CP PLUS

ORANGE

IP Camera User Manual

Version 2.0.1

Foreword

General

This manual introduces the functions and operations of the Network Speed Dome PTZ Camera(here in after referred to as "the Camera").

Safety Instructions

The following signal words might appear in the manual.

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

Privacy Protection Notice

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

Interface Declaration

This manual mainly introduces the relevant functions of the device. The interfaces used in its manufacture, the procedures for returning the device to the factory for inspection and for locating its faults are not described in this manual. Please contact technical support if you need information on these interfaces.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not incompliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Pleasecontact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDFformat) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Camera, hazard prevention, andprevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operation Requirements

⚠

- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objectsfilled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements

⚠ WARNING

- Connect the device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the device.
- Do not connect the device to more than one power supply. Otherwise, the device might becomedamaged.
- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.

⚠

- Do not expose the device to direct sunlight or heat sources.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be nohigher than PS2. Note that the power supply requirements are subject to the device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

1. Overview

1.1. Introduction

Network Speed Dome PTZ Camera is a combination of traditional camera and network technology. Users can remotely connect to the Camera through the network for configuration and management. Get the camera IP address before visiting PTZ Camera through network, which can be searched by IP Finder.

Figure 1-1

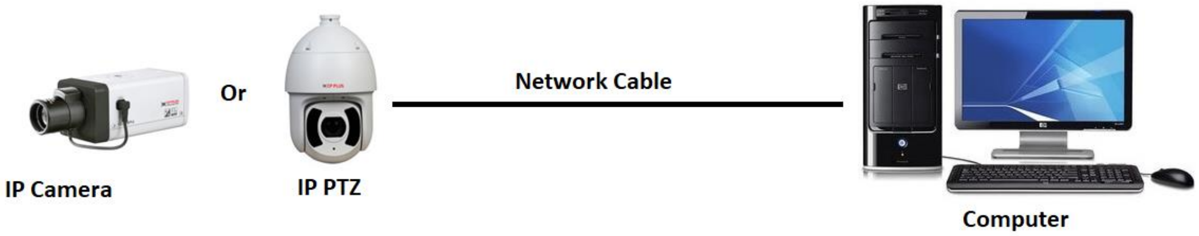
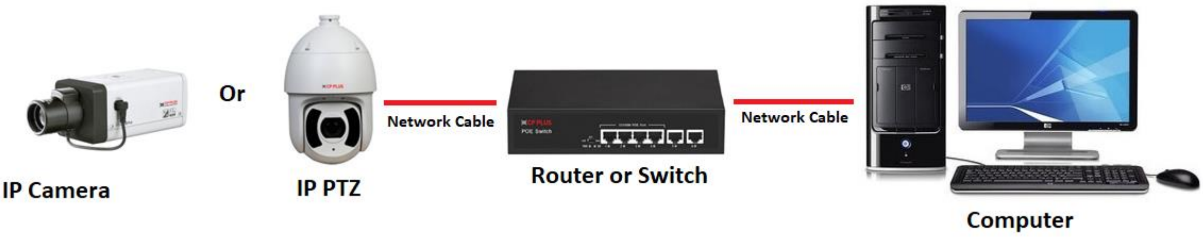


Figure 1-2



1.2. Functions

Functions might be different depending on the model.

1.2.1. Basic Functions

1.2.1.1. Real-time Monitoring

- Live view.
- Displays human face, human body, non-motor vehicle, motor-vehicle, and other metadata during live view.
- When watching the live view, you can enable audio, and talk to people in the monitoring area toquickly process exceptions.
- Adjust the image to the proper position by PTZ.
- Take a snapshot or three snapshots of the abnormal monitoring image for subsequent viewing and processing.
- Record the abnormal monitoring image for subsequent viewing and processing.
- Configure encoding parameters and adjust live view.

1.2.1.2. Recording

- Auto recording as scheduled.
- Play back recorded videos and images.

- Download recorded videos and images.
- Record videos when an alarm is triggered.

1.2.1.3. Account Management

- Add, edit, and delete user groups, and manage user authorities by user group.
- Add, edit, and delete users, and configure user authorities.
- Change user password.

1.2.2. AI Function

1.2.2.1. Alarm

- Set alarm prompt mode and tone by alarm type.
- View alarm messages.

1.2.2.2. Video Detection

- Support motion detection, video tampering detection, defocus detection and scene changingdetection.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email sending, PTZ operation and snapshot taking.

1.2.2.3. Smart Motion Detection

- Support smart motion detection and the movement range of people, non-motor vehicle andmotor vehicle in the image.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email sending and snapshot taking.

1.2.2.4. Audio Detection

- Detect audio input exception and audio intensity change.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email sending, PTZ operation and snapshot taking.

1.2.2.5. IVS

- Support crossing fence detection, tripwire, intrusion, abandoned object, moving object, fast moving, parking detection, people gathering, loitering detection, and more.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output, email sending and snapshot taking.

1.2.2.6. Face detection

- Support human face detection and display the related attributes on the **Live** page.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email

sending and snapshot taking.

1.2.2.7. Face Recognition

- Detect human faces, compares them with face images in the database, and links alarm output.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email sending and snapshot taking.

1.2.2.8. People Counting

- Support counting of people number (including the people flow enter/exit the detection area andpeople stay in the area) and queuing data and generate report.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output, email sending and snapshot taking.

1.2.2.9. Video Metadata

- Support the detection of people, non-motor vehicles, and motor vehicles in the captured video, and displays the related attributes and characteristics on the **Live** page.
- When an alarm is triggered, the system performs linkages such as alarm output.

1.2.2.10. Alarm Setting

- Alarms are triggered when an external alarm input device outputs alarms.
- When an alarm is triggered, the system performs linkages such as video recording, alarm output,email sending, PTZ operation and snapshot taking.

1.2.2.11. Exception Processing

- Supports SD card error detection, network abnormality detection, illegal access detection, security exception detection, PTZ exception detection and battery detection.
- When SD card error, illegal access and security exception alarm is triggered, the system performs linkages such as alarm output and email delivery.
- When network abnormality alarm is triggered, the system performs linkages such as videorecording and alarm output.
- When PTZ abnormality alarm is triggered, the system performs linkages such as alarm output.
- When the battery is over-temperature, the system performs linkages such as alarm output, email sending and playing audio.

2. Configuration Flow

Configure the device as needed.

Figure 2-1

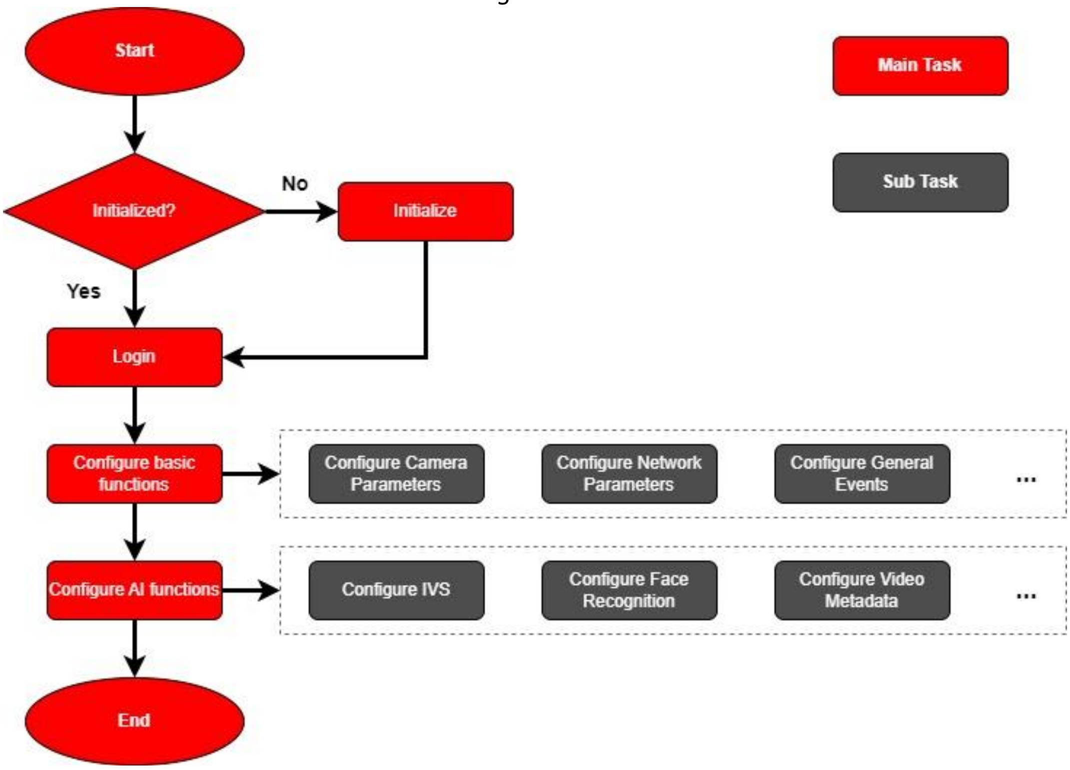


Table 1

Configuration	Description
Initialization	Initialize the camera when you useit for the first time.
Login	Open the browser and enter the IPaddress to log in to the web page. The camera IP address is 192.168.1.250 by default.
Configure basic functions	Configure camera parameters, network parameters, general events and more.
Configure AI functions	Configure detection rules for AIevents.

