AI Network Camera

Web Operation Guide

ISSUE	**V1.1**
DATE	**2026-06-16**

About This Document

Purpose

This document describes the main functions and operations of the web interface for IP cameras. It includes instructions for:

- Network access
- Network configuration
- Troubleshooting

Intended Audience

This document is intended for the following users:

- Technical support engineers
- Maintenance engineers
- IP camera operators

Symbol Conventions

The following symbols are used in this document to indicate important safety information and tips:

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
 NOTE	Highlights important information, best practices, or useful tips not related to personal injury, equipment damage, or environmental concerns.

Contents

About This Document i

Contents ii

1 Quick Overview 5

1.1 Login and Logout 5

1.2 Forget Password 7

1.3 Change Password 9

1.4 Homepage Layout 12

1.5 Playback 16

1.6 Snapshot 18

1.7 LPR Setting 21

1.8 IVS Setting 22

2 Quick Start Settings 23

2.1 Local Network 23

2.2 Video 25

2.3 Display 29

2.3.1 Access the Display Settings 29

2.3.2 Mode 30

2.3.3 Image Setting 30

2.3.4 Scene Mode 31

2.3.5 Exposure 32

2.3.6 White Balance Setting 34

2.3.7 Day/Night 35

2.3.8 Noise Reduction 39

2.3.9 Image Enhancement 41

2.3.10 Zoom Focus (Only for Some Models) 42

2.4 OSD 44

2.5 Date and Time 47

3 System Settings 49

3.1 Settings 49

3.1.1 Device Information 49

3.1.2 Date and Time 51

3.1.3 System 51

3.1.4 Software Licenses 52

3.2 Change Password 52

3.3 Configure User 52

3.3.1 Add User 52

3.3.2 Online User 55

3.4 Query Device Logs 56

3.4.1 Query Operation Logs 56

3.4.2 Query Alarm Logs 57

3.4.3 Collect All Logs 58

3.5 Maintain the Device 60

3.5.1 Reboot Device 60

3.5.2 Upgrade the Software Package 61
3.5.3 Restore Device to Factory Settings 62
3.5.4 Export / Import Configuration 63
3.6 Configure Security 66
3.6.1 IP Filter 66
3.6.2 Security Services 68
4 Configure the Network Service 69
4.1 Basic Settings 69
4.1.1 Local Network 69
4.1.2 Device Port 69
4.1.3 Port Mapping 71
4.1.4 DDNS 72
4.1.5 Set PPPoE 74
4.2 Advanced Settings 76
4.2.1 Set FTP 76
4.2.2 Set SMTP 77
4.2.3 Set HTTPS 79
4.2.4 Set QOS 82
4.2.5 Set 802.1x 83
4.2.6 Set SNMP 83
4.2.7 View ONVIF 87
4.2.8 Set Platform Access 89
4.2.9 Set Multicast Parameters 92
4.2.10 Set CGI Alarm Service Center 93
5 Configuration Video/Audio 97
5.1 Video 97
5.1.1 Set video 97
5.1.2 Snapshot 97
5.1.3 ROI Parameter 98
5.2 Audio 100
5.2.1 Audio 100
5.2.2 Audible File (Feature available only on certain models) 101
6 Configuration Image 103
6.1 Configure Display 103
6.2 Configure OSD 103
6.3 Configure the Privacy Mask 103
6.4 Configure Video Standard 105
7 Configure Event 106
7.1 Motion Alarm Linkage 106
7.2 Alarm In (Only for Some Models) 109
7.3 Alarm Out (Only for Some Models) 112
7.4 Disk Alarm 114
7.5 Network Alarm 115
7.6 Day/Night Switch Alarm 116
7.7 Abnormal Sound Detection (Only for Some Models) 117
7.8 Push Message 118

7.9 Flashlight Alarm Output (Only for Some Models) 118
8 Configure Storage Function 120
8.1 Record Strategy 120
8.2 Record Directory 121
8.2.2 Configure the SD Card 123
8.2.3 Configure the FTP 124
8.2.4 Configure the NAS 125
8.3 Snapshot Policy 126
8.4 EMMC 128
9 IVS Settings 129
9.4 Configure Intelligent Analysis 129
9.4.1 Intrusion 129
9.4.2 Smart Motion 135
9.4.3 Single Line Crossing 136
9.4.4 Double Line Crossing 137
9.4.5 Multi-Loitering 139
9.4.6 Wrong-Way 140
9.4.7 Regional Population Detection 141
9.4.8 Perimeter Detection 142
9.4.9 Running Detection 144
9.4.10 Fall Detection 145
9.4.11 Fight Detection 146
9.4.12 General Parameters 148
9.5 Configure People Counting 148
9.5.1 Setting 148
9.5.2 Report 151
10 Panoramic Cameras 153
10.1 CVBS Function (Only for Some Models) 153
10.2 Dual-Lens 154
10.2.1 Dual-Lens 154
10.3 Panoramic Camera 155
10.3.1 RS458 155
10.3.2 IR Led Config 156
10.3.3 CVBS 157
10.4 For Special Cameras 158
10.4.1 General Parameters 158
10.4.2 Illegal Parking (Only for Some Models) 159
10.4.3 Enter Area(Only for Some Models) 160
10.4.4 Leave Area(Only for Some Models) 160
10.4.5 Heat Map 161
Troubleshooting 164
Acronyms and Abbreviations 166

1 Quick Overview

1.1 Login and Logout

CAUTION

Use a supported browser such as Microsoft Edge, Chrome, or Firefox to access the web interface. Other browsers may result in limited functionality.

Activation

Step 1 Open the Chrome browser.
Step 2 Enter the IP address of the IP camera in the address bar (default: `192.168.0.120`) and press **Enter**.
Step 3 On first login: You will be prompted to create a password. After setting the password, you will be directed to the login page.

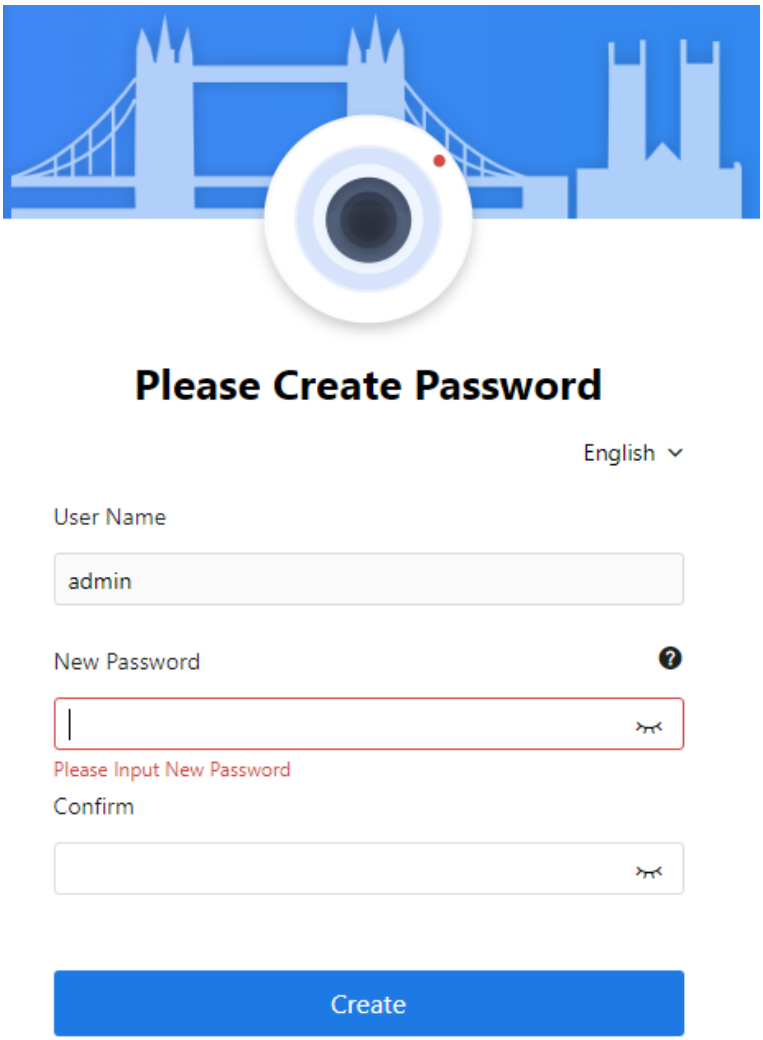
Note: DHCP is enabled by default. Use the provided tool to search for the camera IP.

Default IP: `192.168.0.120`.

Important: After changing the password, wait at least 3 minutes before powering off the device to ensure the change is saved. Alternatively, log in again with the new password to verify.

- You can change the system language on the login page.
- Click **Login** to access the homepage.

Figure 1-1 Create password

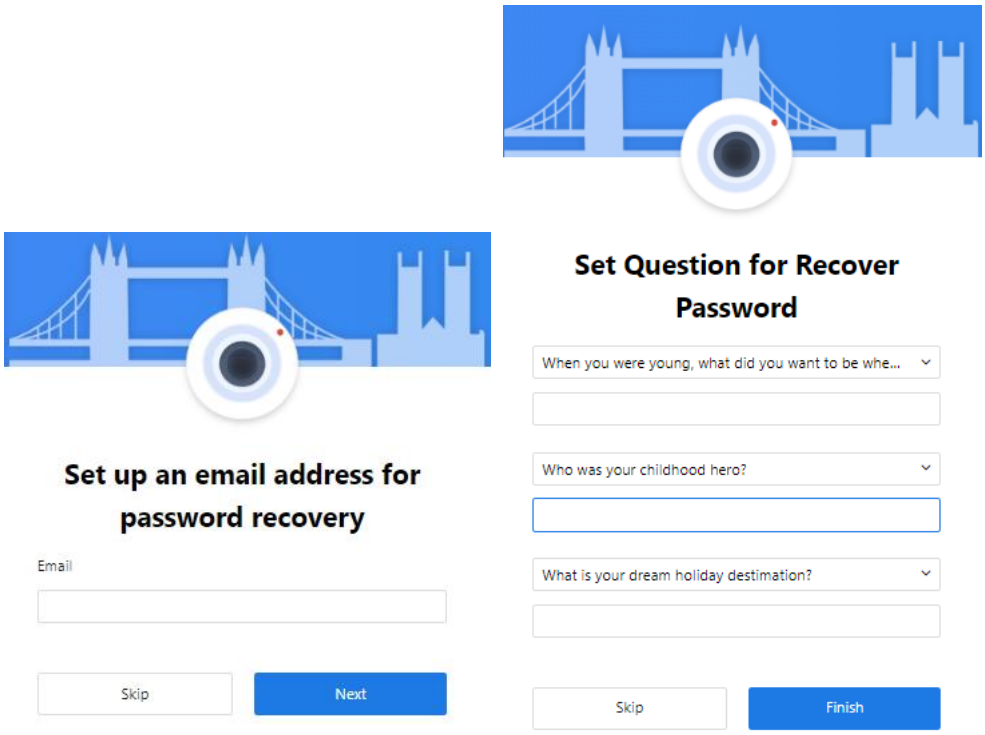


Step 1 Enter your username and password to access the system, as shown in Figure 1-1.

- Default username: `admin`
- The password must be created during the initial login.

Step 2 Set an email address for password recovery, and set the questions for recovery. If you don’t want to set these, you can skip them.

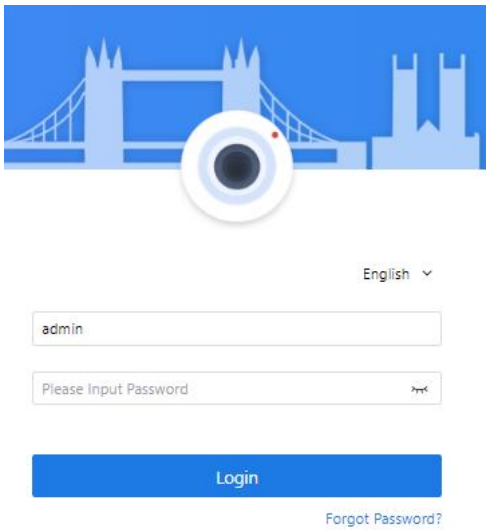
Figure 1-2 password recover



1.2 Forget Password

Input the **super administrator** user name to show the "**Forget password**". If you forget the password, click this button to jump to the "Forget password" page.

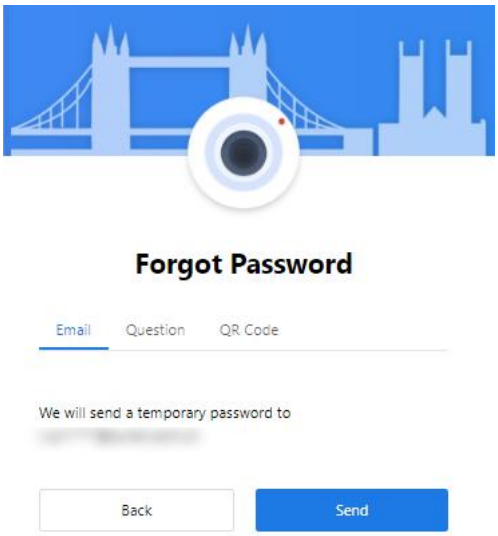
Figure 1-3 Login page



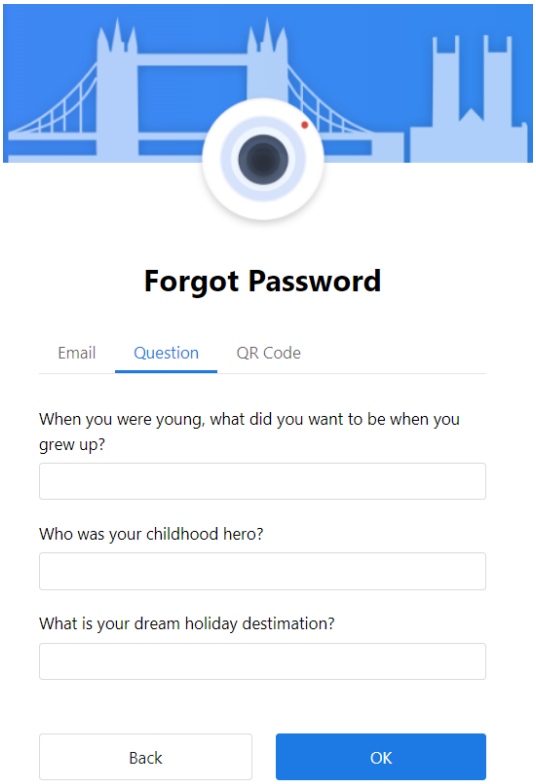
There are three methods available for recovering the password. For Email and Question, the user should set them first during the activation of the camera.

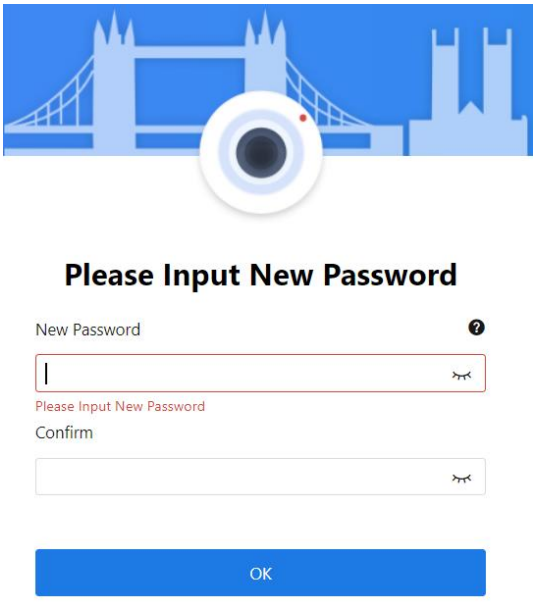
Method 1: **Email.** The camera should be connected to the network so that it can send the temporary password to the email address. The temporary password is **valid for five minutes**; create a new password immediately.

Figure 1-4 Forget password



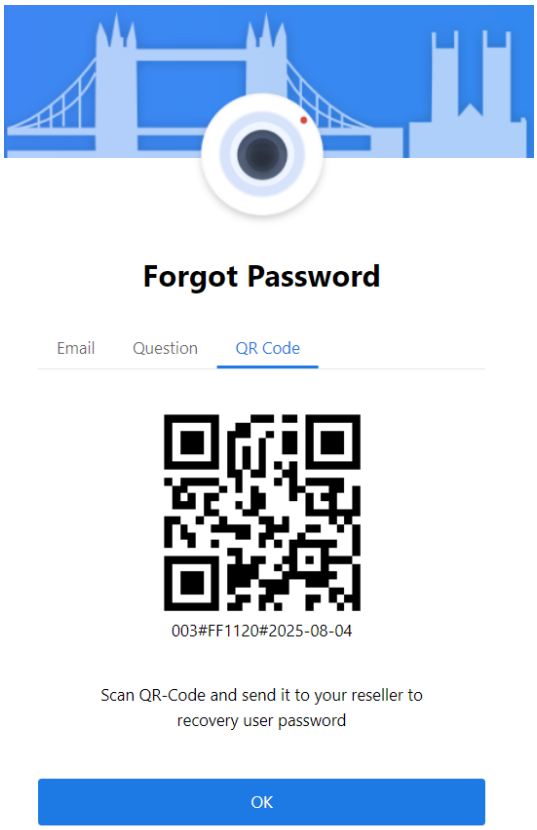
Method 2: **Question** Answer the security questions correctly to enter the “New Password” page.





Method 3: **QR Code.** If the user did not set the recovery email and question, the user can scan the QR Code on the login page and send it to the reseller. We will provide a temporary password that will be valid until 11:59:59PM. Use the temporary or new password to log in and then create a new one.

Figure 1-5 QR Code



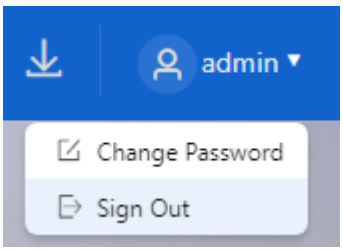
NOTE

Note: DHCP is enabled by default. Use the provided tool to search for the camera IP. Default IP: `192.168.0.120`.

Important: After updating the password, wait at least 3 minutes before powering off the device to ensure the changes are saved. Alternatively, log in with the new password to verify.

- You can change the system language on the login page.

Sign out

Click 

Sign Out in the upper right corner to return to the login screen.

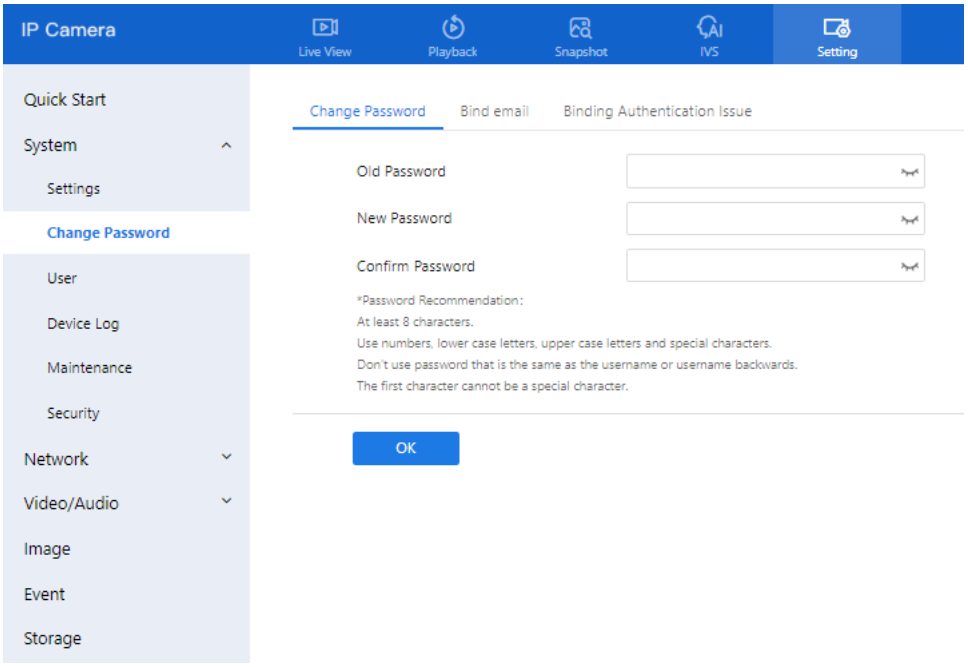
1.3 Change Password

Description

To change your password:

- Click your **username** in the upper right corner and select **Change Password**.
- Or go to **Setting > System > Change Password**.

Figure 1-6 Change the default password page



Procedure

Step 1 Enter the **old password**, **new password**, and **confirm** the new password.
Step 2 Click **OK**.

- A message like "Change your password success!" confirms the change.
- If the password change fails, a tip or error will be displayed (e.g., "Password must be at least 8 characters").

Step 3 It is recommended to wait three minutes before restarting the device after changing the password.
Step 4 Click **OK** to return to the login page.

The “admin” user can set the bind email and binding authentication issue, so that when the “admin” user forgets the password via email and authentication issue, to recovery the password.

Figure 1-7 Bind email

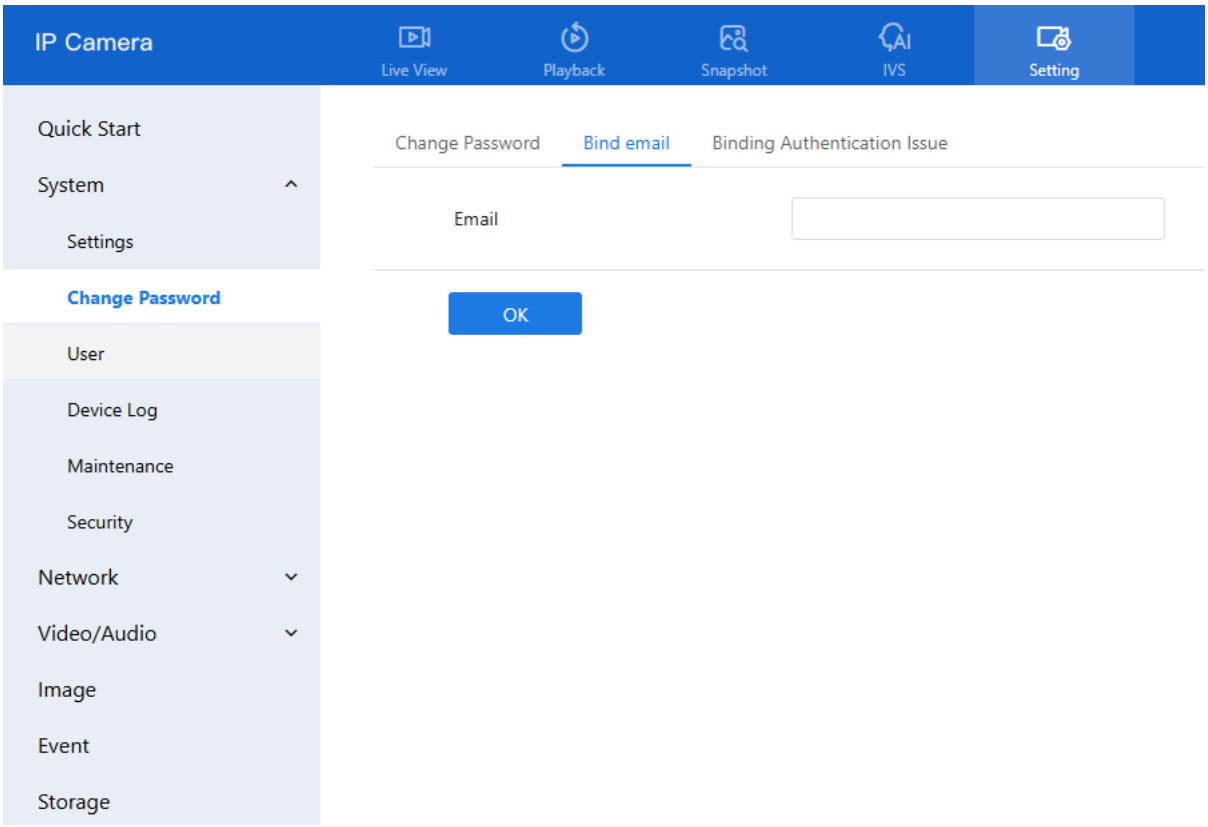
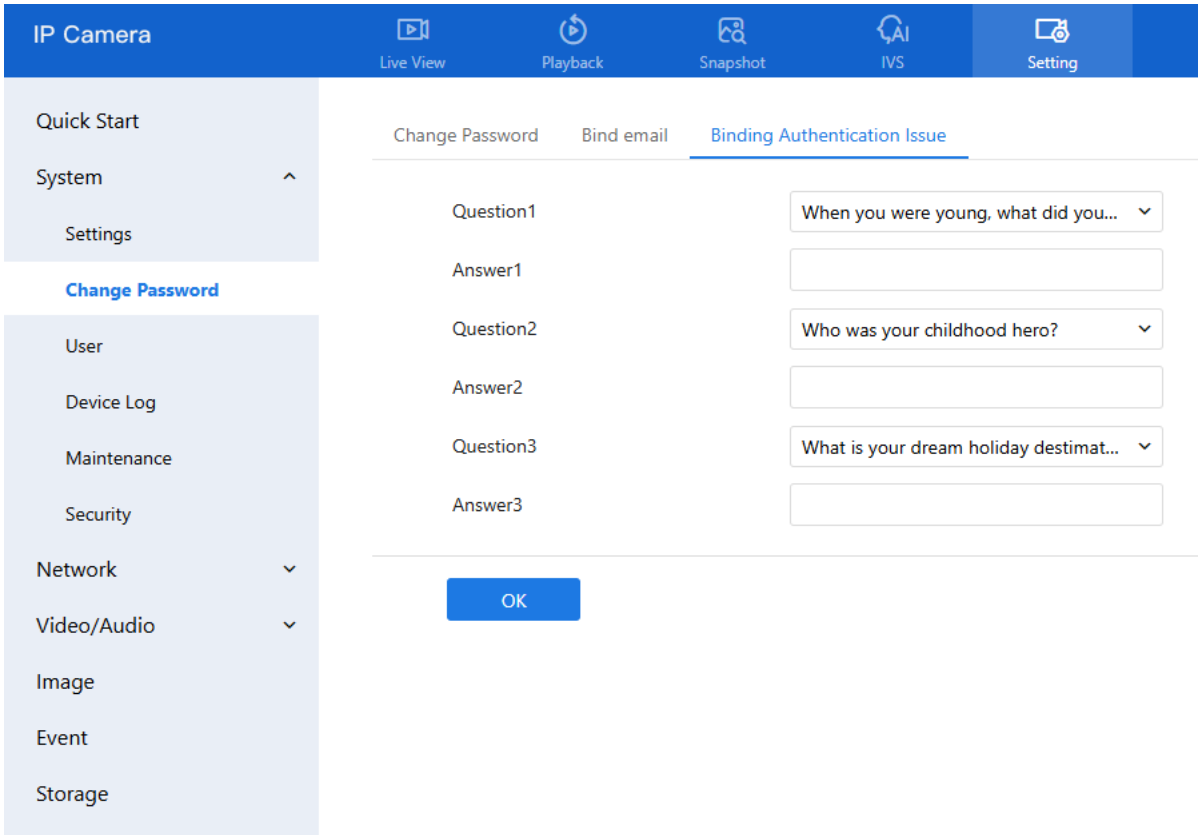


Figure 1-8 Binding authentication issue



1.4 Homepage Layout

The homepage allows you to:

- View real-time video
- Monitor alarms and faults
- Configure system settings
- Change your password
- Log out of the system

Refer to **Figure 1-9** for the layout and **Table 1-1** for descriptions.

Figure 1-9 Homepage layout

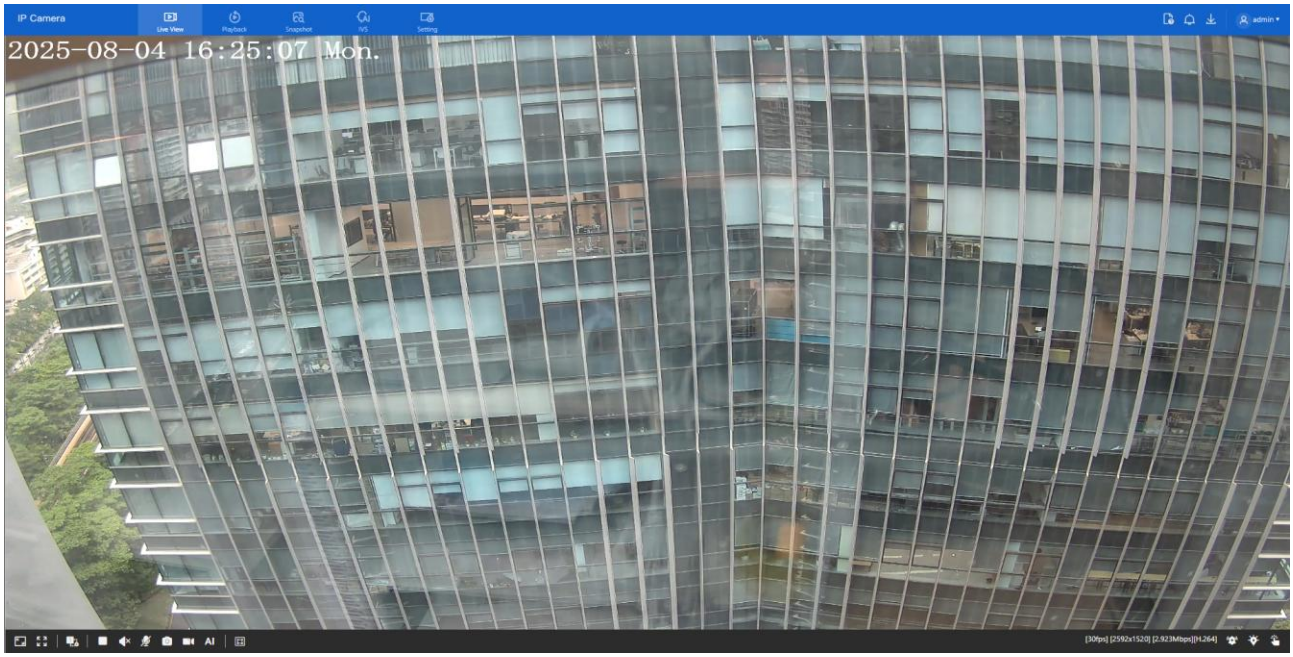


Figure 1-10 PTZ interface

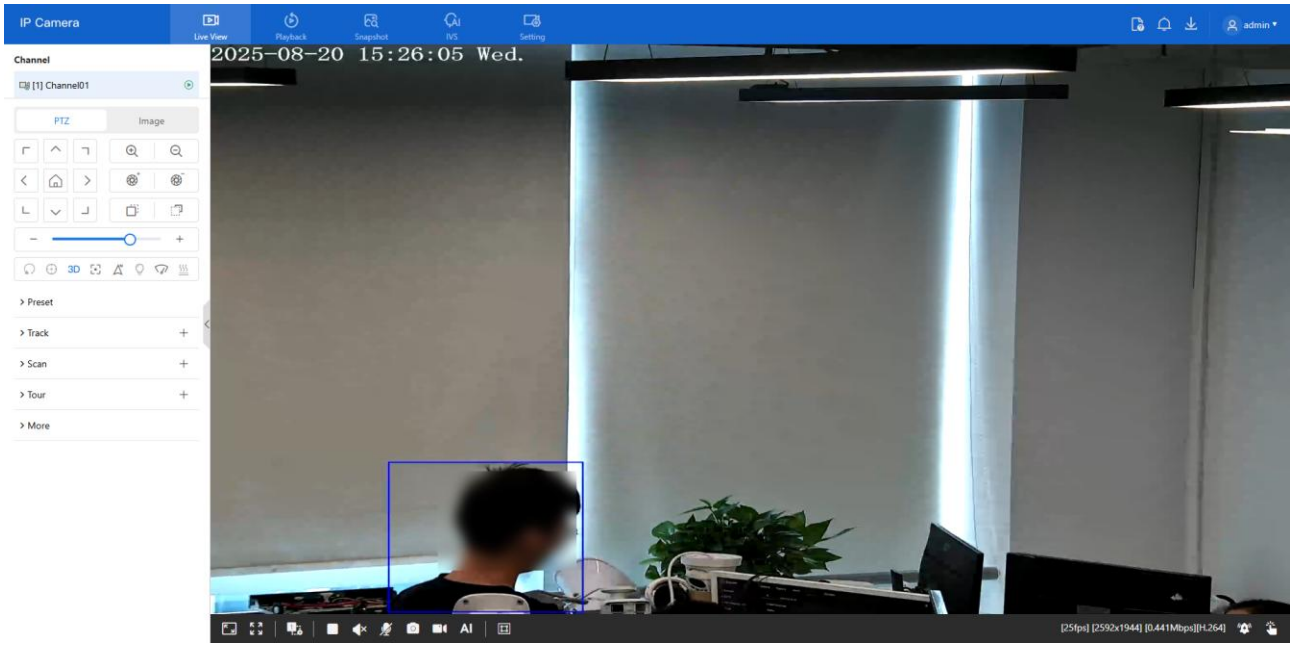
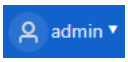


Table 1-1 Elements on the homepage

No.	Element	Description
1	Live View	Displays real-time video streams.
2	Playback	Access recorded videos (requires SD card or NAS with recordings).
3	Snapshot	The user installed the SD card in advance, enabling the snapshot feature. Set the conditions, and click **Search** to search the snapshot of the event.
4	IVS setting	Configure AI multi-target features and intelligent analysis (e.g., intrusion, smart motion, single line crossing, double line crossing, multi-loitering, Wrong-Way, general parameters, and people counting).
5	Setting	Set parameters for Quick Start, System, Network, Audio/Video, Image, Event, and Storage.
6		About the intercom function.
7		Click  to view alarm alerts.
8		Displays SD card video backup and download progress.
9		Sign out, change password, view current user.
10		Zoom +/ zoom – (adjust zoom level).
11		Iris +/ iris – (adjust iris value).
12		Near focus /far focus
13		Auto focus
14	Image	Set brightness, saturation, contrast, and sharpness.
15		Window scale, Adjust display scale for live video.
16		View live video in full-screen mode.
17		Switch between available stream modes (up to 3, depending on model).
18		Pause/Start or Stop live video playback.
19		Enable or disable audio output.
20		Two-way audio. Open or close the intercom (the computer should be plugged in with the microphone).

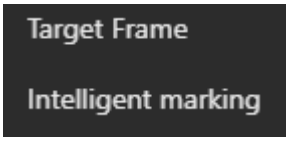
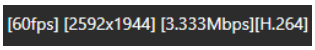
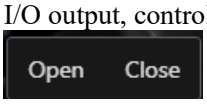
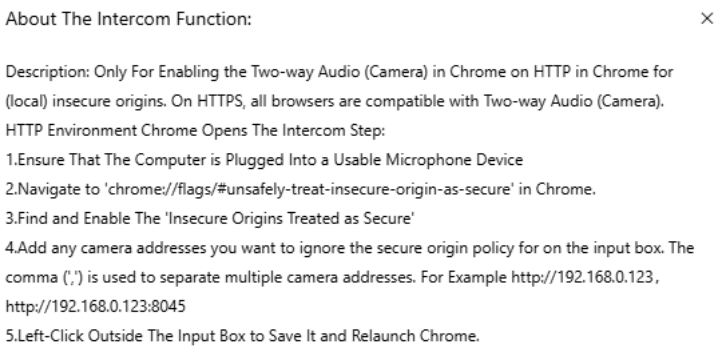
No.	Element	Description
21		Click the icon to snapshot the video and save the images to the specified location.
22		Record the video and save the file to the specified location.
23		View AI-detected targets (e.g., face, vehicle, human body). The snapshot details can be viewed by clicking the “Details” on the picture.
24		 Target frame: Show detection box around targets. Intelligent marking: Display IVS detection areas during live view.
25		Display resolution, frame rate, bit rate, and encoding type.
26		Audio alarm status. Red means it is alarming. Click the icon to show the **Stop** button. Click Stop to close the audio alarm.
27		Open or close the white light /flashing light manually (available only on special models).
28		I/O output, control the I/O alarm output manually. Click  to open the alarm or close the alarm.
29		Applied for a dual-channel camera. Select dual-channel split-screen display mode: side-by-side horizontally or stacked vertically.

Figure 1-11 About the intercom function



Note: The following instructions apply **only when using two-way audio (camera) in Chrome over HTTP** (insecure origin). For HTTPS connections, two-way audio is supported by all major browsers.

If using **Chrome on HTTP**, follow these steps to enable the intercom function:

1. Ensure your computer is connected to a **working microphone**.
2. Open Chrome and navigate to:
   `chrome://flags/#unsafely-treat-insecure-origin-as-secure`

3. Enable the flag: **“Insecure origins treated as secure.”**
4. In the input box that appears, enter the IP addresses of the cameras you want to allow, separated by commas.
    - Example:
      `http://192.168.0.123, http://192.168.1.250:8045`
5. Click outside the input box to save your changes.
6. **Relaunch Chrome** for the changes to take effect.

Figure 1-12 AI multi-object live video interface

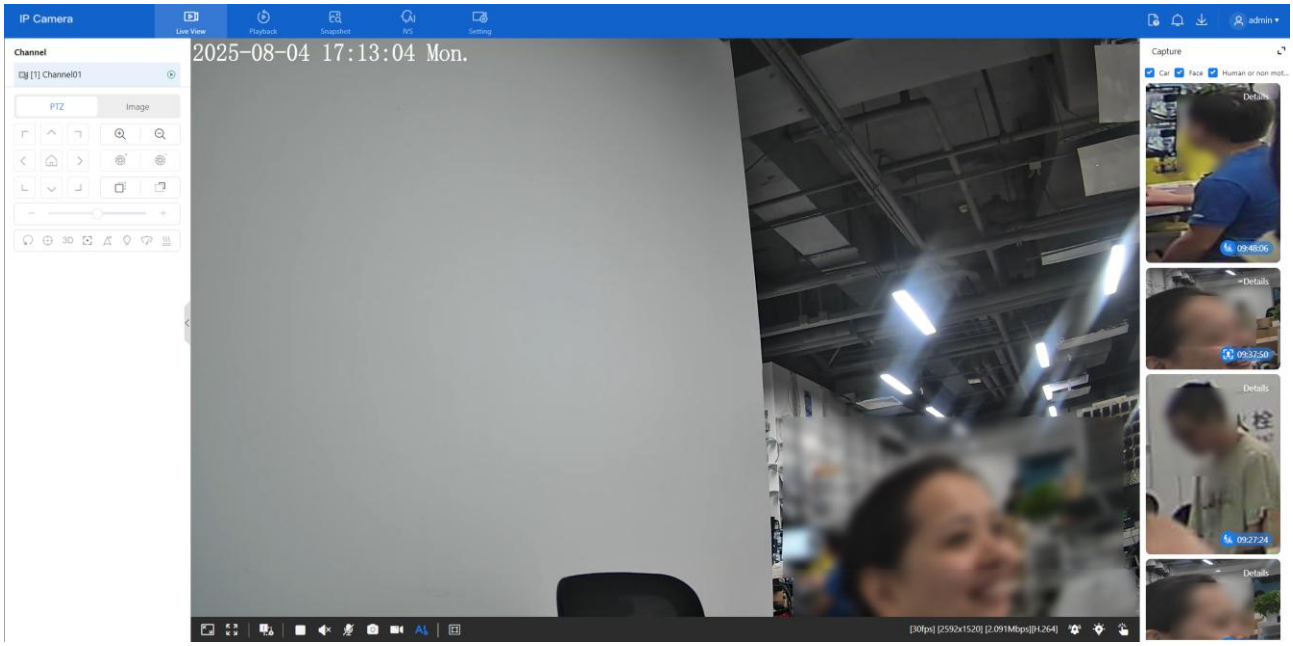
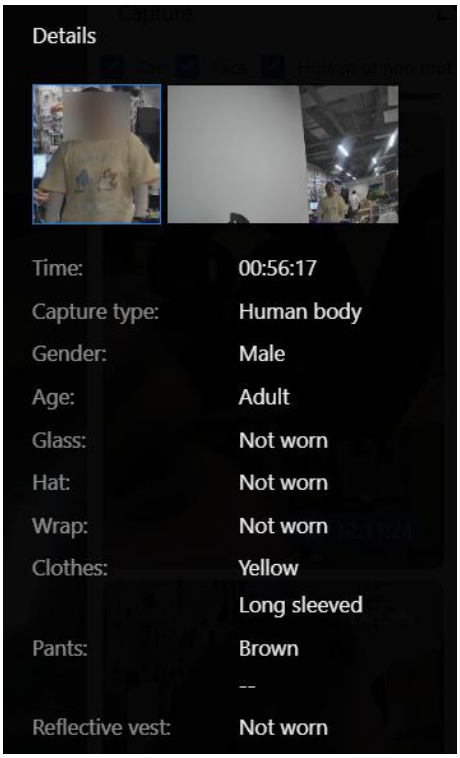
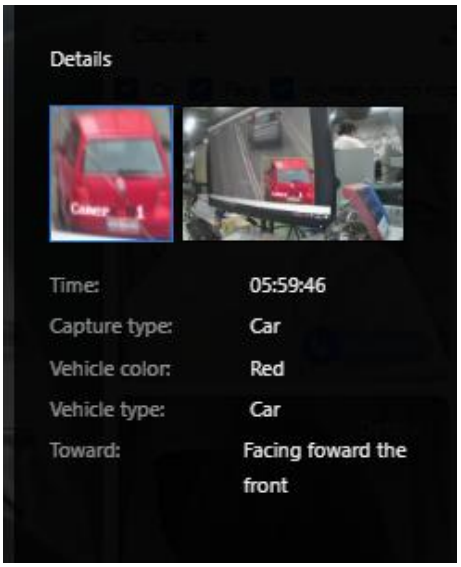


Figure 1-13 Attribute details





1.5 Playback

To review recorded footage:

1. Click **Playback** on the web interface.
2. If an SD card is installed and enabled, recordings will be available.

Refer to **Figure 1-14** for layout and controls.

Figure 1-14 Playback page

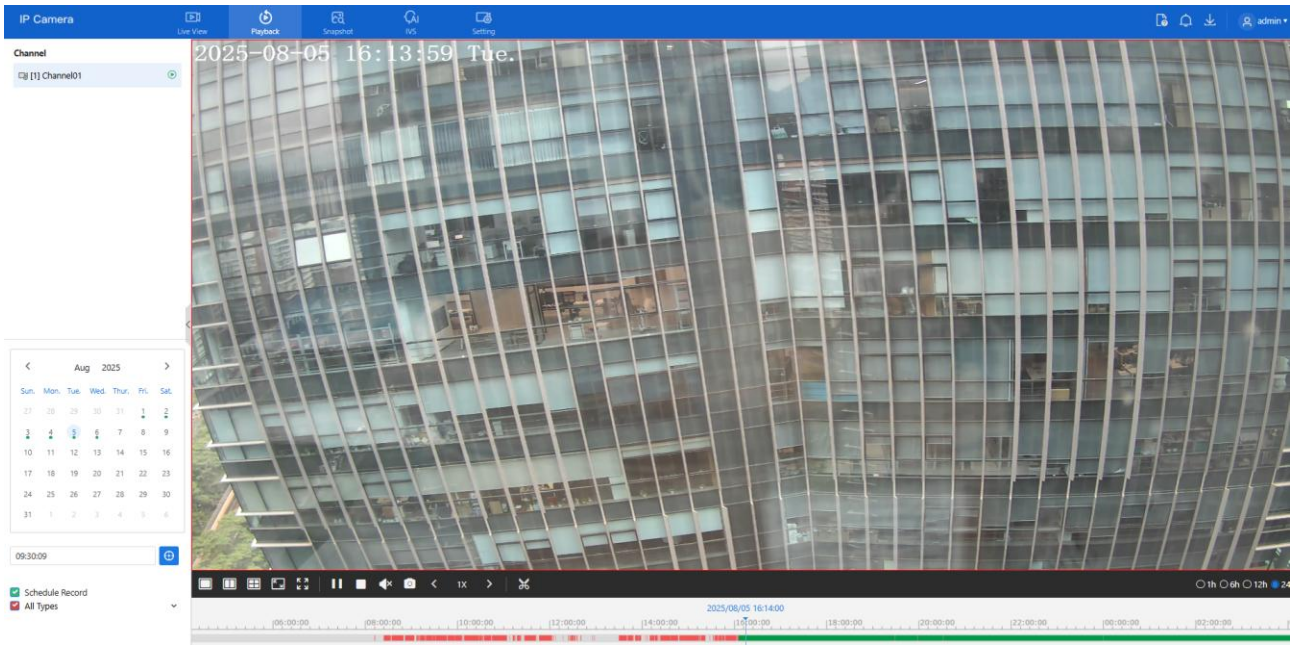


Table 1-2 Playback function

No.	Element	Description
1	Channel	Displays available video channels.
2	Calender	25 Green dots indicate recorded days.

3		The green timeline represents scheduled recording, and the red timeline represents alarm recording. The types of alarm recording vary according to model performance.
4		One screen plays a recording. Choose one day to record, click  to play.
5		Two screens play a recording. Choose the screen, choose the channel, select one day that has a recording(the date shows a green point), click  to play.
6		Four screens play a recording. Choose the screen, choose the channel, select one day that has a recording(the date shows a green point), click  to play.
7		Window scale. Adjust playback scale.
8		View the recording in full-screen mode.
9		Pause or replay playback.
10		Enable or disable audio playback.
11		Capture screenshots from the recording and save the images to a specified location.
12		Fast Forward, 1/16X, 1/8 X, 1/4 X, 1/2 X, 1 X, 2 X, 4 X

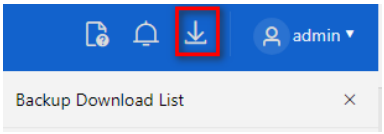
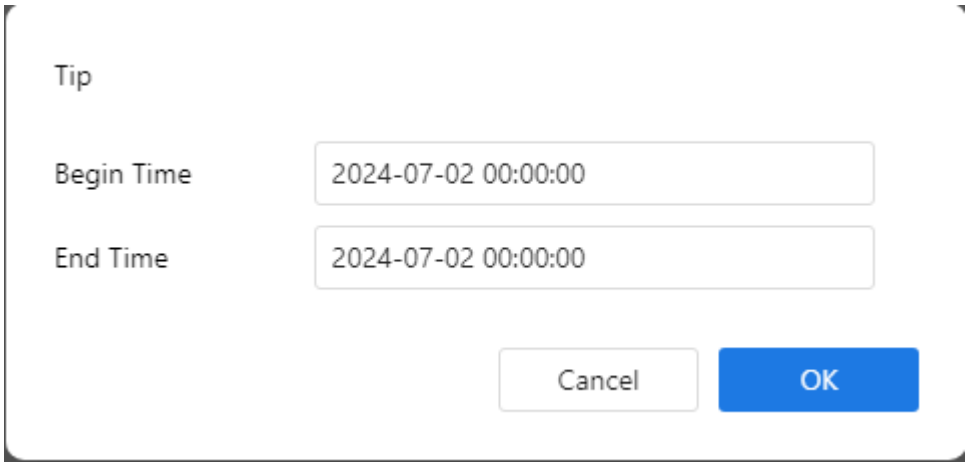
13		Click to begin video backup; select the duration; click again to stop. A dialog will prompt you to save or cancel. In the pop-up window of the tip, as shown in Figure 1-15, click the save to save the video. Click **Cancel** to abandon.  Click the backup list to show the detailed information.
14		Time view options: 1h, 6h, 12h, 24h.

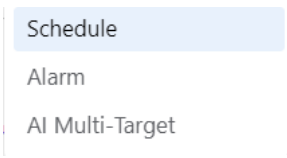
Figure 1-15 Record backup tip



1.6 Snapshot

For AI multi-target cameras, install an SD card (the camera will deploy 1/5 sizes of SD card to store snapshot images) to save and activate the snapshot feature (schedule, alarm, AI multi-target). The results can be retrieved and previewed in this interface.

To review snapshot footage:

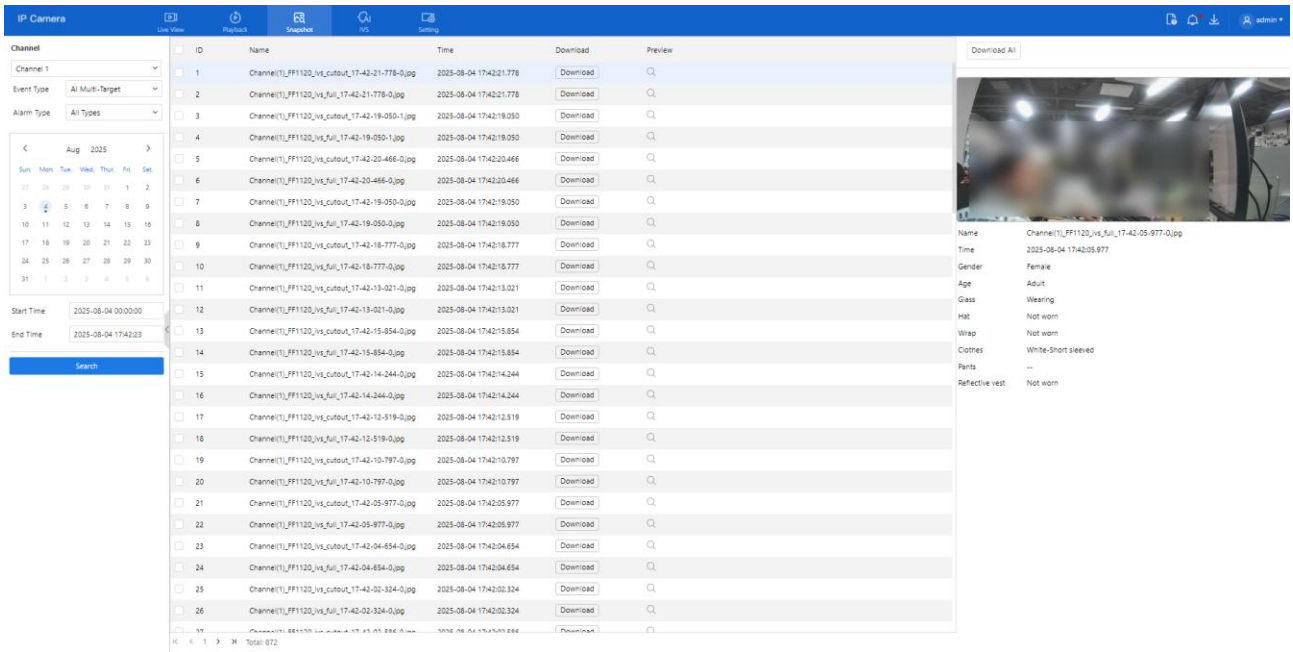
1. Click **Snapshot** on the web interface.
2. If an SD card is installed and enabled, the **Snapshot Policy** is enabled. Or the IVS alarm linkage **Snapshot Event Action** is enabled.
3. Choose the channel; the normal is channel 1. For the multi-channels, you should choose the corresponding channel.
4. Select the **Event Type** 

.
5. Choose the date. The date with a green dot

means it has a snapshot record.
6. Set the detailed **start time** and **end time**.
7. Click **Search** to search the snapshot. The content will show on the page.

Refer to **Figure 1-16** for layout and controls.

Figure 1-16 Snapshot page



Click **Download** to download the picture.
Tick the ID and click **Download All** to download the selected pictures.
Click  to view the detailed information about the snapshot.

