Network Camera Web 5.0

Operation Manual



V1.0.2

Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of network camera.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Date
V1.0.2	• Added "6.2.2.2.14 Configuring Parking Space". • Added "8.5 Setting Vehicle Density". • Added "8.6 Setting Parking Space". • Added "12.1.4 Crowd Distribution". • Added "12.1.5 Vehicle Density". • Updated "8.11 Setting ANPR".	July 2021
V1.0.1	• Added "8.8 Setting People Counting" and "8.10 Setting Heat Map". • Added "6.2.1.9 Fisheye" and "7.4.4 Fisheye". • Updated "8.2 Setting Face Recognition". • Updated "12 Report".	May 2021
V1.0.0	First release.	September 2020

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car 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

Electrical Safety

- All installation and operation shall conform to your local electrical safety codes.
- Use power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to device labels.
- Make sure that the power supply is correct before operating the device.
- A readily accessible disconnecting device shall be incorporated in the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sun light; otherwise it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp, dusty, extremely hot or cold environment, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use and store the device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.
- Install the device in the location where only the professional staff with relevant knowledge of safety guards and warnings can access. The accidental injury might happen to the non-professionals who enter the installation area when the device is operating normally.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scald.
- Carefully follow the instructions in the manual when performing any disassembly operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional disassembly. Please contact after-sale service for desiccant replacement if there is condensed fog on the lens after unpacking or when the desiccant turns green. (Not all models are included with the desiccant).
- It is recommended to use the device together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the device to enhance reliability.
- Do not touch the image sensor (CMOS) directly. Dust and dirt could be removed with air blower, or you can wipe the lens gently with soft cloth that is moistened with alcohol.
- You can clean the device body with soft dry cloth, and for stubborn stains, use the cloth with mild detergent. To avoid possible damage on device body coating which could cause performance to decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on

to clean the device body, nor can strong, abrasive detergent be used.

- Dome cover is an optical component. Do not touch or wipe the cover with your hands directly during installation or operation. For removing dust, grease or fingerprints, wipe gently with moistened oil-free cotton with diethyl or moisten soft cloth. You can also remove dust with an air blower.

WARNING

- Strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong password, changing password regularly, upgrading firmware to the latest version, and isolating computer network. For some device with old firmware versions, the ONVIF password will not be modified automatically along with the modification of the system password, and you need to upgrade the firmware or manually update the ONVIF password.
- Use standard components or accessories provided by manufacturer and make sure that the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supply sources for the device unless otherwise specified. A failure to follow this instruction might cause damage to the device.

Table of Contents

Foreword I

Important Safeguards and Warnings III

1 Overview 1

1.1 Introduction 1

1.2 Network Connection 1

1.3 Function 1

1.3.1 Basic Function 1

1.3.2 AI Function 2

2 Configuration Flow 5

3 Device Initialization 6

4 Login 9

4.1 Device Login 9

4.2 Resetting Password 10

5 Main Interface 12

6 Setting 13

6.1 Local 13

6.2 Camera 14

6.2.1 Setting Image Parameters 14

6.2.1.1 Interface Layout 14

6.2.1.2 Image 16

6.2.1.3 Exposure 17

6.2.1.4 Backlight 19

6.2.1.5 WB 20

6.2.1.6 Day/Night 20

6.2.1.7 Illuminator 21

6.2.1.8 Defog 22

6.2.1.9 Fisheye 23

6.2.2 Setting Encode Parameters 24

6.2.2.1 Encode 24

6.2.2.2 Overlay 26

6.2.2.2.1 Configuring Privacy Masking 26

6.2.2.2.2 Configuring Channel Title 27

6.2.2.2.3 Configuring Time Title 28

6.2.2.2.4 Configuring Location 28

6.2.2.2.5 Configuring Font Properties 29

6.2.2.2.6 Configuring Picture Overlay 29
6.2.2.2.7 Configuring Custom Title 30
6.2.2.2.8 Configuring Target Statistics 30
6.2.2.2.9 Configuring ANPR 31
6.2.2.2.10 Configuring Face Detection 31
6.2.2.2.11 Configuring Face Recognition 32
6.2.2.2.12 Configuring Face Statistics 32
6.2.2.2.13 Configure Face&Body Counting 33
6.2.2.2.14 Configuring Parking Space 34
6.2.2.3 ROI 34
6.2.3 Audio 35
6.2.3.1 Setting Audio Parameters 35
6.2.3.2 Setting Alarm Tone 36
6.3 Network 37
6.3.1 TCP/IP 37
6.3.2 Port 40
6.3.3 PPPoE 41
6.3.4 DDNS 42
6.3.5 Email 43
6.3.6 UPnP 45
6.3.7 SNMP 46
6.3.8 Bonjour 48
6.3.9 Multicast 49
6.3.10 Register 50
6.3.11 QoS 50
6.3.12 Platform Access 51
6.3.12.1 P2P 51
6.3.12.2 ONVIF 51
6.3.12.3 RTMP 52
6.3.13 Basic Service 53
6.4 Event 54
6.4.1 Setting Alarm Linkage 54
6.4.1.1 Setting Alarm-in 54
6.4.1.2 Alarm Linkage 55
6.4.1.2.1 Adding Schedule 55
6.4.1.2.2 Record Linkage 56
6.4.1.2.3 Snapshot Linkage 57
6.4.1.2.4 Alarm-out Linkage 57

6.4.1.2.5 Email Linkage....57
6.4.1.3 Subscribing Alarm....58
6.4.1.3.1 About Alarm Types....58
6.4.1.3.2 Subscribing Alarm Information....58
6.4.2 Setting Exception....59
6.4.2.1 Setting SD Card Exception....59
6.4.2.2 Setting Network Exception....60
6.4.2.3 Setting Voltage Detection....61
6.4.3 Setting Video Detection....61
6.4.3.1 Setting Motion Detection....61
6.4.3.2 Setting Video Tampering....63
6.4.3.3 Setting Scene Changing....64
6.4.4 Setting Audio Detection....64
6.5 Storage....65
6.6 System....66
6.6.1 General....66
6.6.1.1 Basic....66
6.6.1.2 Date & Time....67
6.6.2 Account....68
6.6.2.1 User....68
6.6.2.1.1 Adding User....68
6.6.2.1.2 Resetting Password....71
6.6.2.2 Adding User Group....72
6.6.2.3 ONVIF User....72
6.6.3 Peripheral Management....74
6.6.3.1 Configuring Serial Port....74
6.6.3.2 Configuring External Light....74
6.6.3.3 Configuring Wiper....75
6.6.4 Manager....76
6.6.4.1 Requirements....76
6.6.4.2 Maintenance....76
6.6.4.3 Import/Export....77
6.6.4.4 Default....78
6.6.5 Upgrade....78
6.7 System Information....78
6.7.1 Version....79
6.7.2 Online User....79
6.8 Setting Log....79

6.8.1 Log 79
6.8.2 Remote Log 80
7 Live 81
7.1 Live Interface 81
7.2 Setting Encode 82
7.3 Live View Function Bar 82
7.4 Window Adjustment Bar 83
7.4.1 Adjustment 83
7.4.2 Zoom and Focus 84
7.4.3 Image Adjustment 85
7.4.4 Fisheye 86
7.5 Display Mode 90
8 AI 93
8.1 Setting Crowd Distribution Map 93
8.1.1 Global Configuration 93
8.1.2 Rule Configuration 94
8.2 Setting Face Recognition 95
8.2.1 Setting Face Detection 96
8.2.2 Setting Face Database 99
8.2.2.1 Creating Face Database 99
8.2.2.2 Adding Face Picture 100
8.2.2.2.1 Single Adding 101
8.2.2.2.2 Batch Importing 102
8.2.2.3 Managing Face Picture 103
8.2.2.3.1 Editing Face Information 103
8.2.2.3.2 Deleting Face Picture 104
8.2.2.4 Face Modeling 104
8.2.3 Setting Arming Alarm 105
8.2.4 Viewing Face Recognition Result 108
8.3 Setting Face Detection 109
8.4 Setting IVS 111
8.4.1 Global Configuration 112
8.4.2 Rule Configuration 113
8.5 Setting Vehicle Density 117
8.6 Setting Parking Space 119
8.6.1 Rule Configuration 119
8.6.2 Global Configuration 122
8.7 Setting Video Metadata 123

8.7.1 Global Configuration 123
8.7.2 Rule Configuration 124
8.7.3 Viewing Video Metadata Report 126
8.8 Setting People Counting 127
8.8.1 People Counting 127
8.8.2 Queuing 129
8.8.3 Global Configuration 131
8.9 Face & Body Detection 132
8.9.1 Global Configuration 132
8.9.2 Rule Configuration 133
8.10 Setting Heat Map 135
8.11 Setting ANPR 135
8.11.1 Lane Configuration 135
8.11.2 Rule Configuration 137
8.11.3 Picture 138
8.11.4 Allowlist 139
8.11.5 Blocklist 142
9 Security 143
9.1 Security Status 143
9.2 System Service 144
9.2.1 802.1x 144
9.2.2 HTTPS 145
9.3 Attack Defense 146
9.3.1 Firewall 146
9.3.2 Account Lockout 146
9.3.3 Anti-DoS Attack 147
9.4 CA Certificate 148
9.4.1 Installing Device Certificate 148
9.4.1.1 Creating Certificate 148
9.4.1.2 Applying for and Importing CA Certificate 148
9.4.1.3 Installing Existing Certificate 149
9.4.2 Installing Trusted CA Certificate 150
9.5 A/V Encryption 151
9.6 Security Warning 152
10 Record 153
10.1 Playback 153
10.1.1 Playing Back Video 153
10.1.2 Clipping Video 155

10.1.3 Downloading Video 156
10.2 Setting Record Control 157
10.3 Setting Record Plan 157
10.4 Storage 159
10.4.1 Local Storage 160
10.4.2 Network Storage 160
10.4.2.1 FTP 160
10.4.2.2 NAS 162
11 Picture 164
11.1 Playback 164
11.1.1 Playing Back Picture 164
11.1.2 Downloading Picture 165
11.2 Setting Snapshot Parameters 166
11.3 Setting Snapshot Plan 167
11.4 Storage 167
11.5 Setting Upload Method 167
12 Report 169
12.1 Viewing Report 169
12.1.1 Face Recognition 169
12.1.2 Video Metadata 170
12.1.3 People Counting 171
12.1.4 Crowd Distribution 174
12.1.5 Vehicle Density 175
12.1.6 Heat Map 175
12.1.7 ANPR 177
12.2 Searching for Face Picture 178
12.3 Auto Upload 178
Appendix 1 Cybersecurity Recommendations 183

1 Overview

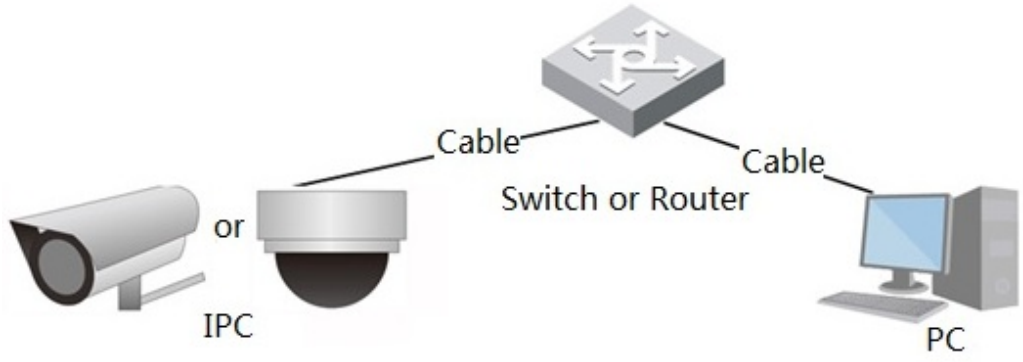
1.1 Introduction

IP camera (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through internet. They are commonly used for surveillance, requiring no local recording device, but only a local area network.
IP camera is divided into single-channel camera and multi-channel camera according to the channel quantity. For multi-channel camera, you can set the parameters for each channel.

1.2 Network Connection

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

Figure 1-1 General IPC network



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

1.3 Function

Functions might vary with different devices.

1.3.1 Basic Function

Real-time Monitoring

- Live view.
- When live viewing the image, you can enable audio, voice talk and connect monitoring center for quick processing on the abnormality.
- Adjust the image to the proper position by PTZ.
- Snapshot and triple snapshot abnormality of the monitoring image for subsequent view and processing.
- Record abnormality of monitoring image for subsequent view and processing.
- Configure coding parameters, and adjust live view image.

Alarm

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

Exception

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

Video Detection

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

Audio Detection

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

Record

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

Account

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

1.3.2 AI Function

IVS

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

Face Detection

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

Crowd Distribution Map

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

Video Metadata

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

People Counting

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

Heat Map

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

ANPR

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

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

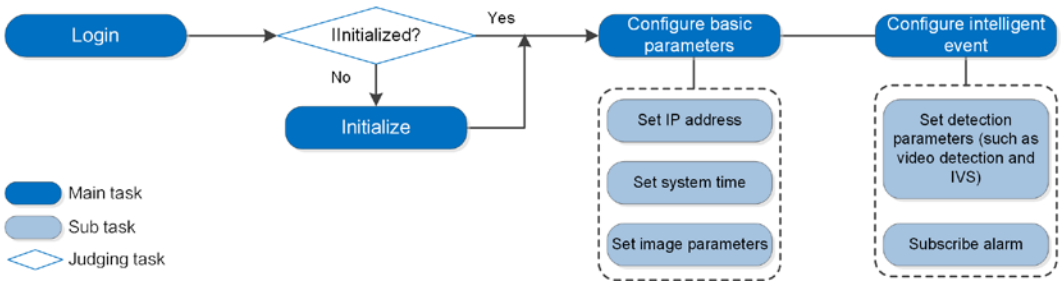


Table 2-1 Description of flow

Configuration		Description	Reference
Login		Open IE browser and enter IP address to log in to the web interface, The camera IP address is 192.168.1.108 by default.	"4 Login".
Initialization		Initialize the camera when you use it for the first time.	"3 Device Initialization"
Basic parameters	Camera parameters	Configure image parameters, encoder parameters, and audio parameters to ensure the image quality.	"6.2 Camera".
	Date & time	Set date and time to ensure the recording time is correct.	"6.6.1.2 Date & Time"
	IP address	Change IP address according to network planning for the first use or during network adjustment.	"6.3.1 TCP/IP"
	Subscribe alarm	Subscribe alarm event. When the subscribed alarm is triggered, the system will record the alarm on the alarm tab.	"6.4.1.3 Subscribing Alarm"
AI	AI rules	Configure the necessary detection rules, such as face detection and IVS.	"8 AI"

3 Device Initialization

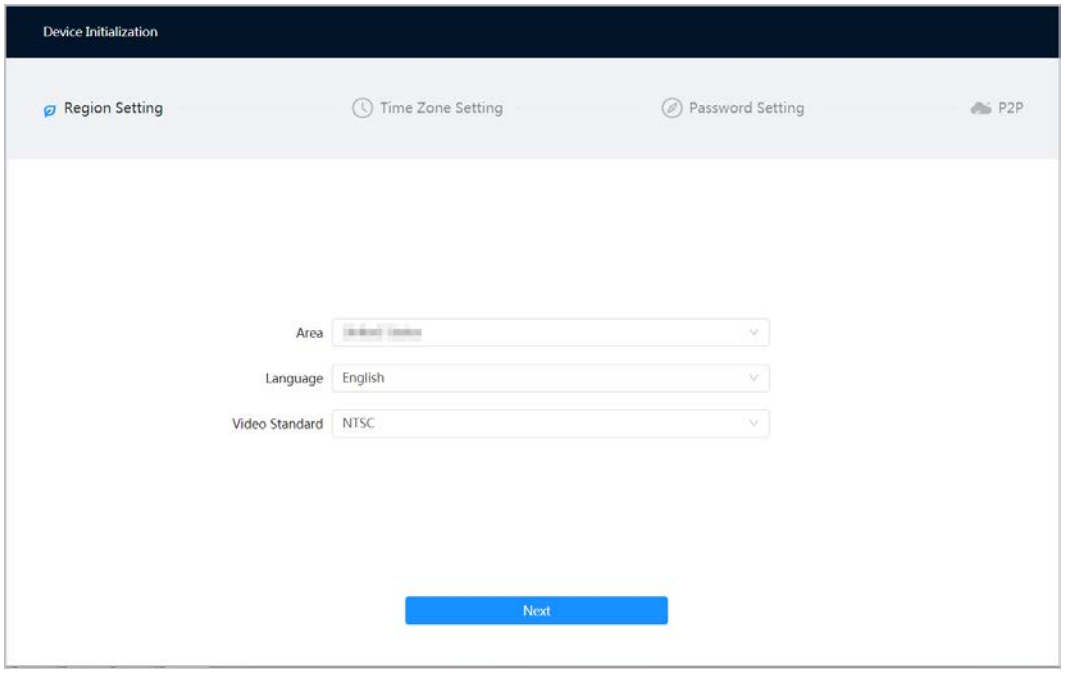
Device initialization is required for the first-time use. This manual is based on the operation on the web interface. You can also initialize device through ConfigTool, NVR, or platform devices.

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

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

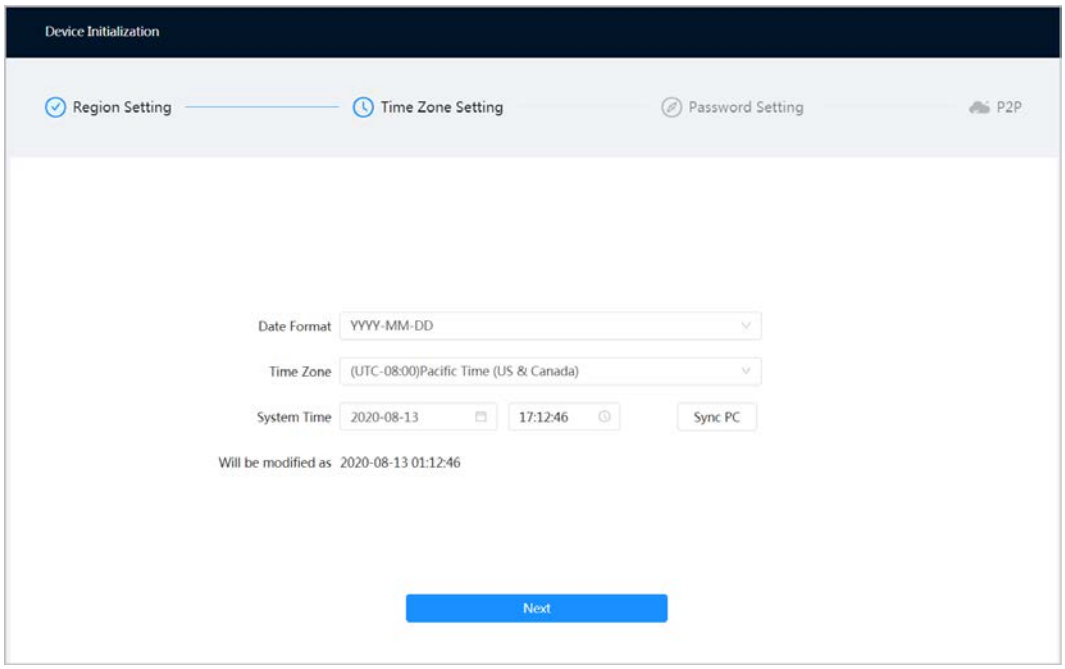
The IP is 192.168.1.108 by default.

Figure 3-1 Region Setting



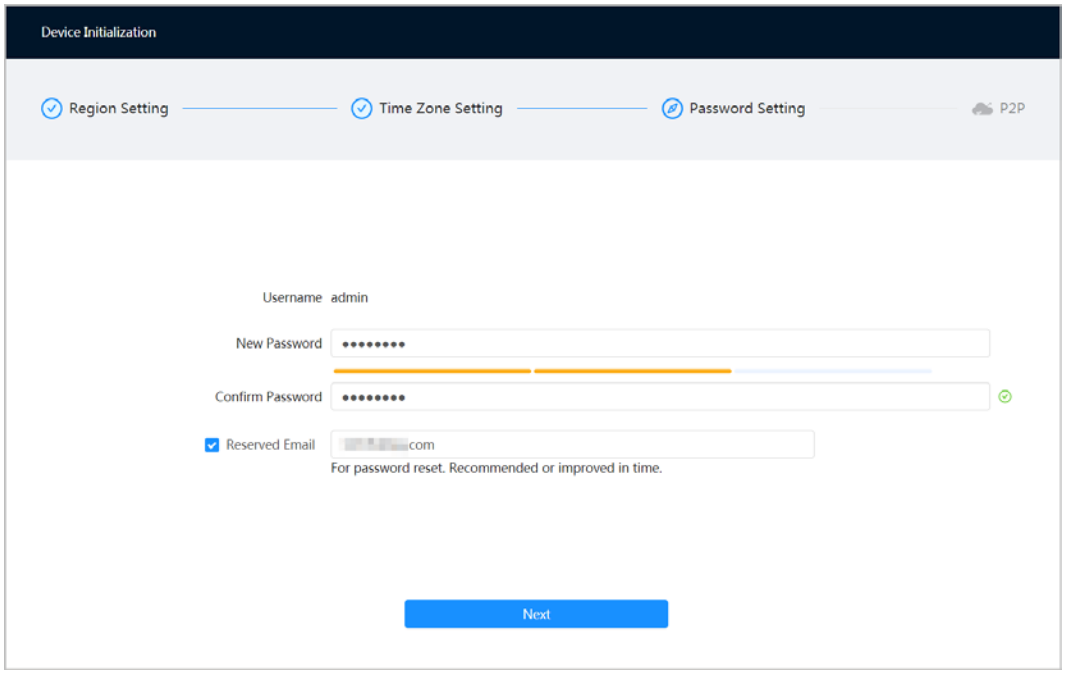
Step 2 Select the area, language, and video standard according to the actual situation, and then click **Next**.

Figure 3-2 Time zone setting



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

Figure 3-3 Password setting



Step 4 Set the password for admin account.

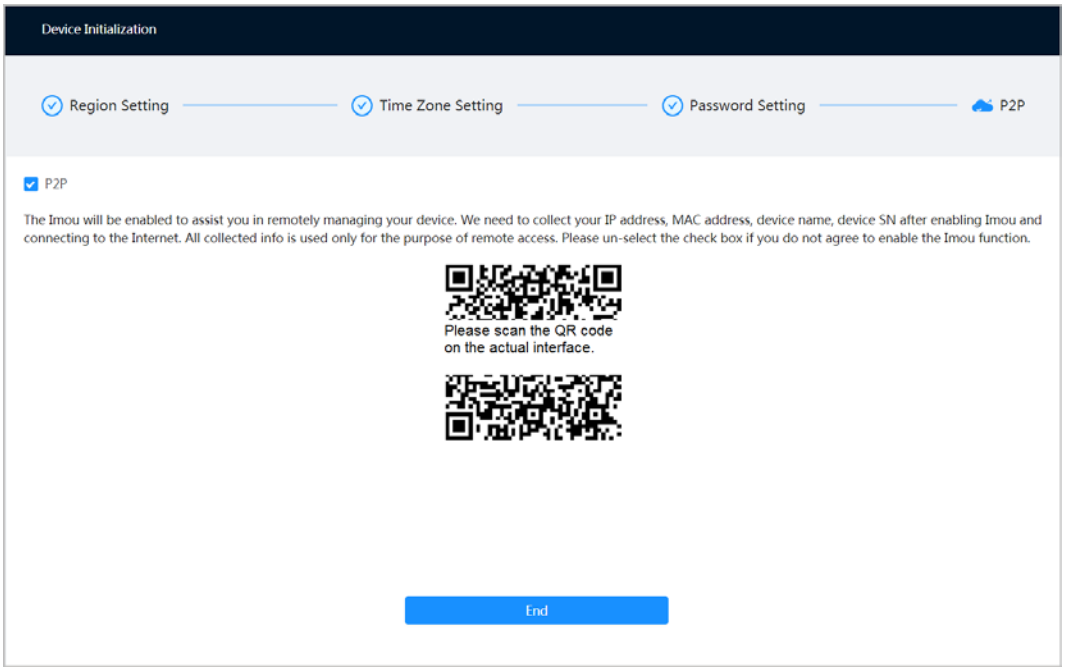
Table 3-1 Description of password configuration

Parameter	Description
Username	The default username is admin.
Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &). Set a high security level password according to the password security notice.
Confirm password	

Parameter	Description
Reserved email	Enter an email address for password resetting, and it is selected by default. When you need to reset the password of the admin account, a security code for password resetting will be sent to the reserved email address.

Step 5 Click **Next**, and then **P2P** interface is displayed.

Figure 3-4 P2P



4 Login

4.1 Device Login

This section introduces how to log in to and log out of the web interface. This section takes Chrome as an example.

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

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

Step 2 Enter the username and password.

The username is admin by default.

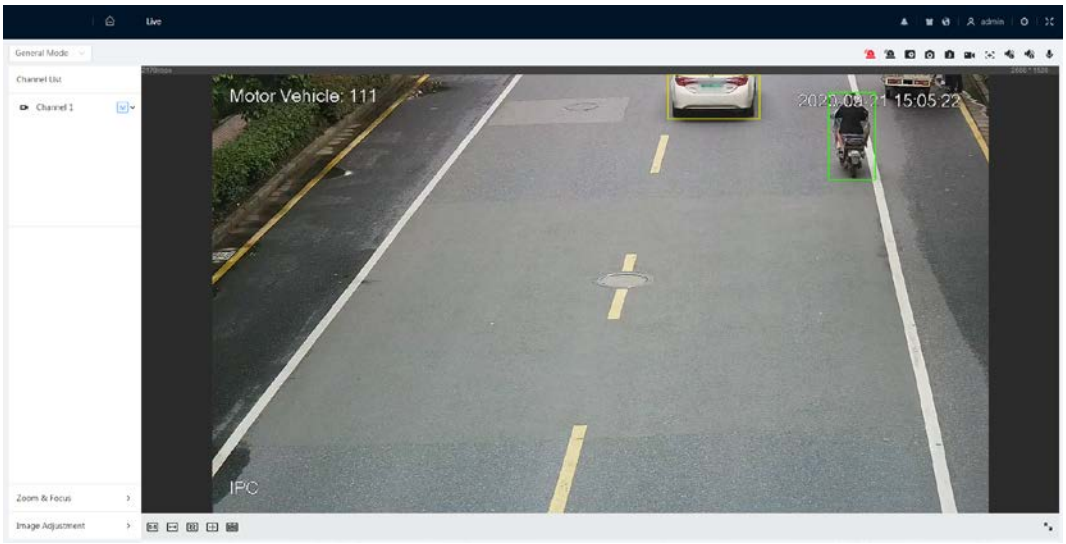
Click **Forget password?**, and you can reset the password through the email address that is set during the initialization. For details, see "4.2 Resetting Password".

Figure 4-1 Login



Step 3 Click **Login**.

Figure 4-2 Live interface



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 "6.6.2.1.2 Resetting Password".

Procedure

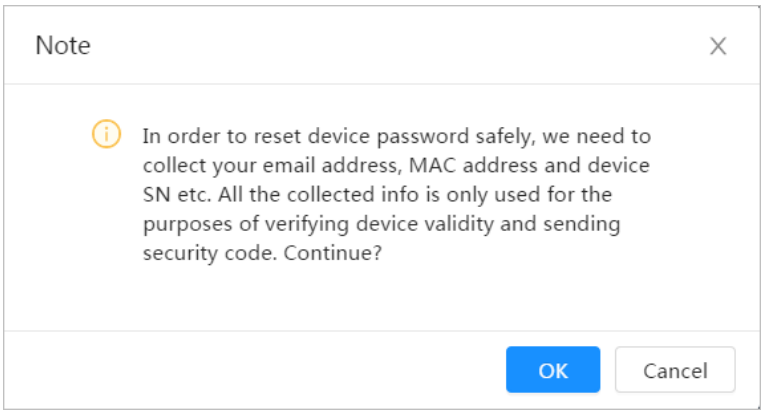
Step 1 Open IE browser, enter the IP address of the device in the address bar and press Enter.

Figure 4-3 Login



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

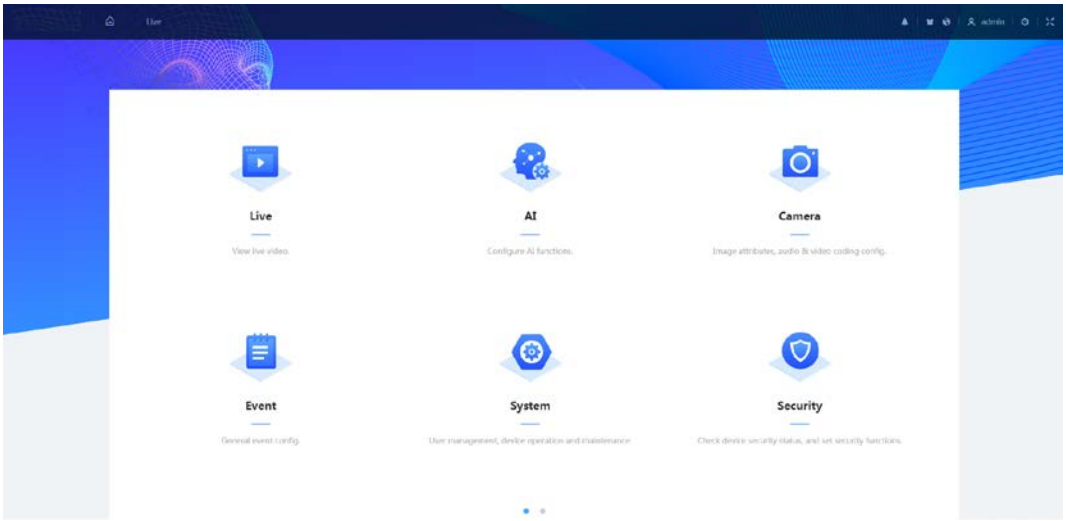
Figure 4-4 Login



5 Main Interface

Click  at the left-upper corner of the interface to display the main interface.

Figure 5-1 Main interface



- Live: View the real-time monitoring image.
- AI: Configure AI functions of the camera.
- Camera: Configure camera parameters, including image parameters, encoder parameters, and audio parameters.
- Event: Configure general events, including alarm linkage exception, video detection, and audio detection.
- Event: Configure system parameters, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.
- Security: Check the device security status and set security functions.
- Record: Play back or download recorded video.
- Picture: Play back or download image files.
- For the camera with multiple channels, through selecting channel numbers, you can set the parameters of the channels.
- Report: Search the AI event report and system report.
- Alarm subscription: Subscribe alarm.
- Skin setting: Set the skin.
- Language setting: Set the language.
- Restart: Click 

at the upper-right corner of the interface, select **Reboot**, and the camera restarts.
- Logout: Click 

at the upper-right corner of the interface, select **Logout** to go to the login interface.
  The system will sleep automatically after idling for a period of time.
- Setting: Click  at the upper-right corner of the interface to set the basic parameters.
- Full screen: Click  at the upper-right corner of the interface to enter full screen mode; click to exit full screen mode.

6 Setting

This section introduces the basic setting of the camera, including the configuration of Local, Camera, Network, Event, Storage, System, System Information and Log.

For **Camera**, **Event** and **System**, you can go to the configuration interface through two methods. This section takes method 1 as an example.

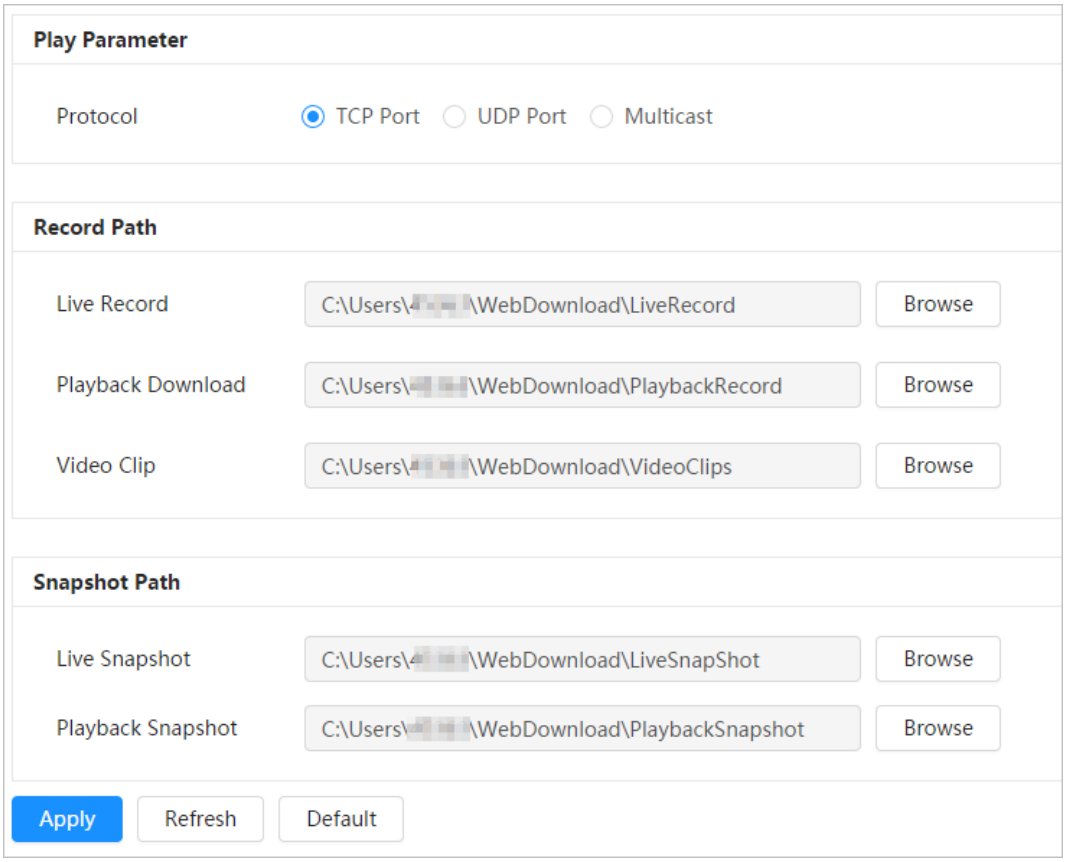
- Method 1: Click , and then select the corresponding item.
- Method 2: Click the corresponding icon on the main interface.

6.1 Local

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

Step 1 Select > **Local**.

Figure 6-1 Local



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

Table 6-1 Description of local parameter

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

Step 3 Click **Save**.

6.2 Camera

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

Camera parameters of different devices might vary.

6.2.1 Setting Image Parameters

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

6.2.1.1 Interface Layout

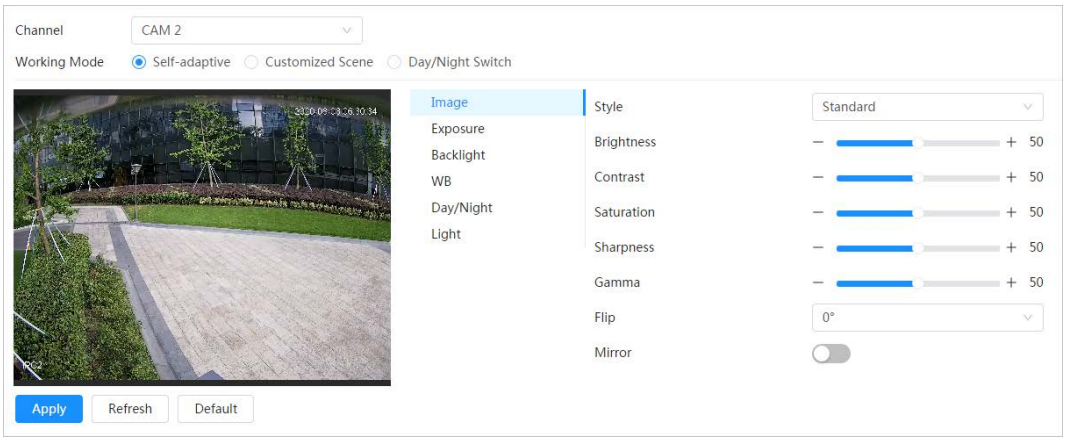
Configure camera parameters to improve the scene clarity, and ensure that surveillance goes properly.

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.

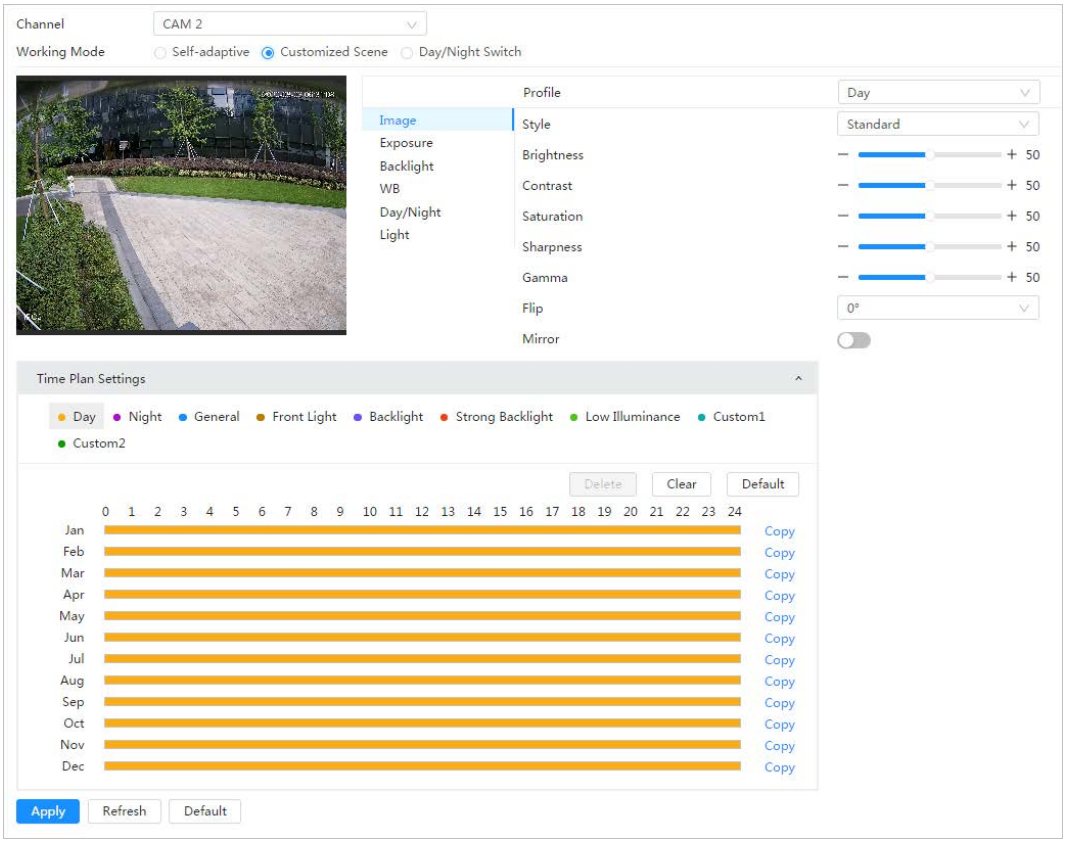
- Self-adaptive: The camera will adjust the image according to the environment.

Figure 6-2 Interface layout (self-adaptive)



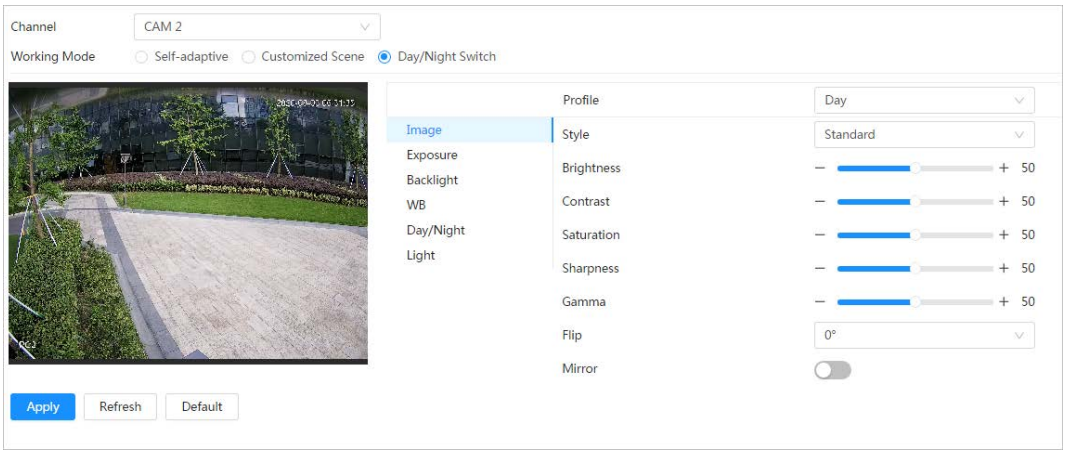
- Customized scene: You can select the profile as needed. Select the profile in **Time Plan Setting** and drag the slide block to set certain time as the selected profile. For example, set 8:00–18:00 as day, and 0:00–8:00 and 18:00–24:00 as night

Figure 6-3 Interface layout (customized scene)



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

Figure 6-4 Interface layout (Day/night switch)

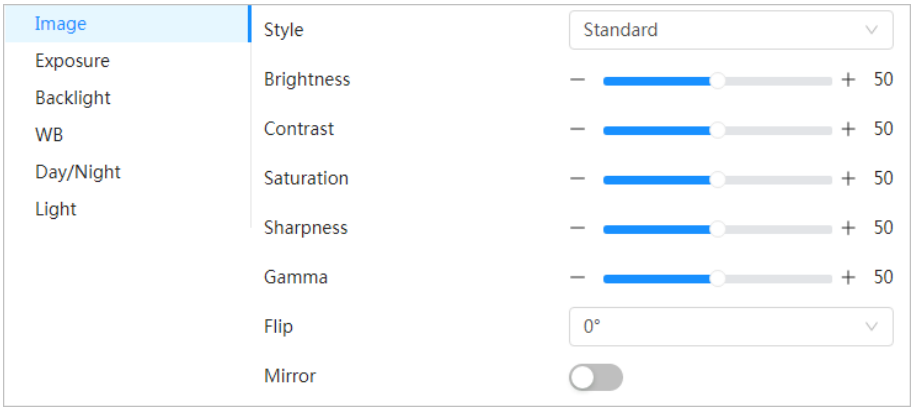


6.2.1.2 Image

You can configure picture parameters as needed.

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

Figure 6-5 Image



Step 2 Configure picture parameters.

Table 6-2 Description of picture parameters

Parameter	Description
Style	Select the picture style from soft, standard and vivid. ● Soft: Default image style, displays the actual color of the image. ● Standard: The hue of the image is weaker than the actual one, and contrast is smaller. ● Vivid: The image is more vivid than the actual one.
Brightness	Changes the value to adjust the picture brightness. The higher the value is, the brighter the picture will be, and the smaller the darker. The picture might be hazy if the value is configured too big.
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 smaller the less. If the value is set too big, the dark area would be too dark and bright area easier to get overexposed. The picture might be hazy if the value is set too small.

Parameter	Description
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 smaller the darker.
Flip	Changes the display direction of the picture, see the options below. • 0°: Normal display. • 90°: The picture rotates 90° clockwise. • 180°: The picture rotates 90° counterclockwise. • 270°: The picture flips upside down. For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "6.2.2 Setting Encode Parameters".
Mirror	Click , and the picture will display with left and right side reversed.

Step 3 Click **Apply**.

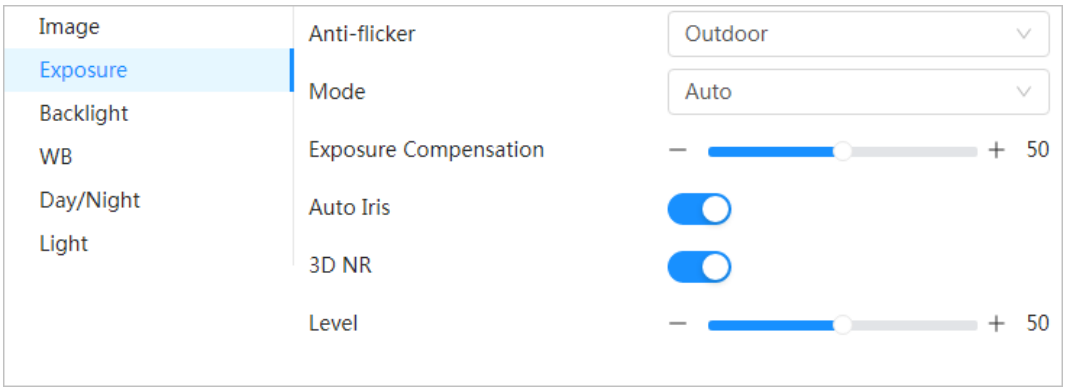
6.2.1.3 Exposure

Configure iris and shutter to improve image clarity.

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

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

Figure 6-6 Exposure



Step 2 Configure exposure parameters.

Table 6-3 Description of exposure parameters

Parameter	Description
Anti-flicker	You can select from 50 Hz, 60 Hz and Outdoor. ● 50 Hz: When the electric supply is 50 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. ● 60 Hz: When the electric supply is 60 Hz, the system adjusts the exposure according to ambient light automatically to ensure that there is no stripe appears. ● Outdoor: You can select any exposure mode as needed.
Mode	Device exposure modes. ● Auto: Adjusts the image brightness according to the actual condition automatically. ● 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. ● 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. ● Manual: Configure gain and shutter value manually to adjust image brightness.  When the **Anti-flicker** is set to **Outdoor**, you can select **Auto**, **Gain priority**, **Shutter priority** or **Manual** in the **Mode** 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 **Gain Priority** or **Manual** in **Mode**, you can set Gain. With minimum illumination, the camera increases Gain automatically to get clearer images.
Auto Iris	This configuration is available only when the camera is equipped with auto-iris lens. ● When auto iris is enabled, the iris size changes automatically according to the ambient lighting condition, and the image brightness changes accordingly. ● When auto iris is disabled, the iris stays at full size and does not change no matter how ambient lighting condition changes.

Parameter	Description
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and latter frames.
Level	This configuration is available only when the 3D NR is enabled. The higher the level is, the better the result will be.

Step 3 Click **Apply**.

6.2.1.4 Backlight

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

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

Figure 6-7 Backlight



Step 2 Configure backlight parameters.

Table 6-4 Description of backlight parameters

Backlight mode	Description
BLC	Enable **BLC**, the camera can get clearer image of the dark areas on the target when shooting against light. You can enable or disable **Customized** mode. • When you enable **Customized** mode, the system auto adjusts exposure only to the set area according to ambient lighting condition to ensure the image of the set area at ideal brightness. • When you disable **Default** mode, the system adjusts exposure according to ambient lighting condition automatically to ensure the clarity of the darkest area.
WDR	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. There might be a few seconds of video loss when the device is switching to WDR mode from other mode.
HLC	Enable **HLC** when extreme strong light is in the environment (such as toll station or parking lot), the camera will dim strong light, and reduce the size of Halo zone to lower the brightness of the whole image, so that the camera can capture human face or car plate detail clearly. The higher the value is, the more obvious the HLC effect will be.

Backlight mode	Description
SSA	Enable **SSA**, the system automatically adjusts the image brightness according to the environment to make the objects in the image clearer.

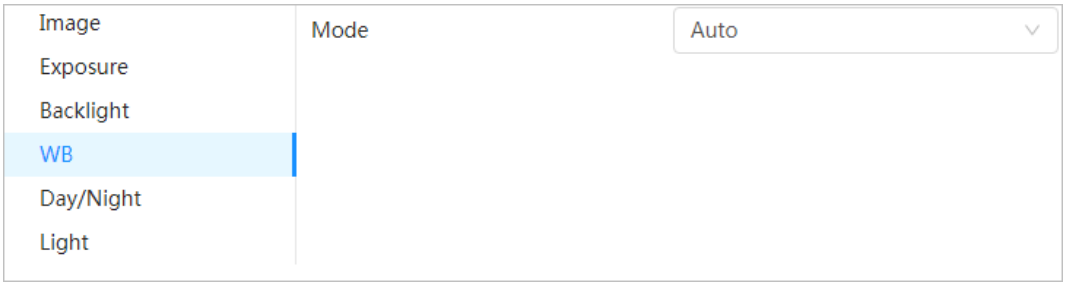
Step 3 Click **Apply**.

6.2.1.5 WB

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

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

Figure 6-8 WB



Step 2 Configure WB parameters.

Table 6-5 Description of WB parameters

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

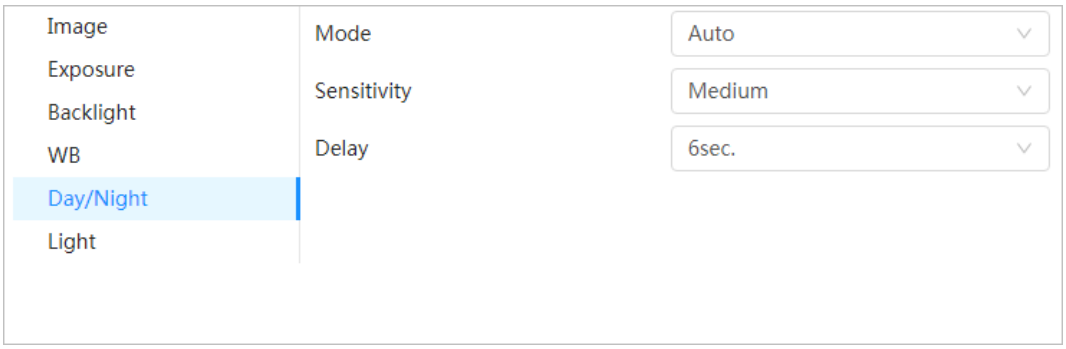
Step 3 Click **Apply**.

6.2.1.6 Day/Night

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

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

Figure 6-9 Day/night



Step 2 Configure day and night parameters.

Table 6-6 Description of day and night parameters

Parameter	Description
Mode	You can select device display mode from **Color**, **Auto**, and **B/W**. Day/Night configuration is independent from profile management configuration. • **Color**: The system displays color image. • **Auto**: The system switches between color and black-and-white display according to the actual condition. • **B/W**: The system displays black-and-white image.
Sensitivity	This configuration is available only when you set **Auto** in **Mode**. You can configure camera sensitivity when switching between color and black-and-white mode.
Delay	This configuration is available only when you set **Auto** in **Mode**. You can configure the delay when camera switching between color and black-and-white mode. The lower the value is, the faster the camera switches between color and black-and-white mode.

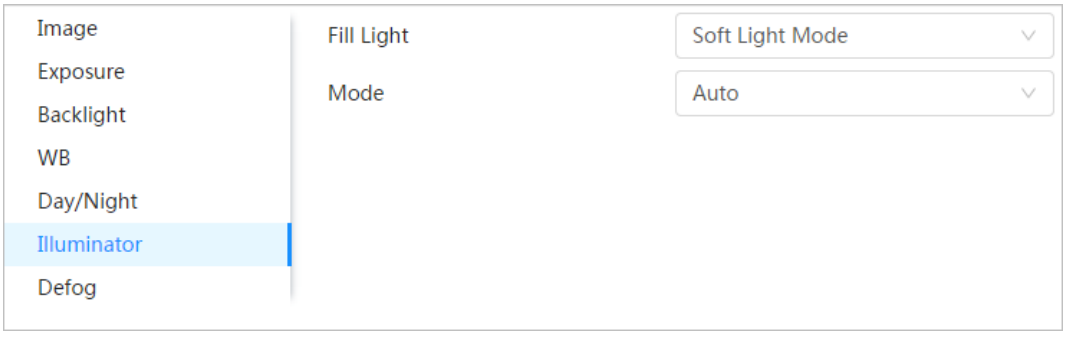
Step 3 Click **Apply**.

6.2.1.7 Illuminator

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

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

Figure 6-10 Light



Step 2 Configure illuminator parameters.

Table 6-7 Description of illuminator parameters

Parameter	Description	
Fill Light	Set **Fill Light** for sound and siren cameras. ● IR Mode: Enable the IR illuminator, and the white light is disabled. When an alarm is triggered, the system will link white light. ● White Light: Enable the white light, and the IR illuminator is disabled. When an alarm is triggered, the system will link white light. ● Soft Light Mode: Enable IR illuminator and white light at the same time, and adjust the brightness of the two illuminators to get clear images.	
Mode	Manual	Adjust the brightness of illuminator manually, and then the system will supply illuminator to the image accordingly.
	Auto	The system adjusts the illuminator intensity according to the ambient lighting condition.
	Zoom Priority	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 then. ● 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 certain wide angle, the system will not turn on high beam light in order to avoid over-exposure in short distance. In the meantime, you can configure light compensation manually to fine-tune IR light intensity.
	Off	Illuminator is off.

Step 3 Click **Apply**.

6.2.1.8 Defog

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

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

Figure 6-11 Light



Step 2 Configure defog parameters.

Table 6-8 Description of defog parameters

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

Step 3 Click **Apply**.