3. Device Initialization

Device initialization is required for first-time use. This manual is focused on the operation on the web page. You can also initialize the device through **IP Finder**, NVR (Network Video Recorder), or platforms such as EVMS Pro.

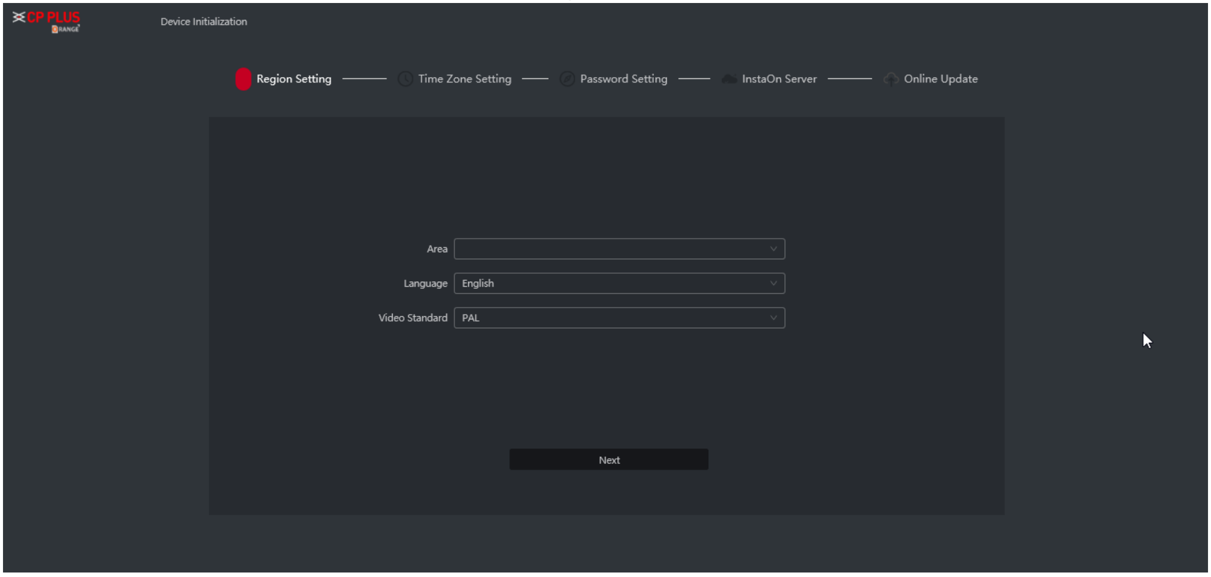
- To ensure device safety, protect your password after initialization and regularly change it.
- When initializing the device, keep the PC IP and Camera IP on the same segment.
- We recommend using Internet Explorer or Google Chrome.

Step 1 Open the browser, enter the IP address of the Camera in the address bar, and then pressthe Enter key.

The IP is 192.168.1.250 by default.

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

Figure 3-1



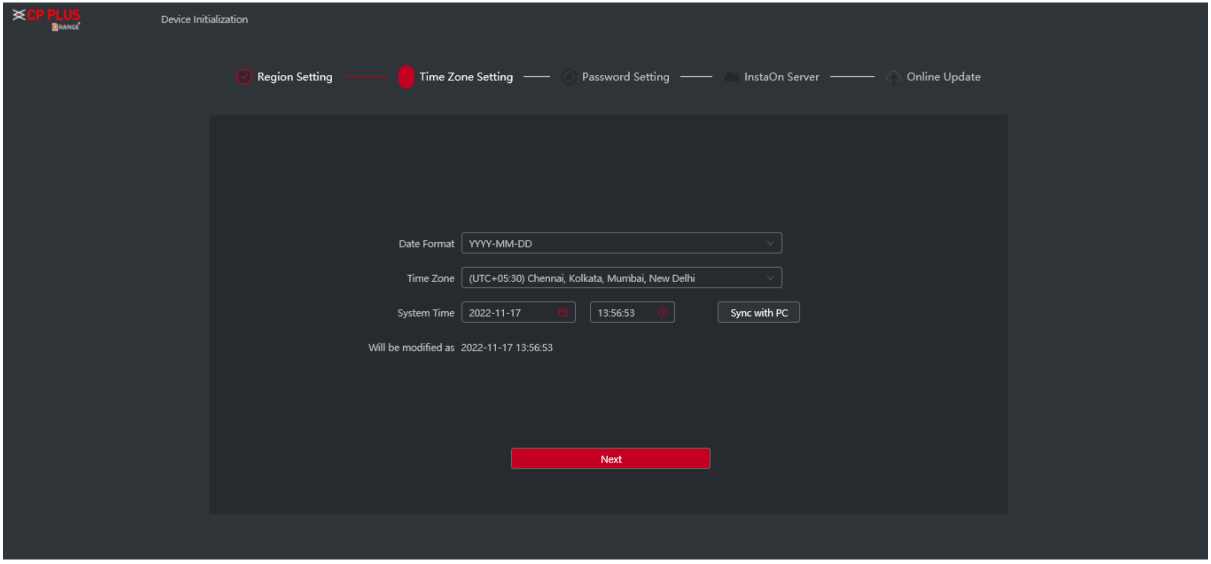
Area:

Language: English

Video Standard: PAL

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

Figure 3-2



Date Format YYYY-MM-DD

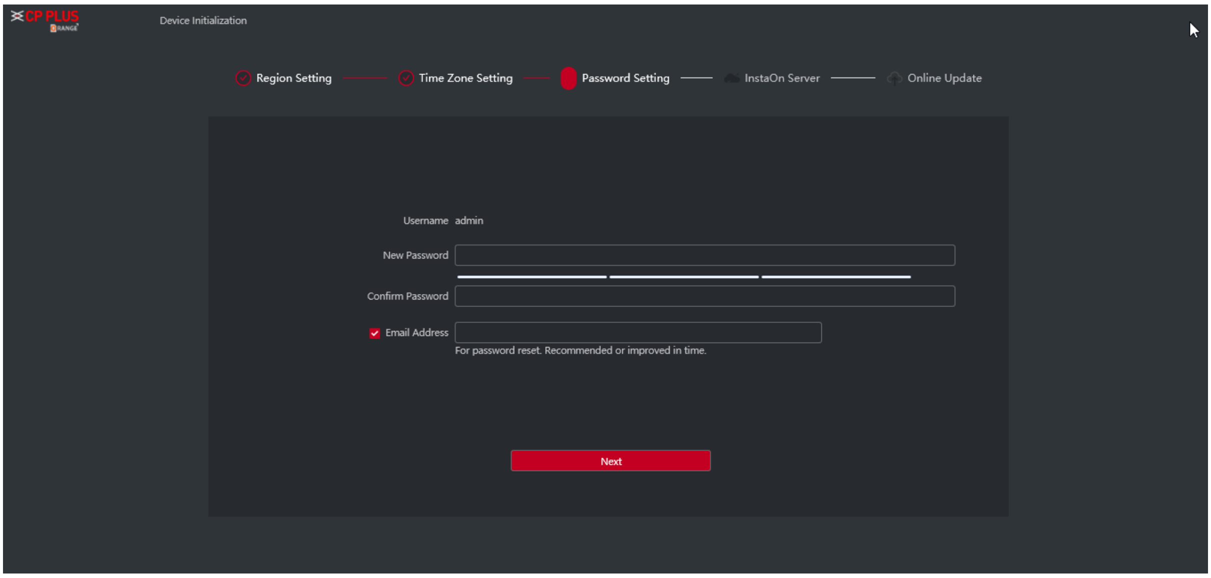
Time Zone (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

System Time 2022-11-17 13:56:53

Will be modified as 2022-11-17 13:56:53

Step 4 Set the password for admin account.

