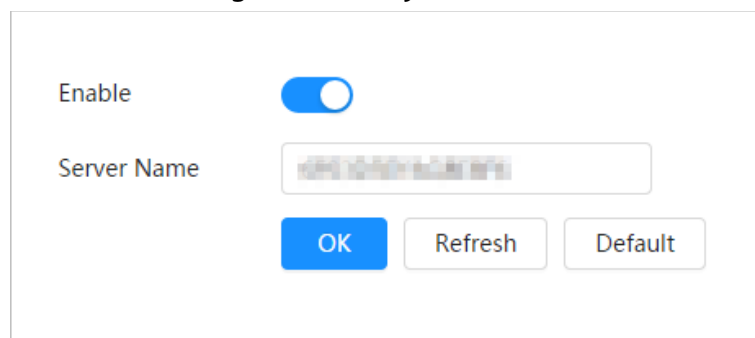


Bonjour is enabled by default.

#### Procedure

**Step 1** Select > Network > Bonjour.

Figure 6-43 Bonjour



**Step 2** Click , and then configure server name.

**Step 3** Click Apply.

#### Result

In the OS and clients that support Bonjour, follow the steps below to visit the network camera with Safari browser.

1. Click Show All Bookmarks in Safari.
2. Enable Bonjour. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click the camera to visit the corresponding web page.

### 6.3.9 Multicast

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

#### Procedure

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

Figure 6-44 Multicast

**Step 2** Click , and enter IP address and port number.

Table 6-18 Description of multicast parameters

Parameter	Description
Multicast Address	The multicast IP address of Main Stream/Sub Stream is 224.1.2.4 by default, and the range is 224.0.0.0–239.255.255.255.
Port	The multicast port of corresponding stream: Main Stream: 40000; Sub Stream 1: 40016; Sub Stream2: 40032, and all the range is 1025–65500.

**Step 3** Click Apply.

## Result

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

## 6.3.10 Register

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

### Procedure

**Step 1** Select > Network > Register.

Figure 6-45 Register

**Step 2** Click , and then configure server name.

Table 6-19 Description of register parameters

Parameter	Description
Server 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.

## 6.3.11 QoS

You can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience.

0–63 means 64 degrees of priority; 0 for the lowest and 63 the highest.

### Procedure

**Step 1** Select > Network > QoS.

Figure 6-46 QoS

**Step 2** Configure QoS parameters.

Table 6-20 Description of QoS parameters

Parameter	Description
Realtime Monitor	Configure the priority of the data packets that used for network surveillance. 0 for the lowest and 63 the highest.
Command	Configure the priority of the data packets that used for configure or checking.

**Step 3** Click Save.

## 6.3.12 Platform Access

### 6.3.12.1 P2P

P2P (peer-to-peer) technology enables users to manage devices easily without requiring DDNS, port mapping or transit server.

### Background Information

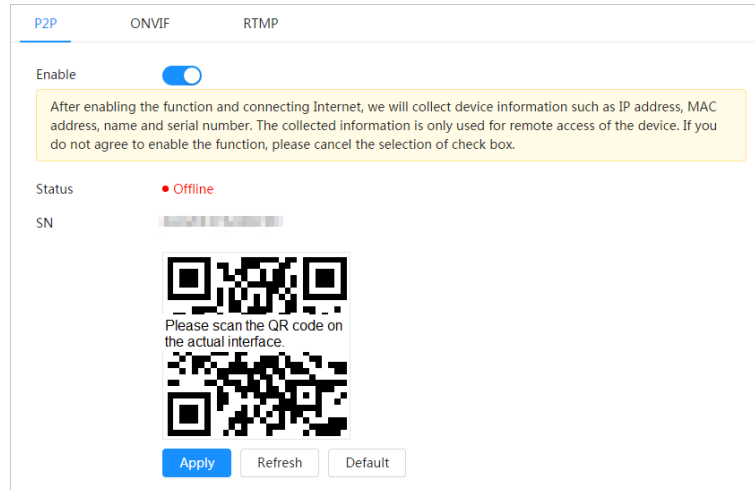
Scan the QR code with your smartphone, and then you can add and manage more devices on

the mobile phone client.

## Procedure

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

Figure 6-47 P2P



- When P2P is enabled, remote management on device is supported.
- When P2P is enabled and the device accesses to the network, the status shows online. The information of the IP address, MAC address, device name, and device SN will be collected. The collected information is for remote access only. You can cancel Enable selection to reject the collection.

**Step 2** Log in to mobile phone client and tap Device management.

**Step 3** Tap + at the upper-right corner.

**Step 4** Scan the QR code on the P2P page.

**Step 5** Follow the instructions to finish the settings.

### 6.3.12.2 ONVIF

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

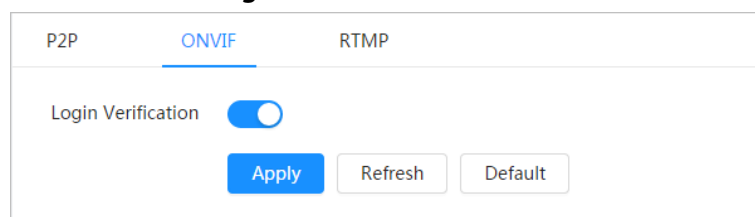


**ONVIF is enabled by default.**

## Procedure

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

Figure 6-48 ONVIF



**Step 2** Click next to ONVIF Verification.

**Step 3** Click Apply.

### 6.3.12.3 RTMP

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



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

#### Procedure

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

Figure 6-49 RTMP

**Step 2** Click .



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

**Step 3** Configure RTMP parameters.

Table 6-21 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	<ul style="list-style-type: none"> <li>• Non-custom: Enter the server IP and domain name.</li> <li>• Custom: Enter the path allocated by the server.</li> </ul>
IP Address	When selecting Non-custom, you need to enter server IP address and port. <ul style="list-style-type: none"> <li>• IP address: Support IPv4 or domain name.</li> <li>• Port: Keep the default value.</li> </ul>
Port	

Parameter	Description
Custom Address	When selecting Custom, you need to enter the path allocated by the server.

**Step 4** Click Apply.

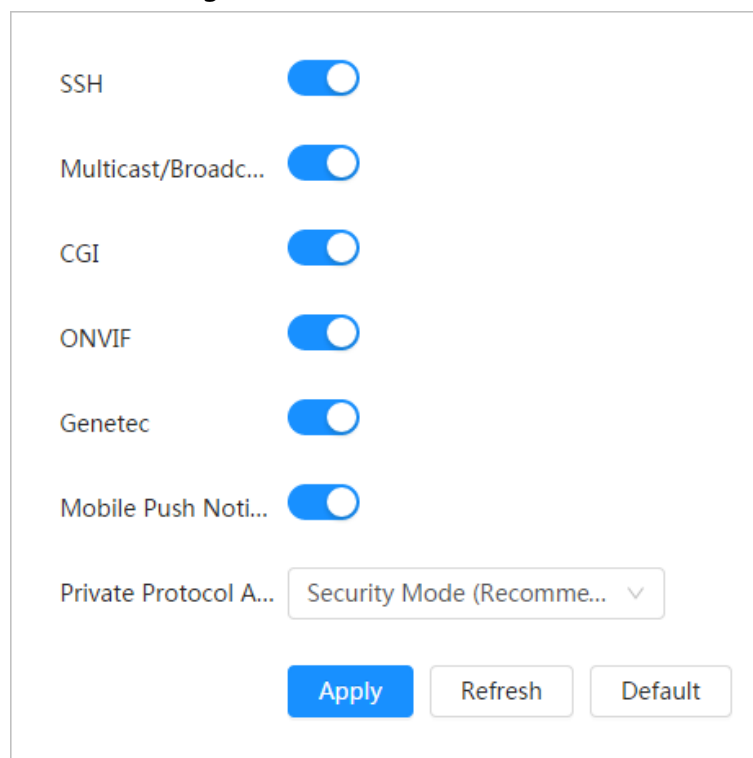
### 6.3.13 Basic Service

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

#### Procedure

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

Figure 6-50 Basic service



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

Table 6-22 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	Enable the function, and then other devices can access through this service. The function is enabled by default.
Onvif	

Function	Description
Genetec	
Mobile Push Notification	Enable this function, and then the system will send the snapshot that was taken when alarm is triggered to your phone, this is enabled by default.
Private Protocol Authentication Mode	Select the authentication mode from Security Mode and Compatible Mode. Security mode is recommended.

**Step 3** Click Apply.

## 6.4 EPTZ

EPTZ function can simultaneously zoom in and track multiple humans and vehicles that trigger alarms. It provides rich details and a panoramic view at the same time.

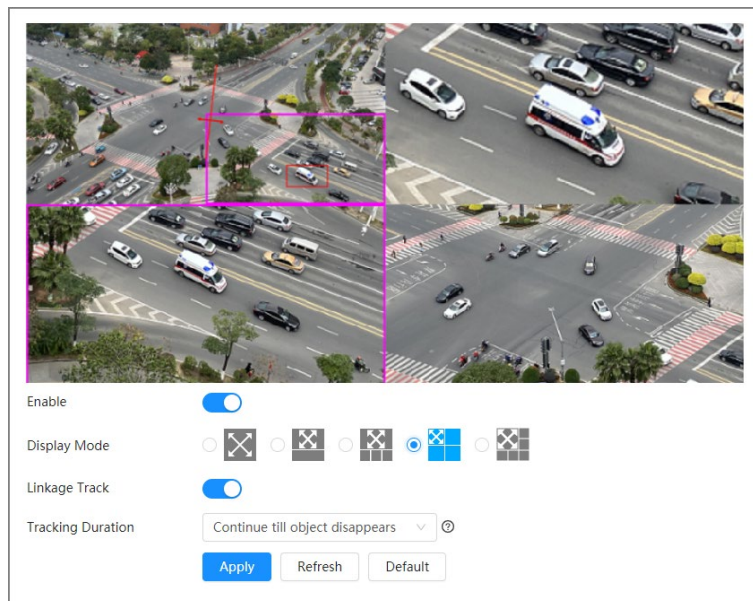


**This function is only available on select devices.**

### Procedure

**Step 1** Select > PTZ > EPTZ Linkage.

Figure 6-51 EPTZ







**Step 2** Enable this function and select the display mode.

Table 6-23 Description of display modes

Mode	Description
	Displays the original screen.
	Displays the original image screen + 1 sub-screen.



Mode	Description	
	Displays the original image screen + 3 sub-screens.	 You can zoom or drag the sub-screen images in the original screen.
		
	Displays the original image screen + 5 sub-screens.	

**Step 3** (Optional) Enable the Linkage Track checkbox and select tracking duration mode from the dropdown list.

- **Custom:** Select the tracking duration time manually. For example, if you set from 30 s to 60 s, after tracking object A for 30 seconds, if object B appears, the camera will start tracking object B; if no other object appears in the process of tracking A, the camera will stop tracking object A after 60 seconds.
- **Continue till object disappears:** The camera will stop tracking when the detected object disappears in the image.

**Step 4** Click Apply.

## 6.5 Event

### 6.5.1 Setting Alarm Linkage

#### 6.5.1.1 Setting Alarm-in

When an alarm is triggered by the device connected to the alarm-in port, the system performs the defined alarm linkage.

#### Procedure

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

**Step 2** Click  next to Enable to enable alarm linkage.

Figure 6-52 Alarm linkage

**Step 3** Select an alarm-in port and a sensor type.

- **Sensor Type:** NO or NC.
- **Anti-Dither:** Only record one alarm event during the anti-dither period.

**Step 4** Select the schedule and arming periods and alarm linkage action. If the schedules cannot meet the scene requirement, you can click Add Schedule to add new schedule. For details, see "6.5.1.2.1 Adding Schedule".

**Step 5** Click Apply.

### 6.5.1.2 Alarm Linkage

When configuring alarm events, select alarm linkages (such as record, snapshot). When the corresponding alarm is triggered in the configured arming period, the system will alarm.

Select > Event > Alarm, and then click next to Enable to enable alarm linkage.

Figure 6-53 Alarm linkage

The screenshot shows a configuration panel for alarm linkage. It contains the following elements:

- Enable:** A blue toggle switch is turned on.
- Alarm-in Port:** A dropdown menu showing "Alarm1".
- Schedule:** A dropdown menu showing "Full Time" and an "Add Schedule" button.
- Anti-Dither:** A text input field with "0" and a unit label "sec.(0-100)".
- Sensor Type:** A dropdown menu showing "NC".
- Enable Alarm:** A blue toggle switch is turned on.
- Alarm-out Port:** Two buttons labeled "1" and "2", with "1" selected.
- Post-Alarm:** A text input field with "10" and a unit label "sec.(10-300)".
- Record:** A blue toggle switch is turned on.
- Record:** Four buttons labeled "1", "2", "3", and "4", with "1" selected.
- Post-Record:** A text input field with "10" and a unit label "sec.(10-300)".
- Send Email:** A grey toggle switch is turned off.
- Snapshot:** A blue toggle switch is turned on, and four buttons labeled "1", "2", "3", and "4", with "1" selected.
- Buttons:** "Apply" (blue), "Refresh", and "Default" (grey) buttons are located at the bottom.

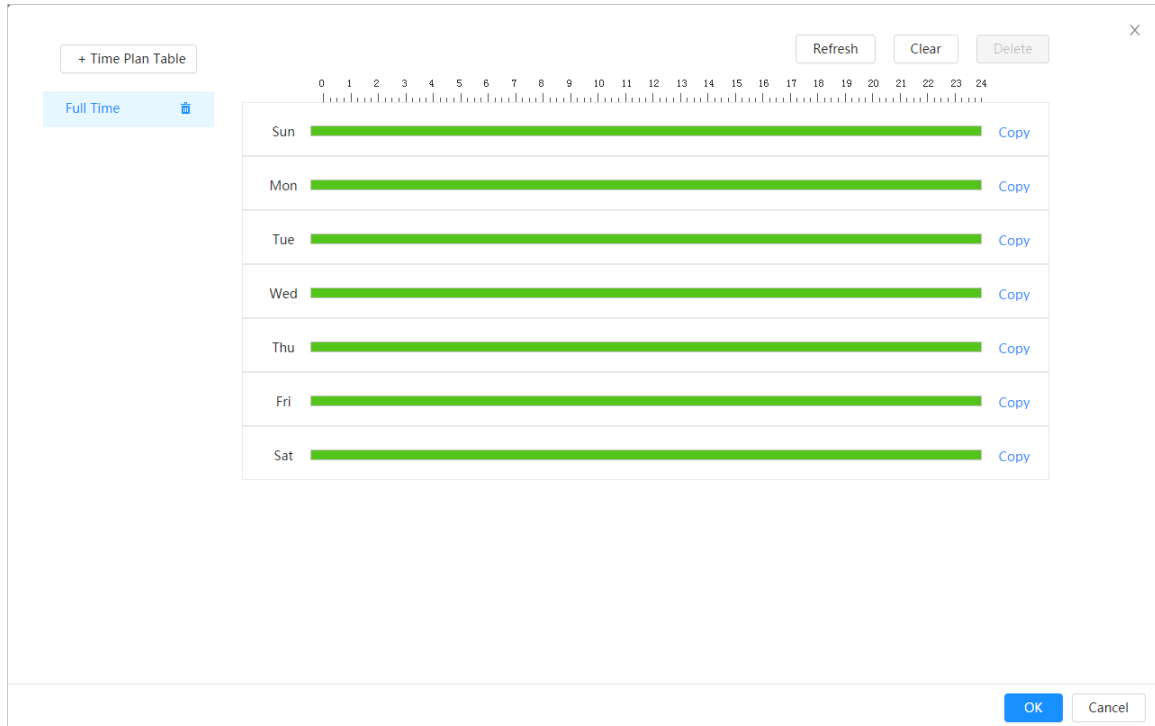
### 6.5.1.2.1 Adding Schedule

Set arming periods. The system only performs corresponding linkage action in the configured period.

#### Procedure

**Step 1** Click Add Schedule next to Schedule.

Figure 6-54 Schedule



**Step 2** Press and drag the left mouse button on the timeline to set arming periods. Alarms will be triggered in the period in green on the timeline.

- 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 check box to select all days to copy the configuration.
- You can set 6 periods per day.

**Step 3** Click Apply.

**Step 4** (Optional) Click Time Plan Table to add a new time plan table.

You can:

- Double-click the table name to edit it.
- Click  to delete the table as needed.


### 6.5.1.2.2 Record Linkage

The system can link record channel when an alarm event occurs. After alarm, the system stops recording after an extended period according to the Post-Record setting.

### Prerequisites

- After the corresponding alarm type (Normal, Motion, or Alarm) is enabled, the record channel links recording. For details, see "10.3 Setting Record Plan".
- Enable auto record mode, the record linkage will take effect. For details, see "10.2 Setting Record Control".

### Setting Record Linkage

On the Alarm page, click  to enable record linkage, select the channel as needed, and set Post-Record to set alarm linkage and record delay.

After Post-Record is configured, alarm recording continues for an extended period after the alarm ends.

Figure 6-55 Record linkage

### 6.5.1.2.3 Snapshot Linkage

After snapshot linkage is configured, the system can automatically alarm and take snapshots when an alarm is triggered.

#### Prerequisites

After the corresponding alarm type (Normal, Motion, or Alarm) is enabled, the snapshot channel links capturing picture. For details, see "10.3 Setting Record Plan".

#### Procedure

On the Alarm page, click  to enable snapshot linkage, and select the channel as needed.

Figure 6-56 Snapshot linkage

### 6.5.1.2.4 Alarm-out Linkage

When an alarm is triggered, the system can automatically link with alarm-out device.

On the Alarm page, click  to enable alarm-out linkage, select the channel as needed, and then configure Post alarm.

When alarm delay is configured, alarm continues for an extended period after the alarm ends.

Figure 6-57 Alarm-out linkage

### 6.5.1.2.5 Email Linkage

When an alarm is triggered, the system will automatically send an email to users. Email linkage takes effect only when SMTP is configured. For details, see "6.3.5 Email".

Figure 6-58 Email linkage



### 6.5.1.3 Subscribing Alarm

#### 6.5.1.3.1 Alarm Types

Table 6-24 Description of alarm types

Alarm Type	Description	Preparation
Motion Detection	The alarm is triggered when moving object is detected.	Motion detection is enabled. For details, see "6.5.3.1 Setting Motion Detection".
Disk Full	The alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For details, see "6.5.2.1 Setting SD Card Exception".
Disk Error	The alarm is triggered when there is failure or malfunction in the SD card.	SD card failure detection is enabled. For details, see "6.5.2.1 Setting SD Card Exception".
Video Tampering	The alarm is triggered when the camera lens is covered or there is defocus in video images.	Video tampering is enabled. For details, see "6.5.3.2 Setting Video Tampering".
External Alarm	The alarm is triggered when there is external alarm input.	The device has alarm input port and external alarm function is enabled. For details, see "6.5.1.1 Setting Alarm-in".
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "6.5.4 Setting Audio Detection".
IVS	The alarm is triggered when intelligent rule is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For details, see "6.5.3.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "6.5.2.3 Setting Voltage Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Security exception is enabled. For details, see "9.1 Security Status".

#### 6.5.1.3.2 Subscribing Alarm Information

You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information at the right side of the page.



Functions of different devices might vary.

## Procedure

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

Figure 6-59 Alarm (subscription)

Enable Alarm  Alarm Subs... ^

All Types

Motion D..  Disk Full  Disk Error  Video Ta...

External ...  Security ...  Audio D...  AI Config

Scene Ch..  Voltage ...

Play Alarm Tone

No.	Time	Alarm Type	Source IP Address	Alarm Channel
<p>No Data</p>				

**Step 2** Click  next to Enable Alarm.

**Step 3** Select alarm type according to the actual need. For details, see "6.5.1.3.2 Subscribing Alarm Information".

The system prompts and records alarm information according to actual conditions. When the subscribed alarm event is triggered and the alarm subscription page is not displayed, a number is displayed on , and the alarm information is recorded automatically. Click to view the details in the alarm list. You can click Clear to clear the record.

**Step 4** Click  next to Play Alarm Tone, and select the tone path.

The system will play the selected audio file when the selected alarm is triggered.

## 6.5.2 Setting Exception

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



Only the device with SD card has the abnormality functions, including No SD Card, SD Card Error, and Capacity Warning.

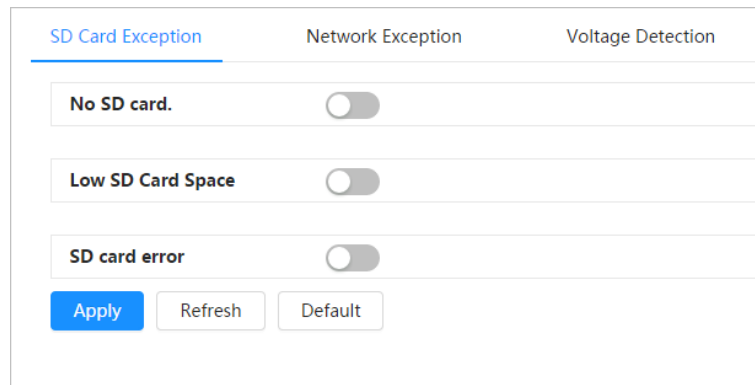
### 6.5.2.1 Setting SD Card Exception

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

#### Procedure

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

Figure 6-60 SD card exception



**Step 2** Click to enable the SD card detection functions.

When enabling Low SD Card Space, set Capacity Limit. When the remaining space of SD card is less than this value, the alarm is triggered.

**Step 3** Set alarm linkage actions. For details, see "6.5.1.2 Alarm Linkage".

**Step 4** Click Apply.

### 6.5.2.2 Setting Network Exception

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

#### Procedure

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



**Figure 6-61 Network exception**

SD Card Exception
Network Exception
Voltage Detection

**Offline**

Enable Alarm

Alarm-out Port

Post-Alarm  sec.(10-300)

Record

Record

Post-Record  sec.(10-300)

**IP Conflict**

Enable Alarm

Alarm-out Port

Post-Alarm  sec.(10-300)

Record

Record

Post-Record  sec.(10-300)

Apply
Refresh
Default

- Step 2** Click  to enable the network detection function.
- Step 3** Set alarm linkage actions. For details, see "6.5.1.2 Alarm Linkage".
- Step 4** Click Apply.

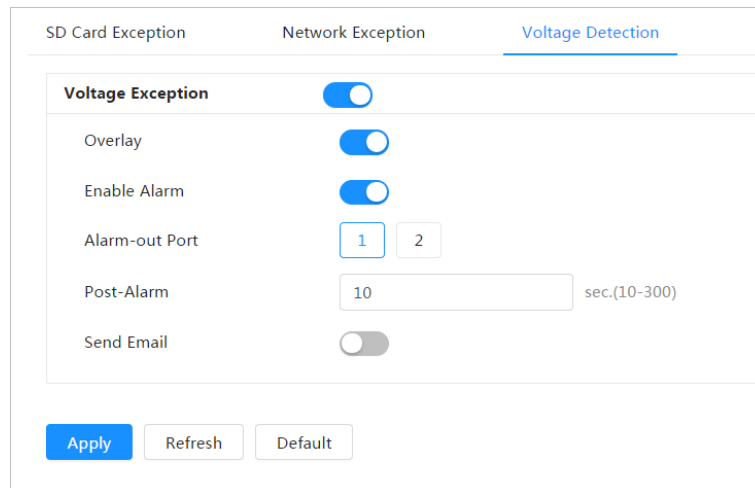
### 6.5.2.3 Setting Voltage Detection

When the input voltage is higher than or lower than the rated value of the device, the system performs alarm linkage.

#### Procedure

- Step 1** Select > Event > Exception > Voltage Detection.

**Figure 6-62 Voltage detection**



**Step 2** Click to enable the voltage detection function.

When enabling Overlay, the alarm icon is displayed by overlapping when the alarm is triggered.

**Step 3** Set alarm linkage actions. For details, see "6.5.1.2 Alarm Linkage".

**Step 4** Click Apply.

## 6.5.3 Setting Video Detection

Check whether there are considerable changes on the video by analyzing video images. In case of any considerable change on the video (such as moving object and fuzzy image), the system performs an alarm linkage.

### 6.5.3.1 Setting Motion Detection

The system performs an alarm linkage when a moving object appears in the image and its moving speed reaches the configured sensitivity.



- If you enable motion detection and smart motion detection simultaneously, and configure the linked activities, the linked activities take effect as follows:
  - ◇ When motion detection is triggered, the camera will record and take snapshots, but other configured linkages such as sending emails, PTZ operation will not take effect.
  - ◇ When smart motion detection is triggered, all the configured linkages take effect.
- If you only enable motion detection, all the configured linkages take effect when motion detection is triggered.

### Procedure

**Step 1** Select > Event > Video Detection > Motion Detection.

**Figure 6-63 Motion detection**

**Step 2** Click to enable the motion detection function.

**Step 3** Set the area for motion detection.

1) Click **Setting** next to Area.

**Figure 6-64 Area**

2) Select a color and set the region name. Select an effective area for motion detection in the image and set Sensitivity and Threshold.

- Select a color on to set different detection parameters for each region.
- **Sensitivity:** Sensitive degree of outside changes. It is easier to trigger the alarm with higher sensitivity.
- **Threshold:** Effective area threshold for motion detection. The smaller the threshold is, the easier the alarm is triggered.
- The whole video image is the effective area for motion detection by default.

- The red line in the waveform indicates that the motion detection is triggered, and the green one indicates that there is no motion detection. Adjust sensitivity and threshold according to the waveform.

3) Click OK.

**Step 4** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". If the exiting schedules cannot meet the scene requirement, you can click Add Schedule to add a new schedule. For details, see "6.5.1.2.1 Adding Schedule".  
**Anti-dither:** After the Anti-dither time is set, the system only records one motion detection event in the period.

**Step 5** Click Apply.

### 6.5.3.2 Setting Video Tampering

The system performs alarm linkage when the lens is covered or video output is mono-color screen caused by light and other reasons.

#### Procedure

**Step 1** Select > Event > Video Detection > Video Tampering.

**Step 2** Select the event type.

- **Video Tampering:** When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered.
- **Defocus Detection:** When the image is blurred, an alarm will be triggered. This function is available on select models.

Figure 6-65 Video tampering

Motion Detection	Video Tampering	Scene Changing
Event Type	Video Tampering	
Enable	<input type="checkbox"/>	
Covered Area	100	% (1-100)
Duration	1	sec. (1-300)
Anti-Dither	1	sec. (0-100)
Schedule	Full Time	<input type="button" value="Add Schedule"/>
Alarm-out Port	<input checked="" type="checkbox"/>	
Alarm Channel	<input type="text" value="1"/> <input type="text" value="2"/>	
Post-Alarm	10	sec. (10-300)
Record	<input checked="" type="checkbox"/>	
Post-Record	10	sec. (10-300)
Send Email	<input type="checkbox"/>	
Snapshot	<input checked="" type="checkbox"/>	
	<input type="button" value="Apply"/>	<input type="button" value="Refresh"/> <input type="button" value="Default"/>

Table 6-25 Description of video temper parameter

Parameter	Description
Covered Area	When the percentage of the tampered image and the duration exceed the configured values, an alarm will be triggered.
Duration	
Anti-Dither	Only record one alarm event during the anti-dither period.

**Step 3** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". If the exiting schedules cannot meet the scene requirement, you can click Add Schedule to add a new schedule. For details, see "6.5.1.2.1 Adding Schedule".

**Step 4** Click Apply.

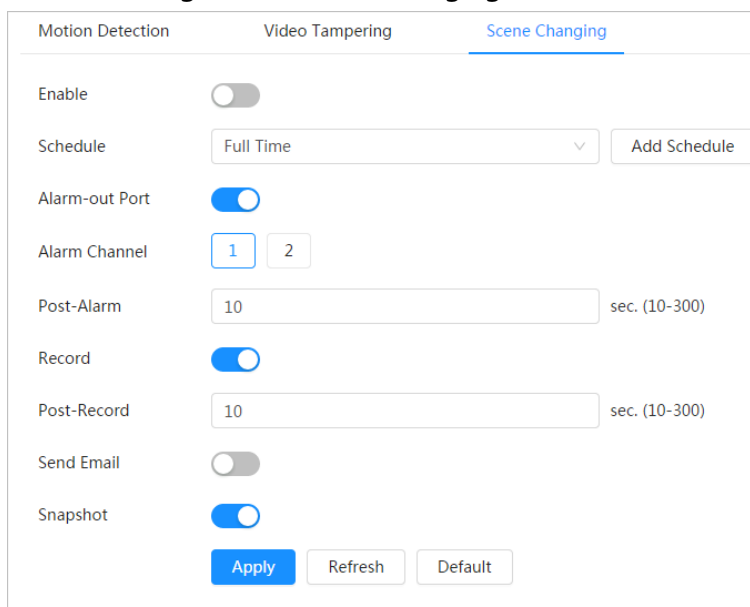
### 6.5.3.3 Setting Scene Changing

The system performs alarm linkage when the image switches from the current scene to another one.

#### Procedure

**Step 1** Select  > Event > Video Detection > Scene Changing.

Figure 6-66 Scene changing



**Step 2** Select the schedule and arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click Add Schedule to add a new schedule. For details, see "6.5.1.2.1 Adding Schedule".

**Step 3** Click Apply.

### 6.5.4 Setting Audio Detection

The system performs alarm linkage when vague voice, tone change, or rapid change of sound intensity is detected.

## Procedure

**Step 1** Select > Event > Video Detection > Audio Detection.

Figure 6-67 Audio detection

**Step 2** Set parameters.

- **Input abnormal:** Click next to **Audio Abnormal**, and the alarm is triggered when the system detects abnormal sound input.
- **Intensity change:** Click next to **Intensity Change**, and then set **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that the sound intensity exceeds the configured threshold.
  - ◇ It is easier to trigger the alarm with higher sensitivity or smaller threshold. Set a high threshold for noisy environment.
  - ◇ The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio detection. Adjust sensitivity and threshold according to the waveform.

**Step 3** Select the schedule and arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".


If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.5.1.2.1 Adding Schedule".

**Step 4** Click **Apply**.

## 6.5.5 Setting Disarming

Supports controlling disarm alarm linkage actions with one-click. After enabling Event Notification, the system only triggers the selected alarm linkage actions.

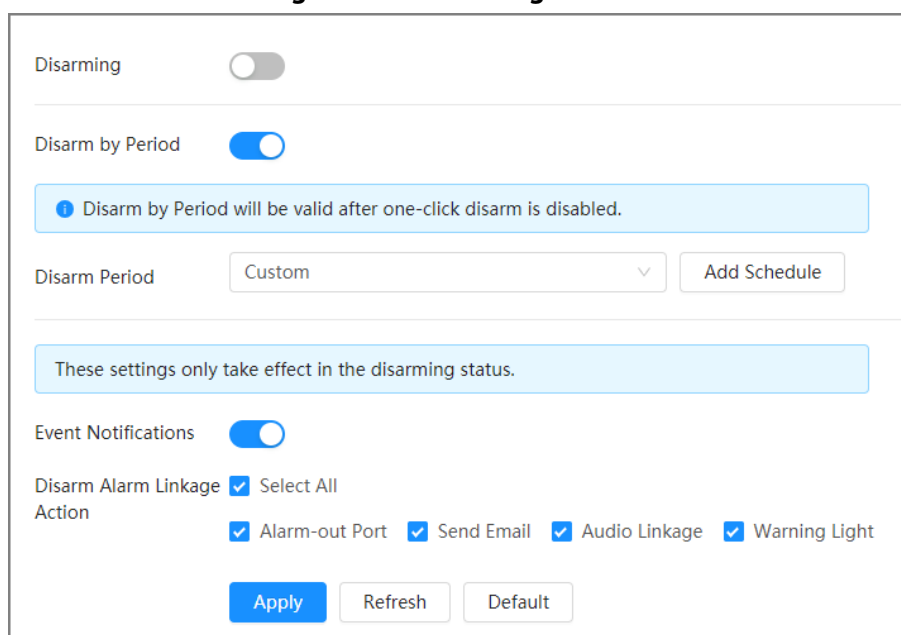
### Procedure

**Step 1** Select  > Event > Disarming.

**Step 2** Enable Disarming or Disarm by Period as needed.

- **Disarming:** The system stops triggering alarm linkage actions all the time.
- **Disarm by Period:** The system stops triggering alarm linkage actions in the selected period. For adding schedule, see "6.5.1.2.1 Adding Schedule".

Figure 6-68 Disarming



**Step 3** Enable Event Notification, and then select the Disarm Alarm Linkage Action as needed.

The system only triggers the selected alarm linkage actions.

**Step 4** Click Apply.

## 6.6 Storage

Displays the information of the local SD card. You can set it as read only or read & write; you can also hot swap and format SD card.



Functions might vary with different models.

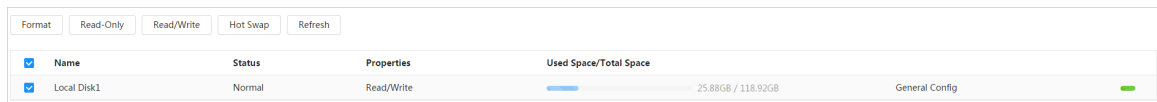
Select  > Storage.

- Click Read-Only, and then the SD card is set to read only.
- Click Read & Write, and then the SD card is set to read & write.
- Click Hot Swap, and then you can pull out the SD card.
- Click Format, and you can format the SD card.



When reading SD card on PC, if the SD card capacity is much less than the nominal capacity, you need to format the SD card. Then the data in SD card will be cleared, and the SD card is formatted to be private file system. The private file system can greatly improve SD card multimedia file read/write performance. Download Diskmanager from Toolbox to read the SD card. For details, contact after-sales technicians.

Figure 6-69 Local



## 6.7 System

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

### 6.7.1 General

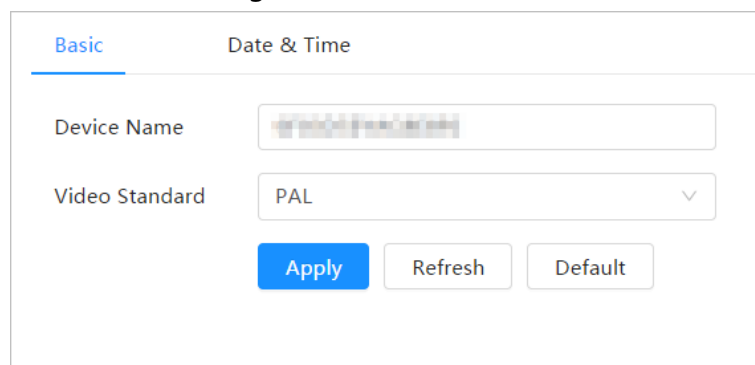
#### 6.7.1.1 Basic

You can configure device name, language and video standard.

#### Procedure

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

Figure 6-70 Basic



**Step 2** Configure general parameters.

Table 6-26 Description of general parameters

Parameter	Description
Name	Enter the device name.
Video Standard	Select video standard from PAL and NTSC.

**Step 3** Click Apply.



### 6.7.1.2 Date & Time

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

#### Procedure

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

**Figure 6-71 Date and time**

**Step 2** Configure date and time parameters.

**Table 6-27 Description of date and time parameters**

Parameter	Description
Date Format	Configure the date format.
Time	<ul style="list-style-type: none"> <li>Manually Setting: Configure the parameters manually.</li> <li>NTP: When selecting NTP, the system then syncs time with the internet server in real time.</li> </ul> <p>You can also enter the IP address, time zone, port, and interval of a PC which installed NTP server to use NTP.</p>
Time Format	Configure the time format. You can select from 12-Hour or 24-Hour.
Time Zone	Configure the time zone that the camera is at.
Current Time	<p>Configure system time.</p> <p>Click Sync PC, and the system time changes to the PC time.</p>

Parameter	Description
DST	Enable DST as needed. Click <input type="checkbox"/> , and configure start time and end time of DST with Date or Week.

**Step 3** Click Apply.

## 6.7.2 Power Consumption Mode

Configure sleep mode, general mode or power saving mode as needed. When the device battery drops to 20%, 15%, or 10%, it automatically reports the low battery event to the platform.

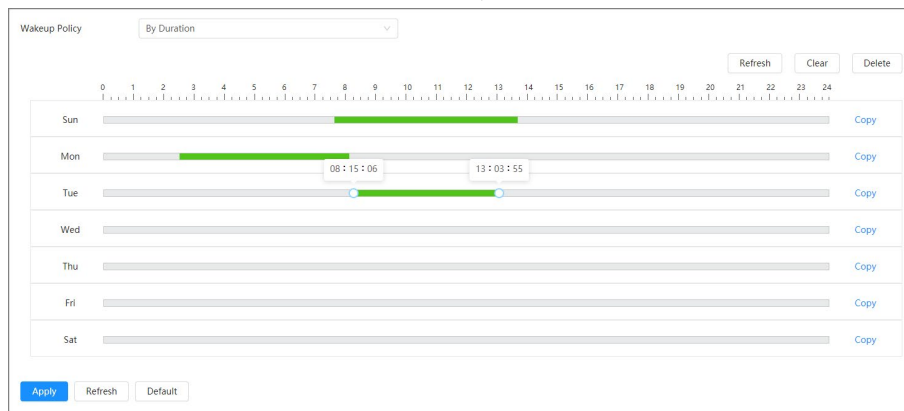
### 6.7.2.1 Setting Sleeping Mode

The device will only work when it is woken up.

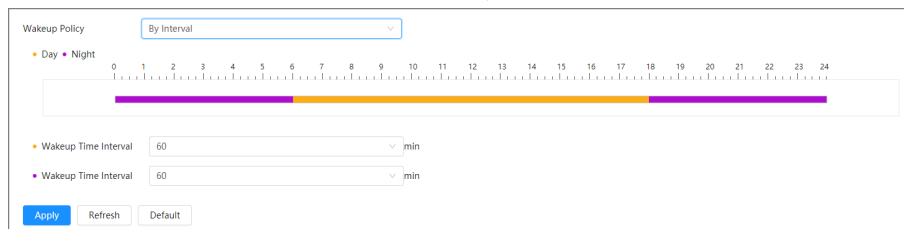
#### Procedure

- Step 1** Select System > Power Consumption Mode > Sleep Mode.
- Step 2** Turn on Scheduled Wakeup.
- Step 3** Select Wakeup Policy.

**Figure 6-72 Wakeup by duration**



**Figure 6-73 Wakeup by interval**



**Step 4** Click Apply.

### 6.7.2.2 Setting General Mode

The device is in normal power consumption state when it is in general mode. Set the power threshold, and then the device will enter to sleep mode if the power is lower than the

threshold configured.

## Procedure

- Step 1** Select System > Power Consumption Mode > General Mode.
- Step 2** Turn on Sleep, and then configure the threshold.
- Step 3** Click Apply.

### 6.7.2.3 Setting Power Saving Mode

When this function is enabled, the device will lower the resolution and frame rate to minimize the power consumption. This mode is enabled by default.

## Procedure

- Step 1** Select System > Power Consumption Mode > Power Saving Mode.
- Step 2** Click Apply.

## 6.7.3 Account

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

Managing users and groups are only available for administrator users.

- The max length of the user or group name is 31 characters which consists of number, letter, underline, dash, dot and @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
- You can have 18 users and 8 groups at most.
- You can manage users through single user or group, and duplicate usernames or group names are not allowed. A user can only be in one group at a time, and the group users can own authorities within group authority range.
- Online users cannot edit their own authority.
- There is one admin by default which has highest authority.
- Select Anonymous Login, and then log in with only IP address instead of username and password. Anonymous users only have preview authorities. During anonymous login, click Logout, and then you can log in with other username.

### 6.7.3.1 User

#### 6.7.3.1.1 Adding User

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

## Procedure

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

**Figure 6-74 User**

The screenshot shows a web interface for user management. At the top, there are tabs for 'User' and 'Group', and a sub-tab 'ONVIF User'. Below the tabs are 'Add' and 'Delete' buttons. On the right, there is an 'Anonymous Login' toggle switch. The main area contains a table with the following data:

No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin 's account	/	

Below the table is a 'Password Reset' section with an 'Enable' toggle switch (turned on). A blue box contains the text: 'If you forgot the password, you can receive security codes through the email address left in advance to reset the password.' There is a 'Reserved Email' input field. At the bottom are 'Apply', 'Refresh', and 'Default' buttons.

**Step 2** Click Add.

**Figure 6-75 Add user (system)**

The screenshot shows a dialog box titled 'Add' with a close button (X). It contains the following fields:

- Username:
- Password:
- Confirm Password:
- Group:  (dropdown menu)
- Remarks:

Below the fields are four tabs: 'System' (selected), 'Live', 'Search', and 'Restricted Login'. Under the 'System' tab, there is a list of permissions, each with a checked checkbox:


- All
- Account
- Manual Control
- Event
- Camera
- Maintenance
- System
- File Backup
- Network
- PTZ
- System Info
- Storage
- Peripheral
- Security

At the bottom right are 'OK' and 'Cancel' buttons.

Figure 6-76 Add user (restricted login)

**Step 3** Configure user parameters.

Table 6-28 Description of user parameters

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

Parameter	Description
Restricted Login	<p>Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to the web page with the defined IP in the defined time range of validity period.</p> <ul style="list-style-type: none"> <li>• IP address: You can log in to web through the PC with the set IP.</li> <li>• Validity period: You can log in to web in the set validity period.</li> <li>• Time range: You can log in to web in the set time range.</li> </ul> <p>Set as follows</p> <ol style="list-style-type: none"> <li>1. IP address: Enter the IP address of the host to be added.</li> <li>2. IP segment: Enter the start address and end address of the host to be added.</li> </ol>

**Step 4** Click Apply.

The newly added user is displayed in the username list.

## Related Operations

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



**For admin account, you can only edit the password.**

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



**The admin account cannot be deleted.**

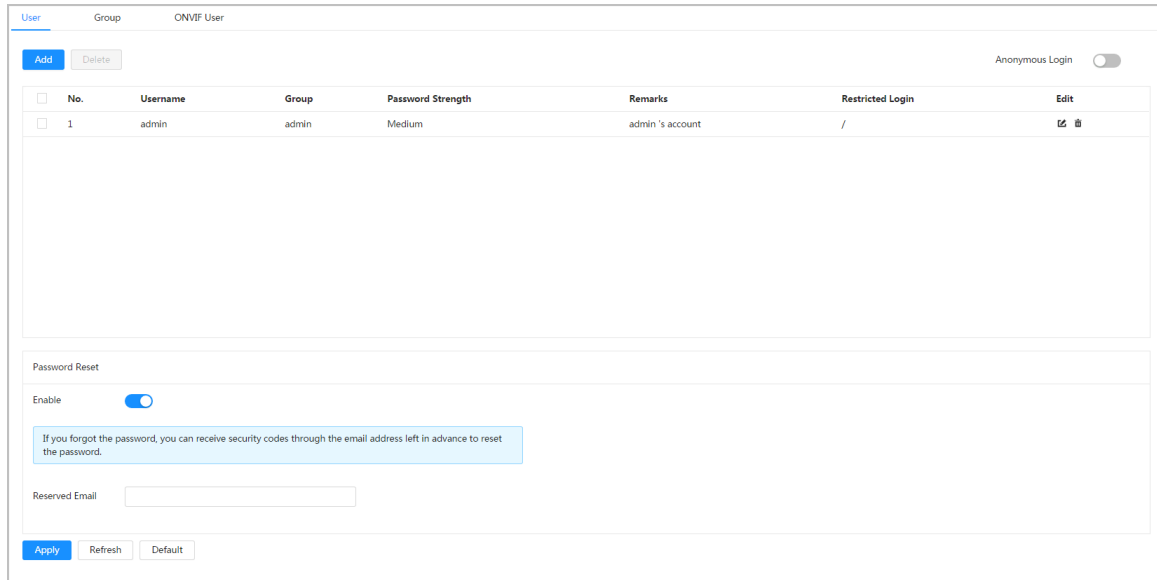
### 6.7.3.1.2 Resetting Password

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

## Procedure

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

**Figure 6-77 User**



- Step 2** Click  next to Enable in Password Reset.  
If the function is not enabled, you can only reset the password by resetting the camera.
- Step 3** Enter the reserved email address.
- Step 4** Click Apply.

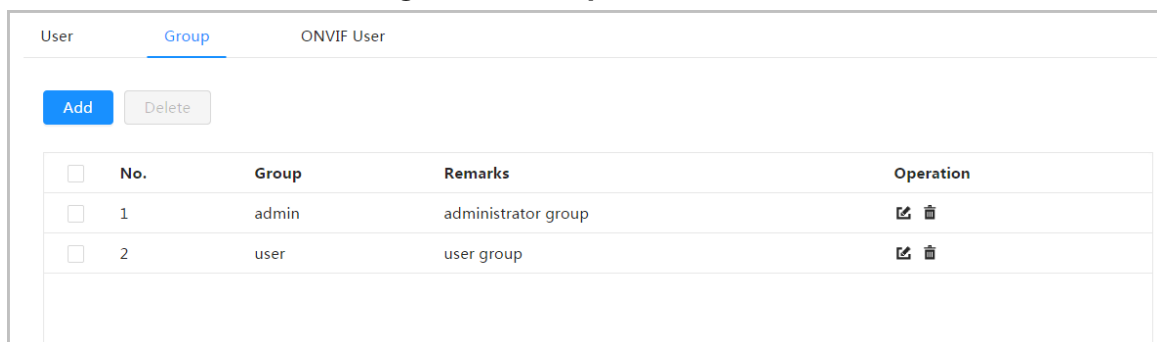
### 6.7.3.2 Adding User Group

You have two groups named admin and user by default, and you can add new group, delete added group or edit group authority and memo.