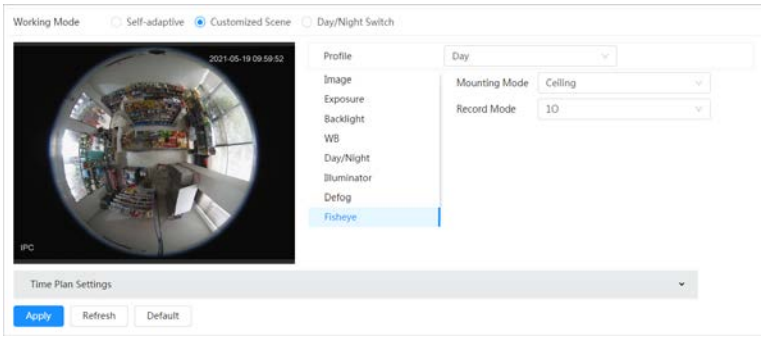
6.2.1.9 Fisheye

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

This function is only available on fisheye device.

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

Figure 6-12 Fisheye



Step 2 Set installation mode and record mode.

Table 6-9 Description of fisheye parameters

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

Parameter	Description
Record Mode	• 1O: The original image before correction. • 1P: 360° rectangular panoramic image. • 2P: When the installation mode is **Ceiling** or **Ground**, you can set this mode. Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. • 1R: Original image screen + independent sub-screen. You can zoom or drag the image in all the screens. • 2R: Original image screen + two independent sub-screens. You can zoom or drag the image in all the screens. • 4R: Original image screen + four independent sub-screens. You can zoom or drag the image in all the screens. • 1O + 3R: Original image screen + three independent sub-screens. You can zoom or drag the image in original image screen, and move the image (upper and lower) in sub-screens to adjust the vertical view.

Step 3 Click **Apply**.

6.2.2 Setting Encode Parameters

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

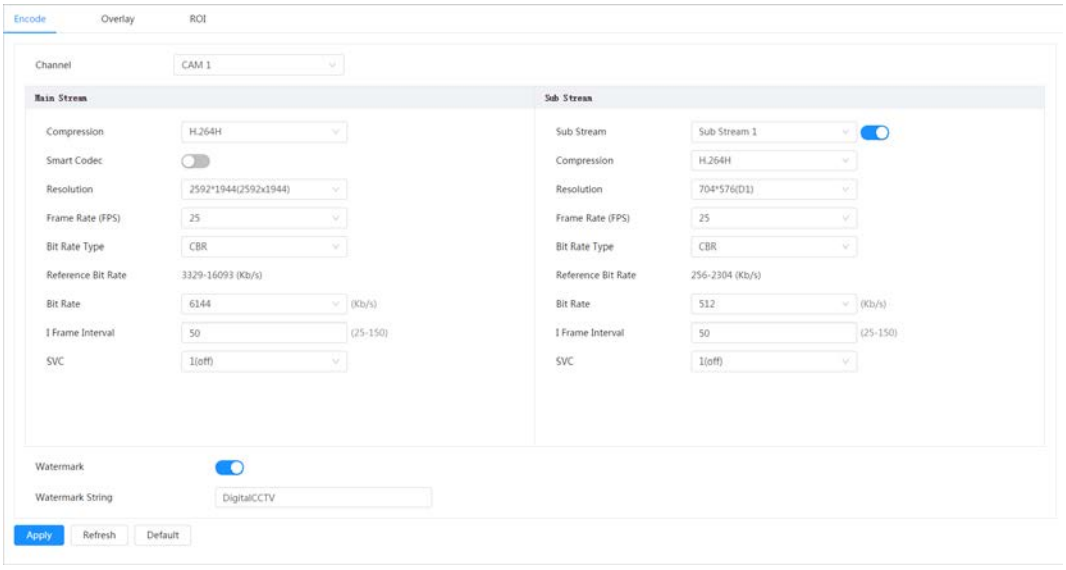
Click **Default**, and the device is restored to default configuration. Click **Refresh** to view the latest configuration.

6.2.2.1 Encode

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

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

Figure 6-13 Encode



Step 2 Configure encode parameters.

Table 6-10 Description of encode parameters

Parameter	Description
Sub Stream	Click to enable sub stream, it is enabled by default. You can enable multiple sub streams simultaneously.
Compression	Select encode mode. • **H.264**: Main profile encode mode. Compared with H.264B, it requires smaller bandwidth. • **H.264H**: High profile encode mode. Compared with H.264, it requires smaller bandwidth. • **H.264B**: Baseline profile encode mode. It requires smaller bandwidth. • **H.265**: Main profile encode mode. Compared with H.264, it requires smaller bandwidth. • **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**.
Smart Codec	Click to enable smart codec to improve video compressibility and save storage space. 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 frame in one second of video. The higher the value is, the clearer and smoother the video will be.
Bit Rate Type	The bit rate control type during video data transmission. You can select bit rate type from: • **CBR** (Constant Bit Rate): The bit rate changes a little and keeps close to the defined bit rate value. • **VBR** (Variable Bit Rate): The bit rate changes as monitoring scene changes. The **Bit Rate Type** can be only be set as **CBR** when **Encode Mode** is set as **MJPEG**.
Quality	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. The better the quality is, but the bigger the required bandwidth will be.
Reference Bit Rate	The most suitable bit rate value range recommended to user according to the defined resolution and frame rate.

Parameter	Description
Max Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
Bit Rate	This parameter can be configured only when the **Bit Rate Type** is set as **CBR**. Select bit rate value in the list according to actual condition.
I Frame Interval	The number of P frames between two I frames, and the **I Frame Interval** range changes as **FPS** changes. It is recommended to set **I Frame Interval** twice as big as **FPS**.
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. ● 1: The default value, which means that there is no layered coding. ● 2, 3 and 4: The lay number that the video stream is packed.
Watermark	You can verify the watermark to check if the video has been tampered.
Watermark String	

Step 3 Click **Apply**.

6.2.2.2 Overlay

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

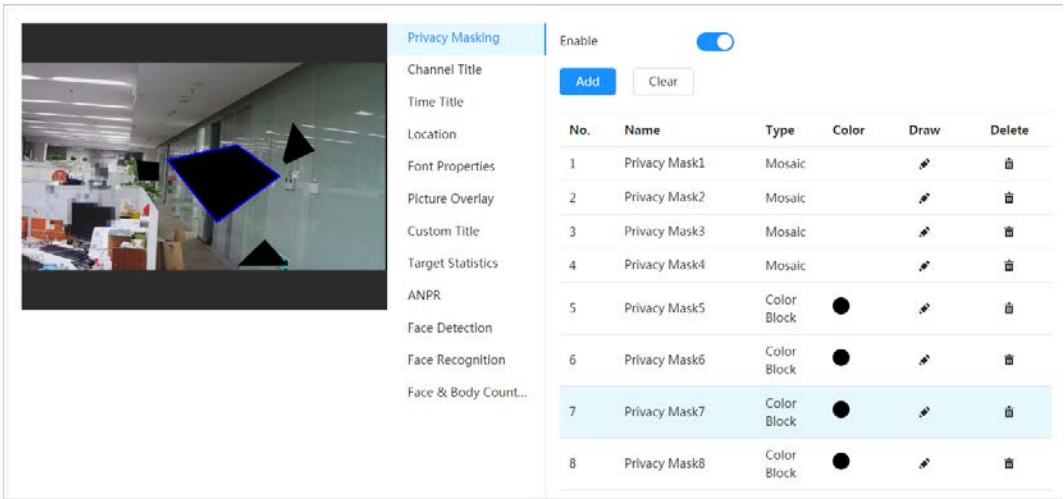
6.2.2.2.1 Configuring Privacy Masking

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

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

Figure 6-14 Privacy masking



Step 2 Configure privacy masking.

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

Related Operations

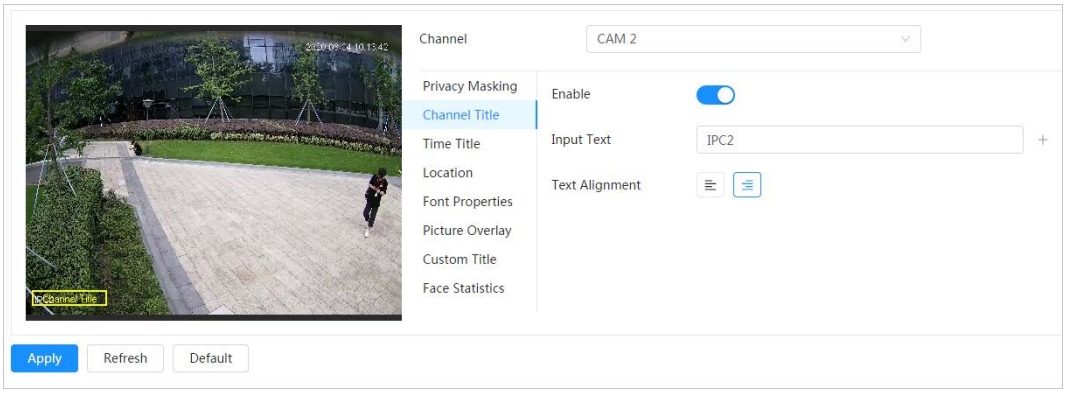
- View and edit the block
  Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame is displayed in the image. You can edit the selected block as needed, including moving the position, and adjusting the size.
- Edit the block name
  Double-click the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

6.2.2.2.2 Configuring Channel Title

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

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

Figure 6-15 Channel title



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

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

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

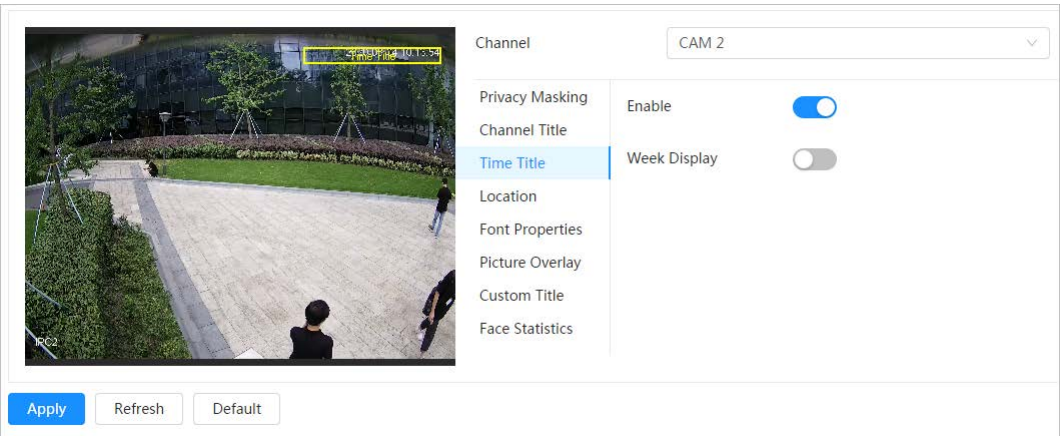
Step 4 Click **Apply**.

6.2.2.2.3 Configuring Time Title

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

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

Figure 6-16 Time title



Step 2 Click next to **Enable**.

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

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

Step 5 Click **Apply**.

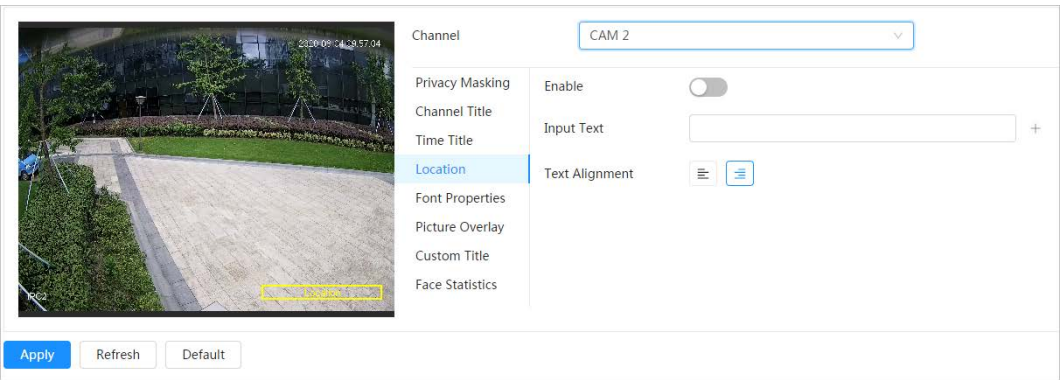
6.2.2.2.4 Configuring Location

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

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

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

Figure 6-17 Location



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

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

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

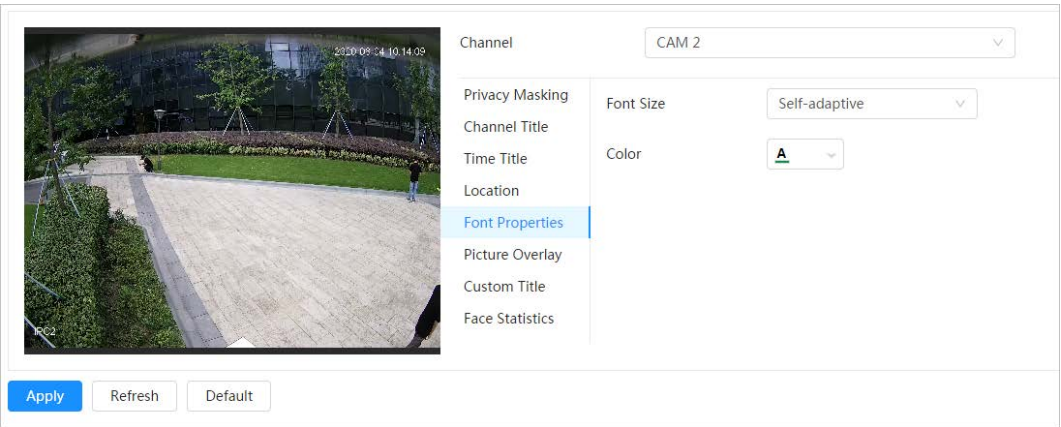
Step 4 Click **Apply**.

6.2.2.2.5 Configuring Font Properties

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

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

Figure 6-18 Font properties



Step 2 Select the font color and size.

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

Step 3 Click **Apply**.

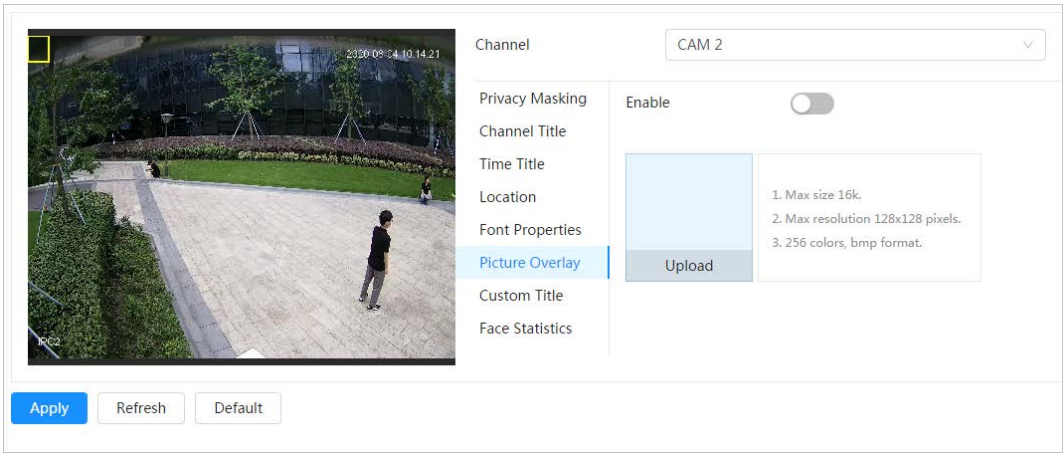
6.2.2.2.6 Configuring Picture Overlay

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

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

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

Figure 6-19 Picture overlay



Step 2 Click next to **Enable**, click **Upload**, and then select the picture to be overlaid.

The picture is displayed on the video image.

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

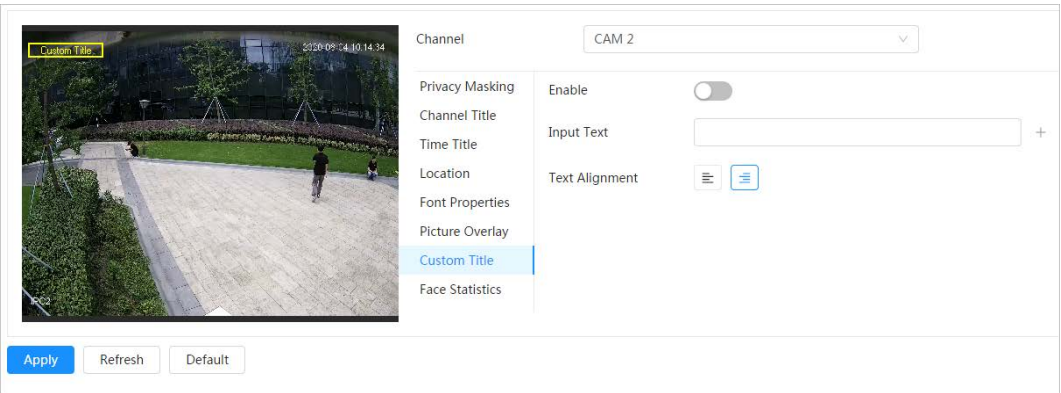
Step 4 Click **Apply**.

6.2.2.2.7 Configuring Custom Title

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

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

Figure 6-20 Custom title



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

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

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

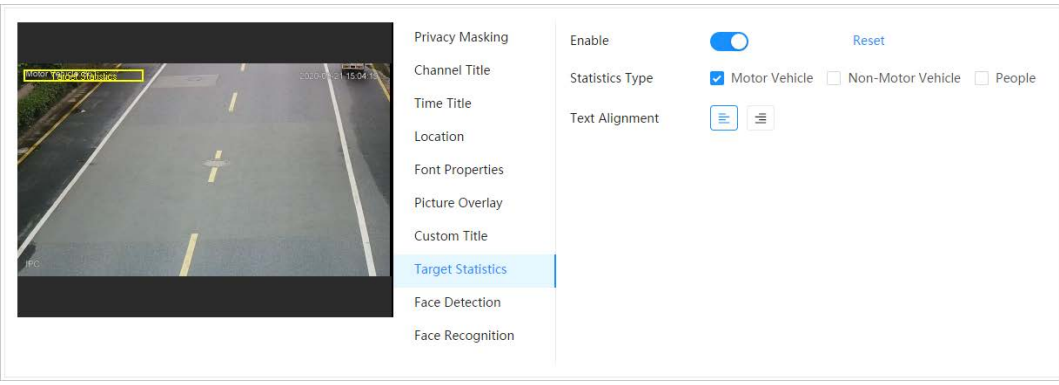
Step 4 Click **Apply**.

6.2.2.2.8 Configuring Target Statistics

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

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

Figure 6-21 Target statistics



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

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

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

Step 4 Click **Apply**.

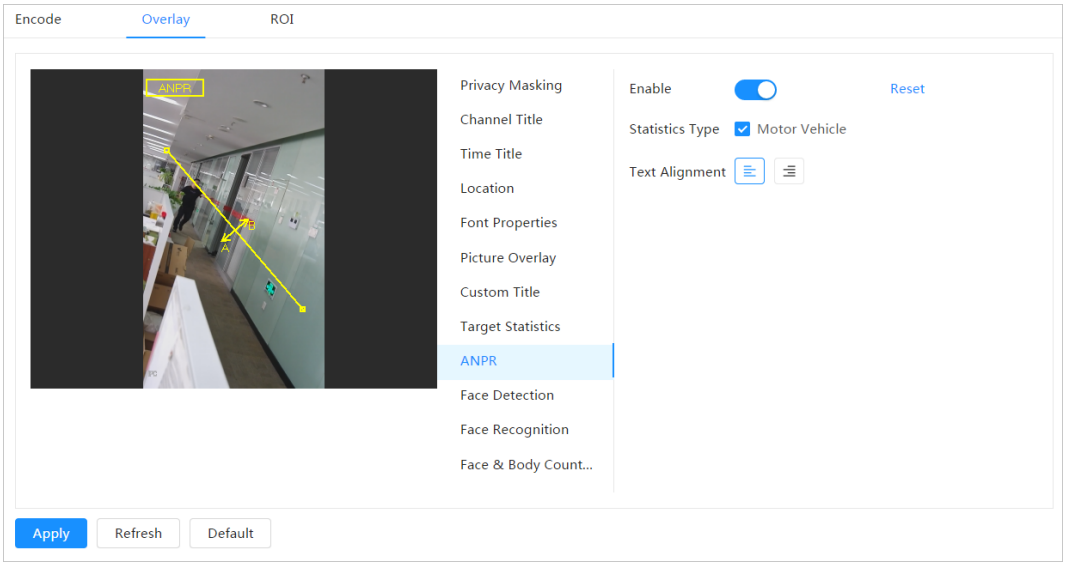
The overlaid information will be displayed after enabling video metadata function.

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.

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

Figure 6-22 ANPR



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

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

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

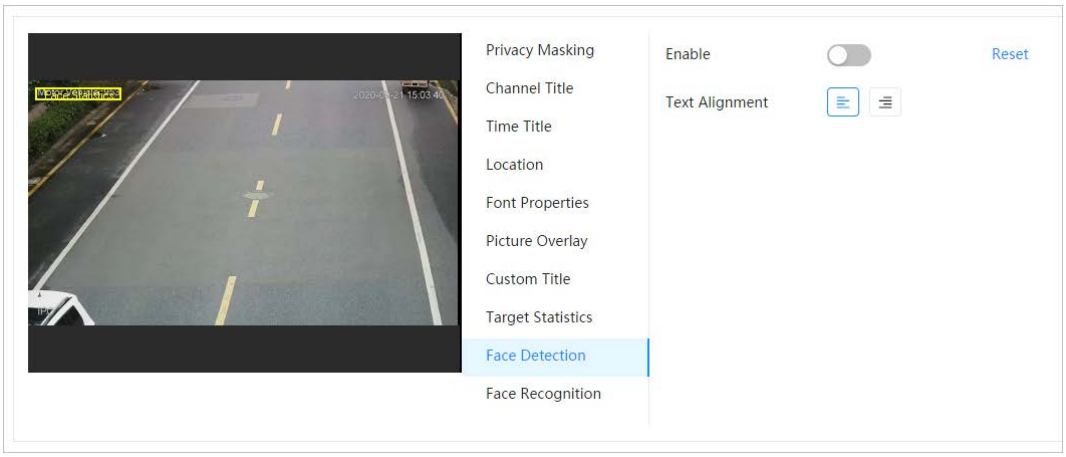
Step 4 Click **Apply**.

6.2.2.2.10 Configuring Face Detection

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

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

Figure 6-23 Face detection



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

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

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

Step 4 Click **Apply**.

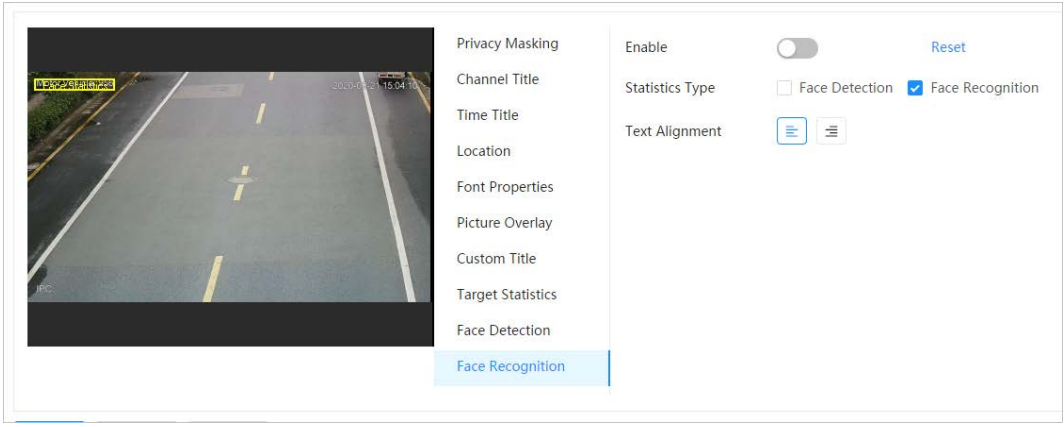
The information will be displayed on the image after the face detection function is enabled.

6.2.2.2.11 Configuring Face 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.

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

Figure 6-24 Face recognition



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

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

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

Step 4 Click **Apply**.

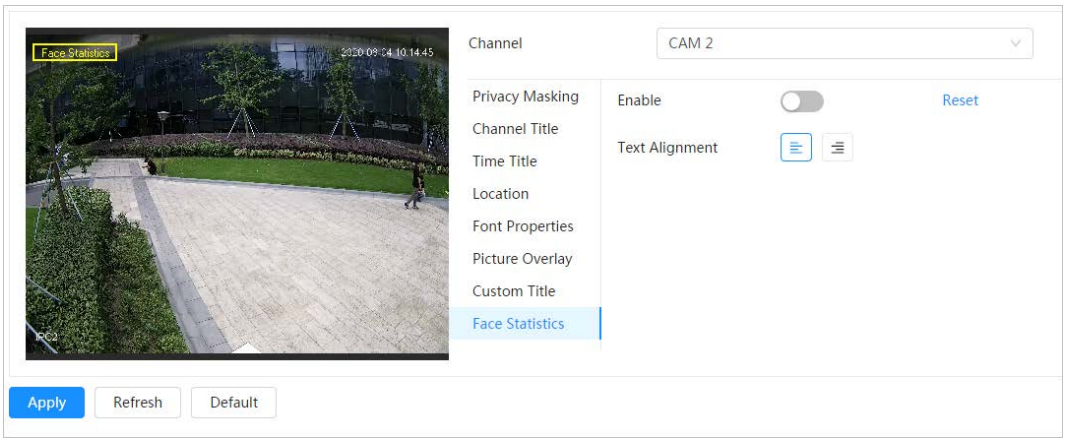
The information will be displayed on the image after the face recognition function is enabled.

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.

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

Figure 6-25 Face statistics



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

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

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

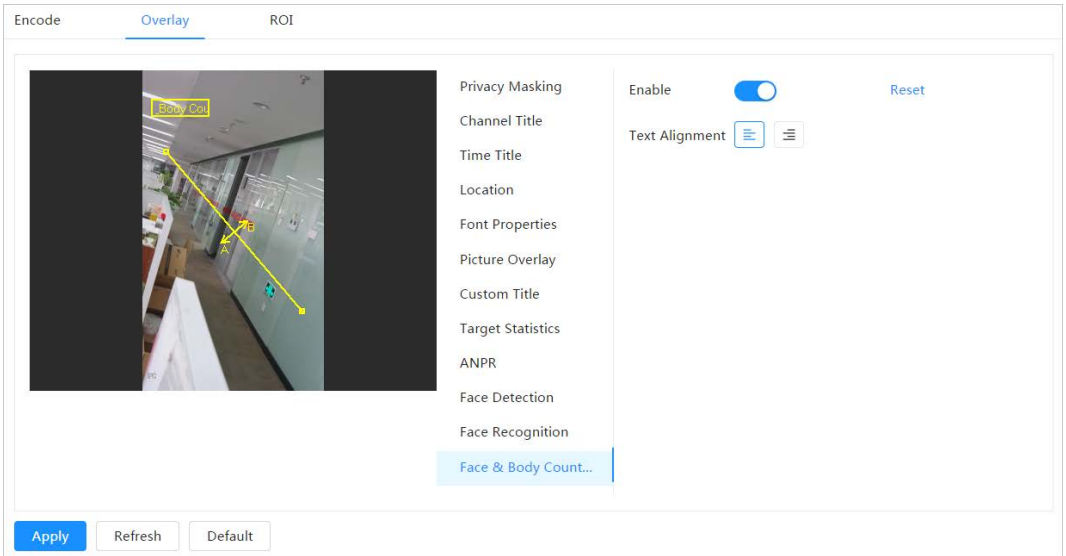
Step 4 Click **Apply**.

6.2.2.2.13 Configure Face&Body Counting

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

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

Figure 6-26 Face&body counting



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

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

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

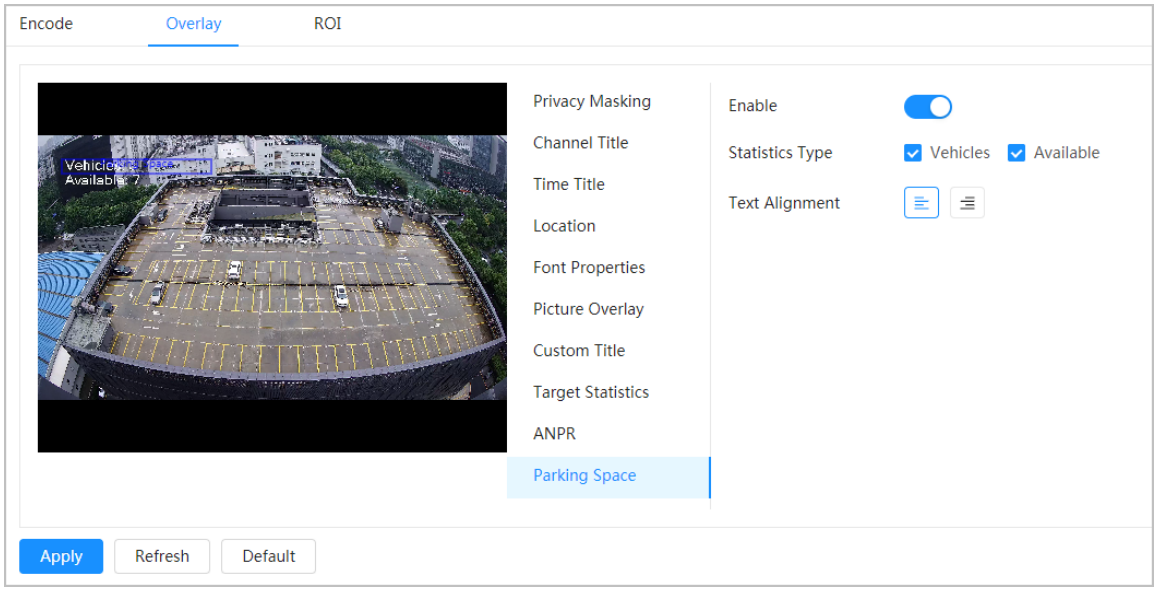
Step 4 Click **Apply**.

6.2.2.2.14 Configuring Parking Space

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

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

Figure 6-27 Parking space



Step 2 Select the **Enable** check box.

Step 3 Select statistic type and text alignment.

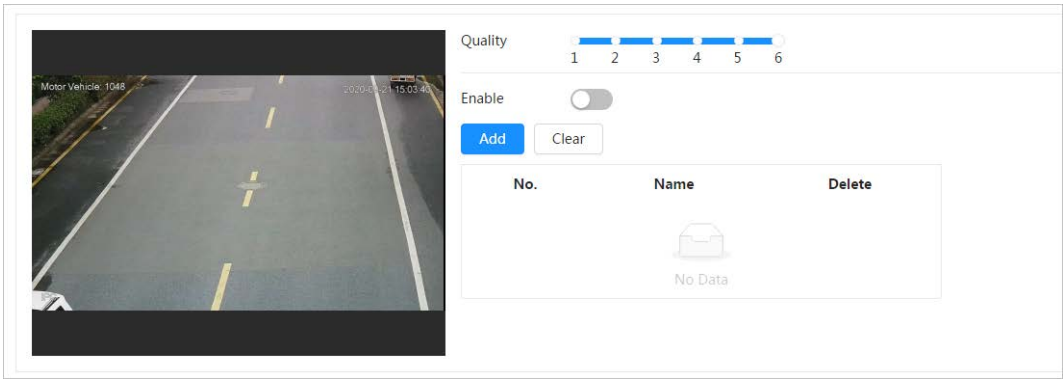
Step 4 Click **Apply**.

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.

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

Figure 6-28 ROI



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

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

Step 3 Click **Apply**.

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

6.2.3 Audio

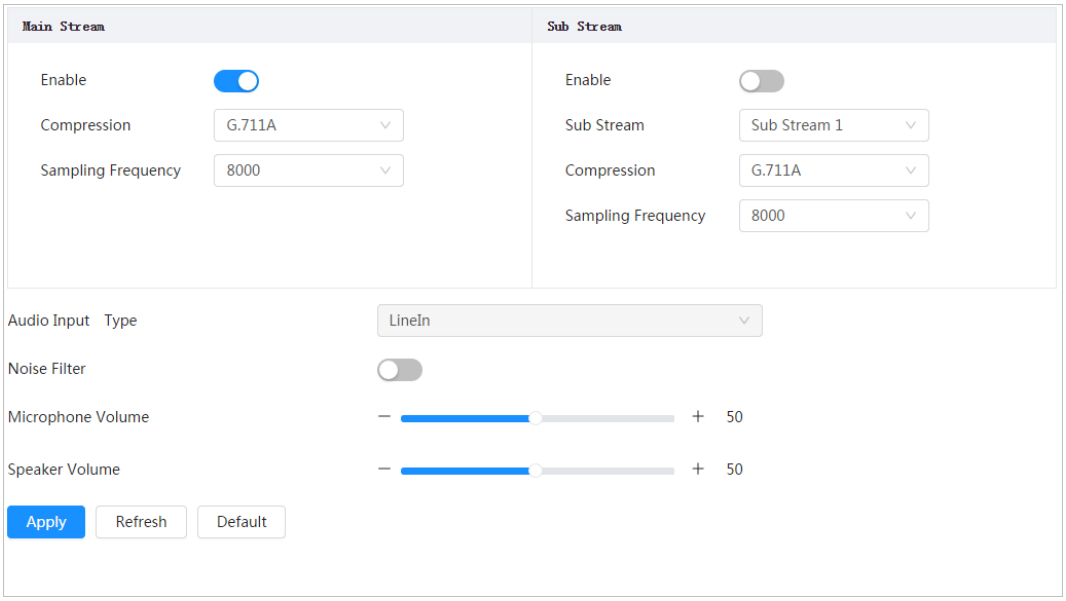
You can configure audio parameters and alarm audio.

6.2.3.1 Setting Audio Parameters

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

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

Figure 6-29 Audio



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

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

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

Step 3 Configure audio parameters.

Table 6-11 Description of audio parameters

Parameter	Description
Compression	You can select audio **Encode Mode** from **PCM**, **G.711A**, **G.711Mu**, **G.726**, **AAC**, **G.723**. The configured audio encode mode applies to both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, the more the sample in a second will be, and the more accuracy the restored signal will be. You can select audio **Sampling Frequency** from **8000**, **16000**, **32000**, **48000**, **64000**.

Parameter	Description
Audio Input Type	You can select audio input type from: • **LineIn**: 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.

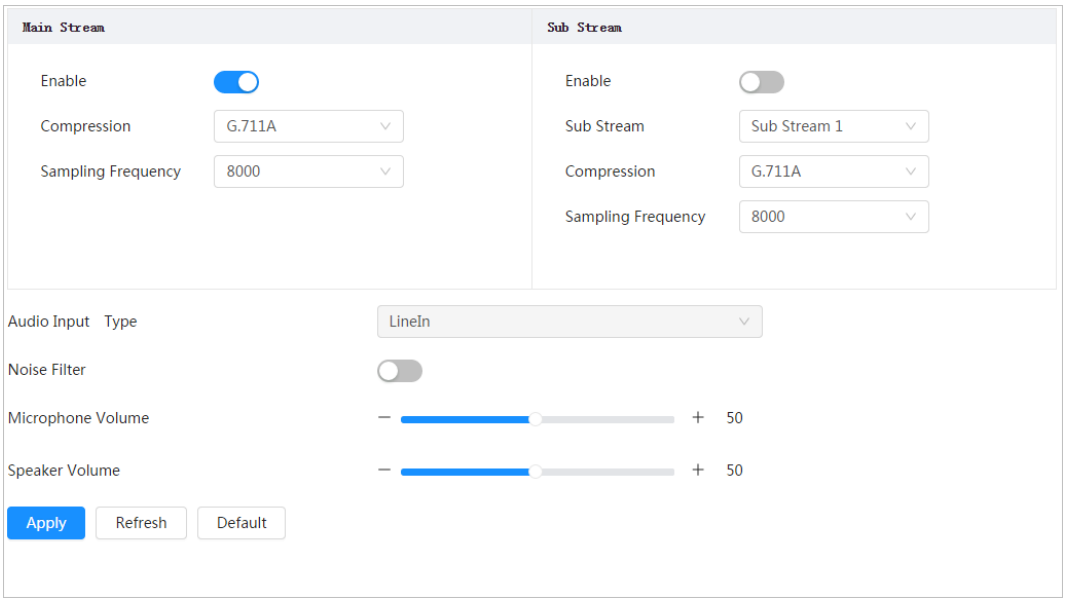
Step 4 Click **Apply**.

6.2.3.2 Setting Alarm Tone

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

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

Figure 6-30 Audio tone



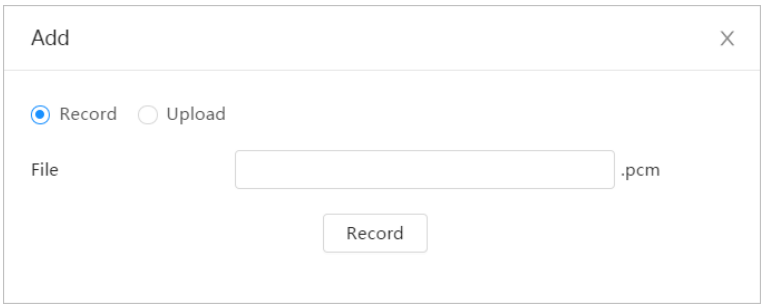
Step 2 Click **Add**.

Step 3 Configure the audio file.

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

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

Figure 6-31 Add alarm tone



Step 4 Select the file that you need.

Related Operations

- Edit audio file

  Click to edit the file name.
- Delete audio file

  Click to delete the file name.
- Play audio file

  Click to play the file name.
- Download audio file

  Click to download the file name.

6.3 Network

This section introduces network configuration.

6.3.1 TCP/IP

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

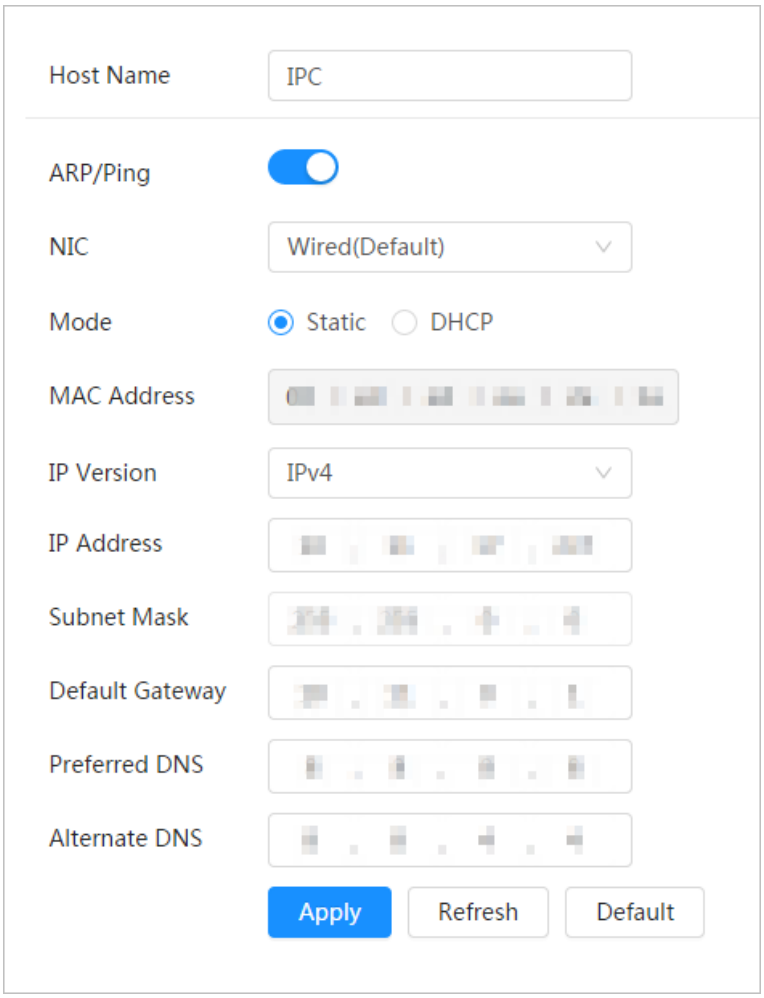
Prerequisites

The camera has connected to the network.

Procedure

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

Figure 6-32 TCP/IP



Step 2 Configure TCP/IP parameters.

Table 6-12 Description of TCP/IP parameters

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

Parameter	Description
ARP/Ping	Click to enable ARP/Ping to set IP address service. Get the camera MAC address, and then you can change and configure the device IP address with ARP/ping command. This is enabled by default. During restart, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configured with ping packet. **A demonstration of configuring IP address with ARP/Ping.** 1. Keep the camera that needs to be configured and the PC within the same local network, and then get a usable IP address. 2. Get the MAC address of the camera from device label. 3. Open command editor on the PC and enter the following command. Windows syntax arp –s <IP Address> <MAC> ping –l 480 –t <IP Address> Windows example 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> ping –s 480 <IP Address> UNIX/Linux/Mac example arp -s 192.168.0.125 11-40-8c-18-10-11 ping -s 480 192.168.0.125 4. Restart the camera. 5. Check the PC command line, if information such as **Reply from 192.168.0.125…**is displayed, the configuration succeeds, and you can turn it off then. 6. Enter http://(IP address) in the browser address bar to log in.
NIC	Select the Ethernet card that need to be configured, and the default one is **Wire**.
Mode	The mode that the camera gets IP: • **Static** Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login interface with the configured IP address is displayed. • **DHCP** When there is DHCP server in the network, select **DHCP**, 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 **Static** in **Mode**, enter the IP address and subnet mask that you need. ● IPv6 does not have subnet mask. ● The default gateway must be in the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

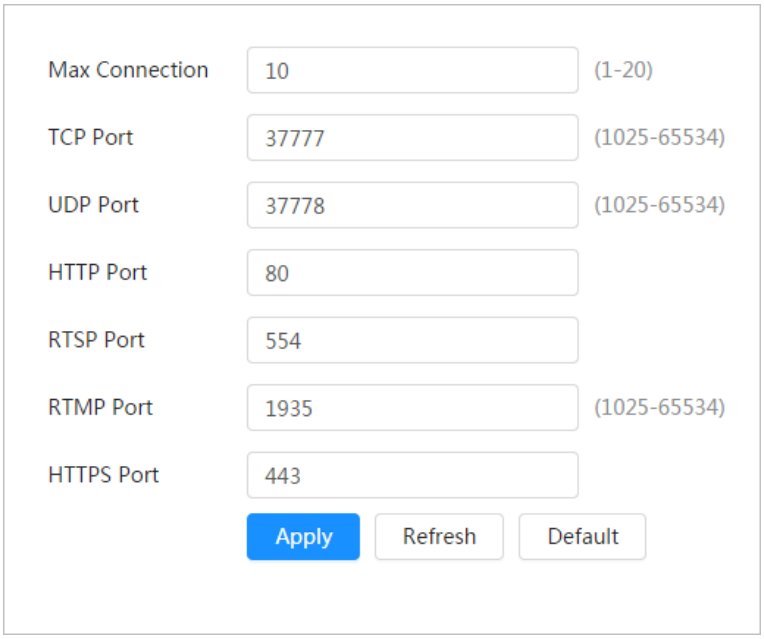
Step 3 Click **Apply**.

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.

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

Figure 6-33 Port



Step 2 Configure port parameters.

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

Table 6-13 Description of port parameters

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.

Parameter	Description
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	● Real time streaming protocol port, and the value is 554 by default. If you play live view with QuickTime, VLC or Blackberry smart phone, the following URL format is available. ● When the URL format requiring RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. ● When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF. URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 Among that: ● Username: The username, such as admin. ● Password: The password, such as admin. ● IP: The device IP, such as 192.168.1.112. ● Port: Leave it if the value is 554 by default. ● Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. ● Subtype: The bit stream type; 0 means main stream (Subtype=0) and 1 means sub stream (Subtype=1). Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: 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.

6.3.3 PPPoE

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

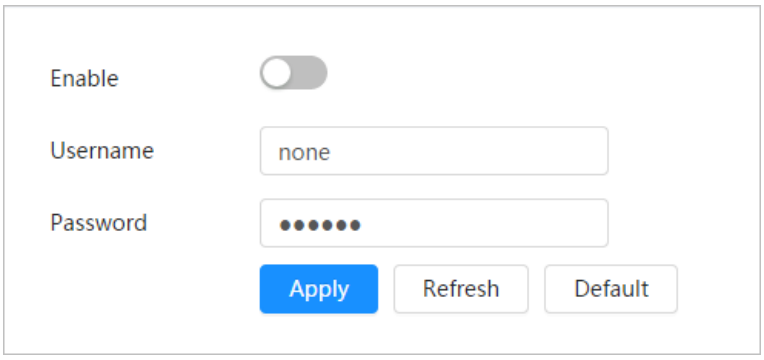
Prerequisites

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

Procedure

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

Figure 6-34 PPPoE



Step 2 Click , and then enter username and password.

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

Step 3 Click **Apply**.

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

6.3.4 DDNS

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

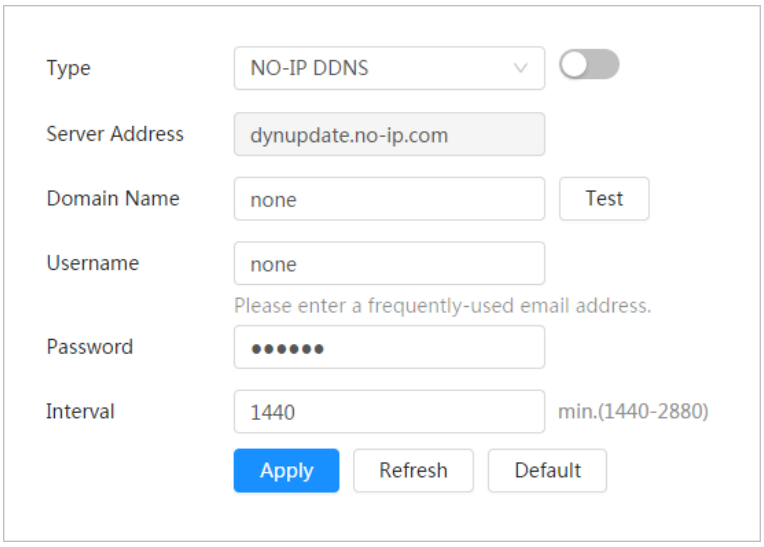
Prerequisites

Check the type of DNS server supported by the camera.

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

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

Figure 6-35 DDNS



Step 2 Click to enable the function.

Step 3 Configure DDNS parameters.

Table 6-14 Description of DDNS parameters

Parameter	Description
Type	The name and web address of the DDNS service provider, see the matching relationship below: ● CN99 DDNS web address: www.3322.org ● NO-IP DDNS web address: dynupdate.no-ip.com ● Dyndns DDNS web address: members.dyndns.org
Server Address	
Domain Name	The domain name you registered on the DDNS website.
Test	Only when selecting **NO-IP DDNS** type, you can click **Test** to check whether the domain name registration is successful.
Username	Enter the username and password that you got from the DDNS server provider. You need to register an account (includes username and password) on the DDNS server provider's website.
Password	
Interval	The update cycle of the connection between the device and the server, and the time is 10 minutes by default.

Step 4 Click **Apply**.

Result

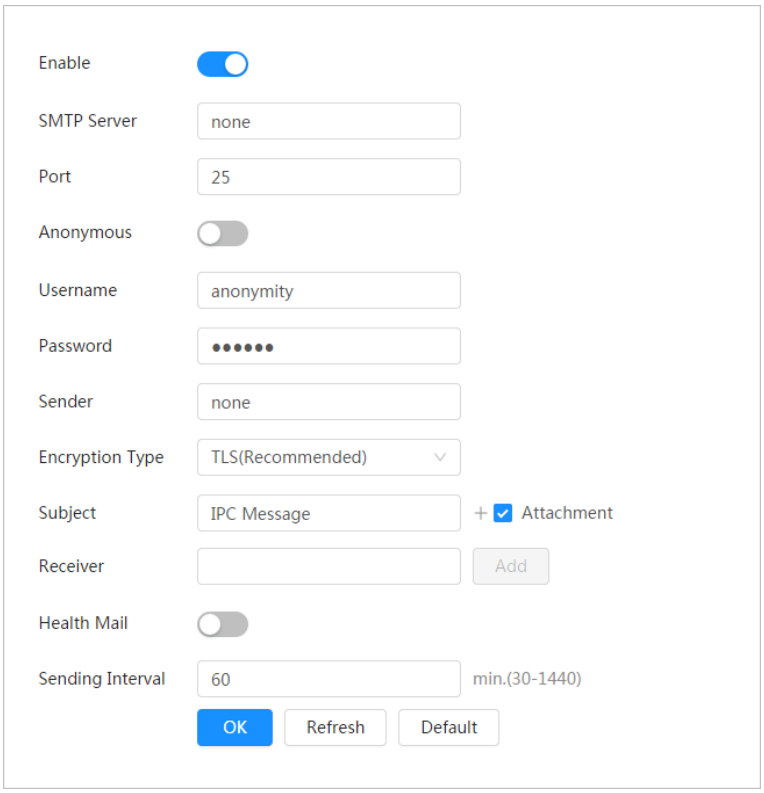
Open the browser on PC, then enter the domain name at the address bar and press **Enter**, the login interface is displayed.

6.3.5 Email

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

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

Figure 6-36 Email



Step 2 Click to enable the function.

Step 3 Configure email parameters.

Table 6-15 Description of email parameters

Parameter	Description	
SMTP Server	SMTP server address	For details, see Table 6-16.
Port	The port number of the SMTP server.	
Username	The account of SMTP server.	
Password	The password of SMTP server.	
Anonymous	Click , and the sender's information is not displayed in the email.	
Sender	Sender's email address.	
Encryption Type	Select from **None**, **SSL** and **TLS**. For details, see Table 6-16.	
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numerals. Click to select title type, including **Device Name**, **Device ID**, and **Event Type**, and you can set maximum 2 titles.	
Attachment	Select the check box to support attachment in the email.	
Receiver	• Receiver's email address. Supports 3 addresses at most. • After entering the receiver's email address, the **Test** button is display. Click **Test** to test whether the emails can be sent and received successfully.	

Parameter	Description
Health Mail	The system sends test mail to check if the connection is successfully configured. Click and configure the **Sending Interval**, and then the system sends test mail as the set interval.

For the configuration of major mailboxes, see Table 6-16.

Table 6-16 Description of major mailbox configuration

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

Step 4 Click **Apply**.

6.3.6 UPnP

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

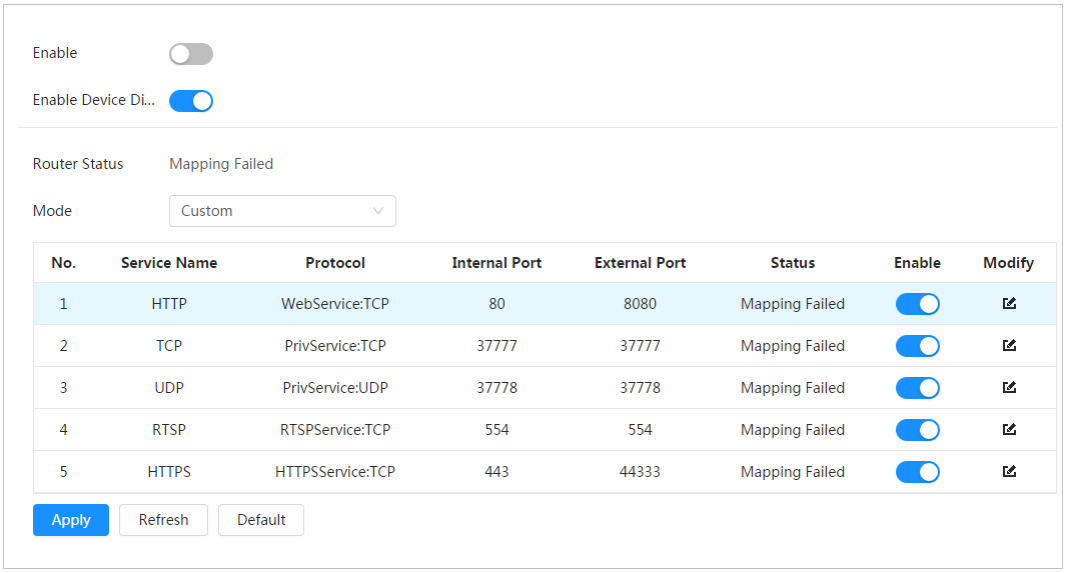
Prerequisites

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

Procedure

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

Figure 6-37 UPnP



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

- Select **Custom**, click and then you can change external port as needed.
- Select **Default**, and then the system finishes mapping with unoccupied port

automatically, and you cannot edit mapping relation.

