



IC Realtime IP Camera Web 3.X

User's Manual
V1.1.0





Foreword

General

This manual introduces the functions, configuration, general operation, and system maintenance of an IC Realtime network camera with the 4.0 web Interface.

Safety Instructions

The following signal words may 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 that, 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
V1.1.0	<ul style="list-style-type: none"> • 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". 	May 2022
V1.0.0	First release.	December 2021

Privacy Protection Notice

As the device user or data controller, you may collect the personal data of others such as their face, fingerprints, and car plate number. Ensure that any users and configurations are in compliance with the local privacy protection laws and regulations and to protect the legitimate rights and interests of other people by implementing measures that 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 may 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 may be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates may result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There may 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 a 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, and 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 to a final explanation.



Important Safeguards and Warnings

Electrical Safety

- All installation and operation shall conform to your local electrical safety codes.
- Use a 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 junction extruded from the device.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sunlight; otherwise, it may 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 dampness 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 a location where only professional staff with relevant knowledge of safety guards and warnings can access it. Accidental injury may happen to 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 scalding.
- Carefully follow the instructions in the manual when performing any disassembly operation on the device; otherwise, it may 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 a lightning arrester to improve lightning protection.
- 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 an air blower, or you can wipe the lens gently with a soft cloth that is moistened with

alcohol.

- You can clean the device body with a soft dry cloth, and for stubborn stains, use the cloth with mild detergent. To avoid possible damage to the device body coating which could cause performance to decrease, do not use volatile solvents such as alcohol, benzene, or diluent to clean the device body, nor can strong, abrasive detergent be used.
- For cameras equipped with a Dome cover, this cover is an optical component. Do not touch or wipe the cover with your hands directly during installation or operation. To remove dust, grease or fingerprints, wipe gently with moistened oil-free cotton with diethyl or moisten a soft cloth. You can also remove dust with an air blower.



- Strengthen the protection of network, device data and personal information by adopting measures that include but not limited to using a strong password, changing passwords regularly, upgrading the firmware to the latest version, and isolating the computer network. For some devices 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 the 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 may 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	10
4.1 Device Login	10
4.2 Resetting Password	11
5 Main Interface	13
6 Setting	14
6.1 Local	14
6.2 Camera	15
6.2.1 Setting Image Parameters	15
6.2.1.1 Interface Layout	15
6.2.1.2 Image	17
6.2.1.3 Exposure	18
6.2.1.4 Backlight	20
6.2.1.5 WB	21
6.2.1.6 Day/Night	22
6.2.1.7 Illuminator	22
6.2.1.8 Defog	24
6.2.1.9 Fisheye	24
6.2.2 Setting Encode Parameters	25
6.2.2.1 Encode	25
6.2.2.2 Overlay	27
6.2.2.2.1 Configuring Privacy Masking	27
6.2.2.2.2 Configuring Channel Title	28
6.2.2.2.3 Configuring Time Title	29
6.2.2.2.4 Configuring Location	29



6.2.2.2.5	Configuring Font Properties	30
6.2.2.2.6	Configuring Picture Overlay	30
6.2.2.2.7	Configuring Custom Title	31
6.2.2.2.8	Configuring Target Statistics	31
6.2.2.2.9	Configuring ANPR	32
6.2.2.2.10	Configuring Face Detection	33
6.2.2.2.11	Configuring Face Recognition	33
6.2.2.2.12	Configuring Face Statistics	34
6.2.2.2.13	Configure Face&Body Counting	34
6.2.2.2.14	Configuring Parking Space	35
6.2.2.3	ROI	36
6.2.3	Audio	36
6.2.3.1	Setting Audio Parameters	36
6.2.3.2	Setting Alarm Tone	37
6.3	Network	39
6.3.1	TCP/IP	39
6.3.2	Port	41
6.3.3	PPPoE	43
6.3.4	DDNS	43
6.3.5	Email	44
6.3.6	UPnP	46
6.3.7	SNMP	47
6.3.8	Bonjour	49
6.3.9	Multicast	50
6.3.10	Register	51
6.3.11	QoS	51
6.3.12	Platform Access	52
6.3.12.1	P2P	52
6.3.12.2	ONVIF	53
6.3.12.3	RTMP	53
6.3.13	Basic Service	54
6.4	Event	56
6.4.1	Setting Alarm Linkage	56
6.4.1.1	Setting Alarm-in	56
6.4.1.2	Alarm Linkage	57
6.4.1.2.1	Adding Schedule	57
6.4.1.2.2	Record Linkage	58



6.4.1.2.3 Snapshot Linkage	59
6.4.1.2.4 Alarm-out Linkage	59
6.4.1.2.5 Email Linkage	59
6.4.1.3Subscribing Alarm	60
6.4.1.3.1 About Alarm Types	60
6.4.1.3.2 Subscribing Alarm Information	60
6.4.2Setting Exception	61
6.4.2.1Setting SD Card Exception	61
6.4.2.2Setting Network Exception	62
6.4.2.3Setting Voltage Detection	63
6.4.3Setting Video Detection	64
6.4.3.1Setting Motion Detection	64
6.4.3.2Setting Video Tampering	66
6.4.3.3Setting Scene Changing	67
6.4.4Setting Audio Detection	67
6.5Storage	68
6.6System	69
6.6.1General	69
6.6.1.1Basic	69
6.6.1.2Date & Time	70
6.6.2Account	71
6.6.2.1User	71
6.6.2.1.1 Adding User	71
6.6.2.1.2 Resetting Password	74
6.6.2.2Adding User Group	75
6.6.2.3ONVIF User	76
6.6.3Peripheral Management	77
6.6.3.1Configuring Serial Port	77
6.6.3.2Configuring External Light	77
6.6.3.3Configuring Wiper	78
6.6.4Manager	79
6.6.4.1Requirements	79
6.6.4.2Maintenance	79
6.6.4.3Import/Export	80
6.6.4.4Default	81
6.6.5Upgrade	81
6.7System Information	82



6.7.1 Version	82
6.7.2 Online User	82
6.8 Setting Log	82
6.8.1 Log	82
6.8.2 Remote Log	83
7 Live	84
7.1 Live Interface	84
7.2 Setting Encode	85
7.3 Live View Function Bar	85
7.4 Window Adjustment Bar	87
7.4.1 Adjustment	87
7.4.2 Zoom and Focus	87
7.4.3 Image Adjustment	88
7.4.4 Fisheye	89
7.5 Display Mode	93
8 AI	97
8.1 Setting Crowd Distribution Map	97
8.1.1 Global Configuration	97
8.1.2 Rule Configuration	98
8.2 Setting Face Recognition	99
8.2.1 Setting Face Detection	100
8.2.2 Setting Face Database	103
8.2.2.1 Creating Face Database	103
8.2.2.2 Adding Face Picture	105
8.2.2.2.1 Single Adding	105
8.2.2.2.2 Batch Importing	107
8.2.2.3 Managing Face Picture	108
8.2.2.3.1 Editing Face Information	108
8.2.2.3.2 Deleting Face Picture	109
8.2.2.4 Face Modeling	110
8.2.3 Setting Arm Alarm	110
8.2.4 Viewing Face Recognition Result	113
8.3 Setting Face Detection	114
8.4 Setting IVS	116
8.4.1 Global Configuration	117
8.4.2 Rule Configuration	118
8.5 Setting Vehicle Density	122



8.6 Setting Parking Space	124
8.6.1 Rule Configuration	124
8.6.2 Global Configuration	128
8.7 Setting Video Metadata	128
8.7.1 Global Configuration	128
8.7.2 Rule Configuration	129
8.7.3 Viewing Video Metadata Report	131
8.8 Setting People Counting	132
8.8.1 People Counting	132
8.8.2 Queuing	135
8.8.3 Global Configuration	137
8.9 Face & Body Detection	138
8.9.1 Global Configuration	138
8.9.2 Rule Configuration	139
8.10 Setting Heat Map	141
8.11 Setting ANPR	141
8.11.1 Lane Configuration	142
8.11.2 Rule Configuration	143
8.11.3 Picture	144
8.11.4 Allowlist	145
8.11.5 Blocklist	148
9 Security	149
9.1 Security Status	149
9.2 System Service	150
9.2.1 802.1x	150
9.2.2 HTTPS	151
9.3 Attack Defense	152
9.3.1 Firewall	152
9.3.2 Account Lockout	153
9.3.3 Anti-DoS Attack	153
9.4 CA Certificate	154
9.4.1 Installing Device Certificate	154
9.4.1.1 Creating Certificate	154
9.4.1.2 Applying for and Importing CA Certificate	155
9.4.1.3 Installing Existing Certificate	156
9.4.2 Installing Trusted CA Certificate	157
9.5 A/V Encryption	158



9.6 Security Warning	159
10 Record	160
10.1 Playback	160
10.1.1 Playing Back Video	160
10.1.2 Clipping Video	162
10.1.3 Downloading Video	163
10.2 Setting Record Control	164
10.3 Setting Record Plan	165
10.4 Storage	166
10.4.1 Local Storage	167
10.4.2 Network Storage	168
10.4.2.1 FTP	168
10.4.2.2 NAS	169
11 Picture	171
11.1 Playback	171
11.1.1 Playing Back Picture	171
11.1.2 Downloading Picture	172
11.2 Setting Snapshot Parameters	173
11.3 Setting Snapshot Plan	174
11.4 Storage	174
11.5 Setting Upload Method	174
12 Report	176
12.1 Viewing Report	176
12.1.1 Face Recognition	176
12.1.2 Video Metadata	177
12.1.3 People Counting	178
12.1.4 Crowd Distribution	181
12.1.5 Vehicle Density	182
12.1.6 Heat Map	182
12.1.7 ANPR	184
12.2 Searching for Face Picture	185
12.3 Auto Upload	186
Appendix 1 Cybersecurity Recommendations	191

1 Overview

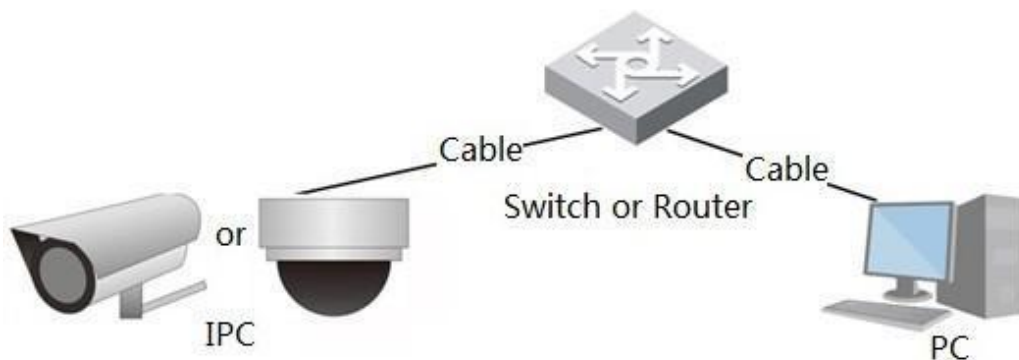
1.1 Introduction

An IPC (Internet Protocol camera), is a type of digital video camera that receives control data and sends image data through the internet. They are commonly used for surveillance, requiring no local recording device, only a local area network. Adding them to an NVR greatly increases its functionality and utility. IP cameras are divided into single-channel and multi-channel cameras according to the Lens quantity. For a multi-channel camera, you can configure the parameters for each channel or lens.

1.2 Network Connection

In the general IP Camera (IPC) network topology, the IPC is connected to the PC through a network switch or router to communicate with other devices on the same network.

Figure 1-1 General IPC network



You can acquire the IP address by searching on ConfigTool, and then access IPC through the network.

1.3 Function

Functions may vary with different devices according to the actual product specifications.

1.3.1 Basic Function

Real-time Monitoring

- Live view.
- When live viewing the image, you can enable audio and voice talk.
- Adjust the PTZ image to the proper position.
- Snapshot or triple snapshot of the monitoring image for subsequent view and processing.



Record

- Record events when monitoring for subsequent view and processing.
- Configure coding parameters, and adjust the live view image.
- Auto record as scheduled.
- Play back recorded video and pictures.
- Download recorded video and pictures.
- Alarm-linked recording.

Account

- Add, modify and delete user groups, and manage user authorities according to the user group.
- Add, modify and delete users, and configure user authorities.
- Modify user password.

1.1.2 Intelligent Function

Alarm

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

Smart Track

- Set calibration and parameters for smart track and enable alarm track.
- Switch between smart track and PTZ camera auto track.

Video Detection

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

Intelligent Motion Detection

- Avoids alarms triggered by environmental changes such as lights and shadows.
- When an event is triggered by a Person or Vehicle, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Audio Detection

- Abnormal audio input detection and intensity change detection.
- When the event is triggered, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

IVS

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



Crowd Map

- View crowd distribution in real-time to avoid accidents like stampedes.
- When the event is triggered, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Face Detection

- This function detect faces and displays the related attributes on the live interface.
- When an event is triggered, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Face Recognition

- After detecting a face, the system will compare the detected face with faces in the face database, and activates events.
- Query the recognition result.

People Counting

- Count the people flow in/out of the detection area and generate a report.
- When an event is triggered, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Heat Map

- Counts the cumulative density of moving objects.
- View the report of the heat map.

ANPR

- Recognizes plate number in the detection area and displays the related information on the live interface.
- When an event is triggered, the system can activate alarm output and send emails or a snapshot.

Video Metadata

- Takes a snapshot of people, non-motor vehicles, and vehicles and displays the related information on the live interface.
- When an alarm is triggered, the system links alarm output.

Alarm Setting

- An event will be triggered when an external alarm input device on the IPC is triggered.
- When an event is triggered, the system can activate linkages such as recording, alarm output, sending email, PTZ operation, and snapshot.

Abnormality

- SD card error, network disconnection, illegal access, voltage detection, and security exception.
- When there is an SD card error or illegal access is triggered, the system can activate the alarm output and send an email.
- When a network disconnection event is triggered, the IPC can activate recording and alarm

output.

- When the input voltage is more or less than the rated voltage, the event is triggered, and the system can activate by sending an email.

2 Configuration Flow

See Figure 2-1. For details, see Table 2-1. Configure the device according to the local environment.

Figure 2-1 Configuration flow

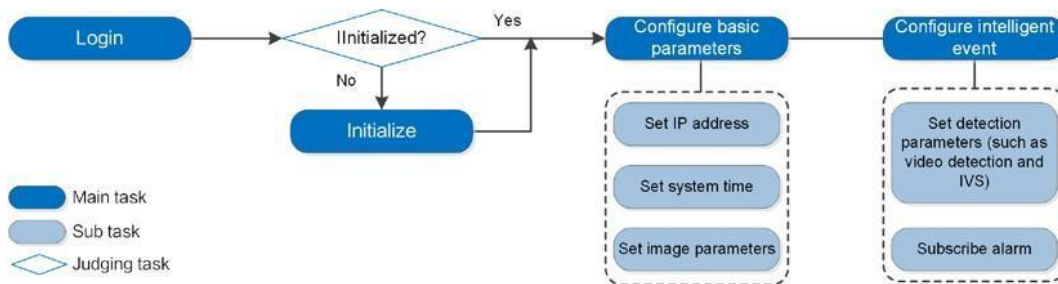


Table 2-1 Description of flow

Configuration	Description	Reference	
Login	Open a web browser and enter the IP address to log in to the web interface, The camera IP address is on 192.168.1.108/ DHCP by default.	"4.1 Login"	
Initialization	Initialize the camera when it is used for the first time.	"3 Device Initialization"	
Basic parameters	Camera parameters	Configure image, encoding, and audio parameters to ensure the image quality.	"6.2 Camera".
	Date & time	Set the date and time to ensure the recording time is correct.	"6.6.1.2 Date & Time"
	IP address	Change the IP address according to network requirements and local standards.	"6.3.1 TCP/IP"
	Subscribe alarm	Subscribe to an 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

The device initialization is a mandatory step for first-time use. This manual is based on the operation of the web interface. You can also initialize the device through the ConfigTool, NVR, or the ITM-9000.



- To ensure the device's security , keep the password properly after initialization and change the password on a regular basis.
- When initializing the IP camera make sure your PC is on the same network segment as the camera.

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



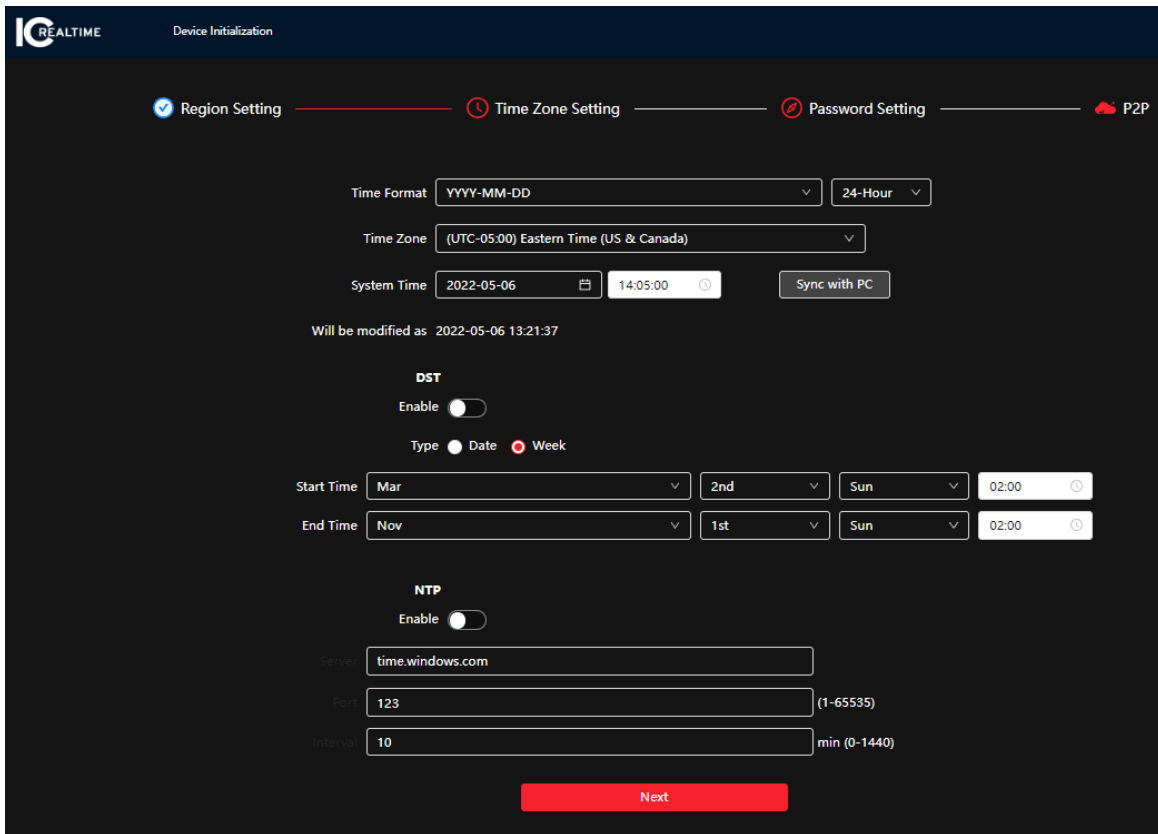
The IP is set on DHCP (or 192.168.1.108 if it is not plugged into a network with DHCP) by default.

Figure 3-1 Region Setting

The screenshot shows the 'Device Initialization' web interface for IC REALTIME. At the top, there is a progress bar with four steps: 'Region Setting' (active, indicated by a red checkmark), 'Time Zone Setting' (disabled, indicated by a red clock icon), 'Password Setting' (disabled, indicated by a red checkmark), and 'P2P' (disabled, indicated by a red cloud icon). Below the progress bar, there are three dropdown menus for configuration: 'Area' is set to 'United States', 'Language' is set to 'English', and 'Video Standard' is set to 'NTSC'. At the bottom center, there is a red 'Next' button.

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

Figure 3-3 Time zone setting



IC REALTIME Device Initialization

Region Setting
 Time Zone Setting
 Password Setting
 P2P

Time Format:

Time Zone:

System Time:

Will be modified as 2022-05-06 13:21:37

DST

Enable:

Type: Date Week

Start Time:

End Time:

NTP

Enable:

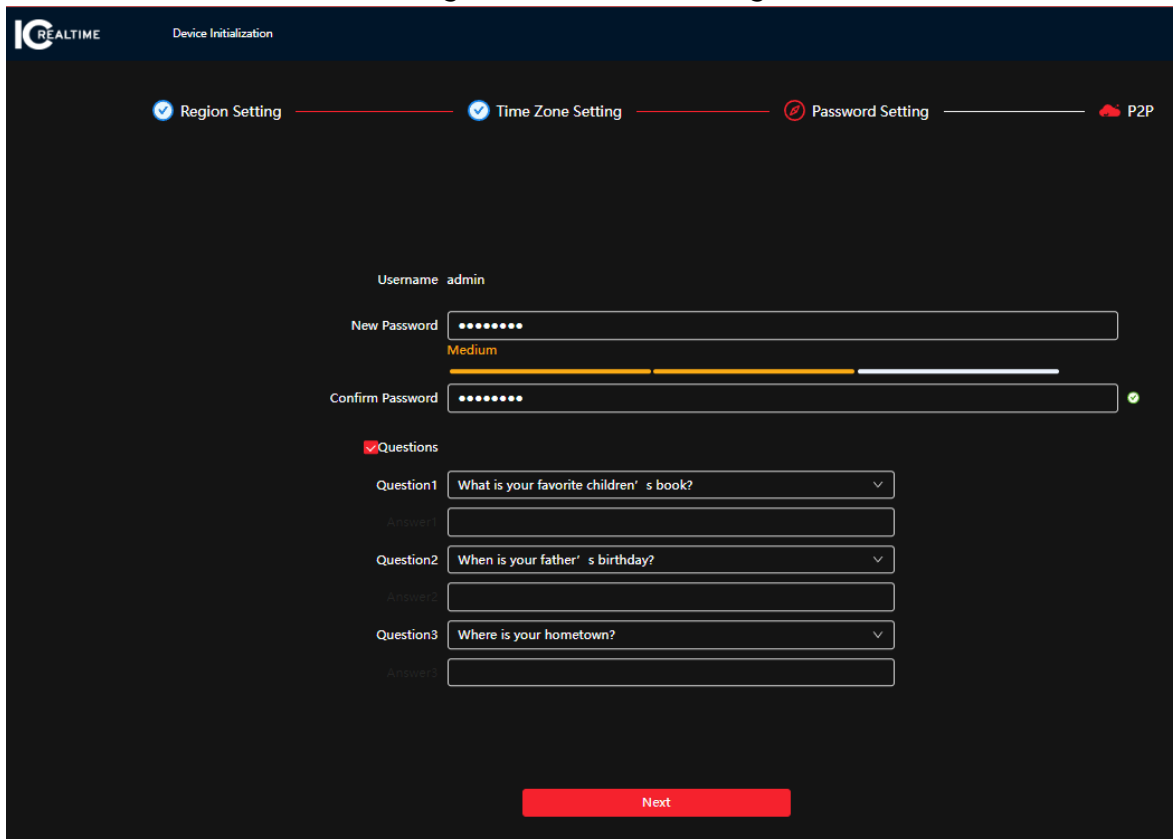
Server:

Port: (1-65535)

Interval: min (0-1440)

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

Figure 3-4 Password setting



IC REALTIME Device Initialization

Region Setting
 Time Zone Setting
 Password Setting
 P2P

Username:

New Password:

Password Strength: Medium

Confirm Password:

Questions

Question1:

Answer1:

Question2:

Answer2:

Question3:

Answer3:

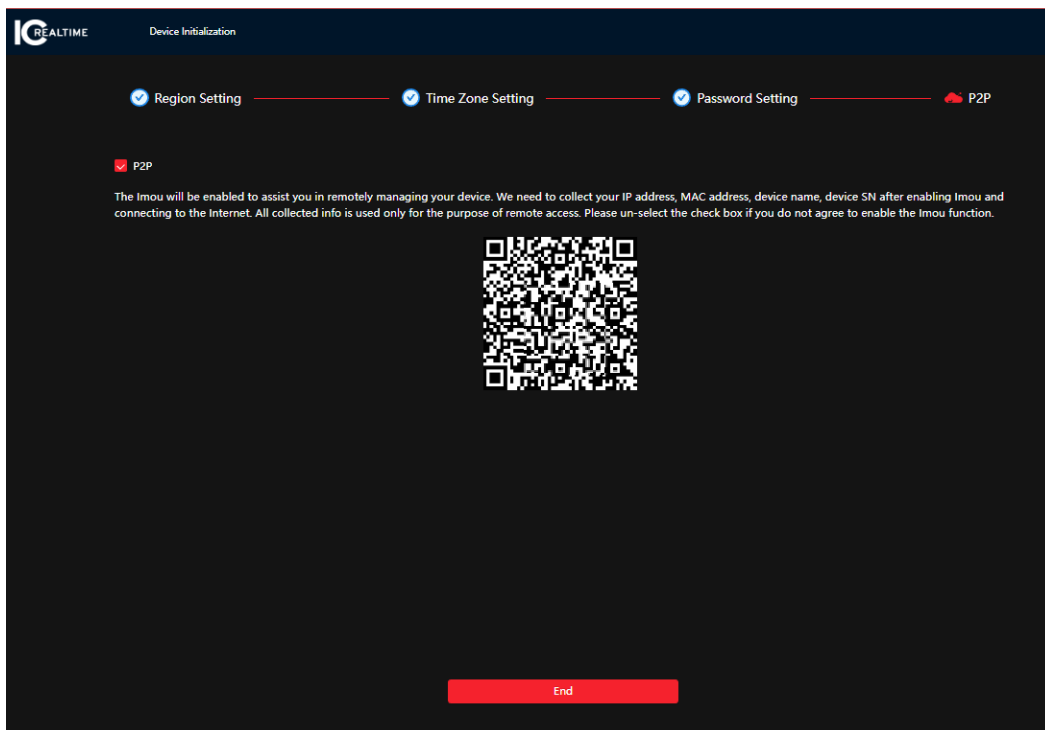
Step 5 Set the password for the admin account.

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: upper case, lower case, number, and special character (excluding ' " ; : &). Set a high-security level password according to the password security requirements.
Confirm password	
Security Questions	Setup answers to the security questions of your choice. The answers will be used for resetting the admin password if it is forgotten.

Step 6 Click **Next**, and then the **P2P** interface will be displayed (in some units).

Figure 3-5 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.

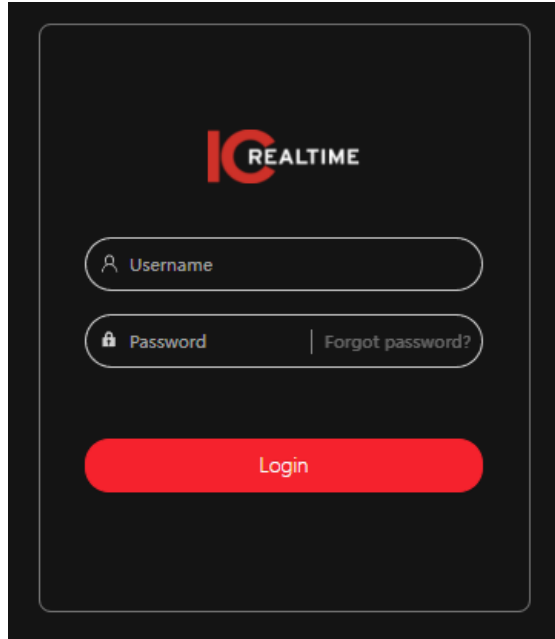


Step 2 Enter the username and password. The username is admin by default.



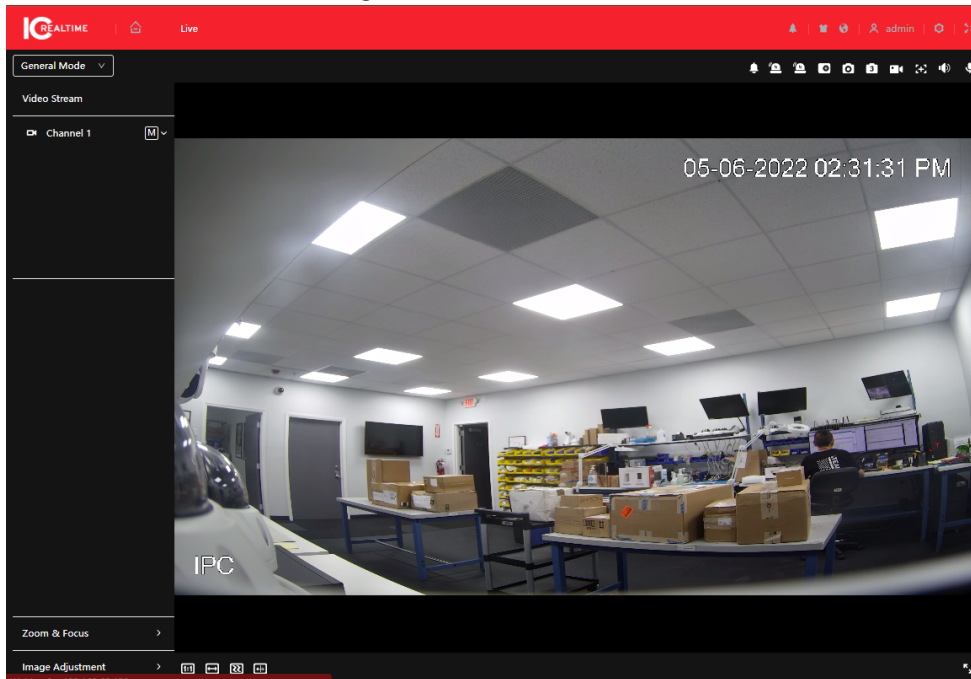
Click **Forgot password?** to reset the password by answering the security questions set during the initialization. For details, see "4.2 Resetting Password".

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 set up answers to the security questions upon camera initialization. For details, see "3. Initialization".

Procedure

Step 1 Open a web browser, enter the IP address of the device in the address bar then press Enter.

Figure 4-3 Login

The login interface features a dark background with the IC REALTIME logo at the top center. Below the logo are two input fields: "Username" with a person icon and "Password" with a lock icon. A "Forgot password?" link is positioned to the right of the password field. A prominent red "Login" button is located at the bottom of the form.

Step 2 Click **Forgot password?** to reset the password by answering the security questions that were set during the initialization.

Figure 4-4 Answering the security questions

The security questions interface has a dark background with the IC REALTIME logo in the top left. At the top, there are two progress indicators: "1 Security Code" (active) and "2 Password Reset". The main area contains three questions, each with a label (Question1, Question2, Question3) and an "Answer" field. A red "Next" button is positioned at the bottom of the question list.

5

Main Interface


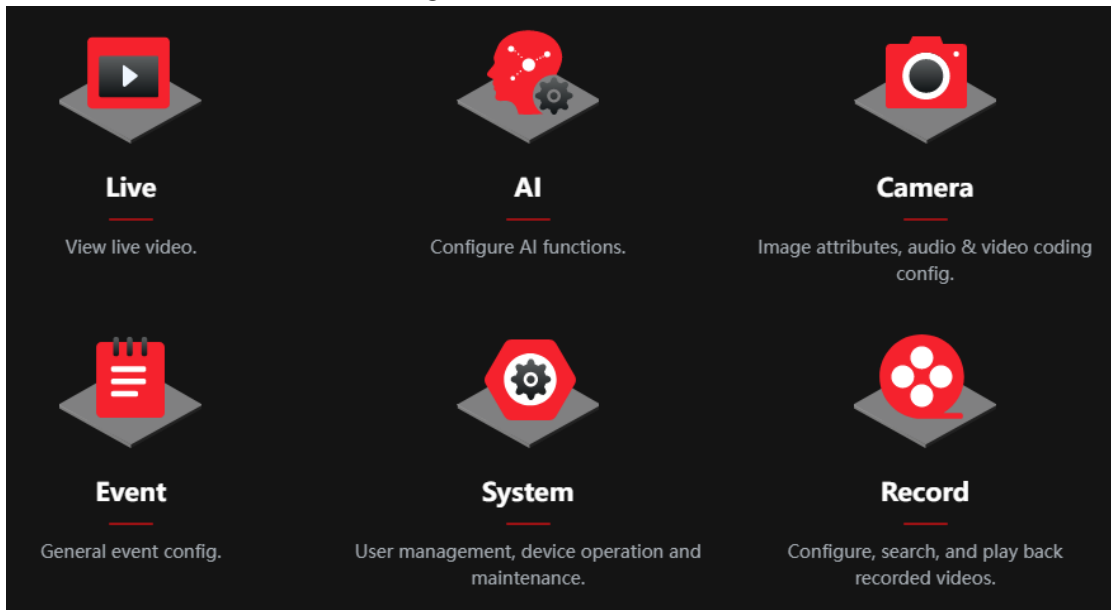
Click  at the left-upper corner of the interface to display the main interface.

Figure 5-1 Main interface




- Live: Monitor the real-time live view 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.
- System: Configure system parameters, including general, date & time, account, safety, PTZ settings, default, import/export, remote, auto maintain and upgrade.
- Security: Monitor the device's security status and set security functions.
- Record: Play back or download a recorded video.
- Picture: Play back or download image files.
- For a camera with multiple lens/ channels, Select a channel number to set the parameters of that channel.
- Report: Search the AI event report and system report.
- Alarm subscription: Subscribe to an alarm.
- Skin setting: Set the visual web skin.
- Language setting: Set the language.
- Restart: Click **admin** at the upper-right corner of the interface, and select **Reboot** to restart the camera.
- Logout: Click **admin** at the upper-right corner of the interface, select **Logout** to log out of the camera and navigate 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.

This section introduces the basic settings 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.

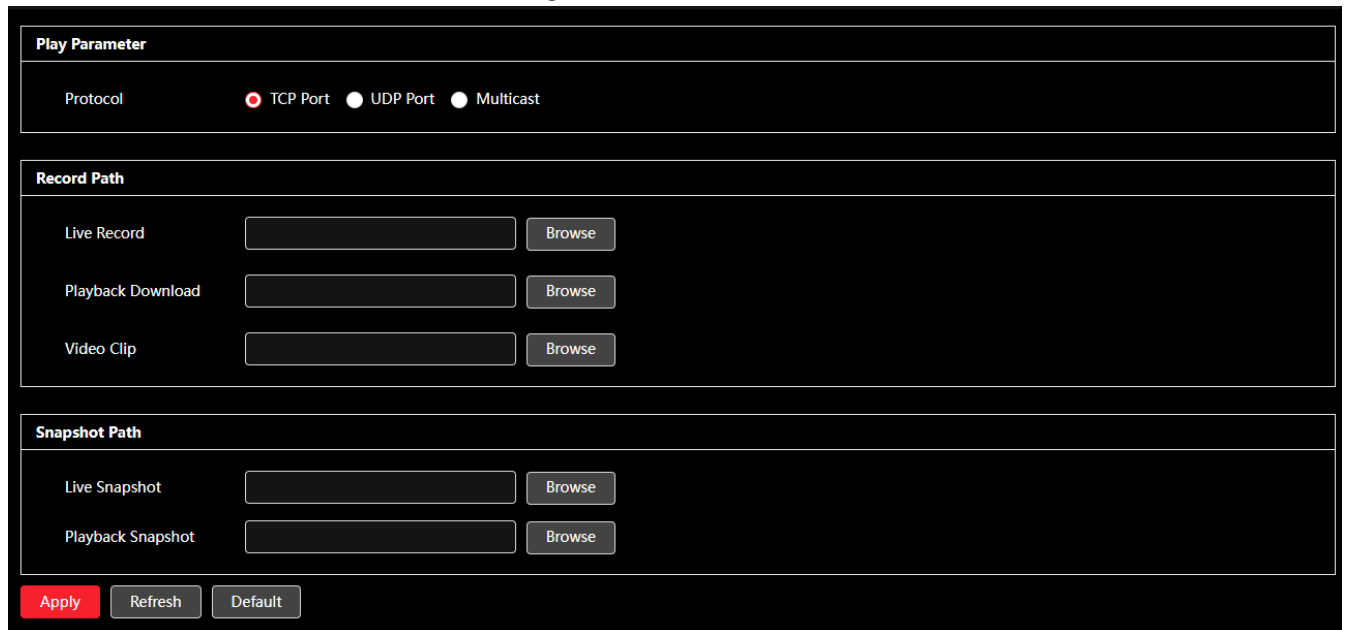
- Method 1: Click , and then select the corresponding item.
- Method 2: Click the corresponding icon on the main interface.

6.1 Local

This section allows you to configure the storage path for live snapshots, live record, playback snapshot, playback download, and video clips.

Step 1 Select  > **Local**.

Figure 6-1 Local




The screenshot shows a configuration window titled "Local" with three main sections: "Play Parameter", "Record Path", and "Snapshot Path".


- Play Parameter:** Includes a "Protocol" section with three radio buttons: "TCP Port" (selected), "UDP Port", and "Multicast".
- Record Path:** Contains three rows, each with a text input field and a "Browse" button:
 - Live Record
 - Playback Download
 - Video Clip
- Snapshot Path:** Contains two rows, each with a text input field and a "Browse" button:
 - Live Snapshot
 - Playback Snapshot

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

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

Table 6-1 Local Parameter description

Parameter	Description
Protocol	Select the network transmission protocol as necessary, The options are TCP, UDP and Multicast .  Before selecting Multicast , make sure that you have set the Multicast parameters prior .
Live Record	The recorded video of live interface. The default path is C:\Users\admin\WebDownload\LiveRecord.
Playback Download	The downloaded video from the playback interface. The default path is C:\Users\admin\WebDownload\PlaybackRecord.
Video Clips	The clipped video of from the playback interface. C:\Users\admin\WebDownload\VideoClips.
Live Snapshot	The snapshot from the live interface. The default path is C:\Users\admin\WebDownload\LiveSnapshot.
Playback Snapshot	The snapshot from the playback interface. The default path is C:\Users\admin\WebDownload\PlaybackSnapshot.


 Admin in the path refers to the PC Operating System account being used.

Step 3 Click **Save**.

6.2 Camera

This section introduces the camera setting, which includes image, encoding, and audio parameters.



Camera parameters may vary depending on the IP camera model.

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

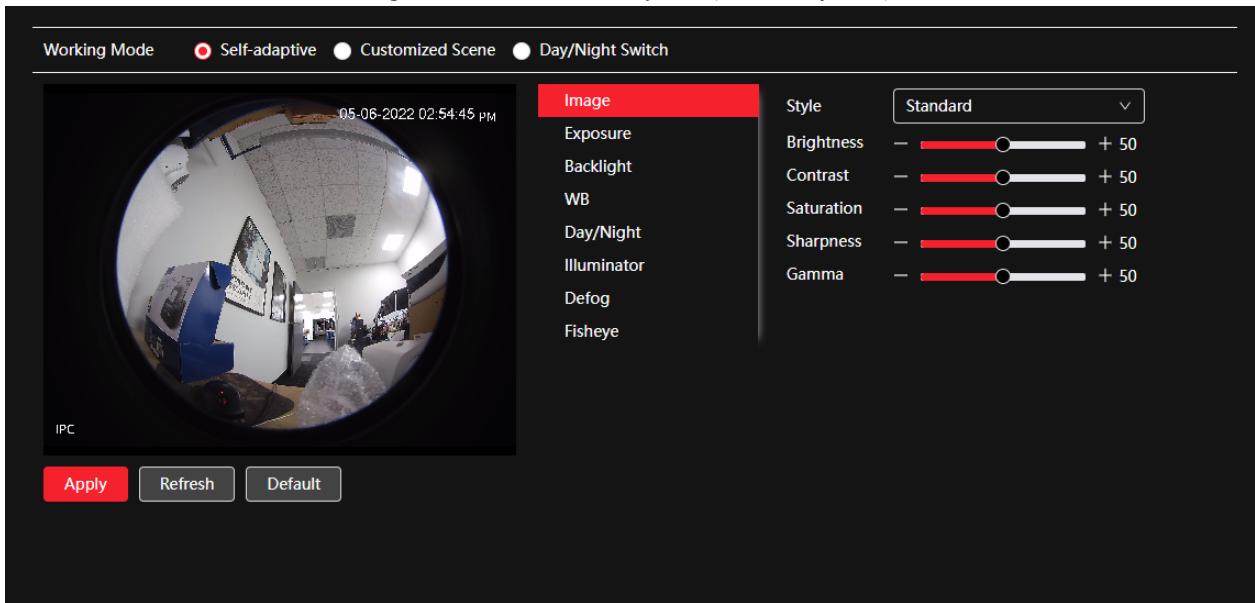
Configure camera parameters to improve the scene clarity, and ensure accurate surveillance.

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 necessary.

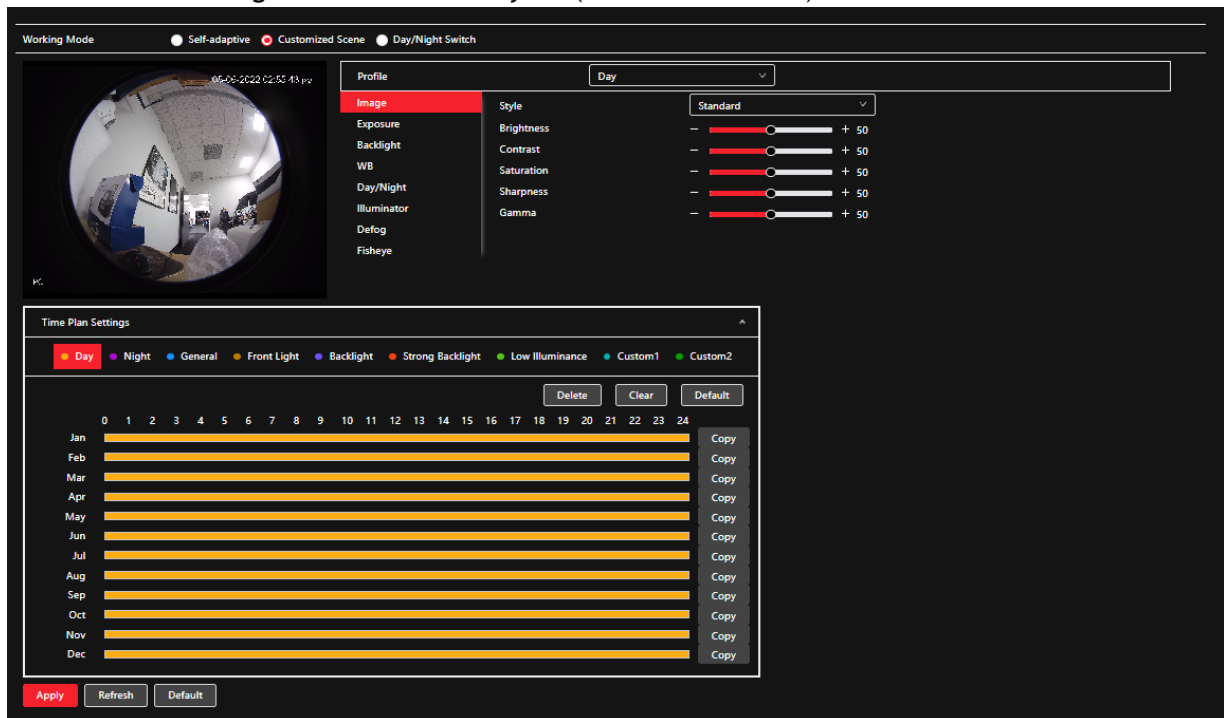
- Self-adaptive: The camera will adjust the image according to the environment.