#### Procedure

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

**Figure 6-78 Group name**



- Step 2** Click Add.

Figure 6-79 Add group

**Step 3** Enter the group name and memo, and then select group authorities.

**Step 4** Click OK to finish configuration.

The newly added group displays in the group name list.

### Related Operations

- Click to edit password, group, memo or authorities.
- Click to delete the added users. Admin user cannot be deleted.



**The admin group and user group cannot be deleted.**

### 6.7.3.3 ONVIF User

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

#### Procedure

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

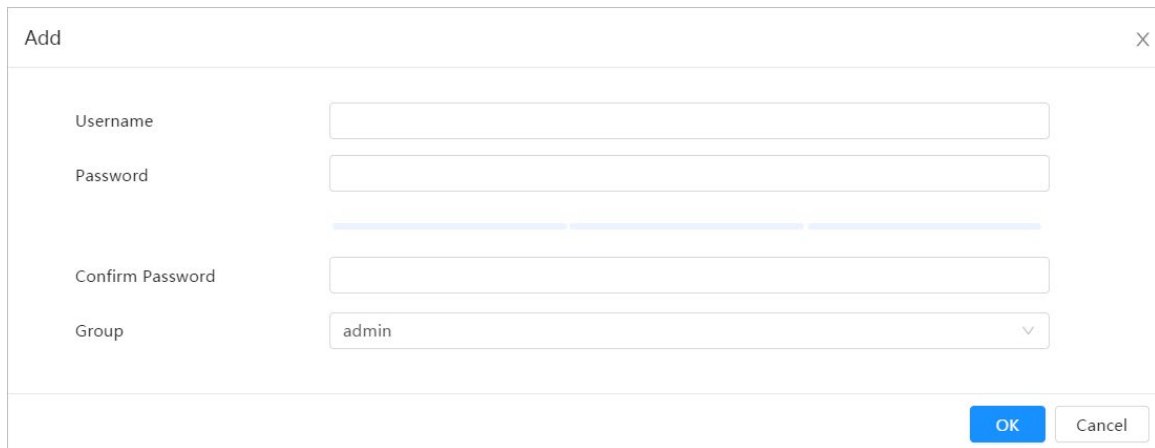
Figure 6-80 ONVIF user

No.	Username	Group	Password Strength	Edit
1	admin	admin	Medium	

**Step 2** Click Add.



Figure 6-81 Add ONVIF user



**Step 3** Configure user parameters.

Table 6-29 Description of ONVIF user parameters

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

**Step 4** Click OK.

The newly added user displays in the username 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 users.



**The admin account cannot be deleted.**

## 6.7.4 Peripheral Management

### 6.7.4.1 Configuring Serial Port

Set the serial port of the external device.

#### Procedure


**Step 1** Select  > System > Peripheral > Serial Port.

**Step 2** Configure parameters.

**Figure 6-82** Serial port settings

Serial Port	External Light	Wiper
Address	<input type="text" value="1"/>	
Baud Rate	<input type="text" value="9600"/>	▼
Data Bit	<input type="text" value="8"/>	▼
Stop Bit	<input type="text" value="1"/>	▼
Parity	<input type="text" value="None"/>	▼
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

**Table 6-30** Description of serial port settings parameters

Parameter	Description
IP Address	<p>Enter the corresponding device address. It is 1 by default.</p>  <p><b>Make sure that the address is the same as the device address; otherwise you cannot control the device.</b></p>
Baud Rate	Configure device baud rate. It is 9600 by default.
Data Bits	It is 8 by default.
Stop Bits	It is 1 by default.
Parity	It is None by default.

**Step 3** Click Apply.

### 6.7.4.2 Configuring External Light

You need to configure external light mode when the external light is used.

#### Prerequisites

- Connect external light with RS-485 port.
- You have configured serial port parameters. For details, see "6.7.4.1 Configuring Serial Port".

#### Procedure

**Step 1**  > System > Peripheral > External Light.

**Step 2** Select working mode as needed.

Figure 6-83 External light

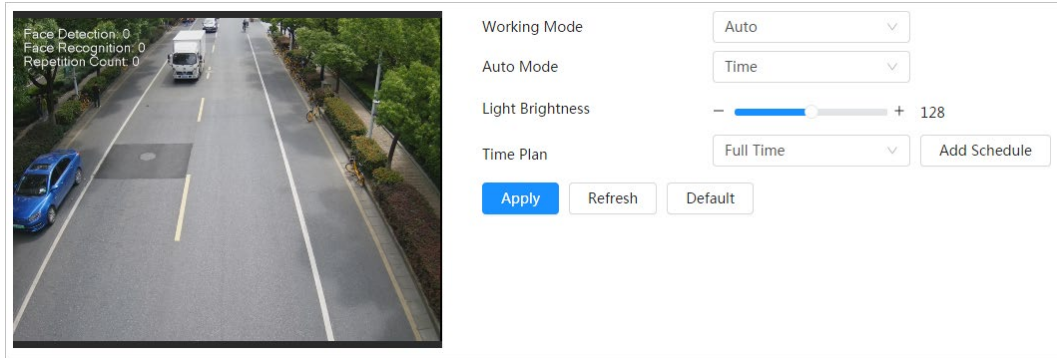



Table 6-31 Lamp parameters

Parameter	Description
Work Mode	<ul style="list-style-type: none"> <li>• <b>Off:</b> The external light is disabled.</li> <li>• <b>Manual:</b> Set the light brightness manually.</li> <li>• <b>Auto:</b> The camera turns on or turns off the light according to the light time and photoresistor automatically.</li> </ul>
Auto Mode	<ul style="list-style-type: none"> <li>• <b>Time:</b> When selecting Time in Auto Mode, set the arming period. During the arming period, the external light is on. Select the added time plan table in the Time Plan list. Click Add Schedule to add new time plan table. For details, see "6.5.1.2 Alarm Linkage".</li> <li>• <b>Photoresistor:</b> When you select Photoresistor in Auto Mode, the camera turns on the external light according to the brightness automatically.</li> </ul>
Light Brightness	<p>Set the brightness of the external light.</p>  <p>For some models, you can set the brightness of each external light separately.</p>

**Step 3** Click Apply.

### 6.7.4.3 Configuring Wiper

#### Procedure

**Step 1** Select >  > System > Peripheral > Wiper.

**Step 2** Configure working mode of wipers.

Figure 6-84 Wiper

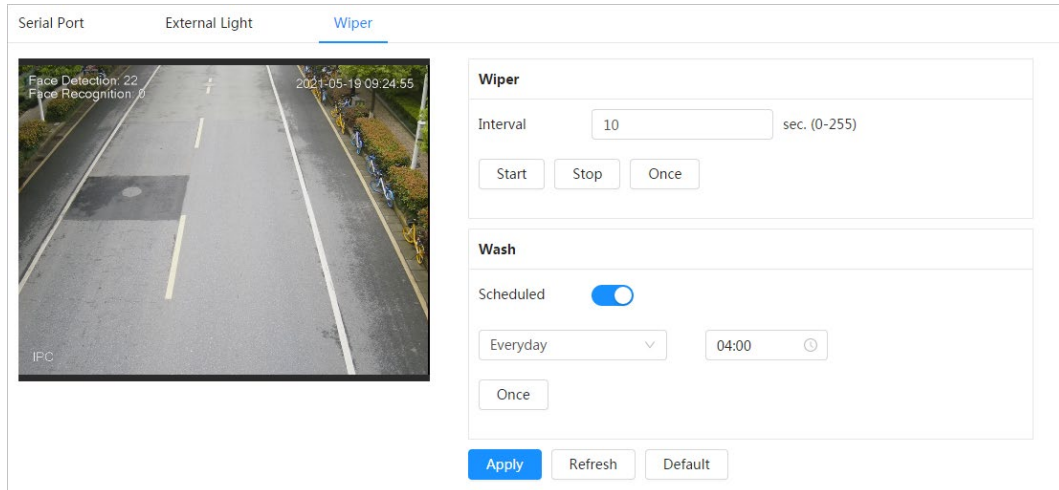


Table 6-32 Wiper parameter description

Parameter	Description
Interval	The interval between stop mode and start mode. For example, set the time to 10 s, and the wiper will work every 10 s.
Start, Stop, Once	Configure working mode of the wiper. <ul style="list-style-type: none"> <li>Click Start, and the wiper works as the set interval time.</li> <li>Click Stop, and the wiper stops working.</li> <li>Click Once, and the wiper works once.</li> </ul>
Wash	Select the Schedule checkbox and set the time, and then the wiper will work as the configured time. Click Once, and the wiper works once. It can be used to check whether the wiper works normally.

**Step 3** Click Apply.

## 6.7.5 Manager

### 6.7.5.1 Requirements

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

- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Change the password every three months. For details, see "6.7.3 Account".
- View system logs and analyze them, and process the abnormality in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

### 6.7.5.2 Maintenance

You can restart the system manually, and set the time of auto reboot and auto deleting old

files. This function is disabled by default.

## Procedure

**Step 1** Select > System > Manager > Maintenance.

Figure 6-85 Maintenance

**Step 2** Configure auto maintain parameters.

- Click next to Auto Reboot in Restart System, and set the reboot time, then the system will automatically restarts at the set time every week.
- Click next to Auto Delete in Delete Old Files, and set the time, then the system will automatically deletes old files at the set time. The time range is 1 to 31 days.



**When you enable and confirm the Auto Delete function, the deleted files cannot be restored. Operate it carefully.**

**Step 3** Click Apply.

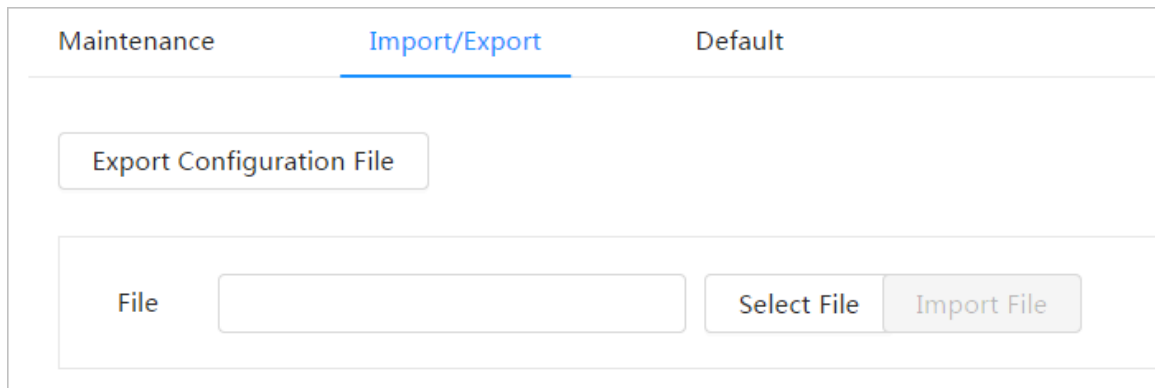
### 6.7.5.3 Import/Export

- Export the system configuration file to back up the system configuration.
- Import system configuration file to make quick configuration or recover system configuration.

## Procedure

**Step 1** Select > System > Manager > Import/Export.

Figure 6-86 Import/Export



**Step 2** Import or export the file.

- **Import:** Select local configuration file, and click **Import File** to import the local system configuration file to the system.
- **Export:** Click **Export Configuration file** to export the system configuration file to local storage.

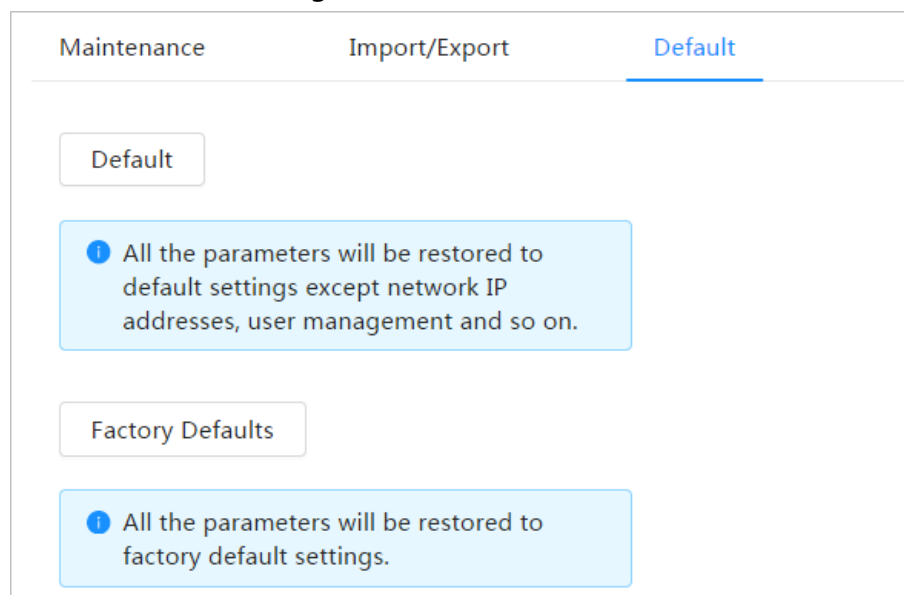
### 6.7.5.4 Default

Restore the device to default configuration or factory settings.

Select > System > Manager > Default.

- Click **Default**, and then all the configurations except IP address and account are reset to default.
- Click **Factory Default**, and all the configurations are reset to factory settings.

Figure 6-87 Default



### 6.7.6 Upgrade

Upgrading to the latest system can refine camera functions and improve stability.

If wrong upgrade file has been used, restart the device; otherwise some functions might not

work properly.

## Procedure


**Step 1** Select  > System > Upgrade.

Figure 6-88 Upgrade



**Step 2** Click Browse, and then upload upgrade file.

The upgrade file should be a .bin file.

**Step 3** Click Update.

## 6.8 System Information

You can view the information, including version, log and online user, and back up or clear log.

### 6.8.1 Version

Select  > System Info > Version to view device information such as hardware, system version, and web version.

### 6.8.2 Online User

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

## 6.9 Setting Log

### 6.9.1 Log

You can view and back up logs.

## Procedure

**Step 1** Select  > Log > Log.

**Step 2** Configure Start Time and End Time, and then select the log type.

The start time should be later than January 1, 2000, and the end time should be earlier than December 31, 2037.

The log type includes All, System, Setting, Data, Event, Record, Account, and Security.

- **System:** Includes program start, abnormal close, close, program reboot, device

shutdown, device reboot, system reboot, and system upgrade.

- **Setting:** Includes saving configuration and deleting configuration file.
- **Data:** Includes configuring disk type, clearing data, hot swap, FTP state, and record mode.
- **Event (records events such as video detection, smart plan, alarm and abnormality):** includes event start and event end.
- **Record:** Includes file access, file access error, and file search.
- **Account:** Includes login, logout, adding user, deleting user, editing user, adding group, deleting group, and editing group.
- **Security:** Includes password resetting and IP filter.

**Step 3** Click Search.


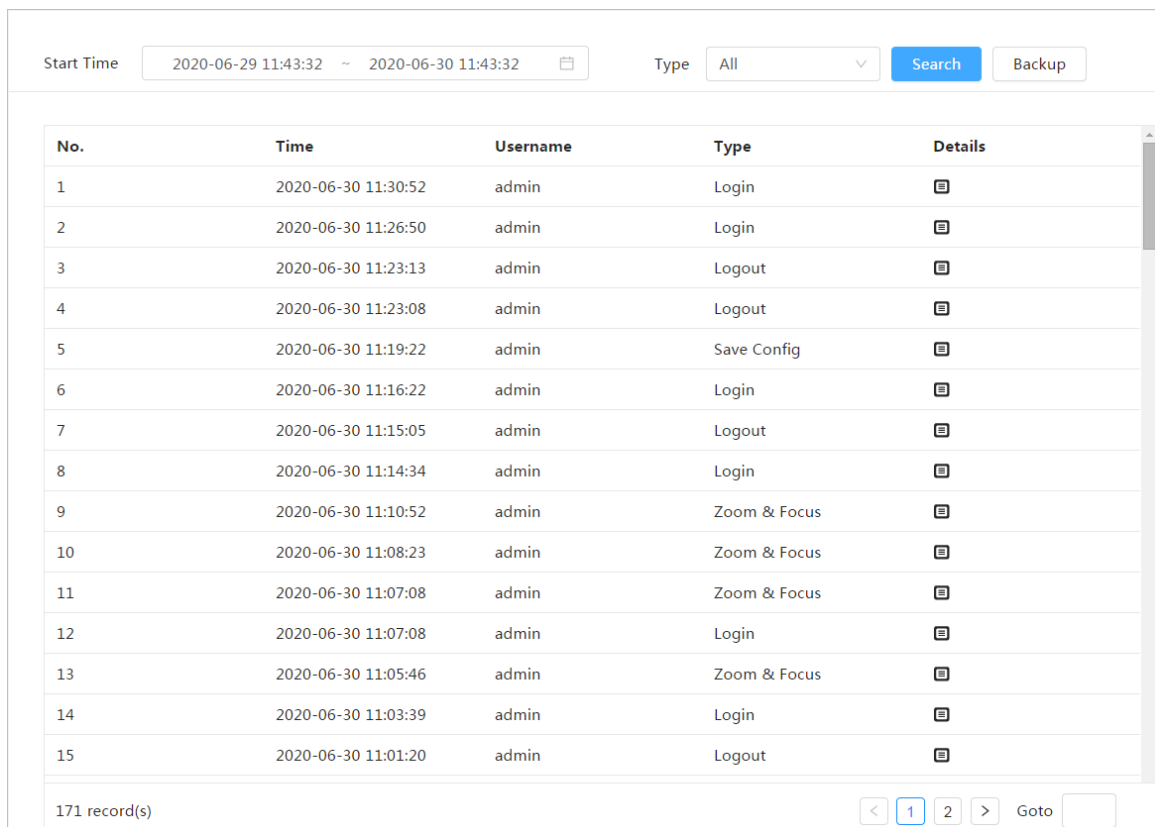















- Click  or click a certain log, and then you can view the detailed information in Details area.
- Click Backup, and then you can back up all found logs to local PC.

Figure 6-89 Log




No.	Time	Username	Type	Details
1	2020-06-30 11:30:52	admin	Login	
2	2020-06-30 11:26:50	admin	Login	
3	2020-06-30 11:23:13	admin	Logout	
4	2020-06-30 11:23:08	admin	Logout	
5	2020-06-30 11:19:22	admin	Save Config	
6	2020-06-30 11:16:22	admin	Login	
7	2020-06-30 11:15:05	admin	Logout	
8	2020-06-30 11:14:34	admin	Login	
9	2020-06-30 11:10:52	admin	Zoom & Focus	
10	2020-06-30 11:08:23	admin	Zoom & Focus	
11	2020-06-30 11:07:08	admin	Zoom & Focus	
12	2020-06-30 11:07:08	admin	Login	
13	2020-06-30 11:05:46	admin	Zoom & Focus	
14	2020-06-30 11:03:39	admin	Login	
15	2020-06-30 11:01:20	admin	Logout	

171 record(s) < 1 2 > Goto

## 6.9.2 Remote Log

Configure remote log, and you can get the related log by accessing the set address.

### Procedure

- Step 1** Select  > Log > Remote Log.
- Step 2** Click  to enable remote log function.
- Step 3** Set address, port and device number.



**Step 4** Click Apply.

**Figure 6-90 Remote log**

The screenshot shows a configuration panel for 'Remote log'. It contains the following elements:

- Enable:** A toggle switch that is currently turned off.
- Server Address:** A text input field containing a blurred IP address.
- Port:** A text input field containing the value '514', with a range '(1-65534)' indicated to the right.
- Device No.:** A text input field containing the value '22', with a range '(0-23)' indicated to the right.
- Buttons:** Three buttons are located at the bottom: 'Apply' (highlighted in blue), 'Refresh', and 'Default'.

# 7 Live

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

## 7.1 Live Page

Log in and click the Live tab.



Pages might vary with different models.

Figure 7-1 Live (single channel)

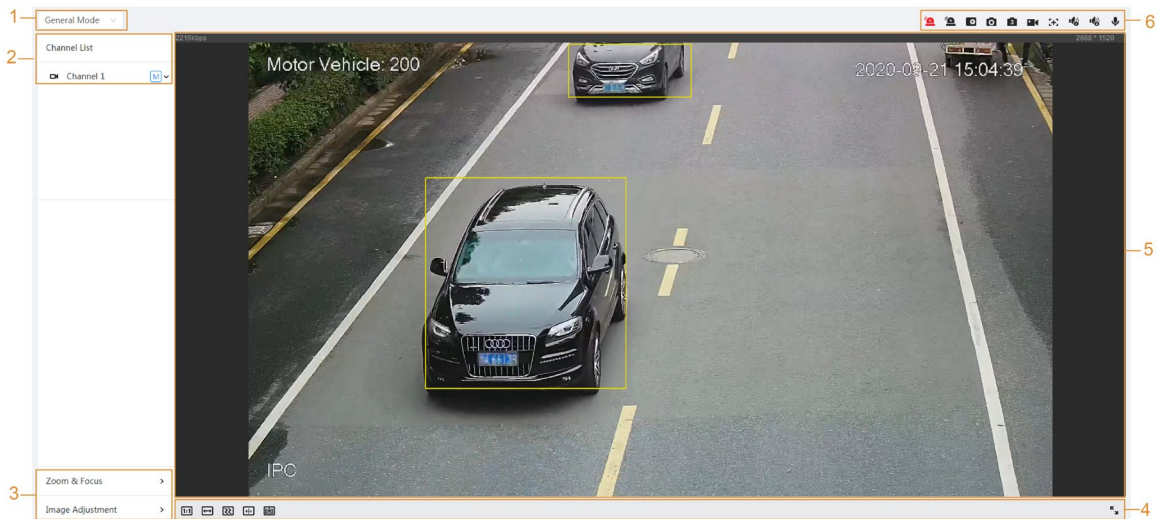


Figure 7-2 Live (multiple channels)

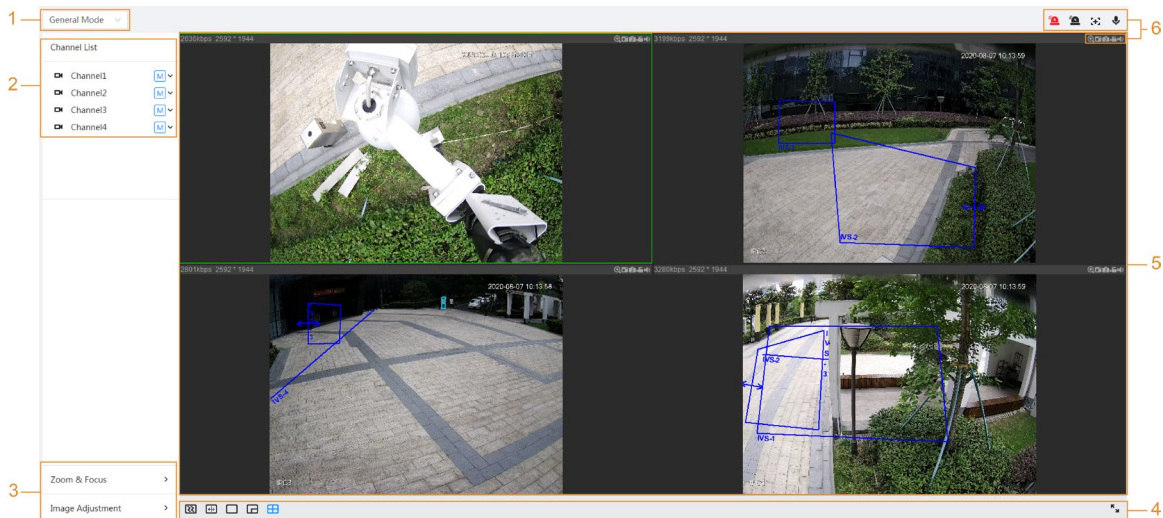


Figure 7-3 Live (EPTZ)

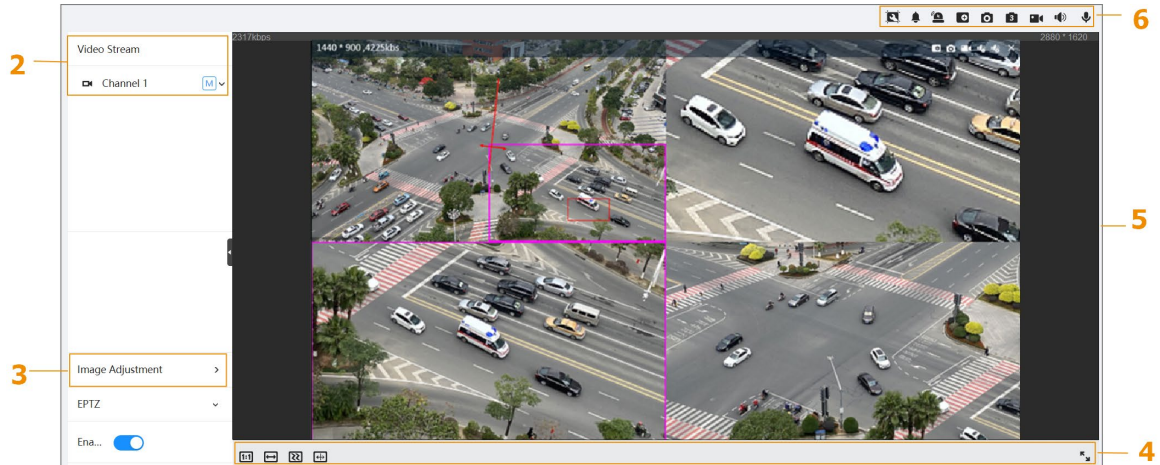


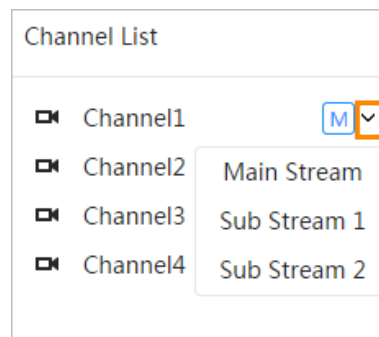
Table 7-1 Description of function bar

No.	Function	Description
1	Display mode	You can select the display mode from General Mode, Face Mode, Analytics Mode, ANPR and Face & Body Detection. For details, see "7.5 Display Mode".
2	Channel list	Displays all channels. You can select the channel as needed and set the stream type.
3	Image adjustment	Adjustment operations in live viewing.
4		
5	Live view	Displays the real-time monitoring image.
6	Live view function bar	Functions and operations in live viewing.

## 7.2 Setting Encode

Click , and then select the stream as needed.

Figure 7-4 Encode bar



- **Main Stream:** It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring. For details, see "6.2.2.1 Encode".
- **Sub Stream:** It has small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth is not enough. For

details, see "6.2.2.1 Encode".

- means the current stream is main stream; means the current stream is sub stream 1; means the current stream is sub stream 1.

## 7.3 Live View Function Bar

For the live view function bar, see Table 7-2.

Table 7-2 Description of live view function bar

Icon	Function	Description
	Force Alarm	<p>Display the status of alarm sound.</p> <p>Click the icon to enable or disable the alarm sound forcibly.</p>
	Digital Zoom	<p>You can zoom video image through two operations.</p> <ul style="list-style-type: none"> <li>• Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area.</li> <li>• Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.</li> </ul>
	Snapshot	<p>Click the icon to capture one picture of the current image, and it will be saved to the configured storage path.</p> <p></p> <p>For details on viewing or configuring storage path, see "6.1 Local".</p>
	Triple Snapshot	<p>Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path.</p> <p></p> <p>For details on viewing or configuring storage path, see "6.1 Local".</p>
	Record	<p>Click the icon to record video, and it will be saved to the configured storage path.</p> <p></p> <p>For details on viewing or configuring storage path, see "6.1 Local".</p>

Icon	Function	Description
	Aux Focus	<p>Click the icon, the AF Peak (focus eigenvalue) and AF Max (max focus eigenvalue) are displayed on the video image.</p> <ul style="list-style-type: none"> <li>• AF Peak: The eigenvalue of image definition, it displays during focus.</li> <li>• AF Max: The best eigenvalue of image definition.</li> <li>• The smaller the difference between AF peak value and the AF max value, the better the focus is.</li> </ul> <p> Aux focus closes automatically after five minutes.</p>
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio talk.

## 7.4 Window Adjustment Bar

### 7.4.1 Adjustment

This section introduces the adjustment of image.

Table 7-3 Description of adjustment bar

Icon	Function	Description
	Original Size	Click the icon, and then the video displays with original size.
	Full Screen	Click the icon to enter full screen mode; double-click or press Esc to exit.
	W:H	Click the icon to resume original ratio or change ratio.

Icon	Function	Description
	Fluency Adjustment	<p>Click the icon to select the fluency from Realtime, General and Fluent.</p> <ul style="list-style-type: none"> <li>• <b>Realtime:</b> Guarantees the real time of the image. When the bandwidth is not enough, the image might not be smooth.</li> <li>• <b>General:</b> It is between Realtime and Fluent.</li> <li>• <b>Fluent:</b> Guarantees the fluency of the image. There might be delay between live view image and real-time image.</li> </ul>
	Analytics+ Rule	<p>Click the icon, and then select Enable to display Analytics+ rules and detection box; select Disable to stop the display. It is enabled by default.</p>
	Crowd Distribution Map	<p>Click the icon and select Enable. The Crowd Distribution Map page is displayed. For details, see "8.1 Setting Crowd Distribution Map".</p>
	Adjust View	<p>Click the icon and select Enable. When moving the mouse pointer to the center of live page, a floating box is displayed. Click and drag the four angles in the box to adjust the views. This function is closed by default.</p> <p> <b>Only Parking Space Detection</b> <b>Fisheye WizMind Network Camera</b> supports this function.</p>
	Window Layout	<p>When viewing multi-channel image, you can select display layout.</p>

## 7.4.2 Zoom and Focus

Click Zoom and Focus at the lower-left corner of Live page to adjust focal length to zoom in or out video image; by adjusting focus manually, automatically or within a certain area, you can change image clarity or correct adjusting errors.



**The focus would adjust automatically after zooming in or out.**

Figure 7-5 Zoom and focus

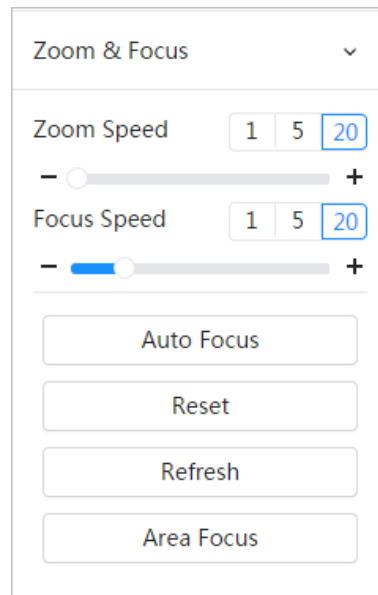




Table 7-4 Description of zoom and focus parameter

Parameter	Description
Zoom Speed	<p>Changes the focal length of the camera to zoom in or out the image.</p> <ol style="list-style-type: none"> <li>Set the speed value. The Zoom Speed is the adjustment range in one click. The larger the value is, the more the image would zoom in or out in one click.</li> <li>Click or hold + or- button, or drag the slider to adjust zoom.</li> </ol>
Focus Speed	<p>Adjusts the optical back focal length to make the image clearer.</p> <ol style="list-style-type: none"> <li>Set the speed value. The Focus Speed is the adjustment range in one click. The larger the value is, the more the adjustment in one click.</li> <li>Click or hold + or- button, or drag the slider to adjust focus.</li> </ol>
Auto Focus	<p>Adjusts image clarity automatically.</p>  <p><b>Do not make any other operation during auto focus process.</b></p>
Reset	<p>Restores focus to default value and corrects errors.</p>  <p><b>You can restore the focus if the image has poor clarity or has been zoomed too frequently.</b></p>
Refresh	<p>Get the latest zoom setting of the camera.</p>
Area Focus	<p>Focus on the subject of a selected area.</p> <p>Click Area Focus, and then select an area in the image, the camera performs auto focus in that area.</p>

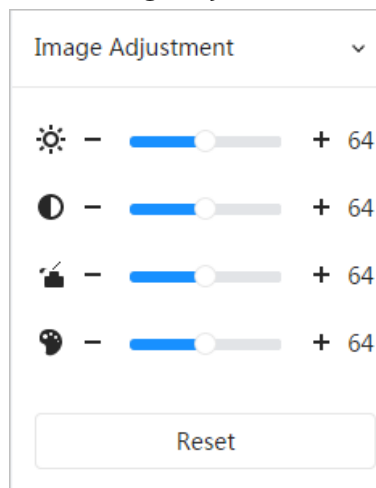
## 7.4.3 Image Adjustment

Click Image Adjustment at the lower-left corner of Live page, and click + or- button, or drag the slider to adjust image parameters, including brightness, contrast, hue, and saturation.



The adjustment is only available on the web page, and it does not adjust the camera parameters.

Figure 7-6 Image adjustment



- ☀ (Brightness adjustment): Adjusts the overall image brightness, and changes the value when the image is too bright or too dark. The bright and dark areas will have equal changes.
- 🌑 (Contrast adjustment): Changes the value when the image brightness is proper but contrast is not enough.
- 🎨 (Saturation adjustment): Adjusts the image saturation, this value does not change image brightness.
- 🌀 (Hue adjustment): Makes the color deeper or lighter. The default value is made by the light sensor, and it is recommended.

Click Reset to restore focus to default value.



You can restore the zoom if the image has poor clarity or has been zoomed too frequently.

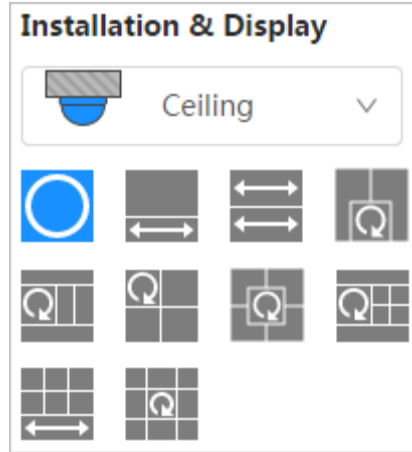
## 7.4.4 Fisheye

You can select the installation mode, display mode and VR mode of fisheye devices as needed. For details, see Table 7-5.

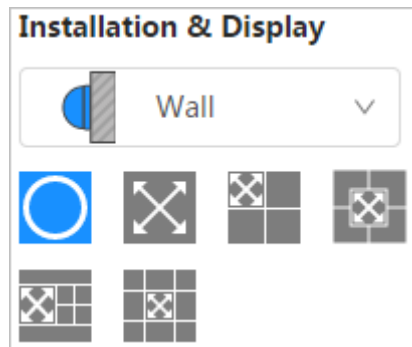
- **Install Mode:** Select the installation mode according to the actual situation.
- **Display Mode:** Select the display mode of live view.
- **VR Mode:** Select VR mode to display images in stereo mode.



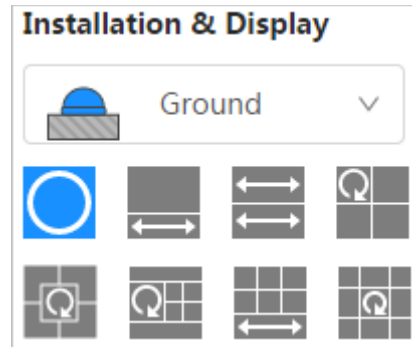
**Figure 7-7 Fisheye-ceiling mount**



**Figure 7-8 Fisheye-wall mount**



**Figure 7-9 Fisheye-ground mount**

















**Figure 7-10 Fisheye-VR mode**






**Table 7-5 Description of fisheye configuration**

Parameter	Description
Installation mode	Includes ceiling mount, wall mount, and ground mount.

Parameter	Description	
Display mode	<p>The display model of the current image. There are different display modes for each installation mode.</p> <ul style="list-style-type: none"> <li>• Ceiling: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8.</li> <li>• Wall: 1P, 1P+3, 1P+4, 1P+8.</li> <li>• Ground: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8.</li> </ul>  <p>The image will be the original size by default when switching installation mode.</p>	
Ceiling/Wall/Ground mount	 Original image	The original image before correction.
Ceiling/Ground mount	 1P+1	360° rectangular panoramic image screen + independent sub-screens. <ul style="list-style-type: none"> <li>• You can zoom or drag the image in all the screens.</li> <li>• You can move the start point (left and right) on rectangular panoramic image screen.</li> </ul>
	 2P	Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. It is also called dual-panoramic image. You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.
	 1+2	Original image screen + two independent sub-screens. Ground mount does not support this display mode. <ul style="list-style-type: none"> <li>• You can zoom or drag the image in all the screens.</li> <li>• You can rotate the image on the original image screen to change the start point.</li> </ul>
	 1+3	Original image screen + three independent sub-screens. <ul style="list-style-type: none"> <li>• You can zoom or drag the image in all the screens.</li> <li>• You can rotate the image on the original image screen to change the start point.</li> </ul>
	 1+4	Original image screen + four independent sub-screens. <ul style="list-style-type: none"> <li>• You can zoom or drag the image in all the screens.</li> <li>• You can rotate the image on the original image screen to change the start point.</li> </ul>

Parameter	Description	
	 <b>1P+6</b>	<b>360° rectangular panoramic screen + six independent sub-screens.</b> <ul style="list-style-type: none"> <li>You can zoom or drag the image in all the screens.</li> <li>You can move the start point (left and right) on rectangular panoramic image screen.</li> </ul>
	 <b>1P+8</b>	<b>Original image screen + eight independent sub-screens.</b> <ul style="list-style-type: none"> <li>You can zoom or drag the image in all the screens.</li> <li>You can rotate the image on the original image screen to change the start point.</li> </ul>
Wall mount	 <b>1P</b>	<b>180° rectangular panoramic image screen (from left to right).</b> You can drag the image in all the screens (up and down) to adjust the vertical view.
	 <b>1P+3</b>	<b>180° rectangular panoramic image screen + three independent sub-screens.</b> <ul style="list-style-type: none"> <li>You can zoom or drag the image in all the screens.</li> <li>You can drag the image in all the screens (upper and lower) to adjust the vertical view.</li> </ul>
	 <b>1P+4</b>	<b>180° rectangular panoramic image screen + four independent sub-screens.</b> <ul style="list-style-type: none"> <li>You can zoom or drag the image in all the screens.</li> <li>You can drag the image in all the screens (upper and lower) to adjust the vertical view.</li> </ul>
	 <b>1P+8</b>	<b>180° rectangular panoramic image screen + eight independent sub-screens.</b> <ul style="list-style-type: none"> <li>You can zoom or drag the image in all the screens.</li> <li>You can drag the image in all the screens (upper and lower) to adjust the vertical view.</li> </ul>
VR mode	 <b>Panorama</b>	<b>Drag or cross the screen 360° to unfold the distortion panorama, and you can drag the image in left/right direction.</b>

Parameter	Description	
	 Semi-circle	<ul style="list-style-type: none"> <li>You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to resume the original size.</li> <li>Press S to rotate the image in anticlockwise direction, and press E to stop the rotation.</li> <li>Scroll the mouse wheel to zoom the image.</li> </ul>
	 Cylinder	<p>Display the distortion panorama in 360° circularity.</p> <ul style="list-style-type: none"> <li>You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size.</li> <li>Press S to rotate the image in anticlockwise direction, and press E to stop the rotation.</li> <li>Scroll the mouse wheel to zoom the image.</li> </ul>
	 Asteroid	<ul style="list-style-type: none"> <li>You can drag the image in upper/lower/left/right direction. Press I to display the panorama, and press O to return to the original size.</li> <li>Press the left mouse-button to slide down to display the image on the plane surface.</li> <li>Scroll the mouse wheel to zoom the image.</li> </ul>

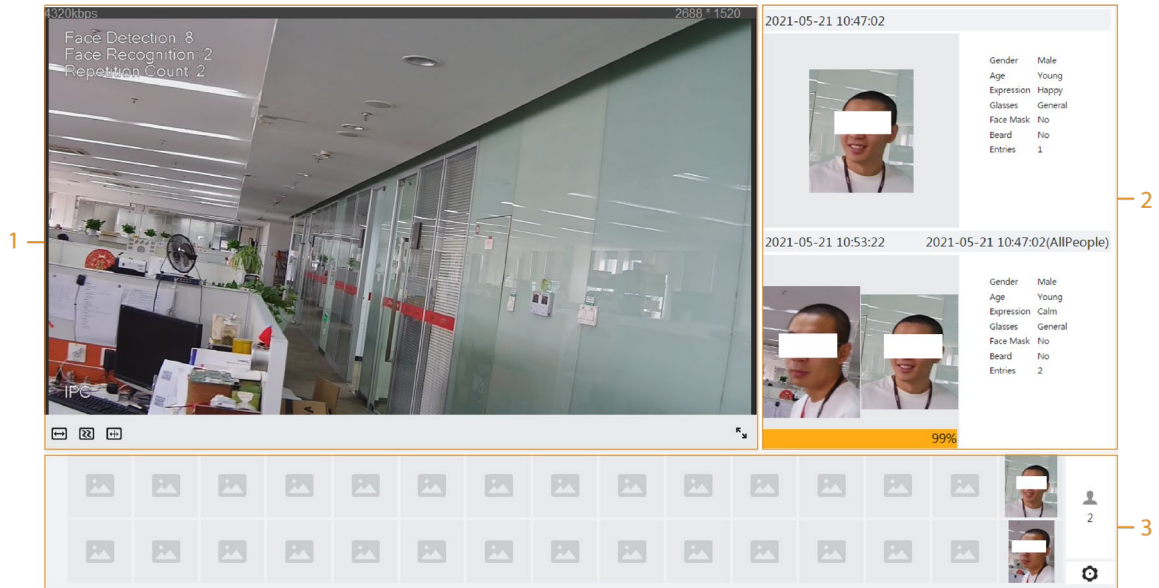
## 7.5 Display Mode

You can select the display mode from General Mode, Face Mode, Analytics Mode, ANPR, Parking Space Detection, PPE Detection Mode and Face & Body Detection. For general mode, see Figure 7-2. This section mainly introduces Face Mode, Analytics Mode, PPE Detection Mode and Parking Space Detection.



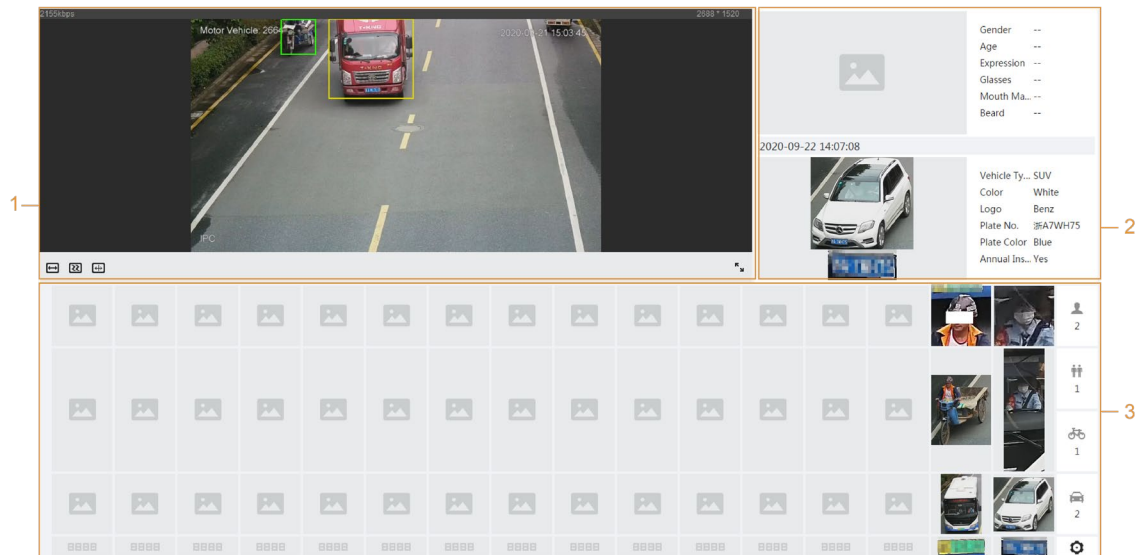
- Pages might vary with different models.
- Make sure that you have enabled the corresponding function.
- Select Face Mode from the display mode drop-down list.