Step 3 Click **Apply**.

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

6.3.7 SNMP

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

Prerequisites

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

Procedure

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

Figure 6-38 SNMP (1)

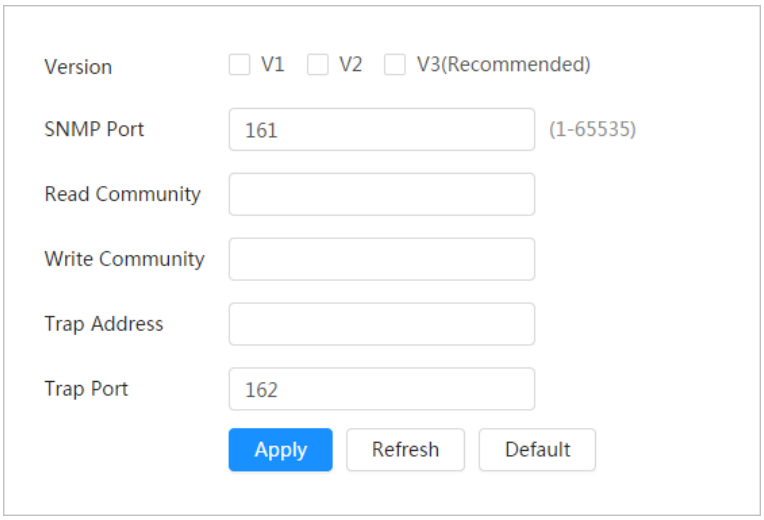
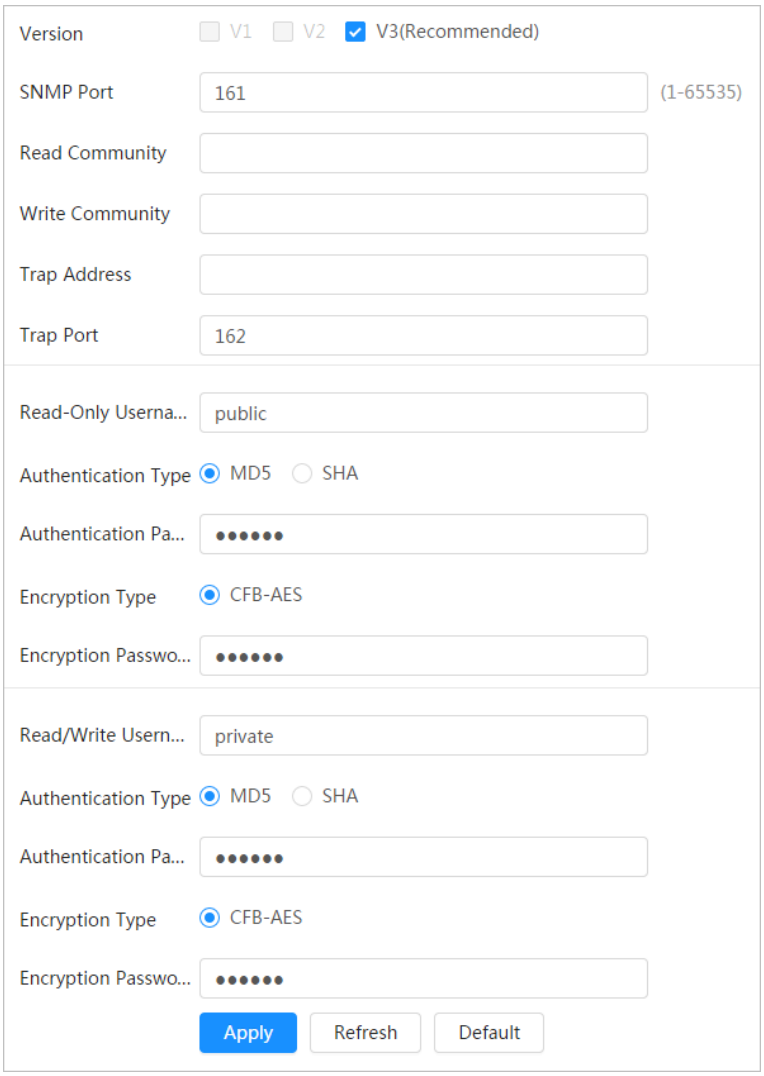


Figure 6-39 SNMP (2)



Step 2 Select SNMP version to enable SNMP.

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

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

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

Table 6-17 Description of SNMP parameters

Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports. You can enter number, letter, underline and dash to form the name.

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

Step 4 Click **Apply**.

Result

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

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

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

6.3.8 Bonjour

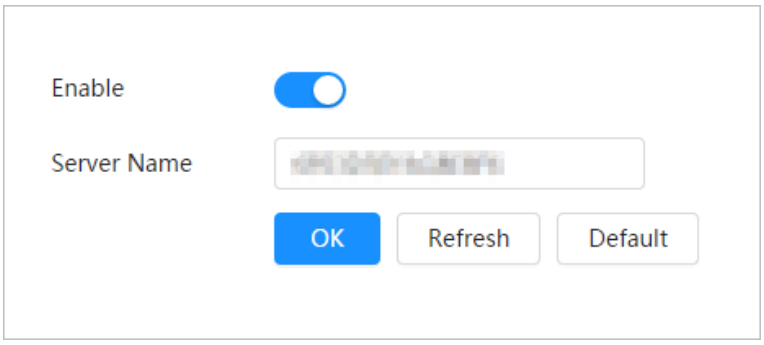
Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser.

Bonjour is enabled by default.

Procedure

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

Figure 6-40 Bonjour



Step 2 Click , and then configure server name.

Step 3 Click **Apply**.

Result

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

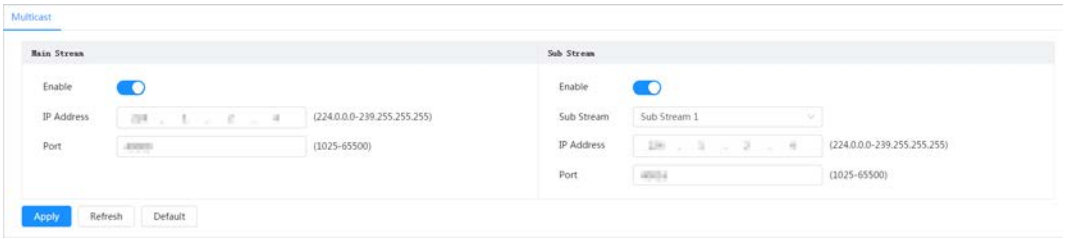
1. Click **Show All Bookmarks** in Safari.
2. Enable **Bonjour**. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click the camera to visit the corresponding web interface.

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.

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

Figure 6-41 Multicast



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

Table 6-18 Description of multicast parameters

Parameter	Description
Multicast Address	The multicast IP address of **Main Stream**/**Sub Stream** is 224.1.2.4 by default, and the range is 224.0.0.0–239.255.255.255.
Port	The multicast port of corresponding stream: **Main Stream**: 40000; **Sub Stream1**: 40016; **Sub Stream2**: 40032, and all the range is 1025–65500.

Step 3 Click **Apply**.

Result

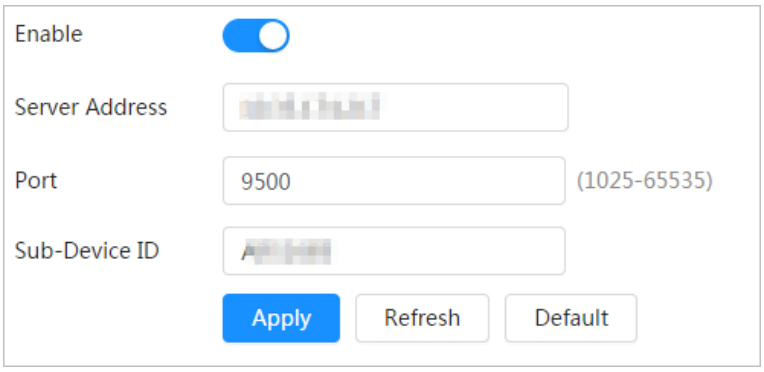
On the **Live** interface, select **RTSP** in **Multicast**, and then you can view the video image with multicast protocol.

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.

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

Figure 6-42 Register



Step 2 Click , and then configure server name.

Table 6-19 Description of register parameters

Parameter	Description
Server Address	The IP address or domain name of the server to be registered.
Port	The port for registration.
Sub-Device ID	The custom ID for the camera.

Step 3 Click **Apply**.

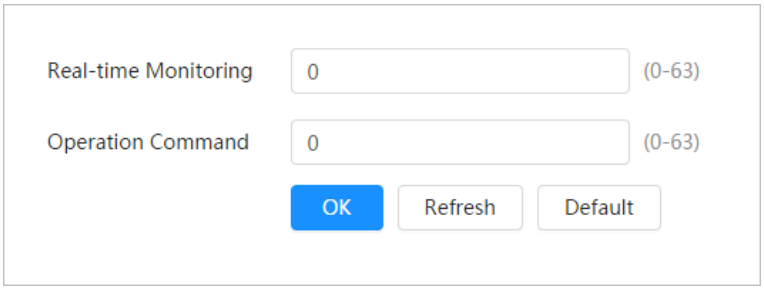
6.3.11 QoS

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

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

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

Figure 6-43 QoS



Step 2 Configure QoS parameters.

Table 6-20 Description of QoS parameters

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

Parameter	Description
Command	Configure the priority of the data packets that used for configure or checking.

Step 3 Click **Save**.

6.3.12 Platform Access

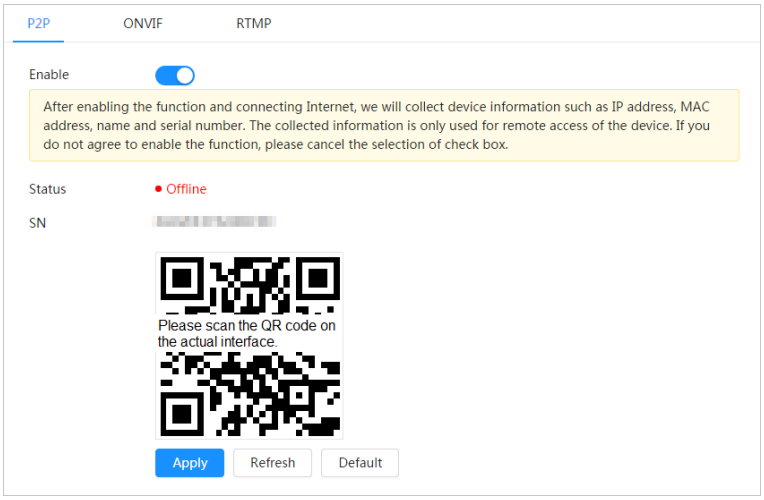
6.3.12.1 P2P

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

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

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

Figure 6-44 P2P



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

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

Step 3 Tap + at the upper-right corner.

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

Step 5 Follow the instructions to finish the settings.

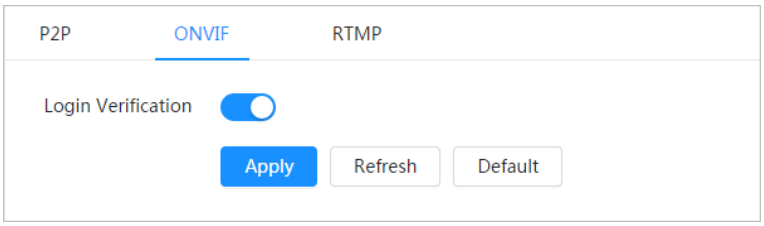
6.3.12.2 ONVIF

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

ONVIF is enabled by default.

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

Figure 6-45 ONVIF



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

Step 3 Click **Apply**.

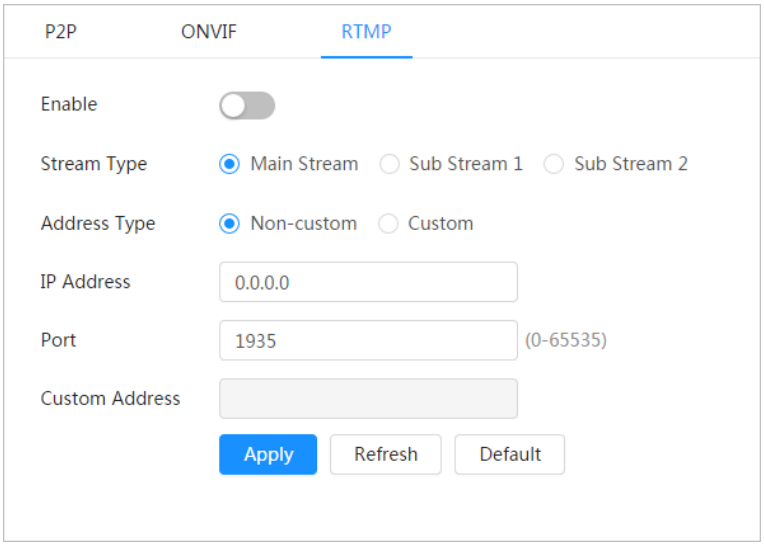
6.3.12.3 RTMP

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

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

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

Figure 6-46 RTMP



Step 2 Click .

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

Step 3 Configure RTMP parameters.

Table 6-21 Description of RTMP parameters

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B and H.264H, and the audio format is AAC.
Address Type	• **Non-custom**: Enter the server IP and domain name. • **Custom**: Enter the path allocated by the server.
IP Address	When selecting **Non-custom**, you need to enter server IP address

Parameter	Description
Port	and port. • **IP address**: Support IPv4 or domain name. • **Port**: Keep the default value.
Custom Address	When selecting **Custom**, you need to enter the path allocated by the server.

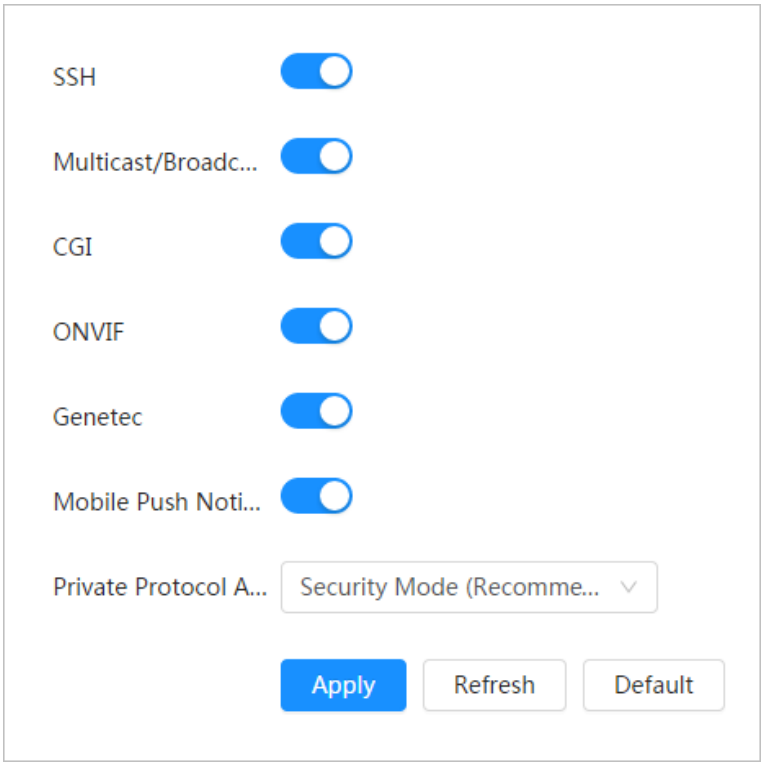
Step 4 Click **Apply**.

6.3.13 Basic Service

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

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

Figure 6-47 Basic service



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

Table 6-22 Description of basic service parameters

Function	Description
SSH	You can enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Enable this function, and then when multiple users are viewing the device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
CGI	Enable the function, and then other devices can access through this service. The function is enabled by default.
Onvif	
Genetec	

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

Step 3 Click **Apply**.

6.4 Event

6.4.1 Setting Alarm Linkage

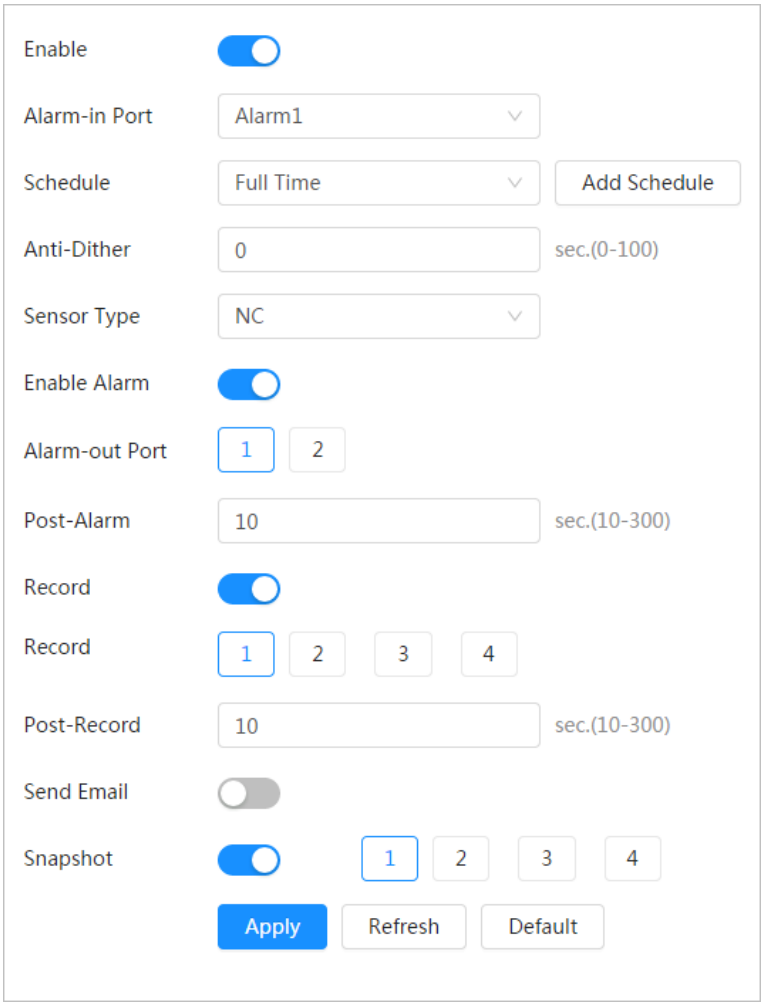
6.4.1.1 Setting Alarm-in

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

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

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

Figure 6-48 Alarm linkage



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

- Sensor Type: NO or NC.

- Anti-Dither: Only record one alarm event during the anti-dither period.

Step 4 Select the schedule and arming periods and alarm linkage action. If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add new schedule. For details, see "6.4.1.2.1 Adding Schedule".

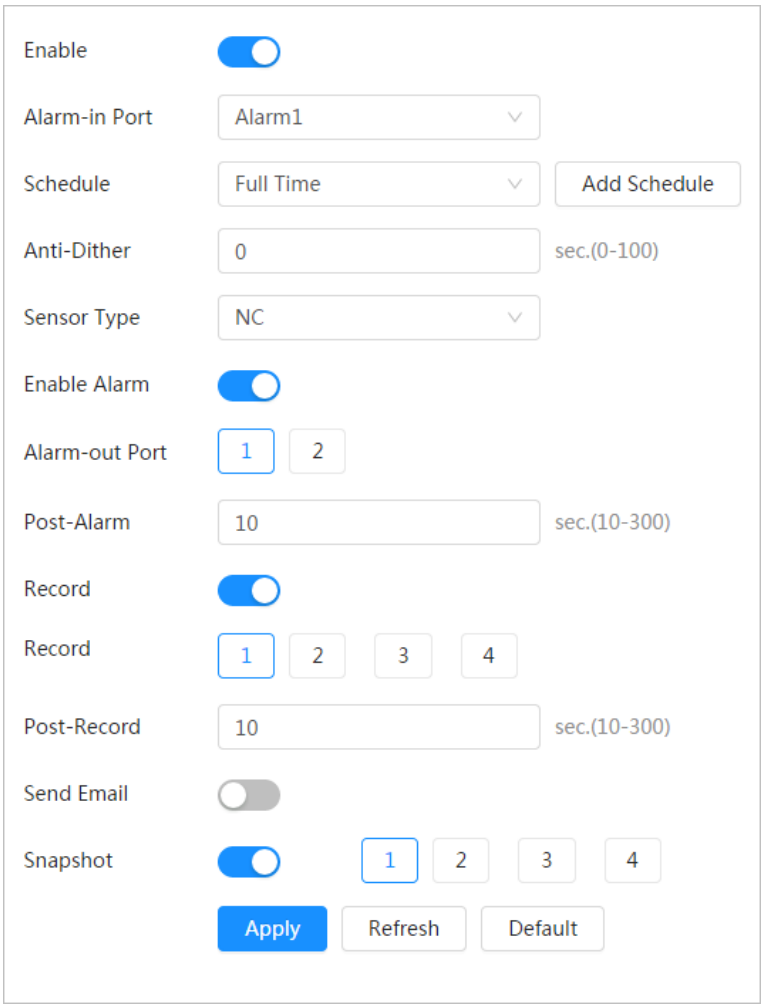
Step 5 Click **Apply**.

6.4.1.2 Alarm Linkage

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

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

Figure 6-49 Alarm linkage

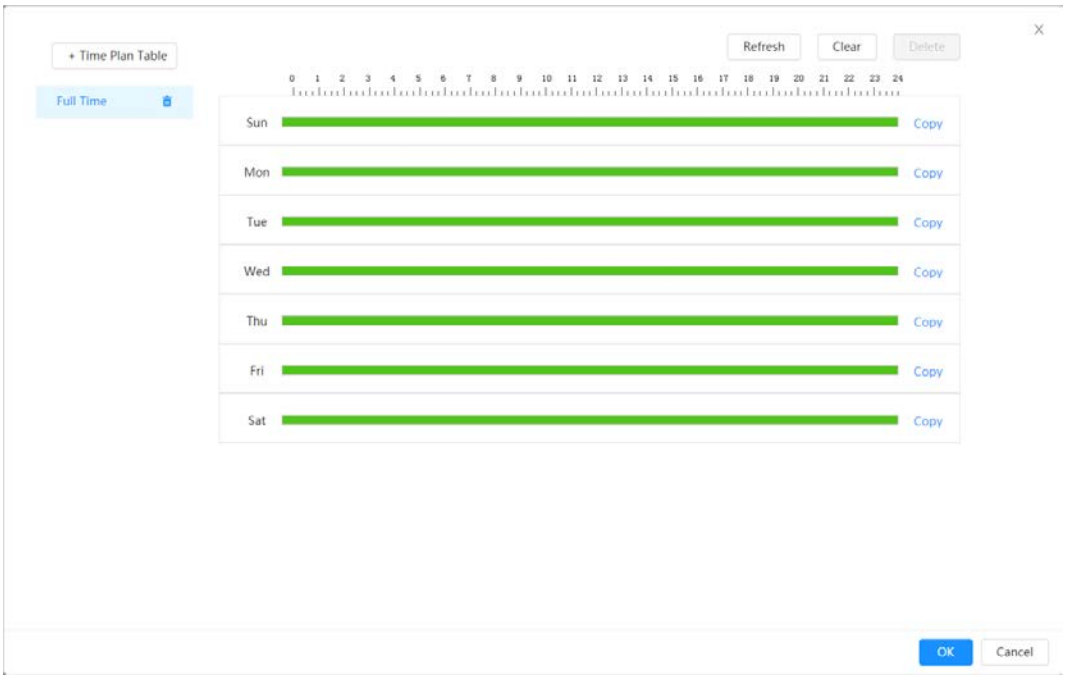


6.4.1.2.1 Adding Schedule

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

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

Figure 6-50 Schedule



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

- Click **Copy** next to a day, and select the days that you want to copy to in the prompt interface, you can copy the configuration to the selected days. Select the **Select All** check box to select all days to copy the configuration.
- You can set 6 periods per day.

Step 3 Click **Apply**.

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

You can:

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

6.4.1.2.2 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** interface, click to enable record linkage, select the channel as needed, and set **Post-Record** to set alarm linkage and record delay.

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

Figure 6-51 Record linkage



6.4.1.2.3 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".

Setting Record Linkage

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

Figure 6-52 Snapshot linkage



6.4.1.2.4 Alarm-out Linkage

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

On the **Alarm** interface, 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 6-53 Alarm-out linkage



6.4.1.2.5 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 6-54 Email linkage



6.4.1.3 Subscribing Alarm

6.4.1.3.1 About Alarm Types

For alarm types and preparations of alarm events, see Table 6-23.

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 "6.4.3.1 Setting Motion Detection".
Disk Full	The alarm is triggered when the free space of SD card is less than the configured value.	The SD card no space function is enabled. For details, see "6.4.2.1 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 "6.4.2.1 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 "6.4.3.2 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 "6.4.1.1 Setting Alarm-in".
Audio Detection	The alarm is triggered when there is audio connection problem.	Abnormal audio detection is enabled. For details, see "6.4.4 Setting Audio Detection".
IVS	The alarm is triggered when intelligent rule is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.
Scene Changing	The alarm is triggered when the device monitoring scene changes.	Scene changing detection is enabled. For details, see "6.4.3.3 Setting Scene Changing".
Voltage Detection	The alarm is triggered when the device detects abnormal voltage input.	Voltage detection is enabled. For details, see "6.4.2.3 Setting Voltage Detection".
Security Exception	The alarm is triggered when the device detects malicious attack.	Voltage detection is enabled. For details, see "9.1 Security Status".

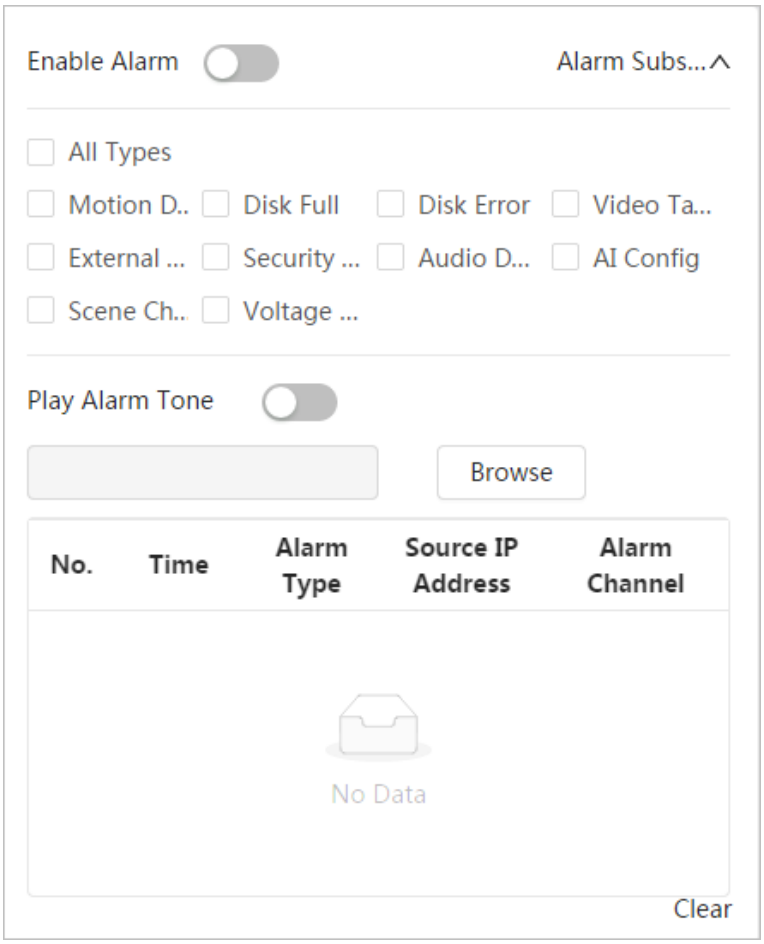
6.4.1.3.2 Subscribing Alarm Information

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

Functions of different devices might vary.

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

Figure 6-55 Alarm (subscription)



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

Step 3 Select alarm type according to the actual need. For details, see "6.4.1.3.2 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 interface is not displayed, a number is displayed on , and the alarm information is recorded automatically. Click to view the details in the alarm list. You can click **Clear** to clear the record.

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

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

6.4.2 Setting Exception

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

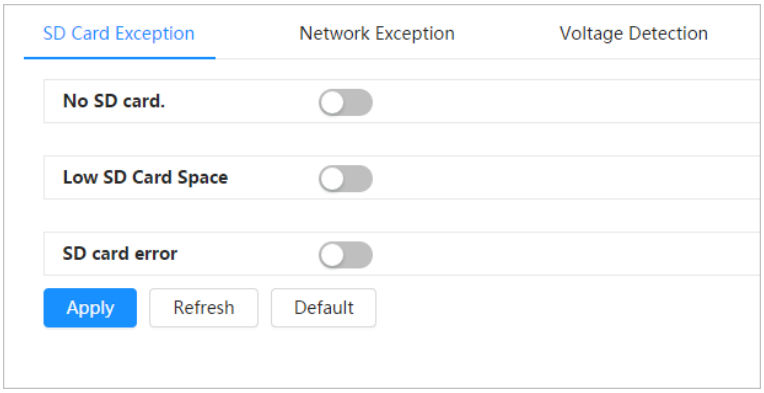
Only the device with SD card has the abnormality functions, including **No SD Card**, **SD Card Error**, and **Capacity Warning**.

6.4.2.1 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.

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

Figure 6-56 SD card exception



Step 2 Click to enable the SD card detection functions.

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

Step 3 Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".

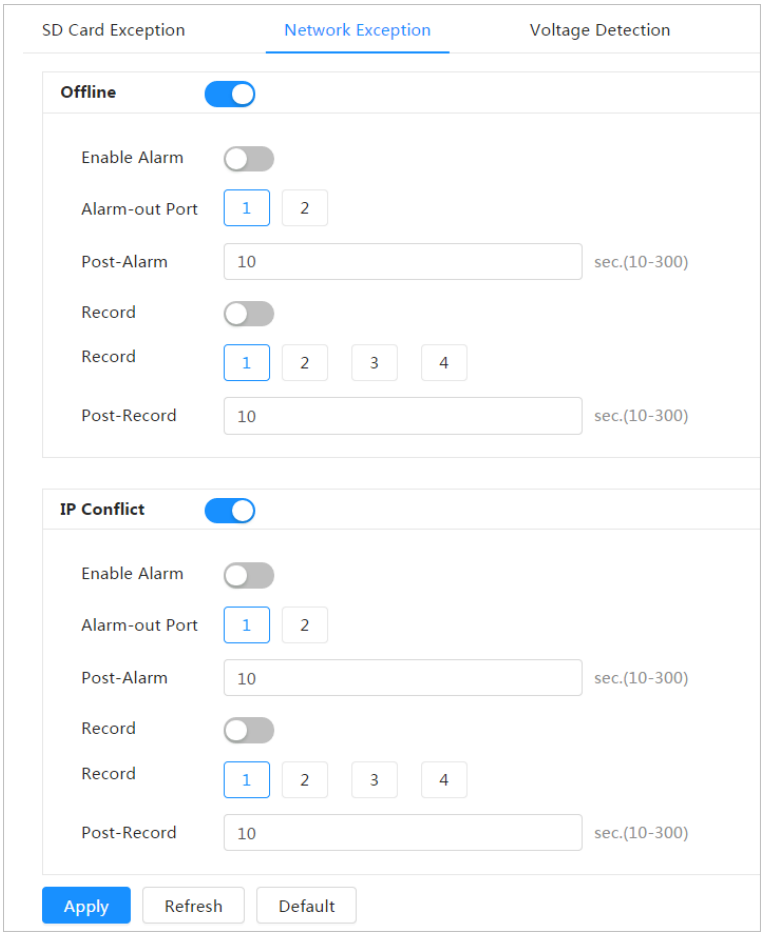
Step 4 Click **Apply**.

6.4.2.2 Setting Network Exception

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

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

Figure 6-57 Network exception



Step 2 Click to enable the network detection function.

Step 3 Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".

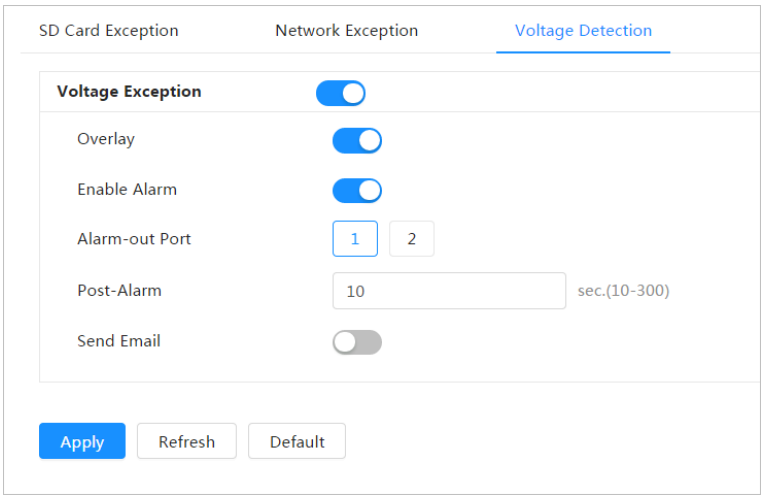
Step 4 Click **Apply**.

6.4.2.3 Setting Voltage Detection

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

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

Figure 6-58 Voltage detection



Step 2 Click to enable the voltage detection function.

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

Step 3 Set alarm linkage actions. For details, see "6.4.1.2 Alarm Linkage".

Step 4 Click **Apply**.

6.4.3 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.

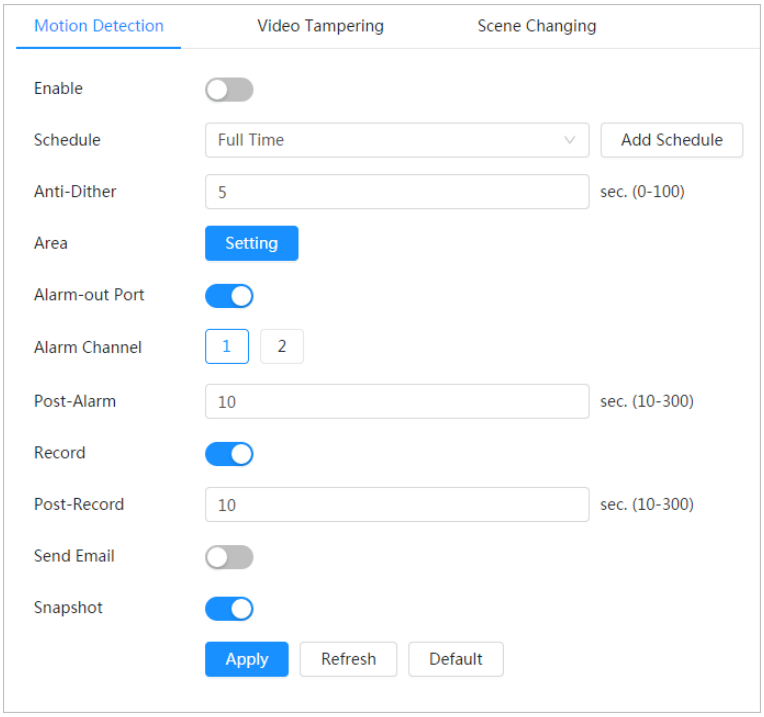
6.4.3.1 Setting Motion Detection

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

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

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

Figure 6-59 Motion detection

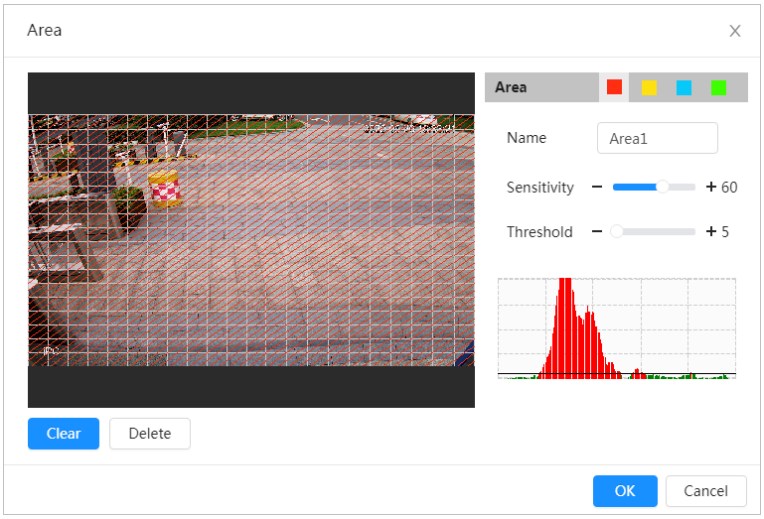


Step 2 Click to enable the motion detection function.

Step 3 Set the area for motion detection.

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

Figure 6-60 Area



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

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

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

3) Click **OK**.

Step 4 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 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**.

6.4.3.2 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.

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

Step 2 Select the event type.

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

Figure 6-61 Video tampering

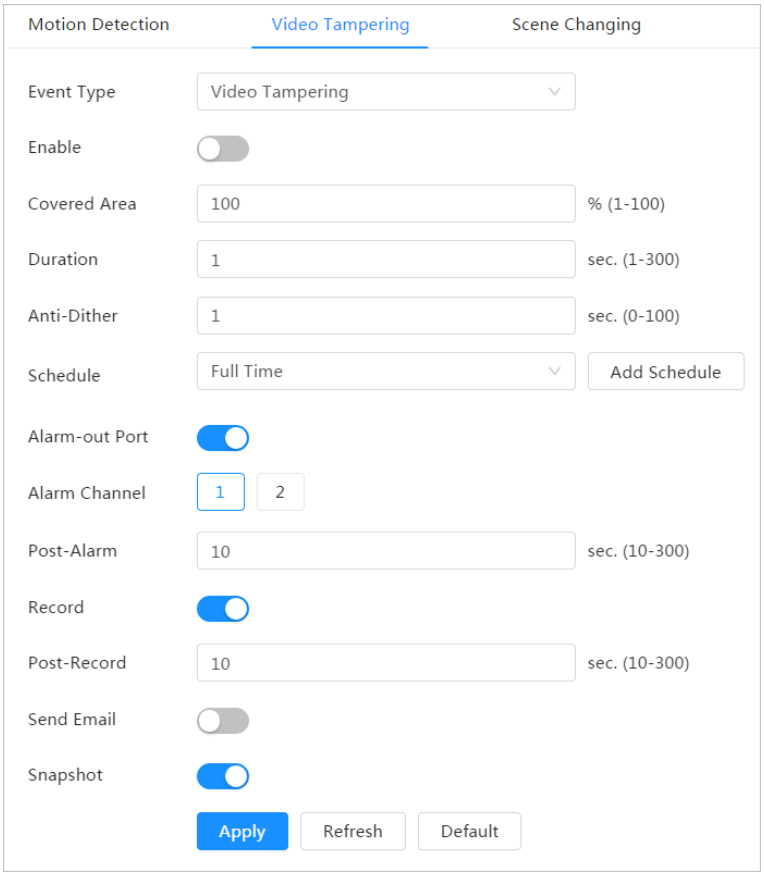


Table 6-24 Description of video temper parameter

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

Step 3 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

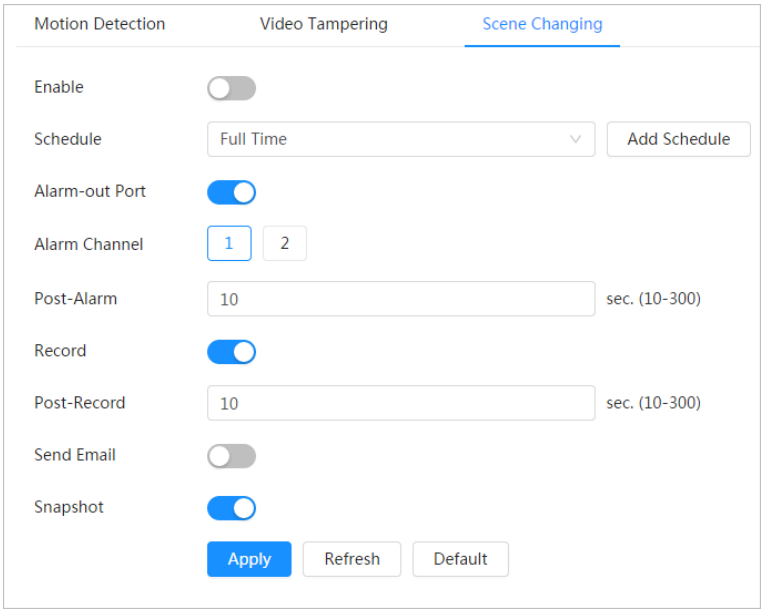
Step 4 Click **Apply**.

6.4.3.3 Setting Scene Changing

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

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

Figure 6-62 Scene changing



Step 2 Select the schedule and arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

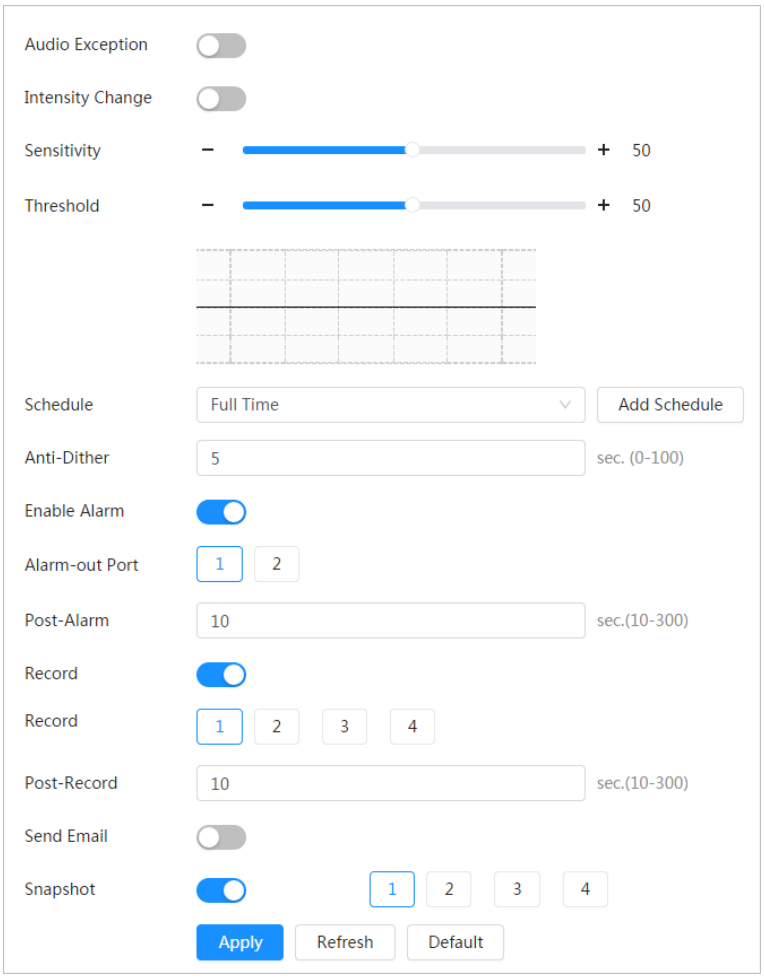
Step 3 Click **Apply**.

6.4.4 Setting Audio Detection

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

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

Figure 6-63 Audio detection



Step 2 Set parameters.

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

Step 3 Select the schedule and arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. For details, see "6.4.1.2.1 Adding Schedule".

Step 4 Click **Apply**.

6.5 Storage

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

Functions might vary with different models.

Select > **Storage**.

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

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

Figure 6-64 Local



6.6 System

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

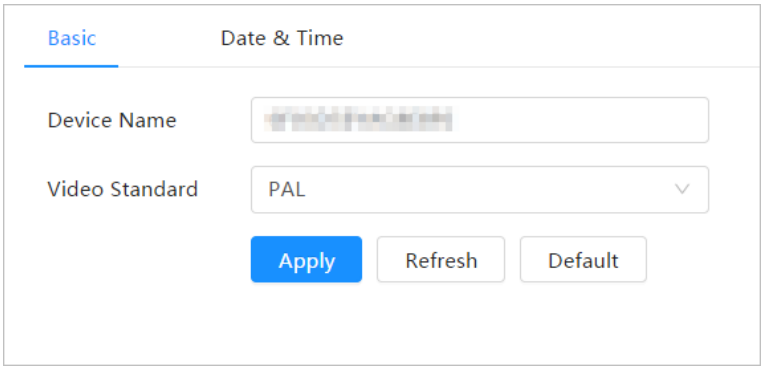
6.6.1 General

6.6.1.1 Basic

You can configure device name, language and video standard.

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

Figure 6-65 Basic



Step 2 Configure general parameters.

Table 6-25 Description of general parameters

Parameter	Description
Name	Enter the device name.

Parameter	Description
Video Standard	Select video standard from **PAL** and **NTSC**.

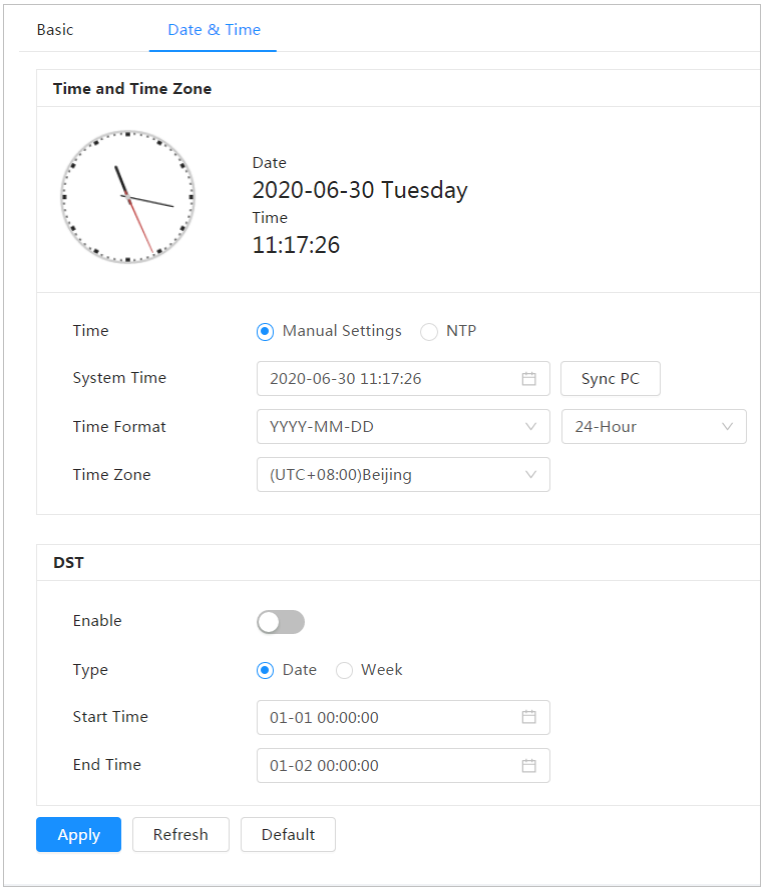
Step 3 Click **Apply**.

6.6.1.2 Date & Time

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

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

Figure 6-66 Date and time



Step 2 Configure date and time parameters.

Table 6-26 Description of date and time parameters

Parameter	Description
Date Format	Configure the date format.
Time	• **Manually Setting**: Configure the parameters manually. • **NTP**: When selecting NTP, the system then syncs time with the internet server in real time. You can also enter the IP address, time zone, port, and interval of a PC which installed NTP server to use NTP.
Time Format	Configure the time format. You can select from **12-Hour** or **24-Hour**.
Time Zone	Configure the time zone that the camera is at.

Parameter	Description
Current Time	Configure system time. Click **Sync PC**, and the system time changes to the PC time.
DST	Enable DST as needed. Click , and configure start time and end time of DST with **Date** or **Week**.

Step 3 Click **Apply**.

6.6.2 Account

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

Managing users and groups are only available for administrator users.

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

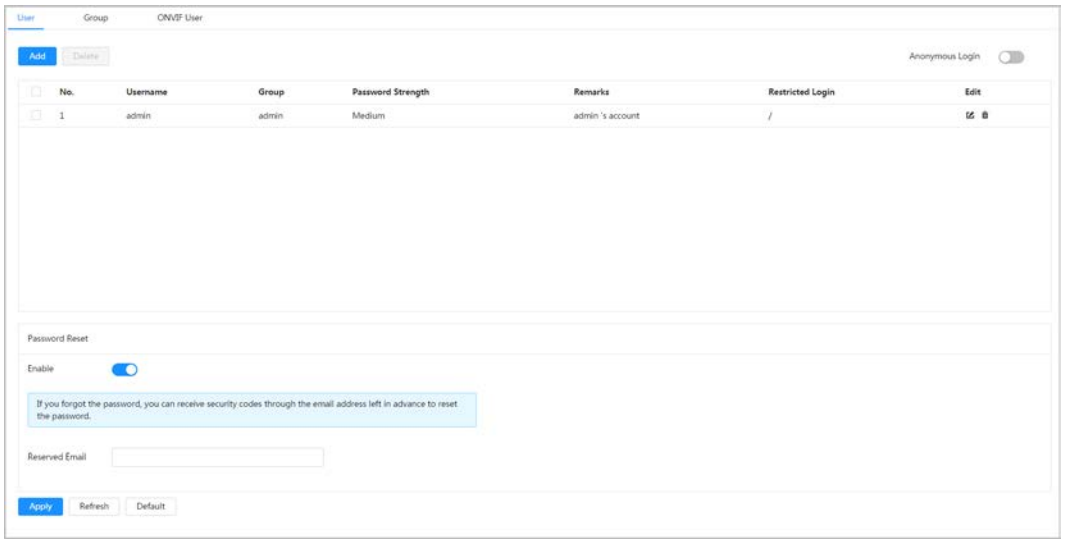
6.6.2.1 User

6.6.2.1.1 Adding User

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

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

Figure 6-67 User



Step 2 Click **Add**.

Figure 6-68 Add user (system)

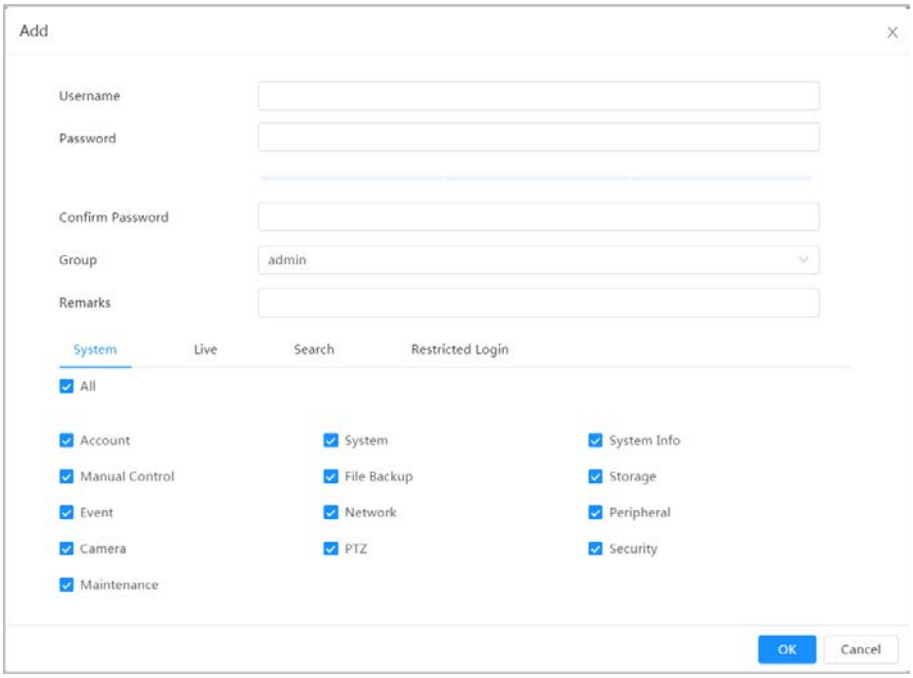
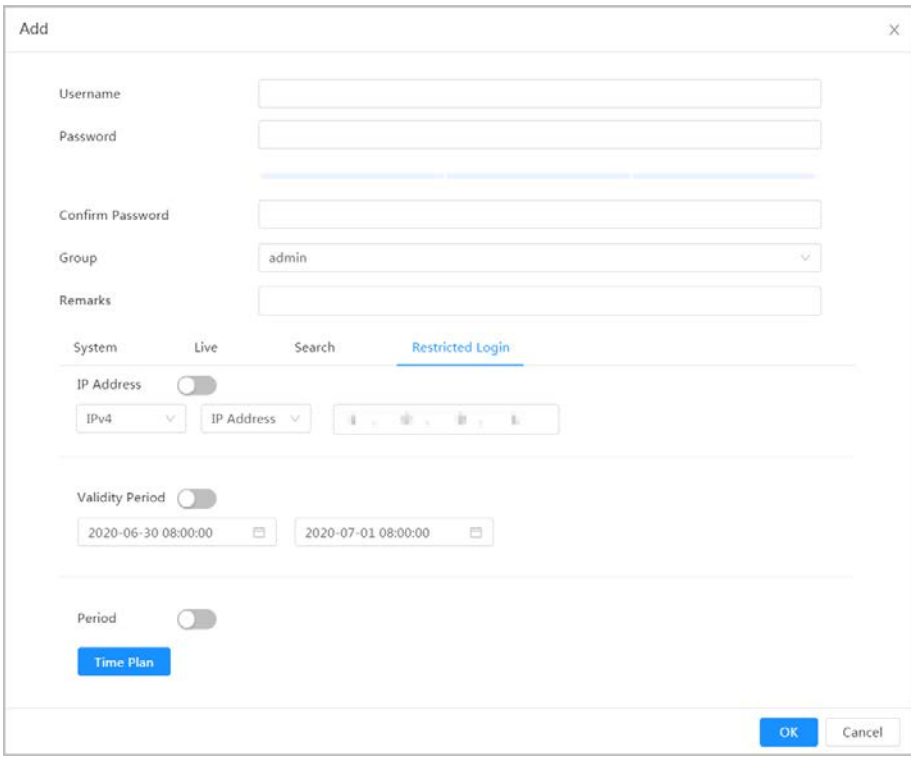


Figure 6-69 Add user (restricted login)



Step 3 Configure user parameters.