Figure 6-2 Interface layout (self-adaptive)



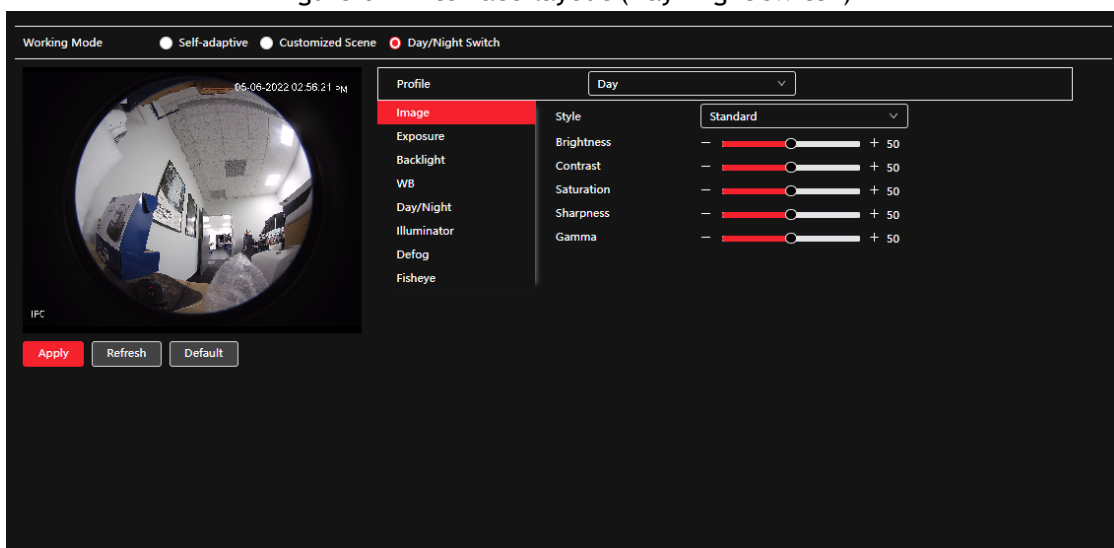
- Customized scene: You can select the profile as necessary. Select the profile in **Time Plan Setting** and drag the slide block to set a certain time as the selected profile. For example, set 8:00-18:00 as day, and 0:00-8:00 and 18:00-24:00 as night

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 necessary.

Step 1 Select  > Camera > Image > Image.


Figure 6-5 Image



Step 2 Configure picture parameters.

Table 6-2 Description of picture parameters

Parameter	Description
Style	<p>Select the picture style from soft, standard and vivid.</p> <ul style="list-style-type: none"> • Soft: Default image style, displays the actual color of the image. • Standard: The hue of the image will be weaker than the actual image, and with a smaller contrast. • Vivid: The image will be more vivid than the actual image.

Parameter	Description
Brightness	Changes the value to adjust the picture brightness. The greater the value, the brighter the picture will be, and the smaller the darker. The picture may be hazy if the value is configured at an extreme value.
Contrast	Changes the contrast of the picture. The greater the value, the more the contrast will be between bright and dark areas, and the smaller the less. If the value is set too large, dark areas will be too dark and bright areas are easier to be overexposed. The picture may be hazy if the value is configured at an extreme value.
Saturation	Makes the color deeper or lighter. The greater the value, 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 greater 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 greater the value, the brighter the picture will be, and the smaller the darker.
Flip	<p>Changes the display direction of the picture, see the options below.</p> <ul style="list-style-type: none"> • 0°: Normal display. • 90°: The picture rotates 90° clockwise. • 180°: The picture rotates 90° counterclockwise. • 270°: The picture flips upside down. <p> For some models, please set the resolution to be 1080p or lower when using 90° and 180°. For details, see "6.2.2 Setting Encode Parameters".</p>
Mirror	Click <input type="checkbox"/> , and the picture will display with left and right side reversed.

Step 3 Click **Apply**.

6.2.1.3 Exposure

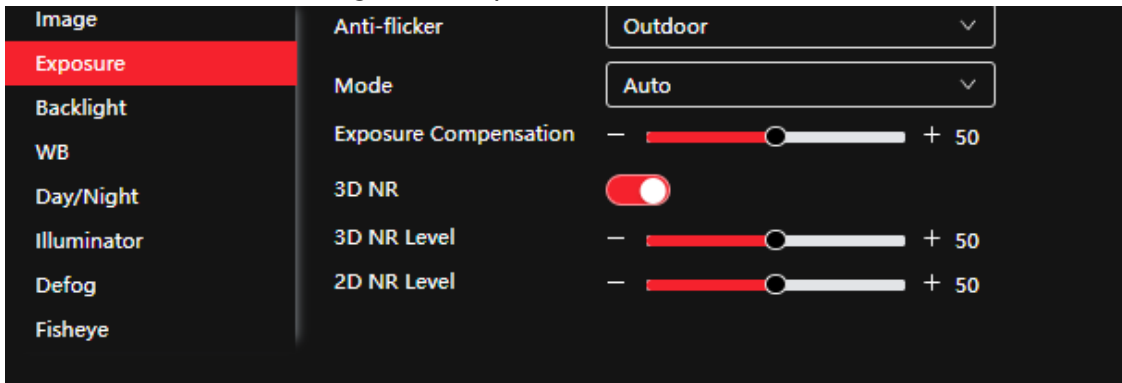
Configure iris and shutter to improve image clarity.



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	<p>Options are 50 Hz, 60 Hz and Outdoor.</p> <ul style="list-style-type: none"> • 50 Hz: If the power source is 50 Hz, the IPC will adjust the exposure according to ambient light automatically to ensure that there is no striping in the image will appear. • 60 Hz: If the power source is 60 Hz, the IPC will adjust the exposure according to ambient light automatically to ensure that there is no striping in the image will appear. • Outdoor: Select if in an outdoor location.
Mode	<p>Device exposure modes.</p> <ul style="list-style-type: none"> • Auto: Adjusts the image brightness according to the actual condition automatically. • Gain Priority: When the exposure range is normal, the camera defaults the configured gain range when auto-adjusting according to the ambient lighting condition. If the image brightness is insufficient and the gain has reached the upper or lower limit, the system adjusts shutter value automatically to ensure a good image at an ideal brightness. You can configure the gain range to adjust the gain level when using gain priority mode. • Shutter priority: When the exposure range is normal, the system defaults to the configured shutter range when auto adjusting according to the ambient lighting condition. If the image brightness is insufficient and the shutter value has reached an upper or lower limit, the system adjusts the gain value automatically to ensure the image is at an ideal brightness. • Manual: Configure gain and shutter value manually to adjust image brightness. <p> If the Anti-flicker is set to Outdoor, you can select Auto, Gain priority, Shutter priority or Manual in the Mode list.</p>

Exposure Compensation	Sets the value, and it ranges from 0 to 50. The greater the value, 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 an auto-iris lens. <ul style="list-style-type: none"> • If 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.
3D NR	Works with multi-frame (no less than 2 frames) images and reduces noise by using the frame information between previous and later frames.
Level	This configuration is available only when the 3D NR is enabled. The greater the level is, the better the result will be.

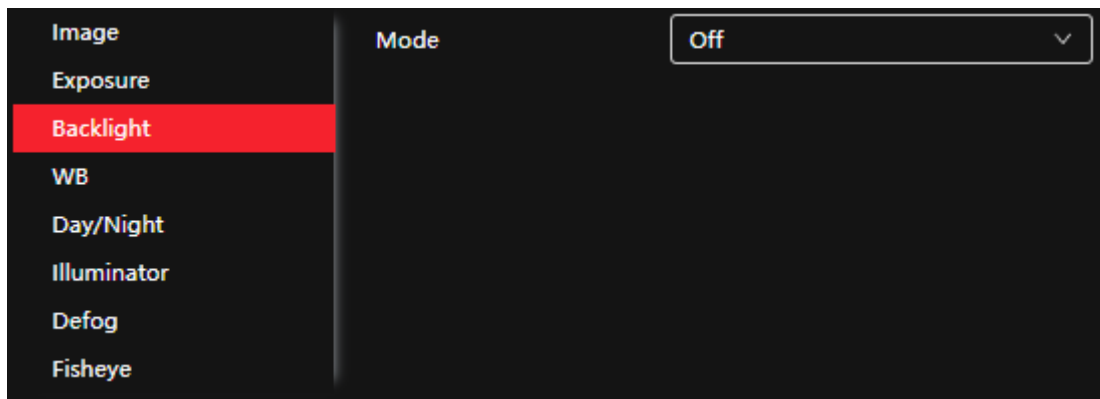
Step 3 Click **Apply**.

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

Step 3 Click **Apply**.

6.2.1.5 WB

The White Balance (WB) function allows white objects to always display a white color in different environments.


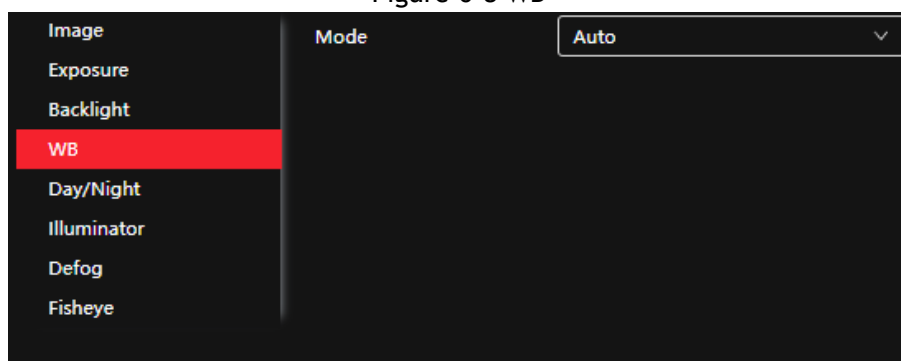
Step 1 Select  > **Camera** > **Image** > **WB**.

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 scenes 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.


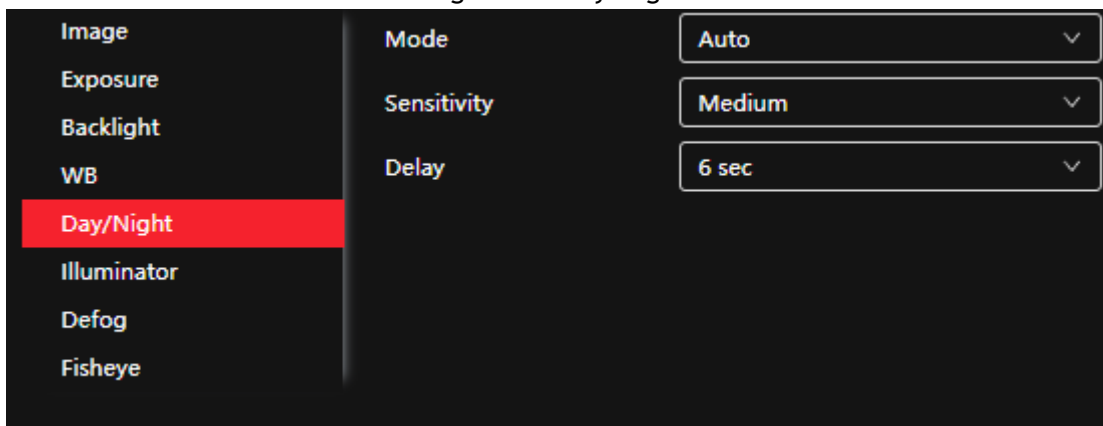

Step 1 Select  > **Camera** > **Image** > **WB**.

Figure 6-9 Day/night



Step 2 Configure day and night parameters.

Table 6-6 Description of day and night parameters

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

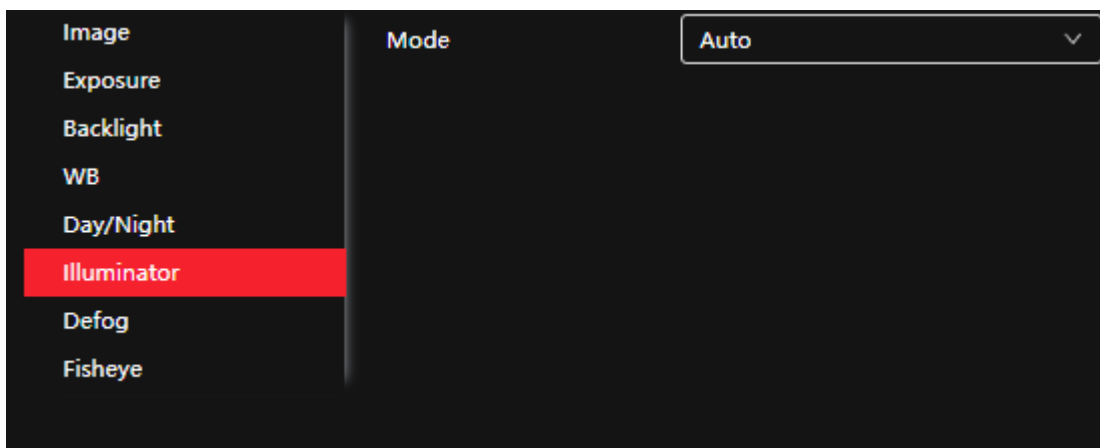
Step 3 Click **Apply**.

6.2.1.7 Illuminator

This configuration is available only if the device is equipped with an illuminator.

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

Figure 6-10 illuminator



Step 2 Configure illuminator parameters.

Table 6-7 Description of illuminator parameters

Parameter	Description	
Fill Light	Set Fill Light for sound and siren cameras (if equipped). <ul style="list-style-type: none"> • IR Mode: If the IR illuminator is enabled, the white light will be disabled. If an alarm is triggered, the system will link the white lights. • White Light: Enables the white light and disables the IR illuminator. If an alarm is triggered, the system will link the white light. • Soft Light Mode: Enables the IR illuminator and white light at the same time, and auto-adjusts the brightness of the two illuminators to acquire the best possible image. 	
Mode	Manual	Adjusts the brightness of the illuminator manually.
	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 in the ambient light. <ul style="list-style-type: none"> • When the ambient light turns darker, the system turns on the low beam lights first, if the brightness is still insufficient, then it turns on the high beam lights. • When the ambient light turns brighter, the system dims high beam lights until they are off, and then the low beam lights. • When the focus reaches a certain wide-angle, the IPC will not turn on the high beam light to avoid short-distance over-exposure. You can configure light compensation manually to fine-tune IR light intensity.
	Off	Illuminator is disabled/ off.

Step 3 Click **Apply**.

6.2.1.8 Defog

If the image quality is compromised in a foggy or hazy environment, defog can be used to improve image clarity.


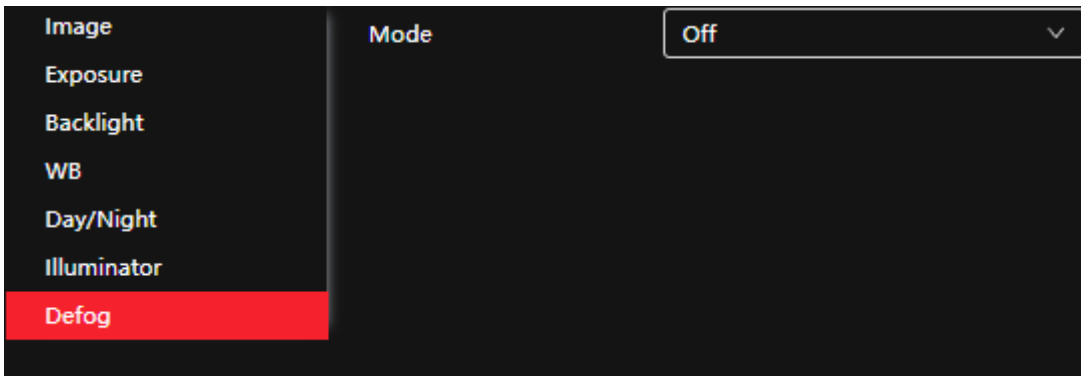
Step 1 Select  > **Camera** > **Image** > **Defog**.

Figure 6-11 Light



Step 2 Configure defog parameters.

Table 6-8 Description of defog parameters

Defog	Description
Manual	Configure the intensity and atmospheric light mode manually. The IPC will adjust the image clarity accordingly. The atmospheric light mode can be adjusted automatically or manually.
Auto	The IPC adjusts image clarity according to the actual conditions.
Off	Defog function is disabled.

Step 3 Click **Apply**.

6.2.1.9 Fisheye

When utilizing 360-degree fisheye cameras, select the installation mode and record mode according to the actual installation configuration. This allows for dewarping the fisheye image to different modes.



This function is only available on a fisheye 360-degree IP camera.

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	Select Ceiling , Wall , or Ground according to the actual location
Record Mode	<ul style="list-style-type: none"> • 1O: The original image before correction. • 1P: 360° rectangular panoramic image. • 2P: This mode is only selectable if the installation mode is Ceiling or Ground. 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 on all the screens. • 2R: Original image screen + two independent sub-screens. You can zoom or drag the image on all the screens. • 4R: Original image screen + four independent sub-screens. You can zoom or drag the image on all the screens. • 1O + 3R: Original image screen + three independent sub-screens. You can zoom or drag the image in the 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.

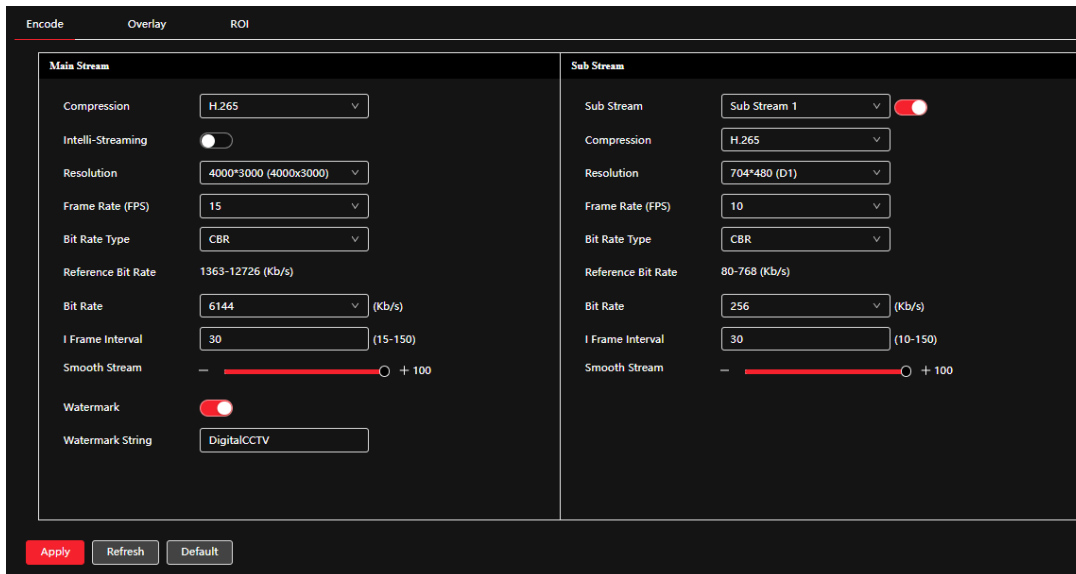


Click **Default**, and the device is restored to the default configuration. Click **Refresh** to view the latest configuration.

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**.



Step 2 Configure encode parameters.

Table 6-10 Description of encoding parameters

Parameter	Description
Sub Stream	Click  to enable sub stream, it is enabled by default.  You can enable multiple substreams simultaneously.
Compression	Select encode mode. <ul style="list-style-type: none"> • 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.  If smart codec is enabled, the device will stop disable the third video stream , ROI , and smart event features .
Output Mode	Options include: Single Stream or Flex Stream .
Resolution	The resolution of the video. The greater the value, the clearer the image will be, but at a greater required bandwidth.

Parameter	Description
Frame Rate (FPS)	The number of frames in one second of video. The greater the value, the clearer and smoother the video will be.
Bit Rate Type	<p>The bit rate control type during video data transmission. You can select bit rate type from:</p> <ul style="list-style-type: none"> ● 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 the monitoring scene changes. <p> The Bit Rate Type can be only be set as CBR when Encode Mode is set as MJPEG.</p>
Quality	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>The better the quality is, the bigger the required bandwidth will be.</p>
Reference Bit Rate	The most suitable bit rate value range recommended to users according to the defined resolution and frame rate.
Max Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as VBR.</p> <p>You can select the value of the Max Bit Rate according to the Reference Bit Rate value. The bit rate then changes as the monitoring scene changes, but the max bit rate keeps close to the defined value.</p>
Bit Rate	<p>This parameter can be configured only when the Bit Rate Type is set as CBR.</p> <p>Select the bit rate value in the list according to the actual condition.</p>
I Frame Interval	<p>The number of P frames between two I frames, and the I Frame Interval range changes as FPS changes.</p> <p>It is recommended to set I Frame Interval twice as large as FPS.</p>
SVC	<p>Scaled video coding: Encodes a high-quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of related lays according to the network status.</p> <ul style="list-style-type: none"> ● 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 if you need to protect the privacy within areas on the video image.

You can select the type of 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.


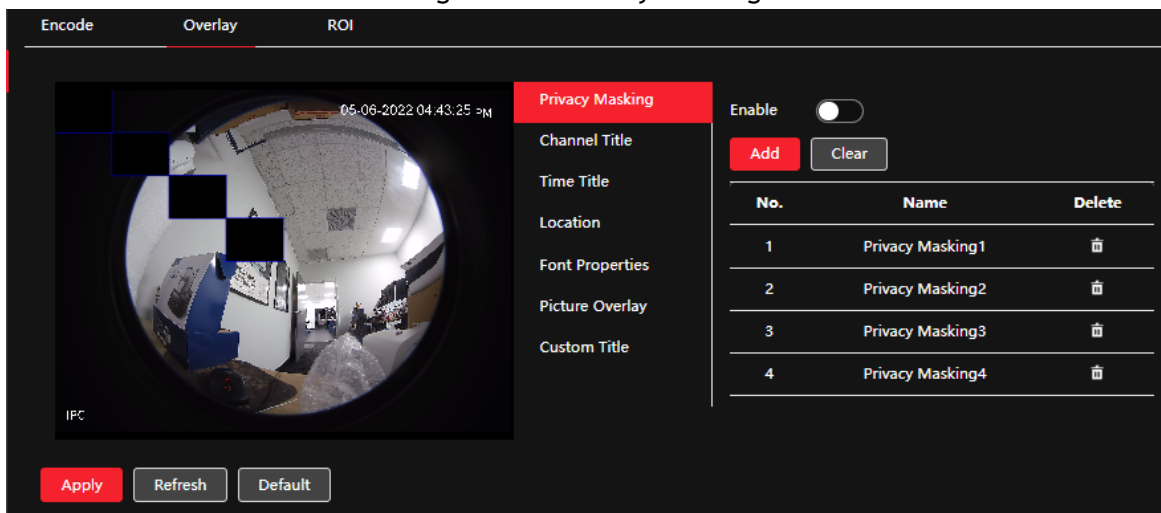

Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Privacy Masking**.


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 privacy.
- 4) Click **Apply**.

Related Operations

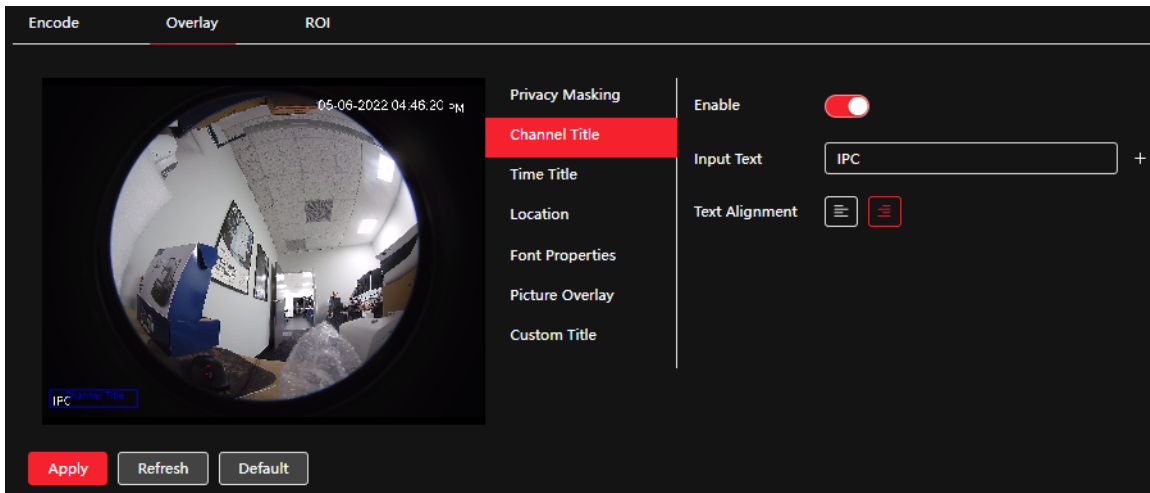
- View and edit the Privacy block
Select the privacy masking rule to be edited in the list, then the rule is highlighted, and the block frame will be displayed in the image. You can edit the selected block as necessary, including moving the position and adjusting the size.
- Edit the block name
Double-click 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 the 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 to add 1 line.

Step 3 Move the title box to the desired position 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.


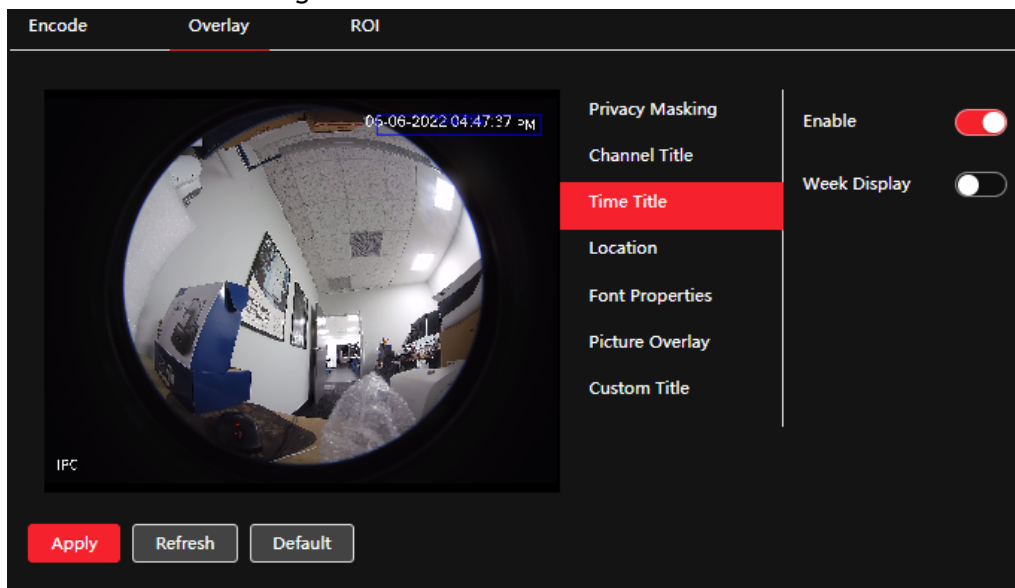
Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Time Title**.

Figure 6-16 Time title



Step 2 Click next to **Enable**.

Step 3 Click next to **Week Display** to display the day of the 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 the location text in the video image.



Text overlay and picture overlay cannot work simultaneously, and an IPC connecting to a mobile NVR with the private protocol will display GPS information as a priority.


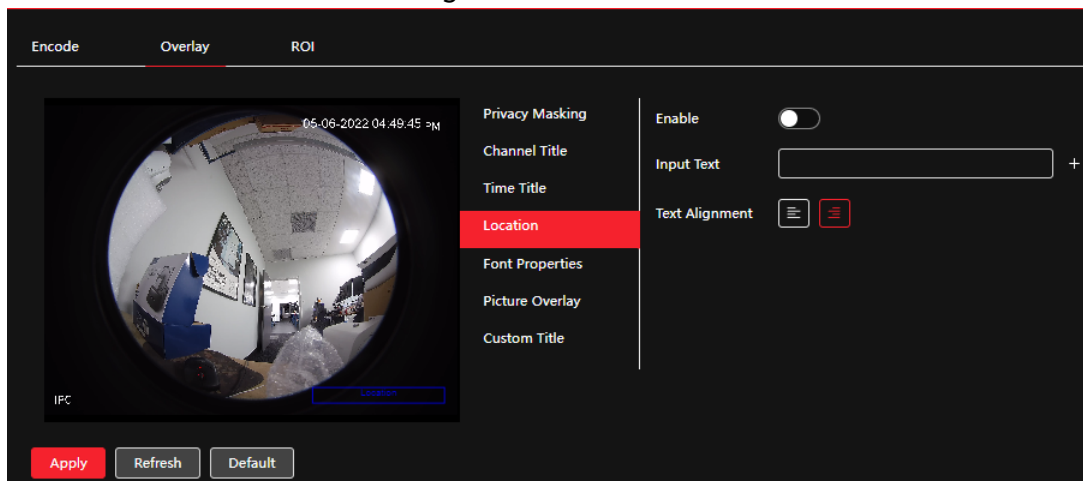
Step 1 Select  > **Camera** > **Encode** > **Overlay** > **Location**.

Figure 6-17 Location



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



Click to add the text overlay to add 13 lines at most.

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

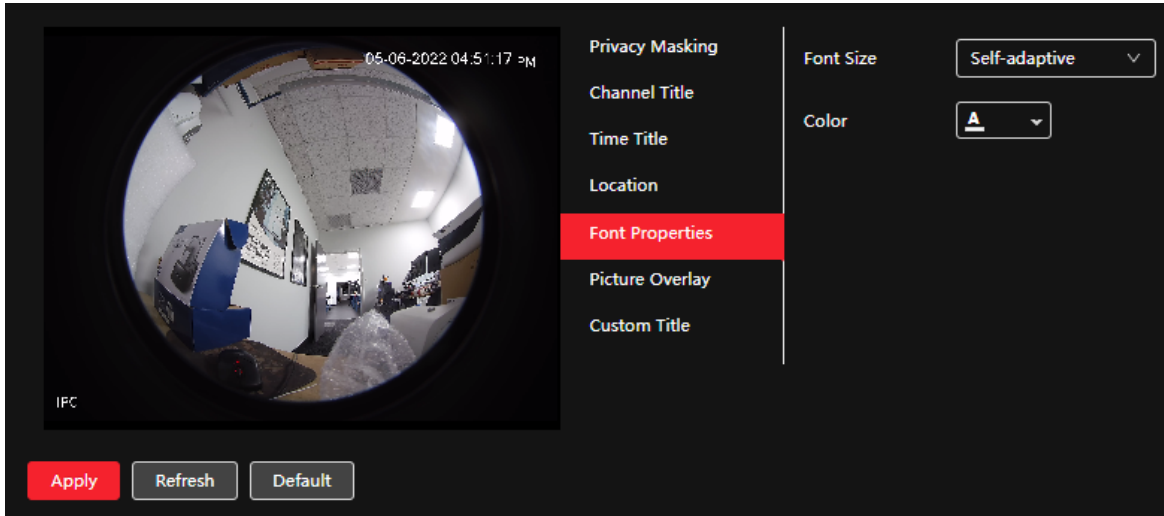
Step 4 Click **Apply**.

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

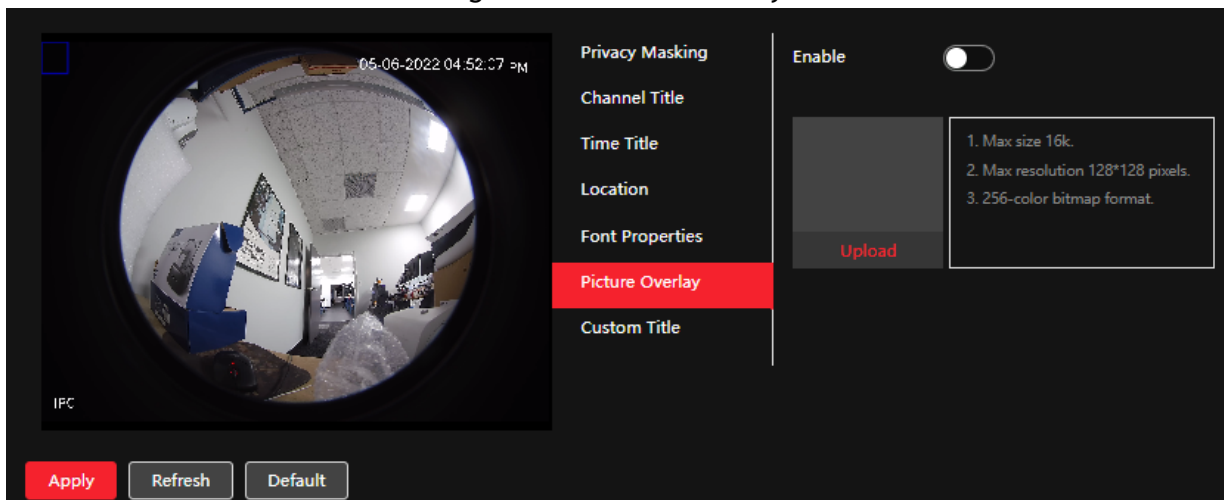
You can enable this function if you need to display picture information on the video image.



Text overlay and picture overlay cannot work simultaneously.

- 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 will be 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.


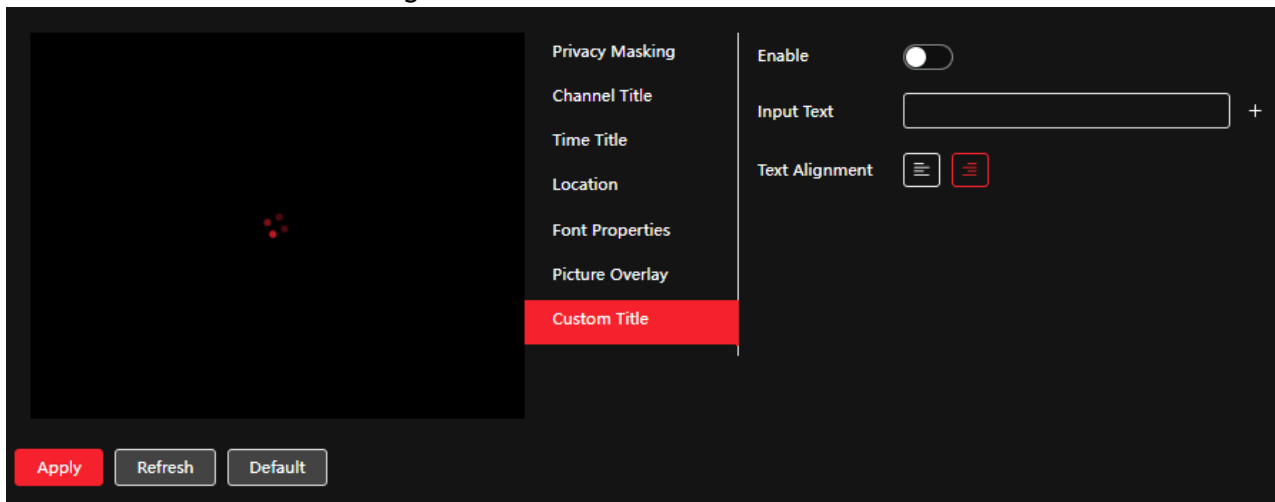
Step 1 Select  > Camera > Encode > Overlay > Custom Title

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 to add 1 line at most.

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

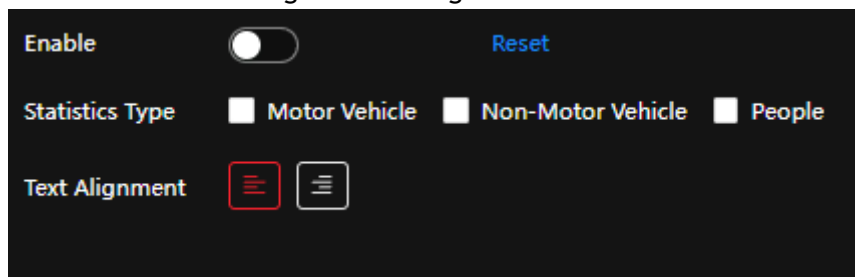
Step 4 Click **Apply**.

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**.

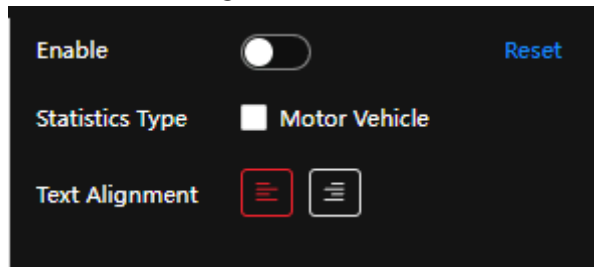
The overlaid information will be displayed after enabling the video metadata function.

6.2.2.2.9 Configuring ANPR

Automatic number-plate recognition. After enabling this function the IPC will detect motor vehicles and their license plates, ANPR statistics information will be displayed on the image. When the overlay function is enabled during intelligent rules configuration, this function is automatically enabled.

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 automatically enabled.


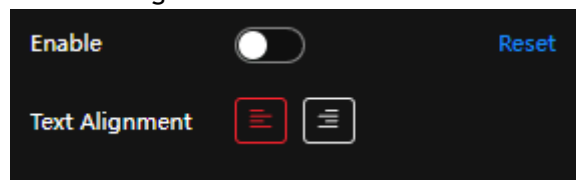
Step 1 Select  > Camera > Encode > Overlay > Face Detection.

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**.

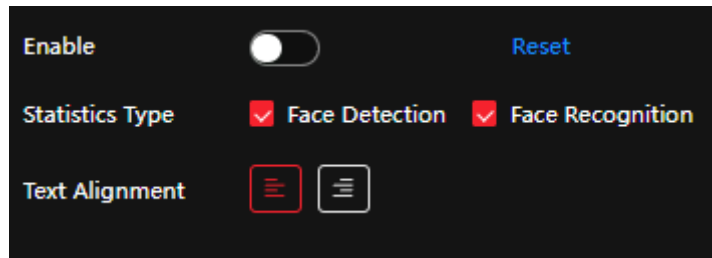
The information will be displayed on the image after the face detection function is enabled.

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 automatically enabled.

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**.

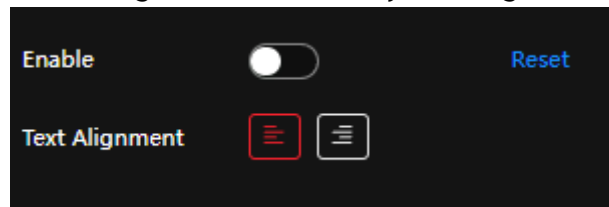
The information will be displayed on the image after the face recognition function is enabled.

6.2.2.2.12 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 automatically.

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**.

6.2.2.3 ROI

Select ROI (region of interest) on the image and configure the image quality of ROI, and then the selected image will be displayed at defined quality.


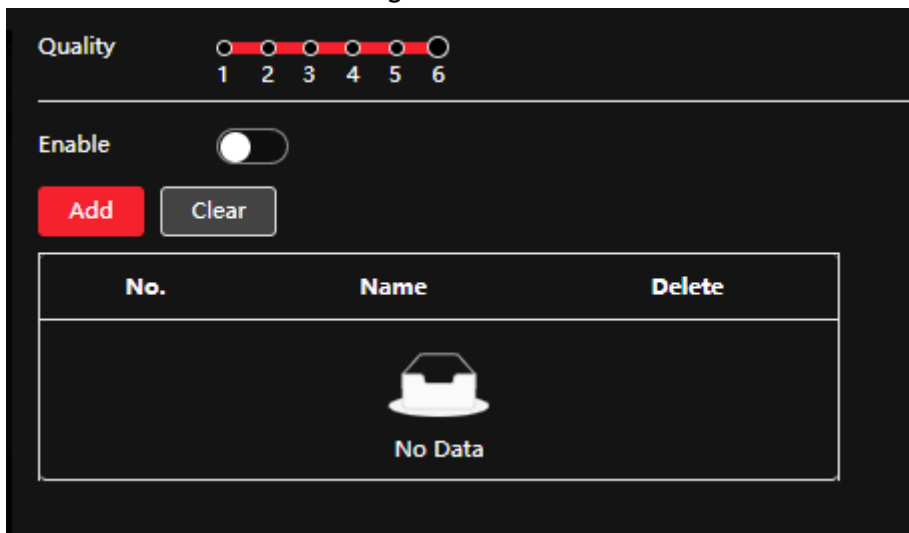
Step 1 Select  > **Camera** > **Encode** > **ROI**.

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, 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

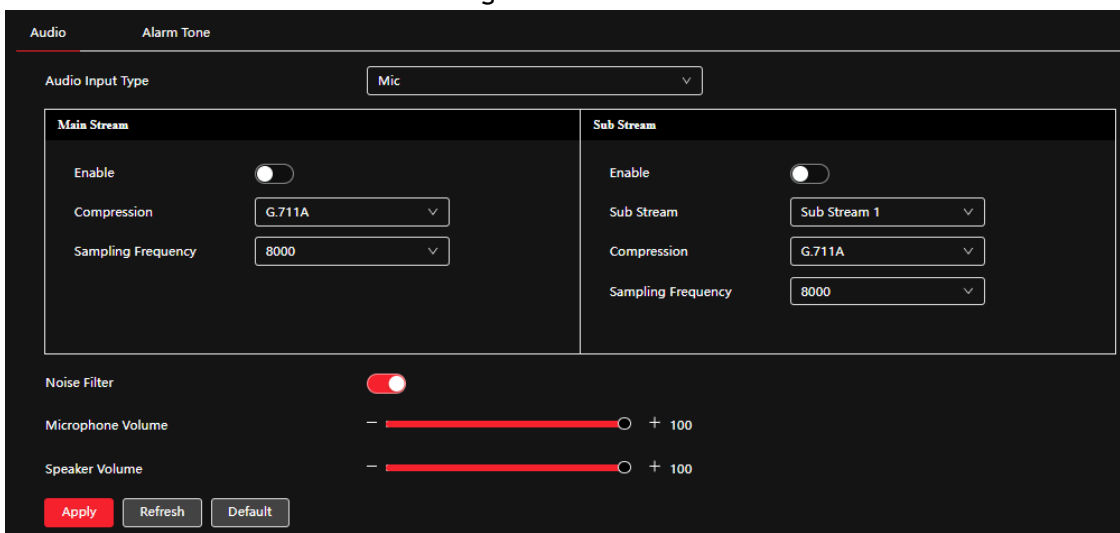
You can configure audio parameters and alarm audio.