**Figure 7-11 Face mode**



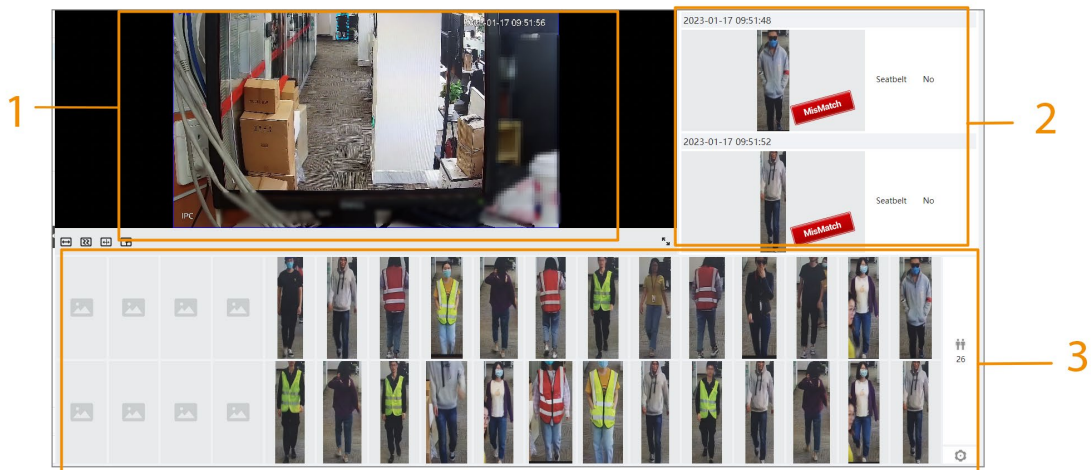
- Select Analytics Mode from the display mode drop-down list.

**Figure 7-12 Analytics mode**



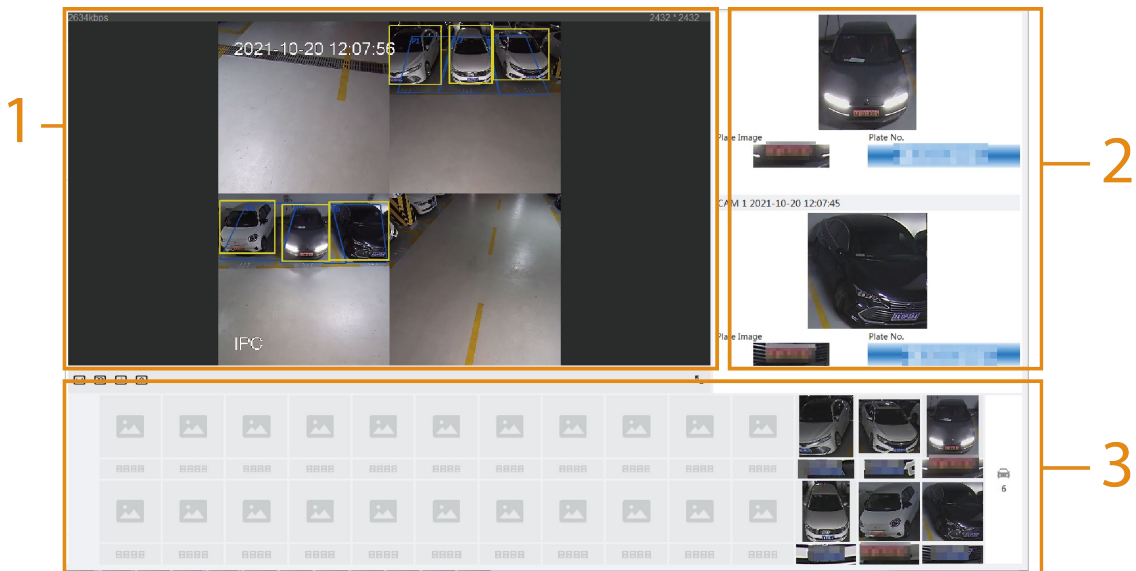
- Select PPE Detection Mode from the display mode drop-down list.

**Figure 7-13 PPE Detection Mode**





- Select Parking Space Detection from the display mode drop-down list.

**Figure 7-14 Parking space detection**



**Table 7-6 Description of layout (face mode, Analytics mode and PPE detection mode)**

No.	Function	Description
1	Live view	Displays the real-time monitoring image. For details, see "7.4.1 Adjustment".
2	Details	Displays the captured image and details.
3	Captured image	<p>Displays the captured images.</p> <ul style="list-style-type: none"> <li>• Click a snapshot in the area, and the details of the snapshot are displayed.</li> <li>• Click  to set the attributes displayed.</li> </ul> <p> <b>This attribute is not available for parking space mode.</b></p>

**Table 7-7 Description of layout (parking space mode)**

No.	Function	Description
1	Live view	Displays the real-time monitoring image. For details, see "7.4.1 Adjustment".
2	Captured image	Displays the latest two events captured.
3	Details	Displays the captured images and details.

## 8 Analytics+

### 8.1 Setting Crowd Distribution Map

You can view crowd distribution on the map in real time for timely arming, to prevent stampede and other accidents.

#### 8.1.1 Global Configuration

Set the calibration parameters of panoramic cameras.




##### Calibration Purpose

Determine corresponding relationship between 2D image captured by the camera and 3D actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

##### Notes

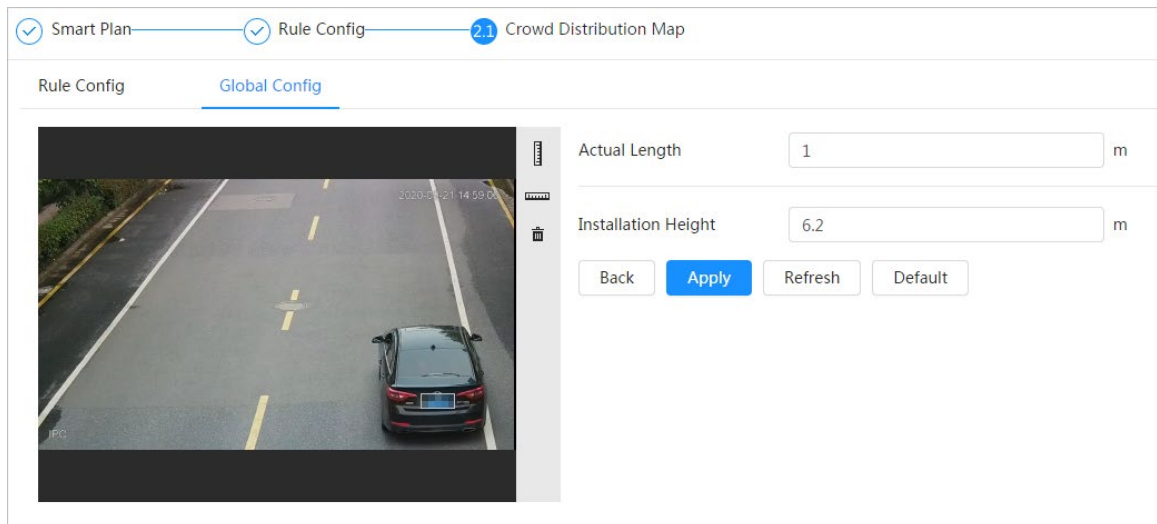
When drawing calibration ruler, keep the ruler length consistent with the actual length of the object.

##### Procedure

1. Select Analytics+ > Smart Plan.
2. Click  next to Crowd Distribution Map to enable crowd distribution map of the corresponding channel, and then click Next.
3. Click the Global Config tab.
4. Click the rule icon to draw one horizontal ruler and three vertical rulers on the image.
  -  is the vertical ruler icon, and  is the vertical horizontal icon.
  - Select the added rulers on the image, and click  to delete them.



**Figure 8-1 Global configuration of crowd distribution map**



5. Select a calibration type and enter the actual length, and then click Add Rulers.
6. Click Apply.

## 8.1.2 Rule Configuration

When the number of people or the crowd density in the detection area exceeds the configured threshold, the system performs alarm linkages.

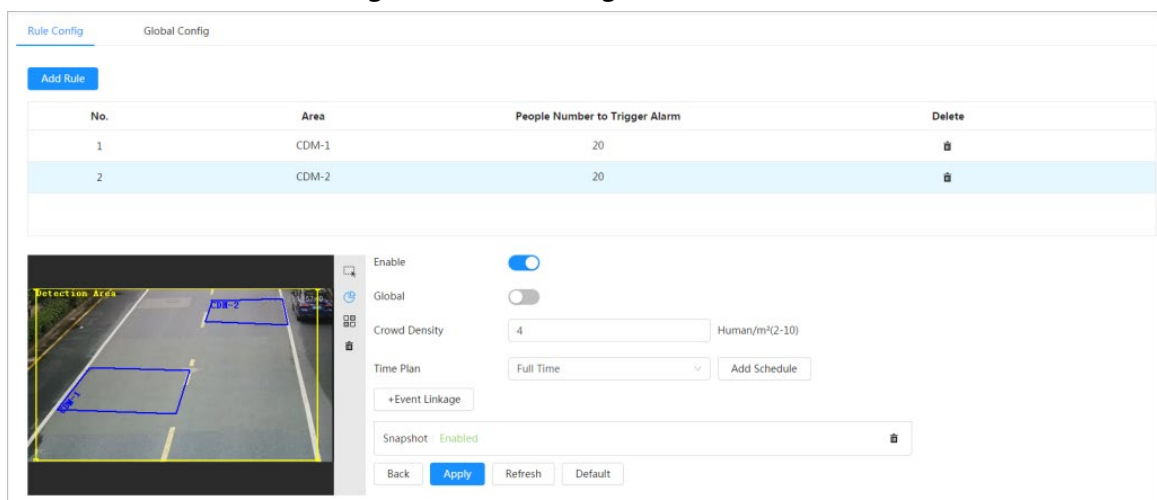
### Prerequisites

- Select Analytics+ > Smart Plan, and enable Crowd Distribution Map.
- You have configured the parameters on the Global Config page.


### Procedure

- Step 1** Select Analytics+ > Smart Plan
- Step 2** Click  next to Crowd Distribution Map, and then click Next.
- Step 3** Click the Rule Config tab.

**Figure 8-2 Rule configuration**



- Step 4** Click  next to Enable, and then the crowd map function is enabled, and the detection area box is displayed on the image.

Click , and you can drag any corner of the box to adjust the size of the area, and press the left mouse button and move the box to adjust the position.

**Step 5** Draw multiple people counting areas in Detection Area as needed.



1) Click Add Rule to add statistical areas.

2) Set the name of Area and People Number to Trigger Alarm.

When the number of the people in the area exceeds the configured threshold, the alarm will be triggered, and the system will perform the linkage actions. The people number to trigger alarm is 20 by default.

3) Click  at the right side of the image, draw people counting areas in the detection area, and then right-click to finish the drawing.

4) Repeat the above steps to add more people counting areas.

- Click , and then press and hold the left mouse button to draw a rectangle, and then pixel size is displayed.
- Click  to delete the drawn detection or people counting areas.

**Step 6** Configure parameters.

Table 8-1 Description of crowd map parameters

Parameter	Description
Global	Click <input type="checkbox"/> next to Global and set the crowd density threshold. The system detects crowd distribution in the global area. When the crowd density exceeds the configured threshold, the system performs alarm linkages.
Crowd Density	

**Step 7** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". Click + Event Linkage to set the linkage action.

**Step 8** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## Result

Click  on the Live page to view the crowd distribution map.

Figure 8-3 Crowd map (1)



Double-click the rendering area at the lower-right corner in the image to view crowd distribution in the area.

Figure 8-4 Crowd map (2)

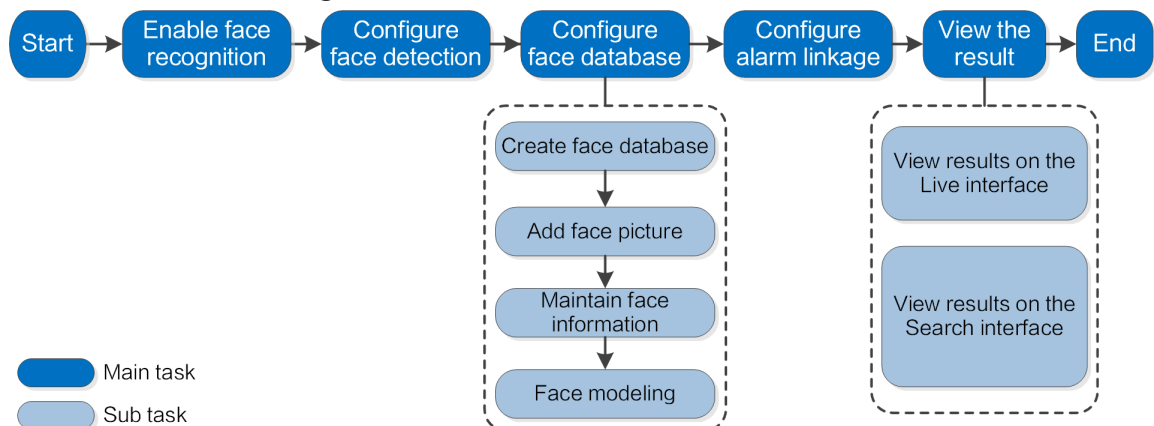


## 8.2 Setting Face Detection+

When a face is detected or recognized in the detection area, the system performs alarm linkage and supports searching face detection and recognition results.

- **Face Detection:** When a face is detected in the area, the system performs alarm linkage, such as recording and sending emails.
- **Face Detection+:** When a face is detected in the area, the system compares the captured face image with the information in the face database, and links alarm according to the comparison result.

Figure 8-5 Face Detection+ flowchart



### 8.2.1 Enabling Face Detection+

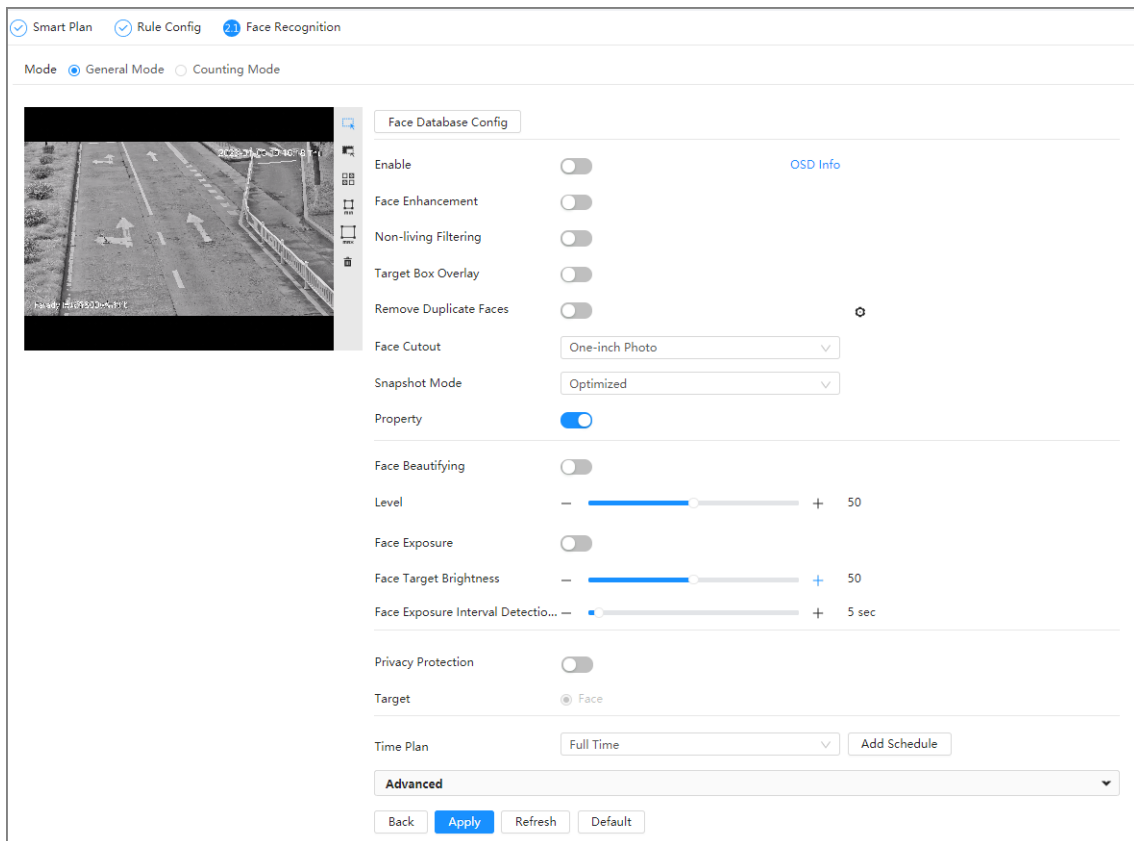
When a face is recognized in the detection area, the system performs alarm linkage.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Face Detection+ to enable Face Detection+ of the corresponding channel, and then click Next.

Figure 8-6 Face Detection+



**Step 3** Select the detection mode.

- **General Mode:** When a face is detected in the detection area, the system performs alarm linkage, such as recording and sending emails.
- **Counting Mode:** You can do precise face counting with two default function databases (all people database and exclude people database). The faces detected by the camera will be uploaded to the all people database automatically; the face in the exclude people database will not be counted. Add faces that you do not want to count (such as repeating faces and loitering faces) into the exclude people database so that the system will not count the faces after detecting them.

**Step 4** Click  next to Enable to enable the face detection function.

**Step 5** (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.



- Click to draw rule line in the image.  
When targets enter or leave the detection area along the direction line, their face images will be uploaded to the all people database, and then the system will determine whether to count it after comparing with that in the exclude database.



**This icon is only available in counting mode.**



- Click to draw a face detection area in the image, and right-click to finish the drawing.
- Click to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click to draw the minimum size of the target, and click to draw the


maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.

- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

**Step 6** Set parameters.

**Table 8-2** Description of face detection parameters

Parameter	Description
OSD Info	Click OSD Info, and the Overlay page is displayed, and then enable the face statistics function. The number of detected faces is displayed on the Live page. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click <input type="checkbox"/> to enable face enhancement, and it can preferably guarantee clear face with low stream.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.
Target Box Overlay	Click <input type="checkbox"/> to enable the function, and then you can add a bounding box to the face in the captured picture to highlight the face.  The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".
Remove Duplicate Faces	During the configured period, the duplicate faces are displayed only once to avoid repeated counting. Click  to configure the parameter, and then click Apply. <ul style="list-style-type: none"> <li>• Time: During the configured time, the function is enabled.</li> <li>• Precision: The larger the precision value, the higher the accuracy.</li> </ul>
Face Cutout	Set a range for the captured face image, including face, one-inch picture, and custom. When selecting Custom, click  , configure the parameters on the prompt page, and then click Apply. <ul style="list-style-type: none"> <li>• Customized width: Set snapshot width; and then enter the times of the original face width. It ranges from 1–5.</li> <li>• Customized face height: Set face height in snapshot; and then enter the times of the original face height. It ranges from 1–2.</li> <li>• Customized body height: Set body height in snapshot; and then enter the times of the original body height. It ranges from 0–4. When the value is 0, it cuts out the face image only.</li> </ul>

Parameter	Description
Snapshot Mode	<ul style="list-style-type: none"> <li>• <b>General mode:</b> <ul style="list-style-type: none"> <li>◇ <b>Optimized Snapshot:</b> Capture the clearest picture within the configured time after the camera detects face.</li> <li>◇ <b>Recognition Priority:</b> Repeatedly compare the captured face to the faces in the armed face database, and capture the most similar face image and send the event. We recommend you use this mode in access control scene.</li> </ul> </li> </ul>  <p>Click Advanced to set the optimized time.</p> <ul style="list-style-type: none"> <li>• <b>Counting mode:</b> The snapshot mode is tripwire by default, and you cannot change it.</li> </ul>
Property	Click <input type="checkbox"/> next to Property to enable the properties display.
Face Beautifying	Enable Face Beautifying to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Enable Face Exposure. When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.
Privacy Protection	Enable this function, and the faces will be blurred by mosaic when they are detected.
Advanced	<ul style="list-style-type: none"> <li>• <b>Snapshot Angle Filter:</b> Set snapshot angle to be filtered during the face detection.</li> <li>• <b>Snapshot Sensitivity:</b> Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>• <b>Optimized Time:</b> Set a period to capture the clearest picture after the camera detects face.</li> </ul>

**Step 7** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

**Step 8** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## 8.2.2 Setting Face Database

By setting face database, the face database information can be used to compare with the face detected.

Face database configuration includes creating face database, adding face picture, and face modeling.



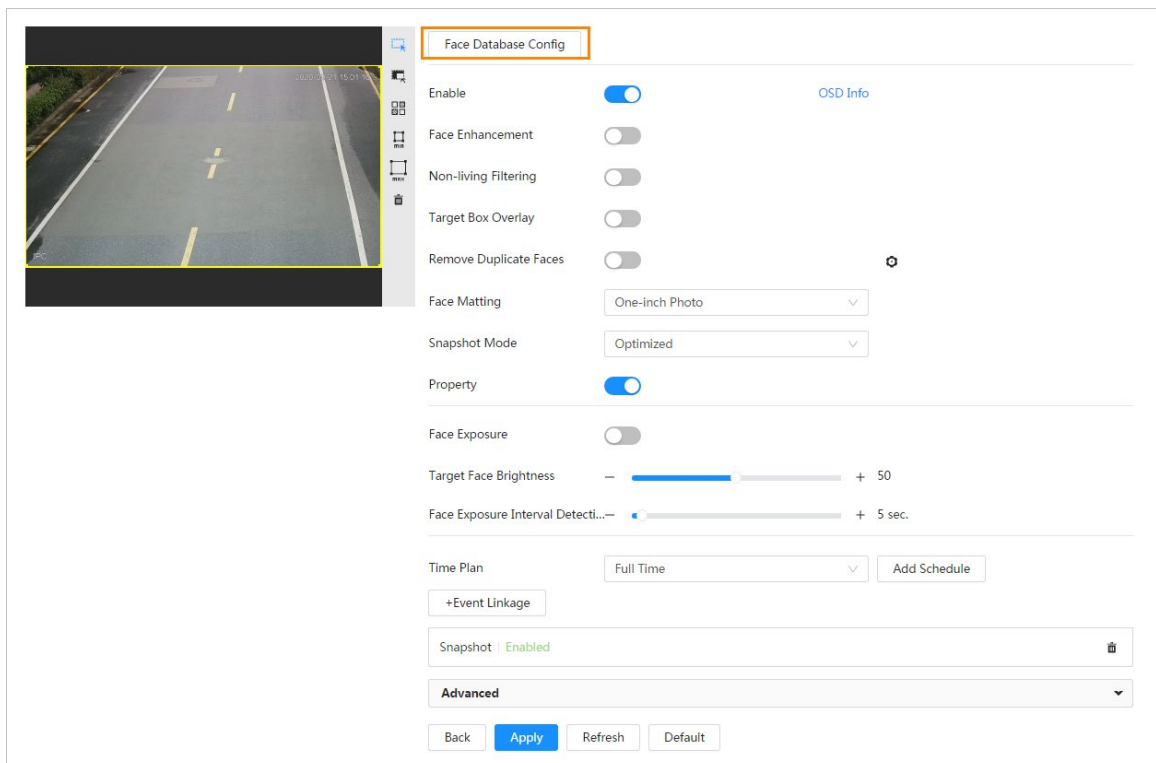
### 8.2.2.1 Creating Face Database

Face database includes face picture, face data and other information. It also provides comparison data for the captured face pictures.

#### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to Face Detection+ to enable Face Detection+ of the corresponding channel, and then click Next.
- Step 3** Select the detection mode.
- Step 4** Click Face Database Config on the Face Detection+ page.

Figure 8-7 Face database configuration



- Step 5** Click Add Face Database.
- Step 6** Set the name of the face database.

Figure 8-8 Add face database



- Step 7** Click OK.
  - **General mode:** You can add 5 databases at most as needed.

Figure 8-9 Face database successfully added (general mode)

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	VIP	0	82	Unconnected			
2	Employees	0	82	Unconnected			
3	5	0	82	Unconnected			
4	6	0	82	Unconnected			
5	test01	0	82	Unconnected			

- **Counting mode:** Except two default function databases (all people database and exclude people database), you can add 5 databases at most. Add faces that you do not want to count (such as repeating faces and loitering faces) into the exclude people database so that the system will not count the faces face after detecting them.

Figure 8-10 Face database successfully added (counting mode)

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	AllPeople	34	82	Connected			
2	ExcludePeople	0	82	Connected			
3	VIP	0	82	Unconnected			
4	Employees	0	82	Unconnected			
5	5	0	82	Unconnected			
6	6	0	82	Unconnected			
7	test01	0	82	Unconnected			

## Related Operations

- **Edit the name of the face database**

Click the text box under Name to edit the name of the face database.



- ◇ You cannot change the name of all people database and exclude database.
- ◇ Do not name the newly added database as AllPeople or ExcludePeople.

- **Arm alarm**

Click to configure the parameters of arm alarm. For details, see "8.2.3 Setting Arm Alarm".

- **Manage face database**

Click to manage the face database. You can search face, register, batch register, modeling all, modeling, and delete faces.



The all people database only supports modeling all, modeling, and delete faces.

- **Delete face database**

Click to delete the face database.



The all people database and exclude database cannot be deleted.

### 8.2.2.2 Adding Face Picture

Add face picture to the created face database. Single adding and batch importing are supported.

Requirements on face pictures.

- A single face picture size is 50K–150K in JPEG format. The resolution is less than 1080p.
- Face size is 30%–60% of the whole picture. Pixel should be no less than 100 pixels between



the ears.

- Taken in full-face view directly facing the camera without makeup, beautification, glasses, and fringe. Eyebrow, mouth and other face features must be visible.

### 8.2.2.2.1 Single Adding

Add face pictures one by one. Select this way when you need to add a small number of face pictures.

#### Procedure

**Step 1** On the Face Database Config page, click  next to the face database to be configured.

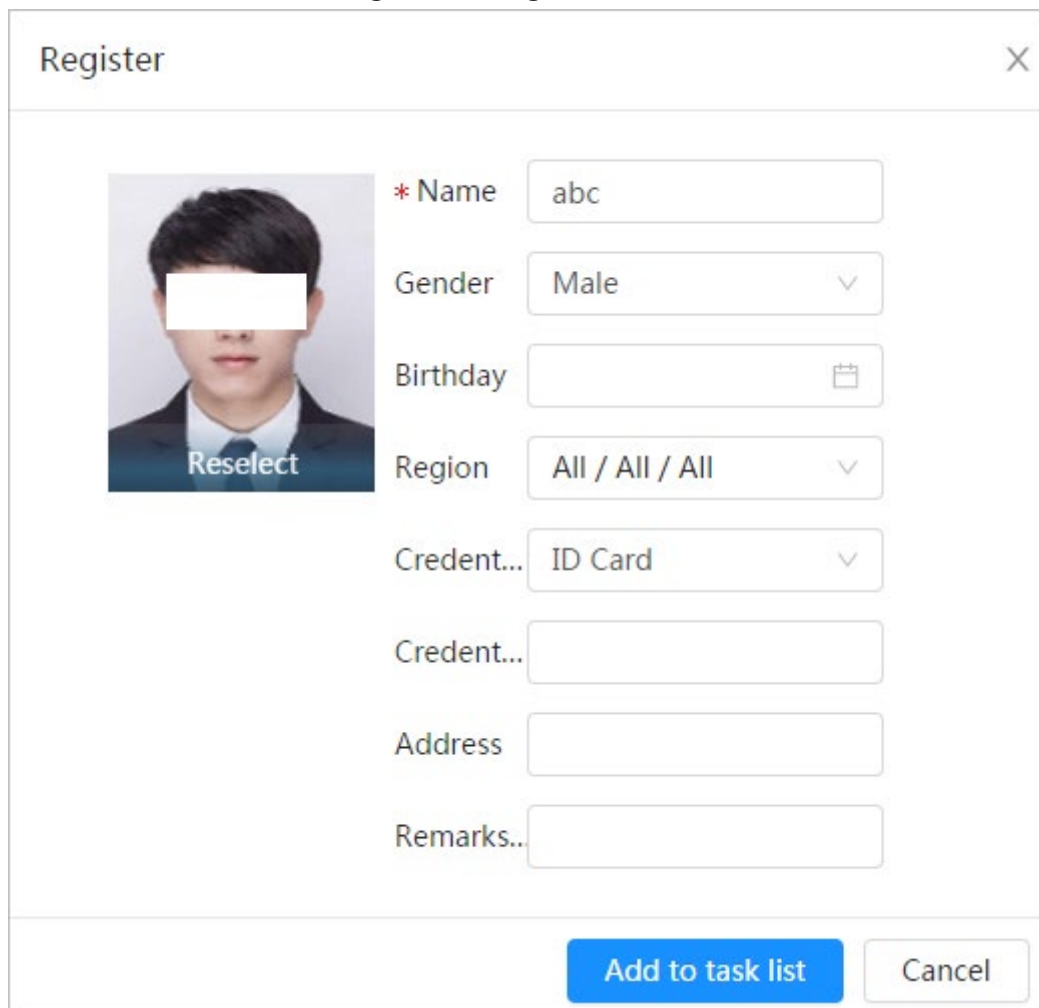
**Step 2** Click Register.

**Step 3** Click Upload, select a face picture to be uploaded, and then click Open.



You can manually select the area for a face. After uploading picture, select a face and click Confirm Screen. When there are multiple faces in a photo, select the target face and click Confirm Screen to save face picture.

Figure 8-11 Register



The screenshot shows a 'Register' dialog box with the following fields and options:

- Name:** abc
- Gender:** Male
- Birthday:** (calendar icon)
- Region:** All / All / All
- Credent...:** ID Card
- Credent...:** (empty)
- Address:** (empty)
- Remarks..:** (empty)

Buttons at the bottom: **Add to task list** (blue) and **Cancel** (white).

**Step 4** Enter the information about face picture according to the actual situation.

**Step 5** Click Add to task list.

**Step 6** Click , and then click Operation.

- If the operation is successful, the system prompts that stored successfully, modeled successfully.
- If adding user fails, the error code is displayed on the page. For details, see Table 8-3. For face modeling operation, see "8.2.2.4 Face Modeling".

Table 8-3 Description of error code

Parameter	Error	Description
0x1134000C	Picture importing error	The picture is too large, and the upper limit is 150K.
0x1134000E		The quality of the added pictures is to the upper limit.
0x11340019		The space of the face database exceeds the upper limit.
1	Picture modeling error	The picture format is not correct. Import the picture in JPG format.
2		No face in the picture or the face is not clear. Change the picture.
3		Multiple faces in the picture. Change the picture.
4		Failed to decode the picture. Change the picture.
5		The picture is not suitable to be imported to the face database. Change the picture.
6		The database error. Restart the camera and model faces again.
7		Fails to get the picture. Import the picture again.
8		System error. Restart the camera and model faces again.

### 8.2.2.2.2 Batch Importing

Import face pictures in batches. Select this way when you need to add a large number of face pictures.

#### Prerequisites

Before importing pictures in batches, name face pictures in a format of "Name#SGender#BDate of Birth#NRegion#TCredentials Type#MID No.jpg" (for example, "John#S1#B1990-01-01#T1#M0000). For naming rules, see Table 8-4.



- **The max. size of a single face picture is 150K, and the resolution is less than 1080p.**

- When naming pictures, name is required, and others are optional.

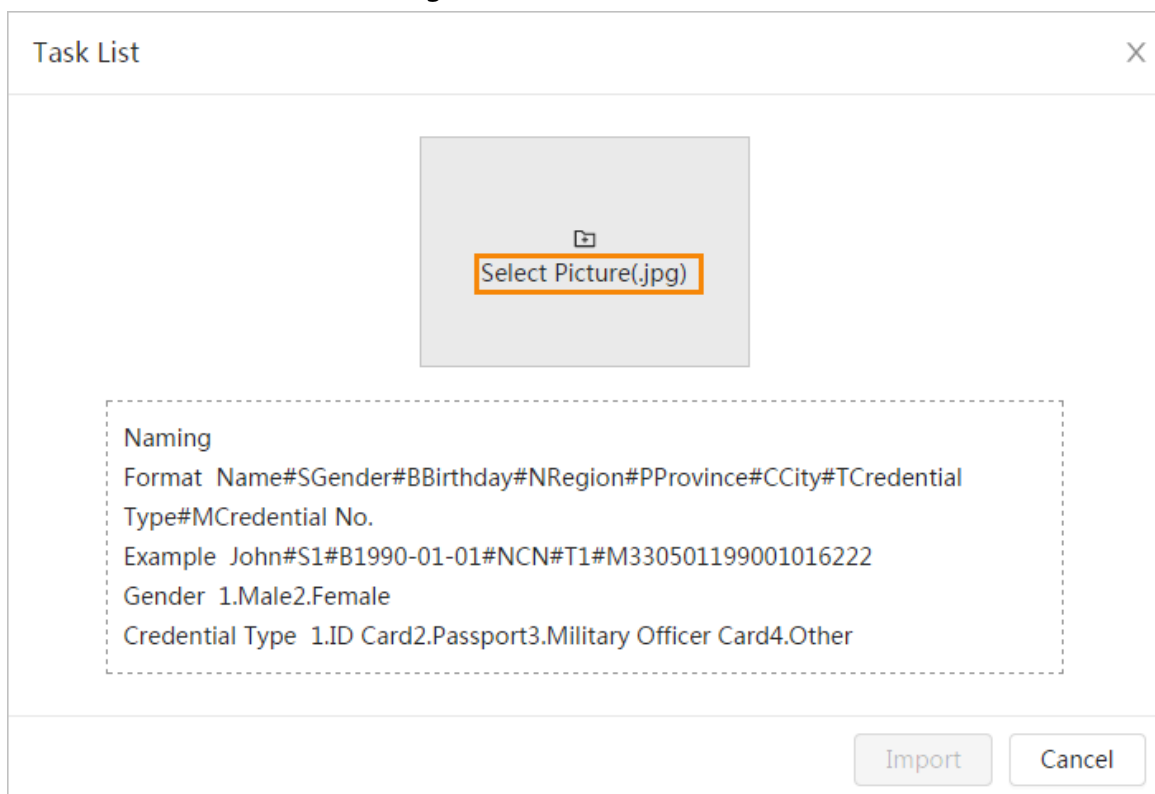
Table 8-4 Description of naming rules for batch import parameters

Parameter	Description
Name	Enter a name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Credentials Type	"1" is ID card and "2" passport.
ID number	Enter ID No.

## Procedure

- Step 1** On the Face Database Config page, click next to the face database to be configured.
- Step 2** Click Batch Register.
- Step 3** Click Select Picture, and select storage path of the file.

Figure 8-12 Task list



- Step 4** Click Import to import the face pictures.  
After the importing is completed, the result will be displayed.
  - If the picture is imported successfully, click Next to do modeling operation.
  - If the picture importing failed, click Query to view the details of the pictures and error code. For details, see Table 8-3. Click Export to export the error details.
- Step 5** Click Next to do modeling operation.  
The modeling result is displayed. If modeling failed, click Query and the failure details will be displayed in the list. Point to the modeling status to view the details. Then you can change picture according to the failure reason. For modeling details,

see "8.2.2.4 Face Modeling".

### 8.2.2.3 Managing Face Picture

Add face pictures to face database, and then manage and maintain face pictures to ensure correct information.

#### 8.2.2.3.1 Editing Face Information

##### Procedure



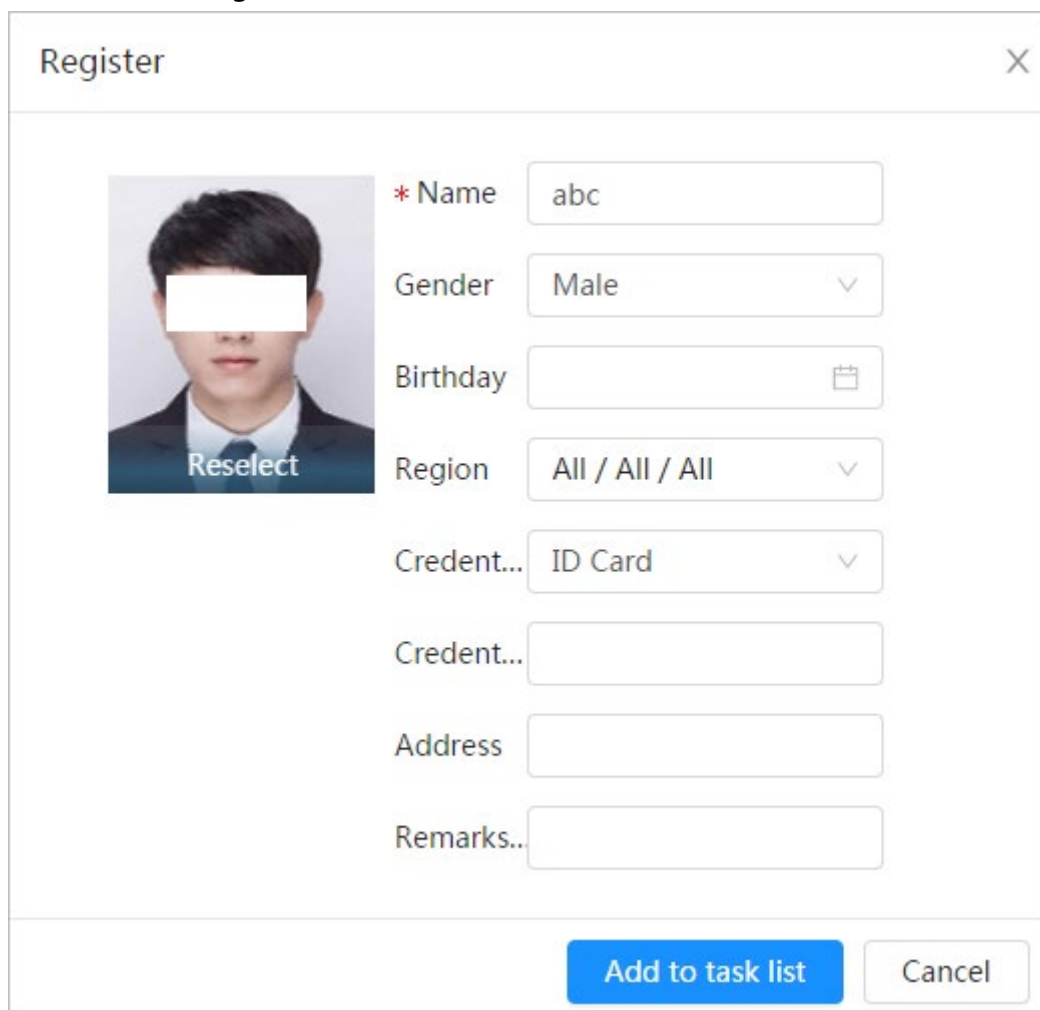

- Step 1** On the Face Database Config page, click  next to the face database to be configured.
- Step 2** Click Query, set the criteria as needed, and then click Search.
- Step 3** Select the row where the face picture or the personnel information is located, and then click .
- Step 4** Edit face information according to the actual need. Click Add to task list.


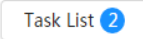
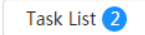
Figure 8-13 Face information modification



- Step 5** Click , and then click Operation.

### 8.2.2.3.2 Deleting Face Picture

On the Face Database Config page, click  next to the face database to be configured. Click Query, set the search criteria as needed, click Search, select the face information that needs to be deleted and delete it.

- **Single delete:** Select the row where the face picture or the personnel information is located, and click  to delete the face picture.
- **Batch delete:** Select  at the upper-right corner of the face picture or  of the row where the personnel information is located. Select the information, click Delete, then click , and then click Operation to delete the selected face pictures.
- **Delete all:** When viewing face pictures in a list, click  of the row where the serial number is located; when viewing by thumbnail, select All to select all face pictures. Click Delete, then click , and then click Operation to delete all face pictures.

### 8.2.2.4 Face Modeling

Face modeling extracts face picture information and imports the information to a database to establish relevant face feature models. Through this function, the Face Detection+ and other intelligent detections can be realized.



- **The more the selected face pictures are, the longer time the face modeling takes. Please wait patiently.**
- **During modeling, some intelligent detection functions (such as Face Detection+) are not available temporarily, and will be available after modeling.**

### Procedure

**Step 1** On the Face Database Config page, click  next to the face database to be configured.

**Step 2** Start modeling.

- **Selective modeling.**

If there are many face pictures in the face database, you can set search criteria to select the pictures that need to be modeled.

1. Set the search criteria, and click Search.
2. Select the face pictures to be modeled.
3. Click Modeling.

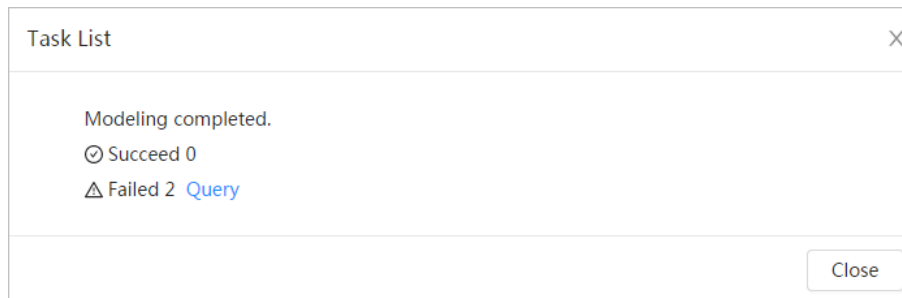
- **All modeling.**

Click Modeling All to complete modeling of all face pictures in the face database.

**Step 3** View the modeling result.

When the modeling failed, Query will be displayed in the result page. Click Query to view the details.

Figure 8-14 Failed modeling



Click  to view the face picture in list format; click  to view the face picture in thumbnail format.

- When the modeling status is Valid in the list or is displayed at the lower-left corner of the thumbnail, it means the modeling succeeded.
- When the modeling status is Invalid in the list or is displayed at the lower-left corner of the thumbnail, it means the modeling failed. Point to the modeling status in the list to view the details of the failure. Change the pictures according to the details.

## 8.2.3 Setting Arm Alarm

When Face Detection+ succeeded or failed, the device links alarm out.

### Procedure

**Step 1** On the Face Database Config page, click  next to the face database to be configured.

**Step 2** Arm face database.

- 1) Click  next to Arm to enable the face database arming.

The snapshot will be compared to the pictures in the armed face database.

- 2) Set the similarity.

The detected face matches the face database only when the similarity between the detected face and the face feature in face database reaches the configured similarity threshold. After successful match, the comparison result is displayed on the Live page.

**Figure 8-15 Arm alarm**

Arm Alarm
✕

Name

---

Arm

Similarity –  + 82

Time Plan

---

Local

Alarm-out Port

Alarm Mode  ⓘ

Post-Alarm  sec. (1-300)

---

Report Mode  ⓘ

General Mode	Stranger Mode
Record <input type="checkbox"/>	Record <input type="checkbox"/>
Post-Record <input type="text" value="10"/> sec. (10-300)	Post-Record <input type="text" value="10"/> sec. (10-300)
Audio Linkage <input type="checkbox"/>	Audio Linkage <input type="checkbox"/>
Send Email <input type="checkbox"/>	Send Email <input type="checkbox"/>
Snapshot <input checked="" type="checkbox"/>	Snapshot <input checked="" type="checkbox"/>

**Figure 8-16 Arm alarm (all people)**

Arm Alarm
✕

Name

---

Arm

Similarity –  + 82

Time Plan

---

Local

Alarm-out Port

Alarm Mode  ⓘ

Post-Alarm  sec. (1-300)

---

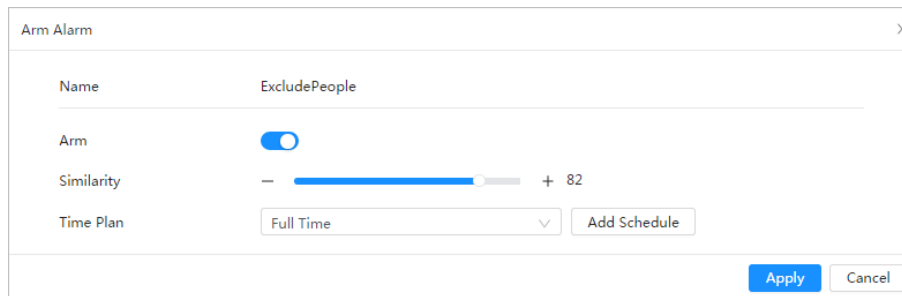
Report Mode  ⓘ

General Mode	Stranger Mode
Record <input type="checkbox"/>	Record <input type="checkbox"/>
Post-Record <input type="text" value="10"/> sec. (10-300)	Post-Record <input type="text" value="10"/> sec. (10-300)
Audio Linkage <input type="checkbox"/>	Audio Linkage <input type="checkbox"/>
Send Email <input type="checkbox"/>	Send Email <input type="checkbox"/>
Snapshot <input checked="" type="checkbox"/>	Snapshot <input checked="" type="checkbox"/>

Auto Delete

Delete Old Files  day(s) ago (1-30)

Figure 8-17 Arm alarm (exclude people)



**Step 3** Set arming periods.

**Step 4** Click  next to Local to enable local alarm output.

Table 8-5 Local alarm output

Parameter	Description
Alarm-out Port	For the device with multiple alarm-out channels, select the channels as needed.
Alarm Mode	<ul style="list-style-type: none"> <li>• <b>All:</b> No matter the comparison result of the detected face and that in the face database, the camera links alarm out.</li> <li>• <b>General:</b> The camera links alarm out when the detected face matches that in the face database, the camera links alarm out.</li> <li>• <b>Stranger:</b> The camera links alarm out when the detected face fails to match that in the face database, the camera links alarm out.</li> <li>• <b>Select none:</b> the camera does not link alarm out no matter the comparison result of the detected face and that in the face database, the camera does not link alarm out.</li> </ul>
Post-Alarm	When alarm delay is configured, alarm continues for the defined period after the alarm ends.