Table 6-27 Description of user parameters (1)

Parameter	Description
Username	User's unique identification. You cannot use existed username.
Password	Enter password and confirm it again. 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 ' " ; : &).
Confirm Password	
Group	The group that users belong to. Each group has different authorities.
Remark	Describe the user.
System	Select authorities as needed. We recommend giving fewer permissions to normal users than premium users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.

Parameter	Description
Restricted Login	Set the PC address that allows the defined user to log in to the camera and the validity period and time range. You can log in to the web interface with the defined IP in the defined time range of validity period. ● IP address: You can log in to web through the PC with the set IP. ● Validity period: You can log in to web in the set validity period. ● Time range: You can log in to web in the set time range. Set as follows 1. IP address: Enter the IP address of the host to be added. 2. IP segment: Enter the start address and end address of the host to be added.

Step 4 Click **Apply**.

The newly added user is displayed in the username list.

Related Operations

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

  For admin account, you can only edit the password.

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

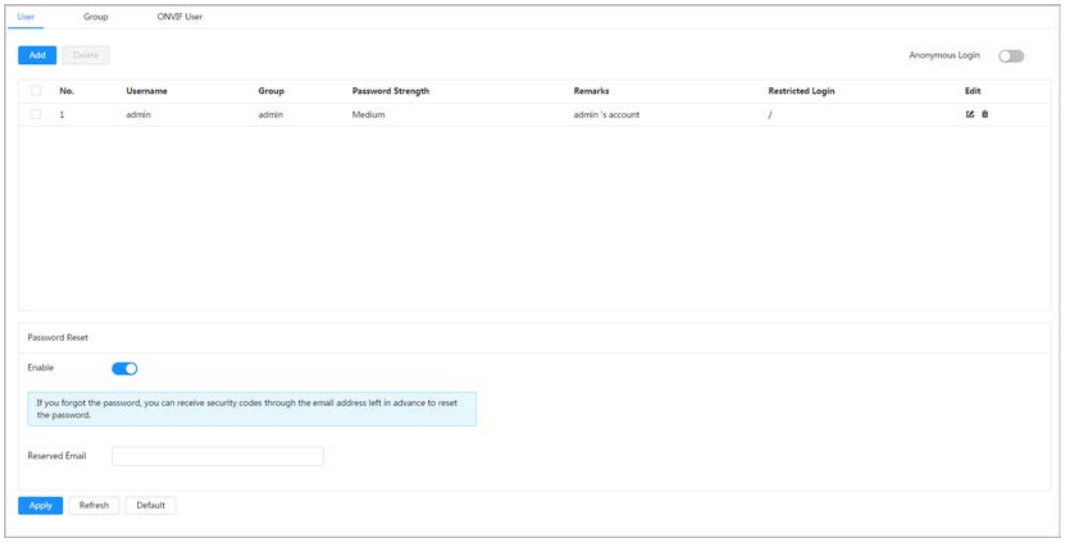
  The admin account cannot be deleted.

6.6.2.1.2 Resetting Password

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

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

Figure 6-70 User



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

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

Step 3 Enter the reserved email address.

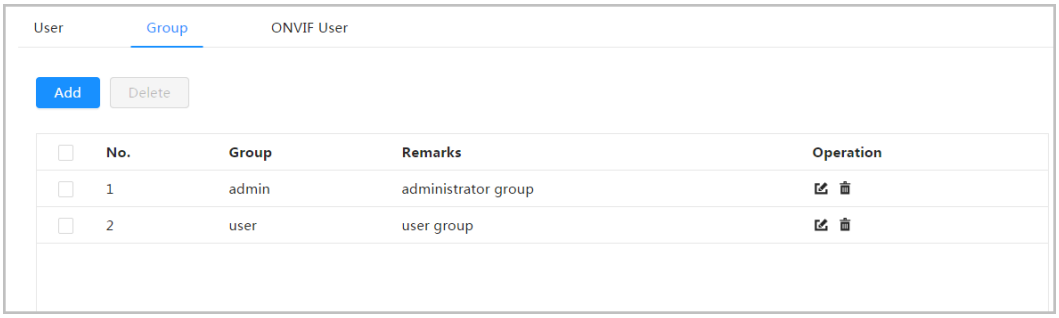
Step 4 Click **Apply**.

6.6.2.2 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.

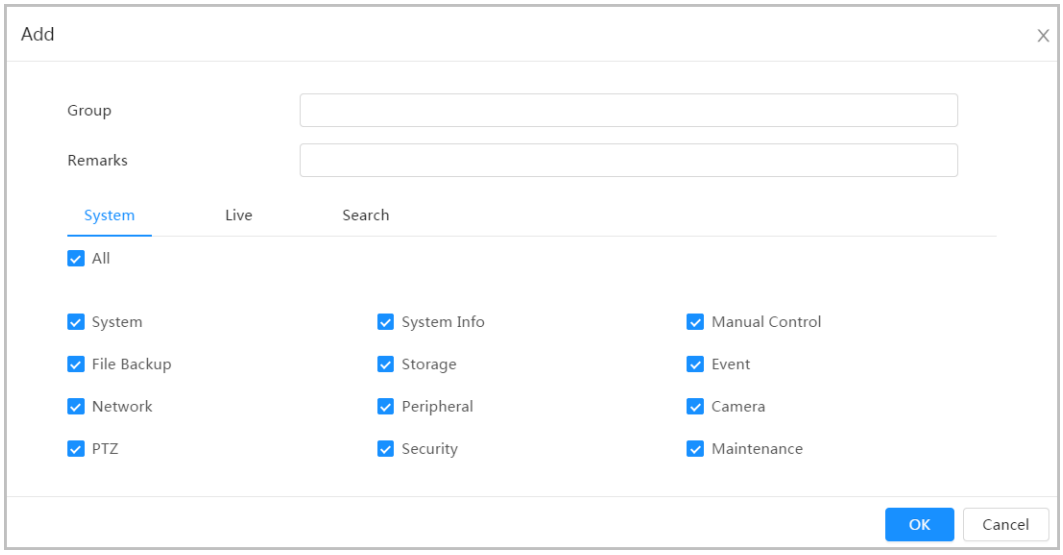
Step 1 Select > **System** > **Account** > **Group**.

Figure 6-71 Group name



Step 2 Click **Add**.

Figure 6-72 Add group



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

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

The newly added group displays in the group name list.

Related Operations

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

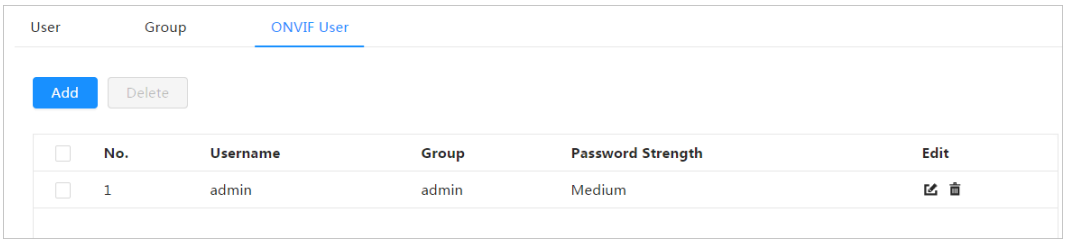
The admin group and user group cannot be deleted.

6.6.2.3 ONVIF User

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

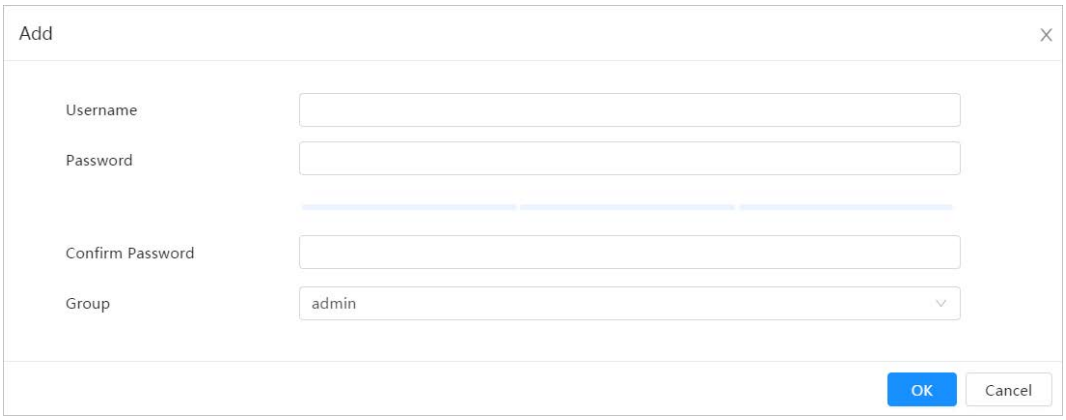
Step 1 Select > **System** > **Account** > **ONVIF User**.

Figure 6-73 ONVIF user



Step 2 Click **Add**.

Figure 6-74 Add ONVIF user



Step 3 Configure user parameters.

Table 6-28 Description of ONVIF user parameters

Parameter	Description
Username	User's unique identification. You cannot use existed username.
Password	Enter password and confirm it again. 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 ' " ; : &).
Confirm Password	
Group Name	The group that users belong to. Each group has different authorities.

Step 4 Click **OK**.

The newly added user displays in the username list.

Related Operations

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

  For admin account, you can only change the password.

- Click to delete the added users.

  The admin account cannot be deleted.

6.6.3 Peripheral Management

6.6.3.1 Configuring Serial Port

Set the serial port of the external device.

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

Step 2 Configure parameters.

Figure 6-75 Serial port settings

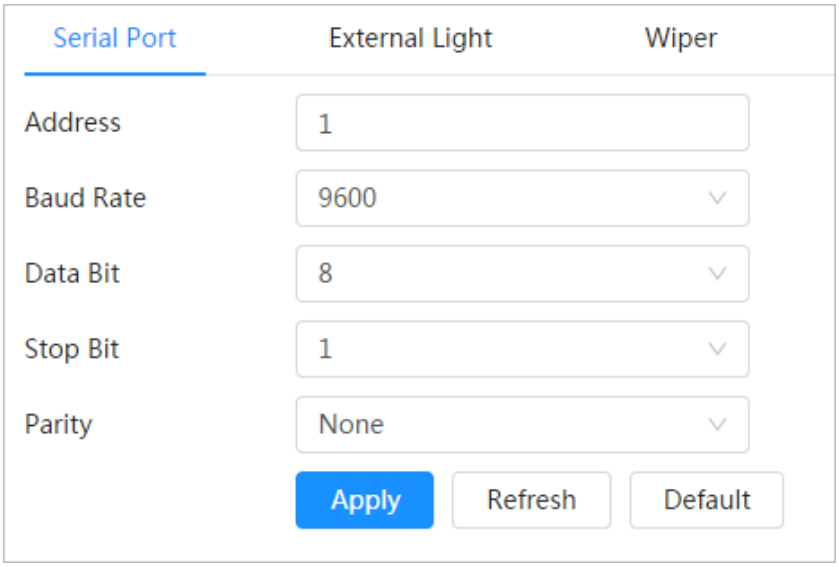


Table 6-29 Description of serial port settings parameters

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

Step 3 Click **Apply**.

6.6.3.2 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 "6.6.3.1 Configuring Serial Port".

Procedure

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

Step 2 Select working mode as needed.

Figure 6-76 External light

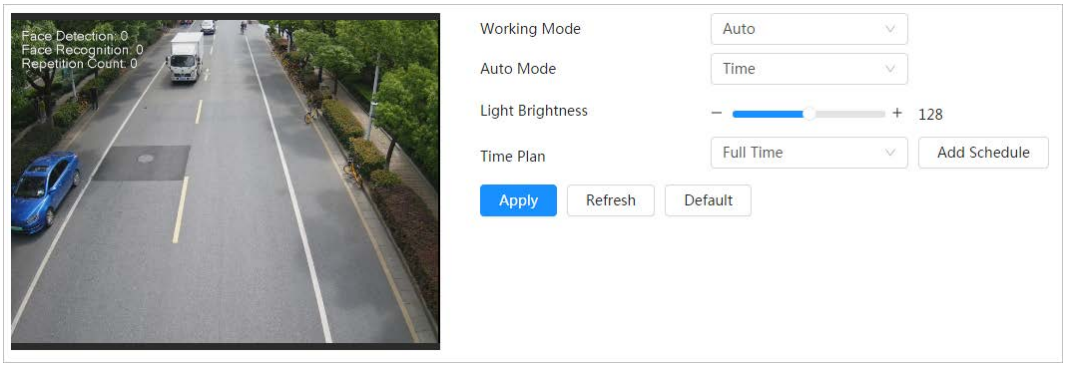


Table 6-30 Lamp parameters

Parameter	Description
Work Mode	• **Off**: The external light is disabled. • **Manual**: Set the light brightness manually. • **Auto**: The camera turns on or turns off the light according to the light time and photoresister automatically.
Auto Mode	• **Time**: When selecting **Time** in **Auto Mode**, set the arming period. During the arming period, the external light is on. Select the added time plan table in the **Time Plan** list. Click **Add Schedule** to add new time plan table. For details, see "6.4.1.2 Alarm Linkage". • **Photoresister:** When you select **Photoresister** in **Auto Mode**, the camera turns on the external light according to the brightness automatically.
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 **OK**.

6.6.3.3 Configuring Wiper

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

Step 2 Configure working mode of wipers.

Figure 6-77 Wiper

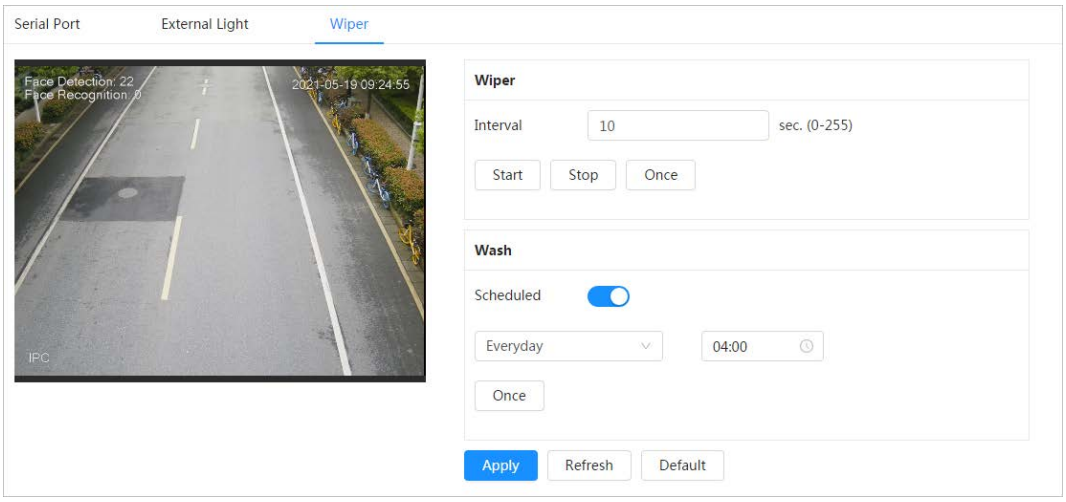


Table 6-31 Wiper parameter description

Parameter	Description
Interval	The interval between stop mode and start mode. For example, set the time to10 s, and the wiper will work every 10 s.
Start, Stop, Once	Configure working mode of the wiper. ● Click **Start**, and the wiper works as the set interval time. ● Click **Stop**, and the wiper stops working. ● Click **Once**, and the wiper works once.
Wash	Select the **Schedule** check box and set the time, and then the wiper will work as the configured time. Click **Once**, and the wiper works once. It can be used to check whether the wiper works normally.

Step 3 Click **Apply**.

6.6.4 Manager

6.6.4.1 Requirements

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

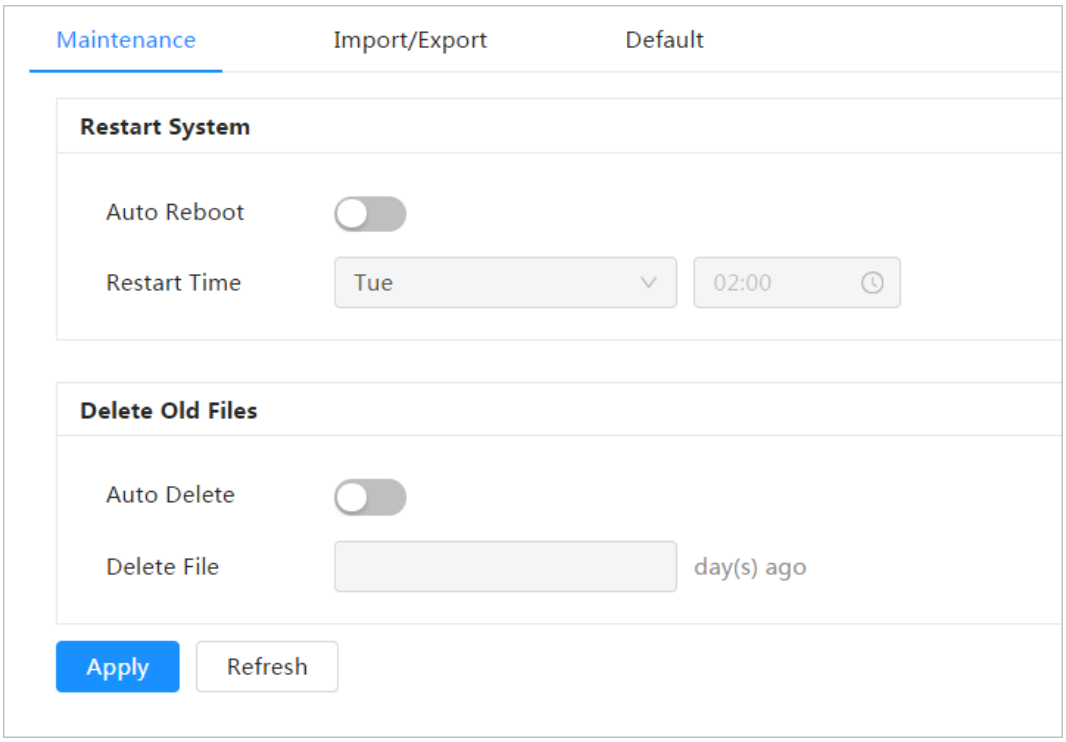
- Check surveillance images regularly.
- Clear regularly user and user group information that are not frequently used.
- Change the password every three months. For details, see "6.6.2 Account".
- View system logs and analyze them, and process the abnormity in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware in time.

6.6.4.2 Maintenance

You can restart the system manually, and set the time of auto reboot and auto deleting old files. This function is disabled by default.

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

Figure 6-78 Maintenance



Step 2 Configure auto maintain parameters.

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

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

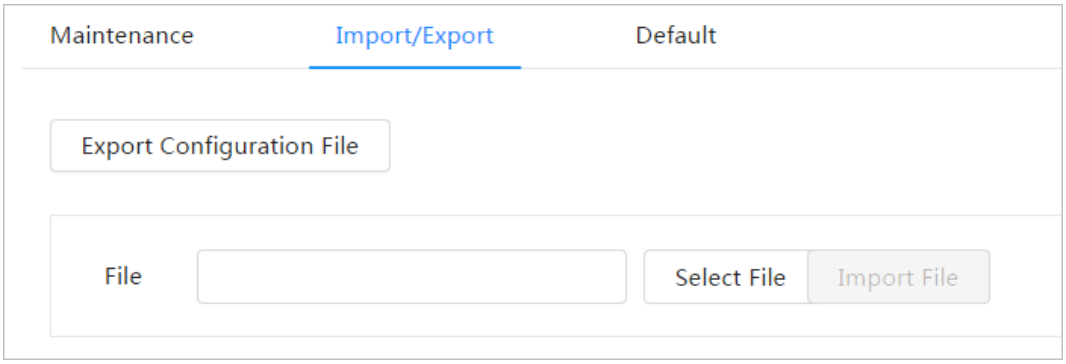
Step 3 Click **Apply**.

6.6.4.3 Import/Export

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

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

Figure 6-79 Import/Export



Step 2 Import or export the file.

- Import: Select local configuration file, and click **Import File** to import the local system

configuration file to the system.

- Export: Click **Export Configuration file** to export the system configuration file to local storage.

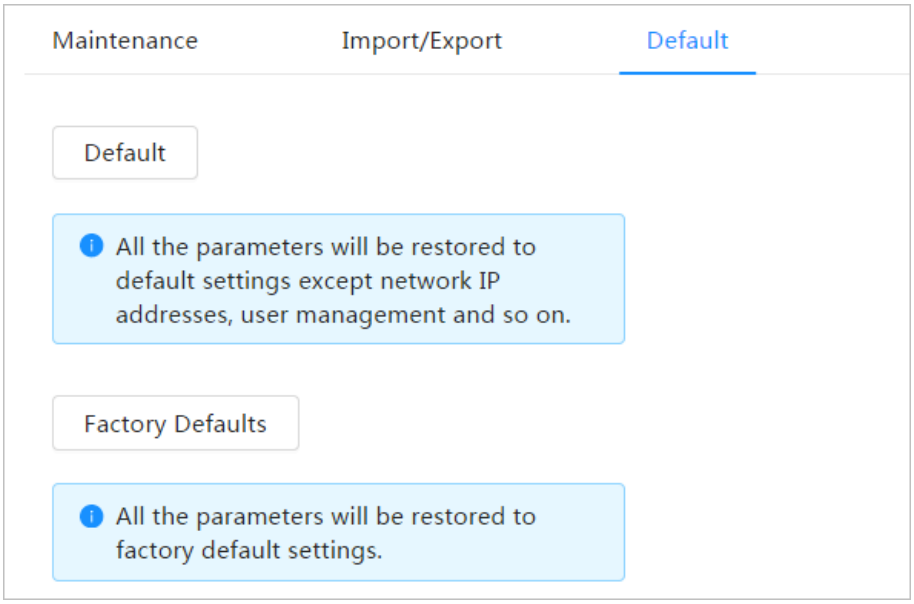
6.6.4.4 Default

Restore the device to default configuration or factory settings.

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

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

Figure 6-80 Default



6.6.5 Upgrade

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

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

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

Figure 6-81 Upgrade



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

The upgrade file should be a .bin file.

Step 3 Click **Update.**

6.7 System Information

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

6.7.1 Version

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

6.7.2 Online User

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

6.8 Setting Log

6.8.1 Log

You can view and back up logs.

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

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

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

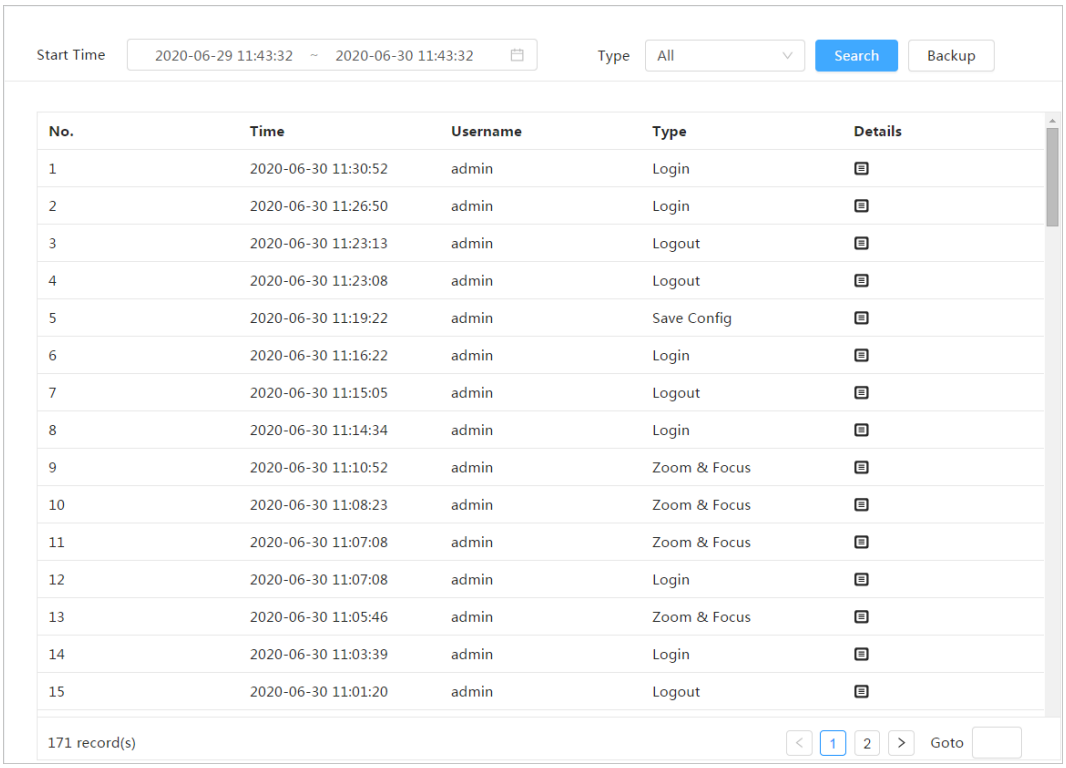
The log type includes All, System, Setting, Data, Event, Record, Account, and Safety.

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

Step 3 Click **Search**.

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

Figure 6-82 Log



6.8.2 Remote Log

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

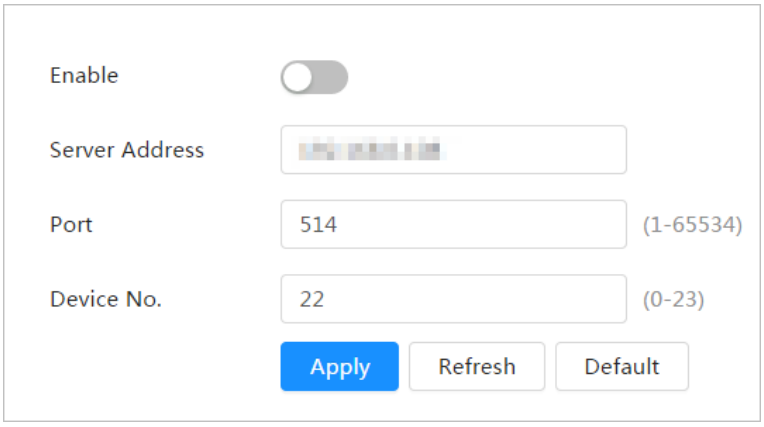
Step 1 Select > **Log** > **Remote Log**.

Step 2 Click to enable remote log function.

Step 3 Set address, port and device number.

Step 4 Click **Apply**.

Figure 6-83 Remote log



7 Live

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

7.1 Live Interface

Log in and click the **Live** tab.

Interfaces might vary with different models.

Figure 7-1 Live (single-channel)

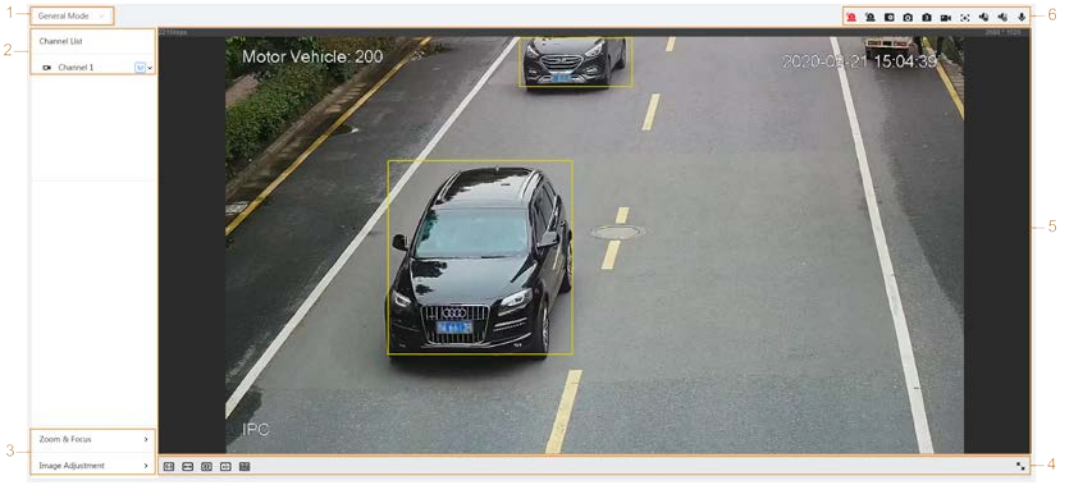


Figure 7-2 Live (multi-channels)

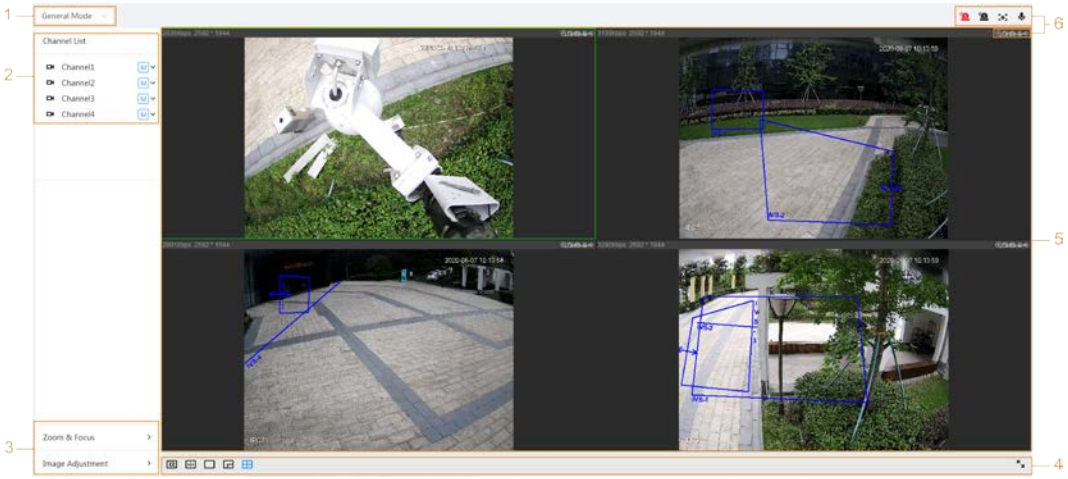


Table 7-1 Description of function bar

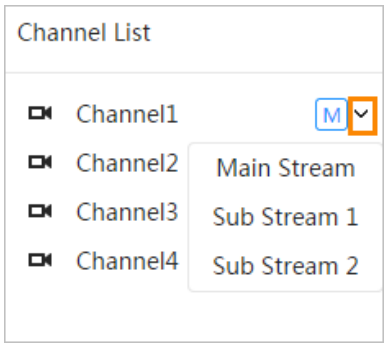
No.	Function	Description
1	Display mode	You can select the display mode from **General Mode**, **Face Mode**, **Metadata Mode**, **ANPR** and **Face & Body Detection**. For details, see "7.5 Display Mode".
2	Channel list	Displays all channels. You can select the channel as needed and set the stream type.

No.	Function	Description
3	Image adjustment	Adjustment operations in live viewing.
4		
5	Live view	Displays the real-time monitoring image.
6	Live view function bar	Functions and operations in live viewing.

7.2 Setting Encode

Click , and then select the stream as needed.

Figure 7-3 Encode bar



- **Main Stream**: It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring. For details, see "6.2.2.1 Encode".
- **Sub Stream**: It has small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth is not enough. For details, see "6.2.2.1 Encode".
- M means the current stream is main stream; S1 means the current stream is sub stream 1; S2 means the current stream is sub stream 1.

7.3 Live View Function Bar

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

Table 7-2 Description of live view function bar

Icon	Function	Description
	Force Alarm	Displays alarm sound state. Click the icon to enable or disable the alarm sound forcibly.
/	Digital Zoom	You can zoom video image through two operations. • 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. • Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.

Icon	Function	Description
	Snapshot	Click the icon to capture one picture of the current image, and it will be saved to the configured storage path. For the details on viewing or configuring storage path, see "6.1 Local".
	Triple Snapshot	Click the icon to capture three pictures of the current image, and they will be saved to the configured storage path. For the details on viewing or configuring storage path, see "6.1 Local".
	Record	Click the icon to record video, and it will be saved to the configured storage path. For the details on viewing or configuring storage path, see "6.1 Local".
	Aux Focus	Click the icon, the **AF Peak** (focus eigenvalue) and **AF Max** (max focus eigenvalue) are displayed on the video image. • **AF Peak**: The eigenvalue of image definition, it displays during focus. • **AF Max**: The best eigenvalue of image definition. • The smaller the difference between AF peak value and the AF max value, the better the focus is. Aux focus closes automatically after five minutes.
	Audio	Click the icon to enable or disable audio output.
	Talk	Click the icon to enable or disable the audio talk.

7.4 Window Adjustment Bar

7.4.1 Adjustment

This section introduces the adjustment of image. For details, see Table 7-3.

Table 7-3 Description of adjustment bar

Icon	Function	Description
	Original Size	Click the icon, and then the video displays with original size.

Icon	Function	Description
	Full Screen	Click the icon to enter full screen mode; double-click or press Esc to exit.
	W:H	Click the icon to resume original ratio or change ratio.
	Fluency Adjustment	Click the icon to select the fluency from **Realtime**, **General** and **Fluent**. • **Realtime**: Guarantees the real time of the image. When the bandwidth is not enough, the image might not be smooth. • **General**: It is between **Realtime** and **Fluent**. • **Fluent**: Guarantees the fluency of the image. There might be delay between live view image and real-time image.
	AI Rule	Click the icon, and then select **Enable** to display AI rules and detection box; select **Disable** to stop the display. It is enabled by default.
	Crowd Distribution Map	Click the icon and select **Enable**. The **Crowd Distribution Map** interface is displayed. For details, see "8.1 Setting Crowd Distribution Map".
	Window Layout	When viewing multi-channel image, you can select display layout.

7.4.2 Zoom and Focus

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

The focus would adjust automatically after zooming in or out.

Figure 7-4 Zoom and focus

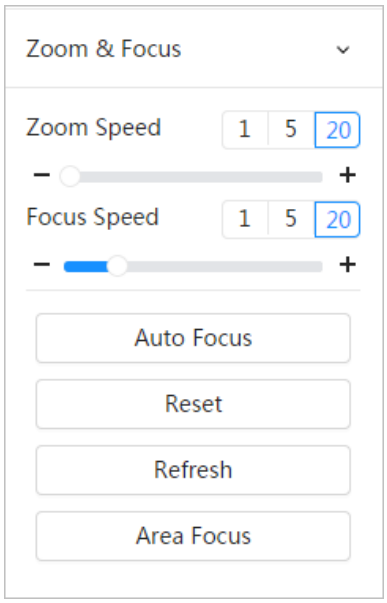


Table 7-4 Description of zoom and focus parameter

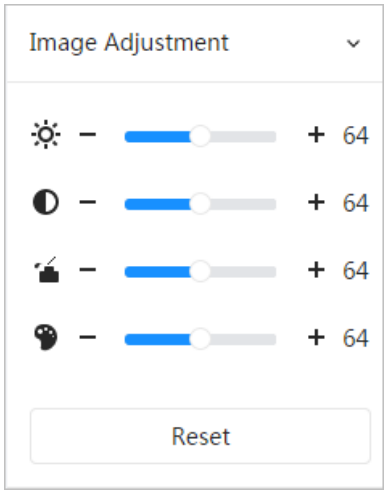
Parameter	Description
Zoom Speed	Changes the focal length of the camera to zoom in or out the image. 1. Set the speed value. The **Zoom Speed** is the adjustment range in one click. The larger the value is, the more the image would zoom in or out in one click. 2. Click or hold + or – button, or drag the slider to adjust zoom.
Focus Speed	Adjusts the optical back focal length to make the image clearer. 1. 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. 2. Click or hold + or – button, or drag the slider to adjust focus.
Auto Focus	Adjusts image clarity automatically. Do not make any other operation during auto focus process.
Reset	Restores focus to default value and corrects errors. 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.
Area Focus	Focus on the subject of a selected area. Click **Area Focus**, and then select an area in the image, the camera performs auto focus in that area.

7.4.3 Image Adjustment

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

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

Figure 7-5 Image adjustment



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

Click **Reset** to restore focus to default value.

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

7.4.4 Fisheye

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

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

Figure 7-6 Fisheye-ceiling mount

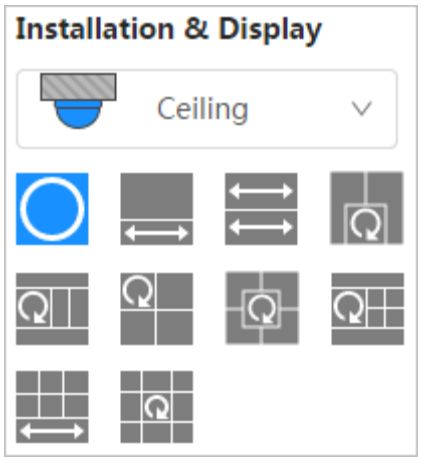


Figure 7-7 Fisheye-wall mount

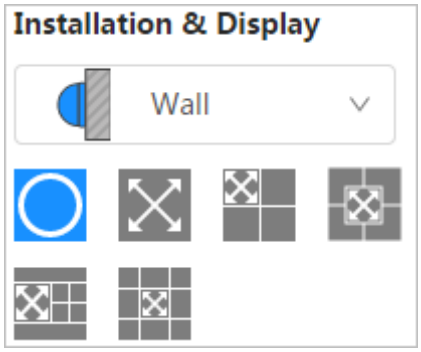


Figure 7-8 Fisheye-ground mount

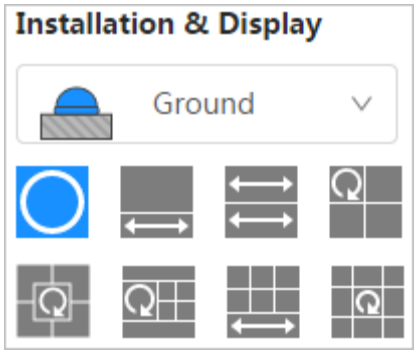


Figure 7-9 Fisheye-VR mode



Table 7-5 Description of fisheye configuration

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

Parameter	Description	
Display mode	The display model of the current image. There are different display modes for each installation mode. ● **Ceiling**: 1P+1, 2P, 1+2, 1+3, 1+4, 1P+6, 1+8. ● **Wall**: 1P, 1P+3, 1P+4, 1P+8. ● **Ground**: 1P+1, 2P, 1+3, 1+4, 1P+6, 1+8. The image will be the original size by default when switching installation mode.	
Ceiling/Wall/Ground mount	 Original image	The original image before correction.
Ceiling/Ground mount	 1P+1	360° rectangular panoramic image screen + 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.
	 2P	Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. It is also called dual-panoramic image. You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.
	  1+2	Original image screen + two independent sub-screens. Ground mount does not support this display mode. ● 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.
	 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.
	  1+4	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.

Parameter	Description	
	 1P+6	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.
	 1P+8	Original image screen + eight 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.
Wall mount	 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.
	 1P+3	180° rectangular panoramic image screen + three independent sub-screens. ● 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.
	  1P+4	180° rectangular panoramic image screen + four independent sub-screens. ● 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.
	 1P+8	180° rectangular panoramic image screen + eight independent sub-screens. ● 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.
VR mode	 Panorama	Drag or cross the screen 360° to unfold the distortion panorama, and you can drag the image in left/right direction.

Parameter	Description	
	 Semi-circle	● 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. ● Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. ● Scroll the mouse wheel to zoom the image.
	 Cylinder	Display the distortion panorama in 360°circularity. ● 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. ● Press S to rotate the image in anticlockwise direction, and press E to stop the rotation. ● Scroll the mouse wheel to zoom the image.
	 Asteroid	● 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. ● Press the left mouse-button to slide down to display the image on the plane surface. ● Scroll the mouse wheel to zoom the image.

7.5 Display Mode

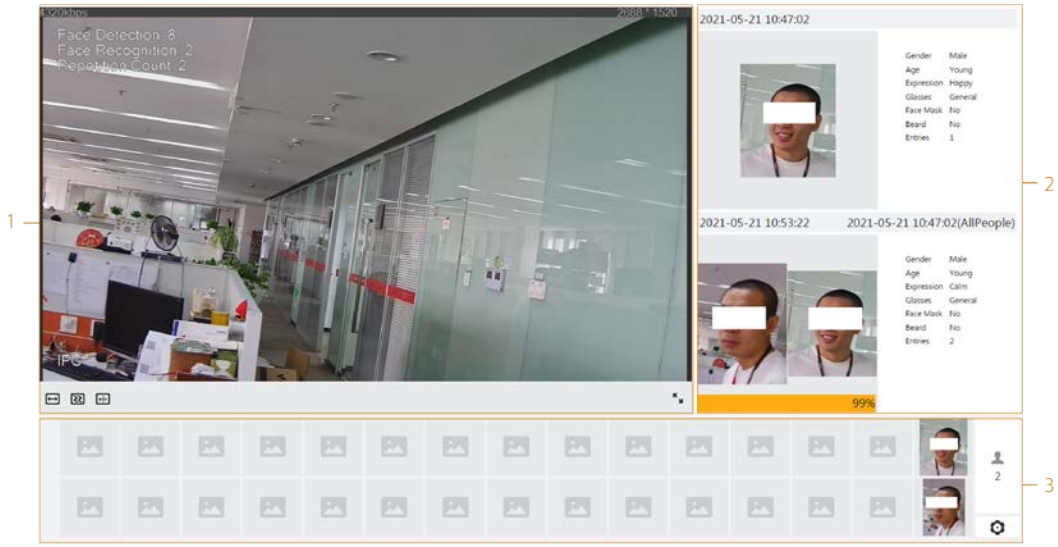
You can select the display mode from **General Mode**, **Face Mode**, **Metadata Mode**, **ANPR** and **Face & Body Detection**. For general mode, see Figure 7-2. This section mainly introduces **Face Mode** and **Metadata Mode**.

Interfaces might vary with different models.

- Select **Face Mode** from the display mode drop-down list.

  Make sure that you have enabled face detection function.

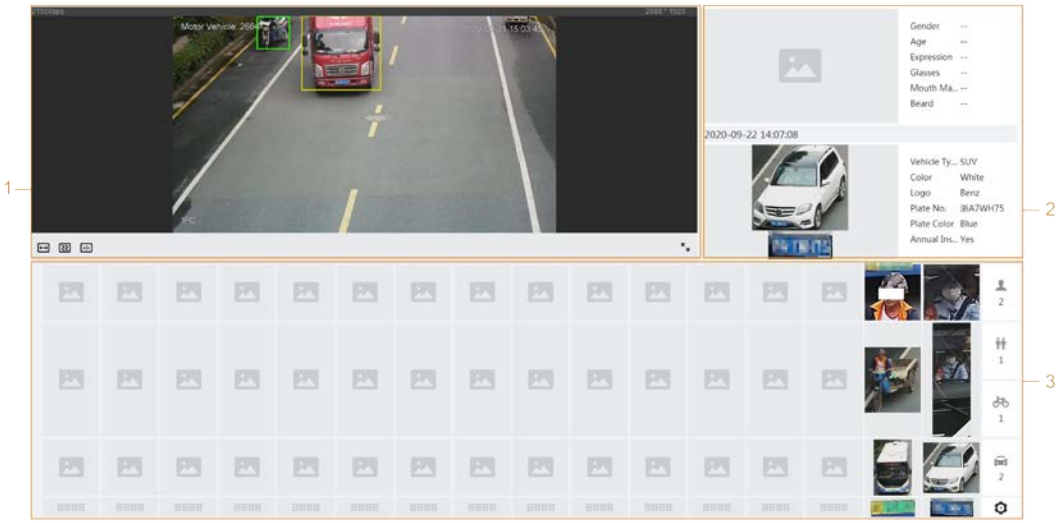
Figure 7-10 Face mode



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

Make sure that you have enabled video metadata detection function.

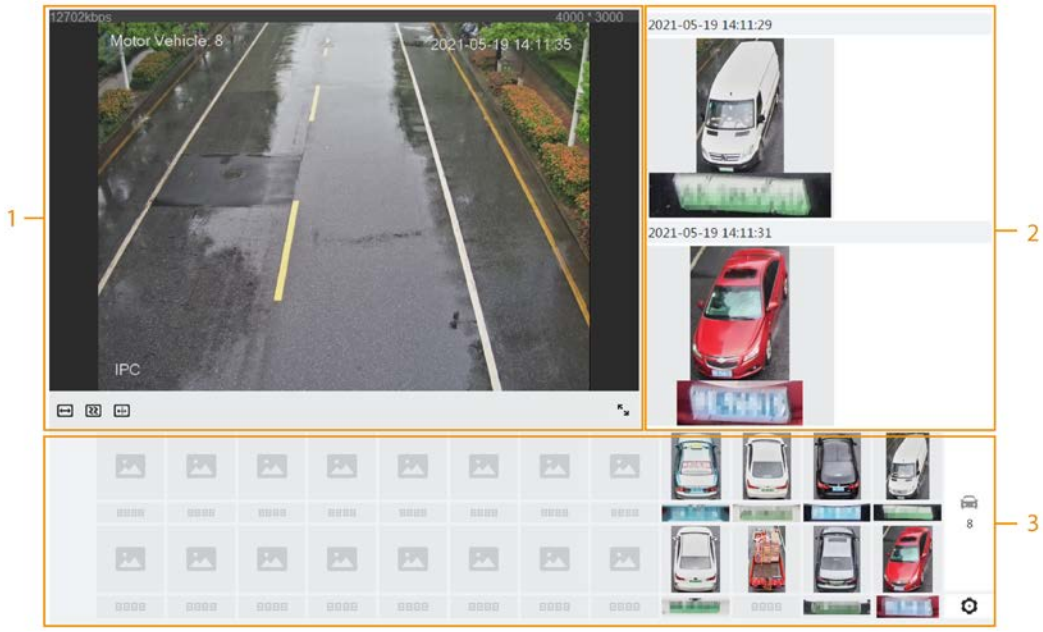
Figure 7-11 Metadata mode



- Select **ANPR** from the display mode drop-down list.

Make sure that you have enabled ANPR function.

Figure 7-12 ANPR



- Select **Face & Body Detection** from the display mode drop-down list.

Make sure that you have enabled face & body detection function.

Figure 7-13 Face & body detection

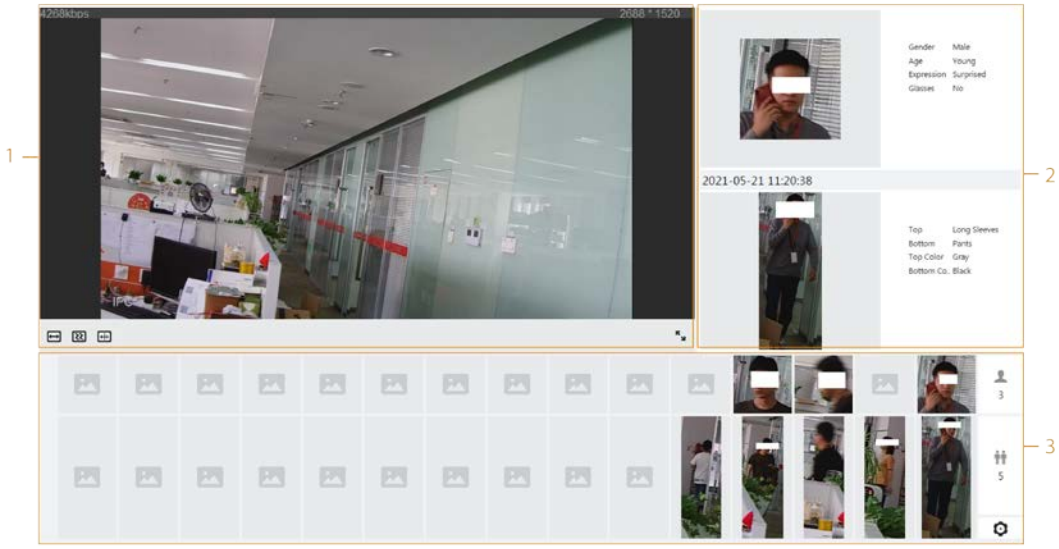


Table 7-6 Description of layout

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	Displays the captured images. ● Click a snapshot in the area, and the details of the snapshot are displayed in the Details area. ● Click to set the attributes displayed in the Details area.

8 AI

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.

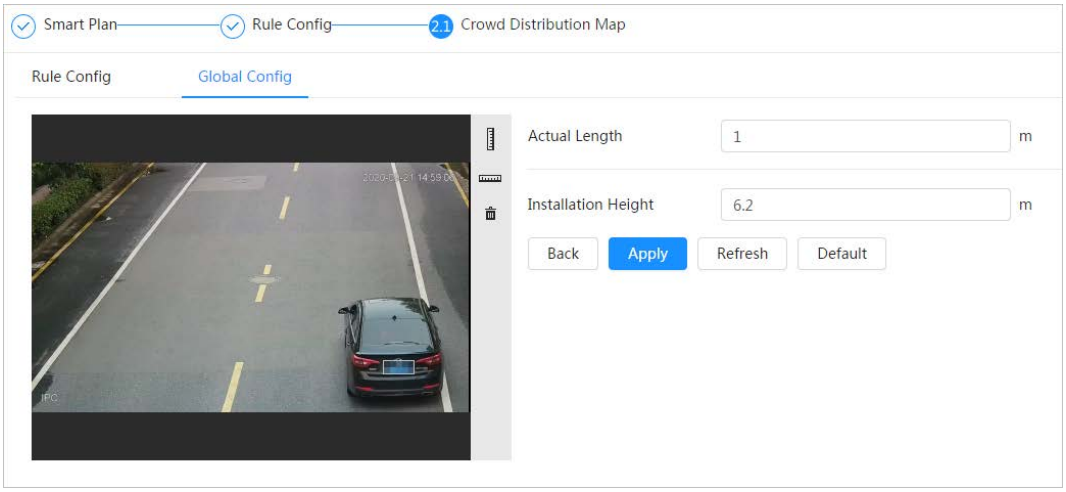
Notes

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 is the vertical horizontal icon.
   - Select the added rulers on the image, and click to delete them.

Figure 8-1 Global configuration of crowd distribution map



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

8.1.2 Rule Configuration

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

Prerequisites

- Select **AI** > **Smart Plan**, and enable **Crowd Distribution Map**.
- You have configured the parameters on the **Global Config** interface.

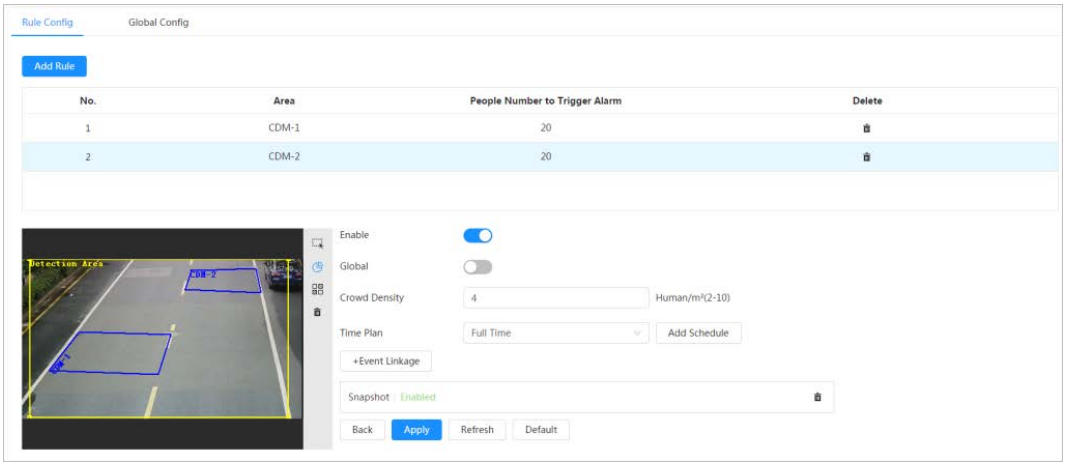
Procedure

Step 1 Select **AI** > **Smart Plan**

Step 2 Click next to **Crowd Distribution Map**, and then click **Next**.