Figure 3-3



Username admin

☑ Email Address

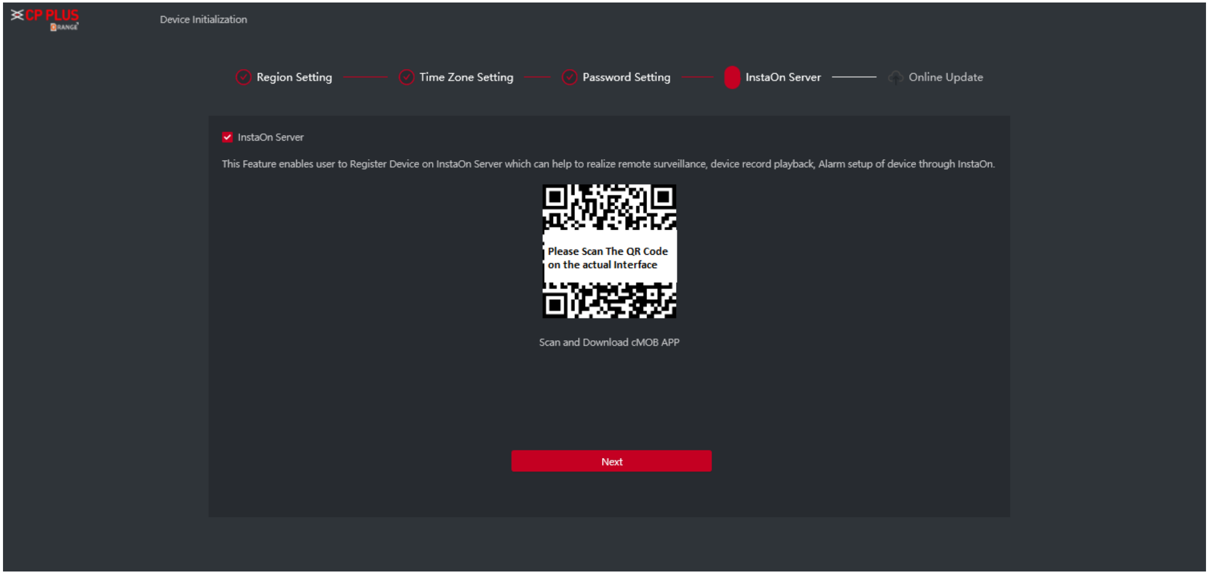
For password reset. Recommended or improved in time.

Table 2

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

Step 5 Click **Next**, and the **InstaOn** page is displayed.

Figure 3-4



☑ InstaOn Server

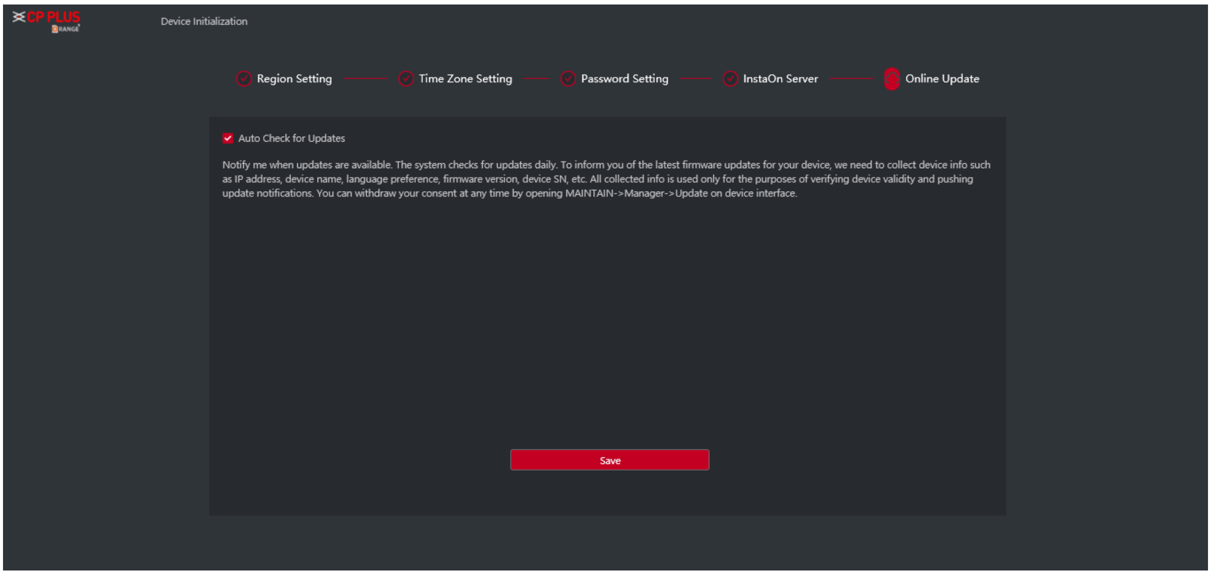
This Feature enables user to Register Device on InstaOn Server which can help to realize remote surveillance, device record playback, Alarm setup of device through InstaOn.

Please Scan The QR Code on the actual Interface

Scan and Download cMOB APP

Step 6 Click **Next**, and then click **End** to complete initialization.

Figure 3-5



☑ Auto Check for Updates

Notify me when updates are available. The system checks for updates daily. To inform you of the latest firmware updates for your device, we need to collect device info such as IP address, device name, language preference, firmware version, device SN, etc. All collected info is used only for the purposes of verifying device validity and pushing update notifications. You can withdraw your consent at any time by opening MAINTAIN->Manager->Update on device interface.

4. Setting

This chapter introduces the basic settings of the Camera, including the configuration of local parameters, camera, network, PTZ, event, storage, system information, log, and more.

You can configure the camera, event, and system through two methods. This section uses method 1as an example.

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

4.1. Device Login

Log in to the device web page through a browser.

Prerequisites

- You need to initialize the Camera before logging in to the web page
- When logging in to the web page, keep the PC IP and device IP on the same network.

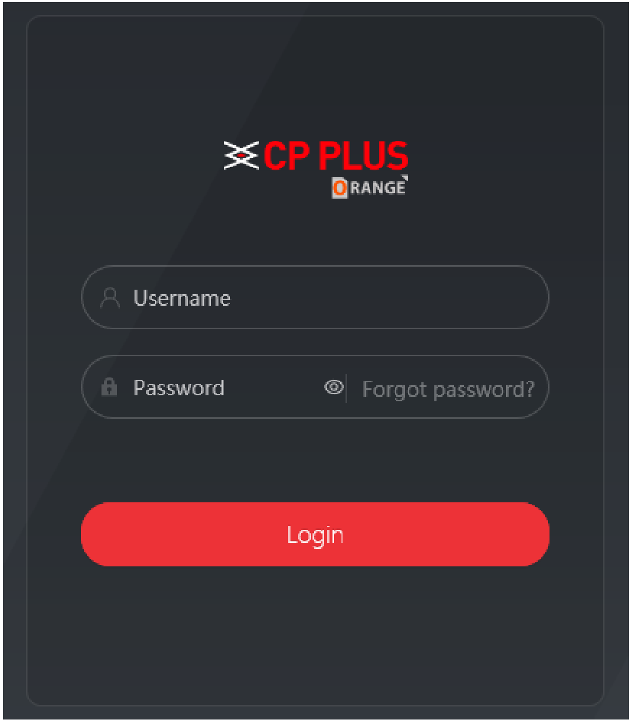
Procedure

Step 1 Open the browser, enter the device IP address (192.168.1.250 by default) in the address box, and then press Enter key.

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

Click **Forgot password?** to reset the password through the email address that is set during the initialization.