**Step 5** Select the report mode and alarm linkage action.

- There are four report modes:
  - ◇ **All:** The camera reports events no matter the comparison result of the detected face and that in the face database, and then configure the linkage action in General Mode and Stranger Mode.
  - ◇ **General:** The camera reports events when the detected face matches that in the face database, and then configure the linkage action in General Mode.
  - ◇ **Stranger:** The camera reports events when the detected face fails to match that in the face database, and then configure the linkage action in Stranger Mode.
  - ◇ **Select none:** The camera does not report events no matter the comparison result of the detected face and that in the face database. You do not need to configure any linkage action.
- Set alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

**Step 6** Enable Auto Delete, set the time.

When the database is full, the camera will delete the old files according to the configured time, and it is 7 days by default.





This function is only available on the all people database.

**Step 7** Click Apply.

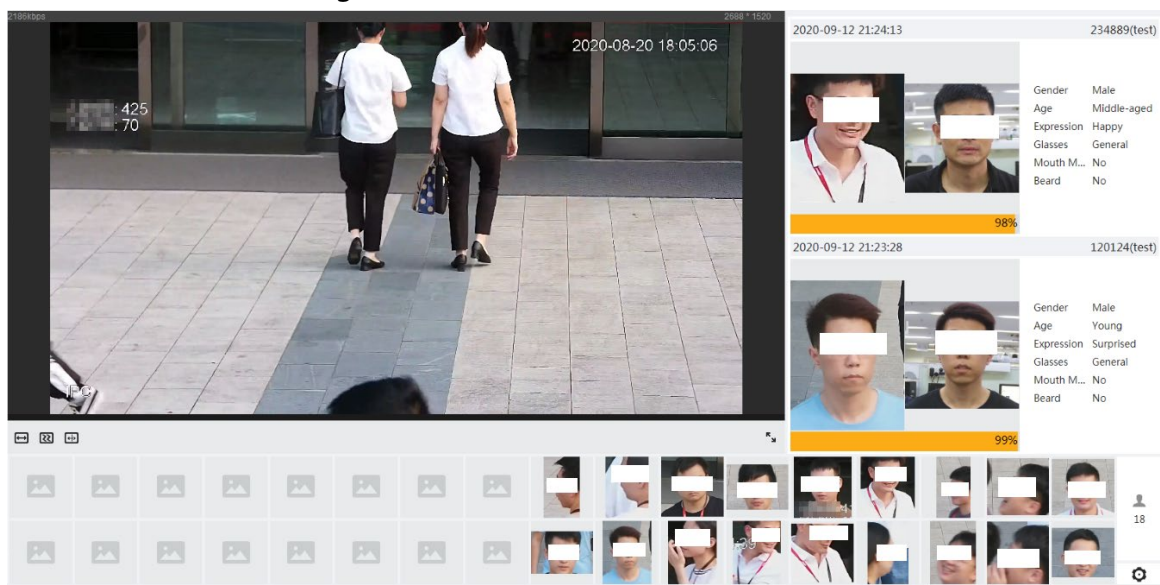
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## 8.2.4 Viewing Face Detection+ Result

Select Face Mode from the display mode drop-down list at the upper-right corner.

- The live image is displayed at the left side, and the captured face pictures and attribute information are displayed at the right side. When the recognition is successful, the captured face pictures, pictures in the database and the similarity of the face pictures and pictures in the database are displayed at the right side; the snapshot counting result and thumbnails are displayed at the bottom of the live image.
- Click to set the attributes. For details, see "7.5 Display Mode".

Figure 8-18 Face Detection+ result



## 8.3 Setting Face Detection

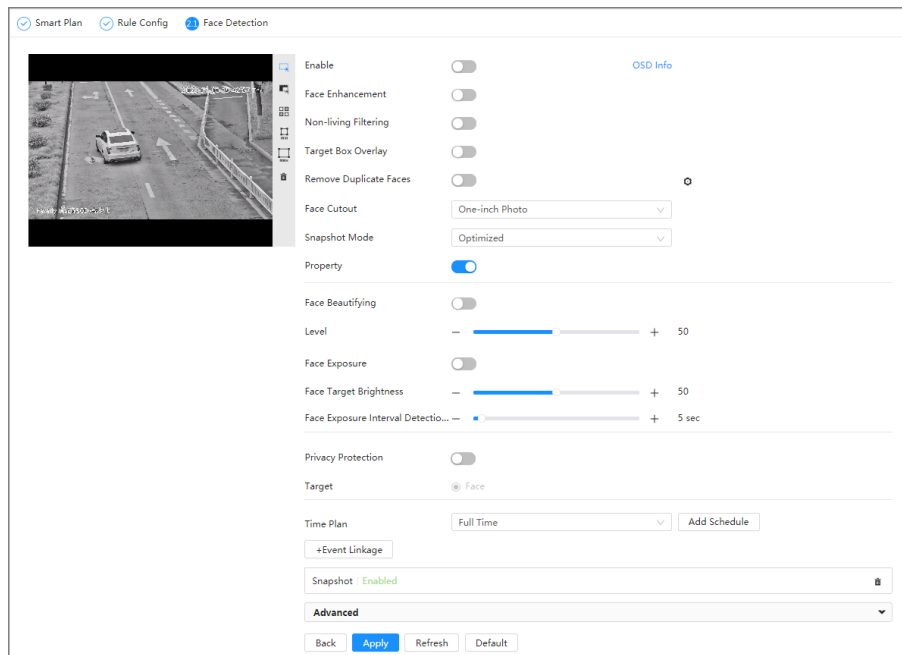
When a face is detected in the detection area, the system performs an alarm linkage.

### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Face Detection to enable face detection of the corresponding channel, and then click Next.

Figure 8-19 Face detection



**Step 3** Click  next to Enable to enable the face detection function.






**Step 4** (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.

- Click to draw a face detection area in the image. The detection area is the whole image by default.
- Click to draw an exclusion area for face detection in the image.
- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

**Step 5** Set parameters.

Table 8-6 Description of face detection parameters

Parameter	Description
OSD Info	Click OSD Info, and the Overlay page is displayed, and then enable the face statistics function. The number of detected faces is displayed on the Live page. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click <input type="checkbox"/> to enable face enhancement, and it can preferably guarantee clear face with low stream.
Non-living filtering	Filter non-living faces in the image, such as a face picture.
Target Box Overlay	Click <input type="checkbox"/> to enable the function, and then you can add a bounding box to the face in the captured picture to highlight the face.  The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".

Parameter	Description
Remove Duplicate Faces	<p>During the configured period, the duplicate faces are displayed only once to avoid repeated counting. Click  next to this function to configure the time and precision.</p> <ul style="list-style-type: none"> <li>• <b>Time:</b> In the configured time, Remove Duplicate Faces is enabled.</li> <li>• <b>Precision:</b> The higher the level, the more sensitive the device will be to remove duplicate faces.</li> </ul>
Face Cutout	<p>Set a range for matting face image, including face, one-inch photo and custom.</p> <p>When selecting Custom, click , configure the parameters on the prompt page, and then click Apply.</p> <ul style="list-style-type: none"> <li>• <b>Customized width:</b> Set snapshot width; enter the times of the original face width. It ranges from 1–5.</li> <li>• <b>Customized face height:</b> Set face height in snapshot; enter the times of the original face height. It ranges from 1–2.</li> <li>• <b>Customized body height:</b> Set body height: in snapshot; enter the times of the original body height. It ranges from 0–4. When the value is 0, it means to cutout the face image only.</li> </ul>
Snapshot Mode	<ul style="list-style-type: none"> <li>• <b>Real-time:</b> Capture the picture immediately after the camera detects face.</li> <li>• <b>Optimized:</b> Capture the clearest picture within the configured time after the camera detects face.</li> <li>• <b>Quality Priority:</b> Repeatedly compare the captured face to the faces in the armed face database, and capture the most similar face image and send the event. We recommend you use this mode in access control scene.</li> </ul> <p></p> <p>Click Advanced to set the optimized time.</p>
Property	Click  next to Property to enable the properties display.
Face Beautifying	Enable Face Beautifying to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Click  next to Face Exposure. When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.
Privacy Protection	Enable this function, and the faces will be blurred by mosaic when they are detected.

Parameter	Description
Advanced	<ul style="list-style-type: none"> <li>• <b>Snapshot Angle Filter:</b> Set snapshot angle to be filtered during the face detection.</li> <li>• <b>Snapshot Sensitivity:</b> Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>• <b>Optimized Time:</b> Set a period to capture the clearest picture after the camera detects face.</li> </ul>

**Step 6** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

**Step 7** Click Apply.

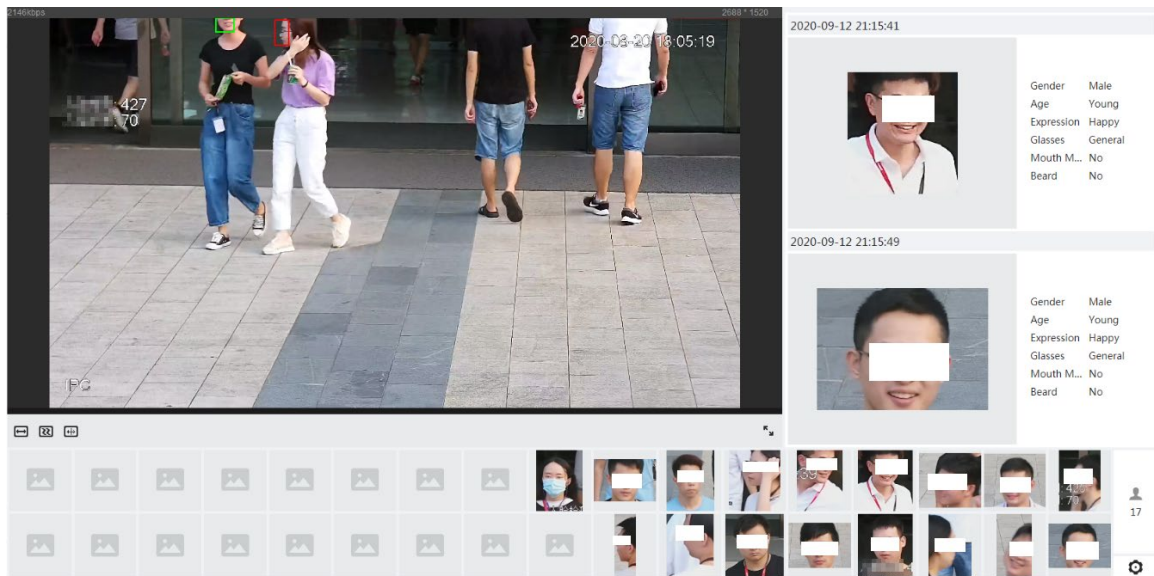
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## Result

The face detection result is displayed on the live page.

- The face pictures snapped in real time and their attribute information are displayed.
- Click a face picture in the display area, and the details are displayed.

Figure 8-20 Face detection result



## 8.4 Setting IVS

This section introduces scene selection requirements, rule configuration, and global configuration for IVS (intelligent video system).

Basic requirements on scene selection are as follows.

- The target should occupy no more than 10% of the whole image.
- The target size in the image should be no less than 10 × 10 pixels. The size of abandoned object in the image should be no less than 15 × 15 pixels (CIF image). The target height and width should no more than a third of the image height and width. The recommended target height is 10% of the image height.
- The brightness difference of the target and the background should be no less than 10 gray

levels.

- The target should be continuously present in the image for no less than two seconds, and the moving distance of the target should be larger than its width and no less than 15 pixels (CIF image) at the same time.
- Reduce the complexity of surveillance scene as much as you can. Intelligent analysis functions are not recommended to be used in scene with dense targets and frequent illumination change.
- Avoid areas such as glass, reflective ground, water surface, and areas interfered by branch, shadow and mosquito. Avoid backlight scene and direct light.

## 8.4.1 Global Configuration

Set global rules for IVS, including anti-disturb, depth of field calibration, and valid motion parameter for targets.

### Calibration Purpose

Determine corresponding relationship between 2D image captured by the camera and 3D actual object according to one horizontal ruler and three vertical rulers calibrated by the user and the corresponding actual distance.

### Applicable Scene

- Medium or distant view with installation height of more than three meters. Scenes with parallel view or ceiling-mounted are not supported.
- Calibrate horizontal plane, not vertical walls or sloping surfaces.
- This function is not applicable to scenes with distorted view, such as the distorted views captured by super wide-angle or fisheye camera.

### Notes

- **Calibration Drawing**
  - ◇ **Calibration area:** The calibration area drawn should be on one horizontal plane.
  - ◇ **Vertical ruler:** The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such as vehicle parked at roadside or road lamp poles. Arrange three persons to draw at each of the three positions in the monitoring scene.
  - ◇ **Horizontal ruler:** Select reference object with known length on the ground, such as sign on the road, or use a tape to measure the actual length.
- **Calibration Verification**

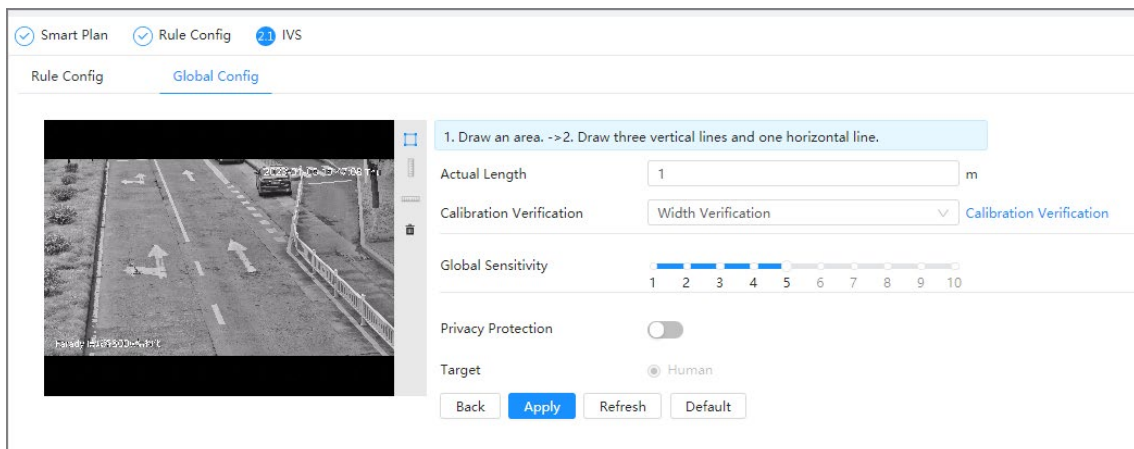
After setting the ruler, draw a straight line on the image, check the estimated value of the straight line, and then compare this value with the value measured in the actual scene to verify calibration accuracy. In case of major difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

### Procedure

1. Select Analytics+ > Smart Plan.

2. Click  next to IVS to enable IVS of the corresponding channel, and then click Next.
3. Click the Global Config tab.

Figure 8-21 Global configuration of IVS



4. Set calibration area and ruler.
  - a. Click and draw a calibration area in the image, and right-click to finish the drawing.
  - b. Click the ruler icon to draw one horizontal ruler and three vertical rulers in the calibration area.
    - indicates vertical ruler, and indicates horizontal ruler
    - Select an added ruler, and click to delete the ruler.
5. Set the global sensitivity.
 

Adjust the filter sensitivity. With higher value, it is easier to trigger an alarm when low-contrast object and small object are captured, and the false detection rate is higher.
6. Enable Privacy Protection. After enabled, the human detected will be blurred by mosaic.
7. Click Apply.

## Result

1. Select the verification type, and then click Calibration Verification.
 

To verify vertical ruler and horizontal ruler, respectively select Height Verification and Width Verification.
2. Draw a straight line in the image to verify whether the rulers are correctly set.
 

In case of big difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

## 8.4.2 Rule Configuration

Set rules for IVS, including cross fence detection, tripwire, intrusion, abandoned object, moving object, fast moving, parking detection, crowd gathering, and loitering detection.

### Prerequisites

- Select Analytics+ > Smart Plan, and enable IVS.
- Select Analytics+ > Smart Plan > Global Config to finish global configuration.

### Background Information

For the functions and applications of the rules, see Table 8-7.

Table 8-7 Description of IVS functions

Rule	Description	Applicable Scene
Tripwire	When the target crosses tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Intrusion	When the target enters, leaves, or appears in the detection area, an alarm is triggered, and the system performs configured alarm linkages.	
Abandoned object	When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> <li>• Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying.</li> <li>• In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.</li> </ul>
Missing object	When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs configured alarm linkages.	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> <li>• Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying.</li> <li>• In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.</li> </ul>



Rule	Description	Applicable Scene
Fast moving	When the motion speed is higher than the configured speed, an alarm is triggered, and then the system performs configured alarm linkages.	Scene with sparse targets and less occlusion. The camera should be installed right above the monitoring area. The light direction should be vertical to the motion direction.
Parking detection	When the target stays over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.
Crowd gathering	When the crowd gathers or the crowd density is large, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. It is not suitable for short-distance view analysis.
Loitering detection	When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs configured alarm linkages. After alarm is triggered, if the target stays in the area within the time interval of alarm, then alarm will be triggered again.	Scenes such as park and hall.

Configure IVS rules. This section takes tripwire as an example.

## Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to IVS to enable IVS of the corresponding channel, and then click Next.

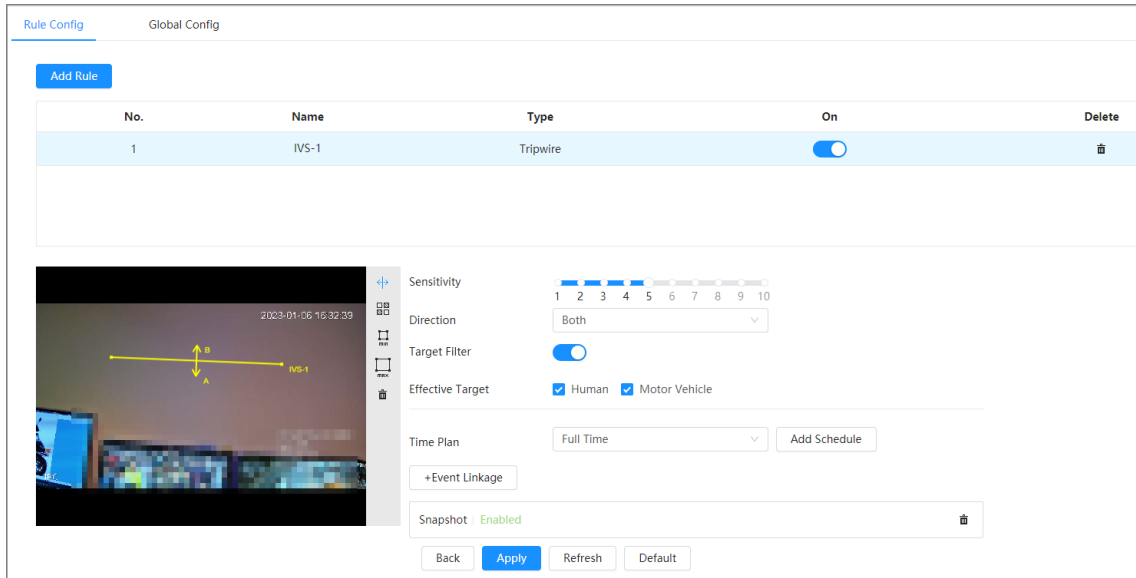
**Step 3** Click the Rule Config tab.

**Step 4** Click Add Rule on the Rule Config page, and then select Tripwire from the drop-down list.

Double-click the name, and you can edit the rule name; the rule is enabled by default.



Figure 8-22 Tripwire



**Step 5** Click to draw rule line in the image. Right-click to finish drawing. For requirements of drawing rules, see Table 8-7. After drawing rules, drag corners of the detection area to adjust the area range.

Table 8-8 Description of IVS analysis



Rule	Description
Tripwire	Draw a detection line.
Intrusion	Draw a detection area.
Abandoned object	<ul style="list-style-type: none"> <li>During the detection of abandoned object, the alarm is also triggered if pedestrian or vehicle stays for a long time. If the abandoned object is smaller than pedestrian and vehicle, set the target size to filter pedestrian and vehicle or properly extend the duration to avoid false alarm triggered by transient staying of pedestrian.</li> <li>During the detection of crowd gathering, false alarm might be triggered by low installation height, large percentage of single person in an image or obvious target occlusion, continuous shaking of the camera, shaking of leaves and tree shade, frequent opening or closing of retractable door, or dense traffic or people flow.</li> </ul>
Missing object	
Fast moving	
Parking detection	
Crowd gathering	
Loitering detection	

**Step 6** (Optional) Click other icons at the right side of the image to filter targets in the image.

- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

**Step 7** Set rule parameters for IVS.

Table 8-9 Description of IVS parameters

Parameter	Description
Direction	Set the direction of rule detection. <ul style="list-style-type: none"> <li>When setting tripwire, select A-&gt;B, B-&gt;A, or A&lt;-&gt;B.</li> <li>When setting intrusion, select Enter, Exit, or Both.</li> </ul>
Action	When setting intrusion action, select Appears, Cross or Inside.  <p>Inside and appears/cross cannot work at the same time.</p>
Target Filter	Click <input type="checkbox"/> to enable this function. <ul style="list-style-type: none"> <li>When you select Human as the alarm target, an alarm will be triggered when the system detects that persons trigger the rule.</li> <li>When you select Motor Vehicle as the alarm target, alarm will be triggered when the system detects that vehicle triggers the rule.</li> </ul>
Duration	<ul style="list-style-type: none"> <li>For abandoned object, the duration is the shortest time for triggering an alarm after an object is abandoned.</li> <li>For missing object, the duration is the shortest time for triggering an alarm after an object is missing.</li> <li>For parking detection, crowd gathering, or loitering detection, the duration is the shortest time for triggering an alarm after an object appears in the area.</li> </ul>
Sensitivity	When the sensitivity is high, detection becomes easier, but the number of false detections increases.  <p>Missing Object, Abandoned Object and Loitering Detection do not support this function.</p>

**Step 8** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".  
Click + Event Linkage to set the linkage action.

**Step 9** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## 8.5 Setting Smart Object Detection

This section introduces scene selection requirements, rule configuration, and global configuration for smart object detection.

Basic requirements on scene selection are as follows.

- The target should occupy no more than 10% of the whole image.
- The target size in the image should be no less than 10 × 10 pixels. The size of abandoned object in the image should be no less than 15 × 15 pixels (CIF image). The target height and width should no more than a third of the image height and width. The recommended

target height is 10% of the image height.

- The brightness difference of the target and the background should be no less than 10 gray levels.
- The target should be continuously present in the image for no less than two seconds, and the moving distance of the target should be larger than its width and no less than 15 pixels (CIF image) at the same time.
- Reduce the complexity of surveillance scene as much as you can. Intelligent analysis functions are not recommended to be used in scene with dense targets and frequent illumination change.
- Avoid areas such as glass, reflective ground, water surface, and areas interfered by branch, shadow and mosquito. Avoid backlight scene and direct light.

## 8.5.1 Global Configuration

### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to Smart Object Detection, and then click Next.
- Step 3** Click the Global Config tab.
- Step 4** Turn on Independent Object Detection.
- Step 5** Click Apply.

## 8.5.2 Rule Configuration

### Prerequisites

You have configured the global config in Smart Object Detection.

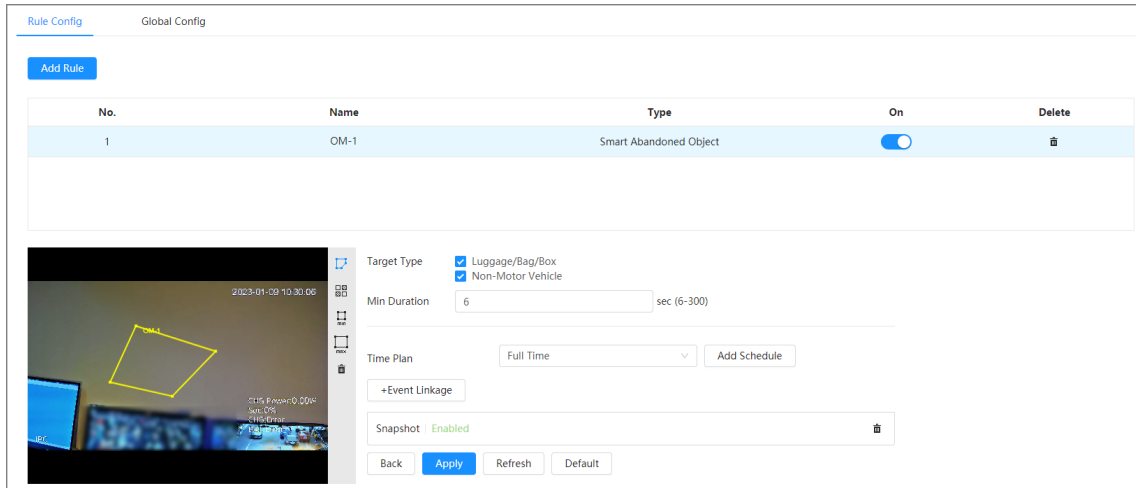
### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to Smart Object Detection, and then click Next.
- Step 3** Click the Rule Config tab.
- Step 4** Click Add Rule on the Rule Config page Here we use Smart Abandoned Object as an example.  
Double-click the name, and then you can edit the rule name; the rule is enabled by default.

Table 8-10 Description of smart object detection functions

Rule	Description	Applicable Scene
<b>Smart Abandoned object</b>	<p>When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.</p>	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> <li>• Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying.</li> <li>• In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.</li> </ul>
<b>Smart Missing object</b>	<p>When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs configured alarm linkages.</p>	<p>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> <li>• Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying.</li> <li>• In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.</li> </ul>

Figure 8-23 Smart abandoned object



**Step 5** Click to draw rule area in the image. Right-click to finish drawing.

**Step 6** (Optional) Click other icons at the right side of the image to filter targets in the image.

- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

**Step 7** Set rule parameters for smart object detection.

Table 8-11 Description of smart object detection parameters

Parameter	Description
Target Type	You can select from Luggage/Bag/Box and Non-Motor Vehicle.
Min Duration	<ul style="list-style-type: none"> <li>• For smart abandoned object, the duration is the shortest time for triggering an alarm after an object is abandoned.</li> <li>• For smart missing object, the duration is the shortest time for triggering an alarm after an object is missing.</li> </ul>

**Step 8** Select time plan, and then Set arming periods and alarm linkage action, and then click + Event Linkage to set the linkage action.

- If the added time plan cannot meet your requirements, click Add Schedule to add an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Click Event Linkage to add linked event and set linkage parameters. For details, see "6.5.1.2 Alarm Linkage".

**Step 9** Click Apply.

## 8.6 Setting Vehicle Density

Configure rules for vehicle density, including road congestion and parking upper limit, and you can view vehicle statistics through the live page.

### Background Information

Configure rules for traffic congestion and parking upper limit. When the counted vehicle exceeds the configured vehicle number and the congestion time exceeds the configured time, an alarm will be triggered.

### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to Vehicle Density, and then click Next.
- Step 3** Click Add Rule to select rules.

Figure 8-24 Add rules

No.	Name	Type	On	Delete
1	VD-1	Traffic Congestion	<input checked="" type="checkbox"/>	
2	VD-2	Parking Upper Limit	<input checked="" type="checkbox"/>	

- Step 4** (Optional) Click other icons at the right side of the image to draw detection area on the image.
  - Click to draw a detection area in the image. The detection area is the whole image by default.
  - Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
  - Click to delete the detection line.

Repeat step 1-4 to add multiple statistical areas. You can add up to 9 rules at most.

Figure 8-25 Vehicle density (traffic congestion)

No.	Name	Type	On	Delete
1	VD-1	Traffic Congestion	<input checked="" type="checkbox"/>	
2	VD-2	Parking Upper Limit	<input checked="" type="checkbox"/>	

Repeat Alarm Time:  sec (0-300)

Vehicle Congestion Alarm:

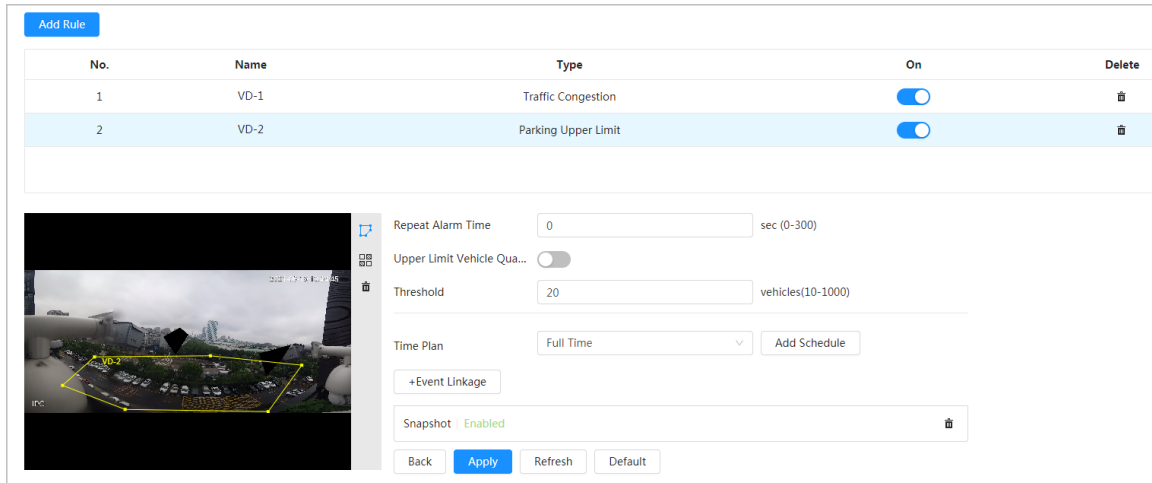
Threshold:  vehicles(10-1000)

Duration:  min (1-100)

Time Plan:

Snapshot: Enabled

Figure 8-26 Vehicle density (parking upper limit)



**Step 5** Set parameters.

Table 8-12 Description of parameters

Parameter		Description
Traffic Congestion	Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.  <b>0 means repeat alarm function disabled.</b>
	Vehicle Congestion Alarm	Enable vehicle congestion alarm to set the upper threshold and duration of vehicles in the area. When the number of vehicles exceeds the threshold and the congestion time exceeds the configured continuous congestion time, an alarm will be triggered.
Parking Upper Limit	Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.  <b>0 means Repeat Alarm function disabled.</b>
	Upper Limit Vehicle Quantity Alarm	Enable upper limit vehicle quantity alarm to set the upper threshold and duration of vehicles in the area. When the number of vehicles exceeds the threshold and the congestion time exceeds the configured continuous congestion time, an alarm will be triggered. The upper threshold of vehicles that trigger an alarm is 20 vehicles by default.

**Step 6** Select time plan and click + Event Linkage.

- If the added time plan cannot meet your requirements, click Add Schedule to add an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Click Event Linkage to add linked event and set linkage parameters. For details, see "6.5.1.2 Alarm Linkage".

**Step 7** Click Apply.

## 8.7 Setting Parking Space

This section introduces rule configuration and global configuration for parking space.

### 8.7.1 Rule Configuration

#### 8.7.1.1 For Parking Space Detection Fisheye WizMind Network Camera

##### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Parking Space Management, and then click Next.

**Step 3** Select the mode.

- 12 parking spaces: Only supports parking space detection.
- 6 parking spaces: Supports both ANPR and parking space detection.



**ANPR is available for customized devices.**

**Step 4** Draw rules.

- **Manual drawing:** Click Draw Rule on the lower-right corner of the image. Click the left mouse button on the image to draw a closed box, and then click the right mouse button to complete the drawing.

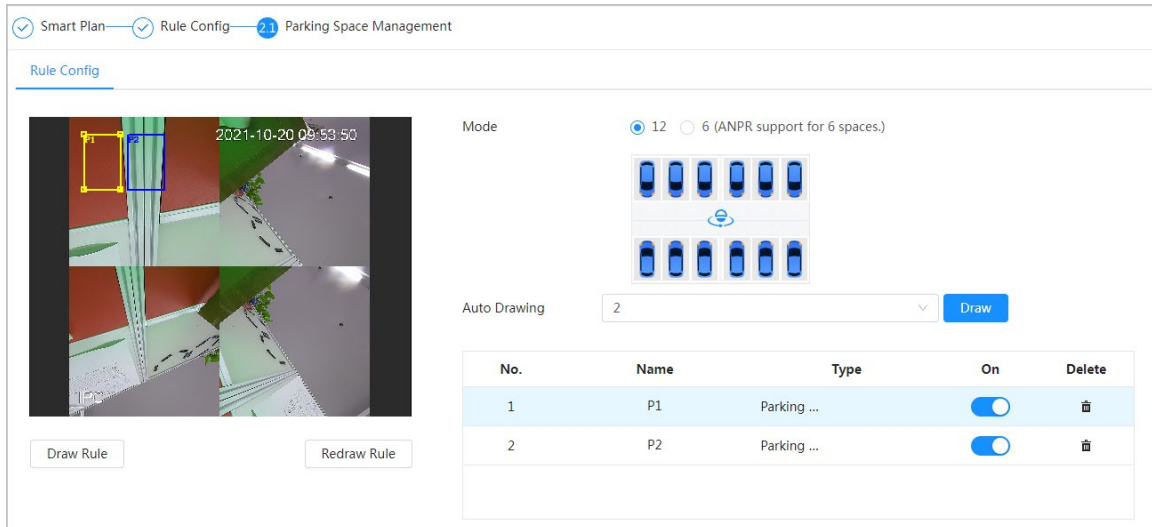


**Click Redraw Rule to redraw the detection area as needed.**

- **Auto drawing:** Select the number from the drop-down list and then click Draw. The added rules will be displayed in the list. Click the text box under Name to edit the rule name. The rule is enabled by default.  
The system automatically shows the number of parking space detection boxes on the image. Click and drag the box according to the actual parking space.

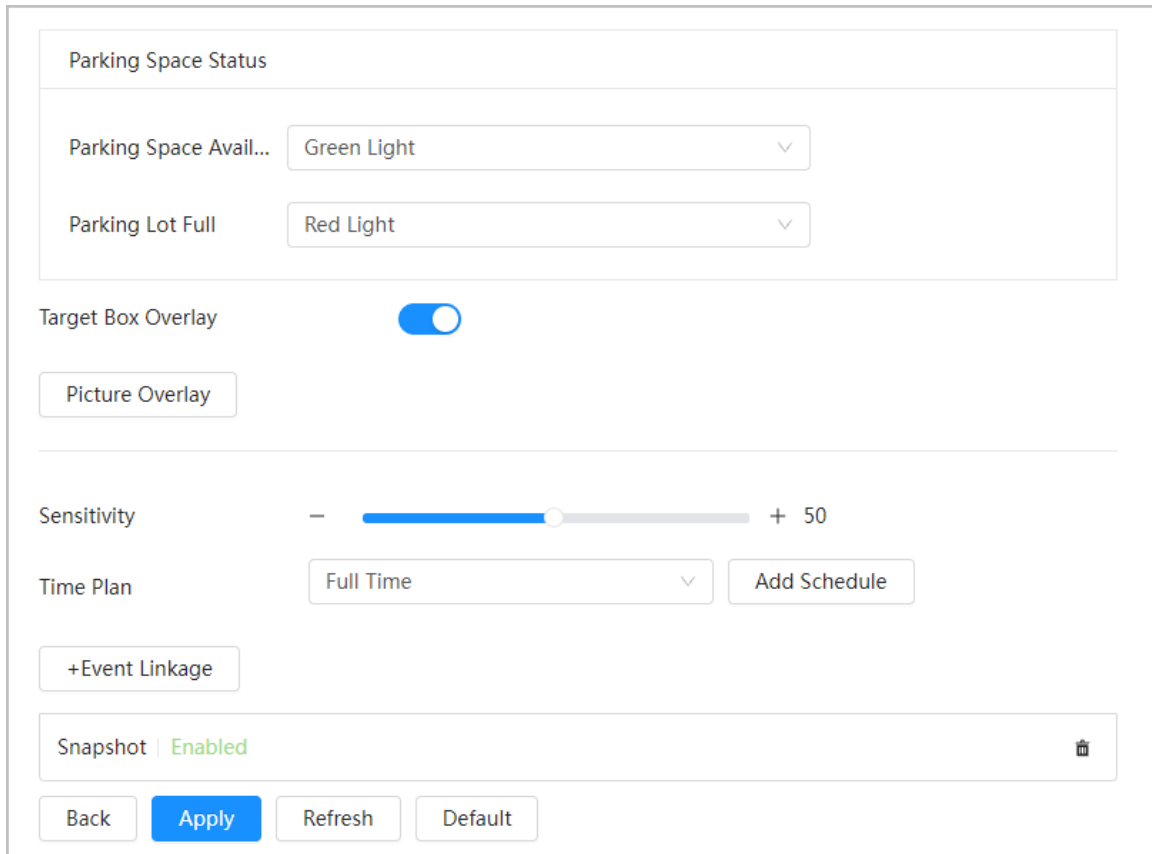


**Figure 8-27 Parking space**



**Step 5** Configure the parameters.

**Figure 8-28 Parking space parameters**



**Table 8-13 Description of parking space parameters**

Parameter	Description
<b>Parking Space Status</b>	<b>Configure the status light for when parking space is available and the parking lot is full. The colors available for both status are: None, red, yellow, green, blue, cyan, pink and white.</b>

Parameter	Description
Target Box Overlay	Overlay the target box on the captured pictures to mark the change of parking space. It is enabled by default. Click Picture Overlay to select the information displayed on the picture. The captured picture is saved in the configured storage path. For the storage path, see "10.4.1 Local Storage".
Sensitivity	Set the sensitivity of parking space detection. When the sensitivity is high, detection becomes easier, but the number of false detections increases. It is 50 by default.

**Step 6** Select time plan and click + Event Linkage.

- If the added time plan does not meet your requirements, click Add Schedule to add an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Click Event Linkage to add linked events and to configure linkage parameters. For details, see "6.5.1.2 Alarm Linkage".

**Step 7** Click Apply.

### 8.7.1.2 For Other Cameras

Set planned or open type for parking space.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Parking Space, and then click Next.

**Step 3** Click the Rule Config tab.

**Step 4** (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.


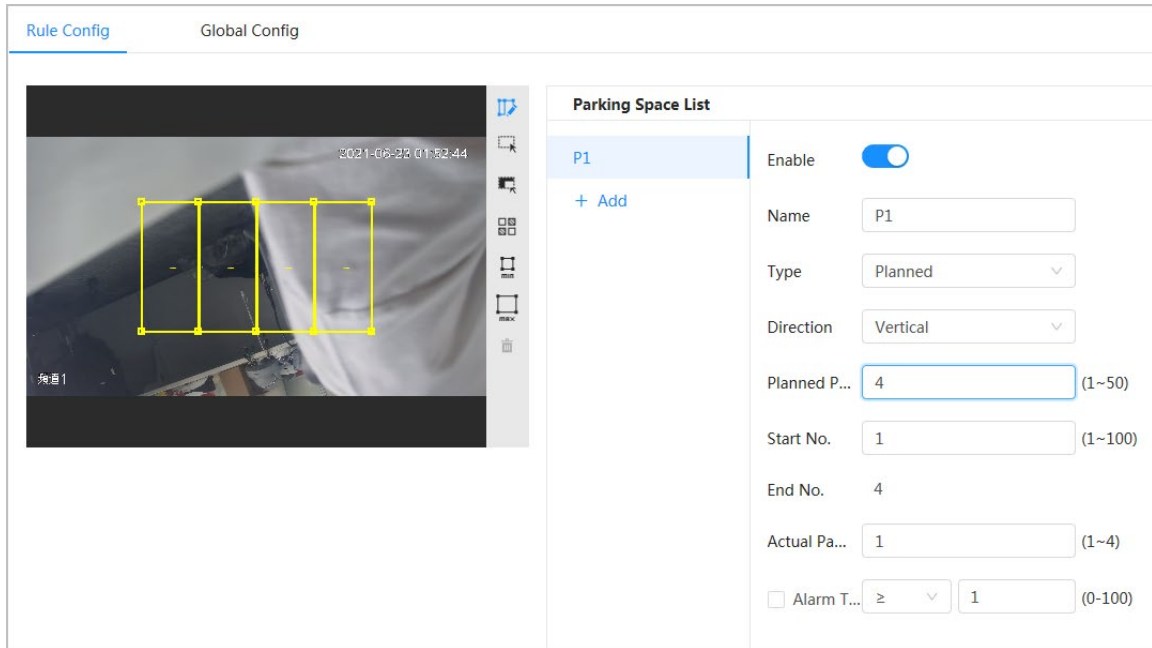
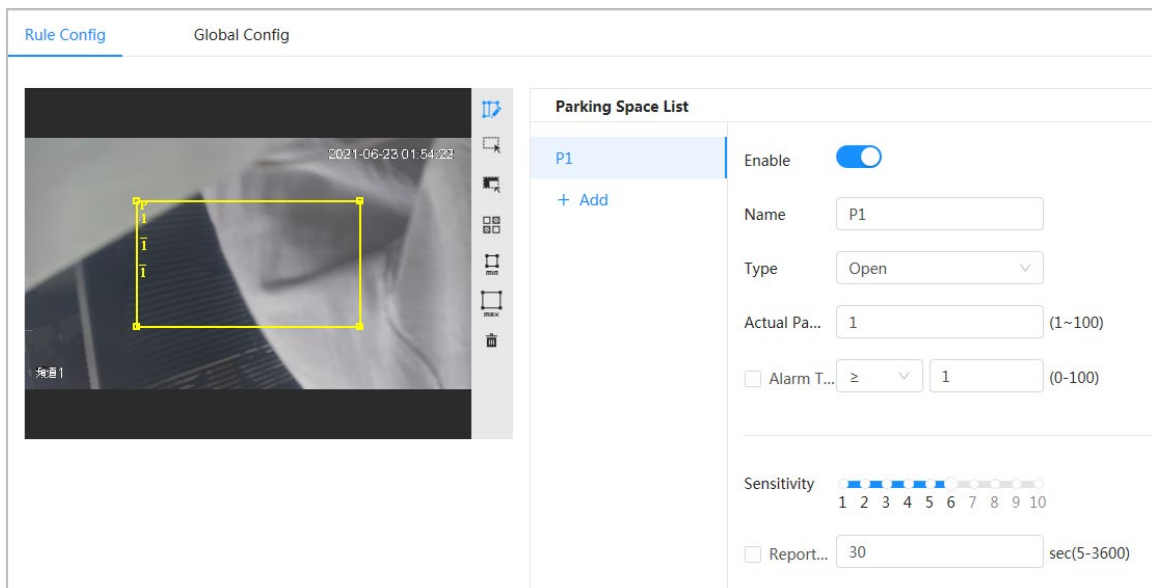
- Click  to draw the rectangle area.
  - ◇ If you select planned parking space, the rectangle area will be divided equally according to the planned parking spaces number that you configured.

Figure 8-29 Rule configuration (1)



◇ If you select open parking space, the rectangle area will not be divided.

Figure 8-30 Rule configuration (2)



- Click to draw a parking space detection area in the image. The detection area is the whole image by default.
- Click to draw an exclusion area for parking space detection in the image.
- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

**Step 5** Select Planned/Open in Type.

- Planned Parking Space

It is used for parking management of planned parking lots (with clearly delineated parking spaces). When there is a car parked in the parking space, a red dot is drawn. And a parking space without a car is drawn a green dot.