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

Figure 8-2 Rule configuration



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

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

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

1) Click **Add Rule** to add statistical areas.
2) Set the name of **Area** and **People Number to Trigger Alarm**.
   When the number of the people in the area exceeds the configured threshold, the alarm will be triggered, and the system will perform the linkage actions. The people number to trigger alarm is 20 by default.
3) Click at the right side of the image, draw people counting areas in the detection area, and then right-click to finish the drawing.
4) Repeat the above steps to add more people counting areas.
   - Click , and then press and hold the left mouse button to draw a rectangle, and then pixel size is displayed.
   - Click to delete the drawn detection or people counting areas.

Step 6 Configure parameters.

Table 8-1 Description of crowd map parameters

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

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

Result

Click on the **Live** interface 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)



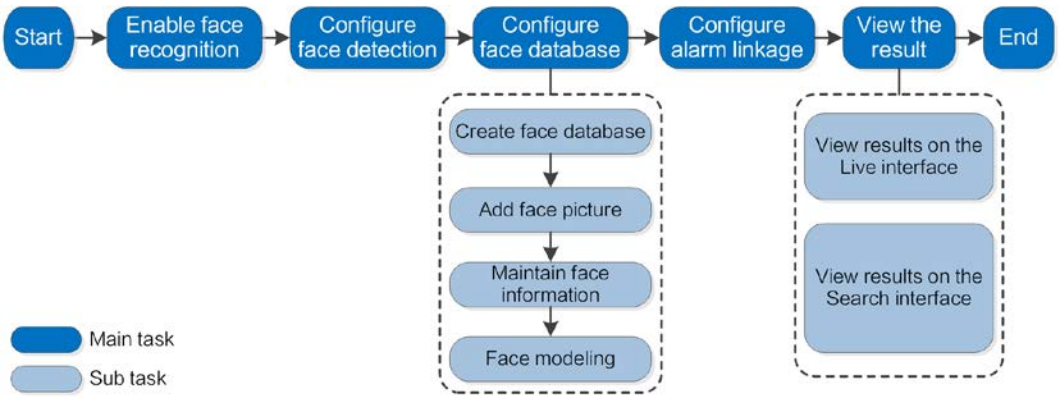
8.2 Setting Face Recognition

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.

For the process of setting face recognition, see Figure 8-5.

Figure 8-5 Face recognition flowchart



8.2.1 Setting Face Detection

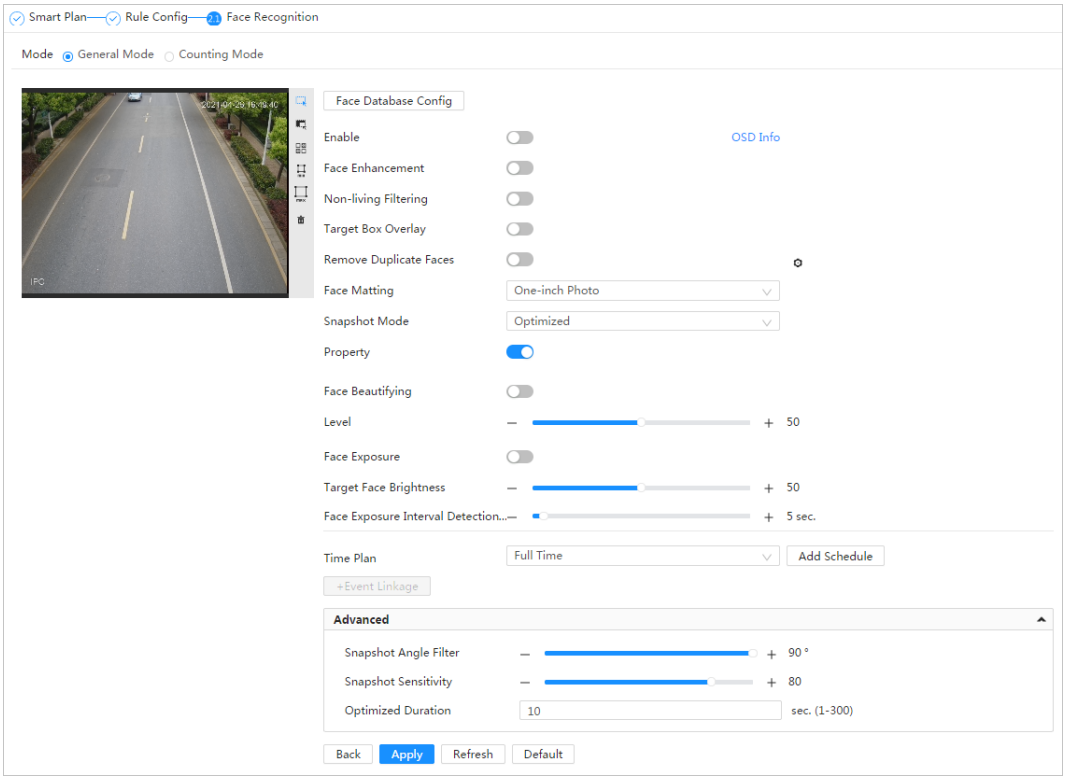
When a face is recognized in the detection area, the system performs alarm linkage.

Procedure

Step 1 Select **AI** > **Smart Plan**.

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

Figure 8-6 Face detection



Step 3 Select the detection mode.

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

repeating faces and loitering faces) into the exclude people database so that the system will not count the faces after detecting them.

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

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

- Click to draw rule line in the image.

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

  This icon is only available in counting mode.
- Click to draw a face detection area in the image, and right-click to finish the drawing.
- Click to draw an exclusion area for face detection in the image, and right-click to finish the drawing.
- Click to draw the minimum size of the target, and click to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

Step 6 Set parameters.

Table 8-2 Description of face detection parameters

Parameter	Description
OSD Info	Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the face statistics function. The number of detected faces is displayed on the **Live** interface. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click to enable face enhancement, and it can preferably guarantee clear face with low stream.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.
Target Box Overlay	Click to enable the function, and you can add a bounding box to the face in the captured picture to highlight the face. The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".
Remove Duplicate Faces	During the configured period, the duplicate faces are displayed only once, to avoid repeated counting. Click to configure the parameter, and then click **Apply**. • **Time**: During the configured time, the function is enabled. • **Precision**: The larger the precision value, the higher the accuracy.

Parameter	Description
Face Matting	Set a range for the captured face image, including face, one-inch picture, and custom. When selecting **Custom**, click , configure the parameters on the prompt interface, and then click **Apply**. ● Customized width: Set snapshot width; enter the times of the original face width. It ranges from 1–5. ● Customized face height: Set face height in snapshot; enter the times of the original face height. It ranges from 1–2. ● 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 cuts out the face image only.
Snap Mode	● General mode: ◇ **Optimized Snapshot**: Capture the clearest picture within the configured time after the camera detects face. ◇ **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 using this mode in access control scene. Click **Advanced** to set the optimized time. ● Counting mode: The snapshot mode is tripwire by default, and you cannot change it.
Property	Click next to **Property** to enable the properties display.
Face Beautifying	Enable **Face Beautifying** to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Enable **Face Exposure**. When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.
Advanced	● **Snapshot Angle Filter**: Set snapshot angle to be filtered during the face detection. ● **Snapshot Sensitivity**: Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity. ● **Optimized Time**: Set a period to capture the clearest picture after the camera detects face.

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

8.2.2 Setting Face Database

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

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

8.2.2.1 Creating Face Database

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

Procedure

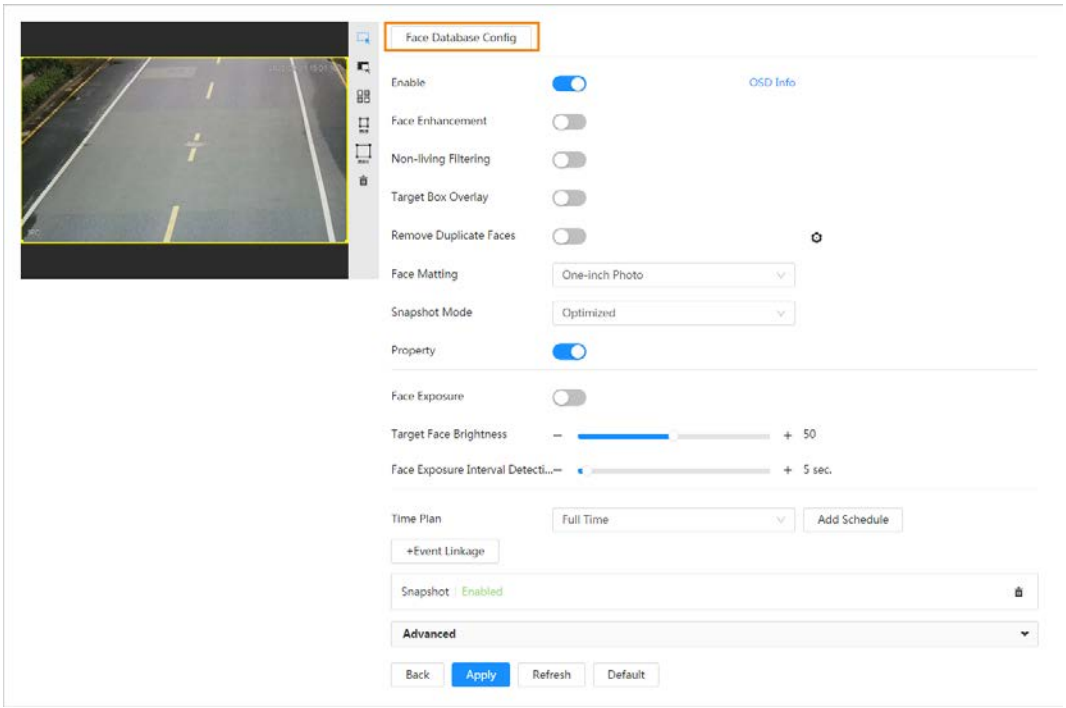
Step 1 Select **AI** > **Smart Plan**.

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

Step 3 Select the detection mode.

Step 4 Click **Face Database Config** on the **Face Recognition** interface.

Figure 8-7 Face database configuration



Step 5 Click **Add Face Database**.

Step 6 Set the name of the face database.

Figure 8-8 Add face database



Step 7 Click **OK**.

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

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



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

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



- 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.

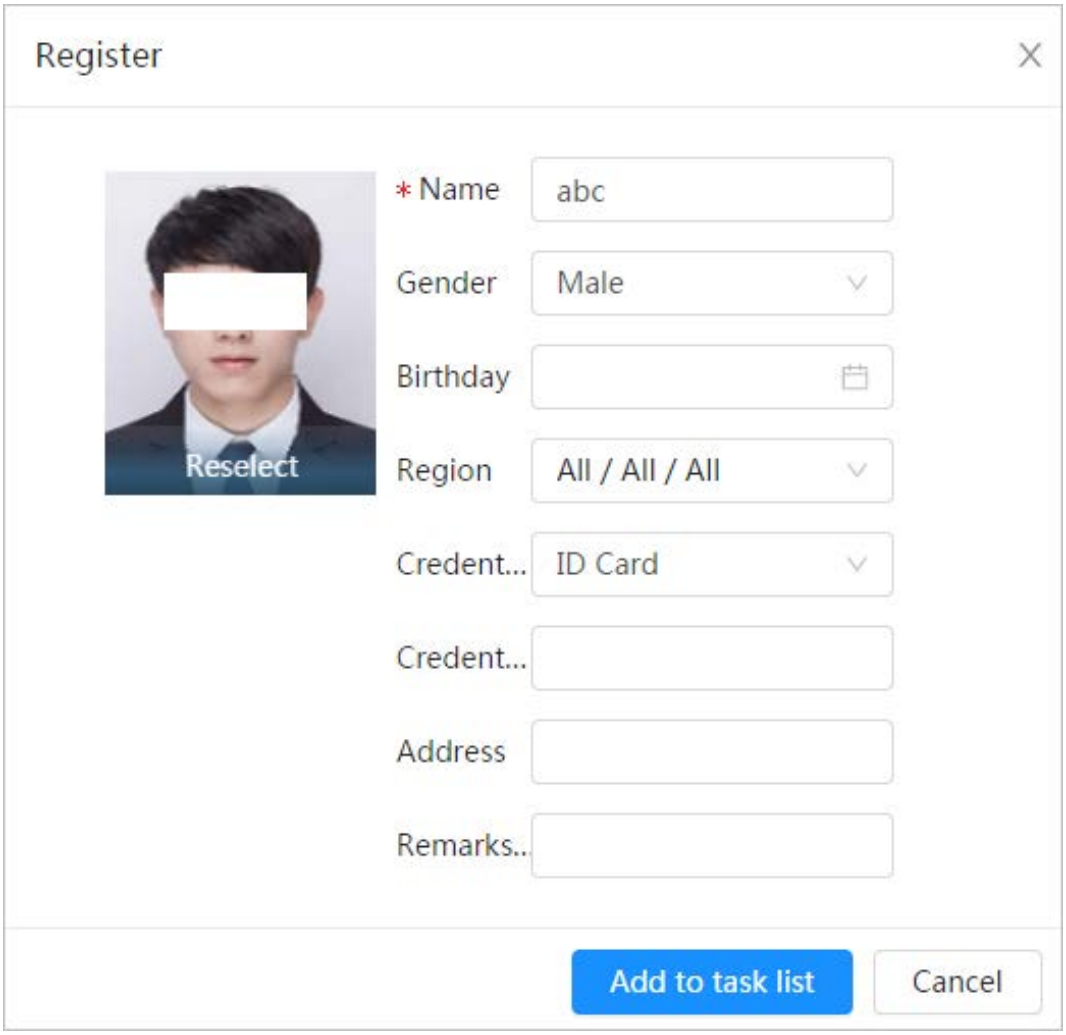
Step 1 On the **Face Database Config** interface, click next to the face database to be configured.

Step 2 Click **Register**.

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

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

Figure 8-11 Register



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

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

Step 6 Click 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 interface. For details, see Table 8-3. For face modeling operation, see "8.2.2.4 Face Modeling".

Table 8-3 Description of error code

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

8.2.2.2.2 Batch Importing

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

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

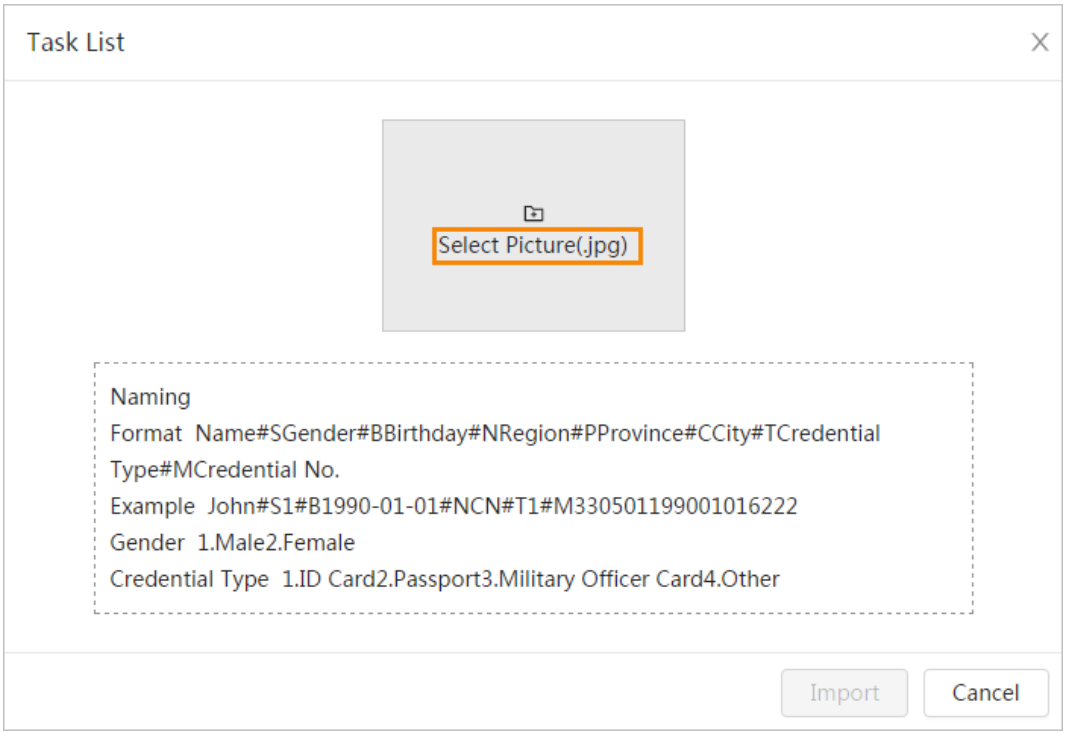
Parameter	Description
Name	Enter a name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Credentials Type	"1" is ID card and "2" passport.
ID number	Enter ID No.

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

Step 2 Click **Batch Register**.

Step 3 Click **Select Picture**, and select storage path of the file.

Figure 8-12 Task list



Step 4 Click **Import** to import the face pictures.

After the importing is completed, the result will be displayed.

- If the picture is imported successfully, click **Next** to do modeling operation.
- If the picture importing failed, click **Query** to view the details of the pictures and error code. For details, see Table 8-3.

  Click **Export** to export the error details.

Step 5 Click **Next** to do modeling operation.

The modeling result is displayed. If modeling failed, click **Query** and the failure details will be displayed in the list. Point to the modeling status to view the details. Then you can change picture according to the failure reason. For modeling details, see "8.2.2.4 Face Modeling".

8.2.2.3 Managing Face Picture

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

8.2.2.3.1 Editing Face Information

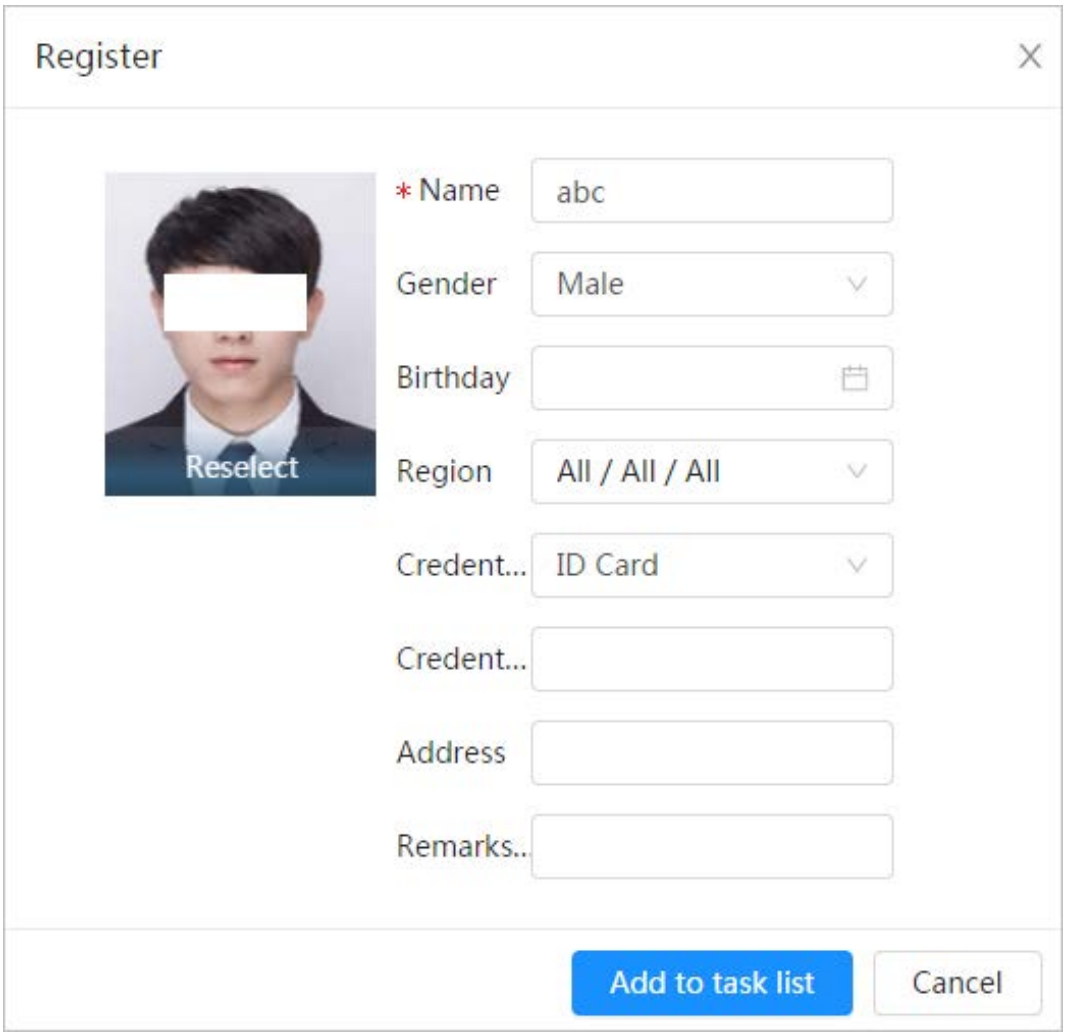
Step 1 On the **Face Database Config** interface, click next to the face database to be configured.

Step 2 Click **Query**, set the criteria as needed, and then click **Search**.

Step 3 Select the row where the face picture or the personnel information is located, and then click .

Step 4 Edit face information according to the actual need. Click **Add to task list**.

Figure 8-13 Face information modification



Step 5 Click Task List 1, and then click **Operation**.

8.2.2.3.2 Deleting Face Picture

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

- Single delete: Select the row where the face picture or the personnel information is located, and click to delete the face picture.
- Batch delete: Select at the upper-right corner of the face picture or of the row where the personnel information is located. Select the information, click **Delete**, then click Task List 2, 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

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.

- 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.

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

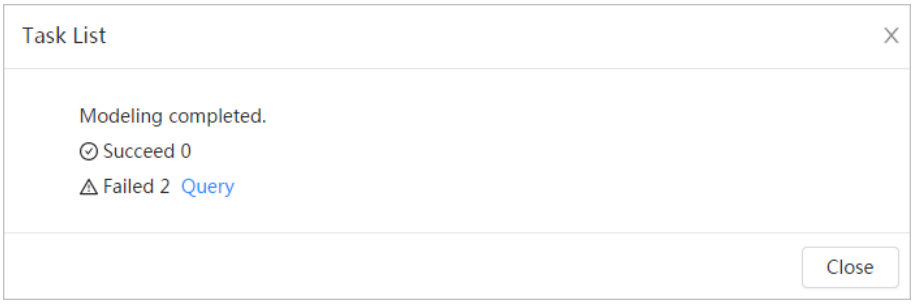
Step 2 Start modeling.

- Selective modeling.
  If there are many face pictures in the face database, you can set search criteria to select the pictures that need to be modeled.
  1. Set the search criteria, and click **Search**.
  2. Select the face pictures to be modeled.
  3. Click **Modeling**.
- All modeling.
  Click **Modeling All** to complete modeling of all face pictures in the face database.

Step 3 View the modeling result.

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

Figure 8-14 Failed modeling



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

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

8.2.3 Setting Arming Alarm

When face recognition succeeded or failed, the device links alarm out.

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

Step 2 Arm face database.

1) Click next to **Arm** to enable the face database arming.
   The snapshot will be compared to the pictures in the armed face database.
2) Set the similarity.

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

Figure 8-15 Arm alarm

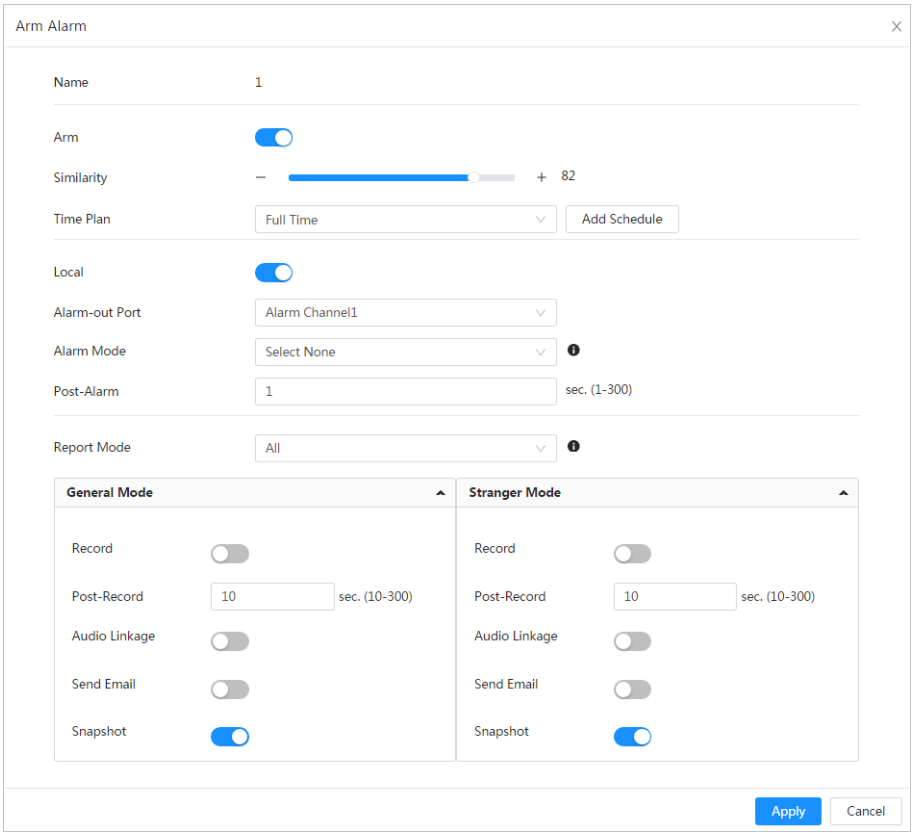


Figure 8-16 Arm alarm (all people)

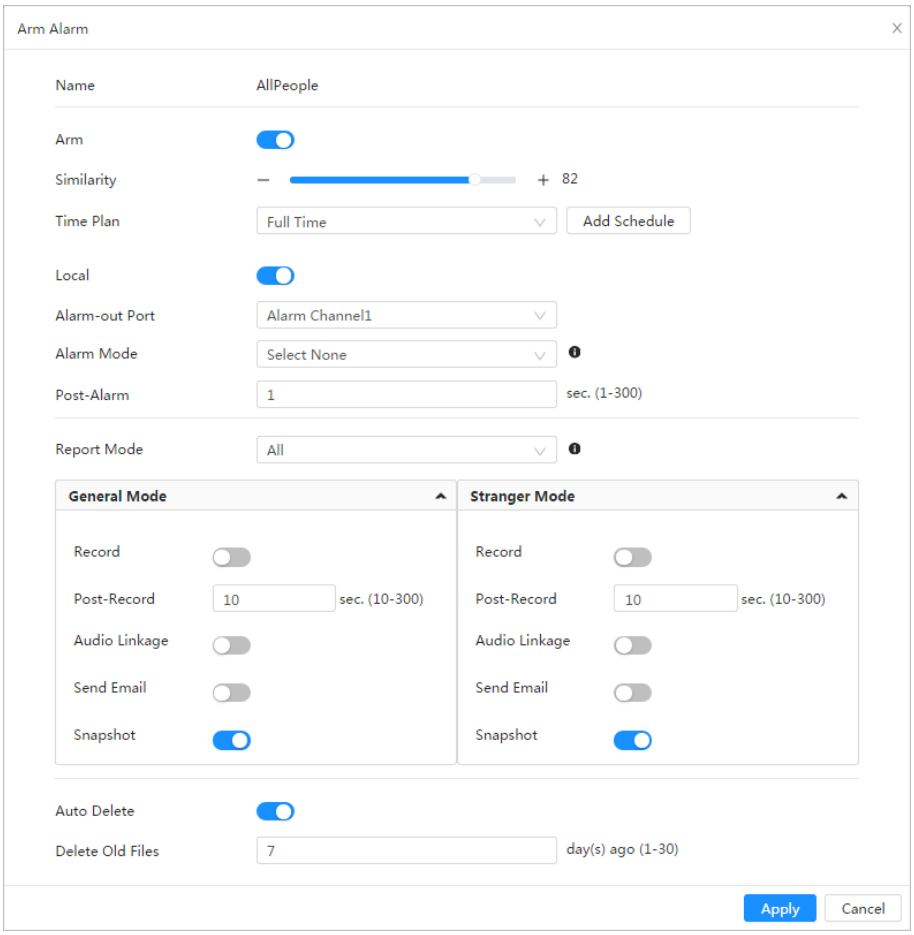
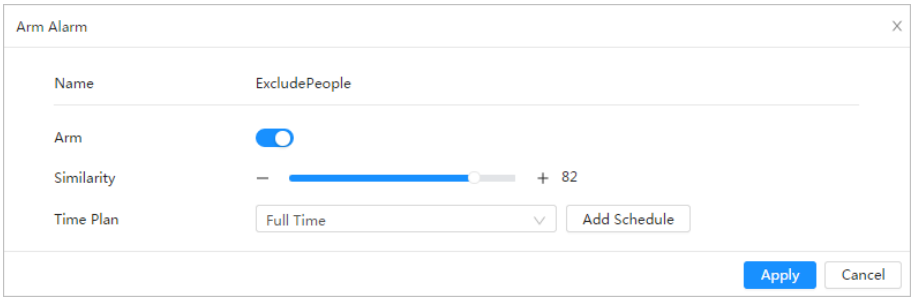


Figure 8-17 Arm alarm (exclude people)



Step 3 Set arming periods.

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

Table 8-5 Local alarm output

Parameter	Description
Alarm-out Port	For the device with multiple alarm-out channels, select the channels as needed.

Parameter	Description
Alarm Mode	● All: No matter the comparison result of the detected face and that in the face database, the camera links alarm out. ● General: The camera links alarm out when the detected face matches that in the face database, the camera links alarm out. ● Stranger: The camera links alarm out when the detected face fails to match that in the face database, the camera links alarm out. ● 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.
Post-Alarm	When alarm delay is configured, alarm continues for the defined period after the alarm ends.

Step 5 Select the report mode and alarm linkage action.

- There are four report modes:
  - ◇ All: The camera reports events no matter the comparison result of the detected face and that in the face database, and then configure the linkage action in **General Mode** and **Stranger Mode**.
  - ◇ General: The camera reports events when the detected face matches that in the face database, and then configure the linkage action in **General Mode**.
  - ◇ Stranger: The camera reports events when the detected face fails to match that in the face database, and then configure the linkage action in **Stranger Mode**.
  - ◇ Select none: The camera does not report events no matter the comparison result of the detected face and that in the face database. You do not need to configure any linkage action.
- Set alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

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

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

This function is only available on the all people database.

Step 7 Click **Apply**.

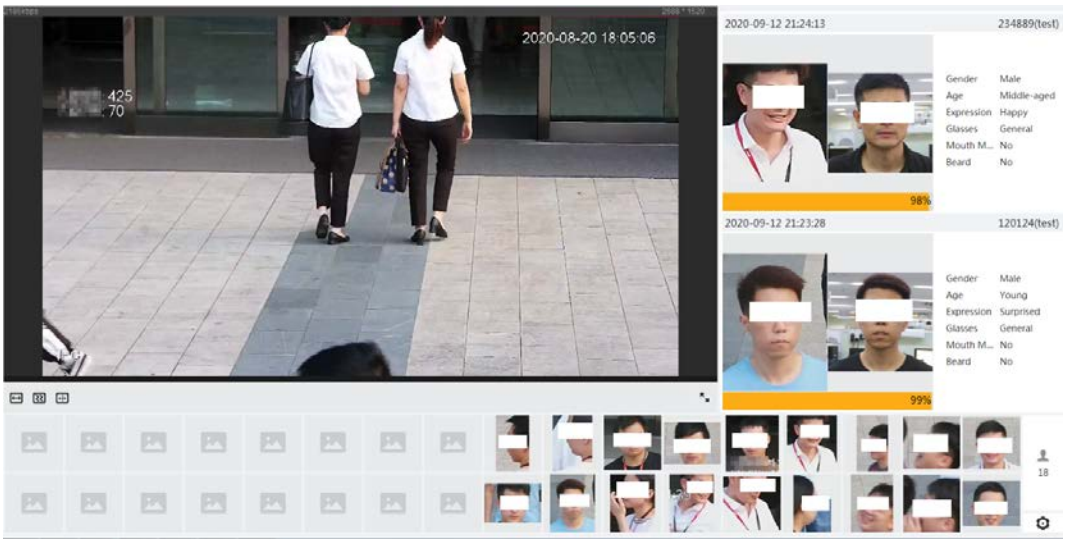
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

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 8-18 Face recognition result



8.3 Setting Face Detection

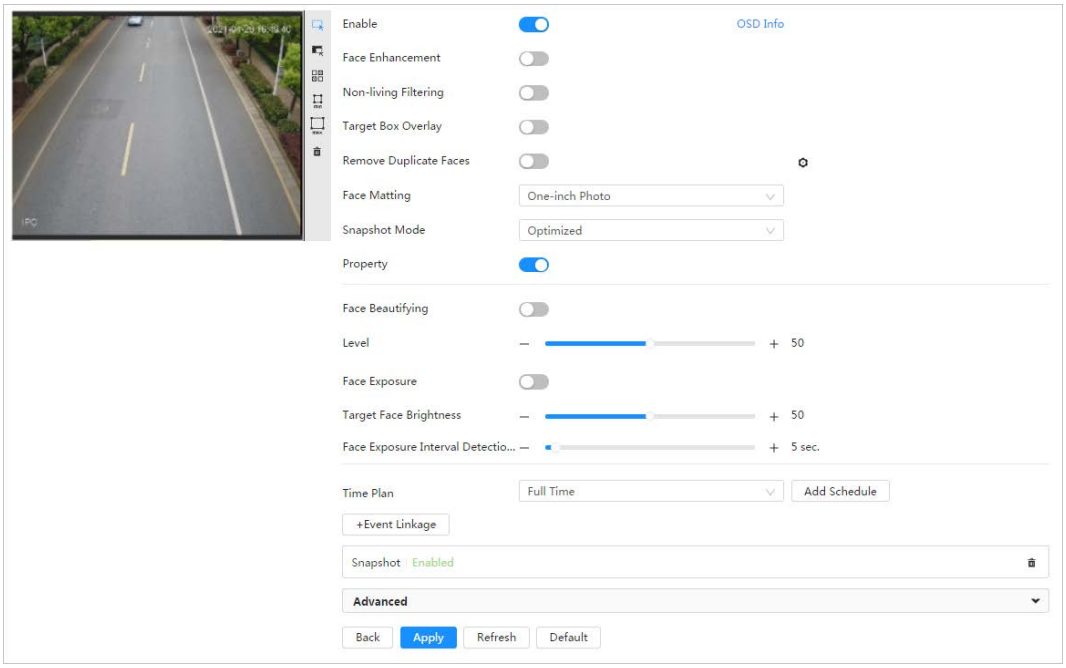
When a face is detected in the detection area, the system performs an alarm linkage.

Procedure

Step 1 Select **AI** > **Smart Plan**.

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

Figure 8-19 Face detection



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

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

- Click to draw a face detection area in the image. The detection area is the whole image by default.
- Click to draw an exclusion area for face detection in the image.

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

Step 5 Set parameters.

Table 8-6 Description of face detection parameters

Parameter	Description
OSD Info	Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the face statistics function. The number of detected faces is displayed on the **Live** interface. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click  to enable face enhancement, and it can preferably guarantee clear face with low stream.
Target Box Overlay	Click  to enable the function, and 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".
Face Matting	During the configured period, the duplicate faces are displayed only once, to avoid repeated counting. When selecting **Custom**, click , configure the parameters on the prompt interface, and then click **Apply**. • Customized width: Set snapshot width; enter the times of the original face width. It ranges from 1–5. • Customized face height: Set face height in snapshot; enter the times of the original face height. It ranges from 1–2. • 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.
Snap Mode	• **Optimized Snapshot**: Capture the clearest picture within the configured time after the camera detects face. • **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. It is recommended to use this mode in access control scene.  Click **Advanced** to set the optimized time.
Property	Click  next to **Property** to enable the properties display.

Parameter	Description
Advanced	• **Snapshot Angle Filter**: Set snapshot angle to be filtered during the face detection. • **Snapshot Sensitivity**: Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity. • **Optimized Time**: Set a period to capture the clearest picture after the camera detects face.
Face Exposure	Click next to **Face Exposure**. When a face is detected, the camera can enhance brightness of the face to make the face image clear.
Face Target Brightness	Set the face target brightness. It is 50 by default.
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. It is five seconds by default.

Step 6 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

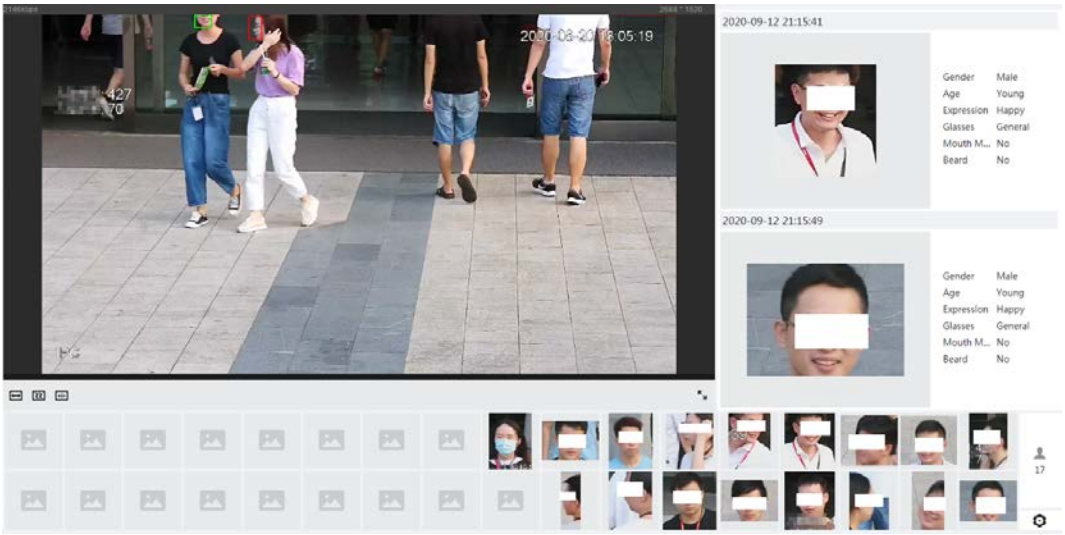
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

Result

The face detection result is displayed on the live interface.

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

Figure 8-20 Face detection result



8.4 Setting IVS

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

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 more than 10 × 10 pixels. The size of abandoned object in the image should be no less than 15 × 15 pixels (CIF image). The target height and width

should no more than a third of the image height and width. The recommended target height is 10% of the image height.

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

8.4.1 Global Configuration

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

Calibration Purpose

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

Applicable Scene

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

Notes

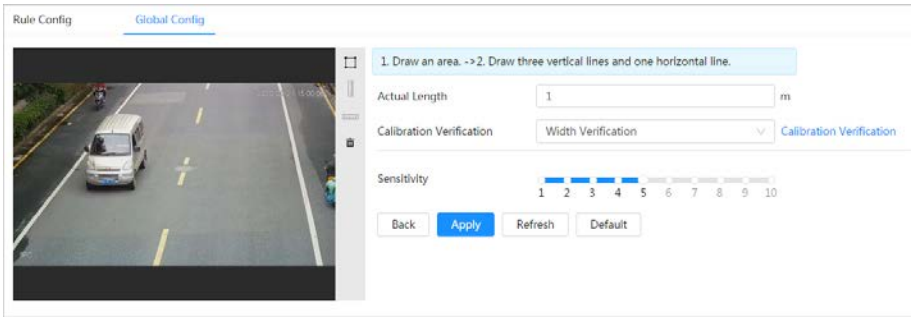
- Calibration Drawing
  - ◇ Calibration area: The calibration area drawn should be on one horizontal plane.
  - ◇ Vertical ruler: The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such as vehicle parked at roadside or road lamp poles. Arrange three persons to draw at each of the three positions in the monitoring scene.
  - ◇ Horizontal ruler: Select reference object with known length on the ground, such as sign on the road, or use a tape to measure the actual length.
- Calibration Verification
  After setting the ruler, draw a straight line on the image, check the estimated value of the straight line, and then compare this value with the value measured in the actual scene to verify calibration accuracy. In case of major difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

Procedure

1. Select **AI** > **Smart Plan**.
2. Click  next to **IVS** to enable IVS of the corresponding channel, and then click **Next**.

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

Figure 8-21 Global configuration of IVS



4. Set calibration area and ruler.
   a. Click and draw a calibration area in the image, and right-click to finish the drawing.
   b. Click the ruler icon to draw one horizontal ruler and three vertical rulers in the calibration area.
      - indicates vertical ruler, and indicates horizontal ruler
      - Select an added ruler, and click to delete the ruler.
5. Set the sensitivity.
   Adjust the filter sensitivity. With higher value, it is easier to trigger an alarm when low-contrast object and small object are captured, and the false detection rate is higher.
6. Click **Apply**.

Result

1. Select the verification type, and then click **Calibration Verification**.
   To verify vertical ruler and horizontal ruler, respectively select **Height Verification** and **Width Verification**.
2. Draw a straight line in the image to verify whether the rulers are correctly set.
   In case of big difference between the estimated value and the actual one, fine-tune or reset parameters until the error requirement is met.

8.4.2 Rule Configuration

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

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

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

Table 8-7 Description of IVS functions

Rule	Description	Applicable Scene
Tripwire	When the target crosses tripwire from the defined motion direction, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.

Rule	Description	Applicable Scene
Intrusion	When the target enters, leaves, or appears in the detection area, an alarm is triggered, and the system performs configured alarm linkages.	
Abandoned object	When an object is abandoned in the detection area over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. ● Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. ● In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
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.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. ● Missed alarm might increase in the scenes with dense targets, frequent occlusion, and people staying. ● In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Fast moving	When the motion speed is higher than the configured speed, an alarm is triggered, and then the system performs configured alarm linkages.	Scene with sparse targets and less occlusion. The camera should be installed right above the monitoring area. The light direction should be vertical to the motion direction.
Parking detection	When the target stays over the configured time, an alarm is triggered, and then the system performs configured alarm linkages.	Road monitoring and traffic management.

Rule	Description	Applicable Scene
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.

Step 1 Select **AI** > **Smart Plan**.

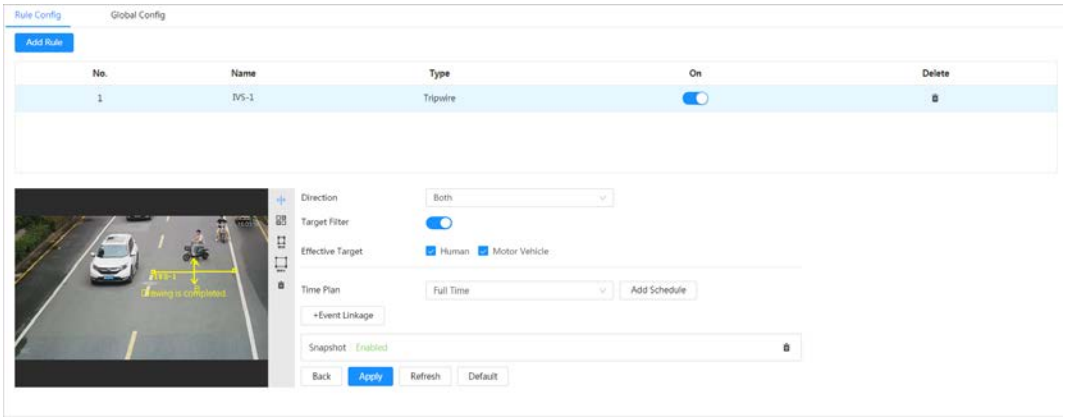
Step 2 Click next to **IVS** to enable IVS of the corresponding channel, and then click **Next**.

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

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

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

Figure 8-22 Tripwire



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

For requirements of drawing rules, see Table 8-7. After drawing rules, drag corners of the detection area to adjust the area range.

Table 8-8 Description of IVS analysis

Rule	Description
Tripwire	Draw a detection line.
Intrusion	Draw a detection area. • During the detection of abandoned object, the alarm is also triggered if pedestrian or vehicle stays for a long time. If the abandoned object is smaller than pedestrian and vehicle, set the target size to filter pedestrian and vehicle or properly extend the duration to avoid false alarm triggered by transient staying of pedestrian.
Abandoned object	
Missing object	
Fast moving	
Parking detection	
Crowd gathering	

Rule	Description
Loitering detection	● During the detection of crowd gathering, false alarm might be triggered by low installation height, large percentage of single person in an image or obvious target occlusion, continuous shaking of the camera, shaking of leaves and tree shade, frequent opening or closing of retractable door, or dense traffic or people flow.

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

- Click  to draw the minimum size of the target, and click  to draw the maximum size of the target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- When the rule of crowd gathering is configured, you do not need to set target filter, but draw the minimum gathering area. Click  to draw the minimum gathering area in the scene. The alarm is triggered when the number of people in the detection area exceeds the minimum area and the duration.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click  to delete the detection line.

Step 7 Set rule parameters for IVS.

Table 8-9 Description of IVS parameters

Parameter	Description
Direction	Set the direction of rule detection. ● When setting tripwire, select **A->B**, **B->A**, or **A<->B**. ● When setting intrusion, select **Enter**, **Exit**, or **Both**.
Action	When setting intrusion action, select **Appears** or **Cross**.
Target Filter	Click  to enable this function. ● When you select **Human** as the alarm target, an alarm will be triggered when the system detects that persons trigger the rule. ● When you select **Motor Vehicle** as the alarm target, alarm will be triggered when the system detects that vehicle triggers the rule.
Duration	● For abandoned object, the duration is the shortest time for triggering an alarm after an object is abandoned. ● For missing object, the duration is the shortest time for triggering an alarm after an object is missing. ● For parking detection, crowd gathering, or loitering detection, the duration is the shortest time for triggering an alarm after an object appears in the area.
Sensitivity	● For fast moving, sensitivity is related to the triggering speed. Lower sensitivity requires faster moving speed to trigger the alarm. ● For crowd gathering, sensitivity is related to the alarm triggering time. It is easier to trigger the alarm with higher sensitivity.

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

8.5 Setting Vehicle Density

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

Background Information

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

Procedure

Step 1 Select **AI** > **Smart Plan**.

Step 2 Click next to **Vehicle Density**, and then click **Next**.

Step 3 Click **Add Rule** to select rules.

Figure 8-23 Add rules



Step 4 (Optional) Click other icons at the right side of the image to draw detection area on the image.

- Click to draw a detection area in the image. The detection area is the whole image by default.
- Click , and then press and hold the left mouse button to draw a rectangle, the pixel size is displayed.
- Click to delete the detection line.

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

Figure 8-24 Vehicle density (traffic congestion)

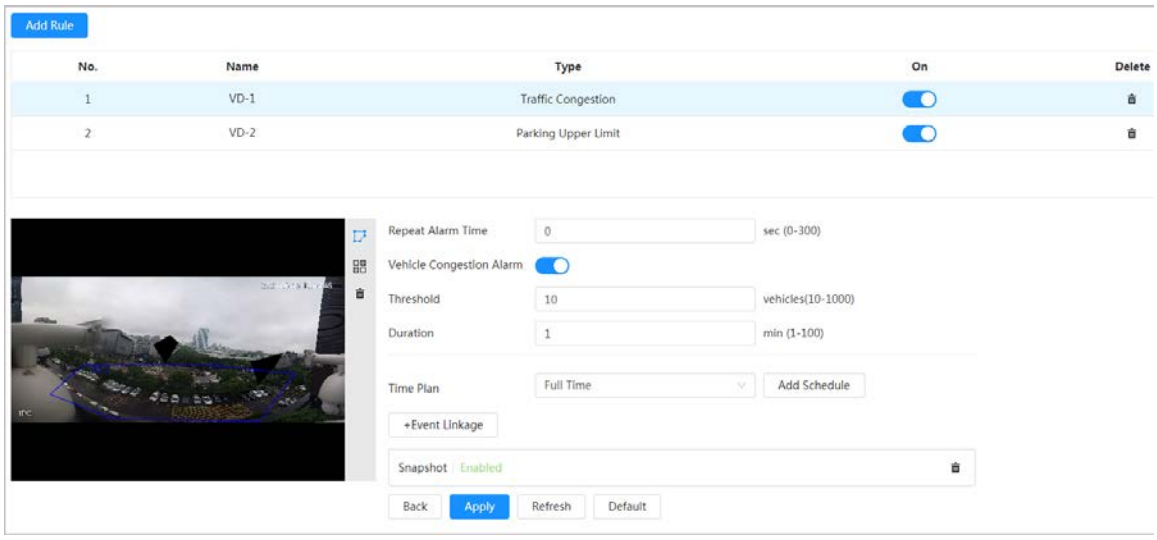
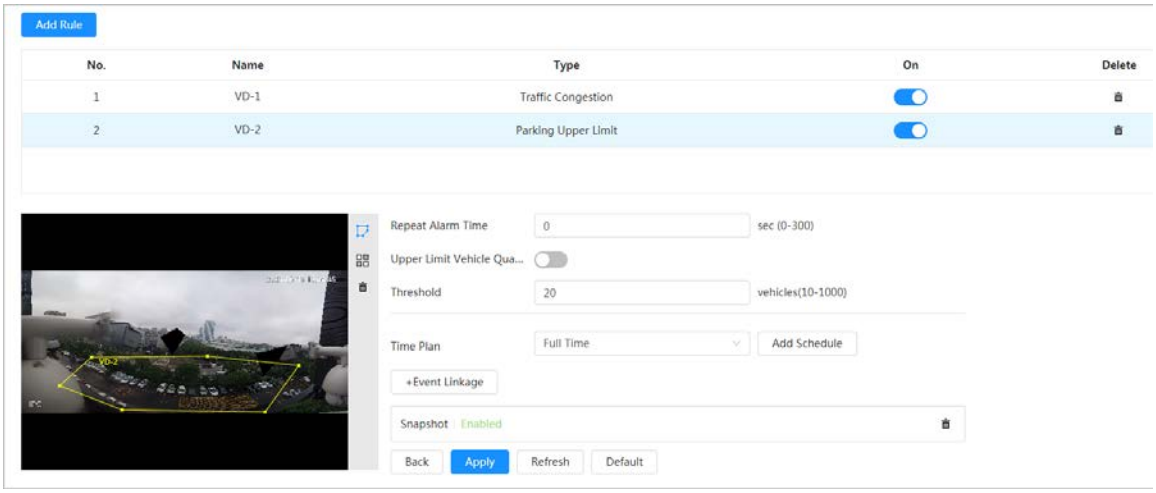


Figure 8-25 Vehicle density (parking upper limit)



Step 5 Set parameters.

Table 8-10 Description of parameters

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

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

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **Event Linkage** to add linked event and set linkage parameters. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

8.6 Setting Parking Space

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

8.6.1 Rule Configuration

Set planned or open type for parking space.

Step 1 Select **AI** > **Smart Plan**.

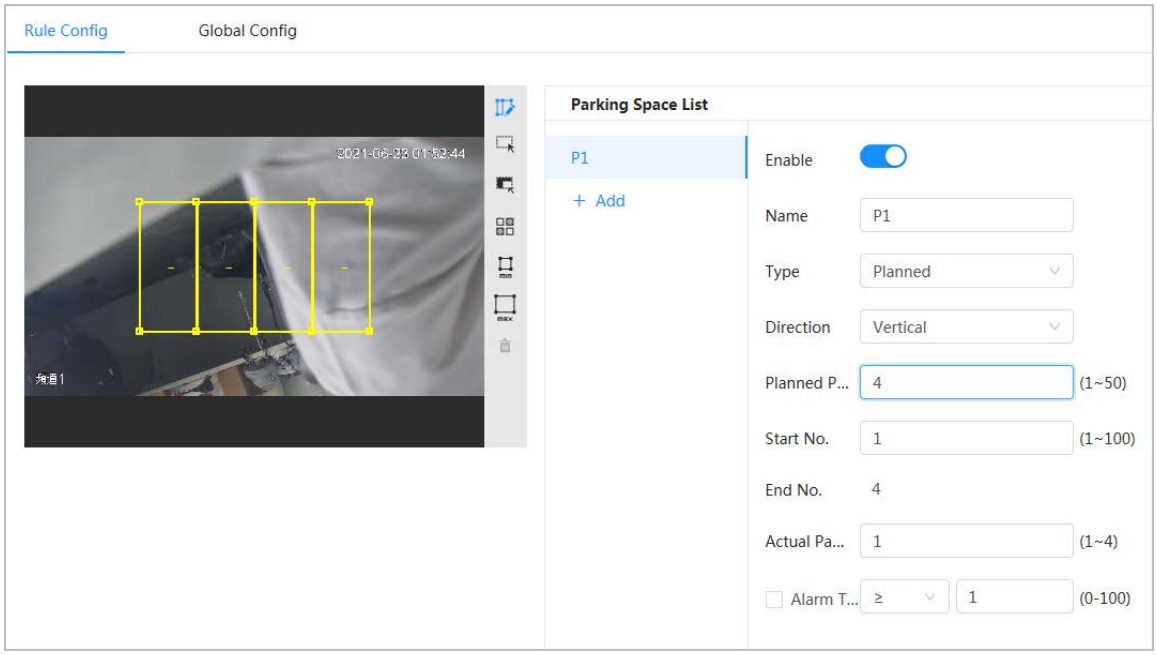
Step 2 Click next to **Parking Space**, and then click **Next**.