Figure 1-17 Schedule snapshot

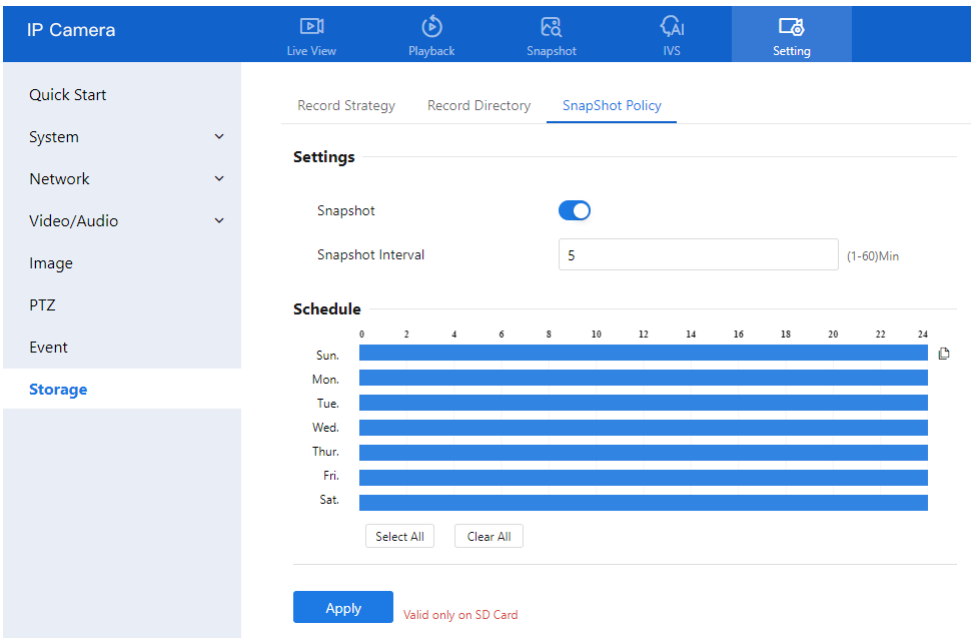


Figure 1-18 AI multi-target snapshot

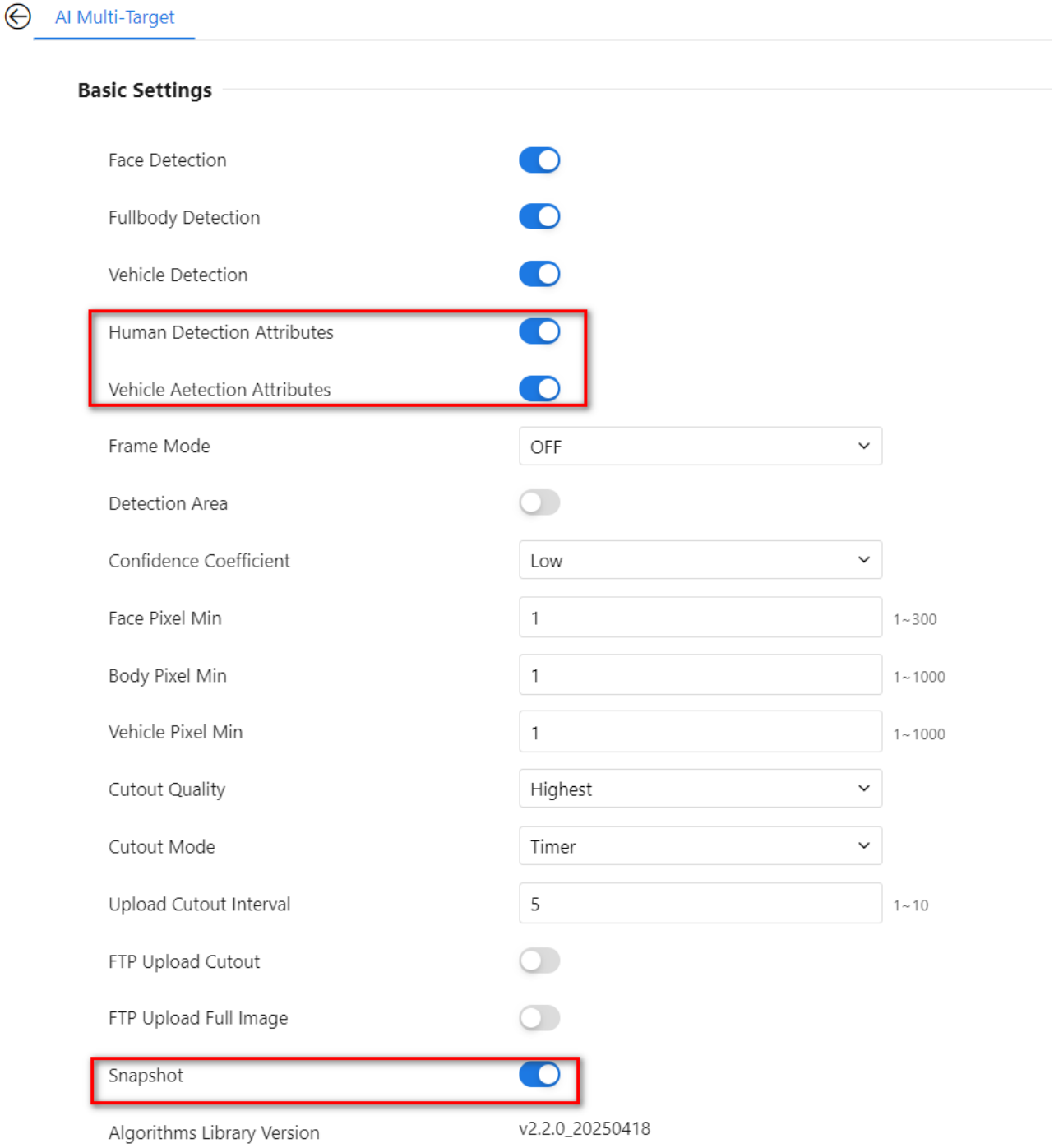
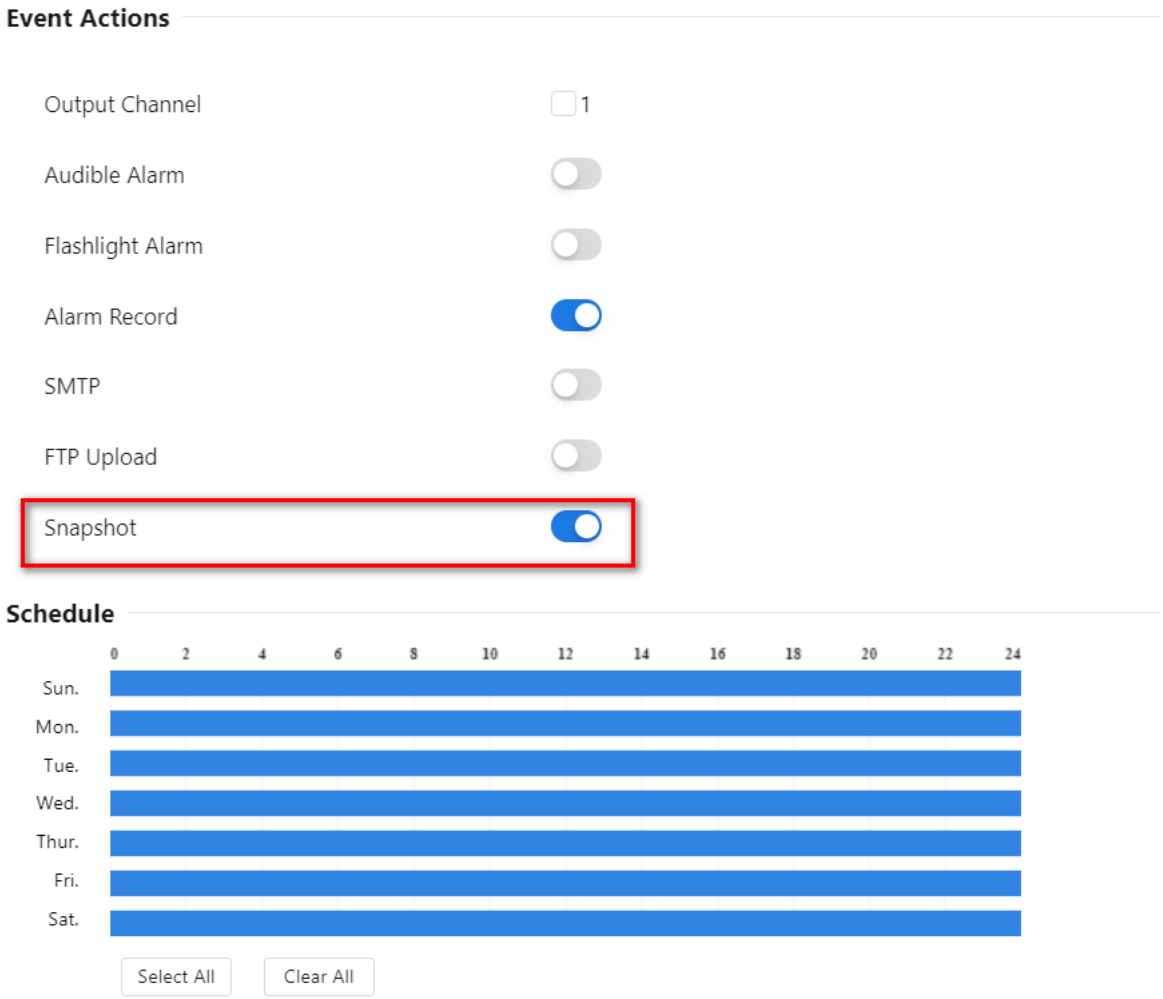


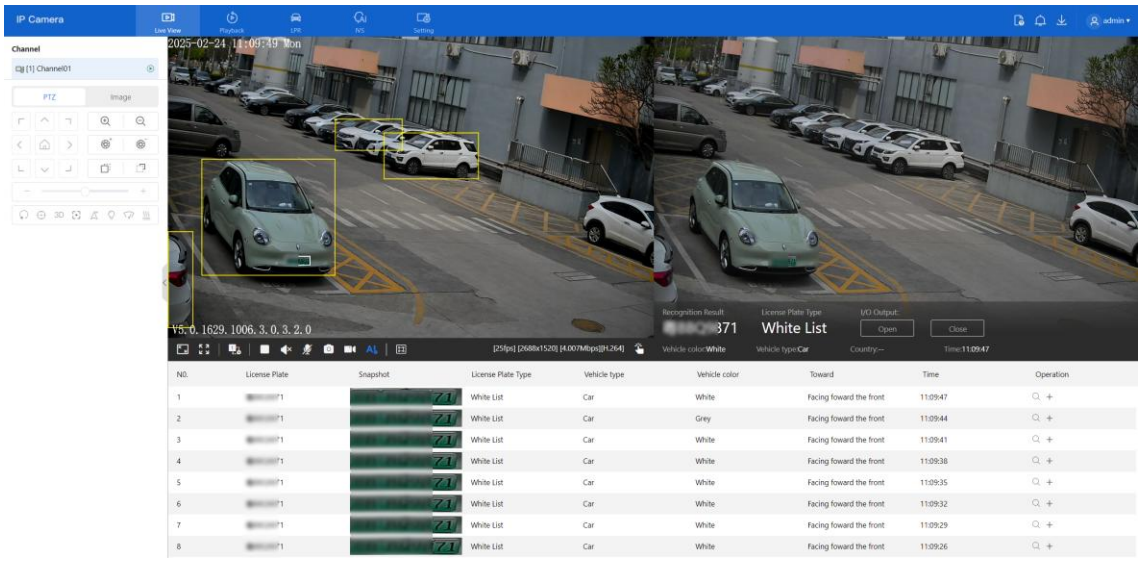
Figure 1-19 Alarm snapshot



1.7 LPR Setting

For LPR cameras, users can directly click on "LPR" on the web page to enter the LPR settings interface.

Figure 1-20 LPR



NOTE

The IVS features vary by device model. Refer to the product specification for supported functionality.

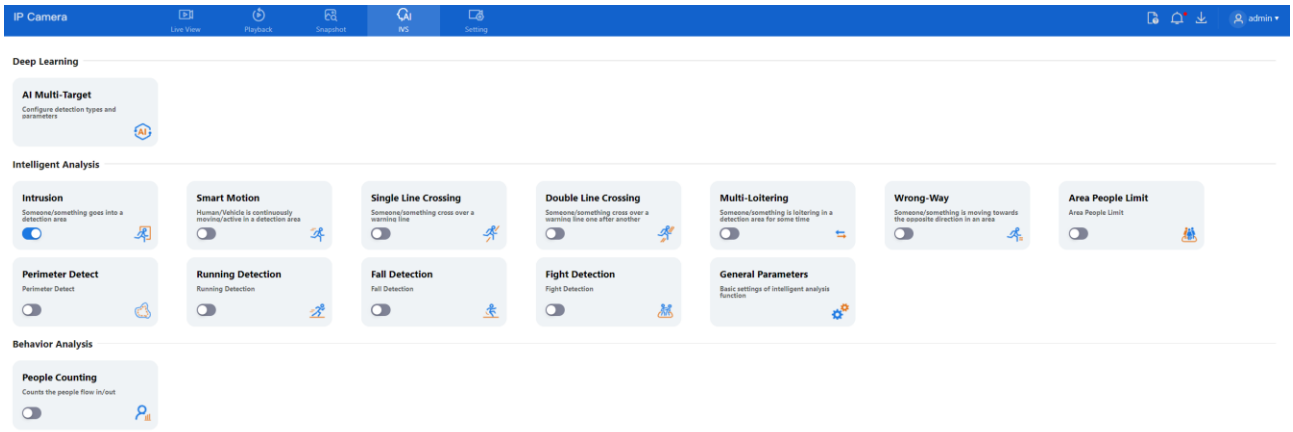
1.8 IVS Setting

Click **IVS** to access the IVS configuration page. You can configure:

- Deep learning settings
- Intelligent video analytics
- Behavior analysis features

Refer to **Figure 1-21** for the IVS setting layout.

Figure 1-21 IVS setting page



NOTE

The IVS features vary by device model. Refer to the product specification for supported functionality.

2 Quick Start Settings

2.1 Local Network

Description

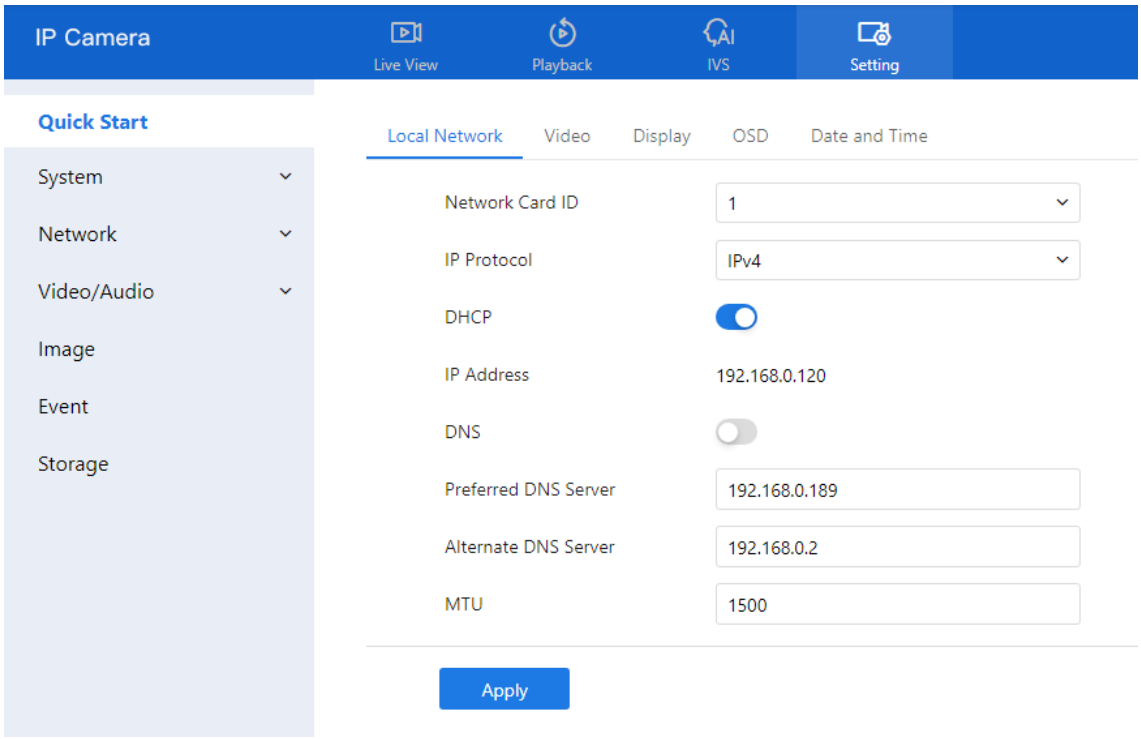
The local network settings include the following parameters:

- IP protocol
- IP address
- Subnet mask
- Default gateway
- Dynamic Host Configuration Protocol (DHCP)
- Preferred Domain Name System (DNS) server
- Alternate DNS server
- MTU (Maximum Transmission Unit)

Procedure

1. Navigate to **Setting > Quick Start > Local Network**. The **Local Network** page is displayed (see Figure 2-1).
2. Configure the parameters, as shown in Figure 2-1.

Figure 2-1 Local network page



Step 2 Set the parameters according to Table 2-1.

Table 2-1 Local network parameters

Parameter	Description	Setting
Network Card ID	--	[Default value] 1
IP Protocol	IPv4 is the IP protocol that uses an address length of 32 bits. IPv6 is the IP protocol that uses an address length of 64 bits.	[Setting method] Select a value from the drop-down list box. [Default value] IPv4
DHCP	Enable DHCP, and the device will automatically obtain the IP address from the DHCP server.	[Setting method] Click the button to enable **DHCP**. NOTE To query the current IP address of the device, you must query it on the platform based on the device name.
IP Address	Device IP address that can be set as required.	[Setting method] Enter a value manually. [Default value] 192.168.0.120
Subnet Mask	DHCP is off. Subnet mask of the network adapter.	[Setting method] Enter a value manually. [Default value] 255.255.255.0
Default Gateway	DHCP is off. This parameter must be set if the client accesses the device through a gateway.	[Setting method] Enter a value manually. [Default value] 192.168.0.1
Preferred DNS Server	DNS is on. IP address of a DNS server.	[Setting method] Enter a value manually. [Default value] 192.168.0.1
Alternate DNS Server	DNS is on. IP address of a domain server. If the preferred DNS server is faulty, the device uses the alternate DNS server to resolve domain names.	[Setting method] Enter a value manually. [Default value] 192.168.0.2

Parameter	Description	Setting
MTU	Set the maximum value of network transmission data packets.	[Setting method] Enter a value manually. NOTE The MTU value ranges from 1280 to 1500; the default value is 1500. Please do not change it arbitrarily.

Step 3 Click **Apply**.

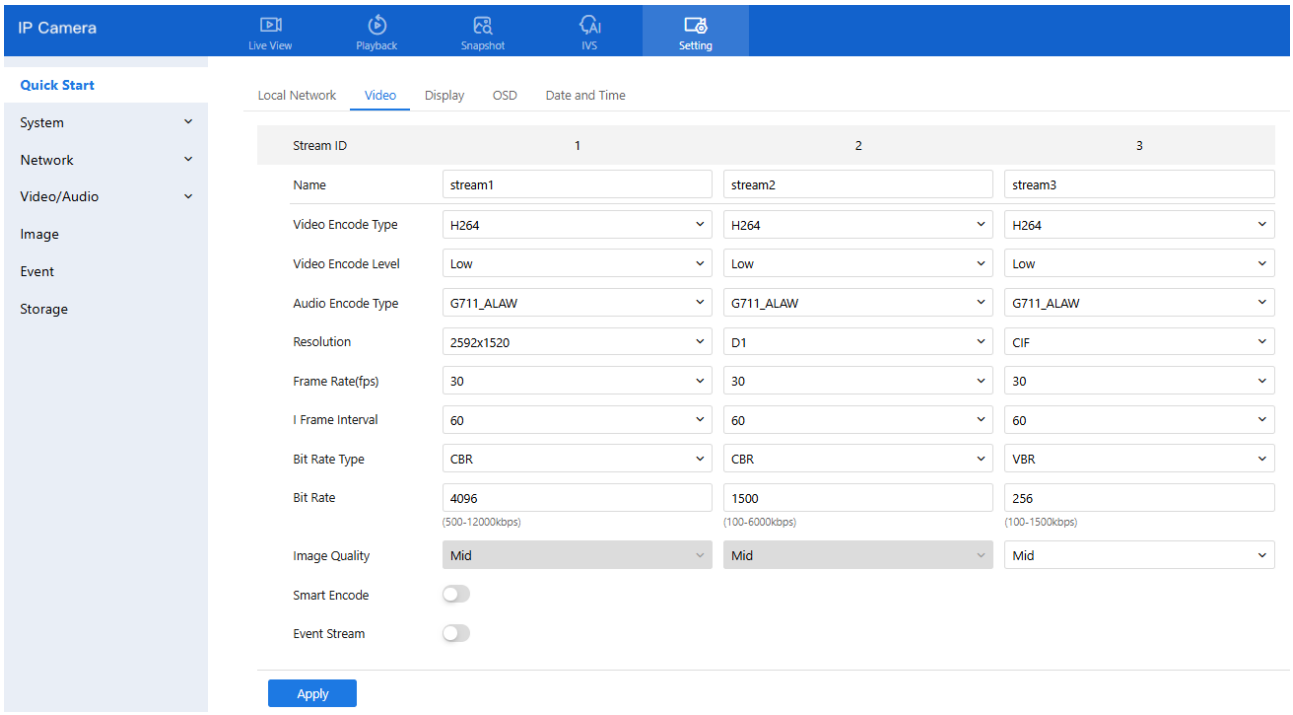
- If the message **"Apply success!"** appears, the system saves the configuration and displays: *"Set network parameter success, please log in to the system again."*
  Reconnect using the new IP address.
- If the message **"Parameter is invalid"** appears, please verify and correct the settings.

2.2 Video

Procedure

Step 1 Go to **Setting > Quick Start > Video**.
The **Video** settings page appears (see Figure 2-2).
Step 2 Configure the parameters according to **Table 2-2**.

Figure 2-2 Video setting page



Step 3 Set the parameters according to Table 2-2.

Table 2-2 Parameters of stream configuration

Parameter	Description	Setting
Stream ID	The device supports up to **three video streams**, depending on the model: • **Stream 1** provides the highest video quality and performance. It is typically used for primary viewing and recording. • **Stream 2** offers lower resolution options, suitable for bandwidth-limited scenarios or secondary viewing. • **Stream 3** delivers the lowest resolution and is ideal for preview purposes or mobile access. **Note:** Some models support only two streams.	[Setting method] Select a value from the drop-down list box.
Name	Stream name. NOTE The stream name must consist of letters, numbers, and underscores. Only these characters are supported.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes. [Default value] Stream 1

Parameter	Description	Setting
Video Encode Type	The video encoding type affects both image quality and the bandwidth required for streaming. The following encoding standards are supported: • **MJPEG** MJPEG (Motion JPEG) is an intra-frame compression format. It delivers high image quality without mosaic artifacts during motion. However, it does not support inter-frame compression, resulting in larger file sizes. MJPEG consumes significant storage and bandwidth, making it unsuitable for continuous recording or long-duration video transmission. It is best suited for capturing and transmitting alarm snapshots. • **H.264** H.264 is a widely-used inter-frame compression standard available in three profiles: **Base**, **Main**, and **High**. o **H.264 High Profile** offers the best compression efficiency but requires higher hardware decoding performance. o **H.264 Main Profile** balances quality and performance. o **H.264 Base Profile** has the lowest hardware requirements, suitable for devices with limited processing power. When using hardware decoders, select the profile according to the device's capabilities. • **H.265** H.265 is the next-generation video compression standard, improving upon H.264 with enhanced compression efficiency, better image quality, and more sophisticated algorithms. It significantly reduces bandwidth and storage usage while maintaining high visual fidelity, making it ideal for high-resolution and long-duration recording scenarios.	[Setting method] Select a value from the drop-down list box. [Default value] H.264 High Profile NOTE H.264 High Profile requires higher hardware decoding capability. Use the Main or Base Profile for low-performance devices. Using MJPEG in Stream 1 may result in playback issues or FTP video upload errors.
Audio Encode Type	The following audio encode standards are supported: □ G. 711_ULAW: mainly used in North America and Japan. □ G. 711_ALAW: mainly used in Europe and other areas. □ RAW_PCM: encode of the original audio data. This encoding is often used for platform data.	[Setting method] Select a value from the drop-down list box.
Resolution	A higher resolution means better image quality. NOTE IP cameras support different resolutions based on the model.	[Setting method] Select a value from the drop-down list box.

Parameter	Description	Setting
Frame Rate(fps)	Frame rate is the number of images, snapshots, or frames that a camera can take per second. The frames per second determine the smoothness of a video. A video whose frame rate is higher than 22.5 f/s is considered smooth by human eyes. Frame rates for different frequencies are as follows: □ 50 Hz: 1–25 f/s □ 60 Hz: 1–30 f/s NOTE The frequency is set on the **Device Configuration** > **Camera** page. The biggest MJPEG coding format frame rate is 12 frames per second.	[Setting method] Select a value from the drop-down list
I Frame Interval(f)	The I frame does not require other frames to decode. A smaller I-frame interval means better video quality but higher bandwidth.	[Setting method] Select a value from the drop-down list
Bit Rate Type	The bit rate is the number of bits transmitted per unit of time. The following bit rate types are supported: □ Constant bit rate (CBR) The compression speed is fast; however, an improper bit rate may cause vague motion images. □ Variable bit rate (VBR) The bit rate changes according to the image complexity. The encoding efficiency is high, and the definition of motion images can be ensured.	[Setting method] Select a value from the drop-down list box.
Bit Rate	Indicates the maximal value of the bit rate. The different models may have different ranges. Please refer to the actual product. The camera will automatically recommend a bit rate based on the selected resolution. If this bitrate does not meet the requirements, it can be manually modified.	[Setting method] Enter a value manually.
Image Quality	The video quality of the camera output.	[Setting method] Select a value from the drop-down list box.
Smart Encode	Smart Encode. □ Smart encode includes H.264 & H.265. □ The storage space will be reduced by fifty percent when smart encode is enabled. □ Only mainstream supports smart encode.	[Setting method] Click the button to enable **Smart Encode**.

Parameter	Description	Setting
Event Stream	Enable Event Stream. Set the event frame rate and event bit rate. It can be recording at the frame rate and bitrate set in the event stream, which facilitates recording with higher image quality when an alarm occurs. During normal periods, recording can be done according to the parameters set above.	[Setting method] Click the button to enable **Event Stream**.

Step 4 Click **Apply**.

- If you see **"Apply success!"**, the settings are saved.
- If **"Apply failed!"** appears, ensure you have *Parameter Configure* permissions (see **Section 3.3 Configure User**).
- If a **bit rate error** is shown, enter a valid bit rate value.

2.3 Display

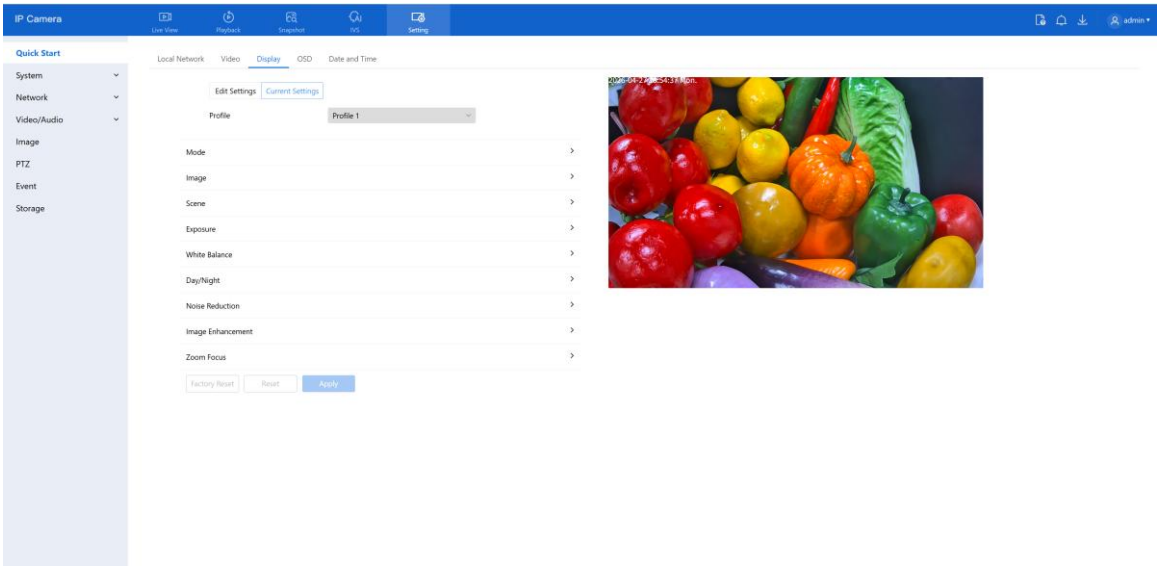
2.3.1 Access the Display Settings

Procedure:

Step 1 Navigate to **Setting > Quick Start > Display**.

The **Image Settings** page appears.

Figure 2-3 Image settings page



Step 2 Click **Edit Settings** under the **Mode** item to configure display profiles. Up to four profiles can be set.

NOTE

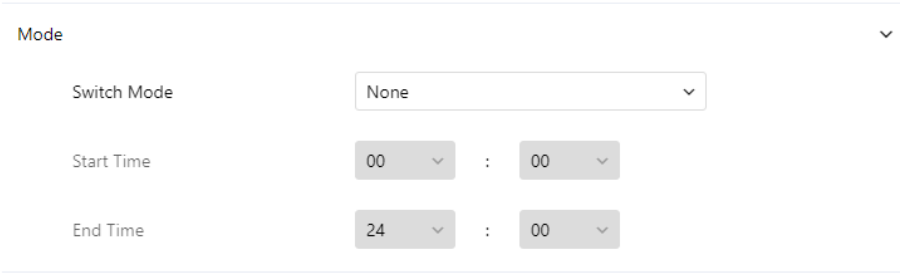
- All image settings can be modified in **Edit Settings**.
- Factory Reset restores all parameters to factory defaults.
- **Reset** reverts settings to the last saved state.

2.3.2 Mode

Procedure:

Step 1 Go to **Setting > Quick Start > Display > Mode**.
The **Mode** page appears, as shown in Figure 2-4.

Figure 2-4 Mode page



Step 2 Click **Switch Mode**. Three options are available:

- **None**: Uses the current active profile with no switching.
- **Time Mode**: Automatically switches profiles at specific times. Set all four profiles in advance.
- **Day/Night (D/N) Linkage Mode**: Automatically switches between day and night profiles based on lighting. When the Day/Night is set to Auto, it is Day mode, which executes Profile 1; When it is Night mode, it executes Profile 2. The specific switching conditions usually depend on the strength of the ambient light, and the camera automatically judges and switches modes through its built-in light sensor.

Step 3 Set the **Start Time** and **End Time** for switching.
Step 4 Click **Apply** to save your settings.

2.3.3 Image Setting

Procedure:

1. Navigate to **Setting > Quick Start > Display > Image**, as shown in Figure 2-5.

Figure 2-5 Image setting page



2. Set the **image setting** parameters as per Table 2-3.

Table 2-3 Parameters of image settings parameters

Parameter	Description	Configuration Method
Brightness	Controls image brightness.	[Setting method] Drag the slider. [Default value] **50**
Saturation	Controls image color richness.	[Setting method] Drag the slider. [Default value] **50**
Sharpness	Controls image clarity.	[Setting method] Drag the slider. [Default value] **50**
Contrast	Adjusts contrast between dark and bright areas.	[Setting method] Drag the slider. [Default value] **50**

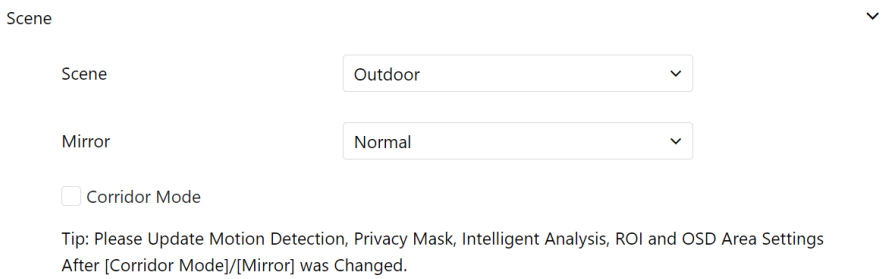
3. Click **Apply** to save your settings.

2.3.4 Scene Mode

Procedure:

1. Go to **Setting > Quick Start > Display > Scene,** as shown in Figure 2-6.

Figure 2-6 Scene mode page



2. Set the FFC mode parameters as per Table 2-4.

Table 2-4 Parameters of FFC

Parameter	Description	Configuration Method
Scene	It indicates the working mode of the camera. □ Outdoor: Suitable for outdoor use. □ Indoor: Suitable for indoor use.	[Configuration method] Select from the drop-down list [Default value] **Outdoor**
Mirror	It is used to select the pixel location of an image. □ Normal: The image does not flip. □ Horizontal: The image flips to the left and right. □ Vertical: The image flips up and down. □ Horizontal and vertical: The image rotates at 180°.	[Setting method] Select a value from the drop-down list. [Default value] **Normal**
Corridor Mode	The image rotates 90°clockwise when aisle mode is enabled. On some models, using Stream 2/3 with H.264/H.265 at CIF or QVGA resolution may prevent live view playback.	[Setting method] Tick the corridor mode. [Default value] Disable

Step 2 Click **Apply** to save the setting.

2.3.5 **Exposure**

Procedure:

Step 1 Navigate to **Setting > Quick Start > Display > Exposure**.

The **Exposure** page appears (see Figures 2-7 and 2-8 for IP cameras and high-speed domes, respectively).

Step 2 Configure the parameters listed in **Table 2-5**.

Figure 2-7 Exposure interface

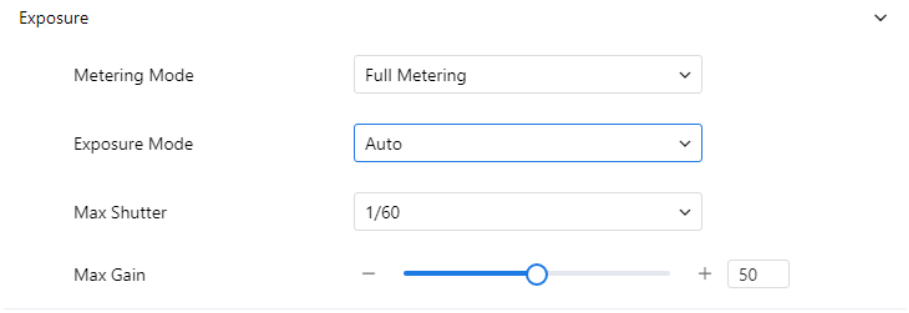


Figure 2-8 Exposure Interface for high-speed home

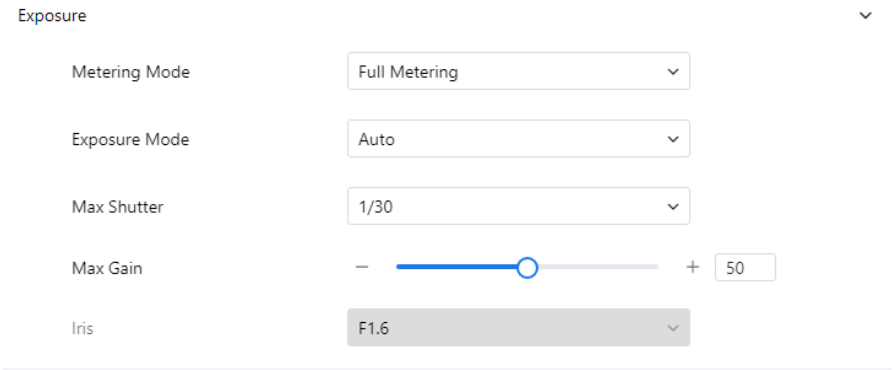


Table 2-5 Parameters of exposure

Parameter	Meaning	Configuration Method
Exposure Mode	The exposure modes include: □ **Auto**: The system performs auto exposure based on the monitoring environment. □ **Manual**: You can adjust the brightness of an image by setting the following three items: **Shutter Setting**, **Iris Setting,** and **Gain Setting**. □ **Shutter Priority**: You can set the **Shutter Setting** to fixed values. The iris and gain are automatically adjusted by the system. □ **Iris Priority (for high-speed dome):** You can set Iris Setting to fixed values. The shutter and gain are automatically adjusted by the system.	[Setting method] Select a value from the drop-down list. [Default value] **Auto**
Meter Mode	It is used to select the metering area. □ **Fulling Metering**: During metering, all areas of an image have equal weight; that is, all areas are involved in the metering. **Spot Metering**: During metering, the central spot of an image has the highest weight. □ **Partial Metering**: During metering, the middle area (1/2 of the total area) of an image has the highest weight, and other areas have the lowest weight.	[Setting method] Select a value from the drop-down list. [Default value] **Whole**
Max Shutter	The device automatically adjusts the shutter time based on the ambient brightness. The shutter time is less than or equal to the value of this parameter.	[Setting method] Select a value from the drop-down list. [Default value] **1/25**

Parameter	Meaning	Configuration Method
Max Gain	The device automatically adjusts the gain based on the external light. The gain is less than or equal to the value of this parameter.	[Setting method] Drag the slider. [Default value] **50**
Iris (for high-speed dome)	It is valid in manual mode and iris priority mode. You can adjust the brightness of an image by setting the iris. As the value increases, the brightness increases (when the shutter and gain remain the same). However, the camera movement automatically adjusts the shutter and gain in this mode. Therefore, the brightness of an image may not increase when you increase the iris.	[Setting method] Select a value from the drop-down list. [Default value] **F1.6**
Iris（for IP camera）	It is used to control the light admitted to the lens. The auto iris can be set to either of the following states: □ **Auto** The iris is automatically adjusted to control the light admitted to the lens. □ **Open fully** The iris is fully open.	[Setting method] Select a value from the drop-down list. [Default value] **Auto**
Iris Speed	It indicates the auto-adjustment speed of the iris. As the value increases, the speed increases. Excessive speed may cause instability. NOTE This parameter is valid when the auto iris is enabled.	[Setting method] Drag the slider. [Default value] **50**
Fixed Gain	When the exposure Mode is Manual, you can set the fixed gain.	[Setting method] Drag the slider. [Default value] **50**

Step 3 Click **Apply** to save the setting.

2.3.6 **White Balance Setting**

Procedure:

Step 1 Navigate to **Setting > Quick Start > Display > White Balance**.
The **White Balance** page appears as shown in Figure 2-9.

Figure 2-9 White balance settings page

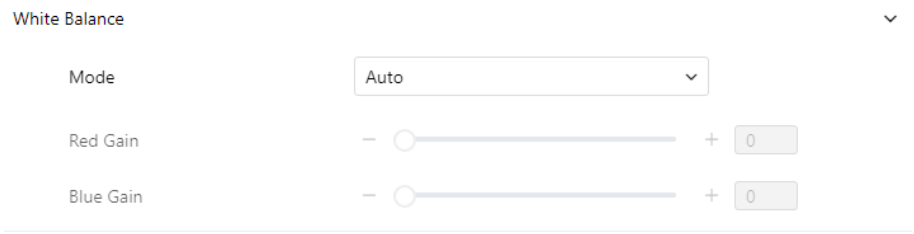


Table 2-6 White Balance (WB) Parameters

Parameter	Meaning	Configuration Method
Mode	Select a white balance mode to improve color accuracy based on lighting conditions: - **Auto**: The system automatically adjusts based on the environment. - **Tungsten:** For incandescent lighting. - **Fluorescent:** For fluorescent lighting. - **Daylight:** For natural sunlight. - **Shadow:** For shaded areas. - **Manual**: Manually configure WB mode based on the monitoring environment.	[Setting method] Select a value from the drop-down list. [Default value] **Auto**
Red Gain	Adjusts the intensity of red tones. Increasing this value lowers the color temperature. NOTE Available only in **Manual Mode** with **Customized** selected.	[Setting method] Drag the slider. [Default value] **0**
Blue Gain	Adjust the intensity of blue tones. Increasing this value raises the color temperature (image becomes cooler). NOTE Available only in **Manual Mode** with **Customized** selected.	[Setting method] Drag the slider. [Default value] **0**

Step 2 Click **Apply** to save the setting.

2.3.7 **Day/Night**

Procedure:

Step 1 Navigate to **Setting > Quick Start > Display > Day/Night**.

The **Day/Night** settings page appears. Display options may vary by device model (see Figure 2-10).

Figure 2-10 Day/Night page (timer)

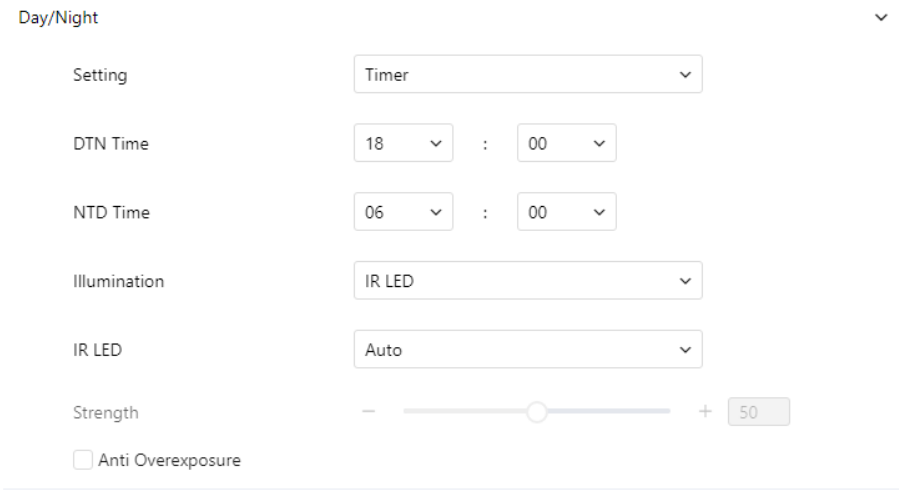
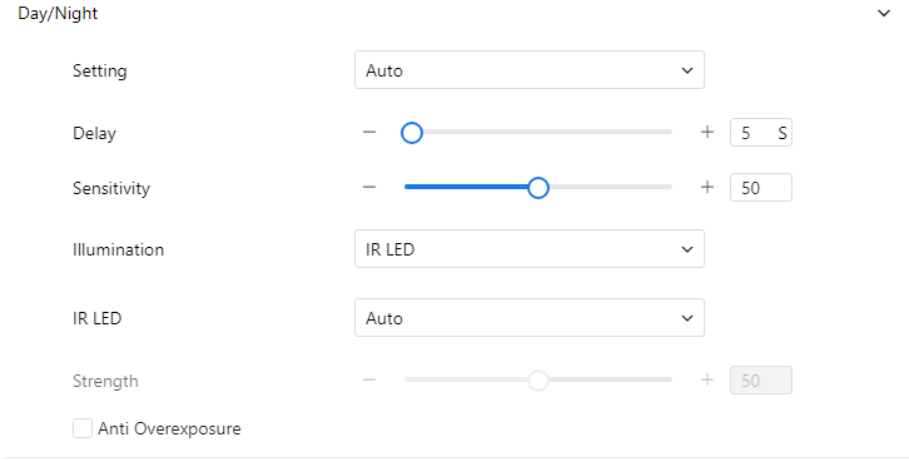


Figure 2-11 Day/Night mode page (auto)



Step 2 Configure the parameters listed in **Table 2-7**.

Table 2-7 Parameters of Day/Night

Parameter	Meaning	Configuration Method
D/N Setting Mode	It can be set to **Auto**, **Day**, **Night,** or **Timer**. □ Auto mode The image color and filter status automatically switch based on the ambient brightness. The filter keeps infrared light from reaching the sensor during the day; The filter allows all light to reach the sensor at night. □ Day mode Forces the camera to stay in **color mode**. The IR filter remains active, blocking infrared light from reaching the sensor. □ Night mode Forces the camera to display in **black and white**. The IR filter is disabled, allowing infrared light to reach the sensor for better night vision. □ Timer Automatically switches between Day and Night modes based on a user-defined schedule.	[Setting method] Select a value from the drop-down list. [Default value] **Auto**
D/N Switch Sensitivity	Adjusts the sensitivity of day-to-night switching. A higher value causes the system to switch at lower light levels. NOTE This parameter is valid in auto mode.	[Setting method] Drag the slider. [Default value] **50**
TRANSI. (D->N) (dB)	High-Speed Dome Gain threshold for switching from Day to Night in Auto mode. The system enters Night mode when the gain exceeds this value. NOTE This parameter is valid in auto mode. The value of **TRANSI.(D->N)** must be greater than the value of **TRANSI.(N->D)**.	[Setting method] Drag the slider. [Default value] **70**
TRANSI. (N->D) (dB)	High-speed Dome Gain threshold for switching from Night to Day. The system enters Day mode when the gain drops below this value. NOTE This parameter is valid in auto mode. The value of **TRANSI.(D->N)** must be greater than the value of **TRANSI.(N->D)**.	[Setting method] Drag the slider. [Default value] **30**

Parameter	Meaning	Configuration Method
Delay(s)	Delay time (in seconds) for switching between Day and Night. NOTE This parameter is valid in auto mode.	[Setting method] Drag the slider. [Default value] **0**
Light Mode	Specifies the lighting mode based on the camera model: **IR LED** **White LED** **Intelligent Dual Light** (uses IR and White LED based on condition) **None**	[Setting method] Select a value from the drop-down list.
IR LED	**Auto**: The infrared lamp is enabled or disabled based on the external environment identified by the light-dependent resistor (LDR). **ON**: The system enters the night mode forcibly. **OFF**: The infrared lamp is disabled. The filter and image color are switched based on the external environment identified by the LDR. NOTE This parameter is valid in auto mode.	[Setting method] Select a value from the drop-down list. [Default value] **Auto**
Strength	Controls IR LED brightness. Higher values produce brighter night images.	[Setting method] Drag the slider. [Default value] **50**
DTN Time	Time to switch from Day to Night.	[Setting method] Select a value from the drop-down list. [Default value] **18:00**
NTD Time	Time to switch from Night to Day.	[Setting method] Select a value from the drop-down list. [Default value] **6:00**

Parameter	Meaning	Configuration Method
Anti Overexposure	When checked, the camera activates overexposure prevention, compensating for overexposed areas to achieve a more balanced overall image.	[Setting method] Tick

Fill light settings

The camera's fill light supports four modes:

1. **Intelligent Dual Light** – Automatically switches from IR to white light during alarms, then reverts after 30 seconds.
2. **Warm Light** – Uses only white light for nighttime illumination.
3. **Infrared Lamp** – Uses IR light only.
4. **Close** – Disables the fill light. The image remains in the last active mode.

Modes of Operation

- **Day Mode**: Used in well-lit environments where the image remains in color. No fill light is needed.
- **Night Mode**: Used in low-light environments with the fill light enabled.
- **Auto Mode**: Automatically adjusts the fill light based on ambient lighting.
- **Timer Mode**: Allows you to define the active time for Day mode.

Brightness Adjustment

- **Automatic Mode**: Adjusts fill light brightness automatically based on the environment.
- **Manual Mode**: You can manually set the brightness using the slider or input value.

2.3.8 **Noise Reduction**

Procedure:

Step 1 Go to **Setting > Quick Start > Display > Noise Reduction**.
Step 2 The Noise Reduction interface will appear (see Figure 2-12).

There are two modes available for noise reduction: **Auto** and **Manual**.

- **Auto Mode**: The system automatically adjusts noise reduction levels based on ambient conditions.
- **Manual Mode**: You can set a fixed level of noise reduction.

Figure 2-12 Noise reduction page (auto)

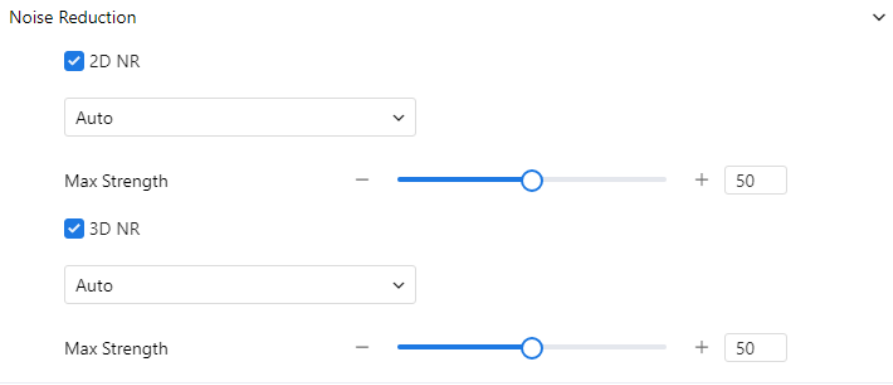


Figure 2-13 Noise reduction page (manual)

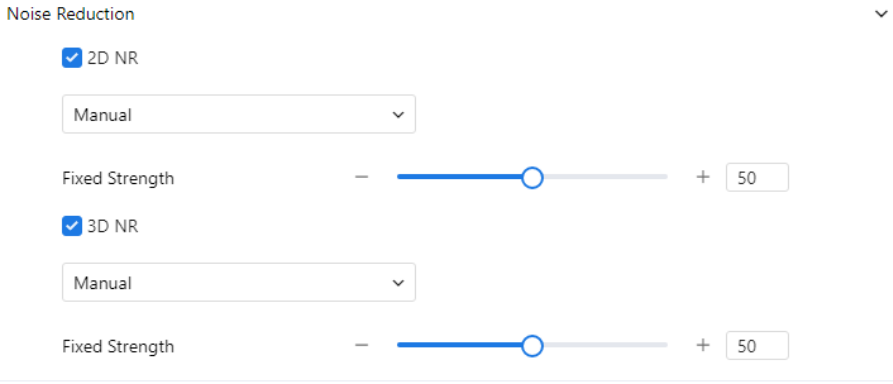


Table 2-8 describes the Noise Reduction parameters.

Table 2-8 Parameters of noise reduction

Parameter	Meaning	Configuration Method
2D NR	Reduces the noise of the image.	[Configuration method] Select from the drop-down list [Default value] **Auto**
3D NR	Reduces the noise of the image.	[Configuration method] Select from the drop-down list [Default value] **Auto**

Parameter	Meaning	Configuration Method
Max Strength	Applicable only in auto noise filter mode. When set to **0**, noise reduction is disabled. When set above **0**, the system automatically adjusts the noise reduction level based on ambient brightness, but will not exceed the configured value.	[Setting method] Drag the slider. [Default value] **50**
Fixed Strength	Applicable only in manual noise filter mode.	[Setting method] Drag the slider. [Default value] **50**

Step 3 Click **Apply** to save the setting.

2.3.9 **Image Enhancement**

Procedure:

Step 1 Go to **Setting > Quick Start > Display > Image Enhancement.**
Step 2 Adjust the parameters listed in Table 2-9.

Figure 2-14 Image Enhancement page



Table 2-9 Parameters of enhance image

Parameter	Meaning	Configuration Method
WDR	Enhances image quality in scenes with strong lighting contrast between foreground background. When brightness contrast is high, increasing the WDR level improves both bright and dark areas.	[Setting method] Tick the WDR mode and drag the slider. [Default value] **50**
HLC	Reduces the intensity of overly bright areas to improve visibility of objects in front of light sources (e.g., headlights). Reduces total brightness to enhance clarity of highlighted regions.	[Setting method] Tick the HLC mode and drag the slider. [Default value] **50**
BLC	Increases overall brightness to make objects in front of backlit scenes more visible. May cause overexposure of the background.	[Setting method] Tick the BLC mode and drag the slider. [Default value] **50**
Anti-shake	Reduces slight shaking or jitter in the image caused by minor camera movement.	[Setting method] Tick the Anti-shake mode.
DeFog	Enhances image clarity in foggy or hazy environments. Higher values increase visibility. **Note**: Available only on some models.	[Setting method] Tick the Defog mode and drag the slider. [Default value] **50**

Step 3 Click **Apply** to save the settings.

2.3.10 **Zoom Focus (Only for Some Models)**

Procedure:

Step 1 Navigate to **Setting > Quick Start > Display > Zoom Focus**.
The **Zoom Focus** interface appears (see Figure 2-15 for IP cameras and Figure 2-16 for high-speed domes).
Step 2 Configure the parameters listed in **Table 2-10**.

Figure 2-15 Zoom focus page for IP camera 1

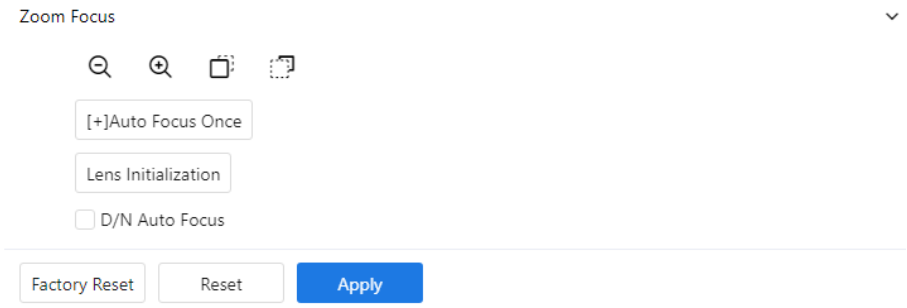


Figure 2-16 Zoom focus interface for high-speed dome

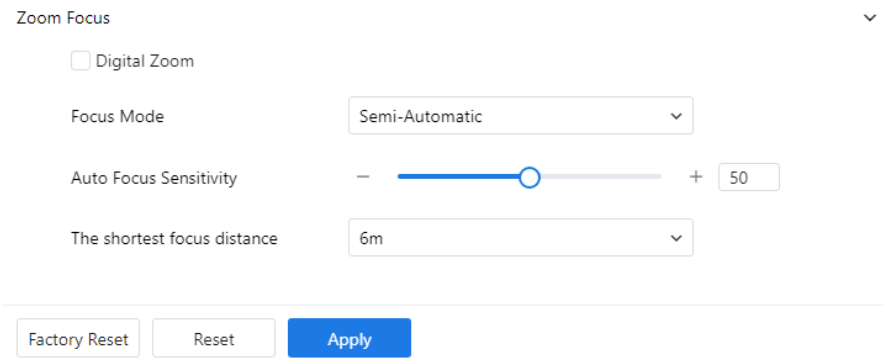


Table 2-10 Parameters of zoom focus

Parameter	**Meaning**	**Configuration Method**
D/N Auto Focus	Enables auto focus when switching between Day and Night modes.	[Setting method] Tick the Auto focus.
Auto Focus Once	Triggers auto focus one time.	[Setting method] Click the button.
Initial	Returns the camera lens to its initial position.	[Setting method] Click the button.
Digital	Enables digital zoom after 37x optical zoom is reached.	[Setting method] Tick the Digital.

Parameter	Meaning	Configuration Method
Focus Mode	Sets the focus mode: • **Auto**: System automatically adjusts focus based on the scene. • **Manual**: The user manually adjusts focus using on-screen controls. • **Semi-Automatic**: Auto focus is triggered once when the PTZ moves or zooms in.	[Configuration method] Select from the drop-down list [Default value] **Semi-automatic**
Auto Focus Sensitivity	Controls how easily the system re-focuses when changes occur in the image. Higher sensitivity means the camera will re-focus with minor scene changes.	[Setting method] Drag the slider. [Default value] **50**
The Least Focus Distance	Defines the minimum distance at which the camera can focus. If the object is closer than this distance, the camera will not focus on it. Example: If set to 1.5 meters, objects must be more than 1.5 meters away to be in focus. NOTE Applicable only to visible light.	[Configuration method] Select from the drop-down list [Default value] **3 m**

Step 3 Click **Apply** to save the settings.

2.4 OSD

Description

The **On-Screen Display (OSD)** function allows you to overlay information on video streams, including:

- Device name
- Channel ID and name
- Time
- Customized content

You can drag and reposition OSD elements on the screen.

Note: When the resolution is set to D1 or CIF, OSD supports up to **22 characters**.
OSD supports **Simplified Chinese**, **English**, **numbers**, and **select special characters**.

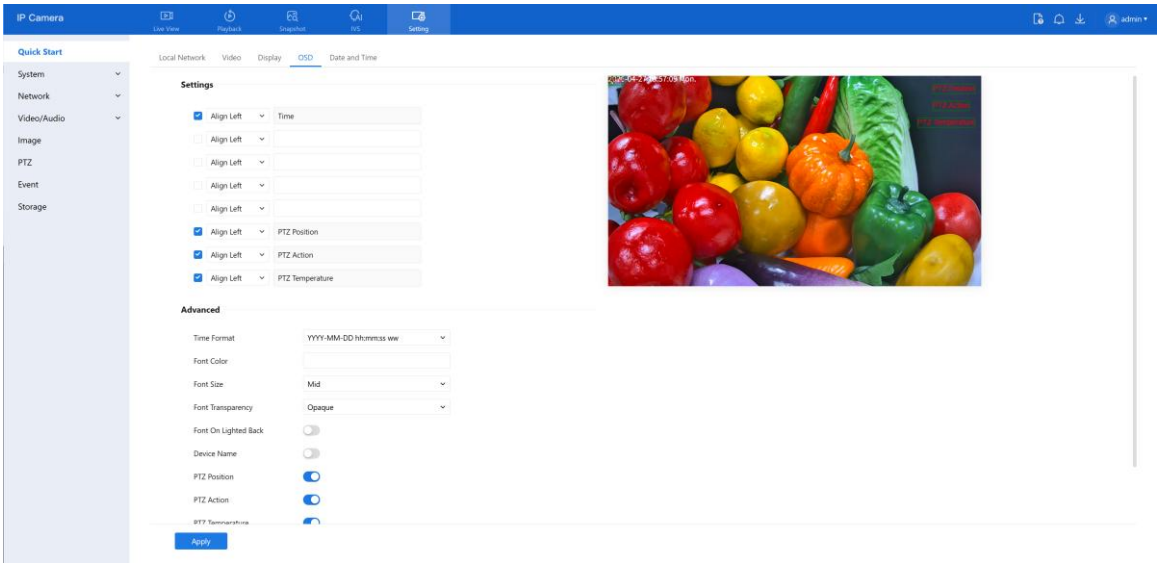
Procedure

Step 1 Go to **Setting > Quick Start > OSD**.