6.2.3.1 Setting Audio Parameters

This section allows you to configure audio parameters and alarm audio.

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 be mindful of local laws and regulations when enabling and recording audio.

Step 3 Configure audio parameters.

Table 6-11 Description of audio parameters

Parameter	Description
Compression	Audio Encode Mode options can include 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, the more the samples in a second, and the more accurate the restored signal will be. You can select audio Sampling Frequencies from 8000, 16000, 32000, 48000, 64000 .
Audio Input Type	Select audio input type from: <ul style="list-style-type: none"> • LineIn: Requires an external audio device. • Mic: Uses the devices built-in microphone.
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

This section allows you to record or upload an alarm audio file. The audio file can be played when an event is triggered.


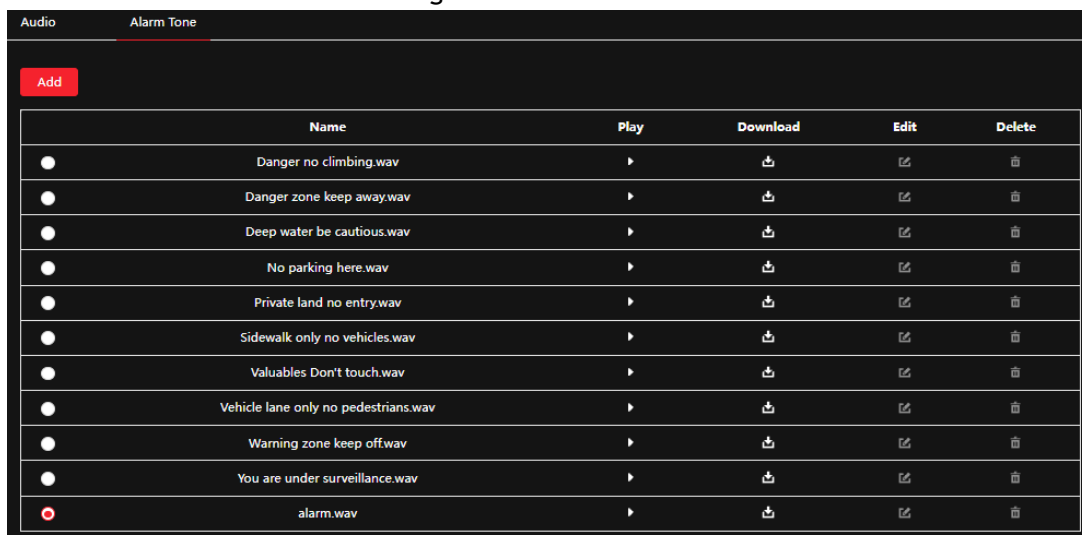












































Step 1 Select  > **Camera** > **Audio Tone**.

Figure 6-30 Audio tone



Name	Play	Download	Edit	Delete
Danger no climbing.wav				
Danger zone keep away.wav				
Deep water be cautious.wav				
No parking here.wav				
Private land no entry.wav				
Sidewalk only no vehicles.wav				
Valuables Don't touch.wav				
Vehicle lane only no pedestrians.wav				
Warning zone keep off.wav				
You are under surveillance.wav				
alarm.wav				

Step 2 Click **Add**.

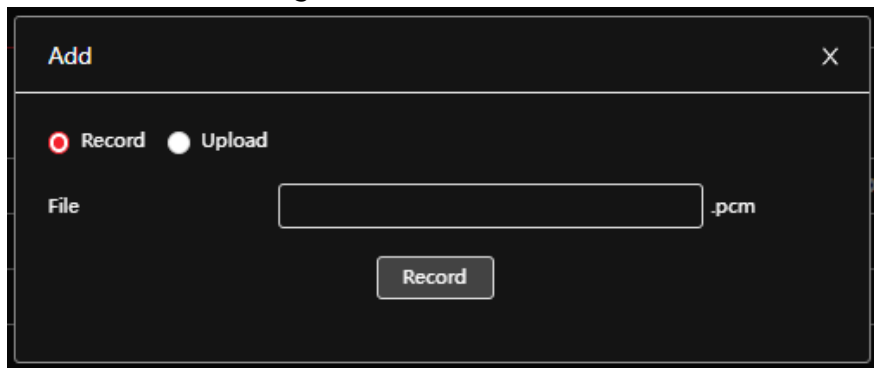
Step 3 Configure the audio file.

- 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 files in .pcm format only. Recordings are 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 desired file.

Related Operations

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

TCP/IP

Host Name

ARP/Ping

NIC ▾

Mode Static DHCP

MAC Address

IP Version ▾

IP Address

Subnet Mask

Default Gateway

Preferred DNS


Alternate DNS

Step 2 Configure TCP/IP parameters.

Table 6-12 Description of TCP/IP parameters

Parameter	Description
Host Name	Enter a hostname. The maximum length is 15 characters.

<p>ARP/Ping</p>	<p>Click <input type="checkbox"/> to enable ARP/Ping to set IP address service. Acquire the camera MAC address to change and configure the device IP address with ARP/ping command.</p> <p>This is enabled by default. During restart, you will have 2 minutes to configure the device's IP address by a ping packet with a 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 a ping packet.</p> <p>A demonstration of configuring IP address with ARP/Ping.</p> <ol style="list-style-type: none"> 1. Connect the camera that needs to be configured and the PC within the same local network, and then acquire a usable IP address. 2. Acquire the MAC address of the camera from the device label. 3. Open the command prompt on a PC and enter the following command. <div data-bbox="544 875 1217 1435" style="border: 1px solid black; padding: 5px;"> <p>Windows syntax↵</p> <pre>arp -s <IP Address> <MAC> ↵ ping -l 480 -t <IP Address> ↵</pre> <p>Windows example↵</p> <pre>arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -l 480 -t 192.168.0.125↵</pre> <p>UNIX/Linux/Mac syntax↵</p> <pre>arp -s <IP Address> <MAC> ↵ ping -s 480 <IP Address> ↵</pre> <p>UNIX/Linux/Mac example↵</p> <pre>arp -s 192.168.0.125 11-40-8c-18-10-11↵ ping -s 480 192.168.0.125↵</pre> </div> <ol style="list-style-type: none"> 4. Restart the camera. 5. Check the PC command line, if information such as Reply from 192.168.0.125... will be displayed, if the configuration succeeds, you can turn it off. 6. Enter <code>http://(IP address)</code> in the browser address bar to log in.
<p>NIC</p>	<p>Select the Ethernet card that needs to be configured. The default one is Wire.</p>
<p>Mode</p>	<p>The mode that the camera gets IP:</p> <ul style="list-style-type: none"> • Static Configure IP Address, Subnet Mask, and Default Gateway manually, and then click Save, the login interface with the configured IP address will be displayed. • DHCP: When there is a DHCP server in the network, select DHCP, and the camera acquires an IP address automatically.

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

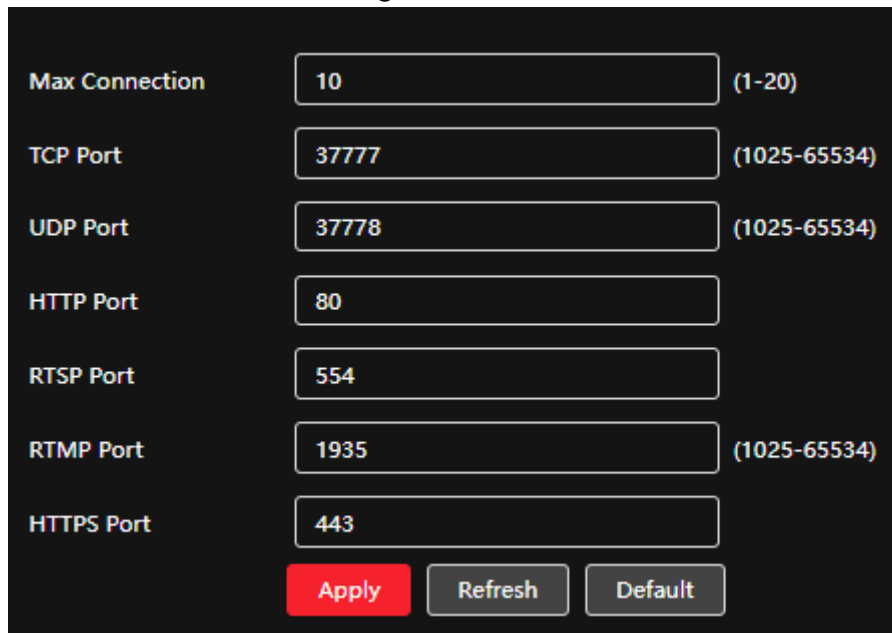
Step 3 Click **Apply**.

6.3.2 Port

This section allows the configuration of the port numbers and the maximum number of users (including web, platform client, and mobile phone clients) that can connect to the device simultaneously.

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

Figure 6-33 Port



Max Connection	<input type="text" value="10"/>	(1-20)
TCP Port	<input type="text" value="3777"/>	(1025-65534)
UDP Port	<input type="text" value="3778"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025-65534)
HTTPS Port	<input type="text" value="443"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Step 2 Configure port parameters.



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

Table 6-13 Description of port parameters

Parameter	Description
Max Connection	The maximum number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. The value is 10 by default.
TCP Port	Transmission control protocol port. The value is 37777 by default.
UDP Port	User datagram protocol port. The value is 37778 by default.
HTTP Port	Hyper text transfer protocol port. The value is 80 by default.
RTSP Port	<ul style="list-style-type: none"> Real time streaming protocol port, and the value is 554 by default. When the URL format requires RTSP, you will need to specify the channel number and bit stream type in the URL, as well as the username and password if needed. To turn off the audio when playing live view with RTSP, set the codec mode to H.264B and resolution to CIF. <p>URL format example: <code>rtsp://username:password@ip:port/cam/realmonitor?channel=1&sub type=0</code></p> <p>Among that:</p> <ul style="list-style-type: none"> 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, 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). <p>Example: If you require the sub stream of channel 2 from a certain device, then the URL should be: <code>rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=2&sub type=1</code></p> <p>If username and password are not needed, then the URL can be: <code>rtsp://ip:port/cam/realmonitor?channel=1&sub type=0</code></p>
RTMP Port	Real Time Messaging Protocol. The port that RTMP provides service. It is 1935 by default.
HTTPS Port	HTTPS communication port. It is 443 by default.

Step 3 Click **Apply**.



The configuration of **Max Connection** takes effect immediately, and others will take effect after rebooting the camera.

6.3.3 PPPoE

Point-to-Point Protocol over Ethernet, a type of remote access protocol that the camera uses to connect to the internet by acquiring a WAN dynamic IP address. You will need to acquire the PPPoE username and password from the internet service provider, and then set up a network connection through PPPoE.

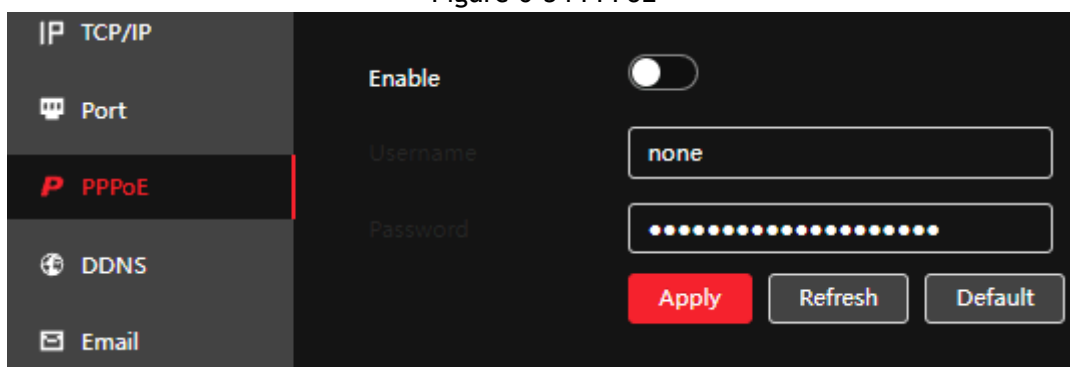
Prerequisites


- The camera has connected to the network.
- You have acquired 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 the web interface

Step 3 Click **Apply**.

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

6.3.4 DDNS

DDNS, most commonly known as Dynamic DNS, can dynamically update DNS records without the need for human interaction. It will automatically update the domain to the external IP when it changes. Some IC Realtime cameras come equipped with ICDDNS and feature custom domain name registration. Remote access via ICDDNS requires port forwarding of the TCP port (and HTTP for web browser access).

Prerequisites

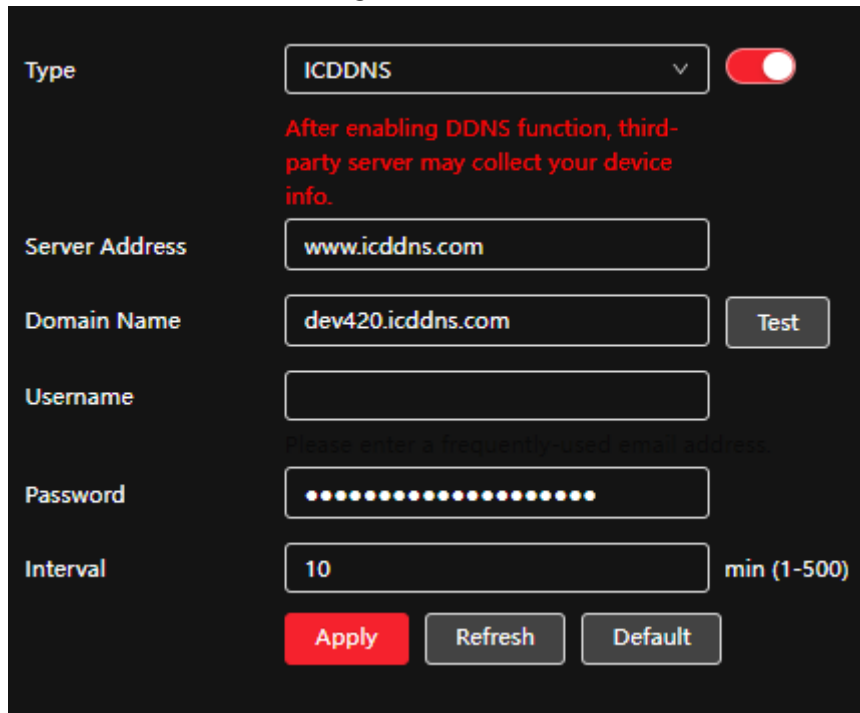
Check the type of DNS server supported by the camera.

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



- Third party services may collect your device information after DDNS is enabled.
- Register and log in to the DDNS website to 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: <ul style="list-style-type: none"> ICDDNS web address: www.icddns.com 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 or a custom domain you create if using ICDDNS.
Test	Only when selecting ICDDNS type, and custom domain 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 (including username and password) on the DDNS server provider's website. This is optional if using ICDDNS.
Password	
Interval	The update cycle of the connection between the device and the server, and the time is 10 minutes by default.

Result

Step 4 Click **Apply**.

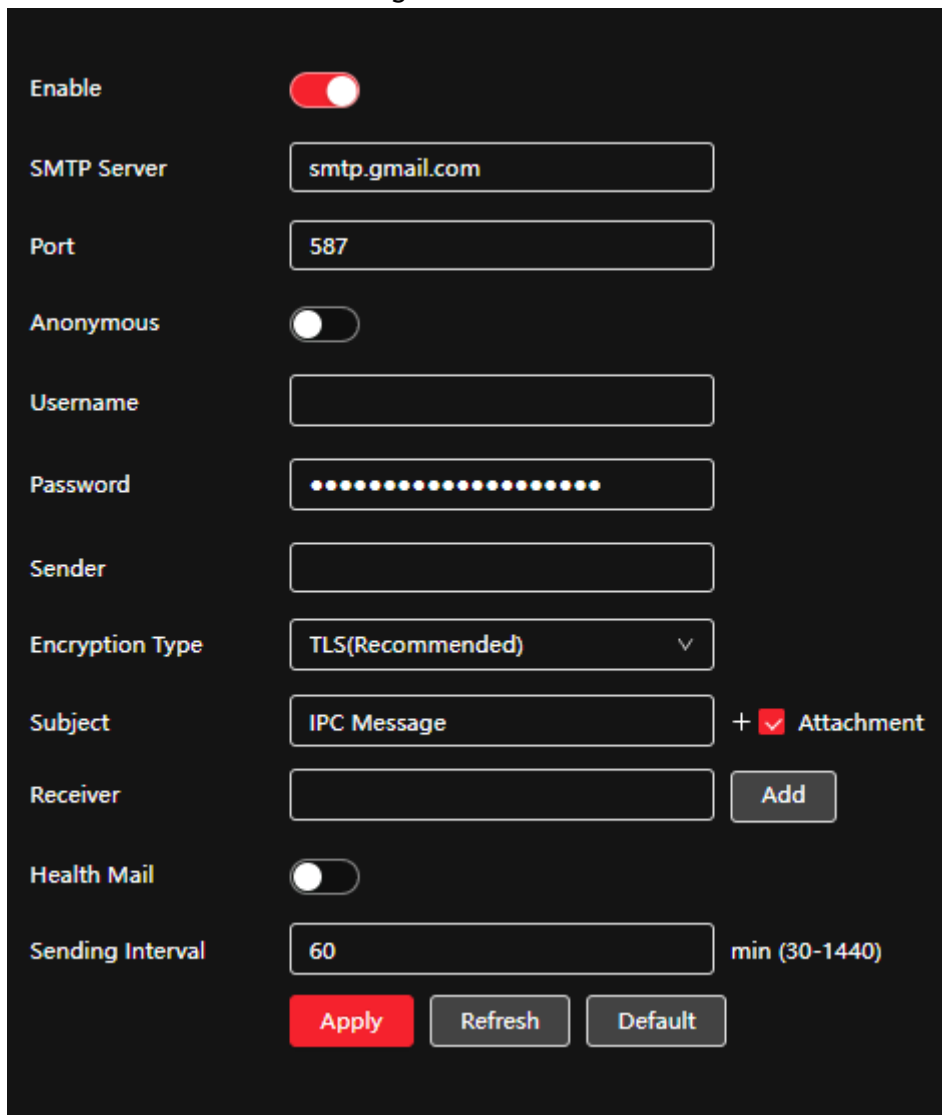
Open the browser on a PC (that is offsite from the IPC), then enter the domain name at the address bar and press **Enter**, the login interface will be displayed.

6.3.5 Email

This section allows for configuring email parameters and enabling email linkage. The IPC can send an email to the defined address when the corresponding alarm is triggered.

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

Figure 6-36 Email




The screenshot shows the following configuration details:



- Enable:**
- SMTP Server:** smtp.gmail.com
- Port:** 587
- Anonymous:**
- Username:** [Empty field]
- Password:** [Masked field with 12 dots]
- Sender:** [Empty field]
- Encryption Type:** TLS(Recommended) [Dropdown arrow]
- Subject:** IPC Message + Attachment
- Receiver:** [Empty field] + Add button
- Health Mail:**
- Sending Interval:** 60 min (30-1440)
- Buttons:** Apply (red), Refresh, Default

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

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	<ul style="list-style-type: none"> The authentication type cannot be None. The SMTP service in your mailbox must be enabled.
		TLS	587	
Yahoo	smtp.mail.yahoo.com	TLS	587	 You may need to create an app password in your Google/ Yahoo account to use as the password.
		SSL	465	

Step 4 Click **Apply**.

6.3.6 UPnP

UPnP (Universal Plug and Play), is a protocol that establishes mapping relation between the local area and wide area network. This function enables you to remotely access your camera by automatically port forwarding with your router.

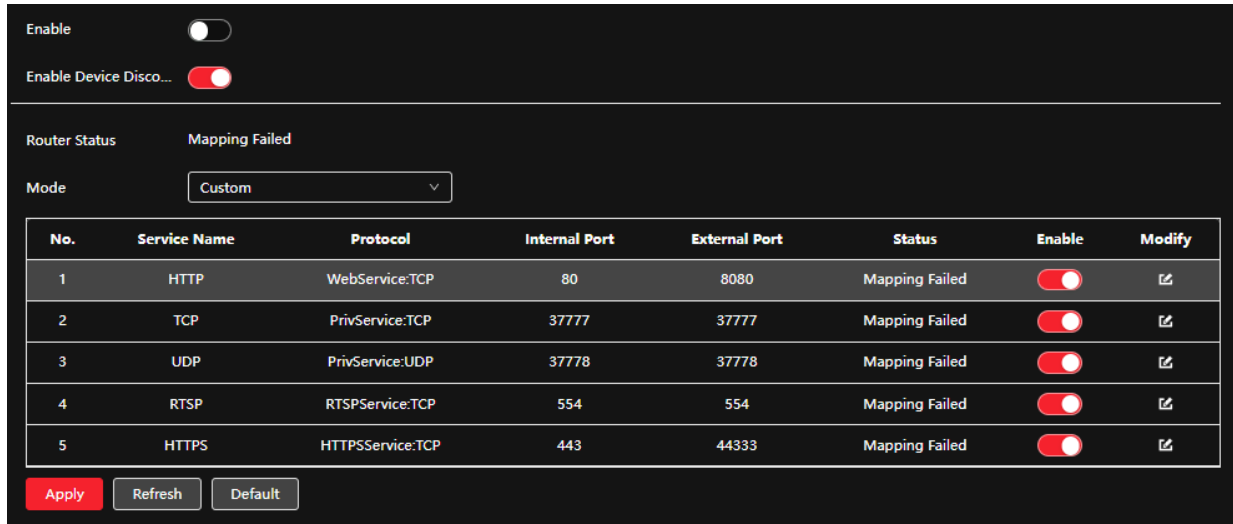
Prerequisites

- Make sure the UPnP service and enabled is installed in the local Router.
- Log in the router, and configure WAN IP address to set up an internet connection.
- 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 the external port as necessary.
- Select **Default**, and then the system will finish mapping with an unoccupied port automatically, and you will not be able to edit the mapping relation.

Step 3 Click **Apply**.

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

6.3.7 SNMP

SNMP (Simple Network Management Protocol) 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)

Version V1 V2 V3(Recommended)

SNMP Port (1-65535)

Read Community

Write Community

Trap Address

Trap Port

Figure 6-39 SNMP (2)

Version V3(Recommended)

SNMP Port (1-65535)

Read Community

Write Community

Trap Address

Trap Port

Read-Only Username

Authentication Type MD5 SHA

Authentication Pass...

Encryption Type CBC-DES CFB-AES

Encryption Password

Read/Write Username

Authentication Type MD5 SHA

Authentication Pass...

Encryption Type CBC-DES CFB-AES

Encryption Password

Step 2 Select the SNMP version to enable SNMP.

- Select **V1** to only process information of V1 version.
- Select **V2** to only process information of V2 version.
- Select **V3**, (**V1** and **V2** will become unavailable.) You can configure the user name,




password and authentication type from your server.



Using V1 and V2 is less secure. V3 is recommended.

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

Table 6-17 Description of SNMP parameters


Parameter	Description
SNMP Port	The listening port of the software agent in the device.
Read Community, Write Community	The read and write community string that the software agent supports.  You can enter number, letter, underline and dash to form the name.
Trap Address	The target address of the Trap information sent by the software agent in the device.
Trap Port	The target port of the Trap information sent by the software agent in the device.
Read-only Username	Set the read-only username accessing the device, it is public by default.  You can enter a number, letter, and underline to form the name.
Read/Write Username	Set the read/to write username access device, it is private by default.  You can enter a number, letter, and underline to form the name.
Authentication Type	Options include 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.

Result

Step 4 Click **Apply**.


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 the version to search.
5. Expand all the tree lists displayed in the MG-SOFT MIB Browser to view the configuration information, video channel amount, audio channel amount, and software version.

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

6.3.8 Bonjour

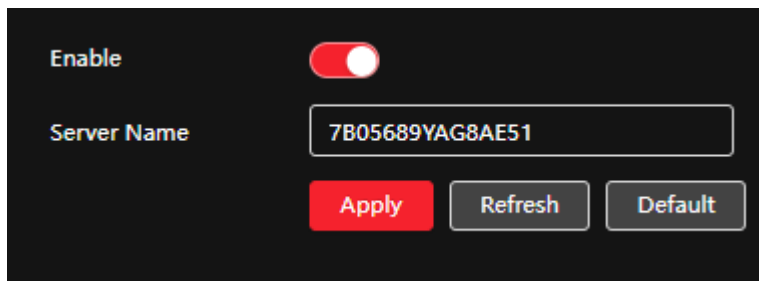
Bonjour allows for zero-configuration networking between different types of devices. You can use it to find other Apple services on a network, connect to other devices like network printers (that provide Bonjour support), or access shared drives.

 Bonjour is enabled by default.


Procedure

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

Figure 6-40 Bonjour



Result

Step 2 Click , and then configure the server name.

Step 3 Click **Apply**.

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

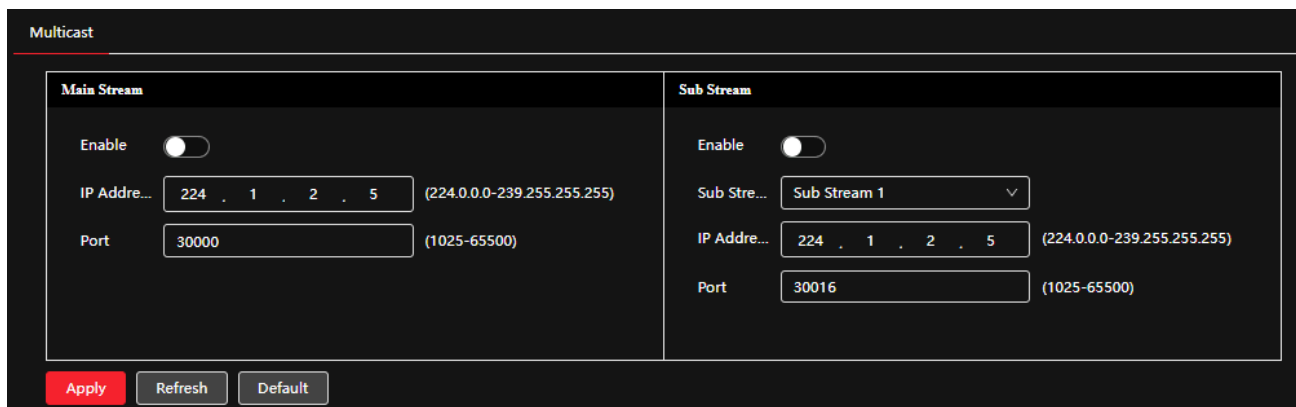
1. Click **Show All Bookmarks** in Safari.
2. Enable **Bonjour**. The OS or client automatically detects the network cameras with Bonjour enabled in the LAN.
3. Click the camera to visit the corresponding web interface.

6.3.9 Multicast

Multicast is where data transmission is simultaneously addressed to a group of destination computers. When multiple users are streaming the IPC video image simultaneously through the network, it may 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 adopting 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 the corresponding stream: Main Stream : 40000; Sub Stream1 : 40016; Sub Stream2 : 40032, and all the range is 1025-65500.

Result

Step 3 Click **Apply**.

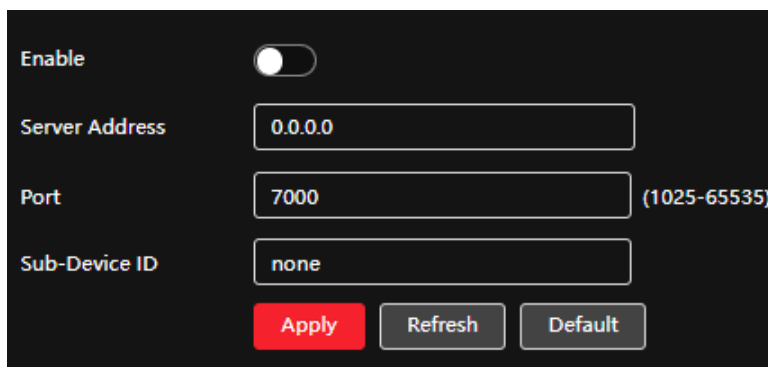
On the **Live** interface, select **RTSP** in **Multicast** to view the video image with multicast protocol.

6.3.10 Register

This function can only be enabled if the camera is connected to the Internet. This function allows the IPC to 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 the 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.

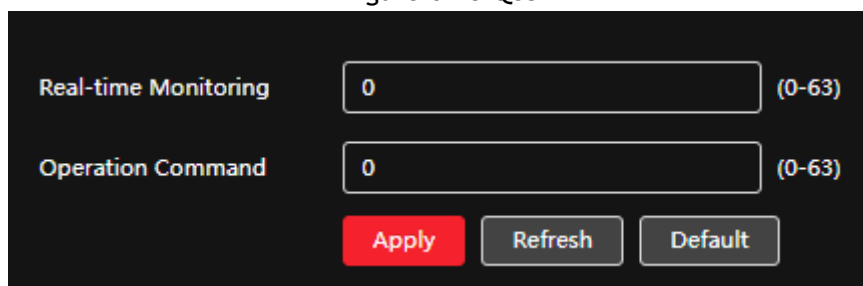
Step 3 Click **Apply**.

6.3.11 QoS

QoS is Quality of Service that can solve problems such as network delay and congestion with this function. It helps to assure bandwidth, and reduce transmission delay, packet loss rate, and delay jitter. 0-63 means 64 degrees of priority; 0 for the lowest and 63 for 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 are used for network surveillance. 0 for the lowest and 63 for the highest.
Command	Configure the priority of the data packets that are used for configuring or checking.

Step 3 Click **Save**.

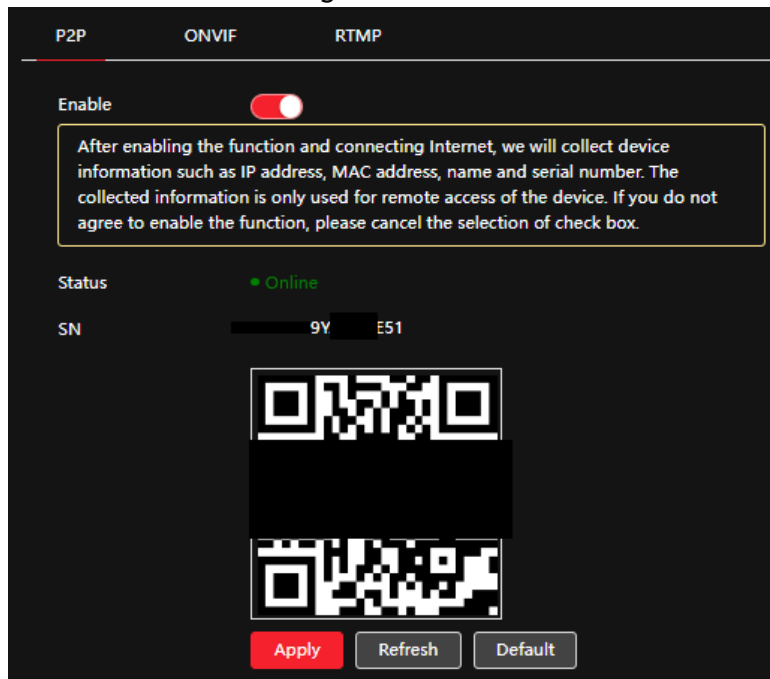
6.3.12 Platform Access

6.3.12.1 P2P

P2P is a private network traversal technology that enables users to manage devices easily without requiring DDNS, port forwarding/ mapping, or a transit server. You can scan the QR code with your smart phone, to view the camera or manage on desktop software client (Smart ICRSS).

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

Figure 6-44 P2P



- If P2P is enabled and the status is Online, remote management on the device is supported.
- When P2P is enabled and the status is Offline, make sure the IPC is connected to a network and set it on DHCP.

Step 2 Log in to the 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

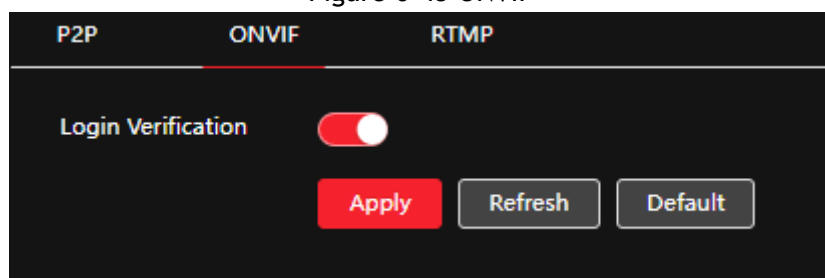
The ONVIF verification is enabled by default, which allows the network video products (including video recording devices and other recording devices) from other manufacturers to connect to your device.



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

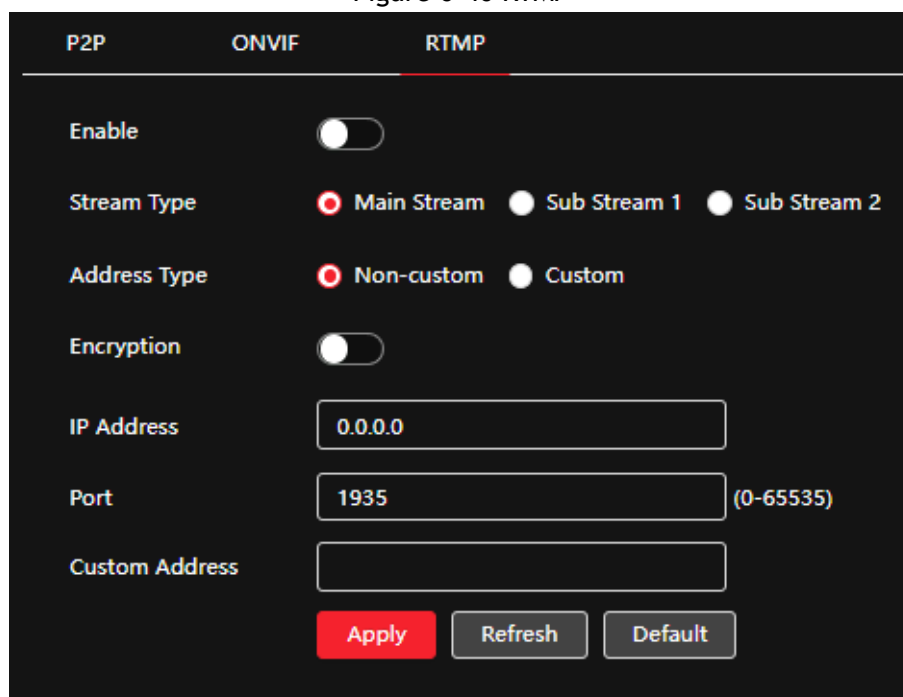
Using RTMP, you can access third-party platforms (such as Ali and YouTube) to stream video live view.



- RTMP can be configured by the admin account 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	<ul style="list-style-type: none"> • 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 the server IP address and port. <ul style="list-style-type: none"> • IP address: Support IPv4 or domain name. • Port: Keep the default value.
Port	
Custom Address	When selecting Custom , you need to enter the path allocated by the server.

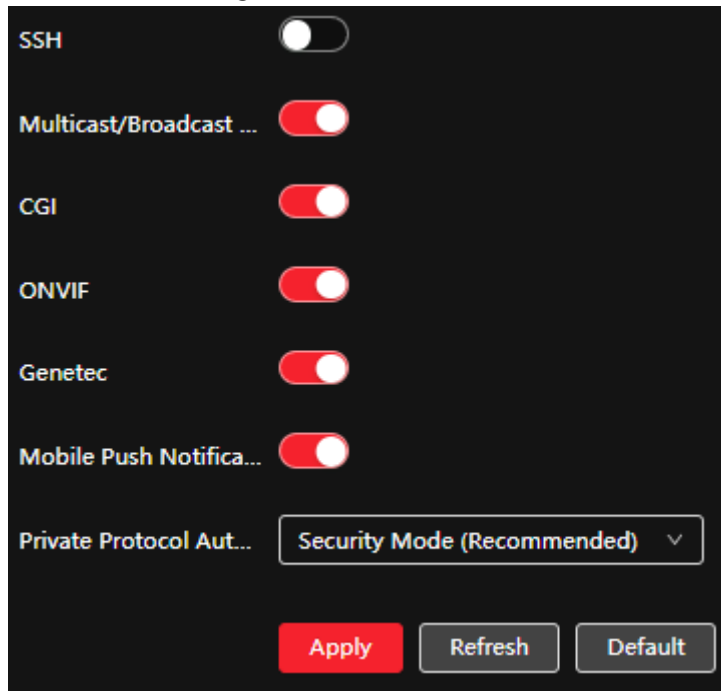
Step 4 Click **Apply**.

6.3.13 Basic Service

This section allows you to toggle different network services and protocols and allows for enhanced 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	Enable SSH authentication to perform safety management.
Multicast/Broadcast Search	Multicast is where data transmission is addressed to a group of destination computers simultaneously. When multiple users are having issues streaming the IPC video image simultaneously through the network, you can solve this problem by setting up a multicast IP.
CGI	Enables the appropriate services.
Onvif	
Genetec	
Mobile Push Notification	Allows snapshots to be sent to the mobile app if an Event is triggered.
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

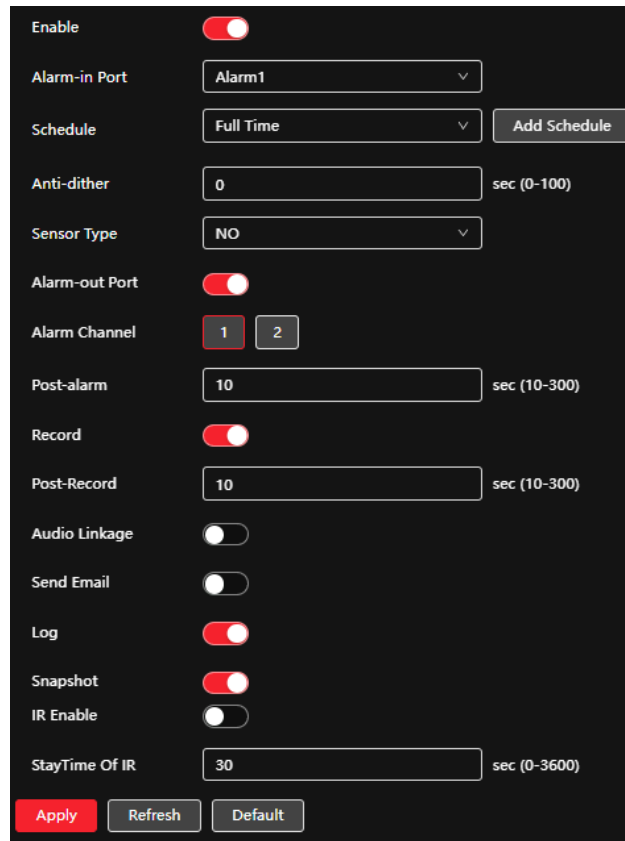
6.4.1.1 Setting Alarm-in

If the device connected to the alarm-in port is triggered, the camera can perform defined alarm linkages.

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

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

Figure 6-48 Alarm linkage



The screenshot shows a configuration panel for alarm linkage. It includes the following settings:

- Enable:** A red toggle switch is turned on.
- Alarm-in Port:** A dropdown menu is set to "Alarm1".
- Schedule:** A dropdown menu is set to "Full Time", with an "Add Schedule" button to its right.
- Anti-dither:** A text input field contains "0", with "sec (0-100)" to its right.
- Sensor Type:** A dropdown menu is set to "NO".
- Alarm-out Port:** A red toggle switch is turned on.
- Alarm Channel:** Two buttons labeled "1" and "2" are present, with "1" selected.
- Post-alarm:** A text input field contains "10", with "sec (10-300)" to its right.
- Record:** A red toggle switch is turned on.
- Post-Record:** A text input field contains "10", with "sec (10-300)" to its right.
- Audio Linkage:** A white toggle switch is turned off.
- Send Email:** A white toggle switch is turned off.
- Log:** A red toggle switch is turned on.
- Snapshot:** A red toggle switch is turned on.
- IR Enable:** A white toggle switch is turned off.
- StayTime Of IR:** A text input field contains "30", with "sec (0-3600)" to its right.

At the bottom of the panel are three buttons: "Apply" (red), "Refresh", and "Default".

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

- Sensor Type: NO or NC. NO for normally open, NC for normally closed.
- Anti-Dither: The IPC only records one alarm event during the anti-dither period.

Step 4 Select the schedule and arming periods and alarm linkage action. If the existing 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".

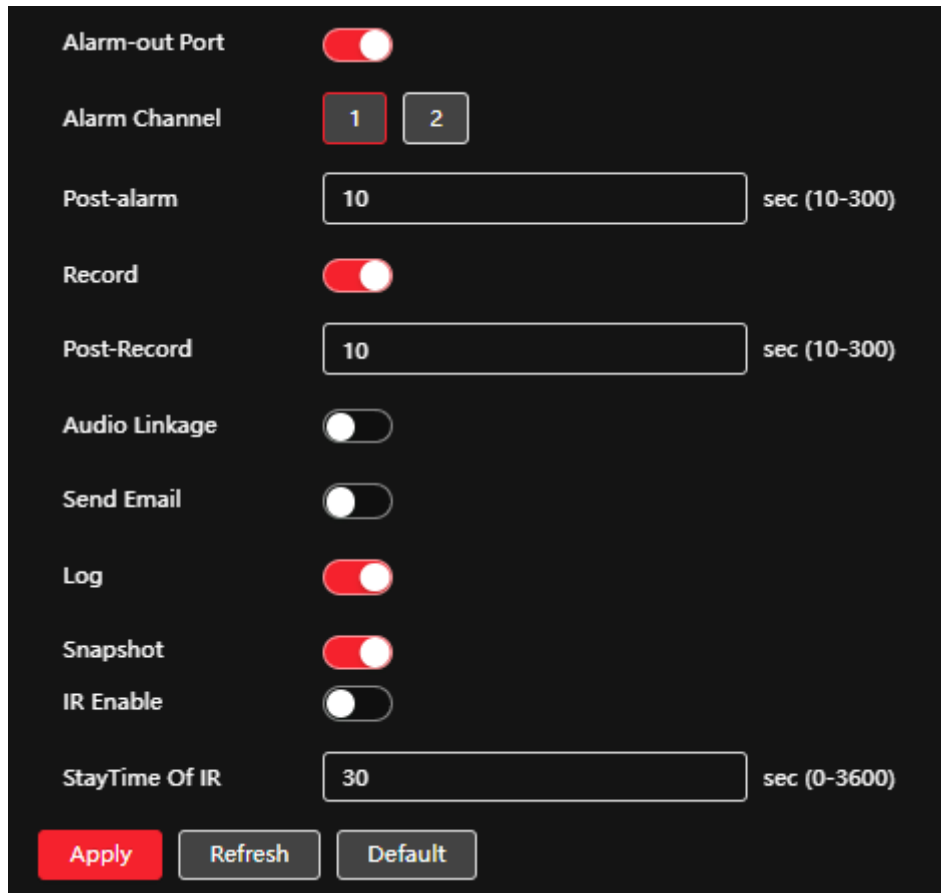
Step 5 Click **Apply**.