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

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

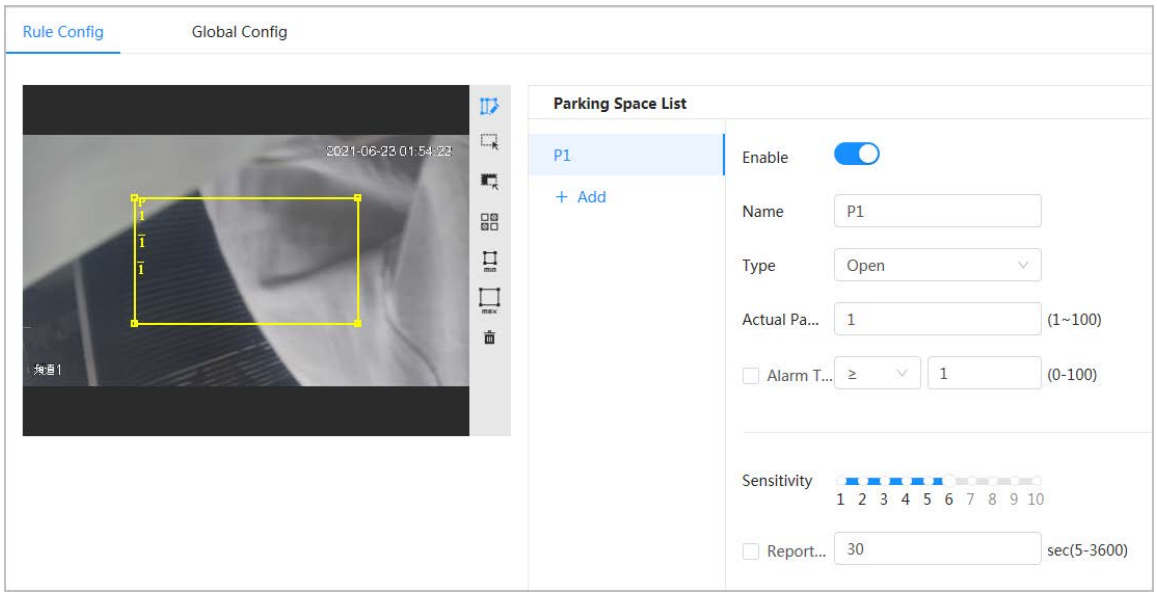
- Click to draw the rectangle area.
  - ◇ If you select planned parking space, the rectangle area will be divided equally according to the planned parking spaces number that you configured.

Figure 8-26 Rule configuration (1)



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

Figure 8-27 Rule configuration (2)



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

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

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

Figure 8-28 Planned parking space

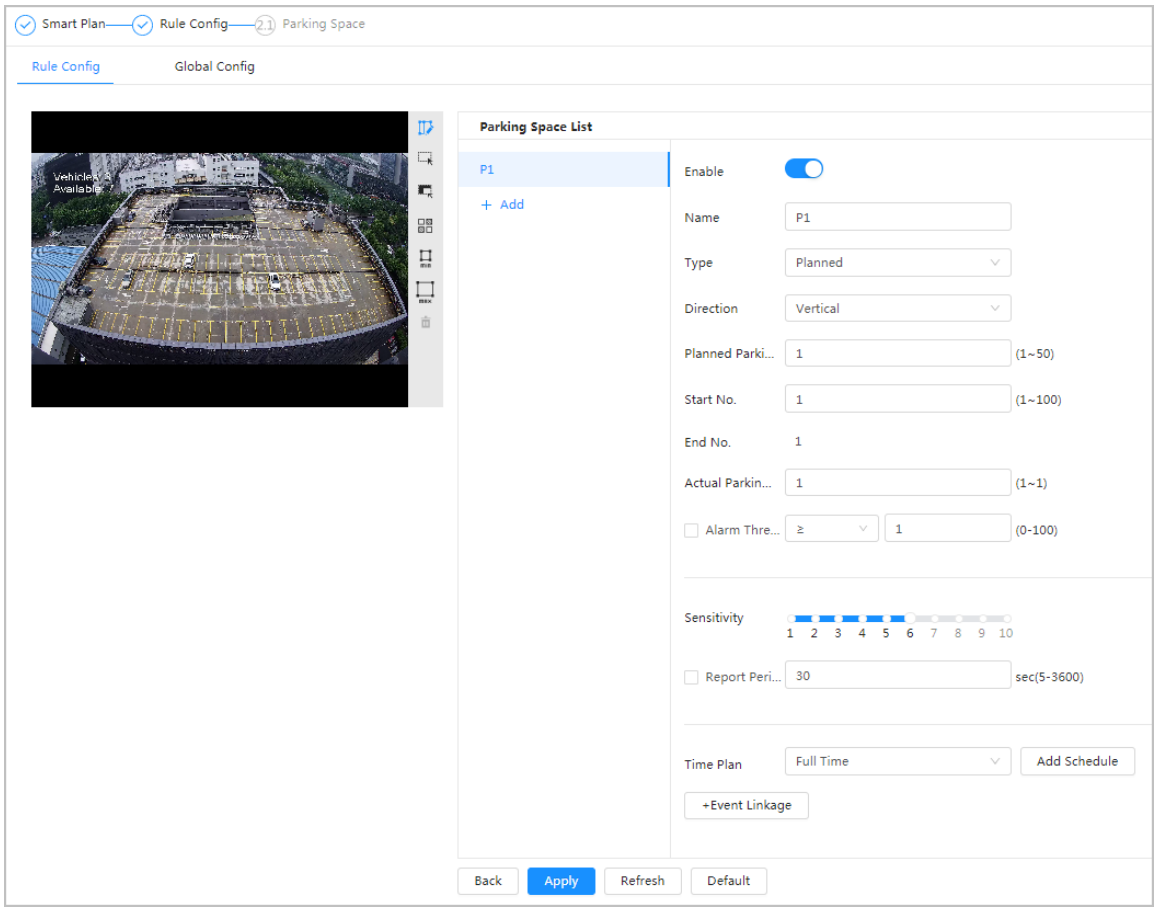


Table 8-11 Description of planned parking space parameters

Parameter	Description
Name	Enter the name of the added parking space.
Direction	You can select **Vertical** or **Horizontal** direction.
Planned Parking Space	It can be used to divide the initial quadrilateral equally, which is convenient for you to draw the rule box
Start No.	Associates with the name of parking spaces.
End No.	Associates with **Planned Parking Space**.
Actual Parking Space	It ranges from 1 to the configured value of planned parking space. **Actual Parking Space** is 1 by default.
Alarm Threshold	You can set it from 0 through 100. When alarm is triggered, the frame of related statistic area will flash red. And the threshold number is 0 by default.
Sensitivity	Adjust the false alarm and miss alarm of the system. And the sensitivity is 6 by default.
Report Period	The report period is 30 seconds by default. And you can set it between 5 to 3600 seconds. It will only upload related data but not pictures or videos.

- Open Parking Space

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

Figure 8-29 Open parking space parameters

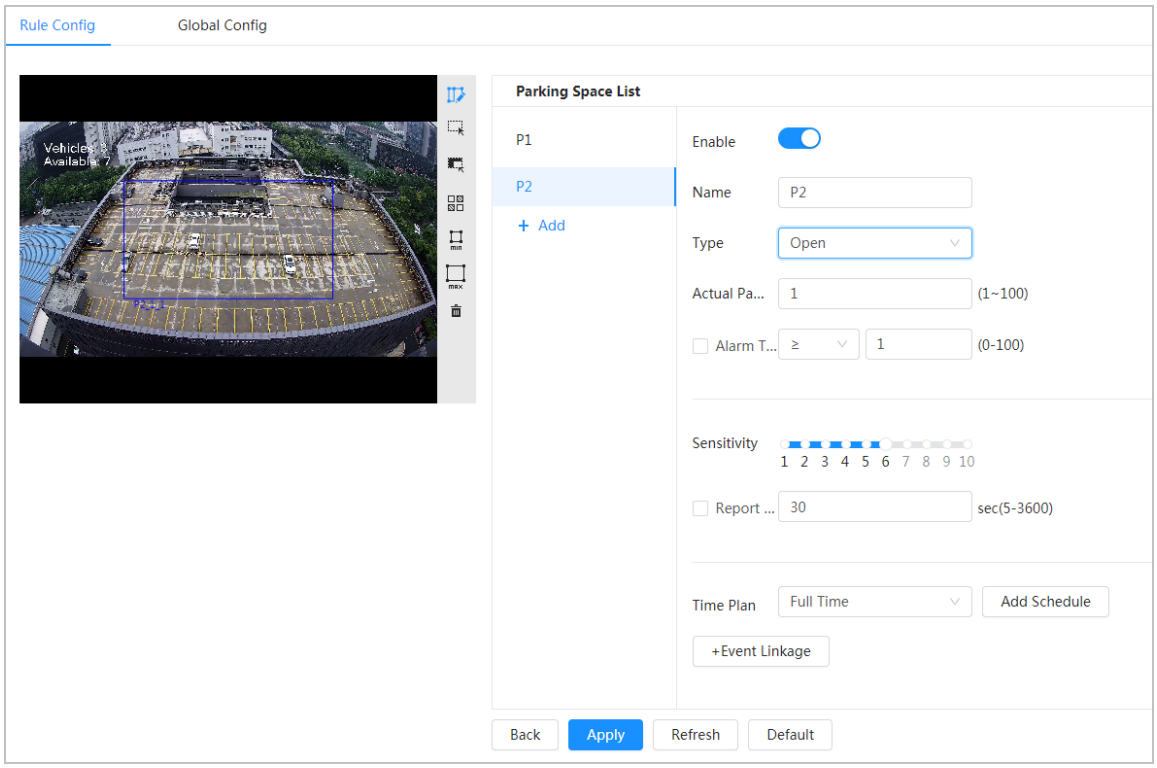


Table 8-12 Description of open parking space parameters

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

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

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **+Event Linkage** to add linked event and set linkage parameters. For details, see "6.4.1.2 Alarm Linkage".

Step 7 Click **Apply**.

8.6.2 Global Configuration

Step 1 (Optional) Set OSD information.

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

Step 2 Adjust confidence level.

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

Step 3 Click **Apply**.

8.7 Setting Video Metadata

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

8.7.1 Global Configuration

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

Step 1 Select **AI** > **Smart Plan**.

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

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

Step 4 Set parameters.

Figure 8-30 Global configuration of video metadata

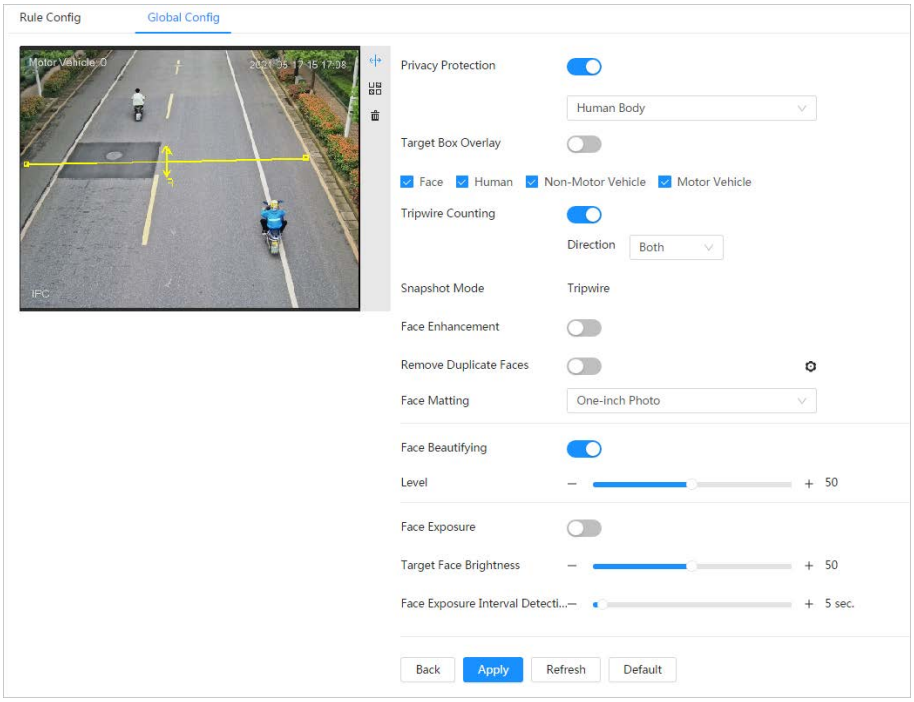


Table 8-13 Description of scene set parameters (video metadata)

Parameter	Description
Privacy Protection	Enable this function, and the faces and bodies will be blurred by mosaic or color blocks when they are detected.

Parameter	Description
Target Box Overlay	Overlay target box on the captured pictures to mark the target position. Four 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".
Tripwire Counting	Enable this function, and set the tripwire direction. The snapshot mode is **Tripwire** by default, and you cannot change it. will be displayed beside the image on the **Rule Config** interface. You can draw the rule as needed.
Face Enhancement	Click next to **Face Enhancement** to preferably guarantee clear face with low stream.
Remove Duplicate Faces	During the configured period, the face that detected several times is displayed only once, to avoid repeated counting. Click to set the parameters, and then click **Apply**. • Time: The function is valid within the configured period. • Precision: The larger the value is, the higher the accuracy will be.
Face Matting	Set a range for matting face image, including face picture and one-inch picture.
Face Beautifying	Enable **Face Beautifying** to make face details clearer at night. After enabling this function, you can adjust the level. The higher the level, the higher the beautifying level.
Face Exposure	Enable **Face Exposure** 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.
Scene	Set scene as **Distant View** or **Close View**.

Step 5 Click **Apply**.

8.7.2 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 **Clobal Config** interface.

Procedure

Step 1 Select **AI** > **Smart Plan**

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

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

Step 4 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.

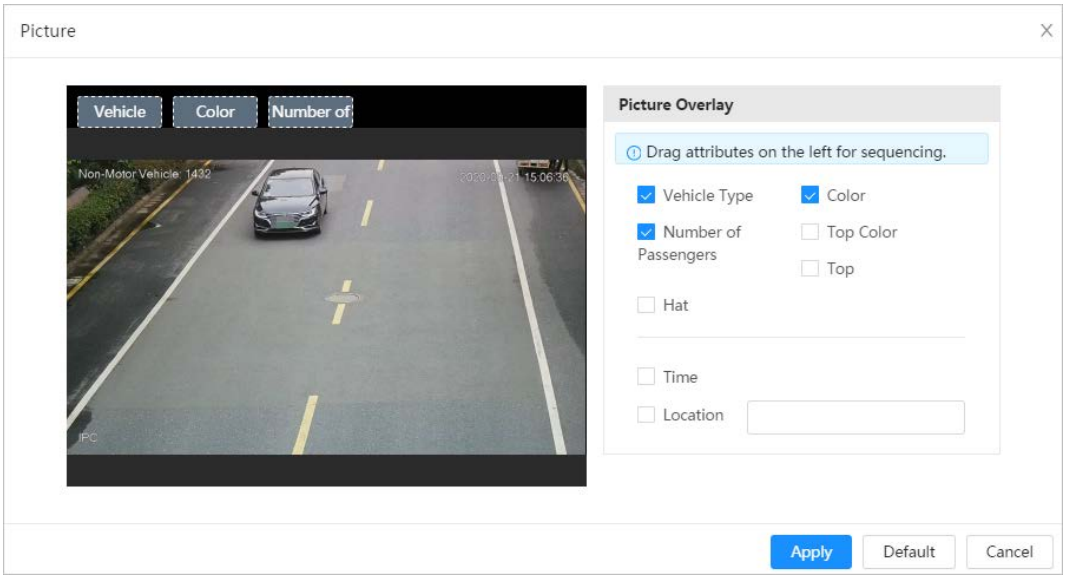
Figure 8-31 Rule configure (video metadata)



Step 5 Configure **Picture**.

1) Click .
2) Set overlay of motor vehicle, non-motor vehicle and people and the box position. This section takes the configuration of non-motor vehicle overlay as an example.

Figure 8-32 Picture (non-motor vehicle)



3) Click **Apply**.

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

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

Step 7 Set parameters.

Table 8-14 Description of crowd map parameters

Parameter	Description
People Flow Statistics	Click next to **People Flow Statistics** to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click next to **Flow Statistics (Non-motor Vehicle)** to count the number of non-motor vehicles in the detection area.
Traffic Flow Stat	Click next to **Traffic Flow Statistics** to count the number of motor vehicles in the detection area.
OSD	Click **OSD Info**, and the **Overlay** interface is displayed. Click next to **Enable** to enable the target statistics function. For details, see "6.2.2.2.8 Configuring Target Statistics".
Snapshot Mode	• Optimized: Capture the pictures until the vehicle disappears from the image, and report the clearest picture. • Tripwire: Capture the pictures when the vehicle triggers tripwire as the configured direction. 1. Select **Tripwire**. 2. Select the direction from **A to B**, **B to A**, and **Both**. 3. Adjust the position of rule line as needed.

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

8.7.3 Viewing Video Metadata Report

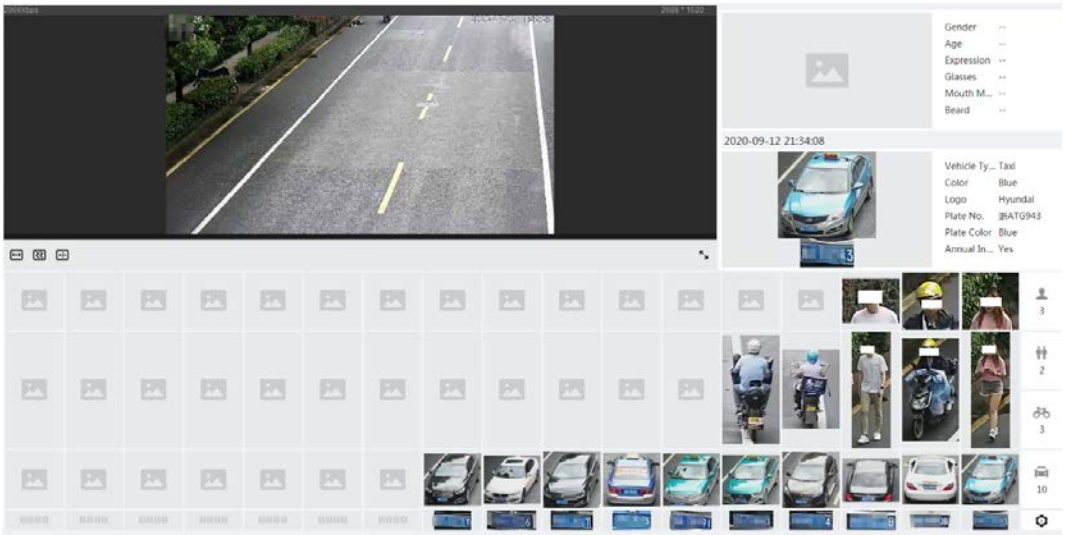
Generate data of video metadata recognition in report form.

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

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

Step 3 Click **Search** to complete the report.
The statistical results are displayed. Click **Export** to export the statistical report.

Figure 8-33 Video metadata report



8.8 Setting People Counting

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

8.8.1 People Counting

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

Background Information

There are two types of people counting rules.

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

Procedure

Step 1 Select **AI** > **Smart Plan**

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

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

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

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

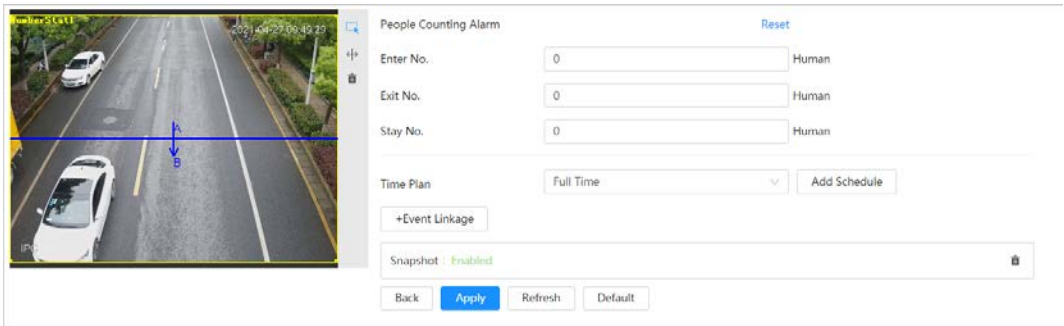
Figure 8-34 Add rule



Step 5 Draw a detection area in the image.

- People counting
  1. 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.
  2. Click to draw rule line in the image.
     When targets enter or leave the detection area along the direction line, they will be counted.

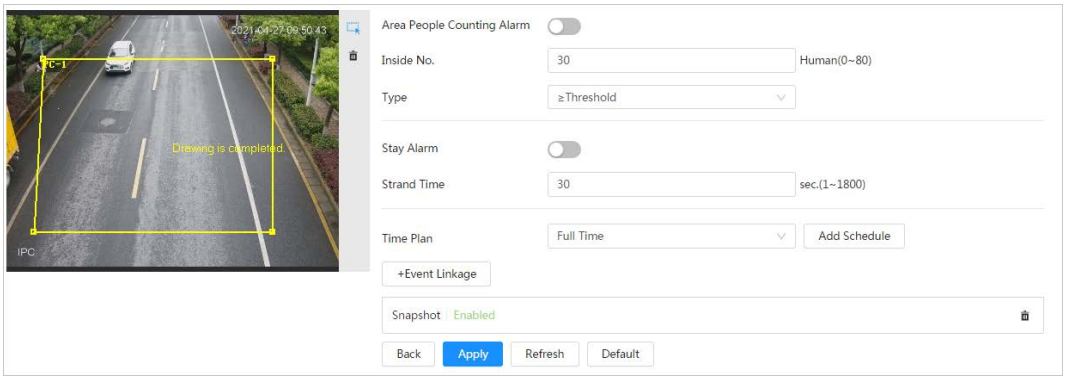
Figure 8-35 People counting (1)



- Area people counting

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

Figure 8-36 People counting (2)



Step 6 Set parameters.

Table 8-15 Description of people counting parameters

Parameter	Description	
People counting	Enter No.	Counts the number of people entering in the direction A-->B. When the number exceeds the configured value, an alarm will be triggered.
	Exit No.	Counts the number of people entering in the direction B-->A. When the number exceeds the configured value, an alarm will be triggered.
	Stay No.	It is the difference between the **Enter No.** and **Exit No.**. When the number exceeds the configured value, an alarm will be triggered.
	Clear	Clears the counted number.
Area people counting	Area people counting	Enable the area people counting function.
Inside Number	Set the number of people in the people counting region. When the people count reaches the configured value, an alarm will be triggered. When you set inside number to 0, and select**≥ Threshold** in **Type**, the system will not perform the alarm linkage.	
Type		
Stay Alarm	Select the **Stay Alarm** check box, and then set the stay time, when the stay duration exceeds the configured value, an alarm will be triggered.	
Strand Time		

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

Result

You can view the counting results on the **Live** interface.

- For **People Counting** rule, the entry and exit numbers are displayed.
- For **Area People Counting** rule, the inside number is displayed.

Figure 8-37 Counting result



8.8.2 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**

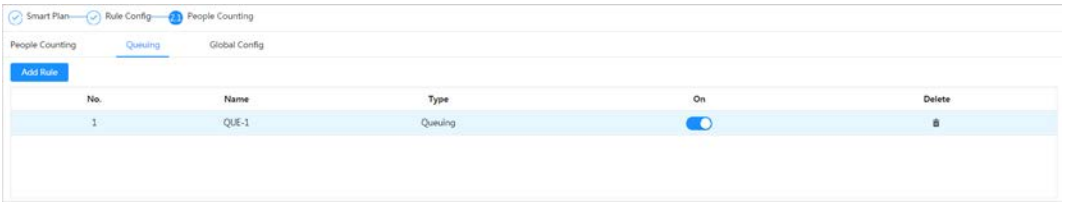
Step 2 Click next to **People Counting**, and then click **Next**.

Step 3 Click the **Queuing** tab.

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

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

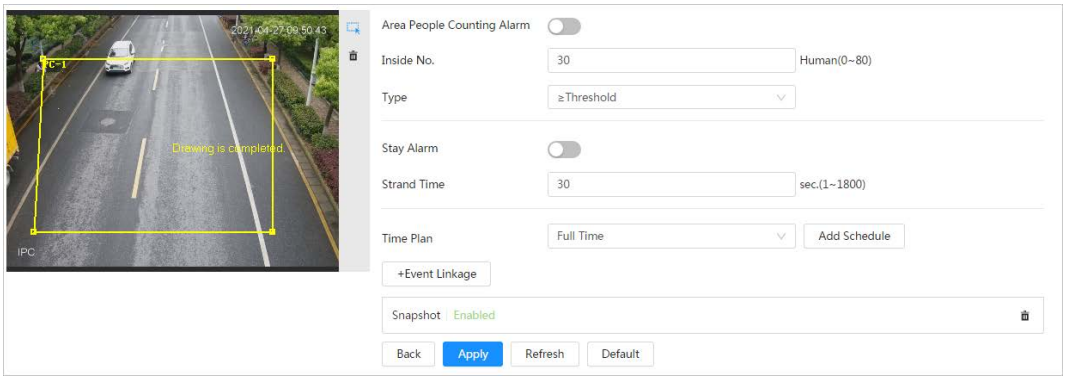
Figure 8-38 Add rule



Step 5 Draw a detection area in the image.

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

Figure 8-39 Queuing



Step 6 Set parameters.

Table 8-16 Description of queuing

Parameter	Description
Queue People No. Alarm	Enable the queue people No. alarm function.
Queue People No.	
Type	Set the queue people number for triggering the alarm and counting type. When the queue people number reaches the configured value, an alarm will be triggered.
Queue Time Alarm	Enable the queue time alarm function.
Queue Time	Set the queue time. When the queue time reaches the configured value, the alarm is triggered.

Step 7 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Click **+ Event Linkage** to set the linkage action.

Step 8 Click **Apply**.

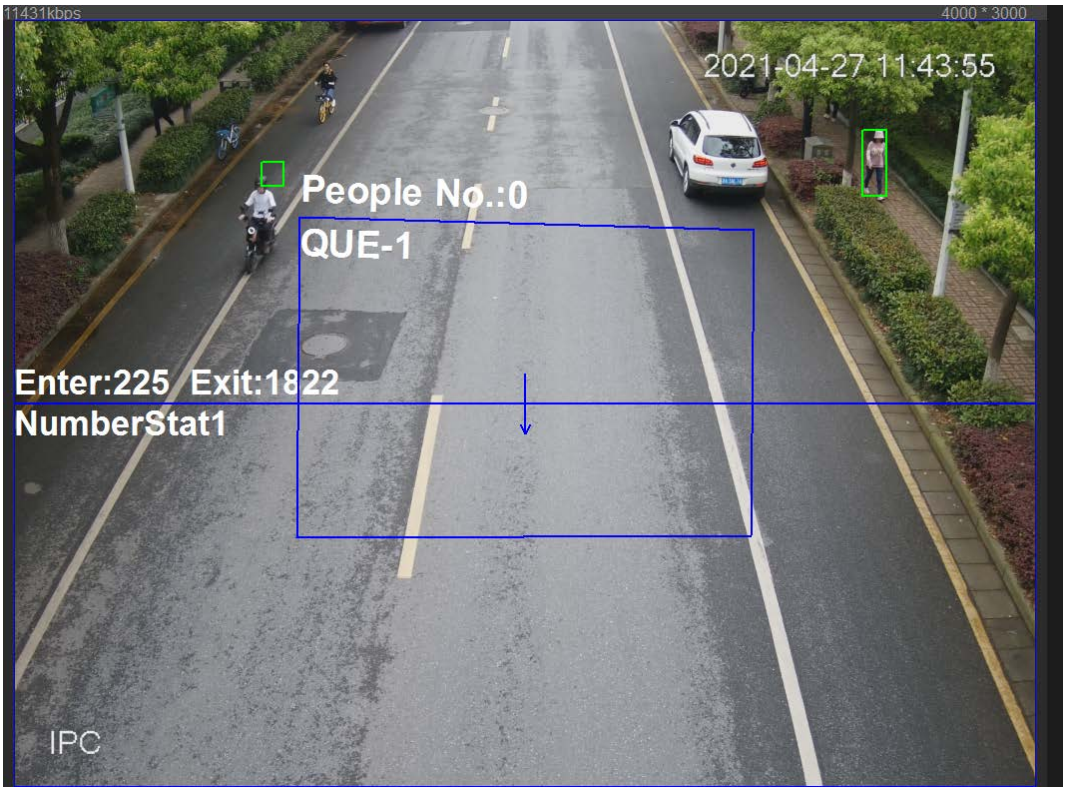
To view alarm information on the alarm subscription tab, you need to subscribe relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

Result

You can view the queuing results on the **Live** interface.

The queuing number and the stay time of each target are displayed on the interface.

Figure 8-40 Queuing result



8.8.3 Global Configuration

Set the sensitivity of each people counting rule.

Procedure

Step 1 Select **AI** > **Smart Plan**

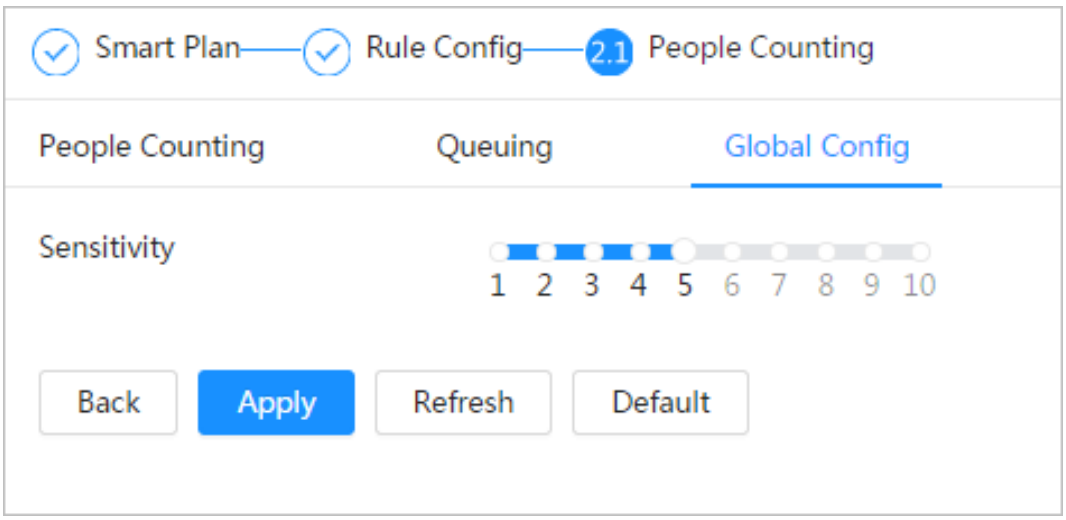
Step 2 Click next to **People Counting**, and then click **Next**.

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

Step 4 Set the sensitivity.

The higher the sensitivity, the easier the detection, but the more the false detections.

Figure 8-41 Global configuration



Step 5 Click **Apply**.

8.9 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.

8.9.1 Global Configuration

Set the global configuration of face & body detection, including face parameter and scene parameter.

Step 1 Select **AI** > **Smart Plan**.

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

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

Step 4 Set parameters.

Figure 8-42 Global configuration of face & body detection

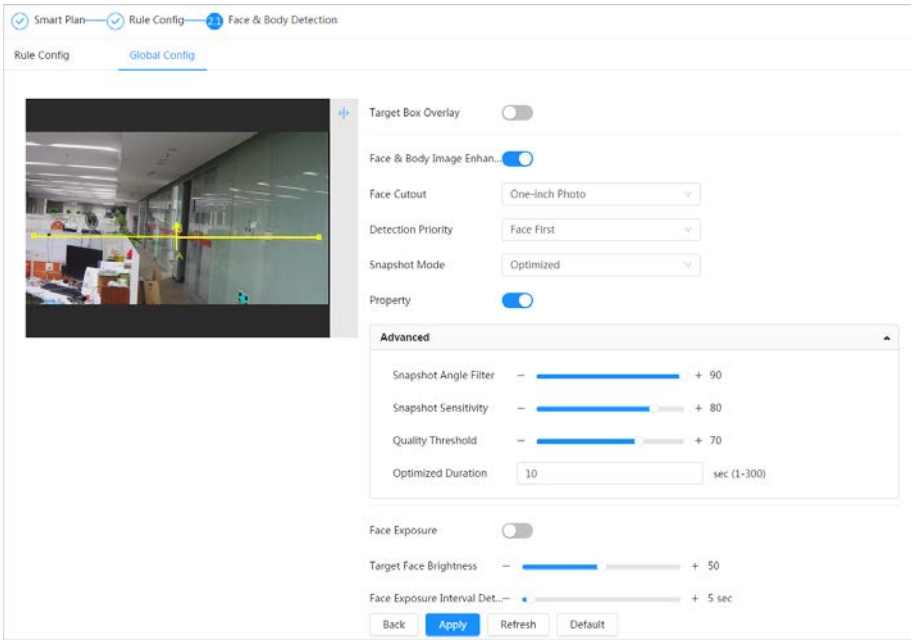


Table 8-17 Description of scene set parameters (face & body detection)

Parameter	Description
Target Box Overlay	Overlay target box on the captured pictures to mark the target position.
Face & Body Image Enhancement	Click 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**.

Parameter	Description
Snapshot Mode	• **Real-time**: Capture the image when the camera detects a face. • **Optimized**: Capture the clearest image within the configured time after the camera detects face. • **Quality Priority**: After detecting the face image quality is higher than the quality threshold, the camera captures the image. • **Tripwire**: This snapshot is available in **PPE Detection Mode**. Click **Advanced** to set the optimized time and quality threshold.
Property	Click next to **Property** to enable the properties display.
Advance	• **Snapshot Angle Filter**: Set snapshot angle to be filtered during the face detection. • **Snapshot Sensitivity**: Set snapshot sensitivity during the face detection. It is easier to detect face with higher sensitivity. • **Optimized Time**: Set a period to capture the clearest picture after the camera detects face.
Face Exposure	Click next to **Face Exposure** to make face clearer by adjusting lens aperture and shutter.
Target Face Brightness	Set the face target brightness, and it is 50 by default.
Face Exposure Interval Detection Time	Set the face exposure interval detection time to prevent image flickering caused by constant adjustment of face exposure. It is 5 seconds by default.

Step 5 Click **Apply**.

8.9.2 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** interface.

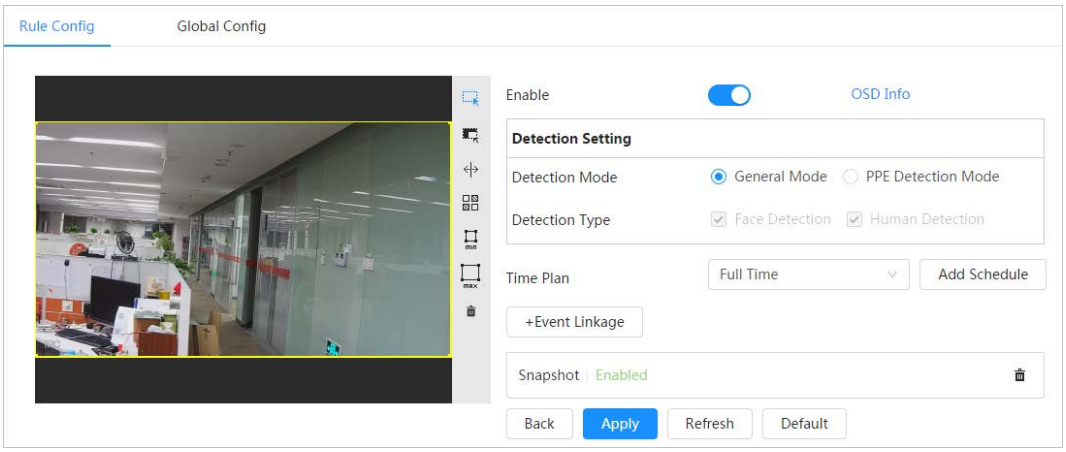
Procedure

Step 1 Select **AI** > **Smart Plan**

Step 2 Click next to **Face & Body Detection**, and then click **Next**.

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

Figure 8-43 Rule configuration



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

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

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

Step 6 (Optional) Set OSD information.

Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the face & body counting function. The number of detected faces and bodies is displayed on the **Live** interface. For details, see "6.2.2.2.12 Configuring Face Statistics".

Step 7 Select the detection mode.

- **General Mode** (selected by default): The system will perform an alarm linkage when the camera detects a face or a person.
- **PPE Detection Mode**:
  1. Click **+** next to **AI 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** interface.
  4. Select the alarm mode.
     - ◇ **Match Attributes Alarm**: When the target's properties are compliant with the configured properties, an alarm will be triggered, and the system performs an alarm linkage.
     - ◇ **Mismatch Attributes Alarm**: When the target's properties are not compliant

with the configured properties, an alarm will be triggered, and the system performs an alarm linkage..

Step 8 Set arming periods and alarm linkage action. For details, see "6.4.1.2 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 "6.4.1.3.2 Subscribing Alarm Information".

8.10 Setting Heat Map

Detect the distribution of dynamically moving objects in the target area within a certain period and displays the distribution on a heat map. Color varies from blue to red. The lowest heating value is in blue, and the highest heating value is in red.

Background Information

When mirroring occurs on the camera or the viewing angle changes, original data on the heat map will be cleared.

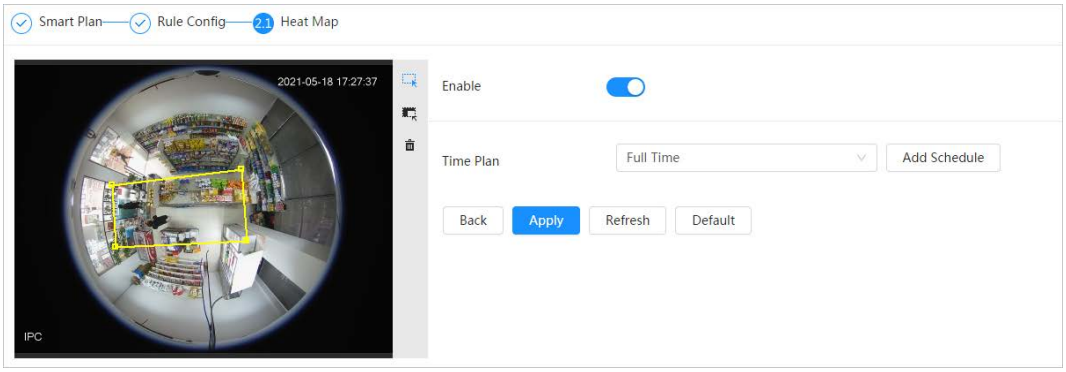
Procedure

Step 1 Select **AI** > **Smart Plan**

Step 2 Click next to **Heat Map**, and then click **Next**.

Step 3 Select the **Enable** check box, and then the heat map function is enabled.

Figure 8-44 Heat Map



Step 4 Draw detection area and exclusion area.

- Click to draw a detection area on the image. Right-click to finish drawing.
- Click to draw an exclusion area on the image. Right-click to finish drawing.
- Click to clear the existing detection area or exclusion area.

Step 5 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Step 6 Click **Apply**.

8.11 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.

8.11.1 Lane Configuration

Configure lane configuration including detection area, lane line, detection line and lane direction.

Procedure

Step 1 Select **AI** > **Smart Plan**.

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

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

Step 4 Click and draw the detection area.

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

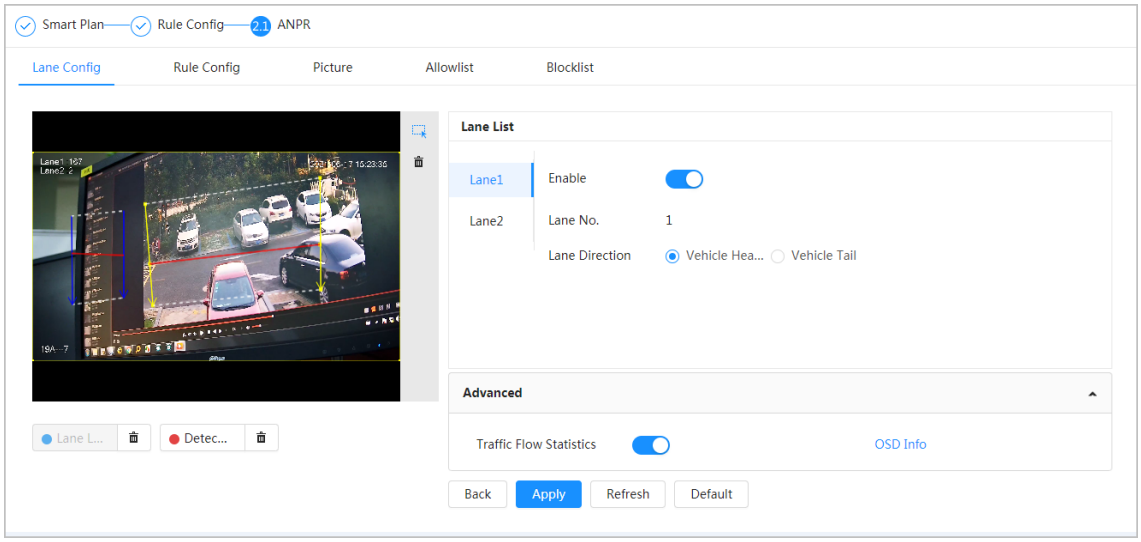
Step 5 Configure lane line information.

- One lane line is composed of two lane lines with an arrow, and the arrow represents the direction of the lane.
- The lane is enabled by default after drawing. If you do not select a lane, the track frame will be displayed on the screen, but the event of license plate recognition will not be reported.
- The lane number of each lane is unique and unchangeable.

Step 6 Select the lane direction.

- **Vehicle Head**: The driving direction of the vehicle in the lane is from top to bottom ↓.
- **Vehicle Tail**: The driving direction of the vehicle in the lane is from bottom to top ↑.

Figure 8-45 ANPR



Step 7 Configure detection line information.

- The detection line is displayed in red and it only available in the drawn lane line.
- When a motor vehicle triggers the detection line, a snapshot will be taken. Also the license plate and its vehicle attributes will be reported.

Step 8 (optional) You can repeat step 4-7 to draw more lane lines and detection lines. You can add two lane lines at most.

Step 9 (optional) Click **Advanced**.

- Click next to **Traffic Flow Statics**. The system only detects the number of motor vehicle and generates report after you enable this function.
- Click **OSD Info**, and the **Overlay** interface is displayed, and then enable the **Parking Space** function. The statistical result is displayed on the **Live** interface. For details, see "6.2.2.2.9 Configuring ANPR".

Step 10 Click **Apply**.

8.11.2 Rule Configuration

When a motor vehicle trigger the lane line associated , the system performs the defined alarm linkage.

Step 1 Select **AI** > **Smart Plan**.

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

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

Step 4 Click lane line to select the line that you configured. If no line is configured, click **Add Lane Line.**

Figure 8-46 Rule configuration (1)

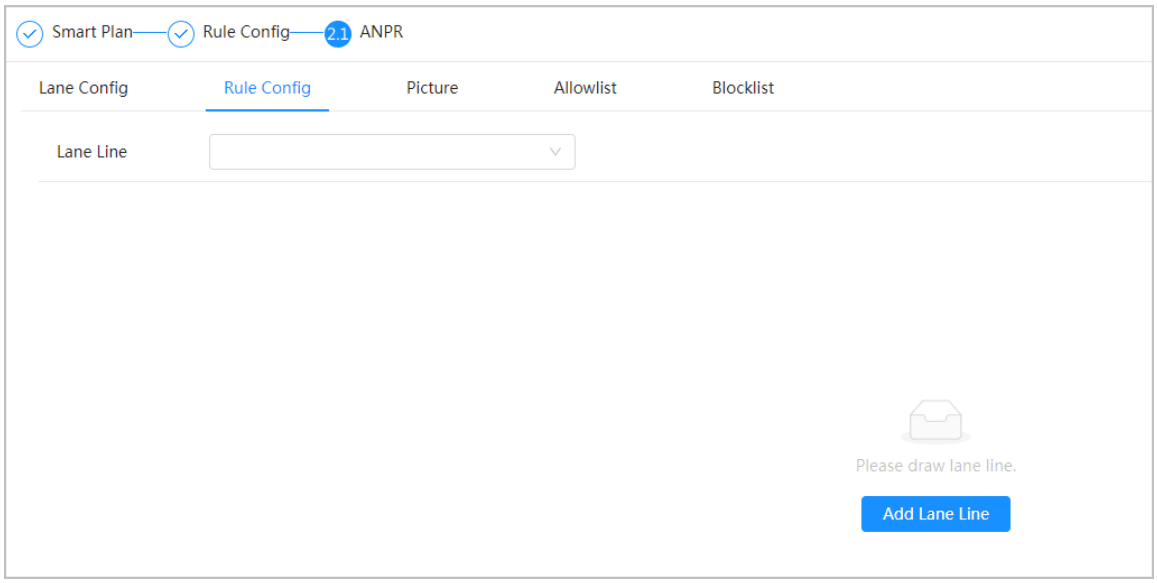
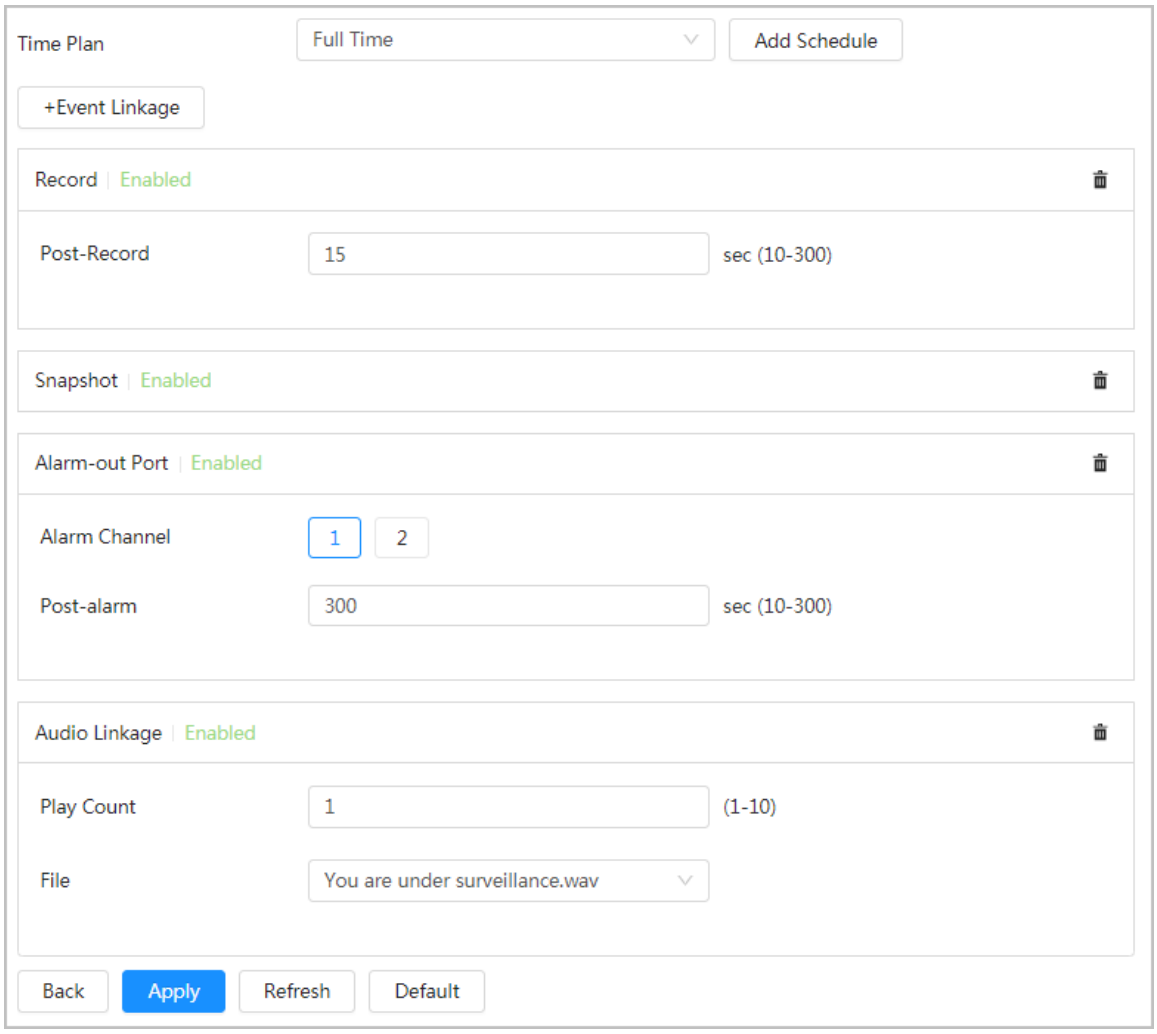


Figure 8-47 Rule configuration (2)



Step 5 Select time plan and click **+ Event Linkage**

- If the added time plan cannot meet your requirements, click **Add Schedule** to add an arming schedule. For details, see "6.4.1.2.1 Adding Schedule".
- Click **+Event Linkage** to add linked event, which support record, send email, snapshot, alarm-out port and audio linkage.

Step 6 Set related alarm linkage.

Step 7 Set audio linkage. For more information, see "6.2.3.2 Setting Alarm Tone"

- Set play count period.
- Select the file needed.

Step 8 (optical) Click to delete related linkage as needed.

Step 9 Click **Apply.**

8.11.3 Picture

Set overlay information and image display position, such as plate number, time, vehicle type, and vehicle logo.

Procedure

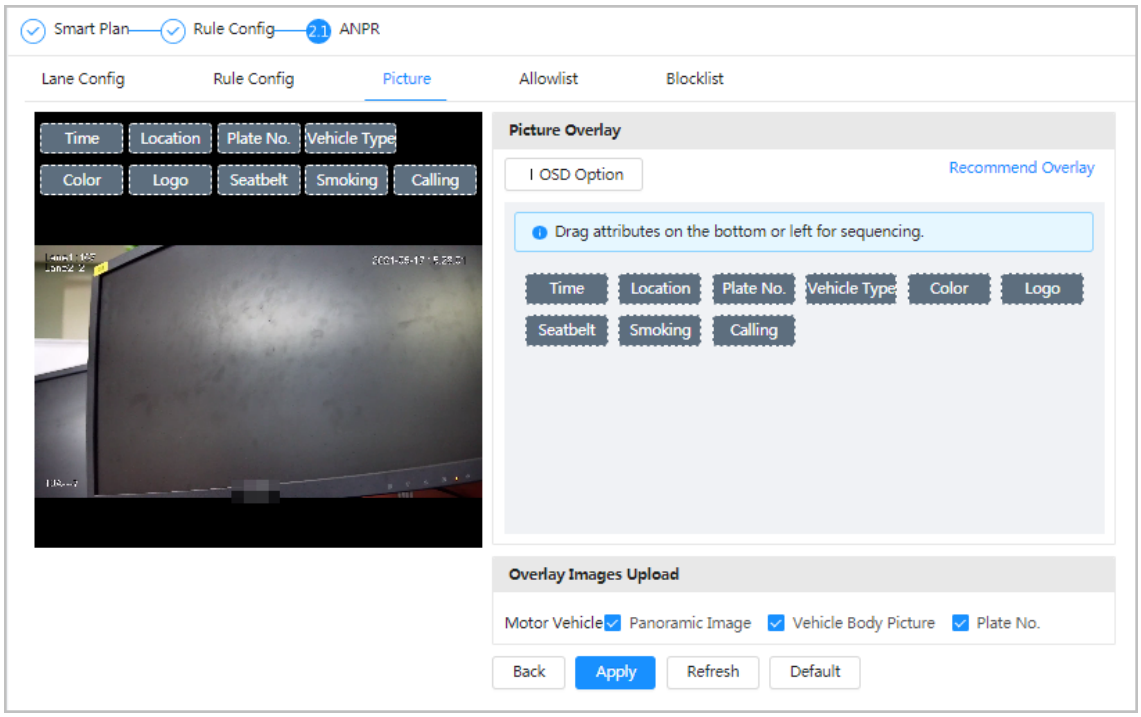
Step 1 Select **AI** > **Smart Plan**.

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

Step 3 Click the **Picture** tab.

Step 4 Click **+ OSD Option** to select the type of overlay information that needs to capture. You can adjust the position of the information displayed.

Figure 8-48 Picture



Step 5 Select the overlay images upload type(s).

Step 6 Click **Apply**.

8.11.4 Allowlist

After enabling allowlist, the camera will upload allowlist event and trigger linkage alarm when it detects the plate number in the allowlist.

Background Information

You can add 10,000 plate information in allowlist at most.