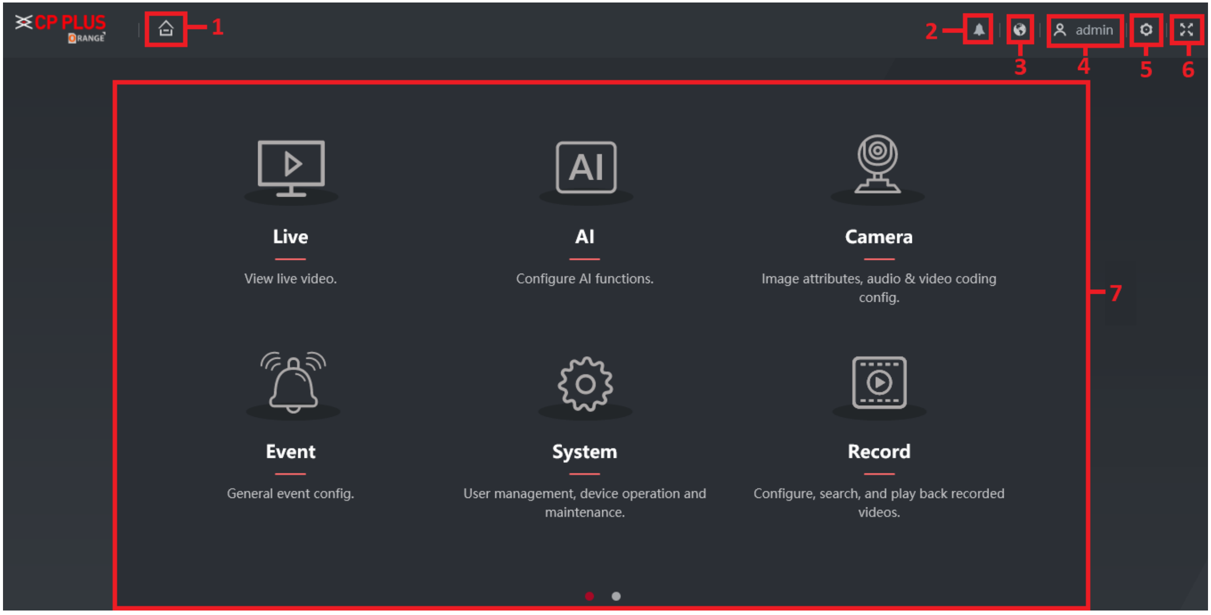
Figure 4-1



Step 3 Click **Login**.

The **Live** page is displayed. Click ⌂ on the left-upper corner of the page to display the main page.

Figure 4-2


CP PLUS ORANGE
1
2
3
4
admin
5
6
7
Live
View live video.
AI
Configure AI functions.
Camera
Image attributes, audio & video coding config.
Event
General event config.
System
User management, device operation and maintenance.
Record
Configure, search, and play back recorded videos.

📖

For first-time login, you need to install the plug-in. Follow the on-screen instructions to complete download and installation.

No.	Button	Description
1	⌂	Display the main page.
2	🔔	Subscribe to alarm messages.
3	🌐	Set the language.
4	👤 admin	- Click and select **Restart**, and the camera restarts. - Click and select **Logout** to go back to the login page.
5	⚙	Configure the basic parameters.
6	⛶	- Click the button to enter full screen mode. - Click ⛶ to exit full screen mode.
7	Main page	The main page includes the following modules. Click ● ● on the bottom of the page to switch between multiple pages. - **Live:** View the real-time monitoring image. The Live view page supports multi-channel display. - **AI:** Configure AI functions of the camera. - **Camera:** Configure camera parameters, including image parameters, encoder parameters, and audio parameters. - **PTZ:** Configure PTZ functions. - **Event:** Configure alarm linkage parameters of general events. - **System:** Configure basic system parameters, manage users and peripherals, maintain, and upgrade the system.

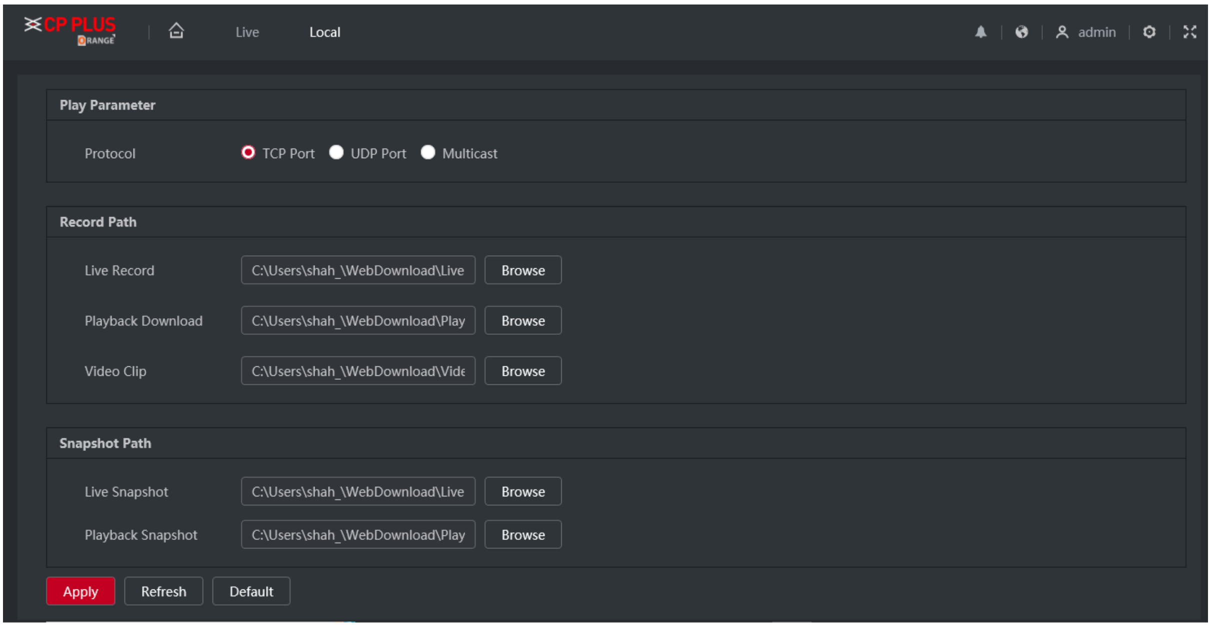
No.	Button	Description
		- **Security:** Check the device security status and set security functions. - **Record:** Configure record functions, playback or download recorded videos. When playing back multi-channel recordings, you can choose channel No. to play back. - **Picture:** Configure image functions, playback or download image files. When playing back multi-channel images, you can choose channel No. to play back. - **Report:** Search the AI event report and system report.

4.2. Local

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

Procedure

Step 1 Select ⚙ → **Local**.



Play Parameter

Protocol ● TCP Port ○ UDP Port ○ Multicast

Record Path

Live Record	C:\Users\shah_\WebDownload\Live	Browse
Playback Download	C:\Users\shah_\WebDownload\Play	Browse
Video Clip	C:\Users\shah_\WebDownload\Vide	Browse

Snapshot Path

Live Snapshot	C:\Users\shah_\WebDownload\Live	Browse
Playback Snapshot	C:\Users\shah_\WebDownload\Play	Browse

Apply Refresh Default

Step 2 Configure play parameters.

Protocol: Network transport protocol type, supporting TCP (Transmission Control Protocol) port, UDP (User Datagram Protocol) port and multicast.

Before selecting **Multicast**, you need to configure multicast parameters in advance.

Step 3 Click **Browse** to select the storage path for live snapshot, live record, playback snapshot, playback download, and video clips.

Table 3

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

Step 4 Click **Apply**.

Related Operations

- Click **Refresh** to refresh the parameters of the current page.
- Click **Default** to restore the default parameter values.

4.3. Camera

This section introduces camera configuration, including configuring image parameters, encoder parameters, and audio parameters.

Camera parameters might differ depending on the device.