6.4.1.2 Alarm Linkage

When configuring alarm events (such as motion detection or IVS), you can select alarm linkages (such as record, and snapshot). When the corresponding alarm is triggered in the configured arming period, the system will trigger.

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

Figure 6-49 Alarm linkage

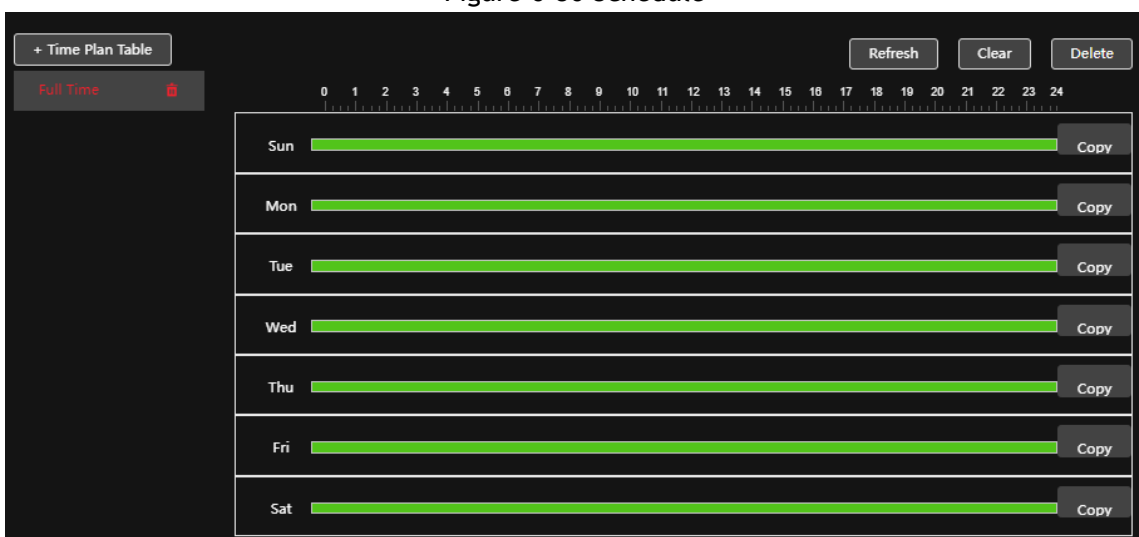


6.4.1.2.1 Adding Schedule

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 table as necessary.


6.4.1.2.2 Record Linkage

The system can record specific channels when an alarm event occurs. After the alarm, the system will stop recording after an extended period according to the **Post-Record** setting.

Prerequisites

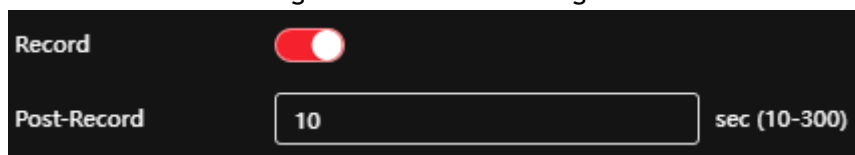
- After the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) is enabled the record channel links recording. For details, see "10.3 Setting Record Plan".
- Enable auto-record mode, the record linkage will take effect. For details, see "10.2 Setting Record Control".

Setting Record Linkage

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

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

Figure 6-51 Record linkage



6.4.1.2.3 Snapshot Linkage

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

Prerequisites

After the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) is enabled, the snapshot channel links capturing pictures. 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 necessary.

Figure 6-52 Snapshot linkage



6.4.1.2.4 Alarm-out Linkage

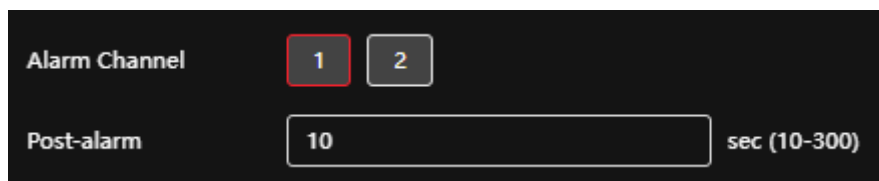
When an alarm is triggered, the system can automatically trigger a device connected to the alarm-out.

On the **Alarm** interface, click  to enable alarm-out linkage, select the channel as necessary, and then

configure **Post alarm**.

When alarm delay is configured, the 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 event is triggered, the system can 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	Prerequisites
Motion Detection	The event is triggered when a moving object is detected.	Motion detection is enabled. For details, see "6.4.3.1 Setting Motion Detection".
Disk Full	The event is triggered when the free space of the 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 event is triggered when there is a 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 event 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 event is triggered when there is external alarm input.	The device has an alarm input port and an external alarm function is enabled. For details, see "6.4.1.1 Setting Alarm-in".
Audio Detection	The event is triggered when there is an audio connection problem.	Abnormal audio detection is enabled. For details, see "6.4.4 Setting Audio Detection".
IVS	The event is triggered when the intelligent rule is triggered.	Enable IVS, crowd map, face detection or people counting, and other intelligent functions.

Scene Changing	The event is triggered when the device monitoring the scene changes.	Scene changing detection is enabled. For details, see "6.4.3.3 Setting Scene Changing".
Voltage Detection	The event 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 event is triggered when the device detects a malicious attack.	Voltage detection is enabled. For details, see "9.1 Security Status".

6.4.1.3.2 Subscribing Alarm Information

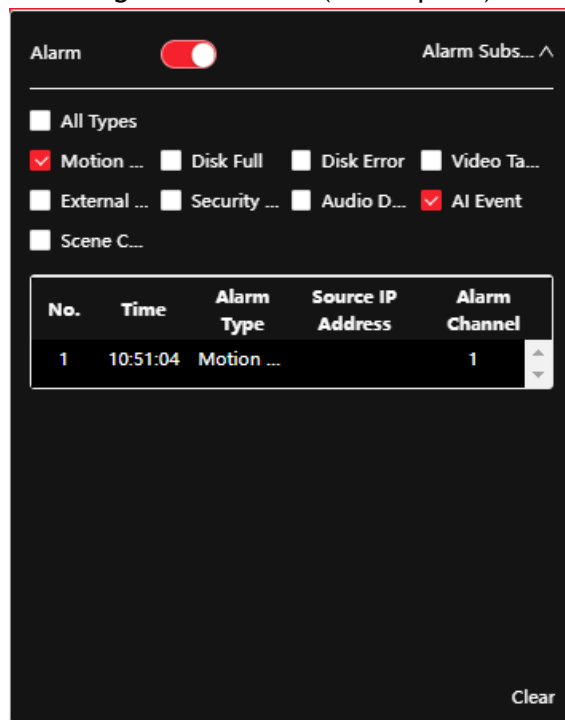
You can subscribe to alarm events so that when a subscribed alarm event is triggered, the system will record detailed alarm information on the right side of the web interface.



The functions of different devices may 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

will be 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.



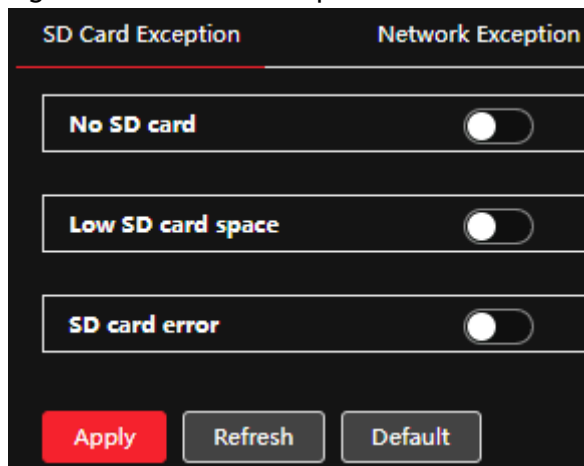
Only the device with SD card has the abnormality functions, including **No SD Card**, **SD Card Error**, and **Capacity Warning**.


6.4.2.1 Setting SD Card Exception

If there are issues with the SD card, the system performs event linkage. The event types include **No SD Card**, **Low SD Card Space**, and **SD Card Error**. Functions may 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 the 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".

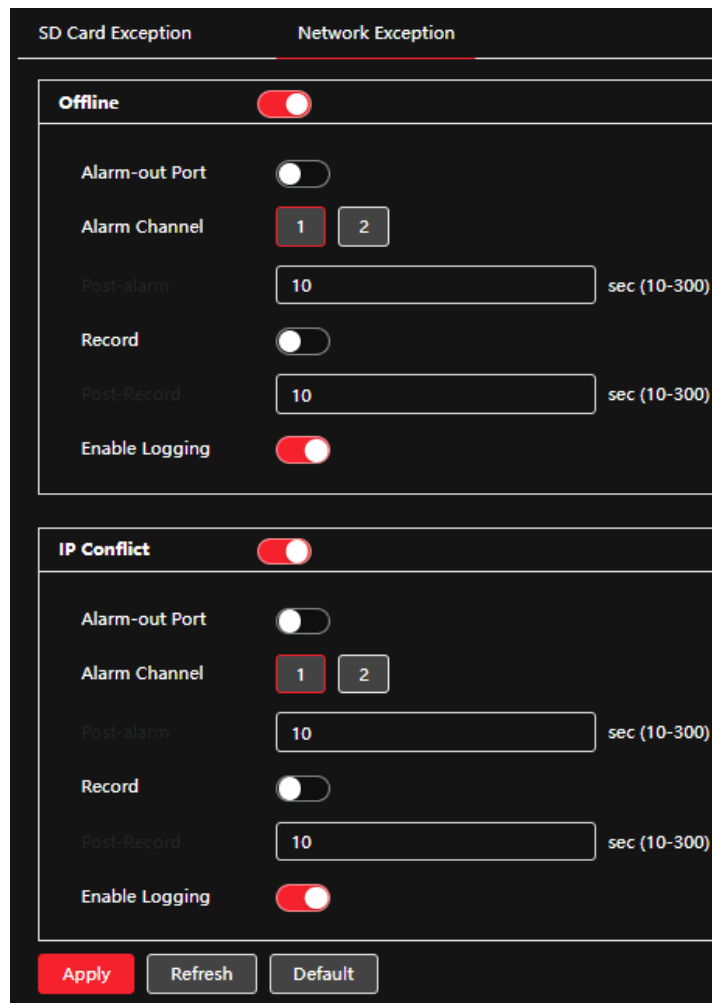
Step 4 Click **Apply**.

6.4.2.2 Setting Network Exception

When the camera detects 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

If the input voltage is higher than or lower than the rated value of the device, the IPC performs an event linkage.


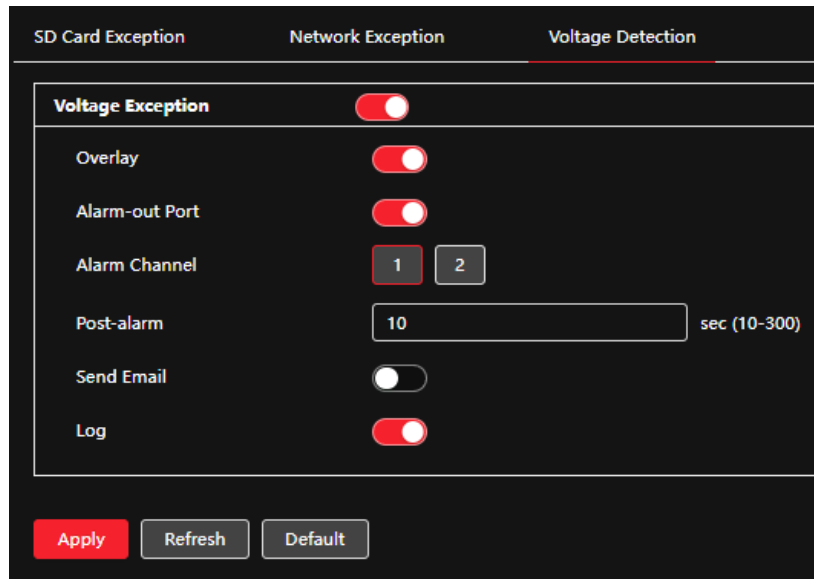
Step 1 Select  > **Event** > **Exception** > **Voltage Detection**.

Figure 6-58 Voltage detection



Step 2 Click to enable the voltage detection function.

When enabling **Overlay**, the alarm icon will be 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

The camera will trigger an event if there are considerable pixelation changes on the video such as moving objects or if the camera has been tampered with and moved from its original position.

6.4.3.1 Setting Motion Detection

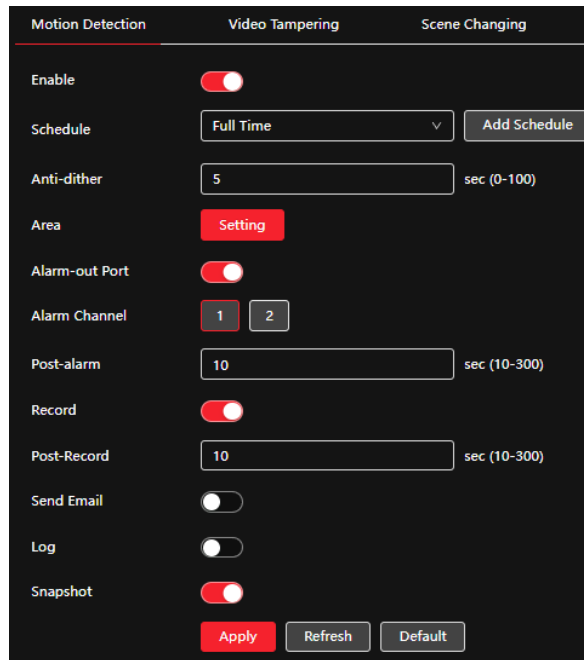
The camera will trigger an event if there is a pixelation change due to movement.



- 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

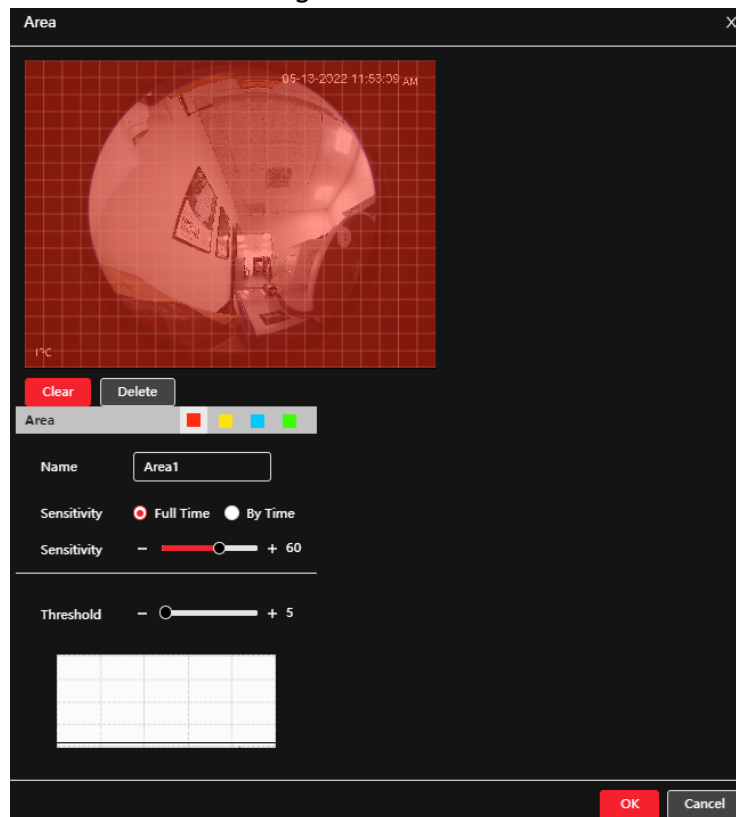


Step 2 Click to enable the motion detection function.


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. Motion events will trigger more frequently 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 IPC will trigger an event if the lens is covered or the video output is mono-color screen caused by lighting or other environmental factors.

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 event will be triggered.
- **Defocus Detection**: When the image is blurred, an event will be triggered. This function is available on some select models.

Figure 6-61 Video tampering

Motion Detection	Video Tampering	Scene Changing
Enable	<input type="checkbox"/>	
Schedule	Full Time <input type="button" value="v"/>	<input type="button" value="Add Schedule"/>
Alarm-out Port	<input checked="" type="checkbox"/>	
Alarm Channel	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	
Post-alarm	<input type="text" value="10"/> sec (10-300)	
Record	<input checked="" type="checkbox"/>	
Post-Record	<input type="text" value="10"/> sec (10-300)	
Send Email	<input type="checkbox"/>	
Log	<input checked="" type="checkbox"/>	
Snapshot	<input checked="" type="checkbox"/>	
	<input type="button" value="Apply"/>	<input type="button" value="Refresh"/> <input type="button" value="Default"/>

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 event 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".

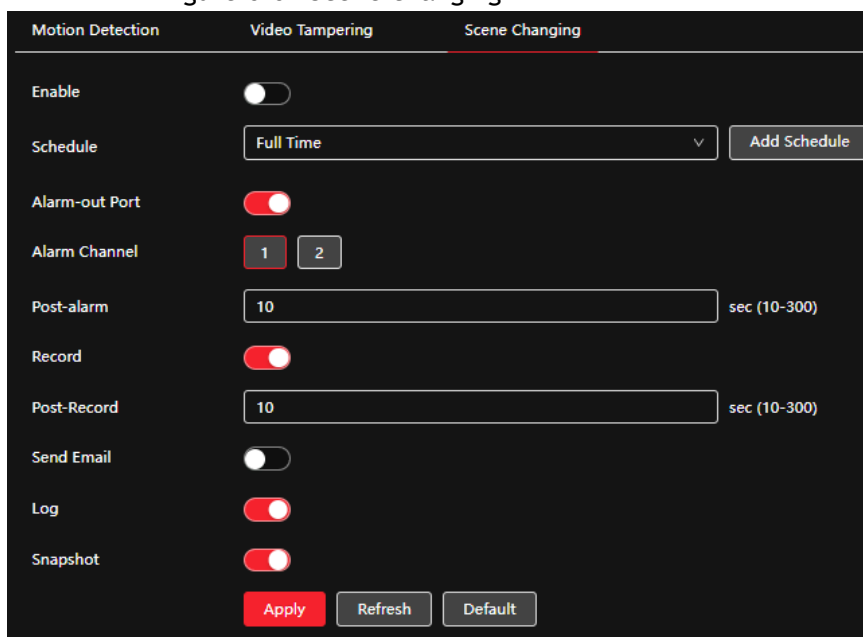
Step 4 Click **Apply**.

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".

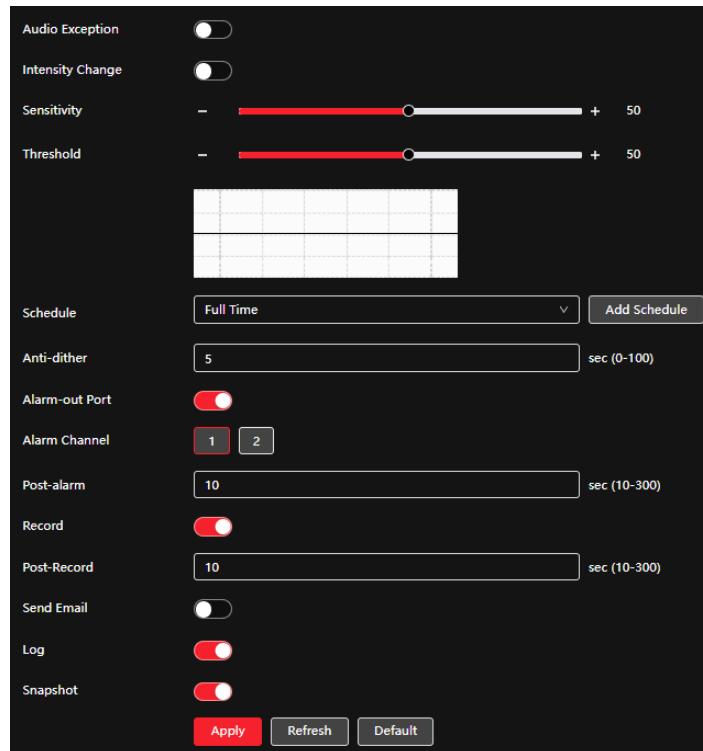
Step 3 Click **Apply**.

6.4.4 Setting Audio Detection

The IP Camera performs event linkage if a strange 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.
 - ◇ The event can be triggered more frequently with higher sensitivity or a smaller threshold. Set a high threshold for a 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 existing 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

This section displays the information on the locally installed SD card. You can set it as read-only or read & write; you can also hot-swap and format SD card.



Functions may vary with different models. Select  > **Storage**.

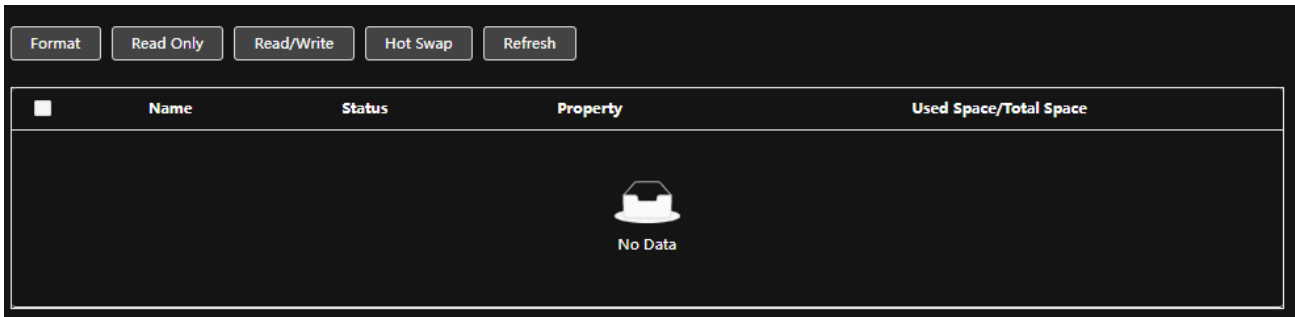
- Click **Read-Only**, and then the SD card is set to read only.
- Click **Read & Write**, and then the SD card is set to read & write.
- Click **Hot Swap** to pull out the SD card.

- Click **Format** to format the SD card.



When reading an SD card on a PC, if the SD card capacity is much less than the nominal capacity, you need to format the SD card. Then the data in the SD card will be cleared, and the SD card is formatted to be a 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 the device name, language, and video standard.


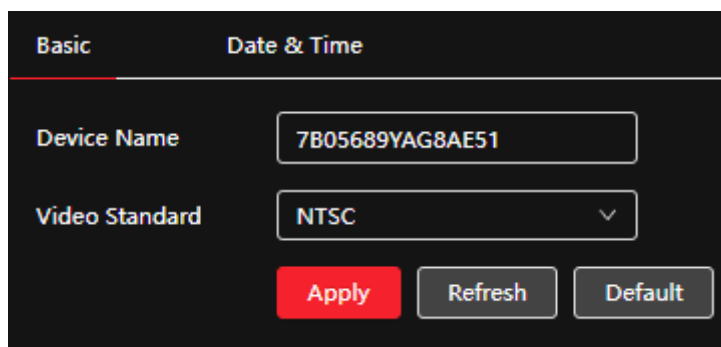
Step 1 Select  > **System** > **General** > **Basic**.

Figure 6-65 Basic



Step 2 Configure general parameters.

Table 6-25 Description of general parameters

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

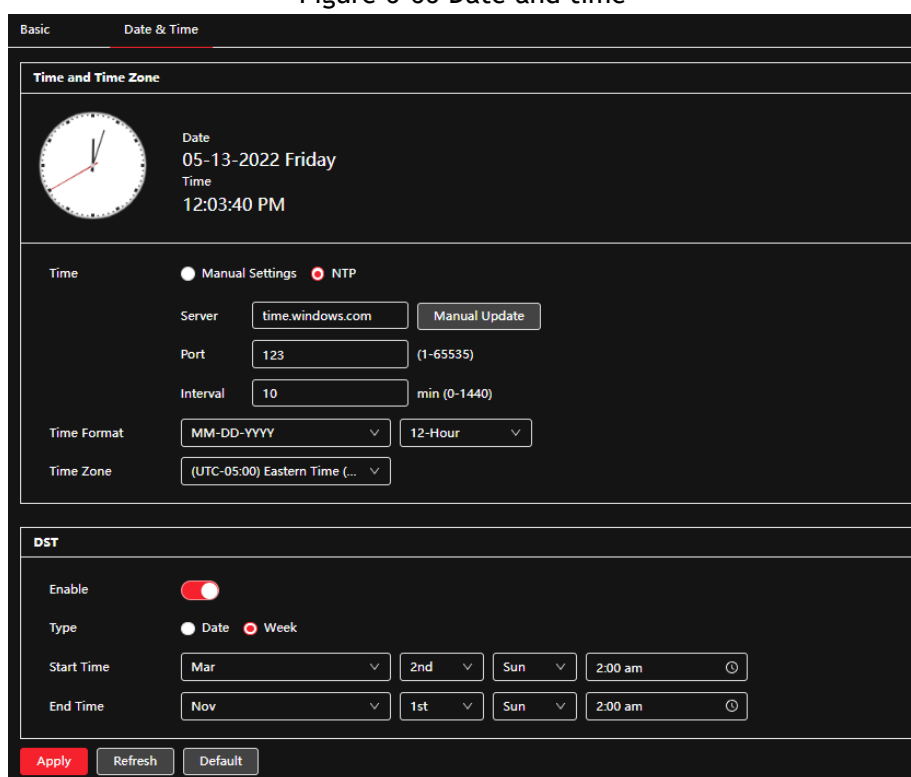
Step 3 Click **Apply**.

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	<ul style="list-style-type: none"> • Manually Setting: Configure the parameters manually. • NTP: When selecting NTP, the system then syncs time with the internet server in real-time.
Time Format	Configure the time format. Options include 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 necessary. Click <input type="checkbox"/> , 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 adding, deleting, or editing them. Users include admin, added users, and ONVIF users.

Managing users and groups are only available for administrator users.

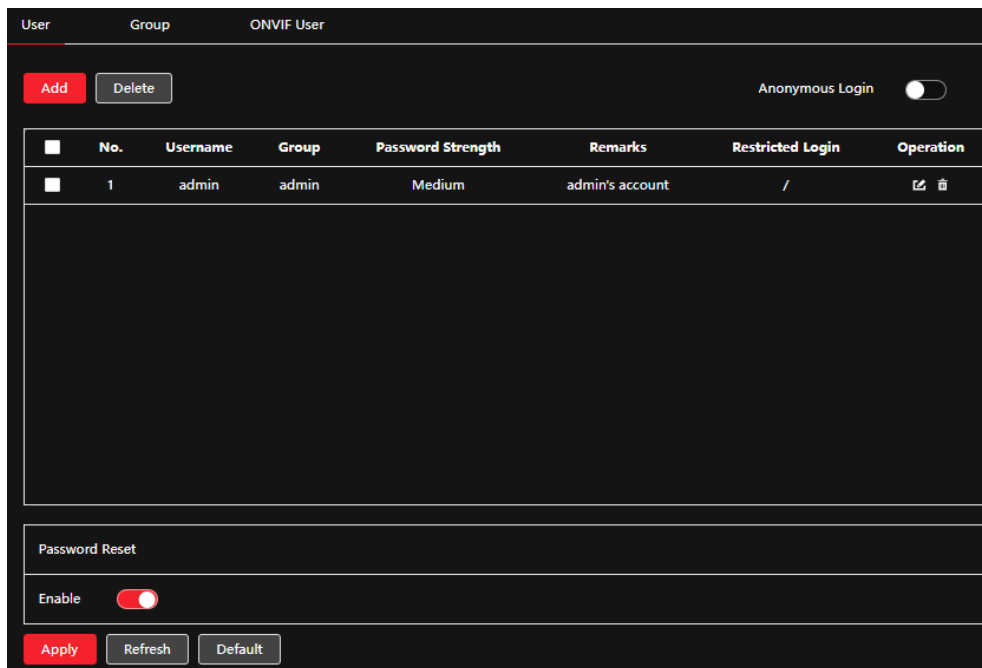
- The max length of the user or group name is 31 characters which can consist of a combination of number, letter, underline, dash, dot and @.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character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

6.6.2.1 User

6.6.2.1.1 Adding User

The admin user is the default account. You can add users, and configure different permissions.

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



Step 2 Click **Add**.

Figure 6-68 Add user (system)

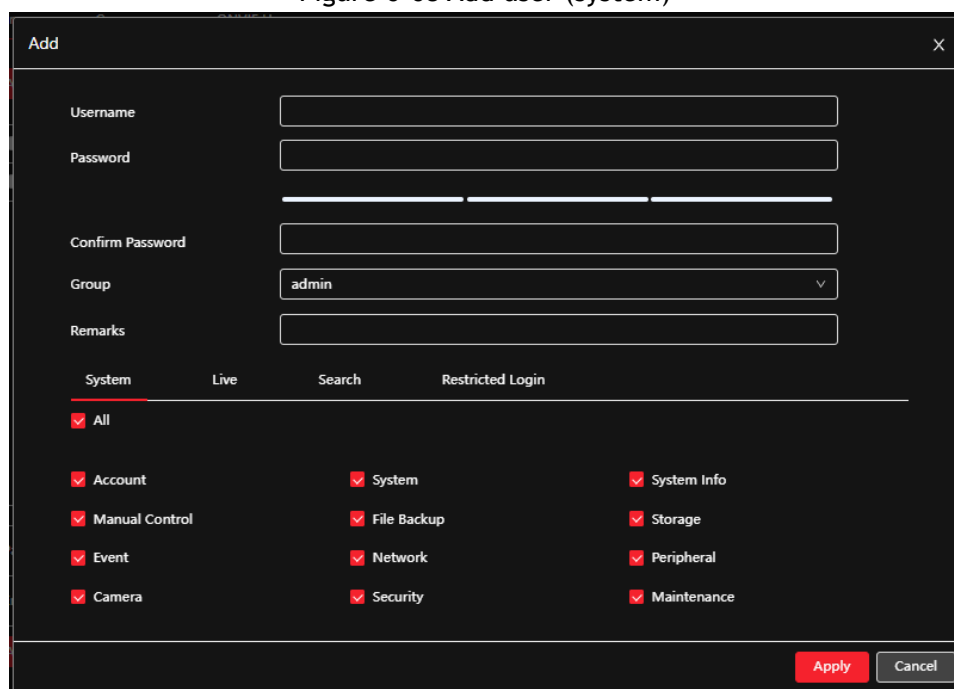


Figure 6-69 Add user (restricted login)

Add
X

Username

Password

Confirm Password ✔

Group

Remarks

System Live Search Restricted Login

IP Address

IPv4

Validity Period

05-13-2022 08:00:00 AM 05-14-2022 08:00:00 AM


Period

Time Plan

Apply
Cancel

Step 3 Configure user parameters.

Table 6-27 Description of user parameters (1)


Parameter	Description
Username	User's unique identification. You cannot use an existing username.
Password	Enter a password and confirm the password on the next field.
Confirm Password	The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).
Group	The group that users belong to. Each group has different authorities.
Remark	Describe the user.
System	Select authorities as necessary.  It is recommended to give as few permissions to non-authority users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.

Parameter	Description
Restricted Login	<p>This allows login restrictions such as the IP addresses allowed to access, duration of validity, and time range.</p> <ul style="list-style-type: none"> • IP address: You can log in to the web through the PC only with the set IP. • Validity period: You can log in to web in the set validity period. • Time range: You can log in to the web in the set time range. <p>Set as follows</p> <ol style="list-style-type: none"> 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 will be 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.



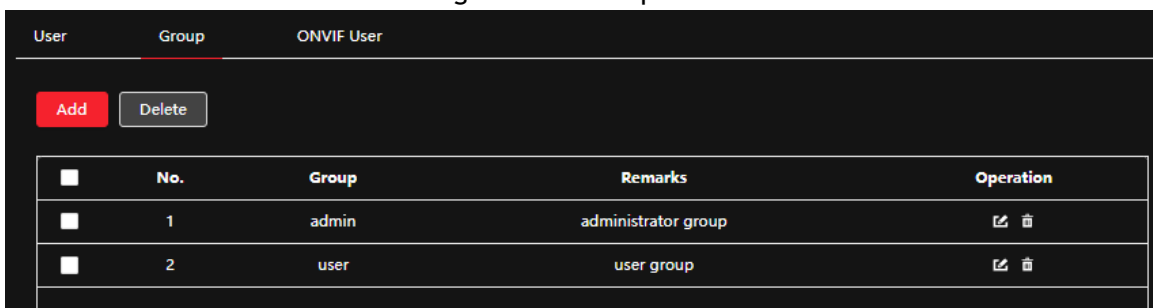
The admin account cannot be deleted.





6.6.2.2 Adding User Group

There are two groups named admin and user by default to add a new group, delete added group or edit group authorities.

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

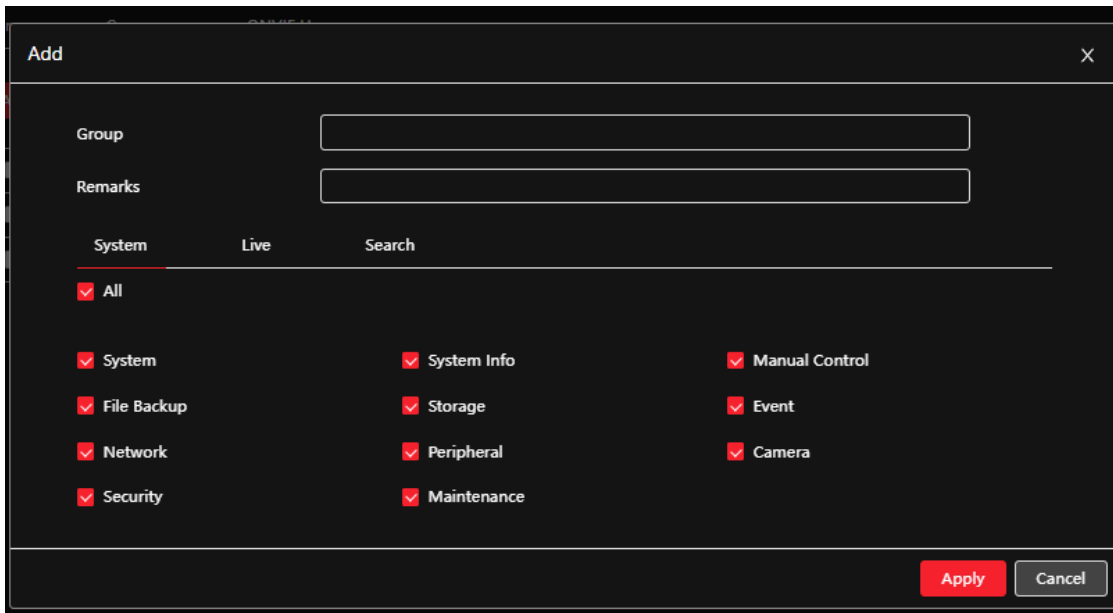
Figure 6-71 Group name



No.	Group	Remarks	Operation
1	admin	administrator group	 
2	user	user group	 

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 the configuration.

The newly added group is displayed in the group name list.

Related Operations

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



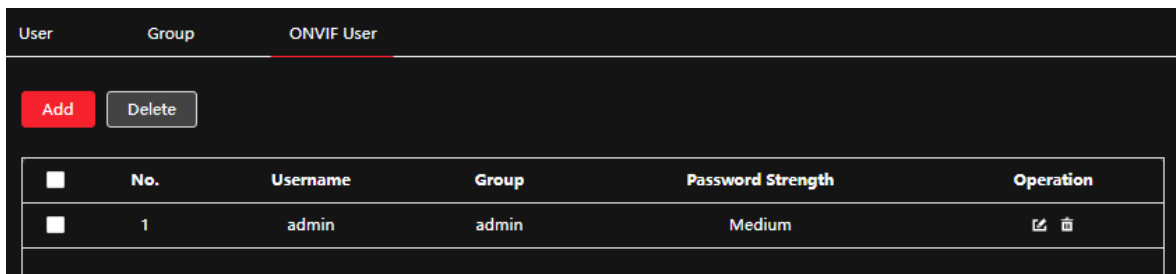
The admin group and user group cannot be deleted.



6.6.2.3 ONVIF User

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

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

Figure 6-73 ONVIF user



No.	Username	Group	Password Strength	Operation
1	admin	admin	Medium	 

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 an existing username.
Password	Enter the password and re-enter under Confirm Password. The password must consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' ' ; : &).
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 configuration of the external device.


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

Step 2 Configure parameters.

Figure 6-75 Serial port settings

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

Table 6-29 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

For attached lighting devices to the camera (not built into the camera).

Prerequisites

- Connect the external light devices to the camera using the RS-485 port.
- You have configured serial port parameters. For details, see "6.6.3.1 Configuring Serial Port".

Procedure

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

Step 2 Select working mode as necessary.

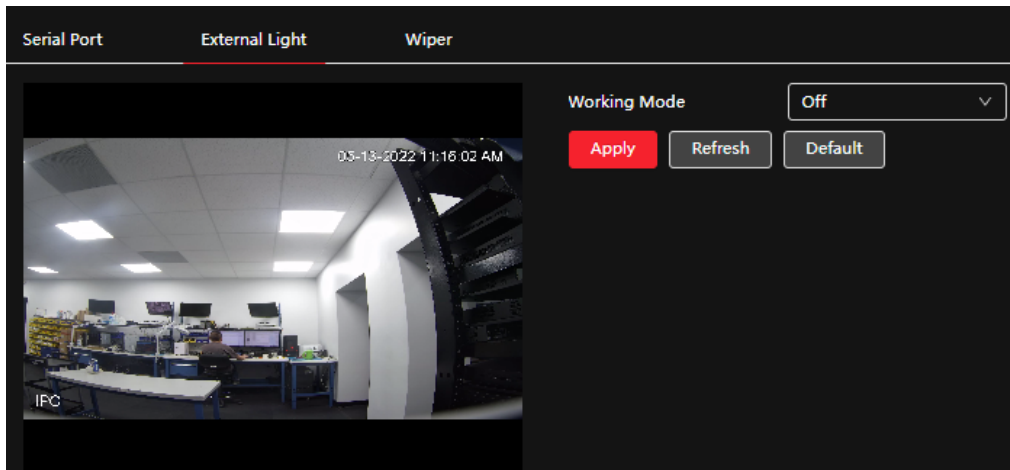



Table 6-30 Lamp parameters

Parameter	Description
Work Mode	<ul style="list-style-type: none"> • Off: The external light will be disabled. • Manual: Sets the light brightness manually. • Auto: The camera turns on or turns off the light according to the light's time and photoresistor automatically.
Auto Mode	<ul style="list-style-type: none"> • Time: Set the arming period. During the arming period, the external light will be on. Select the added time plan table in the Time Plan list. Click Add Schedule to add a new time plan table. For details, see "6.4.1.2 Alarm Linkage". • Photoresistor: When you select Photoresistor in Auto Mode, the camera automatically turns on the external light according to the brightness.
Light Brightness	<p>Sets the brightness of the external light.</p>  <p>For some models, you can set the brightness of each external light separately.</p>

Step 3 Click OK.

6.6.3.3 Configuring Wiper

Step 1 Select  > System > Peripheral > Wiper.

Step 2 Configure the working mode for the external wipers.

Figure 6-77 Wiper

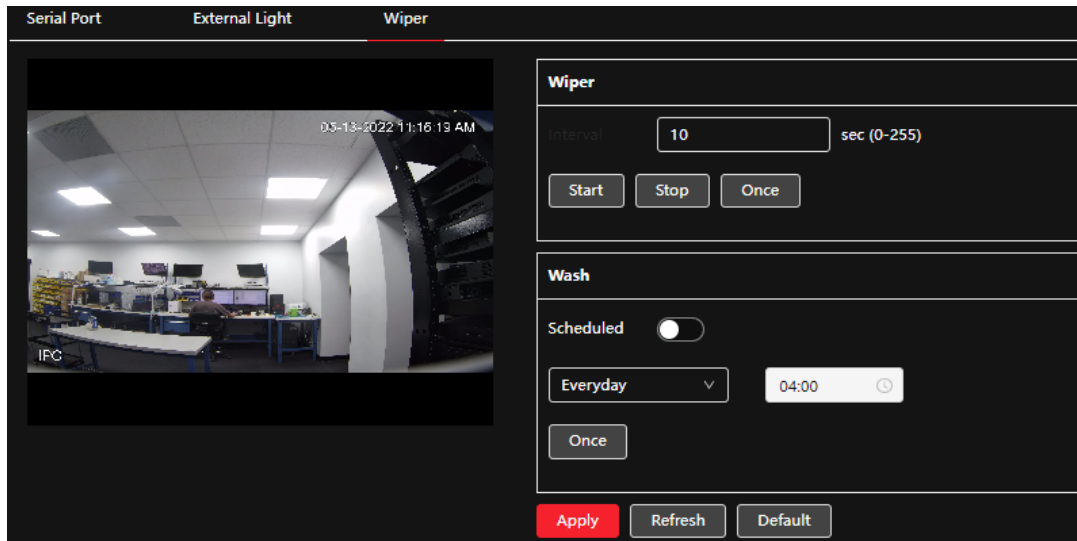


Table 6-31 Wiper parameter description

Parameter	Description
Interval	The interval between stop mode and start mode. For example, set the time to 10 s, and the wiper will work every 10 s.
Start, Stop, Once	Configure the working mode of the wiper. <ul style="list-style-type: none"> 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	Set the time. The wiper will operate at the configured time. Click Once , and the wiper will operate once. It can be used to check whether the wiper is working normally.