Figure 8-31 Planned parking space

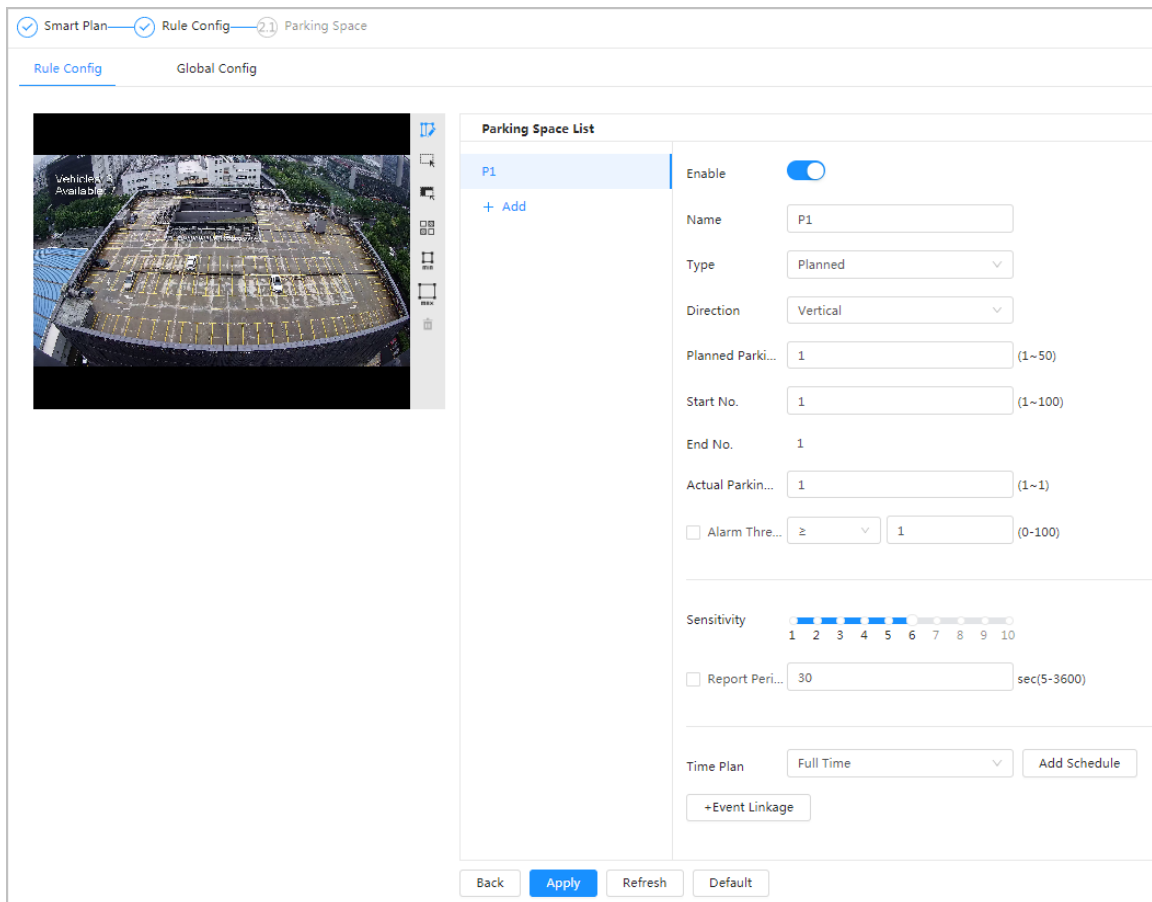


Table 8-14 Description of planned parking space parameters

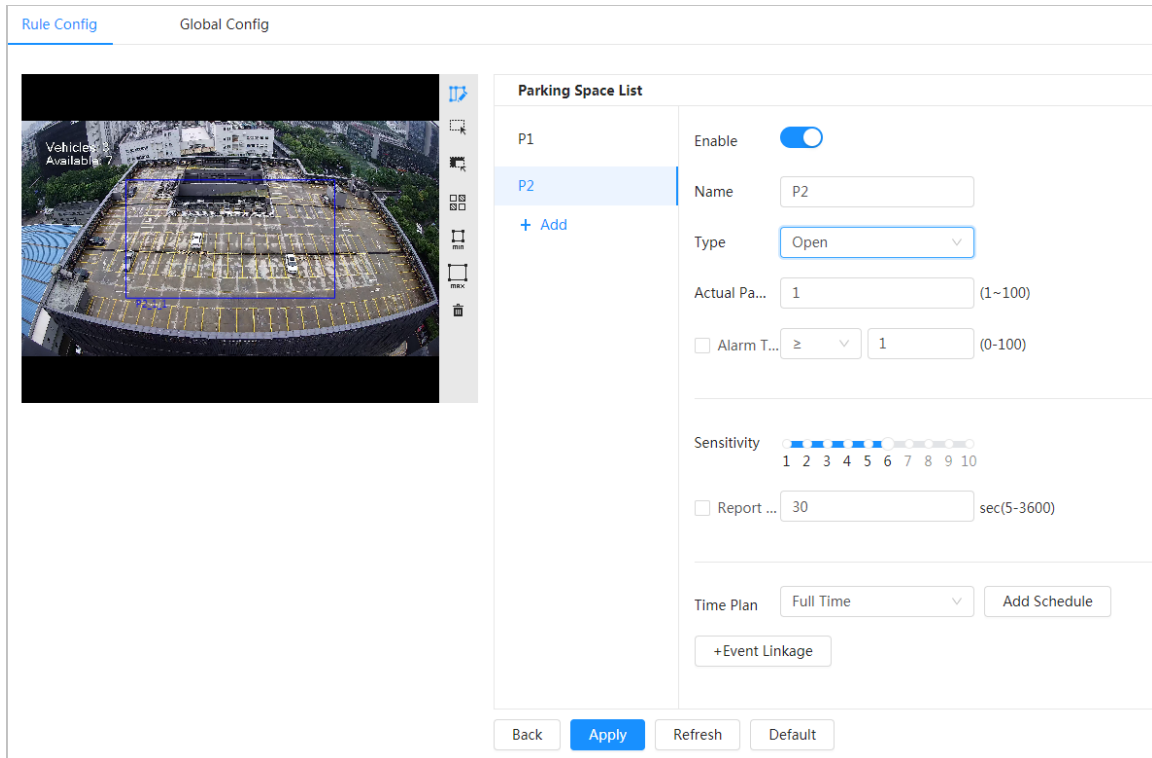
Parameter	Description
Name	Enter the name of the added parking space.
Direction	You can select Vertical or Horizontal direction.
Planned Parking Space	It can be used to divide the initial quadrilateral equally, which is convenient for you to draw the rule box
Start No.	Associates with the name of parking spaces.
End No.	Associates with Planned Parking Space.
Actual Parking Space	It ranges from 1 to the configured value of planned parking space. Actual Parking Space is 1 by default.
Alarm Threshold	You can set it from 0 through 100. When alarm is triggered, the frame of related statistic area will flash red. And the threshold number is 0 by default.
Sensitivity	Adjust the false alarm and miss alarm of the system. And the sensitivity is 6 by default.

Parameter	Description
Report Period	The report period is 30 seconds by default. And you can set it between 5 to 3600 seconds. It will only upload related data but not pictures or videos.

- **Open Parking Space**

It is used for parking management of open parking lots in a large area. When there is a car parked in the parking space, a red dot is drawn. And a parking space without a car will not show any dot.

**Figure 8-32 Open parking space parameters**



**Table 8-15 Description of open parking space parameters**

Parameter	Description
Name	Enter the name of the added parking space.
Actual Parking Space	Actual Parking Space is 1 by default. When you change the planned parking space, the input range would change into 1 - the number of planned parking space.
Alarm Threshold	The threshold number is 0 by default. And you can set it between 0 to 100. When alarm is triggered, the frame of related statistic area will flash in red.
Sensitivity	It is designed to adjust the false alarm and miss alarm of the system. And the sensitivity is 6 by default.
Report Period	The report period is 30 seconds by default. And you can set it between 5 to 3600 seconds. It will only upload related data but not pictures or videos.

**Step 6** Select time plan and click + Event Linkage

- If the added time plan cannot meet your requirements, click Add Schedule to add

an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".

- Click +Event Linkage to add linked event and set linkage parameters. For details, see "6.5.1.2 Alarm Linkage".

**Step 7** Click Apply.

## 8.7.2 Global Configuration

### Procedure

**Step 1** (Optional) Set OSD information.

Click OSD Info, and the Overlay page is displayed, and then enable the Parking Space function. The statistical result is displayed on the Live page For details, see "6.2.2.2.14 Configuring Parking Space".

**Step 2** Adjust confidence level.



**Confidence level is used for algorithm adjustment of false alarm and detection.**

**Step 3** Click Apply.

## 8.8 Setting Video Analytics

Classify people, non-motor vehicles and motor vehicles in the captured video, and display the relevant attributes on the live page.

### 8.8.1 Global Configuration

Set the global configuration of video Analytics, including face parameter and scene parameter.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Video Analytics to enable video Analytics of the corresponding channel, and then click Next.

**Step 3** Click the Global Config tab.

**Step 4** Set parameters.

Figure 8-33 Global configuration of video Analytics

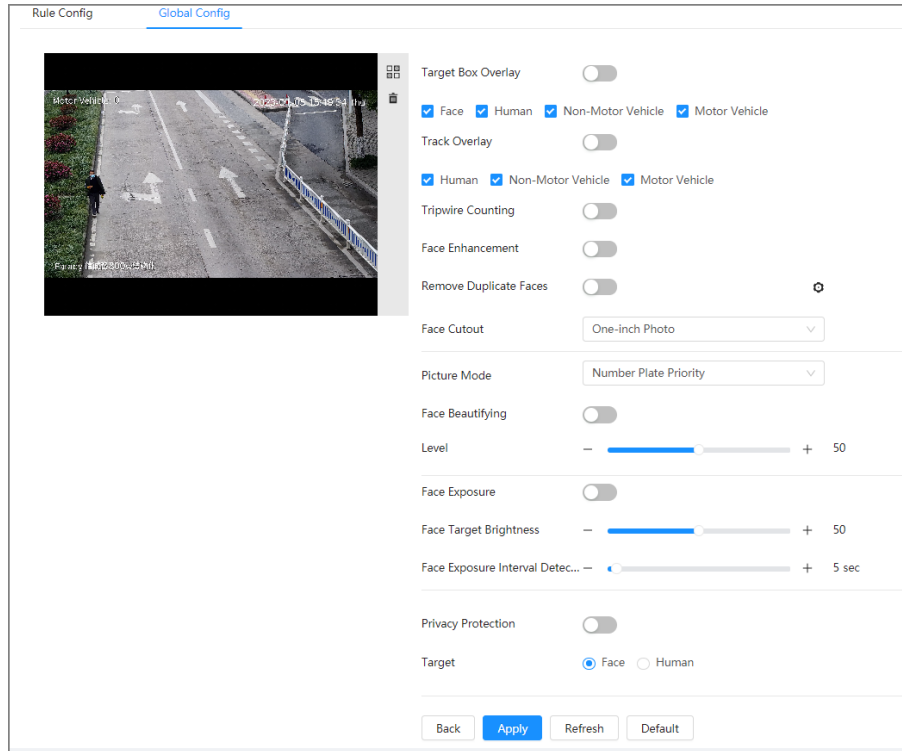


Table 8-16 Description of scene set parameters (video Analytics)

Parameter	Description
Target Overlay	<p>Overlay target box on the captured pictures to mark the target position.</p> <p>Four types of target boxes are supported. Select the target box as needed.</p> <p>The captured pictures are stored in SD card or the configured storage path. For details, see "6.1 Local".</p>
Tripwire Counting	<p>Enable this function, and set the tripwire direction. The snapshot mode is Tripwire by default, and you cannot change it.  will be displayed beside the image on the Rule Config page. You can draw the rule as needed.</p>
Face Enhancement	<p>Click  next to Face Enhancement to preferably guarantee clear face with low stream.</p>
Remove Duplicate Faces	<p>During the configured period, the face that detected several times is displayed only once, to avoid repeated counting. Click  to set the parameters, and then click Apply.</p> <ul style="list-style-type: none"> <li>• Time: The function is valid within the configured period.</li> <li>• Precision: The larger the value is, the higher the accuracy will be.</li> </ul>
Face Cutout	<p>Set a range for matting face image, including face picture and one-inch picture.</p>
Picture Mode	<p>Set picture mode as Number Plate Priority or Face Priority.</p>
Face Beautifying	<p>Enable Face Beautifying to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.</p>

Parameter	Description
Face Exposure	Enable Face Exposure to make face clearer by adjusting lens aperture and shutter.
Target Face Brightness	Set the face target brightness, and it is 50 by default.
Face Exposure Interval Detection Time	Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.
Privacy Protection	Enable this function, and then the selected targets (face or human) will be blurred by mosaic when they are detected.

**Step 5** Click Apply.

## 8.8.2 Rule Configuration

Set the detection scene and rules, including people, non-motor vehicle, and motor vehicle.

### Prerequisites

- Select Analytics+ > Smart Plan, and enable Video Analytics.
- You have configured the parameters on the Global Config page.

### Procedure

**Step 1** Select Analytics+ > Smart Plan.

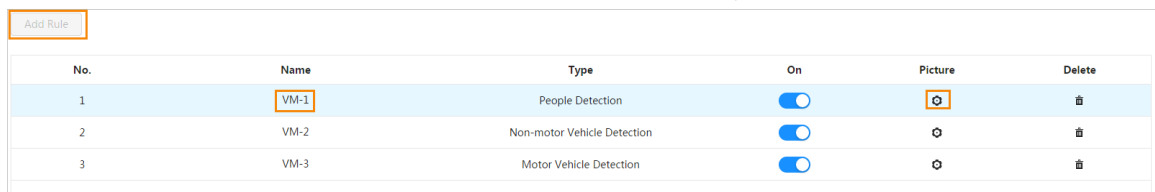
**Step 2** Click  next to Video Analytics, and then click Next.

**Step 3** Click the Rule Config tab.

**Step 4** Click Add Rule to select rules.

The added rules will be displayed in the list. Click the text box under Name to edit the rule name. The rule is enabled by default.

Figure 8-34 Rule configure (video Analytics)



No.	Name	Type	On	Picture	Delete
1	VM-1	People Detection	<input checked="" type="checkbox"/>		
2	VM-2	Non-motor Vehicle Detection	<input checked="" type="checkbox"/>		
3	VM-3	Motor Vehicle Detection	<input checked="" type="checkbox"/>		

**Step 5** Configure Picture.

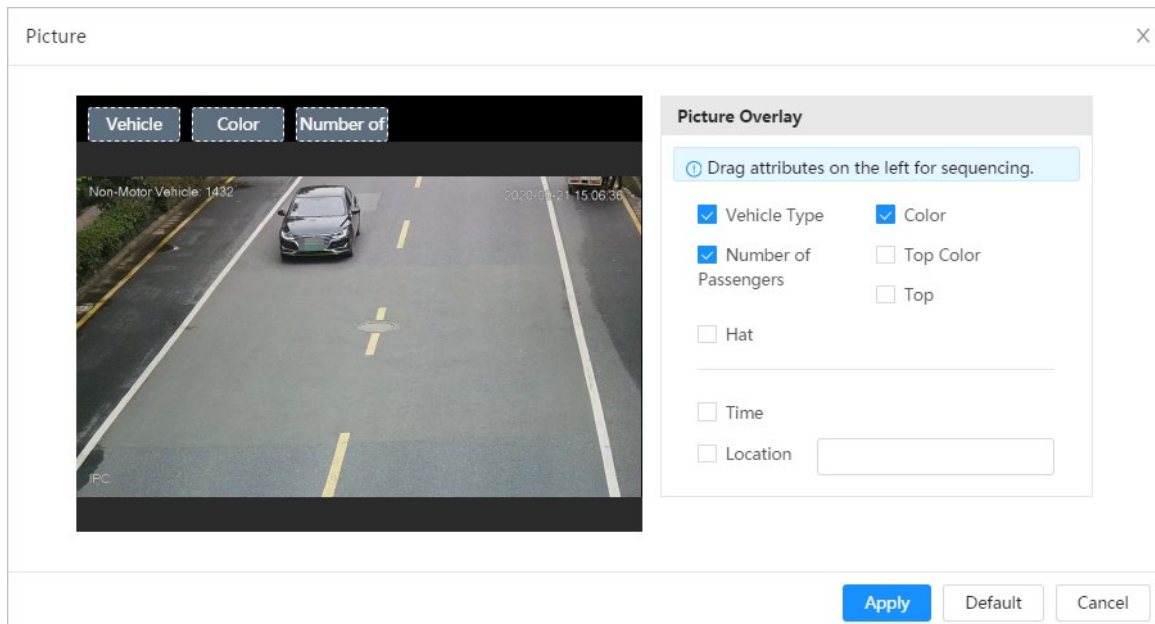
1) Click .

2) Set overlay of motor vehicle, non-motor vehicle and people and the box position.

This section takes the configuration of non-motor vehicle overlay as an example.



Figure 8-35 Picture (non-motor vehicle)



3) Click Apply.


**Step 6** (Optional) Click the icons at the right side of the image to filter targets in the image.

- Click to draw rule line in the image.  
When targets pass the tripwire along the configured direction line, they will be counted.
- After the rule is enabled, the detection area is displayed. Click , and you drag the any corner of the box to adjust the size of the area, and press the left mouse button and move the box to adjust the position.
- Click to draw an area exclusion area for face detection in the image, and right-click to finish the drawing..
- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

**Step 7** Set parameters.

Table 8-17 Description of crowd map parameters

Parameter	Description
People Flow Statistics	Click  next to People Flow Statistics to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click  next to Flow Statistics (Non-motor Vehicle) to count the number of non-motor vehicles in the detection area.
Traffic Flow Stat	Click  next to Traffic Flow Statistics to count the number of motor vehicles in the detection area.

Parameter	Description
OSD	Click OSD Info, and the Overlay page is displayed. Click  next to Enable to enable the target statistics function. For details, see "6.2.2.2.8 Configuring Target Statistics".
Snapshot Mode	<ul style="list-style-type: none"> <li>• <b>Optimized:</b> Capture the pictures until the vehicle disappears from the image, and report the clearest picture.</li> <li>• <b>Tripwire:</b> Capture the pictures when the vehicle triggers tripwire as the configured direction.               <ol style="list-style-type: none"> <li>1. Select Tripwire.</li> <li>2. Select the direction from A to B, B to A, and Both.</li> <li>3. Adjust the position of rule line as needed.</li> </ol> </li> </ul>

**Step 8** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". Click + Event Linkage to set the linkage action.

**Step 9** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

### 8.8.3 Viewing Video Analytics Report

Generate data of video Analytics recognition in report form.

#### Procedure

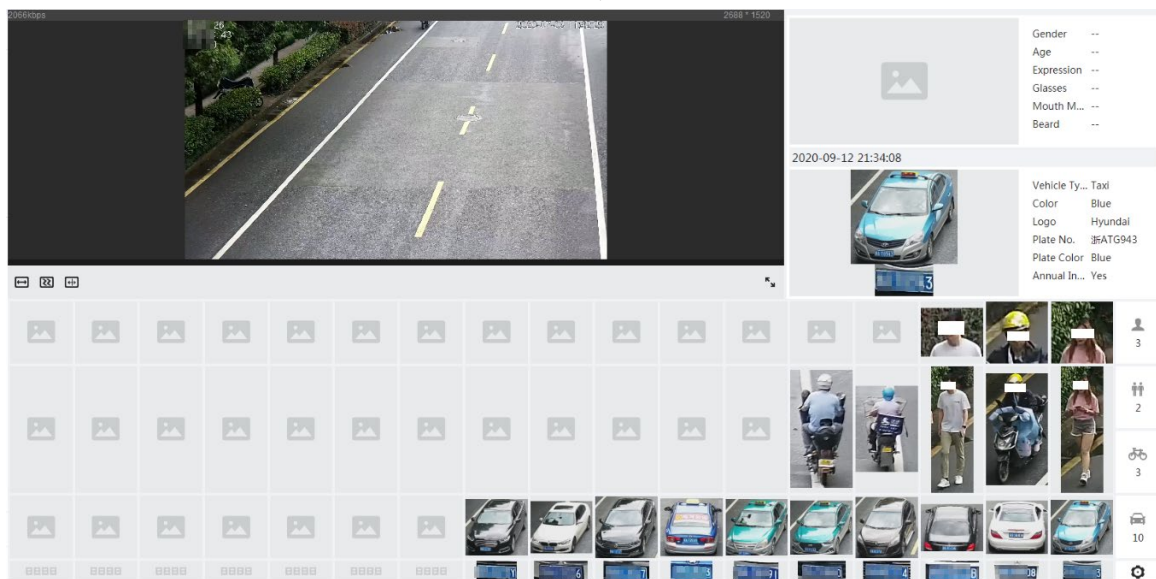
**Step 1** Select Setting > Event > Video Analytics > Report.

**Step 2** Select the report type, start time, end time, and other parameters.

**Step 3** Click Search to complete the report.

The statistical results are displayed. Click Export to export the statistical report.

Figure 8-36 Video Analytics report



## 8.9 Setting People Counting

Set people counting (including entry number, exit number and stay number in area), queuing number, and view the people counting data in report form.

### 8.9.1 People Counting

The system counts the number of people entering and leaving the detection area. When the number of counted people exceeds the configured value, an alarm is triggered and the system performs an alarm linkage.

#### Background Information

There are two types of people counting rules.

- People Counting:** The system counts the people entering and leaving the detection area. When the number of counted number of people who enter, leave, or stay in the area exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage.
- Area People Counting:** The system counts the people in the detection area and the duration that people stay in the area. When the number of counted number of people in the detection area or the stay duration exceeds the configured value, an alarm is triggered, and the system performs an alarm linkage. This function is available on some select models.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan

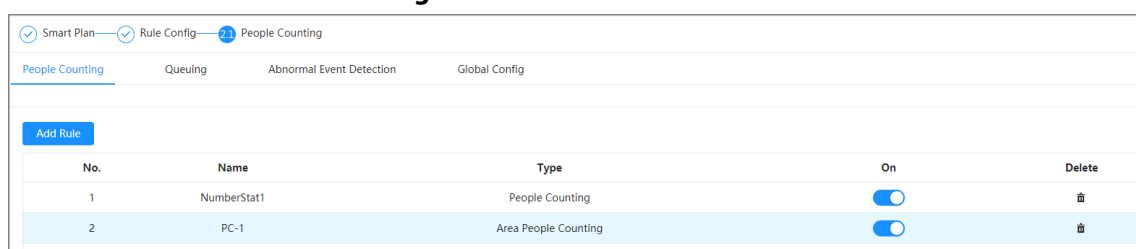
**Step 2** Click  next to People Counting, and then click Next.



**Step 3** Click the People Counting tab.

**Step 4** Click Add Rule to select rules.

- The added rules will be displayed in the list. Click the text box under Name to edit the rule name. The rule is enabled by default.
- For the models that support multiple counting rules, different detection areas can be overlapped. It supports at most 4 people counting rules and 4 area people counting rules.

Figure 8-37 Add rule




No.	Name	Type	On	Delete
1	NumberStat1	People Counting	<input checked="" type="checkbox"/>	
2	PC-1	Area People Counting	<input checked="" type="checkbox"/>	

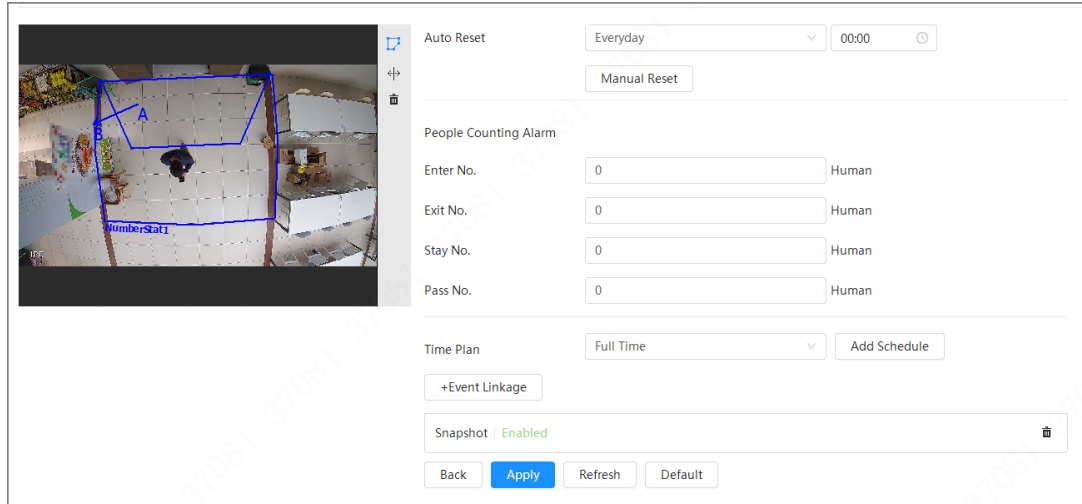
**Step 5** Draw a detection area in the image.

- People counting


1. Click , drag the any corner of the box to adjust the size of the area, press

- the right mouse button, and then move the box to adjust the position.
- Click  to draw rule line in the image.  
When targets enter or leave the detection area along the direction line, they will be counted.

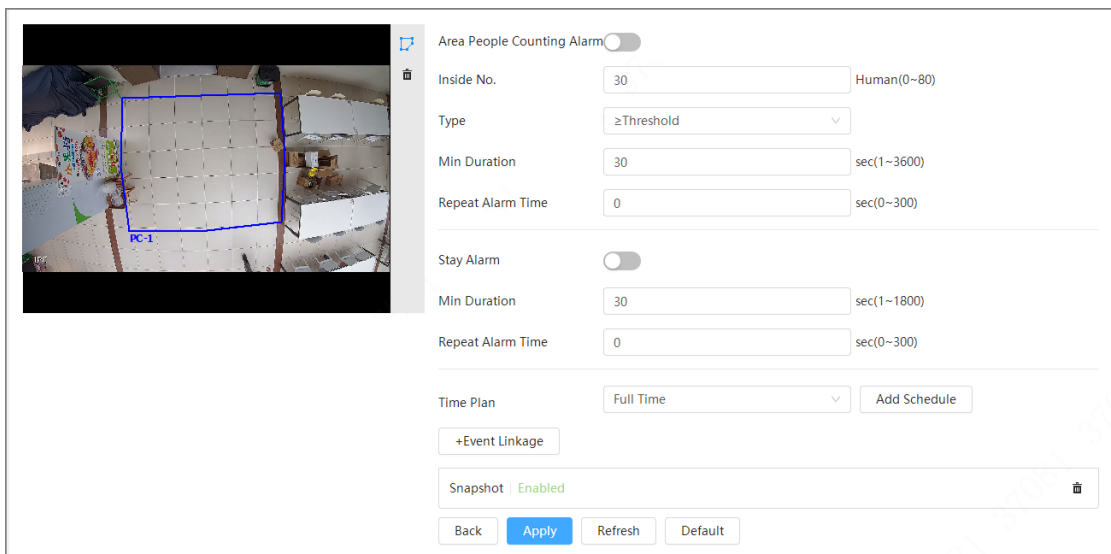
**Figure 8-38 People counting (1)**



- **Area people counting**

Click , and drag the any corner of the box to adjust the size of the area, and press the right mouse button and move the box to adjust the position.


**Figure 8-39 People counting (2)**



**Step 6** Set parameters.

**Table 8-18 Description of people counting parameters**

Parameter	Description	
People counting	Auto Reset	Set the reset period and time, and then the system will clear the countered number according to the configured time automatically.
	Manual Reset	Manually clear the countered number.

Parameter	Description	
	Enter No.	Counts the number of people entering in the direction A-->B. When the number exceeds the configured value, an alarm will be triggered.
	Exit No.	Counts the number of people entering in the direction B-->A. When the number exceeds the configured value, an alarm will be triggered.
	Stay No.	It is the difference between the Enter No. and Exit No.. When the number exceeds the configured value, an alarm will be triggered.
	Pass No.	Counts the number of people entering and exiting the detection area from the direction A. When the number exceeds the configured value, an alarm will be triggered.
Area people counting	Inside Number	Set the number of people in the people counting region. When the people count reaches the configured value, an alarm will be triggered. When you set inside number to 0, and select $\geq$ Threshold in Type, the system will not perform the alarm linkage.
	Type	
	Stay Alarm	Select the Stay Alarm checkbox to enable this function.
	Min Duration	When the stay duration exceeds the configured value, an alarm is triggered.
	Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.  0 means repeat alarm function disabled.

**Step 7** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".  
Click + Event Linkage to set the linkage action.

**Step 8** Click Apply.

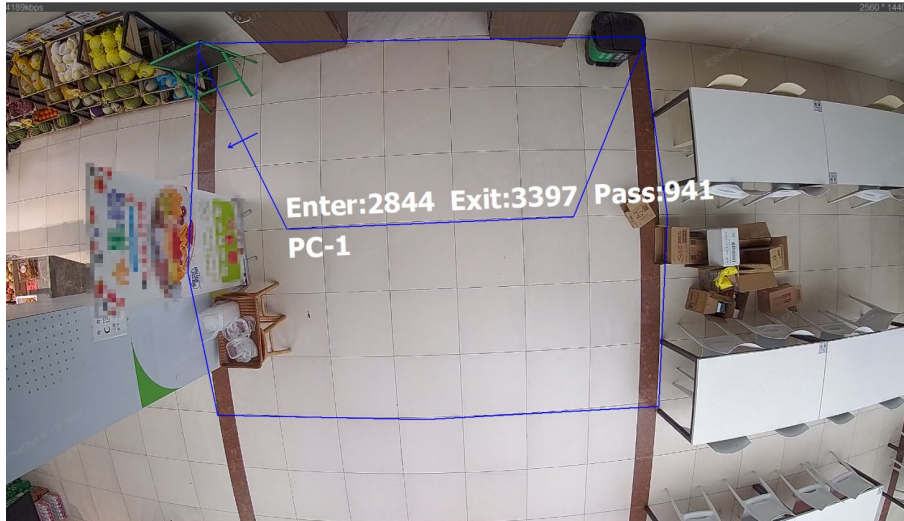
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## Result

You can view the counting results on the Live page.

- For People Counting rule, the entry and exit numbers are displayed.
- For Area People Counting rule, the inside number is displayed.

Figure 8-40 Counting result



## 8.9.2 Queuing

The system counts the queue people in the detection area. When the queue people number exceeds the configured number or the queue time exceeds the configured time, an alarm will be triggered, and the system performs an alarm linkage.

### Procedure

**Step 1** Select Analytics+ > Smart Plan

**Step 2** Click  next to People Counting, and then click Next.

**Step 3** Click the Queuing tab.

**Step 4** Click Add Rule > Queuing to select rules.

- The added rules will be display in the list. Click the text box under Name to edit the rule name. The rule is enabled by default.
- For the models that support multiple counting rules, different detection areas can be overlapped. It supports at most 4 queuing rules.

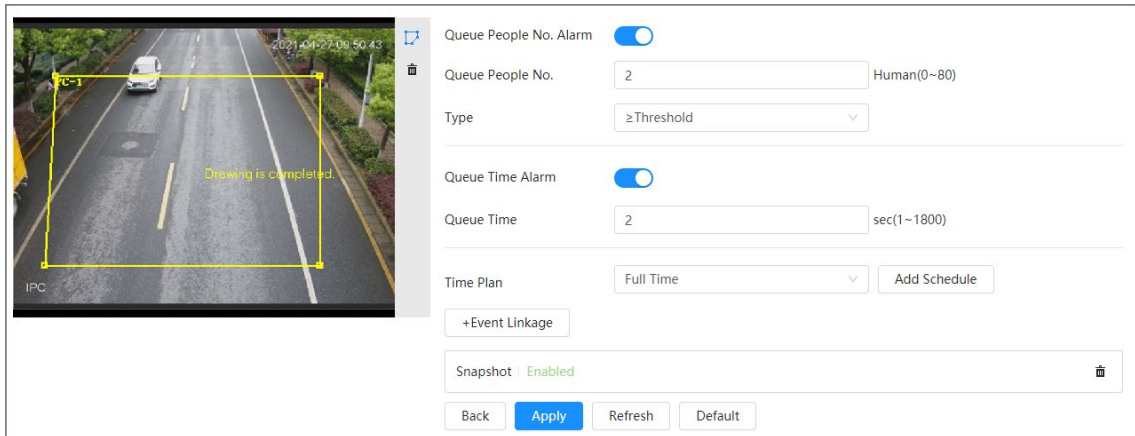
Figure 8-41 Add rule

Smart Plan — Rule Config — <b>People Counting</b>					
People Counting <u>Queuing</u> Abnormal Event Detection    Global Config					
<a href="#">Add Rule</a>					
No.	Name	Type	On	Delete	
1	QUE-1	Queuing	<input checked="" type="checkbox"/>		

**Step 5** Draw a detection area in the image.

Click  to draw the detection area, and press the right mouse button to complete the drawing.

**Figure 8-42 Queuing**



**Step 6** Set parameters.

**Table 8-19 Description of queuing**

Parameter	Description
Queue People No. Alarm	Enable the queue people No. alarm function.
Queue People No.	
Type	Set the queue people number for triggering the alarm and counting type. When the queue people number reaches the configured value, an alarm will be triggered.
Queue Time Alarm	Enable the queue time alarm function.
Queue Time	Set the queue time. When the queue time reaches the configured value, the alarm is triggered.

**Step 7** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".  
Click + Event Linkage to set the linkage action.

**Step 8** Click Apply.  
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

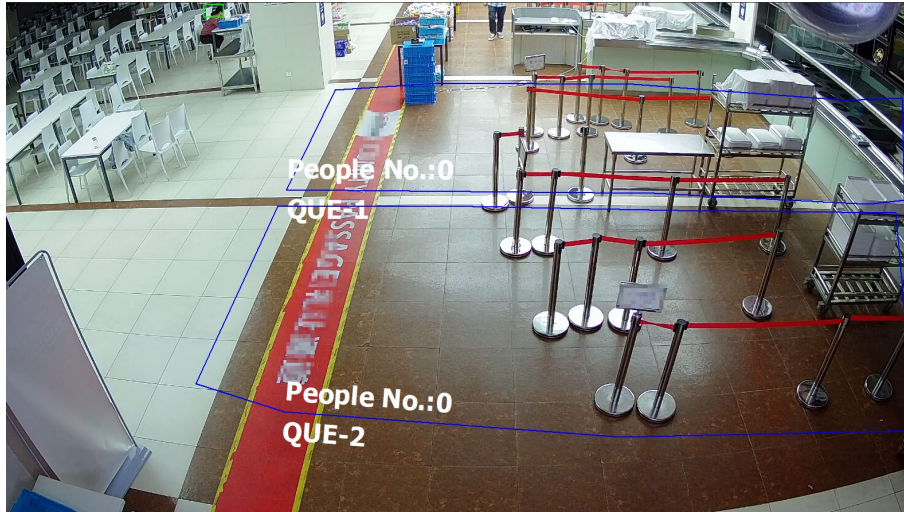
## Result

You can view the queuing results on the Live page.

The queuing number and the stay time of each target are displayed on the page.



Figure 8-43 Queuing result



### 8.9.3 Abnormal Event Detection

The system detects the congestion in the detection area. When the congestion detected exceeds the configured value, an alarm is triggered and the system performs an alarm linkage.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan

**Step 2** Click  next to People Counting, and then click Next.

**Step 3** Click the Abnormal Event Detection tab.


**Step 4** Click Add Rule > Crowd Detection to select rules.

- The added rules will be displayed in the list. Click the text box under Name to edit the rule name. The rule is enabled by default.
- For the models that support multiple counting rules, different detection areas can be overlapped. It supports at most 4 queuing rules

Figure 8-44 Add rule

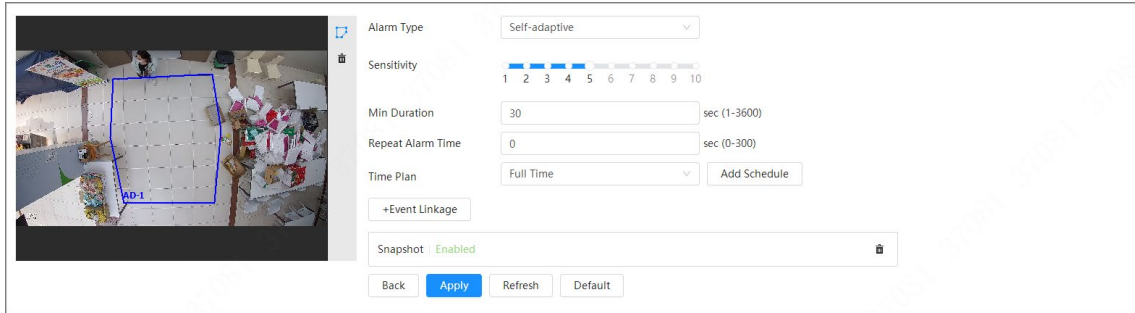
Smart Plan > Rule Config > 2/1 People Counting					
People Counting		Queuing	Abnormal Event Detection	Global Config	
Add Rule					
No.	Name	Type	On	Delete	
1	AD-1	Crowd Detection	<input checked="" type="checkbox"/>	🗑️	
2	AD-2	Crowd Detection	<input checked="" type="checkbox"/>	🗑️	

**Step 5** Draw a detection area in the image.

Click , and drag the any corner of the box to adjust the size of the area, and press the right mouse button and move the box to adjust the position.



**Figure 8-45 Abnormal Event Detection**



**Step 6** Set parameters.

**Step 7** Table 8-20 Description of abnormal event detection

Parameter	Description
Alarm Type	<p>You can select from Self-adaptive and Custom.</p> <ul style="list-style-type: none"> <li><b>Self-adaptive:</b> The system calculates the number of people and the area of detection region to determine whether the alarm is triggered.</li> <li><b>Custom:</b> Configure crowd number for different crowd level. When the number exceed the configured value, an alarm will be triggered. Up to 5 levels can be added.</li> </ul>
Sensitivity	The higher the sensitivity, the easier the detection, but the more the false detections.
Min Deration	When the duration of congestion exceeds the configured value, an alarm is triggered.
Repeat Alarm Time	<p>When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.</p> <p> <b>0 means repeat alarm function disabled.</b></p>
Crowd Level	<p>When the alarm type is Custom, click Add to add crowd level. When the number exceed the configured value, an alarm will be triggered.</p> <p></p> <ul style="list-style-type: none"> <li><b>The number of people in the crowd level added later must be larger than the number added before.</b></li> <li><b>When deleting the crowd level, delete it from the highest level.</b></li> </ul>

**Step 8** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". Click + Event Linkage to set the linkage action.

**Step 9** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

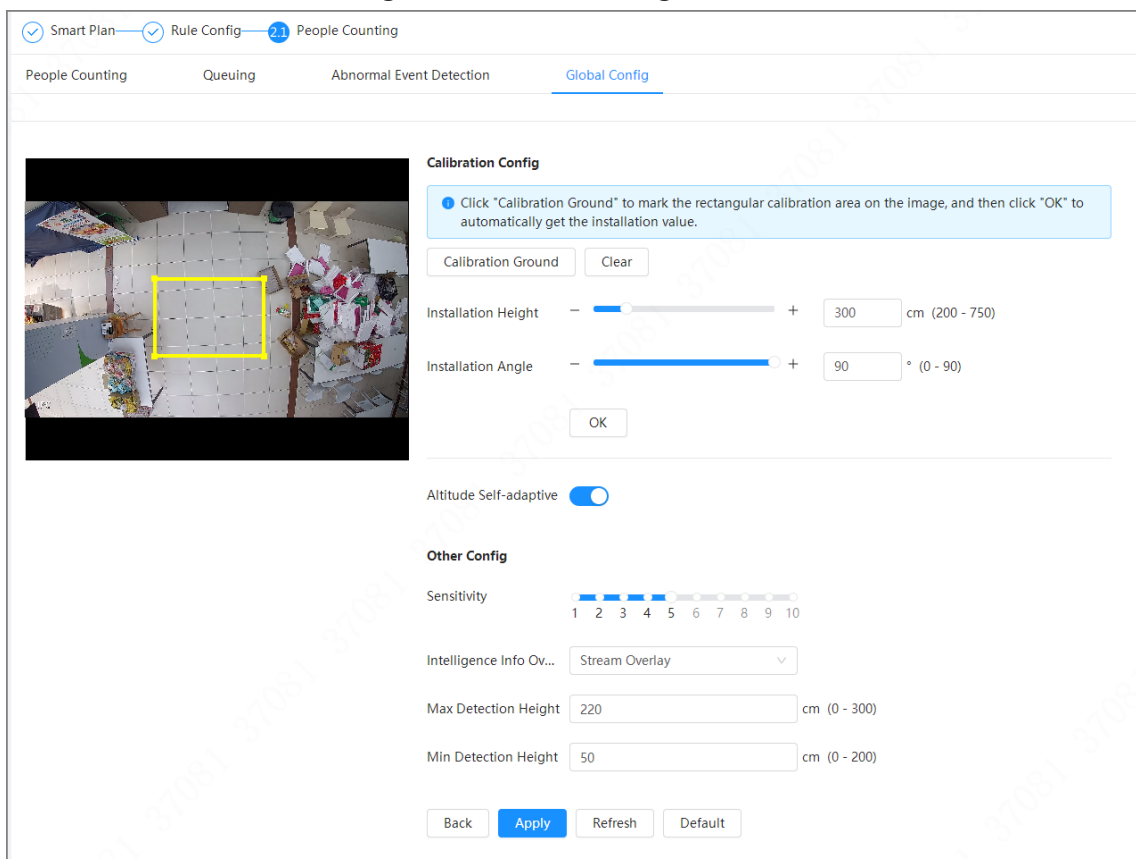
## 8.9.4 Global Configuration

After you configured the calibration ground and enabled altitude self-adaptive, the device could automatically adjust the field of view according to the installation height and angle.

### Procedure

- Step 1** Select Analytics+ > Smart Plan
- Step 2** Click  next to People Counting, and then click Next.
- Step 3** Click the Global Config tab.

Figure 8-46 Global config



**Step 4** Set the calibration config.

- **Method 1:** Configure the installation height and angle manually according to the actual situation.
- **Method 2:** Automatically calculate the installation height and angle by calibration ground.

Here we use method 2 as an example.

1. Click Calibration Ground.
2. Draw the yellow box in the live page.



**Try to choose a position near the middle of the detection region and which is easy to be recognize.**

3. Click OK. The device automatically calculate the installation height and angle.

**Step 5** Enable Altitude self-adaptive.

**Step 6** Set the sensitivity.

When the sensitivity is high, detection becomes easier, but the number of false detections increases.

**Step 7** Set the intelligence info overlay.

- **Stream overlay:** Overlay the information on the stream.



When enabling Stream Overlay, the Overlay function in camera setting will be disabled. When Overlay is enabled again, the function restores and maintains the previous settings.

- **Overlay:** Click OSD Info, and the Overlay page is displayed, and then enable the People Counting function. The number of detected information is displayed on the Live page. For details, see "6.2.2.2.15 Configuring People Counting".

**Step 8** Configure the max and min detection height.

**Step 9** Click Apply.

## 8.10 Face & Body Detection

After enabling this function, the camera detects faces and human body separately, and then correlates the face and the body. When selecting compliant mode, the camera can detect attributes including face masks, helmets, glasses, safety vests, top color, and bottom color, and determine whether PPE requirements are met. PPE compliance or non-compliance alarms can be triggered according to the alarm settings.

### 8.10.1 Global Configuration

Set the global configuration of face & body detection, including face parameter and scene parameter.

#### Procedure

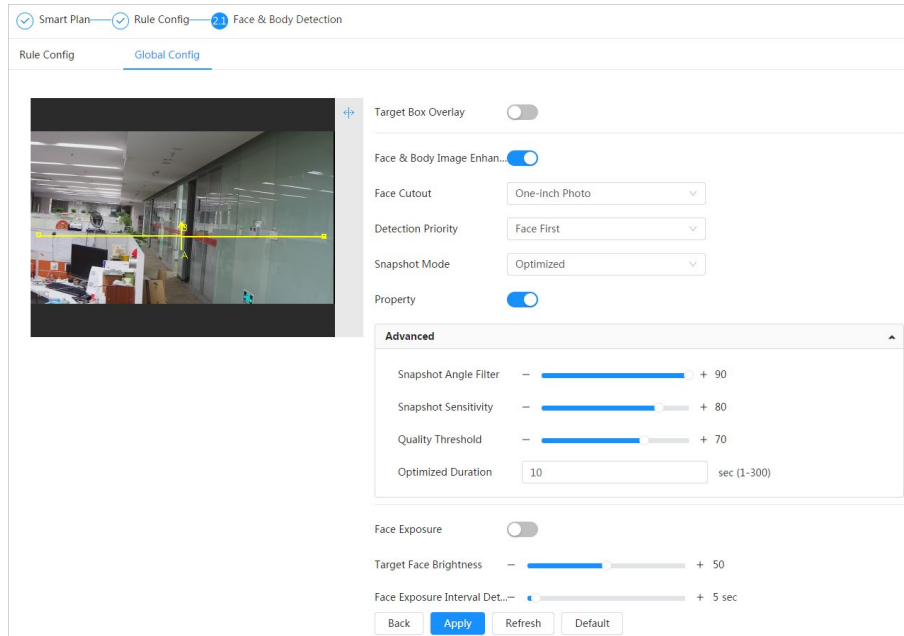
**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to Face & Body Detection to enable face & body detection of the corresponding channel, and then click Next.