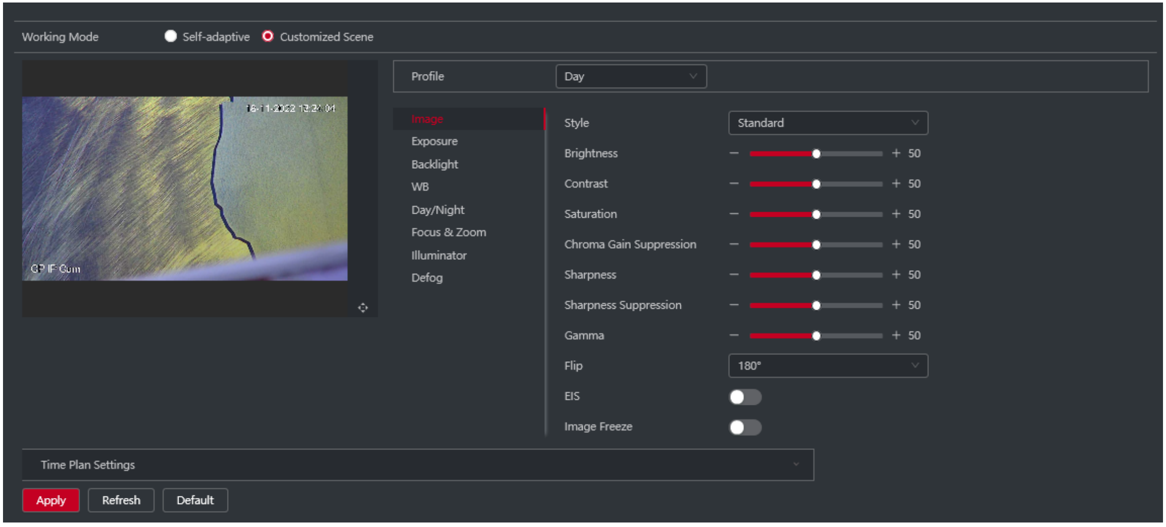
4.3.1. Image Parameters

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

4.3.1.1. Page Layout

Configure camera parameters to improve the image clarity and ensure that surveillance goes well. Camera supports two working modes: **Self-adaptive** and **Customized scene**. You can select 9 configuration file types, including day, night, general and front light, to set and view the configuration parameters and effects under the corresponding type, including image, exposure, andbacklight.

Figure 4-3



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Style	Standard	
Brightness	− +	50
Contrast	− +	50
Saturation	− +	50
Chroma Gain Suppression	− +	50
Sharpness	− +	50
Sharpness Suppression	− +	50
Gamma	− +	50
Flip	180°	
EIS	Off	
Image Freeze	Off	

4.3.1.2. Configuring Operating Mode

Select working mode as needed, including self-adaptive and customized scene.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then select working mode on the top of the page.

- Self-adaptive: Camera automatically matches the appropriate configuration file type according to different environments.

If you select **Self-adaptive**, go straight to Step5.

- Customized scene: Camera monitors according to the settings of the profile type atdifferent times.

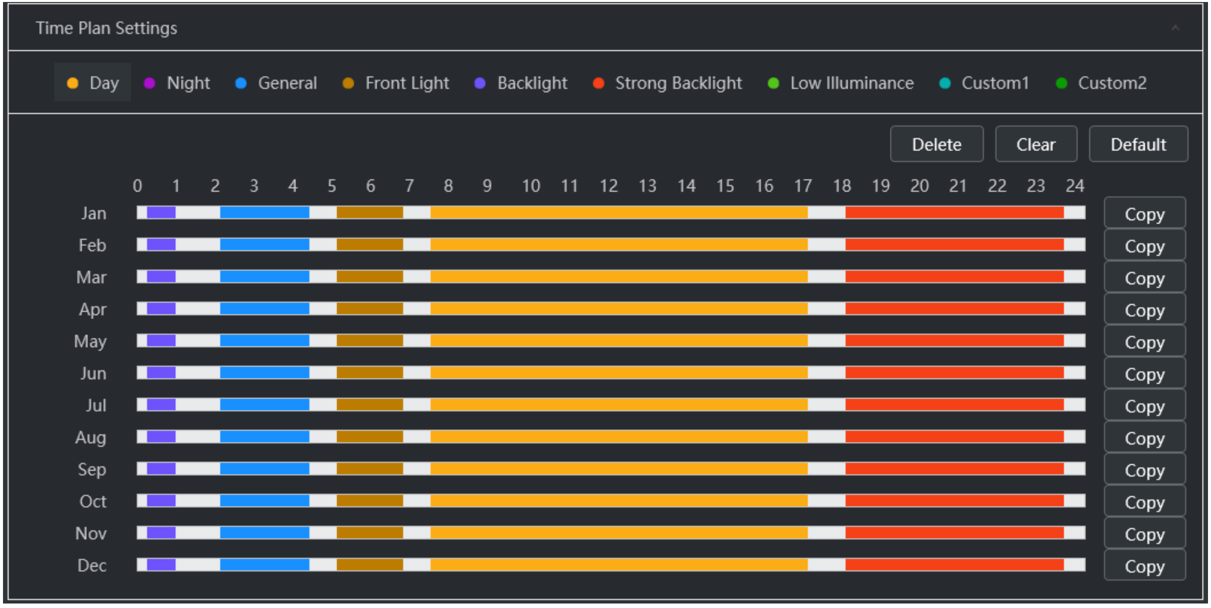
If you select **Customized scene**, go straight to Step3.

Step 3 Select configuration file type.

You can select 9 configuration file types, including **general**, **day**, **night**, **front light,** and backlight to set and view the configuration parameters and effects under the corresponding type, including image, exposure and backlight.

Step 4 Set time plans.
You can set daily schedule by month.

Figure 4-4



- Click **Time Plan Settings** or to open time plan.
- Click to configure file type, for example **general**, left drag on the timeline to set the tmeperiod using **general** type.

In the same way, you can set up separate time periods when applying other file types,including **Day**, **Night,** and **Front Light**.

Time period is set as **Day** and **Night** by default. Click **Delete** or **Clear** before you start setting time period.

- (Optional) Click **Copy**; select a month, then click **Apply**.

Time plan for the current month can be quickly copied to other months.

Step 5 Click **Apply**.

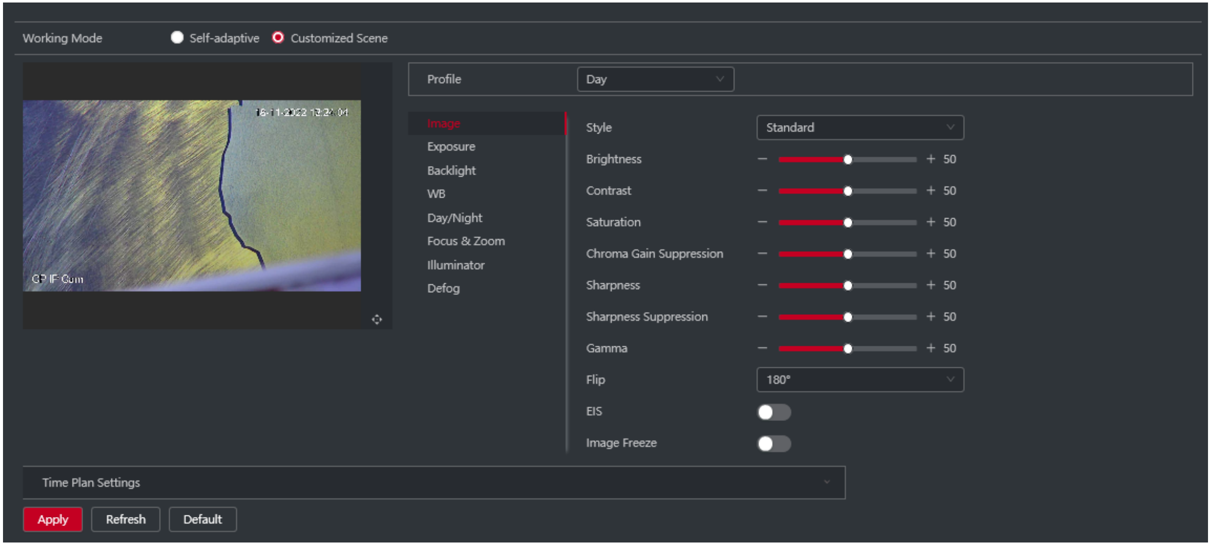
4.3.1.3. Adjusting Image

You can configure image parameters. The actual parameters of the camera can be adjusted here.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → Image.**

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then configure parameters.