Step 3 Click **Apply**.

6.6.4 Manager

6.6.4.1 Requirements

To ensure the system runs normally, maintain it as per the following requirements:

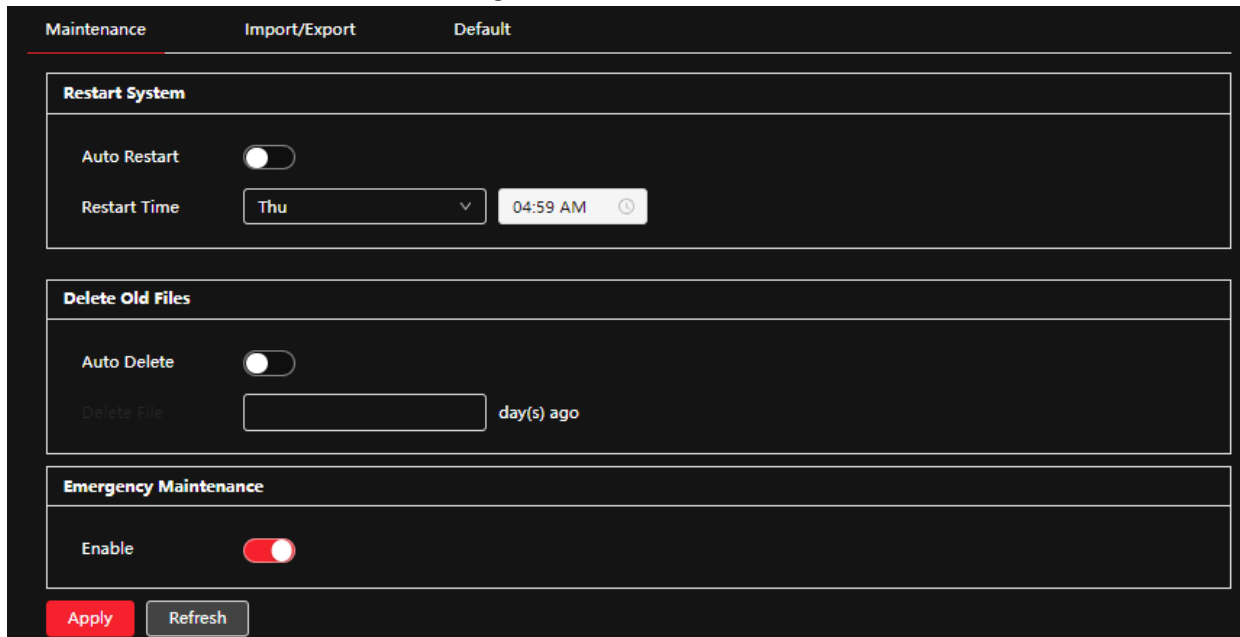
- Check live view images regularly.
- Delete user and user group information that is not frequently used.
- Change the password every three months. For details, see "6.6.2 Account".
- View system logs and analyze them, and fix any abnormalities accordingly.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Upgrade firmware regularly.

6.6.4.2 Maintenance

This section allows for manual camera reboot, as well as set the auto-reboot time and auto-deletion of 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 restart at the set time every week.
- Click next to **Auto Delete** in **Delete Old Files**, and set the time. The system will automatically delete 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 with caution.

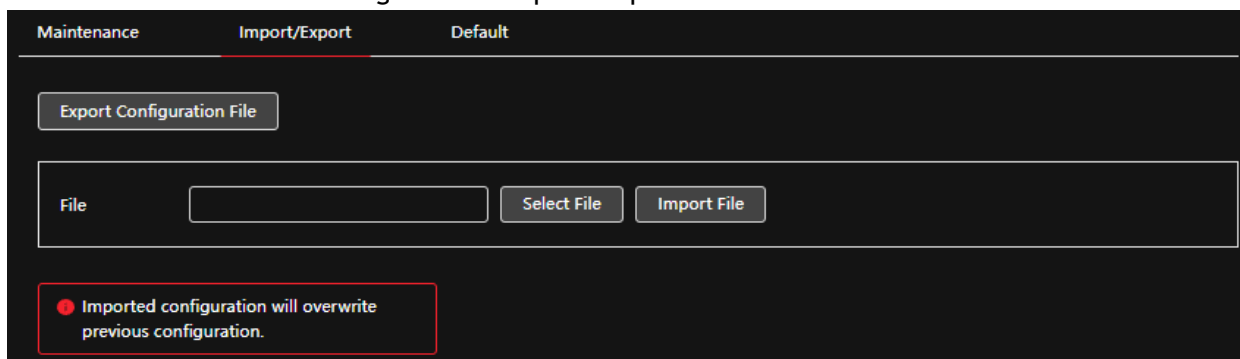
Step 3 Click **Apply**.

6.6.4.3 Import/Export

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

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

Figure 6-79 Import/Export



Step 2 Import or export the file.

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

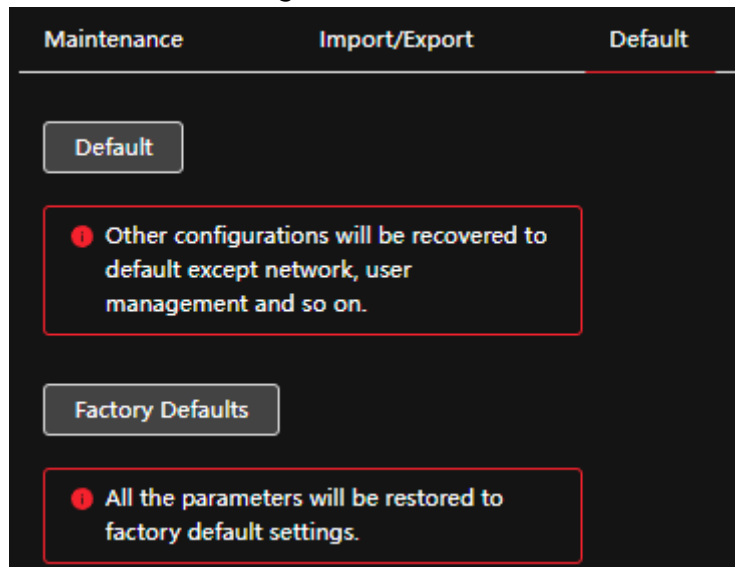
- Export: Click **Export Configuration** file to export the system configuration file to local storage.

6.6.4.4 Default

Restore the device to default configuration or factory settings. Select  > **System** > **Manager** > **Default**.

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

Figure 6-80 Default



6.6.5 Upgrade

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

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

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

Figure 6-81 Upgrade



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


The upgrade file should be a .bin file.

Step 3 Click **Update**.

6.7 System Information

This section allows you to 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 the IPC.

6.8 Setting Log

6.8.1 Log

Allows you to 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 the configuration and deleting the 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 to view the detailed information in the **Details** area.
- Click **Backup** to back up all found logs to a local PC.

Start Time: 05-12-2022 12:18:45 PM ~ 05-13-2022 12:18:45 PM | Type: All | Search | Backup

No.	Time	Username	Type	Details
1	2022-05-13 10:30:58	admin	Save Config	🔍
2	2022-05-13 10:03:16	admin	Login	🔍
3	2022-05-13 08:48:41	System	Lock Account	🔍
4	2022-05-13 03:48:39	System	Lock Account	🔍
5	2022-05-13 00:00:01	System	Save Config	🔍
6	2022-05-13 00:00:00	System	Save Config	🔍
7	2022-05-12 22:48:40	System	Lock Account	🔍
8	2022-05-12 18:48:41	System	Lock Account	🔍
9	2022-05-12 17:08:27	admin	Login	🔍
10	2022-05-12 17:08:27	admin	Login	🔍
11	2022-05-12 17:08:18	admin	Login	🔍
12	2022-05-12 17:04:26	admin	Logout	🔍
13	2022-05-12 17:04:26	admin	Logout	🔍
14	2022-05-12 17:04:26	admin	Logout	🔍
15	2022-05-12 17:04:26	admin	Logout	🔍
16	2022-05-12 14:08:44	admin	Login	🔍
17	2022-05-12 12:48:41	System	Lock Account	🔍

17 record(s)

6.8.2 Remote Log

Configure the remote log to acquire the related log by accessing the set address.

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

Step 2 Click to enable the remote log function.

Step 3 Set address, port, and device number.

Step 4 Click **Apply**.

Figure 6-83 Remote log

Enable

Server Address

Port (1-65534)

Device No. (0-23)

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

7.1 Live Interface

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



Interfaces may vary with different models.

Figure 7-1 Live (single-channel)

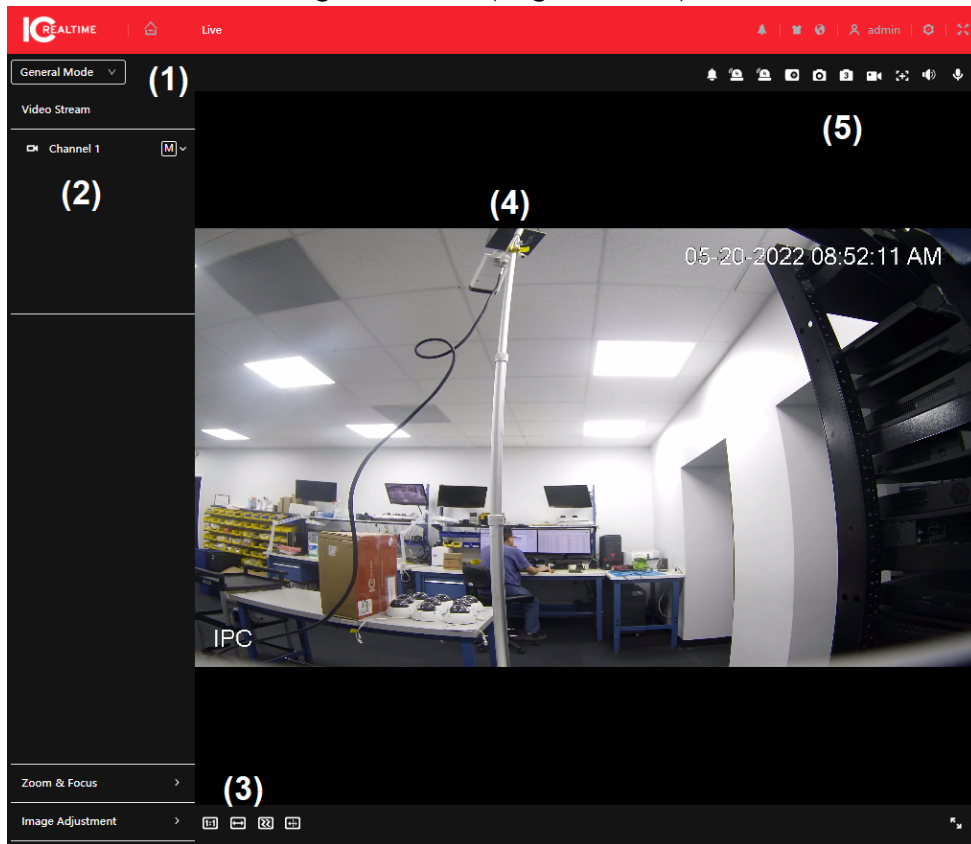


Table 7-1 Description of function bar

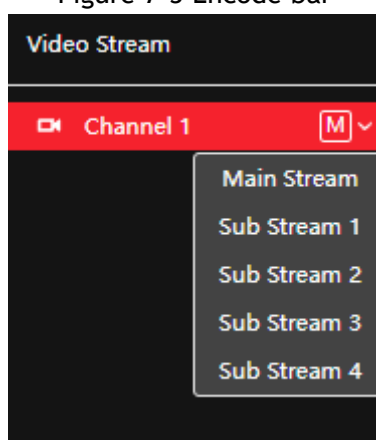
No.	Function	Description
1	Display mode	You can select the display mode from General Mode, Face Mode, Metadata Mode, ANPR and Face & Body Detection . For details, see "7.5 Display Mode".
2	Channel list	Displays all channels. You can select the channel as necessary and set the stream type.
3	Image adjustment	Adjustment operations in live viewing.




4	Live view	Displays the real-time monitoring image.
5	Live view function bar	Functions and operations in live viewing.

7.2 Setting Encode

Click , and then select the stream as necessary.

Figure 7-3 Encode bar















- **Main Stream:** This has a large bit stream value and image with high resolution and requires large bandwidth. This option can be used for storage and monitoring. For details, see "6.2.2.1 Encode".
- **Sub Stream:** This has a small bit stream value and smooth image, and requires less bandwidth. This option is normally used to replace main stream when bandwidth is insufficient. For details, see "6.2.2.1 Encode".
-  represents the main stream;  represents sub stream 1;  represents sub stream 2.

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	<p>You can zoom the video image through two operations.</p> <ul style="list-style-type: none"> • Click the icon then draw a box around the video image to zoom in; right-click on the image to resume the original size. While in the zoom-in state, drag the image to view other areas. • While in the zoom-in state, scroll the mouse wheel in the video image to zoom in or out.
	Snapshot	<p>Click the icon to capture one picture of the current image. It will be saved to the configured storage path.</p>  <p>For details on viewing or configuring storage path, see "6.1 Local".</p>
	Triple Snapshot	<p>Click the icon to capture three pictures of the current image. They will be saved to the configured storage path.</p>  <p>For details on viewing or configuring storage path, see "6.1 Local".</p>
	Record	<p>Click the icon to record a video. It will be saved to the configured storage path.</p>  <p>For details on viewing or configuring storage path, see "6.1 Local".</p>
	Aux Focus	<p>Click the icon, and the AF Peak (focus eigenvalue) and AF Max (max focus eigenvalue) will display on the video image.</p> <ul style="list-style-type: none"> • AF Peak: The eigenvalue of image definition, displayed during focus. • AF Max: The best eigenvalue of image definition. • The smaller the difference between the AF peak value and the AF max value, the better the focus.  <p>Aux focus closes automatically after five minutes.</p>
	Audio	<p>Click the icon to enable or disable audio output.</p>
	Talk	<p>Click the icon to enable or disable the audio talk.</p>

7.4 Window Adjustment Bar

7.4.1 Adjustment

This section explains the image adjustment icons. For details, see Table 7-3.

Table 7-3 Description of adjustment bar

Icon	Function	Description
	Original Size	Click the icon to display the video with the original size.
	Full Screen	Click the icon to enter full-screen mode; double-click or press Esc to exit.
	W:H	Click the icon to resume the original ratio or change ratio.
	Fluency Adjustment	<p>Click the icon to select the fluency from Realtime, General and Fluent.</p> <ul style="list-style-type: none"> • Realtime: Guarantees the real-time streaming of the video. When the bandwidth is insufficient, the image may not be smooth. • General: It is between Realtime and Fluent. • Fluent: Guarantees the fluency of the image. There may be a delay between live view images and real-time images.
	AI Rule	Click the icon, and then select Enable to display AI rules and detection box; select Disable to turn off the display. It is enabled by default.
	Crowd Distribution Map	Click the icon and select Enable to display the Crowd Distribution Map interface. For details, see "8.1 Setting Crowd Distribution Map".
	Window Layout	When viewing a multi-channel image, you can select a display layout.

7.4.2 Zoom and Focus

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



The focus will adjust automatically after zooming in or out.

Figure 7-4 Zoom and focus

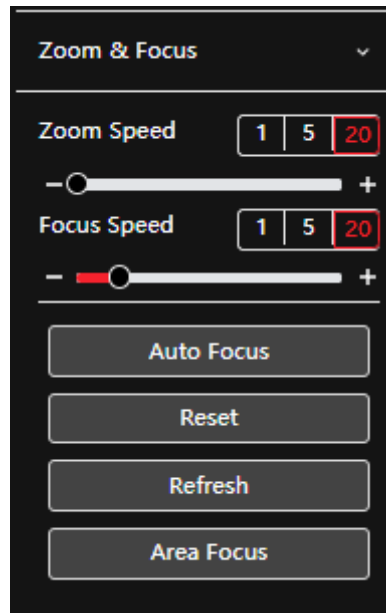




Table 7-4 Description of zoom and focus parameter

Parameter	Description
Zoom Speed	<p>Changes the focal length of the camera to zoom in or out of the image.</p> <ol style="list-style-type: none"> 1. Set the speed value. The Zoom Speed is the adjustment range in one click. The greater the value, 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	<p>Adjusts the optical back focal length to make the image clearer.</p> <ol style="list-style-type: none"> 1. Set the speed value. The Focus Speed is the adjustment range in one click. The greater the value, the more in one click. 2. Click or hold + or – button, or drag the slider to adjust focus.
Auto Focus	<p>Adjusts image clarity automatically.</p>  <p>Do not make any other operation during auto focus process.</p>
Reset	<p>Restores focus to the default value and corrects errors.</p>  <p>You can restore the focus if the image has poor clarity or has been zoomed too frequently.</p>
Refresh	<p>Acquire the latest zoom setting of the camera.</p>
Area Focus	<p>Focus on the subject of a selected area.</p> <p>Click Area Focus, and then select an area in the image, the camera performs autofocus in that area.</p>

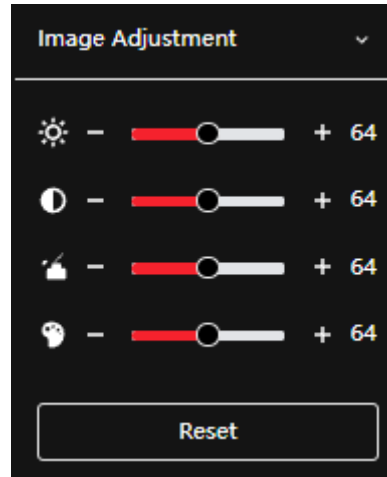
7.4.3 Image Adjustment

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



The adjustment only affects the live view on the Web GUI, 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.
- (Contrast adjustment): Changes the value when the image brightness is proper but contrast is insufficient.
- (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 the default value.

7.4.4 Fisheye

If using a fisheye camera, you can select the installation mode, display mode, and VR mode of fisheye devices as necessary. For details, see Table 7-5.

- **Install Mode:** Select the installation mode according to the actual camera installation position.
- **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

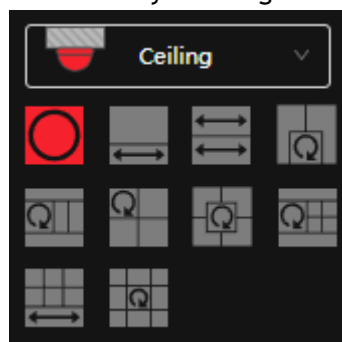


Figure 7-7 Fisheye-wall mount

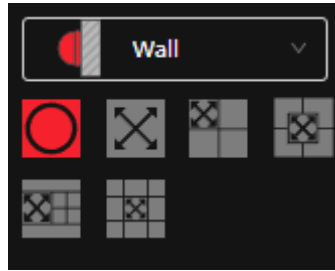


Figure 7-8 Fisheye-ground mount

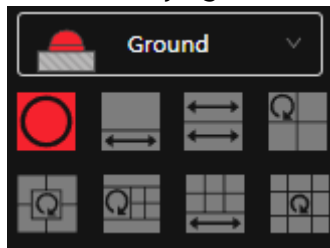


Figure 7-9 Fisheye-VR mode

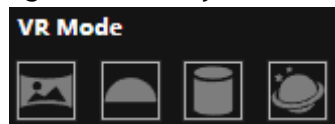






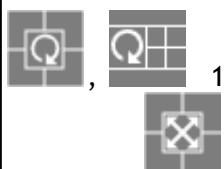


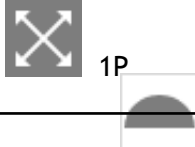


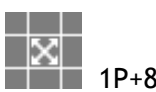




Table 7-5 Description of fisheye configuration


Parameter	Description	
Installation mode	Includes ceiling mount, wall mount, and ground mount.	
Display mode	<p>The display model of the current image. There are different display modes for each installation mode.</p> <ul style="list-style-type: none"> ● 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. <p> The image will be the original size by default when switching installation mode.</p>	
Ceiling/Wall/ Ground mount	 Original image	The original image before dewarping.
	 1P+1	<p>360° rectangular panoramic image screen + independent sub-screens.</p> <ul style="list-style-type: none"> ● You can zoom or drag the image in all the screens. ● You can move the start point (left and right) on a rectangular panoramic image screen.

Ceiling/ Ground mount	 2P	<p>Two associated 180° rectangular image screens; at any time, the two screens form a 360° panoramic image. It is also called a dual-panoramic image.</p> <p>You can move the start point (left and right) on the two rectangular panoramic image screens, and the two screens link each other.</p>
	 1+2	<p>Original image screen + two independent sub-screens. The ground mount does not support this display mode.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can rotate the image on the original image screen to change the start point.
	 1+3	<p>Original image screen + three independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can rotate the image on the original image screen to change the start point.
	 1+4	<p>Original image screen + four independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can rotate the image on the original image screen to change the start point.

Parameter	Description
 1P+6	<p>360° rectangular panoramic screen + six independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image in all the screens. You can move the start point (left and right) on a rectangular panoramic image screen.
 1P+8	<p>Original image screen + eight independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can rotate the image on the original image screen to change the start point.

Wall mount	 1P	<p>180° rectangular panoramic image screen (from left to right).</p> <p>You can drag the image on all the screens (up and down) to adjust the vertical view.</p>
	 1P+3	<p>180° rectangular panoramic image screen + three independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can drag the image on all the screens (upper and lower) to adjust the vertical view.
	 1P+4	<p>180° rectangular panoramic image screen + four independent sub-screens.</p> <ul style="list-style-type: none"> You can zoom or drag the image on all the screens. You can drag the image in all the screens (upper and lower) to adjust the vertical view.
	 1P+8	<p>180° rectangular panoramic image screen + eight independent sub-screens.</p> <ul style="list-style-type: none"> 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	<p>Drag or cross the screen 360° to unfold the distortion panorama to drag the image in left/right direction.</p>

	Semi-circle	<ul style="list-style-type: none"> You can drag the image in the 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 an anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the image.
	 Cylinder	<p>Displays the distortion panorama in 360° circularity.</p> <ul style="list-style-type: none"> You can drag the image in the 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 an anticlockwise direction, and press E to stop the rotation. Scroll the mouse wheel to zoom the

	 Asteroid	<p>image.</p> <ul style="list-style-type: none"> You can drag the image in the 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

When viewing the live view, 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**.



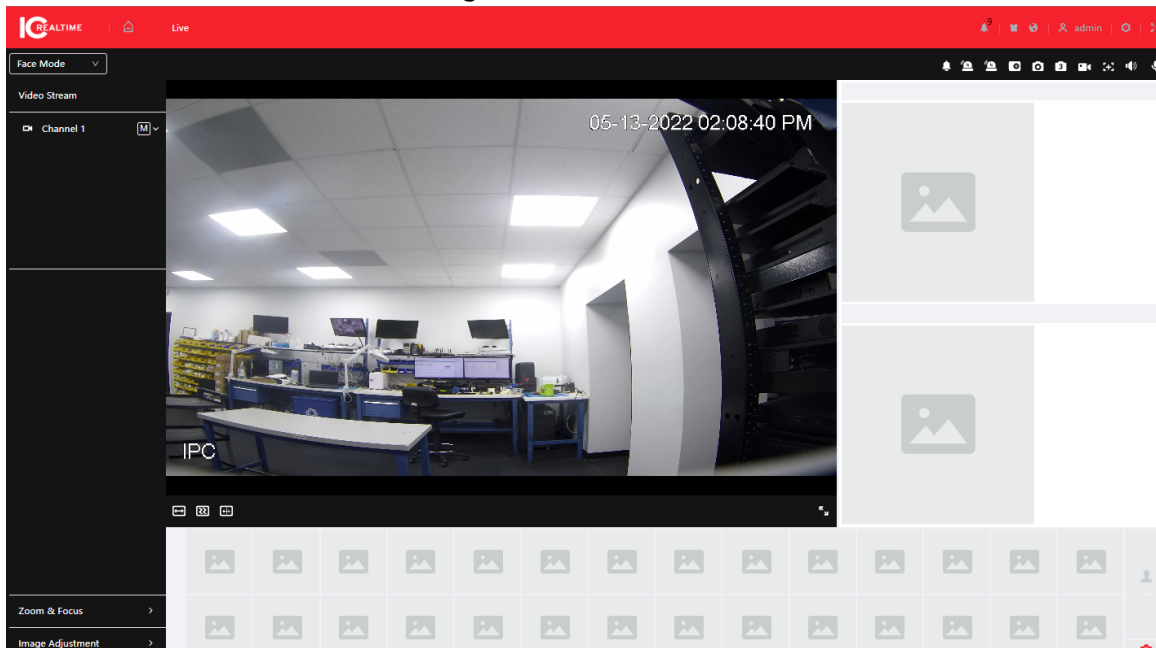
Interfaces may vary with different models.

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



Make sure that you have enabled the face detection function.

Figure 7-10 Face mode

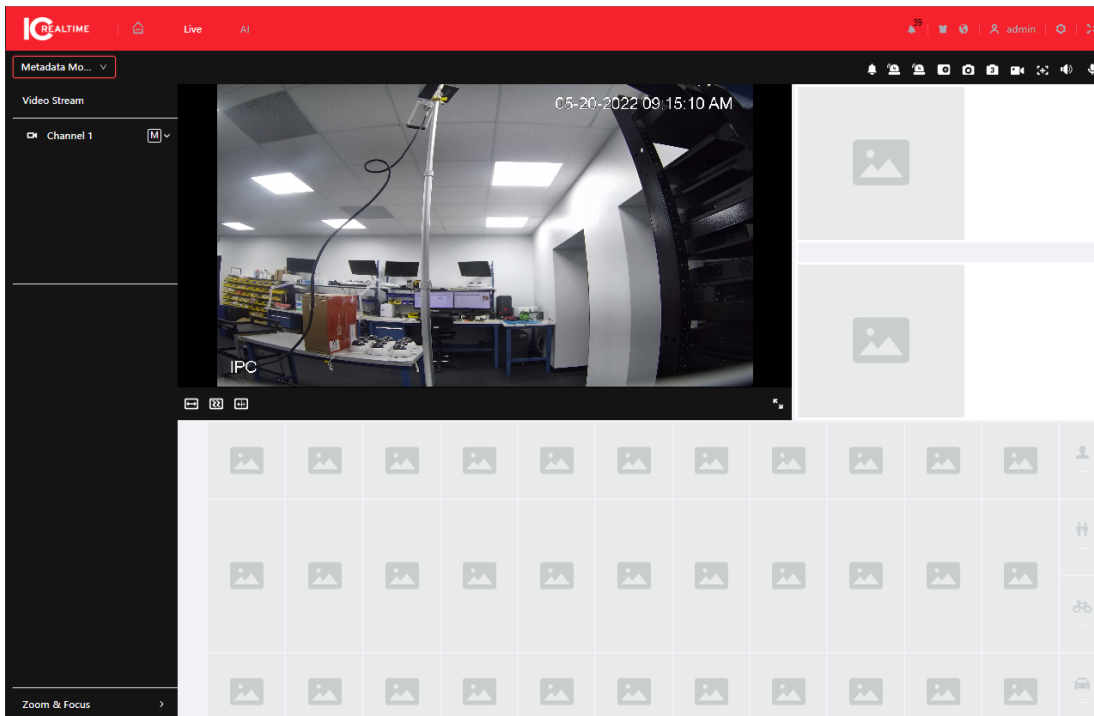


- Select **Metadata Mode** from the display mode drop-down list.



Make sure that you have enabled the video metadata detection function.

Figure 7-11 Metadata mode

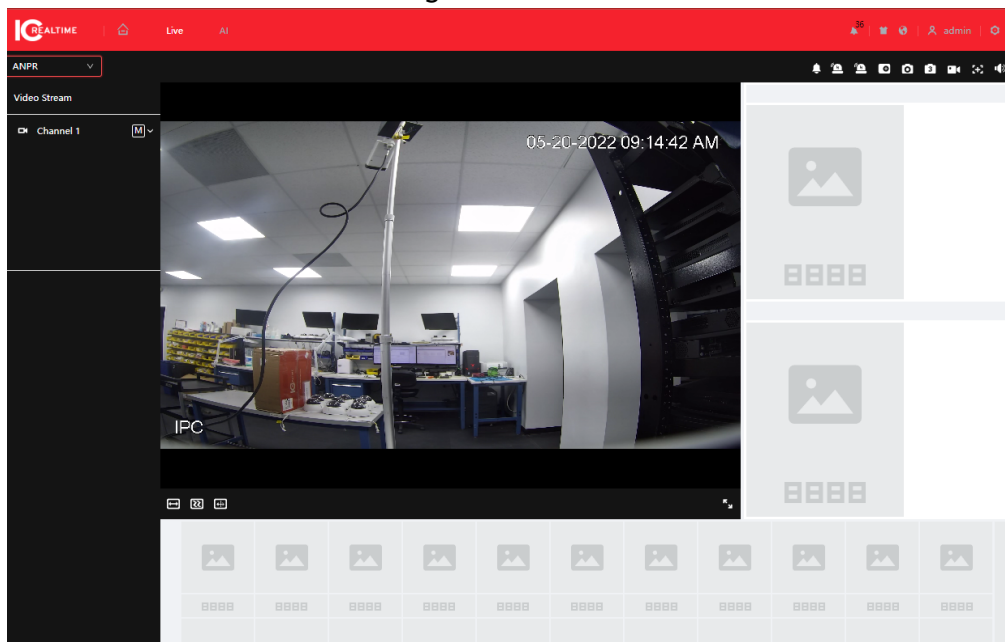


- Select **ANPR** from the display mode drop-down list.



Make sure that you have enabled the 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

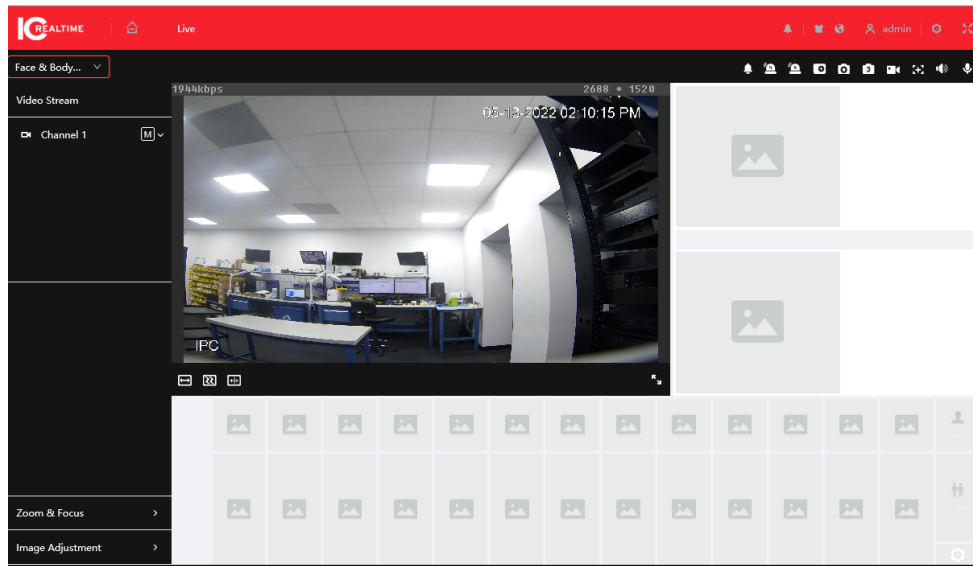



Table 7-6 Description of layout

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.

No.	Function	Description
3	Captured image	<p>Displays the captured images.</p> <ul style="list-style-type: none"> 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.

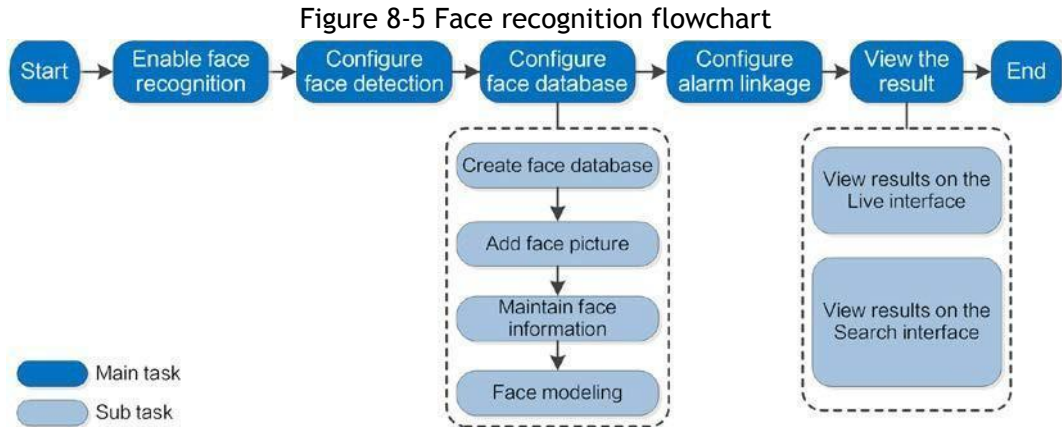
8 AI

8.1 Setting Face Recognition

When a face is detected or recognized in the detection area, the system can perform an alarm linkage and supports searching for 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 an event according to the comparison result.

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



8.1.1 Setting Face Detection

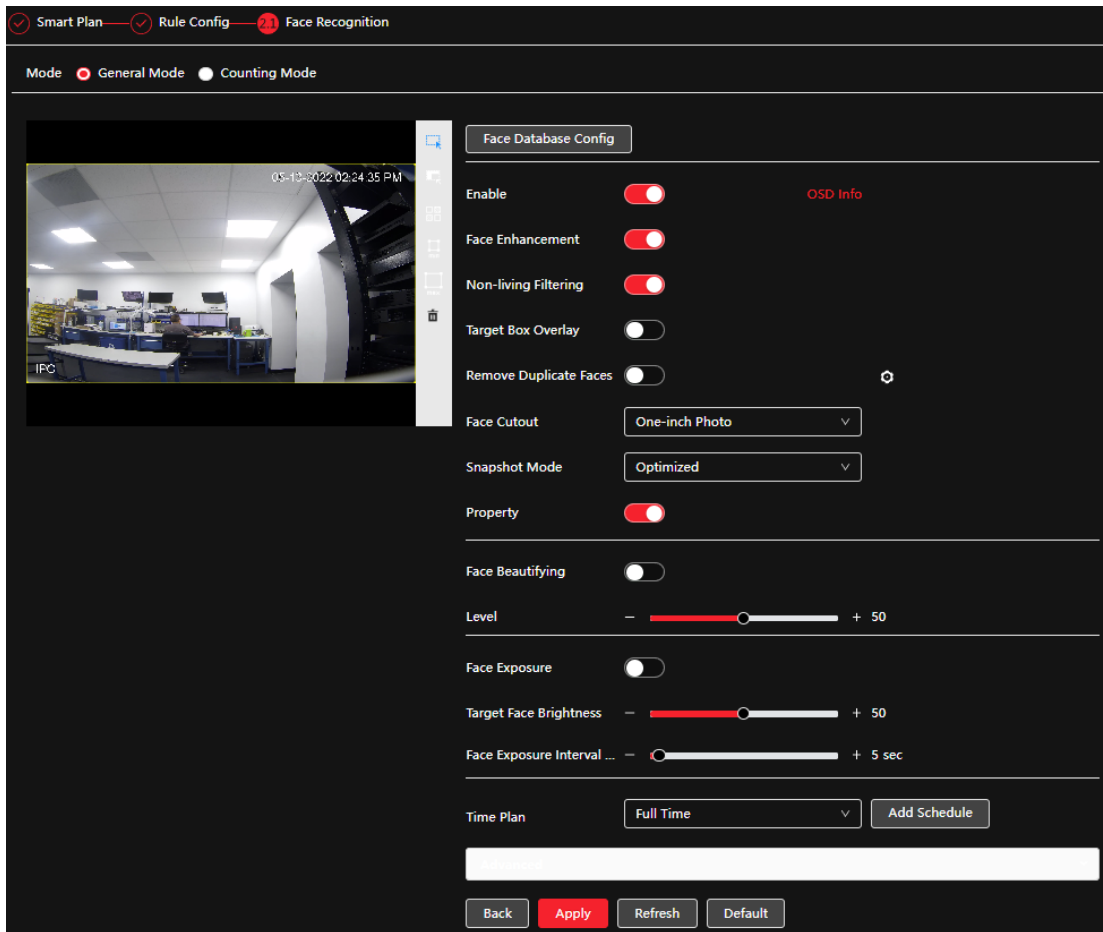
When a face is recognized in the detection area, the system performs alarm linkage.

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 on the right side of the image to draw the detection area, exclusion area, and filter targets in the image.



- Click  to draw a 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 them after comparing it 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 will be 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 will be displayed, and then enable the face statistics function. The number of detected faces will be displayed on the Live interface. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click  to enable face enhancement to enhance and clear faces with a low bit stream.
Non-living Filtering	Filter non-living faces in the image, such as a face picture.
Target Box Overlay	Click  to enable the function to add a boundary box to the face in the captured picture to highlight the face. The captured face picture is saved in SD card or the configured storage path. For the storage path, see "6.1 Local".
Remove Duplicate Faces	During the configured period, the duplicate faces are displayed only once, to avoid repeated counting. Click  to configure the parameter, and then click Apply . <ul style="list-style-type: none"> • Time: During the configured time, the function is enabled. • Precision: The larger the precision value, the higher the accuracy.
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 . <ul style="list-style-type: none"> • 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 a snapshot; enter the times of the original face height. It ranges from 1-2. • Customized body height: Set body height in a 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.

Parameter	Description
-----------	-------------

Snap Mode	<ul style="list-style-type: none"> • General mode: <ul style="list-style-type: none"> ◇ Optimized Snapshot: Capture the clearest picture within the configured time after the camera detects a face. ◇ Recognition Priority: Repeatedly compare the captured face to the faces in the armed face database, capture the most similar face image and send the event. We recommend you use this mode in an access control scene. <p> Click Advanced to set the optimized time.</p> <ul style="list-style-type: none"> • 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 the 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	<ul style="list-style-type: none"> • Snapshot Angle Filter: Set snapshot angle to be filtered during face detection. • Snapshot Sensitivity: Set snapshot sensitivity during face detection. It is easier to detect faces with higher sensitivity. • Optimized Time: Set a period to capture the most precise 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 to the relevant alarm events. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.1.2 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 a face database, adding face pictures, and face modeling.

8.2.2.1 Creating Face Database

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

Procedure

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

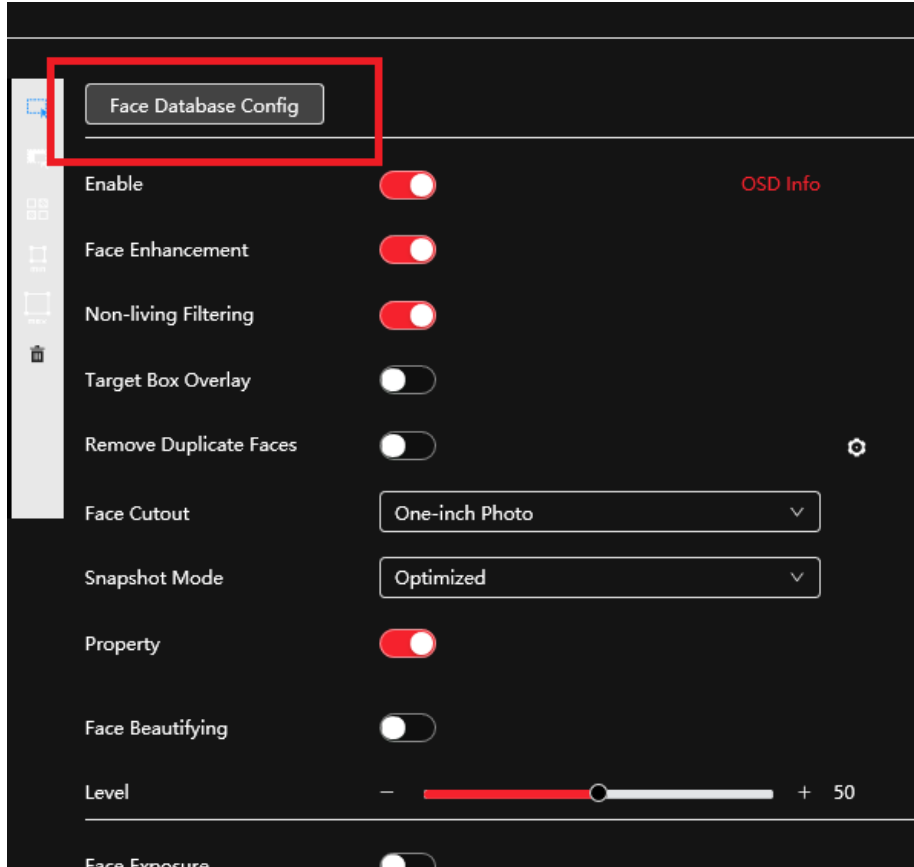
Step 2 Click  next to **Face Recognition** to enable face recognition of the corresponding channel and

then click **Next**.

Step 3 Select the detection mode.

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

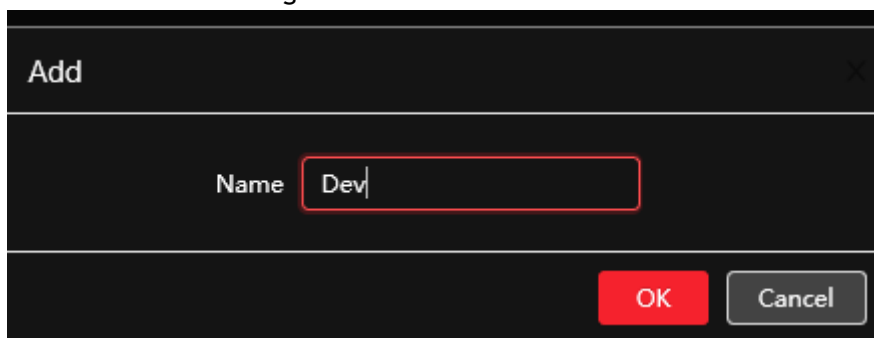
Figure 8-7 Face database configuration



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.

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

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	dev	21	82	Unconnected	🛡️	📄	🗑️

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

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

No.	Name	Register No.	Similarity	Arm Status	Arm Alarm	Details	Delete
1	dev	21	82	Unconnected			

- 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** databases and the **exclude** database.
- ◇ Do not name the newly added database as **AllPeople** or **ExcludePeople**.

- Arm alarm

Click  to configure the parameters of the armed 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 deleting 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

You can add a face picture to the created face database. Single adding and batch importing are supported. Requirements for face pictures are as follows.