Procedure

Step 1 Select **AI** > **Smart Plan** > **Allowlist**

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

Figure 8-49 Enable allowlist



Step 3 Add allowlist.

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

Figure 8-50 Add allowlist plate

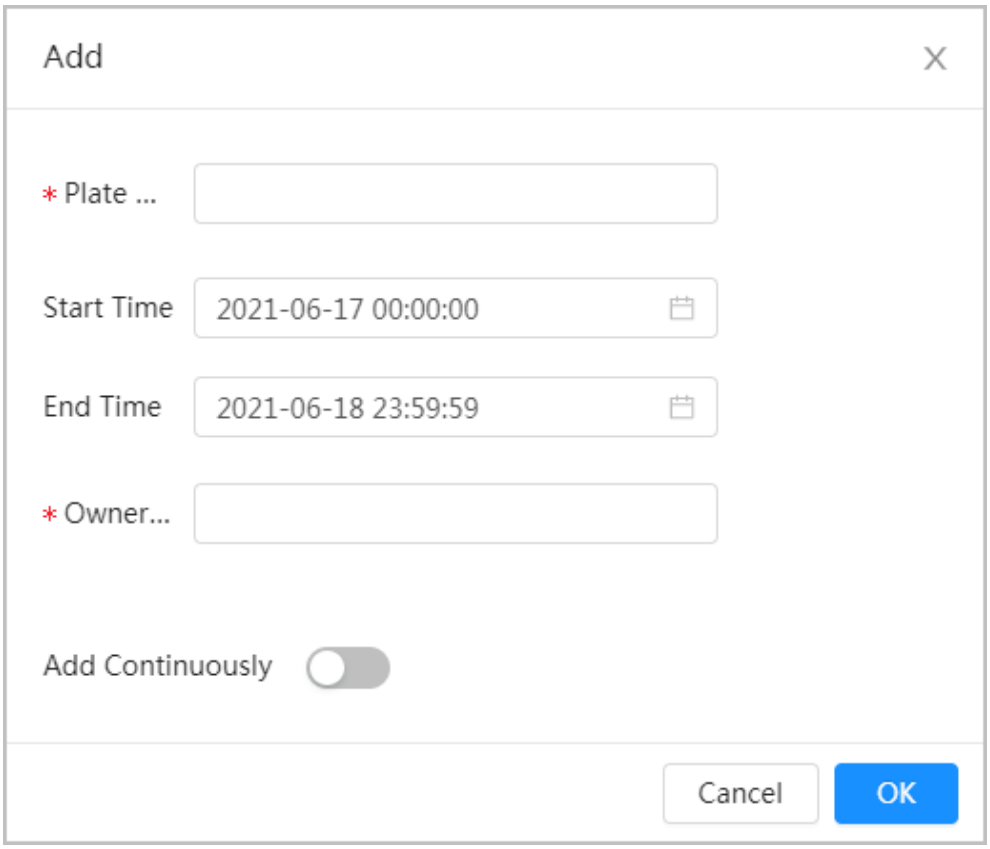


Table 8-18 Description of parameters

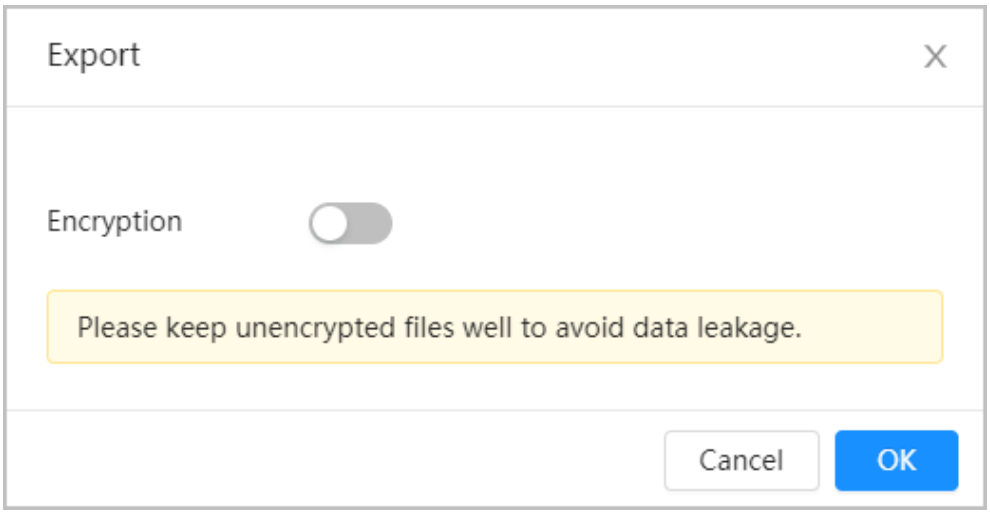
Parameter	Description
Plate No.	Enter the complete plate number.
Start Time/End Time	Set the validity of allowlist for the plate number. After this time range, the vehicle will not be detected even within allowlist.
Owner Name	Enter the name of car owner.

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 8-51 Encryption settings (1)



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

Figure 8-52 Template

Start Time	End Time	Owner Name	Plate No.
2017-1-1 0:00	2037-12-5 23:59	xxx	xxx

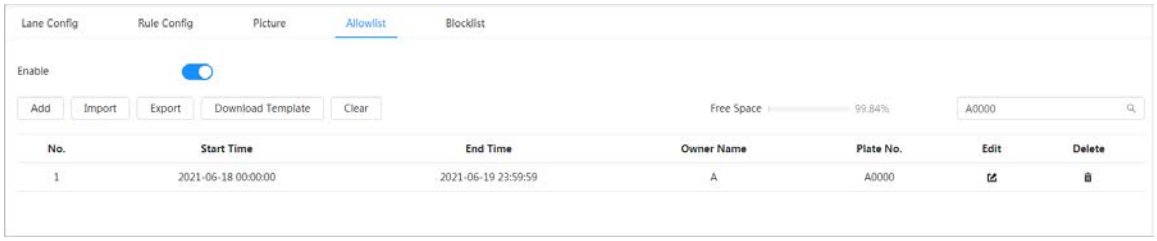
5. Click **Import** to upload allowlist table.
   - ◇ If the table is encrypted, you need to enter the password when uploading.
   - ◇ If the table is unencrypted, you can upload directly.

Related Operations

- Search plate number.

  Enter the plate number in Plate No. and then click . The search result is as below:

Figure 8-53 Search allowlist



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

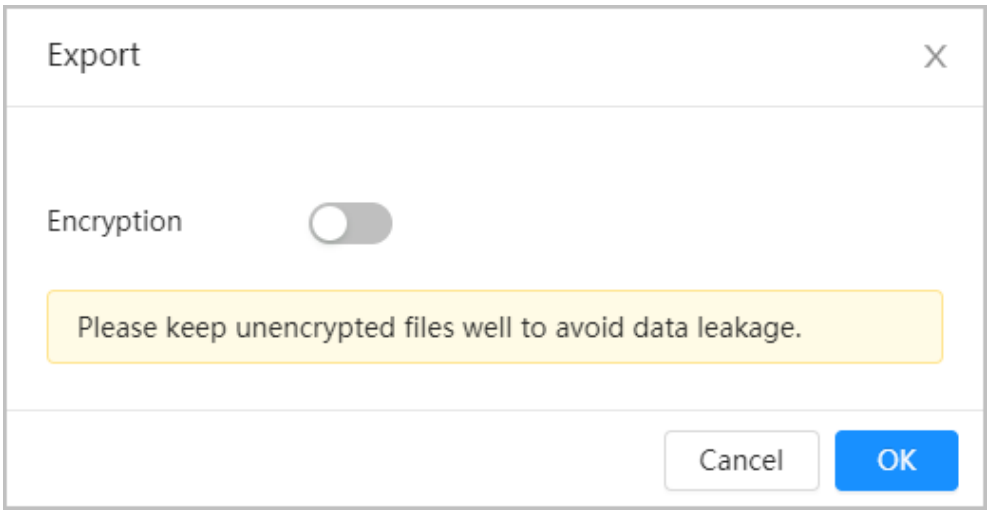
- Edit allowlist information.

  Click to edit **Start Time/End Time** and **Owner Name**.

- Delete allowlist.
  - ◇ Click to delete specific allowlist number.
  - ◇ Click **Clear** to delete all allowlist number.
- Export allowlist.

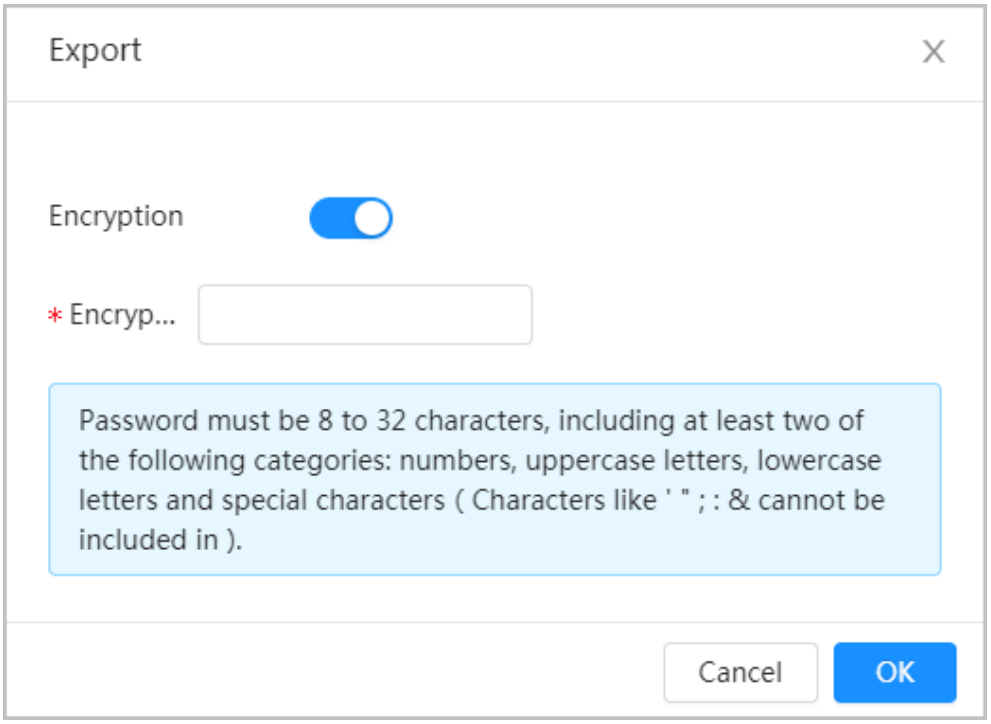
  Click **Export**. Enable encrypted or unencrypted file as needed and then export it to your PC.
  - ◇ Export the file in .csv format if not encrypted, and you can edit the file.

Figure 8-54 Encryption settings (2)



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

Figure 8-55 Encryption settings (3)



8.11.5 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 “8.11.4 Allowlist”.

9 Security

9.1 Security Status

Background Information

Detect the user and service, and scan the security modules to check the security status of the camera, so that when abnormality appears, you can process it timely.

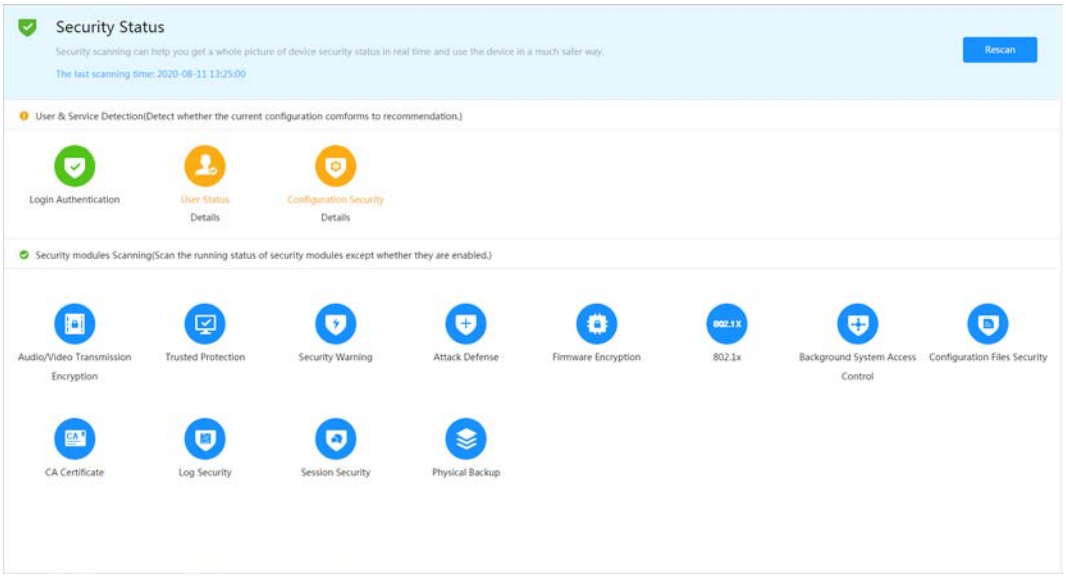
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing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

Procedure

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

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

Figure 9-1 Security Status

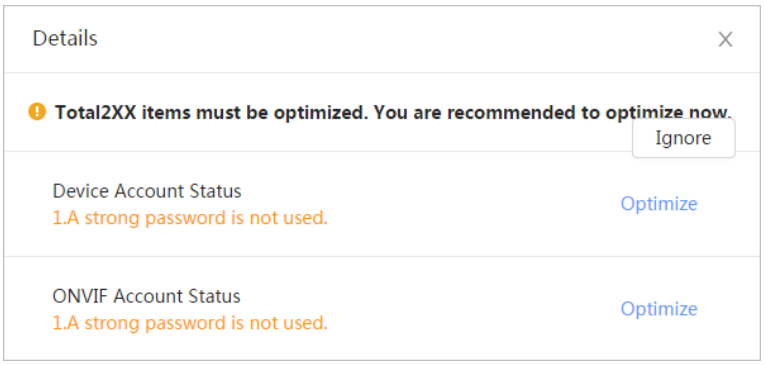


Related Operations

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

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

Figure 9-2 Security Status



9.2 System Service

9.2.1 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

Step 1 Select **Security** > **System Service** > **802.1x**.

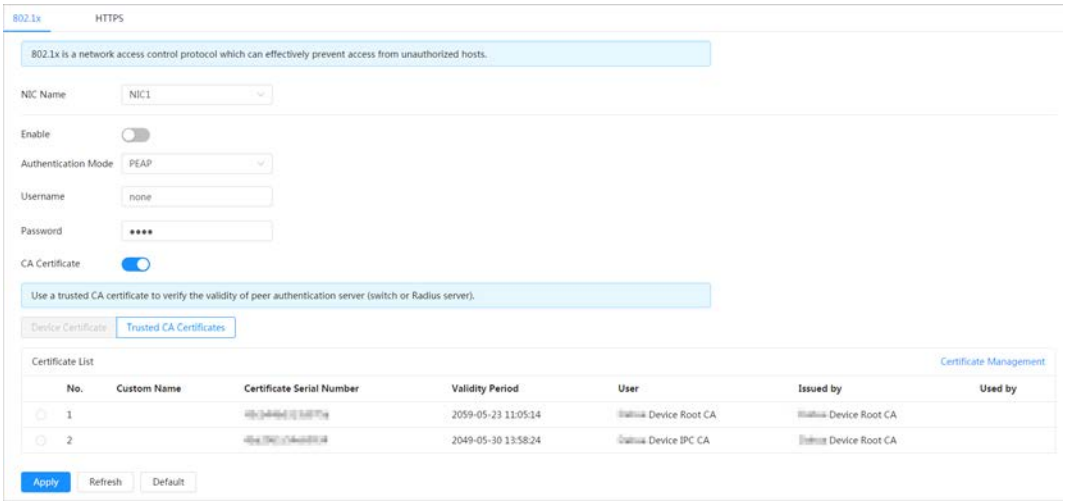
Step 2 Select the NIC name as needed, and click to enable it.

Step 3 Select the authentication mode, and then configure parameters.

- PEAP: Protected EAP protocol.
  1. Select PEAP as the authentication mode.
  2. Enter the username and password that has been authenticated on the server.
  3. Click next to CA certificate, and select the trusted CA certificate in list.

     If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".

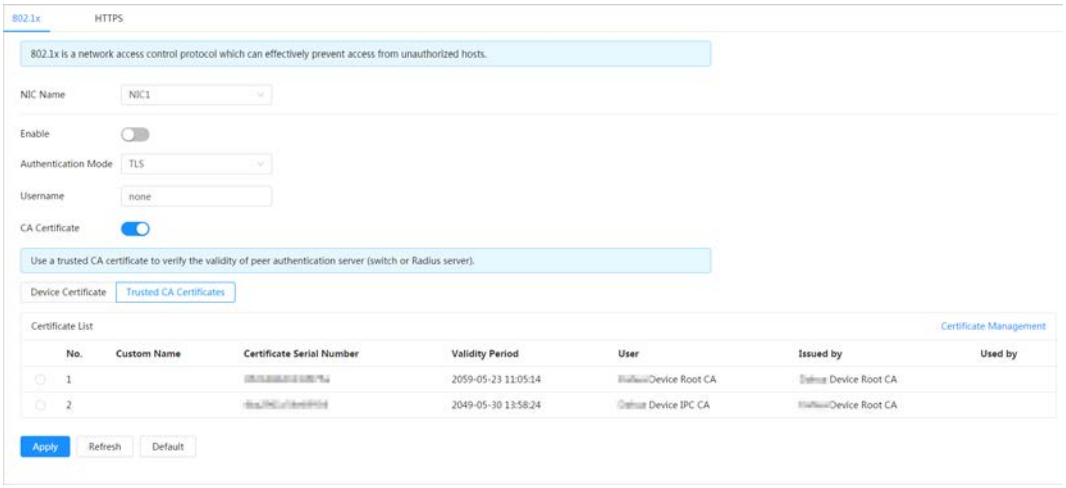
Figure 9-3 802.1x (PEAP)



- TLS: Transport Layer Security. It is applied in two communication application programs to guarantee the security and integrity of the data.
  1. Select TLS as the authentication mode.
  2. Enter the username.
  3. Click next to CA certificate, and select the trusted CA certificate in list.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".

Figure 9-4 802.1x (TLS)



Step 4 Click **Apply**.

9.2.2 HTTPS

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with your PC. The HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing private.

Procedure

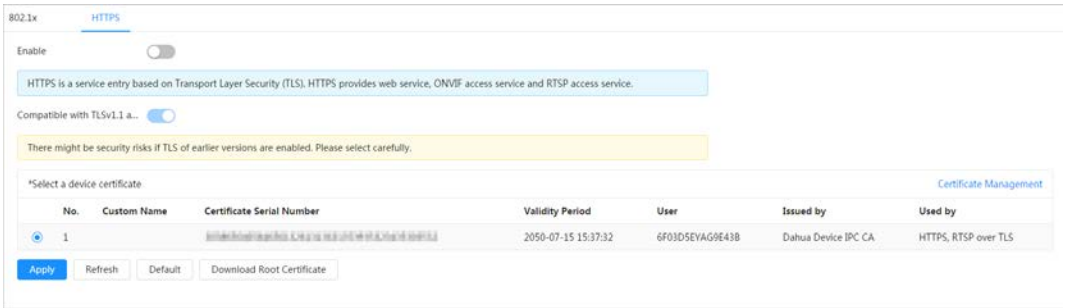
Step 1 Select **Security** > **System Service** > **HTTPS**.

Step 2 Click to enable it.

Step 3 Select the certificate.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar. For details, see "9.4.2 Installing Trusted CA Certificate".

Figure 9-5 HTTPS



Step 4 Click **Apply**.

9.3 Attack Defense

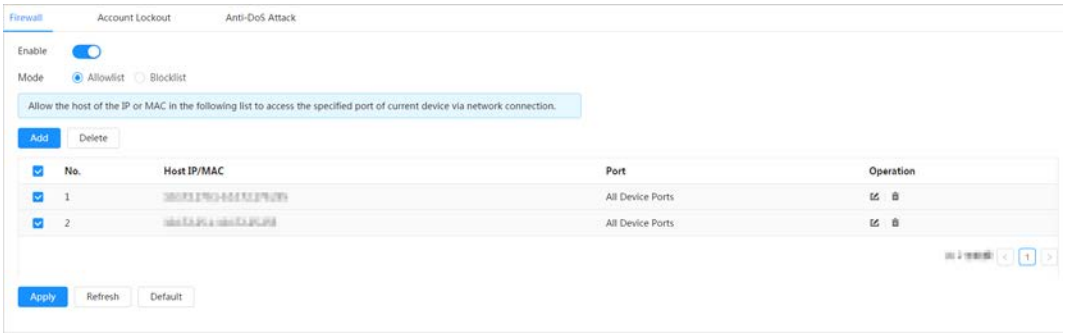
9.3.1 Firewall

Configure firewall to limit access to the camera.

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

Step 2 Click to enable the firewall function.

Figure 9-6 Firewall

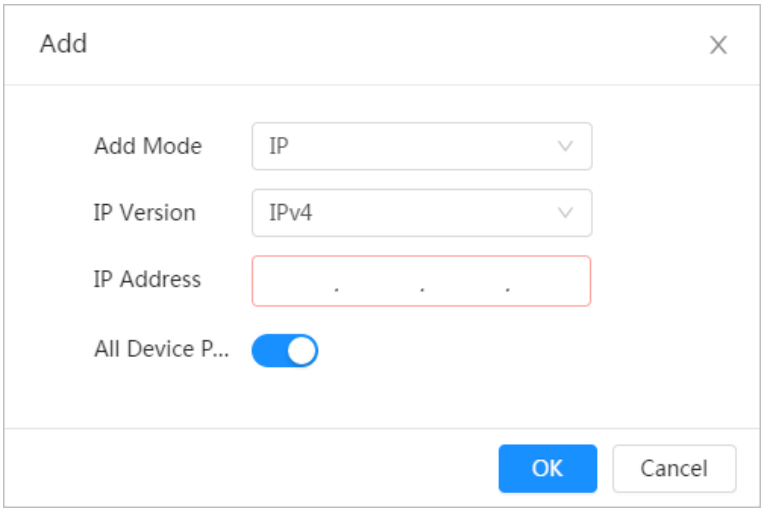


Step 3 Select the mode: **Allowlist** and **Blocklist**.

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

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

Figure 9-7 Firewall



Step 5 Click **Apply**.

Related Operations

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

9.3.2 Account Lockout

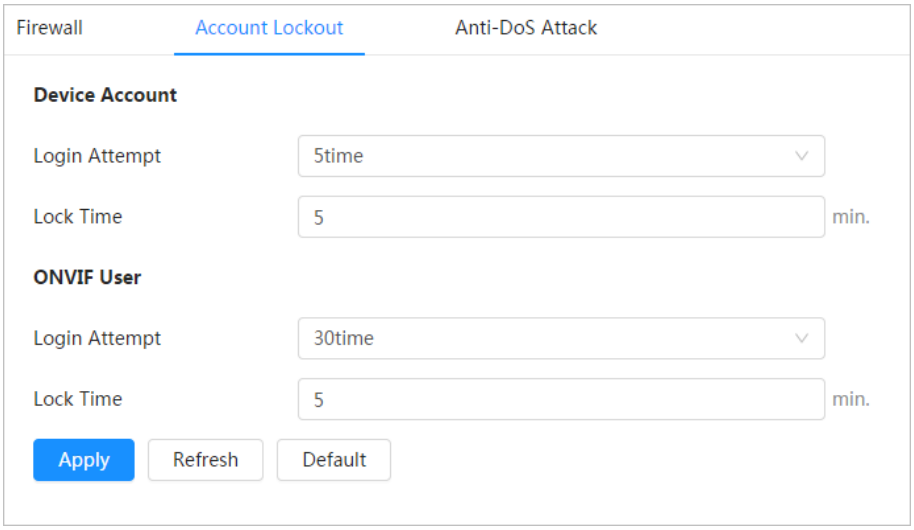
If you consecutively enter a wrong password more than the configured value, the account will be locked.

Step 1 Select **Security** > **Attack Defense** > **Account Lockout**.

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

- Login attempt: Upper limit of login attempts. If you consecutively enter a wrong password more than the configured value, the account will be locked.
- Lock time: The period during which you cannot login after the login attempts reaches upper limit.

Figure 9-8 Account lockout



Step 3 Click **Apply**.

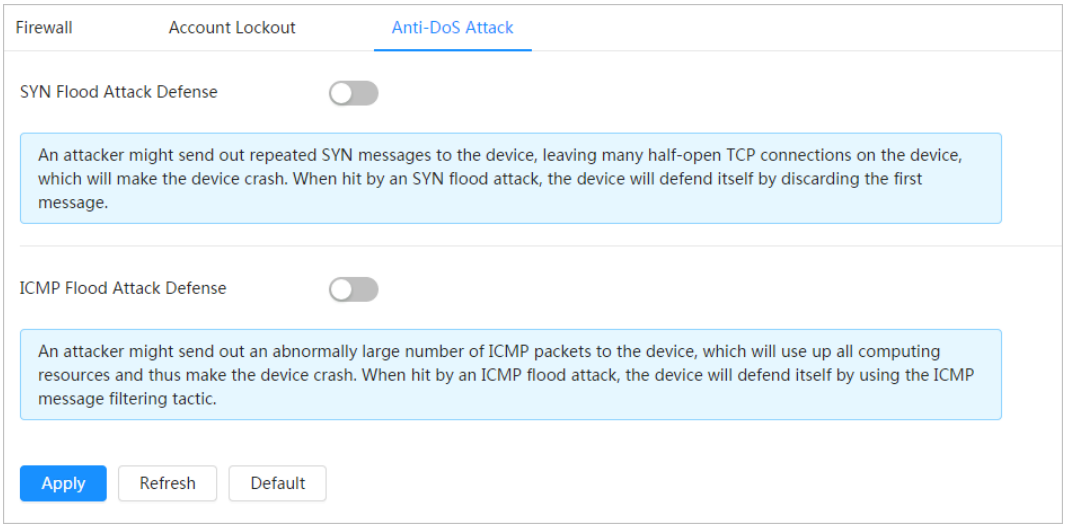
9.3.3 Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the device against Dos attack.

Step 1 Select **Security** > **Attack Defense** > **Anti-DoS Attack**.

Step 2 Select **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** to defend the device against Dos attack.

Figure 9-9 Anti-DoS attack



9.4 CA Certificate

9.4.1 Installing Device Certificate

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

9.4.1.1 Creating Certificate

Creating certificate in the device.

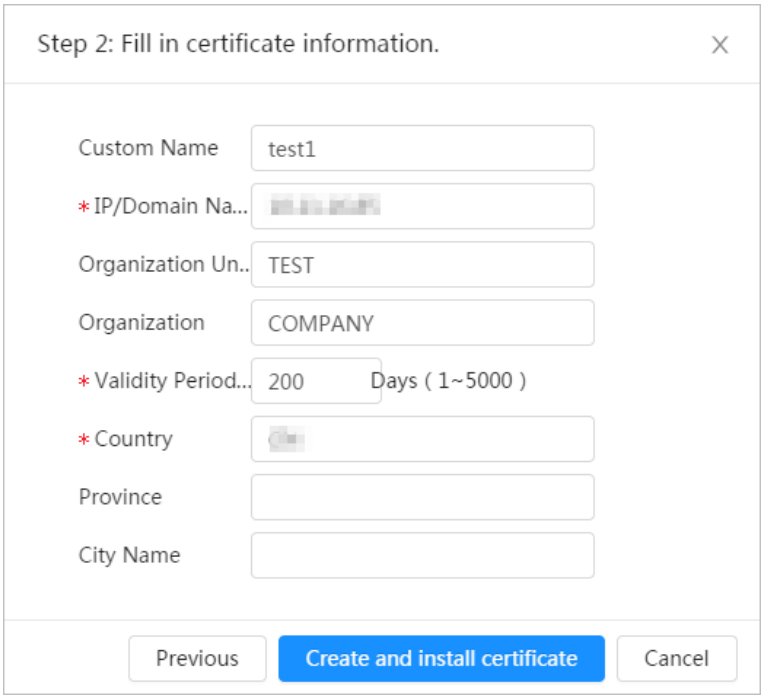
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Create Certificate**, and click **Next**.

Step 4 Enter the certificate information.

Figure 9-10 Certificate information (1)



Step 5 Click **Create and install certificate**.

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

Related Operations

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

9.4.1.2 Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

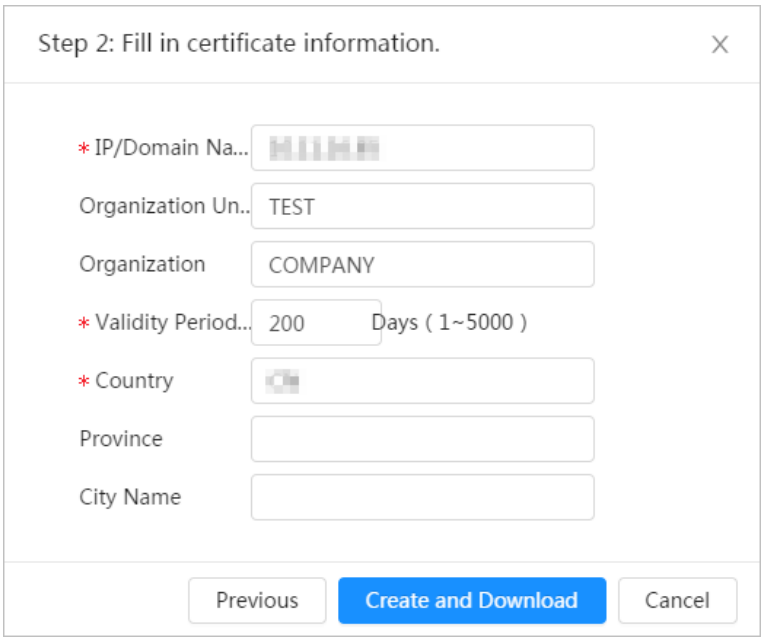
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Apply for CA Certificate and Import (Recommended)**, and click **Next**.

Step 4 Enter the certificate information.

Figure 9-11 Certificate information (2)



Step 5 Click **Create and Download**.

Save the request file to your PC.

Step 6 Apply the CA certificate from the third-party certificate authority.

Step 7 Import the signed CA certificate.

1) Save the CA certificate to the PC.
2) Do Step1 to Step3, 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** interface.

   - Click **Recreate** to create the request file again.
   - Click **Import Later** to import the certificate next time.

Related Operations

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

9.4.1.3 Installing Existing Certificate

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

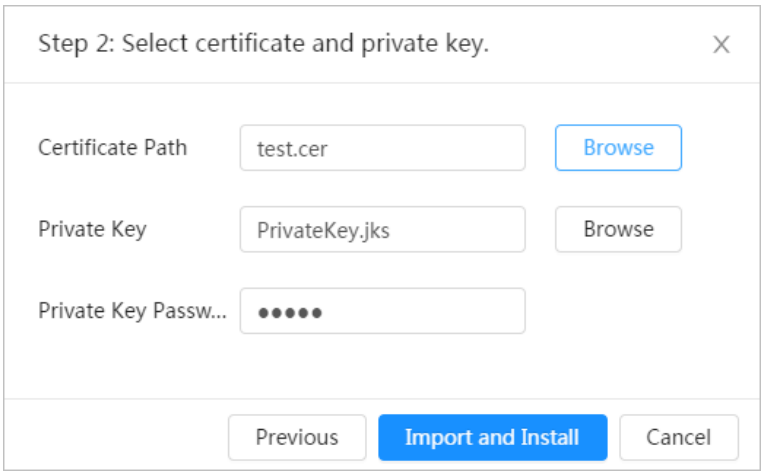
Step 1 Select **Security** > **CA Certificate** > **Device Certificate**.

Step 2 Select **Installing Device Certificate**.

Step 3 Select **Install Existing Certificate**, and click **Next**.

Step 4 Click **Browse** to select the certificate and private key file, and enter the private key password.

Figure 9-12 Certificate and private key



Step 5 Click **Import and Install**.

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

Related Operations

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

9.4.2 Installing Trusted CA Certificate

CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

Step 1 Select **Security** > **CA Certificate** > **Trusted CA Certificates**.

Step 2 Select **Installing Trusted Certificate**.

Step 3 Click **Browse** to select the certificate.

Figure 9-13 Installing trusted certificate



Step 4 Click **OK**.

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

Related Operations

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

9.5 A/V Encryption

The device supports audio and video encryption during data transmission.

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

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

Step 2 Configure the parameters.

Figure 9-14 A/V encryption

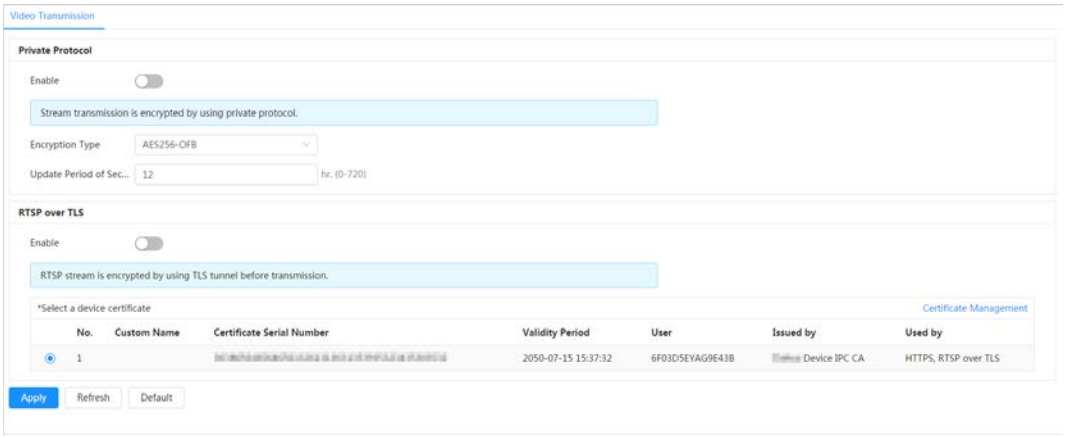


Table 9-1 A/V encryption parameter

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "9.4.1 Installing Device Certificate".

Step 3 Click **Apply**.

9.6 Security Warning

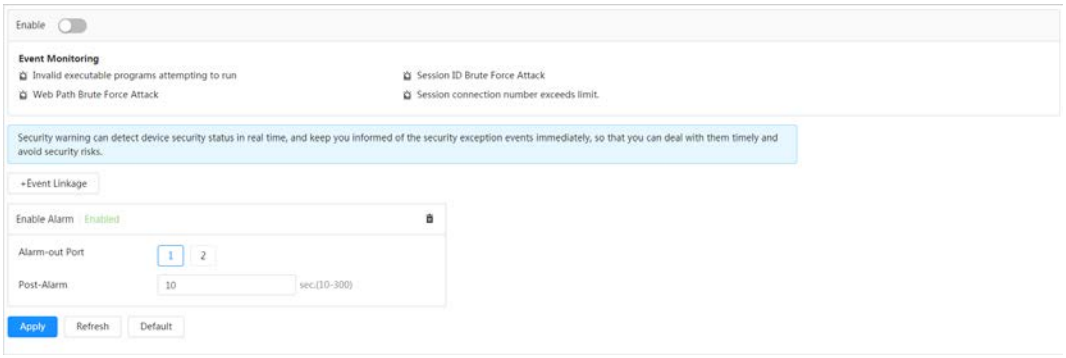
When security exception event is detected, the camera sends a warning to remind you to process it timely, to avoid security risk.

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

Step 2 Click next to **Enable** to enable security warning.

Step 3 Configure the parameters.

Figure 9-15 Security warning



Step 4 Set arming periods and alarm linkage action. For details, see "6.4.1.2 Alarm Linkage".

Click **+ Event Linkage** to set the linkage action.

Step 5 Click **Apply**.

10 Record

This section introduces the functions and operations of video playback.

10.1 Playback

10.1.1 Playing Back Video

This section introduces the operation of video playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back video, configure record time range, record storage method, record schedule and record control. For details, see "10.2 Setting Record Control", "10.3 Setting Record Plan", and "10.4 Storage".

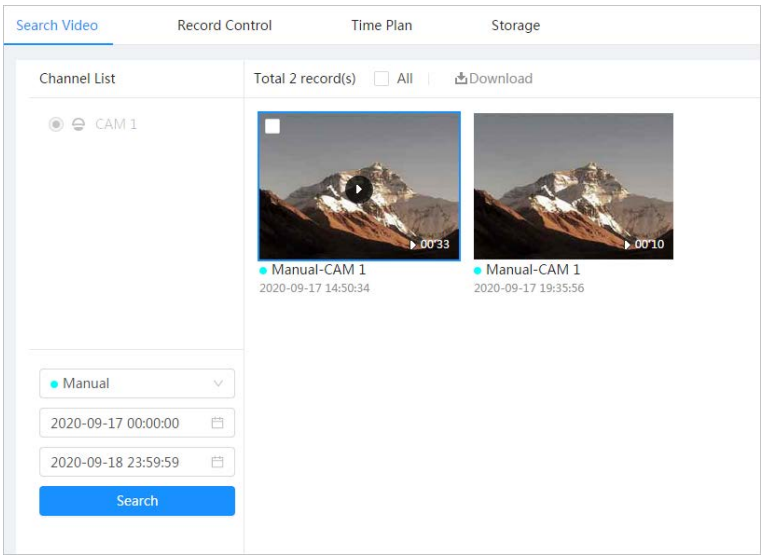
Procedure

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

Step 2 Select the channel, the record type, and record time, and then click **Search**.

- Click **All**, and select the record type from the drop-down list, you can select from **All**, **General**, **Event**, **Alarm**, and **Manual**.
  When selecting **Event** as the record type, you can select the specific event types, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.
- The dates with blue dots indicate there are videos recorded on those days.

Figure 10-1 Search video



Step 3 Point to the searched video, and then click  to play back the selected video.
The video playback interface is displayed.

Figure 10-2 Video playback

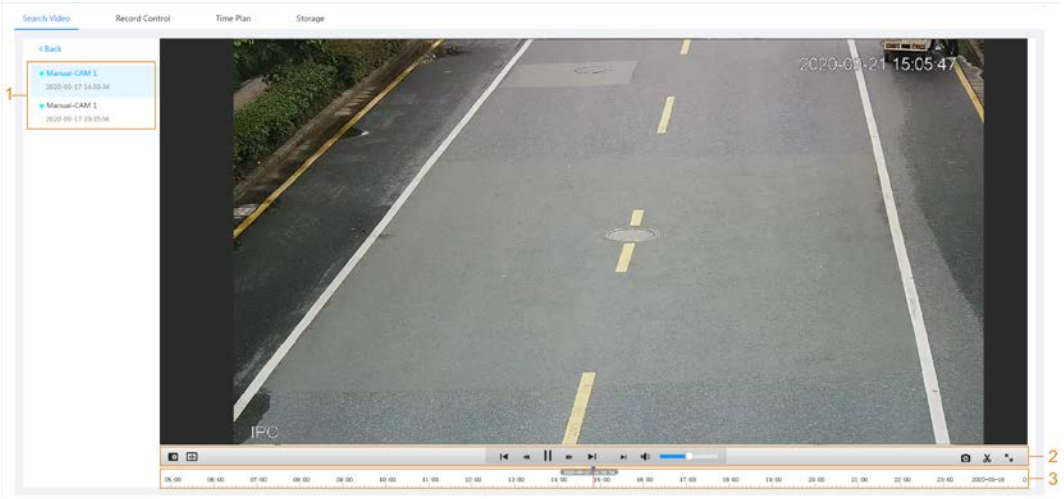


Table 10-1 Description of video playback interface

No	Function	Description
1	Recorded video list	Displays all searched recorded video files. Click any files to play back it. Click **Back** at the upper-left corner to go to the **Search Video** interface.
2	Digital Zoom	You can zoom video image of the selected area through two operations. ● 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. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in or out.
	AI Rule	Click , and then select **Enable** to display AI rules and detection box; select **Disable** to stop the display. It is enabled by default. AI rules is valid only when you enabled the rule during recording.
	Play control bar	Controls playback. ● : Click the icon to play back the previous recorded video in the recorded video list. ● : Click the icon to slow down the playback. ● : Click the icon to stop playing back recorded videos. The icon changes to , click the icon to play back recorded videos. ● : Click the icon to speed up the playback. ● : Click the icon to play back the next recorded video in the recorded video list. ● : Click the icon to play the next frame.

No	Function	Description
	Sound	Controls the sound during playback. ● : Mute mode. ● : Vocal state. You can adjust the sound.
	Snapshot	Click to capture one picture of the current image, and it will be saved to the configured storage path. 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 , and the image is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.
3	Progress bar	Displays the record type and the corresponding period. ● Click any point in the colored area, and the system will play back the recorded video from the selected moment. ● Each record type has its own color, and you can see their relations in **Record Type** bar

10.1.2 Clipping Video

Step 1 Click .

Step 2 Drag the clipping box on the progress bar to select the start time and end time of the target video

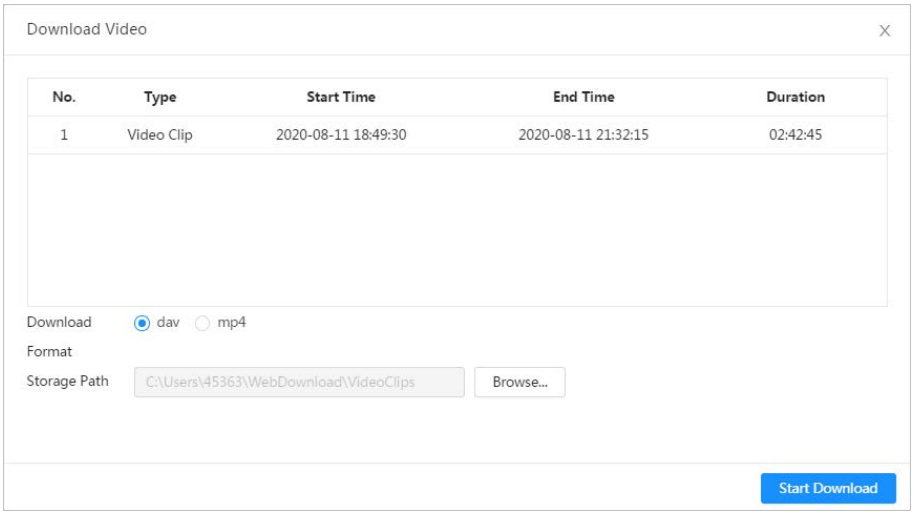
Figure 10-3 Clipping video



Step 3 Click **OK** to download the video.

Step 4 Select the download format and storage path.

Figure 10-4 Clipping video



Step 5 Click **Start Download**.

The playback stops and the clipped file is saved in the configured storage path. For details of storage path, see "6.1 Local".

10.1.3 Downloading Video

Download videos to a defined path. You can download a single video, or download them in batches.

- Playback and downloading at the same time is not supported.
- Operations might vary with different browsers.
- For details of viewing or setting storage path, see "6.1 Local".

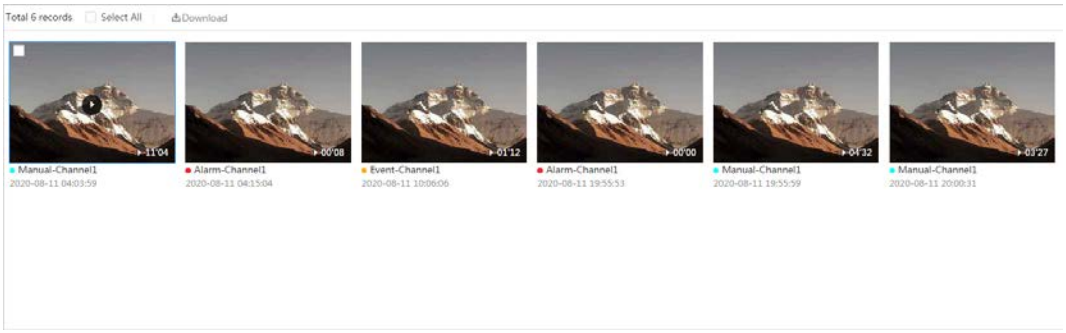
Step 1 Select **Record** > **Search Video**.

Step 2 Select the channel, the record type, and record time, and the click **Search**.

Step 3 Select the videos to be downloaded.

- Select at the upper-right corner of each video file to select one or multiple videos.
- Select next to **Select All** to select all searched videos.

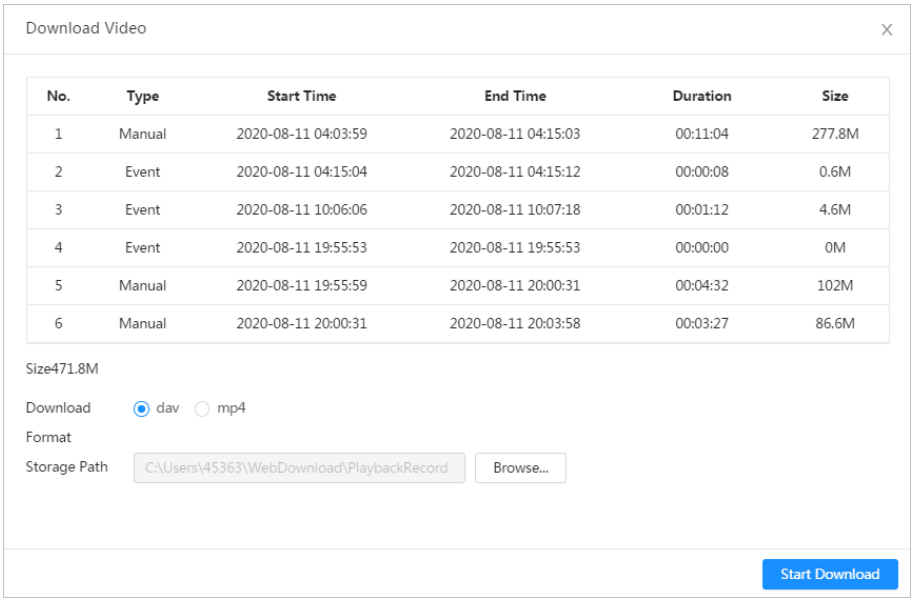
Figure 10-5 Selecting video file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 10-6 Downloading video



Step 6 Click **Start Download**.

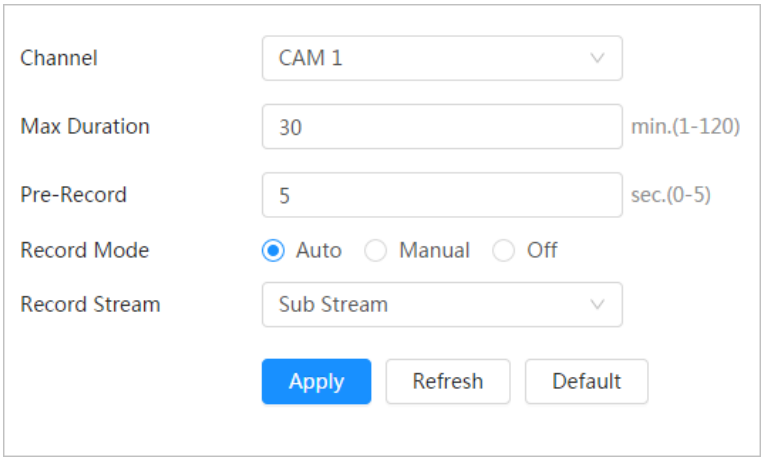
The downloaded files are saved in the configured storage path. For details of storage path, see "6.1 Local".

10.2 Setting Record Control

Set parameters such as pack duration, pre-event record, disk full, record mode, and record stream.

Step 1 Click **Record** in the main interface, and then click the **Record Control** tab.

Figure 10-7 Record control



Step 2 Set parameters.

Table 10-2 Description of record control parameters

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

Step 3 Click **Apply**.

10.3 Setting Record Plan

After the corresponding alarm type (**Normal**, **Motion**, and **Alarm**) is enabled, the record channel links recording.

Set certain days as holiday, and when the **Record** is selected in the holiday schedule, the system records video as holiday schedule defined.

Step 1 Click **Record** on the main interface, and then click the **Time Plan** tab.

Figure 10-8 Time plan



Step 2 Set record plan.

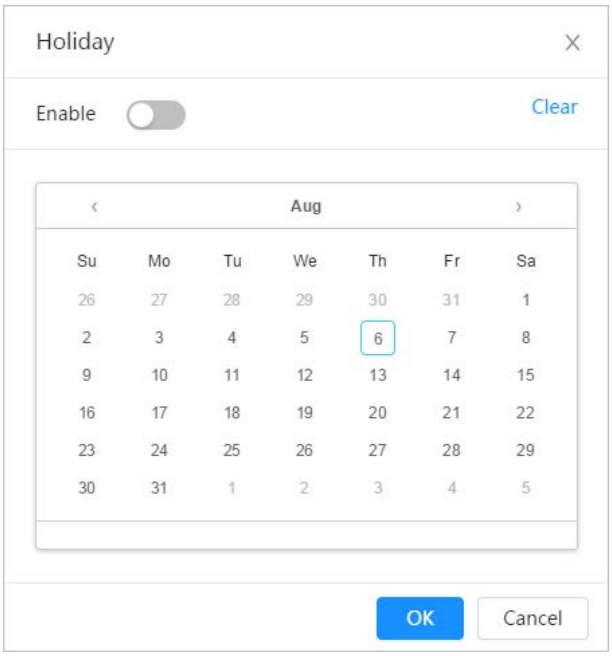
Green represents normal record plan (such as timing recording); yellow represents motion record plan (such as recording triggered by intelligent events); red represents alarm record plan (such as recording triggered by alarm-in). Select a record type, such as **Normal**, and directly press and drag the left mouse button to set the period for normal record on the timeline.

- Click **Copy** next to a day, and select the days that you want to copy to in the prompt interface, you can copy the configuration to the selected days. Select the **Select All** check box to select all day to copy the configuration.
- You can set 6 periods per day.

Step 3 Click **Apply**.

Step 4 Click **Holiday** to set holidays.

Figure 10-9 Time plan



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

Click **Clear** to cancel the selection.

When holiday schedule setting is not the same as the general setting, holiday schedule setting is prior to the general setting. For example, with holiday schedule enabled, if the day is holiday, the system snapshots or records as holiday schedule setting; otherwise, the system snapshots or records as general setting.

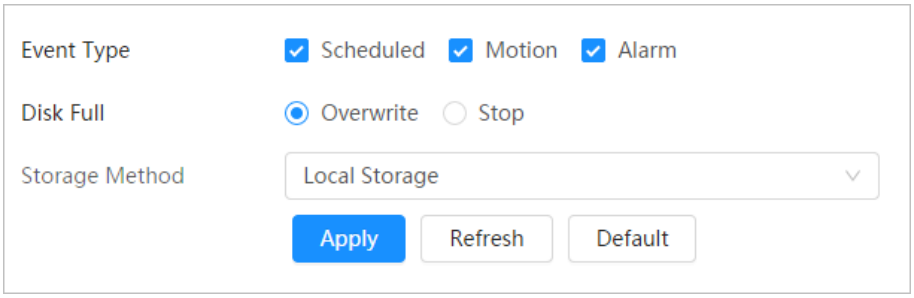
Step 6 Click **OK**.

10.4 Storage

This section introduces the configuration of the storage method for the recorded videos.

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

Figure 10-10 Live



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

Table 10-3 Description of storage parameters

Parameter	Description
Event Type	Select from **Scheduled**, **Motion Detection** and **Alarm**.

Parameter	Description
Disk Full	Recording strategy when the disk is full. • **Overwrite**: Cyclically overwrite the earliest video when the disk is full. • **Stop**: Stop recording when the disk is full.
Storage Method	Select from **Local storage** and **Network storage** • **Local storage**: Save the recorded videos in the internal SD card. **Local storage** is displayed only on models that support SD card. • **Network storage**: Save the recorded videos in the FTP server or NAS.

Step 3 Click **Apply**.

10.4.1 Local Storage

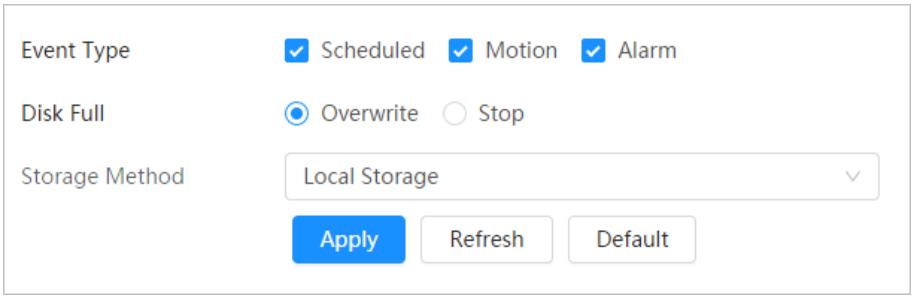
Step 1 Select **Record** > **Storage**.

Step 2 Select the recording strategy in **Disk Full**.

- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

Step 3 Select **Local storage** in **Storage Method** to save the recorded videos in the internal SD card.

Figure 10-11 Local storage



Step 4 Click **Apply**.