Figure 4-5



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Style: Standard

Brightness: 50

Contrast: 50

Saturation: 50

Chroma Gain Suppression: 50

Sharpness: 50

Sharpness Suppression: 50

Gamma: 50

Flip: 180°

EIS: ○

Image Freeze: ○

Table 4

Parameter	Description
Style	Select the image style from soft, standard and vivid. ● **Standard:** Default image style, which displays the actual color of the image. ● **Soft:** The hue of the image is weaker than the actual one, andcontrast is smaller. ● **Vivid:** The image is more vivid than the actual one.
Brightness	Change the overall brightness of the image. The higher the value, the brighter the image. The image might be hazy if the value is configuredtoo high.
Contrast	Change the contrast of the image. The higher the value, the greater thecontrast between bright and dark areas. If the value is too big, the dark area will be too dark and the bright area will be more vulnerable to overexposure. The image might be hazy if the value is set too small.
Saturation	Set the intensity of colors. The higher the value, the deeper the color.Saturation value does not change image brightness.
Chroma Gain Suppression	Reduce the image color and prevents it from being too strong. Thehigher the value, the stronger the effect. 📖 This parameter takes effect only when the Camera is in an environmentwith low luminance.
Sharpness	Change the sharpness of image edges. The higher the value, the clearerthe image edges. If the value is too high, image noise is more likely to appear.
Sharpness Suppression	Change the sharpness NCT level of the Camera. The higher the value, thestronger the sharpness CNT. 📖

Parameter	Description
	This parameter takes effect only when the Camera is in an environmentwith low luminance.
Gamma	Change the image brightness and contrast in a non-linear way. Thehigher the value, the brighter the image.
Flip	Change the display direction of the image. • **Normal:** The normal display of the image. • **Reflection:** The image flips up and down.
OIS	Optical Image Stabilization (OLS) is used to effectively solve the problem of image shaking during use through ISP algorithm and optical technology, thus presenting clearer images. It is on by default. • This function is available on select models. • Optical image stabilization and electronic image stabilization cannot be enabled at the same time.
ELS	Electronic image stabilization (EIS) is used to effectively solve the problem of image shaking during use, thus presenting clearer images. It is Off by default. • This parameter takes effect only when the Device is in an environment with low luminance. • This function is available on select models. • Optical image stabilization and electronic image stabilization cannot be enabled at the same time.
Image Freeze	After enabling this function, the image at the called preset is displayed directly if you call a preset or tour, and no images during the rotation of the camera are displayed.

Step 3 Click **Apply**.

4.3.1.4. Exposure

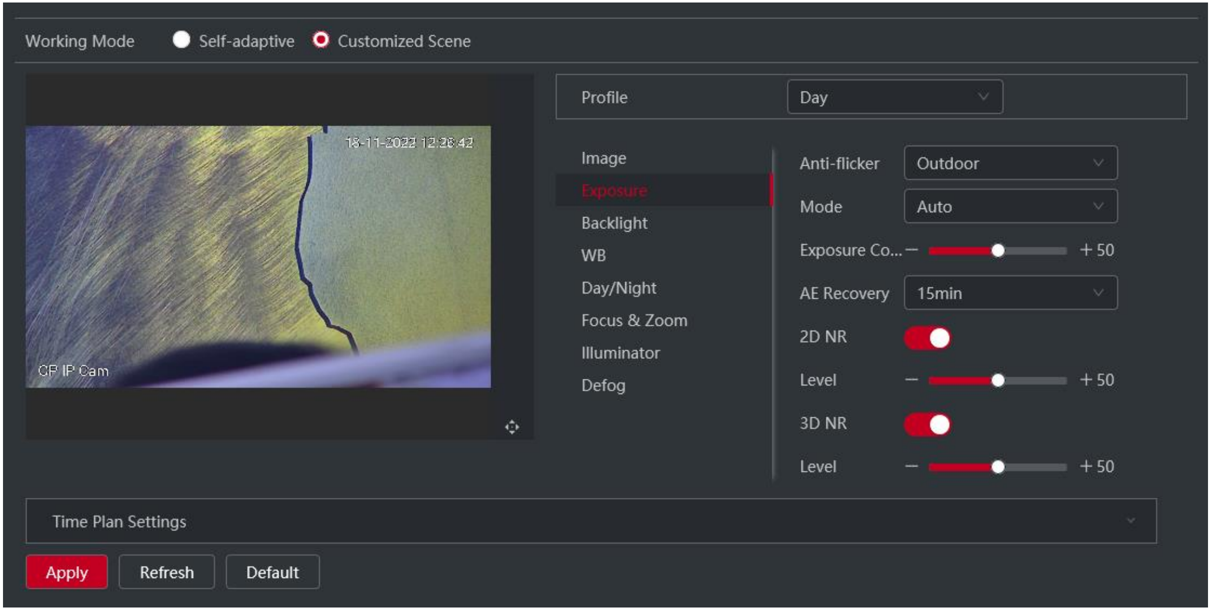
Configure iris and shutter to improve image clarity.

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

Step 1 Click ⚙ on the upper-right corner of the page, and then **select Camera → Image → Exposure**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then configure parameters.

Figure 4-6



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Anti-flicker: Outdoor

Mode: Auto

Exposure Co... − + 50

AE Recovery: 15min

2D NR: on

Level − + 50

3D NR: on

Level − + 50

Table 5

Parameter	Description
Anti-flicker	You can select **50Hz**, **60Hz**, or **Outdoor** from the list. • **50Hz**: The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **60Hz**: The system adjusts the exposure according to ambient light automatically to ensure that stripes do not appear. • **Outdoor**: If you select **Outdoor**, the exposure mode can be set to **Gain** **Priority**, **Shutter Priority** and **Iris Priority**. Different devices supportdifferent exposure modes.
Mode	Set the exposure modes. You can select **Auto**, **Manual**, **Iris Priority**, **ShutterPriority** and **Gain Priority**. The **Auto** mode is selected by default. • **Auto**: Exposure is automatically adjusted according to scene brightness if the overall brightness of images is in the normal exposure range. • **Manual**: You can adjust the **Gain**, **Shutter**, and **Iris** value manually. • **Iris Priority**: You can set the iris to a fixed value, and the Camera will adjustthe shutter value. If the image brightness is not high enough and the shutter value has reached its upper or lower limit, the system adjusts gain value automatically to ensure the image is at an ideal brightness. • **Shutter Priority**: You can customize the shutter range. The Camera automatically adjusts the aperture and gain according to the scene brightness. • **Gain Priority**: Gain value and exposure compensation value can be adjusted manually.

Parameter	Description	
Gain	If you select **Gain Priority** or **Manual**, you can set gain range to automaticallyincrease the gain of the device when the illumination is low, thus obtaining a clear image.	
Shutter	Set the effective exposure time. The smaller the value, the shorter the exposuretime.	
Shutter range	If you select **Shutter Priority** or **Manual**, and select **Shutter** as **Custom**, youcan set the shutter range in ms unit.	
Iris	You can set the camera luminous flux. The larger the Iris value, the brighter the image.	
Exposure Compensation	You can set the exposure compensation value. The value ranges from 0 to 100. The higher the value is, the brighter the image will be.	
Exposure adjustment speed	You can set the exposure adjustment speed. The value ranges from 0 to 100.	
Upper gain threshold	You can set the upper gain threshold of exposure. The value ranges from 0 to 100.	
Low-speed shutter	In a low luminance environment, snapping images by expending the automatic exposure time effectively reduces image noise, but images of moving objects may be blurred.	
Lower threshold of low-speed shutter	You can set the lower threshold of the camera low-speed shutter. The lower the value, the faster the shutter.	
AE Recovery	Automatic exposure is an automated digital camera system that adjusts the aperture and/or shutter speed, based on the external lighting conditions for images and videos. If you have selected an AE Recovery time, the exposure mode will be restored to the previous mode after you adjust the Iris value. There are five options: Off, 5 min, 15 min, 1 hour, and 2 hours.	
2D NR	Average the pixel of a single frame image with other pixels to reduce image noise. The higher the level is, the lower the noise will be, and images appear to be blurrier.	
3D NR	Reduce the noise of multiple-frame (at least two frames) images by using inter-frame information between two adjacent frames in a video. The higher the level is, the lower the noise will be, and the larger the trailing smear will be.	
Level	Noise reduction grade. The value ranges from 0 to 100. The larger the value is, the less the noise will be.	
Advanced NR	You can suppress noise in the time-domainand space-domain based on the video filtermethod.	Some models do not support advanced noisereduction, time domain grade, or space domain grade.
Time domain grade	You can set the time domain grade. The value ranges from 0 to 100.	
Space domain grade	You can set the space domain grade. Thevalue ranges from 0 to 100.	

Step 3 Click **Apply**.