The OSD page is displayed (see Figure 2-17).

Step 2 Configure the parameters listed in **Table 2-11**.

Figure 2-17 OSD (PTZ cameras)



NOTE

Up to **seven OSD display areas** can be configured.

Table 2-11 Parameters of OSD

Parameter	Description	Setting
Time	Enables display of the system time.	[Setting method] Tick the time.
Focusing on the State	Displays focusing status. NOTE: Available only for cameras with auto-focus lenses.	[Setting method] Tick the Focusing on the state.
Custom OSD	Allows you to add a custom line of text.	[Setting method] 1. Tick the custom OSD list. 2. Enter the characters. Click ✔ to save the value.
Time Format	Defines the display format of the time.	[Setting method] Select a value from the drop-down list box. [Default value] YYYY-MM-DD hh:mm:ss ww

Parameter	Description	Setting
Font Color	Sets the color of the displayed text.	[Setting method] Select a value from the drop-down list box. [Default value] Blank
Font Size	Sets the size of the text.	[Setting method] Select a value from the drop-down list box. [Default value] Mid
Font Transparency	Controls the transparency of the OSD text.	[Setting method] Select a value from the drop-down list box. [Default value] Opaque
Font on Lighted Back	Enables background lighting for better text visibility.	[Setting method] Click the button to enable **Font on the lighted back**.
Device Name	Displays the device name in the video.	[Setting method] Click the button to enable **Device Name**
PTZ Position	Only used for PTZ cameras	[Setting method] Click the button to enable
PTZ Action		[Setting method] Click the button to enable
PTZ Temperature		[Setting method] Click the button to enable
Status Display of Focus	Shows live focusing status on the screen.	[Setting method] Click the button to enable
Twelve-hour System	Enables 12-hour clock format.	[Setting method] Click the button to enable
Display Week	Enables the display of the current weekday.	[Setting method] Click the button to enable

Step 3 Click **Advanced** to configure additional options such as:

- Time Format
- Font Color
- Font Transparency

- Font Background

Step 4 Click **Apply**.

The message **"Apply success!"** confirms that the settings have been saved.

2.5 Date and Time

Description

The **Date and Time** page allows you to configure the system's date, time, and synchronization settings. The following parameters can be adjusted:

- Time zone and Daylight Saving Time (DST)
- Date and time (manual or synchronized)
- Network Time Protocol (NTP) server settings

Procedure

Step 1 Go to **Setting > Quick Start > Date and Time**.

The **Date and Time** page appears, as shown in Figure 2-18.

Step 2 Configure the parameters listed in Table 2-12.

Figure 2-18 Date and time page

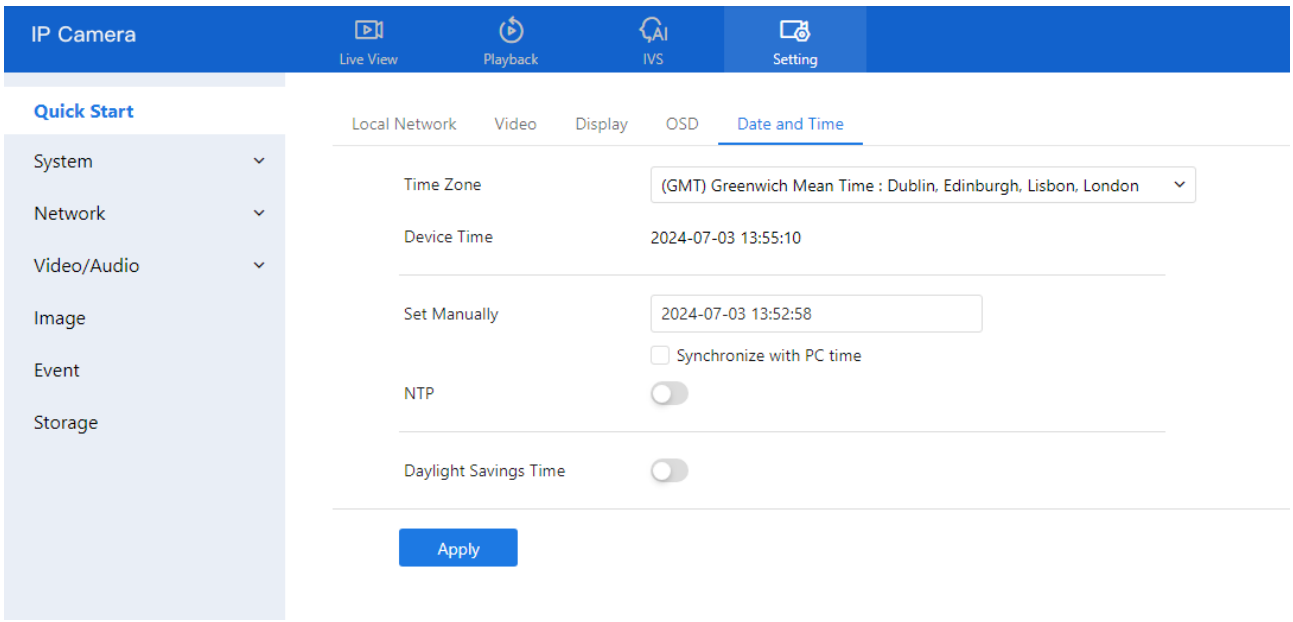


Table 2-12 Parameters of date and time

Parameter	Description	Setting
Time Zone	Sets the time zone of the device. N/A	[Setting method] Select a value from the drop-down list box. [Default value] Greenwich Mean Time

Parameter	Description	Setting
Device Time	Displays the current time on the device.	[Setting method] □ Synchronize the time from the PC. Enter a value manually.
Set Manually	You can set the device time manually or synchronize with PC time.	[Setting method] Click **Set Manually** and set the date and time in the format *YYYY-MM-DD HH:MM: SS.*
NTP	IP address or domain name of the NTP server.	[Setting method] Click the button to enable **NTP** and enter a value manually.
Server Address	NTP is enabled. The NTP server IP.	[Setting method] Enter a value manually.
Port	NTP is enabled. Port number of the NTP server.	[Setting method] Enter a value manually. [Default value] **123**
Interval	NTP is enabled. Set a time interval to check if the device time has synchronized with the NTP server time.	[Setting method] Enter a value manually. [Default value] **60**
Daylight Saving Time	Adjusts the device time for DST: • When DST starts, the device time is moved forward by one hour. • When DST ends, the device time is moved back by one hour.	[Setting method] Click the button to enable **Daylight Saving Time**.

Step 3 Click **Apply** to save the settings. If the message **"Apply success!"** appears, the settings have been saved successfully.

3 System Settings

3.1 Settings

3.1.1 Device Information

Description

The **Device Information** page displays the following system details:

- Device ID, name, type, model, manufacturer name, and MAC address
- Hardware version and software version
- Video channel count, alarm input/output channel count, serial port count, and number of network cards

NOTE

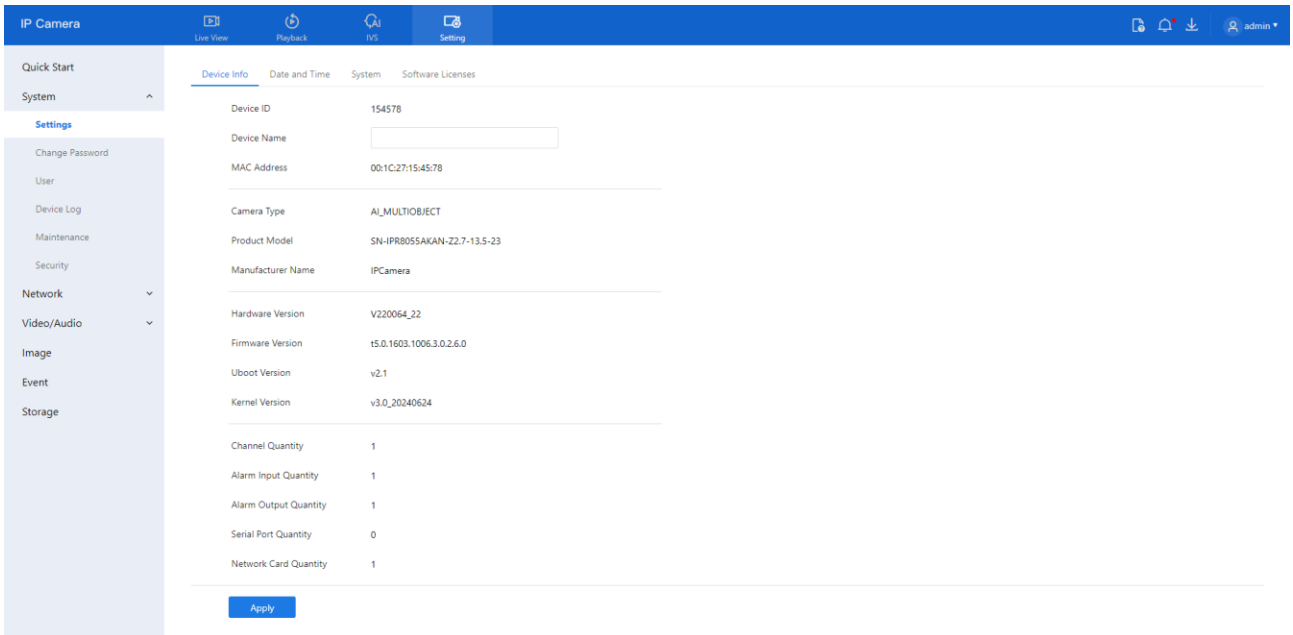
- The device name is the only editable field.
- All other parameters are view-only.
- Device information updates automatically after a software upgrade

Procedure

Step 1 Go to **Setting > System > Settings > Device Info**.

The **Device Info** page is displayed, as shown in Figure 3-1.

Figure 3-1 Device info page



Step 2 View the system information and set the **Device Name** as needed, according to Table 3-1.

Table 3-1 Parameters of the device

Parameter	Description	Setting
Device ID	A unique identifier used for platform management.	[Setting method] The parameter cannot be modified.
QR Code	The code and code characters. NOTE Available on some models.	Click the icon to enlarge the code.
P2P	Enables peer-to-peer (P2P) connection. When the device's P2P status is "Online", users can manage it via mobile apps. NOTE Available on some models.	[Setting method] Enable
Device Name	The name used to identify the device. NOTE Maximum length is **32 bytes** or **10 Simplified Chinese characters**. Modification fails if exceeded.	[Setting method] Enter a value manually.
MAC Address	It shows the performance of the camera	[Setting method] These parameters cannot be modified.
Camera Type		
Product Model		
Manufacturer Name		
Hardware Version		
Firmware Version		
Uboot version		
Kernel version		
Video Channel(s)		
Channel Quantity		
Alarm Input Quantity		
Alarm Output Quantity		
Serial Port Quantity		

Parameter	Description	Setting
Network card Quantity		

Step 3 Click **Apply**.

- If the message **"Apply success!"** appears, the settings have been saved.
- If **"Apply failed!"** appears, you must request **Parameter Configure** permissions from an administrator.

3.1.2 Date and Time

For detailed information, please refer to **Chapter 2.5**

3.1.3 System

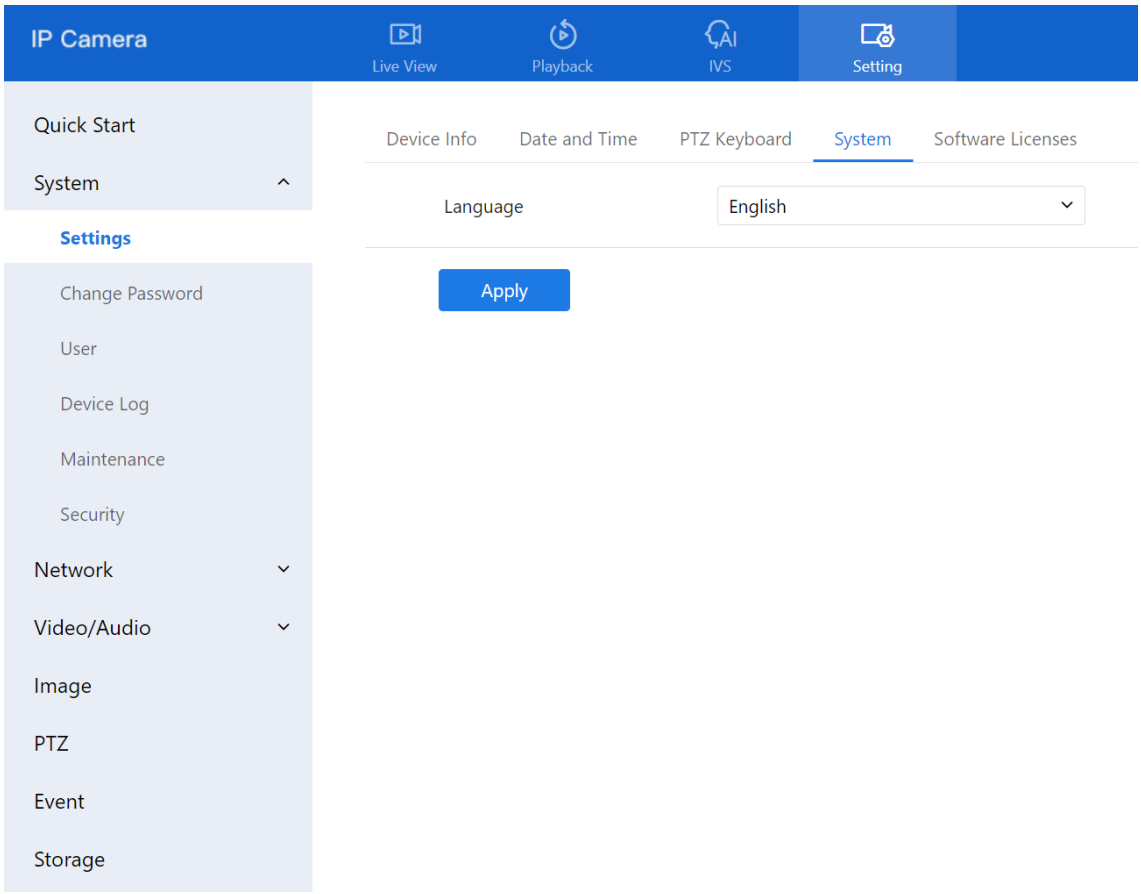
Procedure:

Step 1 Go to **Setting > System > Settings > System.**

The **System** page is displayed (see Figure 3-2).

Step 2 Choose the language from the drop-down list.

Figure 3-2 System



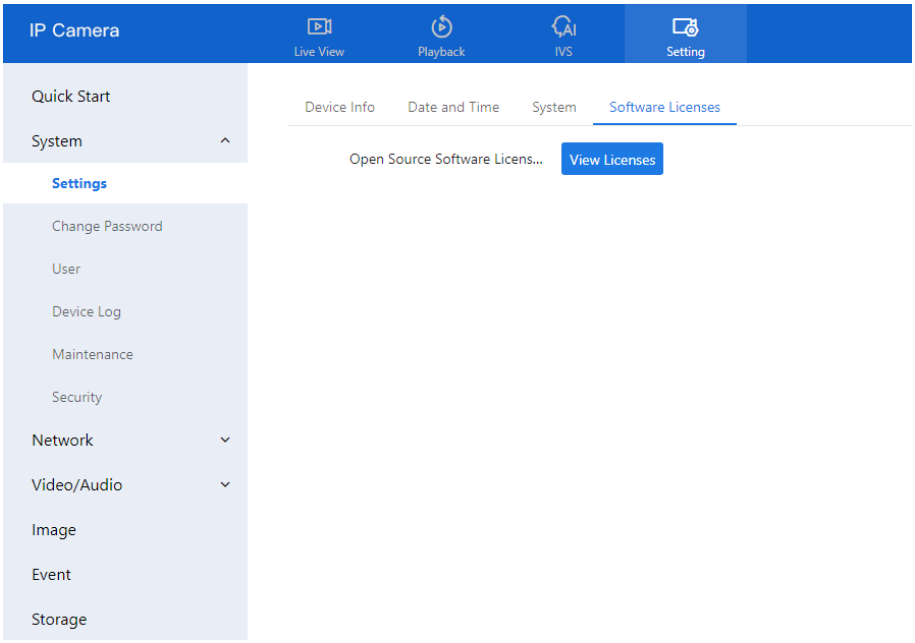
3.1.4 Software Licenses

Procedure

Step 1 Go to **Setting > System > Settings > Software Licenses**.

The **Software Licenses** page is displayed, as shown in Figure 3-3.

Figure 3-3 Software licenses page



Step 2 Click **View Licenses** to display the list of open-source software licenses used in the system.

3.2 Change Password

1.3 For detailed information, please refer to **Chapter 1.2**.

3.3 Configure User

3.3.1 Add User

Description

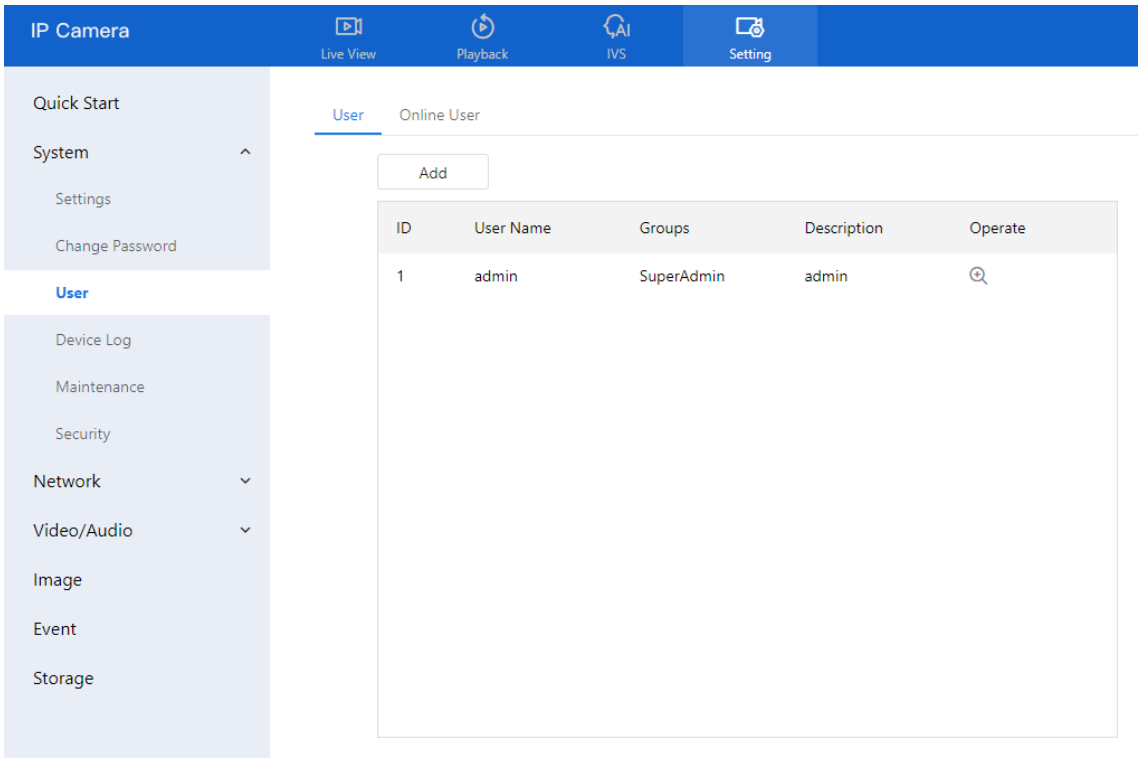
This function allows you to add, modify, or delete users in the **Privilege Manager** section.

Procedure

Step 1 Navigate to **Setting > System > User**.

The **User** page is displayed, as shown in Figure 3-4. Table 3-2 describes the parameters.

Figure 3-4 User page



Step 2 Add, modify, or delete users as needed.

Table 3-2 Parameters of the user

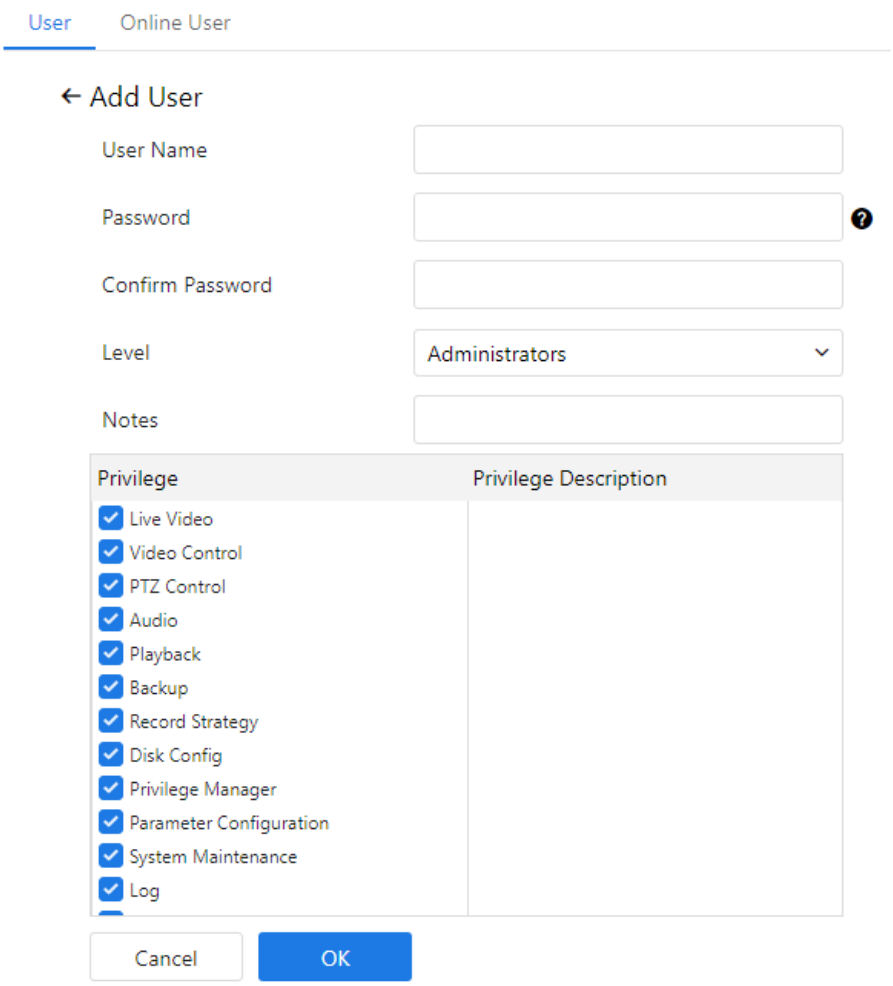
Parameter	Description	Setting
ID	User ID	User ID (not configurable).
User Name	Name used to log in to the camera.	[Setting method] Select a value from the drop-down list box.
Groups	Specifies the user group. Default groups include: • **Super Admin**: Full access to all system features • **Administrators**: Access to live video, playback, PTZ, audio, system, log, record policies, disk config, privilege, and parameter settings • **Operator**: Access to live video, playback, PTZ, parameter config, and maintenance • **Media User**: Live video only	[Setting method] Click **Add**, then select a value from the drop-down list box.

Parameter	Description	Setting
Notes	Optional notes for the user.	[Setting method] Click **Add**, then enter a value manually.
Operate	Actions include view, modify, and delete. NOTE Super Admin can be viewed only.	[Setting method] Click the icon as required.

Table 3-3 Operation description

Function	Procedure	Description
Add	1. Click **Add**. The **Add User** page is displayed, as shown in Figure 3-5. 2. Enter a user name, password, and confirm password. 3. Select a group from the drop-down list box. 4. Enter the notes (Optional). 5. Check the privilege. 6. Click **OK**. The user is added successfully.	Add an administrator or a common user as shown in Figure 3-5.
Modify	1. Click . The **Modify User** page is displayed. 2. Modify the user name, password, group, or privilege. 3. Click **OK**. The user is modified successfully. The **User** page is displayed.	Modify the user name, password, group, or privilege.
Delete	Click the  **icon**. When prompted with *"Confirm to delete?"*, click **OK**	Deletes a user.

Figure 3-5 Add user page



NOTE

Click the privilege list to view a detailed breakdown of functions associated with each user group.

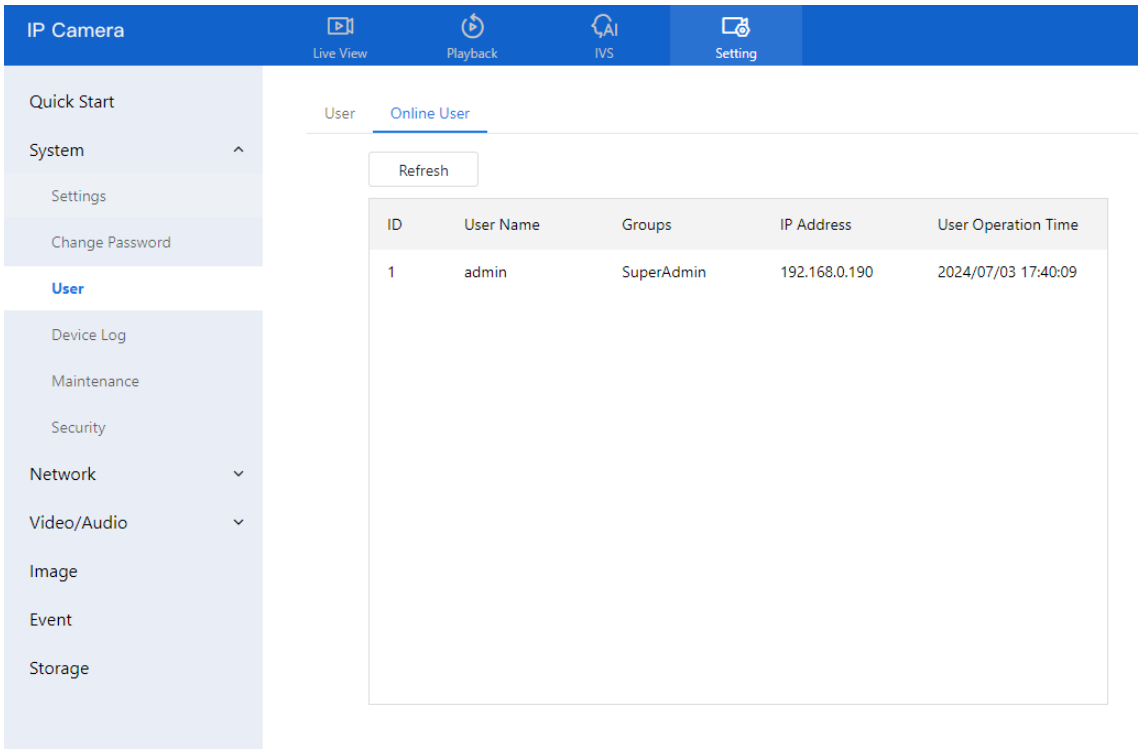
3.3.2 Online User

Procedure

Step 1 Navigate to **Setting > System > User > Online User**. The **Online User** page is displayed, as shown in Figure 3-6.

Step 2 View all users currently connected to the system in real time.

Figure 3-6 Online user



3.4 Query Device Logs

3.4.1 Query Operation Logs

Description

The operation log records user actions and scheduled task instructions during device operation. These logs are categorized as follows:

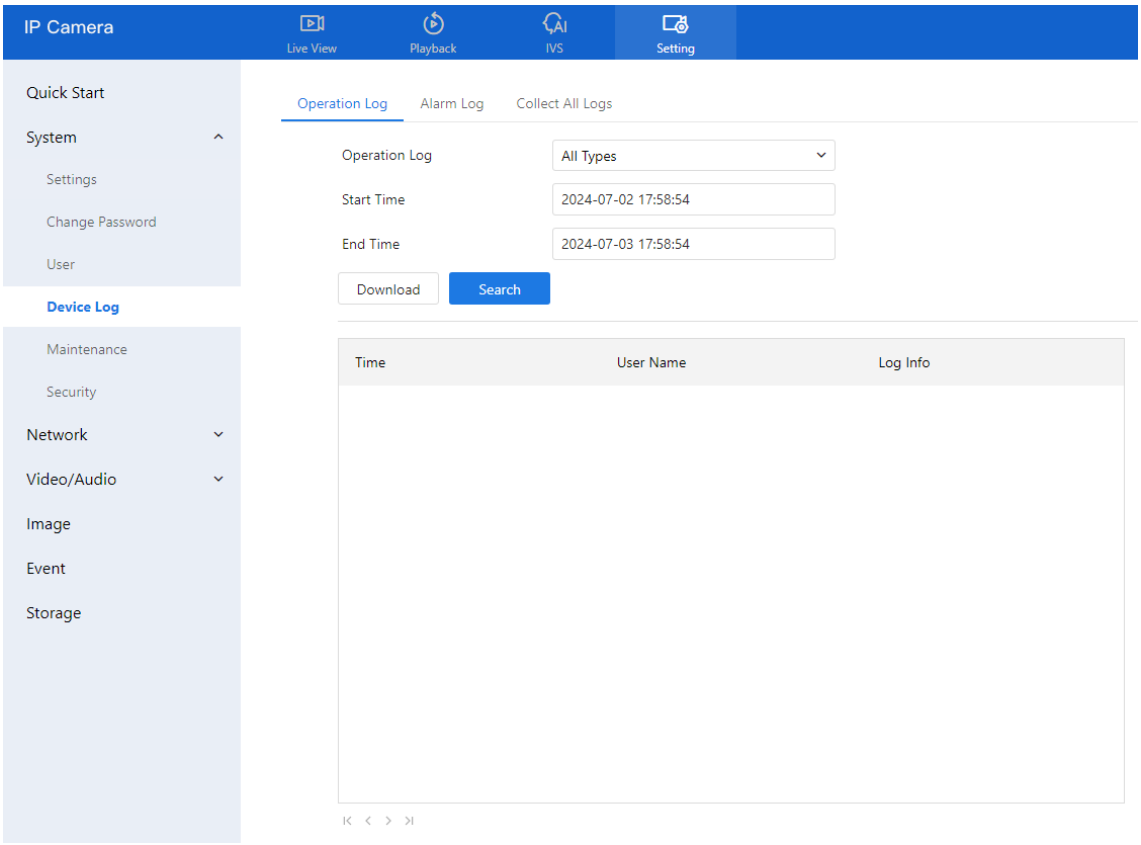
- Privilege manager
- System maintenance
- Device operations
- Recording operations
- Video control
- Live video

Procedure

Step 1 Navigate to **Setting > System > Device Log > Operation Log**.

The **Operation Log** page appears, as shown in Figure 3-7.

Figure 3-7 Operation log page



Step 2 Set the query conditions.

- Select the type of operation logs from the **Operation Log** drop-down list.
- Click the **Begin Time** and **End Time** text boxes to display the time selection panel, and set the desired time range.
- Select the username from the **User Name** drop-down list.

Step 3 Click **Search**. The logs matching the specified criteria are displayed.

Download the operation logs.

To download logs:

Step 1 Select the log type.
Step 2 Set the **start time**, **end time**, and **log type**.
Step 3 Click **Download**.
Step 4 The log Excel file will be saved automatically to the browser's default download path.

3.4.2 Query Alarm Logs

Description

Alarm logs capture events triggered by system alerts, including:

- Security alarms
- Disk alarms

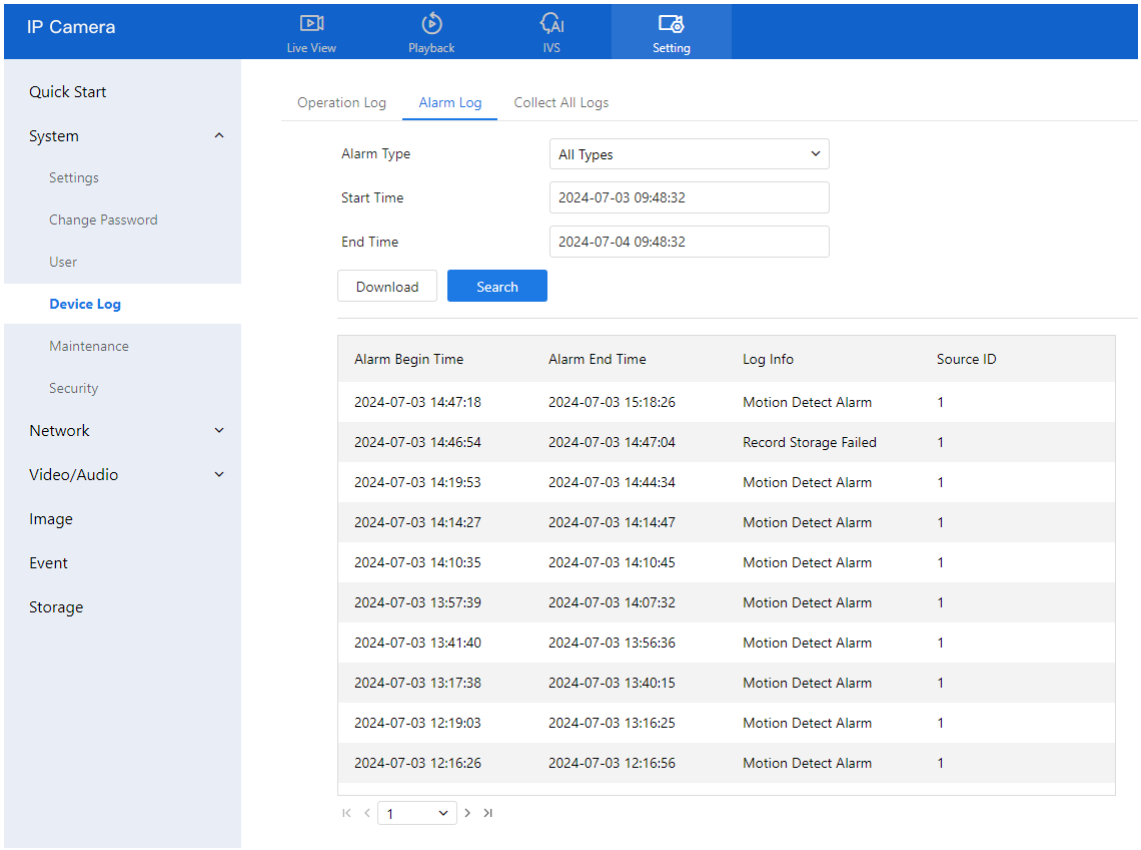
- Recording alarms
- Intelligent analysis alarms

Procedure

Step 1 Navigate to **Setting > System > Device Log > Alarm Log**.

The **Alarm Log** page appears, as shown in Figure 3-8.

Figure 3-8 Alarm log page



Step 2 Set the search conditions.

- Click the **Begin Time** and **End Time** text boxes to set the time range.
- Select the alarm type from the **Alarm Type** drop-down list.

Step 3 Click **Search**.

The alarm logs of the specified type are displayed.

Step 4 Download the alarm logs.

1. Select a log type.
2. Set the start time and end time.
3. Click **Download** to download the logs.
4. The Excel file will be saved to the default download path of the browser.

3.4.3 Collect All Logs

Description

This feature allows you to download all logs related to the device for troubleshooting and analysis. Log types include:

- Device overview

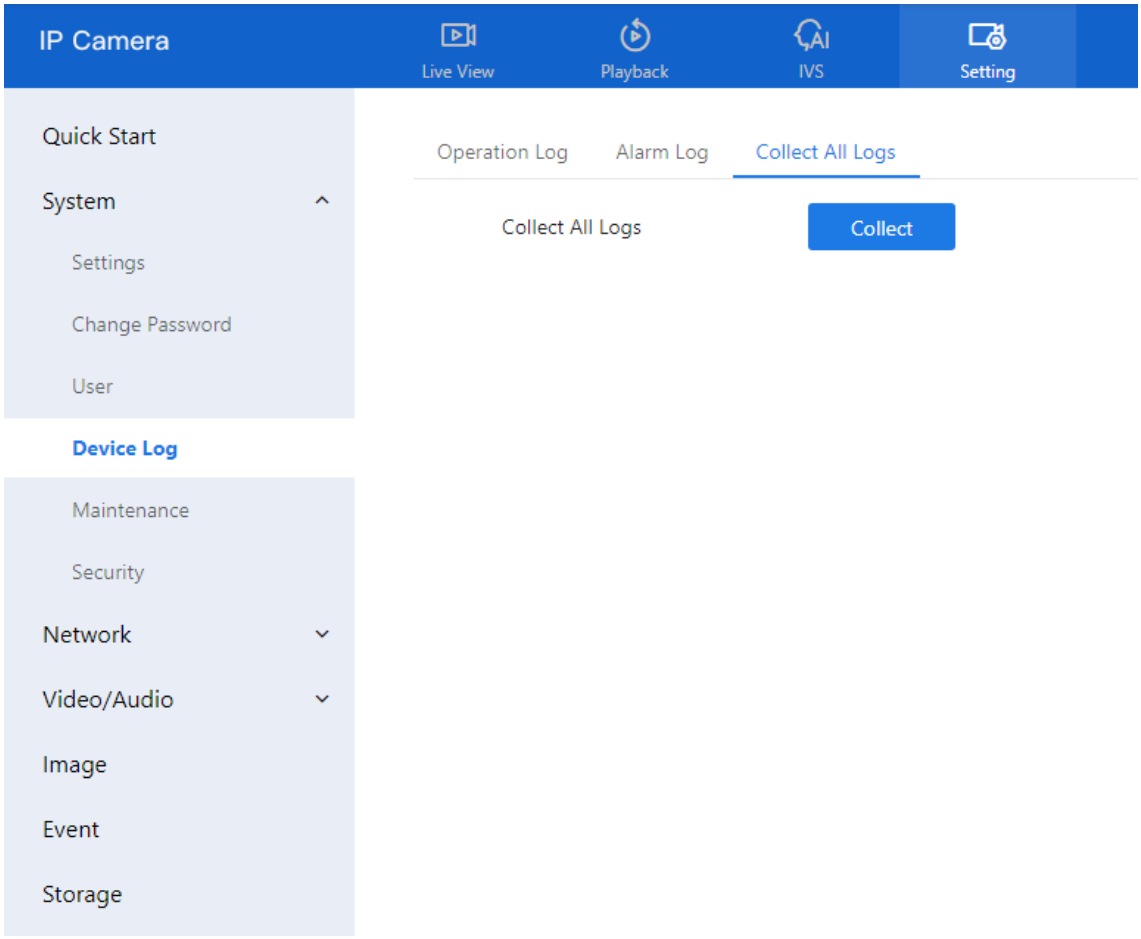
- Key parameters
- Operation logs
- Alarm logs
- Upgrade logs
- Debugging logs

Procedure

Step 1 Navigate to **Setting > System > Device Log > Collect All Log**.

The **Collect Log** page appears, as shown in Figure 3-9.

Figure 3-9 Collect the log page



Step 2 Collect logs with one click.

1. Click **Collect**, and a download pop-up window will appear.
2. The log file will automatically be saved to the browser's default download location.

3.5 Maintain the Device

3.5.1 Reboot Device

Description

Use this feature to reboot the device in scenarios including, but not limited to:

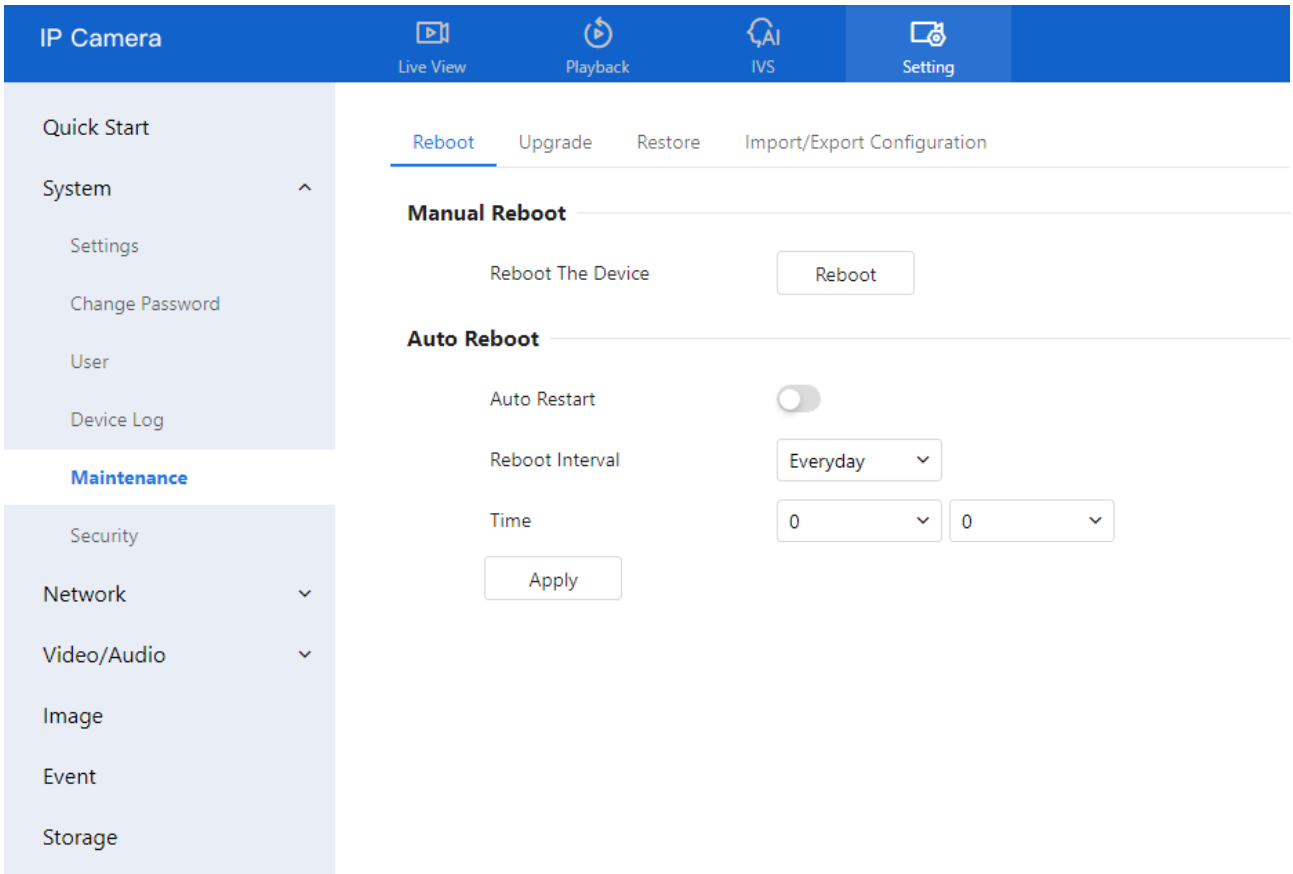
- Device parameters have been configured incorrectly, causing improper operation.
- A parameter reset is needed for the changes to take effect.
- Remote reboot is required for maintenance or troubleshooting.

Procedure

Step 1 Navigate to **Setting > System > Maintenance > Reboot**.

The **Camera Maintenance** page is displayed as shown in Figure 3-10.

Figure 3-10 Reboot device page



Step 2 Click **Reboot**.

- A confirmation message appears: **"Are you sure to restart?"**
- Click **OK** to proceed.

Step 3 The device will restart successfully within approximately **five minutes.**

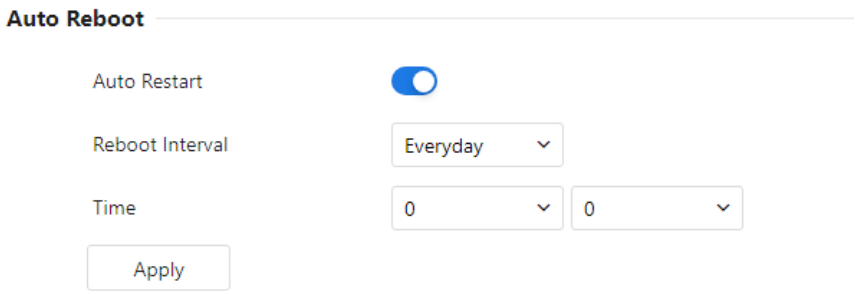
Auto Reboot Configuration:

You can also configure the device to reboot automatically at scheduled intervals.

Step 1 Enable **Auto Reboot** by checking the appropriate option.
Step 2 Choose the desired **reboot interval** from the drop-down list:

- **Every Day**
- **Every Week**
- **Every Month**

Figure 3-11 Camera auto-restart



Step 3 Click **Apply**. The auto reboot schedule will take effect, and settings will be saved.

3.5.2 Upgrade the Software Package

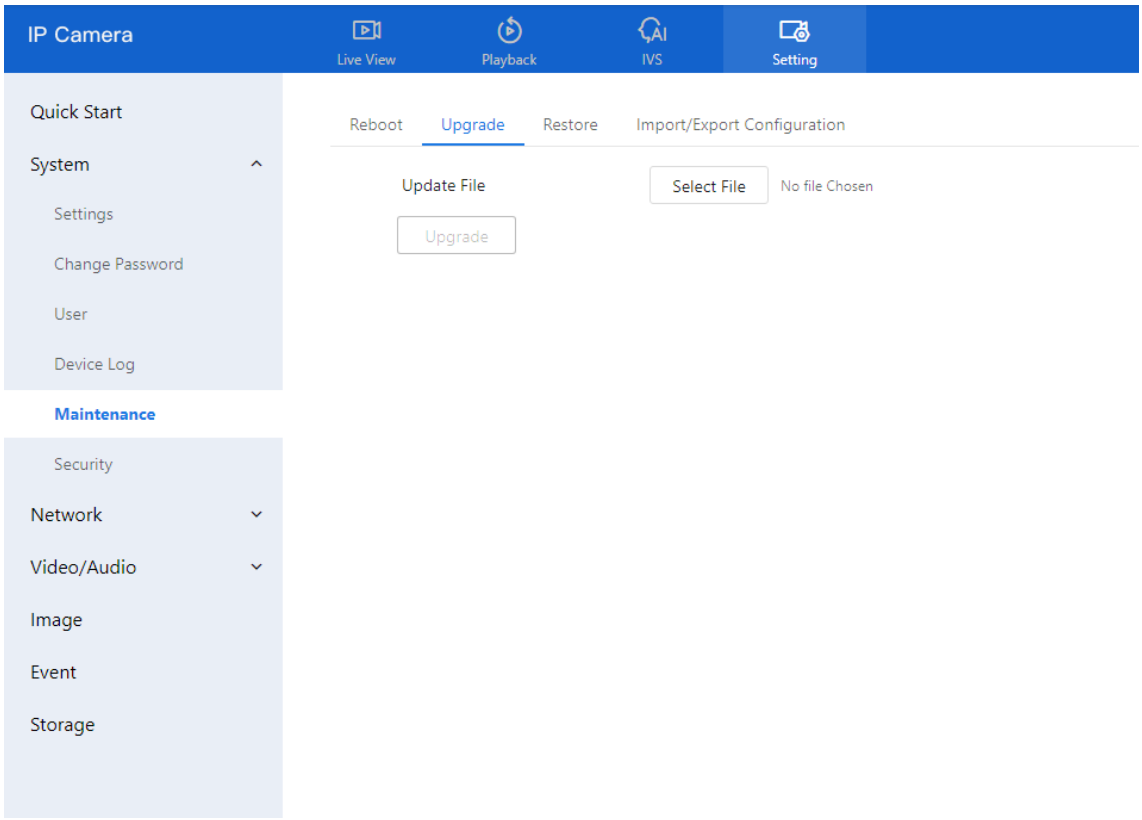
Description

You can upgrade the device software package through the web interface. This process ensures the device runs the latest version with improved features or resolved issues.

Procedure

Step 1 Navigate to **Setting > System > Maintenance > Upgrade**.
The **Upgrade** page is displayed.

Figure 3-12 Update file



Step 2 Click **Select File** to browse and choose the appropriate upgrade file.
Step 3 Click **Update** to begin the upgrade process.

If the message **"Updating, please wait a few minutes, and do not close the browser"** is displayed:

- The upgrade is in progress.
- The device will automatically reboot after the update completes.

If another message is displayed, ensure you have selected the correct upgrade package and try again.

CAUTION

Do **not** power off the camera during the upgrade process.
Power failure during an upgrade may result in device malfunction.

3.5.3 Restore Device to Factory Settings

Description

You can restore the device to its factory default settings. This feature is recommended in the following scenarios:

- The device configuration is incorrect, causing operational issues

- You want to reset all parameters
- A clean factory default state is required for troubleshooting

CAUTION

After clicking **Restore**, all configuration settings will be reset to factory defaults.

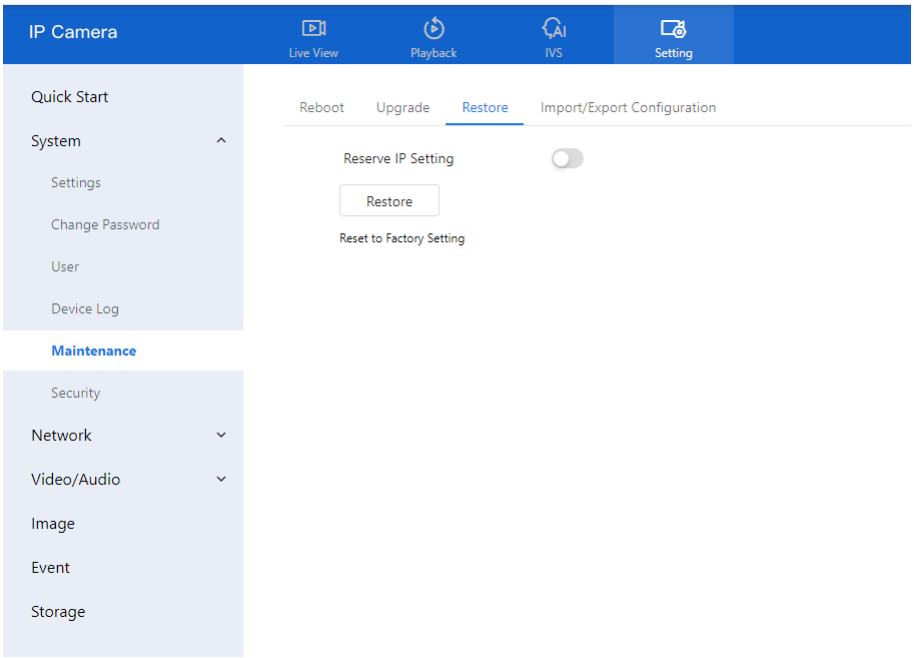
You may choose whether or not to retain the current IP address.

Use the function carefully.

Procedure

Step 1 Navigate to **Setting > System > Maintenance > Restore**.
The **Restore** page is displayed.

Figure 3-13 Restore device



Step 2 Click **Restore**. The message "Are you sure to restore?" is displayed.
Step 3 Click **OK**. The device begins restoring to its factory default settings. After the process completes, the device will reboot with factory defaults applied.

3.5.4 Export / Import Configuration

Description

This feature allows you to back up the current configuration and restore it later. You can export the settings to a local hard drive and import the same configuration to:

- The current device
- Other cameras of the same model

The configuration file is saved as **config.bin**.

Procedure

Export Configuration

Step 1 Navigate to **Setting > System > Maintenance > Import/Export Configuration**.

The **Export / Import Configuration** page is displayed (see Figure 3-14).

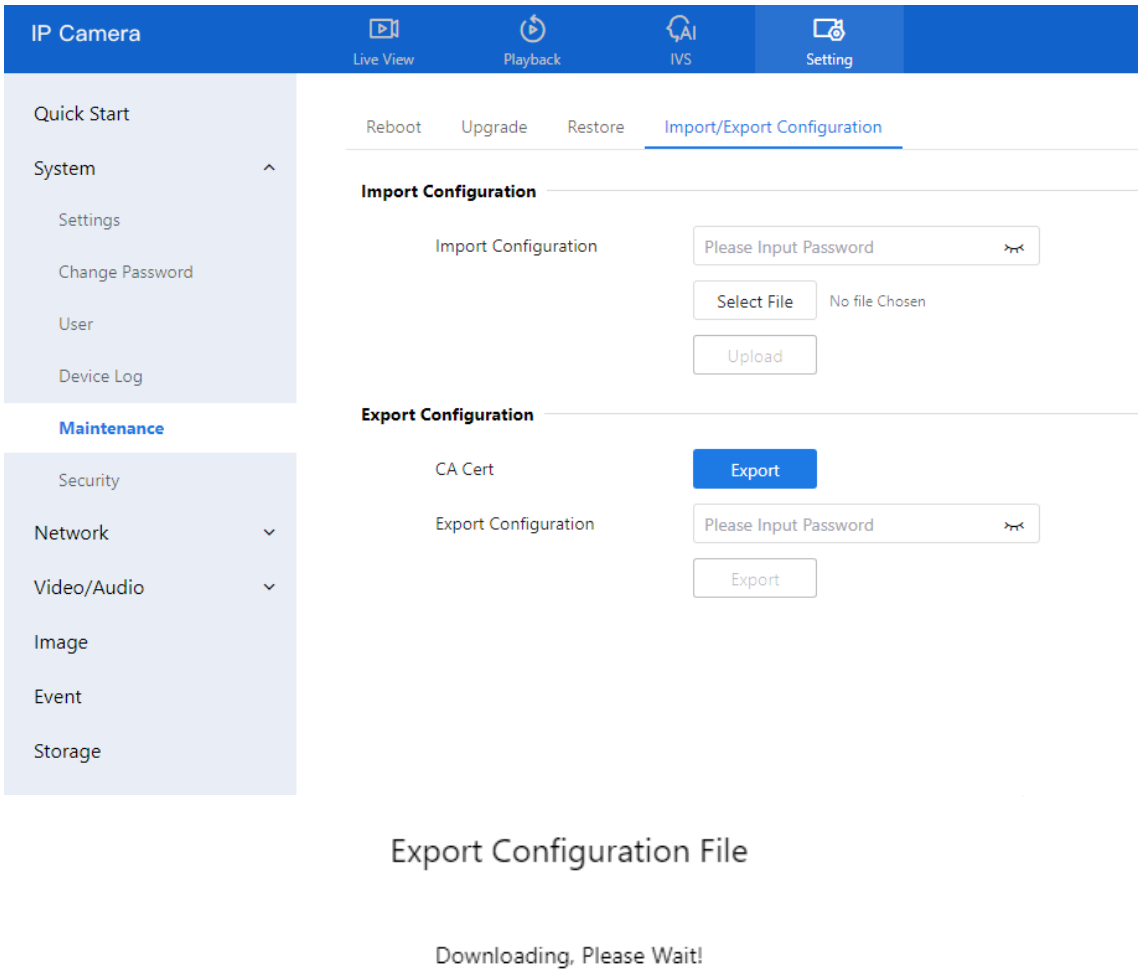
Step 2 Under **Export Configuration**:

- Enter the **password**.
- Click **Export**.