10.4.2 Network Storage

You can select from **FTP** and **NAS**.

When the network does not work, you can save all the files to the internal SD card for emergency.

10.4.2.1 FTP

Enable this function, and you can save all the files in the FTP server.

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

Step 2 Select the recording strategy in **Disk Full**.

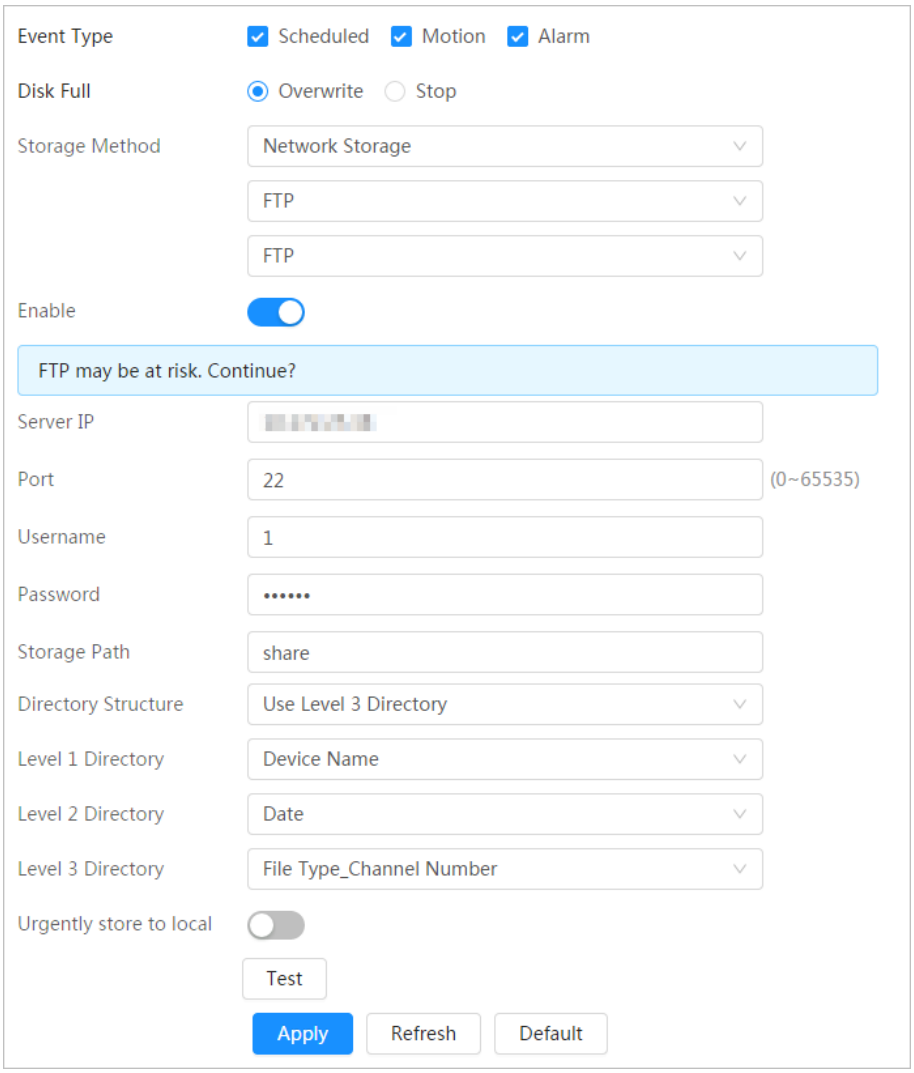
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

Step 3 Select **Network storage** in **Storage Method**, and select **FTP** to save the recorded videos in FTP server.

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

Step 4 Click next to **Enable** to enable the FTP function.

Figure 10-12 FTP



Step 5 Configure FTP parameters.

Table 10-4 Description of FTP parameters

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The destination path in the FTP server.
Directory Structure	Set the directory structure, and you can select **Use Level 1 Directory**, **Use Level 2 Directory**, and **Use Level 3 Directory**
Level 1 Directory	Set the Level 1 directory name, and you can select from **Device name**, **Device IP**, and **Custom**. When you select **Custom**, please enter the custom directory.
Level 2 Directory	Set the Level 2 directory name, and you can select from **File Type**,

Parameter	Description
Level 3 Directory	**Date**, **File Type_Channel Number**, and **Custom**. When you select **Custom**, please enter the custom directory.
Urgently store to local	Click , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 6 Click **Save**.

Step 7 Click **Test** to test whether FTP function works normally.

10.4.2.2 NAS

Enable this function, and you can save all the files in the NAS.

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

Step 2 Select the recording strategy in **Disk Full**.

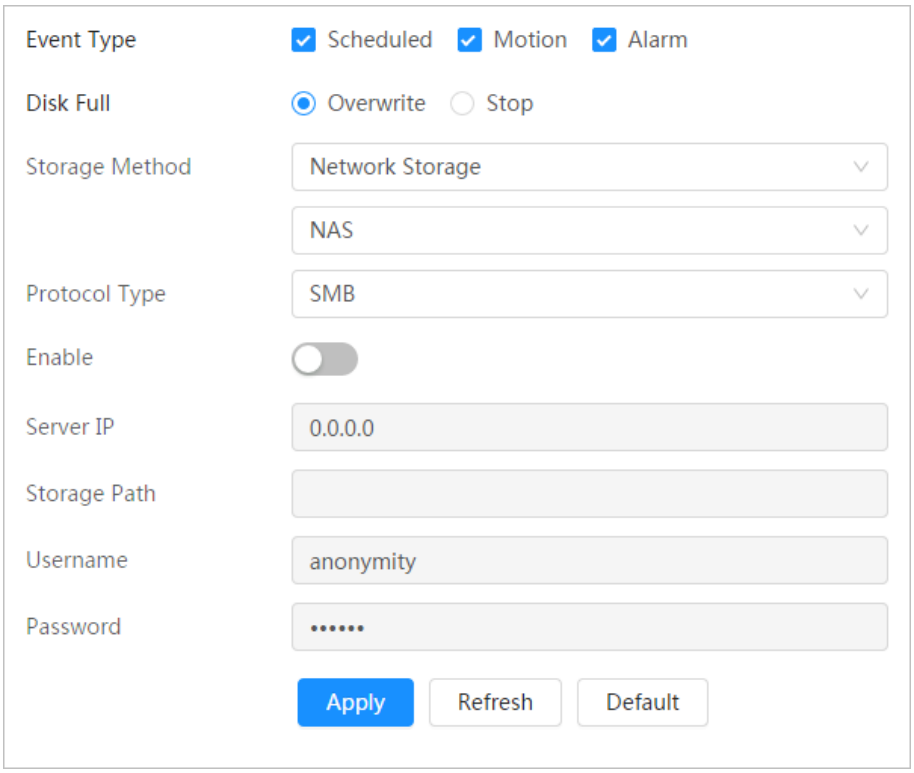
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

Step 3 Select **Network storage** in **Storage Method**, and select **NAS** to save the recorded videos in NAS server.

Step 4 Select NAS protocol type.

- **NFS** (Network File System): A file system which enables computers in the same network share files through TCP/IP.
- **SMB** (Server Message Block): Provides shared access for clients and the server.

Figure 10-13 FTP



Step 5 Configure NAS parameters.

Table 10-5 Description of NAS parameters

Parameter	Description
Server IP	The IP address of the NAS server.

Parameter	Description
Storage Path	The destination path in the NAS server.
Username	When selecting **SMB** protocol, you are required to enter username and password. Enter them as needed.
Password	

Step 6 Click **Apply**.

11 Picture

This section introduces the related functions and operations of picture playback.

11.1 Playback

11.1.1 Playing Back Picture

This section introduces the operation of picture playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back picture, configure snapshot time range, snapshot storage method, snapshot plan. For details, see"11.3 Setting Snapshot Plan".

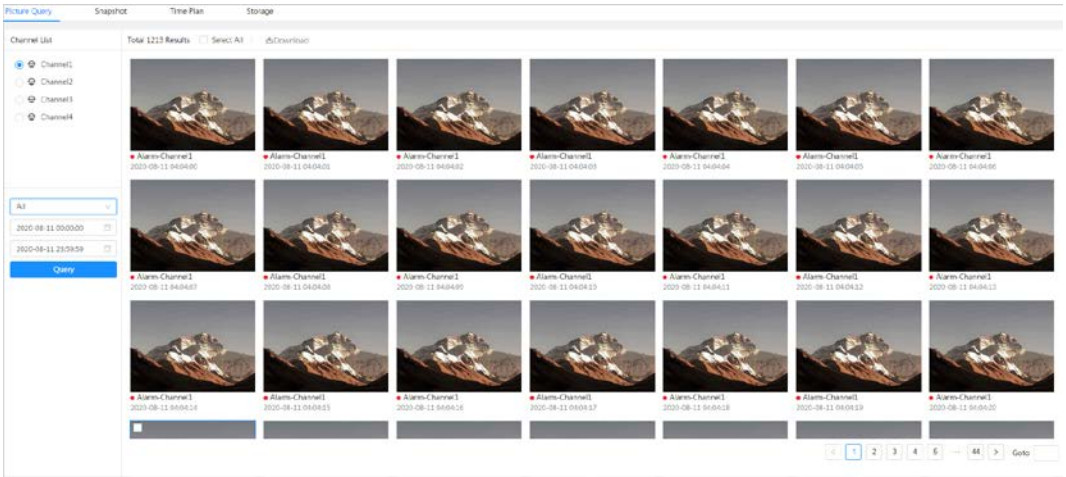
Procedure

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

Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.

- Click **All**, and select the record type from the drop-down list, you can select from **All**, **General**, **Event**, and **Alarm**.
  When selecting **Event** as the snapshot type, you can select the specific event types, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.
- The dates with blue dots indicate there are snapshots on those days.

Figure 11-1 Picture query



Step 3 Point to the searched picture, and then click  to play back the selected picture.
The picture playback interface is displayed.

Figure 11-2 Picture playback



Table 11-1 Description of playback interface

No	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play back it. Click **Back** at the upper-left corner to go to the **Picture Query** interface.
2	Manual display	• Click to display the previous snapshot in the snapshot list. • Click to display the nest snapshot in the snapshot list.
3	Slide show	Click to display the snapshots list one by one in slide show mode.
4	Full screen	Click , and the snapshot is displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.

11.1.2 Downloading Picture

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

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

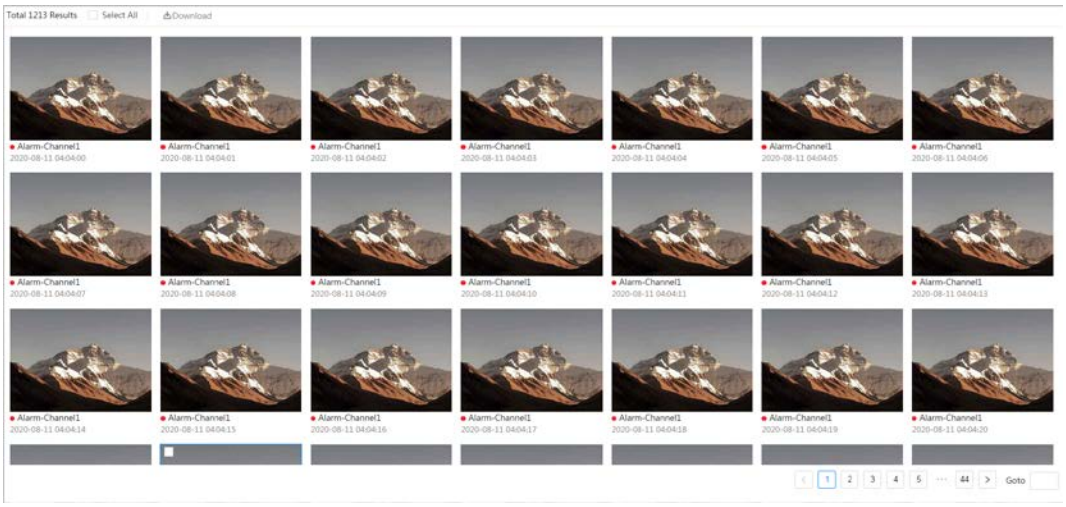
Step 1 Select **Picture** > **Picture Query**.

Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.

Step 3 Select the pictures to be downloaded.

- Select at the upper-right corner of each picture file to select one or multiple pictures.
- Select next to **Select All** to select all searched pictures.

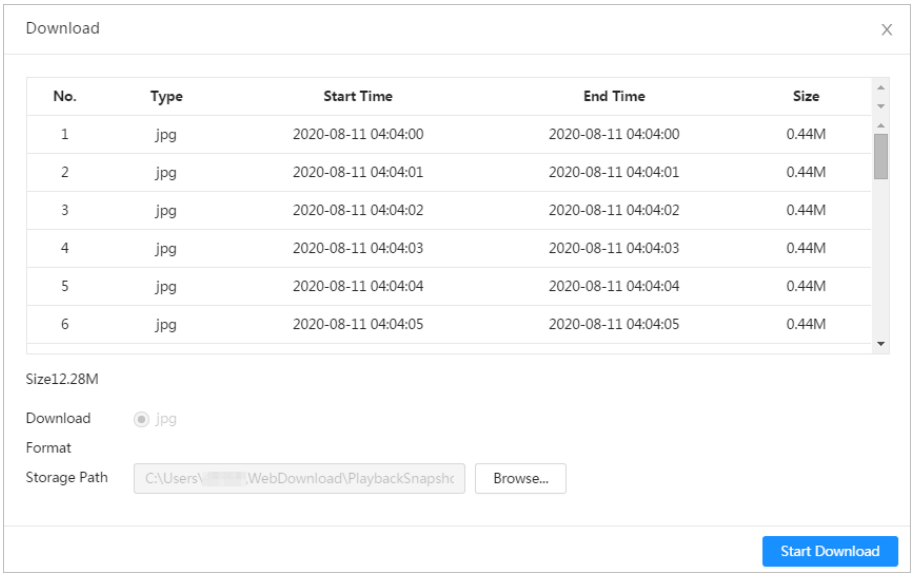
Figure 11-3 Selecting picture file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 11-4 Downloading picture



Step 6 Click **Start Download**.

The downloaded pictures are saved in the configured storage path. For details of storage path, see "6.1 Local".

11.2 Setting Snapshot Parameters

Set the snapshot parameters, including type, size, quality and Interval.

Step 1 Select **Picture** > **Snapshot**.

Step 2 Select the channel and set the parameters.

Figure 11-5 Snapshot

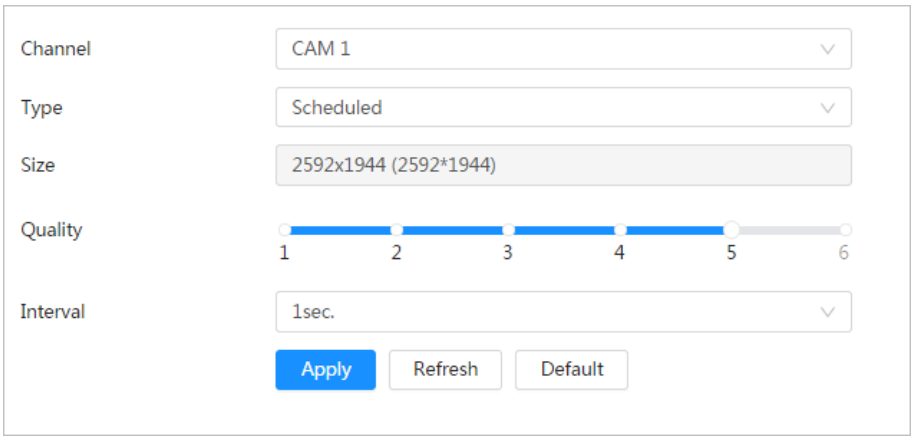


Table 11-2 Description of snapshot parameters

Parameter	Description
Type	You can select from **Scheduled** and **Event**. • **Scheduled**: Capture images in configured period. For details, see • **Event**: Capture images when configured event is triggered, such as **Motion Detection**, **Video Tamper** and **Scene Changing**. Make sure that you have enable the corresponding event detection and the snapshot function.
Size	It is same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select **Custom** to set the frequency as needed.

Step 3 Click **Apply**.

11.3 Setting Snapshot Plan

According to the configured snapshot plan, the system enables or disables snapshot at corresponding time. For detailed operation, see "10.3 Setting Record Plan".

11.4 Storage

Set the storage method for the snapshot. For detailed operation, see "10.4 Storage".

11.5 Setting Upload Method

Automatically upload images to the defined server through HTTP protocol, and configure parameters.

Background Information

You do not need to set upload period. When an alarm is triggered, images will be automatically uploaded to the defined server.

Procedure

Step 1 On the web interface, select **Picture** > **Auto Upload**.

Step 2 Enable the function.

Step 3 Click **Add**, and then configure parameters of HTTP upload method.

You can add two server information at most.

Figure 11-6 Image Upload



Table 11-3 Description of HTTP mode Parameter

Parameter	Description
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Event type	Select the event type form the drop-down list. You can select more than one types at the same time. 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.

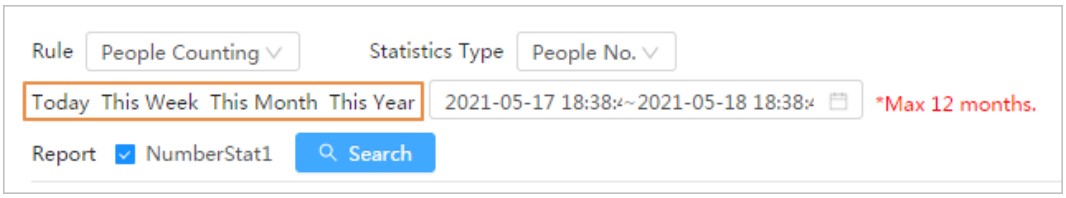
Step 4 Click **Apply**.

12 Report

12.1 Viewing Report

View the statistics results of AI functions in report form.

Figure 12-1 Report



- The period for the report is the latest 24 hours by default.
- Click to customize the period for the report.
- Click **Today**, **This Week**, **This Month**, or **This Year**. The start time of the period is 0 o'clock of the first day, and the end time is the current time.

12.1.1 Face Recognition

View the statistics result of face recognition in report form.

Procedure

Step 1 Select **Report** > **Report** > **Face Recognition**.

Step 2 Set the period for the report.

For multi-channel camera, select the channel first.

Step 3 Select the gender and age.

Step 4 Click **Search**.

Figure 12-2 Face Recognition report



Related Operations

- Select the report form
  Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner.
  The statistics result of unselected types will not be displayed.
- Export reports
  Select the file format, and then click **Export**.
  - Select **png**: Displays the report in picture format.
  - Select **csv**: Displays the report in list format.

12.1.2 Video Metadata

View the statistics result of video metadata in report form.

Procedure

Step 1 Select **Report** > **Report** > **Video Metadata**.

Step 2 Set the period for the report.

For multi-channel camera, select the channel first.

Step 3 Select the tripwire direction.

Step 4 Click **Search**.

Figure 12-3 Video metadata report



Related Operations

- Select the report form

  Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner.

  The statistics result of unselected types will not be displayed.
- Export reports

  Select the file format, and then click **Export**.
  - Select **png**: Displays the report in picture format.
  - Select **csv**: Displays the report in list format.

12.1.3 People Counting

Search for the counting results with different rules and counting methods.

Prerequisites

Make sure that you have configured the rule before searching for the report.

Procedure

Step 1 Select **Report** > **Report** > **People Counting**.

Step 2 Set search conditions.

For multi-channel camera, select the channel first.

Table 12-1 Set search conditions

Parameter	Description
Rule	Select the rule as needed, and then you need to select the statistics type according to the select rule.

Parameter	Description
Statistics Type	The statistics type of the people counting report. • **People No.**: Displays the report of the number of people that meet the configured condition. • **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.
Stay Time	When selecting rule to **Area People Counting**, and statistics type to **People No.**, you need to configure this parameter. The report displays the number of people whose stay time < the stay time threshold and≥ the stay time threshold
Queue Time	When selecting rule to **Queuing**, and statistics type to **People No.**, you need to configure this parameter. The report displays the number of people whose stay time **< Queuing Time** and**≥ Queuing Time**.
Period for the report	Set the period for the report. • When selecting rule to **People Counting**, you can view the daily, weekly, monthly and yearly report, and you can also customize the period. • 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.
Report	Select the rule name of the report that you want to search. You can select multiple rule names at the same time.

Step 3 Click **Search**.

Figure 12-4 People counting

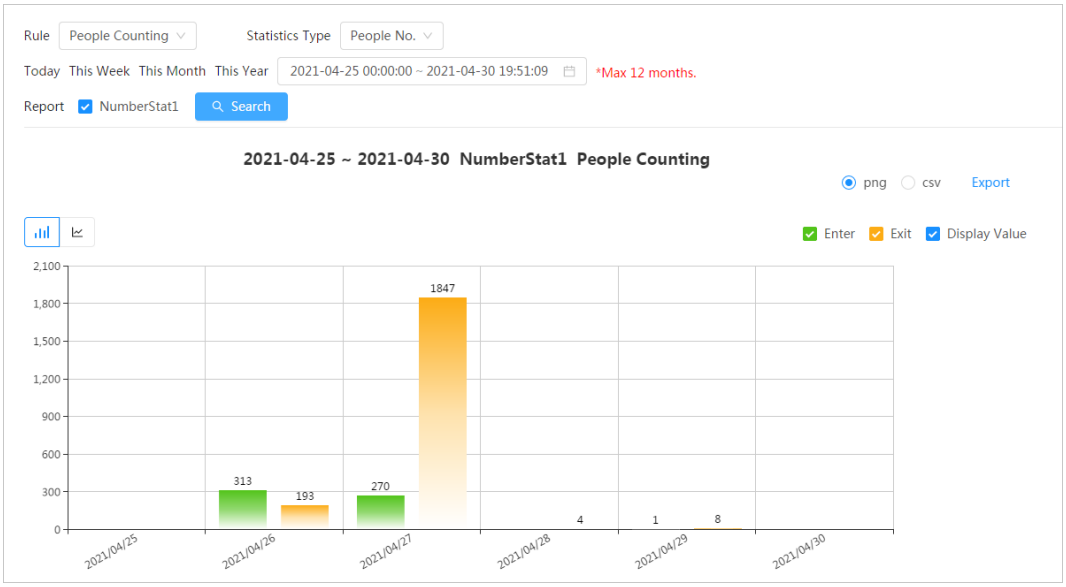


Figure 12-5 Area People Counting (number of people)

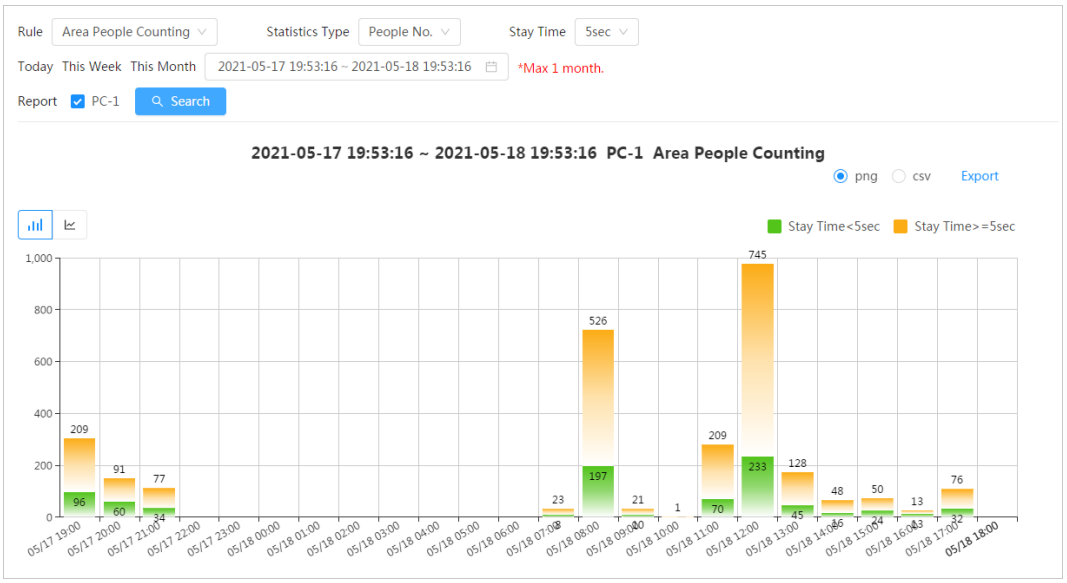


Figure 12-6 Region People Counting (stay time)

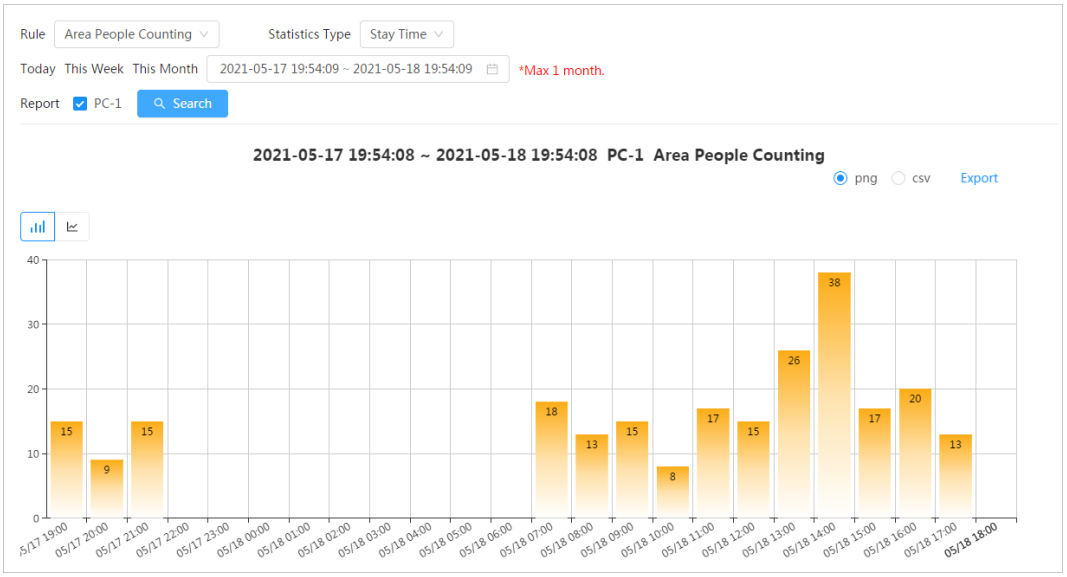
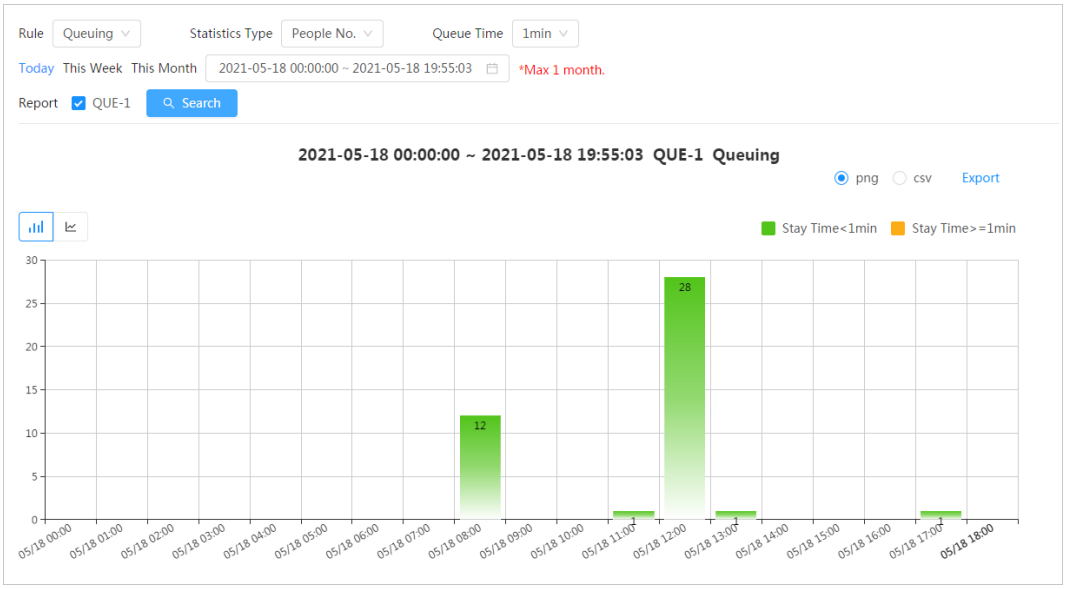


Figure 12-7 Queuing



Related Operations

- Select the report form
  Click to display the report in line chart; click to display the report in bar chart.
- Select the statistics type on the upper-right corner.
  The statistics result of unselected types will not be displayed.
- Export reports
  Select the file format, and then click **Export**.
  - ◇ Select **png**: Displays the report in picture format.
  - ◇ Select **csv**: Displays the report in list format.

12.1.4 Crowd Distribution

You can search for the number of people at a certain moment and get daily/weekly/monthly reports.

Prerequisites

Confirm that crowd distribution map function has already set; otherwise the corresponding report cannot be searched.

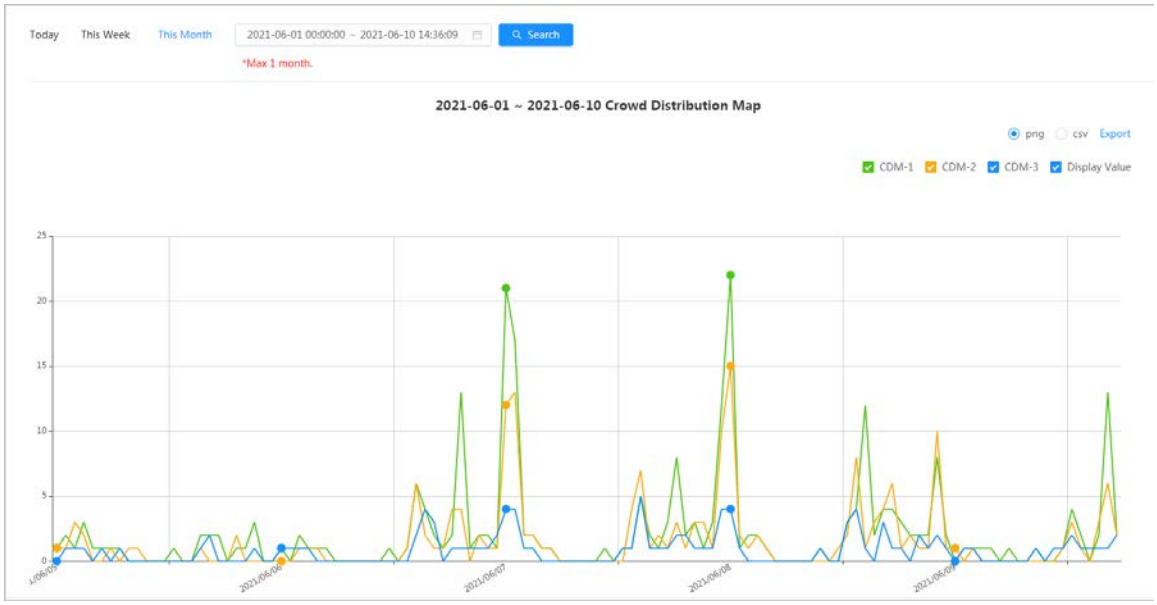
Procedure

Step 1 Select **Report** > **Report** > **Crowd Distribution Map**.

Step 2 Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the period.

Step 3 Click **Search**.

Figure 12-8 Crowd distribution map



Related Operations

- Select statistics type
  Click CDM-1 CDM-2 CDM-3 Display Value and select the type needed.
- Export statistic report
  Select the exact format and click **Export**, the report will be saved to the storage path of your browser.
  - ◇ Select **png**: Displays the report in picture format.

◇ Select **csv**: Displays the report in list format.

12.1.5 Vehicle Density

Search for the number of cars at a certain moment in each statistical area.

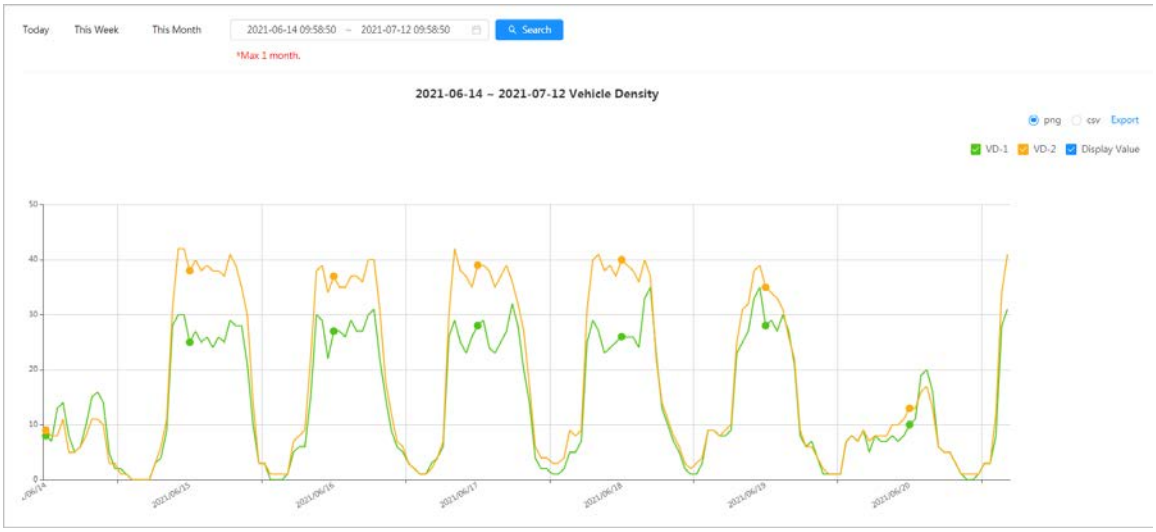
Procedure

Step 1 Select **Report** > **Report** > **Vehicle Density**.

Step 2 Select the period for report statistics. You can view daily reports, weekly reports and monthly reports, or customize the time period.

Step 3 Click **Search**.

Figure 12-9 Vehicle density map



Related Operations

- Select statistics type
  Click VD-1 VD-2 Display Value to select the type as needed.
- Export statistic report
  Select the exact format and click **Export**, the report will be saved to the save path of your browser.
  ◇ Select **png**: Displays the report in picture format.
  ◇ Select **csv**: Displays the report in list format.

12.1.6 Heat Map

View heat map and track map. You can search the detection results by number of people and stay time, and then generate the heat map. Heat map is not available on economic fisheye cameras.

Procedure

Step 1 Select **Report** > **Report** > **Heat Map.**

Step 2 Set search conditions.

For multi-channel camera, select the channel first.

Table 12-2 Set search conditions

Parameter	Description
Channel	For multi-channel camera, select the channel first.
Type	You can select report type form **Heat Map** and **Track Map**.
People No.	When selecting type as **Heat Map**, select **People No.**, and then set the threshold. The system will display the heat map for people density.
Threshold	
Time	When selecting type as **Heat Map**, select **Time** and then set the threshold. The system will display the heat map for stay time.
Threshold	
Period for the report	Set the period for the report. You can view the daily and weekly report, and you can also customize the period.

Step 3 Click **Search.**

Figure 12-10 Heat map (people No.)

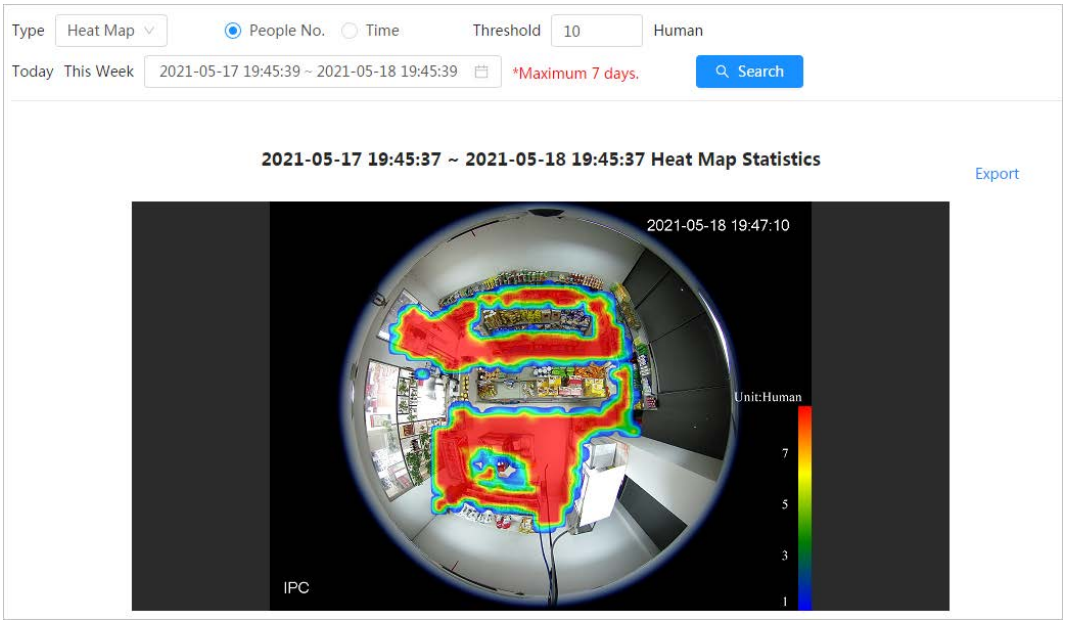


Figure 12-11 Heat map (time)

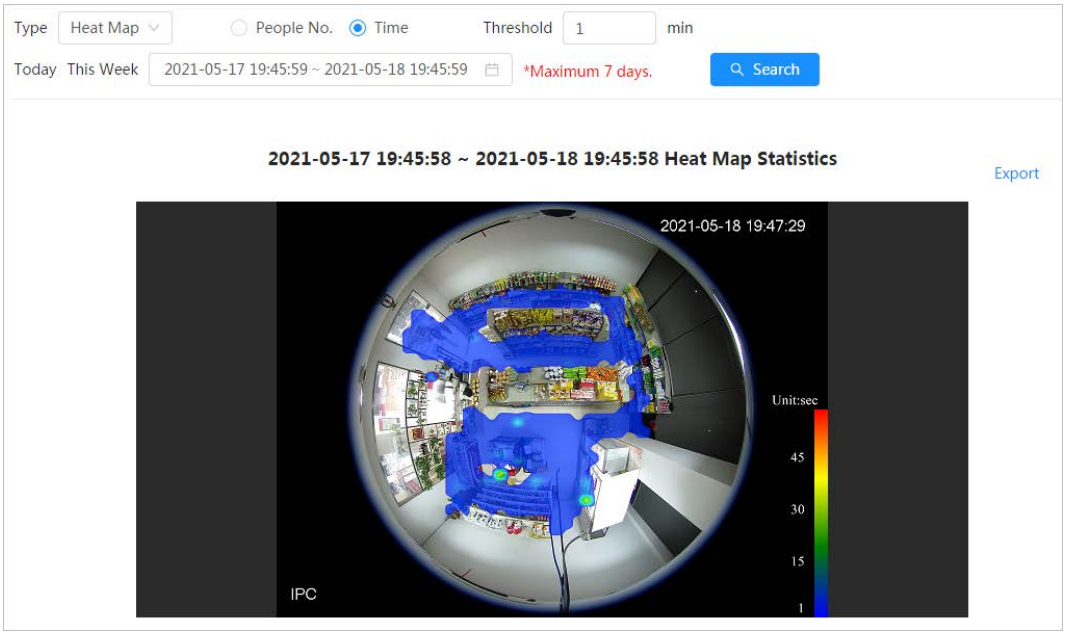
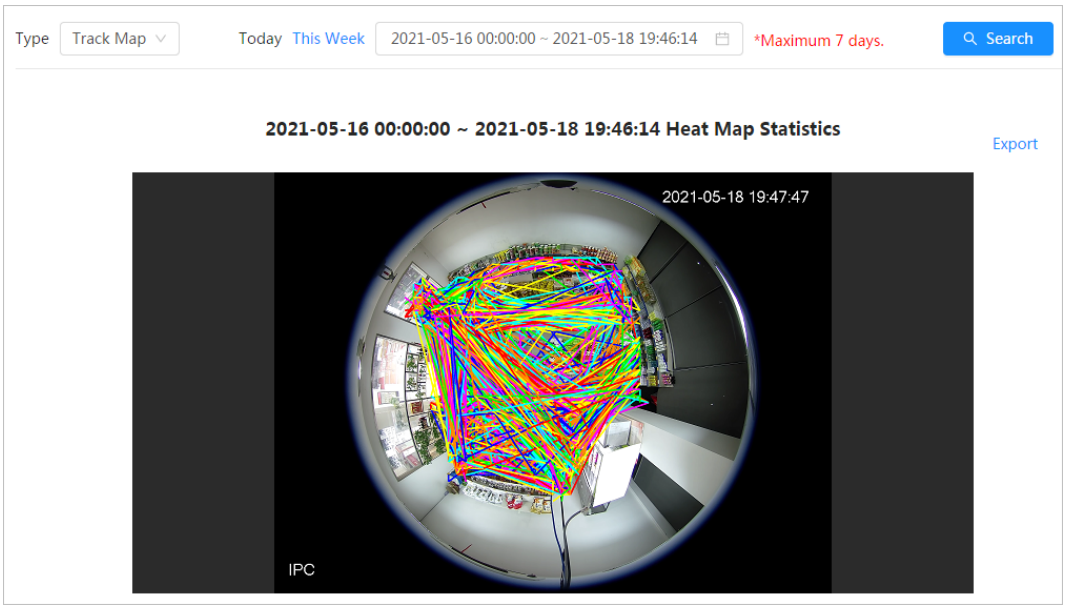


Figure 12-12 Track map



Related Operations

Click **Export**, and select the storage path for the exported report in .bmp format.

12.1.7 ANPR

View the statistics result of ANPR in report form.

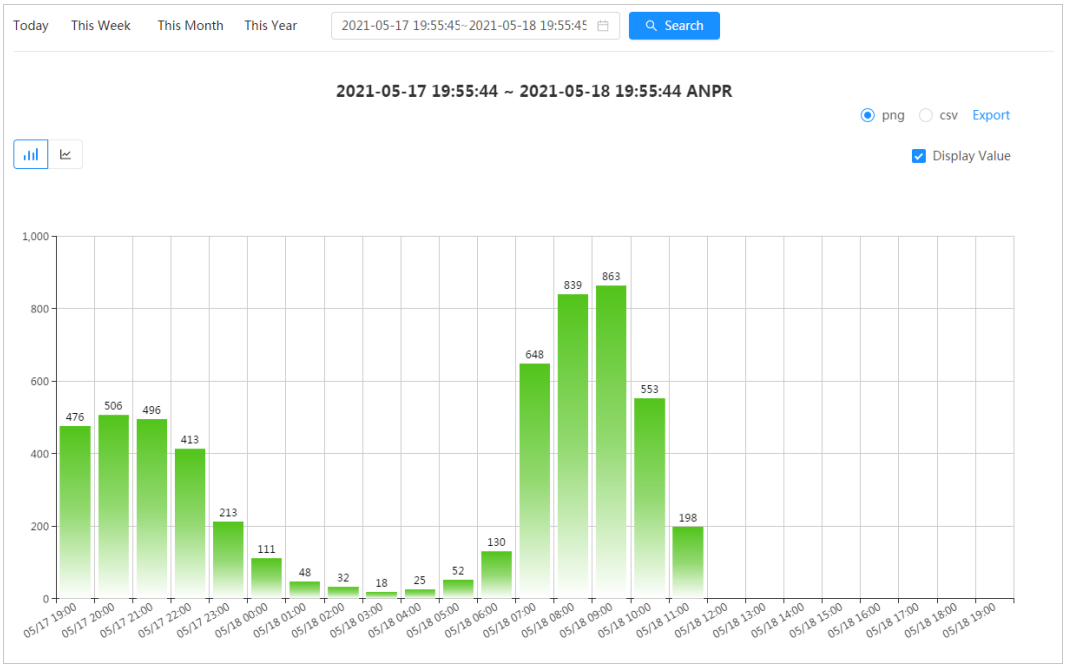
Step 1 Select **Report** > **Report** > **ANPR**.

Step 2 Set the period for the report.

For multi-channel camera, select the channel first.

Step 3 Click **Search**.

Figure 12-13 ANPR report



- Select the report form

Click to display the report in line chart; click to display the report in bar chart.

- Select the **Display Value** check box 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

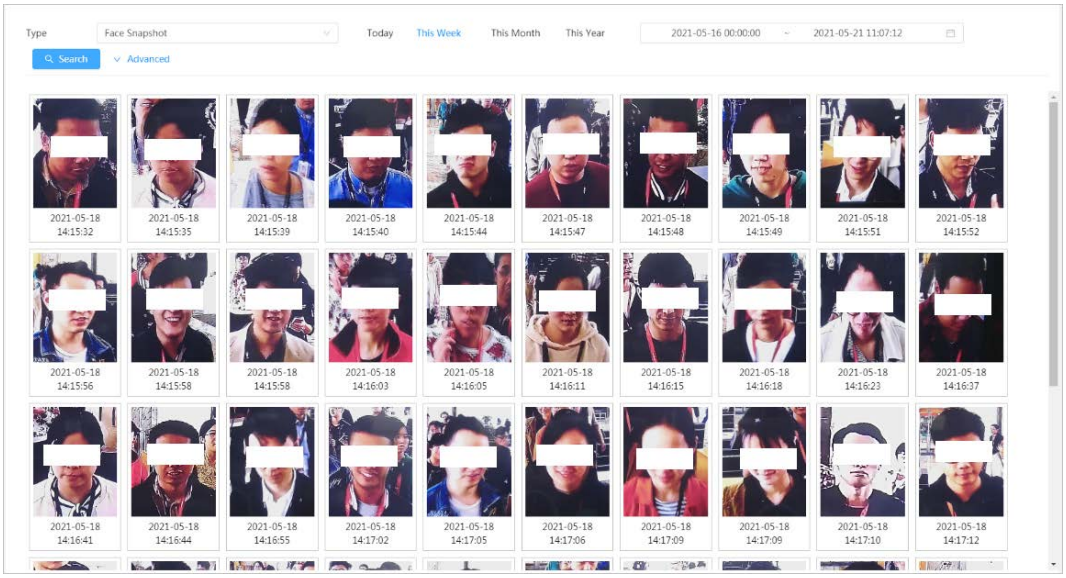
Step 1 Select **Report** > **Picture Query** > **Face**.

Step 2 Select the type and set the period for the report.

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

Step 3 Click **Search**. The search result is displayed.

Figure 12-14 Face report



Step 4 Click the picture, and then you can view the details.

12.3 Auto Upload

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

Step 1 Select **Report** > **Auto Upload**.

Step 2 Select the upload method, and then enable it.

Step 3 Set parameters.

Parameters of different upload methods are different.

- **HTTP**

  Click **Add**, and then add the information of server. You can add two server information at most.

Figure 12-15 HTTP upload method



Table 12-3 Description of HTTP mode parameter

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
IP/Domain name	The IP address and port number of the server which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Report type	Select the report type form the drop-down list. You can select more than one types at the same time. The report types in the drop-down list are the same with that supported 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.

- **FTP** upload method

Figure 12-16 FTP upload method

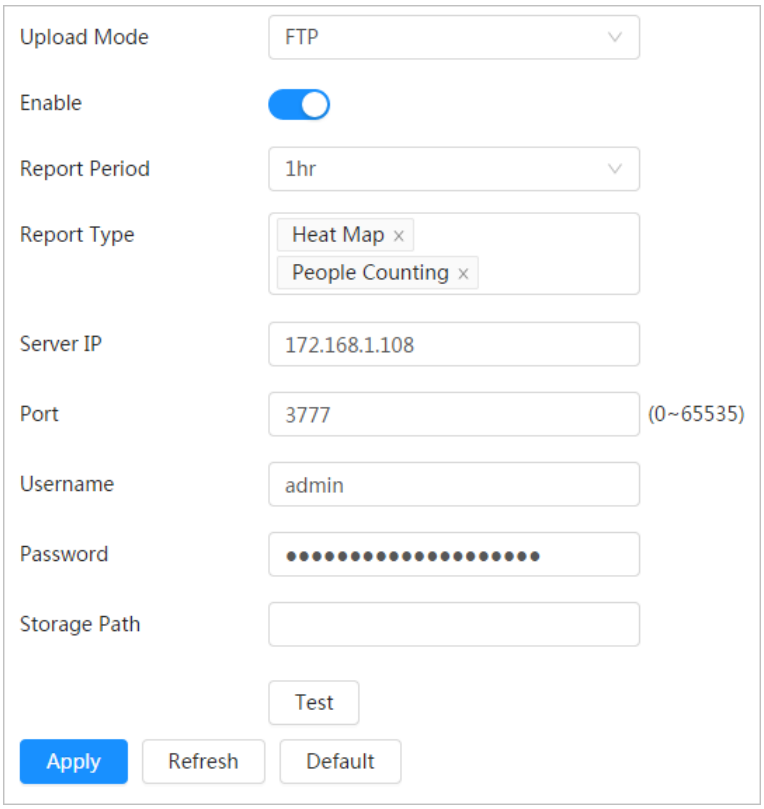


Table 12-4 Description of FTP mode parameter

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

- Email upload method

Figure 12-17 Email upload method

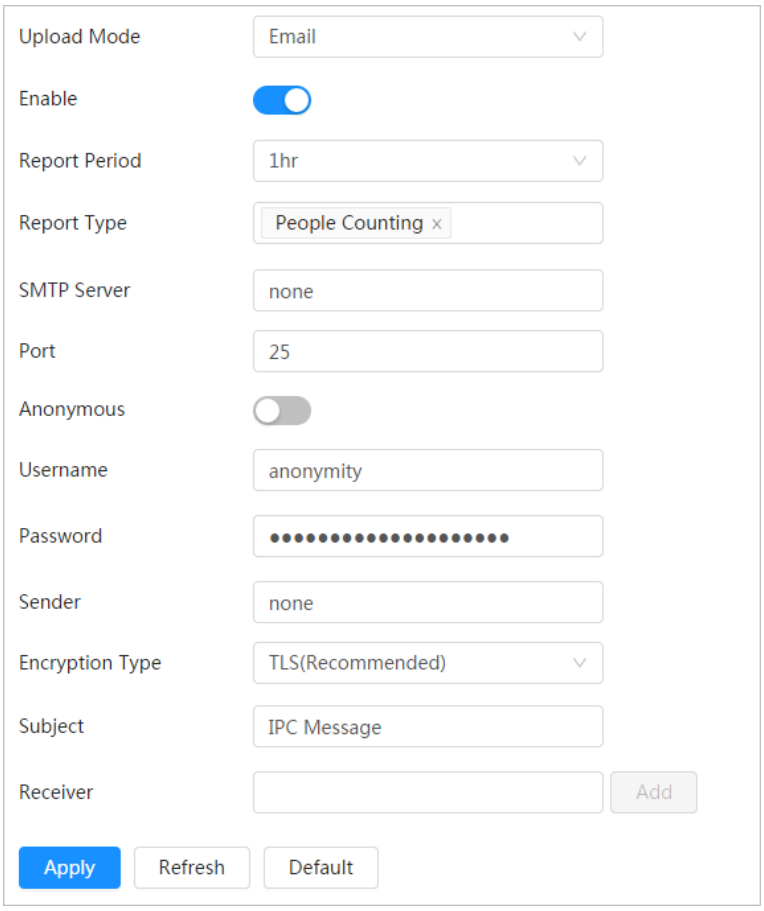


Table 12-5 Description of email mode parameter

Parameter	Description
Report Period	Select the report period from the drop-down list. It is 1 hour by default, which indicates that upload the report every 1 hour.
Report Type	Select the report type form the drop-down list. You can select more than one types at the same time. - 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. - 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.
SMTP server	SMTP (Simple Mail Transfer Protocol) server IP address and port number. See Table 12-6 for details.
Port	
Anonymous	Select **Anonymous**, and the sender's information is not displayed in the email.
Username	Username and password used to log in server. See Table 12-6 for details.
Password	

Parameter	Description
Sender	Sender's email address.
Encryption Type	Select the encryption type from None, SSL (Secure Sockets Layer) and TLS (Transport Layer Security).  See Table 12-6 for details.
Subject	Email subject. You can enter up to 120 characters in Chinese, English, and Arabic numerals.
Receiver	Email addresses of receivers. Click **add** to set more than one receivers. Supports 3 addresses at most.

Table 12-6 Description of major mailbox configuration

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

Step 4 Click **Apply**.

Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

2. **Update Firmware and Client Software in Time**

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

3. **Set and Update Passwords Reset Information Timely**

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**

   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
8. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
9. **Disable Unnecessary Services and Choose Secure Modes**
   If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
   If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
   - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
   - SMTP: Choose TLS to access mailbox server.
   - FTP: Choose SFTP, and set up strong passwords.
   - AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.
10. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
11. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
12. **Network Log**
    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
13. **Construct a Safe Network Environment**
    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:
    - Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
    - The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
    - Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
    - Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.