

# **Network Camera Web 5.0**

# **Operation Manual**



ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.2.3



# Foreword

### General

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

## Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable result.
NOTE NOTE	Provides additional information as a supplement to the text.

### **Revision History**

Version	Revision Content	Release Date
V1.2.3	Updated encode.	October 2024
V1.2.2	<ul> <li>Added description of auxiliary calibration and angle adjustment.</li> <li>Updated the description of IVS.</li> </ul>	August 2024
V1.2.1	<ul> <li>Added HDMI output.</li> <li>Added experience database and long distance mode.</li> <li>Added animal for effective target.</li> </ul>	May 2024
V1.2.0	<ul> <li>Added resources.</li> <li>Added maintenance center.</li> <li>Added stereo analysis.</li> <li>Updated the function of disarming.</li> <li>Updated face recognition, face detection, people counting and video metadata.</li> <li>Updated subscribing alarm information.</li> </ul>	January 2024
V1.1.0	Updated the network connection.	October 2023
V1.0.9	<ul><li>Updated the live view function bar.</li><li>Updated the information of audio.</li></ul>	October 2023

Ι



Version	Revision Content	Release Date
V1.0.8	<ul> <li>Updated the description of illuminator, splicing and alarm linkage.</li> <li>Updated encode.</li> <li>Added ABR of bit rate type.</li> </ul>	July 2023
V1.0.7	<ul> <li>Updated the description of people counting.</li> <li>Added the function of AcuPick and disarming.</li> </ul>	June 2023
V1.0.6	<ul> <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
V1.0.2	<ul> <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> <li>Added "8.9 Setting People Counting" and "8.12 Setting Heat Map".</li> <li>Added "6.2.1.11 Fisheye" and "7.4.6 Fisheye".</li> <li>Updated "8.2 Setting Face Recognition".</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, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: 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.

٧



- 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 WarningsI	V
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 AI Functions	3
2 Configuration Flow	6
3 Device Initialization	7
4 Login	9
4.1 Device Login	9
4.2 Resetting Password 1	0
5 Home Page 1	2
6 Setting 1	4
6.1 Local1	4
6.2 Camera1	5
6.2.1 Setting Image Parameters1	5
6.2.2 Setting Encode Parameters	8
6.2.3 Splicing4	2
6.2.4 Audio	4
6.3 Network	6
6.3.1 TCP/IP	6
6.3.2 Port	9
6.3.3 PPPoE5	1
6.3.4 DDNS	1
6.3.5 Email	3
6.3.6 UPnP	4
6.3.7 SNMP	5
6.3.8 Bonjour5	8
6.3.9 Multicast5	8
6.3.10 Register	9
6.3.11 QoS	0
6.3.12 Platform Access	51
6.3.13 Basic Services6	3
6.4 EPTZ	4
6.5 Event	6



	6.5.1 Setting Alarm Linkage	66
	6.5.2 Setting Exception	73
	6.5.3 Setting Video Detection	75
	6.5.4 Setting Audio Detection	79
	6.5.5 Setting Disarming	81
	6.5.6 Setting Auto Upload	81
6.6	Storage	82
6.7	System	83
	6.7.1 General	83
	6.7.2 Power Consumption Mode	86
	6.7.3 Account	87
	6.7.4 Resources	93
	6.7.5 Peripheral Management	94
7 Live.		97
7.1	Live Page	97
7.2	Setting Encode	99
7.3	Live View Function Bar	99
7.4	Window Adjustment Bar	101
	7.4.1 Adjustment	101
	7.4.2 Zoom and Focus	102
	7.4.3 Auxiliary Calibration	103
	7.4.4 Angle Adjustment	104
	7.4.5 Image Adjustment	105
	7.4.6 Fisheye	105
7.5	Display Mode	109
8 Al		113
8.1	Setting Crowd Distribution Map	113
	8.1.1 Global Configuration	113
	8.1.2 Rule Configuration	114
8.2	Setting Face Recognition	116
	8.2.1 Enabling Face Recognition	116
	8.2.2 Setting Face Database	120
	8.2.3 Setting Arm Alarm	128
	8.2.4 Viewing Face Recognition Result	130
8.3	Setting Face Detection	131
8.4	Setting IVS	135
	8.4.1 Global Configuration	135
	8.4.2 Rule Configuration	139
8.5	Setting Smart Object Detection	144
	8.5.1 Global Configuration	144



	8.5.2 Rule Configuration	. 145
8.6	5 Setting Vehicle Density	. 147
8.7	7 Setting Parking Space	149
	8.7.1 Rule Configuration	. 149
	8.7.2 Global Configuration	155
8.8	3 Setting Video Metadata	155
	8.8.1 Global Configuration	155
	8.8.2 Rule Configuration	.158
	8.8.3 Viewing Video Metadata Report	.160
8.9	9 Setting People Counting	.160
	8.9.1 People Counting	.160
	8.9.2 Queuing	.164
	8.9.3 Abnormal Event Detection	166
	8.9.4 Global Configuration	168
8.1	10 Face & Body Detection	169
	8.10.1 Global Configuration	169
	8.10.2 Rule Configuration	.171
8.1	11 PPE Detection	172
	8.11.1 Rule Configuration	
	8.11.2 Global Configuration	175
	8.11.3 Setting Arming Database	
8.1	12 Setting Heat Map	.176
8.1	13 Setting ANPR	.177
	8.13.1 Lane Configuration	
	8.13.2 Rule Configuration	.178
	8.13.3 Picture	. 180
	8.13.4 Allowlist	181
	8.13.5 Blocklist	.184
8.1	14 Setting Panoramic Linkage	.184
	8.14.1 Enabling Linkage Track	184
	8.14.2 Configuring Calibration Parameter	. 185
8.1	15 Setting AcuPick	.187
8.1	16 Setting Stereo Analysis	188
	8.16.1 Global Configuration	188
	8.16.2 Rule Configuration	
	urity	
	I Security Status	
9.2	2 System Service	. 193
	9.2.1 802.1x	.193
	9.2.2 HTTPS	194



9.3 Attack Defense	195
9.3.1 Firewall	195
9.3.2 Account Lockout	196
9.3.3 Anti-DoS Attack	
9.4 CA Certificate	197
9.4.1 Installing Device Certificate	197
9.4.2 Installing Trusted CA Certificate	200
9.5 A/V Encryption	
9.6 Security Warning	202
10 Record	203
10.1 Playback	203
10.1.1 Playing Back Video	203
10.1.2 Clipping Video	
10.1.3 Downloading Video	206
10.2 Setting Record Control	207
10.3 Setting Record Plan	
10.4 Storage	210
10.4.1 Local Storage	211
10.4.2 Network Storage	211
11 Picture	215
11.1 Playback	
11.1.1 Playing Back Picture	215
11.1.2 Downloading Picture	
11.2 Setting Snapshot Parameters	218
11.3 Setting Snapshot Plan	218
11.4 Storage	
11.5 Setting Upload Method	219
12 Report	
12.1 Viewing Report	220
12.1.1 Face Recognition	
12.1.2 Video Metadata	
12.1.3 People Counting	222
12.1.4 Crowd Distribution	226
12.1.5 Vehicle Density	226
12.1.6 Heat Map	227
12.1.7 ANPR	229
12.2 Searching for Face Picture	230
12.3 Auto Upload	231
13 Maintenance Center	
13.1 One-click Diagnosis	



13.2 Syste	m Information	237
-	Viewing Device Information	
	-	
13.2.2	Viewing Online Users	237
13.2.3	Viewing Legal Information	237
13.3 Log Ir	nformation	237
13.3.1	Viewing Local Logs	238
13.3.2	Setting Remote Logs	239
13.4 Maint	tenance Management	239
13.4.1	Requirements	239
13.4.2	Maintenance	239
13.4.3	Import/Export	240
13.4.4	Default	241
13.4.5	Font Pack	241
13.5 Upda	te	242
13.6 Adva	nced Maintenance	243
13.6.1	Export	243
13.6.2	Packet Capture	243
13.6.3	Run Log	244
Appendix 1 S	ecurity Commitment and Recommendation	245



# **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 the 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. Use Windows system to manage the camera. It does not support macOS system.

## **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.

1



• Configure coding parameters, and adjust live view image.

### Alarm

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

### Exception

- Includes 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 an email.
- When network disconnection alarm is triggered, the system links the 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

- Includes 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

- Includes 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

- Record automatically as schedule.
- Play back recorded video and picture as needed.
- Download recorded video and picture.
- Alarm linked recording.

### Account

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



# **1.3.2 Al Functions**

IVS

- Rules: 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 displays the related attributes.
- When an alarm is triggered, the system performs linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

### Face Recognition

- Displays the recognition result on the live view page
- In general mode, compares 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 Metadata

- 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 of the detection area, and generates a 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 the 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 selected 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.



#### Figure 2-1 Configuration flow

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"
	Camera parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	"6.2 Camera"
Basic	Date & time	Set date and time to ensure the recording time is correct.	"6.7.1.2 Date & Time"
parameters	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"
AI	Al rules	Configure the necessary detection rules, such as face detection and IVS.	"8 AI"



# **3 Device Initialization**

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

### **Background Information**

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

### Procedure

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

	Т		n.
	Т		Ш.
5	-	~	4

The IP is 192.168.1.108 by default.

Figure 3-1 Region setting

Orvice Initialization			
💋 Region Setting 🛛 📄 Discl	aimer	() Time Zone Setting	Password Setting P2P
Area			
Language	English		
Video Standard	PAL		
		Next	

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

<u>Step 3</u> Configure the time parameters, and then click **Next**.



Figure 3-2 Password setting

Device Initialization	
	claimer ———— 🧭 Time Zone Setting ——— 🤌 Password Setting ——— 🖉 P2P
Username	admin
New Password	
Confirm Password	
✓ Email Address	For password reset. Recommended or improved in time.
	Next

<u>Step 4</u> Set the password for admin account.

Parameter	Description
Username	The default username is admin.
New Password	The password must consist of 8 to 32 non-blank characters and
Confirm Password	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.
	Enter an email address for password resetting, and it is enabled by default.
Email Address	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.

<u>Step 5</u> Click **Next**, and then **P2P** page is displayed.



# 4 Login

# 4.1 Device Login

### **Background Information**

This section introduces how to log in to the webpage. Here we take Chrome as an example.

- You need to initialize the camera before logging in to the web page. For details, see "3 Device Initialization".
- Follow the instruction to download and install the plug-in for the first login.

### Procedure

- <u>Step 1</u> Open IE browser, enter the IP address of the camera (192.168.1.108 by default) in the address bar and press Enter.
- <u>Step 2</u> Enter the username and password.

The username is admin by default.

 $\square$ 

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".

<b>EXAMPLE</b>
A Username
Password Forgot password?
Login

Figure 4-1 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

<u>Step 1</u> Open IE browser, enter the IP address of the device in the address bar and press Enter.

С	hua IOLOGY
( A Username	
A Password	Forgot password?
Lo	ogin

Figure 4-3 Login



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



# 5 Home Page

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

- Live: View the real-time monitoring image.
- Al: Configure Al 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.
- Maintenance center: Diagnose the running status of devices and perform maintenance.
- Report: Search the AI event report and system report.

🗅 Live		A   1	ම   & admin   O   X
et i how			
		_	
Live	AI	Camera	
View live video.	Configure AI functions.	Image attributes, audio & video coding config.	
Event	Curtury .	Country (	
Event	System	Security	
General event config.	User management, device operation and maintenance.	Check device security status, and set security functions.	
	• •		

#### Figure 5-1 Home page

The icons located on the upper-right corner of the home page serve the following functions:

- Alarm subscription: Subscribe alarm.
- Skin setting: Set the skin.
- Language setting: Set the language.
- Restart: Click **A** admin at the upper-right corner of the page, select **Reboot**, and the camera restarts.
- Logout: Click 2 admin at the upper-right corner of the page, select **Logout** to go to the login page.

The system will log out 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.



### 

For the camera with multiple channels, through selecting channel numbers, you can set the parameters of the channels.



# 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**, **PTZ**, **Event**, **System** and **Maintenance Center**, 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

<u>Step 1</u>	Select 🜻	> Local.
---------------	----------	----------

ay Parameter		
Protocol	● TCP Port ○ UDP Port ○ Multicast	
cord Path		
Live Record	C:\Users\- WebDownload\LiveRecord	Browse
Playback Download	C:\Users\ \WebDownload\PlaybackRecord	Browse
Video Clip	C:\Users\4 \WebDownload\VideoClips	Browse
apshot Path		
Live Snapshot	C:\Users\ \WebDownload\LiveSnapShot	Browse
Playback Snapshot	C:\Users\ WebDownload\PlaybackSnapshot	Browse

Figure 6-1 Local

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



Parameter	Description	
	You can select the network transmission protoco options are <b>TCP</b> , <b>UDP</b> and <b>Multicast</b> .	l as needed, and the
Protocol		
	Before selecting <b>Multicast</b> , make sure that you h parameters.	ave set the <b>Multicast</b>
	The recorded video of live page.	
Live Record	The default path is C:\Users\admin \WebDownload\LiveRecord.	
	The downloaded video of playback page.	
Playback Download	The default path is C:\Users\admin \WebDownload\PlaybackRecord.	~
	The clipped video of playback page.	
Video Clip	The default path is C:\Users\admin \WebDownload\VideoClips.	Admin in the path refers to the account being used.
	The snapshot of live page.	
Live Snapshot	The default path is C:\Users\admin \WebDownload\LiveSnapshot.	
	The snapshot of playback page.	
Playback Snapshot	The default path is C:\Users\admin \WebDownload\PlaybackSnapshot.	

Step 3 Click **Apply**.

## 6.2 Camera

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

 $\square$ 

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 illuminator.

### 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)

Working Mode  Self-adaptive  Customi	zed Scene O Day/Night	Switch		
Apply Refresh Default	AI SSA Image Exposure Backlight WB Day/Night Illuminator Defog AFSA	Mode	Off	S

• 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 lay	out (cust	omized	scene)

		Profile	Day V			
	Alter of Local p	AI SSA	Mode		Off	
THE A ATA STRA	. E	Image				
and a start starting	And the second s	Exposure				
	a ser all a st	Backlight				
		WB				
100 M		Day/Night				
		Illuminator				
4007 (62.4) 10 M K	Start Start	Defog				
		AFSA				
Time Plan Settings				^		
Fime Plan Settings  Day  Night	• General • Front Light •	<ul> <li>Backlight</li> <li>Strong Bac</li> </ul>	klight <ul> <li>Low Illuminance</li> <li>Custom1</li> <li>(</li> </ul>			
	• General • Front Light •	Backlight • Strong Bac	klight • Low Illuminance • Custom1 • G Delete Clear			
• Day • Night				Default		
• Day • Night			Delete Clear	Default Copy		
• Day • Night 0 1 2 Jan			Delete Clear	Default Copy Copy		
• Day • Night 0 1 2 Jan Feb			Delete Clear	Default Copy		
Day     Night     O     1 2     Jan     Feb     Mar			Delete Clear	Default Copy Copy Copy Copy		
• Day • Night 0 1 2 Jan Feb Mar Apr			Delete Clear	Default Default Copy Copy Copy Copy		
Day     Night     Day     Night     Jan     Feb     Mar     Apr     May			Delete Clear	Default Default Copy Copy Copy Copy Copy		
• Day • Night Jan Feb Mar May Jun			Delete Clear	Default Default Copy Copy Copy Copy Copy Copy		
• Day • Night			Delete Clear	Default Default Copy Copy Copy Copy Copy Copy Copy Copy		
Day     Night     Day     Apr     Apr     Jun     Jul     Aug			Delete Clear	Custom2 Default Copy Copy Copy Copy Copy Copy Copy Copy		
Day     Night     Day     Day     Night     Day     Au     Jun     Jun     Jun     Sep			Delete Clear	Default Default Copy Copy Copy Copy Copy Copy Copy Copy		

• 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)

	Profile	Day	
a provide a second s	AI SSA Image Exposure	Style Brightness	Standard         v           -         +         50           -         +         50
	Backlight WB Day/Night Illuminator Defog	Contrast Saturation Sharpness Gamma	- + 50 - + 50 - + 50 - + 50 - + 50
	AFSA	Flip Mirror	0. ~

### 6.2.1.2 AI SSA

By enabling AI SSA (AI 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

<u>Step 1</u>	Select 🜻	> Camera > Image > AI SSA
Stop 2	Soloct On	in the drandown list

<u>Step 2</u> Select **On** in the dropdown list.

 $\square$ 

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 Se

Figure 6-5 Image

Image	Style	Standard	$\sim$
Exposure Backlight	Brightness		+ 50
WB	Contrast		+ 50
Day/Night	Saturation		+ 50
Light	Sharpness	-	+ 50
	Gamma		+ 50
	Flip	0°	$\sim$
	Mirror		

<u>Step 2</u> Configure picture parameters.



Parameter	Description
	Select the picture style from soft, standard and vivid.
Style	<ul> <li>Standard: Default image style, displays the actual color of the image.</li> <li>Soft: The hue of the image is weaker than the actual one, and contrast is smaller.</li> <li>Vivid: The image is more vivid than the actual one.</li> </ul>
Brightness	Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the lower the darker. The picture might be hazy if the value is configured too big.
Contrast	Changes the contrast of the picture. The higher the value is, the more the contrast will be between bright and dark areas, and the lower 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.
Saturation	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.
Sharpness	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.
Gamma	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 lower the darker.
Flip	<ul> <li>Changes the display direction of the picture, see the options below.</li> <li>0°: Normal display.</li> <li>90°: The picture rotates 90° clockwise.</li> <li>180°: The picture flips upside down.</li> <li>270°: The picture rotates 90° counterclockwise.</li> <li>Image: The picture rotates 90° counterclockwise.</li> <li>For some models, set the resolution to be 1080p or lower when using 90° and 180°. For details, see "6.2.2 Setting Encode Parameters".</li> </ul>
Mirror	Click , and the picture will display with left and right side reversed.

Table 6-2 Description of picture parameters

Step 3 Click Apply.

## 6.2.1.4 Exposure

Configure iris and shutter to improve image clarity.

### Background Information

## $\square$

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



### Procedure

Figure 6-6 Exposure			
Image	Anti-flicker	Outdoor	$\sim$
Exposure	Mode	Auto	~
Backlight WB	Exposure Compensation		+ 5
Day/Night	Auto Iris		
Light	3D NR		
	Level	-	+ 5

<u>Step 2</u> Configure exposure parameters.

### Table 6-3 Description of exposure parameters

Parameter	Description
Anti-flicker	<ul> <li>You can select from 50 Hz, 60 Hz and Outdoor.</li> <li>50 Hz: 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>60 Hz: 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>Outdoor: You can select any exposure mode as needed.</li> </ul>



Parameter	Description		
	Device exposure modes.		
Mode	<ul> <li>Auto: Adjusts the image brightness according to the actual condition automatically.</li> <li>Gain Priority: 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>Shutter priority: 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>Manual: Configure gain and shutter value manually to adjust image brightness.</li> </ul>		
	When the <b>Anti-flicker</b> is set to <b>Outdoor</b> , you can select <b>Auto</b> , <b>Gain priority</b> , <b>Shutter priority</b> or <b>Manual</b> in the <b>Mode</b> list.		
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 <b>Gain Priority</b> or <b>Manual</b> in <b>Mode</b> , you can set <b>Gain</b> . With minimum illumination, the camera increases <b>Gain</b> automatically to get clearer images.		
	This configuration is available only when the camera is equipped with auto-iris lens.		
Auto Iris	<ul> <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.		
	This configuration is available only when the 3D NR is enabled.		
Level	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 Se

Figure 6-7 Backlight

Mode	Off V	
	Mode	Mode Off v

<u>Step 2</u> Configure backlight parameters.

#### Table 6-4 Description of backlight parameters

Backlight mode	Description
BLC	Enable <b>BLC</b> , the camera can get clearer image of the dark areas on the target when shooting against light. You can enable or disable <b>Customized</b> mode.
	<ul> <li>When you enable <b>Customized</b> 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 <b>Default</b> mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area.</li> </ul>
	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.
WDR	
	There might be a few seconds of video loss when the device is switching to WDR mode from other mode.
HLC	Enable <b>HLC</b> 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.
SSA	Enable <b>SSA</b> , the system automatically adjusts the image brightness according to the environment to make the objects in the image clearer.

Step 3 Click Apply.



### 6.2.1.6 WB

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

### Procedure

Step 1 Select Select Select Select Step 1 Select Se

Figure 6-8 WB

Image	Mode	Auto	
Exposure			
Backlight			
WB			
Day/Night			
Light			

<u>Step 2</u> 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 Se



### Figure 6-9 Day/night

Profile	Day	~	
Image	Mode	Auto	$\sim$
Exposure Backlight	Sensitivity	2	$\vee$
WB	Delay	6 sec	$\vee$
Day/Night			
Illuminator			

<u>Step 2</u> Configure day and night parameters.

Table 6-6 Description of day and night parameters

Parameter	Description	
	You can select device display mode from <b>Color</b> , <b>Auto</b> , and <b>B/W</b> .	
Mada	<ul> <li>Color : The system displays color image.</li> <li>Auto : The system switches between color and black-and-white display according to the actual condition.</li> <li>B/W : The system displays black-and-white image.</li> </ul>	
Mode	<ul> <li>Day/Night configuration is independent from profile management configuration.</li> <li>For Triple-Sight Perimeter Protection Bullet WizMind Network Camera, the mode of distant view channel will automatically synchronize with the panorama and medium view channels. For instance, if the distant view channel is set to <b>B/W</b>, the panorama and medium view channels will also switch to <b>B/W</b>.</li> </ul>	
Sensitivity	You can configure camera sensitivity when switching between color and black-and-white mode. Hover over ⑦ to get detailed information. This configuration is available only when you set <b>Auto</b> in <b>Mode</b> .	
Delay	This configuration is available only when you set <b>Auto</b> in <b>Mode</b> . 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.	

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 Se



#### Figure 6-10 Light

Image	Fill Light	Soft Light Mode 🗸 🗸	
Exposure	Mode	Auto	
Backlight	Mode	Auto	
WB			
Day/Night			
Illuminator			
Defog			

<u>Step 2</u> Select the fill light for the camera.

- IR Mode : The system will link IR light in the dark environment.
- **Soft Light Mode** : The system will link IR light and warm light at the same time in the dark environment, and adjust the brightness of the two lights to get clear images.
- Warm Light Mode : The system will link the warm light in the dark environment.

#### $\square$

Brightness Upper Limit: Set the brightness upper limit to adjust the image.

• **Smart Illumination** : The system will link IR light in the dark environment. If the human body is detected, the warm light will be triggered.

### $\square$

- Illuminator Delay: Set the duration that the warm light remains on after the detection object left.
- Brightness Upper Limit: Set the brightness upper limit to adjust the image.

#### Figure 6-11 Smart illumination

Fill Light	Smart Illumination	~
Mode	Auto	V
Illuminator Delay	60	sec (30-300
Brightness Upper Limit	-	+ 50
Illumination Overexposure Remover	Off	~

- **By Time** : Set different fill light modes at different times.
  - 1. Click Setting next to Time Plan.
  - 2. Select the fill light mode, and then drag the time slider.

### $\square$

Configure the light mode for one day, click **Copy**, and then you can easily copy the settings to other dates.

3. Click **OK**.


#### Figure 6-12 Time plan settings



#### <u>Step 3</u> Select the mode.

• **Manual** : Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.

	r -	

Some models support illumination by area in this mode.

- Auto : The system adjusts the illuminator intensity according to the ambient lighting condition.
- **Zoom Priority** : The system adjusts the illuminator intensity automatically according to the change of the ambient light.
  - 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.
  - When the ambient light turns brighter, the system dims high beam lights until they are off, and then the low beam lights.
  - When the focus reaches a defined 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.
- **Off** : Illuminator is off.

#### <u>Step 4</u> (Optional) Configure **Illumination Overexposure Remover**.

Only some fill light modes support this function.

Step 5 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

<u>Step 1</u> Select **Select** Select Selec



#### Figure 6-13 Light

nage		Mode	Mode Auto
posure			
acklight			
В			
ay/Night			
uminator			
efog	1		

## <u>Step 2</u> Configure defog parameters.

## Table 6-7 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

		5-14 AFSA	
AI SSA	Mode	Off	^
Image Exposure		Off	
Backlight		On	
WB		Auto	
Day/Night			
Illuminator			
Defog			
AFSA			
Select <b>On</b> or <b>Auto</b> in	the drandown lis	+	

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.