- 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 facial 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.

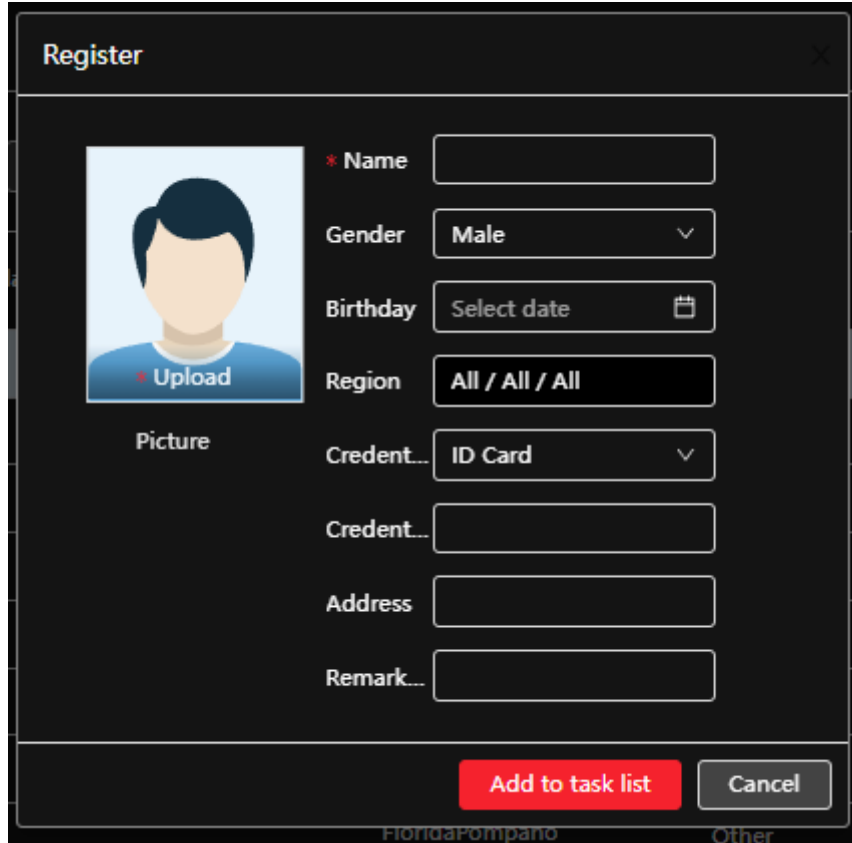
Step 2 Click **Register**.

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 a 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 the face image.

Figure 8-11 Register



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

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

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

- If the operation is successful, the system prompts that stored successfully and modeled successfully.
- If adding a user fails, the error code will be 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 codes

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		The picture format is not correct. Import the picture in JPG format.

2	Picture modeling error	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

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

Before importing pictures in batches, you can name the picture files 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, only the name is required, and others are optional.

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

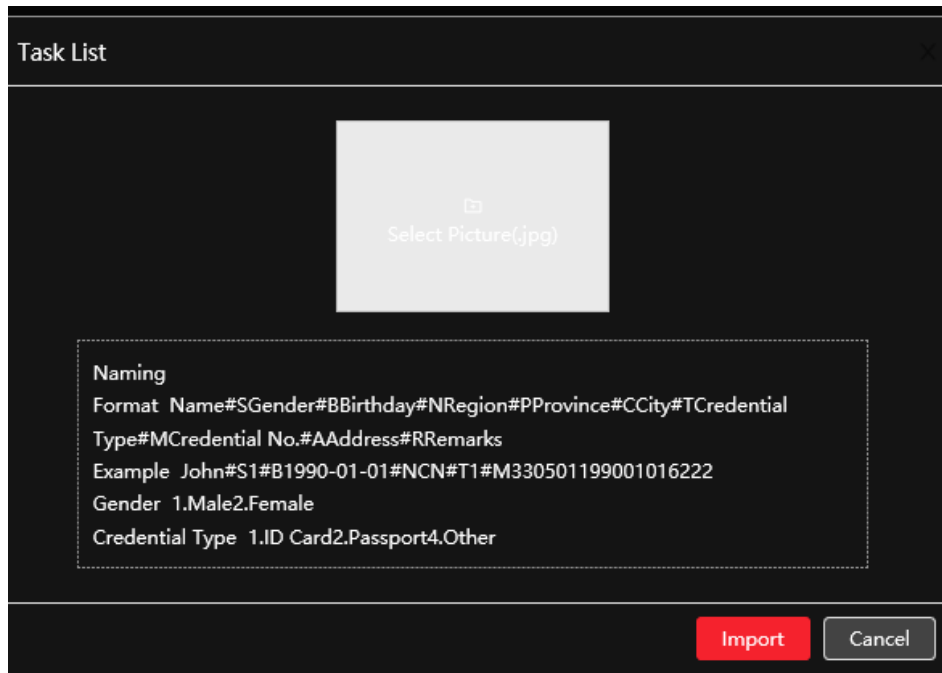
Parameter	Description
Name	Enter a name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Credentials Type	"1" is ID card and "2" passport.
ID number	Enter ID No.

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 the 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 perform the modeling operation.
- If the picture importing failed, click **Query** to view the details of the pictures and the error code. For details, see Table 8-3.
Click **Export** to export the error details.

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

The modeling result will be 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 the picture according to the failure reason. For modeling details, see "8.2.2.4 Face Modeling".


8.2.2.3 Managing Face Picture

You can manage and maintain the added 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.

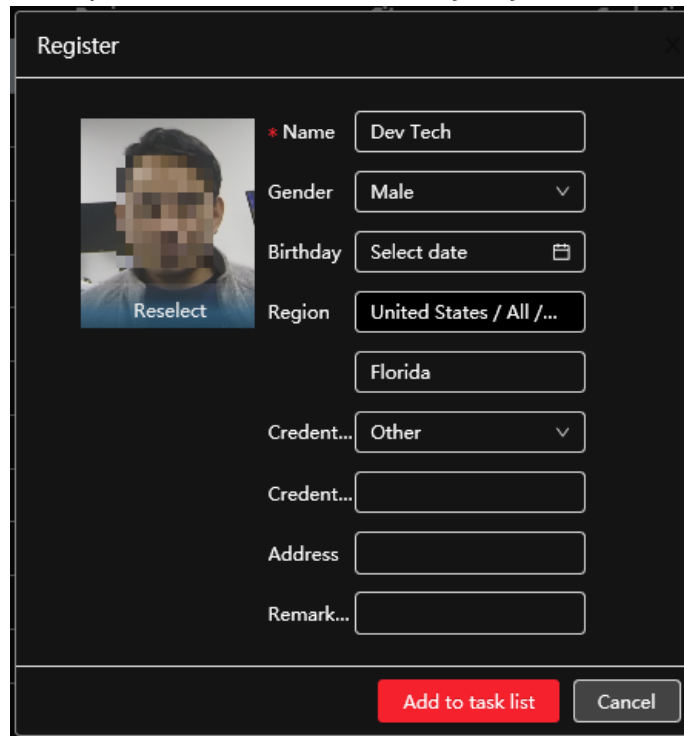
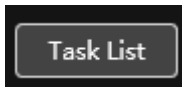
Step 2 Click **Query**, set the criteria as necessary, and then click **Search**.

Step 3 Select the row where the face picture or the 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


*Note that the face in the examples are blurred due to anonymity. The actual image will not be blurred.

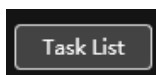
Step 5 Click , and then click **Operation**.

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 necessary, click **Search**, select the face information that needs to be deleted and delete it.

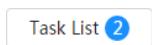
- Single delete: Select the row where the face picture or the personnel information is located, and click  to delete the face picture.

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



, and then click **Operation** to delete the selected face pictures.

- Delete all: When viewing face pictures in a list, click of the row where the serial number is located; when viewing by thumbnail, select **All** to select all face pictures. Click **Delete**, then click



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

8.2.2.4 Face Modeling

Face modeling extracts face picture information and import the information to a database to establish relevant face feature models. By modeling, face recognition and other intelligent detections can function reliably.



- The modeling time can vary depending on how many pictures are being processed.
- 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.

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

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 will be displayed at the lower-left corner of the thumbnail, it means the modeling succeeded.
- When the modeling status is **Invalid** in the list or will be 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

After setting the arm alarm settings, if the face recognition succeeds or fails, the device can trigger an event and alarm linkage.

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

Step 2 Arm face database.

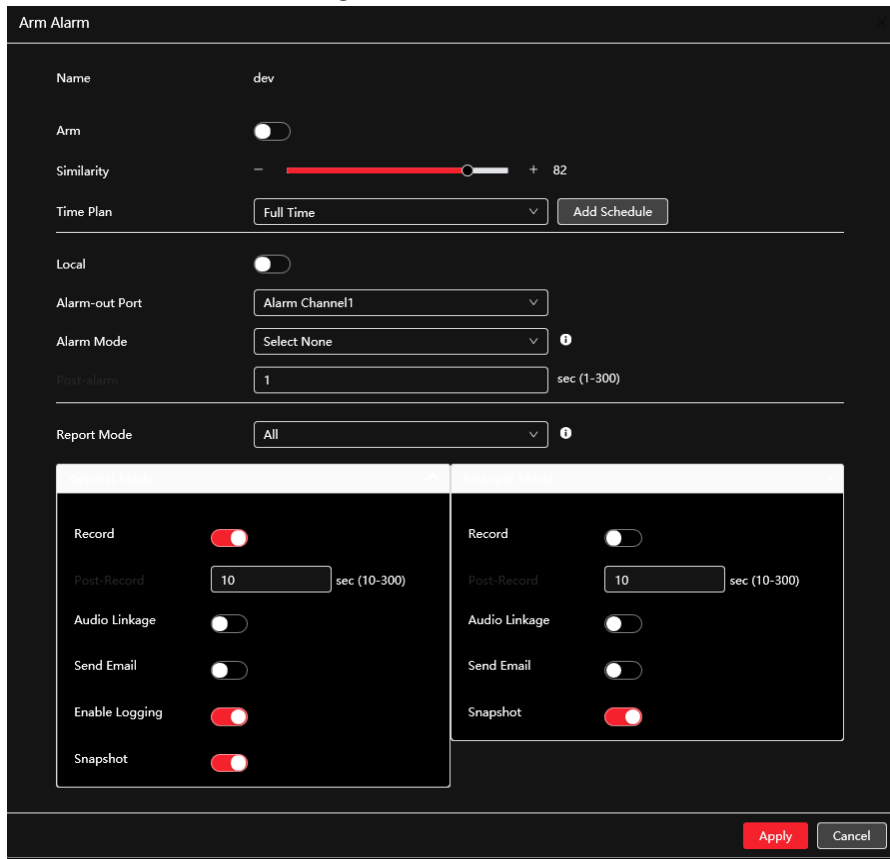
- 1) Click  next to **Arm** to enable the face database arming.

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 a successful match, the comparison result will be displayed on the **Live** interface.

Figure 8-15 Arm alarm



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 necessary .
Alarm Mode	<ul style="list-style-type: none"> • 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 performs 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 performs 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 performs 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**, and set the time.

When the database is full, the camera will delete the old files according to the configured time. 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 to relevant alarm events. 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.


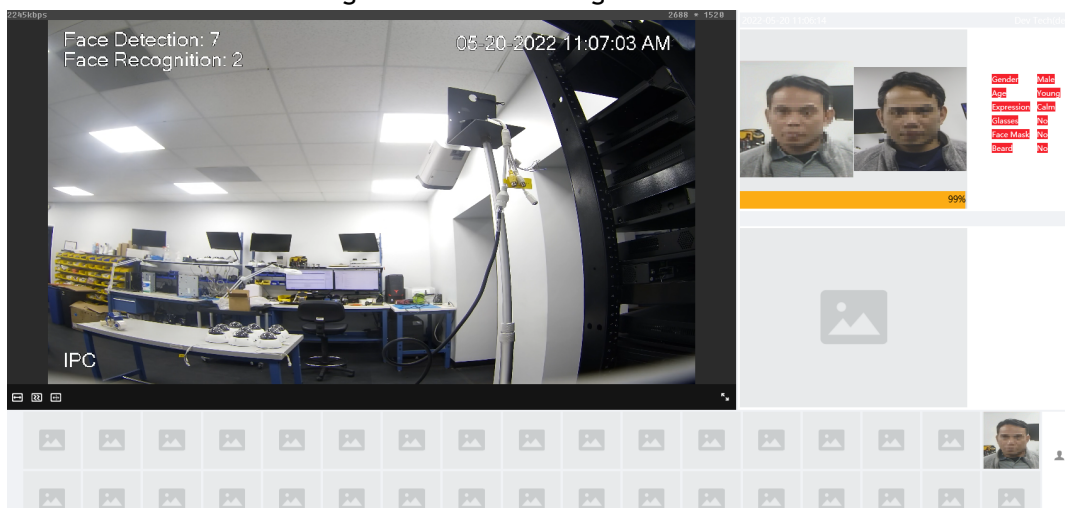
- The live image will be displayed at the left side, and the captured face pictures and attribute information are displayed at the right side. When the recognition is successful, the captured face pictures, pictures in the database and the similarity of the face pictures and pictures in the database 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

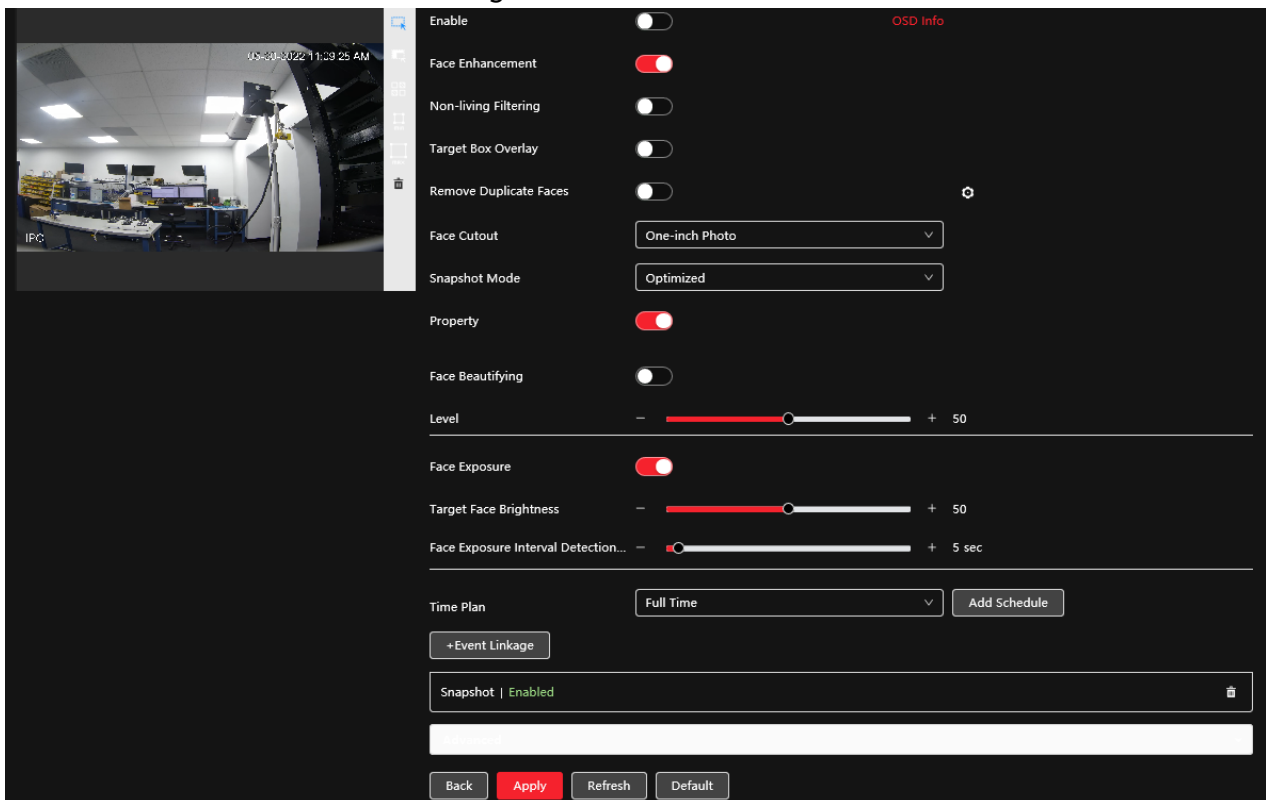
When a face is detected in the detection area, the system performs an alarm linkage.

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 on the right side of the image to draw the 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 will be 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 , to display the Overlay interface then enable the face statistics function. The number of detected faces will be displayed on the Live interface. For details, see "6.2.2.2.12 Configuring Face Statistics".
Face Enhancement	Click <input type="checkbox"/> to enable face enhancement, to maximize a clear face image when using a low bit stream.
Target Box Overlay	Click <input type="checkbox"/> to enable the function to add a boundary box to the face in the captured picture to highlight the face. The captured face picture is saved in an SD card or the configured storage path. For the storage path, see"6.1 Local".
Face Matting	During the configured period, the duplicate faces will be displayed only once to avoid repeated counting. When selecting Custom , click  , configure the parameters on the prompt interface, and then click Apply . <ul style="list-style-type: none"> • 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 a snapshot; enter the times of the original face height. It ranges from 1-2. • Customized body height: Set body height: in a snapshot; enter the times of the original body height. The range is from 0-4. If the value is 0, it will cut out the face image only.
Snap Mode	<ul style="list-style-type: none"> • Optimized Snapshot: Capture the clearest picture within the configured time after the camera detects a face. • Recognition Priority: Repeatedly compare the captured face to the faces in the armed face database, capture the most similar face image and send the event. It is recommended to use this mode in an access control environment. <p> Click Advanced to set the optimized time.</p>
Property	Click <input type="checkbox"/> next to Property to enable the properties display.
Advanced	<ul style="list-style-type: none"> • Snapshot Angle Filter: Set snapshot angle to be filtered during face detection. • Snapshot Sensitivity: Set snapshot sensitivity during face detection. It is easier to detect faces with higher sensitivity. • Optimized Time: Set a period to capture the clearest picture after the camera detects a face.
Face Exposure	Click <input type="checkbox"/> next to Face Exposure . When a face is detected, the camera can enhance the brightness of the face to make the face image clear.
Face Target	Sets the face target brightness. It is 50 by default.



Brightness	
Face Exposure Detection Interval	Set the face exposure detection interval to prevent image flickering caused by constant adjustment of face exposure. This is five seconds by default.

Result

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 to relevant alarm events. For details, see "6.4.1.3.2 Subscribing Alarm Information".

The face detection result will be displayed on the live interface.

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

8.4 Setting IVS

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

The basic requirements for scene selection are as follows.

- Reduce the complexity of the target area as much as possible.
- If IVS rules are set up on a channel, make sure motion detect/ Intelligent motion detect is disabled on that channel, as having both IVS rules and motion detect enabled on the same channel has been known to cause issues.
- Avoid target areas such as glass, reflective surfaces, water surfaces, heavily wooded locations as well as Insects flying close to the camera lens as these can generate false positive alerts.
- Target areas with a dense amount of target objects is not recommended.
- Target areas should avoid heavy backlit, direct light and locations with frequent illumination changes (shadows, etc).
- Disable Intellistreaming if enabled. Intellistreaming disables features such as IVS rules.
- The recommended target size should be less than 10% of the overall image.
- The minimum recommended target size is 50×50 pixels.
- The target object should be continuously present within the frame for at least two seconds.
- The target object and the background brightness difference should not be less than 10 greyscale.

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 the corresponding relationship between a 2D image captured by the camera and the 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 an installation height of more than three meters. Scenes with a 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 a distorted view, such as the distorted views captured by super-wide-angle or fisheye camera.

Notes

Calibration Drawing

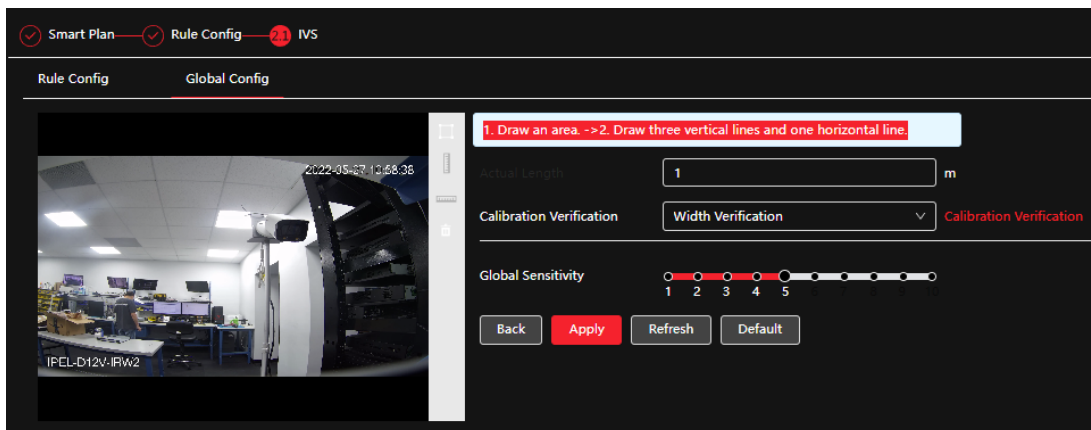
- ◇ Calibration area: The calibration area drawn should be on one horizontal plane.
- ◇ Vertical ruler: The bottom of three vertical rulers should be on the same horizontal plane. Select three reference objects with fixed height in triangular distribution as vertical rulers, such as vehicles parked on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




Result

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.

4. Set the sensitivity.

Adjust the filter sensitivity. With a higher value, it is easier to trigger an alarm when a low-contrast and small objects are captured, but the false detection rate will be greater.

5. Click **Apply**.

- Select the verification type, and then click **Calibration Verification**.
- To verify vertical ruler and horizontal ruler, respectively select **Height Verification** and **Width Verification**.
- Draw a straight line in the image to verify whether the rulers are correctly set.

In the event of a large difference between the estimated and the actual value, 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 the 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 the virtual tripwire from the defined motion direction, the IPC will trigger an event.	Scenes with sparse targets and no occlusion among targets.
Intrusion	When the target enters, leaves, or appears in the detection area, IPC will trigger an event	

Abandoned object	When a (non-human) object is left abandoned in the detection area over a set time, IPC will trigger an event.	<p>Scenes with sparse targets and without obvious and frequent light change. A simple scene in the detection area is recommended.</p> <ul style="list-style-type: none"> • Missed alarms may increase in scenes with dense targets, frequent occlusion, and people staying. • In scenes with complex foreground and background, false alerts may be triggered for abandoned or missing object.
Missing object	When an object is removed from the detection area over a defined time, the IPC will trigger an event.	<p>Scenes with sparse targets and without obvious and frequent light change. A simple scene in the detection area is recommended</p> <ul style="list-style-type: none"> • Missed alarms may increase in the scenes with dense targets, frequent occlusion, and people staying. • In scenes with a complex foreground and background, false alerts may be triggered for the abandoned or missing object.
Fast moving	When an object's speed is greater than the configured speed, the IPC will trigger an event.	<p>A scene with sparse targets and less occlusion. The camera should be installed right above the monitoring area.</p> <p>The light direction should be vertical to the motion direction.</p>
Parking detection	When a target vehicle stays at an area over the configured time, the IPC will trigger an event.	Road monitoring and traffic management.
Crowd gathering	When a crowd gathers or the crowd density is greater than the configured value, the IPC will trigger an	Scenes with medium or long distances, such as outdoor plazas, government entrance, station entrance, and exit. It is not suitable for short viewing angles.

	event.	
Loitering detection	When a target loiters over the minimum alarm time, the IPC will trigger an event. After the event is triggered, if the target stays in the area within the time interval of alarm, the event will be triggered again.	Scenes such as parking lots and storefronts.

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

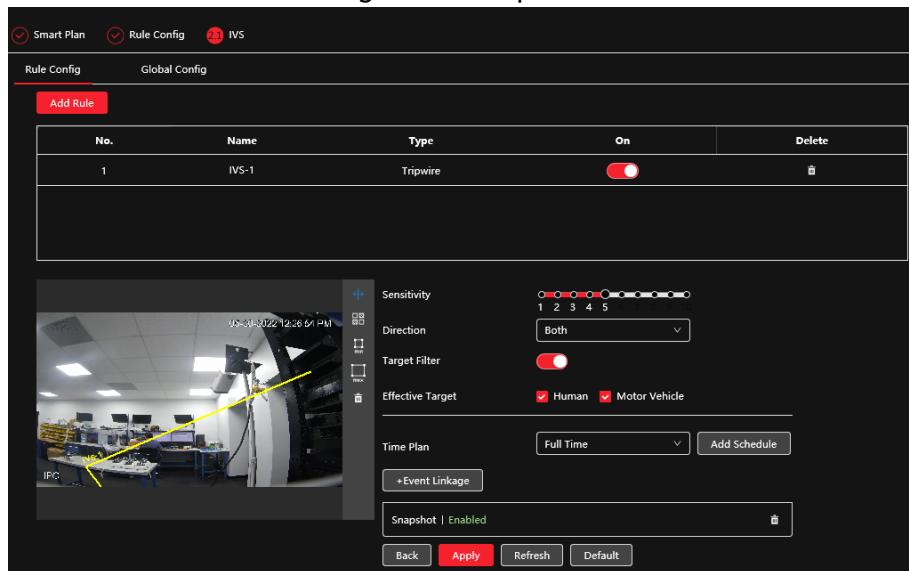
Step 1 Select **AI > Smart Plan**.

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 to edit the rule name; the rule is enabled by default.

Figure 8-22 Tripwire



Step 5 Click to draw the 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	<p>Draw a detection area.</p> <ul style="list-style-type: none"> During the detection of an abandoned object, the alarm is also triggered if a pedestrian or vehicle stays for a long time. If the abandoned object is smaller than the pedestrian and vehicle, set the target size to filter pedestrian and vehicle or properly extend the duration to avoid false alarm triggered by the transient staying of a pedestrian. During the detection of crowd gathering, a false alarm may be triggered by low installation height, a large percentage of a 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 a retractable door, or dense traffic or people flow.
Abandoned object	
Missing object	
Fast-moving	
Parking detection	
Crowd gathering	
Loitering detection	

Step 6 (Optional) Click other icons on 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 a 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 will be displayed.
- Click  to delete the detection line.

Step 7 Set rule parameters for IVS.

Table 8-9 Description of IVS parameters

Parameter	Description
Direction	<p>Set the direction of rule detection.</p> <ul style="list-style-type: none"> When setting tripwire, select A->B, B->A, or A<->B. When setting intrusion, select Enter, Exit, or Both.
Action	<p>When setting intrusion action, select Appears or Cross.</p>
Target Filter	<p>Click  to enable this function.</p> <ul style="list-style-type: none"> When you select Human as the target, an event will be triggered when the system detects that persons trigger the rule. When you select Motor Vehicle as the target, an event will be triggered when the system detects that vehicle triggers the rule.

Duration	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 to a relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.5 Setting Video Metadata

Metadata allows for classifying people, non-motor vehicles, and motor vehicles in the captured video. The relevant attributes can be displayed on the live interface.

8.7.1 Global Configuration

Set the global configuration of video metadata, including the 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

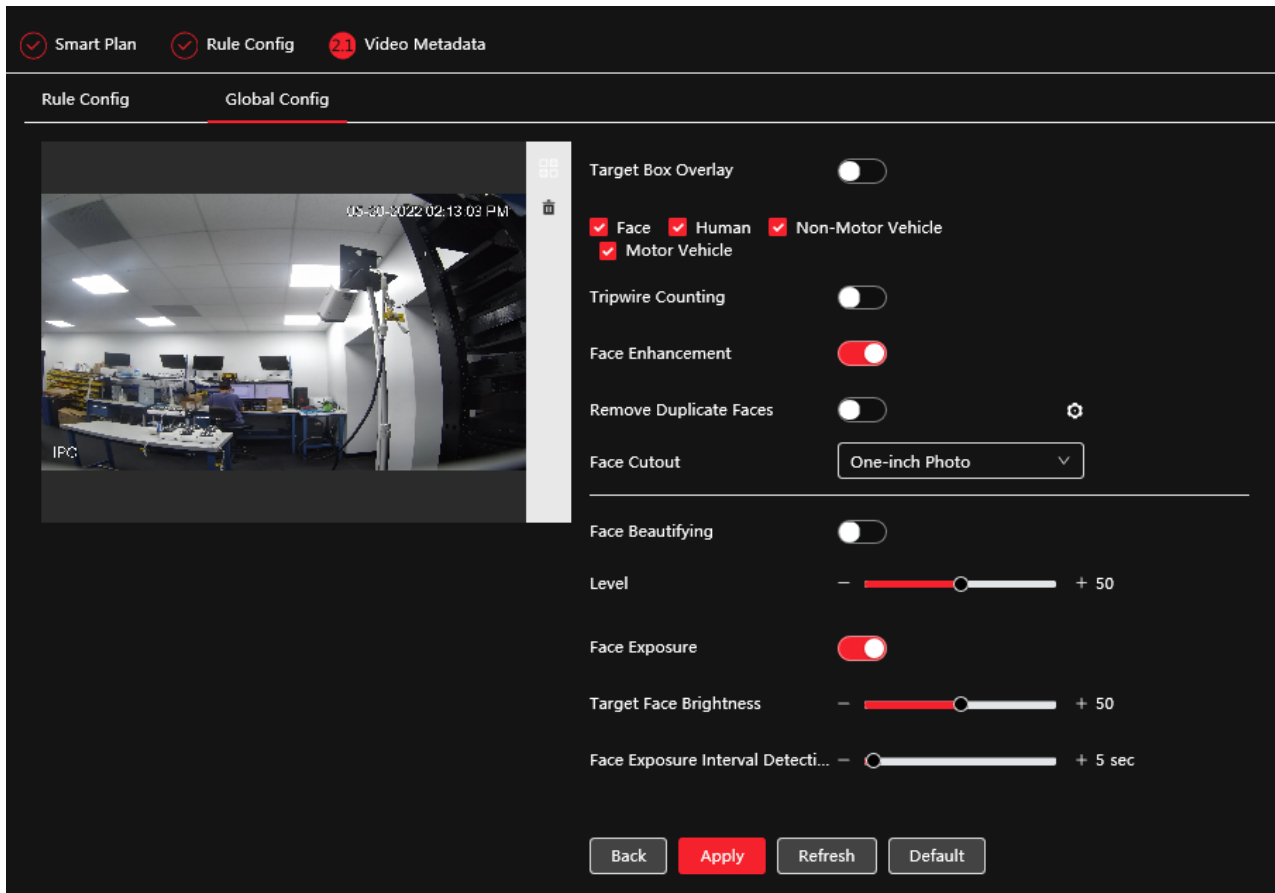





Table 8-13 Description of scene set parameters (video metadata)

Parameter	Description
Privacy Protection	Enable this function, and the faces and bodies will be blurred by mosaic or color blocks when they are detected.
Target Box Overlay	<p>Overlay the target box on the captured pictures to mark the target position.</p> <p>Four types of target boxes are supported. Select the target box as necessary.</p> <p>The captured pictures are stored on an SD card or the configured storage path. For details, see "6.1 Local".</p>
Tripwire Counting	<p>Enable this function and set the tripwire direction. The snapshot mode is Tripwire by default, and you cannot change it.  will be displayed beside the image on the Rule Config interface. You can draw the rule as necessary.</p>
Face Enhancement	Click  next to Face Enhancement to preferably guarantee a clear face if using a low bit stream.

Remove Duplicate Faces	<p>During the configured period, the face that was detected several times will be displayed only once, to avoid repeated counting. Click  to set the parameters, and then click Apply.</p> <ul style="list-style-type: none"> • Time: The function is valid within the configured period. • Precision: the greater the value, the higher the accuracy will be.
Face Matting	Set a range for matting face images, 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 the face clearer by adjusting the 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 vehicles, and motor vehicles.

Prerequisites

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

Procedure

Step 1 Select **AI > Smart Plan**

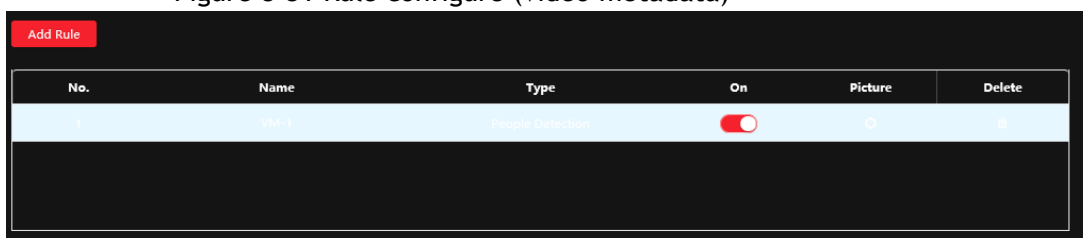
Step 2 Click  next to **Video Metadata**, and then click **Next**.




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)



No.	Name	Type	On	Picture	Delete
1	VM-1	People Detection			

Step 5 Configure **Picture**.


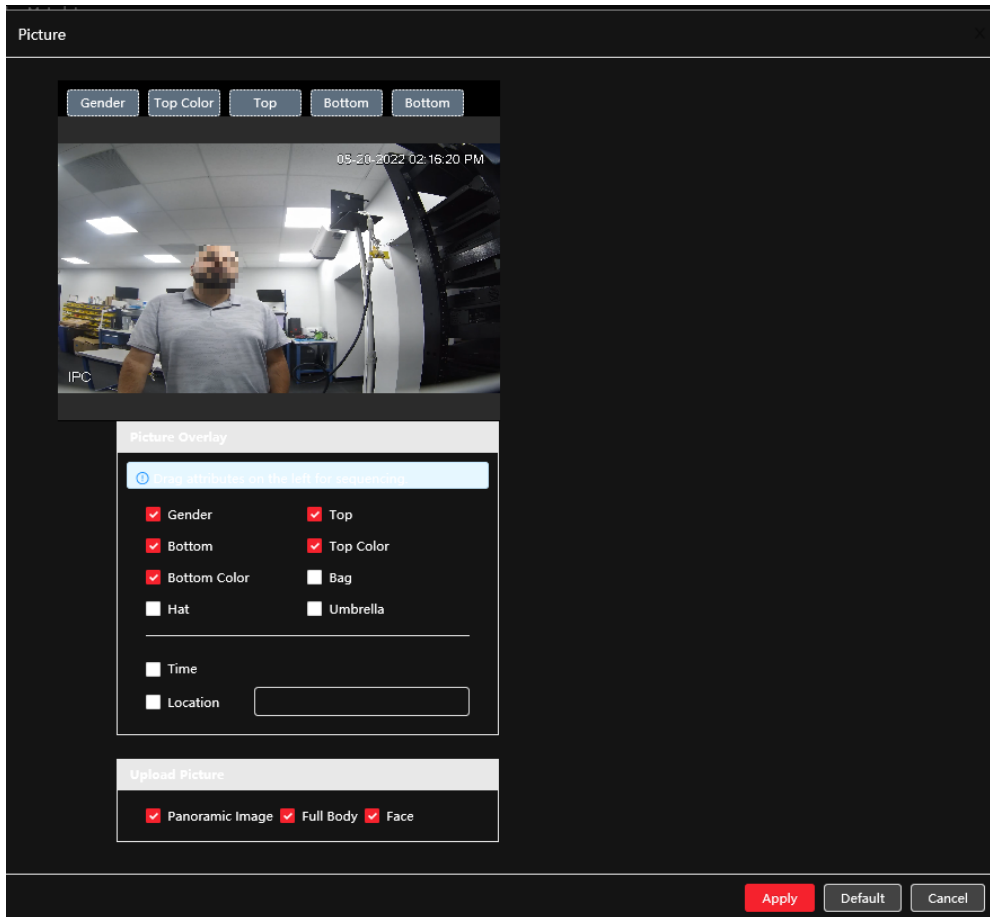







- 1) Click .
- 2) Set overlay of motor vehicle, non-motor vehicle, and people and the box position. This section takes the configuration of non-motor vehicle overlay as an example.

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 will be displayed. Click , and you 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.
- 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 will be 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 <input type="checkbox"/> next to People Flow Statistics to count the number of people in the detection area.
Flow Statistics (Non-motor Vehicle)	Click <input type="checkbox"/> next to Flow Statistics (Non-motor Vehicle) to count the number of non-motor vehicles in the detection area.
Traffic Flow Stat	Click <input type="checkbox"/> next to Traffic Flow Statistics to count the number of motor vehicles in the detection area.
OSD	Click OSD Info , and the Overlay interface will be displayed. Click <input type="checkbox"/> next to Enable to enable the target statistics function. For details, see "6.2.2.2.8 Configuring Target Statistics".
Snapshot Mode	<ul style="list-style-type: none"> • 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. <ol style="list-style-type: none"> 1. Select Tripwire. 2. Select the direction from A to B, B to A, and Both. 3. Adjust the position of rule line as necessary.

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 to the 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.

8.6 Setting People Counting

The People counting function includes 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 event 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 counted number of people who enter, leave, or stay in the area exceeds the configured value, an event 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 the counted 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**

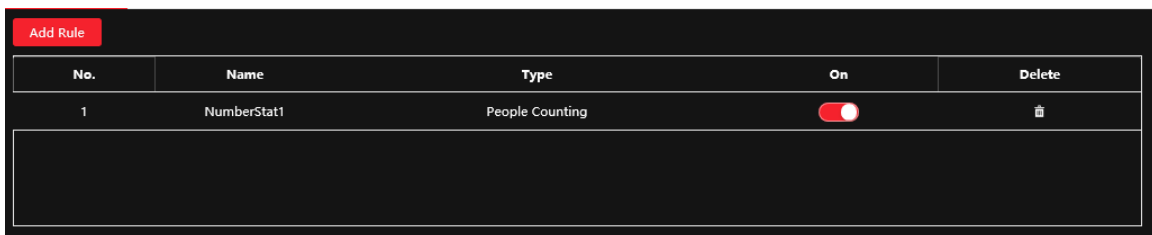
Step 2 Click next to **People Counting**, and then click **Next**.

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

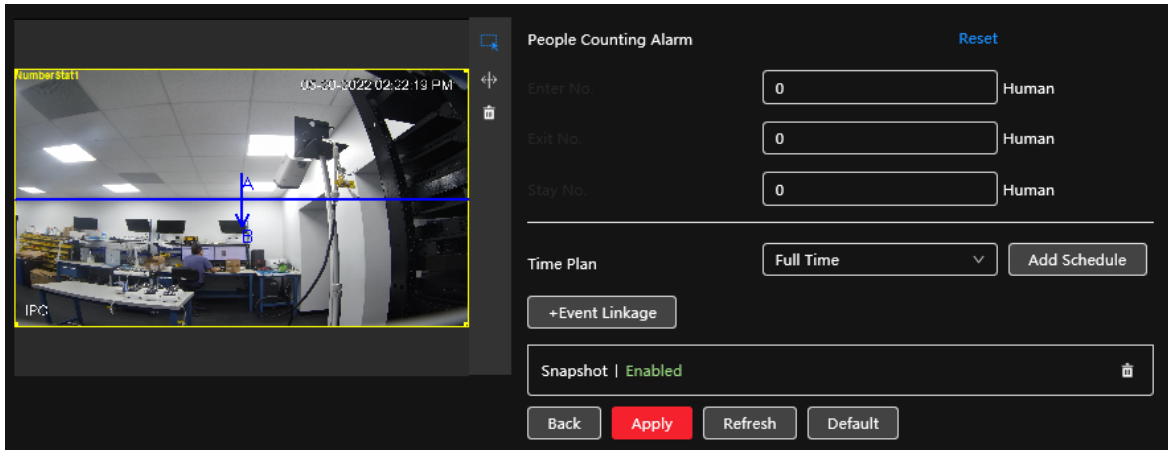


No.	Name	Type	On	Delete
1	NumberStat1	People Counting	<input checked="" type="checkbox"/>	

Step 5 Draw a detection area in the image.

- People counting
 1. Click , and drag any corner of the box to adjust the size of the area, click the right mouse button and move the box to adjust the position.
 2. Click to draw a 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


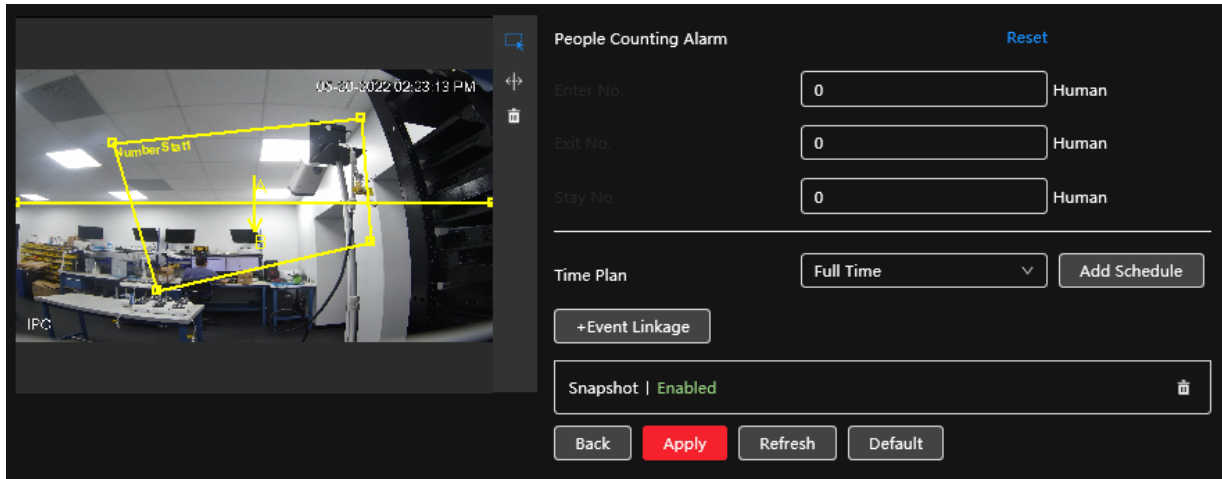
Click , and drag any corner of the box to adjust the size of the area, and press the right mouse button and move the box to adjust the position.

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	Area people counting	Enable the area people counting function.

counting	
Inside Number	Set the number of people in the people counting region. When the people count reaches the configured value, an alarm will be triggered.
Type	When you set the inside the number to 0, and select \geq Threshold in Type , the system will not perform the alarm linkage.
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	

Result

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 to the relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

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

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

Figure 8-37 Counting result



8.8.2 Queuing

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

Figure 8-38 Add rule

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

Step 5 Draw a detection area in the image.