**Step 3** Click the Global Config tab.

**Step 4** Set parameters.

**Figure 8-47 Global configuration of face & body detection**



**Table 8-21 Description of scene set parameters (face & body detection)**

Parameter	Description
Target Box Overlay	Overlay target box on the captured pictures to mark the target position.
Face & Body Image Enhancement	Click <input type="checkbox"/> next to Face & Body Image Enhancement to preferably guarantee clear face and body with low stream.
Face Cutout	Set a range for matting face image, including face, one-inch photo, and custom.
Detection Priority	Select from Face First or Human Body First.
Snapshot Mode	<ul style="list-style-type: none"> <li>● <b>Real-time:</b> Capture the image when the camera detects a face.</li> <li>● <b>Optimized:</b> Capture the clearest image within the configured time after the camera detects face.</li> <li>● <b>Quality Priority:</b> After detecting the face image quality is higher than the quality threshold, the camera captures the image.</li> <li>● <b>Tripwire:</b> This snapshot is available in PPE Detection Mode.</li> </ul> <p> Click Advanced to set the optimized time and quality threshold.</p>
Property	Click <input type="checkbox"/> next to Property to enable the properties display.

Parameter	Description
Advance	<ul style="list-style-type: none"> <li>• <b>Snapshot Angle Filter:</b> Set snapshot angle to be filtered during the face detection.</li> <li>• <b>Snapshot Sensitivity:</b> Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>• <b>Optimized Time:</b> Set a period to capture the clearest picture after the camera detects face.</li> </ul>
Face Exposure	Click <input type="checkbox"/> next to Face Exposure to make face clearer by adjusting lens aperture and shutter.
Target Face Brightness	Set the face target brightness, and it is 50 by default.
Face Exposure Interval Detection Time	Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.

**Step 5** Click Apply.

## 8.10.2 Rule Configuration

Set the detection scene and rules, including people, non-motor vehicle, and motor vehicle.

### Prerequisites

- Select Analytics+ > Smart Plan, and enable Face & Body Detection.
- You have configured the parameters on the Global Config page.

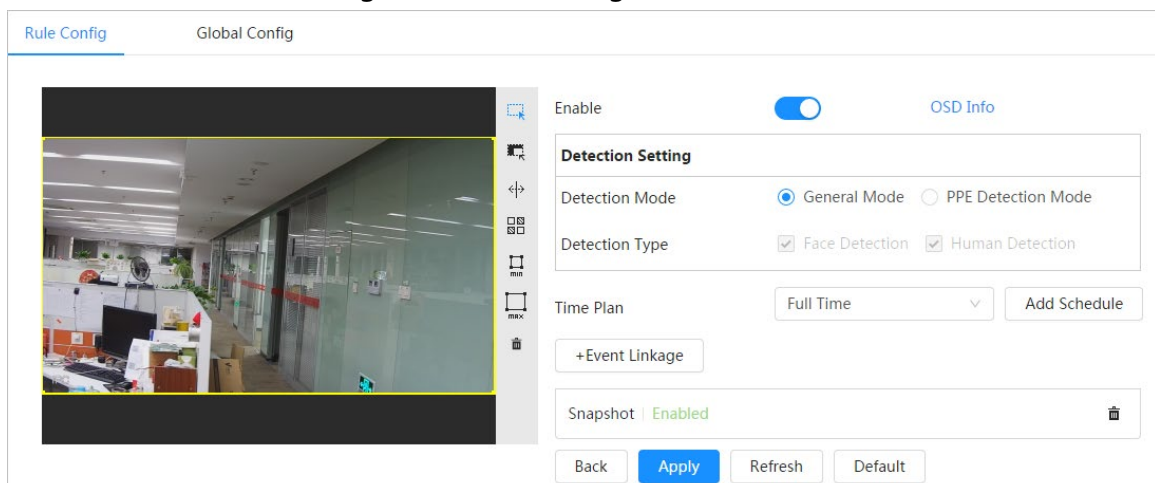
### Procedure

**Step 1** Select Analytics+ > Smart Plan

**Step 2** Click  next to Face & Body Detection, and then click Next.








**Step 3** Click the Rule Config tab.

Figure 8-48 Rule configuration



**Step 4** Click  next to Enable to enable the face detection function.

**Step 5** (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.

- Click  to draw a face detection area in the image, and right-click to finish the drawing.
- Click  to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click  to draw rule line in the image.
- Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

**Step 6** (Optional) Set OSD information.

Click OSD Info, and the Overlay page is displayed, and then enable the face & body counting function. The number of detected faces and bodies is displayed on the Live page. For details, see "6.2.2.2.12 Configuring Face Statistics".

**Step 7** Select the detection mode.

- **General Mode** (selected by default): The system will perform an alarm linkage when the camera detects a face or a person.
- **PPE Detection Mode:**
  1. Click + next to Analytics+ Attributes.
  2. Select Analytics+ attributes that you want to detect.  
The Analytics+ attributes include mouth mask, vest, safety helmet, glasses, top color, and bottom color. For glasses, you need to select the glass type; for safety helmet, top color, and bottom color, you need to select colors.
  3. Click Apply to go back to the Rule Config page.
  4. Select the alarm mode.
    - ◇ **Match Attributes Alarm:** When the target's properties are compliant with the configured properties, an alarm will be triggered, and the system performs an alarm linkage.
    - ◇ **Mismatch Attributes Alarm:** When the target's properties are not compliant with the configured properties, an alarm will be triggered, and the system performs an alarm linkage.

**Step 8** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

**Step 9** Click Apply.

To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.5.1.3.2 Subscribing Alarm Information".

## 8.11 PPE Detection

After PPE (Personal Protective Equipment) detection is enabled and related rules are configured, when the target attributes are inconsistent with the configured attributes, the alarm is triggered. This function can be widely used in energy, finance, retail, manufacturing and other industries of employee service compliance.

## 8.11.1 Rule Configuration

### Procedure


- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to PPE Detection, and then click Next.
- Step 3** Click the Rule Config tab.
- Step 4** Click Add Rule, and then select PPE Detection.  
Currently only one rule can be added.
- Step 5** Draw the detection area.  
Click , drag the any corner of the box to adjust the size of the area, and then press the right mouse button and move the box to adjust the position.
- Step 6** Configure the detection parameters.

Figure 8-49 PPE detection

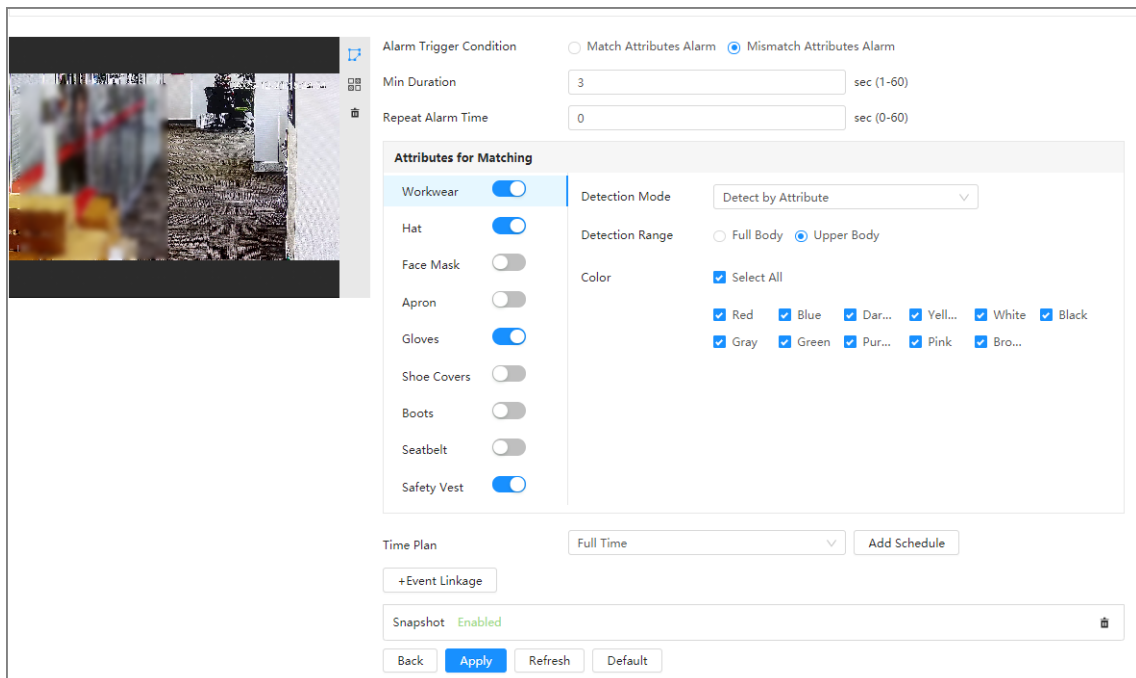



Table 8-22 Description of PPE detection parameters

Parameter	Description
Alarm Trigger Condition	<ul style="list-style-type: none"> <li>● <b>Match Attributes Alarm:</b> When the detected object matches all of the configured attributes, the system triggers alarm.</li> <li>● <b>Mismatch Attributes Alarm:</b> When the detected object does not match the configured attributes, the system triggers alarm.</li> </ul> <p></p> <p><b>Each detected attribute which does not match the configured attributes will trigger a new alarm.</b></p>



Parameter	Description
Min Duration	The minimum duration between the detected object appears and trigger the alarm.
Repeat Alarm Time	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.  0 means repeat alarm function disabled.
Attributes for Matching	Set the alarm attributes. For details, see Table 8-23.

Table 8-23 Description of attributes for matching

Attribute	Description
Workwear	<p>Select the detection mode.</p> <ul style="list-style-type: none"> <li>Registration Mode: Detect the attribute Yes or No, and this mode can be used when the clothes of upper body and lower body are in different color.</li> </ul> <p>Compare the detected workwear with the information in linked arming database. You should configure the arming database in advance. For details, see "8.11.3 Setting Arming Database".</p>  <p>Up to 5 arming databases can be added to the same rule.</p> <ul style="list-style-type: none"> <li>Detect by Attribute:               <ol style="list-style-type: none"> <li>Select the detection range from Full Body and Upper Body.</li> <li>Select the color.</li> </ol> </li> </ul>
Hat	<ol style="list-style-type: none"> <li>Select the detection attribute: Yes or No.</li> <li>Select the detection range: Safety helmet or cap. If you choose safety helmet, select the color.</li> </ol>
Face Mask	Select the detection attribute: Yes or No.
Apron	
Gloves	
Shoe Covers	
Boots	
Seatbelt	
Safety Vest	

**Step 7** Select time plan, and then click + Event Linkage.

- If the added time plan cannot meet your requirements, click Add Schedule to add an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Click Event Linkage to add linked event and set linkage parameters. For details, see "6.5.1.2 Alarm Linkage".

**Step 8** Click Apply.



## 8.11.2 Global Configuration

Set the privacy protection for PPE detection.

### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to PPE Detection, and then click Next.
- Step 3** Click the Global Config tab.
- Step 4** Turn on Privacy Protection, and then choose the target.
- Step 5** Click Apply.

## 8.11.3 Setting Arming Database

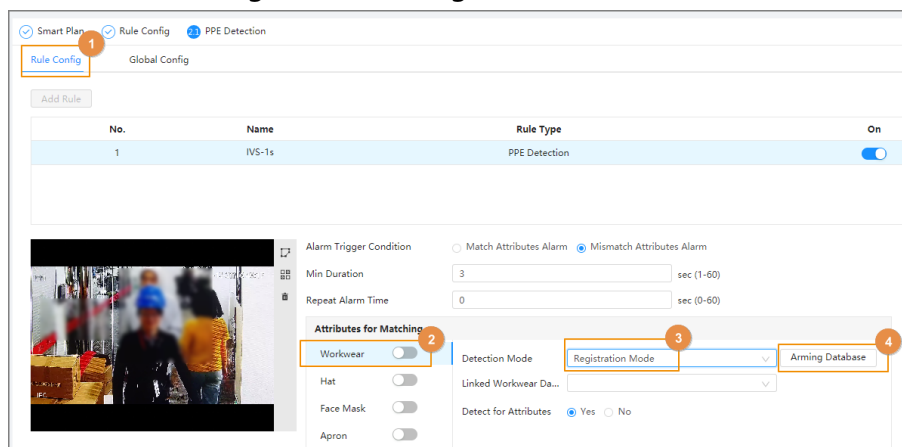
### Prerequisites


Added PPE detection in Rule Config tag.

### Procedure

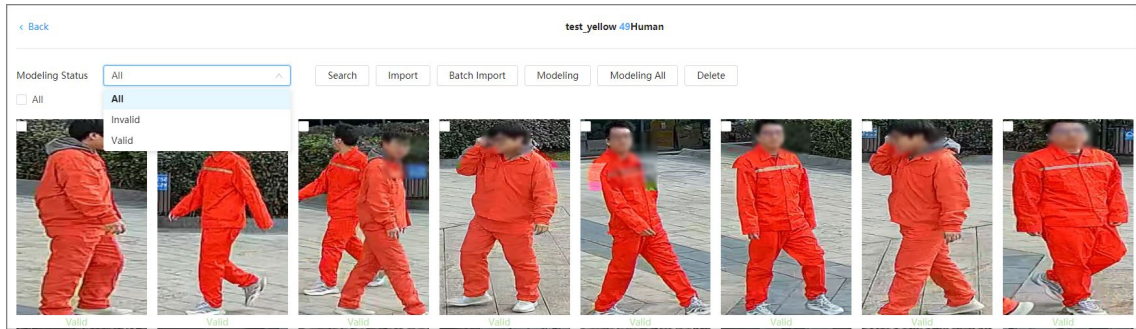
- Step 1** Select Analytics+ > Smart Plan > PPE Detection.
- Step 2** Click Rule Config tag.
- Step 3** Select Workwear > Registration Mode > Arming Database.

Figure 8-50 Arming database



- Step 4** Click Add in Arming Database page.  
Up to 5 arming databases can be added.
- Step 5** Create the name of database, and then select the optional plan. You can select to detect full body or half body.
- Step 6** Configure the database.
  - 1) Click  below Details.
  - 2) Import the modeling pictures.
    - Import: Import one picture.
    - Batch import: Import up to 40 pictures at the same time.
  - 3) Select imported pictures, and then click Modeling.
  - 4) After modeling, you can check the modeling status in the drop-down list.

**Figure 8-51 Search the modeling status**

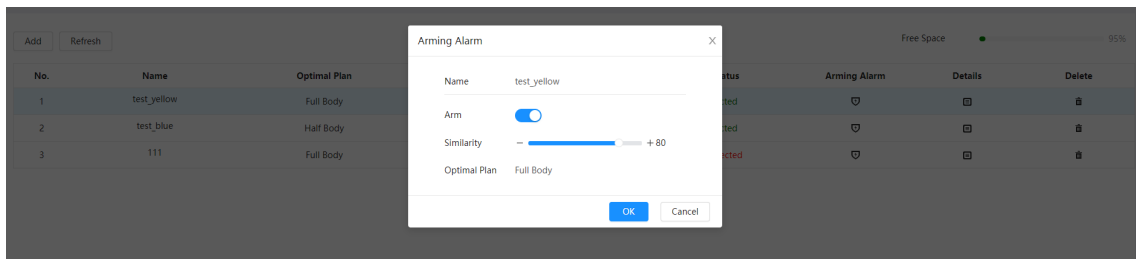


**Step 7** Click Back, and then go back to arming database page.

**Step 8** Click below Arming Alarm to set the parameters of arming alarm.

- 1) Enable Arm checkbox.
- 2) Set the similarity as needed.
- 3) Click OK.

**Figure 8-52 Arming alarm**



**Step 9** Link workwear attributes. For details, see Table 8-23.

## 8.12 Setting Heat Map

Detect the distribution of dynamically moving objects in the target area within a certain period and displays the distribution on a heat map. Color varies from blue to red. The lowest heating value is in blue, and the highest heating value is in red.

### Background Information

When mirroring occurs on the camera or the viewing angle changes, original data on the heat map will be cleared.

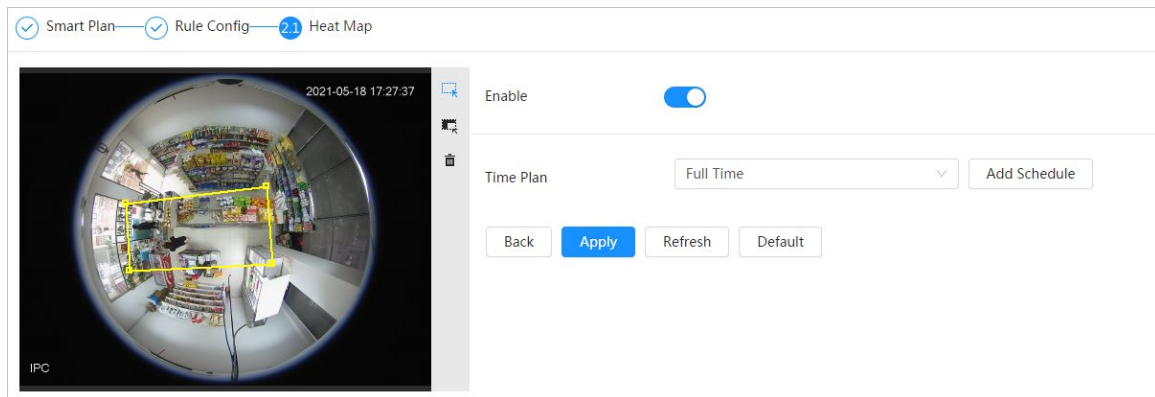
### Procedure

**Step 1** Select Analytics+ > Smart Plan

**Step 2** Click next to Heat Map, and then click Next.

**Step 3** Select the Enable check box, and then the heat map function is enabled.

Figure 8-53 Heat Map



**Step 4** Draw detection area and exclusion area.

- Click to draw a detection area on the image. Right-click to finish drawing.
- Click to draw an exclusion area on the image. Right-click to finish drawing.
- Click to clear the existing detection area or exclusion area.

**Step 5** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage".

**Step 6** Click Apply.

## 8.13 Setting ANPR

When a motor vehicle triggers the rule line in the detection area, it will capture the license plate and report the attributes of the motor vehicle.

### 8.13.1 Lane Configuration

Configure lane configuration including detection area, lane line, detection line and lane direction.

#### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to ANPR, and then click Next.

**Step 3** Click the Lane Config tab.

**Step 4** Click and draw the detection area.

Press the left mouse button to draw the detection area, and press the right mouse button to finish.

**Step 5** Configure lane line information.

- One lane line is composed of two lane lines with an arrow, and the arrow represents the direction of the lane.
- The lane is enabled by default after drawing. If you do not select a lane, the track frame will be displayed on the screen, but the event of license plate recognition will not be reported.
- The lane number of each lane is unique and unchangeable.

**Step 6** Select the lane direction.

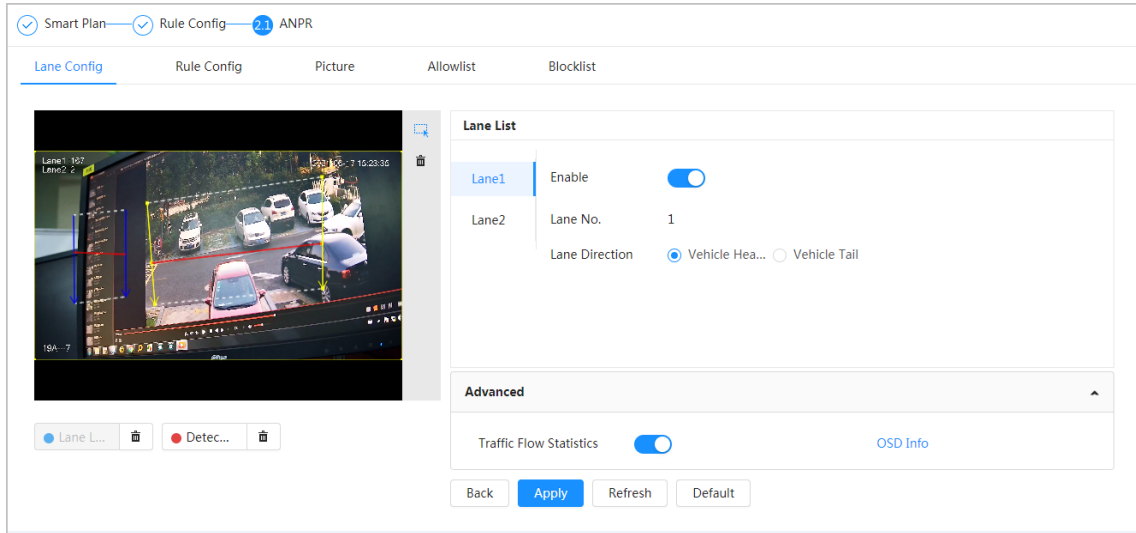
- **Vehicle Head:** The driving direction of the vehicle in the lane is from top to bottom

↓.

- **Vehicle Tail:** The driving direction of the vehicle in the lane is from bottom to top

↑.

Figure 8-54 ANPR



**Step 7** Configure detection line information.

- The detection line is displayed in red and it only available in the drawn lane line.
- When a motor vehicle triggers the detection line, a snapshot will be taken. Also the license plate and its vehicle attributes will be reported.

**Step 8** (Optional) You can repeat step 4-7 to draw more lane lines and detection lines. You can add two lane lines at most.

**Step 9** (Optional) Click Advanced.

- Click  next to Traffic Flow Statics. The system only detects the number of motor vehicle and generates report after you enable this function.
- Click OSD Info, and the Overlay page is displayed, and then enable the Parking Space function. The statistical result is displayed on the Live page. For details, see "6.2.2.2.9 Configuring ANPR".

**Step 10** Click Apply.

## 8.13.2 Rule Configuration

When a motor vehicle trigger the lane line associated, the system performs the defined alarm linkage.

### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to ANPR, and then click Next.

**Step 3** Click the Rule Config tab.

**Step 4** Click lane line to select the line that you configured. If no line is configured, click Add Lane Line.

**Figure 8-55 Rule configuration (1)**

Smart Plan > Rule Config > ANPR

Lane Config    Rule Config    Picture    Allowlist    Blocklist

Lane Line

Please draw lane line.

Add Lane Line

**Figure 8-56 Rule configuration (2)**

Time Plan  Add Schedule

+Event Linkage

Record | Enabled

Post-Record  sec (10-300)

Snapshot | Enabled

Alarm-out Port | Enabled

Alarm Channel

Post-alarm  sec (10-300)

Audio Linkage | Enabled

Play Count  (1-10)

File

Back Apply Refresh Default

**Step 5** Select time plan and click + Event Linkage.

- If the added time plan cannot meet your requirements, click Add Schedule to add an arming schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Click +Event Linkage to add linked event, which support record, send email,

snapshot, alarm-out port and audio linkage.

- Step 6** Set related alarm linkage.
- Step 7** Set audio linkage. For more information, see "6.2.4.2 Setting Alarm Tone".
  - Set play count period.
  - Select the file needed.
- Step 8** (Optical) Click to delete related linkage as needed.
- Step 9** Click Apply.

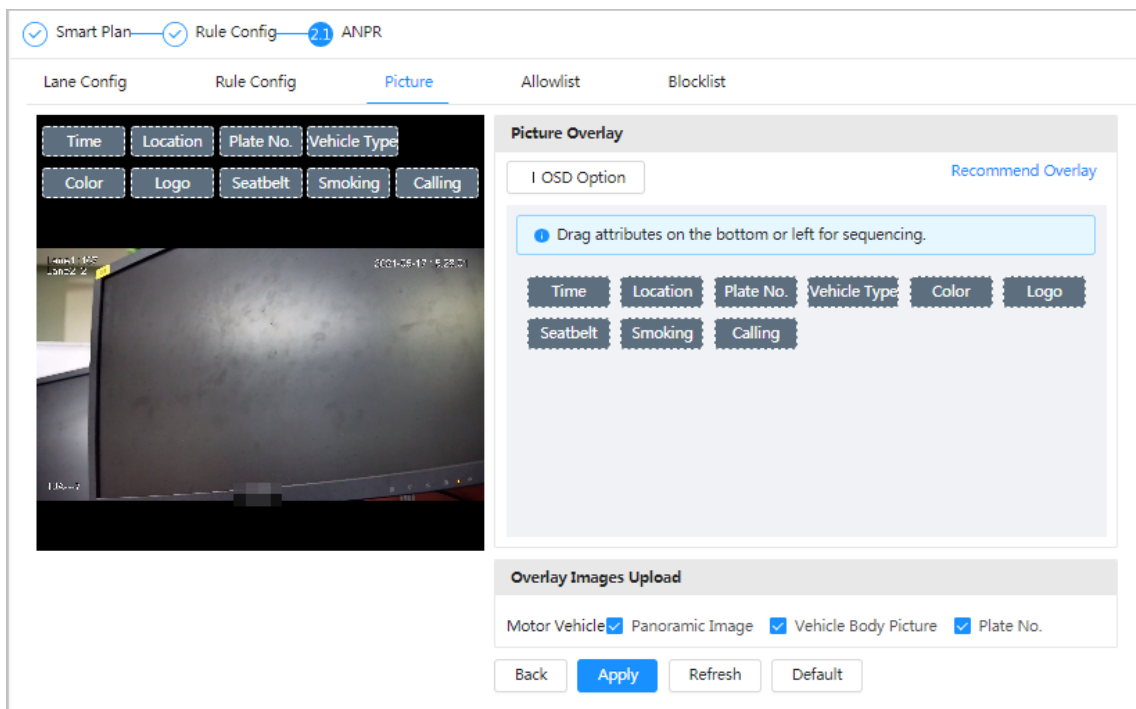
### 8.13.3 Picture

Set overlay information and image display position, such as plate number, time, vehicle type, and vehicle logo.

#### Procedure

- Step 1** Select Analytics+ > Smart Plan.
- Step 2** Click  next to ANPR, and then click Next.
- Step 3** Click the Picture tab.
- Step 4** Click + OSD Option to select the type of overlay information that needs to capture. You can adjust the position of the information displayed.

Figure 8-57 Picture



- Step 5** Select the overlay images upload type(s).
- Step 6** Click Apply.

### 8.13.4 Allowlist

After enabling allowlist, the camera will upload allowlist event and trigger linkage alarm when it detects the plate number in the allowlist.

## Background Information

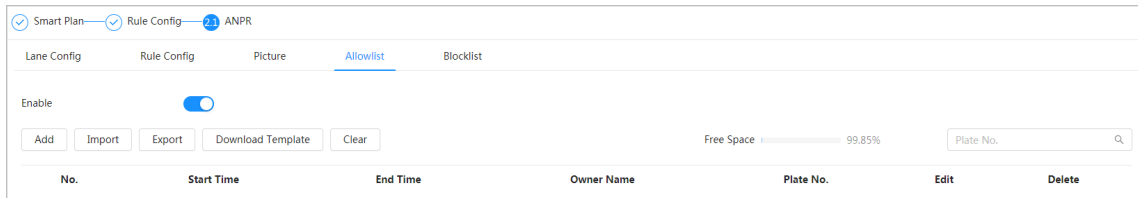
You can add 10,000 plate information in allowlist at most.

## Procedure

**Step 1** Select Analytics+ > Smart Plan > Allowlist.

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

Figure 8-58 Enable allowlist



**Step 3** Add allowlist.

- Add allowlist one by one.
  1. Click Add.
  2. Set plate information.

Figure 8-59 Add allowlist plate

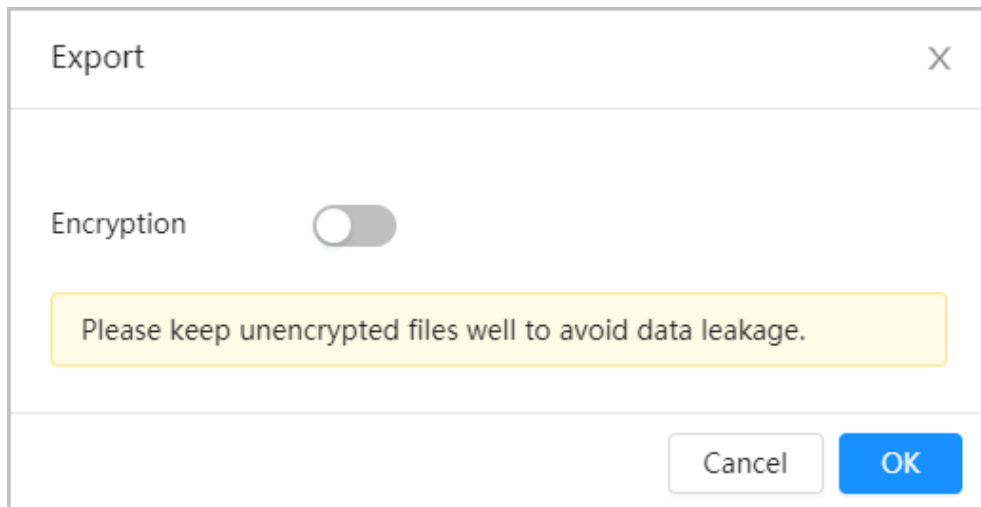
Table 8-24 Description of parameters

Parameter	Description
Plate No.	Enter the complete plate number.
Start Time/End Time	Set the validity of allowlist for the plate number. After this time range, the vehicle will not be detected even within allowlist.

Parameter	Description
Owner Name	Enter the name of car owner.

3. Click OK.  
Click Add Continuously to add more plate number.
- Add allowlist in batches.
  1. Refer to the steps "Add allowlist one by one".
  2. Click Export.
  3. Do not select Encryption and then click OK to export the unencrypted allowlist file.

Figure 8-60 Encryption settings (1)



4. Add the license plate information according to the sample of the exported file, and then save the table.

Figure 8-61 Template

Start Time	End Time	Owner Name	Plate No.
2017-1-1 0:00	2037-12-5 23:59	xxx	xxx

5. Click Import to upload allowlist table.
  - ◇ If the table is encrypted, you need to enter the password when uploading.
  - ◇ If the table is unencrypted, you can upload directly.

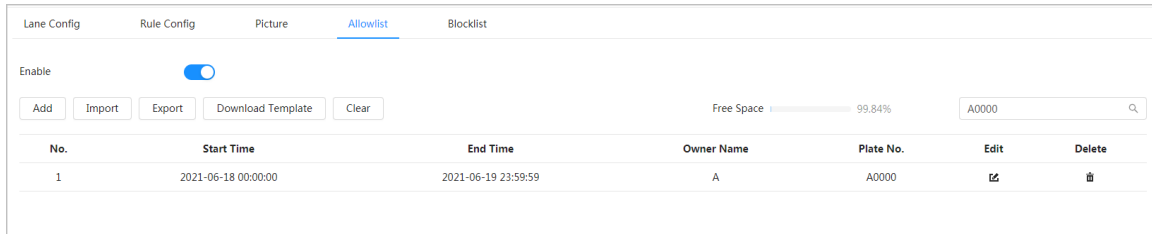
## Related Operations

- Search plate number.

Enter the plate number in  and then click . The search result is as below:



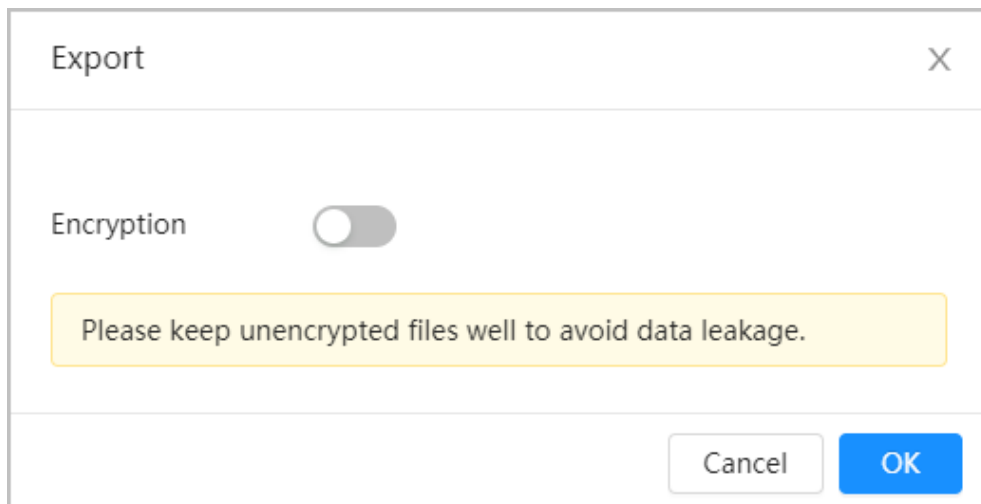
Figure 8-62 Search allowlist



**If you do not enter anything, it will show all the allowlist plate numbers added.**

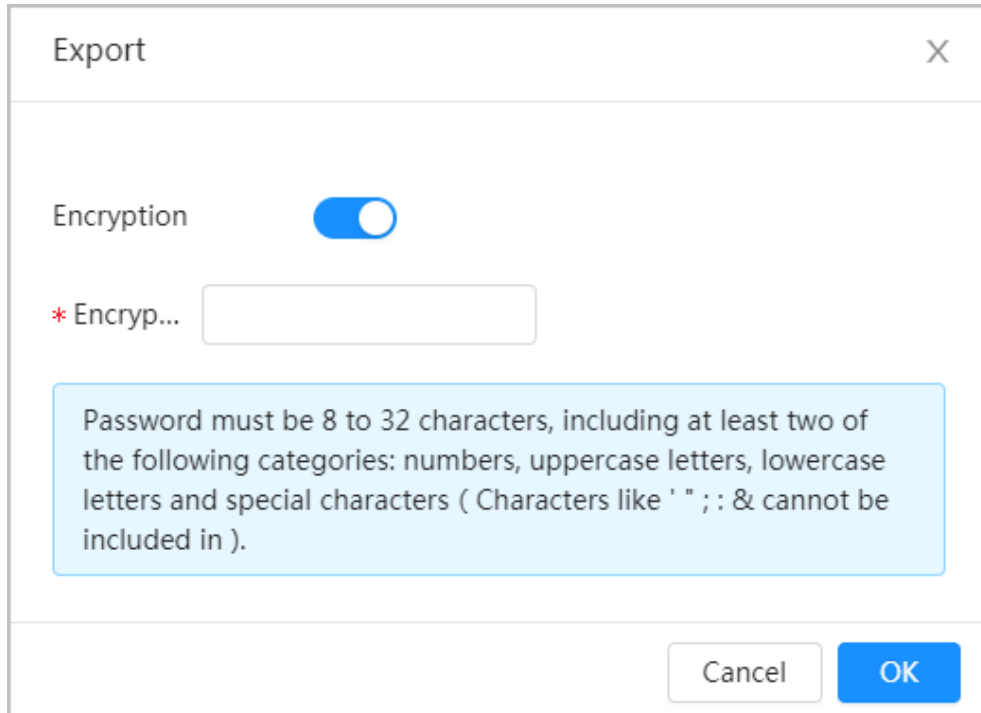
- **Edit allowlist information.**  
Click to edit Start Time/End Time and Owner Name.
- **Delete allowlist.**
  - ◇ Click to delete specific allowlist number.
  - ◇ Click Clear to delete all allowlist number.
- **Export allowlist.**  
Click Export. Enable encrypted or unencrypted file as needed and then export it to your PC.
  - ◇ Export the file in .csv format if not encrypted, and you can edit the file.

Figure 8-63 Encryption settings (2)



- ◇ Export the file in .backup format if encrypted, and you cannot edit the file.

Figure 8-64 Encryption settings (3)



Export

Encryption

\* Encryp...

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters ( Characters like ' ' ; : & cannot be included in ).

Cancel OK

## 8.13.5 Blocklist

After enabling blocklist, an alarm will be triggered when a plate number in blocklist is detected.

An alarm will be triggered when a plate number in the block list is detected.

You can add 10,000 plate information in blocklist at most.

The operation of blocklist is same as allowlist. For details, see "8.13.4 Allowlist".

## 8.14 Setting Panoramic Linkage

### 8.14.1 Enabling Linkage Track

#### Background Information



**Linkage Track is not enabled by default. Please enable it when necessary.**

#### Procedure

**Step 1** Select Analytics+ > Panoramic Linkage > Linkage Track.

**Step 2** Click  next to Enable to enable Linkage Track.

Figure 8-65 Linkage track

**Step 3** Configure other parameters.

Table 8-25 Parameters of linkage track

Parameters	Description
Tracking Duration	<ul style="list-style-type: none"> <li><b>Continue till object disappears:</b> When alarm is triggered, the camera automatically links to the corresponding position and tracks the object until the object exceeds the monitoring range.</li> <li><b>Custom:</b> Set the tracking duration for the camera.</li> </ul>
Tracking Target Size Ratio	Sets the ratio of the tracked object in the detail camera frame.
Idle Interval	Set the idle interval and idle position. If the PTZ does not receive any tracking command within the idle interval you set, the camera will automatically turn to the idle position. For example, if the idle interval is 5 seconds and idle position is preset 1, when the PTZ does not receive any tracking command for 5 seconds, it will turn to preset 1 automatically.
Idle Position	

You need to set presets in advance.

**Step 4** Click OK.

## 8.14.2 Configuring Calibration Parameter



Auto calibration mode is available on select models.

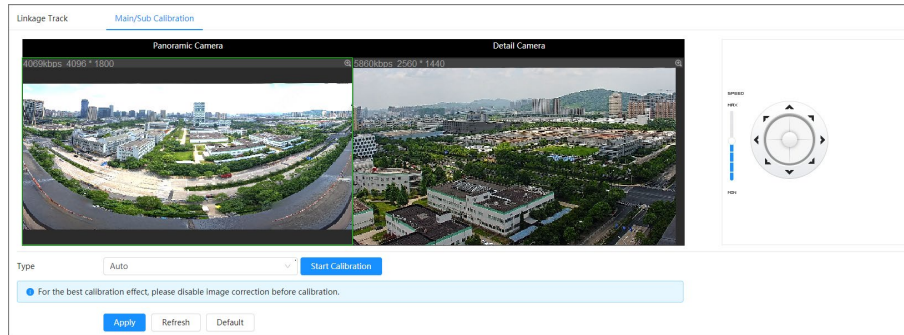
### Procedure

**Step 1** Select Analytics+ > Panoramic Linkage > Main/Sub Calibration.

**Step 2** Configure calibration parameters.

- **Auto calibration**  
Select Auto in Type, and then click Start Calibration.

Figure 8-66 Auto calibration



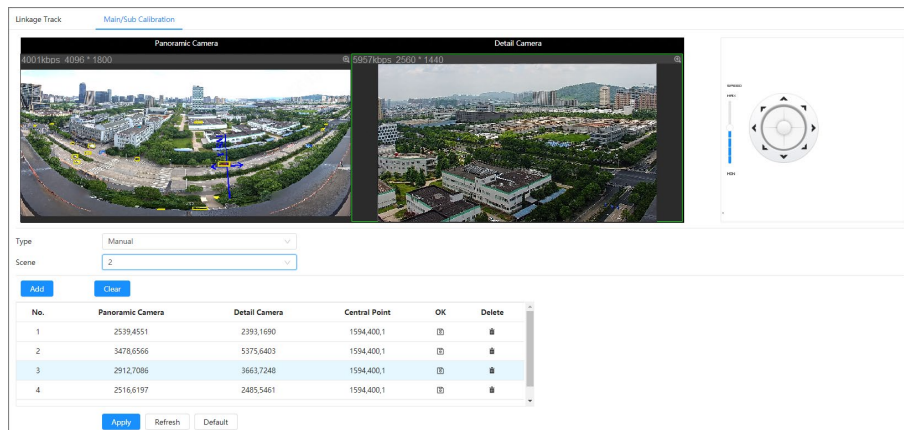
- **Manual calibration**

Select Manual in Type, select the scene, and then add calibration point for it in the live image.



Web pages might vary with different models.

Figure 8-67 Manual calibration



1) Adjust the speed dome lens and turn it to the same view as the chosen lens, and then click Add.

The calibration dots are displayed in both images.

2) Pair each dot in the two images, and keep the paired dots at the same spot of the live view.

3) Click .

At least 4 pairs of calibration dots are needed to ensure the views of the PTZ camera and the panoramic camera as similar as possible.

**Step 3** Click Apply.

## 8.15 Setting AcuPick

Enable this function to achieve accurate and quick search on the connected NVR.



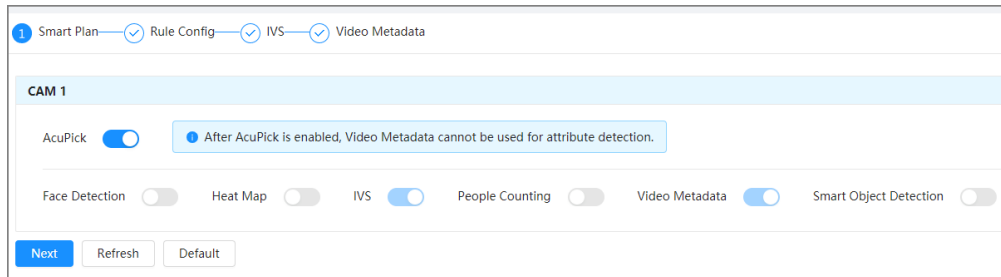
Make sure that the connected NVR supports AcuPick mode.

### Procedure

**Step 1** Select Analytics+ > Smart Plan.

**Step 2** Click  next to AcuPick, and then click Next.

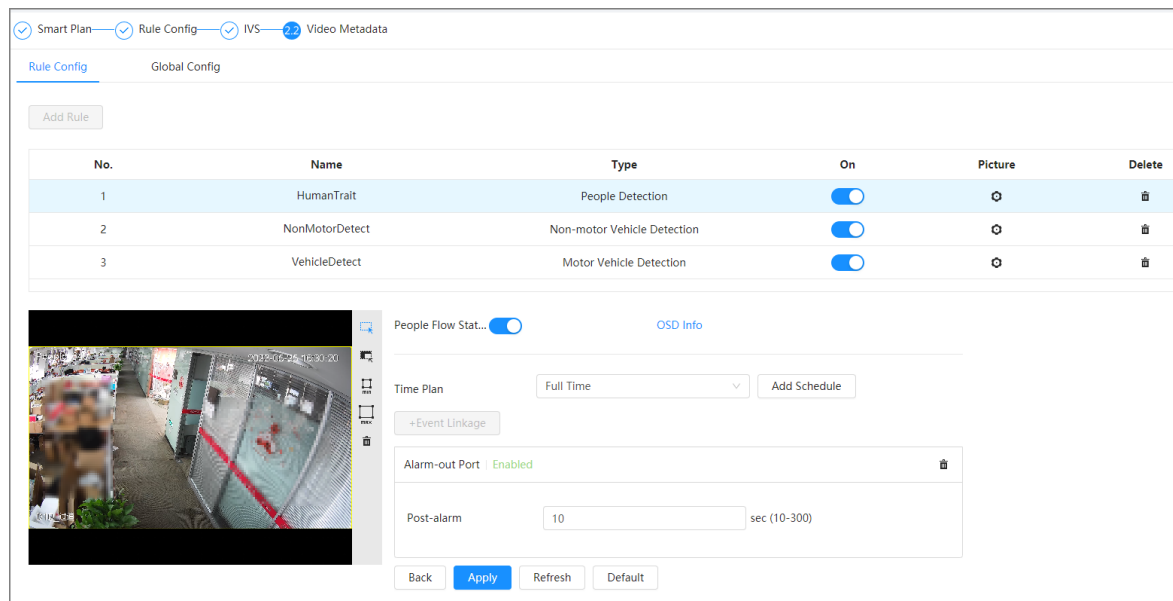
**Figure 8-68 Enable AcuPick**



**Step 3** (Optional) Set IVS function as needed, and then click Next. For details, see "8.4 Setting IVS".

**Step 4** Set video Analytics function. For details, see "8.8 Setting Video Analytics" Support People Detection, Non-motor Vehicle Detection and Motor Vehicle Detection. Only when you enable the rules will the device push the corresponding information to the connected NVR.

**Figure 8-69 Set video Analytics**



**Step 5** Click Apply.

# 9 Security

## 9.1 Security Status

### Background Information

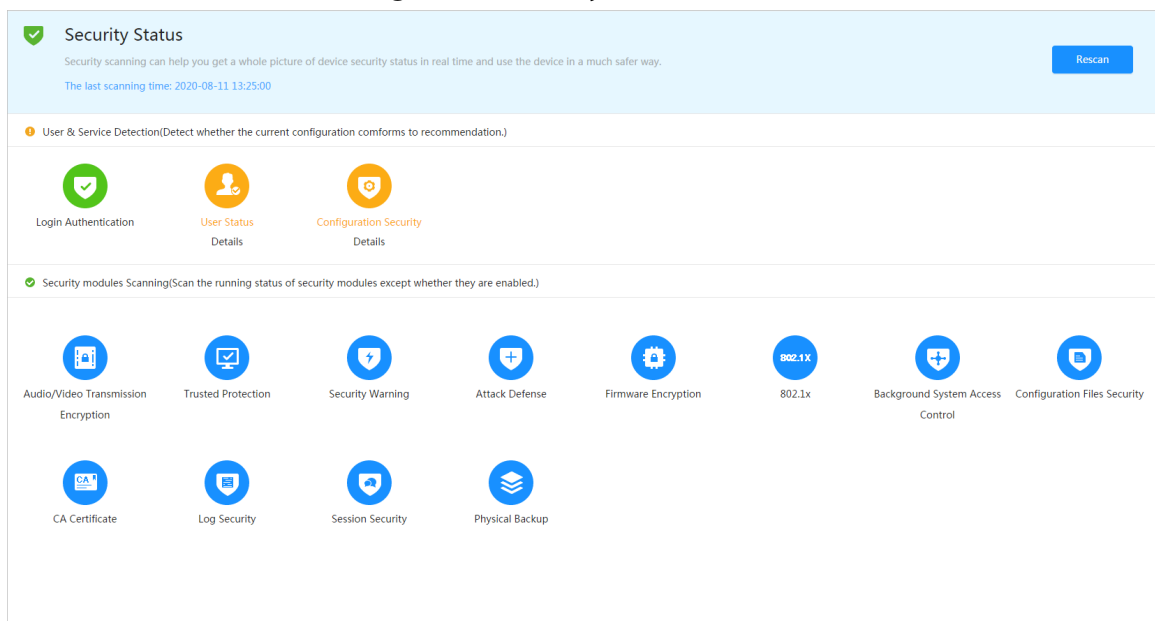
Detect the user and service, and scan the security modules to check the security status of the camera, so that when abnormality appears, you can process it timely.