# **Background Information**

 $\square$ 

This function is only available on fisheye device.

Procedure

Step 1 Select Se



Figure 6-15 Fisheye

<u>Step 2</u> Set mounting mode and record mode.

Table 6-8 Description of fisheye parameters

Parameter	Description
Mounting Mode	You can select <b>Ceiling</b> , <b>Wall</b> , or <b>Ground</b> .
Record Mode	<ul> <li>10: The original image before correction.</li> <li>1P: 360° rectangular panoramic image.</li> <li>2P: When the installation mode is <b>Ceiling</b> or <b>Ground</b>, 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>10 + 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>





# 6.2.2 Setting Encode Parameters

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

 $\square$ 

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
 Select
 Figure 6-16 Encode.

 Main Stream
 Sub Stream
 Sub Stream

 Compression
 H265
 Sub Stream

Commenter	H.265		Sub Stream	Sub Stream 1 V	
Compression	H.265		Sub Stream	Sub Stream 1	
Encoding Strategy	AI Coding		Sub Window	Window 1 $\vee$	
Resolution	2560*2560 (2560x2560)		Compression	H.265 V	
Frame Rate (FPS)	25		Resolution	1440*1440 (1440x1440) V	
Bit Rate Type	ABR		Frame Rate (FPS)	25 V	
Reference Bit Rate	1280-9728 (Kb/s)		Bit Rate Type	CBR V	
Max Bit Rate	Custom	(Kb/s)	Reference Bit Rate	512-5632 (Kb/s)	
	5504	(3-16384)(Kb/s)	Bit Rate	512 ~	(Kb/s)
Average Bit Rate	4096	(Kb/s)	I Frame Interval	50	(25-150)
I Frame Interval	2 sec		Smooth Stream	+ 50	[Smooth <->Clear
Watermark					
Watermark String	DigitalCCTV				

<u>Step 2</u> Configure encode parameters.

Table 6-9 Description of encode parameters

Parameter	Description
Sub Stream	Click O to enable sub stream, it is enabled by default.
	You can enable multiple sub streams simultaneously.



Parameter	Description
	Select the sub window. Supports selecting <b>Panoramic View</b> or <b>Window</b> <i>x</i> ( <i>x</i> determined by record mode).
	• <b>Panoramic View</b> : The sub stream displays the original fisheye
	<ul> <li>Window <i>x</i>: The sub stream displays the selected sub window.</li> </ul>
	• This feature is supported only when the camera record mode is
	2P, 2R or 4R. You can select 2 > <b>Camera</b> > <b>Image</b> > <b>Fisheye</b> to set record mode.
Sub Window	<ul> <li>On the Live page, you can long-press on the live view to display the corresponding order number for each window.</li> </ul>
	Select encode mode.
	• <b>H.264</b> : Main profile encode mode. Compared with H.264B, it
	<ul> <li>requires smaller bandwidth.</li> <li>H.264H : High profile encode mode. Compared with H.264, it</li> </ul>
Compression	<ul> <li>requires smaller bandwidth.</li> <li>H.264B : Baseline profile encode mode.</li> </ul>
	<ul> <li>H.265 : Main profile encode mode. Compared with H.264H, it requires smaller bandwidth.</li> </ul>
	<ul> <li>MJPEG : 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>
	Click <b>C</b> to enable smart codec to improve video compressibility and save storage space.
Smart Codec	
	After smart codec is enabled, the device would stop supporting the third bit stream, ROI, and smart event detection.
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.
Frame Rate (FPS)	The number of frames in one second of video. The higher the value is, the clearer and smoother the video will be.



Parameter	Description	
	The bit rate control type during video data transmission. You can select bit rate type from:	
Bit Rate Type	<ul> <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</li> </ul>	
	<ul> <li>changes.</li> <li>ABR (Average Bit Rate): The bit rate takes into account bandwidth savings and image quality improvement.</li> </ul>	
	• The <b>Bit Rate Type</b> can only be set as <b>CBR</b> when <b>Encode Mode</b> is set as <b>MJPEG</b> .	
	<ul> <li>The Bit Rate Type can be set as ABR only when Encoding Strategy is set as AI Coding.</li> </ul>	
	This parameter can be configured only when the <b>Bit Rate Type</b> is set as <b>VBR</b> .	
Quality	The better the quality is, but the bigger the required bandwidth will be.	
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.	
	This parameter can be configured only when the <b>Bit Rate Type</b> is set as <b>VBR</b> or <b>ABR</b> .	
Max Bit Rate	Supports for custom max bit rate.	
	You can select the value of the <b>Max Bit Rate</b> according to the <b>Reference Bit Rate</b> value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.	
	This parameter can be configured only when the <b>Bit Rate Type</b> is set as <b>CBR</b> .	
Bit Rate	Supports for custom bit rate.	
	You can select bit rate value according to actual condition.	
	This parameter can be configured only when the <b>Bit Rate Type</b> is set as <b>ABR</b> .	
Average Bit Rate	The default value of the average bit rate is half of the max bit rate, and the max bit rate keeps higher than the average bit rate.	
	Supports for custom average bit rate.	
	The average bit rate should be greater than the max bit rate.	



Parameter	Description
	The number of P frames between two I frames, and the <b>I Frame</b> Interval range changes as <b>FPS</b> changes.
	It is recommended to set I Frame Interval twice as big as FPS.
l Frame Interval	When Encoding Strategy is AI Coding, the I Frame Interval under CBR supports 1 second and 2 seconds for selection, and the I Frame Interval under VBR or ABR supports 1 second and even values between 1 second and 30 seconds for selection.
	This parameter can be configured only when the <b>Bit Rate Type</b> is set as <b>VBR</b> or <b>ABR</b> .
Virtual I Frame	<b>Virtual I Frame</b> is inserted starting from an I frame interval of 4 seconds or more.
	You can enable or disable <b>Virtual I Frame</b> only when <b>I Frame</b> <b>Interval</b> is greater than or equal to 4 seconds. It is enabled by default and can be manually disabled.
SVC	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.
	<ul> <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
Watermark String	tampered.

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 Se



#### Figure 6-17 Privacy masking

Privacy Masking Channel Title Time Title	Enable Add	Clear				
Location	No.	Name	Туре	Color	Draw	Delete
Font Properties	1	Privacy Mask1	Mosaic		.*'	â
Picture Overlay	2	Privacy Mask2	Mosaic		.**	亩
Custom Title	3	Privacy Mask3	Mosaic		.**	亩
Target Statistics	4	Privacy Mask4	Mosaic		.**	亩
ANPR Face Detection	5	Privacy Mask5	Color Block	•		亩
Face Recognition	6	Privacy Mask6	Color Block	•	.51	ā
Face & Body Count	7	Privacy Mask7	Color Block	•	.91	ā
	8	Privacy Mask8	Color Block	•	.*`	ā

<u>Step 2</u> 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
  - $\diamond$  Click  $\mathbf{\overline{\mathbf{m}}}$  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 Se



#### Figure 6-18 Channel title



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

- <u>Step 3</u> 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

<u>Step 1</u> Select **Select** > Camera > Encode > Overlay > Time Title.

	Channel	1(Details)		
	Privacy Masking	Enable		
A A A A	Channel Title			
	Time Title	Week Display		
ANG.	Location	Location	Front	$\sim$
	Font Properties			
	Picture Overlay			
	Custom Title			
	Target Statistics			
	Face Detection			
	Face Recognition			
Apply Refresh Default				

Figure 6-19 Time title

<u>Step 2</u> Click Onext to **Enable**.

<u>Step 3</u> Click One next to **Week Display** to display the day of week, and then select the location.

<u>Step 4</u> 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.

## **Background Information**

 $\square$ 

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



- <u>Step 2</u> 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.

- <u>Step 3</u> 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

<u>Step 1</u> Select **Select** Select Selec



#### Figure 6-21 Font properties

\$100 gp 54 10 14 03	Channel	1(Details)		~
	Privacy Masking Channel Title	Font Size	Self-adaptive	~
and the second sec	Time Title	Color	Custom	✓ ▲ *
AND AS	Location	Line Spacing	1.0	~
	Font Properties			
	Picture Overlay			
	Custom Title			
	Target Statistics			
	Face Detection			
	Face Recognition			
Apply Refresh Default				

<u>Step 2</u> Select the font size, color and line spacing.

For color, you can choose **Black and White Reverse** or **Custom** (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.

# Background Information

 $\square$ 

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

# Procedure

# <u>Step 1</u> Select Select

Figure 6-22 Picture overlay

No.		America	Privacy Masking Channel Title	Enable		
1-1-1	Manufacture of the Constanting	and the second	Time Title			
Then			Location		1. Max size 16k.	
			Font Properties		<ol> <li>Max resolution 128x128 pixels.</li> <li>3. 256 colors, bmp format.</li> </ol>	
			Picture Overlay	Upload		
	THE SHE	1	Custom Title			
Pro2	the state		Face Statistics			

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



<u>Step 3</u> 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 Se

Figure 6-23 Custom title

Caston Title.	Channel	CAM 2	v	
	Privacy Masking Channel Title Time Title Location Font Properties Picture Overlay Custom Title Face Statistics	Enable Input Text Text Alignment		+
Apply Refresh Default				

- 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.
- <u>Step 3</u> Move the custom box to the position that you want in the image.
- Step 4 Click **Apply**.

 $\square$ 

### 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** 

<u>Step 1</u> Select Select

Figure 6-24 Target statistics





<u>Step 2</u> Click Omega next to **Enable**, select the statistics type, and then select the text alignment.

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

- <u>Step 3</u> 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 metadata 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



Encode	Overlay	ROI			
			Privacy Masking Channel Title Time Title Location Font Properties Picture Overlay Custom Title Target Statistics ANPR Face Detection Face Recognition Face & Body Count	Enable 💽 Motor V Statistics Type <table-cell> Motor V Text Alignment 📄 🚍</table-cell>	<b>Reset</b> /ehicle
Apply R	efresh De	efault			

Figure 6-25 ANPR

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

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

- <u>Step 3</u> 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

<u>Step 1</u> Select Select



#### Figure 6-26 Face detection

	Privacy Masking	Enable		Reset
2020-01-21 15 03 40	Channel Title	Text Alignment	E E	
	Time Title			
	Location			
$\dot{\tau}$	Font Properties			
	Picture Overlay			
	Custom Title			
	Target Statistics			
	Face Detection			
	Face Recognition			

<u>Step 2</u> Click Onext to **Enable**, and select the text alignment.

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

- <u>Step 3</u> Move the statistics box to the position that you want in the image.
- Step 4 Click **Apply**.

 $\square$ 

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

#### 6.2.2.2.11 Configuring Face Recognition

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

# <u>Step 1</u> Select **Select** > Camera > Encode > Overlay > Face Recognition.



	Privacy Masking Channel Title Time Title Location	Enable Statistics Type Text Alignment	Face Detection	Reset ✓ Face Recognition
<i>†</i>	Font Properties Picture Overlay Custom Title			
JPC	Target Statistics Face Detection Face Recognition			



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

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



<u>Step 3</u> 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 recognition 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 Se

Face Statistics	Channel	CAM 2		~
	Privacy Masking	Enable		Reset
	Channel Title Time Title	Text Alignment	= =	
	Location			
	Font Properties			
	Picture Overlay			
	Custom Title			
	Face Statistics			
Apply Refresh Default				

Figure 6-28 Face statistics

<u>Step 2</u> Click Onext to **Enable**, and select the text alignment.

Click Reset to clear the statistics data.

- <u>Step 3</u> 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 Se



#### Figure 6-29 Face&body counting

Privacy Masking Enable Reset   Channel Title Time Title   Location Font Properties   Picture Overlay Custom Title   Target Statistics ANPR   Face Detection	Encode	Overlay	ROI		
Face & Body Count			The second second	Channel Title Time Title Location Font Properties Picture Overlay Custom Title Target Statistics ANPR Face Detection Face Recognition	Reset

<u>Step 2</u> Select the **Enable** check box, and then select text alignment.

$\sim$	
Click Reset	to clear the statistics data.

- <u>Step 3</u> Move the face&body counting box to the position that you want in the image.
- Step 4 Click **Apply**.

 $\square$ 

### 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



Encode	Overlay	ROI			
Vehicles			Privacy Masking Channel Title Time Title Location Font Properties Picture Overlay Custom Title Target Statistics ANPR Parking Space	Enable Statistics Type Text Alignment	Vehicles Vailable
Apply	Refresh Def	ault			

Figure 6-30 Parking space



<u>Step 2</u> Select the **Enable** check box.

- <u>Step 3</u> 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.

Figure 6-31 People counting

## Procedure

# <u>Step 1</u> Select Select

Encode Overlay	Privacy Masking Channel Title Time Title Location Font Properties Picture Overlay Custom Title Face Statistics People Counting	Enable Statistics Type Text Alignment	<ul> <li>✓ Enter No. ✓ Exit No. ✓ Pass No. ✓ In Area No.</li> <li>✓ Queue People No.</li> <li>Ξ</li> </ul>
Apply Refresh Default			

- <u>Step 2</u> Click Onext to **Enable**, select the statistics type, and then select the text alignment.
- <u>Step 3</u> 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 <a> Camera > Encode > ROI.</a>



#### Figure 6-32 ROI



- <u>Step 2</u> Click next to **Enable**, draw an area on the image, and then configure the image quality of ROI.
  - $\square$
  - 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 it to delete it.
- Step 3 Click Apply.
- <u>Step 4</u> Click **Add** to add more ROI. You can draw 4 area boxes at most.

# 6.2.3 Splicing

# 6.2.3.1 Panorama 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



<u>Step 2</u> 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.

# 6.2.3.2 Dual-lens Splicing

## Procedure

- Step 1 Select O > Camera > Splicing.
- <u>Step 2</u> Select the type. Supports **Splice by Distance** and **Auto Splicing**.
  - Splice by distance

Configure the splicing distance of the object to be detected, and then click **Apply**. The system automatically shows the corresponding splicing result.

#### Figure 6-34 Splice by distance



- Auto splicing
  - 1. Click **Start**, the system starts to splice the image.
  - 2. Wait for 3 minutes, the system displays the splicing results after splicing is complete.
  - 3. Check the result, and then click **Apply**. The splicing will take effect.



#### Figure 6-35 Auto splicing



# 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 Select Select

Main Stream			Sub Stream	
Enable			Enable	
Compression	G.711A	$\checkmark$	Sub Stream	Sub Stream 1 V
Sampling Frequency	8000	$\vee$	Compression	G.711A V
			Sampling Frequency	8000 ~
udio Input Type		LineIn		×
oise Filter				
licrophone Volume			+	50
peaker Volume			+ :	50
Apply Refresh	Default			

Figure 6-36 Audio

<u>Step 2</u>

Click Omenation next to Enable in Main Stream or Sub Stream.

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



# $\wedge$

Please activate or deactivate the audio acquisition function based on the requirements of the scene.

<u>Step 3</u> Configure audio parameters.

#### Table 6-10 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 <b>Sampling Frequency</b> from <b>8000</b> , <b>16000</b> , <b>32000</b> , <b>48000</b> , <b>64000</b> .	
Audio Input TypeYou can select audio input type from:• Lineln : Requires external audio device.• Mic : Not require external audio device.		
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

- <u>Step 1</u> Select **Select** Select Selec
- Step 2 Click Add.
- <u>Step 3</u> 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**.

 $\square$ 

- 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 6-37 Add alarm tone

Add			×
• Record 🛛 Upload			
File		.pcm	
	Record		

<u>Step 4</u> 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 <a>> Network Settings > TCP/IP.</a>



Figure 6-38 TCP/IP

Host Name	IPC
ARP/Ping	
NIC	Wired(Default) V
Mode	• Static ODHCP
MAC Address	01 + 101 + 101 + 101 + 101 + 101
IP Version	IPv4 v
IP Address	
Subnet Mask	29.29.4.4
Default Gateway	30.31.01.1
Preferred DNS	88.8.8
Alternate DNS	1.1.4.4
	Apply Refresh Default

<u>Step 2</u> Configure TCP/IP parameters.

Table 6-11 Description of TCP/IP parameters

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



Parameter	Description		
	Click		
	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. It this is not enabled, the IP address cannot be configured with ping packet.		
	A demonstration of configuring IP address with ARP/Ping.		
	<ol> <li>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>Get the MAC address of the camera from device label.</li> <li>Open command editor on the PC and enter the following command.</li> </ol>		
	Windows syntax+2		
ARP/Ping	arp –s <ip address=""> <mac> ↔ ping –I 480 –t <ip address=""> ↔</ip></mac></ip>		
	Windows example+3		
	arp -s 192.168.0.125 11-40-8c-18-10-11+ ping -l 480 -t 192.168.0.125+		
	UNIX/Linux/Mac syntax+		
	arp -s <ip address=""> <mac> +/</mac></ip>		
	ping -s 480 <ipaddress> 🕫</ipaddress>		
	UNIX/Linux/Mac example+ <sup>3</sup>		
	arp -s 192.168.0.125 11-40-8c-18-10-11+ ping -s 480 192.168.0.125+		
	<ol> <li>Restart the camera.</li> <li>Check the PC command line, if information such as <b>Reply from</b> <b>192.168.0.125</b> is displayed, the configuration succeeds, and you can turn it off then.</li> <li>Enter http://(IP address) in the browser address bar to log in.</li> </ol>		
NIC	Select the Ethernet card that need to be configured, and the default one is <b>Wired</b> .		
	The mode that the camera gets IP:		
Mode	<ul> <li>Static : Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Apply, the login page with the configured IP address is displayed.</li> <li>DHCP : When there is DHCP server in the network, select DHCP,</li> </ul>		
	and the camera acquires IP address automatically.		
MAC Address	Displays host MAC address.		



Parameter	Description	
IP Version	Select IPv4 or IPv6.	
IP Address	When you select <b>Static</b> in <b>Mode</b> , enter the IP address and subnet mask that you need.	
Subnet Mask		
Default Gateway	<ul> <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 Settings > Port.

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

Figure 6-39 Port

<u>Step 2</u> Configure port parameters.

# $\square$

- 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.



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.	
	<ul> <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>	
	URL format example:	
	rtsp://username:password@ip:port/cam/realmonitor? channel=1&subtype=0	
	Among that:	
RTSP Port	<ul> <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>	
	Example: If you require the sub stream of channel 2 from a certain device, then the URL should be:	
	rtsp://admin:admin@10.12.4.84:554/cam/realmonitor? channel=2&subtype=1	
	If username and password are not needed, then the URL can be:	
	rtsp://ip:port/cam/realmonitor?channel=1&subtype=0	
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.



through

# 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

<u>Step 1</u>	Select <sup>O</sup>	Select 🝳 > Network Settings > PPPoE.		
			Figure 6-40 PPPoE	
		Enable Username Password	none •••••• Apply Refresh Default	
			Apply Refresh Delault	
<u>Step 2</u>	Click	, and then enter u	sername and password.	
		- making PPPoE conr	y PPPoE to avoid possible influence. nection, the device IP address cannot be modified	
<u>Step 3</u>	Click App	oly.		

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 **Select** > Network Settings > DDNS.

 $\square$ 

• 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.

Туре	NO-IP DDNS V		
Server Address	dynupdate.no-ip.com		
Port	80	(1-65535)	
Domain	none	Test	
Username	none	]	
Password	•••••	)	
Interval	1440	min (1440-2880)	
	Apply Refresh Defau	lt	

Figure 6-41 DDNS

<u>Step 2</u> Click Contact to enable the function.

Step 3 Configure DDNS parameters.

#### Table 6-13 Description of DDNS parameters

Parameter	Description	
Туре	The name and web address of the DDNS service provider, see the matching relationship below:	
Server Address	<ul> <li>CN99 DDNS web address: www.3322.org</li> <li>NO-IP DDNS web address: dynupdate.no-ip.com</li> <li>Dyndns DDNS web address: members.dyndns.org</li> </ul>	
Domain	The domain you registered on the DDNS website.	
Test	Only when selecting <b>NO-IP DDNS</b> type, you can click <b>Test</b> 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**.

# Results

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

<u>Step 1</u>

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

# Procedure

Select > Network Settings > Email.

Enable				
SMTP Server	none			
Port	25			
Anonymous				
Username	anonymity			
Password	•••••			
Sender	none			
Encryption Type	TLS(Recommended) V			
Subject	IPC Message	+ 🛃 Attachment	✓ 3 Images	Interval 1 v sec(1-5)
Receiver		Add		
Health Mail				
Sending Interval	60	min (30-1440)		
	Apply Refresh Default			

Figure 6-42 Email

Step 2 Click to enable the function.

<u>Step 3</u> Configure email parameters.

Table 6-14 Description of email parameters

Parameter	Description			
SMTP Server	SMTP server address			
Port	The port number of the SMTP server.			
Username	The account of SMTP server.	For details, see Table 6-15 .		
Password	The password of SMTP server.			
Anonymous	Click O, and the sender's information is not displayed in the email.			
Sender	Sender's email address.			
	Select from <b>None</b> , <b>SSL</b> and <b>TLS</b> .			
Encryption Type				
	For details, see Table 6-15 .			



Parameter	Description
Subject	<ul> <li>Enter maximum 63 characters in Chinese, English, and Arabic numerals.</li> <li>Click + to select title type, and you can set maximum 2 titles.</li> <li>Select Attachment, the system sends 1 image to the configured Email by default.</li> <li>You can select 3 Images, and then configure the interval. The system sends 3 images according to the configured interval after the alarm is triggered.</li> </ul>
Attachment	Select the check box to support attachment in the email.
Receiver	<ul> <li>Receiver's email address. Supports 3 addresses at most.</li> <li>After entering the receiver's email address, the <b>Test</b> button is displayed. Click <b>Test</b> 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 and configure the <b>Sending Interval</b> , and then the system sends test mails as the set interval.

Table 6-15 Description of major mailbox configuration

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

<u>Step 4</u>	Click <b>Apply</b> .
---------------	----------------------

# 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 Settings > 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 Settings > UPnP.



#### Figure 6-43 UPnP

Enable De	vice Di	$\bigcirc$						
Router Sta	itus M	apping Fai	iled					
Mode		Custom	~					
No.	Service N	lame	Protocol	Internal Port	External Port	Status	Enable	Modif
1	HTT	p	WebService:TCP	80	8080	Mapping Failed		区
2	тср		PrivService:TCP	37777	37777	Mapping Failed		Ľ
3	UDF	)	PrivService:UDP	37778	37778	Mapping Failed		Ľ
4	RTSI	0	RTSPService:TCP	554	554	Mapping Failed		Ľ
5	HTTP	c	HTTPSService:TCP	443	44333	Mapping Failed		M

#### <u>Step 2</u> Click One next to **Enable**, and there are two mapping modes: **Custom** and **Default**.

- Select **Custom**, click **I** 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 Select Settings > SNMP.



Figure 6-44 SNMP (1)

Version	V1 V2 V3(Recomn	nended)
SNMP Port	161	(1-65535)
Read Community		
Write Community		
Trap Address		
Trap Port	162	
	Apply Refresh D	efault

Figure 6-45 SNMP (2)

Version	V1 V2 V3(Recommended)	
SNMP Port	161	(1-65535)
Read Community		
Write Community		
Trap Address		
Trap Port	162	
Read-Only Userna	public	
Authentication Type	● MD5 ○ SHA	
Authentication Pa	•••••	
Encryption Type	• CFB-AES	
Encryption Passwo	•••••	
Read/Write Usern	private	
Authentication Type	● MD5 ○ SHA	
Authentication Pa	•••••	
Encryption Type	• CFB-AES	
Encryption Passwo	•••••	
	Apply Refresh Default	

<u>Step 2</u> 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.

 $\square$ 

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

<u>Step 3</u> 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.

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
	The read and write community string that the software agent supports.
Read Community, Write Community	
,	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.
	Set the read-only username accessing device, and it is <b>public</b> by default.
Read-only Username	
	You can enter number, letter, and underline to form the name.
	Set the read/write username access device, and it is <b>private</b> by default.
Read/Write Username	
	You can enter number, letter, and underline to form the name.
Authentication Type	You can select from <b>MD5</b> and <b>SHA</b> . The default type is <b>MD5</b> .
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.