Step 3 A message will appear: **"Export Configuration File — Downloading, Please Wait!"**

The configuration file will be downloaded to your local system.

Figure 3-14 Export / Import Configuration page



Import Configuration

Step 1 Under **Import Configuration**:

- Enter the **password**.

- Click **Select File**, then browse and select the **backup.bin** file (backup-model-version of software, backup-SN-IPS8655WDR-Z30-28-v5.2.1628.2412.3.0.1.1.0.20260121) from your local drive.
- Click **Upload** to begin the import process.

3.6 Configure Security

3.6.1 IP Filter

Description

The **IP Filter** function allows you to control access to the device based on IP address ranges. You can specify whether to allow or deny access to certain IP segments using whitelist or blacklist rules.

Procedure

Step 1 Go to **Setting > System > Security > IP Filter**.

The **IP Filter** page is displayed (see Figure 3-15).

Step 2 Click the toggle switch to enable **IP Filter**.

Step 3 Configure the parameters listed in **Table 3-4**.

Figure 3-15 IP filter page

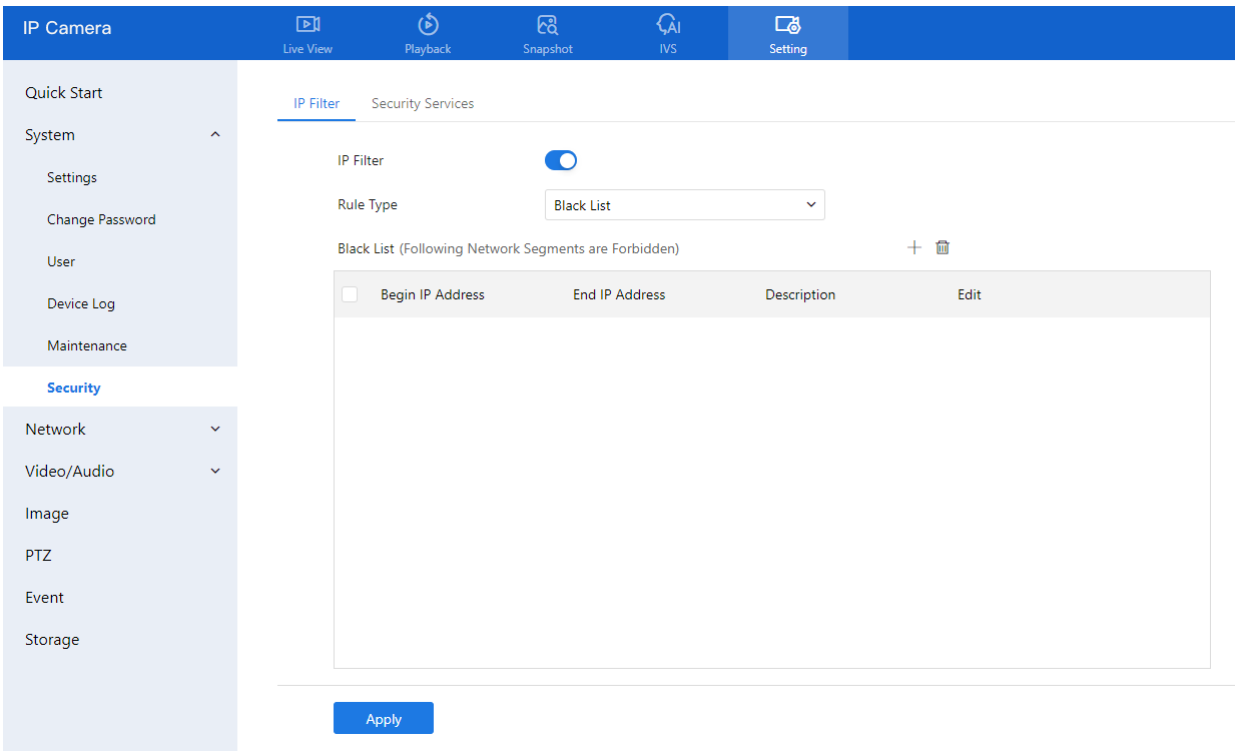
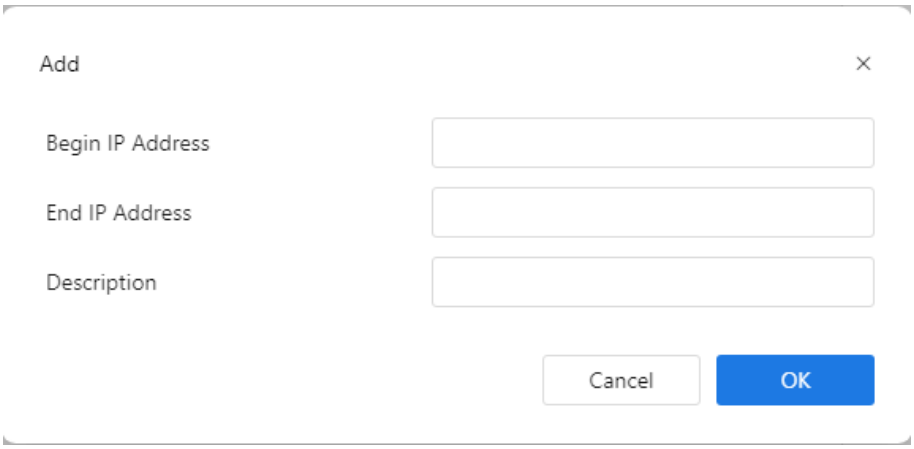


Table 3-4 Parameters of the IP filter

Parameter	Description	Setting
IP Filter	Enables or disables the IP Filter function.	[Setting method] Click the button on. [Default value] OFF

Parameter	Description	Setting
Rule Type	IP filter type, including black list and whitelist.	[Setting method] Select a value from the drop-down list box. [Default value] Black List
Black List	The specified network segment should be banned.	[Setting method] 1. Click + to enter the add black/white list page, as shown in Figure 3-16 2. Enter Begin IP Address. 3. Enter End IP Address. 4. Enter Description. 5. Click OK, the black list added successfully.
White List	Allow the specified network segment to access.	[Setting method] 1. Click + to enter the add black/white list page, as shown in Figure 3-16. 2. Enter Begin IP Address. 3. Enter End IP Address. 4. Enter Description. 5. Click OK, and add the white list successfully.

Figure 3-16 Add IP filter page



NOTE

Click to modify the parameters of setting black list or a whitelist.

Click to delete the setting black list or whitelist.

Step 4 Click **Apply**.

If the message "Apply success!" appears, the IP Filter has been successfully configured.

.

3.6.2 Security Services

Description

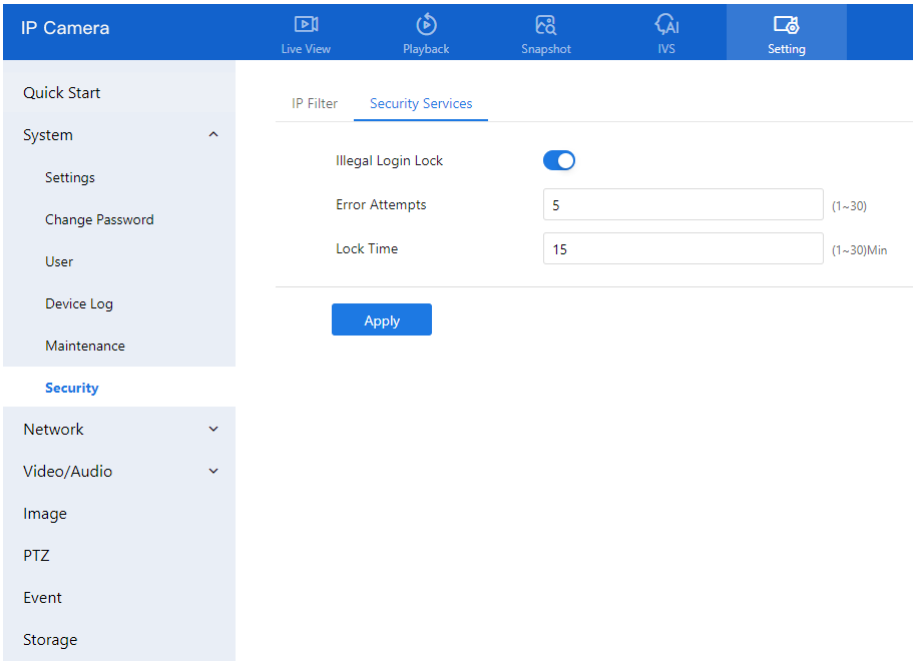
To enhance device security, you can enable the **Illegal Login Lock** feature. When enabled, the system will lock the user account for a specified duration after a defined number of incorrect password attempts.

Procedure

Step 1 Navigate to **Setting > System > Security > Security Services**.

The **Security Services** page is displayed, as shown in Figure 3-17.

Figure 3-17 Security services page



Step 2 Configure the following settings:

- **Illegal Login Lock**: Toggle this switch **ON** to enable account lockout for failed login attempts.
- **Error Attempts**: Enter the number of allowed incorrect password attempts before lockout is triggered.
    - **Range**: 1–30
    - **Example**: Setting this to 5 means the account will be locked after 5 failed login attempts.
- **Lock Time**: Enter the duration (in minutes) for which the account will remain locked after exceeding the allowed attempts.
    - **Range**: 1–30 minutes
    - **Example**: Setting this to 15 means the account will be locked for 15 minutes.

Step 3 Click **Apply**.

- A message **"Apply success!"** confirms that the settings have been saved.

4 Configure the Network Service

4.1 Basic Settings

4.1.1 Local Network

For detailed information on Local Network Settings, please refer to **Chapter 2.5**

4.1.2 Device Port

Description

To enable proper network routing within a LAN, you must configure the following ports:

- **HTTP Port**
- **Control Port**
- **RTSP (Real-Time Streaming Protocol) Port**
- **HTTPS (SSL) Port**

These ports are essential for web access, video streaming, and secure communication.

Procedure

Step 1 Navigate to **Setting > Network > Settings > Device Port**.

The **Device Port** page is displayed (see Figure 4-1).

Step 2 Set the parameters, as shown in Table 4-1.

Figure 4-1 Device port page

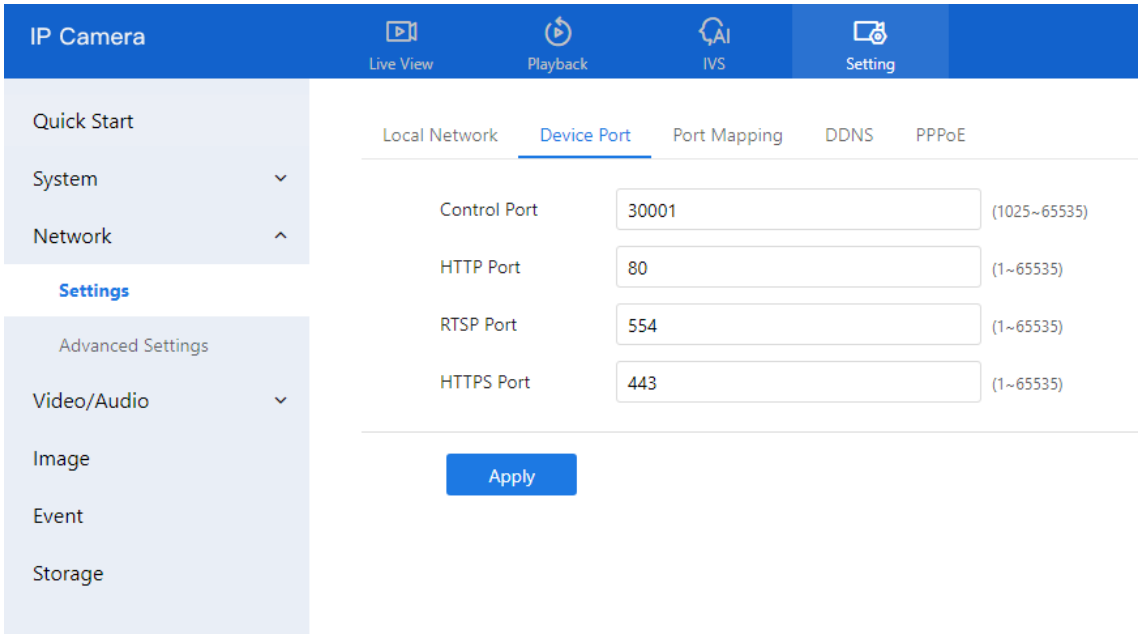


Table 4-1 Parameters of the device port

Parameter	Description	Setting
Control Port	Used for audio, video transmission, and signaling interaction.	[Setting method] Enter a value manually. [Default value] 30001
HTTP Port	Port used for standard web access. If changed (e.g., to 86), access the device using: `http://192.168.0.120:86/`	[Setting method] Enter a value manually. [Default value] 80
RTSP Port	Port for RTSP protocol (streaming). Example: Input `rtsp://192.168.0.120:554/snl/live/1/1` into VLC to view live video. Refer to **Configuration > Protocol > Protocol Info** for further details.	[Setting method] Enter a value manually. [Default value] 554
HTTPS Port	secure port for web access using SSL. Before use, ensure **Web Mode** is set to **HTTPS** under **Configuration > Device > System**. Access format: `https://192.168.0.120:443`	[Setting method] Enter a value manually. [Default value] 443
SSL Control Port	Secure socket layer control port. **Note:** This option is available on select models only.	[Setting method] Enter a value manually. [Default value] 20001

NOTE

It is generally **not recommended** to change the **Control Port**.

Refer to the **Communication Matrix** for valid port ranges for Control, HTTP, and SSL ports.

Step 3 Click **Apply**.

- If the message **"Apply success!"** appears, the settings have been saved.
- If you see **"Port invalid, please check it,"** review and re-enter valid port numbers.

4.1.3 Port Mapping

Description

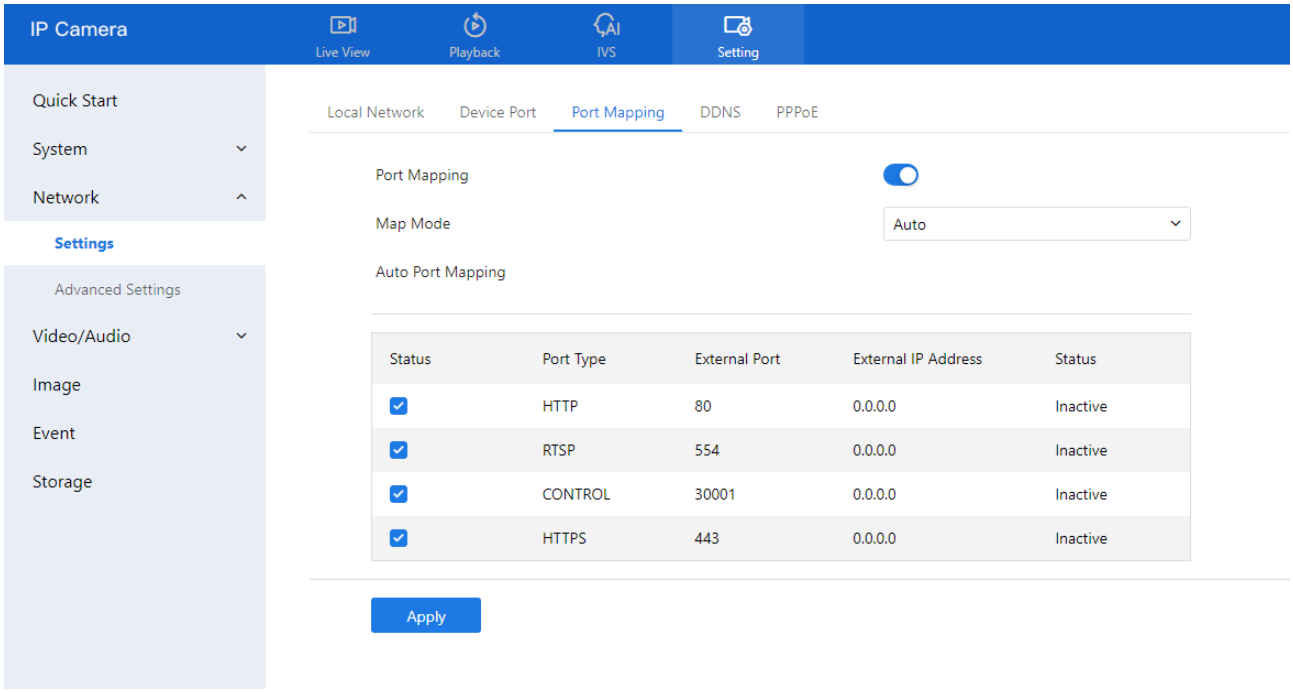
Port mapping helps establish a mapping relationship between the private network and the external network. Port mapping allows outside computers to access intranet devices so that the network works efficiently.

Procedure

Step 1 Choose **Setting > Network > Settings > Port Mapping**.

The **Port Mapping** page is displayed, as shown in Figure 4-2.

Figure 4-2 Port mapping page



Step 2 Click the button to enable **Port Mapping**.

Step 3 Set the parameters according to Table 4-2.

Table 4-2 Parameters of port mapping

Parameter	Description	Setting
Port Mapping	Enables or disables the port mapping service.	[Setting method] Click the button on. [Default value] OFF
Map Mode	Defines how Auto and Manual	[[Setting method]

Parameter	Description	Setting
	ports are mapped	Select a value from the drop-down list box. [Default value] Auto
Port Type	Types of ports used in the mapping: Includes **HTTP**, **RTSP**, **CONTROL**, and **HTTPS**.	N/A
External Port	The port number used on the external (public) network.	[Setting method] Enter a value manually in map mode.
External IP Address	IP address used on the external network to access the device.	N/A
State	Displays the current mapping status for each port.	N/A

Step 4 Click **Apply**.

- If the message **"Apply success!"** appears, the settings have been saved.
- If any other message appears, review and correct the parameters.

4.1.4 DDNS

Preparation

Before configuring DDNS, ensure that:

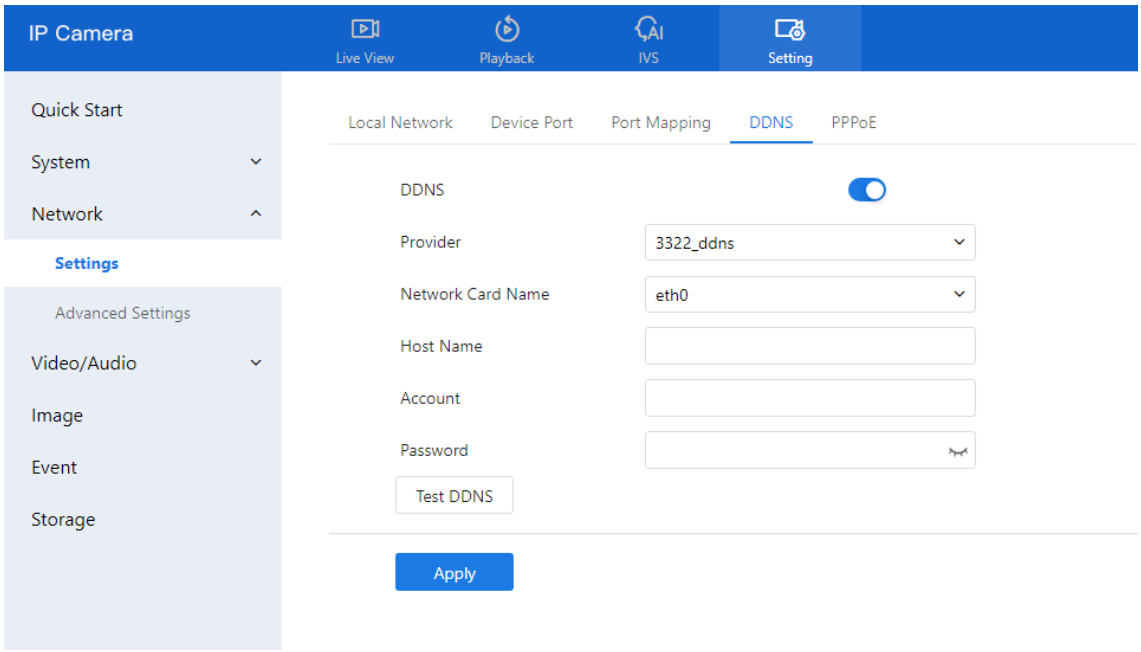
- The camera is connected to the Internet.
- You have obtained a valid **username** and **password** for logging into the Dynamic Domain Name System (DDNS) server.

Procedure

Step 1 Navigate to **Setting > Network > Settings > DDNS**.

The **DDNS** page is displayed, as shown in Figure 4-3.

Figure 4-3 DDNS page



Step 2 Click the toggle switch to enable **DDNS**.
Step 3 Configure the parameters as shown in Table 4-3.

Table 4-3 Parameters of DDNS

Parameter	Description	Setting
DDNS	Enables or disables the DDNS service.	[Setting method] Click the button to enable DDNS. [Default value] OFF
Provider	Select your DDNS service provider. Currently supported providers: • 3322_DDNS • Dyndns	[Setting method] Select a value from the drop-down list box. [Default value] 3322 NOTE Set this parameter based on the site requirements.
Network Card Name	Specifies which network card to use for DDNS.	[Setting method] Select a value from the drop-down list box. [Default value] Eth0

Parameter	Description	Setting
Host Name	Custom domain name set by the user.	[Setting method] Enter a value manually. [Default value] Blank
Accounts	Username for logging into the DDNS service.	[Setting method] Enter a value manually. [Default value] Blank
Password	Password for logging into the DDNS service. Note: Set all parameters according to your DDNS service provider's instructions and site requirements.	[Setting method] Enter a value manually. [Default value] Blank

Step 4 Click **Apply**.

- If the message "Apply success!" appears, the configuration has been saved.
- If an error appears, review the settings and correct any incorrect values.

4.1.5 Set PPPoE

Preparation

Before configuring PPPoE, obtain your **username** and **password** from your Internet service provider (ISP).

Description

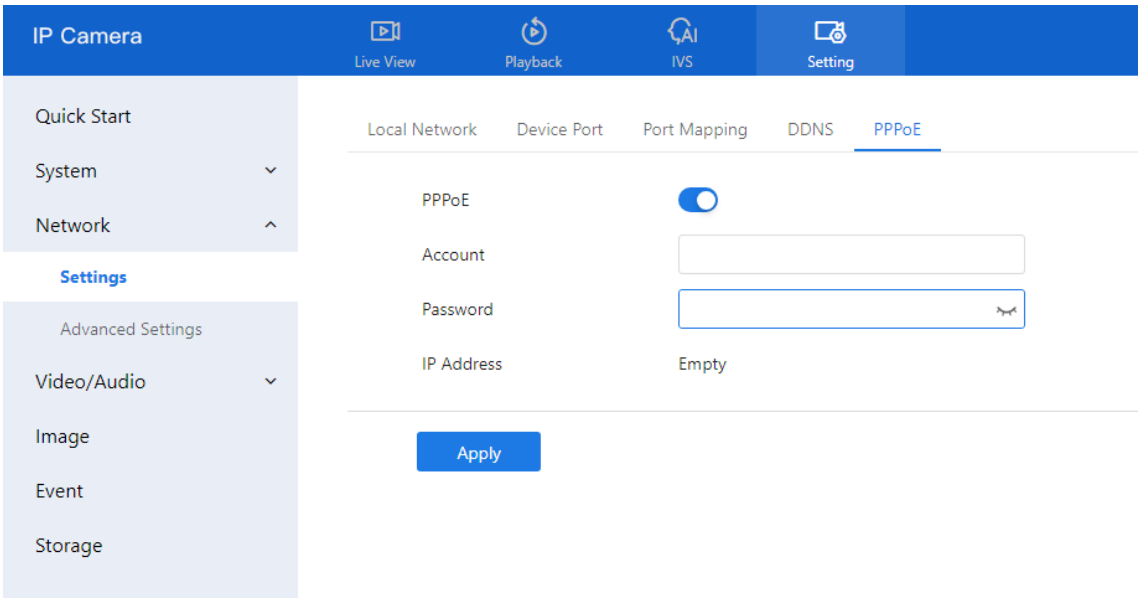
If the camera connects to the Internet via **PPPoE (Point-to-Point Protocol over Ethernet)**, you must enter the provided credentials on the PPPoE configuration page. Once the device restarts, the PPPoE settings take effect, and the system will obtain a **public IP address**.

Procedure

Step 1 Navigate to **Setting > Network > Settings > PPPoE**.

The **PPPoE** page is displayed, as shown in Figure 4-4.

Figure 4-4 PPPoE page



Step 2 Click the toggle button to **enable PPPoE**.
Step 3 Set the parameters according to Table 4-4.

Table 4-4 Parameters of PPPoE

Parameter	Description	Setting
PPPoE	Click to enable PPPoE dialing.	[Setting method] Click the button on. [Default value] OFF
Accounts	User name of PPPoE provided by the network carrier.	[Setting method] Enter a value manually.
Password	The password of PPPoE is provided by the network carrier.	[Setting method] Enter a value manually.

Step 4 Click **Apply**.

- If the message **"Apply success!"** appears, the settings have been saved.
- If another message appears, review and correct the entered credentials.

Note: The IP address assigned via PPPoE will be displayed after a successful connection.

4.2 Advanced Settings

4.2.1 Set FTP

Description

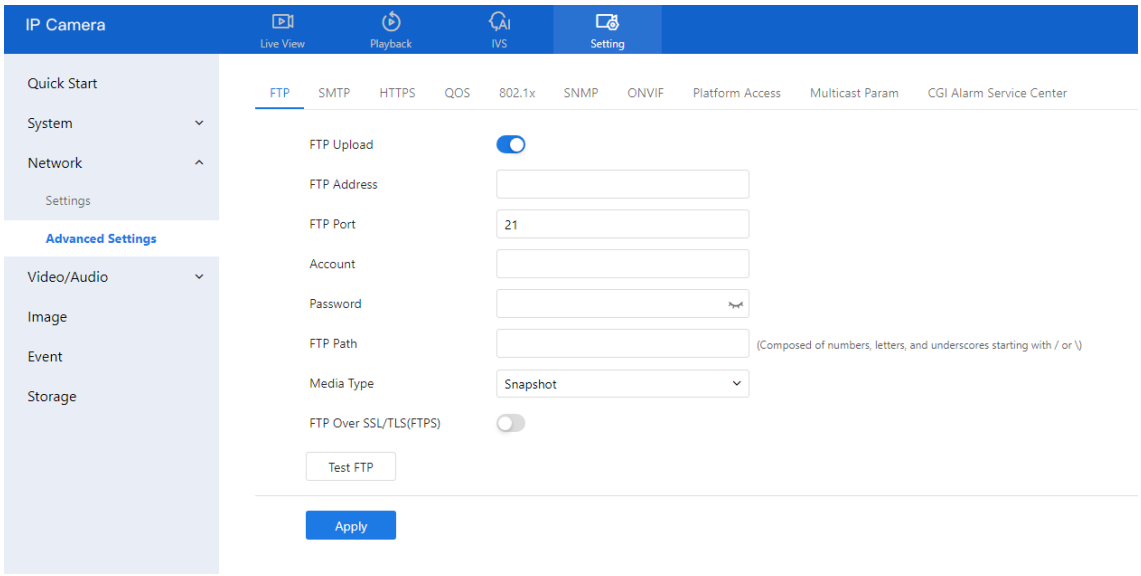
When **FTP (File Transfer Protocol) Upload** is enabled, the device will automatically send captured alarm snapshots (JPG images) to a designated FTP server.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > FTP**.

The **FTP** configuration page is displayed as shown in Figure 4-5.

Figure 4-5 FTP page



Step 2 Click the toggle button to **enable FTP Upload**.

Step 3 Set the parameters as shown in Table 4-5.

Table 4-5 Parameters of FTP

Parameter	Description	Setting
FTP Upload	Enables or disables FTP upload functionality.	[Setting method] Click the button on. [Default value] OFF
FTP Address	IP address of the FTP server.	[Setting method] Enter a value manually.
FTP Port	Port number of the FTP server.	[Setting method] N/A [Default value] 21

Parameter	Description	Setting
Account	Username for FTP server login.	[Setting method] Enter a value manually.
Password	Password for FTP server login.	[Setting method] Enter a value manually.
FTP Path	FTP Path on the FTP server to store images.	[Setting method] Enter a value manually.
Media Type	Specifies the type of media to upload. • **Snapshot** (JPG image) • **Video Clip** (only if supported)	[Setting method] Select a value from the drop-down list box. [Default value] Snapshot
FTP over SSL/TLS (FTPS)	Enables encryption during file transfer using SSL/TLS.	[Setting method] Tick

Step 4 Click **Test FTP** to verify the connection.

If **"Test succeeded"** appears, the configuration is correct.

If **"Test failed"** appears, review and correct the FTP settings.

Step 5 Click **Apply**.

- If the message **"Apply success!"** appears, the configuration has been saved successfully.
- If an error message appears, revise the input accordingly.

4.2.2 Set SMTP

Description

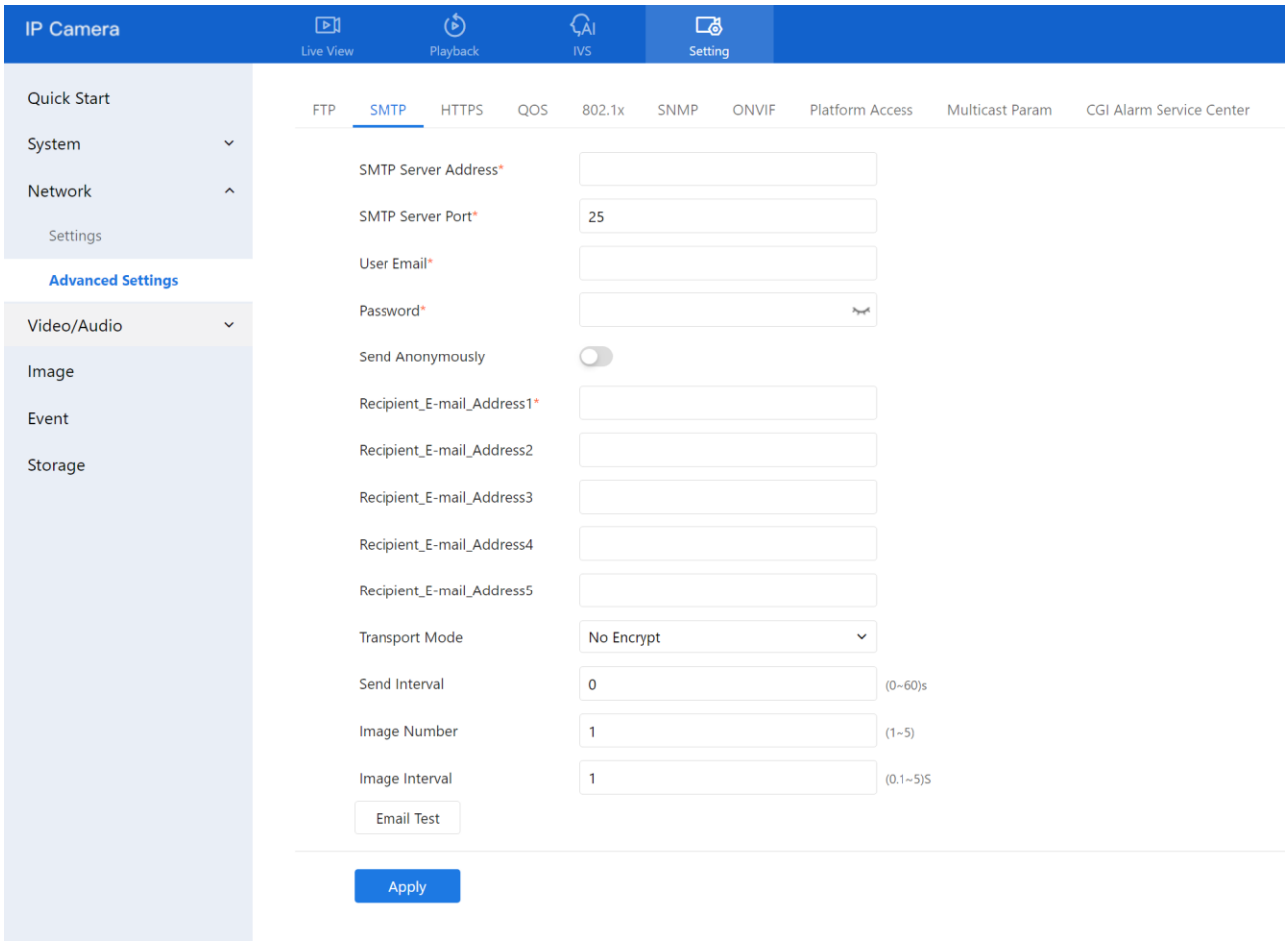
If the Simple Mail Transfer Protocol (SMTP) function is enabled, the device will automatically send JPG images and alarm information to specified email addresses when an alarm is generated.

Procedure

Step 1 Choose **Setting > Network > Advanced Settings > SMTP**.

The **SMTP** page is displayed, as shown in Figure 4-6.

Figure 4-6 SMTP page



Step 2 Set the parameters according to Table 4-6.

NOTE

Fields marked with an asterisk (*) are mandatory.

Table 4-6 Parameters of SMTP

Parameter	Description	Setting
SMTP Server Address	IP address of the SMTP server.	[Setting method] Enter a value manually.
SMTP Server Port	Port number of the SMTP server.	[Setting method] Enter a value manually. [Default value] 25
User Name	Username of the sender's email account.	[Setting method] Enter a value manually.
Password	Password for the sender's email account.	[Setting method] Enter a value manually.
Sender E-mail Address	Email address used to send alerts.	[Setting method] Enter a value manually.

Parameter	Description	Setting
Recipient_E-mail_Address 1	Primary recipient email address.	[Setting method] Enter a value manually.
Recipient_E-mail_Address 2	Optional second recipient.	
Recipient_E-mail_Address3	Optional third recipient.	
Recipient_E-mail_Address 4	Optional fourth recipient.	
Recipient_E-mail_Address 5	Optional fifth recipient.	
Attachment Image Quality	Higher quality uses more storage. Set based on requirements.	N/A
Transport Mode	Email encryption mode. Set this parameter based on the encryption modes supported by the SMTP server.	[Setting method] Select a value from the drop-down list box. [Default value] No Encrypted

Step 3 Click **Apply**.

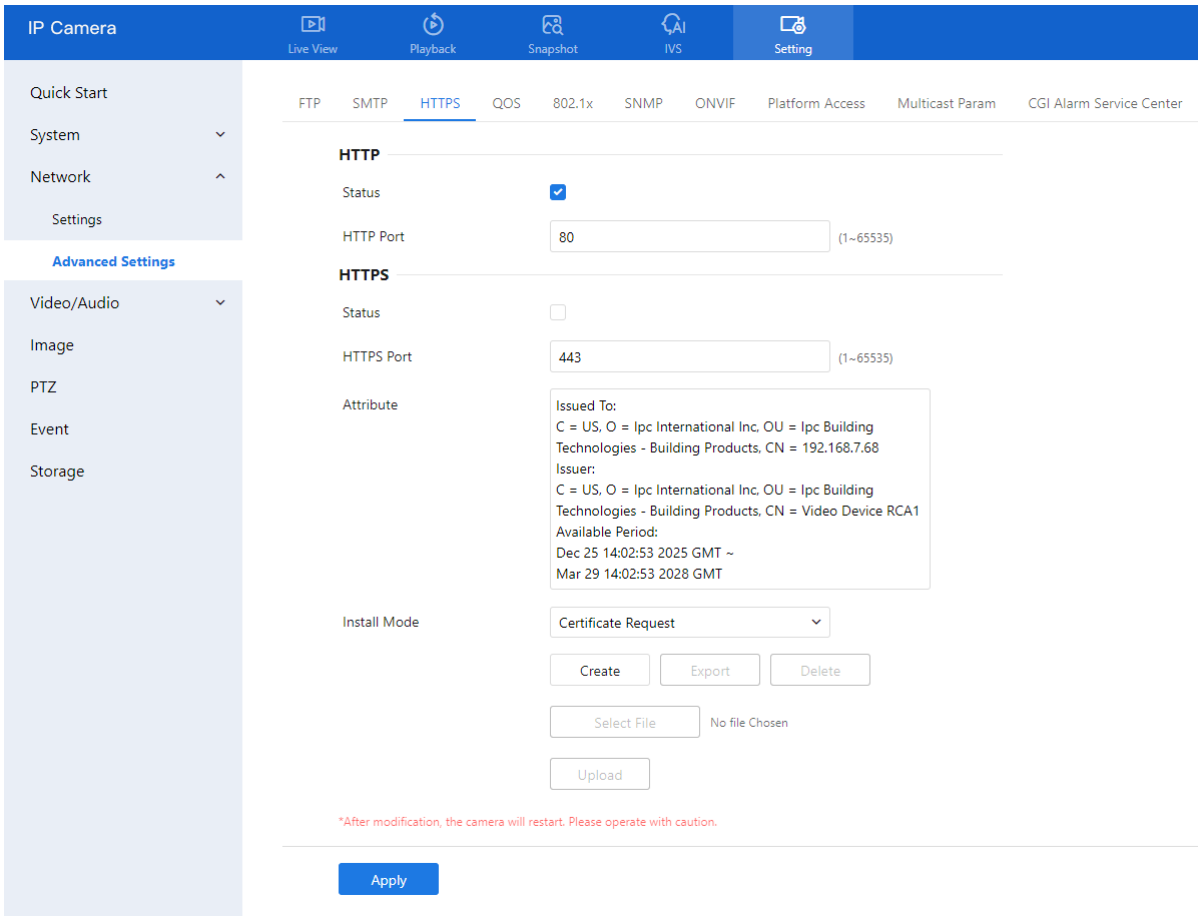
- If the message **"Apply success!"** appears, the settings have been saved successfully.
- If another message appears, review and correct any parameter errors.

4.2.3 Set HTTPS

Preparation

If users wish to access the camera's web interface securely via **HTTPS**, they must first configure the HTTPS port. For example, to access the web interface, input:
https://192.168.0.120:443

Figure 4-7 HTTPS page



Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > HTTPS**.
The **HTTPS** configuration page is displayed (see Figure 4-7).
Step 2 Toggle the **Status** switch to **enable HTTPS**.
Step 3 In the **HTTPS Port** field, enter the desired port number.

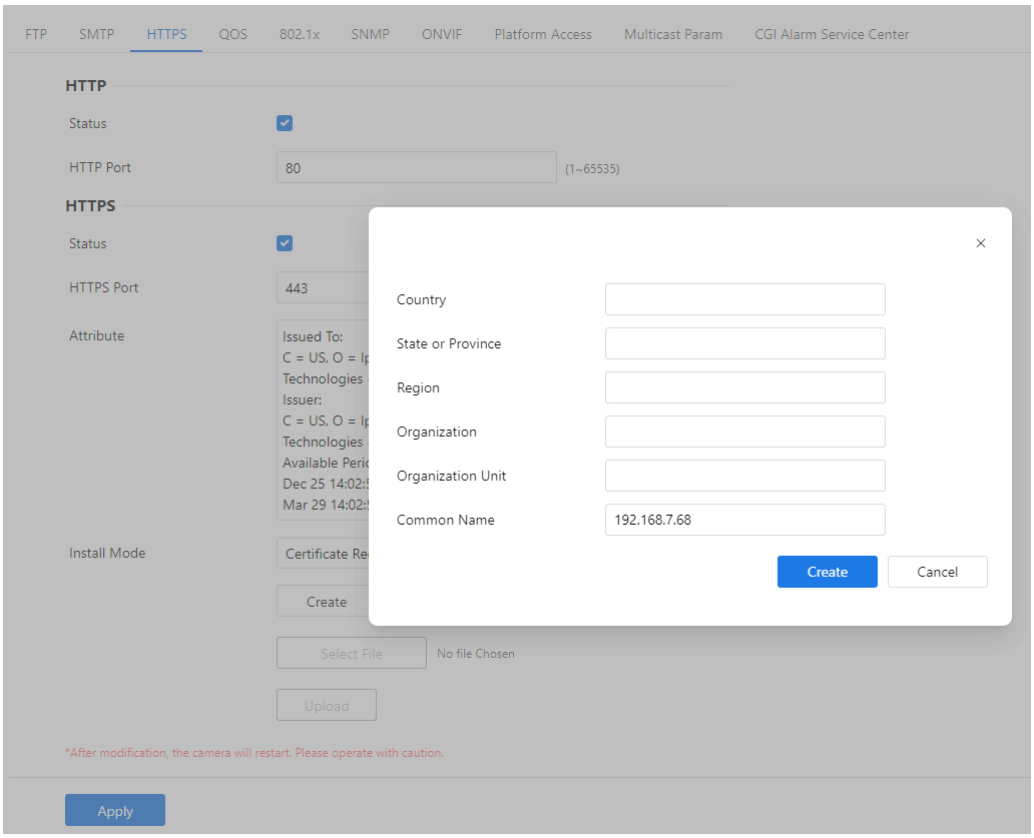
- **Valid Range**: 1–65535
- **Default**: 443

Step 4 Click **Apply**.

- If the message **"Apply success!"** appears, the HTTPS configuration has been saved.
- You can now access the device securely using the designated port.

This section allows you to generate and install an HTTPS certificate for encrypted communication between the camera and your browser. You can create a certificate request, upload a third-party certificate, or manage existing certificates.

Figure 4-8 HTTPS Certificate



Step 1 **Create the certificate request.**

1. Fill in the certificate request details:

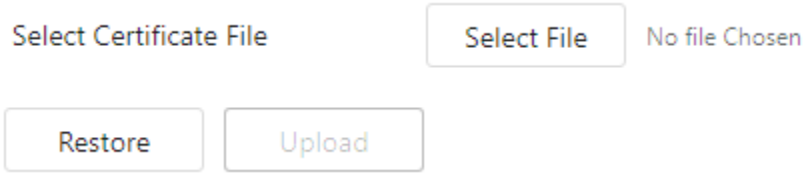
- **Country**
- **State or Province**
- **Location**
- **Organization**
- **Organization Unit**
- **Common Name** (e.g., the device's IP address or domain name)

2. Click **Create** to generate the certificate request file.

3. Send the generated file to a third-party Certificate Authority (CA) to obtain the signed certificate.

- After receiving the certificate from the CA, click **Select File** under the appropriate field and upload it.

- Once successfully uploaded, the certificate will be visible and active on the HTTPS web interface.



Step 2 **To import the certificate from a third party:**

1. Under the **Upload File** section:

- In the **Server Cert** field, click **Select File** and choose the certificate file issued by the CA.
- In the **Server Key** field, click **Select File** and upload the corresponding private key file.

2. Click **Upload** to apply the certificate.

3. **Reboot the camera** for the HTTPS certificate to take effect.

Step 3 **Delete an Existing Certificate**

- To remove a previously uploaded certificate, click **Delete**.

4.2.4 Set QOS

Description

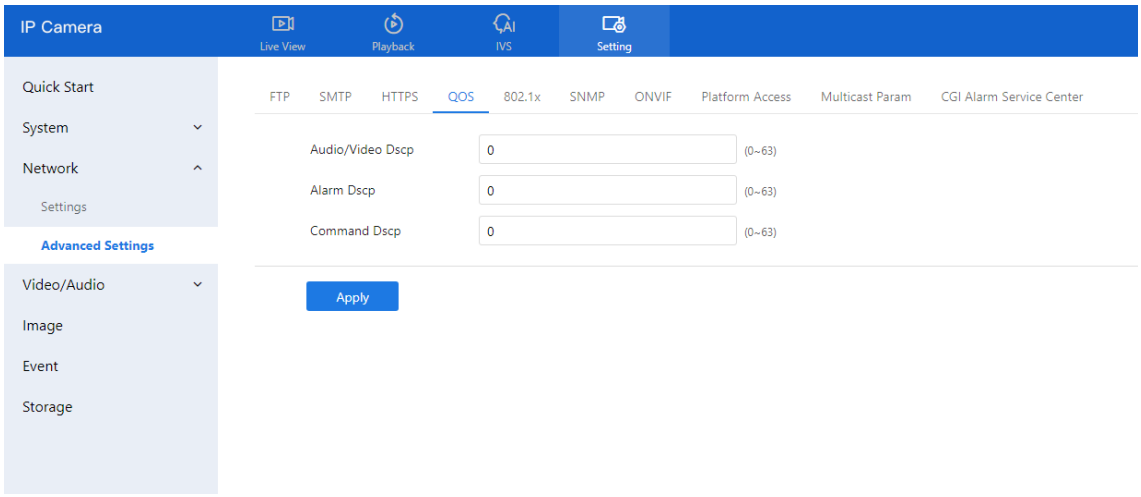
If the device is connected to a **router or switch** that supports **QoS (Quality of Service)**, and the network equipment is configured with appropriate priority rules, data packets from the device will be prioritized accordingly.

This setting helps ensure better performance and bandwidth management for critical services such as video streaming, alarms, and control commands.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > QOS**.
The **QOS** page is displayed, as shown in Figure 4-9.

Figure 4-9 QOS page



Step 2 Enter values for the following fields. Valid input range for each is **0–63**:

- **Audio/Video DSCP**: Priority level for audio/video data
- **Alarm DSCP**: Priority level for alarm signals
- **Command DSCP**: Priority level for control commands

Step 3 Click **Apply**.

- If the message **"Apply success!"** appears, the settings have been successfully applied.
- If any error occurs, verify the DSCP values entered and correct them.

4.2.5 Set 802.1x

Preparation

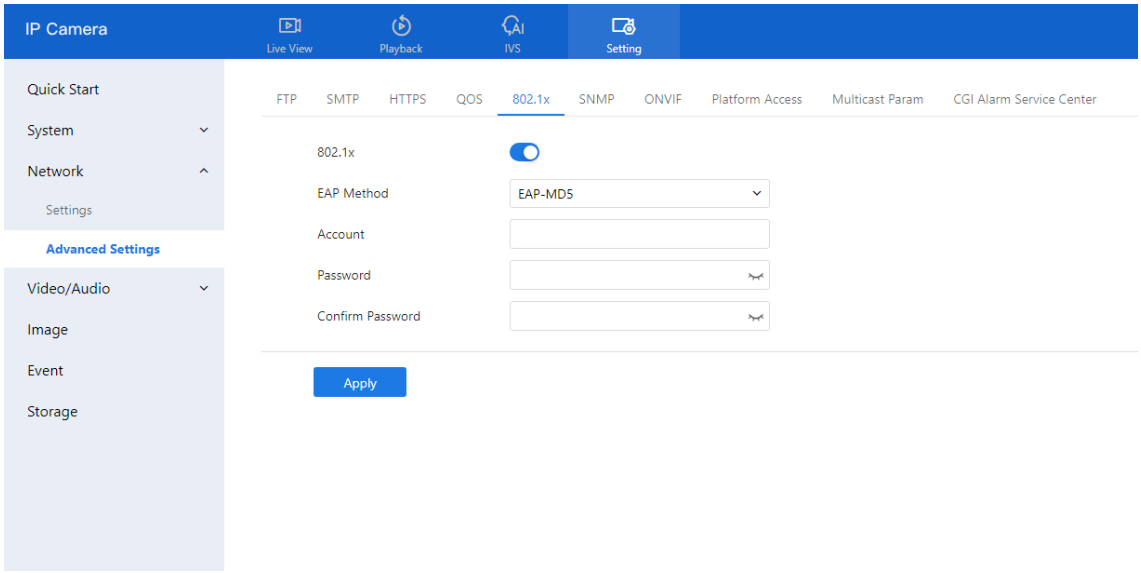
Ensure that **802.1x authentication** is configured on the device's network port. This standard verifies user identity and helps control access to network resources.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > 802.1x**.

The **802.1x** configuration page is displayed, as shown in Figure 4-10.

Figure 4-10 802.1x page



Step 2 Toggle the **802.1x** switch to **enable** authentication.

Step 3 Choose the **EAP Method (Extensible Authentication Protocol)** from the drop-down list:

- **EAP-MD5**
- **EAP-TLS**

Step 4 Enter the **Account Name**.

Step 5 Enter and confirm the **Password**.

Step 6 Click **Apply**.

If the message "Apply success!" is displayed, the settings have been saved successfully.

4.2.6 Set SNMP

Description

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used for managing devices on IP networks. This system supports:

- **SNMPv1**
- **SNMPv2c**
- **SNMPv3**

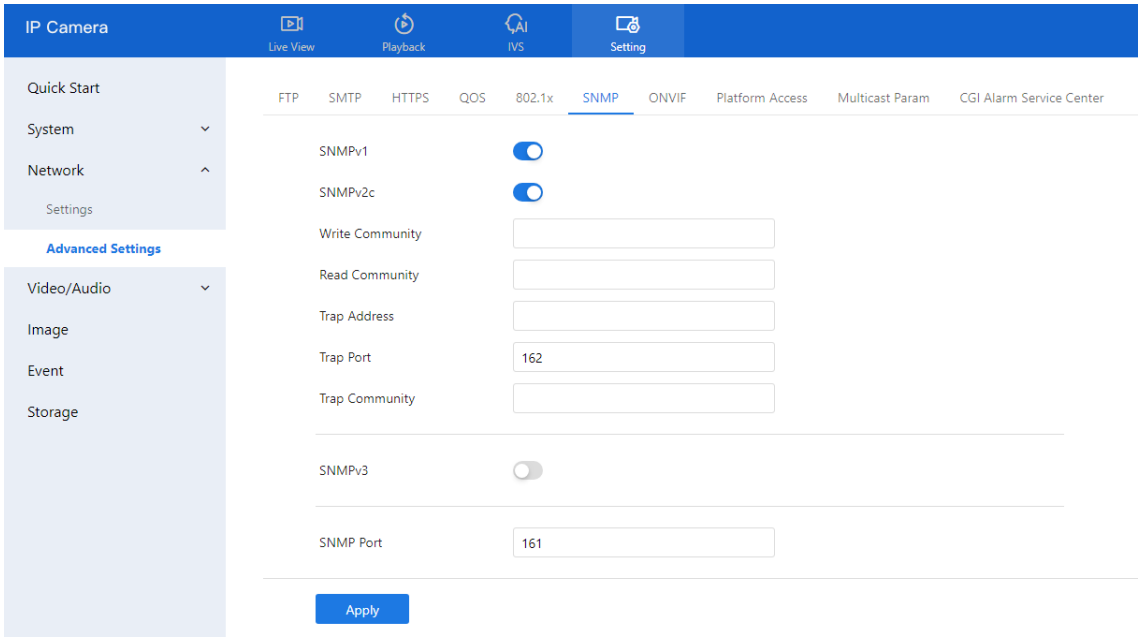
Each version has unique security models and configuration parameters.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > SNMP**.

The **SNMP** page is displayed, as shown in Figure 4-11.

Figure 4-11 SNMP page



Step 2 Toggle the appropriate buttons to enable **SNMPv1**, **SNMPv2c**, or **SNMPv3**.
Step 3 Configure parameters as shown in Table 4-7.

Table 4-7 Parameters of SNMP

Parameter	Description	Setting
SNMPv1	Version of SNMP. SNMPv1 and SNMPv2c use communities to establish trust between managers and agents. Agents support three community names: write community, read community, and trap.	[Setting method] Click the button on. [Default value] OFF
SNMPv2c		
Write Community	Name of write community. The write community can only modify data.	[Setting method] Enter a value manually.
Read Community	Name of the read community. The write community can only read data.	
Trap Address	IP address of the trap.	
Trap Port	Management port of accepting a message from the trap.	
Trap Community	Community string of trap. The trap community string allows the manager to receive asynchronous information from the agent.	
SNMPv3	Version of SNMP. SNMPv3 uses community strings, but allows for secure authentication and communication between the SNMP manager and agent.	[Setting method] Click the button on. [Default value] OFF
Read Security Name	Name of read security.	[Setting method] Enter a value manually.
Write Security Name	Name of write security.	
Security Level	Security Level between SNMP manager and agent, includes three levels: No auth: No authentication and no encryption Auth: Authentication, but no encryption Priv: Authentication and encryption	[Setting method] Select a value from the drop-down list box. [Default value] Blank

Parameter	Description	Setting
Auth Algorithm	Authentication Algorithm, includes MD5and SHA.	[Setting method] Select a value from the drop-down list box. [Default value] Blank
Auth Password	Authentication password.	[Setting method] Enter a value manually.
Encrypt Algorithm	Encryption Algorithm, includes DES and AES.	[Setting method] Select a value from the drop-down list box. [Default value] Blank
Encrypt Password	Encryption password.	[Setting method] Enter a value manually.
SNMP Port	Port of SNMP.	[Setting method] Enter a value manually. [Default value] 161

Step 4 Click **Apply**.

- If the message **"Apply success!"** is displayed, your SNMP settings are saved.
- If another message appears, verify and correct the configuration.

4.2.7 View ONVIF

Description

The **ONVIF** page displays details about the protocol configuration used for external integration with ONVIF-compliant systems.

Procedure:

Step 1 Navigate to **Setting > Network > Advanced Settings > ONVIF**.