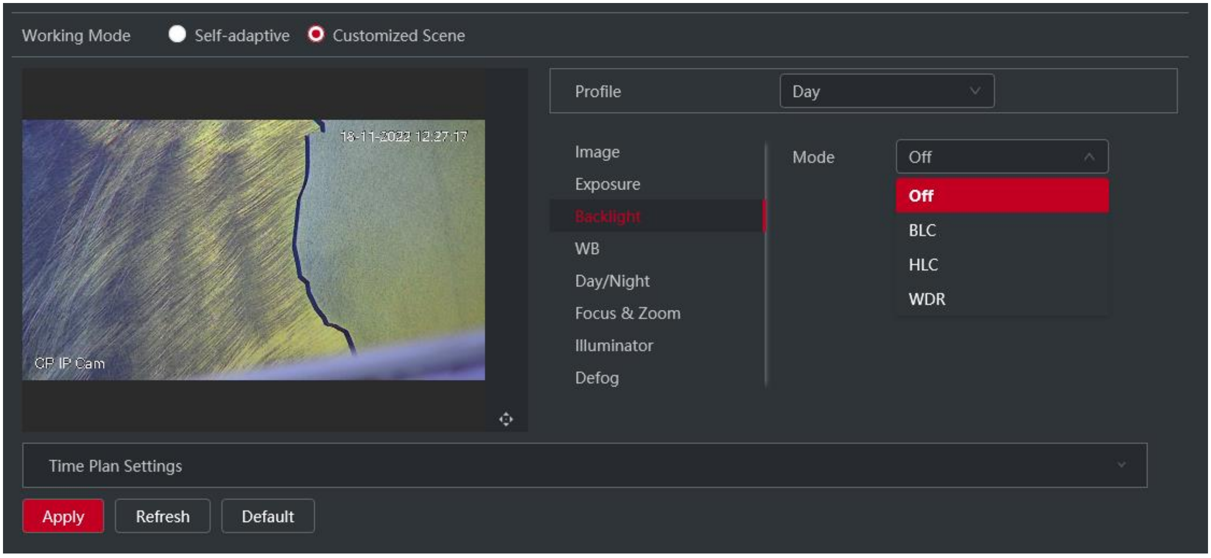
4.3.1.5. Backlight

You can select backlight mode from BLC, WDR and HLS.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → Backlight**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then select a backlight mode from the list.

Figure 4-7



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Mode: Off

Table 6

Parameter	Description
BLC	Enable BLC, the camera can get a clearer image of the dark areas on thetarget when shooting against light. You can select default mode or customized mode. • When in default mode, the system automatically adjusts exposure according to ambient lighting conditions to ensure the clarity of thedarkest area. • When in customized mode, the system auto adjusts exposure only to the set area according to ambient lighting conditions to ensurethe image of the set area is at its ideal brightness.
WDR	The system dims bright areas and compensates for dark areas to ensurethe clarity of all areas. The higher the value is, the stronger the darknesswill be, but the more intense the noise will be. 📖 There might be a few seconds of video loss when the device is switching to WDR mode from other modes.
HLC	Enable HLC when extremely strong light is in the environment (such as atoll station or parking lot). The Camera dims strong lights and reduce the size of Halo zone to lower the brightness of the whole image, so thatthe camera can capture human faces or car plate details clearly. The larger the value is, the more obvious the HLS effect will be.

Step 3 Click **Apply**.

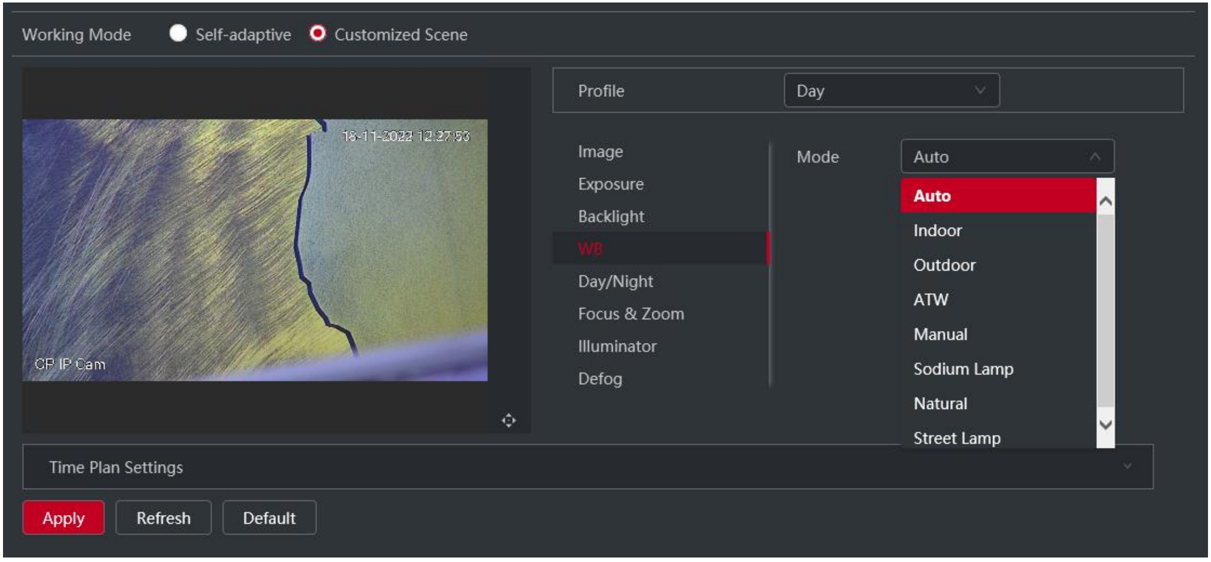
4.3.1.6. White Balance

The white balance function can correct the color deviation to ensure color precision. When in WB mode, white objects are displayed in a white color depending on the environment.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → WB**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then configure **White Balance Mode**.

Figure 4-8



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Mode: Auto

Table 7

Parameter	Description
Auto	The system compensates WB according to color temperature to ensure color precision.
Indoor	The system compensates WB for the general situation of indoor lighting toensure color precision.
Outdoor	The system auto compensates WB to most outdoor environments with natural or artificial light to ensure color precision.
ATW	When the device is tracked, the system auto compensates WB to ensure color precision.
Manual	Configure red gain and blue gain manually. The system auto compensates WB according to color temperature.
Sodium Lamp	The system compensates WB to sodium lamp to ensure color precision.
Natural Light	The system auto compensates WB to environments without artificial light toensure color precision.
Streetlamp	The system compensates WB to ensure color precision in outdoor scenes atnight.

Step 3 Click **Apply**.

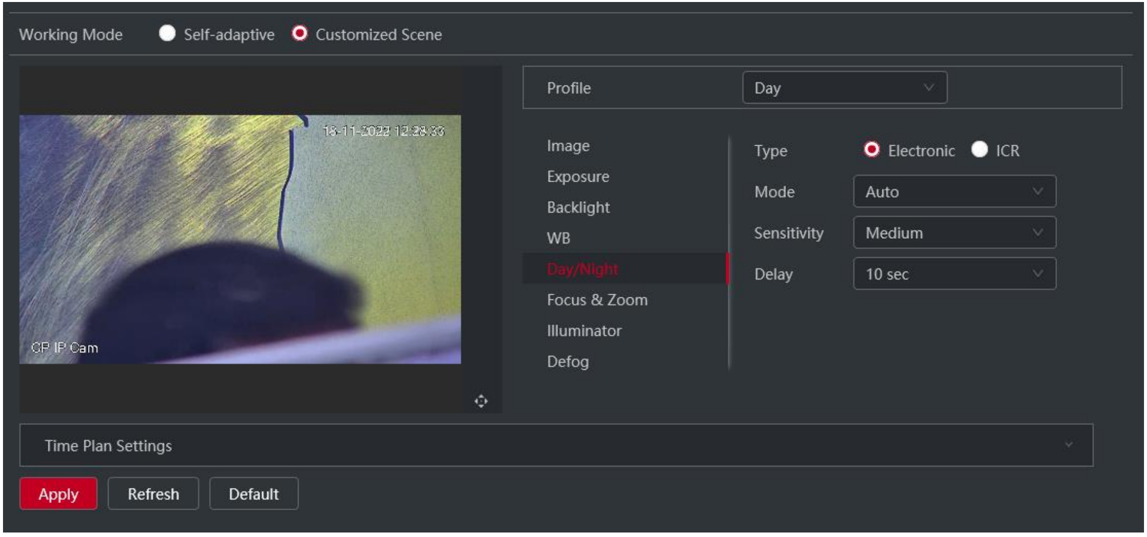
4.3.1.7. Day/Night

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

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → Day/Night**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then configure parameters.