Table 6-16 Description of SNMP parameters

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

#### Results

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

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



5. Unfold all the tree lists displayed in the MG-SOFT MIB Browser, and then you can view the configuration information, video channel amount, audio channel amount, and software version.

 $\square$ 

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.

## **Background Information**

 $\square$ 

Bonjour is enabled by default.

# Procedure

# Step 1 Select > Network Settings > Bonjour.

Figure 6-46 Bonjour

Enable			
Server Name	SPECIAL INCOME.		
	ОК	Refresh	Default

<u>Step 2</u> Click , and then configure server name.

Step 3 Click Apply.

# Results

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 Select Settings > Multicast.



#### Figure 6-47 Multicast

ulticast					
Main Stream			Sub Stream		
Enable			Enable		
IP Address	20	(224.0.0.0-239.255.255.255)	Sub Stream	Sub Stream 1 $$\vee$$	
Port	-000	(1025-65500)	IP Address	100 - 1 - 2 - 0	(224.0.0239.255.255.255)
			Port	49034	(1025-65500)
Apply Refn	esh Default				

<u>Step 2</u> Click , and enter IP address and port number.

Parameter	Description
IP Address	The multicast IP address of <b>Main Stream</b> / <b>Sub Stream</b> 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: <b>Main Stream</b> : 40000; <b>Sub Stream1</b> : 40016; <b>Sub Stream2</b> : 40032, and all the range is 1025–65500.

Step 3 Click Apply.

## Results

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

# 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

	Figure 6-48 Register			
	Enable			
	Server Address	1010110307		
	Port	9500	(1025-65535)	
	Sub-Device ID	Allegen		
		Apply Refresh D	efault	

<u>Step 2</u> Click , and then configure server name.



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.

Table 6-18 Description of register parameters

Click Apply. Step 3

# 6.3.11 QoS

# **Background Information**

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 Settings > **Network Settings** > **QoS**.

Figure 6-49 QoS

Live Video	0		(0-63)
Operation Command	0 (0-63)		(0-63)
	Apply	Refresh	Default

Configure QoS parameters. Step 2

Table 6-19 Description of QoS parameters

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

Step 3 Click Apply.


# 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

<u>Step 1</u> Select **Select** > Network Settings > Platform Access > P2P.



Figure 6-50 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.
- <u>Step 2</u> Log in to mobile phone client and tap **Device management**.
- <u>Step 3</u> Tap + at the upper-right corner.
- <u>Step 4</u> Scan the QR code on the **P2P** page.
- <u>Step 5</u> 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.

## **Background Information**

ONVIF is enabled by default.



## Procedure

<u>Step 1</u>	Select	> Network Settings > Platform Access > ONVIF. Figure 6-51 ONVIF			
		P2P	ONVIF	RTMP	
		Login Ve	rification	)	
			Ар	ply Refresh Default	
<u>Step 2</u>	Click	next to	o <b>Login Veri</b>	fication.	

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.

## **Background Information**

 $\square$ 

- 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

# <u>Step 1</u> Select **Select** > Network Settings > Platform Access > RTMP.

Figure 6-52 RTMP

		P2P	ONVIF RTMP	
		Enable		
		Stream Type	● Main Stream ○ Sub Stream 1 ○ Sub Strear	m 2
		Address Type	● Non-custom ○ Custom	
		IP Address	0.0.0.0	
		Port	1935 (0-65535)	
		Custom Address		
			Apply Refresh Default	
Step 2	Click 🔾			
	$\wedge$			
	Make su	ire that the IP a	address is trustable when enabling RTMP.	
<u>Step 3</u>	Configure 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> <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 <b>Non-custom</b> , you need to enter server IP address and port.	
Port	<ul> <li>IP address : Support IPv4 or domain name.</li> <li>Port : Keep the default value.</li> </ul>	
Custom Address When selecting <b>Custom</b> , you need to enter the path allocated server.		

Step 4 Click **Apply**.

# 6.3.13 Basic Services

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

## Procedure

<u>Step 1</u>	Select	Network Settings > Basic Services.					
		Figu	Figure 6-53 Basic service				
		SSH					
		Multicast/Broadc					
		CGI					
		ONVIF					
		Genetec					
		Mobile Push Noti					
		Private Protocol A	Security Mode (Recomme $\lor$				
			Apply Refresh Default				

<u>Step 2</u> Enable the basic service according to the actual needs.



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		
Genetec		
Mobile Push Notifications	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 <b>Security Mode</b> and <b>Compatible Mode</b> . Security mode is recommended.	

Table 6-21 Description of basic service parameters

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.

# **Background Information**

#### $\square$

This function is only available on select devices.

## Procedure

Step 1 Select Se



#### Figure 6-54 EPTZ



#### <u>Step 2</u> Enable this function and select the display mode.

#### Table 6-22 Description of display modes

Mode	Description	
$\times$	Displays the original screen.	
X	Displays the original image screen + 1 sub-screen.	
	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.	

# <u>Step 3</u> (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

## Procedure

- Step 1 Select > Event > Alarm.
- <u>Step 2</u> Click Onext to **Enable** to enable alarm linkage.
- <u>Step 3</u> Select the alarm-in port.
- <u>Step 4</u> Select the mode.
  - **Alarm**: When an alarm is triggered by the device connected to the alarm-in port, the system performs the defined alarm linkage.

Enable		
Alarm-in Port	Alarm1 V	
Mode	Alarm	)
Schedule	Full Time $\lor$	Add Schedule
Anti-dither	0	sec (0-100)
Sensor Type	NO V	
+Event Linkage		
Record   Enabled		â
Post-Record	10	sec (10-300)
Snapshot Enabled		û
Alarm-out Port   Ena	bled	â
Post-alarm	10	sec (1-300)
Apply Refresh	Default	

Figure 6-55 Alarm

- 1. Configure the sensor type (NO or NC).
- 2. Configure anti-dither. Only record one alarm event during the anti-dither period.
- 3. Select the schedule and arming periods and alarm linkage actions. You can click **Add Schedule** to add new schedule. For details, see "6.5.1.2.1 Adding Schedule".
- Arming/Disarming : Enable/disable the arming function of the alarm-in device.



#### Figure 6-56 Arming/disarming

Enable		
Alarm-in Port	Alarm1	$\sim$
Mode	Arming/Disarming	$\sim$
Sensor Type	NO	~
Arming/Disarming		
Apply Refresh	Default	

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 Se

Figure 6-57 Alarm linkage

Enable		
Alarm-in Port	Alarm1 v	
Schedule	Full Time V	Add Schedule
Anti-Dither	0	sec.(0-100)
Sensor Type	NC v	
Enable Alarm		
Alarm-out Port	1 2	
Post-Alarm	10	sec.(10-300)
Record		
Record	1 2 3 4	
Post-Record	10	sec.(10-300)
Send Email		
Snapshot		3 4
	Apply Refresh De	fault



### 6.5.1.2.1 Adding Schedule

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

### Procedure

#### <u>Step 1</u> Click **Add Schedule** next to **Schedule**.



Figure 6-58 Schedule

- <u>Step 2</u> 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.
- <u>Step 4</u> (Optional) Click **Time Plan Table** to add a new time plan table.

You can:

- Double-click the table name to edit it.
- Click <sup>III</sup> 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 **O** 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 6-59 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 **O** to enable snapshot linkage, and select the channel as needed. Figure 6-60 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 6-61 Alarm-out linkage

Enable Alarm		
Alarm-out Port	1 2	
Post-Alarm	10	sec.(10-300)

#### 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 6-62 Email linkage

Send Email		
------------	--	--

### 6.5.1.2.6 Send Command Linkage

When an alarm is triggered, the system can automatically send the alarm information to the defined IP address.

#### Procedure

- <u>Step 1</u> In the Alarm page, click +Event Linkage. In the drop-down list, select Send Command.
- <u>Step 2</u> Configure the server.
  - 1. Click Server Config.

Figure 6-63 Server config

Send Command   Ena	bled		â
Server		 Server Config	
Command			

2. Click **Add**, and then enter the information such as name, IP/Domain name and port.

Figure 6-64 Add the server

Add	Delete							
	No.	Name	IP/Domain Name	Port	HTTPS	Authentication	Test	Delete
	1	11	12,124	10		2	Test	â
Apply	Refres	h Default						

- 3. (Optional) Configure other information.
  - Click O under **HTTPS** to enable HTTPS.
  - Click <sup>III</sup> under **Authentication** to configure the information of authentication.
  - Click **Test** to check whether the IP/Domain name and port are available.



- Click  $\stackrel{fin}{=}$  to delete the server information.
- 4. Click **Apply**, and then close the **Server Config** page.
- <u>Step 3</u> In the **Server** drop-down list, select the configured server.

The system automatically displays the IP address and port, and then you can enter the rest information as needed.

Figure 6-65 Select the server

Send Command Enabled				
Server	test1	<ul> <li>✓ Server Config</li> </ul>		
Command	http://1 /	test	]	

Step 4 Click **Apply**.

# 6.5.1.3 Subscribing Alarm

## 6.5.1.3.1 Alarm Types

Table 6-23	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 FullThe 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".
Al Event	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".



Alarm Type	Description	Preparation
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 Warming	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.

### **Background Information**

Functions of different devices might vary.

## Procedure

<u>Step 1</u> Click  $\square$  at the right-upper corner of the main page.

Figure 6-66 Alarm (subscription)

Alarm	C		Alarm Su	ubscription 🔨
All T	ypes			
Moti	on Det	Disk Full	Disk	Error
Vide	o Tam	External A	I Secu	urity W
Audi	o Dete	Al Event	Scer	ne Chan
No.	Time	Alarm	Browse Source IP	Alarm
NO.	Time	Туре	Address	Channel
		No Dat	ta	
				Clear
		View All	>	



- Step 2 Click next to Alarm.
- <u>Step 3</u> 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.

<u>Step 4</u> Click **Description** next to **Play Alarm Tone**, and select the tone path.

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

#### **Related Operations**

- View all: Check the complete information on all alarm messages.
- Clear: Delete all alarm messages.

# 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.

Figure 6-67 SD card exception

### Procedure

Step 1 Select Se

SD Card Exception	Network Exception	Voltage Detectio
No SD card.		
Low SD Card Space		
SD card error		
Apply Refresh	Default	

Step 2

Click 💴 to enable the SD card detection functions.

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

<u>Step 3</u> 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 Se

	sec.(10-300)
	sec.(10-300)
	sec.(10-300)
10	sec.(10-300)
1 2 3 4	
10	sec.(10-300)
$\bigcirc$	
1 2	
10	sec.(10-300)
1 2 3 4	

Figure 6-68 Network exception

- <u>Step 2</u> Click **C** to enable the network detection function.
- <u>Step 3</u> 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

<u>Step 1</u> Select **Select** Select Selec



Figure 6-69 Voltage detection

SD Card Exception	Network Exception	Voltage Detection
Voltage Exception		
Overlay		
Enable Alarm		
Alarm-out Port	1 2	
Post-Alarm	10	sec.(10-300)
Send Email		
Apply Refresh	Default	

<u>Step 2</u> Click **C** to enable the voltage detection function.

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

- <u>Step 3</u> 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.

#### **Background Information**

 $\square$ 

- 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

<u>Step 1</u> Select **Select** Select Selec



Motion Detection	Video Tampering	Scene Changing
Enable		
Schedule	Full Time	Add Schedule
Anti-Dither	5	sec. (0-100)
Area	Setting	
Alarm-out Port		
Alarm Channel	1 2	
Post-Alarm	10	sec. (10-300)
Record		
Post-Record	10	sec. (10-300)
Send Email		
Snapshot		
	Apply Refresh D	efault

Figure 6-70 Motion detection

- <u>Step 2</u> Click **C** to enable the motion detection function.
- <u>Step 3</u> Set the area for motion detection.
  - 1. Click **Setting** next to **Area**.



Figure 6-71 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 **example** 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**.

<u>Step 4</u> 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

- <u>Step 1</u> Select **Select** Select Selec
- <u>Step 2</u> 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.



Motion Detection	Video Tampering Sce	ene Changing
Event Type	Video Tampering	$\vee$
Enable		
Covered Area	100	% (1-100)
Duration	1	sec. (1-300)
Anti-Dither	1	sec. (0-100)
Schedule	Full Time	∨ Add Schedule
Alarm-out Port		
Alarm Channel	1 2	
Post-Alarm	10	sec. (10-300)
Record		
Post-Record	10	sec. (10-300)
Send Email		
Snapshot		
	Apply Refresh Default	

Figure 6-72 Video tampering

Table 6-24 Description of video temper parameter

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

<u>Step 3</u> 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 Se



Figure 6-73 Scene changing

Motion Detection	Video Tampering	Scene Changing	_
Enable			
Schedule	Full Time	~ ) (	Add Schedule
Alarm-out Port			
Alarm Channel	1 2		
Post-Alarm	10	s	sec. (10-300)
Record			
Post-Record	10	S	sec. (10-300)
Send Email			
Snapshot			
	Apply Refresh	Default	

<u>Step 2</u> 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 > Audio Detection.



Audio Exception	
Intensity Change	
Sensitivity	- + 50
Threshold	- + 50
Schedule	Full Time         V         Add Schedule
Anti-Dither	5 sec. (0-100)
Enable Alarm	
Alarm-out Port	1 2
Post-Alarm	10 sec.(10-300)
Record	
Record	1 2 3 4
Post-Record	10 sec.(10-300)
Send Email	
Snapshot	
	Apply Refresh Default

Figure 6-74 Audio detection

#### <u>Step 2</u> Set parameters.

- Input abnormal: Click O next to **Audio Exception**, and the alarm is triggered when the system detects abnormal sound input.
- - 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.
- <u>Step 3</u> 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 Se

Select > Event > One-click Disarm.

<u>Step 2</u> Enable **One-click Disarm** or **Disarm by Period** as needed.

- **One-click Disarm** : 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".

One-click Disarm	
Disarm by Period	
1 Disarm by Peri	od will be valid after one-click disarm is disabled.
Disarm Period	Full Time     V     Add Schedule
These settings on	ly take effect in the disarming status.
Event Notifications	
Disarm Alarm Linka	ge <mark>v</mark> Select All
Action	🗹 Alarm-out Port 🔽 Send Email 🔽 Audio Linkage 🔽 Send Command
	Apply Refresh Default

Figure 6-75 One-click disarm

<u>Step 3</u> Enable **Event Notifications**, and then select the **Disarm Alarm Linkage Action** as needed.

The system only triggers the selected alarm linkage actions.

 $\square$ 

The type of disarm alarm linkage action might vary on different devices. Currently we support Alarm-out Port, Send Email, Audio Linkage, Warning Light and Send Command.

Step 4 Click **Apply**.

# 6.5.6 Setting Auto Upload

Select the upload mode, enable it, and then configure the parameters. The camera will upload reports of AI functions to a defined server periodically.

Procedure

```
<u>Step 1</u> Select Event > Auto Upload.
```



<u>Step 2</u> Enable the function.

<u>Step 3</u> Click **Add**, and then configure parameters of HTTP upload method.

You can add 2 server information at most.

Figure 6-76 Auto upload

Jpload Mode	HTTP							
inable								
Add Delet	e							
No.	IP/Domain Name	Port	HTTPS	Path	Authentication	Event Type	Test	Delet

Table 6-25 Description of HTTP mode parameters

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will
Port	be uploaded to.
HTTPS	Click corresponding 🔍 to enable HTTPS.
Path	The storage path of the server for the report.
Authentication	Enable this function, and then configure the username and password. The defined server would receive the images only when you entered the correct username and password.
	Select the event type form the drop-down list. You can select more than one types at the same time.
Event Type	
	The event types in the drop-down list are the same with that of picture playback.
Test	Test the network connection between the camera and the server.
Step 4 Click <b>Apply</b>	,

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 **O** > **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.



#### Ш

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.

Lique	6 77	Local
Figure	: 0-77	LUCai

Form	at Read-Only Read/Write	Hot Swap Refresh					
	Name	Status	Properties	Used Space/Total Space			
	Local Disk1	Normal	Read/Write	25.8	88GB / 118.92GB	General Config	-

# 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 the device name, video standard, and HDMI output.

## Procedure

Step 1

Select System > General > Basic.

Figure 6-78 Basic

Basic Da	ite & Time	
Device Name	AC08EBBYAGD40B0	
Video Standard	PAL	\[         \]     \[         \[         \]     \[
HDMI Output		Automatic Mode
	Apply Refresh Default	

#### <u>Step 2</u> Configure general parameters.

Table 6-26 Description of general parameters

Parameter	Description
Device Name	Enter the device name.
Video Standard	Select video standard from <b>PAL</b> and <b>NTSC</b> .



Parameter	Description		
	Transmits video signals from the device to other display devices, such as a monitor and LED display.		
	• Automatic Mode : The device obtains the resolutions supported by the connected display device and automatically selects the maximum resolution to output the video signals. Automatic Mode is enabled by default.		
HDMI Output	In automatic mode, the device supports $2560 \times 1440$ , $1920 \times 1080$ , and $1280 \times 720$ resolution, with a frame rate of 25 or 30 frames per second, corresponding to the current video standard of the device.		
	<ul> <li>Manual mode: If the video displayed on the connected device is abnormal, disable <b>Automatic Mode</b> to manually configure the resolution and frame rate</li> </ul>		
	50 and 60 frames per second are only available in manual mode.		

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 6-79 Date and time

Basic Date 8	۵ Time		
Time and Time Zone			
$(\mathcal{F})$	Date 2020-06-30 Tuesday <sup>Time</sup> 11:17:26		
Time	Manual Settings ONTP		
System Time	2020-06-30 11:17:26	Ħ	Sync PC
Time Format	YYYY-MM-DD	$\vee$	24-Hour
Time Zone	(UTC+08:00)Beijing	$\vee$	
DST			
Enable			
Туре	• Date Veek		
Start Time	01-01 00:00:00	÷	
End Time	01-02 00:00:00		
Apply Refresh	Default		

## <u>Step 2</u> Configure date and time parameters.

Table 6-27 Description of date and time parameters

Parameter	Description
Time	<ul> <li>Manual Settings : Configure the parameters manually.</li> <li>NTP : When selecting NTP, the system then syncs time with the internet server in real time.</li> </ul>
	You can also enter the IP address, time zone, port, and interval of a PC which installed NTP server to use NTP.
Suctor Time	Configure system time.
System Time	Click <b>Sync PC</b> , and the system time changes to the PC time.
Time Format	Configure the time format. You can select from <b>12-Hour</b> or <b>24-Hour</b> .
Time Zone	Configure the time zone that the camera is at.
DST	Enable DST as needed. Click , and configure start time and end time of DST with <b>Date</b> or <b>Week</b> .

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

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

#### Figure 6-80 Wakeup by duration

Wakeup Policy	By Duration V	
	Refresh Clear	Delete
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	
Sun		Сору
Mon	08:15:06 13:03:55	Сору
Tue		Сору
Wed		Сору
Thu		Сору
Fri		Сору
Sat		Сору
Apply	effesh Default	

#### Figure 6-81 Wakeup by interval

keup Policy	By Interval	v .	
Day • Night			
0	1 2 3 4 5		
Wakeup Time Interval	60	< ∽ min	
	60 60	✓ min	
Wakeup Time Interval     Wakeup Time 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

- <u>Step 1</u> Select System > Power Consumption Mode > General Mode.
- <u>Step 2</u> 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

- <u>Step 1</u> 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 6-82 User

Id Delete						Anonymous Login
No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin 's account	1	6 23
ssword Reset						
assword Reset						
able						
able If you forgot the		security codes through the en	ail address left in advance to reset			
able If you forgot the		security codes through the em	ail address left in advance to reset			
able If you forgot the the password.		security codes through the em	ail address left in advance to reset			
able		security codes through the em	ail address left in advance to reset			

Step 2 Click Add.



Username	test			
Password	•••••			
Confirm Password	•••••			] ⊘
Group	admin		$\vee$	
Timeout Duration	30		~	min
Remarks				
System	Live Search	Restricted Login		
✓ All				
Account		System	✓ System Info	
✓ Manual Control		File Backup	Storage	
✓ Event	<b>~</b>	Network	Peripheral	
✓ Camera		Security	✓ Maintenance	
				Apply Ca



Figure 6-84 Add user (restricted login)

Username	test	
Password	•••••	
Confirm Password	•••••	$\odot$
Group	admin $\vee$	
Timeout Duration	30 ~	min
Remarks		
System	Live Search Restricted Login	
IP Address		
IPv4 V	IP Address $\lor$ 1 . 0 . 0 . 1	
Validity Period 2023-12-13 08:00	2023-12-14 08:00:00	
Period C		
Time Plan		
		Apply Ca

<u>Step 3</u> Configure 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 2 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.
Timeout Duration for Automatic Logout	Set automatic logout time for the user. If the duration that the user does not operate the system exceeds the specified timeout period, the system forcibly logs out the account.
Remarks	Describe the user.
System	Select authorities as needed.
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
	Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to the webpage with the defined IP in the defined time range of validity period.
Restricted Login	<ul> <li>IP address: You can log in to the webpage through the PC with the set IP.</li> <li>Validity period: You can log in to the webpage in the set validity period.</li> <li>Time range: You can log in to the webpage in the set time range. Set as follows:</li> </ul>
	<ol> <li>Select the type, and then enter the IP address or the start address and end address of the host.</li> <li>Select Validity Period, and then configure the start time and end time.</li> <li>Select Period, and then click Time Plan to configure the allowed login time.</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 <sup>the</sup> to delete the added users. Admin user 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 6-85 User

_							
idd I	Delete						Anonymous Login
No.		Username	Group	Password Strength	Remarks	Restricted Login	Edit
1		admin	admin	Medium	admin 's account	/	12 û
issword Re	eset						
		D					
able If you forg	got the pass	word, you can receive security co	odes through the email	address left in advance to reset			
the passw	got the pass word.		odes through the email	address left in advance to reset			
able If you forg	got the pass word.		odes through the email	address left in advance to reset			
able If you forg the passw	got the pass word.		odes through the email	address left in advance to reset			

<u>Step 2</u> Click **O** next to **Enable** in **Password Reset**.

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

- <u>Step 3</u> 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 6-86 Group name

User	Group	ONVIF User		
Add	Delete			
	No.	Group	Remarks	Operation
	1	admin	administrator group	区 直
	2	user	user group	区前

Step 2 Click Add.



Figure 6-87 Add group

1				
Group				
Remarks				
System	Live	Search		
V All				
✓ System		✓ System Info	✓ Manual Control	
🗸 File Backup		✓ Storage	✓ Event	
Vetwork		Peripheral	Camera	
_				

<u>Step 3</u> Enter the group name and memo, and then select group authorities.

<u>Step 4</u> 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 <sup>th</sup> to delete the added users. Admin user cannot be deleted.

 $\square$ 

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 6-88 ONVIF user

lser	Group	ONVIF User			
Add	Delete				
	No.	Username	Group	Password Strength	Edit





#### Figure 6-89 Add ONVIF user

4

#### <u>Step 3</u> 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	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 <sup>th</sup> to delete the added users.



The admin account cannot be deleted.

# 6.7.4 Resources

## Procedure

Step 1 Select > System > Resources.

Step 2

- Select **Resource Config** as needed.
- **Prioritize Videos** : The video of the device can reach to 25/30 fps, but Al functions are not available.



• **Prioritize Intelligence** : Al functions are available for the device, but the video cannot reach to 25/30 fps.

	Figure	6-90 Resources	
Modifying resource a	llocation mi	ght cause the device t	o restart.
Resource Config		Prioritize Videos	O Prioritize Intelligence
Apply Refresh	Default		

#### Step 3 Click Apply.

Modifying resource allocation might cause the device to restart.

# 6.7.5 Peripheral Management

## 6.7.5.1 Configuring Serial Port

Set the serial port of the external device.

### Procedure

- <u>Step 1</u> Select **System** > **Peripheral** > **Serial Port**.
- <u>Step 2</u> Configure parameters.

Serial Port	External Light	Wiper
Address	1	
Baud Rate	9600	~
Data Bit	8	~
Stop Bit	1	~
Parity	None	~
	Apply Refrest	n Default

Figure 6-91 Serial port settings

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

Parameter Description	
Address	Enter the corresponding device address. It is <b>1</b> by default.
	Make sure that the address is the same as the device address; otherwise you cannot control the device.