The **ONVIF** page is displayed, as shown in Figure 4-12. Table 4-8 describes the protocol-related parameters

Figure 4-12 ONVIF page

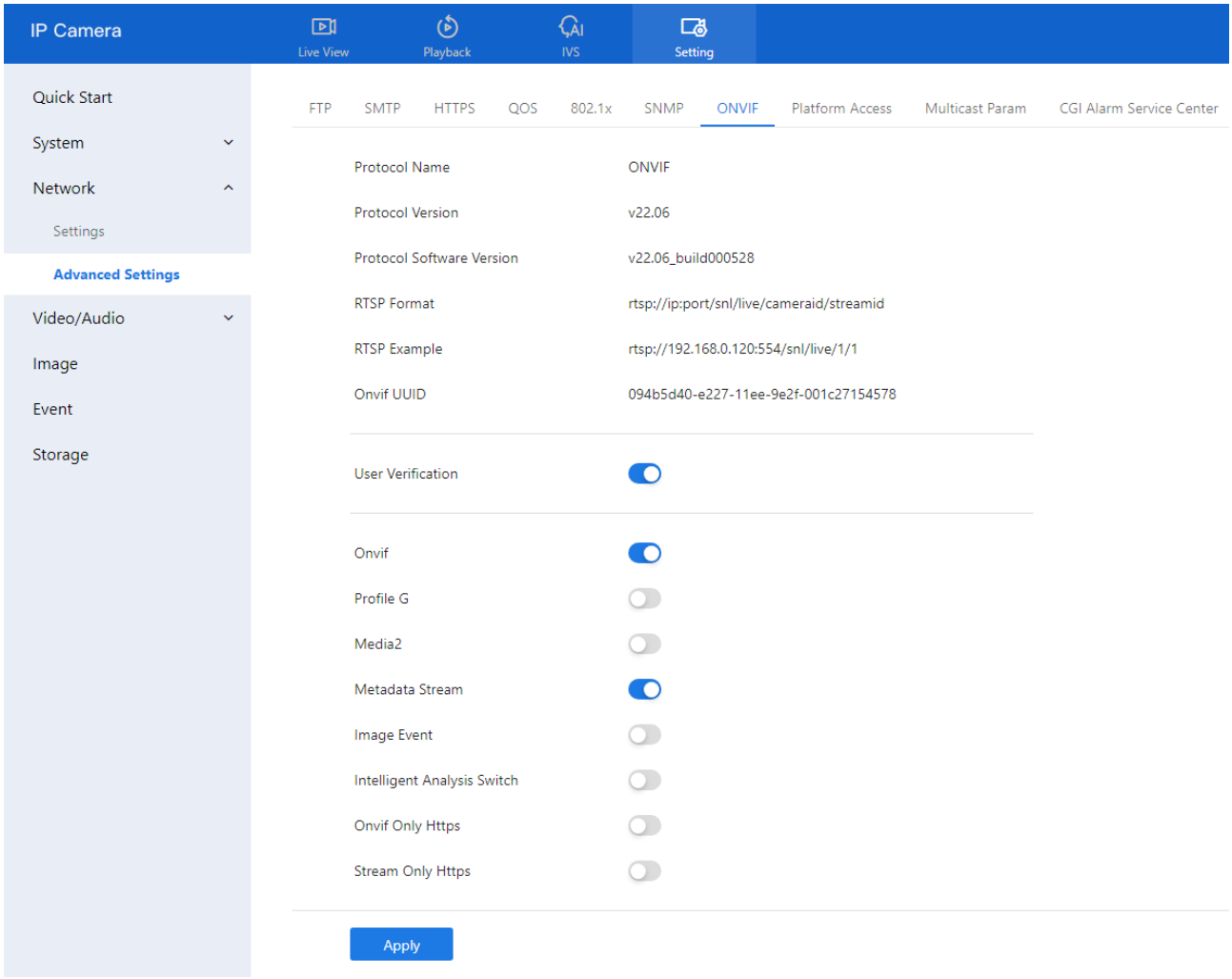


Table 4-8 Parameters of protocol-related

Parameter	Description
Protocol Name	Type of the access protocol.
Protocol Version	Version number of the access protocol.
Protocol Software Version	Software version number of the access protocol.
RTSP Format	URL rule of Real Time Streaming Protocol.
RTSP Example	URL example of Real Time Streaming Protocol.
Onvif UUID	Universally Unique Identifier.

Parameter	Description
User Verification	When you select the **User Verification** check box, the user name and password must be the same as those for logging in to the device web page. NOTE When an ONVIF-compliant device connects to the platform, you must authenticate the username and password to ensure the connection security.
Onvif	Enable Onvif
Profile G	Enable Onvif profile G
Intelligent Analysis Switch	Enable the intelligent analysis switch
Media 2	Enable media 2
Image Event	Enable image event
Intelligent Analysis Switch	Enable active onvif
Onvif only Https	Onvif can use a more secure HTTPS mode for connection, command interaction, and video data transmission, which are transmitted in an encrypted way to enhance network security.
Stream only https	

Step 2 Click **Apply**.

A confirmation dialog appears. Click **Confirm** to restart the device and apply changes.

4.2.8 **Set Platform Access**

Description

Use **Platform Access** to connect the IP camera to a centralized management platform outside the local network. This is useful when the device and the platform are on different networks.

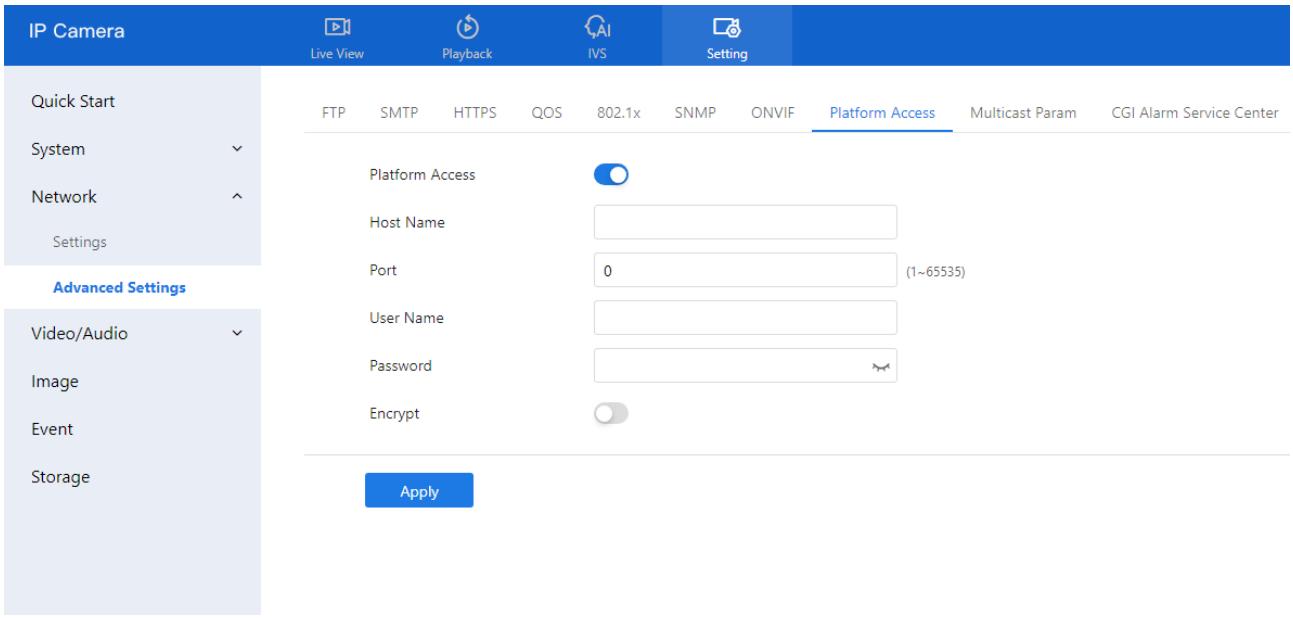
You must prepare and configure a **platform server** in advance.
Ensure that **port forwarding** or **NAT mapping** is set on the external network.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > Platform Access**.

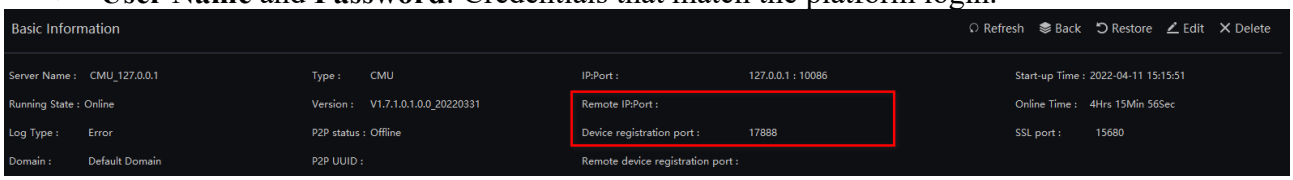
The **Platform Access** page is displayed, as shown in Figure 4-13

Figure 4-13 Platform access page



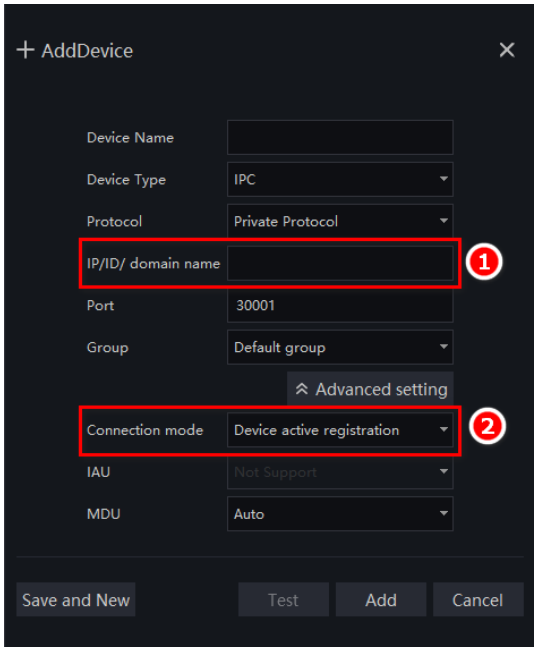
Step 2 Input the following connection parameters:

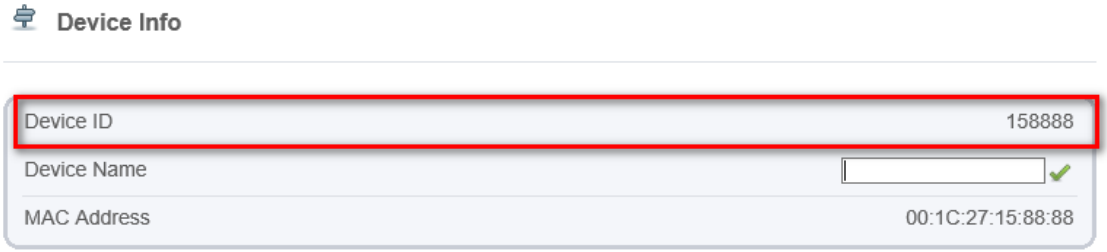
- **Host Name**: Enter the IP address or domain name of the external platform server.
- **Port**: Port used by the platform.
- **User Name** and **Password**: Credentials that match the platform login.



Step 3 When adding the IP camera to the platform, use the following information:

- **IP / ID / Domain Name**: Device ID of the IP camera.
- **Connection Mode**: Choose **Device Active Registration**.





Step 4 Enable **Encrypt** to secure the connection between the camera and the platform.
Step 5 Click **Apply**.

If the message **"Apply success!"** appears, the settings are saved and applied.

4.2.9 **Set Multicast Parameters**

Description

This section allows you to configure multicast streaming settings, including stream ID, video/audio ports, and source addresses for efficient data distribution across multicast-capable networks.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > Multicast Param**.

The **Multicast Param** page is displayed as shown in Figure 4-14. Table 4-9 describes the parameters on the **Multicast Param** page.

Figure 4-14 Multicast param page

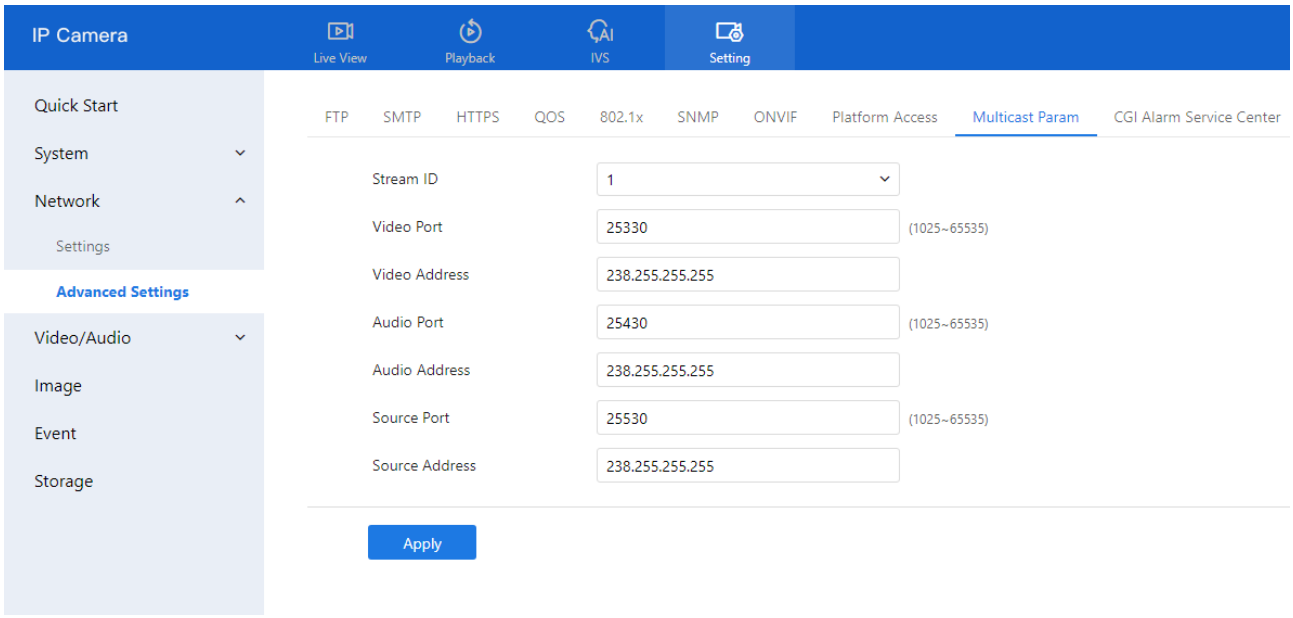


Table 4-9 Parameter description

Parameter	Description	Setting
Stream ID	ID for the stream.	[Setting method] Select a value from the drop-list box. [Default value] 1
Video address	IP address to receive video multicast data.	[Setting method] Enter a value manually. [Default value] 238.255.255.255
Video Port	Port for receiving a video stream.	[Setting method] Enter a value manually. [Default value] 25330

Parameter	Description	Setting
Audio Port	Port for receiving the audio stream.	[Setting method] Enter a value manually. [Default value] 25430
Source Port	Port for receiving source data.	[Setting method] Enter a value manually. [Default value] 25530

Step 2 Click **Apply**.

A confirmation message will appear. Settings take effect after the device restarts.

4.2.10 Set CGI Alarm Service Center

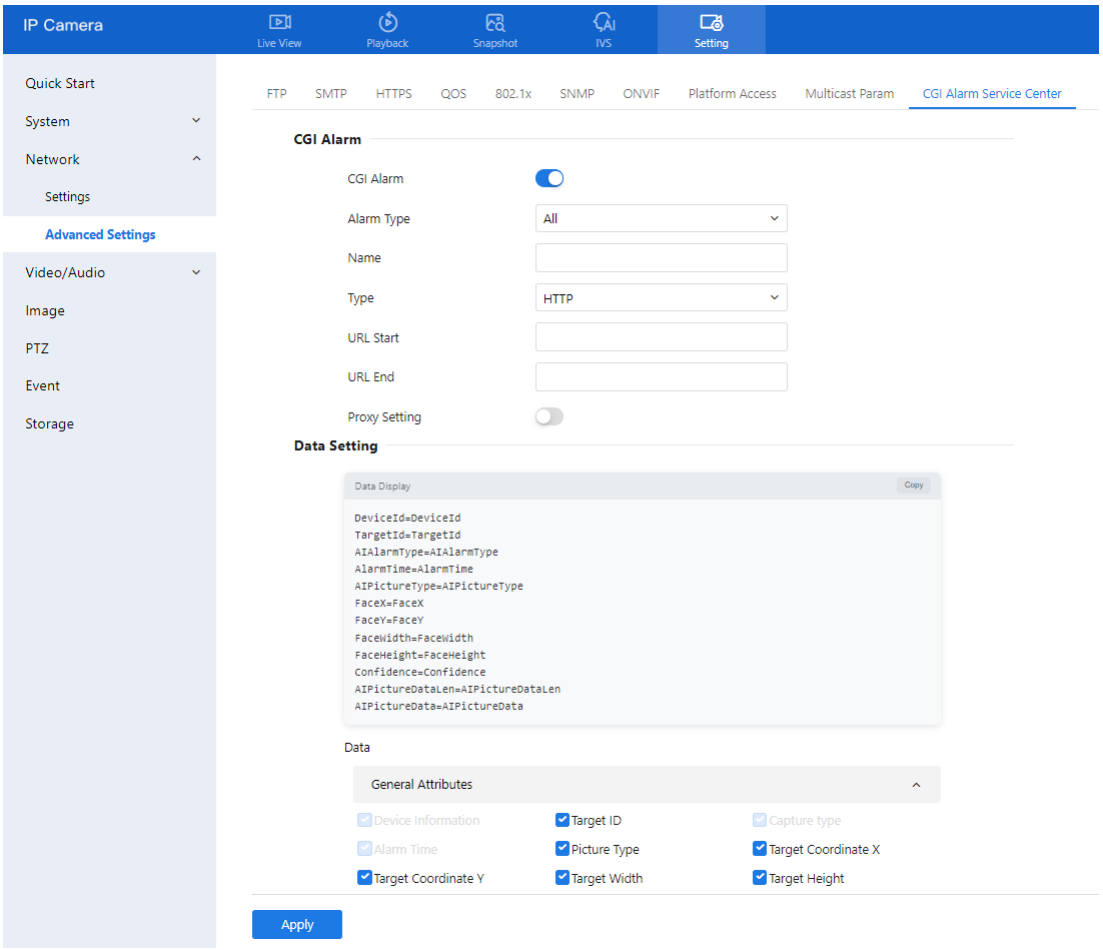
Description

When enabled, the device can send alarm messages using **CGI (Common Gateway Interface)** through specified **Start URL** and **End URL** using the **HTTP** protocol. Alarm data is embedded in the **User-Agent** field of HTTP headers and forwarded to a configured CGI server.

Procedure

Step 1 Navigate to **Setting > Network > Advanced Settings > CGI Alarm Service Center**.
The page is displayed, as shown in Figure 4-15.

Figure 4-15 CGI alarm service center page



Step 2 Click the toggle to **enable CGI Alarm**.
Step 3 Set the parameters according to Table 4-10.

Table 4-10 Parameters of the CGI Alarm service center

Parameter	Description	Setting
CGI Alarm	Enable or disable CGI alarm functionality.	[Setting method] Click the button on. [Default value] OFF
Alarm Type	Enable or disable CGI alarm functionality.	[Setting method] Select a value from the drop-down list box. [Default value] All
Name	Custom name for the CGI alarm.	[Setting method] Enter a value manually.

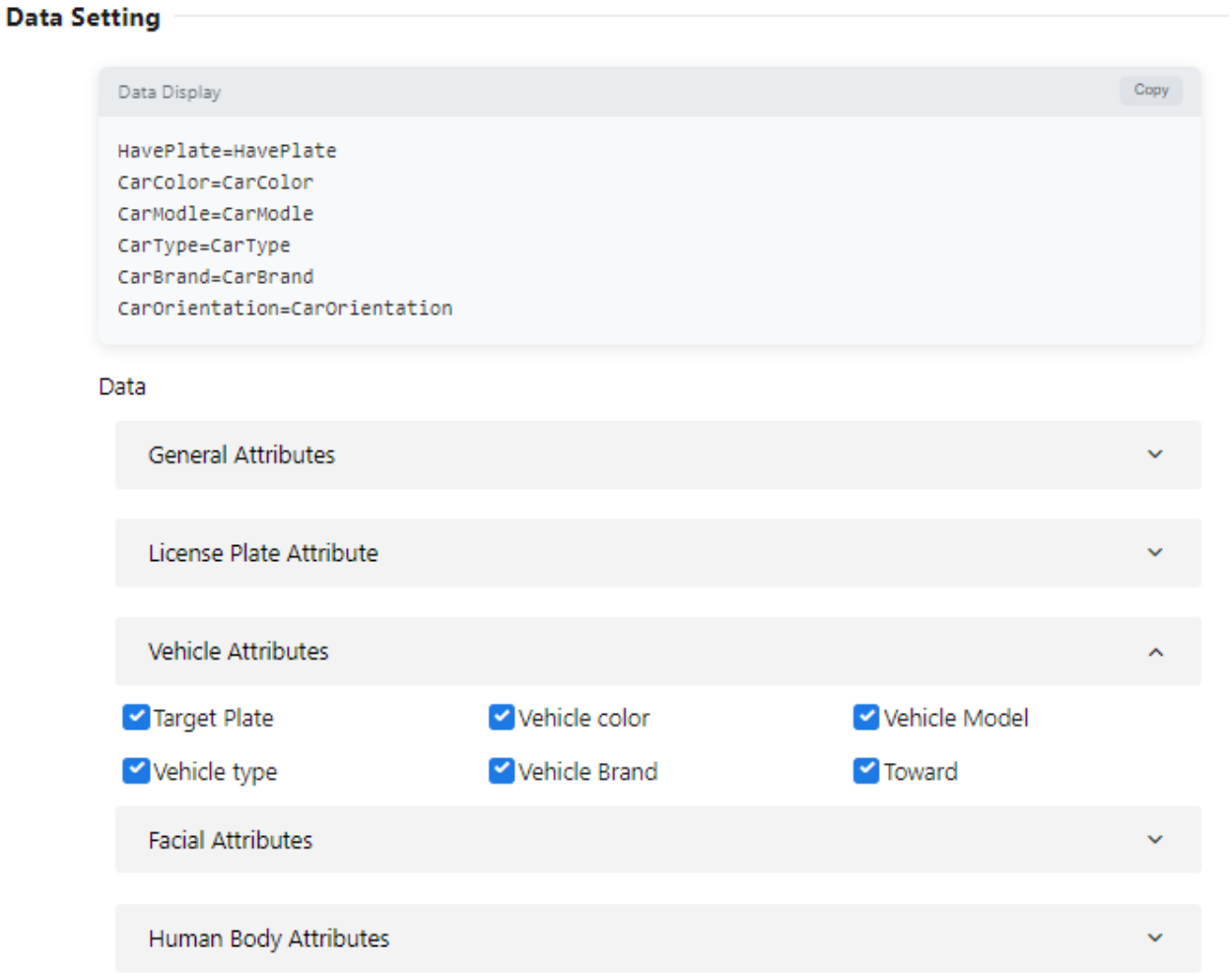
Parameter	Description	Setting
Type	Protocol type for pushing the alarm (e.g., HTTP).	[Setting method] Select a value from the drop-down list box. [Default value] HTTP
URL Start	URL to which the alarm is pushed at start.	[Setting method] Enter a value manually. For example: http://192.168.35.74:80/MajorAlarmType&MinorAlarmType&SourceName&DeviceID&DeviceIP&AlarmTime&Description
URL End	URL to which the alarm is pushed at the end.	[Setting method] Enter a value manually. For example: http://192.168.35.74:80/MajorAlarmType&MinorAlarmType&SourceName&DeviceID&DeviceIP&AlarmTime&Description
Proxy Setting	Enable proxy for forwarding CGI alarms.	[Setting method] Click the button on. [Default value] OFF
Address	IP address of the proxy server.	[Setting method] Enter a value manually.
Port	Proxy server port.	[Setting method] Enter a value manually.
Platform User Name	Username for proxy platform login.	[Setting method] Enter a value manually.
Platform Password	Password for proxy platform login.	[Setting method] Enter a value manually.
Test the connection to the specified HTTP server	Test if the device connects to the proxy successfully.	[Setting method] Click Test, if the device connects to the proxy successfully, the message “Test CGI alarm success” is displayed.
Data setting	Tick the general attributes, and the detailed information will show.	[Setting method] Tick

Step 4 Click **Apply**.

- If **"Apply success!"** appears, the settings are saved.

- If **"Parameter is invalid"** appears, check and correct the configuration.

Figure 4-16 Data setting



5 Configuration Video/Audio

5.1 Video

5.1.1 Set video

For detailed instructions on setting video parameters, please refer to **Chapter 2.5**

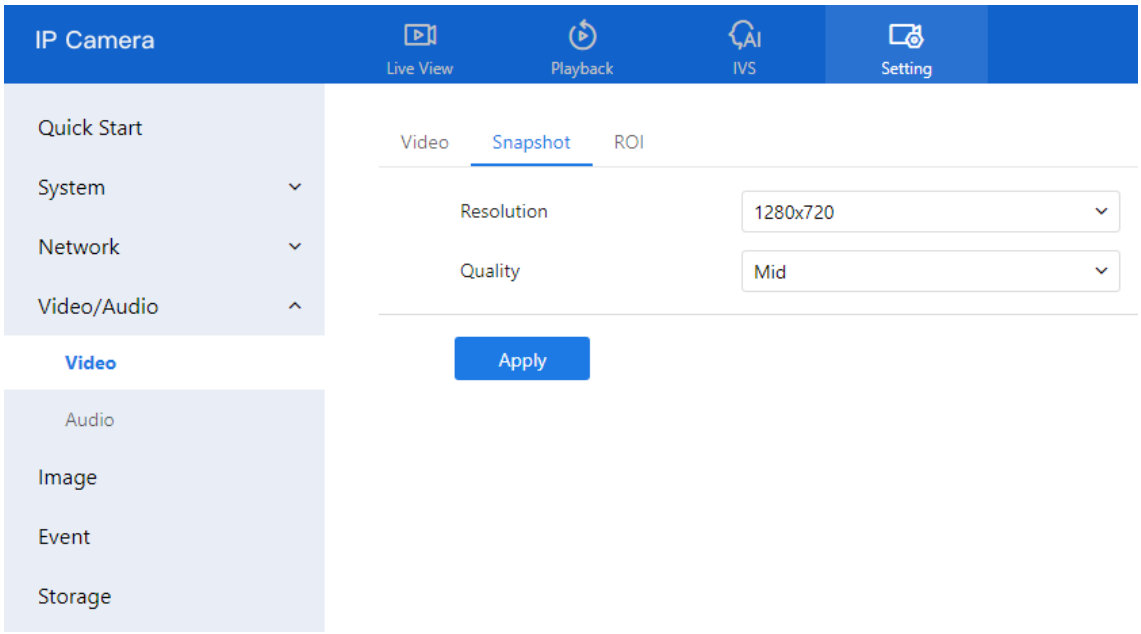
5.1.2 Snapshot

Procedure

Step 1 Navigate to **Setting > Video/Audio > Snapshot**.

The **Snapshot** configuration page is displayed, as shown in Figure 5-1.

Figure 5-1 Snapshot configuration page



Step 2 Set the parameters according to Table 5-1.

Table 5-1 Parameters of snapshot configuration

Parameter	Description	Setting
Snapshot Resolution	Choose the resolution of the snapshot.	[Setting method] Select a value from the drop-down list box. [Default value] **1280*720**

Parameter	Description	Setting
Snapshot Quality	Choose the quality of the snapshot.	[Setting method] Click the button. [Default value] **Mid**

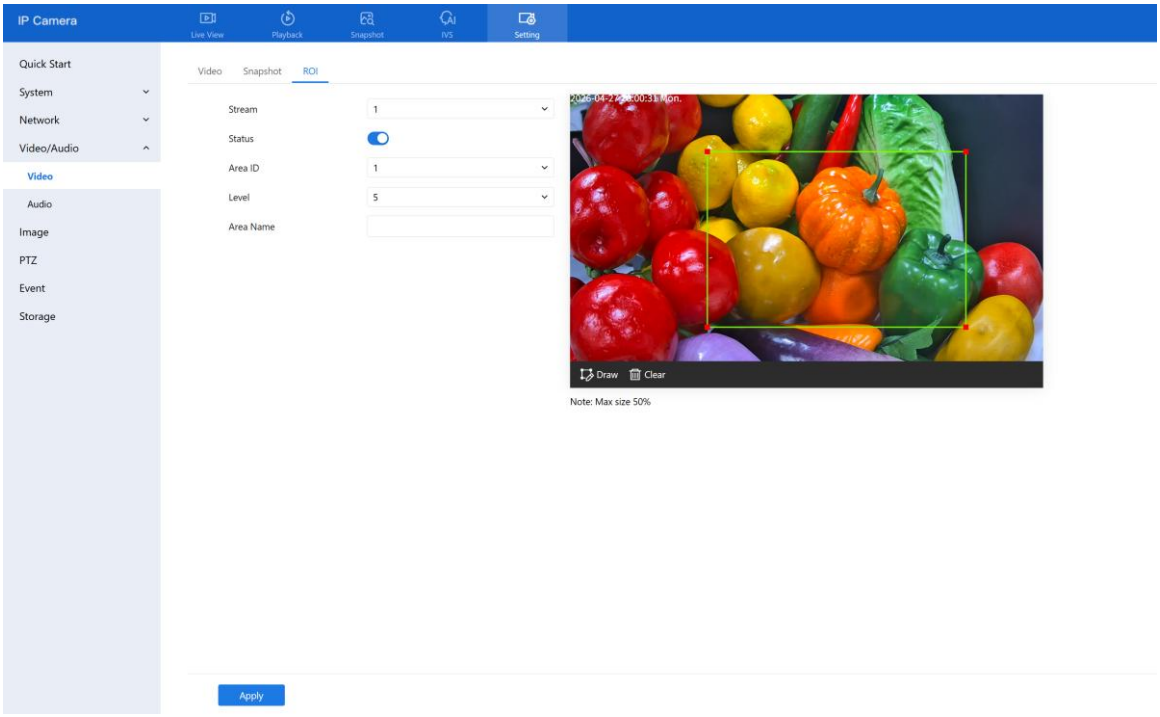
5.1.3 ROI Parameter

Procedure

Step 1 Navigate to **Setting > Video/Audio > Snapshot**.

The **Snapshot** configuration page is displayed as shown in Figure 5-2.

Figure 5-2 ROI configuration page



Step 2 Set the parameters according to Table 5-2.

Table 5-2 Parameters of ROI

Parameter	Description	Setting
Channel	For general cameras, the default is channel l. For bi-spectrum cameras, 1 is the optical channel, and 2 is the thermal channel.	[Setting method] Select a value from the drop-down list box. [Default value] Stream 1
Stream	Stream ID.	[Setting method] Select a value from the drop-down list box. [Default value] Stream 1
Status	Enable or disable the ROI	[Setting method] Click the button. [Default value] OFF
Area ID	ROI area ID	[Setting method] Select a value from the drop-down list box. [Default value] 1
Level	The visual effect of ROI. The higher the level is, the clearer the area is; the more blurred outside the area.	[Setting method] Select a value from the drop-down list box. [Default value] 5
Area Name	The marked name is used for areas.	[Setting method] Enter a value manually. The value cannot exceed 32 bytes.

Step 3 Click **Draw** to show the red frame, and drag the four corners of the rectangle to adjust the position.

Step 4 Click **Apply**.

If the message **"Apply success!"** is displayed, the settings have been saved.

5.2 Audio

5.2.1 Audio

Description

On this page, you can configure **audio input and output** settings, including type, volume, and noise reduction.

Procedure

Step 1 Navigate to **Setting > Video/Audio > Audio**. The **Audio Input** page is displayed, as shown in Figure 5-3. Table 5-3 describes the parameters.

Figure 5-3 Audio input page

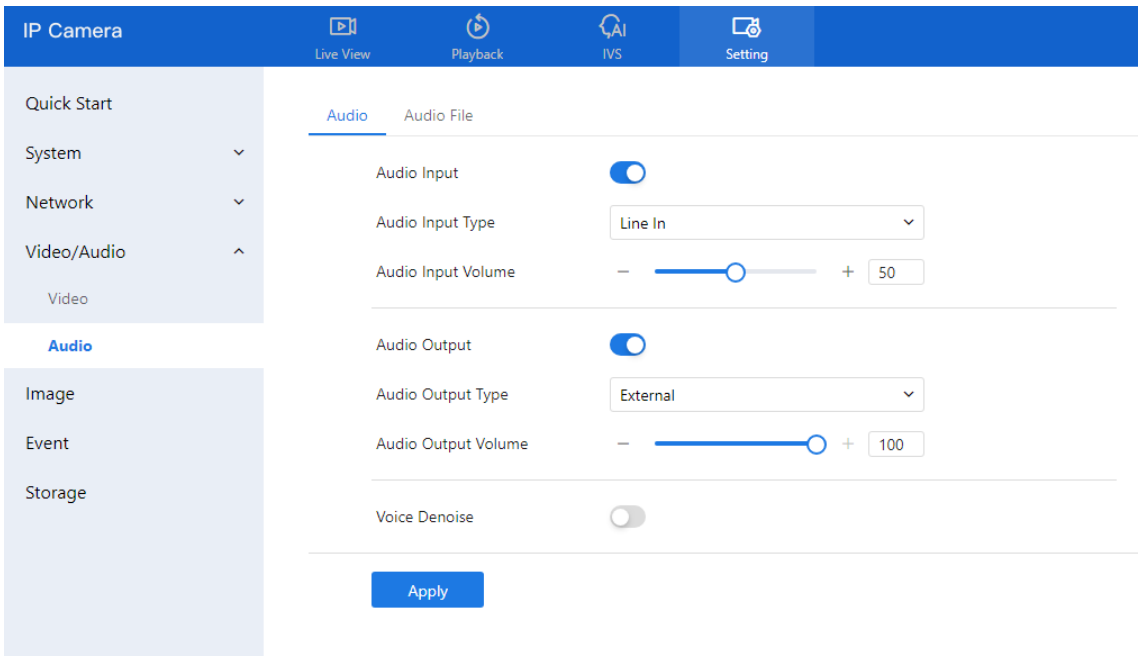


Table 5-3 Parameters of audio input

Parameter	Description	Setting
Enable Audio Input	Indicates whether to enable the audio input function.	[Setting method] Click the button to enable audio input.
Audio Input Type	Audio input types include: Line In / Internal An active audio input is required.	[Setting method] Select a value from the drop-down list box.

Parameter	Description	Setting
Audio Input Volume	Allows you to adjust the audio input volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.
Enable Audio Output	Indicates whether to enable the audio output function.	[Setting method] Click the button to enable audio output.
Audio Output Type	Microphone types include: □ External An active audio output is required. Internal means the camera own speaker.	[Setting method] Select a value from the drop-down list box.
Audio output Volume	Allows you to adjust the audio output volume.	[Setting method] Slide the slider left or right. [Default value] 50 NOTE The value ranges from 0 to 100.
Voice Denoise	Reduces background noise on internal mic.	[Setting method] Click the button to enable.

Step 2 Click **Apply**.

If **"Apply success!"** is displayed, the settings have been saved.

5.2.2 **Audible File (Feature available only on certain models)**

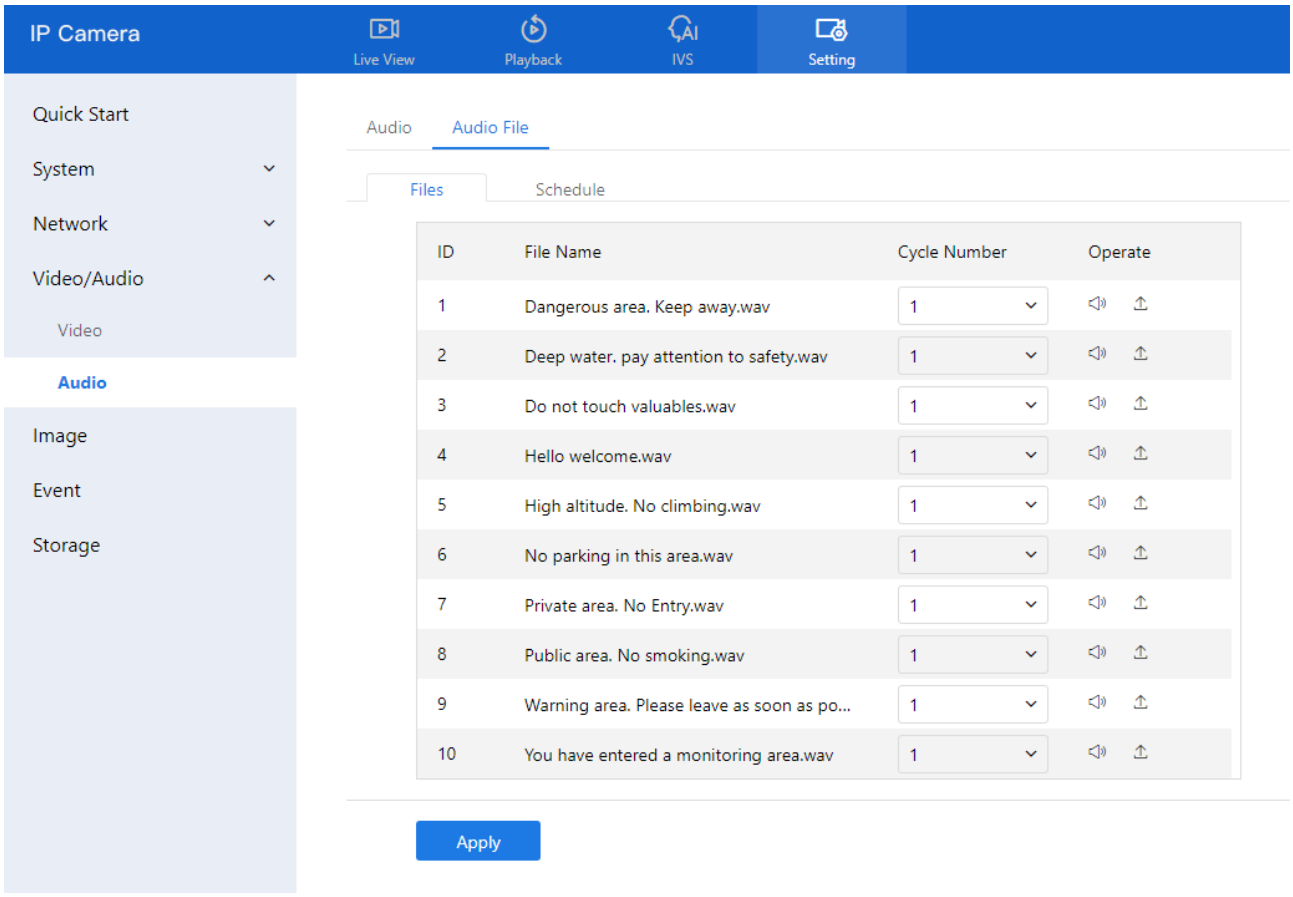
Procedure:

Step 1 Navigate to **Setting > Video/Audio > Audio > Audio File**.

The **Audio File** configuration page is displayed, as shown in Figure 5-4.

- Volume for playback can be adjusted at **Setting > Video/Audio > Audio** > **Audio Output**, as shown in Figure 5-4.

Figure 5-4 Audio file page



Step 2 The interface provides a list of 13 default audio files. For each file, you can:

- **Set Cycle Number**: The number of times the file will play when triggered.
- **Test Playback**: Click the **(speaker icon)** to listen to the file.

Step 3 To upload a custom audio file:

- Click the **Upload** icon.
- In the upload window, select a **WAV** file from your computer.
- **File requirements:**
- Format: `.wav`
- Size: less than **250 KB**
- Bitrate: **128 kbps**
- Click **Apply** to upload the file.

Step 4 . Click **Apply** to save the overall audio alarm configuration.

Step 5 CCVC Proceed to configure the **armed schedule** to define when audible alarms should be triggered.

6 Configuration Image

6.1 Configure Display

For detailed information, please refer to **Chapter 2.3**

6.2 Configure OSD

For detailed information, please refer to **Chapter 2.4**

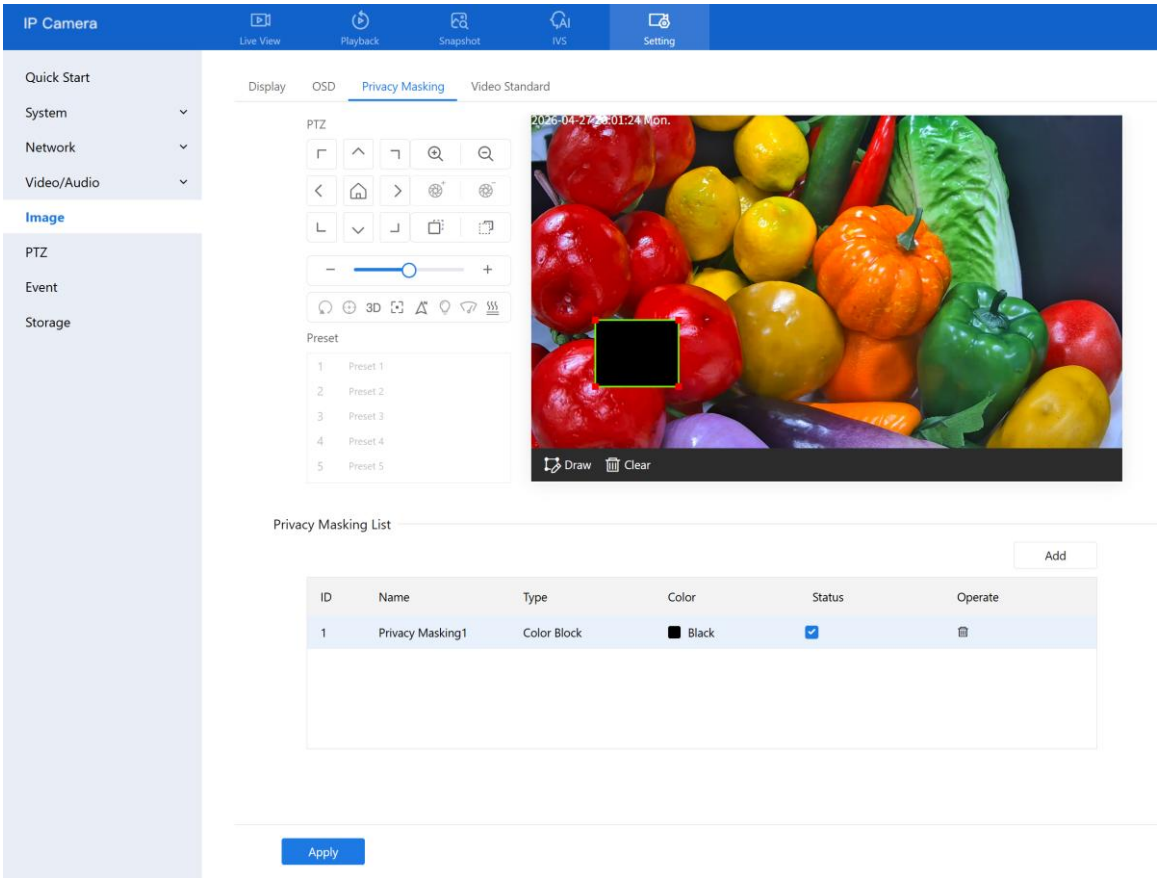
6.3 Configure the Privacy Mask

Procedure

Step 1 Navigate to **Setting > Image > Privacy Masking**.

The **Privacy Masking** page is displayed, as shown in Figure 6-1.

Figure 6-1 Privacy masking page



Step 2 Click **Draw** to display a red frame over the video preview. Drag the four corners of the rectangle to adjust its position and size.

Step 3 Click **Clear** to remove the selected frame.

NOTE

- The maximum maskable area depends on the device model (refer to on-screen tips).

- You can mask up to **four areas**.
- To delete a masking area: Tick the corresponding ID in the **Privacy Masking List**, then click **Delete**.

Step 4 Set the parameters according to Table 6-1.

Table 6-1 Parameters of privacy masking

Parameter	Description	Setting
ID	Identifier for each masking area.	N/A
Name	Name for the masking area.	[Setting method] Click the name and enter a value manually. [Default value] **Blank**
Type	Type of privacy masking.	[Setting method] Select a value from the drop-down list box. [Default value] **Color Block**
Color	Color of privacy masking.	[Setting method] Select a value from the drop-down list box. [Default value] **Black**
Enable	Indicates whether to enable the privacy masking.	[Setting method] Select a value from the drop-down list box. [Default value] **Yes**
Delete	Delete a privacy masking.	[Setting method] 1. Select a privacy masking from the Privacy Masking List. 2. Click **Delete**, and the privacy masking is deleted successfully.
Modify	Modify the privacy masking.	[Setting method] 1. Select a privacy masking from the Privacy Masking List. 2. Click a parameter and modify it. 3. Click **Modify**, and the privacy masking is modified successfully.

Step 5 Click **Add** to add privacy masking.

6.4 Configure Video Standard

Procedure

Step 1 Navigate to **Setting > Image > Video Standard**.

The **Camera** page is displayed, as shown in Figure 6-2. Set the video format parameters according to Table 6-2.

Figure 6-2 Camera page

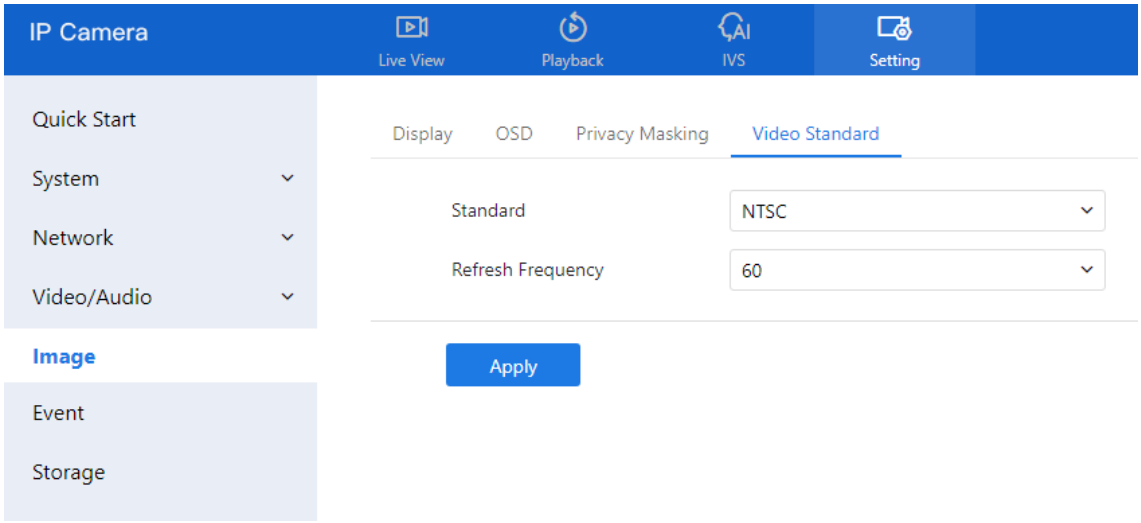


Table 6-2 Parameters of the camera

Parameter	Description	Setting
Video System	The options are as follows: □ PAL: Used in Europe, China mainland, India, Pakistan, etc. □ NTSC: Used in the USA, Japan, South Korea, and Taiwan, etc.	[Setting method] Select a value from the drop-down list box. [Default value] PAL NOTE Whether the video system can be changed depends on the device model.
Video Refresh Frequency	The options are as follows: □ 50 Hz: corresponds to the PAL system. □ 60 Hz: corresponds to the NTSC system.	[Setting method] Follow the video standard.

Step 2 Click **Apply**. If the message **"Apply success!"** is displayed, the settings are saved.

NOTE

If the message **"The device will restart. Are you sure to modify?"** appears, confirm to proceed.
The system will restart and apply the new video standard.

7 Configure Event

Alarm linkage actions vary by camera model and hardware capabilities. Please refer to your specific device documentation for supported features.

7.1 Motion Alarm Linkage

Description

The **Motion Alarm** page allows you to:

- Enable or disable motion detection.
- Configure detection schedules and areas.
- Link motion events to alarms (e.g., audible alerts, recordings, light signals).
- Trigger notifications via FTP or SMTP.

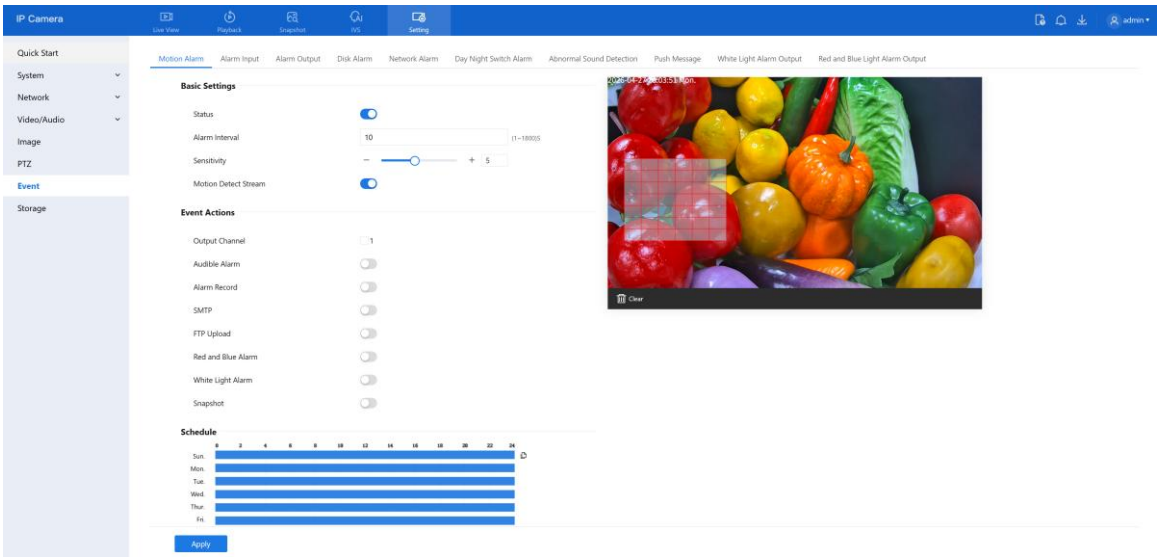
When motion is detected within a predefined area and schedule, the camera generates an alarm and triggers the configured linkage actions.

Procedure

Step 1 Go to **Setting > Event > Motion Alarm**.

The **Motion Alarm** page is displayed, as shown in Figure 7-1.

Figure 7-1 Motion alarm page



Step 2 Configure all parameters. Please refer to Table 7-1.

Table 7-1 Motion alarm parameters

Parameter	Description	Setting
Status	Enables or disables motion detection.	[How to set] Click Enable to enable. [Default value] **OFF**

Parameter	Description	Setting
Alarm Interval	Sets the time interval (1–1800 seconds) during which repeated alarms are suppressed.	[How to set] Input a value, 1~1800s
Sensitivity	Determines motion detection sensitivity. Higher values detect smaller movements but may reduce accuracy.	[How to set] Choose from the drop-down list [Default value] **5**
Motion Detect Stream	Enables or disables motion detection.	[How to set] Click to enable [Default value] **OFF**
Output Channel	If you check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals when an alarm is triggered. Only for Some Models. (Set at the "**Setting > Event > Alarm Output**", the details please refer to ***Chapter 7.3***)	[How to set] Click to select an ID.
Audible Alarm	Triggers audio warning playback (configured in **Setting > Video/Audio > Audio File**).	[How to set] Click to enable Audible alarm [Default value] **OFF**
Alarm Record	Records alarm-triggered video to the SD card	[How to set] Click to enable alarm record. [Default value] **OFF**
SMTP	Sends alarm notifications via email. SMTP must be configured.	[How to set] Click to enable SMTP. [Default value] **OFF**
FTP Upload	Uploads alarm snapshots to an FTP server. FTP must be configured.	[How to set] Click to enable FTP Upload. [Default value] **OFF**

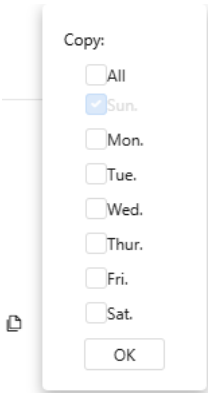
Parameter	Description	Setting
Snapshot	Uploads alarm snapshots and full-screen images to SD card or NAS. The SD card should be inserted in advance. NAS should be configured. The result can be searched at the Snapshot page; for the details, please refer to ***Chapter 1.6 Snapshot***	[How to set] Click to enable Snapshot. [Default value] **OFF**
Flashlight Alarm	The camera should have the flashlight. The light will be flashing during an alarm (only on supported models).	[Setting method] Click to enable Flashlight Alarm [Default value] **OFF**
Whited Light Alarm	The camera should have white light or dual lights. Flickers white light during an alarm (only on supported models).	[Setting method] Click to enable White Light Alarm [Default value] **OFF**
Red and Blue Light Alarm	The camera should have red and blue lights. Flickers alternating red and blue lights during an alarm (only on supported models).	[Setting method] Enable Red and Blue Light Alarm [Default value] **OFF**

Step 3 Enable **Motion Detect Stream** if you want to visualize object tracking during motion events.

Step 4 Configure Deployment Schedule.

Method 1: Click and drag within the time grid (00:00–24:00) from Monday to Sunday.
Method 2: Click **Select All** to apply full-time deployment for all days.
Method 3: Set one day's schedule and click the **Copy icon** to replicate it to other days.

Figure 7-2 Copy



To delete all time slots, click **Clear All**.
To remove a specific time block, click it and then click **Delete**.



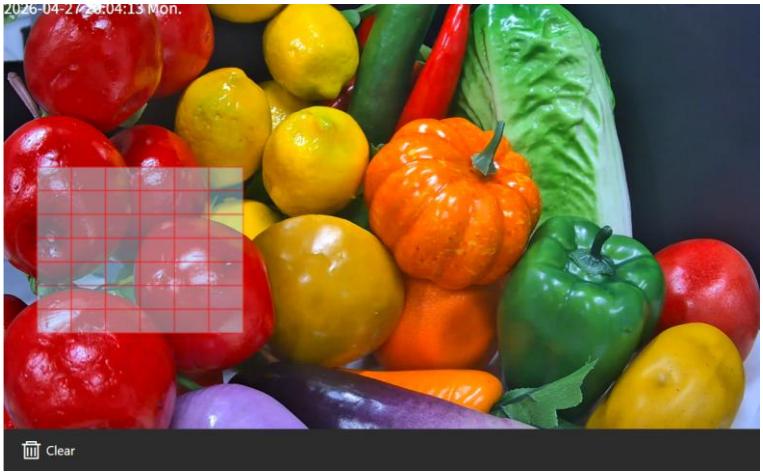
Configure the detection area.