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

### Procedure

- Step 1** Select Security > Security Status.
- Step 2** Click Rescan to scan the security status of the camera.

Figure 9-1 Security Status

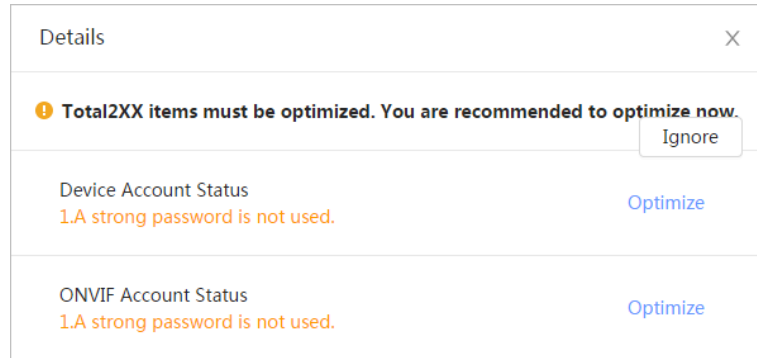


### Related Operations

After scanning, different results will be displayed with different color. 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 Joint Detection, and the exception will be scanned in next scanning.
3. Click Optimize, and the corresponding page is displayed, and you can edit the configuration to clear the exception.

**Figure 9-2 Security Status**



## 9.2 System Service

### 9.2.1 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

#### Procedure

**Step 1** Select Security > System Service > 802.1x.

**Step 2** Select the NIC name as needed, and click  to enable it.

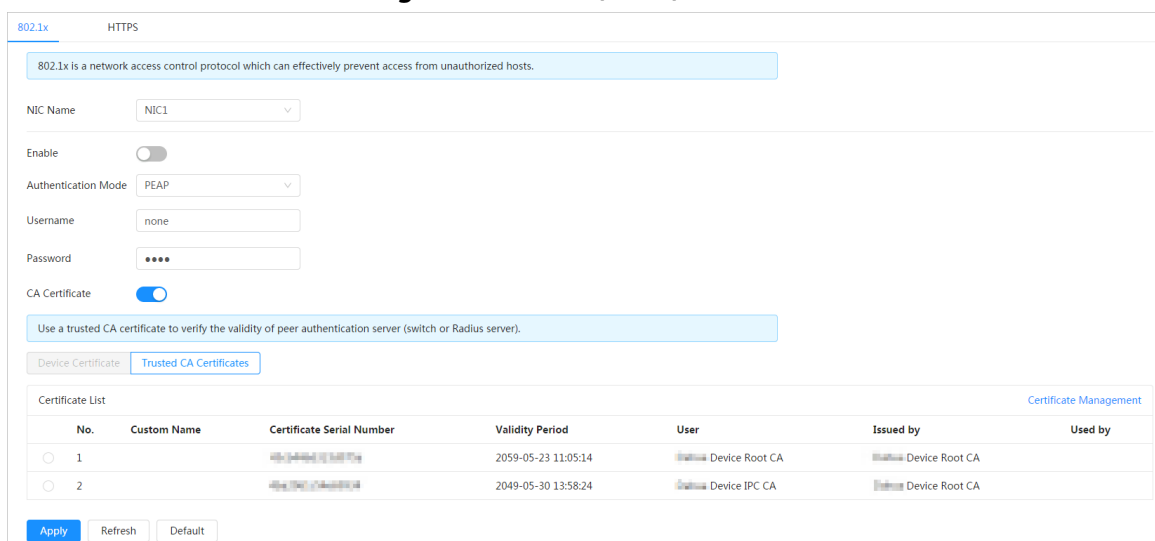
**Step 3** Select the authentication mode, and then configure parameters.

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



**If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".**

**Figure 9-3 802.1x (PEAP)**



- **TLS: Transport Layer Security. It is applied in two communication application**

programs to guarantee the security and integrity of the data.

1. Select TLS as the authentication mode.
2. Enter the username.
3. Click  next to CA certificate, and select the trusted CA certificate in list.



**If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".**

**Figure 9-4 802.1x (TLS)**

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

NIC Name:

Enable:

Authentication Mode:

Username:

CA Certificate:

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

Device Certificate:  Trusted CA Certificates

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
<input type="radio"/> 1		XXXXXXXXXXXX	2059-05-23 11:05:14	Device Root CA	Device Root CA	
<input type="radio"/> 2		XXXXXXXXXXXX	2049-05-30 13:58:24	Device IPC CA	Device Root CA	

**Step 4** Click Apply.

## 9.2.2 HTTPS

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

### Procedure

**Step 1** Select Security > System Service > HTTPS.

**Step 2** Click  to enable it.

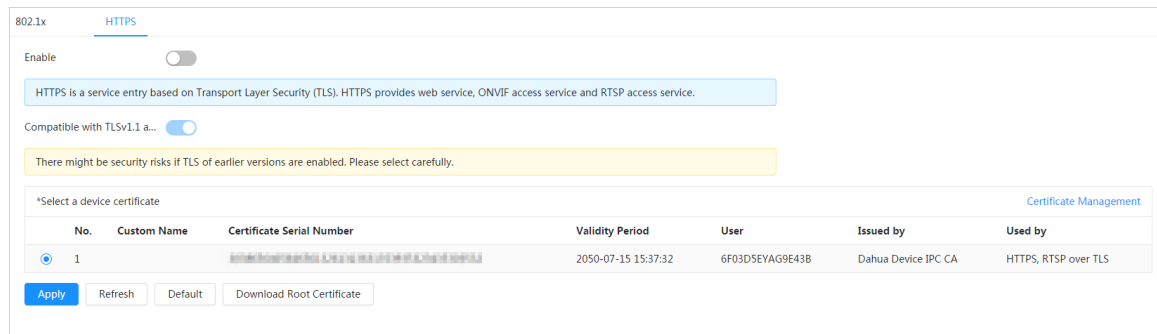
**Step 3** Select the certificate.



**If there is no certificate in the list, click Certificate Management at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".**



Figure 9-5 HTTPS



**Step 4** Click Apply.

## 9.3 Attack Defense

### 9.3.1 Firewall

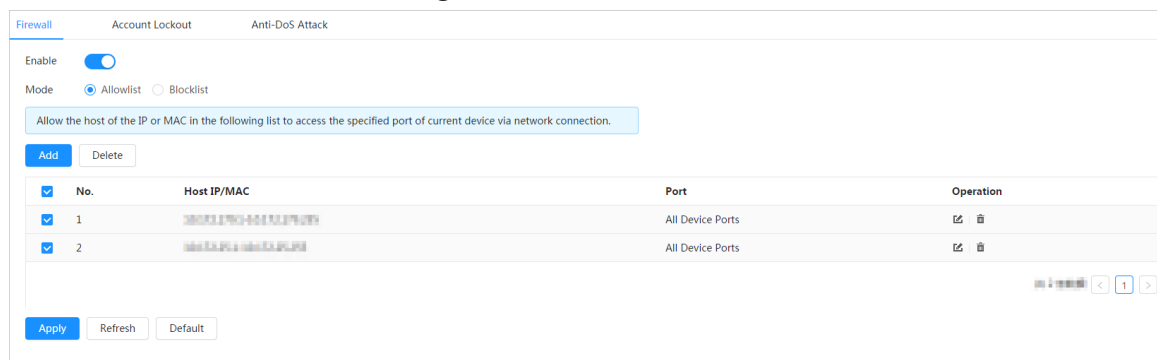
Configure firewall to limit access to the camera.

#### Procedure

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

**Step 2** Click  to enable the firewall function.

Figure 9-6 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 9-7 Firewall

**Step 5** Click Apply.

### Related Operations

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

## 9.3.2 Account Lockout

If you consecutively enter a wrong password 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 login after the login attempts reaches upper limit.

Figure 9-8 Account lockout

**Step 3** Click Apply.

### 9.3.3 Anti-DoS Attack

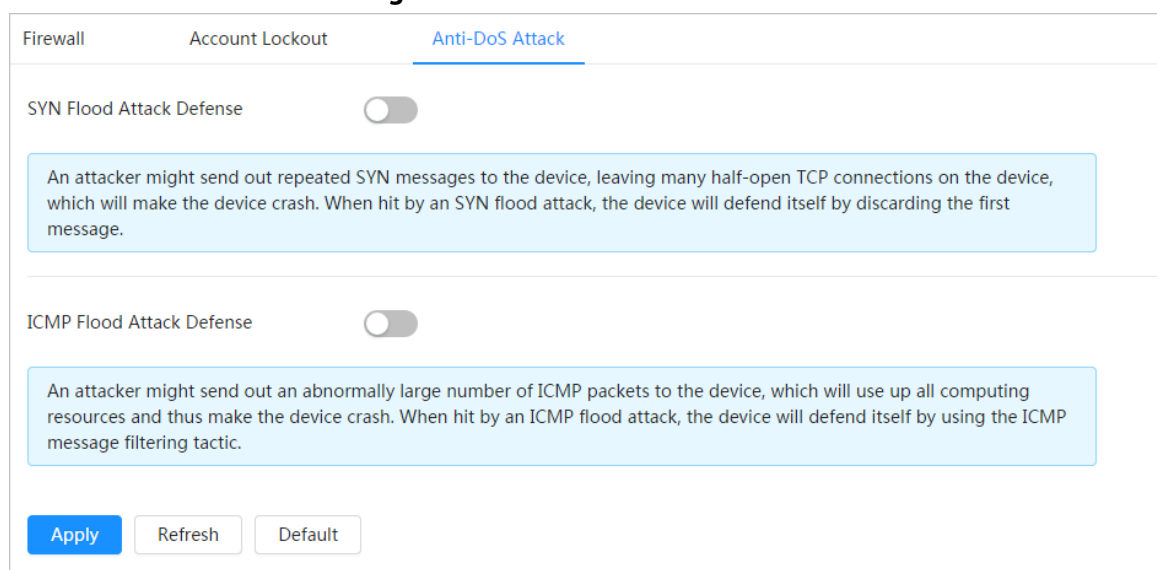
You can enable SYN Flood Attack Defense and ICMP Flood Attack Defense to defend the device against Dos attack.

#### Procedure

**Step 1** Select Security > Attack Defense > Anti-DoS Attack.

**Step 2** Select SYN Flood Attack Defense or ICMP Flood Attack Defense to defend the device against Dos attack.

**Figure 9-9 Anti-DoS attack**



## 9.4 CA Certificate

### 9.4.1 Installing Device Certificate

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

#### 9.4.1.1 Creating Certificate

Creating certificate in the device.

#### Procedure

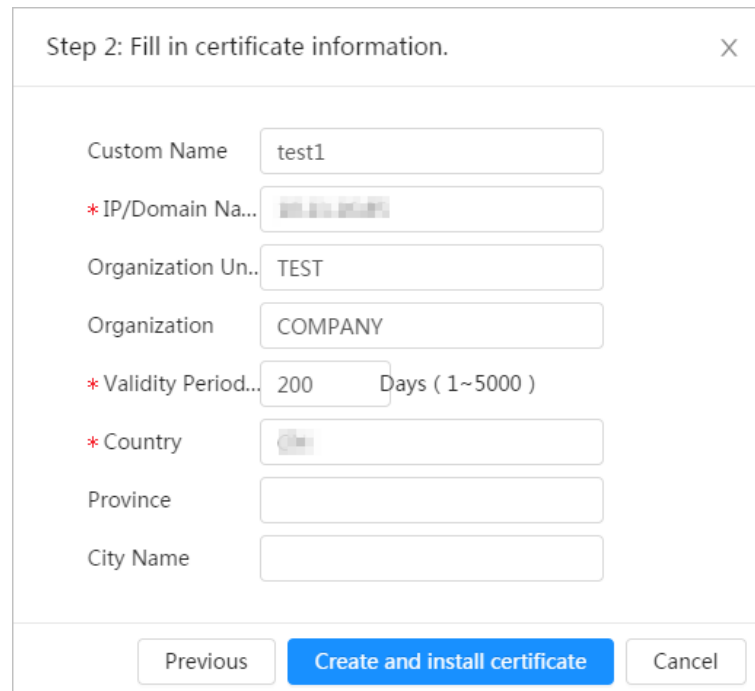
**Step 1** Select Security > CA Certificate > Device Certificate.

**Step 2** Select Installing Device Certificate.

**Step 3** Select Create Certificate, and click Next.

**Step 4** Enter the certificate information.

Figure 9-10 Certificate information (1)



Step 2: Fill in certificate information. [X]

Custom Name

\* IP/Domain Na...

Organization Un...

Organization

\* Validity Period...  Days ( 1~5000 )

\* Country

Province



City Name

Previous  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.

### 9.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

#### Procedure

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

**Step 2** Select Installing Device Certificate.

**Step 3** Select Apply for CA Certificate and Import (Recommended), and click Next.

**Step 4** Enter the certificate information.

**Figure 9-11 Certificate information (2)**

**Step 5** Click **Create and Download**.

Save the request file to your PC.

**Step 6** Apply the CA certificate from the third-party certificate authority.

**Step 7** Import the signed CA certificate.

1) Save the CA certificate to the PC.



2) Do **Step 1** to **Step 3**, and click **Browse** to select the signed CE certificate.

3) Click **Install and Import**.

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

- Click **Recreate** to create the request file again.
- Click **Import Later** to import the certificate next time.

## Related Operations

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

### 9.4.1.3 Installing Existing Certificate

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

#### Procedure

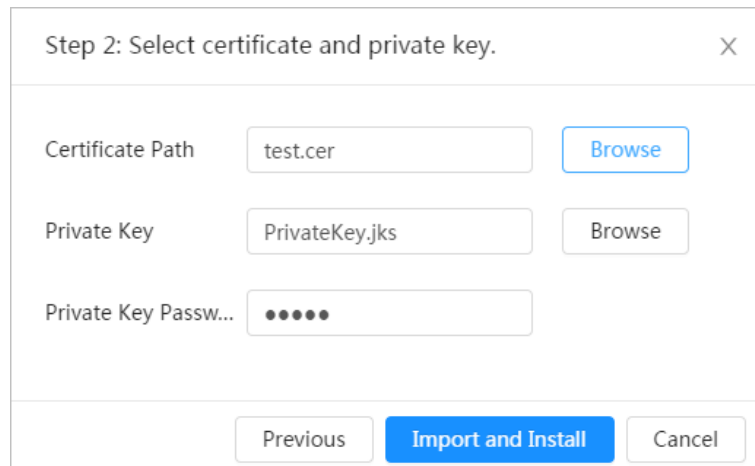
**Step 1** Select **Security > CA Certificate > Device Certificate**.

**Step 2** Select **Installing Device Certificate**.

**Step 3** Select **Install Existing Certificate**, and click **Next**.

**Step 4** Click **Browse** to select the certificate and private key file, and enter the private key password.



**Figure 9-12 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**, you can edit the custom name of the certificate.
- Click  to download the certificate.
- Click  to delete the certificate.

## 9.4.2 Installing Trusted CA Certificate

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.

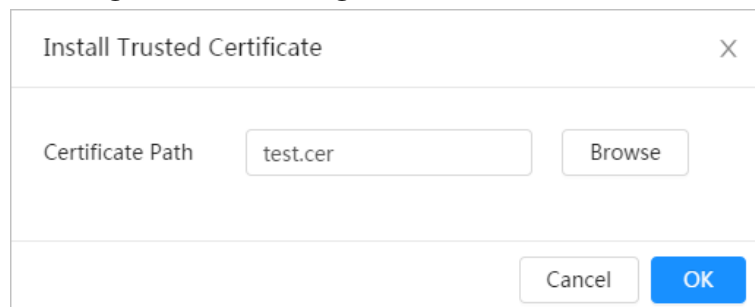
### Procedure

**Step 1** Select **Security > CA Certificate > Trusted CA Certificates**.

**Step 2** Select **Installing Trusted Certificate**.

**Step 3** Click **Browse** to select the certificate.

**Figure 9-13 Installing trusted certificate**



**Step 4** Click **OK**.

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

### Related Operations

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

- Click to download the certificate.
- Click to delete the certificate.

## 9.5 A/V Encryption

The device supports audio and video encryption during data transmission.



**You are recommended to enable A/V Encryption function. There might be safety risk if this function is disabled.**

### Procedure

**Step 1** Select Security > A/V Encryption.

**Step 2** Configure the parameters.

Figure 9-14 A/V encryption

Table 9-1 A/V encryption parameter

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol.  <b>There might be safety risk if this service is disabled.</b>
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.

Area	Parameter	Description
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "9.4.1 Installing Device Certificate".

**Step 3** Click Apply.

## 9.6 Security Warning

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

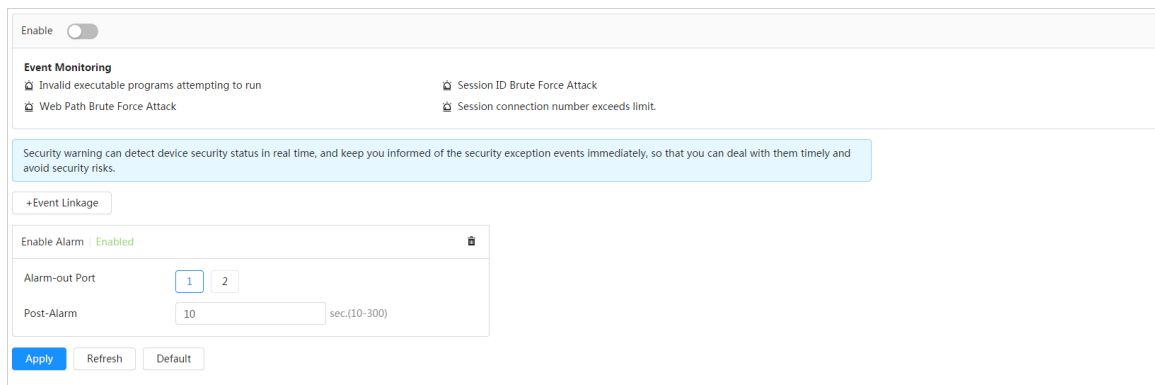
### Procedure

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

**Step 2** Click  next to Enable to enable security warning.

**Step 3** Configure the parameters.

Figure 9-15 Security warning



**Step 4** Set arming periods and alarm linkage action. For details, see "6.5.1.2 Alarm Linkage". Click + Event Linkage to set the linkage action.

**Step 5** Click Apply.



# 10 Record

This section introduces the functions and operations of video playback.

## 10.1 Playback

### 10.1.1 Playing Back Video

This section introduces the operation of video playback.

#### Prerequisites

- This function is available on the camera with SD card.
- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "10.2 Setting Record Control", "10.3 Setting Record Plan", and "10.4 Storage".

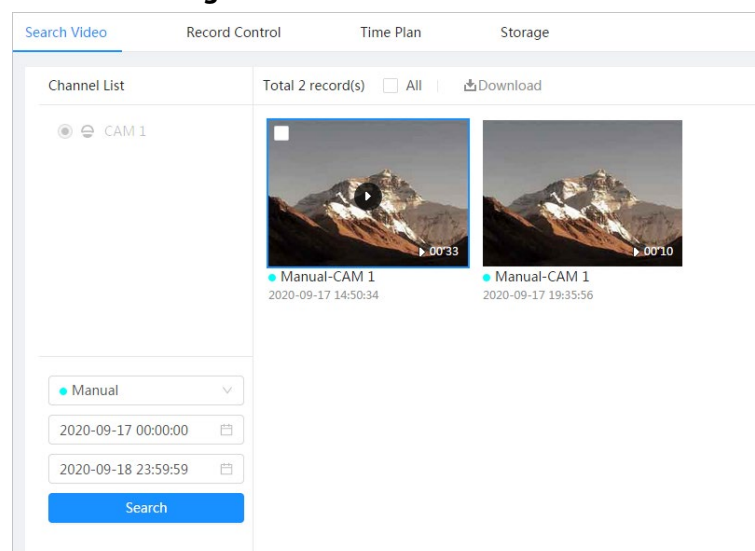
#### Procedure

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

**Step 2** Select the channel, the record type, and record time, and then click Search.

- Click All, and select the record type from the drop-down list, you can select from All, General, Event, Alarm, and Manual.  
When selecting Event as the record type, you can select the specific event types, such as Motion Detection, Video Tamper and Scene Changing.
- The dates with blue dots indicate there are videos recorded on those days.

Figure 10-1 Search video



**Step 3** Point to the searched video, and then click to play back the selected video. The video playback page is displayed.

Figure 10-2 Video playback

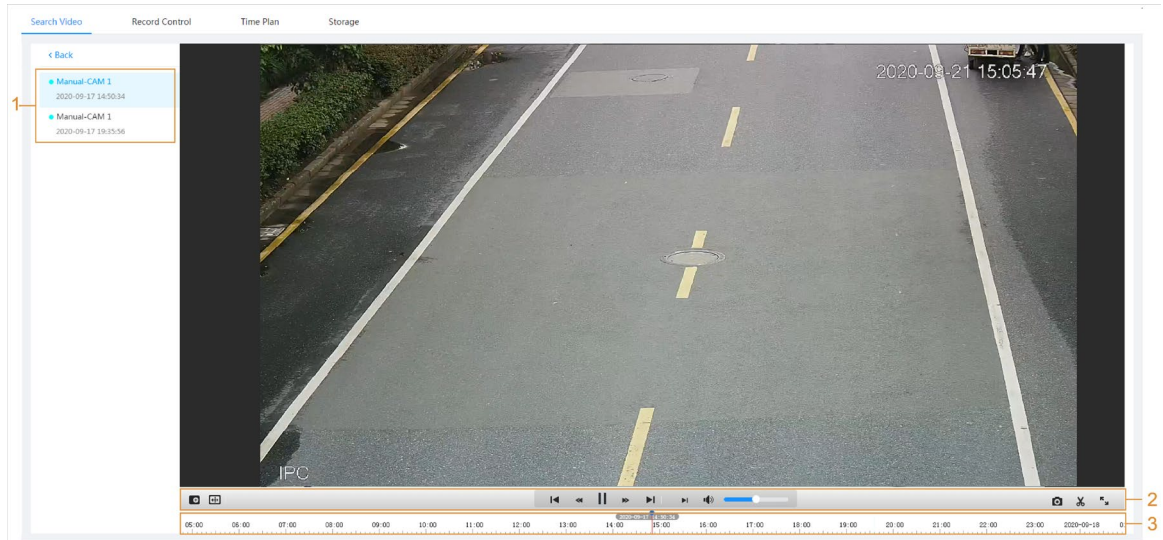

















Table 10-1 Description of video playback page

No	Function	Description
1	Recorded video list	<p>Displays all searched recorded video files. Click any files to play back it.</p> <p>Click Back at the upper-left corner to go to the Search Video page.</p>
2	Digital Zoom	<p>You can zoom video image of the selected area through two operations.</p> <ul style="list-style-type: none"> <li>Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area.</li> <li>Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.</li> </ul>
	Analytics+ Rule	<p>Click , and then select Enable to display Analytics+ rules and detection box; select Disable to stop the display. It is enabled by default.</p> <p> Analytics+ rules is valid only when you enabled the rule during recording.</p>

No	Function	Description
	Play control bar	<p><b>Controls playback.</b></p> <ul style="list-style-type: none"> <li>• : Click the icon to play back the previous recorded video in the recorded video list.</li> <li>• : Click the icon to slow down the playback.</li> <li>• : Click the icon to stop playing back recorded videos. The icon changes to , click the icon to play back recorded videos.</li> <li>• : Click the icon to speed up the playback.</li> <li>• : Click the icon to play back the next recorded video in the recorded video list.</li> <li>• : Click the icon to play the next frame.</li> </ul>
	Sound	<p><b>Controls the sound during playback.</b></p> <ul style="list-style-type: none"> <li>• : Mute mode.</li> <li>• : Vocal state. You can adjust the sound.</li> </ul>
	Snapshot	<p>Click  to capture one picture of the current image, and it will be saved to the configured storage path.</p>  <p><b>About viewing or configuring storage path, see "6.1 Local".</b></p>
	Video clip	<p>Click , and clip a certain recorded video and save it. For details, see "10.1.2 Clipping Video".</p>
	Full Screen	<p>Click , and the image is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.</p>
3	Progress bar	<p><b>Displays the record type and the corresponding period.</b></p> <ul style="list-style-type: none"> <li>• Click any point in the colored area, and the system will play back the recorded video from the selected moment.</li> <li>• Each record type has its own color, and you can see their relations in Record Type bar.</li> </ul>

## 10.1.2 Clipping Video

### Procedure

**Step 1** Click .

**Step 2** Drag the clipping box on the progress bar to select the start time and end time of the target video

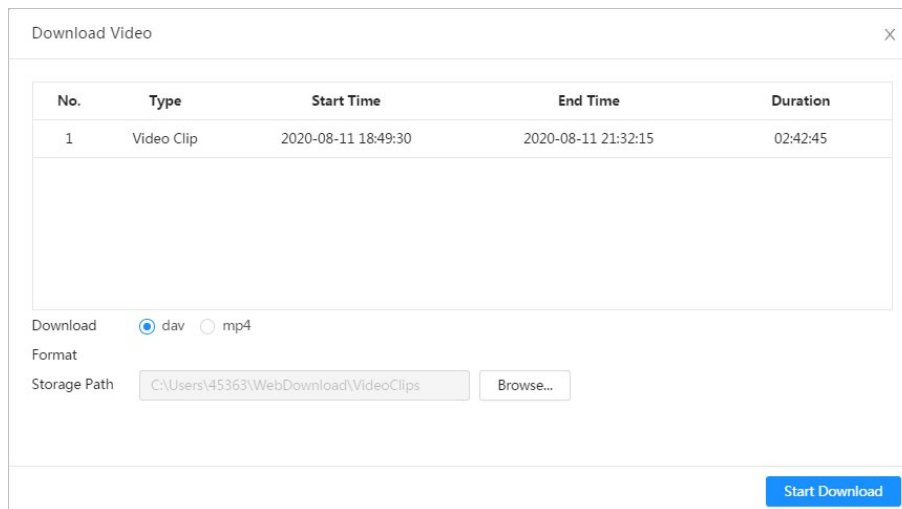
Figure 10-3 Clipping video



**Step 3** Click OK to download the video.

**Step 4** Select the download format and storage path.

Figure 10-4 Clipping video



**Step 5** Click Start Download.

The playback stops and the clipped file is saved in the configured storage path. For details of storage path, see "6.1 Local".

### 10.1.3 Downloading Video

Download videos to a defined path. You can download a single video, or download them in batches.



- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "6.1 Local".

#### Procedure

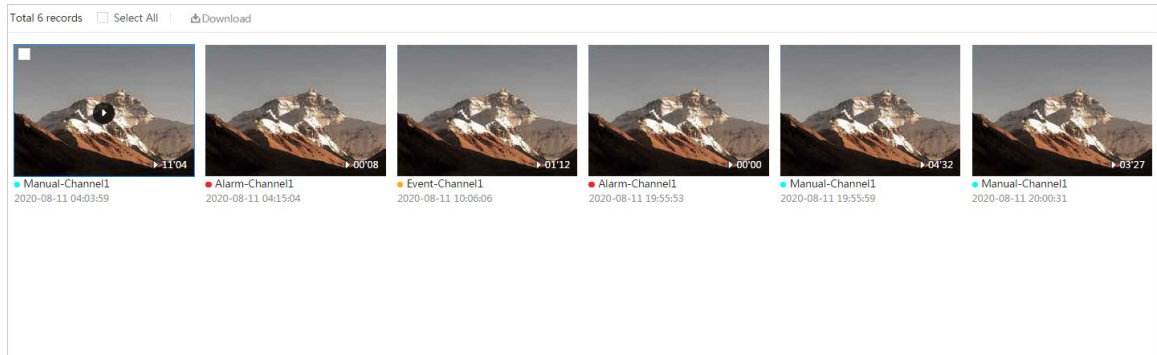
**Step 1** Select Record > Search Video.

**Step 2** Select the channel, the record type, and record time, and the click Search.

**Step 3** Select the videos to be downloaded.

- Select  at the upper-right corner of each video file to select one or multiple videos.
- Select  next to Select All to select all searched videos.

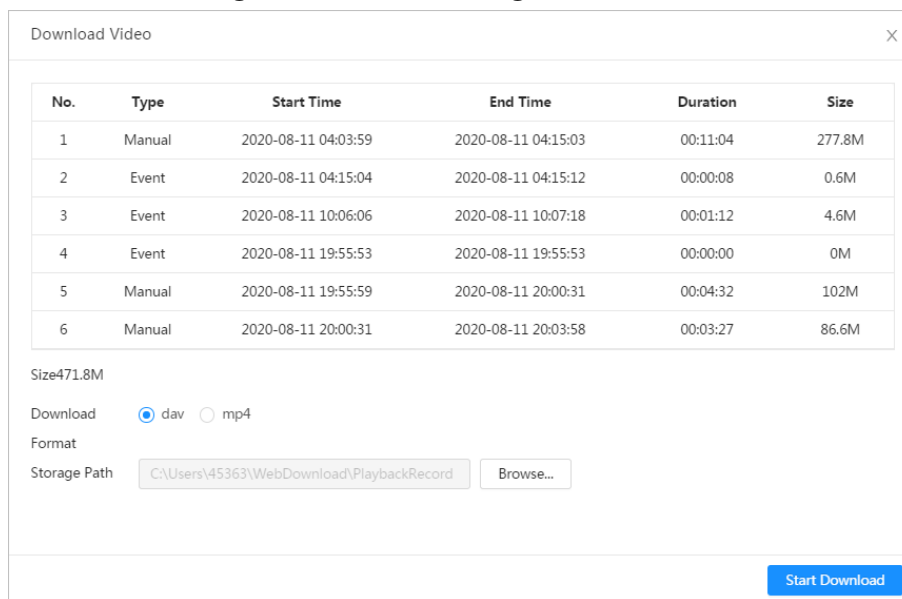
**Figure 10-5 Selecting video file**



**Step 4** Click Download.

**Step 5** Select the download format and storage path.

**Figure 10-6 Downloading video**



**Step 6** Click Start Download.

The downloaded files are saved in the configured storage path. For details of storage path, see "6.1 Local".

## 10.2 Setting Record Control

Set parameters such as pack duration, pre-event record, disk full, record mode, and record stream.

### Procedure


**Step 1** Click Record in the home page, and then click the Record Control tab.

Figure 10-7 Record control

Channel	<input type="text" value="CAM 1"/>	
Max Duration	<input type="text" value="30"/>	min.(1-120)
Pre-Record	<input type="text" value="5"/>	sec.(0-5)
Record Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual <input type="radio"/> Off	
Record Stream	<input type="text" value="Sub Stream"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

**Step 2** Set parameters.

Table 10-2 Description of record control parameters

Parameter	Description
Max Duration	The time for packing each video file.
Pre-Record	<p>The time to record the video in advance of a triggered alarm event. For example, if the pre-event record is set to be 5 s, the system saves the recorded video 5 s before the alarm is triggered.</p>  <p>When an alarm or motion detection links recording, and the recording is not enabled, the system saves the video data within the pre-event record time to the video file.</p>
Record Mode	When you select Manual, the system starts recording; when you select Auto, the system starts recording in the configured period of record plan.
Record Stream	Select record stream, including Main Stream and Sub Stream.

**Step 3** Click Apply.

## 10.3 Setting Record Plan

After the corresponding alarm type (Normal, Motion, and Alarm) is enabled, the record channel links recording.

Set certain days as holiday, and when the Record is selected in the holiday schedule, the system records video as holiday schedule defined.

### Procedure

**Step 1** Click Record on the home page, and then click the Time Plan tab.

Figure 10-8 Time plan



**Step 2** Set record plan.

Green represents normal record plan (such as timing recording); yellow represents motion record plan (such as recording triggered by intelligent events); red represents alarm record plan (such as recording triggered by alarm-in). Select a record type, such as Normal, and directly press and drag the left mouse button to set the period for normal record on the timeline.



- 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 check box to select all day to copy the configuration.
- You can set 6 periods per day.

**Step 3** Click Apply.

**Step 4** Click Holiday to set holidays.

Figure 10-9 Time plan

- Step 5** Click  to enable the holiday configuration, and select the days that you need to set as holiday.  
Click Clear to cancel the selection.



**When holiday schedule setting is not the same as the general setting, holiday schedule setting is prior to the general setting. For example, with holiday schedule enabled, if the day is holiday, the system snapshots or records as holiday schedule setting; otherwise, the system snapshots or records as general setting.**

- Step 6** Click OK.

## 10.4 Storage

This section introduces the configuration of the storage method for the recorded videos.

### Procedure


- Step 1** Select Record > Storage.

Figure 10-10 Live

- Step 2** Select the storage method that you need for different types of recorded videos.



Table 10-3 Description of storage parameters

Parameter	Description
Event Type	Select from Scheduled, Motion Detection and Alarm.
Disk Full	<p>Recording strategy when the disk is full.</p> <ul style="list-style-type: none"> <li>• <b>Overwrite:</b> Cyclically overwrite the earliest video when the disk is full.</li> <li>• <b>Stop:</b> Stop recording when the disk is full.</li> </ul>
Storage Method	<p>Select from Local storage and Network storage</p> <ul style="list-style-type: none"> <li>• <b>Local storage:</b> Save the recorded videos in the internal SD card.</li> </ul>  <p>Local storage is displayed only on models that support SD card.</p> <ul style="list-style-type: none"> <li>• <b>Network storage:</b> Save the recorded videos in the FTP server or NAS.</li> </ul>

**Step 3** Click Apply.

## 10.4.1 Local Storage

### Procedure

**Step 1** Select Record > Storage.

**Step 2** Select the recording strategy in Disk Full.

- **Overwrite:** Cyclically overwrite the earliest video when the disk is full.
- **Stop:** Stop recording when the disk is full.

**Step 3** Select Local storage in Storage Method to save the recorded videos in the internal SD card.

Figure 10-11 Local storage

**Step 4** Click Apply.

## 10.4.2 Network Storage

You can select from FTP and NAS.

When the network does not work, you can save all the files to the internal SD card for emergency.

### 10.4.2.1 FTP

Enable this function, and you can save all the files in the FTP server.

#### Procedure

**Step 1** Select Record > Storage.

**Step 2** Select the recording strategy in Disk Full.

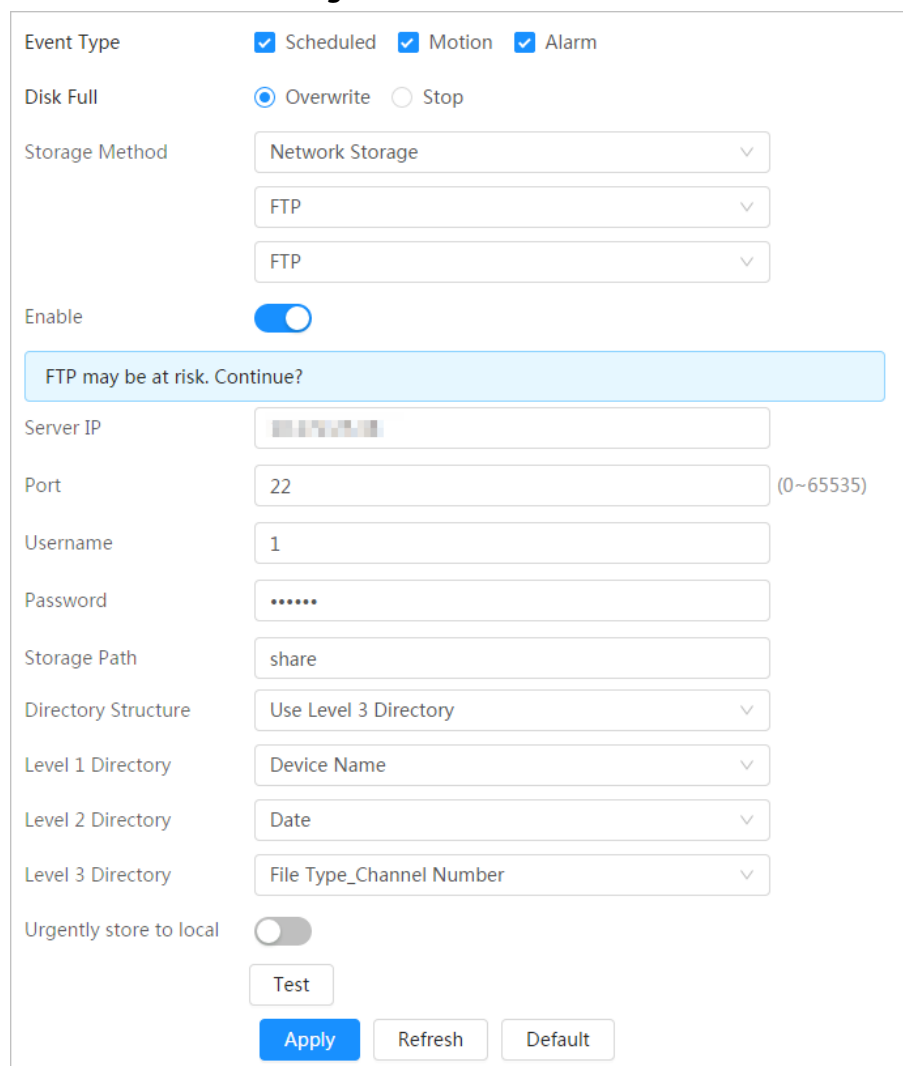
- **Overwrite:** Cyclically overwrite the earliest video when the disk is full.
- **Stop:** Stop recording when the disk is full.

**Step 3** Select Network storage in Storage Method, and select FTP to save the recorded videos in FTP server.

You select FTP or SFPT from the drop-down list. SFPT is recommended to enhance network security.

**Step 4** Click  next to Enable to enable the FTP function.

Figure 10-12 FTP



The screenshot shows the FTP configuration page with the following settings:

- Event Type:** Scheduled, Motion, Alarm (all checked).
- Disk Full:** Overwrite (selected), Stop.
- Storage Method:** Network Storage (selected), FTP (selected), FTP (selected).
- Enable:**  (checked).
- Warning:** FTP may be at risk. Continue?
- Server IP:** [Redacted]
- Port:** 22 (range 0~65535)
- Username:** 1
- Password:** [Redacted]
- Storage Path:** share
- Directory Structure:** Use Level 3 Directory
- Level 1 Directory:** Device Name
- Level 2 Directory:** Date
- Level 3 Directory:** File Type\_Channel Number
- Urgently store to local:**  (unchecked)
- Buttons:** Test, Apply, Refresh, Default.

**Step 5** Configure FTP parameters.

Table 10-4 Description of FTP parameters

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Directory Structure	Set the directory structure, and you can select Use Level 1 Directory, Use Level 2 Directory, and Use Level 3 Directory
Level 1 Directory	Set the Level 1 directory name, and you can select from Device name, Device IP, and Custom. When you select Custom, please enter the custom directory.
Level 2 Directory	Set the Level 2 directory name, and you can select from File Type, Date, File Type_Channel Number, and Custom. When you select Custom, please enter the custom directory.
Level 3 Directory	
Urgently store to local	Click <input type="checkbox"/> , and when the FTP server does not work, all the files are saved to the internal SD card.

**Step 6** Click Save.

**Step 7** Click Test to test whether FTP function works normally.

### 10.4.2.2 NAS

Enable this function, and you can save all the files in the NAS.

#### Procedure

**Step 1** Select Record > Storage.

**Step 2** Select the recording strategy in Disk Full.

- Overwrite: Cyclically overwrite the earliest video when the disk is full.
- Stop: Stop recording when the disk is full.

**Step 3** Select Network storage in Storage Method, and select NAS to save the recorded videos in NAS server.

**Step 4** Select NAS protocol type.

- NFS (Network File System): A file system which enables computers in the same network share files through TCP/IP.
- SMB (Server Message Block): Provides shared access for clients and the server.

**Figure 10-13 FTP**

Event Type	<input checked="" type="checkbox"/> Scheduled <input checked="" type="checkbox"/> Motion <input checked="" type="checkbox"/> Alarm
Disk Full	<input checked="" type="radio"/> Overwrite <input type="radio"/> Stop
Storage Method	Network Storage <input type="button" value="v"/>
	NAS <input type="button" value="v"/>
Protocol Type	SMB <input type="button" value="v"/>
Enable	<input type="checkbox"/>
Server IP	0.0.0.0
Storage Path	
Username	anonymity
Password	.....
	<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>

**Step 5** Configure NAS parameters.

**Table 10-5 Description of NAS parameters**

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
Username	When selecting SMB protocol, you are required to enter username and password. Enter them as needed.
Password	

**Step 6** Click Apply.

# 11 Picture

This section introduces the related functions and operations of picture playback.

## 11.1 Playback

### 11.1.1 Playing Back Picture

This section introduces the operation of picture playback.

#### Prerequisites

- This function is available on the camera with SD card.
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see "11.3 Setting Snapshot Plan".

#### Procedure

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

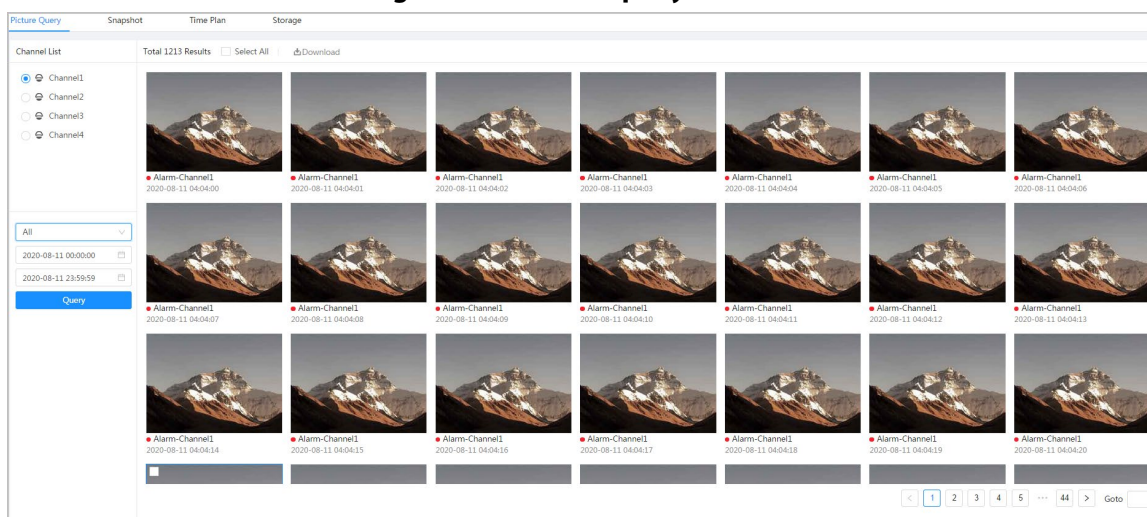
**Step 2** Select the channel, the snapshot type, and snapshot time, and then click Search.

- Click All, and select the record type from the drop-down list, you can select from All, General, Event, and Alarm.

When selecting Event as the snapshot type, you can select the specific event types, such as Motion Detection, Video Tamper and Scene Changing.

- The dates with blue dots indicate there are snapshots on those days.

Figure 11-1 Picture query



**Step 3** Point to the searched picture, and then click to play back the selected picture. The picture playback page is displayed.