Description
Configure device baud rate. It is <b>9600</b> by default.
It is <b>8</b> by default.
It is <b>1</b> by default.
It is <b>None</b> by default.

Step 3 Click **Apply**.

# 6.7.5.2 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 "6.7.5.1 Configuring Serial Port".

## Procedure



<u>Step 2</u> Select working mode as needed.

#### Figure 6-92 External light

Face Detection 0	Working Mode	Auto 🗸	
Face Recognition 0 Repetition Count: 0	Auto Mode	Time v	
	Light Brightness	+	128
	Time Plan	Full Time V	Add Schedule
	Apply Refresh De	efault	

#### Table 6-31 Lamp parameters

Parameter	Description			
Working Mode	<ul> <li>Off : The external light is disabled.</li> <li>Manual : Set the light brightness manually.</li> <li>Auto : The camera turns on or turns off the light according to the light time and photoresister automatically.</li> </ul>			
Auto Mode	<ul> <li>Time : When selecting Time in Auto Mode, set the arming period. During the arming period, the external light is on.</li> <li>Select the added time plan table in the Time Plan list. Click Add</li> <li>Schedule to add new time plan table. For details, see"6.5.1.2 Alarm</li> </ul>			
	<ul> <li>Linkage".</li> <li>Photoresistor : When you select Photoresistor in Auto Mode, the camera turns on the external light according to the brightness automatically.</li> </ul>			



Parameter Description	
Light Brightness	Set the brightness of the external light.
	For some models, you can set the brightness of each external light separately.

Step 3 Click **Apply**.

# 6.7.5.3 Configuring Wiper

# Procedure

<u>Step 1</u> Select **System** > **Peripheral** > **Wiper**.

<u>Step 2</u> Configure working mode of wipers.

Serial Port	External Light	Wiper	
Face Detection: 22 Face Recognition (	+ 	2021-05-19 09:24-55	Wiper       Interval     10   sec. (0-255)
-			Start Stop Once
IPC	1		Scheduled C Everyday V 04:00 O
			Once Apply Refresh Default

Figure 6-93 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.		
	Configure working mode of the wiper.		
Start, Stop, Once	<ul> <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 <b>Scheduled</b> checkbox and set the time, and then the wiper will work as the configured time.		
	Click <b>Once</b> , and then the wiper works once. It can be used to check whether the wiper works normally.		

Step 3 Click Apply.




# 7 Live

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

# 7.1 Live Page

Log in the webpage, and then click the **Live** tab.

Pages might vary with different models.



Figure 7-1 Live (single channel)

## Figure 7-2 Live (multiple channels)





alhua



Figure 7-4 Live (3-channel camera with panorama, medium and distant view)



## Table 7-1 Description of function bar

No.	Function	Description
1	Display mode	You can select the display mode from <b>General Mode</b> , Face Mode, Metadata Mode, ANPR, Parking Space Detection, PPE Detection Mode 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		Adjustment operations in live viewing.
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  $\checkmark$  , and then select the stream as needed.

Channel List		
	Channel1	M
	Channel2	Main Stream
	Channel3	Sub Stream 1
	Channel4	Sub Stream 2

- **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".
- M means the current stream is main stream; 1 means the current stream is sub stream 1; 2 means the current stream is sub stream 2.

# 7.3 Live View Function Bar

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

lcon	Function	Description
<b>*</b>	Force Alarm	Display the status of alarm sound. Click the icon to enable or disable the alarm sound forcibly.
● ⊕	Digital Zoom	<ul> <li>You can zoom video image through two operations.</li> <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>
0	Snapshot	Click the icon to capture one picture of the current image, and it will be saved to the configured storage path. For details on viewing or configuring storage path, see "6.1 Local".

Figure 7-5 Encode bar



lcon	Function	Description	
3 / 🖻	Triple Snapshot	Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path.	
		For details on viewing or configuring storage path, see "6.1 Local".	
		Click the icon to record video, and it will be saved to the configured storage path.	
	Record		
		For details on viewing or configuring storage path, see "6.1 Local".	
		Click the icon, the <b>AF Peak</b> (focus eigenvalue) and <b>AF Max</b> (max focus eigenvalue) are displayed on the video image.	
(+)	Aux Focus	<ul> <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>	
		Aux focus closes automatically after five minutes.	
<b>18</b>	Audio	Click the icon to enable or disable audio output.	
Ŷ	Talk	Click the icon to enable or disable the audio talk.	
		This function is used in device installation and configuration process to make the size of the target in the screen meets the capturing requirements. Here we use <b>IVS</b> as an example.	
	Auxiliary Installation	1. Click in the upper-right corner of the live view page, and then select <b>IVS</b> . The image pops up the human-shape box.	
-			
		The default human-shape box is the minimum pixel requirement that can be detected.	
		<ol> <li>In the live screen, click the human-shape box, and then drag it to the position you want.</li> <li>Adjust the size of the box through the following 2 methods.</li> </ol>	
		<ul> <li>Click Auxiliary Installation in the lower-left corner of the page, and then enter the width pixel number.</li> <li>Drag the corner of the human-shape box. You can check the width pixel number of the box in the lower-left corner of the page.</li> </ul>	





# 7.4 Window Adjustment Bar

# 7.4.1 Adjustment

This section introduces the adjustment of image.

Table 7-3 Description of adjustment bar

lcon	Function	Description
1:1	Original Size	Click the icon, and then the video displays with original size.
к. м	Full Screen	Click the icon to enter full screen mode; double- click or press Esc to exit.
Ð	W:H	Click the icon to resume original ratio or change ratio.
22	Fluency Adjustment	<ul> <li>Click the icon to select the fluency from Realtime , General and Fluent.</li> <li>Realtime : Guarantees the real time of the image. When the bandwidth is not enough, the image might not be smooth.</li> <li>General : It is between Realtime and Fluent.</li> <li>Fluent : Guarantees the fluency of the image. There might be delay between live view image and real-time image.</li> </ul>
⊕	Al Rule	Click the icon, and then select <b>Enable</b> to display Al rules and detection box; select <b>Disable</b> to stop the display. It is enabled by default.
	Crowd Distribution Map	Click the icon and select <b>Enable</b> . The <b>Crowd</b> <b>Distribution Map</b> page is displayed. For details, see "8.1 Setting Crowd Distribution Map".
$\overline{\bigcirc}$	Adjust View	Click the icon and select <b>Enable</b> . When moving the mouse printer 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. Only Parking Space Detection Fisheye WizMind Network Camera supports this function.
Ē	Intelligence Area	Click the icon, and then select <b>Enable</b> to display all the intelligent rules in the image.



lcon	Function	Description
	Scene Box	Click the icon, and then select <b>Enable</b> to display the rule box of the medium and distant-view channels in the panorama channel, and display the rule box of the distant-view channel in the medium-view channel.
		Only Triple-Sight Perimeter Protection Bullet WizMind Network Camera supports this function.
	Window Layout	When viewing multi-channel image, you can select display layout.

# 7.4.2 Zoom and Focus

Click **Zoom & 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.

 $\square$ 

The focus would adjust automatically after zooming in or out.

Figure 7-6 Zoom and focus

Zoom & Focus	Ý		
Zoom Speed 1	5 20		
Focus Speed 1	5 20		
	+		
Auto Focus			
Reset			
Refresh			
Area Focus			



Parameter	Description	
	Changes the focal length of the camera to zoom in or out the image.	
Zoom Speed	1. Set the speed value. The <b>Zoom Speed</b> is the adjustment range in one click. The larger the value is, the more the image would zoom in or out in one click.	
	2. Click or hold + or – button, or drag the slider to adjust zoom.	
	Adjusts the optical back focal length to make the image clearer.	
Focus Speed	<ol> <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> </ol>	
	2. Click or hold + or – button, or drag the slider to adjust focus.	
	Adjusts image clarity automatically.	
Auto Focus		
	Do not make any other operation during auto focus process.	
	Restores focus to default value and corrects errors.	
Reset		
	You can restore the focus if the image has poor clarity or has been zoomed too frequently.	
Refresh	Get the latest zoom setting of the camera.	
	Focus on the subject of a selected area.	
Area Focus	Click <b>Area Focus</b> , and then select an area in the image, the camera performs auto focus in that area.	

Table 7-4 Description of zoom and focus parameter

# 7.4.3 Auxiliary Calibration

When installing and commissioning the camera, you can enable this function to assist in achieving horizontal installation of the camera in some specific scenes such as long-distance perimeter scenes.

## Procedure

<u>Step 1</u> Adjust the camera angle until the bubble on the spirit level is within 3 degrees.

Spirit level is available on select models.

- <u>Step 2</u> Place an object 6 meters away from the camera in a horizontal position for distance tagging.
- <u>Step 3</u> On the **Live** page, click the panorama image, and then click **Auxiliary Calibration**.
- <u>Step 4</u> Enter the installation height, and then click **Setting**.

A horizontal line is displayed in the panorama image, which is positioned horizontally 6.0 meters away from the camera.



#### Figure 7-7 Configure auxiliary calibration





When the tagged object is aligned with the horizontal line, it means that the auxiliary calibration is successful.

# 7.4.4 Angle Adjustment

Click **Angle Adjustment** at the upper-left corner of **Live** page to adjust the camera angle by controlling the PTZ.



#### Figure 7-8 Adjust camera angle

 $\square$ 

- For 3-channel camera with panorama, medium and distant views, you can select one channel to adjust the angle, which will be apply to other 2 channels automatically.
- The PTZ function might vary depending on the camera models.
  - Some models only support up and down adjustment, not left and right adjustment.



 For some models of multi-channel cameras, adjusting the angle of one channel will adjust the angles of other channels synchronously. However, for some other models, adjust the angle of one channel will not affect other channels.

# 7.4.5 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.

 $\square$ 

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



Figure 7-9 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.
- **O** (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.
- Y (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.

 $\square$ 

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

# 7.4.6 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 7-10 Fisheye-ceiling mount



Figure 7-11 Fisheye-wall mount



Figure 7-12 Fisheye-ground mount



Figure 7-13 Fisheye-VR mode



Table 7-5 Description of fisheye configuration

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



Parameter	Description		
	The display model of the current image. There are different display modes for each installation mode.		
	<ul> <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> </ul>		
Display mode	• Ground : 1P+1, 2P, 1+3	, 1+4, 1P+6, 1+8.	
	~	inal size by default when switching installation	
	mode.	, ,	
Ceiling/Wall/ Ground mount	Original image	The original image before correction.	
		360° rectangular panoramic image screen + independent sub-screens.	
	←→ 1P+1	• You can zoom or drag the image in all the screens.	
		• You can move the start point (left and right) on rectangular panoramic image screen.	
	$\longleftrightarrow$	Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. It is also called dual-panoramic image.	
Ceiling/Ground	<b>←</b> 2P	You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.	
mount		Original image screen + two independent sub- screens. Ground mount does not support this display mode.	
	Q ,  1+2	• You can zoom or drag the image in all the screens.	
		• You can rotate the image on the original image screen to change the start point.	
	Q 1+3	Original image screen + three independent sub- screens.	
		• You can zoom or drag the image in all the screens.	
		• You can rotate the image on the original image screen to change the start point.	



Parameter	Description	
		Original image screen + four independent sub- screens.
		• You can zoom or drag the image in all the screens.
	,	• You can rotate the image on the original image screen to change the start point.
		360° rectangular panoramic screen + six independent sub-screens.
	↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	• You can zoom or drag the image in all the screens.
		• You can move the start point (left and right) on rectangular panoramic image screen.
		Original image screen + eight independent sub- screens.
	1P+8	• You can zoom or drag the image in all the screens.
		• You can rotate the image on the original image screen to change the start point.
	× 1P	180° rectangular panoramic image screen (from left to right).
		You can drag the image in all the screens (up and down) to adjust the vertical view.
		180° rectangular panoramic image screen + three independent sub-screens.
	1P+3	• You can zoom or drag the image in all the screens.
		• You can drag the image in all the screens (upper and lower) to adjust the vertical view.
Wall mount		180° rectangular panoramic image screen + four independent sub-screens.
	1P+4	• You can zoom or drag the image in all the screens.
		• You can drag the image in all the screens (upper and lower) to adjust the vertical view.
		180° rectangular panoramic image screen + eight independent sub-screens.
	1P+8	• You can zoom or drag the image in all the screens.
		• You can drag the image in all the screens (upper and lower) to adjust the vertical view.



Parameter	Description				
	Panorama	Drag or cross the screen 360° to unfold the distortion panorama, and you can drag the image in left/right direction.			
	Semi-circle	<ul> <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>			
VR mode	Cylinder	<ul> <li>Display the distortion panorama in 360° circularity.</li> <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> <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, Metadata 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, Metadata Mode, PPE Detection Mode and Parking Space Detection.

 $\square$ 

- 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 7-14 Face mode



• Select Metadata Mode from the display mode drop-down list.

Figure 7-15 Metadata mode



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

#### Figure 7-16 PPE Detection Mode



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





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	<ul> <li>Displays the captured images.</li> <li>Click a snapshot in the area, and the details of the snapshot are displayed.</li> <li>Click  to set the attributes displayed.</li> <li>Image: This attribute is not available for parking space mode.</li> </ul>			



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.

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





# 8 AI

The camera locates, recognizes and tracks the changes in the monitoring scene, and analyzes and judges the behavior of the target on this basis, which is called the AI function of video monitoring.

When the intelligent function is enabled, the configured rules and their effects can be displayed both on the live video and the intelligent rule configuration page. When a target triggers the AI function, the rule lines are displayed as red flashing.

## $\square$

Vehicle Density, Crowd Distribution Map and Heat Map do not support red flashing when the alarm is triggered.

# 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 AI > 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 IIIII is the vertical horizontal icon.
  - Select the added rulers on the image, and click III to delete them.



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

Smart Plan	Rule Config	2.1 Crowd	Distribution Map			
Rule Config	Global Config					
and the second	Nicesang		Actual Length	1		m
	/; ***	0:0+21 14 59 0	Installation Height	6.2		m
	<i>†</i>		Back Apply	Refresh	Default	

- 5. Select a calibration type and enter the actual length, and then click Add Rule.
- 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 AI > Smart Plan, and enable Crowd Distribution Map.
- You have configured the parameters on the **Global Config** page.

## Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to Crowd Distribution Map , and then click Next.

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

Figure 8-2 Rule configuration

hd Rule No. 1 2	Area CDM-1 CDM-2	Enable	People Number to Trigger Alarn 20 20	n	Delete Či	
1 2	CDM-1 CDM-2	Fachts	20	n	÷	
2	CDM-2	Easter				
ection Area		Enable	20		ŝ	
		Enable				
		Enable				
		Global Crowd Density	4	Human/m <sup>2</sup> (2-10)		
		Time Plan	Full Time	<ul> <li>Add Schedule</li> </ul>		
		+Event Linkage				
		Snapshot Enabled			ŝ	
	And in case of the local division of the loc					

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



Click , and then 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.

- <u>Step 5</u> 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 <sup>(L)</sup> 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.

<u>Step 6</u> Configure parameters.

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

#### Table 8-1 Description of crowd map parameters

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".

# Results

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 Recognition

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 Recognition: 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 recognition flowchart

# 8.2.1 Enabling Face Recognition

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

# Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click next to **Face Recognition** to enable face recognition of the corresponding channel, and then click **Next**.
- <u>Step 3</u> Select the detection mode.

Pages and functions might vary on different devices. Please refer to the actual device for detailed information.



#### Figure 8-6 Face recognition (1)

😔 Smart Plan 🛛 😔 Rule Config 🛛 🙆 Face Recognition				
Mode 💿 General Mode 🔿 Counting Mode				
	Face Database Config			
	Enable		OSD Info	
	Face Enhancement			
	Non-living Filtering			
	Target Box Overlay			
	Remove Duplicate Faces			o
	Face Cutout	One-inch Photo	$\vee$	
	Snapshot Mode	Optimized	$\vee$	
	Property			
	Face Beautifying			
	Level		+	50
	Face Exposure			
	Face Target Brightness	-	+	50
	Face Exposure Interval Detectio.	•	+	5 sec
	Privacy Protection			
	Target	Face		
	Time Plan	Full Time	$\vee$	Add Schedule
	Advanced			•
	Back Apply Refrest	Default		

Figure 8-7 Face recognition (2)

Smart Plan— Rule Config—2.1 Face Recognition				
Channel 1(Details)	V			
	Face Database Config			
*	Enable	•	ISD Info	
	Target Box Overlay			
	Remove Duplicate Faces			0
	Face Cutout	One-inch Photo	~	
	Snapshot Mode Property	Optimized	~	
	Face Snapshot Enhancement	Off	V	
	Face Exposure			
	Face Target Brightness	-	+	50
	Face Exposure Interval Detecti	•	+	5 sec
	Time Plan	Full Time	V	Add Schedule
	Advanced			¥
	Back Apply Re	fresh Default		

• **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 2 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.

<u>Step 4</u> Click One next to **Enable** to enable the face detection function.

- <u>Step 5</u> (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.

 $\square$ 

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 <sup>III</sup> to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click in to draw the minimum size of the target, and click is 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.
- <u>Step 6</u> Set parameters.

Parameter	Description			
OSD Info	Click <b>OSD Info</b> , and the <b>Overlay</b> page is displayed, and then enable the face statistics function. The number of detected faces is displayed on the <b>Live</b> page. For details, see "6.2.2.2.12 Configuring Face Statistics".			
Face Enhancement	Click <b>C</b> to enable face enhancement. Priority should be given to ensuring facial clarity when the bitstream is relatively low.			
Non-living Filtering	Filter non-living faces in the image, such as a face picture.			
Target Box Overlay	Click 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".			

Table 8-2 Description of face detection parameters



Parameter	Description
	During the configured period, the duplicate faces are displayed only once to avoid repeated counting.
Remove Duplicate Faces	Click 🗿 to configure the parameter, and then click <b>Apply</b> .
	<ul> <li>Time : During the configured time, the function is enabled.</li> <li>Precision : The larger the precision value, the higher the accuracy.</li> </ul>
	Set a range for the captured face image, including face, one-inch picture, and custom.
	When selecting <b>Custom</b> , click <sup>O</sup> , configure the parameters on the prompt page, and then click <b>Apply</b> .
Face Cutout	<ul> <li>Customized width: Set snapshot width; and then enter the times of the original face width. It ranges from 1–5.</li> </ul>
	<ul> <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.</li> </ul>
	When the value is 0, it cuts out the face image only.
Snapshot Mode	<ul> <li>General mode:</li> <li>Optimized Snapshot : Capture the clearest picture within the configured time after the camera detects face.</li> <li>Recognition Priority : 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>
	Click <b>Advanced</b> to set the optimized time.
	<ul> <li>Counting mode: The snapshot mode is tripwire by default, and you cannot change it.</li> </ul>
Property	Click <b>D</b> next to <b>Property</b> to enable the properties display.
Face Beautifying	After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
	Select the mode to enhance the snapshot.
Face Snapshot Enhancement	<ul> <li>Auto: The system automatically improves the quality of the snapshot.</li> <li>Manual: You can adjust NR Level , Sharpening Level, Brightness Level and Redness Level manually.</li> <li>Off: Turn off the function.</li> </ul>
Face Exposure	Enable <b>Face Exposure</b> . 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.



Parameter	Description
Face Exposure Interval Detection	Set the face exposure interval detection 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> <li>Snapshot Angle Filter : Set snapshot angle to be filtered during the face detection.</li> <li>Snapshot Sensitivity : Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>Optimized Time : Set a period to capture the clearest picture after the camera detects face.</li> </ul>
Step 7 Set arming per	riods 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.

## **Background Information**

• General mode: You can add 5 databases at most as needed.

#### Figure 8-8 General mode

Add Refresh					Fr	ee Space	99%
No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	VIP	0	82	Unconnected	Ø		â
2	Employees	0	82	Unconnected	0		
3	5	0	82	Unconnected	0		ů.
4	6	0	82	Unconnected	Ø		ė.
5	test01	0	82	Unconnected	0		â

• 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 8-9 Counting mode

Add Refresh					Fr	ee Space	99%
No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	AllPeople	34	82	Connected	Ø		8
2	ExcludePeople	0	82	Connected	0	Ð	8
3	VIP	0	82	Unconnected	Ø		8
4	Employees	0	82	Unconnected	0	Ð	8
5	5	0	82	Unconnected	Ø		a
6	6	0	82	Unconnected	0		8
7	test01	0	82	Unconnected	Q		8



## Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to **Face Recognition** to enable face recognition of the corresponding channel, and then click **Next**.
- <u>Step 3</u> Select the detection mode.
- <u>Step 4</u> Click Face Database Config on the Face Recognition page.

Figure 8-10 Face database configuration

<b>Q</b>	Face Database Config		
	Enable	OSD Info	
	Face Enhancement		
T 📑	Non-living Filtering		
	Target Box Overlay		
	Remove Duplicate Faces	•	
	Face Matting	One-inch Photo V	
	Snapshot Mode	Optimized $\lor$	
	Property		
	Face Exposure		
	Target Face Brightness	- + 50	
	Face Exposure Interval Detec	ti • + 5 sec.	
	Time Plan	Full Time V Add	d Schedule
	+Event Linkage		
	Snapshot Enabled		â
	Advanced		•
	Back Apply R	Refresh Default	

<u>Step 5</u> Click **Add**, and then set the name of the face database.

#### Figure 8-11 Add face database

Add			Х
Name	test01		
		ОК	Cancel

Step 6 click **OK**.

# **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

- <u>Step 1</u> On the **Face Database Config** page, click **I** next to the face database to be configured.
- Step 2 Click **Register**.
- <u>Step 3</u> Click **Upload**, select a face picture to be uploaded, and then click **Open**.

 $\square$ 

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 8-12 Register

	* Name	abc		
	Gender	Male	~	
E	Birthday		Ë	
Reselect	Region	All / All / All	$\sim$	
	Credent	ID Card	×	
	Credent			
	Address			
	Remarks			

<u>Step 4</u> Enter the information about face picture according to the actual situation.

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

Click

<u>Step 6</u>

Task List 1, 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".

Parameter	Error	Description
0x1134000C		The picture is too large, and the upper limit is 150K.
0x1134000E	Picture importing error	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	The picture format is not correct. Import the picture in JPG format.
2	error	No face in the picture or the face is not clear. Change the picture.

Table 8-3 Description of error code



Parameter	Error	Description
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

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



Figure 8-13 Task list

Task List ×
Select Picture(.jpg)
Naming Format Name#SGender#BBirthday#NRegion#PProvince#CCity#TCredential Type#MCredential No. Example John#S1#B1990-01-01#NCN#T1#M330501199001016222 Gender 1.Male2.Female Credential Type 1.ID Card2.Passport3.Military Officer Card4.Other
Import Cancel

<u>Step 4</u> 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.

<u>Step 5</u> 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

- <u>Step 1</u> On the **Face Database Config** page, click **I** next to the face database to be configured.
- <u>Step 2</u> 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





	* Name			
	* Name	abc		
	Gender	Male	× ]	
)Ë	Birthday		Ħ	
Reselect	Region	AII / AII / AII	~	
	Credent	ID Card	~	
	Credent			
	Address			
	Remarks			
		Add to task list	Can	ce

8.2.2.3.2 Deleting Face Picture

Step 5

On the **Face Database Config** page, click **I** 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

Task List 2 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

Task List 2 , and then click **Operation** to delete all face pictures.



# 8.2.2.4 Face Modeling

## **Background Information**

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

 $\square$ 

- 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 recognition) are not available temporarily, and will be available after modeling.

## Procedure

<u>Step 1</u> On the **Face Database Config** page, click  $\blacksquare$  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.

<u>Step 3</u> View the modeling result.

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

Figure 8-15 Fail	ed modeling
------------------	-------------

Task List	X
Modeling completed. ⊘ Succeed 0 ▲ Failed 2 Query	
	Close

Click  $\equiv$  to view the face picture in list format; click  $\stackrel{\texttt{BB}}{=}$  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 recognition 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.

<u>Step 2</u> Arm face database.