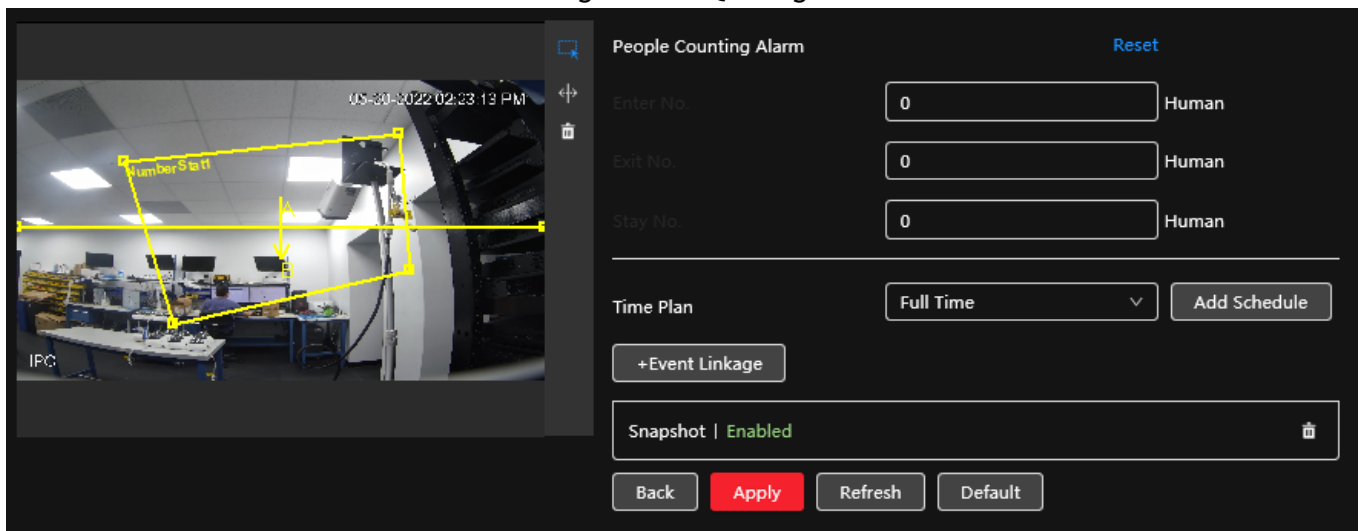
Click  to draw the detection area, and press the right mouse button to complete the drawing.

Figure 8-39 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.

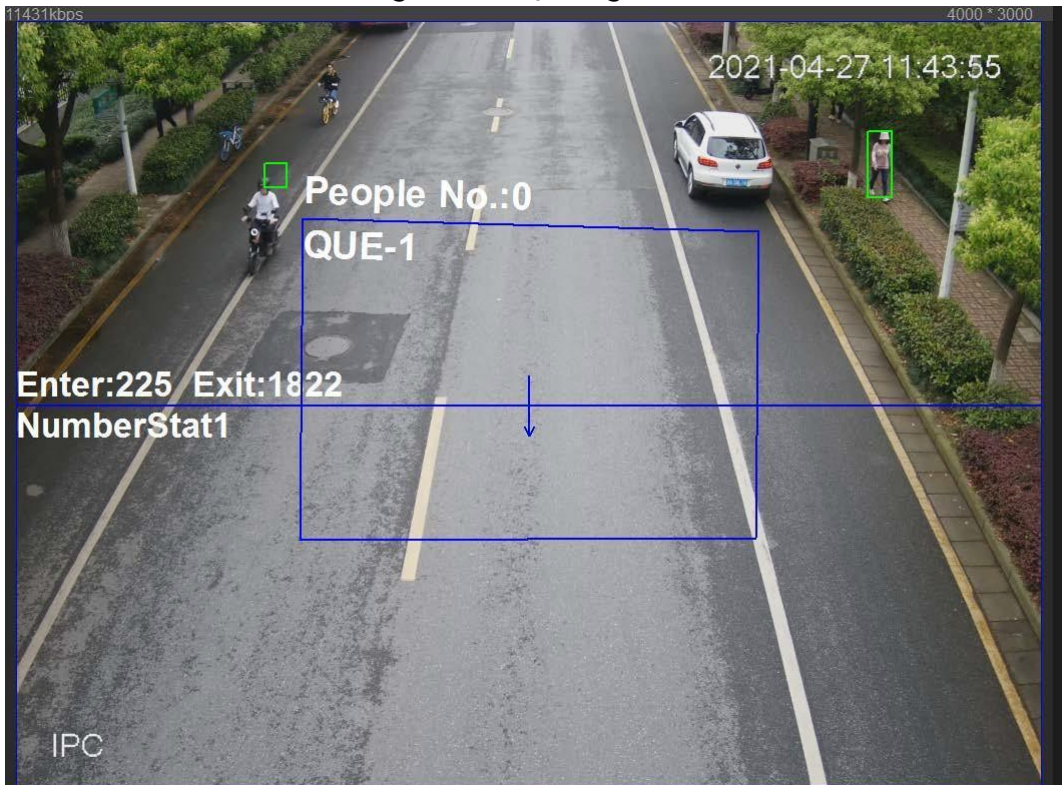
Step 8 Click **Apply**.

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

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 the people counting rule.

Procedure

Step 1 Select **AI > Smart Plan**

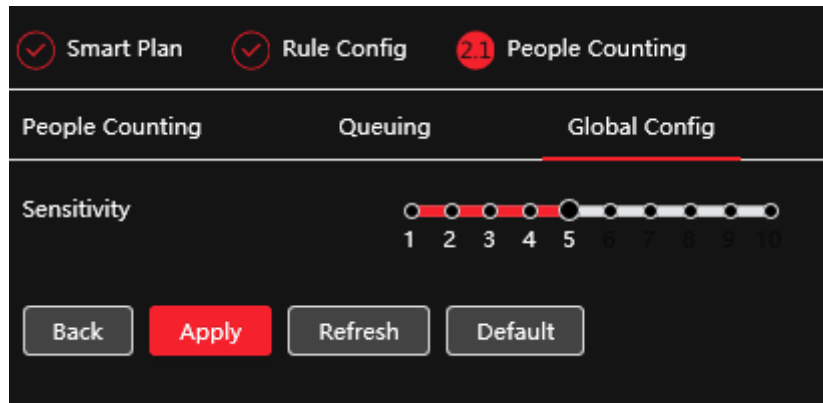
Step 2 Click next to **People Counting**, and then click **Next**.

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

Step 4 Set the sensitivity.

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

Figure 8-41 Global configuration



Step 5 Click **Apply**.

8.7 Face & Body Detection

After enabling this function, the camera detects faces and the 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

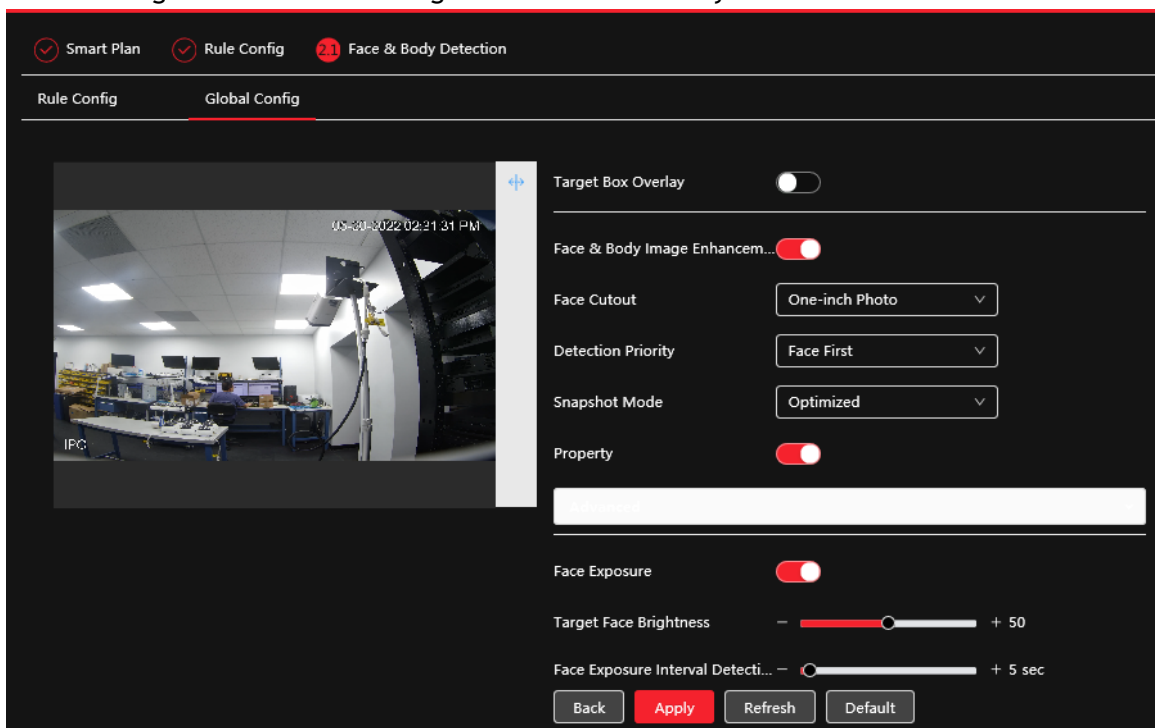





Table 8-17 Description of scene set parameters (face & body detection)

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	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● 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, and motor vehicles.

Prerequisites

- Select **AI > Smart Plan**, and enable **Face & Body Detection**.
- You have configured the parameters on the **Global Config** interface.

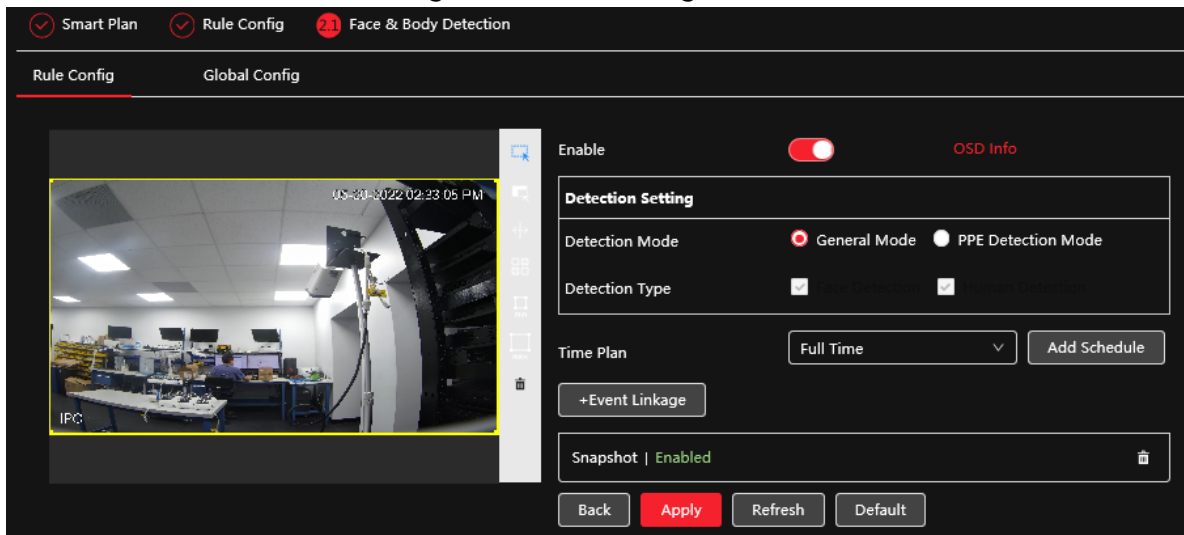
Procedure

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 on the right side of the image to draw the 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 a 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 will be displayed.
- Click  to delete the detection line.

Step 6 (Optional) Set OSD information.

Click **OSD Info**, and the **Overlay** interface will be displayed, and then enable the face & body counting function. The number of detected faces and bodies will be 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 helmets, 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 to the relevant alarm event. For details, see "6.4.1.3.2 Subscribing Alarm Information".

8.8 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.

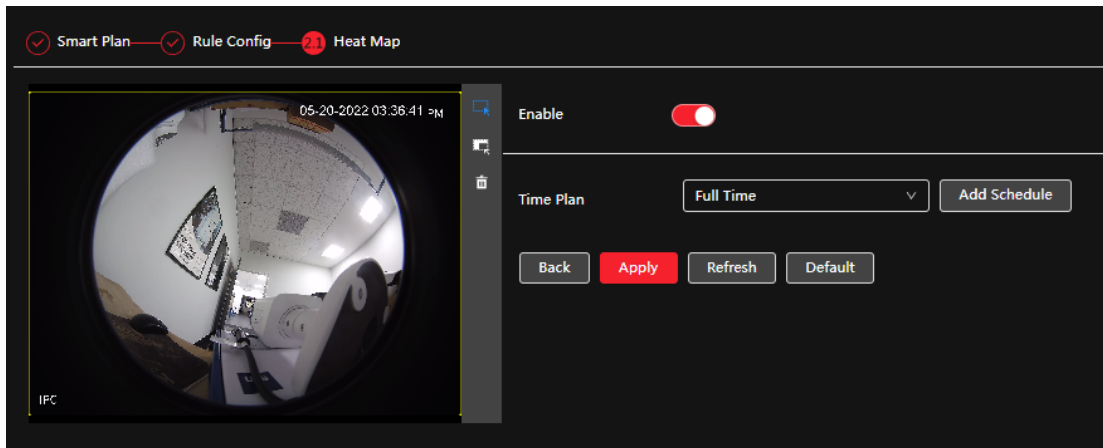
Procedure

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**.


8.9 Setting ANPR

When this function is enabled, if a motor vehicle triggers the rule line in the detection area, the IPC will capture the license plate and report the attributes of the motor vehicle.

8.11.1 Rule Configuration

When a motor vehicle triggers 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)

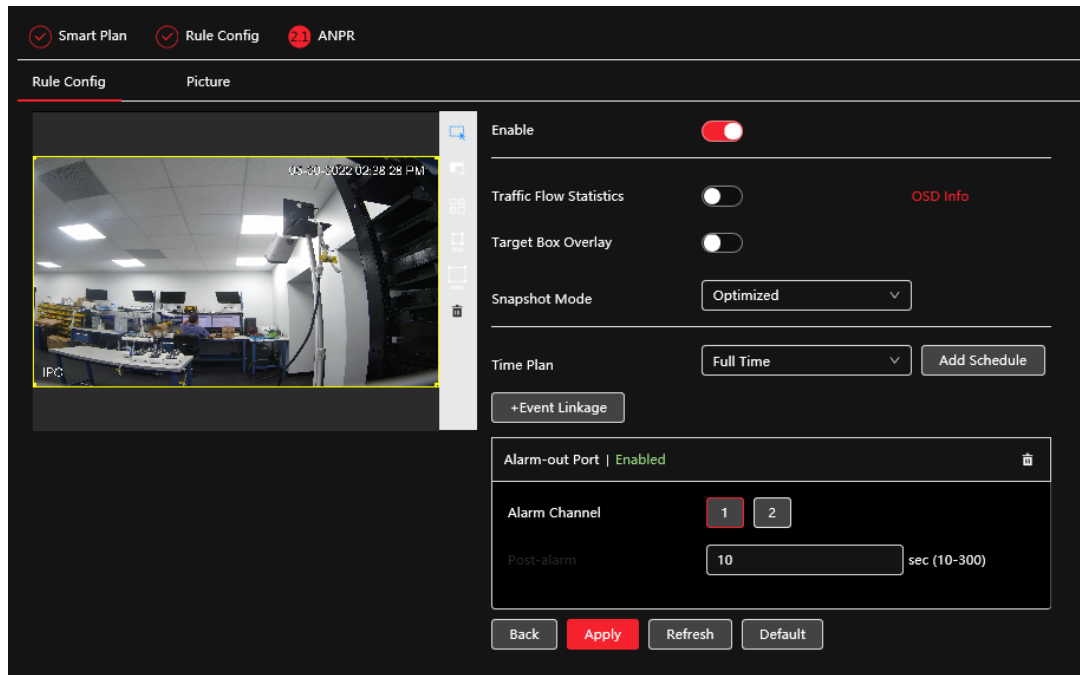
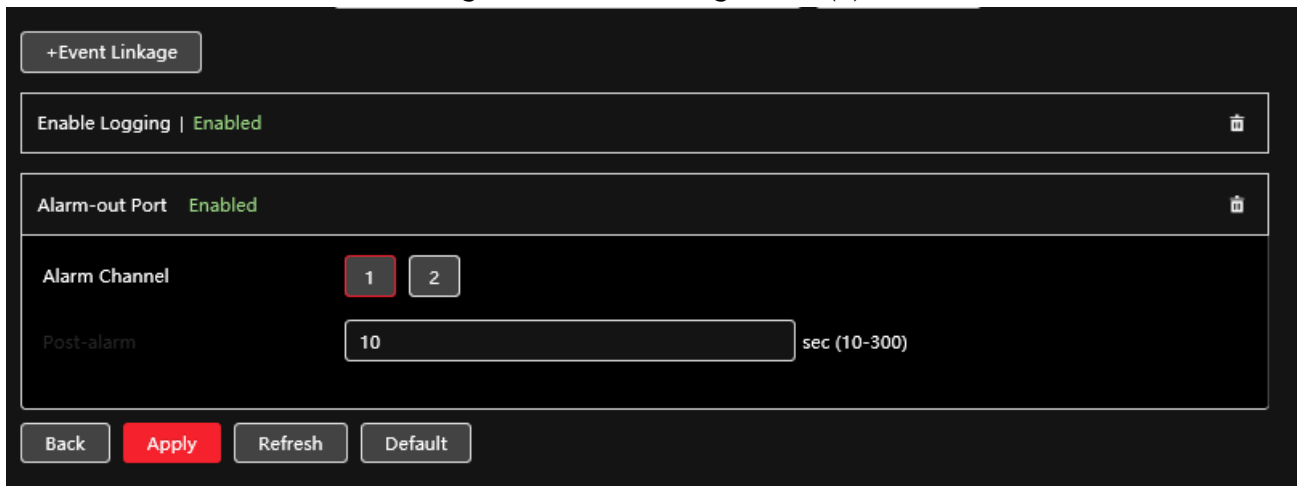


Figure 8-47 Rule configuration (2)



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 a linked event, which supports recording, sending 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 necessary.

Step 9 Click **Apply**.

9 Security

9.1 Security Status

Background Information

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

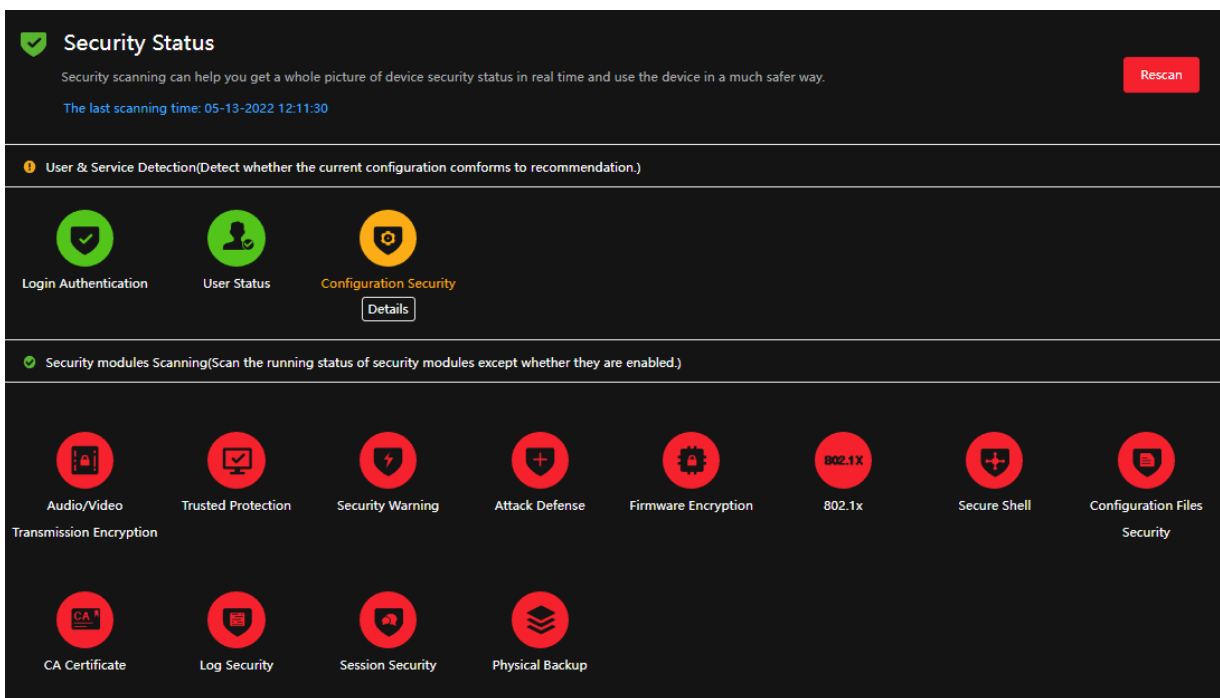
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to a recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing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

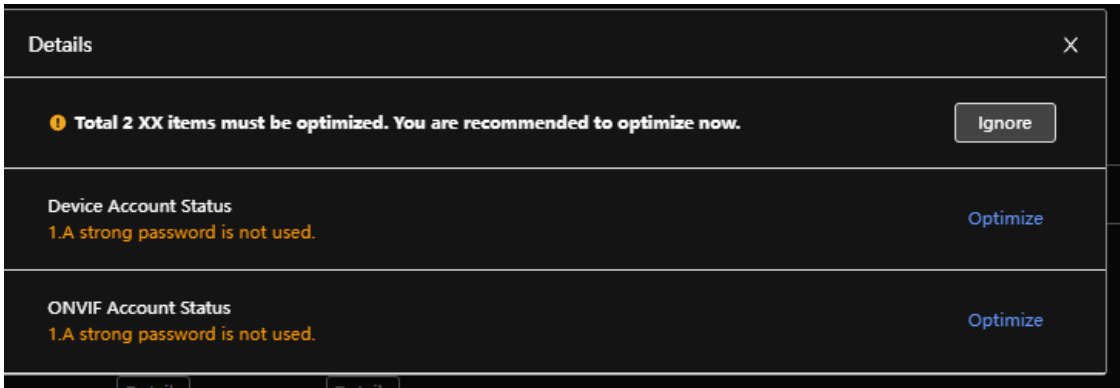


Related Operations

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

1. Click **Details** to view the details of the scanning result.
2. Click **Ignore** to ignore the exception, and it will not be scanned in the next scanning. Click **Joint Detection**, and the exception will be scanned in the next scanning.
3. Click **Optimize**, and the corresponding interface will be 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 necessary and click to enable it.

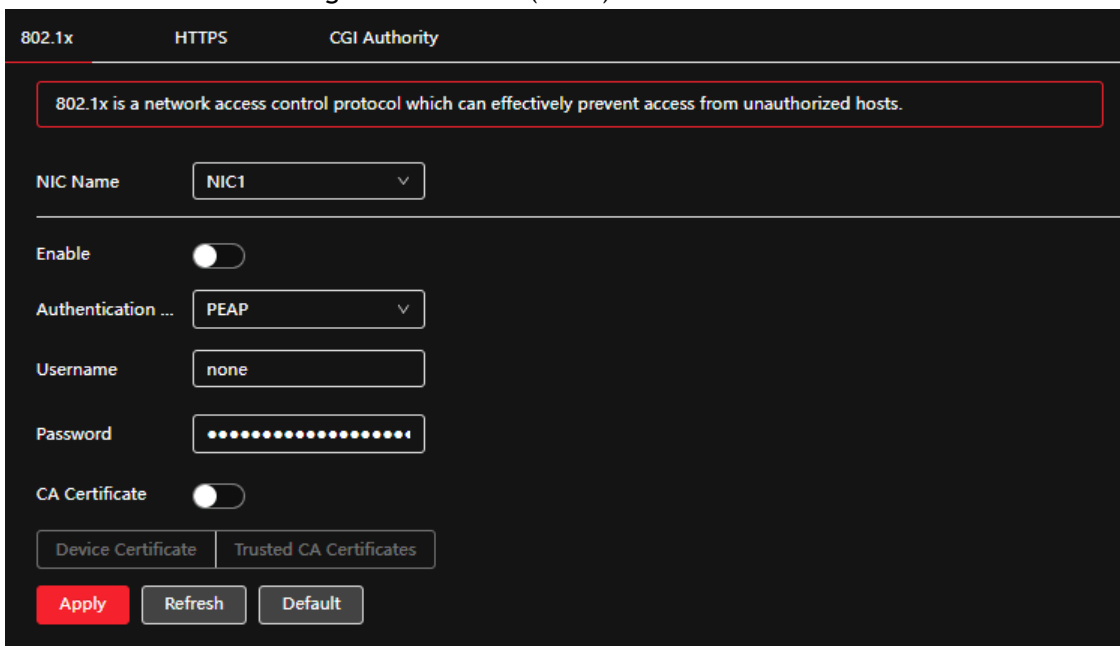
Step 3 Select the authentication mode and then configure parameters.

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

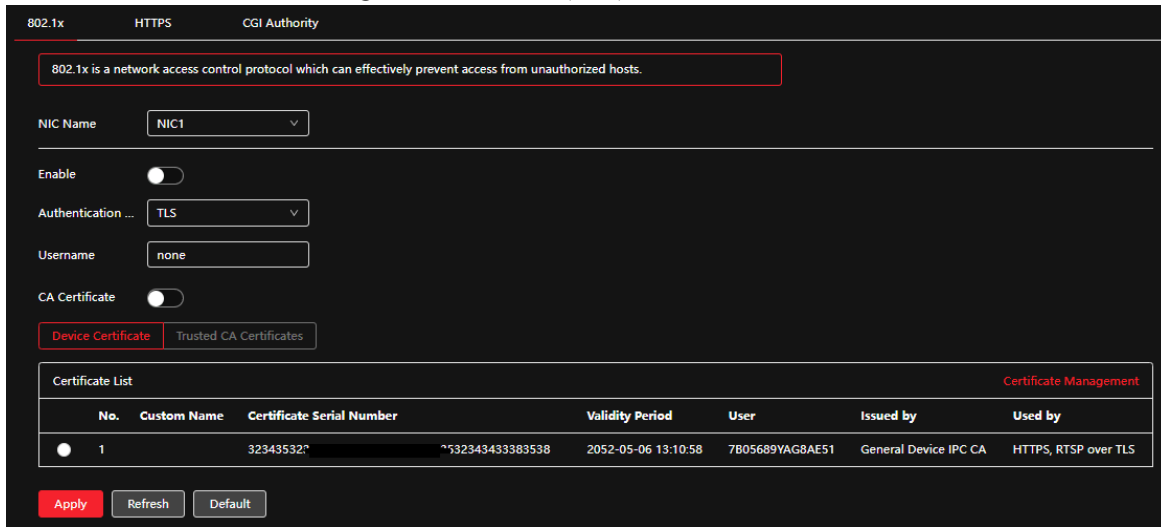
guarantee the security and integrity of the data.

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



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

Figure 9-4 802.1x (TLS)



802.1x is a network access control protocol which can effectively prevent access from unauthorized hosts.

NIC Name:

Enable:

Authentication:

Username:

CA Certificate:

Device Certificate | Trusted CA Certificates

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
1		32343532?*	2052-05-06 13:10:58	7805689YAG8AE51	General Device IPC CA	HTTPS, RTSP over TLS

Apply Refresh Default

Step 4 Click **Apply**.

9.2.2 HTTPS

This section allows you to create a certificate or upload an authenticated certificate to log in through HTTPS with your PC. HTTPS can protect page authenticity on all types of websites, secure accounts, and keep user communications, identity, as well as web browsing privacy.

Procedure

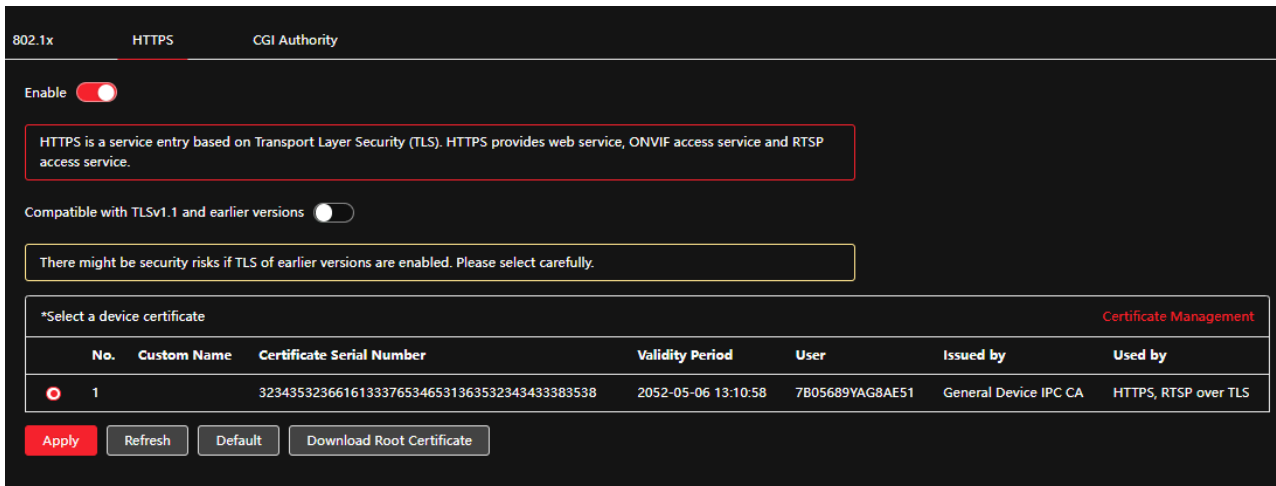
Step 1 Select **Security > System Service > HTTPS**. **Step 2** Click to enable it.

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

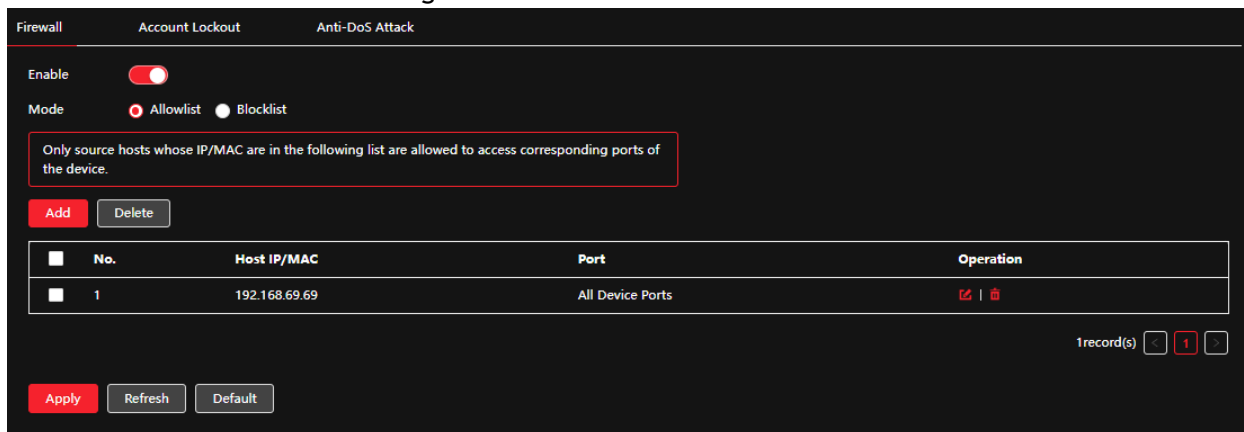
9.3.1 Firewall

This section allows for configuring the firewall to limit network 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 the IP/MAC devices in the allow list are allowed to access the camera. The ports are the same.
- **Blocklist:** If the IP/MAC of a device is in the block list, those devices cannot access the camera. The 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



The screenshot shows a dark-themed 'Add' dialog box. The title bar contains the text 'Add' and a close icon. The main area has the following elements:

- 'Add Mode': A dropdown menu with 'IP' selected.
- 'IP Version': A dropdown menu with 'IPv4' selected.
- 'IP Address': An empty text input field with a red border.
- 'All Device P...': A red toggle switch that is currently turned on.

At the bottom right, there are two buttons: a red 'OK' button and a grey 'Cancel' button.

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 the device account and ONVIF user.

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

Figure 9-8 Account lockout

The screenshot shows the 'Account Lockout' configuration page. It has three tabs: 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Account Lockout' tab is active. Under the heading 'Device Account', there are two rows of settings. The first row is for 'Device Account' with 'Login Attempt' set to '5time(s)' and 'Lock Time' set to '5 min'. The second row is for 'ONVIF User' with 'Login Attempt' set to '30time(s)' and 'Lock Time' set to '5 min'. At the bottom, there are three buttons: 'Apply' (highlighted in red), 'Refresh', and 'Default'.

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 (Denial of Service) attacks.

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

The screenshot shows the 'Anti-DoS Attack' configuration page. It has three tabs: 'Firewall', 'Account Lockout', and 'Anti-DoS Attack'. The 'Anti-DoS Attack' tab is active. There are two sections, each with a toggle switch and a descriptive text box. The first section is 'SYN Flood Attack Defense' with a toggle switch that is currently off. The text box below it reads: 'An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.' The second section is 'ICMP Flood Attack Defense' with a toggle switch that is currently off. The text box below it reads: 'An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.' At the bottom, there are three buttons: 'Apply' (highlighted in red), 'Refresh', and 'Default'.

9.4 CA Certificate

9.4.1 Installing Device Certificate

Create a certificate or upload an authenticated certificate to 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.

Step 2: Fill in certificate information. X

Custom Name

* IP/Domain Na... 192.168.1.147

Organization U...

Organization

* Validity Period Days (1~5000)

* Region

Province



City Name

Back Create and install certificate Cancel

Step 5 Click **Create and install a 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

This section allows you to 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.

Step 2: Fill in certificate information. X

* IP/Domain Na... 192.168.1.147

Organization U...

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

Back Create and Download Cancel

Step 5 Click **Create and Download**.

Save the requested file to your PC.

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



Step 7 Import the signed CA certificate.

- 1) Save the CA certificate to the PC.
- 2) Do Step 1 to Step 3, and click **Browse** to select the signed CE certificate.
- 3) Click **Install and Import**.

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

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

Related Operations

- Click **Enter Edit Mode**; you then 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 applying for the third-party certificate, you will also need to apply for the private key file and private key password.

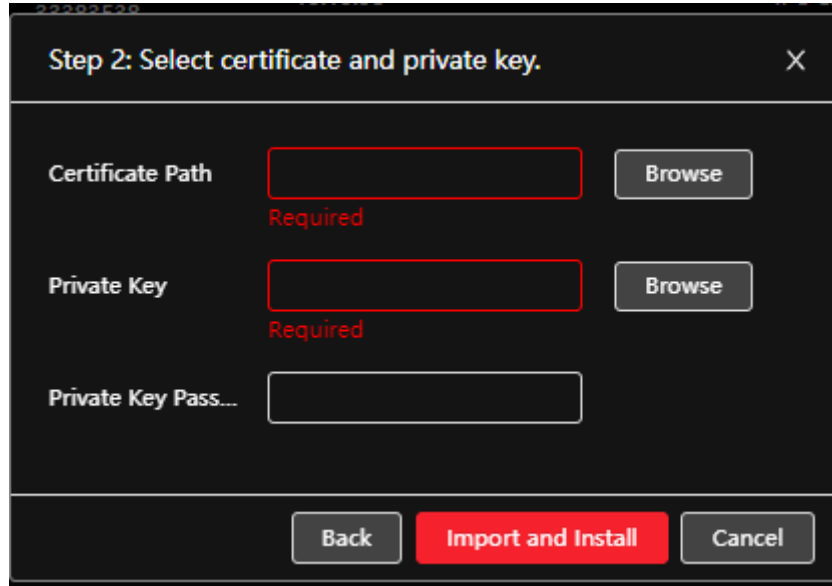
Step 1 Select **Security > CA Certificate > Device Certificate**.

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



The dialog box titled "Step 2: Select certificate and private key." contains three input fields: "Certificate Path", "Private Key", and "Private Key Pass...". Each of the first two fields has a "Browse" button to its right. Below the "Certificate Path" and "Private Key" fields, the word "Required" is written in red. At the bottom of the dialog, there are three buttons: "Back", "Import and Install" (highlighted in red), and "Cancel".

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

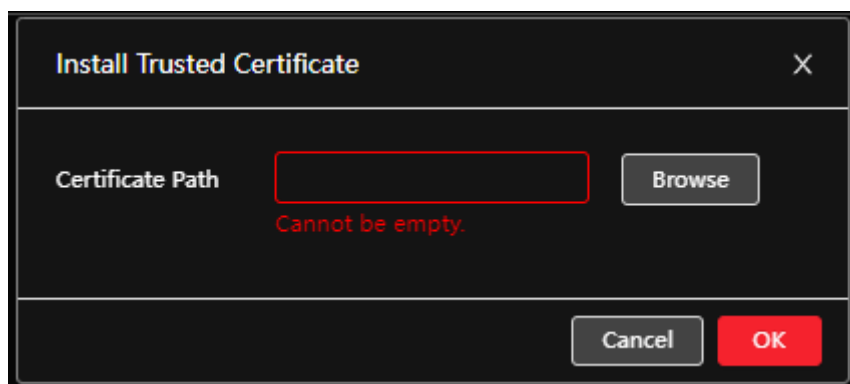
A CA certificate is a digital certificate for the legal identity of the camera. For example, when the camera accesses the LAN through 802.1x, the CA certificate is required.

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





The dialog box titled "Install Trusted Certificate" contains one input field: "Certificate Path". To the right of this field is a "Browse" button. Below the "Certificate Path" field, the text "Cannot be empty." is written in red. At the bottom of the dialog, there are two buttons: "Cancel" and "OK" (highlighted in red).

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

Some IP Camera models support audio and video encryption during data transmission.



You are recommended to enable A/V Encryption function. There may be a 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

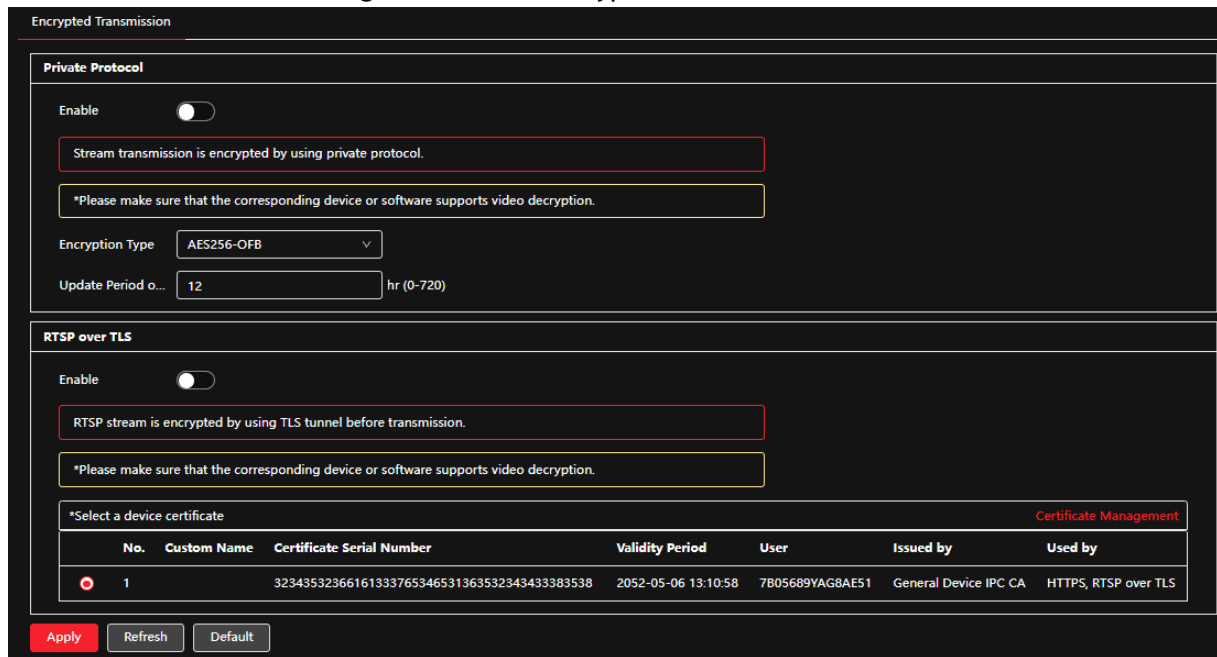




Table 9-1 A/V encryption parameter

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using the private protocol.  There may be a security 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. Setting to 0 will never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS.  There may be security 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

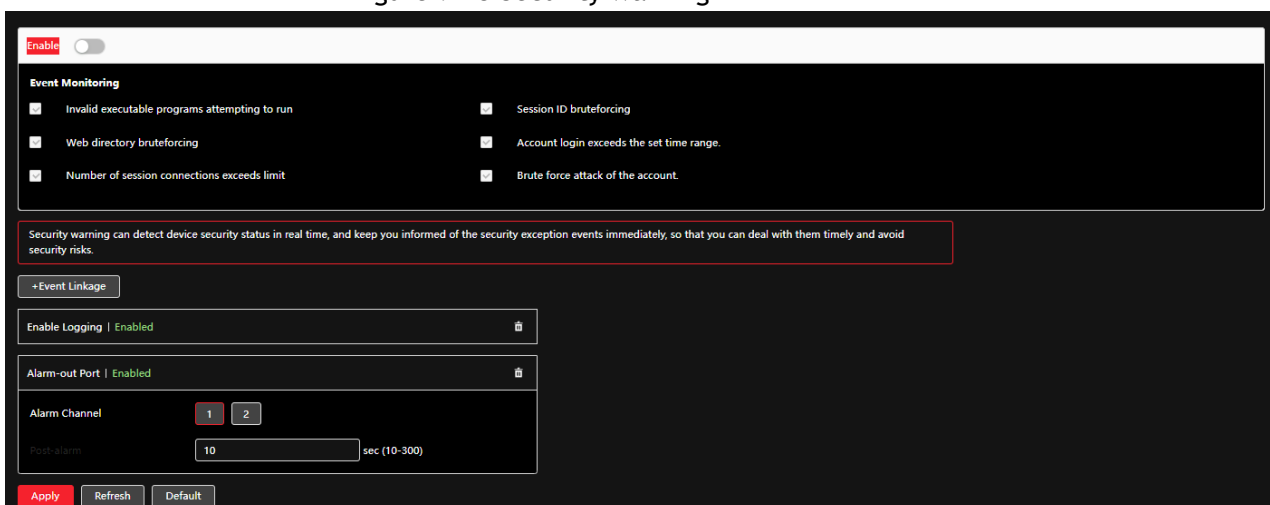
When a security exception event is detected, the camera sends a warning to remind you to process it quickly, to avoid security risks.