Step 1 Press and hold the left mouse button and drag over the video preview to draw the detection zone (see Figure 7-3).

Step 2 To remove an area, click **Clear**.

Step 3 To disarm a specific block, click on the red grid square.

Figure 7-3 Motion area setting page



NOTE

Click **Clear** to delete a detection area. Click the red block to disarm this area.

Step 4 If the message **"Apply success!"** is displayed, all configurations are saved successfully.

7.2 Alarm In (Only for Some Models)

Description

When an external alarm is received through the **alarm input port**, the device can trigger various alarm linkages based on the configuration.

The **Alarm In** page allows you to:

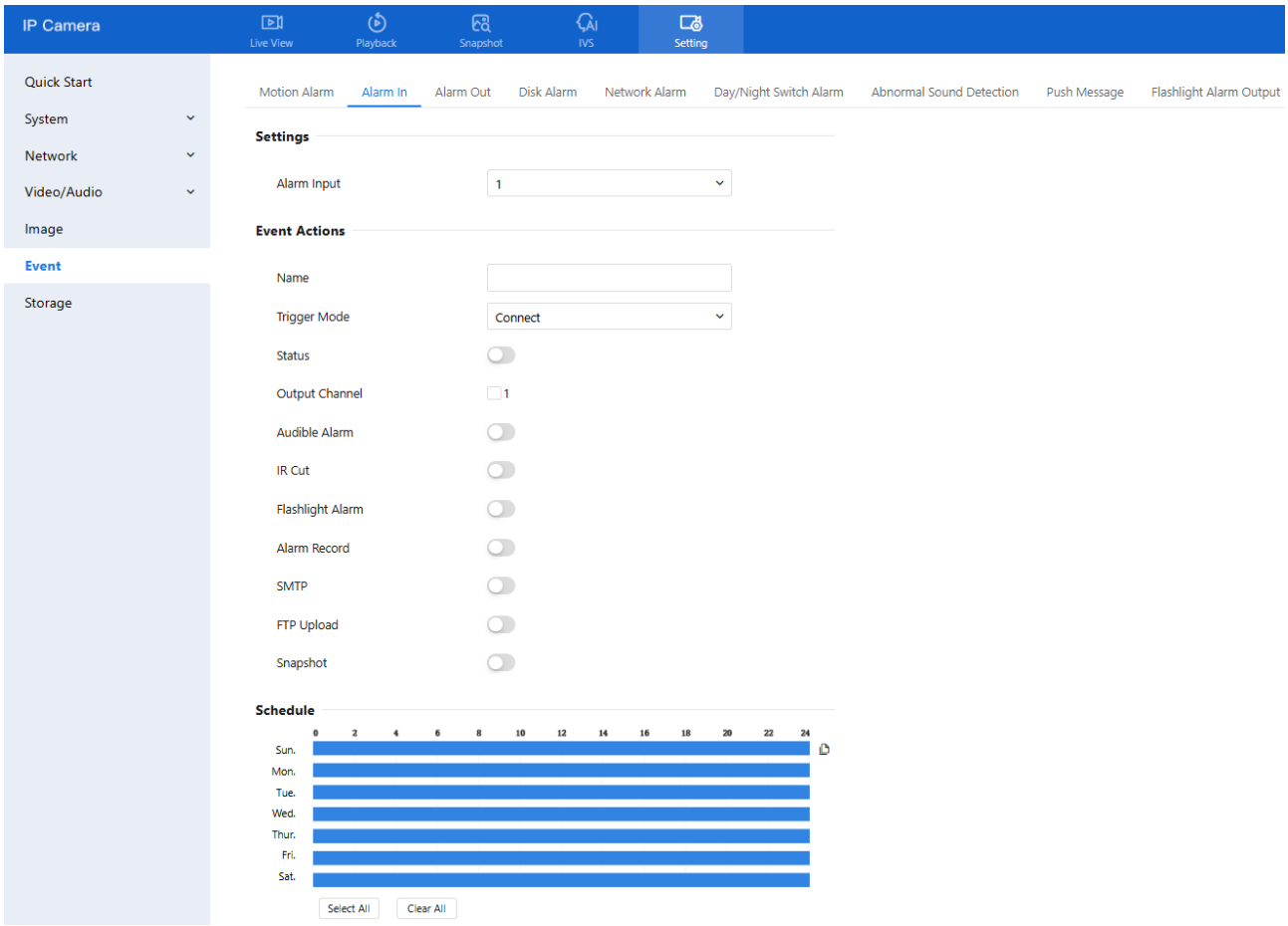
- Enable or disable I/O alarm inputs
- Configure schedules for alarm input monitoring
- Link inputs to other actions such as audible alerts, light warnings, or alarm recording

Procedure

Step 1 Navigate to **Setting > Event > Alarm In**.

The **Alarm In** page is displayed, as shown in Figure 7-4.

Figure 7-4 Alarm in page



Step 2 Set the parameters as outlined in Table 7-2

Table 7-2 Parameters of I/O alarm linkage

Parameter	Description	Setting
Alarm input	ID of the alarm input channel. NOTE The number of alarm input channels depends on the device model.	[Setting method] Select a value from the drop-down list box. [Default value] 1
Name	Alarm input channel name.	[Value range] 0 to 32 bytes
Trigger Mode	The options are as follows: □ **Connect**: An alarm is generated when an external alarm device is connected. □ **Disconnect**: An alarm is generated when the external alarm device is disconnected.	[Setting method] Select a value from the drop-down list box. [Default value] Connect

Parameter	Description	Setting
Status	When the device receives an alarm signal, it sends the alarm information to an external alarm device.	[Setting method] Enable [Default value] OFF
Output channel	Linkage the output channel alarm device to send alarm information.	[Setting method] Tick
Audible Alarm	After enabling Audible Warning and setting Audible Alarm Output, the built-in speaker of the device or the connected external speaker plays warning sounds when an alarm happens. (set at the "**Setting > Video / Audio > Audio File**")	[How to set] Click to enable Audible alarm [Default value] **OFF**
IR Cut	The camera should have an IR light. When an alarm occurs, the device will open the IR light to send alarm information.	[Setting method] Enable [Default value] OFF
Alarm Record	The device will record an alarm on the SD card.	[Setting method] Enable [Default value] OFF
SMTP	When an alarm occurs, the device will send an email. The mail parameters should be set in advance.	[Setting method] Enable [Default value] OFF
FTP Upload	When an alarm occurs, the device will send alarm information to the FTP server. The FTP parameters should be set in advance.	[Setting method] Enable [Default value] OFF
Snapshot	Snapshot the image to the SD card.	[How to set] Click to enable Snapshot. [Default value] **OFF**
Flashlight Alarm	After enabling Flashing Light and setting the Flashing Light Alarm Output, the light flashes when an alarm event is detected.	[How to set] Click the button on. [Default value] **OFF**

Parameter	Description	Setting
White Light Alarm	The camera should have white light or dual lights. When an alarm occurs, the device will flicker the white light.	[Setting method] Enable [Default value] OFF
Red and Blue Light Alarm	The camera should have red and blue lights. When an alarm occurs, the device will flicker alternating red and blue light.	[Setting method] Enable [Default value] OFF

Step 3 Set the **Deployment Schedule** using the same method as described in, please refer to 7.1 Step 4.

Step 4 Click **Apply**. If the message **"Apply success!"** is displayed, the settings are saved.

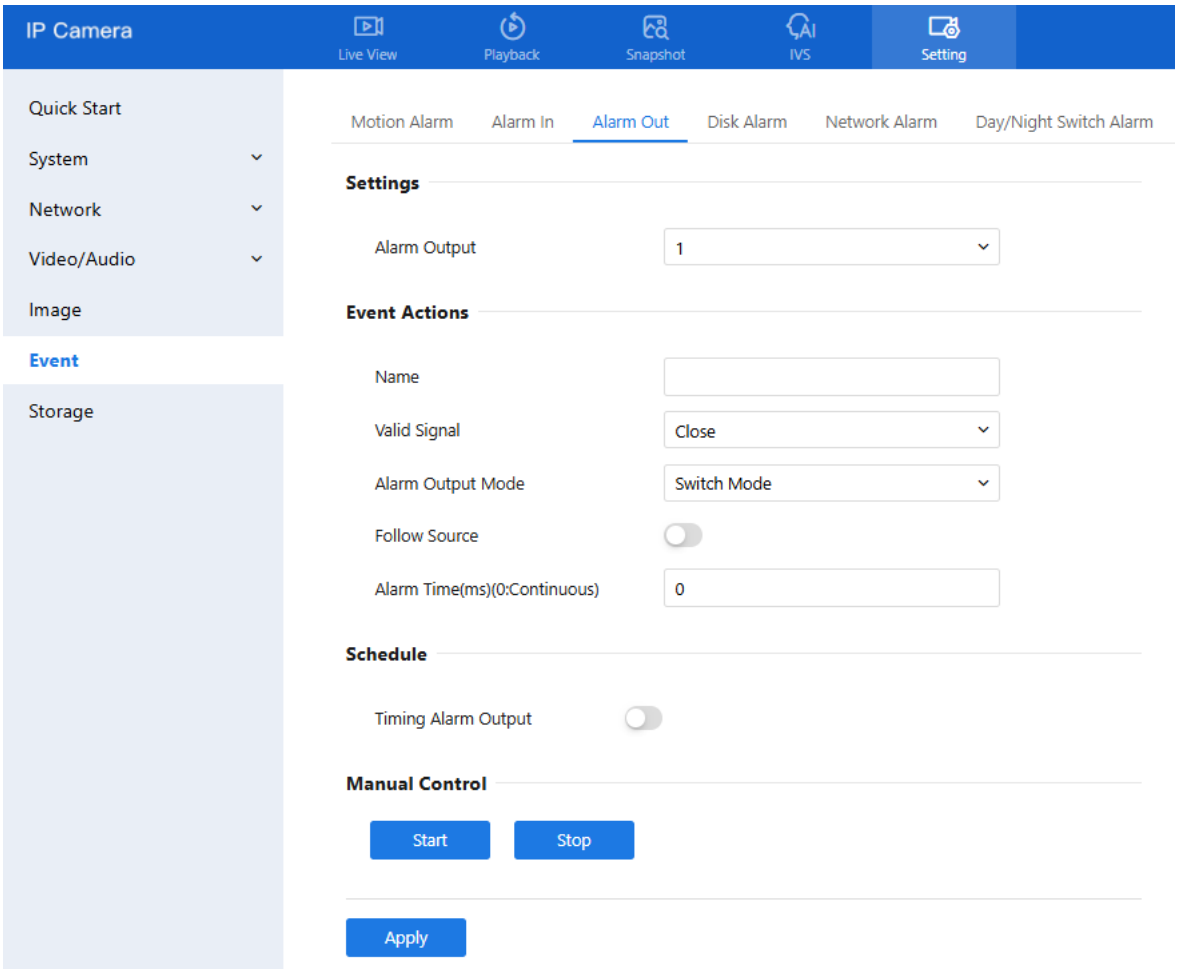
7.3 Alarm Out (Only for Some Models)

Procedure

Step 1 Navigate to **Setting > Event > Alarm Out**.

The **Alarm Out** page is displayed, as shown in Figure 7-5.

Figure 7-5 Alarm output page



Step 2 Configure the parameters according to Table 7-3.

Table 7-3 Parameters of alarm output

Parameter	Description	Setting
Alarm Output	ID of the alarm output channel. NOTE The number of alarm output channels depends on the device model.	[Setting method] Select a value from the drop-down list box. [Default value] 1
Name	Alarm output channel name.	[Value range] 0 to 32 bytes
Valid Signal	The options are as follows: □ **Close**: An alarm is generated when an external alarm signal is received. □ **Open**: An alarm is generated when no external alarm signal is received.	[Setting method] Select a value from the drop-down list box. [Default value] Close

Parameter	Description	Setting
Alarm Output Mode	When the device receives I/O alarm signals, it sends the alarm information to an external alarm device in the mode specified by this parameter. The options include the switch mode and pulse mode. NOTE If the switch mode is used, the alarm frequency of the device must be the same as that of the external alarm device. If the pulse mode is used, the alarm frequency of the external alarm device can be configured.	[Setting method] Select a value from the drop-down list box. [Default value] Switch Mode
Follow Source	Alarm output follows the duration of the alarm source.	[Setting method] Enable [Default value] OFF
Alarm Time (ms) (0: Continuous)	The status of the alarm is on. Alarm output duration. The value **0** indicates that the alarm remains valid.	[Setting method] Enter a value manually. [Default value] 0 [Value range] 0 to 86400 seconds
Timing Alarm Output	Enable timing alarm output, set the schedule to time alarm。 NOTE If there are two alarm outputs, this setting is only valid for Alarm output 1.	[Setting method] Enable [Default value] OFF
Manual Control	Control the alarm output.	N/A

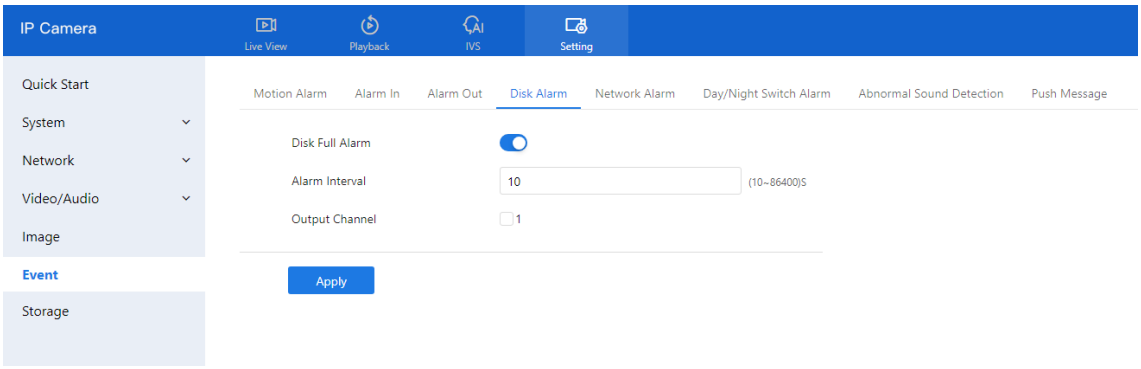
Step 3 Click **Apply**. If "Apply success!" appears, the settings have been saved successfully.

7.4 Disk Alarm

Procedure

Step 1 Navigate to **Setting > Event > Disk Alarm**.
The **Disk Alarm** page is displayed, as shown in Figure 7-6.

Figure 7-6 Disk alarm page



Step 2 Click the toggle button on to enable the disk alarm.

Step 3 Configure the **Alarm Interval**. This sets how often the system triggers alarms for disk issues. Enter a value in seconds (range: 10–86400).

Step 4 Select the **Out Channel** number (Please refer to the actual product).

Step 5 Click **Apply**. When the message **"Apply success!"** appears, the configuration is saved.

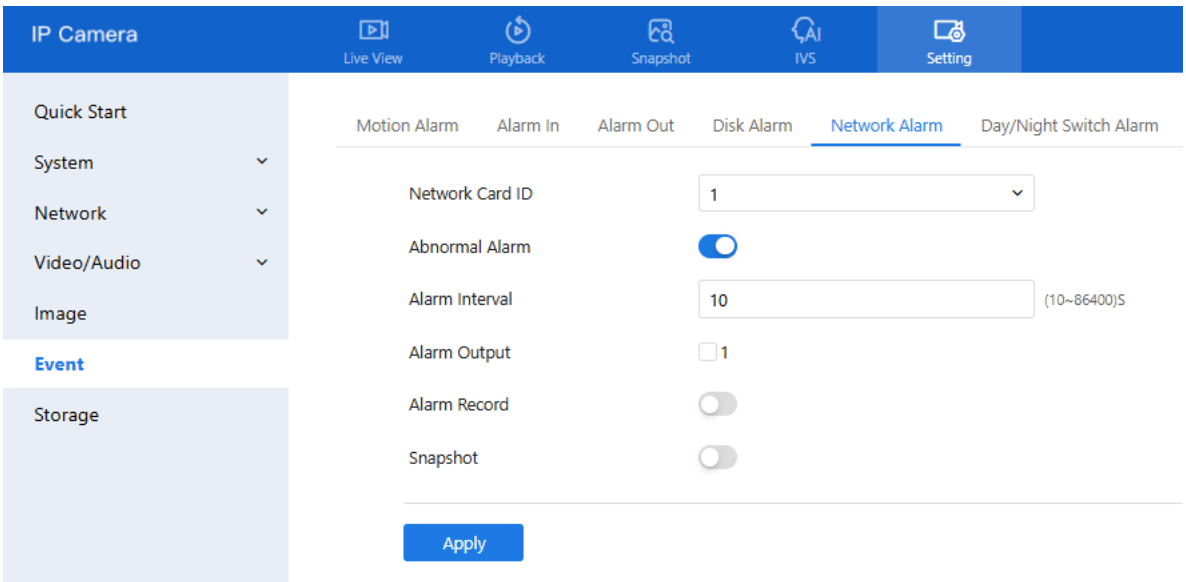
7.5 Network Alarm

Procedure

Step 1 Navigate to **Setting > Event > Network Alarm**.

The **Network Alarm** page is displayed, as shown in Figure 7-7.

Figure 7-7 Network alarm page



Step 2 Click the toggle button to enable **Abnormal Alarm.** The system will monitor the network interface for abnormalities.

Step 3 Configure the **Network Alarm Interval**. Enter how frequently the system should check for network errors.

Step 4 Select the **Output Channel** for alarm notifications. You may also enable **Alarm Record** if an SD card is installed.

Step 5 Click **Apply**. A message stating "Apply success!" confirms that settings have been saved.

7.6 Day/Night Switch Alarm

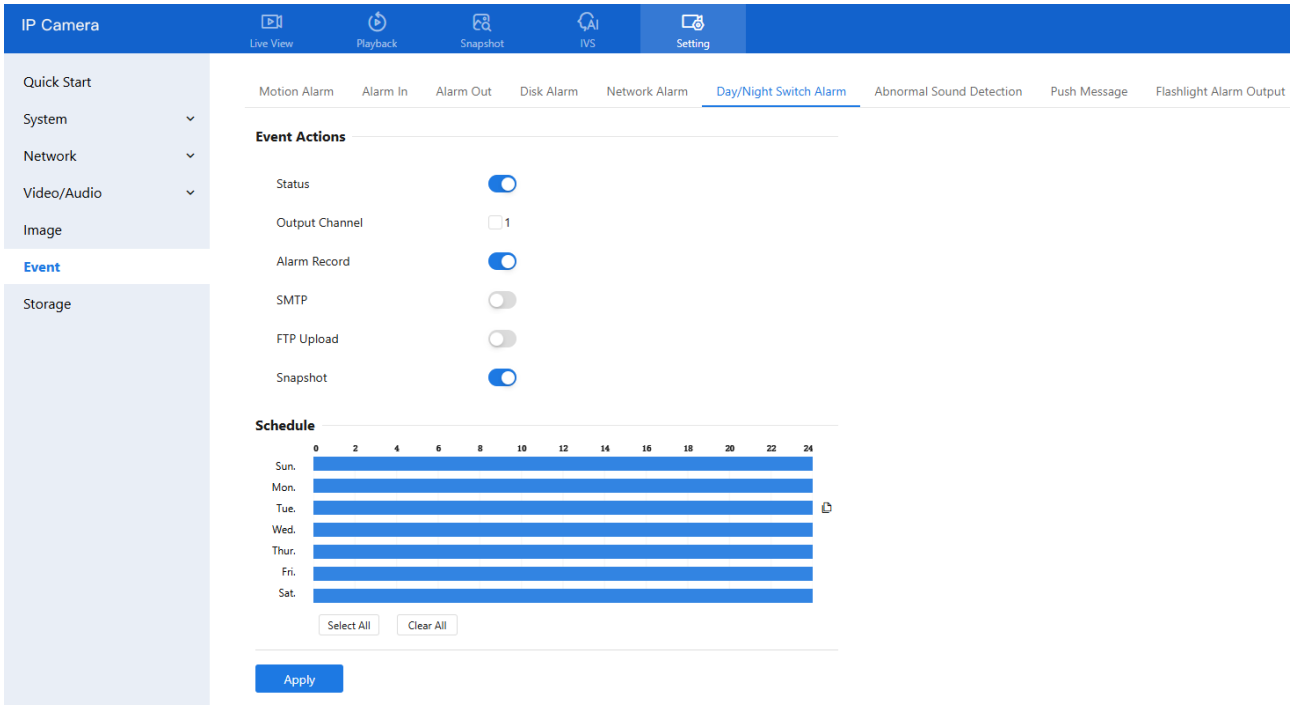
Description

The **Day/Night Switch Alarm** function triggers an alert whenever the camera switches between day and night modes according to the defined schedule.

Procedure

Step 1 Navigate to **Setting > Event > Day/Night Switch Alarm**.
The **Day/Night Switch Alarm** page is displayed, as shown in Figure 7-8.

Figure 7-8 Day/Night switch alarm



Step 2 Click the toggle to **enable Day/Night Switch Alarm**.
Step 3 Configure the **alarm schedule**.
Define the specific time ranges during which the alarm should be active.
Step 4 Enable **Alarm Record** if you want the event recorded to an SD card.
Toggle the switch to activate.
Step 5 Enable **SMTP** if you wish to receive an email notification.
SMTP must be configured under **Network > Advanced Settings > SMTP**.
Step 6 Enable **FTP Upload** to send alarm data to an FTP server.
FTP must be pre-configured in system settings.
Step 7 Enable **Snapshot** to save to SD card or NAS.
NAS must be pre-configured in storage settings.
Step 8 Click **Apply**.
When the message **"Apply success!"** appears, the settings are successfully saved.

7.7 Abnormal Sound Detection (Only for Some Models)

Description

The camera is equipped with a built-in microphone or supports external audio input (Line In). On the **Audio Abnormal Detection** page, you can perform the following actions:

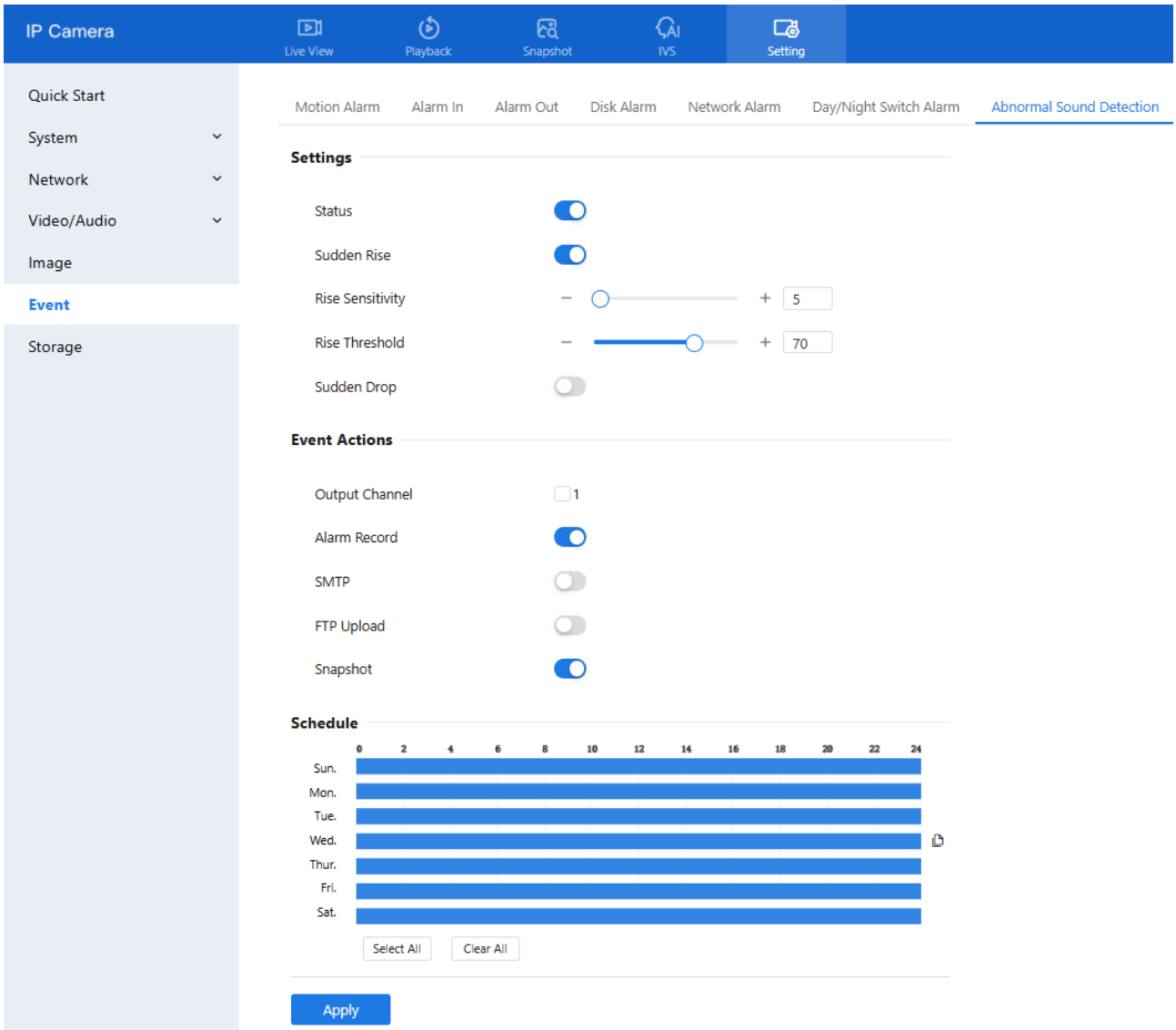
- Enable the **Abnormal Sound Detection** function.
- Set the schedule during which abnormal sound detection is active.
- Configure the alarm output channel for abnormal sound events.

When this function is enabled, and a sudden rise or drop in audio levels is detected during the scheduled time, the camera triggers an alarm and executes the corresponding linkage actions.

Procedure

Step 1 Navigate to **Setting > Event > Abnormal Sound Detection**.
The **Audio Abnormal Detection** page is displayed, as shown in Figure 7-9.

Figure 7-9 Audio abnormal detection page



Step 2 Click the toggle button to **enable Audio Abnormal Detection**.
Step 3 Enable either or both of the following:

Sudden Rise — detects sharp increases in sound level.
Sudden Drop — detects sharp decreases in sound level.

Step 4 Select the **Output Channel** for triggering the external alarm.

Step 5 Click the toggle button on to enable **Alarm Record**, **SMTP**, **FTP Upload, and Snapshot**.

Step 6 Configure the **Schedule** (deployment time). For details about how to set **the schedule**, please refer to 7.1 Step 4.

7.8 Push Message

Description

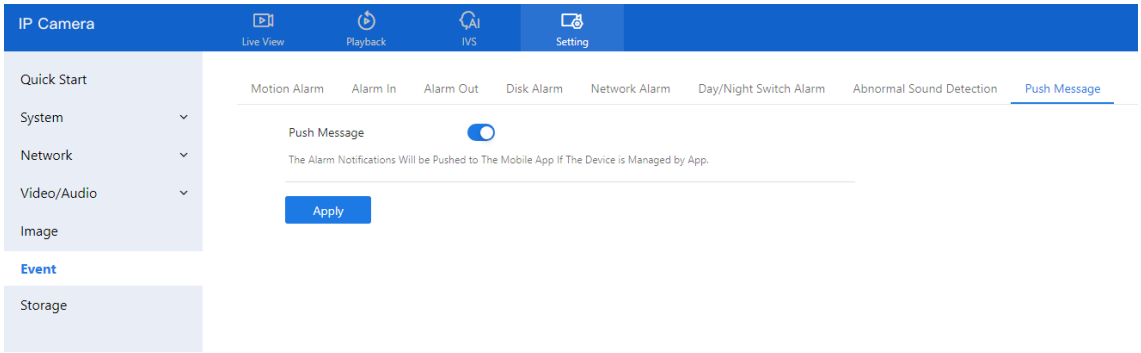
When alarms are triggered, a notification can be pushed to the mobile app (if the device is connected to and managed through the app).

Procedure

Step 1 Navigate **Setting > Event > Push Message**.

The **Push Message** page is displayed, as shown in Figure 7-10.

Figure 7-10 Push message page

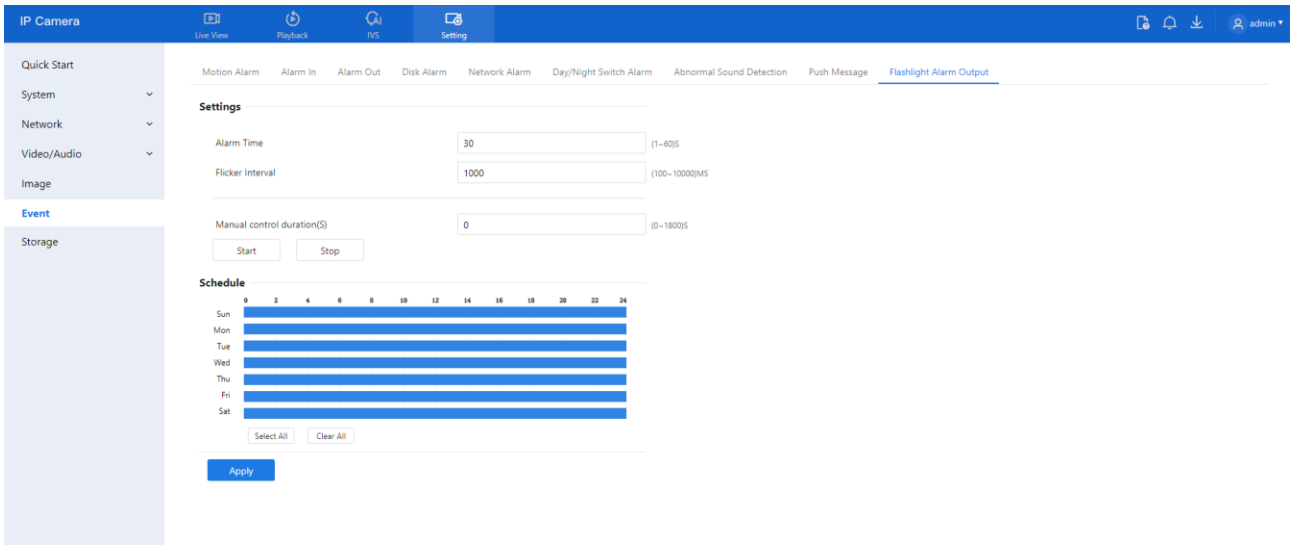


Step 2 Click **Apply**. A message stating **"Apply success!"** will confirm the configuration is saved.

7.9 Flashlight Alarm Output (Only for Some Models)

Step 1 Go to **Setting > Event > Flashlight Alarm Output** interface and set the schedule to enable flashlight alarm, as shown in Figure 7-11.

Figure 7-11 Flashlight alarm page



Step 2 Configure the **Alarm Duration** and **Flicker Interval**.

Step 3 Set the **Manual Control Duration**:

Click **Start** to turn on the flashlight manually for the set time.

Click **Stop** to end the flashlight operation manually.

Step 4 Set the **Schedule** to determine when the flashlight alarm should be active.

Step 5 Click **Apply**.

The message **"Apply success!"** confirms the settings are saved.

8 Configure Storage Function

NOTE

Some models do not support SD cards. If unsupported, recording functionality will be disabled. Please refer to the specifications of your actual device.

8.1 Record Strategy

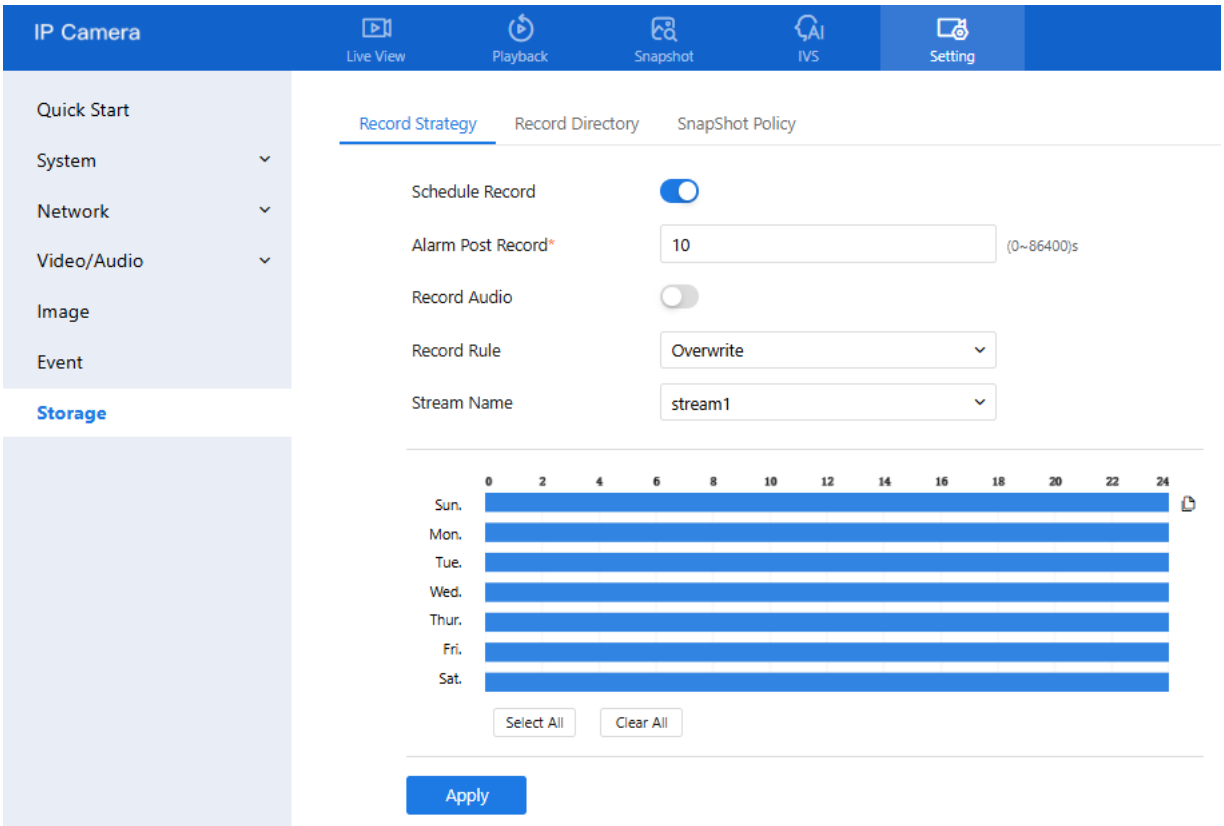
You can configure the scheduled recording, alarm recording duration, audio recording, storage rules, and stream selection.

Procedure

Step 1 Navigate to **Setting > Storage > Record Strategy**.

The **Record Strategy** page is displayed, as shown in Figure 8-1.

Figure 8-1 Record strategy page



Step 2 Configure the parameters according to Table 8-1.

Table 8-1 Parameters of recording policy

Parameter	Description	Setting
Schedule Record	Enables time-based recording.	[Setting method] Click the button to enable the schedule record. [Default value] OFF
Alarm Post Record	Time in seconds to continue recording after an alarm. (0–86400 sec)	[Setting method] Enter a value manually.
Record Audio	Records audio along with video.	[Setting method] Click the button to enable audio recording.
Record Rule	Rule for saving recordings. The options are as follows: □ **Cycle Store**: Saves recordings in cycles. □ **Save Days:** Duration (in days) for saving a recording. The duration can be a maximum of 99999 days. NOTE The value **0** indicates that recordings are not overwritten.	[Setting method] Select a value from the drop-down list box.
Stream Name	Specifies the stream used for recording.	[Setting method] Select a value from the drop-down list box.

Step 3 Configure the **Schedule** (deployment time). Refer to section 7.1 Step 4.
Step 4 Click **Apply**.

If the message "Apply success!" appears, settings are saved successfully.

If other information is displayed, set the parameters correctly.

8.2 Record Directory

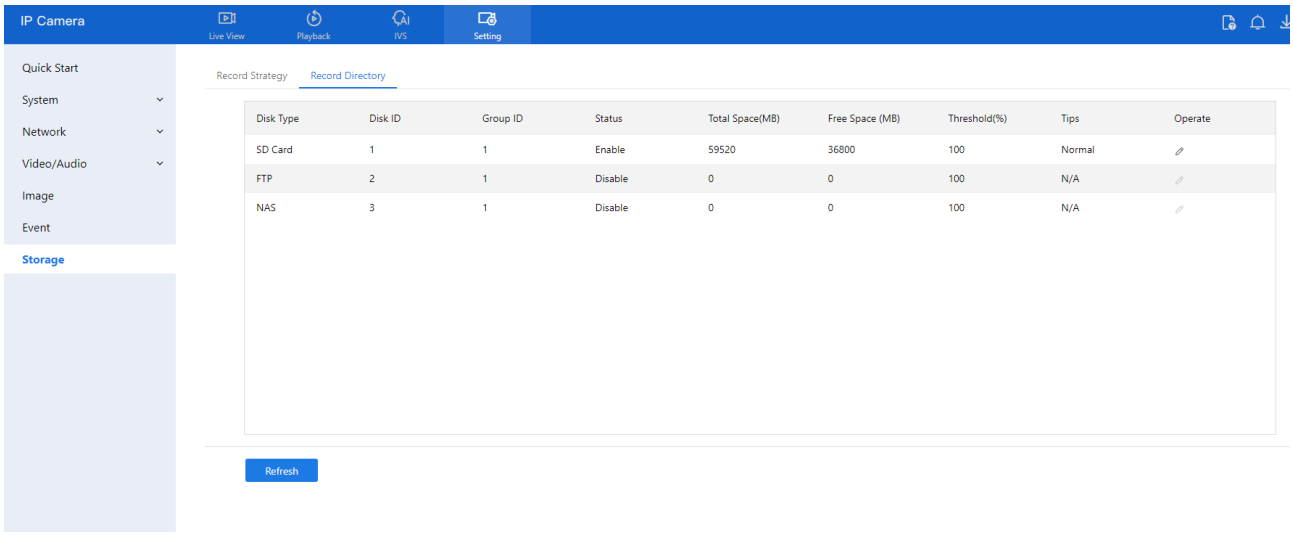
Description

Recordings can be saved to an **SD Card**, **FTP**, or **NAS** (Network Attached Storage), depending on your device model.

Procedure

Step 1 Go to **Setting > Storage > Record Directory**.
The **Record Directory** page will appear, as shown in Figure 8-2.

Figure 8-2 Record directory page



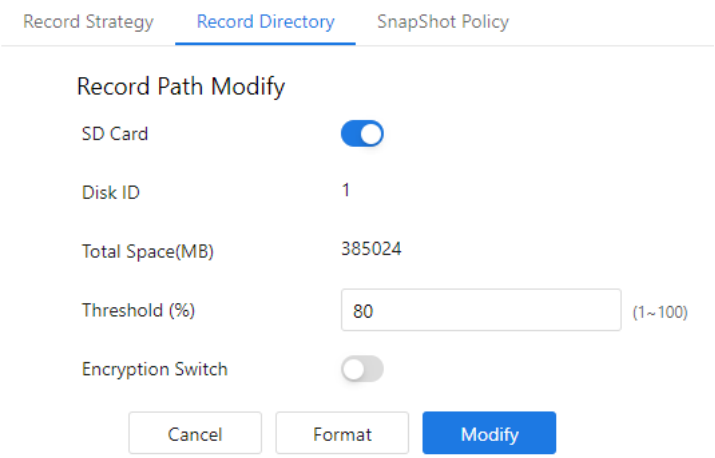
Step 2 Set the parameters according to Table 8-2.

Table 8-2 Parameters of Record directory

Parameter	**Description**	**Setting**
Disk Type	Recording device type (e.g., SD card, FTP, NAS).	[Setting method] The parameter cannot be set manually.
Disk ID	Identification number of the disk.	
Group ID	Group assignment ID.	
Enable	Enables selected storage.	
Total Space (MB)	Total capacity of the storage device.	
Free Space (MB)	Remaining usable space.	
Alarm Threshold (%)	Triggers an alarm when the used space exceeds this threshold.	
Status	Shows the connection status of the storage device.	

Step 3 Click **Modify** to update directory parameters.
(See Figure 8-3).

Figure 8-3 Record path modify



8.2.2 **Configure the SD Card**

Procedure

Step 1 Go to **Setting > Storage > Record Directory**
Step 2 Select the SD Card, then click the edit icon.
Step 3 Set parameters as per Table 8-3.

Table 8-3 Parameters of SD card recording

Parameter	Description	Setting
SD Card	Enables SD card recording.	[Setting method] Click the button to enable the SD card.
Disk ID	Identifier of the SD card.	N/A
Total Space(MB)	Total disk capacity.	[Setting method] The parameter cannot be set manually.
Alarm Threshold (1-100)	Set alert threshold for used space (1~100).	[Setting method] Enter a value from 1-100.
Encryption switch	Enable input of the encryption key. It will protect the data on the SD card. Other people can't read the recorded videos.	[Setting method] Click the button to enable. [Default value] OFF

Step 4 Click **Apply**.
The message **"Apply success!"** confirms the settings are saved.

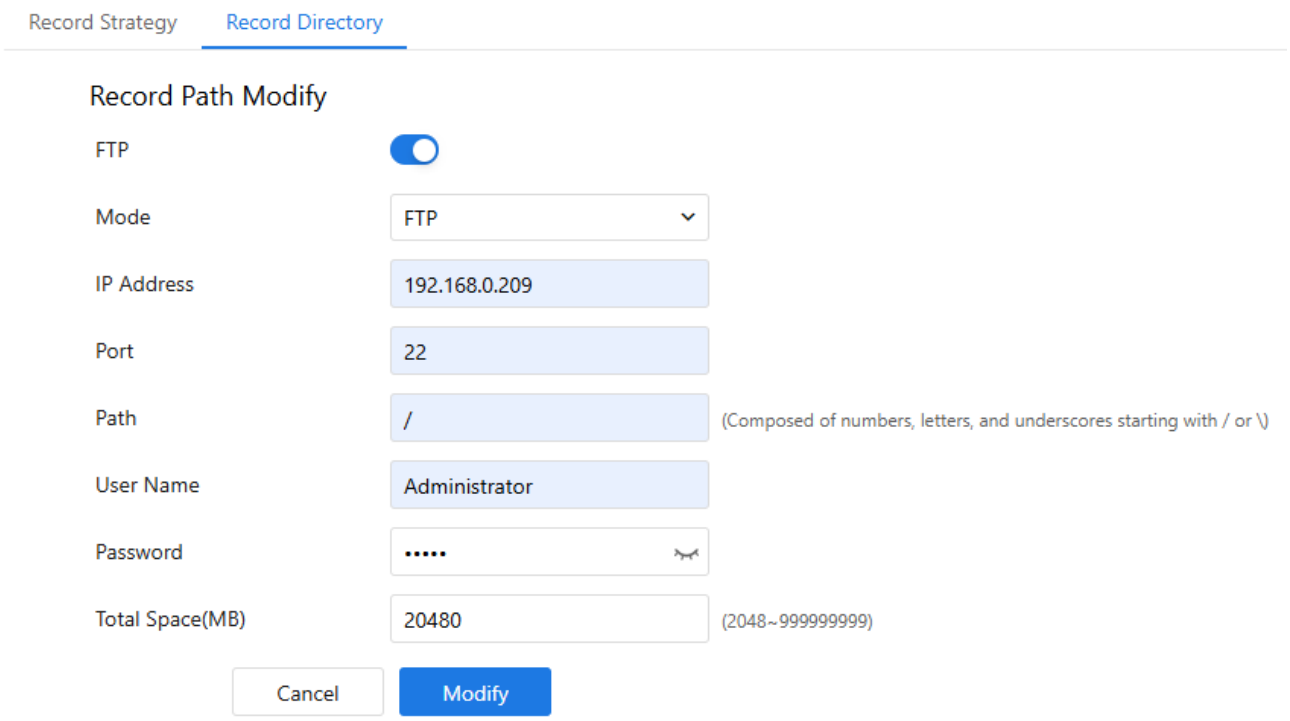
8.2.3 Configure the FTP

Procedure

Step 1 **Step 1:** Navigate to **Setting > Storage > Record Directory**.
Ensure the **SD card type is OFF**.

Step 2 **Step 2:** Choose **FTP** and click the **edit icon**.
The **FTP Record Path Modify** page appears (see Figure 8-4).

Figure 8-4 FTP record path modify page



Step 3 Set the parameters according to Table 8-4.

Table 8-4 Parameters of FTP recording

Parameter	Description	Setting
FTP	Enables recording to an FTP server.	[Setting method] Enable
IP Address	IP address of FTP server.	[Setting method] Enter a value manually.
Port	Communication port for FTP.	[Setting method] Enter a value manually.
Path	FTP Directory path to store recordings.	[Setting method] Enter a value manually.
User Name	FTP server account.	[Setting method] Enter a value manually.
Password	FTP server password.	[Setting method] Enter a value manually.

Parameter	Description	Setting
Confirm	Confirm the password.	[Setting method] Enter a value manually.
Free Space (MB)	Available space on FTP server.	[Setting method] Enter a value.
FTP over SSL / TLS (FTPS)	Available space on FTP server.	[Setting method] Tick

Step 4 Click **Apply**. A message stating **"Apply success!"** confirms your settings.

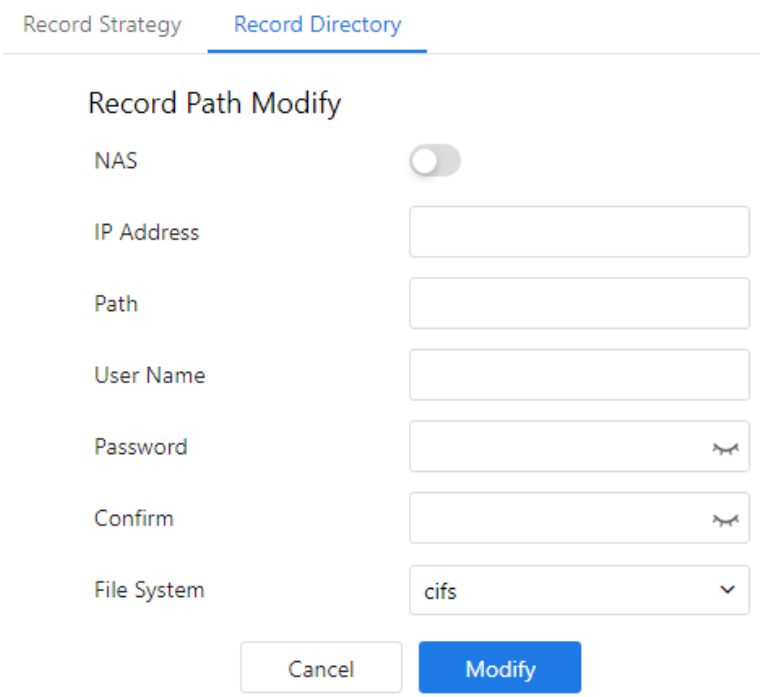
8.2.4 Configure the NAS

Procedure

Step 1 Navigate to **Setting > Storage > Record Directory**.
Ensure the **SD card type is OFF**.

Step 2 Choose **NAS** and click the **edit** icon.
The **NAS Record Path Modify** page is displayed (see Figure 8-5).

Figure 8-5 NAS record path modify page



Step 3 Set the parameters according to Table 8-5.

Table 8-5 Parameters of NAS recording

Parameter	Description	Setting
NAS	Enables video storage on NAS.	[Setting method] Enable

Parameter	Description	Setting
IP Address	IP address of the NAS server.	[Setting method] Enter a value manually.
Path	IP address of the NAS device.	[Setting method] Enter a value manually.
User Name	NAS device account.	[Setting method] Enter a value manually.
Password	NAS device Password.	[Setting method] Enter a value manually.
Confirm	Confirm the password.	[Setting method] Enter a value manually.
File System	Choose between CIFS and NFS protocols.	[Setting method] Choose from the drop-down list. [Default value] **cifs**

Step 4 Click **Apply**. The message **"Apply success!"** confirms the settings have been stored.

8.3 Snapshot Policy

Description

For scheduled snapshots, you should enable the snapshot policy at this interface. The 1/5 size of the SD card will be deployed for snapshotting; This section is up to save 20000 images. Some models only support 1000 images. Please refer to actual products.

Procedure

Step 1 Go to **Setting > Storage > Snapshot Policy**.

The **Snapshot Policy** page will appear, as shown in Figure 8-6.

Figure 8-6 Snapshot policy page

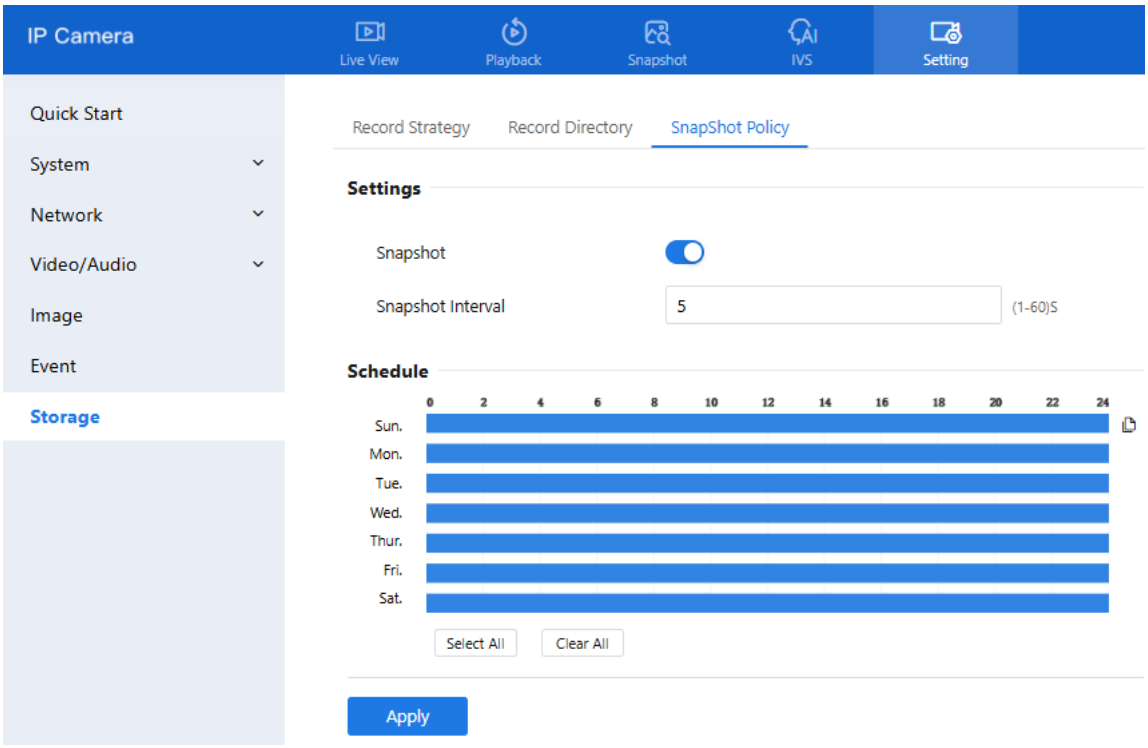
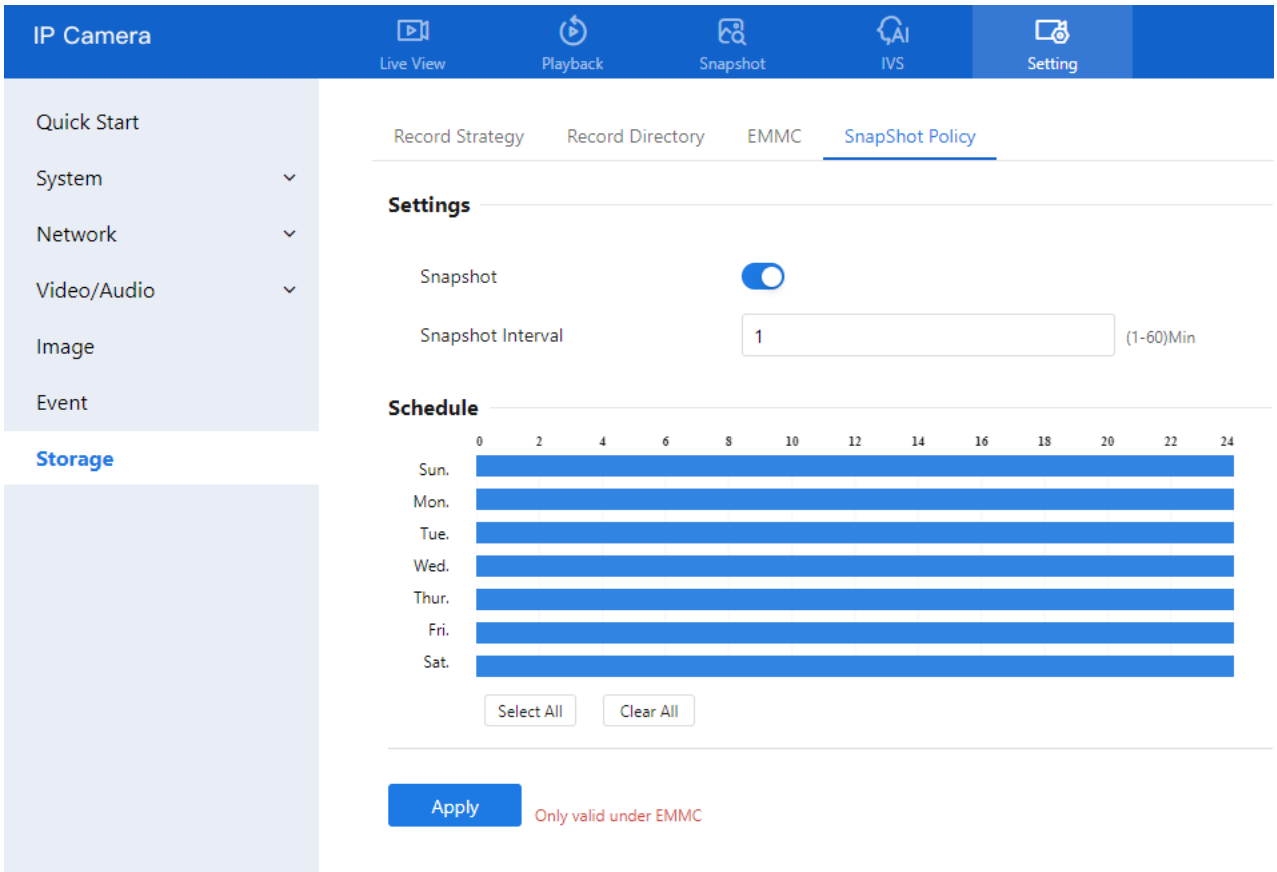


Figure 8-7 Snapshot policy page (EMMC)



Step 2 Enable snapshot. Set the interval; the camera will snapshot a panoramic image at this interval.