1. Click Omet 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.

Name	1	
Arm		
Similarity	-	+ 82
Time Plan	Full Time	<ul> <li>✓ Add Schedule</li> </ul>
Local		
Alarm-out Port	Alarm Channel1	$\checkmark$
Alarm Mode	Select None	· • •
Post-Alarm	1	sec. (1-300)
Report Mode	All	· 0
General Mode	•	Stranger Mode
Record		Record
Post-Record	10 sec. (10-300)	Post-Record 10 sec. (10-300)
Audio Linkage		Audio Linkage
Send Email		Send Email
Snapshot		Snapshot

Figure 8-16 Arm alarm



Figure 8-17 Arm alarm (all people)

Name	AllPeople	
INAME AIIPEOPIE		
Arm		
Similarity	-	+ 82
Time Plan	Full Time	✓ Add Schedule
Local		
Alarm-out Port	Alarm Channel1	$\checkmark$
Alarm Mode	Select None	√ 0
Post-Alarm	1	sec. (1-300)
Report Mode	All	∨ 0
General Mode	*	Stranger Mode
Record		Record
Post-Record	10 sec. (10-300)	Post-Record 10 sec. (10-300)
Audio Linkage		Audio Linkage
Send Email		Send Email
Snapshot		Snapshot
Auto Delete		
Delete Old Files	7	day(s) ago (1-30)

Figure 8-18 Arm alarm (exclude people)

Arm	Alarm		$\times$
	Name	ExcludePeople	
	Arm		
	Similarity	- + 82	
	Time Plan	Full Time         V         Add Schedule	
		Apply Cancel	

- <u>Step 3</u> Set arming periods.
- <u>Step 4</u> Click Onext 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.



Parameter Description			
	<ul> <li>All: No matter the comparison result of the detected face and that in the face database, the camera links alarm out.</li> </ul>		
	<ul> <li>General: The camera links alarm out when the detected face matches that in the face database, the camera links alarm out.</li> </ul>		
Alarm Mode	<ul> <li>Stranger: The camera links alarm out when the detected face fails to match that in the face database, the camera links alarm out.</li> <li>Select none: 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.		

<u>Step 5</u> Select the report mode and alarm linkage action.

- There are four report modes:
  - All: The camera reports events no matter the comparison results 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".
- <u>Step 6</u> Enable **Auto Delete**, set the time.

The camera will delete the old files at 0:00 according to the configured time or when the database is full.

```
\square
```

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 Recognition 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 8-19 Face recognition result



# 8.3 Setting Face Detection

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

# Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- Step 2 Click Onext to Face Detection to enable face detection of the corresponding channel, and then click Next.
- Step 3 Click mean next to **Enable** to enable the face detection function.

Pages and functions might vary on different devices. Please refer to the actual device for detailed information.



#### Figure 8-20 Face detection (1)

Smart Plan			
	Enable Face Enhancement Non-living Filtering Target Box Overlay Remove Duplicate Faces Face Cutout Snapshot Mode Property	One-inch Photo Optimized	OSD Info C V
	Face Beautifying Level Face Exposure Face Target Brightness Face Exposure Interval Detectio Privacy Protection		+ 50 + 50 + 5 sec
	Target Time Plan +Event Linkage Snapshot   Enabled Advanced Back Apply Refresh	Face     Full Time     Default	✓ Add Schedule â



Smart Plan 🔗 Rule Config 🔕 Face Detection				
Channel 1(Details)	~			
	Enable		OSD Info	
1027-12-11 (1.49.48				
				0
	Face Cutout	One-inch Photo	$\vee$	
IPE	Snapshot Mode	Optimized	V	
	Property			
	Face Snapshot Enhancement	Off	$\vee$	
	Face Exposure			
	Face Target Brightness		+	50
	Face Exposure Interval Detectio	– •	+	5 sec
	Time Plan	Full Time	$\sim$	Add Schedule
	+Event Linkage			
	Snapshot Enabled			â
	Channel	1(Details)		
	Advanced			•
	Back Apply Refre	Default		

<u>Step 4</u> (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.

<u>Step 5</u> Set parameters.

Parameter	Description	
OSD Info	Click <b>OSD Info</b> , and the <b>Overlay</b> page is displayed, and then enable the face statistics function. The number of detected faces is displayed on the <b>Live</b> page. For details, see "6.2.2.2.12 Configuring Face Statistics".	
Face Enhancement	Click C to enable face enhancement. Priority should be given to ensuring facial clarity when the bitstream is relatively low.	
Non-living Filtering	Filter non-living faces in the image, such as a face picture.	
Target Box Overlay	Click 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	<ul> <li>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.</li> <li>Time: In the configured time, <b>Remove Duplicate Faces</b> is enabled.</li> </ul>	
	• Precision: The higher the level, the more sensitive the device will be to remove duplicate faces.	
	Set a range for matting face image, including face, one-inch photo and custom.	
Face Cutout	When selecting <b>Custom</b> , click <sup>O</sup> , configure the parameters on the prompt page, and then click <b>Apply</b> .	
	<ul> <li>Customized width: Set snapshot width; enter the times of the original face width. It ranges from 1–5.</li> <li>Customized for a bright fact for a bright in group bet enter the times.</li> </ul>	
	<ul> <li>Customized face height: Set face height in snapshot; enter the times of the original face height. It ranges from 1–2.</li> </ul>	
	• Customized body height: 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.	

Table 8-6 Description of face detection parameters



Parameter	Description	
Snapshot Mode	<ul> <li>Real-time : Capture the picture immediately after the camera detects face.</li> <li>Optimized : Capture the clearest picture within the configured time after the camera detects face.</li> <li>Quality Priority : 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> <li>Click Advanced to set the optimized time.</li> </ul>	
Property	Click <b>D</b> next to <b>Property</b> to enable the properties display.	
Face Beautifying	Enable <b>Face Beautifying</b> 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 Snapshot Enhancement	<ul> <li>Select the mode to enhance the snapshot.</li> <li>Auto: The system automatically improves the quality of the snapshot.</li> <li>Manual: You can adjust NR Level , Sharpening Level, Brightness Level and Redness Level manually.</li> <li>Off: Turn off the function.</li> </ul>	
Face Exposure	Click <b>A provide a constant of Face Exposure</b> . 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 Interval Detection	Set the face exposure interval detection 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> <li>Snapshot Angle Filter : Set snapshot angle to be filtered during the face detection.</li> <li>Snapshot Sensitivity : Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>Optimized Time : Set a period to capture the clearest picture after the camera detects face.</li> </ul>	

<u>Step 6</u> 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".

## Results

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 8-22 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 calibration area, calibration verification, and global sensitivity.

### Background Information

- 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.

## $\square$

- 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

- <u>Step 1</u> Select AI > Smart Plan.
- <u>Step 2</u> Click Omega next to IVS to enable IVS of the corresponding channel, and then click Next.
- Step 3 Click the **Global Config** tab.

Smart Plan— Rule Config—21 IVS			
Rule Config Global Config			
	1. Draw an area>2. Draw	three vertical lines and one horizontal line.	
Carl - I have !!	Actual Length	1	m
	Calibration Verification	Width Verification	Calibration Verification
	Global Sensitivity	1 2 3 4 5 6 7 8 9	0 10
	Long Distance Mode		
	Self-Learning		0
	Linked Experience Databa		Experience Database
	Back Apply I	Refresh Default	

Figure 8-23 Global configuration of IVS

<u>Step 4</u> Set calibration area and ruler.

- 1. Click  $\square$  and draw a calibration area in the image, and right-click to finish the drawing.
- 2. Click the ruler icon to draw one horizontal ruler and three vertical rulers in the calibration area.
  - Indicates vertical ruler, and Immi indicates horizontal ruler.
  - Select an added ruler, and click muture to delete the ruler.

<u>Step 5</u> Set the global sensitivity.



Adjust the filter sensitivity. With higher value, it is easier to trigger an alarm when lowcontrast object and small object are captured, and the false detection rate is higher.

<u>Step 6</u> (Optional) Enable **Long Distance Mode**.

- We recommend you enable **Long Distance Mode** when there are fewer targets but higher requirements for detection distance.
- When **Long Distance Mode** is enabled, target filter is not available on the **Rule Config** tab.
- Long Distance Mode is not available when AcuPick is enabled.
- <u>Step 7</u> Configure experience database.

# 

If false alarms frequently occur, you can import the false alarm targets to the experience database for algorithm self-learning. The next time the same target occurs, it will be filtered to reduce false alarms.

- 1. Click Experience Database.
- 2. Click Add , enter the name of the experience database, and then click OK.
- 3. Click <sup>(III)</sup> on the **Details** column, and then click **Import Videos**.
- 4. Select channel, event, and time, and then click **Search**.

Figure 8-24 Search for events

- 5. Select the event video, and then click Next.
- 6. Drag the progress bar to select the video clip where the target is falsely reported, and then click **Next**.

 $\square$ 

The time of the video clip cannot exceed 10 seconds.



### Figure 8-25 Clip videos



- 7. Play the video clip, and then pause it when the target detection box is displayed.
- 8. Click **Select Target**, and then select the target to be imported in the video.
- 9. Select the sampling interval, and then click **Import**.

### Figure 8-26 Import target samples





#### Figure 8-27 Modeling completed

5			
Modeling Status All V	Search Import Videos Modeling All Modeling Delete		6 Images
		Vid	

- 10. On the **Experience Database** page, click 💟 on the **Arming Alarm** column to configure arming alarm and similarity.
- <u>Step 8</u> Enable **Self-learning**, and then select the predefined experience database from **Linked Experience Database** drop-down list.
- Step 9 Enable Privacy Protection.

After it is enabled, the person detected will be blurred by mosaic.

Step 10 Click Apply.

## **Related Operations**

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

## **Background Information**

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

 $\square$ 

Some models only support some of the functions listed below.



Table 8-7 Description of IVS fu	nctions
---------------------------------	---------

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.		
		Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.	
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.	<ul> <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>	
		Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.	
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.	<ul> <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>	
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.	



Rule	Description	Applicable Scene
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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to **IVS** to enable IVS of the corresponding channel, and then click **Next**.
- Step 3 Click the **Rule Config** tab.
- <u>Step 4</u> 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 8-28 Tripwire

e Config Global Config				
Add Rule				
No.	Name	Туре	On	Delete
1	IVS-1	Tripwire		÷
	4+ Sensitiv	ty 1 2 3 4 5 6 7	8 9 10	
	BB Directio	Both		
The seal	Target F			
	Effective		Asimal	
AND A	A CONTRACTOR OF CONTRACTOR	Target 🛛 Pluman 🗹 Wotor Venicie	Animai	
	Time Pla	n Full Time	✓ Add Schedule	
	+Eve	nt Linkage		
	Dura	Enabled		
	Recor	LINURU	â	
	Snaps	not Enabled	â	

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	• During the detection of abandoned object, the alarm is also
Missing object	<ul> <li>triggered if pedestrian or vehicle stays for a long time. If the</li> <li>abandoned object is smaller than pedestrian and vehicle, set the</li> </ul>
Fast moving	target size to filter pedestrian and vehicle or properly extend the
Parking detection	<ul> <li>duration to avoid false alarm triggered by transient staying of pedestrian.</li> </ul>
Crowd gathering	<ul> <li>During the detection of crowd gathering, false alarm might be</li> </ul>
Loitering detection	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.

<u>Step 6</u> (Optional) Click other icons at the right side of the image to filter targets in the image.

- Click min 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.
- <u>Step 7</u> Set rule parameters for IVS.

### Table 8-9 Description of IVS parameters

Parameter	Description
Direction	<ul> <li>Set the direction of rule detection.</li> <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 <b>Appears</b> , <b>Cross</b> or <b>Inside</b> .



ription
n <b>Target Filter</b> is enabled, the system only detects the selected tive targets, and only the selected targets can trigger the alarm
<b>arget Filter</b> are only available under tripwire, intrusion, and fast oving rules. <b>uman</b> and <b>Motor Vehicle</b> are selected by default. urrently, the algorithm primarily supports the detection of cats and dogs in the animal category. Although it can also attempt to etect other four-legged animals, the accuracy of such detections annot be guaranteed.
or abandoned object, the duration is the shortest time for iggering an alarm after an object is abandoned. or missing object, the duration is the shortest time for triggering n alarm after an object is missing. or parking detection, crowd gathering, or loitering detection, the uration is the shortest time for triggering an alarm after an object opears in the area.
n the sensitivity is high, detection becomes easier, but the per of false detections increases. ing Object , Abandoned Object and Loitering Detection do not
0

<u>Step 8</u> 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".

# **Related Operations**

For Triple-Sight Perimeter Protection Bullet WizMind Network Camera, only the panorama channel supports IVS, and it only supports tripwire and intrusion.



Figure 8-29 Configure IVS for the panorama channel

No.	Name	т	ype	On		Delete
51	IVS-1	Tri	pwire			â
		Sensitivity	1 2 3 4 5 6 Both			
	<b>C</b>	Time Plan +Event Linkage Snapshot Enabled	Full Time	Add Schedule	ŧ	
Please adjust the rule line in full- accuracy of the rule line.	screen mode to improve th Distant View	Channel	1(Panorama)			
		Back Apply	Refresh Default			

- After you configure the rules for the panorama channel, you can click Medium View and Distant View below the image to view the medium view and distant view.
- On the image of medium view or distant view, you can drag the rules as a whole or drag the nodes on the rules within the current image to adjust the rules, and then click **Apply** to save the configurations to the panorama channel.
- You can click to display the image in full screen.

# 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

<u>Step 1</u> Select **AI** > **Smart Plan**.



- <u>Step 2</u> Click Onext to Smart Object Detection , and then click Next.
- <u>Step 3</u> Click the **Global Config** tab.
- <u>Step 4</u> 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

<u>Step 1</u>	Select AI > Smart Plan.
<u>Step 2</u>	Click 🔍 next to <b>Smart Object Detection</b> , and then click <b>Next</b> .
<u>Step 3</u>	Click the <b>Rule Config</b> tab.
<u>Step 4</u>	Click <b>Add Rule</b> on the <b>Rule Config</b> page Here we use <b>Smart Abandoned Object</b> as an example.
	Devide a state of the second state of the seco

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

Rule	Description	Applicable Scene
Smart 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.	<ul> <li>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</li> <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>
Smart 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.	<ul> <li>Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended.</li> <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 8-30 Smart abandoned object

Rule Config Global Config				
Add Rule				
No.	Name	Туре	On	Delete
1	OM-1	Smart Abandoned Object		亩
			å	

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

<u>Step 6</u> (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.

<u>Step 7</u> 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> <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>			

<u>Step 8</u> 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

<u>Step 1</u> Select **AI** > **Smart Plan**.

- <u>Step 2</u> Click Onext to **Vehicle Density**, and then click **Next**.
- Step 3 Click Add Rule to select rules.

Figure 8-31 Add rules

Add Rule				
No.	Name	Туре	On	Delete
1	VD-1	Traffic Congestion		亩
2	VD-2	Parking Upper Limit		亩

<u>Step 4</u> (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 8-32 Vehicle density (traffic congestion)

Add Rule						
No.	Name			Туре	On	Delete
1	VD-1		Tr	affic Congestion		亩
2	VD-2		Par	rking Upper Limit		â
			Repeat Alarm Time	0	sec (0-300)	
			Vehicle Congestion Alarm			
	3527 - CRY 8 152 - 45	亩	Threshold	10	vehicles(10-1000)	
The States	en la		Duration	1	min (1-100)	
A CONTRACTOR						
Carlor A	950-301- 004 100		Time Plan	Full Time v	Add Schedule	
IPC 2			+Event Linkage			
			Snapshot Enabled		亩	
			Back Apply	Refresh Default		



### Figure 8-33 Vehicle density (parking upper limit)

Add Rule						
No.	Name		Туре		On	
1	VD-1		Traffic Congestion			
2	VD-2		Parking Upper Limit			
	Lar Ors Lore	Repeat Alarm Time Upper Limit Vehici Threshold Time Plan +Event Linkage	20 Full Time	vehicles(10-1000) vehicles(10-1000) vehicles(10-1000)		
120		Snapshot Enat			à	

<u>Step 5</u> Set 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.
	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.
	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.

<u>Step 6</u> 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to Parking Space Management , and then click Next.
- <u>Step 3</u> Select the mode.
  - 12 parking spaces: Only supports parking space detection.
  - 6 parking spaces: Supports both ANPR and parking space detection.

	_	-	-
n		r	n
		L	-11
	_		

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.

 $\square$ 

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.

2021	-10-20 09-53:50	Mode Auto Drawing		(ANPR support for 6 spaces.)	Draw	
1.2.1		No.	Name	Туре	On	Delete
150		1	P1	Parking		ā
			P2	Parking		Ť.

Figure 8-34 Parking space

<sup>&</sup>lt;u>Step 5</u> Configure the parameters.



Fiaure 8-35	Parking space	parameters

Parking Space Avail	Green Light V	
Parking Lot Full	Red Light 🗸	
arget Box Overlay		
Picture Overlay		
ensitivity	- + 50	
ime Plan	Full Time     V     Add Schedu	le
+Event Linkage		
Snapshot   Enabled		亩

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

Parameter	Description
Parking Space Status	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.
Target Box Overlay	Overlay the target box on the captured pictures to mark the change of parking space. It is enabled by default. Click <b>Picture Overlay</b> 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.

<u>Step 6</u> 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

<u>Step 1</u> Select **AI** > **Smart Plan**.

- <u>Step 2</u> Click Onext to **Parking Space**, and then click **Next**.
- Step 3 Click the **Rule Config** tab.
- <u>Step 4</u> (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.

Rule Config	Global Config				
Rule Config	Global Config	Parking Space List P1 + Add	Enable Name Type Direction Planned P	P1 Planned Vertical V	
			Start No.	1	(1~100)
			End No.	4	
			Actual Pa	1	(1~4)
			Alarm T	. ≥ ∨ 1	(0-100)

### Figure 8-36 Rule configuration (1)

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



## Figure 8-37 Rule configuration (2)

Rule Config Global Config					
		Parking Space List			
2021-06-23 01:54:22		P1	Enable		
		+ Add	Name	P1	
	min		Туре	Open v	
	max max		Actual Pa	1	(1~100)
/按:首			Alarm T	. ≥ × 1	(0-100)
			Sensitivity	<b>1 2 3 4 5 6</b> 7 8 9 1	
			Report	30	sec(5-3600)

- Click to draw a parking space detection area in the image. The detection area is the whole image by default.
- Click T 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.

### <u>Step 5</u> 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 8-38 Planned parking space

Rule Config Global Config				
κu.	Parking Space List			
Vehicles A Available 7	P1	Enable		
Available B	+ Add	Name	P1	
		Туре	Planned V	
		Direction	Vertical $\vee$	
		Planned Parki	1	(1~50)
		Start No.	1	(1~100)
		End No.	1	
		Actual Parkin	1	(1~1)
		Alarm Thre	2 v 1	(0-100)
		Sensitivity		
			1 2 3 4 5 6 7 8 9 1	0
		Report Peri	30	sec(5-3600)
		Time Plan	Full Time V	Add Schedule
		+Event Linkag	je	

## 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 <b>Planned Parking Space</b> .
Actual Parking Space	It ranges from 1 to the configured value of planned parking space. <b>Actual Parking Space</b> 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.
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.

Rule Config Global Config			
τ.	Parking Space List		
Vehicles Analable 7	P1	Enable	
Available 7	P2	Name P2	
	+ Add	Type Open v	
		Actual Pa 1 (1~100)	
		☐ Alarm T ≥ ∨ 1 (0-100)	
		Sensitivity 1 2 3 4 5 6 7 8 9 10 Report 30 sec(5-3600)	
		Time Plan Full Time v Add Schedule +Event Linkage	
	Back Apply	Refresh Default	

#### Figure 8-39 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 Spaces	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.

<u>Step 6</u> 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to Parking Space or Parking Space, and then click Next.
- Step 3 Click the **Global Config** tab.
- <u>Step 4</u> (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".

<u>Step 5</u> Adjust confidence level.

 $\square$ 

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

Step 6 Click Apply.

# 8.8 Setting Video Metadata

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 metadata, including face parameter and scene parameter.

## Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click next to **Video Metadata** to enable video metadata of the corresponding channel, and then click **Next**.
- <u>Step 3</u> Click the **Global Config** tab.
- <u>Step 4</u> Set parameters.

Pages and functions might vary on different devices. Please refer to the actual device for detailed information.



Rule Config	Global Config					
			Target Box Overlay			
Motor Vehicle C	-2 / 2 / 500	94834 Mu =	🗹 Face 🗹 Human 🗹 I	Non-Motor Vehicle 🗹 Motor Vehicle		
			Track Overlay			
			🗹 Human 🔽 Non-Moto	r Vehicle 🔽 Motor Vehicle		
		Contraction of the second	Tripwire Counting			
			Face Enhancement			
Farany Husik 800	are entr		Remove Duplicate Faces		¢	
			Face Cutout	One-inch Photo		
			Picture Mode	Number Plate Priority		
			Face Beautifying			
			Level		+ 50	
			Face Exposure			
			Face Target Brightness		+ 50	
			Face Exposure Interval Dete	c –	+ 5 sec	
			Privacy Protection			
			Target	● Face ◯ Human		
			Back Apply	Refresh Default		

Figure 8-40 Global configuration of video metadata (1)



Rule Config	Global Config		
Channel	1(Details)	v	
		Target Box Overlay	
	2028-12-11 1	120/21 💼 🔽 Face 🔽 Human 🗹 Non-Motor Vehicle 🔽 Motor Vehicle	
2		Track Overlay	
		V Human V Non-Motor Vehicle V Motor Vehicle	
		Remove Duplicate Faces	0
IPC		Face Cutout One-Inch Photo	
		Face Snapshot Enhancement Auto V	
		Face Exposure	
		Face Target Brightness – +	50
		Face Exposure Interval Det • • +	5 sec
		Back Apply Refresh Default	



Parameter	Description
	Overlay target box on the captured pictures to mark the target position.
Target Box Overlay	4 types of target boxes are supported. Select the target box as needed.
	The captured pictures are stored in SD card or the configured storage path. For details, see "6.1 Local".
	Enable this function, and set the tripwire direction. The snapshot
Tripwire Counting	mode is <b>Tripwire</b> by default, and you cannot change it. $\Leftrightarrow$ will be displayed beside the image on the <b>Rule Config</b> page. You can draw the rule as needed.
Face Enhancement	Click <b>C</b> to enable face enhancement. Priority should be given to ensuring facial clarity when the bitstream is relatively low.
	During the configured period, the face that detected several times is displayed only once, to avoid repeated counting. Click
Remove Duplicate Faces	• to set the parameters, and then click <b>Apply</b> .
	<ul> <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	Set a range for matting face image, including face picture and one-inch picture.
Picture Mode	Set picture mode as Number Plate Priority or Face Priority.
Face Beautifying	Enable <b>Face Beautifying</b> 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.
	Select the mode to enhance the snapshot.
Face Snapshot Enhancement	<ul> <li>Auto: The system automatically improves the quality of the snapshot.</li> <li>Manual: You can adjust NR Level , Sharpening Level, Brightness Level and Redness Level manually.</li> <li>Off: Turn off the function.</li> </ul>
Face Exposure	Enable <b>Face Exposure</b> to make face clearer by adjusting lens aperture and shutter.
Face Target 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.

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

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 AI > Smart Plan, and enable Video Metadata.
- You have configured the parameters on the **Global Config** page.

## Procedure

<u>Step 1</u>	Select AI	> Smart Plan.
---------------	-----------	---------------

- <u>Step 2</u> Click Onext to Video Metadata , and then click Next.
- Step 3 Click the **Rule Config** tab.
- <u>Step 4</u> Click **Add Rule** 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.

#### Figure 8-42 Rule configure (video metadata)

Add Rule					
No.	Name	Туре	On	Picture	Delete
1	VM-1	People Detection		0	亩
2	VM-2	Non-motor Vehicle Detection		٥	ά.
3	VM-3	Motor Vehicle Detection		٥	亩

### <u>Step 5</u> 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.

- a. Select the type of overlay that needs to be captured. You can adjust the position of the information displayed.
- b. Select the overlay images upload type(s).
- c. **Display Video OSD** is enabled by default. Disable this function, and then the overlay information configured in "6.2.2.2 Overlay" will not be displayed in the image.



icture	Х
Vehicle     Color     Number of       Non-Maser Vehicle     100     100       Display Video     Elack Edge Loc     Above	Picture Overlay            • Drag attributes on the left for sequencing.             • Vehicle Type         • Color             • Vehicle Type         • Color             • Number of         • Top             • Passengers             • Top Color             • Hat             • Custon 1
OSD Separator Blank v	Upload Picture
Black Edge Hei 8 (4-32)×8Pixel	<ul> <li>✓ Panoramic Image</li> <li>✓ Vehicle Body Picture</li> <li>✓ Face</li> </ul>
	Apply Default Cancel

#### 3. Click Apply.

<u>Step 6</u> (Optional) Click the icons at the right side of the image to filter targets in the image.