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

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

This section introduces the functions and operations of video playback. Note that the IP Camera will need to be equipped with micro SD storage media to record video/ images.

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 an SD card.
- Before playing back the video, configure the 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**.

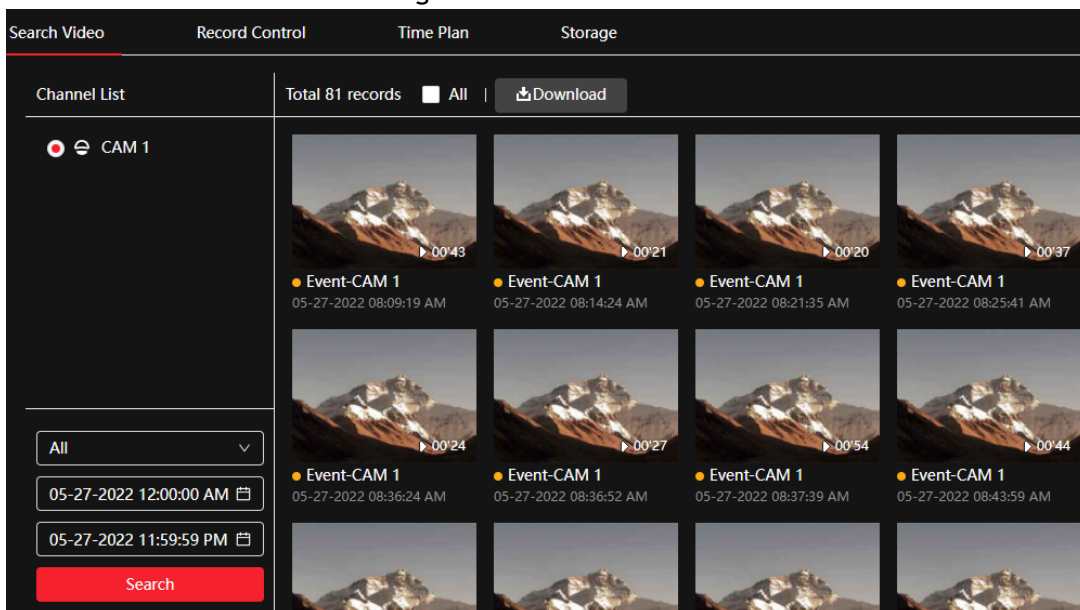
Step 2 Select the channel, the record type, and record time, and then click **Search**.

- Click **All**, and select the record type from the drop-down list, Options include **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 will be displayed.

Figure 10-2 Video playback

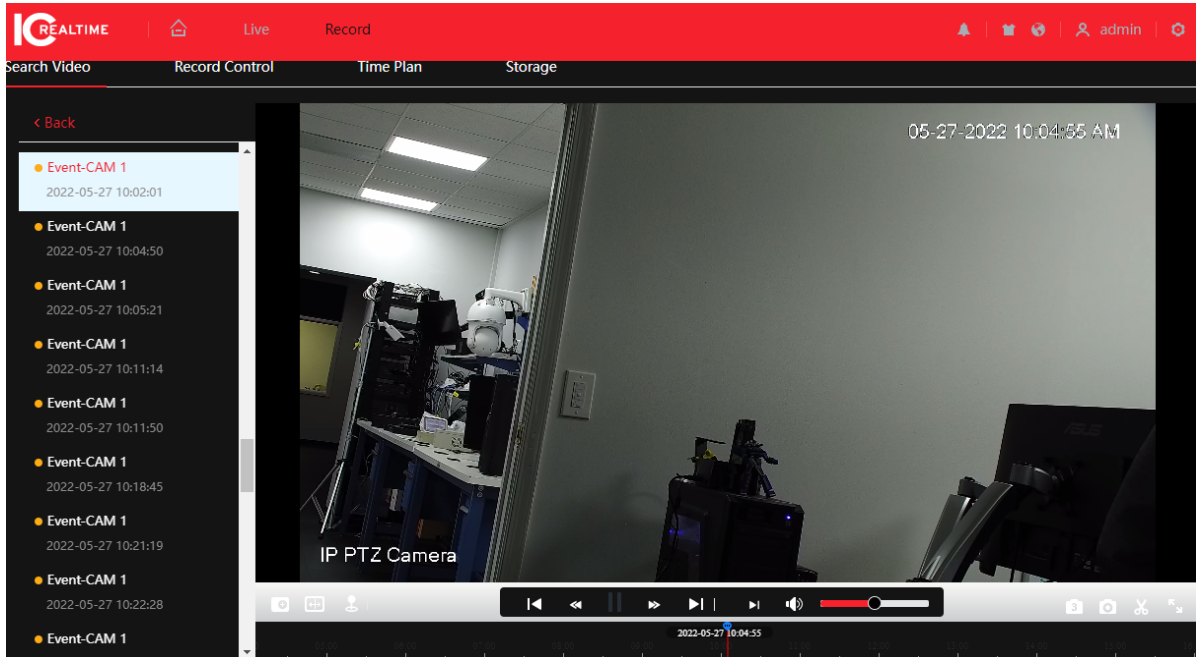





Table 10-1 Description of video playback interface

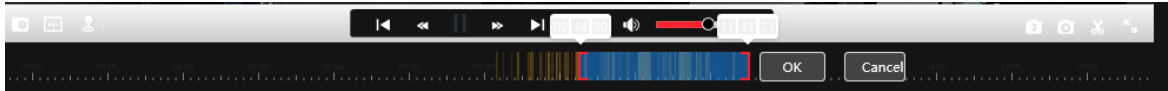
No	Function	Description
1	Recorded video list	Displays all searched recorded video files. Click any files to play back the file. Click Back at the upper-left corner to go to the Search Video interface.
2	Digital Zoom	You can zoom the video image of the selected area through two operations. <ul style="list-style-type: none"> 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 are valid only when you enabled the rule during recording.

No	Function	Description
	Play control bar	<p>Controls playback.</p> <ul style="list-style-type: none"> ◀: 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. <p>The icon changes to ▶, click the icon to play back recorded videos.</p> <ul style="list-style-type: none"> ⏭: 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.
	Sound	<p>Controls the sound during playback.</p> <ul style="list-style-type: none"> 🔇: Mute mode. 🔊: Vocal state. You can adjust the sound.
	Snapshot	<p>Click 📷 to capture one picture of the current image, and it will be saved to the configured storage path.</p> <p>📖</p> <p>About viewing or configuring storage path, see "6.1 Local".</p>
	Video clip	<p>Click 📏, and clip a certain recorded video and save it. For details, see "10.1.2 Clipping Video".</p>
	Full Screen	<p>Click 🖥, and the image will be displayed in full-screen mode; double-click the image or press Esc button to exit full-screen mode.</p>
3	Progress bar	<p>Displays the record type and the corresponding period.</p> <ul style="list-style-type: none"> 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

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

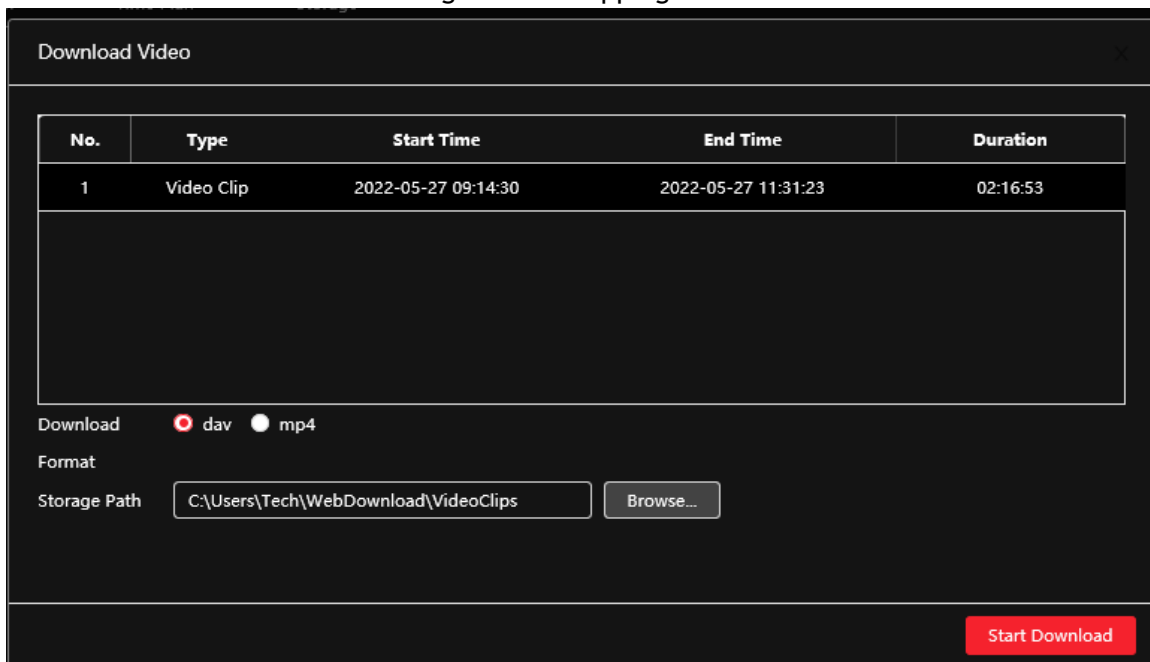
Figure 10-3 Clipping video



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

You can download videos to a defined path on a computer. You can download a single video, or in batches.



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

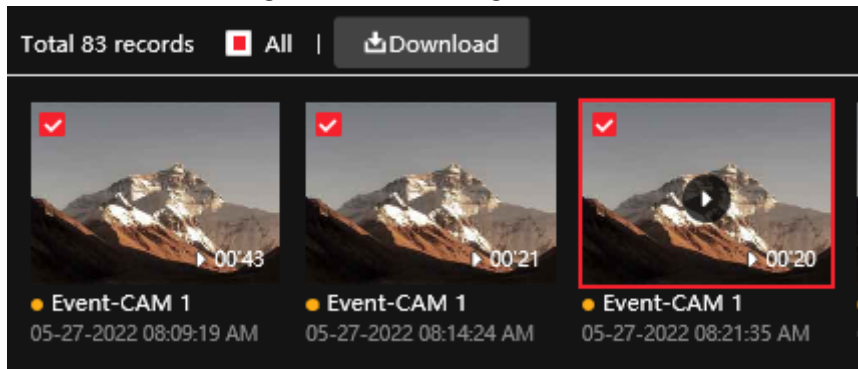
Step 1 Select **Record > Search Video**.

Step 2 Select the channel, the record type, record time, then 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.

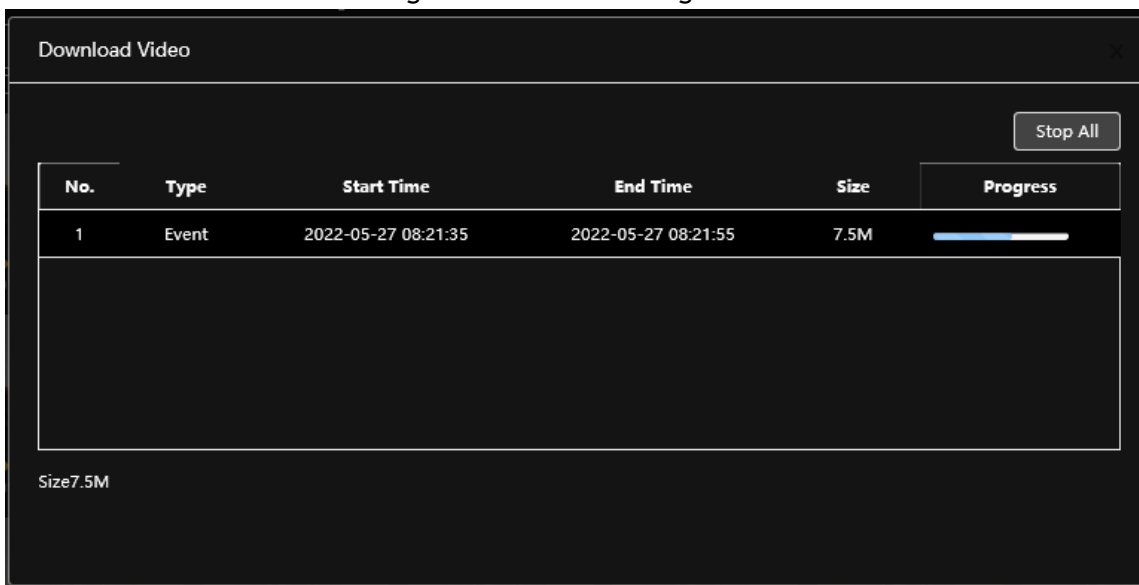
Figure 10-5 Selecting video file



Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 10-6 Downloading video



Step 6 Click **Start Download**.

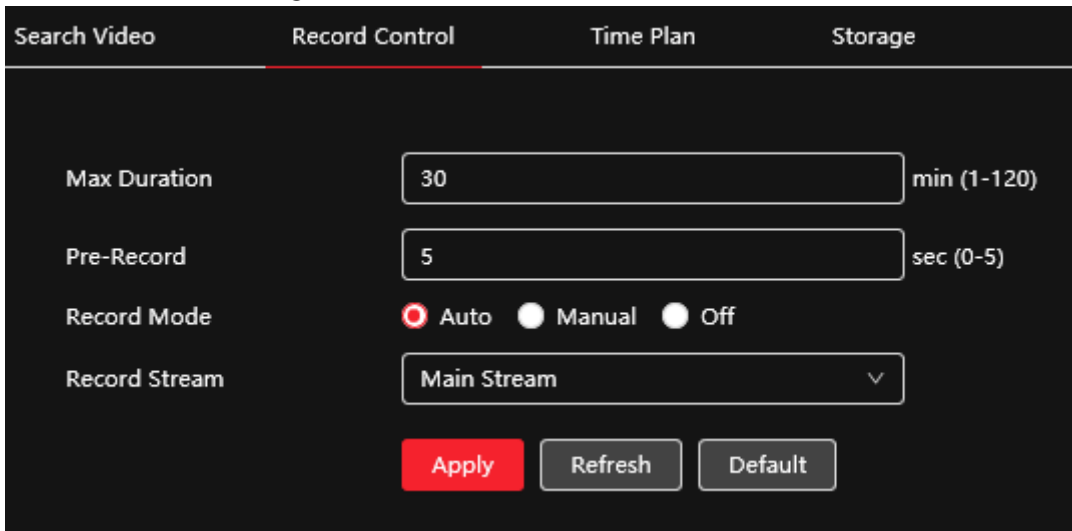
The downloaded files are saved in the configured storage path. For details of storage path, see "6.1 Local".

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




The screenshot shows a dark-themed interface with four tabs: Search Video, Record Control (active), Time Plan, and Storage. Under the Record Control tab, there are four settings:

- Max Duration:** A text input field containing '30' with a unit label 'min (1-120)' to its right.
- Pre-Record:** A text input field containing '5' with a unit label 'sec (0-5)' to its right.
- Record Mode:** Three radio buttons labeled 'Auto', 'Manual', and 'Off'. The 'Auto' radio button is selected.
- Record Stream:** A dropdown menu showing 'Main Stream' with a downward arrow.

At the bottom of the interface are three buttons: 'Apply' (red), 'Refresh' (grey), and 'Default' (grey).

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 .

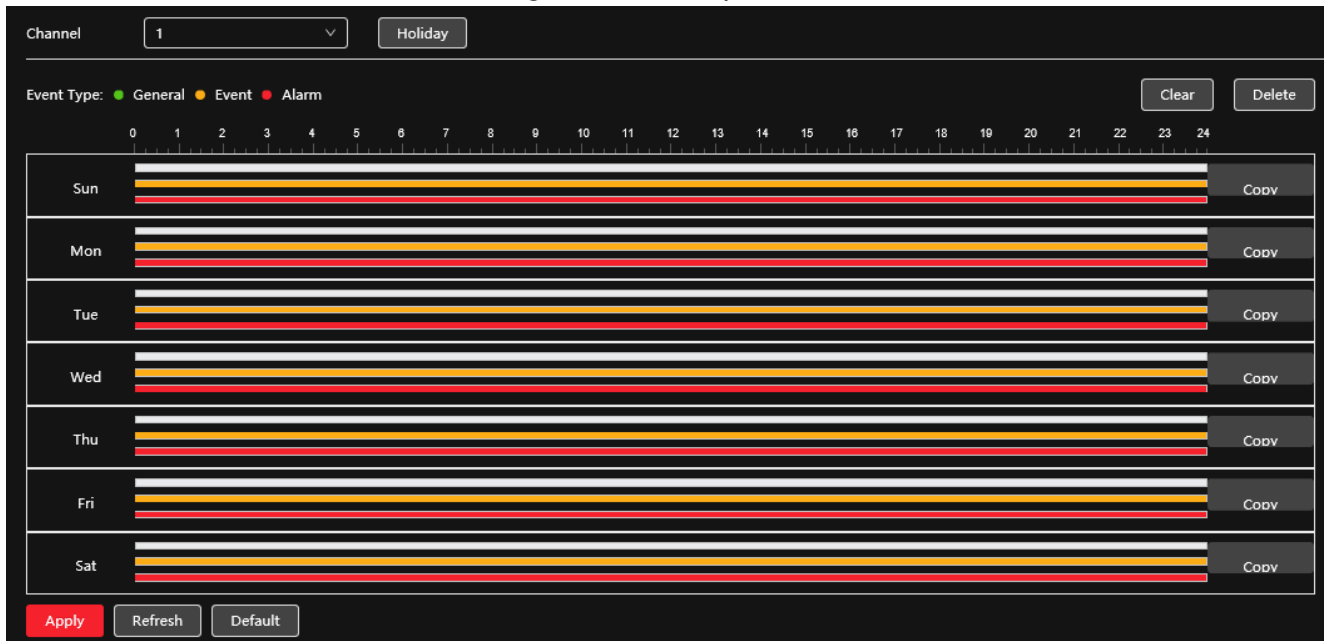
Step 3 Click **Apply**.

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 holidays, and when the **Record** is selected in the holiday schedule, the system records the video as the 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 a normal record on the timeline.

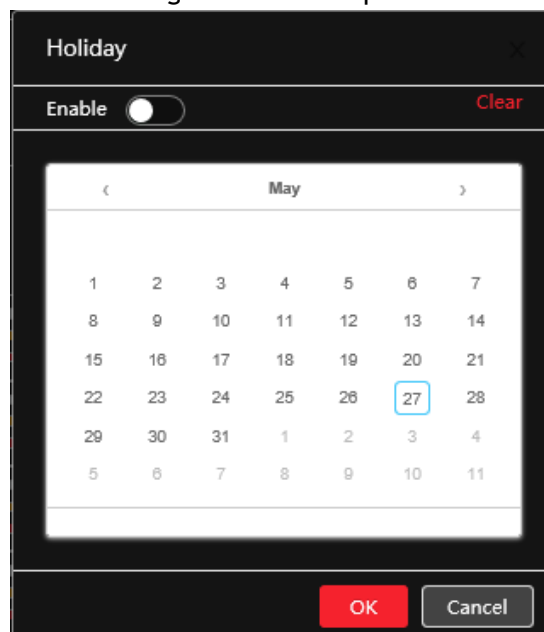


- Click **Copy** next to a day, and select the days that you want to copy to in the prompt interface, you can copy the configuration to the selected days. Select the **Select All** check box to select all day to copy the configuration.
- You can set 6 periods per day.

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.

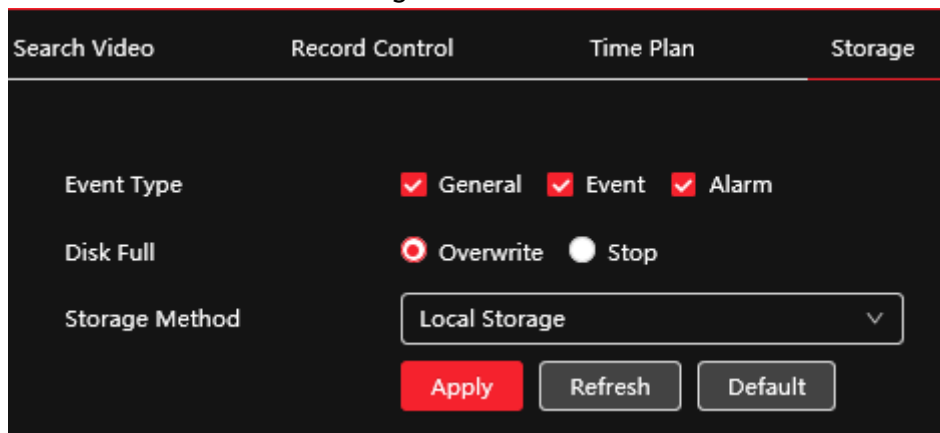
Step 6 Click **OK**.

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 .
Disk Full	Recording strategy when the disk is full. <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Local storage: Save the recorded videos in the internal SD card. <div data-bbox="528 1906 580 1944" data-label="Image">  </div> <p>Local storage will be displayed only on models that support SD card.</p> Network storage: Save the recorded videos in the FTP server or NAS.

Step 3 Click **Apply**.

10.4.1 Local Storage

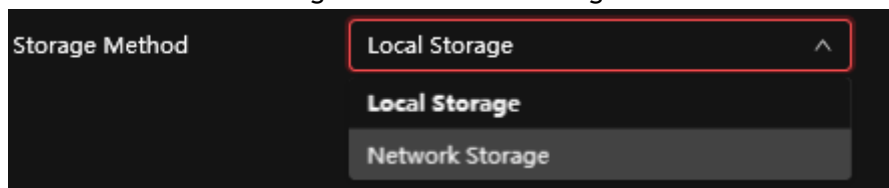
Step 1 Select **Record > Storage**.

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

Options include: **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 to 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

Event Type General Event Alarm

Disk Full Overwrite Stop

Storage Method ▾

▾

Mode ▾

Enable

Server IP

Port (0~65535)

Username

Password

Storage Path

Urgently store to local

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 to select Use Level 1 Directory , Use Level 2 Directory , and Use Level 3 Directory
Level 1 Directory	Set the Level 1 directory name, and options include 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 options include File Type , Date , File Type_Channel Number , and Custom .
Level 3 Directory	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 the FTP function works normally.

10.4.2.2 NAS

Enable this function to 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 the NAS server.

Step 4 Select NAS protocol type.

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

Figure 10-13 FTP

The screenshot shows the 'Storage' configuration page. At the top, there are four tabs: 'Search Video', 'Record Control', 'Time Plan', and 'Storage', with 'Storage' being the active tab. Below the tabs, the configuration is as follows:

- Event Type**: Three checkboxes are checked: 'General', 'Event', and 'Alarm'.
- Disk Full**: Two radio buttons are present; 'Overwrite' is selected (indicated by a red dot), and 'Stop' is unselected.
- Storage Method**: A dropdown menu is set to 'Network Storage'.
- NAS**: A dropdown menu is set to 'NAS'.
- Enable**: A toggle switch is currently turned off.
- Server IP**: A text input field contains '0.0.0.0'.
- Storage Path**: An empty text input field.

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

Step 5 Configure NAS parameters.

Table 10-5 Description of NAS parameters

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
Username	When selecting SMB protocol, you are required to enter username and password. Enter them as necessary .
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 an SD card.
- Before playing back picture, configure snapshot time range, snapshot storage method, and snapshot plan. For details, see "11.3 Setting Snapshot Plan".

Procedure

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

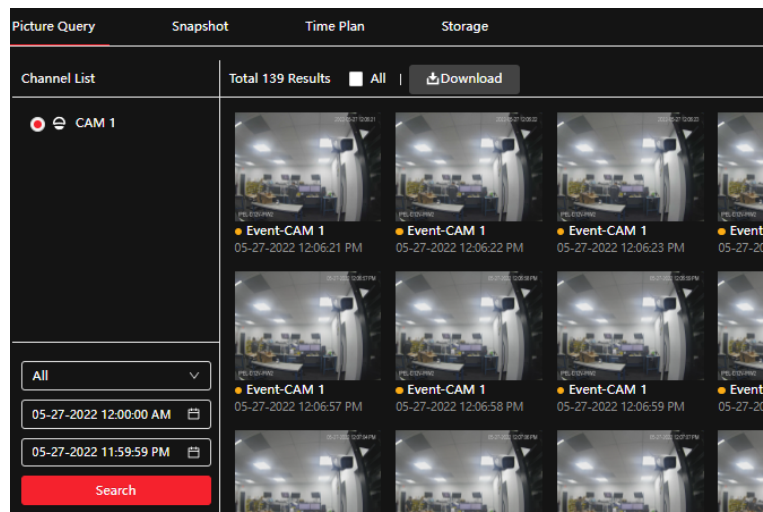
Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Search**.

- Click **All**, and select the record type from the drop-down list, options include: **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 will be displayed.

Figure 11-2 Picture playback

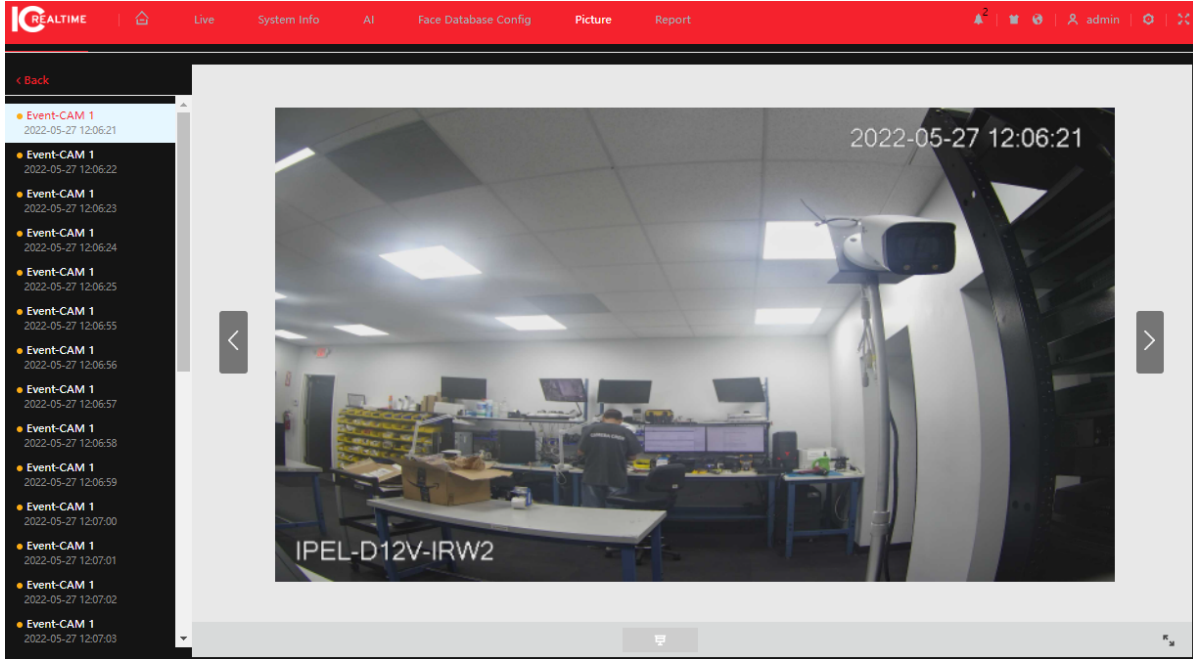






Table 11-1 Description of playback interface

No.	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play back the snapshot. Click Back at the upper-left corner to go to the Picture Query interface.
2	Manual display	<ul style="list-style-type: none"> Click  to display the previous snapshot in the snapshot list. Click  to display the next 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 will be 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 may vary with different browsers.

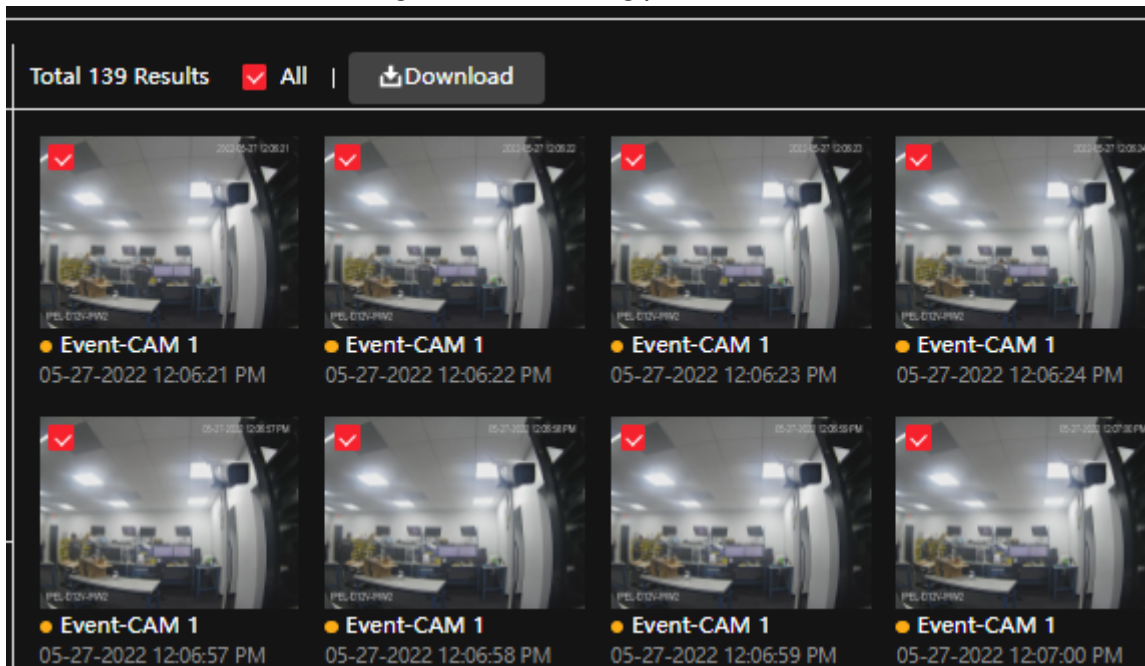
- For details of viewing or setting storage path, see "6.1 Local". [Step 1](#)

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.

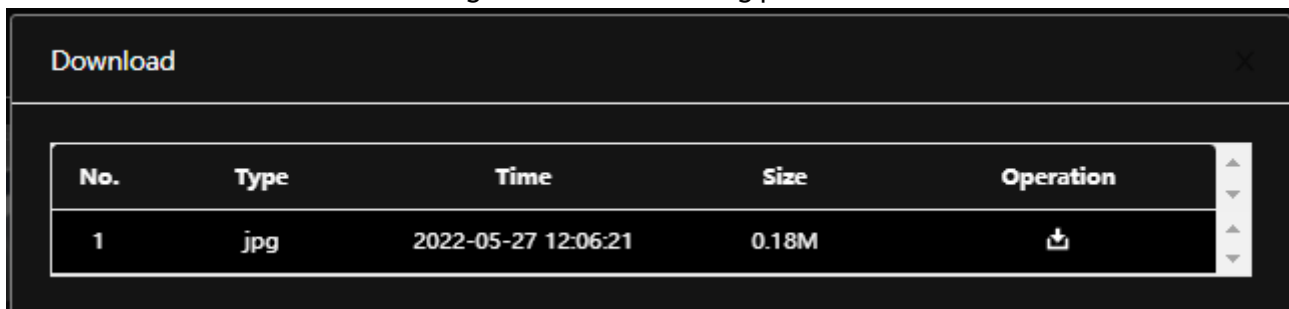
Figure 11-3 Selecting picture file



[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

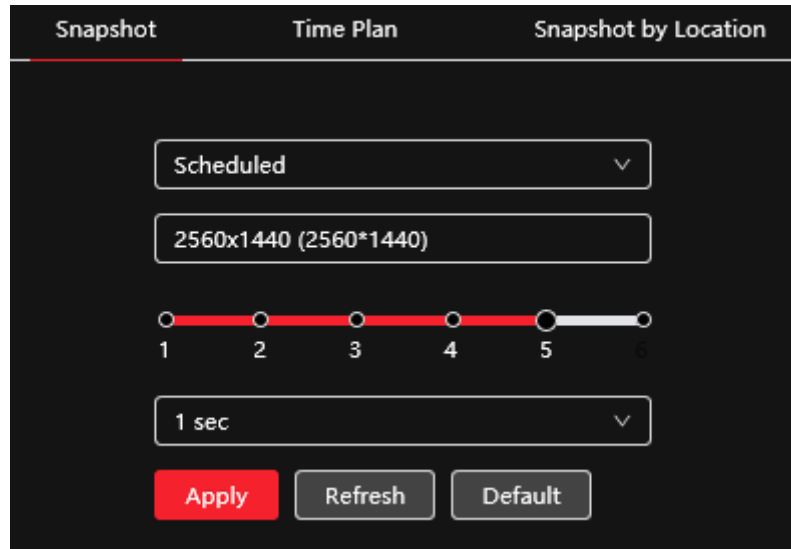



Table 11-2 Description of snapshot parameters

Parameter	Description
Type	<p>Options include: Scheduled and Event.</p> <ul style="list-style-type: none"> • Scheduled: Capture images in configured period. • Event: Capture images when configured event is triggered, such as Motion Detection, Video Tamper and Scene Changing. <p> Make sure that you have enable the corresponding event detection and the snapshot function.</p>
Size	It is same with the resolution of the main stream.
Quality	Set the quality of the snapshot. The higher the value, the better the quality.
Interval	Set the frequency of snapshot. You can select Custom to set the frequency as necessary .

Step 3 Click **Apply**.

11.3 Setting Snapshot Plan

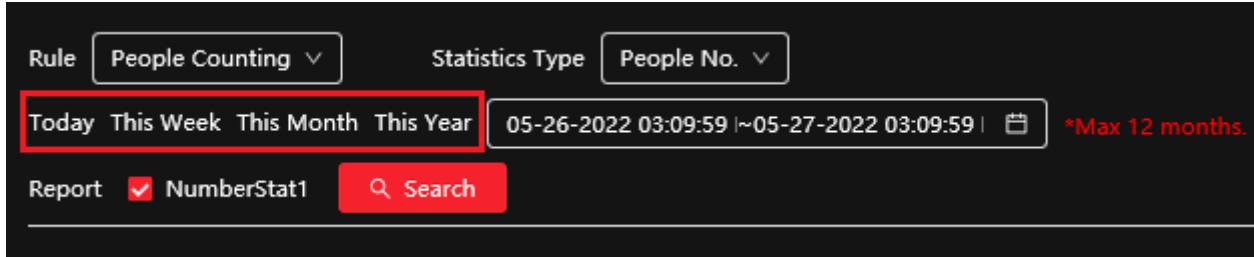
According to the configured snapshot plan, the system enables or disables snapshot at a corresponding time. For detailed operation, see "10.3 Setting Record Plan".

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**.

Related Operations

- Select the report form
Click to display the report in line chart; click to display the report in a 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.

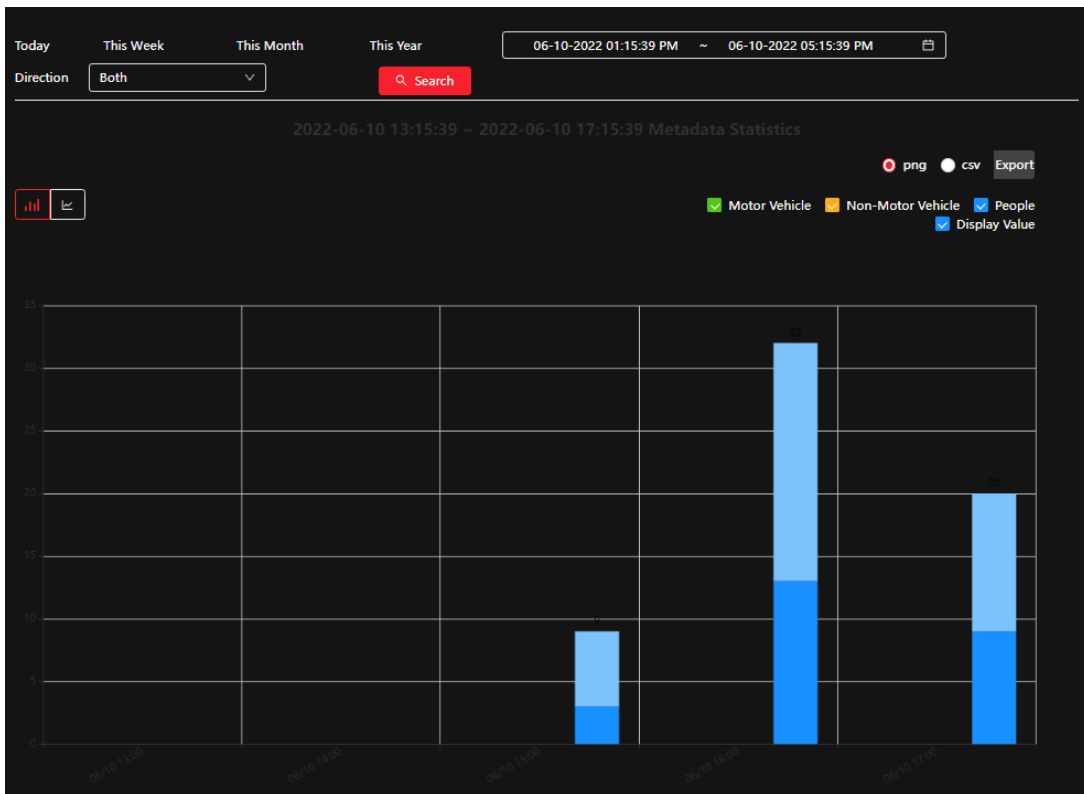


For multi-channel camera, select the channel first.

Step 3 Select the tripwire direction.

Step 4 Click **Search**.

Figure 12-3. 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 the search conditions.



For multi-channel camera, select the channel first.

Table 12-1 Set search conditions



Parameter	Description
Rule	Select the rule as necessary, and then you need to select the statistics type according to the select rule.
Statistics Type	The statistics type of the people counting report. <ul style="list-style-type: none"> ● 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 the 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. <ul style="list-style-type: none"> ● When selecting a rule to People Counting, you can view the daily, weekly, monthly and yearly report, and you can also customize the period. ● When selecting a 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



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

This section allows you to search for the number of people at a certain moment and get daily/weekly/monthly reports.

Prerequisites

Confirm that the 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**.

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 Heat Map

View heat map and track map. You can search the detection results by the number of people and stay time, and then generate the heat map.

Procedure

Step 1 Select **Report > Report > Heat Map**.

Step 2 Set search conditions.



For a 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 a report type from 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 reports, and you can also customize the period.

Step 3 Click **Search**.

Related Operations

Click **Export**, and select the storage path for the exported report in **.bmp** format.

12.1.6 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**.

- 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.

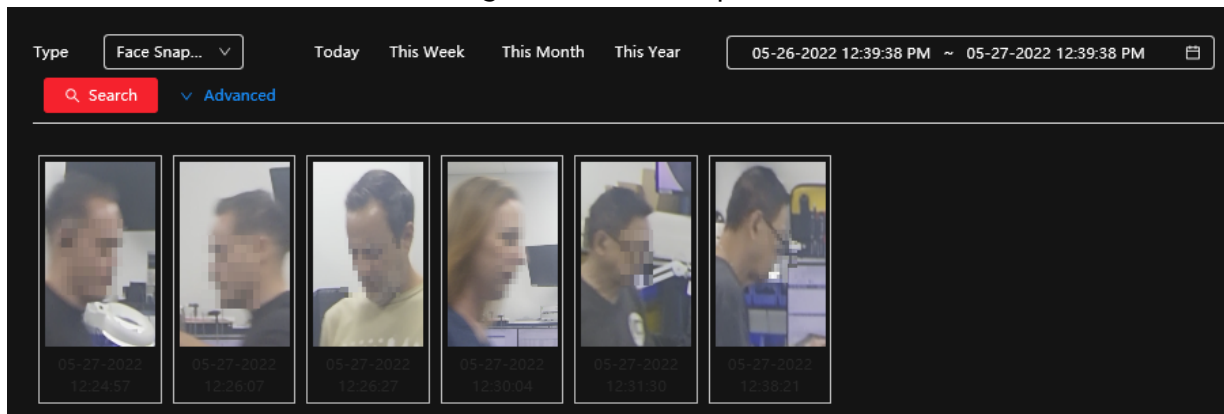
Prerequisites

Make sure that you have an 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 will be displayed.

Figure 12-14 Face report



- Step 4 Click the picture to 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 the server. You can add two server information at most.

Table 12-3 Description of HTTP mode parameter

Parameter	Description
Report Period	Select the reporting 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 to which the report will be uploaded to.
Port	
Path	The storage path of the server for the report.
Report type	Select the report type from the drop-down list. You can select more than one type 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**

Table 12-4 Description of FTP mode parameter

Parameter	Description
Report Period	Select the reporting 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 from the drop-down list. You can select more than one type at the same time.  The report types in the drop-down list are the same as 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 to 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

Table 12-5 Description of email mode parameter

Parameter	Description
Report Period	Select the reporting 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 from the drop-down list. You can select more than one type at the same time.  <ul style="list-style-type: none"> • 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. • The heat map report will not be uploaded when you select email upload method, so the 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	The username and password used to log in server.
Password	 See Table 12-6 for details.
Sender	Sender's email address.
Encryption Type	Select the encryption type from None, SSL (Secure Sockets Layer) and TLS (Transport Layer Security).  See Table 12-6 for details.
Subject	Email subject. You can enter up to 120 characters in Chinese, English, and Arabic numerals.
Receiver	Email addresses of receivers. Click add to set more than one receiver. 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 keeping 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 on



firmware updates released by the manufacturer.

- We suggest that you download and use the latest version of the client software.

"Nice to have" recommendations to improve your equipment network security:

1. Physical Protection

We suggest that you perform physical protection on 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, and unauthorized connection of removable equipment (such as USB flash drives, 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 the password reset function. Please set up related information for password reset in time, including the 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 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 enable HTTPS so that you visit Web services through a secure communication channel.

7. MAC Address Binding

We recommend you 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 the 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 an encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: the 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 an external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two subnetworks, 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 the IP/MAC address filtering function to limit the range of hosts allowed to access the device.



Your security is our business, no matter what it takes!

IC Realtime LLC

Address: 3050 N Andrews Ave Ext Pompano Beach, FL USA 33064 | Website: www.icrealtime.com.com | Email: tech@ICRealtime.com
Tel: 1(866) 997-9009