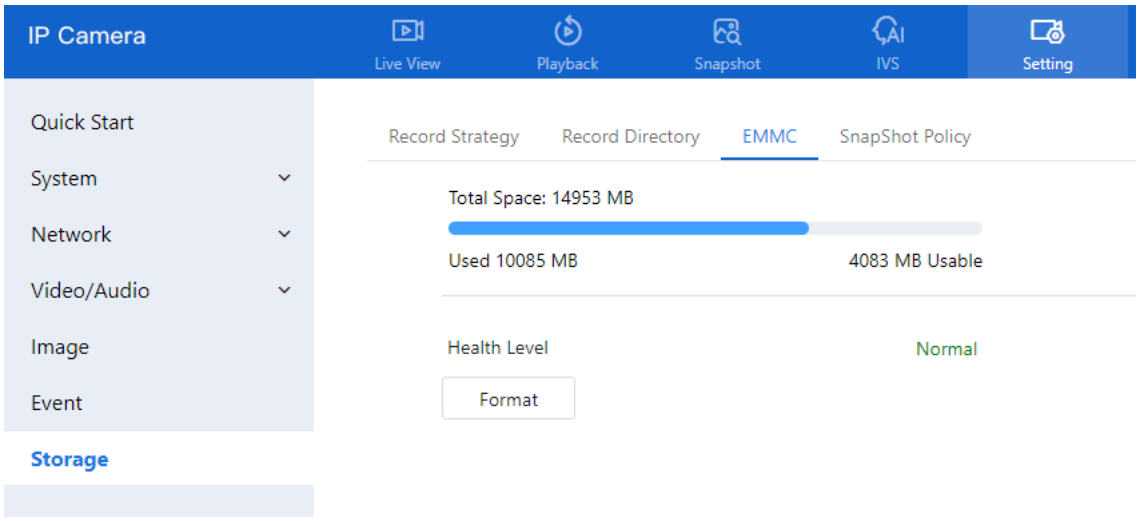
Step 3 Set the schedule; only during the armed time, the camera will snap a snapshot for the schedule.

Step 4 Click **Apply**. The message **"Apply success!"** confirms the settings have been stored.

8.4 EMMC

This feature is supported on specific models.
It displays the usage status of the EMMC. Formatting will erase all captured images; proceed with caution.

Figure 8-8 EMMC



9.4 Configure Intelligent Analysis

9.4.1 Intrusion

Description

Generates an alarm when a target (person or vehicle) enters a defined detection area.

- Factory walls, research institute perimeters, school grounds, and large community enclosures. During non-working hours, these systems trigger alarms for attempts to scale or damage the walls.
- Open-air warehouses, storage yards, parking lots, and construction sites. Prevents theft or damage to materials.
- Establishes virtual security zones in areas where physical barriers are impractical (e.g., open plazas, riverbanks). Triggers alarms upon intrusion by individuals or vehicles.
- Entrances to finance offices, archives, server rooms, laboratories, and vaults. Detect any entry after hours or during unmanned periods.
- Sensitive access points: fire exits, rooftop entrances, and passages from underground parking to buildings. Prevent security risks during non-emergency access.
- Unattended Zones: Data center corridors, museum galleries at night, bank ATM rooms. Any movement triggers an alarm.
- Intrusion detection alarms can be installed in restricted areas, high-risk zones, and designated areas where unauthorized presence is prohibited.

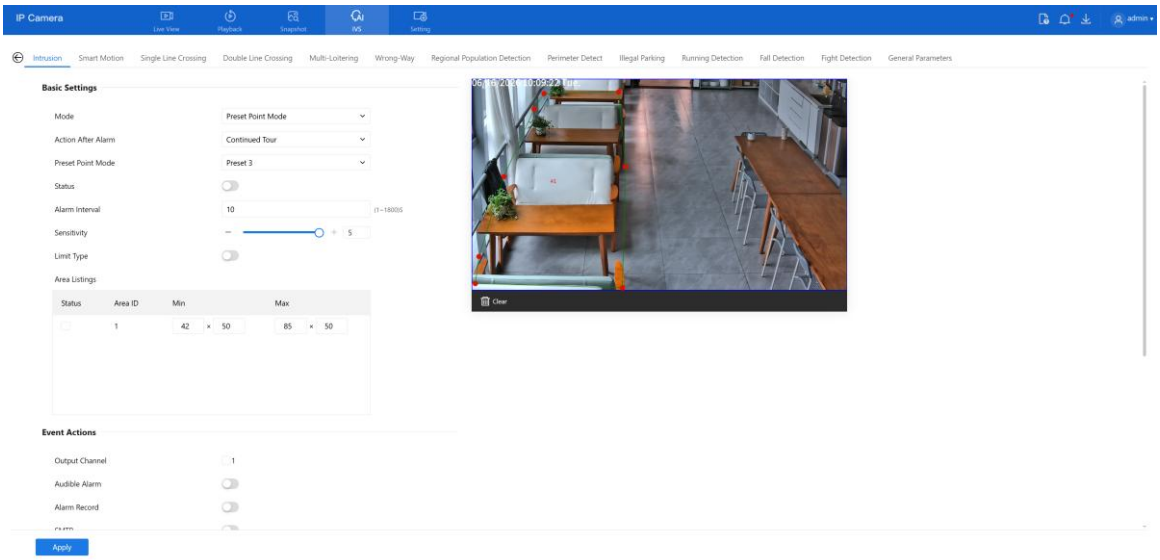
Procedure

Step 1 Go to **IVS > Intelligent Analysis > Intrusion**.

The **Intrusion Settings** page appears (see Figure 9-2).

Step 2 Set the intrusion parameters as listed below.

Figure 9-1 Intrusion settings page

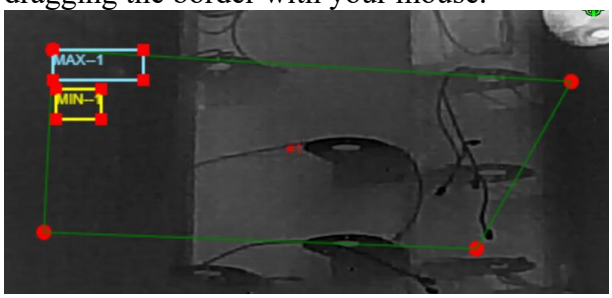


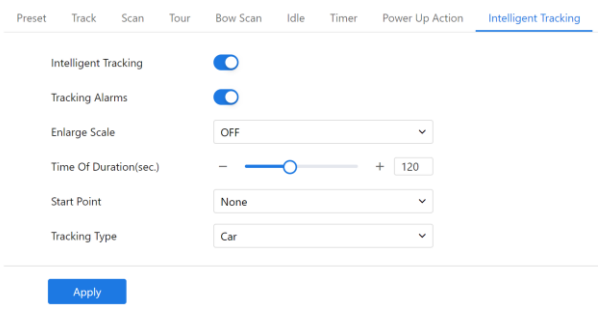
Step 3 Set all parameters of intrusion. Table 9-1 describes the specific parameters.

Table 9-1 Intrusion parameter description

Parameter	Description	Setting
Mode	Normal mode and preset mode. Preset mode: choose one preset to set parameters on it. It applies to PTZ cameras.	[How to set] Choose from the drop-down list [Default value] **Normal mode**
Status	Enables the intrusion alarm.	[How to set] Click the button on. [Default value] **OFF**

Parameter	Description	Setting
Preset point mode	You can choose between Normal Mode and Preset Mode. Preset Mode: Pre-set positions in advance, select the corresponding preset point for configuration, and choose post-alarm actions (continued tour or pause tour).  Tour refers to the camera itself performing a tour action. During the tour, if an alarm is triggered at a preset point, the camera will continue the tour after the alarm action concludes. If the camera is not performing a tour action, the post-alarm action settings are ineffective.	[How to set] Choose from the drop-down list [Default value] **Preset 1**
Video Stream Draw Line	Enable video stream draw line. Detection area drawing frames will appear in the live video. It applied to some models. 	
Alarm Interval	Time interval (in seconds) during which identical alarms will not be repeated (1–1800s).	[How to set] Input a value, 1~1800s

Parameter	Description	Setting
Sensitivity	Sensitivity of target detection: Higher sensitivity makes targets easier to detect, but accuracy decreases. High security, low false alarm tolerance: Open areas, virtual perimeters: select low sensitivity (1, 2) Theft prevention requires immediate response: Residential perimeter, factory/warehouse exteriors, commercial complexes, construction sites: select medium-high sensitivity (3) Indoor critical area protection: Select medium-high sensitivity (3, 4, 5)	[How to set] Choose from the drop-down list [Default value] **5**
Limit Type	Choose detection target: Person/Vehicle/ Person or Vehicle.	[How to set] Click the button on. [Default value] **OFF**
Area Listings	The set area will now appear in the list. Set the minimum and maximum pixel thresholds for triggering an alarm. Checking the "Enable" option displays the maximum and minimum regions within the area for easy comparison. MAX indicates the largest detectable target size, while MIN represents the smallest size. Targets exceeding the detection range will be filtered and will not trigger an alarm. You can manually adjust the size by dragging the red points and move the position by dragging the border with your mouse. 	[How to set] Set the detection area.
Output Channel	If you check to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals when an alarm is triggered. Only for Some Models. (Set at the "**Setting > Event > Alarm Output**", the details please refer to ***Chapter 7.3***)	[How to set] Click to select an ID.

Parameter	Description	Setting
Audible Alarm	After enabling Audible Warning and setting Audible Alarm Output, the built-in speaker of the device or the connected external speaker plays warning sounds when an alarm happens. (“**Setting > Video / Audio > Audio File**”, for the detailed information, please refer to Chap***ter 5.2.2***).	[How to set] Click to enable Audible alarm [Default value] **OFF**
Alarm Record	The alarm recording is stored on the SD card.	[How to set] Click to enable alarm record. [Default value] **OFF**
SMTP	Enable the button to enable the SMTP server.	[How to set] Click to enable SMTP. [Default value] **OFF**
FTP Upload	Enable the button to enable File Transfer Protocol. **Configuration > Network Service > Advanced Settings > FTP**). The detailed, please refer to ***Chapter 4.2.1***	[How to set] Click to enable FTP Upload. [Default value] **OFF**
Linkage Tracking	Enable, when an alarm target is detected, the lens tracks the target's movement. The linked tracking action is executed via the “Setting > PTZ > Intelligent Tracking” parameters. During linkage tracking, the current alarm remains active continuously, preventing other alarms from triggering during this period. Whether Intelligent Tracking is enabled does not affect the linked tracking action. 	[How to set] Click to enable Linkage Tracking. [Default value] **OFF**

Parameter	Description	Setting
Snapshot	When enabled and the alarm is triggered, the camera snaps an image to the SD card.	[How to set] Click to enable Snapshot. [Default value] **OFF**
Flashlight Alarm	After enabling Flashing Light and setting the Flashing Light Alarm Output, the light flashes when an alarm event is detected.	[How to set] Click the button on. [Default value] **OFF**
White light Alarm	When the **Day/Night** mode is chosen the **Night** mode, and the light is **IR LED** or **NON**E mode, this linkage action is valid. Enable the white light alarm when it triggers the alarm, and the white light will be on. Only for Some Models.	[How to set] Click the button on. [Default value] **OFF**
Red and Blue Light Alarm	The camera should have red and blue lights. When an alarm occurs, the device will flicker alternating red and blue lights.	[Setting method] Enable Red and Blue Light Alarm [Default value] **OFF**

Step 4 Set a deployment area.

To configure the detection area:

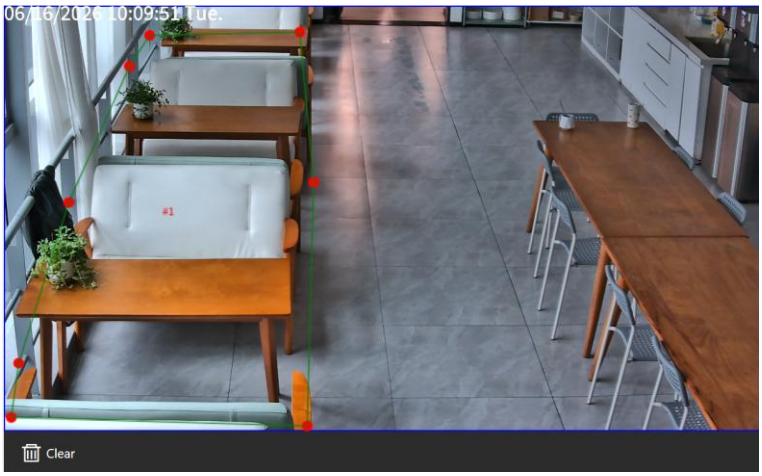
Step 1 **Move the cursor** to the drawing interface.
Step 2 **Click to create a point**—this marks the starting vertex of the area.
Step 3 **Move the cursor and click again** to create the next point, forming a line segment.
Step 4 **Repeat** this process to form a polygon that outlines the detection area.
Step 5 Once your shape is complete, **right-click** to finish the drawing.

Note:

- Lines cannot intersect each other.
- Each shape can have **up to 8 sides**.
- You can draw **up to 8 separate detection areas**.

See **Figure 9-3** for a visual reference of the drawing interface.

Figure 9-2 Deployment area setting page



9.4.2 **Smart Motion**

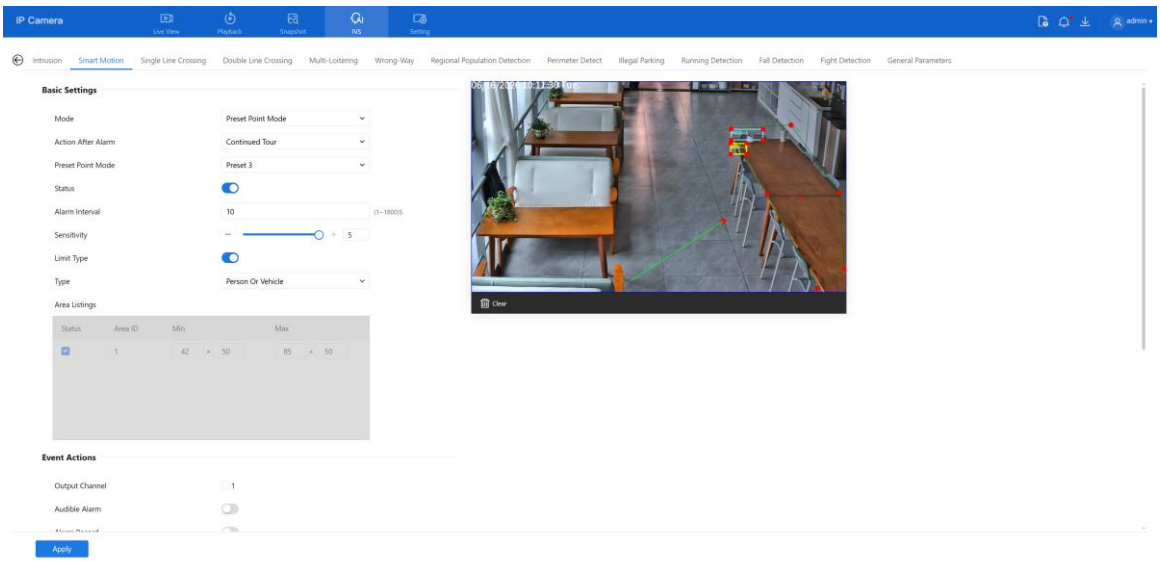
Description

Smart motion detection generates an alarm when specified target objects—such as people, vehicles, or both—move within a predefined area.

Procedure

Step 1 Go to **IVS > Intelligent Analysis** > **Smart Motion.** The **Smart Motion settings** page appears as shown in Figure 9-3.

Figure 9-3 Smart motion settings page



Step 2 Configure all parameters. Refer to section 9.4.1 Step 3 for details

Step 3 Define the **detection area**:

- Move the cursor to the live view.
- Click to place the first point.
- Continue clicking to form a polygonal area.

- **Right-click** to finish drawing.

NOTE

- Lines **must not intersect**.
- You can draw a shape with up to **8 sides**.
- You can define up to **8 deployment areas**.

Step 4 Set the deployment time. Refer to 7.1 Step 4.

Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.3 Single Line Crossing

Description

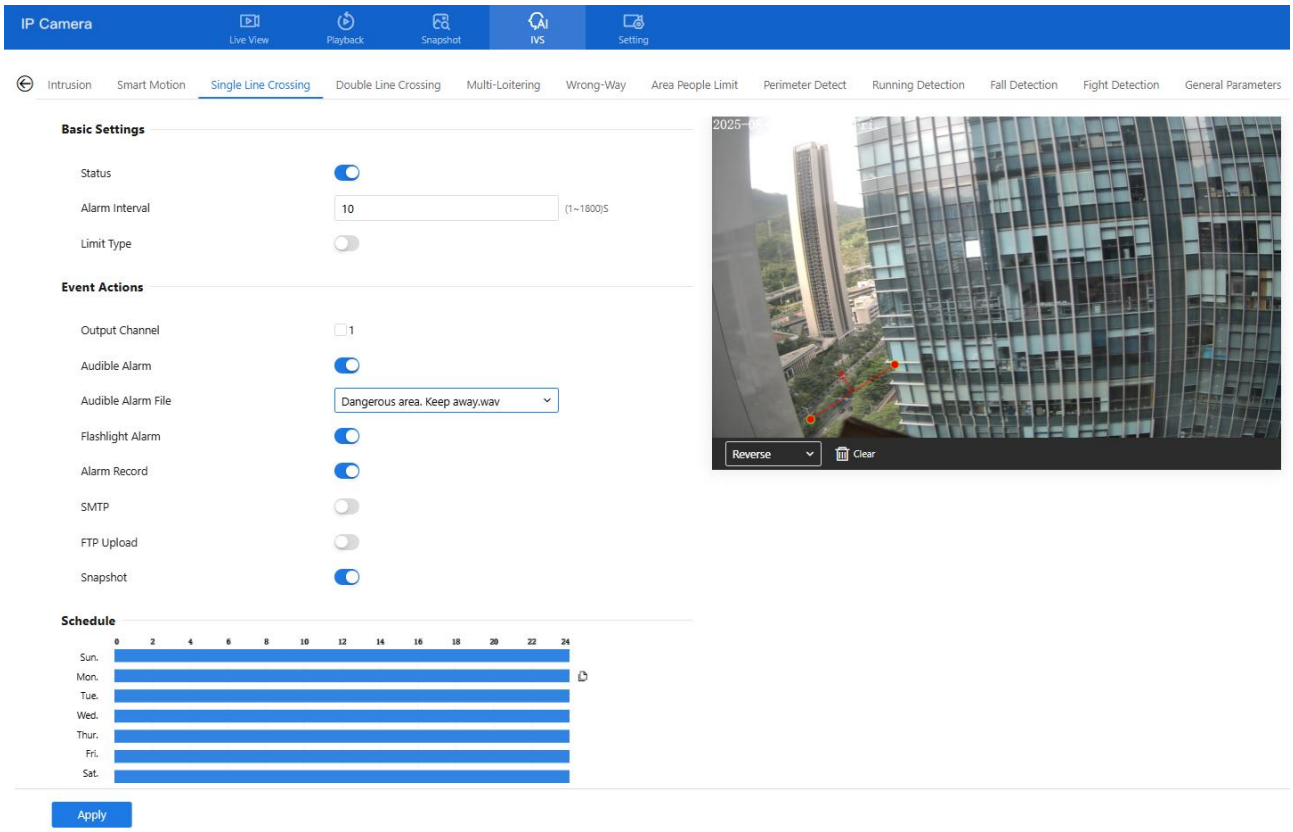
Single line crossing detection monitors a virtual line placed in the camera's field of view. An alarm is triggered when a target (such as a person or vehicle) crosses the line in a specified direction.

Procedure

Step 1 Go to **IVS > Intelligent Analysis > Single Line Crossing**.

The **Single Line Crossing** settings page appears, as shown in Figure 9-4.

Figure 9-4 Single line crossing setting interface



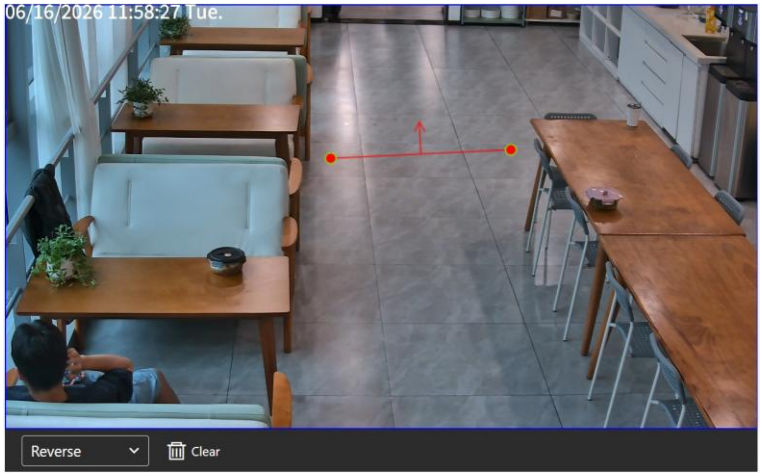
Step 2 Set all parameters of the single line crossing, please refer to 9.4.1 Step 3.

Step 3 Draw and configure the crossing line:

- Hold down the **left mouse button** and draw a straight line.
- Release the button to create the single line crossing.

- **Click** the line to select it (it turns red when selected).
- Set the direction: **Positive**, **Reverse**, or **Bidirectional**.
- To reposition the line, drag from either endpoint.
- **Right-click** to delete the line, as shown in Figure 9-5.

Figure 9-5 Deployment area setting page



NOTE

- Draw the line toward the center of the screen for better recognition timing.
- Ensure the line is long enough; short lines may miss detection, especially for targets recognized by foot position.

Step 4 Set the deployment time. Refer to section 7.1 Step 4.

Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.4 Double Line Crossing

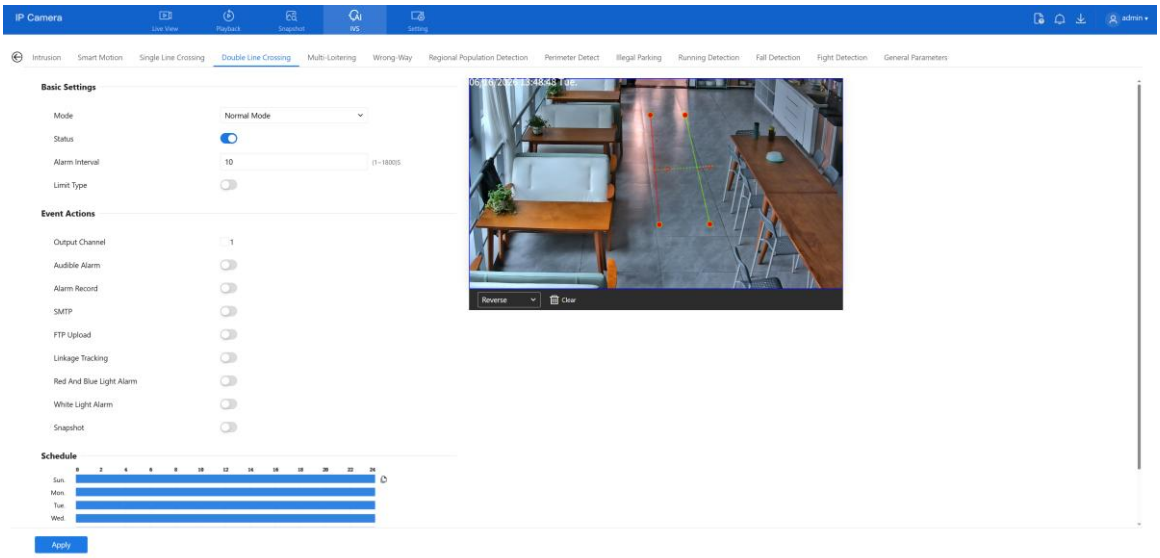
Description

Double line crossing defines two virtual lines in the monitored area. An alarm is triggered when a target (such as a person or vehicle) crosses both lines in a specific direction and order—first Line 1, then Line 2—within a predefined time frame.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Double Line Crossing** to access the **Double Line Crossing** setting interface, as shown in Figure 9-6.

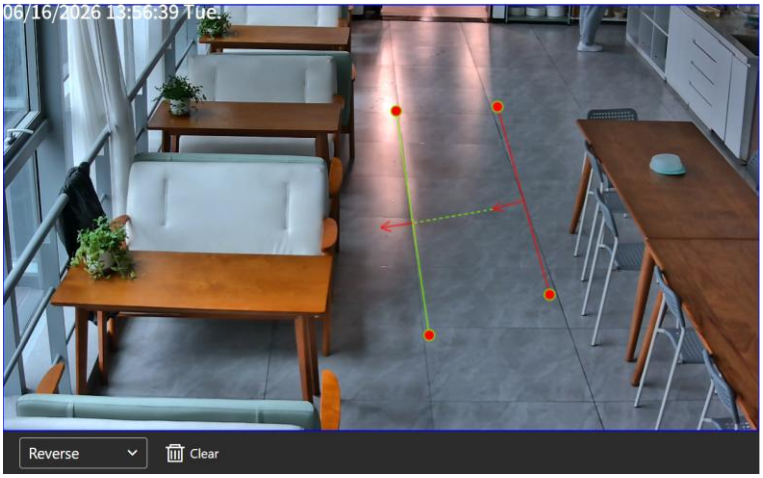
Figure 9-6 Double line crossing settings interface



Step 2 Set all parameters of the double line crossing, please refer to 9.4.1 Step 3.
Define the deployment area.

- **Drawing lines**: Hold down the **left mouse button** and draw two lines in sequence. Release to generate two virtual fences labeled "1" and "2."
- **Setting direction**: Click on either fence (it will turn red when selected). Choose **Positive** or **Reverse** direction from the drop-down.
- **Editing lines**: Drag the endpoints to adjust the size or position. Right-click to delete a line, as shown in Figure 9-7.

Figure 9-7 Deployment area settings page



NOTE

- The system recognizes a valid crossing only if **Virtual Fence 1** is crossed **before Virtual Fence 2**.
- Draw the fences toward the **center** of the screen to ensure the target is fully recognized before crossing.
- The fence **length must be sufficient** for reliable foot-based detection.
- Direction cannot be manually adjusted other than by selecting **Reverse**.

Step 3 Set the deployment time. Refer to Section 7.1 Step 4.

Step 4 Click **Apply**. A message saying "Apply success!" confirms that the settings have been saved.

9.4.5 Multi-Loitering

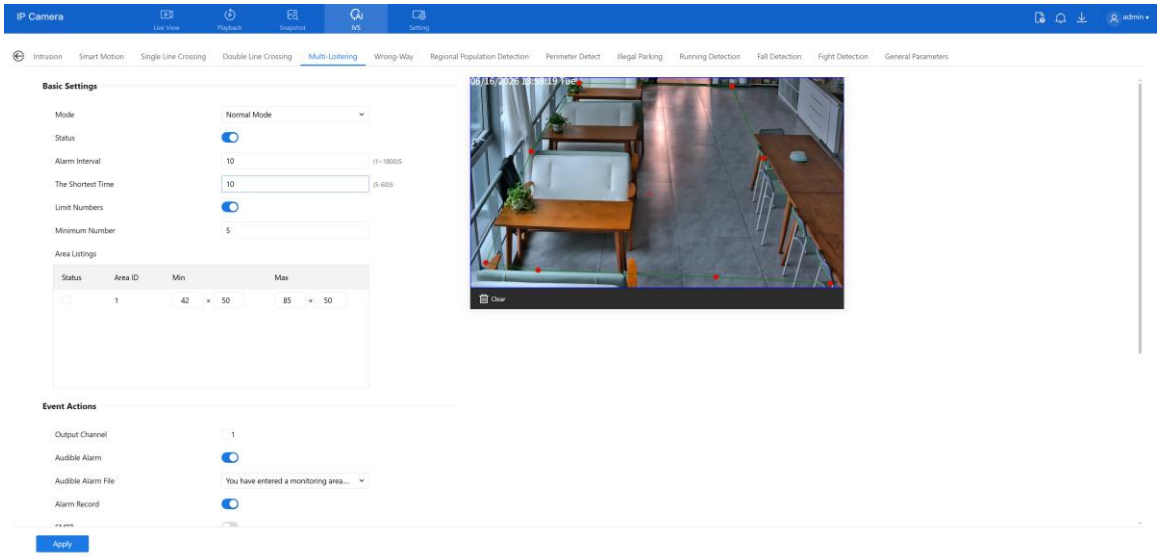
Description

Multi-loitering detection triggers an alarm when multiple targets (e.g., persons or vehicles) remain in a defined area longer than a specified minimum loitering time.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Multi-Loitering** to access the **Multi-Loitering** setting interface, as shown in Figure 9-8.

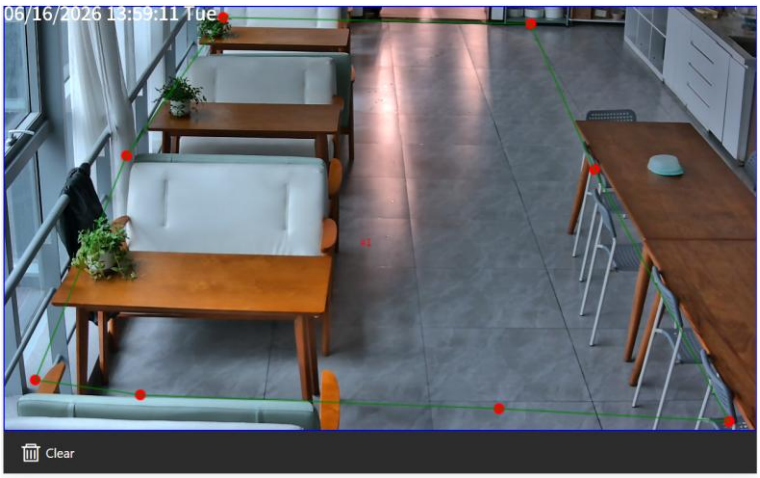
Figure 9-8 Multi-Loitering setting page



Step 2 Set all parameters of multi-loitering, please refer to 9.4.1 Step 3.
Step 3 Set a deployment area:

- Move the cursor and **click** to define points.
- Click again to add vertices and create a polygon.
- **Right-click** to complete the shape, as shown in Figure 9-9.

Figure 9-9 Deployment area settings page



NOTE

- A line cannot cross another line.
- You may define up to 8-sided shapes.
- A maximum of 8 deployment areas is supported.

Step 4 Set the deployment time. Refer to section 7.1 Step 4.
Step 5 Click **Apply**. The system will save the configuration and display "Apply success!

9.4.6 **Wrong-Way**

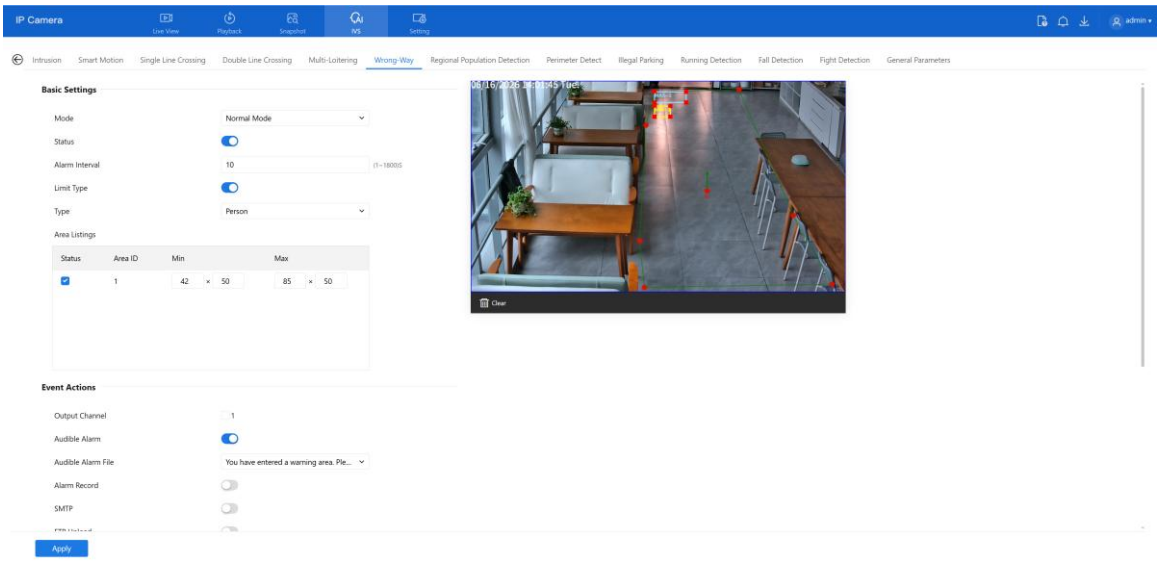
Description

Wrong-Way monitors directional movement within a designated area. An alarm is triggered when a target (such as a person or vehicle) moves in the opposite direction of the configured travel path.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Wrong-Way** to access the Wrong-Way settings interface, as shown in Figure 9-10.

Figure 9-10 Wrong-Way settings page



Step 2 Set all parameters of Wrong-Way, please refer to 9.4.1 Step 3.
Step 3 Define the deployment area.

- Move the cursor on the video interface and click to create a point.
- Continue clicking to form lines and enclose a custom shape.
- Right-click to finish the area drawing.
- Use the **arrow tool** within the field to define the reverse direction of travel, as shown in Figure 9-11.

Figure 9-11 Deployment area setting interface



NOTE

- Lines **must not intersect**, or the drawing will fail.
- A **maximum of 8 sides per shape** and **up to 8 zones** are supported.

Step 4 Set deployment time, please refer to 7.1 Step 4.
Step 5 Click **Apply**. The system will save your settings and display the message **"Apply success!".**

9.4.7 Regional Population Detection

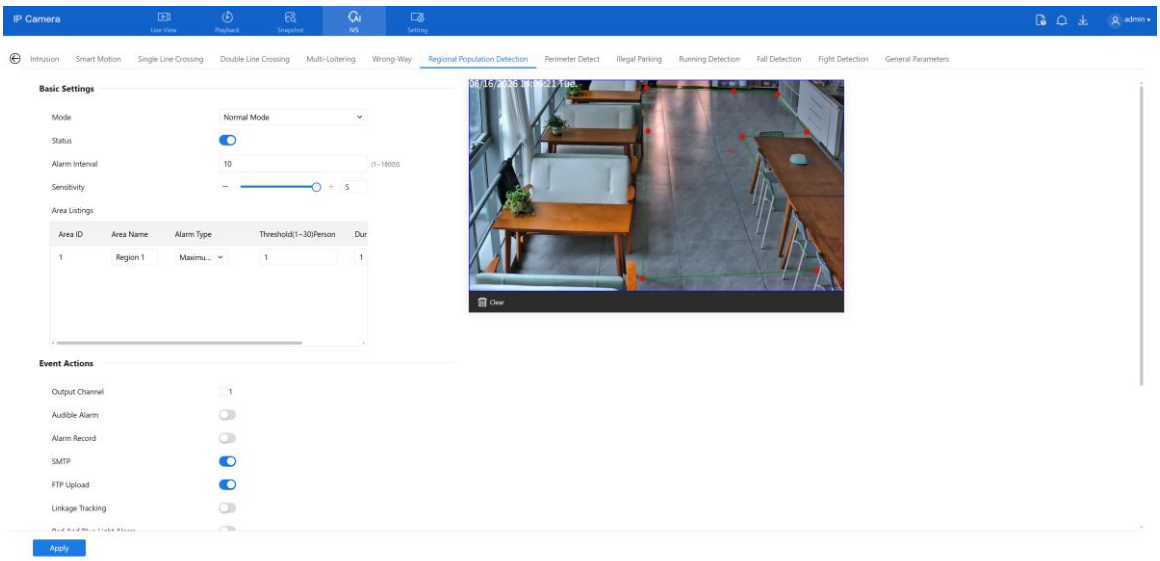
Description

Regional population detection means the number of people is over the set maximum number or is less than the set minimum number in deployed areas. It will trigger the alarm.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Regional Population Detection** to access the Regional Population Detection settings interface, as shown in Figure 9-10.

Figure 9-12 Area People Limit settings page



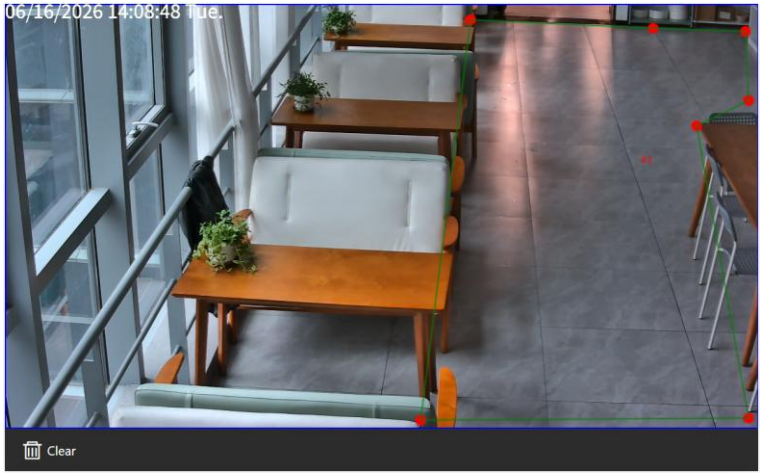
Step 2 Set all parameters of Regional Population Detection. Please refer to 9.4.1 Step 3.
Step 3 Set the Area list parameters.

- Set the Area Name.
- Choose the Alarm Type, Maximum Number, or Minimum Number.
- Set the Threshold Person; it ranges from 1 to 30.
- Persons stay in the area for more than the set duration.

Step 4 Define the deployment area.

- Move the cursor on the video interface and click to create a point.
- Continue clicking to form lines and enclose a custom shape.
- Right-click to finish the area drawing.

Figure 9-13 Deployment area setting interface



NOTE

- Lines **must not intersect**, or the drawing will fail.
- A **maximum of 8 sides per shape** and **up to 8 zones** are supported.

Step 5 Set deployment time, please refer to 7.1 Step 4.

Step 6 Click **Apply**. The system will save your settings and display the message **"Apply success!".**

9.4.8 Perimeter Detection

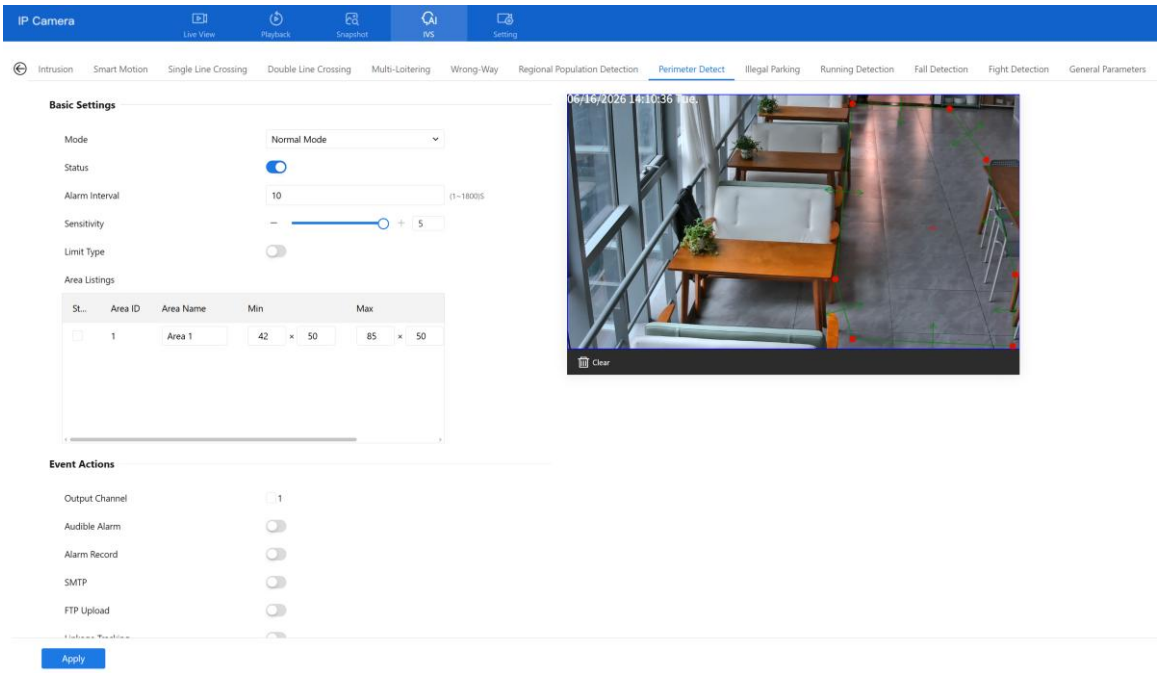
Description

When targets (person or vehicle) are across the perimeter of the set detection area during the scheduled period, the alarm will be triggered.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Perimeter Detection** to access the Perimeter Detection settings interface, as shown in Figure 9-14.

Figure 9-14 Perimeter detection settings page

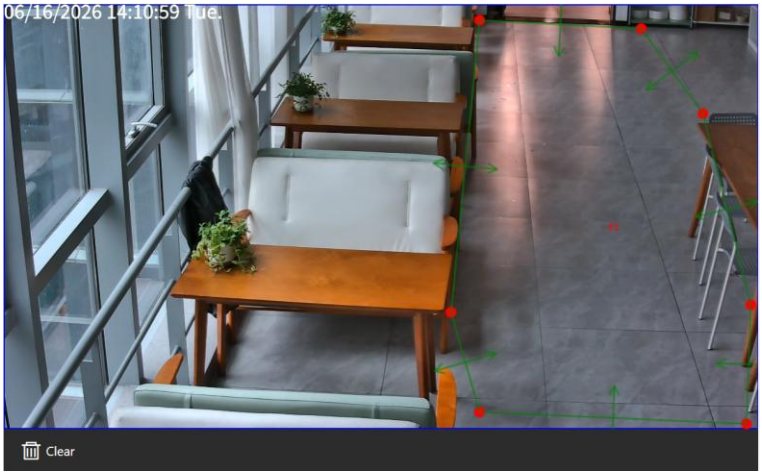


Step 2 Set all parameters of Perimeter Detection, please refer to 9.4.1 Step 3.

Step 3 Define the **detection area**:

- Move the cursor to the live view.
- Click to place the first point.
- Continue clicking to form a polygonal area.
- **Right-click** to finish drawing.

Figure 9-15 Deployment area setting interface



NOTE

- Lines **must not intersect**.
- You can draw a shape with up to **8 sides**.
- You can define up to **8 deployment areas**.

Step 4 Set the deployment time. Refer to 7.1 Step 4.

Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.9 **Running Detection**

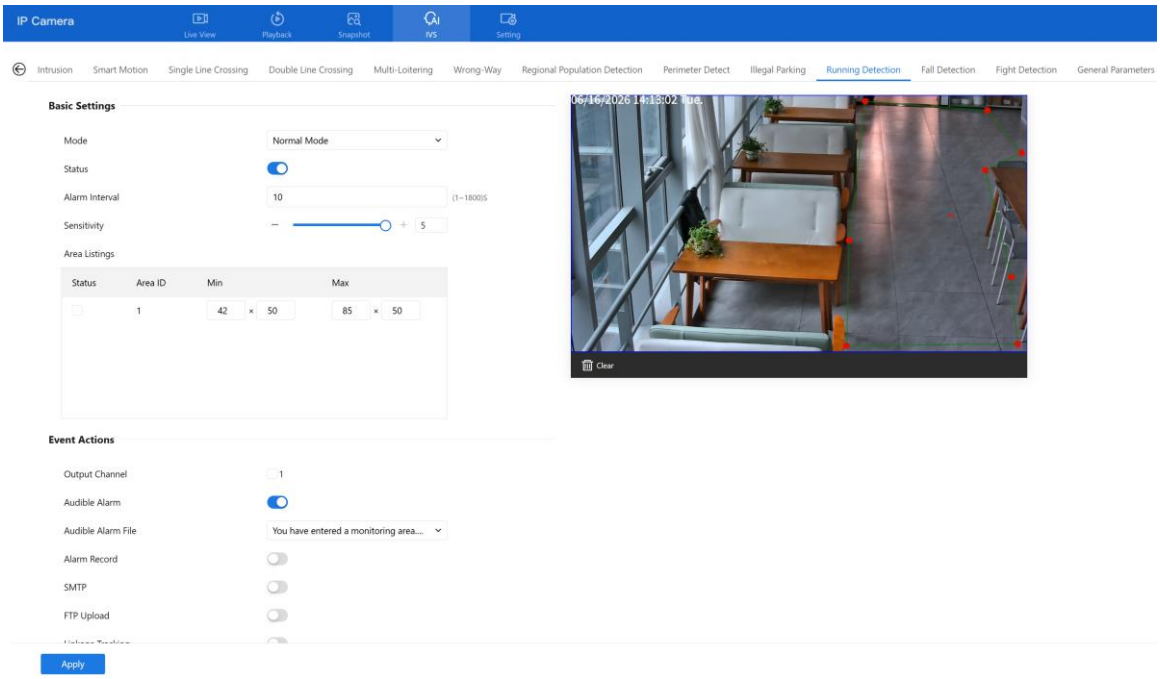
Description

When a person is running in the set detection area during the scheduled period, the alarm will be triggered.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Running Detection** to access the Running Detection settings interface, as shown in Figure 9-16.

Figure 9-16 Running detection settings page

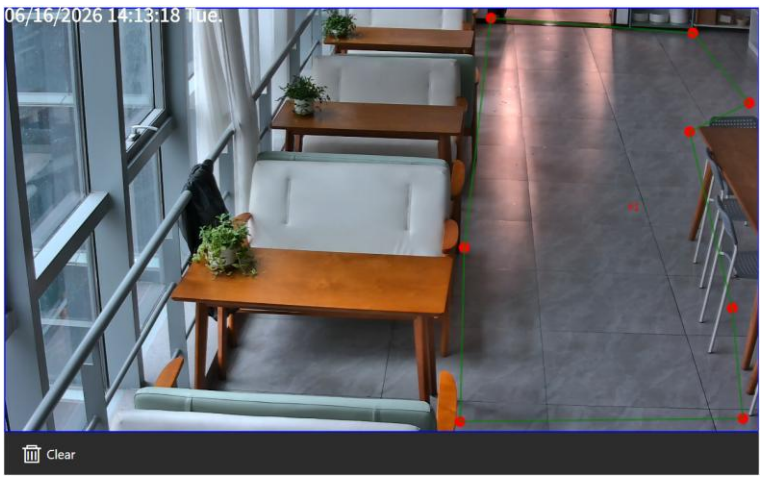


Step 2 Set all parameters of Running Detection, please refer to 9.4.1 Step 3.

Step 3 Define the **detection area**:

- Move the cursor to the live view.
- Click to place the first point.
- Continue clicking to form a polygonal area.
- **Right-click** to finish drawing.

Figure 9-17 Deployment area setting interface



NOTE

- Lines **must not intersect**.
- You can draw a shape with up to **8 sides**.
- You can define up to **8 deployment areas**.

Step 4 Set the deployment time. Refer to 7.1 Step 4.

Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.10 Fall Detection

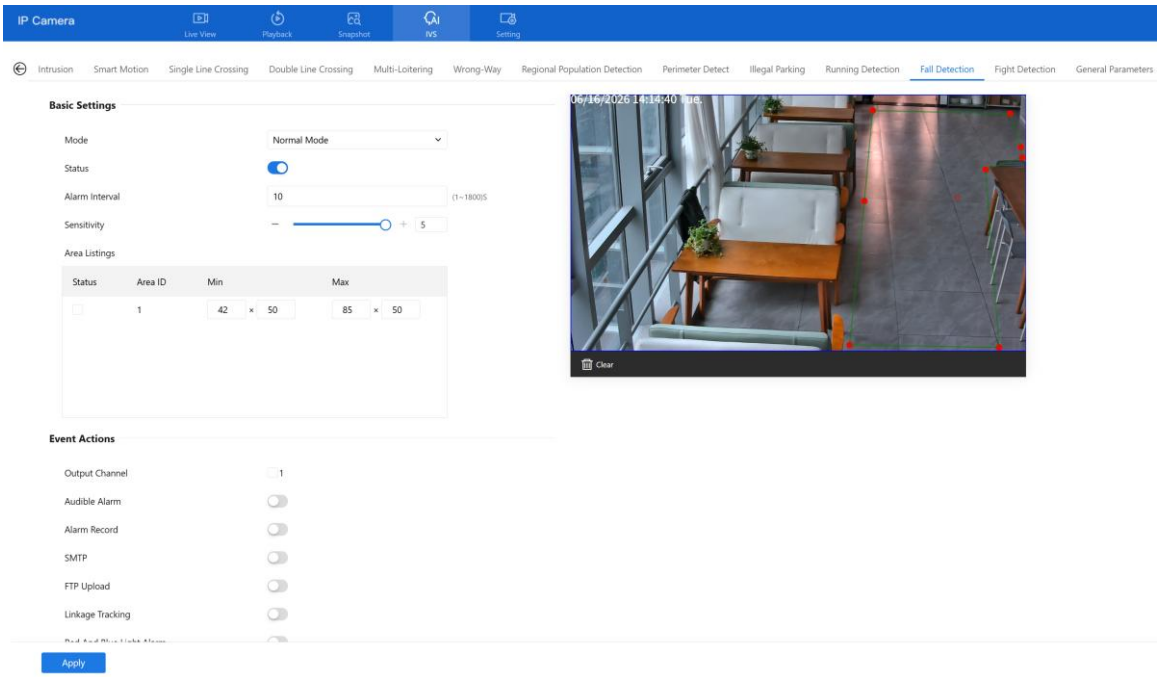
Description

When the person falls over the set detection area during the scheduled period, the alarm will be triggered.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Fall Detection** to access the Fall Detection settings interface, as shown in Figure 9-18.

Figure 9-18 Fall detection settings page

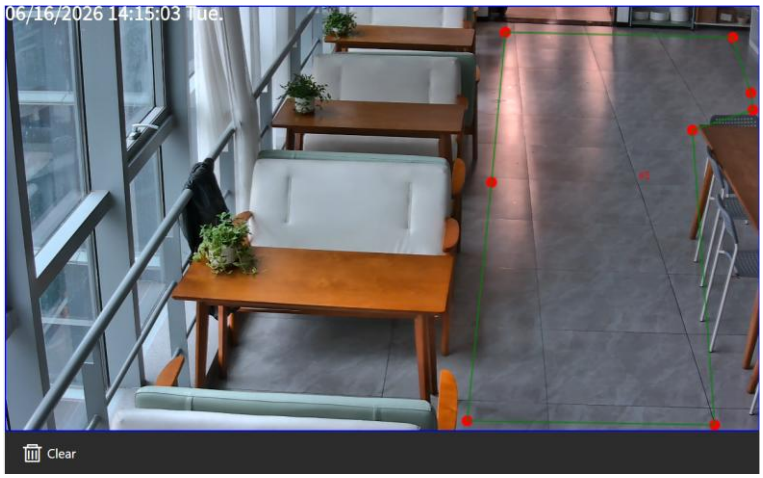


Step 2 Set all parameters of Fall Detection. Please refer to 9.4.1 Step 3.

Step 3 Define the **detection area**:

- Move the cursor to the live view.
- Click to place the first point.
- Continue clicking to form a polygonal area.
- **Right-click** to finish drawing.

Figure 9-19 Deployment area setting interface



NOTE

- Lines **must not intersect**.
- You can draw a shape with up to **8 sides**.
- You can define up to **8 deployment areas**.

Step 4 Set the deployment time. Refer to 7.1 Step 4.

Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.11 Fight Detection

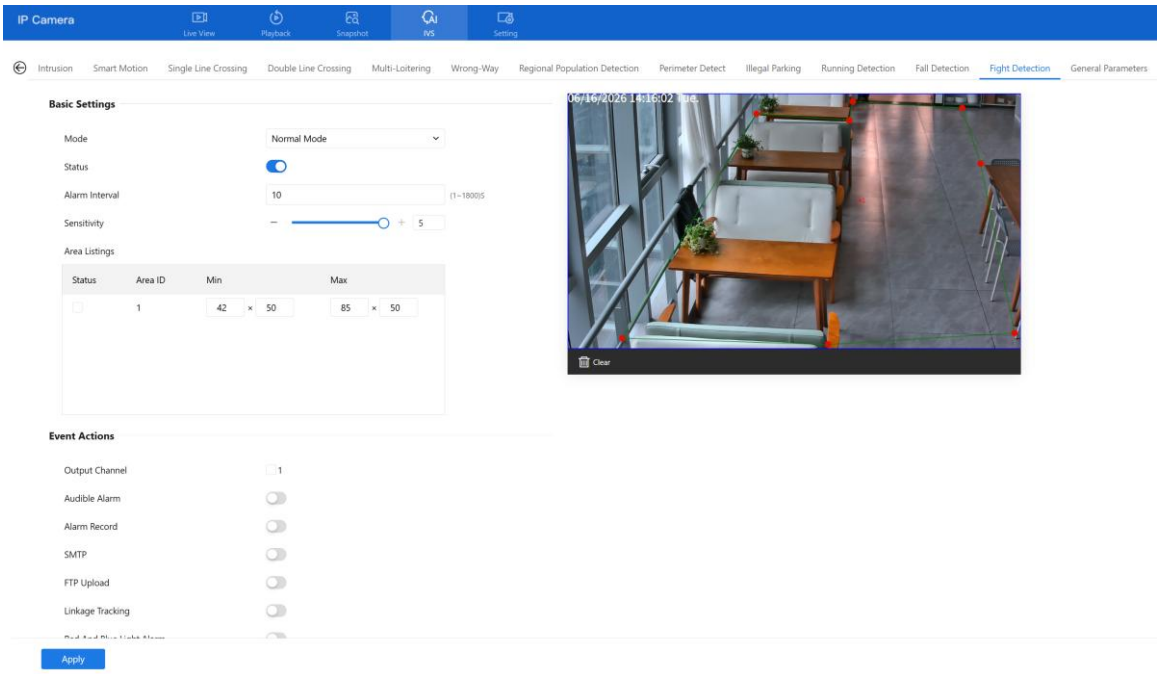
Description

When people fight in a set detection area during the scheduled period, the alarm will be triggered.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Fight Detection** to access the Fight Detection settings interface, as shown in Figure 9-20.