Figure 11-2 Picture playback

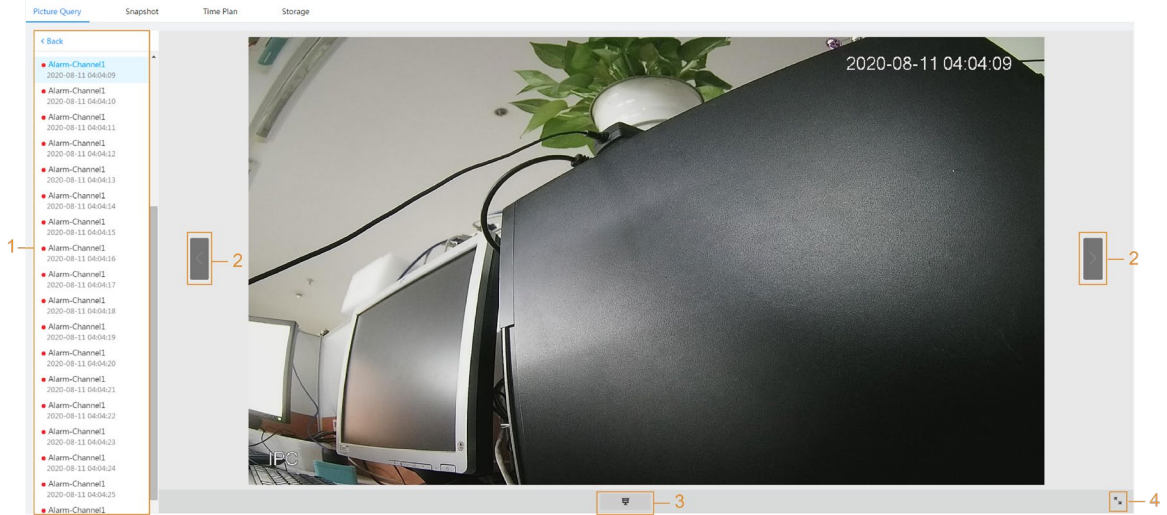


Table 11-1 Description of playback page

No.	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play back it. Click Back at the upper-left corner to go to the Picture Query page.
2	Manual display	<ul style="list-style-type: none"> <li>Click  to display the previous snapshot in the snapshot list.</li> <li>Click  to display the next snapshot in the snapshot list.</li> </ul>
3	Slide show	Click  to display the snapshots list one by one in slide show mode.
4	Full screen	Click , and the snapshot is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.

### 11.1.2 Downloading Picture

Download pictures to a defined path. You can download a single picture, or download them in batches.



- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "6.1 Local".

#### Procedure

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

**Step 2** Select the channel, the snapshot type, and snapshot time, and then click Search.

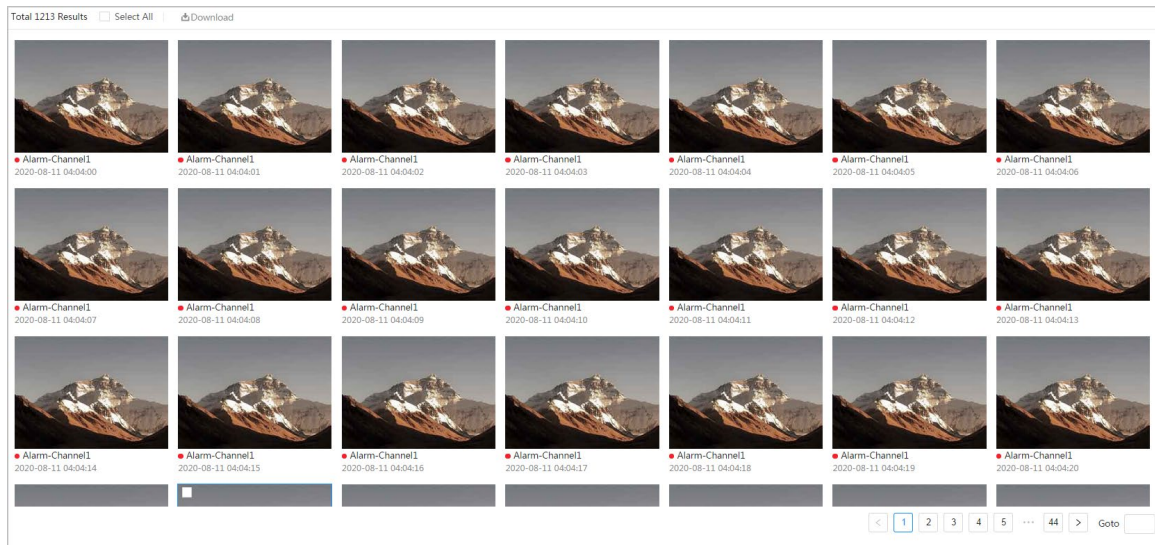
**Step 3** Select the pictures to be downloaded.

- Select  at the upper-right corner of each picture file to select one or multiple

pictures.

- Select  next to Select All to select all searched pictures.

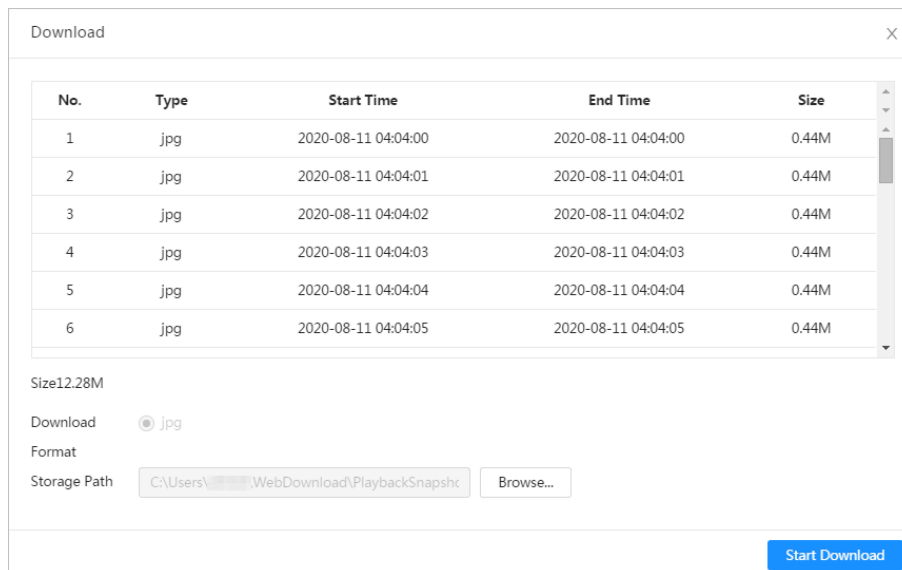
**Figure 11-3 Selecting picture file**



**Step 4** Click Download.

**Step 5** Select the download format and storage path.

**Figure 11-4 Downloading picture**



**Step 6** Click Start Download.

The downloaded pictures are saved in the configured storage path. For details of storage path, see "6.1 Local".

## 11.2 Setting Snapshot Parameters

Set the snapshot parameters, including type, size, quality and Interval.


### Procedure

**Step 1** Select Picture > Snapshot.

**Step 2** Select the channel and set the parameters.

Figure 11-5 Snapshot

Table 11-2 Description of snapshot parameters

Parameter	Description
Type	<p>You can select from Scheduled and Event.</p> <ul style="list-style-type: none"> <li>Scheduled: Capture images in configured period.</li> <li>Event: Capture images when configured event is triggered, such as Motion Detection, Video Tamper and Scene Changing.</li> </ul> <p> <b>Make sure that you have enable the corresponding event detection and the snapshot function.</b></p>
Size	It is same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select Custom to set the frequency as needed.

**Step 3** Click Apply.

## 11.3 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time. For detailed operation, see "10.3 Setting Record Plan".

## 11.4 Storage

Set the storage method for the snapshot. For detailed operation, see "10.4 Storage".

## 11.5 Setting Upload Method

Automatically upload images to the defined server through HTTP protocol, and configure parameters.



## Background Information

You do not need to set upload period. When an alarm is triggered, images will be automatically uploaded to the defined server.


## Procedure

- Step 1** On the web page, select Picture > Auto Upload.
- Step 2** Enable the function.
- Step 3** Click Add, and then configure parameters of HTTP upload method.  
You can add two server information at most.

Figure 11-6 Image Upload

No.	IP/Domain Name	Port	Path	Event Type	Test	Delete
1	Example : 172.16.1.1	Example : 80	Example : /example/	None	Test	✖
2	Example : 172.16.1.1	Example : 80	Example : /example/	None	Test	✖

Table 11-3 Description of HTTP mode Parameter

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Event type	<p>Select the event type form the drop-down list. You can select more than one types at the same time.</p>  <p>The event types in the drop-down list are the same with that of picture playback.</p>
Test	Test the network connection between the camera and the server.

- Step 4** Click Apply.

# 12 Report

## 12.1 Viewing Report

View the statistics results of Analytics+ functions in report form.

Figure 12-1 Report

- The period for the report is the latest 24 hours by default.
- Click to customize the period for the report.
- Click Today, This Week, This Month, or This Year. The start time of the period is 0 o'clock of the first day, and the end time is the current time.

### 12.1.1 Face Detection+

View the statistics result of Face Detection+ in report form.

#### Procedure

**Step 1** Select Report > Report > Face Detection+.

**Step 2** Set the period for the report.



**For multi-channel camera, select the channel first.**

**Step 3** Select the gender and age.

**Step 4** Click Search.

**Figure 12-2 Face Detection+ report**



## Related Operations

- **Select the report form**  
Click to display the report in line chart; click to display the report in bar chart.
- **Select the statistics type on the upper-right corner**  
The statistics result of unselected types will not be displayed.
- **Export reports**  
Select the file format, and then click Export.
  - ◇ **Select png:** Displays the report in picture format.
  - ◇ **Select csv:** Displays the report in list format.

## 12.1.2 Video Analytics

View the statistics result of video Analytics in report form.

### Procedure

- Step 1** Select Report > Report > Video Analytics.
- Step 2** Set the period for the report.

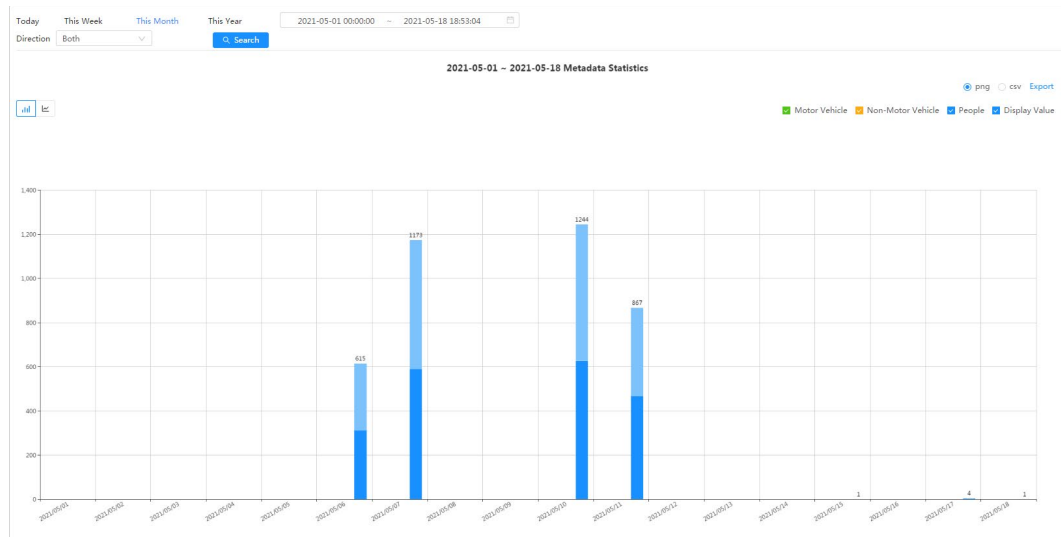


**For multi-channel camera, select the channel first.**

**Step 3** Select the tripwire direction.

**Step 4** Click Search.

**Figure 12-3 Video Analytics report**



## Related Operations

- **Select the report form**  
Click to display the report in line chart; click to display the report in bar chart.
- **Select the statistics type on the upper-right corner**  
The statistics result of unselected types will not be displayed.
- **Export reports**  
Select the file format, and then click Export.
  - ◇ **Select png:** Displays the report in picture format.
  - ◇ **Select csv:** Displays the report in list format.

## 12.1.3 People Counting

Search for the counting results with different rules and counting methods.

### Prerequisites

Make sure that you have configured the rule before searching for the report.

### Procedure

**Step 1** Select Report > Report > People Counting.

**Step 2** Set search conditions.



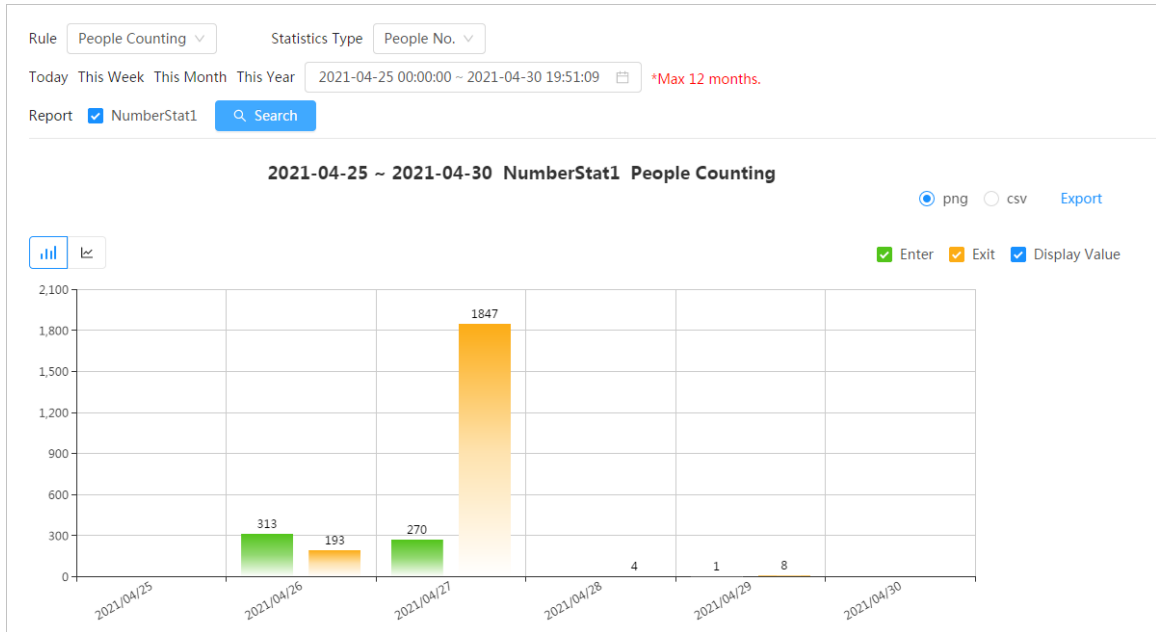
**For multi-channel camera, select the channel first.**

Table 12-1 Set search conditions

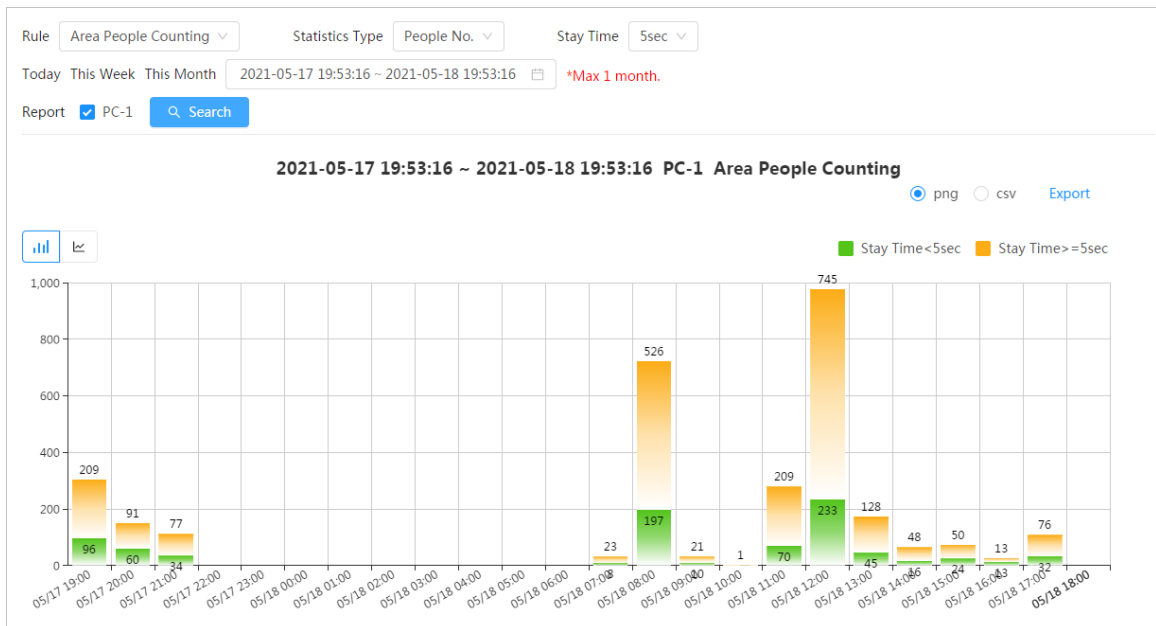
Parameter	Description
Rule	Select the rule as needed, and then you need to select the statistics type according to the select rule.
Statistics Type	<p>The statistics type of the people counting report.</p> <ul style="list-style-type: none"> <li>• <b>People No.:</b> Displays the report of the number of people that meet the configured condition.</li> <li>• <b>Strand Time:</b> Displays the report of the average stranding time in the detection area during a certain period. It is available when the rule of Area People Counting is selected.</li> </ul>
Stay Time	<p>When selecting rule to Area People Counting, and statistics type to People No., you need to configure this parameter.</p> <p>The report displays the number of people whose stay time is shorter than the stay time threshold and is equal to or longer than the stay time threshold.</p>
Queue Time	<p>When selecting rule to Queuing, and statistics type to People No., you need to configure this parameter.</p> <p>The report displays the number of people whose stay time is shorter than Queuing Time and is equal or longer than Queuing Time.</p>
Period for the report	<p>Set the period for the report.</p> <ul style="list-style-type: none"> <li>• When selecting rule to People Counting, you can view the daily, weekly, monthly and yearly report, and you can also customize the period.</li> <li>• When selecting rule to Area People Counting or Queuing, you can view the daily, weekly, and monthly report, and you can also customize the period.</li> </ul>
Report	Select the rule name of the report that you want to search. You can select multiple rule names at the same time.

**Step 3** Click Search.

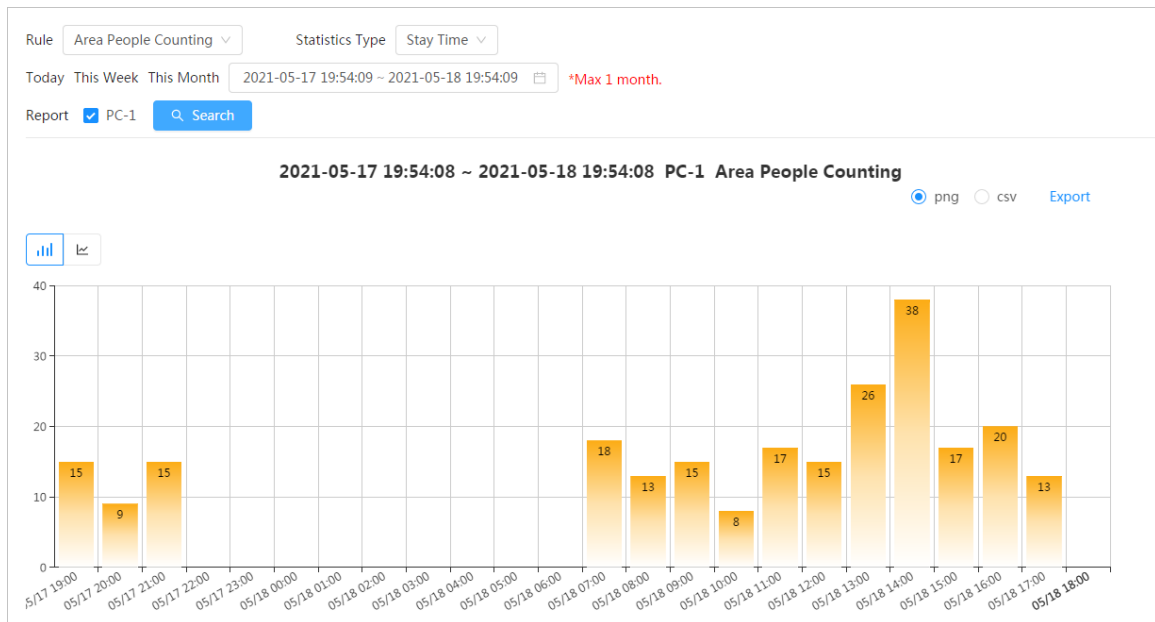
**Figure 12-4 People counting**



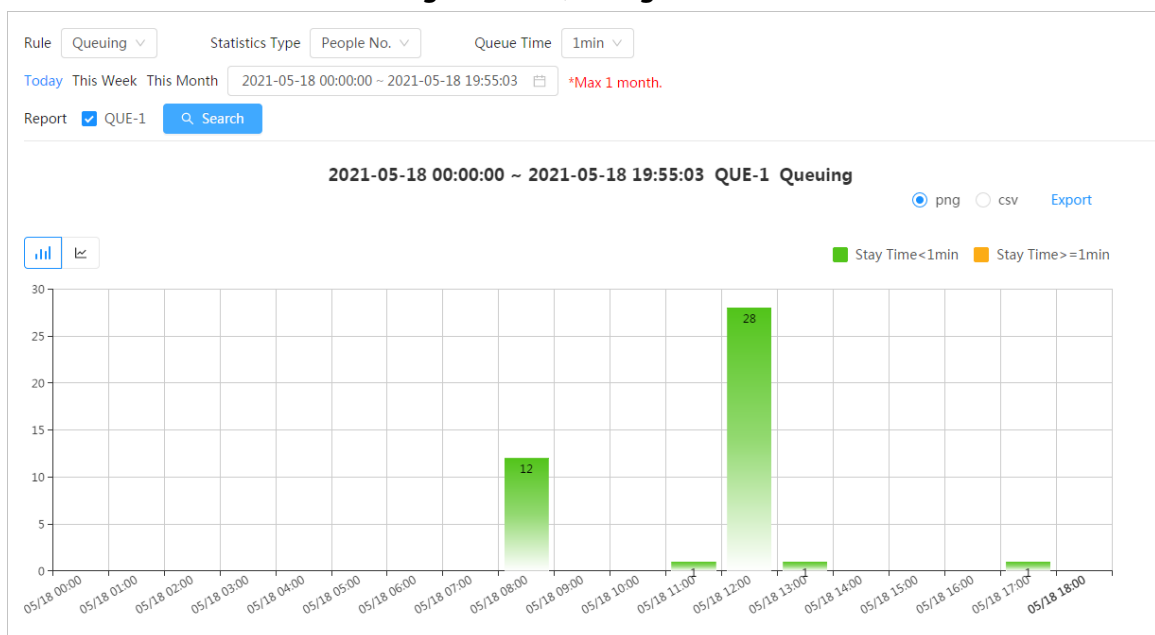
**Figure 12-5 Area people counting (number of people)**



**Figure 12-6 Area people counting (stay time)**



**Figure 12-7 Queuing**



## Related Operations

- **Select the report form**  
Click to display the report in line chart; click to display the report in bar chart.
- **Select the statistics type on the upper-right corner**  
The statistics result of unselected types will not be displayed.
- **Export reports**  
Select the file format, and then click Export.
  - ◇ **Select png:** Displays the report in picture format.
  - ◇ **Select csv:** Displays the report in list format.

## 12.1.4 Crowd Distribution

You can search for the number of people at a certain moment and get daily/weekly/monthly reports.

### Prerequisites

Confirm that crowd distribution map function has already set; otherwise the corresponding report cannot be searched.

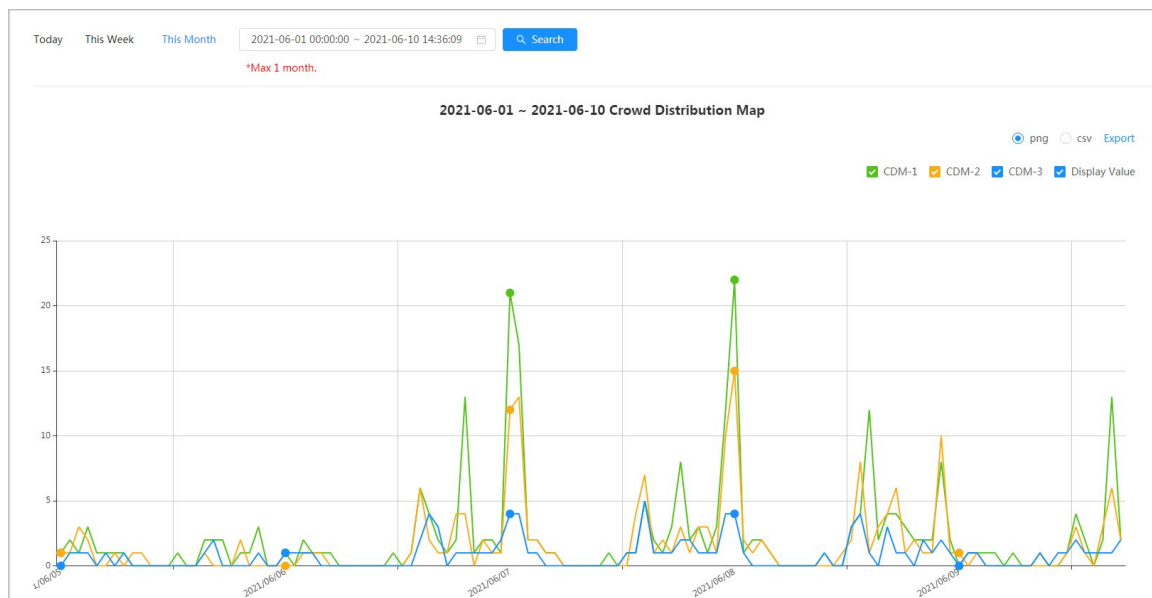
### Procedure

**Step 1** Select Report > Report > Crowd Distribution Map.

**Step 2** Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the period.

**Step 3** Click Search.

Figure 12-8 Crowd distribution map



### Related Operations

- **Select statistics type**

Click  CDM-1  CDM-2  CDM-3  Display Value and select the type needed.

- **Export statistic report**

Select the exact format and click Export, the report will be saved to the storage path of your browser.

- ◇ Select png: Displays the report in picture format.
- ◇ Select csv: Displays the report in list format.

## 12.1.5 Vehicle Density

Search for the number of cars at a certain moment in each statistical area.

### Procedure

**Step 1** Select Report > Report > Vehicle Density.



**Step 2** Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the period.

**Step 3** Click Search.

**Figure 12-9 Vehicle density map**



## Related Operations

- **Select statistics type**

Click  VD-1  VD-2  Display Value to select the type as needed.

- **Export statistic report**

Select the exact format and click Export, the report will be saved to the save path of your browser.

- ◇ Select png: Displays the report in picture format.
- ◇ Select csv: Displays the report in list format.

## 12.1.6 Heat Map

View heat map and track map. You can search the detection results by number of people and stay time, and then generate the heat map. Heat map is not available on economic fisheye cameras.

### Procedure

**Step 1** Select Report > Report > Heat Map.

**Step 2** Set search conditions.



**For multi-channel camera, select the channel first.**

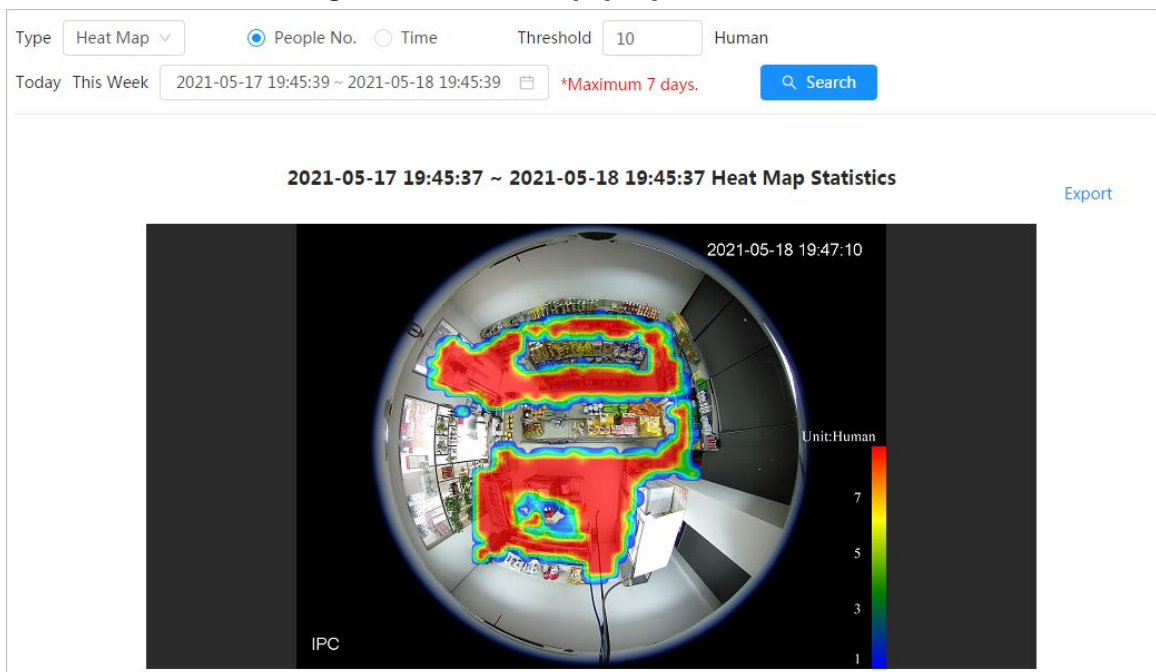
**Table 12-2 Set search conditions**

Parameter	Description
Channel	For multi-channel camera, select the channel first.
Type	You can select report type form Heat Map and Track Map.
People No.	When selecting type as Heat Map, select People No., and then set

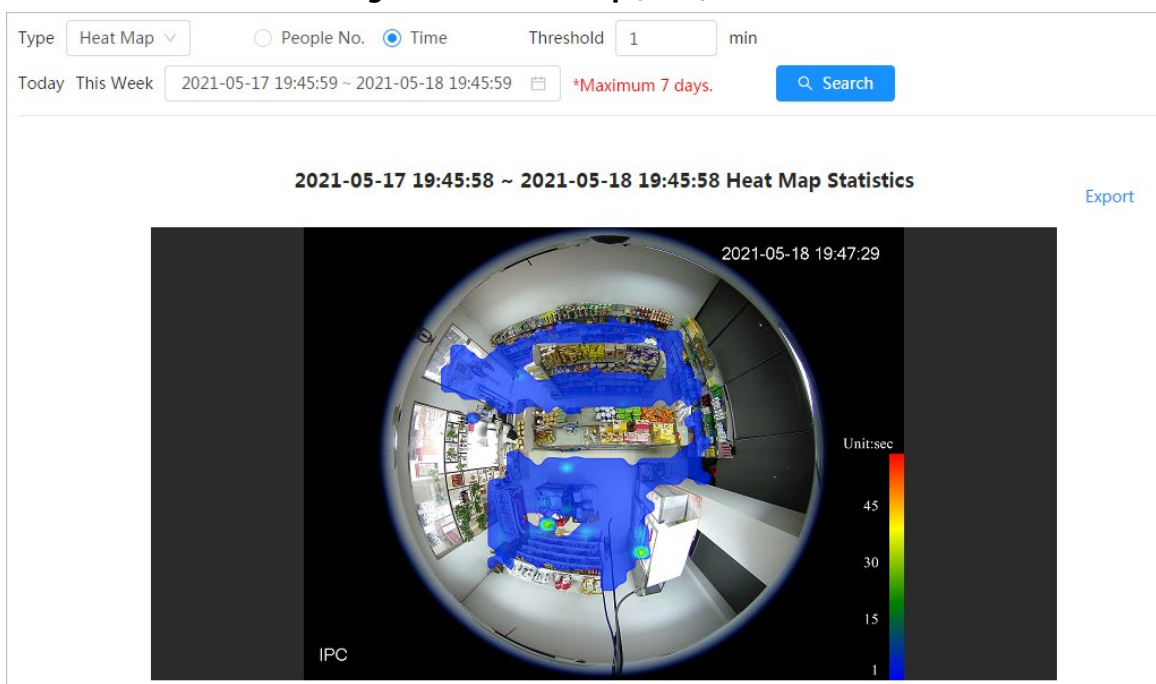
Parameter	Description
Threshold	the threshold. The system will display the heat map for people density.
Time	When selecting type as Heat Map, select Time and then set the threshold. The system will display the heat map for stay time.
Threshold	
Period for the report	Set the period for the report. You can view the daily and weekly report, and you can also customize the period.

**Step 3** Click Search.

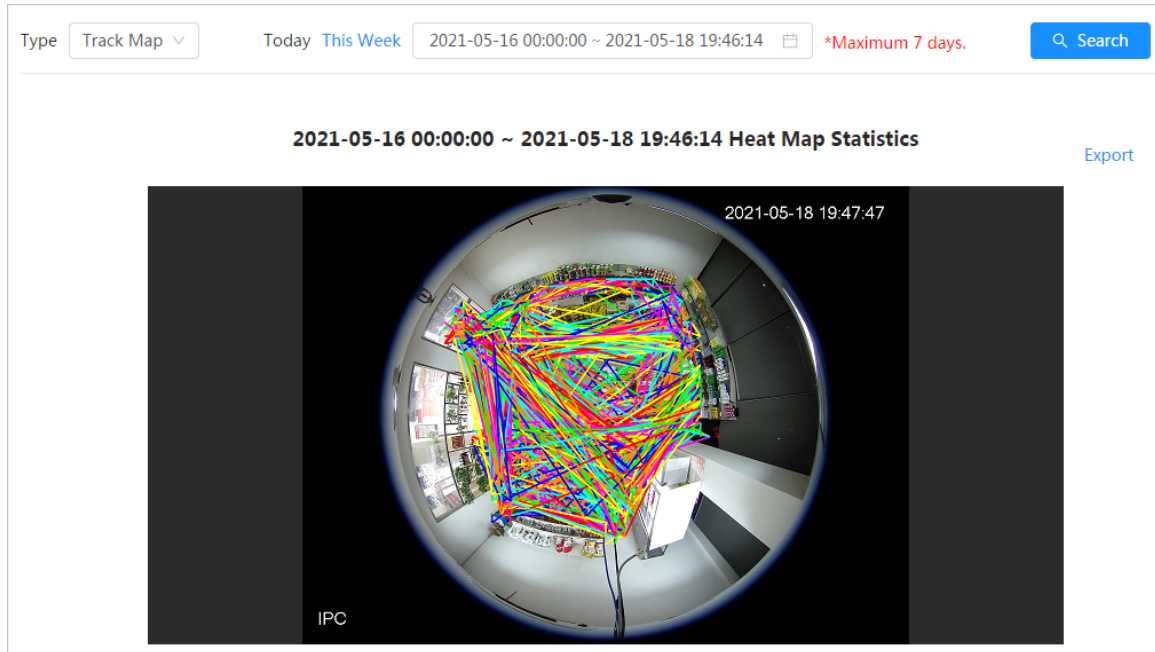
**Figure 12-10 Heat map (people No.)**



**Figure 12-11 Heat map (time)**



**Figure 12-12 Track map**



## Related Operations

Click **Export**, and select the storage path for the exported report in **.bmp** format.

## 12.1.7 ANPR

View the statistics result of ANPR in report form.

### Procedure

**Step 1** Select **Report > Report > ANPR**.

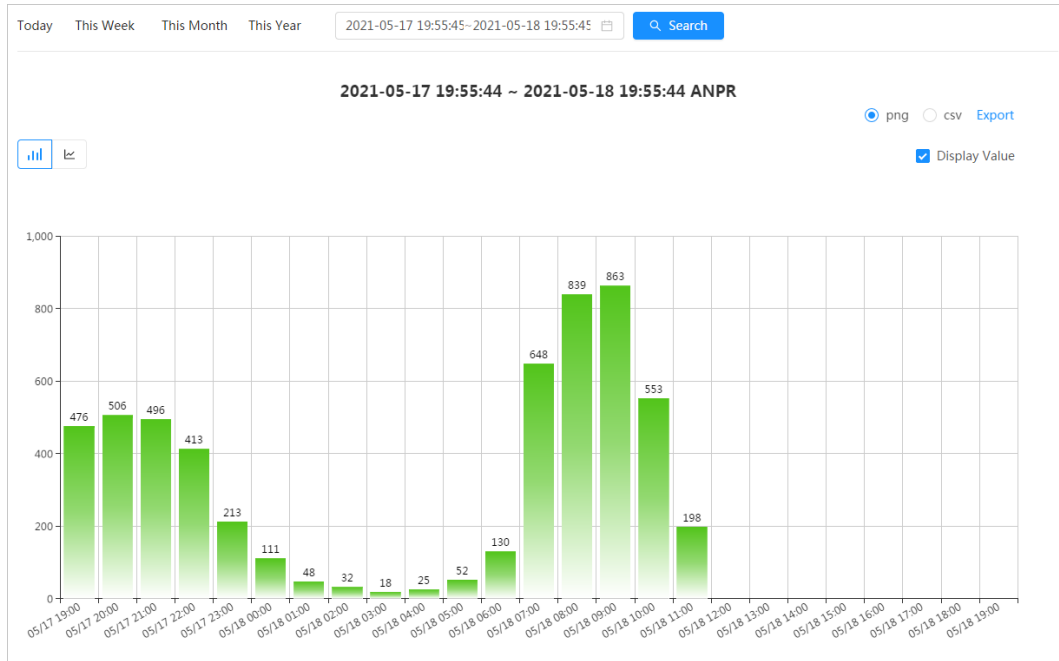
**Step 2** Set the period for the report.



**For multi-channel camera, select the channel first.**

**Step 3** Click **Search**.

**Figure 12-13 ANPR report**



### Related Operations

- **Select the report form**  
Click to display the report in line chart; click to display the report in bar chart.
- **Select the Display Value checkbox to display the value in the report**
- **Export reports**  
Select the file format, and then click Export.
  - ◇ Select png: Displays the report in picture format.
  - ◇ Select csv: Displays the report in list format.

## 12.2 Searching for Face Picture

Search for the Face Detection+ or snapshot results by pictures.

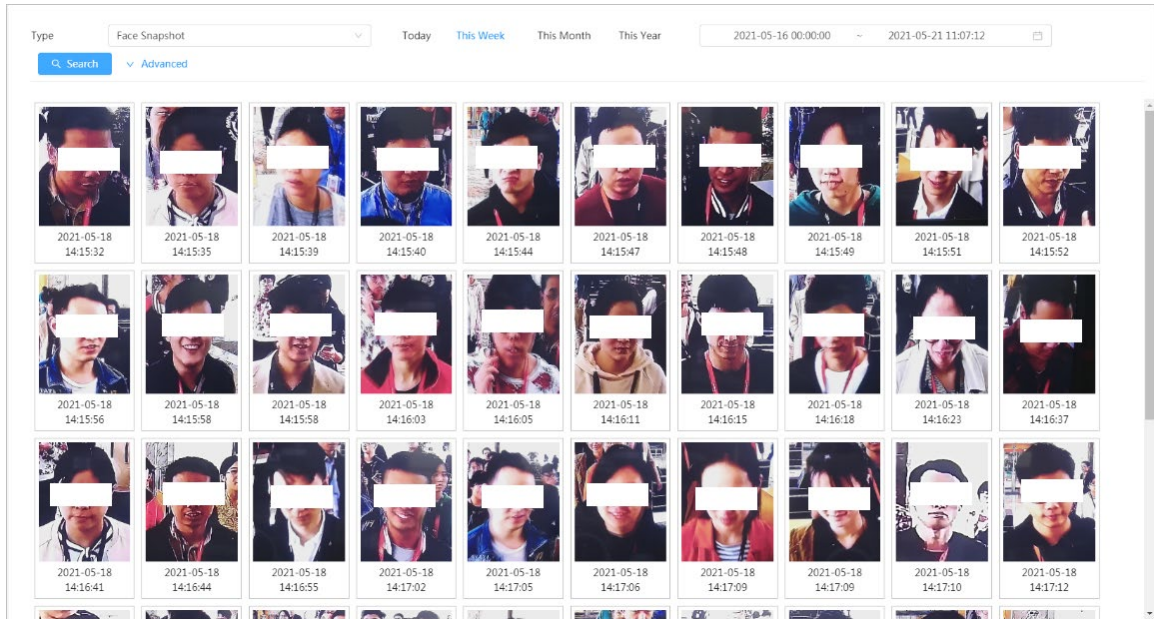
### Prerequisites

Make sure that you have installed SD card.

### Procedure

- Step 1** Select Report > Picture Query > Face.
- Step 2** Select the type and set the period for the report.  
Click Advance to set face attributes for precise search.
- Step 3** Click Search. The search result is displayed.

Figure 12-14 Face report



**Step 4** Click the picture, and then you can view the details.

## 12.3 Auto Upload

Select the upload mode, enable it, and configure the parameters. The camera will upload reports of Analytics+ functions to a defined server periodically.

### Background Information

There are three upload methods:

- **HTTP:** Upload reports to a server through HTTP protocol.
- **FTP:** Upload reports to a server through FTP protocol. You need to set the parameters, such as the server IP, username, password, and storage path.
- **Email:** Send reports to receivers through emails. You need to set the parameters, such as the username, password, sender and receiver.

### Procedure

**Step 1** Select Report > Auto Upload.

**Step 2** Select the upload method, and then enable it.

**Step 3** Set parameters.


Parameters of different upload methods are different.

- **HTTP**

Click Add, and then add the information of server. You can add two server information at most.

**Figure 12-15 HTTP upload method**


**Table 12-3 Description of HTTP mode parameter**

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Report type	Select the report type form the drop-down list. You can select more than one types at the same time.  The report types in the drop-down list are the same with that supported Analytics+ function. For example: If the camera supports people counting, heat map, and video Analytics, the 3 report types are displayed in the drop-down list.
Test	Test the network connection between the camera and the server.

- FTP upload method

Figure 12-16 FTP upload method

Table 12-4 Description of FTP mode parameter



Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
Report type	Select the report type form the drop-down list. You can select more than one types at the same time.  The report types in the drop-down list are the same with that supported Analytics+ function. For example: If the camera supports people counting, heat map, and video Analytics, the 3 report types are displayed in the drop-down list,
Server IP	The IP address and port number of the FTP server which the report will be uploaded to.
Port	
Username	Username and password for logging in to FTP server.
Password	
Storage Path	Username and password for logging in to FTP server.
Test	Test the network connection between the camera and the server.

- Email upload method

**Figure 12-17 Email upload method**

Upload Mode	<input type="text" value="Email"/>
Enable	<input checked="" type="checkbox"/>
Report Period	<input type="text" value="1hr"/>
Report Type	<input type="text" value="People Counting x"/>
SMTP Server	<input type="text" value="none"/>
Port	<input type="text" value="25"/>
Anonymous	<input type="checkbox"/>
Username	<input type="text" value="anonymity"/>
Password	<input type="password" value="....."/>
Sender	<input type="text" value="none"/>
Encryption Type	<input type="text" value="TLS(Recommended)"/>
Subject	<input type="text" value="IPC Message"/>
Receiver	<input type="text" value=""/> <input type="button" value="Add"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

**Table 12-5 Description of email mode parameter**

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
Report Type	Select the report type form the drop-down list. You can select more than one types at the same time.  <ul style="list-style-type: none"> <li>The report types in the drop-down list are the same with that supported Analytics+ function. For example: If the camera supports people counting, and video Analytics the 2 report types are displayed in the drop-down list,</li> <li>Heat map report will not be uploaded when you select email upload method, so heat map will not be displayed in the drop-down list.</li> </ul>
SMTP server	SMTP (Simple Mail Transfer Protocol) server IP address and port number.
Port	 See Table 12-6 for details.





Parameter	Description
Anonymous	Select Anonymous, and the sender's information is not displayed in the email.
Username	Username and password used to log in server.
Password	 See Table 12-6 for details.
Sender	Sender's email address.
Encryption Type	Select the encryption type from None, SSL (Secure Sockets Layer) and TLS (Transport Layer Security).  See Table 12-6 for details.
Subject	Email subject. You can enter up to 120 characters in Chinese, English, and Arabic numerals.
Receiver	Email addresses of receivers. Click add to set more than one receivers. Supports 3 addresses at most.

Table 12-6 Description of major mailbox configuration

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

**Step 4** Click Apply.

# Appendix 1 Cybersecurity Recommendations

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

**Mandatory actions to be taken for basic device network security:**

## 1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

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

## 2. Update Firmware and Client Software in Time

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

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

## 1. Physical Protection

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

## 2. Change Passwords Regularly

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

## 3. Set and Update Passwords Reset Information Timely

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

## 4. Enable Account Lock

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

#### 5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

#### 6. Enable HTTPS

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

#### 7. MAC Address Binding

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

#### 8. Assign Accounts and Privileges Reasonably

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

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

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

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

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

#### 10. Audio and Video Encrypted Transmission

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

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

#### 11. Secure Auditing

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

#### 12. Network Log

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

#### 13. Construct a Safe Network Environment

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

- **Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.**
- **The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested**

to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.

- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

## More information

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

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [overseas@dahuatech.com](mailto:overseas@dahuatech.com) | Fax: +86-571-87688815 | Tel: +86-571-87688883