• Click  $\Leftrightarrow$  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 its size, 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.
- <u>Step 7</u> Set parameters.

Table 8-17 Description of crowd map parameters

Parameter	Description
People Flow Statistics	Click <b>O</b> next to <b>People Flow Statistics</b> to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click Onext to <b>Flow Statistics (Non-motor Vehicle)</b> to count the number of non-motor vehicles in the detection area.



Parameter	Description
Traffic Flow Stat	Click next to <b>Traffic Flow Statistics</b> to count the number of motor vehicles in the detection area.
OSD	Click <b>OSD Info</b> , and the <b>Overlay</b> page is displayed. Click <b>OD</b> next to <b>Enable</b> to enable the target statistics function. For details, see "6.2.2.2.8 Configuring Target Statistics".
Snapshot Mode	<ul> <li>Optimized: Capture the pictures until the vehicle disappears from the image, and report the clearest picture.</li> <li>Tripwire: Capture the pictures when the vehicle triggers tripwire as the configured direction.</li> </ul>
	<ol> <li>Select Tripwire.</li> <li>Select the direction from A to B , B to A, and Both.</li> <li>Adjust the position of rule line as needed.</li> </ol>

<u>Step 8</u> 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 Metadata Report

Generate data of video metadata recognition in report form.

Procedure

- <u>Step 1</u> Select **Report** > **Report** > **Video Metadata**.
- <u>Step 2</u> Select the report type, start time, end time, and other parameters.
- <u>Step 3</u> Click **Search** to complete the report.

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

- <u>Step 1</u> Select AI > Smart Plan.
- <u>Step 2</u> Click Onext to **People Counting**, and then click **Next**.
- <u>Step 3</u> Click the **People Counting** tab.
- <u>Step 4</u> 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.

Smart Plan— Rule Config— 21 People Counting				
People Counting	Queuing Abnormal Event Detection	Global Config		
Add Rule				
No.	Name	Туре	On	Delete
1	NumberStat1	People Counting		亩
2	PC-1	Area People Counting		亩

#### Figure 8-44 Add rule

<u>Step 5</u> 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.
  - 2. Click  $\Leftrightarrow$  to draw rule line in the image.

When targets enter or leave the detection area along the direction line, they will be counted.



Figure	8-45	People	counting

NumberStat1, Enter, 867 Exit. 275 Pass 160, 2023-12-13 17:10:14	Auto Reset	Everyday V	00:00 (5)
NumberStart I. Effer (957 px): 275 Pass 190 2023-12-13 17: 1014	People Counting Alarm	0	Human
IPC	Exit No. Stay No.	0	Human
Please draw a direction line across the rule area.	Pass No.	0	Human
Prease draw a direction line across the rule area. Diagram	Time Plan +Event Linkage	Full Time 🗸	Add Schedule
B	Snapshot   Enabled Back Apply R	Default	â

• Area people counting

Click Click click click click click click and control of the box to adjust its size, press the right mouse button, and then move the box to adjust the position.

Figure 8-46	Area peop	le counting
-------------	-----------	-------------

	Area People Counting Alarm		
NumberStaff, Enter, 967 Exit, 275 Pass, 160 2023-12-13 17:14:39	Inside No.	2	Human(0~80)
	Туре	≥Threshold ∨	
	Min Duration	30	sec(1~3600)
	Repeat Alarm Time	0	sec(0~300)
IPC	Stay Alarm		
	Min Duration	2	sec(1~1800)
Please draw a direction line across the rule area.	Repeat Alarm Time	0	sec(0~300)
Diagram	Time Plan +Event Linkage	Full Time $\lor$	Add Schedule
B	Snapshot Enabled	lefresh Default	â
D	back Apply	Delaut	

<u>Step 6</u> 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 <b>Enter No.</b> and <b>Exit</b> <b>No.</b> . 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.
	Inside No.	Set the number of people in the people counting
	Туре	region. When the people count reaches the configured value, an alarm will be triggered.
	Stay Alarm	Select the <b>Stay Alarm</b> checkbox to enable this function.
Area people counting	Min Duration	When the stay duration exceeds the configured value, an alarm is triggered.
counting	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.

<u>Step 7</u> 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".

## Results

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 8-47 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 AI	> Smart Plan.
------------------	---------------

- <u>Step 2</u> Click Onext to **People Counting**, and then click **Next**.
- <u>Step 3</u> Click the **Queuing** tab.
- <u>Step 4</u> 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	8-48	Add	rule
--------	------	-----	------

Smart Plan— 🔗 R	tule Config—21 Peop	ble Counting			
eople Counting	Queuing	Abnormal Event Detection	Global Config		
Add Rule					
No.		Name	Туре	On	Delet
1		QUE-1	Queuing		亩

<u>Step 5</u> Draw a detection area in the image.

Click 🔽 to draw the detection area, and press the right mouse button to complete the drawing.



### Figure 8-49 Queuing

	Queue People No. Alarm Queue People No. Type	2 ≥Threshold ∨	Human(0~80)
statement to charge and	Queue Time Alarm Queue Time	2	sec(1~1800)
	Time Plan +Event Linkage	Full Time $\lor$	Add Schedule
	Snapshot   Enabled Back Apply	Refresh Default	亩

<u>Step 6</u> Set parameters.

### Table 8-19 Description of queuing

Parameter	Description				
Queue People No. Alarm	Enable the queue people No. alarm function				
Queue People No.	Enable the queue people No. alarm function.				
Туре	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.				

<u>Step 7</u> 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".

## Results

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 8-50 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

<u>Step 1</u> Select **AI** > **Smart Plan**.

- <u>Step 2</u> Click Onext to **People Counting** , and then click **Next**.
- <u>Step 3</u> Click the **Abnormal Event Detection** tab.
- <u>Step 4</u> Click Add Rule > Crow 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 8-51 Add rule

	Rule Config—21 People Counting			
ople Counting	Queuing Abnormal Event De	etection Global Config		
Add Rule				
Add Rule				
No.	Name	Туре	On	Dele
	Name AD-1	Type Crowd Detection	On	Dele

<u>Step 5</u> 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 8-52 Abnormal event detection

1	Alarm Type	Self-adaptive V		
<b></b>	Sensitivity	1 2 3 4 5 6 7 8 9		. S
	Min Duration	30	sec (1-3600)	5
	Repeat Alarm Time	0	sec (0-300)	
	Time Plan	Full Time	Add Schedule	
	+Event Linkage			
1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -	Snapshot   Enabled		â	
	Back Apply	Refresh Default		

<u>Step 6</u> Set parameters.

Parameter	Description			
	You can select from Self-adaptive and Custom.			
Alarm Type	<ul> <li>Self-adaptive: The system calculates the number of people and the area of detection region to determine whether the alarm is triggered.</li> <li>Custom: 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.			
	When the alarm is triggered and this state lasts for repetitive alarm time, the alarm will be triggered again.			
Repeat Alarm Time				
	0 means repeat alarm function disabled.			
	When the alarm type is <b>Custom</b> , click <b>Add</b> to add crowd level. When the number exceed the configured value, an alarm will be triggered.			
Crowd Level				
	<ul> <li>The number of people in the crowd level added later must be larger than the number added before.</li> <li>When deleting the crowd level, delete it from the highest level.</li> </ul>			

### Table 8-20 Description of abnormal event detection

<u>Step 7</u> 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".



# 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to **People Counting**, and then click **Next**.
- <u>Step 3</u> Click the **Global Config** tab.

Figure 8-53 Global config

eople Counting	Queuing	Abnormal Eve	ent Detection	Global Config				
			Calibration Config					
		11		on Ground" to mark the rectan et the installation value.	gular calibrati	on area on t	he image, and then click "OK"	to
	-+-+		Calibration Ground	d Clear				
		图和出	Installation Height		+	300	cm (200 - 750)	
			Installation Angle	-	+	90	° (0 - 90)	
	1 Landa			ОК				
			Alatau de Celé e desetiu					
			Altitude Self-adaptive					
			Other Config					
			Sensitivity	1 2 3 4 5 6 7	8 9 10			
			Intelligence Info Ov	Stream Overlay	$\vee$			
			Max Detection Heigh	t 220	cn	n (0 - 300)		
			Min Detection Heigh	t 50		n (0 - 200)		

<u>Step 4</u> 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.

 $\square$ 

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 calculates the installation height and angle.
- <u>Step 5</u> Enable **Altitude self-adaptive**.


#### <u>Step 6</u> Set the sensitivity.

When the sensitivity is high, detection becomes easier, but the number of false detections increases.

- <u>Step 7</u> Set the intelligence info overlay.
  - Stream overlay: Overlay the information on the stream.

 $\square$ 

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".
- <u>Step 8</u> 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.

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to Face & Body Detection to enable face & body detection of the corresponding channel, and then click **Next**.
- <u>Step 3</u> Click the **Global Config** tab.
- <u>Step 4</u> Set parameters.



Rule Config	Global Config				
		<del>(</del>	Target Box Overlay		
-		-	Face & Body Image Enhan		
-		=	Face Cutout	One-inch Photo	
<u> </u>		1 <u>.</u>	Detection Priority	Face First	
		1	Snapshot Mode	Optimized	
			Property		
			Advanced		
			Snapshot Angle Filter	0	+ 90
			Snapshot Sensitivity		+ 80
			Quality Threshold	-	+ 70
			Optimized Duration	10	sec (1-300)
			Face Exposure		
			Target Face Brightness	-	+ 50
			Face Exposure Interval Det	L- C	+ 5 sec
			Back Apply	Refresh Default	

Figure 8-54 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 O 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> <li>Real-time : Capture the image when the camera detects a face.</li> <li>Optimized : Capture the clearest image within the configured time after the camera detects face.</li> <li>Quality Priority : After detecting the face image quality is higher than the quality threshold, the camera captures the image.</li> <li>Tripwire : This snapshot is available in PPE Detection Mode.</li> <li>Click Advanced to set the optimized time and quality threshold.</li> </ul>		
Property	Click O next to <b>Property</b> to enable the properties display.		



Parameter	Description		
Advanced	<ul> <li>Snapshot Angle Filter : Set snapshot angle to be filtered during the face detection.</li> <li>Snapshot Sensitivity : Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity.</li> <li>Optimized Duration : Set a period to capture the clearest picture after the camera detects face.</li> </ul>		
Face Exposure	Click <b>O</b> next to <b>Face Exposure</b> 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 AI > Smart Plan, and enable Face & Body Detection.
- You have configured the parameters on the **Global Config** page.

#### Procedure

<u>Step 1</u> Select **AI** > **Smart Plan**.

<u>Step 2</u> Click Omega next to Face & Body Detection , and then click Next.

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

Figure 8-55 Rule configuration

Rule Config	Global Config				
		Q	Enable	OSD Info	
		Ę.	Detection Setting		
		← <sup>↔</sup>	Detection Mode	General Mode OPPE De	etection Mode
	W. K. L		Detection Type	🕑 Face Detection 🕑 Huma	n Detection
			Time Plan	Full Time $\vee$	Add Schedule
		â	+Event Linkage		
			Snapshot   Enabled		亩
			Back Apply	Refresh Default	

- <u>Step 4</u> Click One next to **Enable** to enable the face detection function.
- <u>Step 5</u> (Optional) Click other icons at the right side of the image to draw detection area, exclusion area, and filter targets in the image.



- Click Let to draw a face detection area in the image, and right-click to finish the drawing.
- Click <sup>III</sup> to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click <sup>(+)</sup> to draw rule line in the image.
- Click is to draw the minimum size of the target, and click is 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.

<u>Step 6</u> (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".

- <u>Step 7</u> 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 **Al Attributes**.
    - 2. Select AI attributes that you want to detect.

The AI 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.
- <u>Step 8</u> 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to **PPE Detection**, and then click **Next**.
- Step 3 Click the **Rule Config** tab.
- <u>Step 4</u> Click **Add Rule**, and then select **PPE Detection**.

Currently only one rule can be added.

<u>Step 5</u> Draw the detection area.

Click  $\square$ , 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.

<u>Step 6</u> Configure the detection parameters.

Figure 8-56 PPE detection

<b>u</b>	Alarm Trigger Condition	O Match Attributes Alarm	<ul> <li>Mismatch Attribut</li> </ul>	tes Alarm	
	Min Duration	3		sec (1-60)	
	Repeat Alarm Time	0		sec (0-60)	
and the second se	Attributes for Matching				
	Workwear 💽	Detection Mode	Detect by Attribute	V	
	Hat 💽	Detection Range	🕞 Full Body 💿 Upper	Body	
	Face Mask	Color	Select All		
	Apron		🗸 Red 🔽 Blue	🗸 Dar 🗸 Yell 🔽 White 🔽 Black	
	Gloves 💽		🗸 Gray 🔽 Green	🗸 Pur 🗹 Pink 🔽 Bro	
	Shoe Covers				
	Boots				
	Seatbelt				
	Safety Vest				
	Time Plan	Full Time	~	Add Schedule	
	+Event Linkage				
	Snapshot Enabled			â	
	Back Apply Refre	sh Default			

Parameter	Description			
Alarm Trigger Condition	<ul> <li>Match Attributes Alarm : When the detected object matches all of the configured attributes, the system triggers alarm.</li> <li>Mismatch Attributes Alarm : When the detected object does not match the configured attributes, the system triggers alarm.</li> </ul>			
	Each detected attribute which does not match the configured attributes will trigger a new alarm.			
Min Duration	The minimum duration between the detected object appears and trigger the alarm.			



Parameter	Description		
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 .		

Attribute	Description				
	Select the detection mode.				
	• <b>Registration Mode</b> : Detect the attribute <b>Yes</b> or <b>No</b> , and this mode can be used when the clothes of upper body and lower body are in different color.				
Workwear	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".				
	Up to 5 arming databases can be added to the same rule.				
	Detect by Attribute :				
	<ol> <li>Select the detection range from Full Body and Upper Body.</li> <li>Select the color.</li> </ol>				
	1. Select the detection attribute: <b>Yes</b> or <b>No</b> .				
Hat	2. Select the detection range: Safety helmet or cap. If you choose safety helmet, select the color.				
Face Mask					
Apron					
Gloves					
Shoe Covers	Select the detection attribute: <b>Yes</b> or <b>No</b> .				
Boots					
Seatbelt					
Safety Vest					

<u>Step 7</u> 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Onext to **PPE Detection**, and then click **Next**.
- Step 3 Click the **Global Config** tab.
- <u>Step 4</u> 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

- <u>Step 1</u> Select AI > Smart Plan > PPE Detection.
- <u>Step 2</u> Click the **Rule Config** tag.
- <u>Step 3</u> Select Workwear > Registration Mode > Arming Database.

Figure 8-57 Arming database

$\odot$	Smart Plan	PPE Detection			
	Rule Config Global Config				
	Add Rule				
	No.	Name		Rule Type	On
	1	IVS-1s		PPE Detection	
		12		Match Attributes Alarm      Mismatch Att	rributes Alarm
			Min Duration	3	sec (1-60)
			Repeat Alarm Time	0	sec (0-60)
			Attributes for Matching		-0
			Workwear	Detection Mode Registration Mod	
	LARSE AND		Hat	Linked Workwear Da	
			Face Mask	Detect for Attributes 💿 Yes 🔿 No	
			Apron		

<u>Step 4</u> Click **Add** on the **Arming Database** page.

Up to 5 arming databases can be added.

- <u>Step 5</u> Create the name of database, and then select the optional plan. You can select to detect full body or half body.
- <u>Step 6</u> 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 8-58 Search the modeling status

- L	All					
		Search Import	Batch Import Modelin	g Modeling All Delet	e	
All IA	All					
Constanting of the second	Invalid Valid	Value	Vid	Vela Vela	Veli	Vid

<u>Step 7</u> 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 8-59 Arming alarm

Add Refr	esh		Arming Alarm			×	Free	Space •	
No.	Name	Optimal Plan	Name	test_yellow		atus	Arming Alarm	Details	Delete
	test_yellow	Full Body	Arm			ted	Ū		â
2	test_blue	Half Body				ted	₪		û
3		Full Body	Similarity	-	+ 80	ected	J		â
			Optimal Plan	Full Body					
					OK Can	cel			

<u>Step 9</u> 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

<u>Step 1</u> Select **AI** > **Smart Plan**.

- <u>Step 2</u> Click Omega next to **Heat Map** , and then click **Next**.
- <u>Step 3</u> Select the **Enable** check box, and then the heat map function is enabled.



#### Figure 8-60 Heat map

Smart Plan Rule Config 21 Heat Map			
2021-05-18 17:27:37	Enable		
	Time Plan	Full Time	✓ Add Schedule
	Back Apply	Refresh Default	
IPC			

<u>Step 4</u> 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 in to clear the existing detection area or exclusion area.
- <u>Step 5</u> 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click **O** next to **ANPR**, and then click **Next**.
- <u>Step 3</u> Click the Lane Config tab.
- <u>Step 4</u> Click  $\square$  and draw the detection area.

Press the left mouse button to draw the detection area, and press the right mouse button to finish.

- <u>Step 5</u> 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.

<u>Step 6</u> Select the lane direction.

- Vehicle Head : The driving direction of the vehicle in the lane is from top to bottom  $\downarrow$  .
- Vehicle Tail : The driving direction of the vehicle in the lane is from bottom to top † .



#### Figure 8-61 ANPR

Smart Plan—	Rule Config 21	ANPR					
Lane Config	Rule Config	Picture	Alle	owlist	Blocklist		
Lane: 187 Lane: 2 1970: 2 1980: 7 1980: 7		10 22 33 10 22 35 10 20 10 10 20 10 10 20 10 10 20 10 10 10 10 10 10 10 10 10 10 10	i ☐	Lane List Lane1 Lane2	Enable Lane No. Lane Direction	1 Vehicle Hea O Vehicle Tail	
				Advanced			•
🕒 Lane L 💼	• Detec 💼			Traffic Flo	ow Statistics	D	OSD Info
				Back	Apply Refresh	Default	

<u>Step 7</u> 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.
- <u>Step 8</u> (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 Onext 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 "6.2.2.9 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.

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click **O** next to **ANPR**, and then click **Next**.
- Step 3 Click the **Rule Config** tab.
- <u>Step 4</u> Click lane line to select the line that you configured. If no line is configured, click **Add** Lane Line.



Figure 8-62 Rule configuration (1)

🔗 Sma	rt Plan——	Rule Config—2.1 ANI	PR			
Lane (	Config	Rule Config	Picture	Allowlist	Blocklist	
Lan	e Line			~		
						Please draw lane line.
						Add Lane Line

Figure 8-63 Rule configuration (2)

Time Plan	Full Time	Add Schedule	
+Event Linkage			
Record Enabled			Ê
Post-Record	15	sec (10-300)	
Snapshot   Enabled			â
Alarm-out Port   Enabled			ò
Alarm Channel	1 2		
Post-alarm	300	sec (10-300)	
Audio Linkage   Enabled			ò
Play Count	1	(1-10)	
File	You are under surveillance.wav		
Back Apply Ref	fresh Default		

<u>Step 5</u> 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.

<u>Step 6</u> Set related alarm linkage.

- <u>Step 7</u> Set audio linkage. For more information, see "6.2.4.2 Setting Alarm Tone".
  - Set play count period.
  - Select the file needed.

<u>Step 8</u> (Optical) Click in 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

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Omega next to **ANPR**, and then click **Next**.
- <u>Step 3</u> Click the **Picture** tab.
- <u>Step 4</u> Click + **OSD Option** to select the type of overlay information that needs to capture. You can adjust the position of the information displayed.



Figure 8-64 Picture

<u>Step 5</u> 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

<u>Step 1</u> Select **AI** > **Smart Plan** > **Allowlist**.

<u>Step 2</u> Click Onext to **Enable** to enable the allowlist function.

Figure 8-65 Enable allowlist



#### <u>Step 3</u> Add allowlist.

- Add allowlist one by one.
  - 1. Click **Add**.
  - 2. Set plate information.

#### Figure 8-66 Add allowlist plate

Add			×
* Plate			
Start Time	2021-06-17 00:00:00	Ë	
End Time	2021-06-18 23:59:59	Ë	
* Owner			
Add Contin	uously		
		Cancel	ок



#### 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.
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 8-67 Encryption settings (1)

Export	x
Encryption	
Please keep unencrypted files well to avoid data leakage.	
Cancel	
Cancel	

4. Add the license plate information according to the sample of the exported file, and then save the table.

#### Figure 8-68 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.
  - $\diamond$   $\;$  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  $\bigcirc$  and then click  $\checkmark$  . The search result is as below:



#### Figure 8-69 Search allowlist

Lane Config	Rule Config	Picture	Allowlist	Blocklist				
Enable								
Add	Import Export Do	ownload Template	Clear		Free Space	99.84%	A0000	Q
No.	Start	Time		End Time	Owner Name	Plate No.	Edit	Delete
1	2021-06-1	8 00:00:00		2021-06-19 23:59:59	А	A0000	12	ά

### $\square$

If you do not enter anything, it will show all the allowlist plate numbers added.

• Edit allowlist information.

Click <sup>III</sup> 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 computer.

• Export the file in .csv format if not encrypted, and you can edit the file.

Figure 8-70 Encryption settings (2)

Export	X
Encryption	
Please keep unencrypted files well to avoid data leakage.	
Cancel	

• Export the file in .backup format if encrypted, and you cannot edit the file.



Figure 8-71 Encryption settings (3)

Export	Х
Encryption  * Encryp	
Password must be 8 to 32 characters, including at least two the following categories: numbers, uppercase letters, lowerc letters and special characters ( Characters like ' " ; : & cannot included in ).	ase
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** 

 $\square$ 

Linkage Track is not enabled by default. Please enable it when necessary.

### Procedure

<u>Step 1</u> Select **AI** > **Panoramic Linkage** > **Linkage Track**.

<u>Step 2</u> Click **D** next to **Enable** to enable **Linkage Track**.



Figure 8-72 Linkage track

Linkage Track	Main/Sub Calibration	
Enable		
Auto Tracking		
Tracking Duration	Continue till object disappears $\lor$	
Tracking Target Siz	+ 30	30
Idle Interval	5	sec (1-1800)
Idle Position	Preset1 V	
	OK Refresh Default	

<u>Step 3</u> Configure other parameters.

#### Table 8-25 Parameters of linkage track

Parameters	Description
Tracking Duration	<ul> <li>Continue till object disappears: 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>Custom: 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
Idle Position	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 receivce any tracking command for 5 seconds, it will turn to preset 1 automatically.
	You need to set presets in advance.

Step 4 Click **OK**.

# 8.14.2 Configuring Calibration Parameter

### **Background Information**

Auto calibration mode is available on select models.

- <u>Step 1</u> Select **AI** > **Panoramic Linkage** > **Main/Sub Calibration**.
- <u>Step 2</u> Configure calibration parameters.



Auto calibration

Select Auto in Type, and then click Start Calibration.

Figure 8-73 Auto calibration



Manual calibration

Select **Manual** in **Type**, select the scene, and then add calibration point for it in the live image.

 $\square$ 

Web pages might vary with different models.

Figure 8-74 Manual calibration

	Panoramic Ca	amera			Detail C	mera			
001kbps 40			@ 5957kbps 2560	* 1440			0		
							D		
pe	Manual	•				ę,		HEN	
pe ene Add	Manual 2 Clear	>				~~			ý.
ene	2	V V	Central Point	ок	Delete				Ş.
Add	2 Clear		Central Point 1594.400.1	ок	Delete				Ş.
Add No.	2 Clear Panoramic Camera							100	Ŷ.
Add No. 1	2 Clear Panoramic Camera 2539,4551	2393,1690	1594,400,1	10				100	Ų.

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.

### Prerequisites

Make sure that the connected NVR supports AcuPick mode.