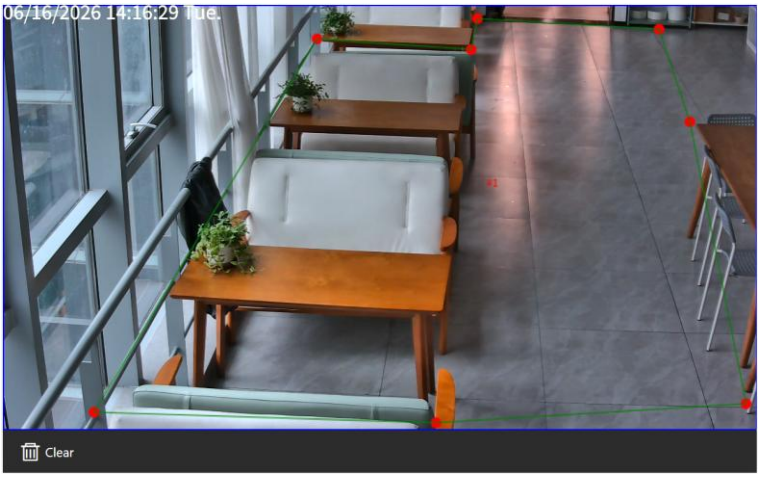
Figure 9-20 Fight detection settings page



Step 2 Set all parameters of Fight Detection, please refer to 9.4.1 Step 3.
Step 3 Define the **detection area**:

- Move the cursor to the live view.
- Click to place the first point.
- Continue clicking to form a polygonal area.
- **Right-click** to finish drawing.

Figure 9-21 Deployment area setting interface



NOTE

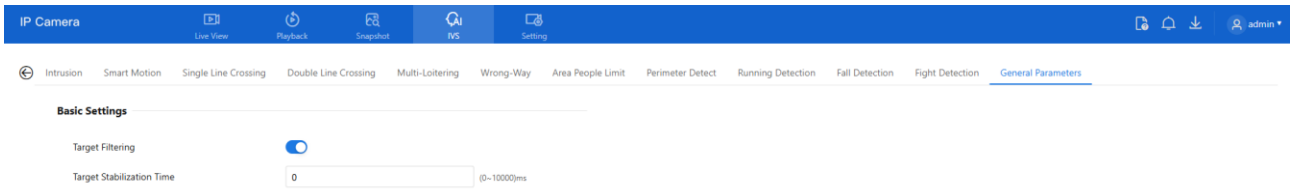
- Lines **must not intersect**.
- You can draw a shape with up to **8 sides**.
- You can define up to **8 deployment areas**.

Step 4 Set the deployment time. Refer to 7.1 Step 4.
Step 5 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.4.12 General Parameters

Set the target filtering parameters for all Intelligent Analysis functions (intrusion, smart motion, single line crossing, double line crossing, multi-loitering, wrong-way, area people limit, perimeter detection, running detection, fight detection, and so on). The alarm can only be triggered if the target appears in the set area for more than the filtering time. For example, if the target stabilization time value is 5000ms, the relevant intelligent analysis actions will only be detected after the target is within the area for 5 seconds.

Figure 9-22 General parameters



Step 1 Enable Target Filtering.
Step 2 Set the target stabilization time.
Step 3 Click **Apply**. A message "Apply success!" will confirm that the settings have been saved.

9.5 Configure People Counting

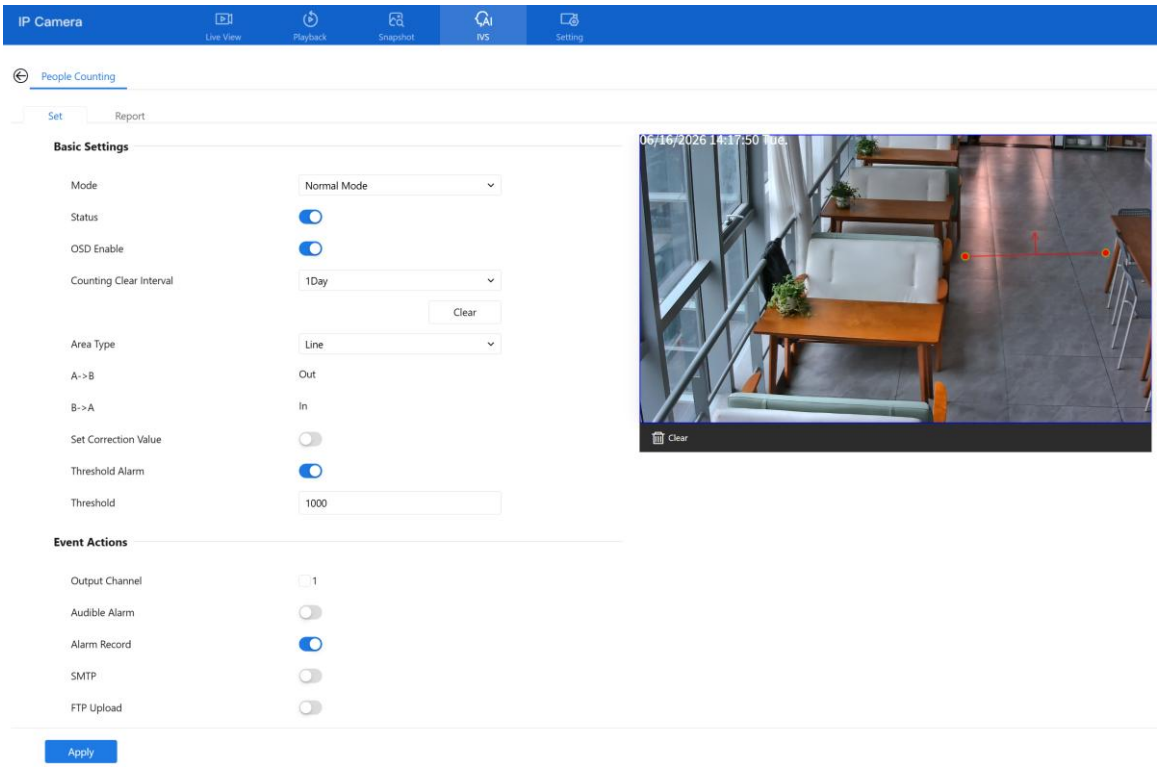
9.5.1 Setting

People Counting allows the camera to count entries and exits across a defined line in the monitored area. This is useful for analyzing foot traffic.

Procedure

Step 1 Navigate to **IVS > Behavior Analysis** > **People Counting** to access the **People Counting** setting interface, as shown in Figure 9-23.

Figure 9-23 People counting page



Step 2 Set all parameters of illegal parking. Table 9-2 describes the specific parameters.

Table 9-2 Parameters of people counting

Parameter	Description	Setting
Mode (only for PTZ camera)	Choose between **Normal** and **Preset Point** mode. Preset mode requires selecting a predefined point.	[How to set] Choose from the drop-down list [Default value] **Normal mode**
Enable	Enables the button to enable the alarm.	[How to set] Click the button on. [Default value] **OFF**
OSD Enable	Enable the OSD, and the count data will show on the live video screen.	[How to set] Click the button on. [Default value] **OFF**
Counting Clear Interval	Automatically resets the count at set intervals (e.g., 10 min, 1 hour, etc.). Manual reset is also available via **Clear Counting**.	[How to set] Choose from the drop-down list. [Default value] **12 hours**

Parameter	Description	Setting
Area Type	Defines the counting method (e.g., line). Labels **A** and **B** indicate "In" and "Out."	[How to set] Choose from the drop-down list. [Default value] **Line**
Set Correction Value	Enable, set the count correction value, which can be positive or negative. For example, if there are 30 people who enter the area before counting, input 30 to correct. If 30 people go out of the area, input -30.	[How to set] Enable /Input a value in the area box. [Default value] **0**
Threshold alarm	Triggers an alarm if the count exceeds a defined threshold.	[How to set] Click the button on. [Default value] **OFF**
Output Channel	If you click to set the Output Channel and the device is connected to an external alarm indicator, the alarm indicator signals when an alarm is triggered. Only for Some Models.	[How to set] Click to select an ID.
Flashlight Alarm	After enabling Flashing Light and setting the Flashing Light Alarm Output, the light flashes when an alarm event is detected. Only for Some Models.	[How to set] Click the button on. [Default value] **OFF**
Audible Alarm	After enabling Audible Warning and setting Audible Alarm Output, the built-in speaker of the device or the connected external speaker plays warning sounds when an alarm happens. (set at the "**Setting > Video / Audio > Audio File**") Only for some models.	[How to set] Click the button on. [Default value] **OFF**
Alarm Record	Enable the button to enable the alarm record.	[How to set] Click to enable Alarm Record. [Default value] **OFF**

Parameter	Description	Setting
SMTP	Enable the button to enable the SMTP server. The parameters of SMTP can be set at **Setting > Network > Advanced Settings > SMTP** interface.	[How to set] Click to enable SMTP. [Default value] **OFF**
FTP Upload	Enable the button to enable File Transfer Protocol. The parameters of FTP can be set at **Setting > Network > Advanced Settings > FTP** interface.	[How to set] Click to enable FTP Upload. [Default value] **OFF**
White light Alarm	When the **Day/Night** mode is chosen the **Night** mode, and the light is **IR LED** or **NON**E, this linkage action is valid. Enable the white light alarm when it triggers the alarm, and the white light will be on. Only for Some Models.	[How to set] Click the button on. [Default value] **OFF**

Step 3 Set the deployment area:

- Click to generate points on the live video screen.
- Continue to form a line or shape.
- Right-click to finish drawing.

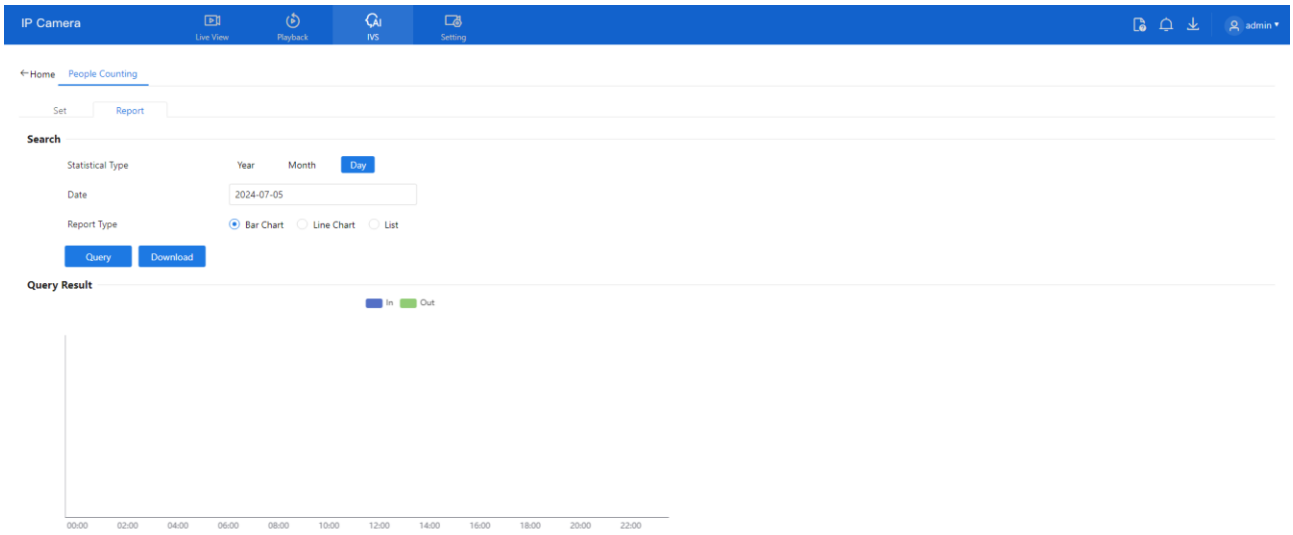
Step 4 Set the deployment time. Refer to section 7.1 Step 4.

Step 5 Click **Apply**. The system saves your configuration and confirms with **"Apply success!"**.

9.5.2 Report

The **People Counting** interface allows you to view statistical data by setting specific query conditions, including a defined time range. The data can be visualized in three formats: **Line Chart**, **Histogram**, or **List**, as shown in Figure 9-24.

Figure 9-24 People counting page



Procedure

Step 1 **Set the Time Range**:

- Use the calendar pop-up to select the **Start** and **End** time for the query.
- Select the **Year** and **Month** as needed.

Step 2 **Choose Report Type**:

- Available display formats include:
  - **Line Chart**
  - **Histogram**
  - **List**

Step 3 **Query the Data**:

- Click the **Query** button to retrieve the people counting results based on the specified conditions.

Step 4 **Download Results**:

- Click **Download** to export the query results. The data can be saved to a local folder for further analysis or reporting.

.

10 Panoramic Cameras

10.1 CVBS Function (Only for Some Models)

Preparation

Ensure a display device is connected to the camera's **VIDEO OUT** port.

Description

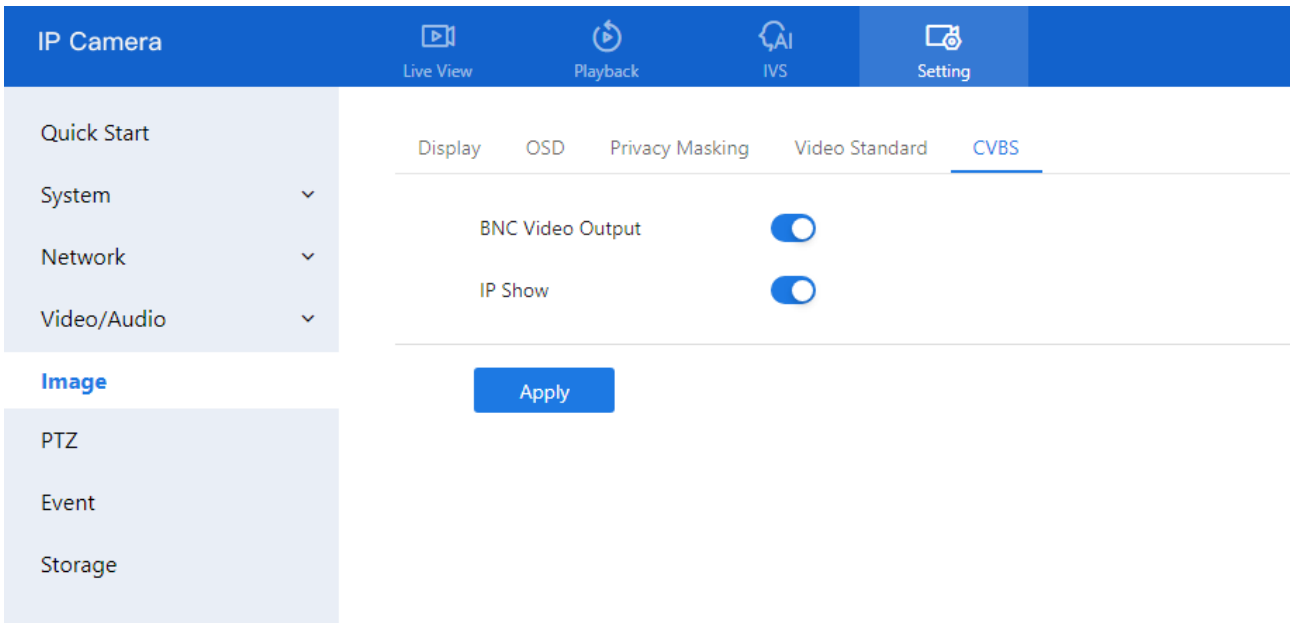
When the analog output function is enabled, the IP camera can transmit analog video signals to a video server or display device via the VIDEO OUT port. This is useful for legacy analog systems or real-time local display.

Procedure

Step 1 Navigate to **Setting > Image > CVBS**.

The **BNC Video Output** page is displayed, as shown in Figure 10-1.

Figure 10-1 BNC video output page



Step 2 Toggle the switch **ON** to enable **BNC Video Output**.

Step 3 Toggle the switch **ON** to enable **IP Show** if you want the IP address displayed on the video output.

Step 4 Click **Apply**.

A message will appear: "Apply success!", indicating the settings have been saved.

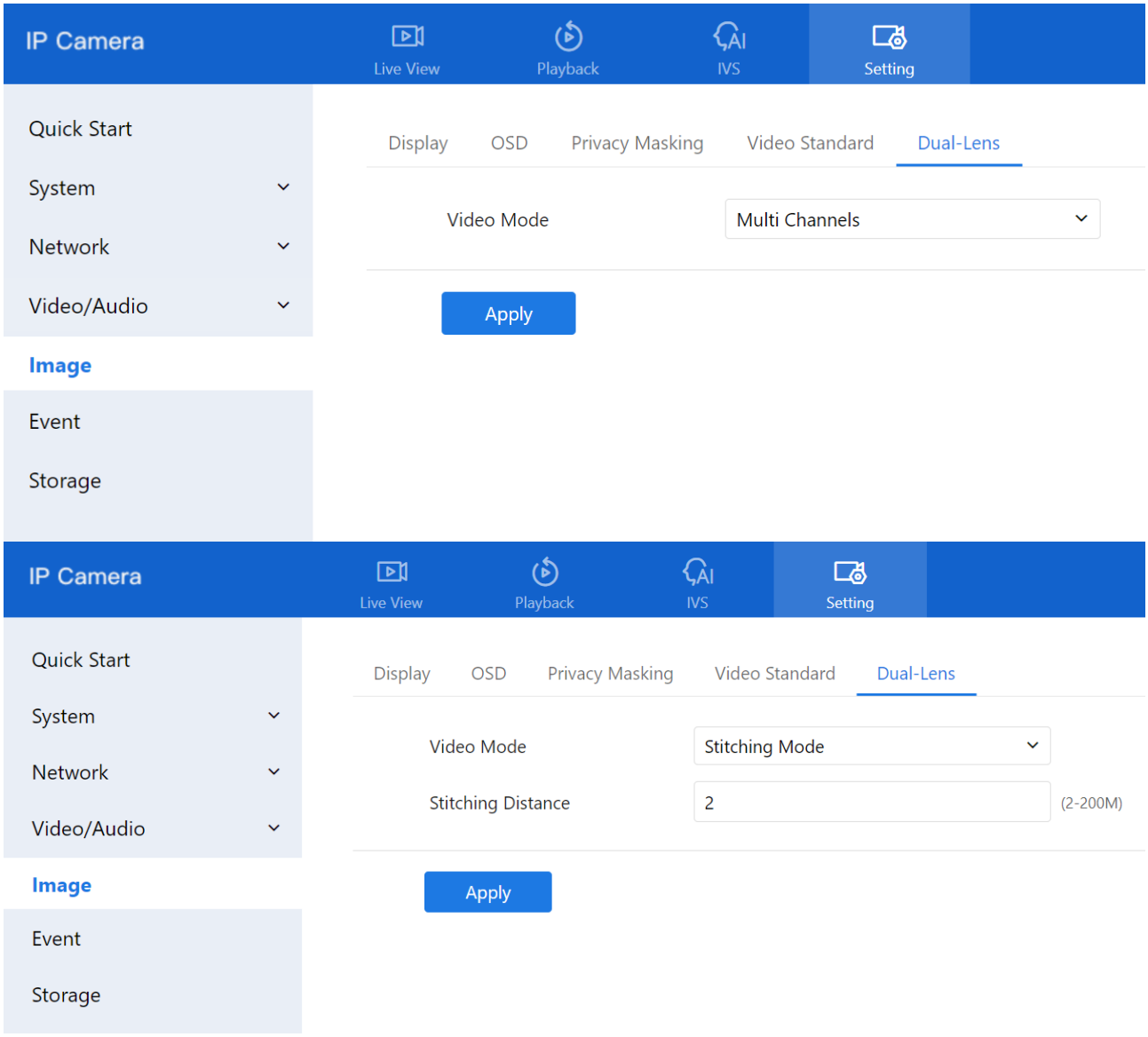
Note: This function is only supported on specific camera models with analog output capabilities.

10.2 Dual-Lens

10.2.1 Dual-Lens

For cameras equipped with dual lenses, you can configure the video output mode from **Setting > Image > Dual-Lens**, as shown in Figure 10-2.

Figure 10-2 Dual-Lens



Available Video Modes:

- **Multi-Channels**
  - Each lens operates independently.
  - Two separate video streams are displayed — each corresponding to a different channel.
- **Stitching Mode**
  - Combines video from both lenses into one seamless panoramic view.
  - You can set the **Stitching Distance** (range: 2–200 meters) to achieve smooth, natural blending based on the physical installation environment.

NOTE

Important:
Switching between video modes will **reset all IVS (Intelligent Video Surveillance) settings**. Make sure to back up your configuration if necessary before changing the mode.

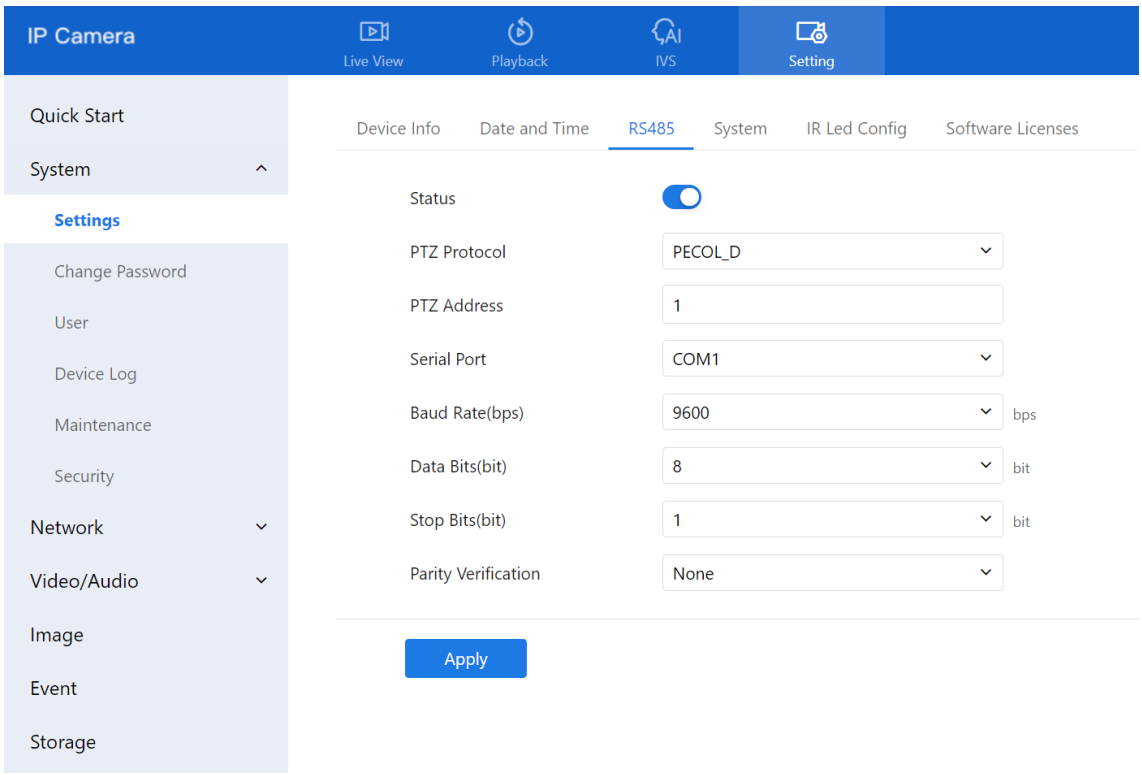
10.3 Panoramic Camera

10.3.1 RS458

Purpose:
Configure the RS485 interface to connect the panoramic camera with an external high-speed PTZ camera.

Step 1 Go to **Setting > System > Settings > RS485**

The RS485 configuration interface is shown in Figure 11-4.



Parameter	Description	Setting
Status	Enable this function if the device connects to a high-speed camera. NOTE This check box is dimmed for an IP dome camera.	[Setting method] Click the button to enable PTZ configuration.
PTZ Protocol	Protocol used by the external PTZ, such as PELCO_D and PELCO_P.	[Setting method] Select a value from the drop-down list box.
PTZ Address	Address of the high-speed camera.	
Serial Port	The default value is **COM1**.	

Parameter	Description	Setting
Baud Rate	Baud rate used by the external PTZ. The value ranges from 300 bit/s to 115200 bit/s. The default value is **4800** bit/s.	NOTE When parameters are configured, these parameters must match the settings on the high-speed camera.
Data Bits	The value must match the setting used by the external PTZ. It can be set to a value ranging from 4 to 8. Generally, the value is 8.	
Stop Bits	N/A	
Parity Verification	N/A	

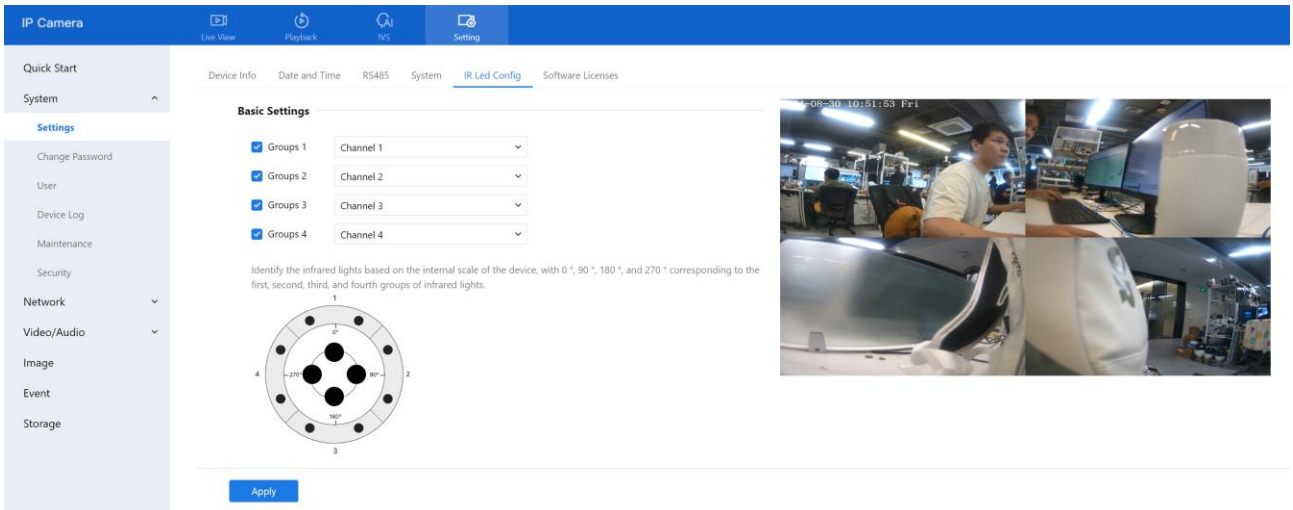
Step 2 Click **Apply**. The message "Apply success!" is displayed, and the system will save the settings.

10.3.2 **IR Led Config**

Purpose:
Configure the infrared (IR) LEDs for panoramic cameras to ensure proper night vision functionality based on camera orientation.

Step 1 Go to **Setting > System > Settings > IR Led Config.** The IR LED configuration interface is shown in Figure 11-4.

Figure 10-3 IR led config



Procedure:

Step 2 **Channel Assignment:**
Each IR LED group corresponds to a direction on the internal camera dial:

- **Group 1** = 0°
- **Group 2** = 90°

- **Group 3** = 180°
- **Group 4** = 270°

Assign channels based on the installation direction, as marked on the device housing.

Step 3 **Adjust as Needed:**
If the camera is physically moved or rotated, update the channel assignments so the IR LEDs align with the actual field of view.
Step 4 Click **Apply**.
When the message **"Apply success!"** appears, the settings are saved.

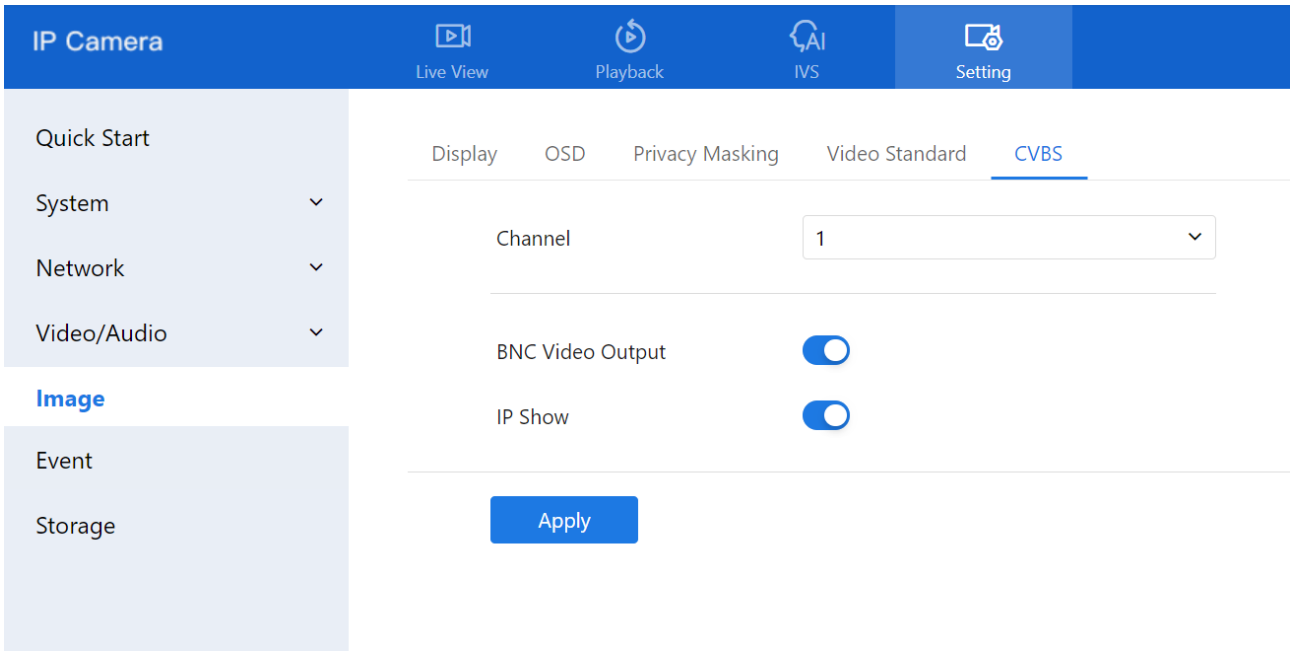
Note: Correct LED-to-channel alignment is critical for effective illumination.

10.3.3 **CVBS**

Purpose: Enable analog video display through a BNC cable.

Step 1 Go to **Setting > Image > CVBS.** The **CVBS configuration interface** is shown in **Figure 11-5.**

Figure 10-4 CVBS



Step 2 Enable **BNC Video Output** to activate analog signal output.
Step 3 Enable **IP Show** to display the IP address on the analog output screen.
Step 4 Use the **dipswitch** on the device to switch video channels if needed.

10.4 For Special Cameras

10.4.1 General Parameters

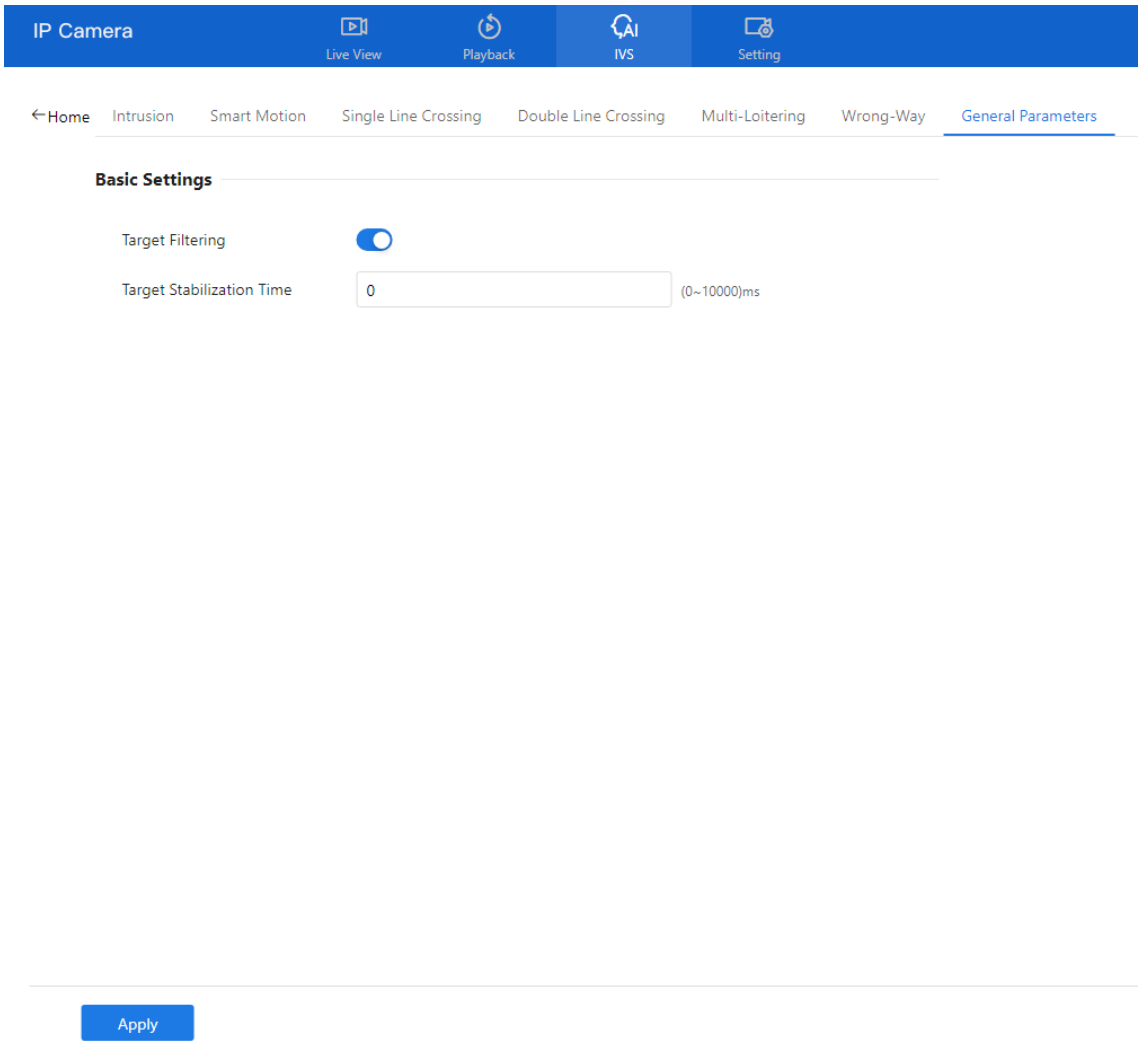
Description

Target filtering helps reduce false alarms by ignoring brief or unstable appearances of people or vehicles in the detection area. Only stable, continuous targets will trigger intelligent analysis alarms.

Procedure

Step 1 Go to **IVS > Intelligent Analysis** > **General Parameters** to access the advanced setting interface, as shown in Figure 10-5.

Figure 10-5 General parameters page



Step 2 **Enable Target Filtering**

- Toggle the switch to activate the feature.

Step 3 **Set Target Stabilization Time**

- This is the minimum duration a person or vehicle must remain in the detection area before an alarm is triggered.
- Input the desired stabilization time in seconds.

Step 4 Click **Apply**

- When the message **"Apply success!"** appears, the settings are successfully saved.

Note: This function is useful in environments with frequent brief movements, helping the system focus only on sustained activity.

10.4.2 Illegal Parking (Only for Some Models)

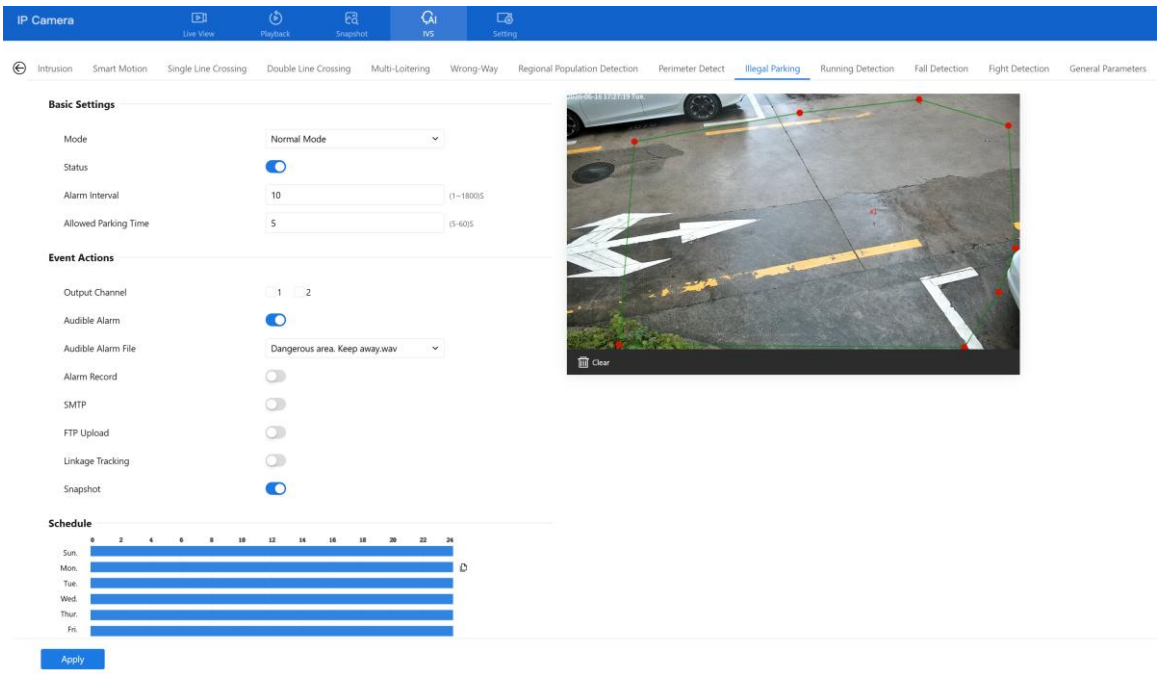
Description

This function generates an alarm when a vehicle remains in a designated detection area longer than the allowed parking time.

Procedure

Step 1 Navigate to **IVS > Intelligent Analysis** > **Illegal Parking**, as shown in Figure 10-6.

Figure 10-6 Illegal parking settings page



Step 2 **Configure the following parameters:**
(Refer to Section 9.2.1 Step 2 for details on parameter settings such as sensitivity, interval, and output actions.)

Step 3 **Set a Deployment Area:**

- Use the mouse to draw a region on the live video feed.

Step 4 **Set the Schedule Time:**

- See Section 7.1 Step 4 for instructions on setting active monitoring times.

Step 5 **Click Apply**

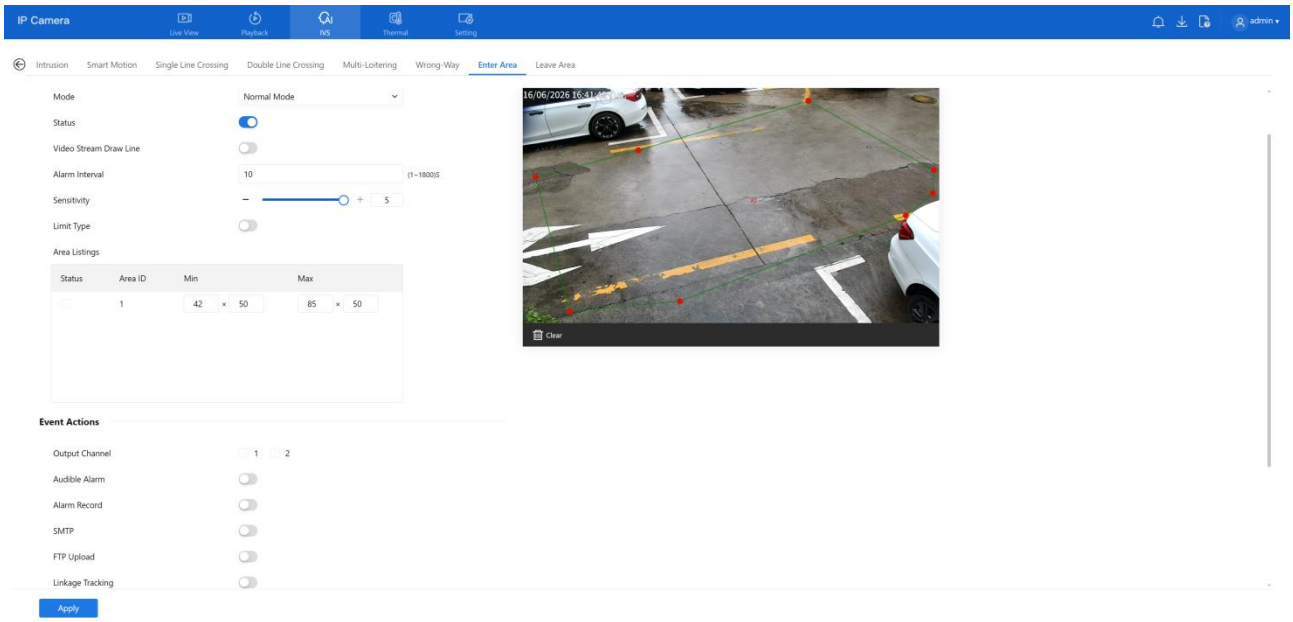
- A confirmation message **"Apply success!"** will confirm that the settings have been saved.

10.4.3 **Enter Area(Only for Some Models)**

Description: Triggers an alarm when a target (such as a person or vehicle) enters a designated area during a scheduled time.

Step 1 Navigate to **Configuration** > **Intelligent Analysis** > **Enter Area**, as shown in Figure 10-7.

Figure 10-7 Enter Area



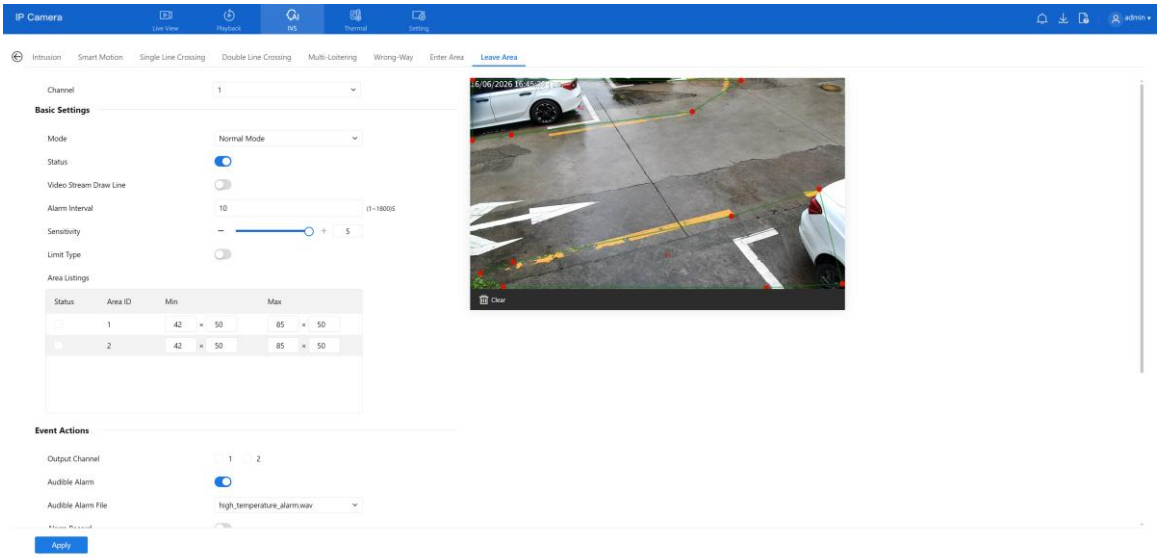
Set all parameters for enter area, please refer to 9.4.1 Step 3.

10.4.4 **Leave Area(Only for Some Models)**

Description: Triggers an alarm when a target exits a predefined area during a valid monitoring period.

Step 1 Navigate to **Configuration** > **Intelligent Analysis** > **Leave Area**, as shown in Figure 10-8.

Figure 10-8 Leave Area



Set all parameters for the leave area. Please refer to 9.4.1 Step 3.

10.4.5 **Heat Map**

10.4.5.1 Heat Map Set (Only for Some Models)

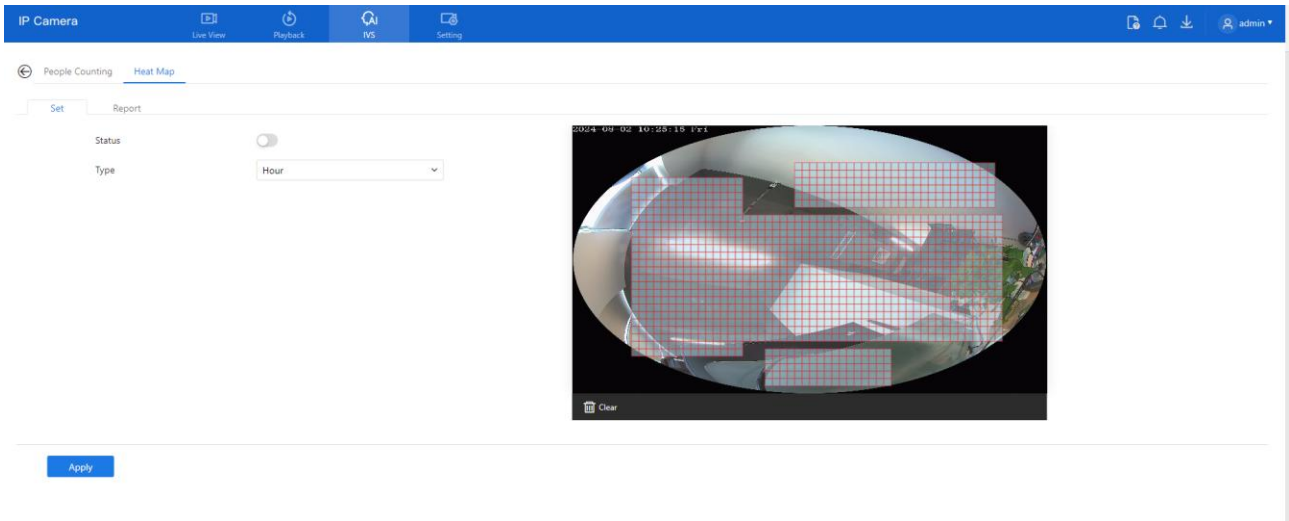
The heat map is a visual data analysis tool that highlights areas of interest—such as customer movement patterns, target locations, and activity zones—using color-coded overlays. Once enabled, the camera automatically monitors and counts foot traffic within the detection area. It then visualizes the frequency of activity through varying color intensities, making it easy to identify high and low traffic regions.

NOTE

The setting and export of the heat map are only applied to some models.

Step 1 Navigate to **IVS > Behavior Analysis > Heat map > Set** interface, as shown in Figure 10-9.

Figure 10-9 Heat map set page



Step 2 **Enable Heat Map Function:**

- Toggle the **Status** button to turn on the heat map function.
- *Note: This feature is disabled by default and must be manually activated.*

Step 3 **Select Type:**

- Choose the statistical granularity:
  - **Hour**: Collects and displays 24 data segments per day.
  - **Day**: Displays one aggregated data point per day.
- *Switching between types will clear previously collected data. Please proceed with caution.*

Step 4 **Click "Apply":**

- Once the settings are configured, click **Apply** to save.
- The system will confirm with the message: **"Apply success!"**

10.4.5.2 Heat Map Report

Step 1 Navigate to **IVS > Behavior Analysis > Heat Map > Report,** as shown in Figure 10-10.

Figure 10-10 Heat map report page

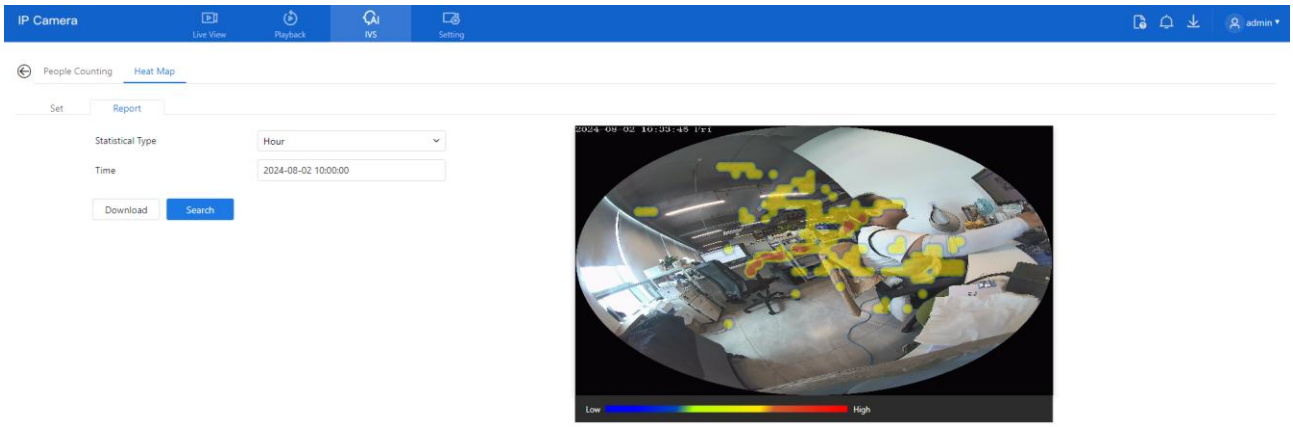


Table 10-1 Parameters of heat map

Parameter	Description	Setting
Type	Select either **Data** or **Picture**. Data is shown in numerical format and can be downloaded. Pictures display different heat levels via color mapping.	[How to set] Choose from the drop-down list [Default value] **Normal mode**
Statistics type	Select the time unit for analysis: Year, Month, Day, or Hour.	[How to set] Click the button on. [Default value] **OFF**

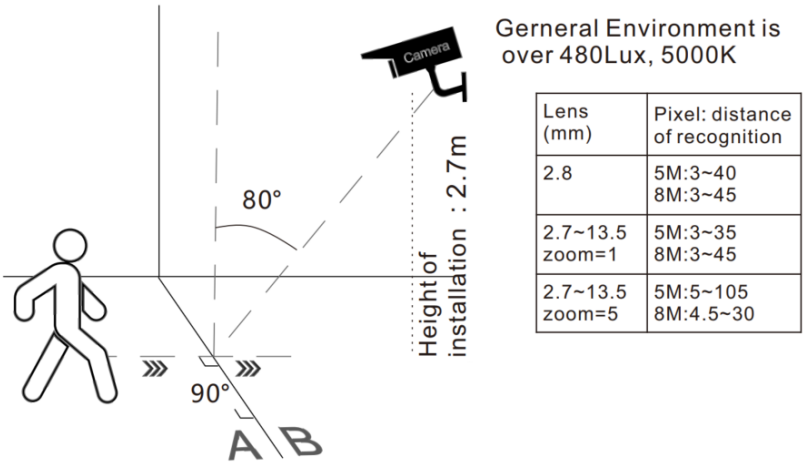
Parameter	Description	Setting
Time	Specify the time range for searching or downloading heat map data.	[How to set] Choose from the drop-down list
Heat map bar	Displays color-coded heat levels. Each color represents a different level of activity. The maximum value reflects the peak data in any area during the selected time.	Null

Step 2 Set the time range for analysis.
Step 3 Click Search to view the heat map directly, or
Step 4 Click Download to export the data in CSV format to your local folder.

Table 10-2 describes the common faults and solutions.

Table 10-2 Common faults and solutions

Common Fault	Possible Cause	Solution
When you enter the device IP address in the address box of Internet Explorer and press **Enter**, the message "There is a problem with this website's security certificate" is displayed.	The certificate is not installed.	Click **Continue to this website (not recommended) to proceed**.
The web management system cannot be accessed.	The network is disconnected.	Connect the PC directly to the camera, and verify that the web management system can be accessed. Run the **ping** command to verify that the camera is reachable.
	The IP address is used by another device.	Connect the PC directly to the camera and configure the IP address of the camera.
	The IP addresses of the PC and the IP camera are on different networks.	Check the IP address, subnet mask, and gateway settings on the IP camera, and change the settings as required.
The PTZ or dome cannot be controlled.	The protocol, baud rate, or address is incorrect.	Change the protocol, baud rate, and address in the web management system to those used by the PTZ or dome.
	The signal cable is not properly connected.	Check the signal strength and connect the signal cable properly.

<table>
<tr><th>Common Fault</th><th>Possible Cause</th><th>Solution</th></tr>
<tr><td>After the IP camera is upgraded, the web management system cannot be accessed.</td><td>The browser cache is not deleted.</td><td>To delete the browser cache, proceed as follows:
1. Open a browser.
2. Press Ctrl + Shift +Delete.
The Delete Browsing History dialog box is displayed.
3. Select all check boxes.
4. Click Delete.
Log in to the web management system again.</td></tr>
<tr><td rowspan="2">The IP camera cannot be upgraded.</td><td>The network is disconnected.
The network settings are incorrect.</td><td>Confirm that the upgrade network is connected.
Check the network settings.</td></tr>
<tr><td>The upgrade package is incorrect.</td><td>Obtain the correct upgrade package and upgrade the IP camera again.</td></tr>
<tr><td>The accuracy of people counting is bad.</td><td>The installation method is faulty.</td><td>Install the camera and draw the line following as figure.

</td></tr>
<tr><td>The capture performance of AI Multi-target is bad.</td><td>The lens is too short.</td><td>It is recommended to use a 6mm focus length lens or above.</td></tr>
</table>

Acronyms and Abbreviations

A	
ADSL	Asymmetric Digital Subscriber Line
C	
CBR	Constant Bit Rate
CGI	Common Gateway Interface
CMS	Central Management System
D	
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DDNS	Dynamic Domain Name Server
E	
EAP	Extensible Authentication Protocol
F	
FTP	File Transfer Protocol
G	
GAMA	Graphics Assisted Management Application
H	
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I	
ID	Identity
ISO	International Standard Organization
IP	Internet Protocol
IPC	Internet Protocol Camera
IVS	Intelligent Video System
L	
LPS	Limited Power Source
M	
MJPEG	Motion Joint Photographic Experts Group

MAC	Media Access Control
MTU	Media Transmission Unit
N	
NAS	Network Attached Storage
NTP	Network Time Protocol
NTSC	National Television Standards Committee
O	
OSD	On-Screen Display
P	
PAL	Phase Alteration Line
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
PTZ	Pan/Tilt/Zoom
R	
ROI	Region of Interest
RSTP	Rapid Spanning Tree Protocol
S	
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
V	
VBR	Variable Bit Rate