#### Procedure

<u>Step 1</u> Select **AI** > **Smart Plan**.

<u>Step 2</u> Click Onext to AcuPick , and then click Next.

Figure 8-75 Enable AcuPick

1 Smart Plan— 🔗 Rule	e Config—— 🔗 IVS—— 🔗	Video Metadata					
CAM 1							
AcuPick	After AcuPick is enable	d, Video Metadata c	annot be used for attri	bute detection.			
Face Detection	Heat Map	IVS	People Counting	Video	Metadata 🗾	Smart Object Detection	
Next Refresh	Default						

<u>Step 3</u> (Optional) Set IVS function as needed, and then click **Next**. For details, see "8.4 Setting IVS".

<u>Step 4</u> Set video metadata function. For details, see "8.8 Setting Video Metadata".

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 8-76 Set video metadata

tule Config Global Co	nfig					
Add Rule						
No.	Name		Туре	On	Picture	De
1	HumanTrait		People Detection		٥	ī
2	NonMotorDetect		Non-motor Vehicle Detection		٥	i
3	VehicleDetect		Motor Vehicle Detection		0	
		Time Plan	Full Time v	Add Schedule		
	<b>1</b>	+Event Linkage			â	
		Alami-out Port   Enable				
finder (NSS)		Post-alarm	10 sec	(10-300)		





## 8.16 Setting Stereo Analysis

By drawing and setting the rules of stereo behavior analysis, the system will perform alarm linkage actions when the video matches the detection rule.

## 8.16.1 Global Configuration

Set global rules for stereo analysis, including calibration configuration, privacy protection, altitude self-adaptive and filter height.

#### Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Omega next to Stereo Analysis , and then click Next.
- Step 3 Click the **Global Config** tab.

Figure 8-77 Global configuration of stereo analysis

Calibration Config       Auto: Draw the calibration area on a flat ground and then click Calibrate.         Manual: Enter the height and angle of camera installation and then click Calibrate.       Manual: Enter the height and angle of camera installation and then click Calibrate.         Auto: Draw the calibration is complete, you can check the effect of the calibration through calibration verification.       Manual: Enter the height and angle of camera installation and then click Calibrate.         Filter Height       Filter Height       Mode       Auto       Manual         Installation Angle       30.8       *(0-90)       Calibration Verification         Calibration Verification       Height Verific       Calibration Verification	Rule Config	Global Config						
Privacy Protection     Calibrate.       Altitude Self-adaptive     After calibration is complete, you can check the effect of the calibration through calibration verification.       Filter Height     Mode <ul> <li>Auto</li> <li>Manual</li> <li>Installation Angle</li> <li>30.8</li> <li>(0-90)</li> </ul>				Calibration Config	1	Auto: Draw the calibrat	ion area on a flat grour	d and then click Calibrate.
Attitude self-adaptive     through calibration verification.       Filter Height     Mode        • Auto     Manual       Installation Height     259     cm(0~1000)       Installation Angle     30.8     *(0~90)		5733-11-23 15:51.02	ā	Privacy Protection	1		nt and angle of camera	installation and then click
Installation Height 259 cm(0~1000) Installation Angle 30.8 *(0~90)				Altitude Self-adaptive				e effect of the calibration
Installation Angle 30.8 *(0-90)	NK Der			Filter Height	1	Mode	Auto O Manual	
	3				1	Installation Height	259	cm(0~1000)
	Ťĸ	No-Yang M				Installation Angle	30.8	°(0~90)
	and the second s					Calibration Verification	Height Verific ∨	Calibration Verification

<u>Step 4</u> Select the mode according to the page instruction.

#### • Auto

1. Click I to draw a calibration area in the image.

	Click 🔲 to delete the calibration area.
2.	Select the calibration verification from Height Verification or Ground
	Verification.
3.	Click Calibrate.
Ma	anual
1.	Enter the installation height and installation angle.
2.	Select the calibration verification from Height Verification or Ground
	Verification.

3. Click **Calibrate.** 

### <u>Step 5</u> (Optional) Configure other information as needed, and then click **Apply**.

- Enable **Privacy Protection** as needed to mosaic the object. You can select to mosaic face or human.
- Enable **Altitude Self-adaptive** to automatically adjust the field of view according to the installation height and angle.



• Enable Filter Height , and then configure the Min Detection Height and Max Detection Height.

## 8.16.2 Rule Configuration

Prerequisites

- Select AI > Smart Plan, and then enable Stereo Analysis.
- Select **AI** > **Smart Plan** > **Global Config** to finish global configuration.

Background Information

Rule	Description
Crossing Warning Line	When the target crosses the warning line from the defined motion direction, an alarm is triggered, and the system performs configured alarm linkages.
Warning Area Intrusion	When the target enters, leaves, or appears in the detection area, an alarm is triggered, and the system performs configured alarm linkages.
Running Detection	When the moving speed of the object in the detection area is faster than the defined threshold, an alarm will be triggered, and the system performs configured alarm linkages.
People Approach Detection	When two people stay in the same detection area longer than the defined duration or when the distance between two people is larger or smaller than the defined threshold, an alarm will be triggered, and the system performs configured alarm linkages.
Fall Detection	When someone falls from a height in the detection area and the duration of the action is greater than the defined threshold, an alarm will be triggered, and the system performs configured alarm linkages.
Violence Detection	When the target in the detection region has large body movements such as smashing and fighting, an alarm will be triggered, and the system performs configured alarm linkages.
Abnormal Number of People Detection	When the system detects an abnormal number of people in the same detection area, an alarm will be triggered, and the system performs configured alarm linkages.
People Stay Detection	When the target stays in the detection area longer than the defined duration, an alarm will be triggered, and the system performs configured alarm linkages.

Table 8-26 Functions description

Here we use **Crossing Warning Line** as an example.

### Procedure

- <u>Step 1</u> Select **AI** > **Smart Plan**.
- <u>Step 2</u> Click Omega next to **Stereo Analysis** , and then click **Next**.
- <u>Step 3</u> Click the **Rule Config** tab.
- <u>Step 4</u> Click **Add Rule** on the **Rule Config** page, and then select **Crossing Warning Line** from the drop-down list.

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



Up to 10 rules can be added in total. And 3 rules for **Violence Detection** can be added.

Rule Config	Global Config			
Add Rule				
No.	Name	Туре	On	Delete
1	SA-1	Crossing Warning Line		ŵ
2	SA-2	People Approach Detection		亩
		Direction     Both     V     Direction     Both     V     Direction     Both     V     Direction     Sensitivity     1 2 3 4 5 6 7 8 9 10     Time Plan     Full Time     V     Add Schedule     +Event Linkage     Snapshot Enabled     Back     Apply     Refresh     Default	â	

Step 5 Click 🕂 to draw rule line in the image. Right-click to finish drawing.

After drawing rules, drag corners of the detection line to adjust the area range.

Table 8-27 Description of stereo analysis

Rule	Description
Crossing Warning Line	Draw the detection line.
Warning Area Intrusion	
Running Detection	
People Approach Detection	
Fall Detection	Draw the detection area.
Violence Detection	
Abnormal Number of People Detection	
People Stay Detection	

<u>Step 6</u> Set rule parameters.

Parameters might vary on different sub rules. Please refer to the actual page for detailed information.

Parameter	Description
	Set the direction of rule detection.
Direction	<ul> <li>When setting crossing warning line, select Both , B to A, or A to B.</li> <li>When setting warning area intrusion, select Enter , Exit, or Both.</li> </ul>



Parameter	Description
Sensitivity	When the sensitivity is high, detection becomes easier, but the number of false detections increases.
	Select the detection type.
Туре	<ul> <li>When setting people approach detection, select Less than or Greater than, and then configure the Spacing Threshold. After that, if the distance between two people is larger or smaller than the defined threshold, an alarm will be triggered.</li> <li>When setting violence detection, select Smashing or Fighting.</li> <li>When setting abnormal number of people detection, select Greater than, Equal to, Less than or Unequal to.</li> </ul>
Min Duration	The shortest time for triggering an alarm.
Step 7 Set arming per	iods 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".



# 9 Security

## 9.1 Security Status

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.

### **Background Information**

- 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

#### <u>Step 1</u> Select Security > Security Status.

<u>Step 2</u> 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

Details	×
• Total2XX items must be optimized. You are rec	commended to optimize now. Ignore
Device Account Status 1.A strong password is not used.	Optimize
ONVIF Account Status 1.A strong password is not used.	Optimize

## 9.2 System Service

### 9.2.1 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Procedure

- <u>Step 1</u> Select Security > System Service > 802.1x.
- <u>Step 2</u> Select the NIC name as needed, and click **(Delta )** to enable it.
- <u>Step 3</u> 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 Omega 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)

B02.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.         NIC Name       NIC1         Enable       Image: Control protocol which can effectively prevent access from unauthorized hosts.         Authentication Mode       PEAP	
Enable Contraction Mode PEAP V	
Enable Contraction Mode PEAP V	
Authentication Mode PEAP <	
Username none	
Password	
CA Certificate	
Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).	
Device Certificate Trusted CA Certificates	
Certificate List Certificate Manager	ent
No. Custom Name Certificate Serial Number Validity Period User Issued by Used by	
1         2059-05-23 11:05:14         Image: Device Root CA         Image: Device Root CA	
2 2049-05-30 13-58-24 Device IPC CA Device Root CA	
Apply Refresh Default	

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



- 1. Select TLS as the authentication mode.
- 2. Enter the username.
- 3. Click next to CA certificate, and select the trusted CA certificate in list.

 $\square$ 

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 HTT	PS					
802.1x is a network	access control protocol whi	ich can effectively prevent access from unautho	rized hosts.			
NIC Name	NIC1					
Enable						
Authentication Mode	TLS					
Username	none					
CA Certificate						
Use a trusted CA ce	ertificate to verify the validity	y of peer authentication server (switch or Radius	s server).			
Device Certificate	Trusted CA Certificates	]				
Certificate List						Certificate Management
No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
0 1		15-14-14-14-14-14-14-14-14-14-14-14-14-14-	2059-05-23 11:05:14	Device Root CA	Device Root CA	
○ 2		0420020340000	2049-05-30 13:58:24	Device IPC CA	Device Root CA	
Apply Refree	sh Default					

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

<u>Step 1</u> Select Security > System Service > HTTPS.

- Step 2 Click Control to enable it.
- <u>Step 3</u> 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	HT	ΓPS

2.1x	HTTPS								
nable									
HTTPS is a s	service entry b	based on Trar	sport Layer Security (TLS). HTTPS provides web se	rvice, ONVIF access service	e and RTSP access service.				
ompatible w	vith TLSv1.1 a	. 💽							
There might	it be security r	risks if TLS of	earlier versions are enabled. Please select carefully						
There might	it be security r	risks if TLS of	earlier versions are enabled. Please select carefully						
	it be security r evice certificat		earlier versions are enabled. Please select carefully						Certificate Managem
	evice certificat	te	earlier versions are enabled. Please select carefully Certificate Serial Number		Validity Period	User		Issued by	Certificate Managerr Used by
*Select a de	evice certificat	te			Validity Period 2050-07-15 15:37:32	User 6F03D5EYA	59E43B	Issued by Dahua Device IPC CA	





## 9.3 Attack Defense

## 9.3.1 Firewall

Configure firewall to limit access to the camera.

Procedure

- <u>Step 1</u> Select Security > Attack Defense > Firewall.
- <u>Step 2</u> Click Content to enable the firewall function.

Figure 9-6 Firewall

Firewall	Account Lock	out Anti-DoS Attack		
Enable				
Mode	● Allowlist ○ B	locklist		
Allow t	the host of the IP or M	AC in the following list to access the specified port of current device via network connection.		
Add	Delete			
	No.	Host IP/MAC	Port	Operation
	1	SEXLPROM MURPHIN	All Device Ports	12 ô
	2	MARCH AND A CONTRACT OF A CONT	All Device Ports	12 ô
Apply	Refresh	efault		

#### <u>Step 3</u> 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.
- <u>Step 4</u> Click **Add** to add the host IP/MAC address to **Allowlist** or **Blocklist**, and then click **OK**.

Figure 9-7 Firewall

Add			Х
Add Mode	IP	~	
IP Version	IPv4	~	
IP Address			
All Device P			
		ОК	Cancel

Step 5 Click Apply.

### **Related Operations**

- Click 🗹 to edit the host information.
- Click  $\stackrel{fin}{=}$  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

#### <u>Step 1</u> Select Security > Attack Defense > Account Lockout.

<u>Step 2</u> 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.

Firewall	Account Lockout	Anti-DoS Attack	
Device Account	t		
Login Attempt	5time	~	
Lock Time	5		min
ONVIF User			
Login Attempt	30time	$\vee$	
Lock Time	5		min
Apply	Refresh Default		

#### 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.

- <u>Step 1</u> Select Security > Attack Defense > Anti-DoS Attack.
- <u>Step 2</u> Select **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against Dos attack.



#### Figure 9-9 Anti-DoS attack

Firewall	Account Lockout	Anti-DoS Attack	
SYN Flood Atta	ick Defense		
	· ·	N messages to the device, leaving many half-open TCP connections on the de hit by an SYN flood attack, the device will defend itself by discarding the first	
ICMP Flood Att	ack Defense		
	d thus make the device cras	ly large number of ICMP packets to the device, which will use up all computir h. When hit by an ICMP flood attack, the device will defend itself by using the	-
Apply	Refresh Default		

## 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.

- <u>Step 1</u> Select Security > CA Certificate > Device Certificate.
- <u>Step 2</u> Select **Installing Device Certificate**.
- <u>Step 3</u> Select **Create Certificate** , and click **Next**.
- <u>Step 4</u> Enter the certificate information.



Figure 9-10 Certificate information (1)

Step 2: Fill in certific	Step 2: Fill in certificate information.					
Custom Name	test1					
∗IP/Domain Na	10.10.10.05					
Organization Un	TEST					
Organization	COMPANY					
* Validity Period	200 Days ( 1~5000 )					
* Country	(Dei					
Province						
City Name						
Previous	Create and install certificate	Cancel				

#### <u>Step 5</u> 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 <sup>th</sup> to delete the certificate.

### 9.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

- <u>Step 1</u> 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.
- <u>Step 4</u> Enter the certificate information.



Figure 9-11 Certificate information (2)

Step 2: Fill in certificate information. $\times$		
* IP/Domain Na		
Organization Un TEST		
Organization COMPANY		
* Validity Period 200 Days ( 1~5000 )		
* Country		
Province		
City Name		
Previous Create and Download	Cancel	

#### Step 5 Click Create and Download.

Save the request file to your PC.

- <u>Step 6</u> Apply the CA certificate from the third-party certificate authority.
- <u>Step 7</u> Import the signed CA certificate.
  - 1. Save the CA certificate to the PC.
  - 2. Do <u>Step 1 to Step 3</u>, 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 <sup>th</sup> 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.

- <u>Step 1</u> Select Security > CA Certificate > Device Certificate.
- <u>Step 2</u> Select Installing Device Certificate.
- <u>Step 3</u> Select Install Existing Certificate , and click Next.
- <u>Step 4</u> Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 9-12 Certificate and private key

Step 2: Select cert	ificate and private key.		×
Certificate Path	test.cer	Browse	
Private Key	PrivateKey.jks	Browse	
Private Key Passw	••••		
	Previous Import and I	nstall Cano	el

#### 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  $\stackrel{\text{\tiny left}}{=}$  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

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

Figure 9-13 Installing trusted certificate

Install Trusted C	ertificate	Х
Certificate Path	test.cer	Browse
		Cancel OK

#### 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 <sup>th</sup> to delete the certificate.

## 9.5 A/V Encryption

The device supports audio and video encryption during data transmission.

### Background Information

 $\wedge$ 

You are recommended to enable A/V Encryption function. There might be safety risk if this function is disabled.

### Procedure

<u>Step 1</u> Select **Security** > **A/V Encryption**.

<u>Step 2</u> Configure the parameters.

#### Figure 9-14 A/V encryption

vate Protocol						
Enable						
Stream transmission	is encrypted by	using private protocol.				
Encryption Type	AES256-OFB					
Jpdate Period of Sec	12	hr. (0-720)				
SP over TLS						
RTSP stream is encry	pted by using T	LS tunnel before transmission.				
*Select a device certif	icate					Certificate Managemer
	tom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
No. Cus				6F03D5EYAG9E43B		HTTPS, RTSP over TLS

#### Table 9-1 A/V encryption parameter

Area	Parameter Description	
	Fnable	Enables stream frame encryption by using private protocol.
		There might be safety risk if this service is disabled.
Private Protocol	Encryption Type	Use the default setting.
		Secret key update period.
	Update Period of Secret Key	Value range: 0–720 hours. 0 means never update the secret key.
		Default value: 12.



Area	Parameter	Description
	Enable Select a device certificate	Enables RTSP stream encryption by using TLS.
RTSP over TLS		There might be safety risk if this service is disabled.
		Select a device certificate for RTSP over TLS.
Certificate Management	Certificate Management	For details about certificate management, see "9.4.1 Installing Device Certificate".



## 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

- <u>Step 1</u> Select Security > Security Warning.
- <u>Step 2</u> Click next to **Enable** to enable security warning.
- <u>Step 3</u> Configure the parameters.

Figure 9-15 Security warning

Enable	
Event Monitoring	
Invalid executable programs attempting to run	查 Session ID Brute Force Attack
Web Path Brute Force Attack	Session connection number exceeds limit.
avoid security risks.	u informed of the security exception events immediately, so that you can deal with them timely and
+Event Linkage	
Enable Alarm   Enabled	à
Alarm-out Port 1	
Post-Alarm 10 sec.(10-30	0)
Apply Refresh Default	

<u>Step 4</u> 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 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

#### <u>Step 1</u> Select **Record** > **Search Video**.

- <u>Step 2</u> 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

<u>Step 3</u> 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		Displays all searched recorded video files. Click any files to play back it.
	Click <b>Back</b> at the upper-left corner to go to the <b>Search Video</b> page.	
		You can zoom video image of the selected area through two operations.
2	Digital Zoom	<ul> <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 areas.</li> <li>Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.</li> </ul>
Al Rule	Al Rule	Click 🖶, and then select <b>Enable</b> to display AI rules and detection box; select <b>Disable</b> to stop the display. It is enabled by default.
	AI rules is valid only when you enabled the rule during recording.	


No	Function	Description
		Controls playback.
		<ul> <li>Id: Click the icon to play back the previous recorded video in the recorded video list.</li> </ul>
		• Click the icon to slow down the playback.
		• III: Click the icon to stop playing back recorded videos.
	Play control bar	The icon changes to <b>b</b> , click the icon to play back recorded videos.
		<ul> <li>Dick the icon to speed up the playback.</li> </ul>
		• Elick the icon to play back the next recorded video in the recorded video list.
		• Elick the icon to play the next frame.
		Controls the sound during playback.
	Sound	• 📭 Mute mode.
		<ul> <li>W: Volume. You can adjust the sound.</li> </ul>
	Spanshot	Click <b>O</b> to capture one picture of the current image, and it will be saved to the configured storage path.
	Snapshot	
		About viewing or configuring storage path, see "6.1 Local".
	Video clip	Click 🗖, and clip a certain recorded video and save it. For details, see "10.1.2 Clipping Video".
	Full Screen	Click S, and the image is displayed in full-screen mode; double-click the image or press Esc button to exit full- screen mode.
		Displays the record type and the corresponding period.
3	Progress bar	<ul> <li>Click any point in the colored area, and the system will play back the recorded video from the selected moment.</li> </ul>
		• Each record type has its own color, and you can see their relations in <b>Record Type</b> bar.

# **Related Operations**

- Download: Click it to download the selected videos. For details, see "10.1.3 Downloading Video".
- Delete: Click it to delete the selected videos.



# 10.1.2 Clipping Video

# Procedure

- Step 1 Click 4
- <u>Step 2</u> 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

•						15:	53:15			18:36:00	•		<b>F</b> I	•			
09:00	10:00	11:00	12:00	13:00	14:00	15:00	6:00	17:00	18:00		OK	Cancel	21	: 00	22:00	23:00	2020-08-12

- <u>Step 3</u> Click **OK** to download the video.
- <u>Step 4</u> Select the download format and storage path.

Figure 10-4 Clipping video

No.	Туре	Start Time	End Time	Duration
1	Video Clip	2020-08-11 18:49:30	2020-08-11 21:32:15	02:42:45
ownload	● dav _ m	54		
ownload	● dav _ mp	54		
		o4 3\WebDownload\VideoClips	Browse	

#### 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.

## **Background Information**

 $\square$ 

- Playback with 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

- <u>Step 1</u> Select **Record** > **Search Video**.
- <u>Step 2</u> Select the channel, the record type, and record time, and the click **Search**.
- <u>Step 3</u> 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 Select video file



#### Step 4 Click **Download**.

<u>Step 5</u> Select the download format and storage path.

Figure 10-6 Download video

No.	Туре	Start Time	End Time	Duration	Size
1	Manual	2020-08-11 04:03:59	2020-08-11 04:15:03	00:11:04	277.8M
2	Event	2020-08-11 04:15:04	2020-08-11 04:15:12	00:00:08	0.6M
3	Event	2020-08-11 10:06:06	2020-08-11 10:07:18	00:01:12	4.6M
4	Event	2020-08-11 19:55:53	2020-08-11 19:55:53	00:00:00	0M
5	Manual	2020-08-11 19:55:59	2020-08-11 20:00:31	00:04:32	102M
6	Manual	2020-08-11 20:00:31	2020-08-11 20:03:58	00:03:27	86.6M
ze471.8M ownload ormat corage Path	dav     C:\Users\	) mp4 45363\WebDownload\PlaybackF	Record Browse		

#### 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

<u>Step 1</u> Click **Record** in the home page, and then click the **Record Control** tab.



Figure 10-7 Record control

Channel	CAM 1 v
Max Duration	30 min.(1-120)
Pre-Record	5 sec.(0-5)
Record Mode	● Auto 🔵 Manual 🔵 Off
Record Stream	Sub Stream $\lor$
	Apply Refresh Default

<u>Step 2</u> Set parameters.

Parameter	Description
Max Duration	The time for packing each video file.
	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.
Pre-Record	
	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.
Record Mode	When you select <b>Manual</b> , the system starts recording; when you select <b>Auto</b> , the system starts recording in the configured period of record plan.
Record Stream	Select record stream, including Main Stream and Sub Stream.

Table 10-2 Description of record control parameters

Step 3 Click **Apply**.

# 10.3 Setting Record Plan

## **Background Information**

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

<u>Step 1</u> Click **Record** on the home page, and then click the **Time Plan** tab.



#### Figure 10-8 Time plan



#### <u>Step 2</u> 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.

 $\square$ 

- 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**.
- <u>Step 4</u> Click **Holiday** to set holidays.



Figure 10-9 Time plar
-----------------------

nable						CI
٢			Aug			>
Su	Mo	Tu	We	Th	Fr	Sa
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

Step 5 Click Control to enable the holiday configuration, and select the days that you need to set as holiday.

Click **Clear** to cancel the selection.

```
\square
```

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

<u>Step 1</u> Select **Record** > **Storage**.



<u>Step 2</u> Select the storage method that you need for different types of recorded videos.



Parameter	Description
Event Type	Select from Scheduled , Motion and Alarm.
Disk Full	<ul> <li>Recording strategy when the disk is full.</li> <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>
	<ul> <li>Select from Local storage and Network storage.</li> <li>Local Storage : Save the recorded videos in the internal SD card.</li> </ul>
Storage Method	<ul> <li>Local Storage is displayed only on models that support SD card.</li> <li>Network Storage : Save the recorded videos in the FTP server or NAS.</li> </ul>

Table 10-3 Description of storage parameters

Step 3 Click Apply.

# 10.4.1 Local Storage

## Procedure

<u>Step 1</u> Select **Record** > **Storage**.

- <u>Step 2</u> 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.
- <u>Step 3</u> Select **Local storage** in **Storage Method** to save the recorded videos in the internal SD card.

#### Figure 10-11 Local storage

Event Type	🗸 Scheduled 🔽 Motion 🔽 Alarm	
Disk Full	● Overwrite ○ Stop	
Storage Method	Local Storage	~
	Apply Refresh Default	



# 10.4.2 Network Storage

You can select from  $\ensuremath{\textbf{FTP}}$  and  $\ensuremath{\textbf{NAS}}.$ 

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

- <u>Step 1</u> Select **Record** > **Storage**.
- <u>Step 2</u> 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.
- <u>Step 3</u> Select **Network storage** in **Storage Method**, and select **FTP** to save the recorded videos in FTP server.

You select **FTP** or **SFTP** from the drop-down list. **SFTP** is recommended to enhance network security.

<u>Step 4</u> Click Onext to **Enable** to enable the FTP function.

Figure 10-12 FTP

Event Type	🖌 Scheduled 🔽 Motion 🔽 Alarm	
Disk Full	Overwrite      Stop	
Storage Method	Network Storage $\vee$	
	FTP $\vee$	
	FTP $\vee$	
Enable		
FTP may be at risk. Co	ntinue?	
Server IP	0.07575.0	
Port	22	(0~65535)
Username	1	
Password	•••••	
Storage Path	share	
Directory Structure	Use Level 3 Directory $\vee$	
Level 1 Directory	Device Name $\lor$	
Level 2 Directory	Date	
Level 3 Directory	File Type_Channel Number	
Urgently store to local		
	Test	
	Apply Refresh Default	

<u>Step 5</u> 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 <b>Use Level 1</b> <b>Directory</b> , <b>Use Level 2 Directory</b> , and <b>Use Level 3 Directory</b> .
Level 1 Directory	Set the Level 1 directory name, and you can select from <b>Device</b> name , <b>Device IP</b> , and <b>Custom</b> . When you select <b>Custom</b> , please enter the custom directory.
Level 2 Directory	Set the Level 2 directory name, and you can select from <b>File Type</b> ,
Level 3 Directory	<b>Date, File Type_Channel No.</b> , and <b>Custom</b> . When you select <b>Custom</b> , please enter the custom directory.
Urgently store to local	Click O, and when the FTP server does not work, all the files are saved to the internal SD card.

#### Step 6 Click Apply.

<u>Step 7</u> 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

- <u>Step 1</u> Select **Record** > **Storage**.
- <u>Step 2</u> 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.
- <u>Step 3</u> Select **Network Storage** in **Storage Method**, and select **NAS** to save the recorded videos in NAS server.
- <u>Step 4</u> 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.



Event Type 🔽 Scheduled 🔽 Motion 🔽 Alarm Disk Full ● Overwrite ○ Stop Storage Method Network Storage  $\sim$ NAS  $\vee$ Protocol Type SMB Enable Server IP 0.0.0.0 Storage Path Username anonymity Password ••••• Refresh Default Apply

#### Figure 10-13 FTP

#### <u>Step 5</u> 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 <b>SMB</b> protocol, you are required to enter
Password	username and password. Enter them as needed.

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

#### <u>Step 1</u> Select **Picture** > **Picture Query**.

- <u>Step 2</u> 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.

# Reture Query Snaphot Time Plan Storage Auto Upload Channel List Total 400 Results All Download Delete Image: Channel List Image: Cha

#### Figure 11-1 Picture query

<u>Step 3</u> 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





No.	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play back it. Click <b>Back</b> at the upper-left corner to go to the <b>Picture</b> <b>Query</b> page.
2	Manual display	<ul> <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 S, and the snapshot is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.

## **Related Operations**

- Download: Click it to download the selected pictures. For details, see "11.1.2 Downloading Picture".
- Delete: Click it to delete the selected pictures.

# **11.1.2 Downloading Picture**

Download pictures to a defined path. You can download a single picture, or download them in batches.

# **Background Information**

- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "6.1 Local".



## Procedure

<u>Step 1</u> Select **Picture** > **Picture Query**.

- <u>Step 2</u> Select the channel, the snapshot type, and snapshot time, and then click **Search**.
- <u>Step 3</u> 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**.

<u>Step 5</u> Select the download format and storage path.

Figure 11-4 Downloading picture

No.	Туре	Start Time	End Time	Size
1	jpg	2020-08-11 04:04:00	2020-08-11 04:04:00	0.44M
2	jpg	2020-08-11 04:04:01	2020-08-11 04:04:01	0.44M
3	jpg	2020-08-11 04:04:02	2020-08-11 04:04:02	0.44M
4	jpg	2020-08-11 04:04:03	2020-08-11 04:04:03	0.44M
5	jpg	2020-08-11 04:04:04	2020-08-11 04:04:04	0.44M
6	jpg	2020-08-11 04:04:05	2020-08-11 04:04:05	0.44M
12.28M				
vnload	🔘 jpg			
mat				

#### 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

- <u>Step 1</u> Select **Picture** > **Snapshot**.
- <u>Step 2</u> Select the channel and set the parameters.

Figure 11-5 Snapshot

CAM 1					$\sim$
Schedu	iled				~
2592x1	.944 (2592*:	1944)			
1	0 2	3	0 4	5	0 6
1sec.					$\sim$
Apply	Refre	esh De	fault		
	Schedu 2592x1 1 1sec.	1 2 1sec.	Scheduled           2592x1944 (2592*1944)           1         2         3           1sec.         2         3	Scheduled           2592x1944 (2592*1944)           1         2         3         4           1sec.	Scheduled           2592x1944 (2592*1944)           1         2         3         4         5           1sec.

#### Table 11-2 Description of snapshot parameters

Parameter	Description		
Туре	<ul> <li>You can select from Scheduled and Event.</li> <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> <li>Make sure that you have enable the corresponding event detection and the sure that for the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the corresponding event detection and the sure that you have enable the you have</li></ul>		
Size	the snapshot function. 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 <b>Custom</b> 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

- <u>Step 1</u> Select **Picture** > **Auto Upload**.
- <u>Step 2</u> Enable the function.
- <u>Step 3</u> Click **Add**, and then configure parameters of HTTP upload method.

You can add two server information at most.

#### Figure 11-6 Image upload

Ipload Mode	HTT	2							
nable	0								
Add	Delete								
	No.	IP/Domain Name	Port	HTTPS	Path	Authentication	Event Type	Test	Dele
	1	Example: 172.168.1.108	Example: 80		Example: /example/	2	None	Test	â
	2	Example: 172.168.1.108	Example: 80		Example: /example/	12	None	Test	ċ
Apply	Refresh	Default							

Parameter	Description				
IP/Domain name	The IP address and port number of the server which the report will				
Port	be uploaded to.				
HTTPS	Click corresponding 🔍 to enable HTTPS.				
Path	The storage path of the server for the report.				
Authentication	Enable this function, and then configure the username and password. The defined server would receive the images only when you entered the correct username and password.				
Event Tune	Select the event type form the drop-down list. You can select more than one types at the same time.				
Event Type					
	The event types in the drop-down list are the same with that of picture playback.				
Test	Test the network connection between the camera and the server.				
Stop 4 Click Apply					

Step 4 Click **Apply**.



# 12 Report

# **12.1 Viewing Report**

View the statistics results of AI functions in report form.

Figure 12-1 Report

Rule	People Counting $\vee$	Statist	ics Type	People No. $\vee$		
Today	/ This Week This Mor	nth This Year	2021-0	5-17 18:38:4~202:	1-05-18 18:38:4 📋	*Max 12 months.
Repo	t 🔽 NumberStat1	Q Search				

- The period for the report is the latest 24 hours by default.
- Click <sup>(iii)</sup> 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 Recognition

View the statistics result of face recognition in report form.

## Procedure

- <u>Step 1</u> Select **Report** > **Report** > **Face Recognition**.
- <u>Step 2</u> Set the period for the report.

 $\square$ 

For multi-channel camera, select the channel first.

- <u>Step 3</u> Select the gender and age.
- Step 4 Click Search.







## **Related Operations**

• Select the report form

Click  $\bowtie$  to display the report in line chart; click  $\bowtie$  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 Metadata

View the statistics result of video metadata in report form.

# Procedure

<u>Step 1</u> Select **Report** > **Report** > **Video Metadata**.

<u>Step 2</u> Set the period for the report.



#### 

For multi-channel camera, select the channel first.

- <u>Step 3</u> Select the tripwire direction.
- Step 4 Click Search.

#### Figure 12-3 Video metadata report



## **Related Operations**

• Select the report form

Click  $\bowtie$  to display the report in line chart; click  $\bowtie$  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

<u>Step 1</u> Select **Report** > **Report** > **People Counting**.

<u>Step 2</u> Set search conditions.

 $\square$ 

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	<ul> <li>The statistics type of the people counting report.</li> <li>People No. : Displays the report of the number of people that meet the configured condition.</li> <li>Strand Time : 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	When selecting rule to <b>Area People Counting</b> , and statistics type to <b>People No.</b> , you need to configure this parameter. 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.
Queue Time	When selecting rule to <b>Queuing</b> , and statistics type to <b>People No.</b> , you need to configure this parameter. The report displays the number of people whose stay time is shorter than <b>Queuing Time</b> and is equal or longer than <b>Queuing Time</b> .
Period for the report	<ul> <li>Set the period for the report.</li> <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 12-7 Queuing



# **Related Operations**

• Select the report form

Click  $\bowtie$  to display the report in line chart; click  $\bowtie$  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

- $\underline{Step 1} \qquad Select \, \textbf{Report} > \textbf{Report} > \textbf{Crowd Distribution Map}.$
- <u>Step 2</u> 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 ...... 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

<u>Step 1</u> Select **Report** > **Report** > **Vehicle Density**.



<u>Step 2</u> 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 **Click** 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

<u>Step 1</u> Select **Report** > **Report** > **Heat Map.** 

<u>Step 2</u> 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.
Туре	You can select report type form <b>Heat Map</b> and <b>Track Map</b> .
People No.	When selecting type as <b>Heat Map</b> , select <b>People No.</b> , and then set the
Threshold	threshold. The system will display the heat map for people density.



Parameter	Description
Time	When selecting type as <b>Heat Map</b> , select <b>Time</b> and then set the
Threshold	threshold. The system will display the heat map for stay time.
	Set the period for the report.
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

- <u>Step 1</u> Select **Report** > **Report** > **ANPR**.
- <u>Step 2</u> 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 recognition or snapshot results by pictures.

## Prerequisites

Make sure that you have installed SD card.

## Procedure

- Step 1
   Select Report > Picture Query > Face.
- <u>Step 2</u> Select the type and set the period for the report.

Click **Advance** to set face attributes for precise search.

<u>Step 3</u> Click **Search**. The search result is displayed.



Figure 12-14 Face report





# 12.3 Auto Upload

Select the upload mode, enable it, and configure the parameters. The camera will upload reports of AI 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

- <u>Step 1</u> Select **Report** > **Auto Upload**.
- <u>Step 2</u> Select the upload method, and then enable it.
- <u>Step 3</u> 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

pload Mode	HTTP							
able								
Add Delete		ain Name Port	HTTPS	Path	Authentication	Event Type	Test	Delete
1		72.168.1.108 Example:		Example: /example/	Authentication	None	Test	Deleti
2	Example: 1	172.168.1.108 Example:		Example: /example/	12	None	Test	à
Apply Refre								



Parameter	Description
	Select the report period from the drop-down list.
Report Period	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
Port	be uploaded to.
HTTPS	Click corresponding 🔍 to enable HTTPS.
Path	The storage path of the server for the report.
	Select the report type form the drop-down list. You can select more than one types at the same time.
Report Type	The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, heat map, and video metadata, the 3 report types are displayed in the drop-down list.
Test	Test the network connection between the camera and the server.

## Table 12-3 Description of HTTP mode parameter

# Figure 12-16 FTP upload method

Upload Mode	FTP v	
Enable		
Report Period	1hr v	
Report Type	Heat Map × People Counting ×	
Server IP	17 08	
Port	3777	(0~65535)
Username	admin	
Password	•••••	
Storage Path		
	Test	
Apply Refresh	Default	



Parameter	Description
	Select the report period from the drop-down list.
Report Period	It is 1 hour by default, which indicates that upload the report every 1 hour.
	Select the report type form the drop-down list. You can select more than one types at the same time.
Report Type	The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, heat map, and video metadata, 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
Port	will be uploaded to.
Username	
Password	Username and password for logging in to FTP server.
Storage Path	Username and password for logging in to FTP server.
Test	Test the network connection between the camera and the server.

Table 12-4 Description of FTP mode parameter

• Email upload method



Upload Mode	Email v	
Enable		
Report Period	1hr v	
Report Type	People Counting ×	
SMTP Server	none	
Port	25	
Anonymous		
Username	anonymity	
Password	•••••	
Sender	none	
Encryption Type	TLS(Recommended) V	
Subject	IPC Message	
Receiver		Add
Apply Refresh	Default	

Figure 12-17 Email upload method

Table 12-5 Description of email mode parameter

Parameter	Description
Papart Pariod	Select the report period from the drop-down list.
Report Period	It is 1 hour by default, which indicates that upload the report every 1 hour.
	Select the report type form the drop-down list. You can select more than one types at the same time.
Report Type	<ul> <li>The report types in the drop-down list are the same with that supported AI function. For example: If the camera supports people counting, and video metadata the 2 report types are displayed in the drop-down list,</li> </ul>
	<ul> <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 <b>Anonymous</b> , and the sender's information is not displayed in the email.
Username	Username and password used to log in server.
Deserverd	
Password	See Table 12-6 for details.
Sender	Sender's email address.
	Select the encryption type from None, SSL (Secure Sockets Layer) and TLS (Transport Layer Security).
Encryption Type	
	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 <b>add</b> to set more than one receivers.
Receiver	Supports 3 addresses at most.

## Table 12-6 Description of major mailbox configuration

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

Step 4 Click **Apply**.



# **13 Maintenance Center**

# 13.1 One-click Diagnosis

## Procedure

<u>Step 1</u>	Select 🜻	> Maintenance Center > One-click Diagnosis.
---------------	----------	---

Step 2 Click **Diagnose**.

Diagnosis information is generated and displayed on the page.

Figure 13-1 One-click diagnosis

9	One-click Diagnosis One-click diagnosis detects the configurations and status of your device to improve its performance. The last scanning time: 2023-06-11 14:12:32	Diagnose Again
Network	Condition-3 records	
	IP Address Config Normal Checks If the IP address configuration is normal.	
	DHCP Normal Checks if the DHCP function is normal.	
	Network Routing Normal Checks if the routing configuration is normal.	
Working	Condition-1 records	
9	Power Supply Abnormal Checks If the power is being normally supplied.	Details

# **Related Operations**

After the one-click diagnosis is completed, the page displays the time and results of the last scanning. Click **Diagnose Again** to diagnose the camera again.

Click **Details** to view the corresponding diagnosis information.

- Click **Ignore** to ignore the scanning results of the module. The module will not be scanned again when the camera is diagnosed next time.
- Click **Processed** to trigger a new diagnosis based on the current status of the camera.





Figure 13-2 Details

	power supply of the de the power supply is sta	vice might behave abnor able.	mally. Please
No.	Contents	Time Error Occurred	End Time
			2022 02 44 40 24 20
1	Power off and exit.	2023-08-14 10:31:38	2023-08-14 10:34:28

# 13.2 System Information

# **13.2.1 Viewing Device Information**

Select Se

# **13.2.2 Viewing Online Users**

Select Select

# 13.2.3 Viewing Legal Information

Select Se

# 13.3 Log Information



# 13.3.1 Viewing Local Logs

View and back up the log information of the system.

## **Background Information**

The log type includes All, System, Config, Storage, Alarm Event, Record, Account and Security.

- **System** : Includes program start, abnormal close, close, program reboot, device closedown, device reboot, system reboot, and system upgrade.
- **Config** : Save configurations and delete configuration files.
- **Storage** : Configuring the disk type, clear data, perform hot swap, view the FTP status and select the record mode.
- Alarm Event (recording events such as video detection, AI, alarms, and anomalies) : View information on when the event started and ended.
- **Record** : Access files, review files with errors and search for files.
- Account : Log in and out, and add, delete and edit users and groups.
- Security : Reset the password and filter IPs.

## Procedure

- <u>Step 1</u> Select Select
- <u>Step 2</u> Configure the start time and end time, and then select the log type.

The start time should be no earlier than January 1, 2000, and the end time should be no later than December 31, 2037.

- Step 3 Click Search.
  - Click 🗉 or click a certain log to view the details in the **Details** area.
  - Click **Backup** to back up all the logs that were found on the local computer. If you select **Encrypt Log Backup** and set **Password**, you need to enter a password to open a local log file.
  - Click **Clear** to clear logs.

#### Figure 13-3 Search local logs

Start Time	2003-08-01 09:33:00 ~ 202	3-08-14 09:33:00 🗇 Type C	onfig V Search Clear		
Backup	<ul> <li>Encrypt Log Backup</li> </ul>	Password			
	No.	Time	Username	Туре	Details
	1	2023-08-14 09:32:10	admin	Save Config	
	2	2023-08-14 09:21:31	System	Save Config	
	3	2023-08-14 09:21:20	System	Save Config	
	4	2023-08-11 15:36:15	admin	Save Config	
	5	2023-08-11 15:18:09	admin	Save Config	
	6	2023-08-11 15:14:47	System	Save Config	
	7	2023-08-11 15:14:39	System	Save Config	
	8	2023-08-11 14:46:22	System	Save Config	
	9	2023-08-11 14:46:11	System	Save Config	
	10	2023-08-11 14:30:38	System	Save Config	
	11	2023-08-11 14:30:26	System	Save Config	
	12	2023-08-11 14:23:14	admin	Save Config	
	13	2023-08-11 10:35:06	System	Save Config	
	14	2023-08-11 10:34:53	System	Save Config	
	15	2023-08-11 10:34:28	System	Save Config	



# 13.3.2 Setting Remote Logs

Configure remote logs to receive logs by accessing the set address.

Procedure

- <u>Step 1</u> Select Select
- <u>Step 2</u> Click Contended to enable remote log function.
- <u>Step 3</u> Configure address, port and device number.

Figure 13-4 Remote log

Server Address	192,168.0.108		
Server Address	192.106.0.106		
Port	514	(1-65534)	
Device No.	22	(0-23)	
EnableTLS			
RTSP stream is er	crypted by using TLS tunnel before transmis	ion.	
	Apply Refresh Default		

- <u>Step 4</u> Click Corresponding to **EnableTLS** to encrypt RTSP stream by using TLS tunnel before transmitting the data to prevent data leakage.
- Step 5 Click **Apply**.

# **13.4 Maintenance Management**

# 13.4.1 Requirements

To make sure the system runs normally, fulfill the following requirements for maintenance:

- Check surveillance images regularly.
- Regularly clear user and user group information that is not frequently used.
- Change the password every 3 months. For details, see "6.7.3 Account".
- View system logs, analyze them and process abnormalities as early as possible.
- Back up the system configuration regularly.
- Restart the camera and delete the old files regularly.
- Update the firmware as updates become available.

# 13.4.2 Maintenance

You can restart the system manually, and then set the time for auto reboot and to automatically delete old files. This function is enabled by default.

Procedure

Step 1 Select Se





estart System		
Auto Restart		
Restart Time	Fri	v 03:42 O
elete Old Files		
Auto Delete		
Delete File		day(s) ago
mergency Mainter	lance	
Enable		
	to our after-sales service, enable /stem will automatically enable tl	e this function. If the device has any trouble performing functions, such as his function.
pply Refresh	n Default	

Step 2

Configure auto maintain parameters.

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

 $\square$ 

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

Step 3 Click Apply.

# 13.4.3 Import/Export

**Background Information** 

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

## Procedure

Select > Maintenance Center > Maintenance Management > Import/Export. Step 1

Figure 13-6 Import/export

File	Select File Import File
------	-------------------------

- Step 2 Import and export.
  - Import: Select local configuration file, and then 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.

# 13.4.4 Default

Restore the camera to default configuration or factory settings.

 $\square$ 

This function will restore the camera to default configuration or factory settings. Operate it carefully.

Select > Maintenance Center > Maintenance Management > Default.

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

Default
Other configurations will be recovered to default except network, user management and so on.
Factory Defaults
<ol> <li>All the parameters will be restored to factory default settings.</li> </ol>

#### Figure 13-7 Default

# 13.4.5 Font Pack

You can upload the selected front pack into the device, and then all the OSD information will be displayed in the selected font.

## Prerequisites

Prepare the authenticated font pack. You can contact the after-sales technicians to get it.

# Procedure

<u>Step 1</u> Select Select



#### Figure 13-8 Font pack

File		Select File Import Pack
<ul> <li>Importing a new font particular particular</li></ul>	ck will cause the original to be overwritten.	
	imported pack. After deletion, the default pack	

<u>Step 2</u> Click **Select File**, select the font pack, and then click **Import Pack**.

You can add a new front pack if necessary. Importing a new font pack will overwrite the original one.

## **Related Operations**

Click **Delete Pack** to delete the imported pack.

# 13.5 Update

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

## Procedure

Step 1 Sele

# Select Se

Figure 13-9 Upgrade

Jpgrade					
System Version: 3.1	۲	Build Date:	2023-11-22		
Online Update					
Auto Check for Update	is:				
Manual Check					
ile Update					
Path				Browse	Jpdate

<u>Step 2</u> Click **Browse**, and then upload upgrade file.

The upgrade file should be a .bin file.

- Click I next to Auto Check for Updates, the system regularly checks for a new version.
- Click **Manual Check**, the system immediately checks for a new version.
- Step 3 Click Update.

The upgrade starts.



# 13.6 Advanced Maintenance

# 13.6.1 Export

Export the serial number, firmware version, device operation logs, configuration information, and other information.

## Procedure

# Step 1 Select Se

Figure 13-10 Export



<u>Step 2</u> Click **Export**, and the page will display the export progress. Click **End Export** to cancel the current export.

After the export is complete, the page will prompt **Exported successfully**.

# 13.6.2 Packet Capture

Retrieve network interaction data between the camera and a specified network card on the client, and store it on the computer.

## Procedure

```
Step 1 Select Se
```

Figure 13-11 Packet capture

NIC	Device Address		IP 1: Port 1			IP 2: Port 2		Packet Sniffer Size	Packet Sniffer Backup
eth0	1.11.11.11.11.11	Optional	:	Optional	Optional	:	Optional	0.00MB	۲
lo		100.000	:	Optional	Optional	:	Optional	0.00MB	۲

<u>Step 2</u> (Optional) In the **Packet Capture** area, set the IP addresses and ports for **IP 1: Port 1** and **IP 2: Port 2** respectively.

Obtain the network interaction data between the camera and the specified client.

- The addresses and ports of IP 1: Port 1 and IP 2: Port 2 cannot be the same.
- IP 1: Port 1 and IP 2: Port 2 are optional, you can enter one IP address and port or leave them blank.

Step 3 Capture.

Click **b** to start capturing. **Packet Sniffer Size** will display the size of the packet.



Click II to end capturing. The capture file will be saved locally.

# 13.6.3 Run Log

Run log refers to the serial port information automatically recorded by the camera during operation. Viewing the run log helps to locate problems and improve work efficiency.

## Procedure

<u>Step 1</u>

<u>1</u> Select Se

Figure 13-12 Run log

No.	Date	Size	Download
1	2023_12_02	0.071M	÷

<u>Step 2</u> Export the log.

- Select one log, and then click 💾 . You can export the log one by one.
- Select more than one log, and then click **Export**. You can export the logs in batch.

## **Related Operations**

- Click **Refresh** to refresh information displayed on the page.
- Select one or more logs, and then click **Delete** to delete the log.

 $\square$ 

After deleted, the log cannot be recovered.



# Appendix 1 Security Commitment and Recommendation

Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

# Account Management

## 1. Use complex passwords

Please refer to the following suggestions to set passwords:

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

## 2. Change passwords periodically

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

## 3. Allocate accounts and permissions appropriately

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

## 4. Enable account lockout function

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

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

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



# Service Configuration

#### 1. Enable HTTPS

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

#### 2. Encrypted transmission of audio and video

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

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

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

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

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

#### 4. Change HTTP and other default service ports

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

# Network Configuration

#### 1. Enable Allow list

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

#### 2. MAC address binding

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

#### 3. Build a secure network environment

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

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

# Security Auditing

#### 1. Check online users

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

2. Check device log



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

#### 3. Configure network log

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

## Software Security

#### 1. Update firmware in time

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

#### 2. Update client software in time

We recommend you to download and use the latest client software.

## **Physical Protection**

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

# ENABLING A SMARTER SOCIETY AND BETTER LIVING