Figure 4-9



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Type: ● Electronic ○ ICR

Mode: Auto

Sensitivity: Medium

Delay: 10 sec

Table 8

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

Step 3 Click **Apply**.

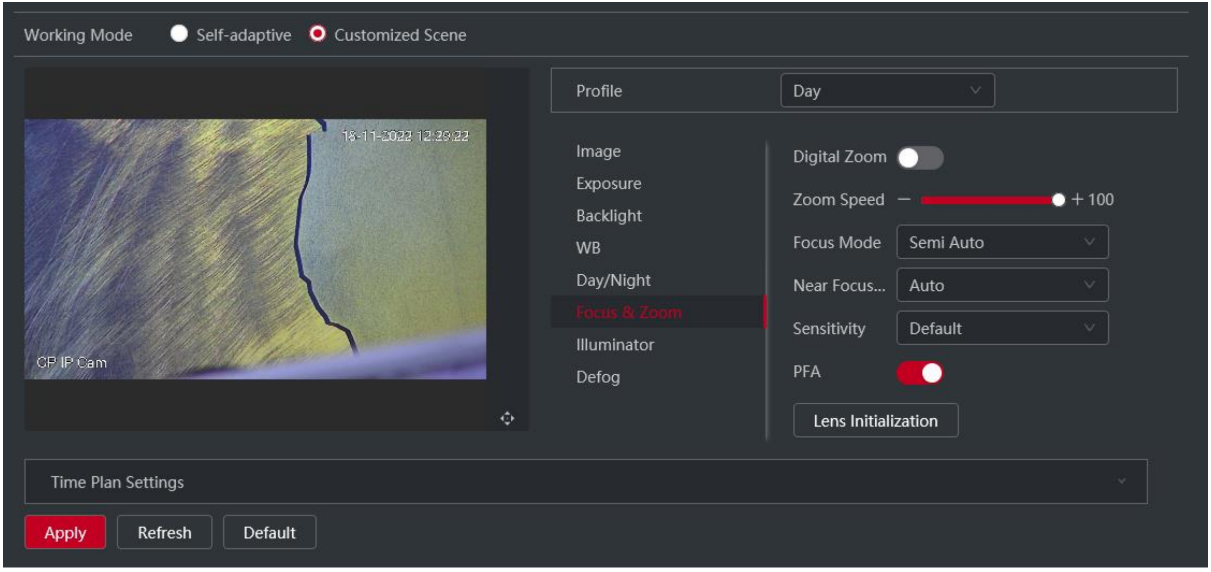
4.3.1.8. Focus & Zoom

Focus & Zoom (digital zoom) refers to capturing a part of the image to magnify it. The higher the magnification is, the blurrier the images will become.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → Focus& Zoom**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and thenconfigure focus & zoom parameters.

Figure 4-10



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Digital Zoom: off

Zoom Speed: 100

Focus Mode: Semi Auto

Near Focus...: Auto

Sensitivity: Default

PFA: on

Table 9

Parameter	Description
Digital Zoom	Click ○ to enable Digital Zoom function. You can use the digital zoom to continue zooming operation even if the optical zoom is at its maximum value.
Zoom Speed	Adjust the zoom speed of the camera. The larger the value, thefaster the zoom speed.
Focus Mode	Set focus mode. • **Auto**: Once there is any movement or change of an object onthe video image and the image turns blurry, the camera will focus again automatically. • **Semi-Auto**: The camera will focus automatically when you click **Focus** or **Zoom** or when a preset change or PTZ switch isdetected. • **Manual**: The Device cannot focus automatically. You need to adjust the focus manually.
Near Focus Limit	Set the near focus limit of the camera. If the focus limit is too small,the camera might get the camera focus on its dome. By changing the focus limit, the focus speed can be changed.
Sensitivity	Trigger the focusing sensitivity of the camera. The higher thesensitivity, the easier to trigger focus.
PFA	Enable **PFA**. When moving the image, the camera automaticallyfocuses for a clear image.

Parameter	Description
Lens Initialization	Click this button, and the lens will be initialized automatically. Thelens will be extended to calibrate the zoom and focus.

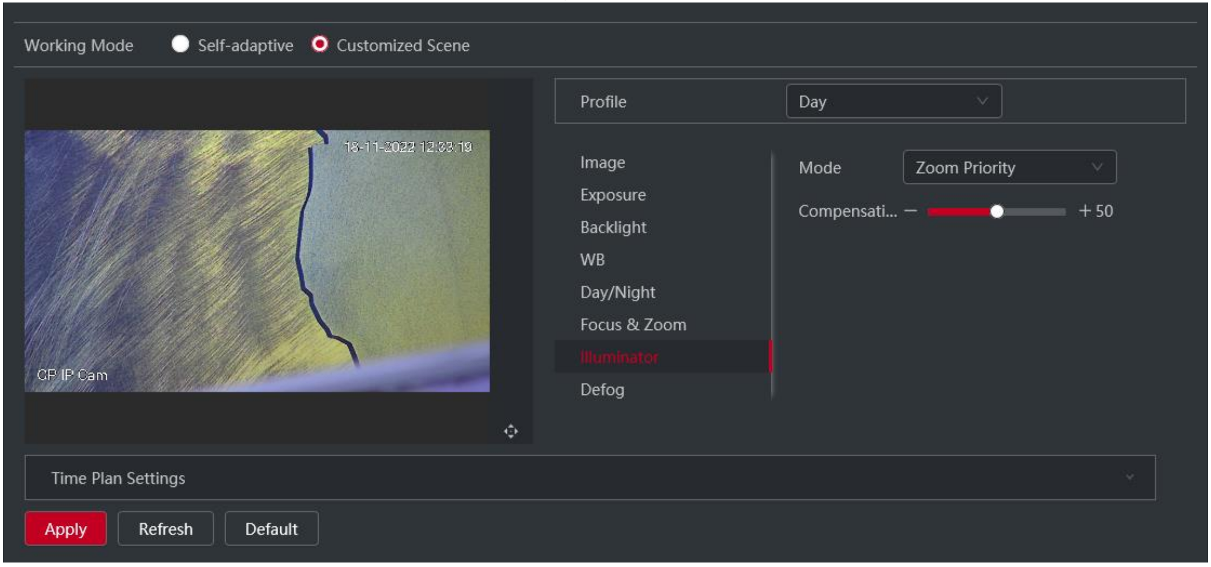
4.3.1.9. Illuminator

This configuration is available only when the device is equipped with illuminator. Common illuminators are classified into IR lights, white light, laser lights, and full-spectrum lights. Different device models support different types of illuminators. This manual is for reference only and might differ from the actual page.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Image → Illuminator**.

Step 2 Select the camera that needs to be configured from the **Channel** drop-down list and then configure illuminator mode.

Figure 4-11



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Mode: Zoom Priority

Compensati... — + 50

Table 10

Parameter		Description
Mode	Manual	Adjust the brightness of illuminator manually, and thenthe system will illuminate the image accordingly.
	Auto	The system adjusts the illuminator intensity according tothe ambient lighting condition. Some devices support setting the brightness upper limit and sensitivity of the illuminator. • Sensitivity: The higher the sensitivity setting, the higher the brightness can turn on the illuminator when the actual scene darkens. When the actual scene becomes bright, a higher brightness is requiredto turn off the illuminator. • Brightness upper limit: If the filling light is too bright, the

Parameter		Description
		center of the image may be overexposed. We recommend adjusting to adjust the brightness upper limit according to the actual scene. The value range is 0-100, and the default is 100.
	Zoom Priority	The system adjusts the illuminator intensity automatically according to the change of the ambient light. You can configure light **Compensation** manually to fine-tune the brightness of the illuminator. • When the ambient light turns darker, the system turns on the low beam lights first, if the brightness is still not enough, it turns on the high beam lights. • When the ambient light turns brighter, the system dims high beam lights until they are off, and then thelow beam lights. • When the focus reaches certain wide angle, the system will not turn on high beam light in order toavoid over-exposure in short distance. Some devices support setting the sensitivity of theilluminator.
	Off	Illuminator is off.

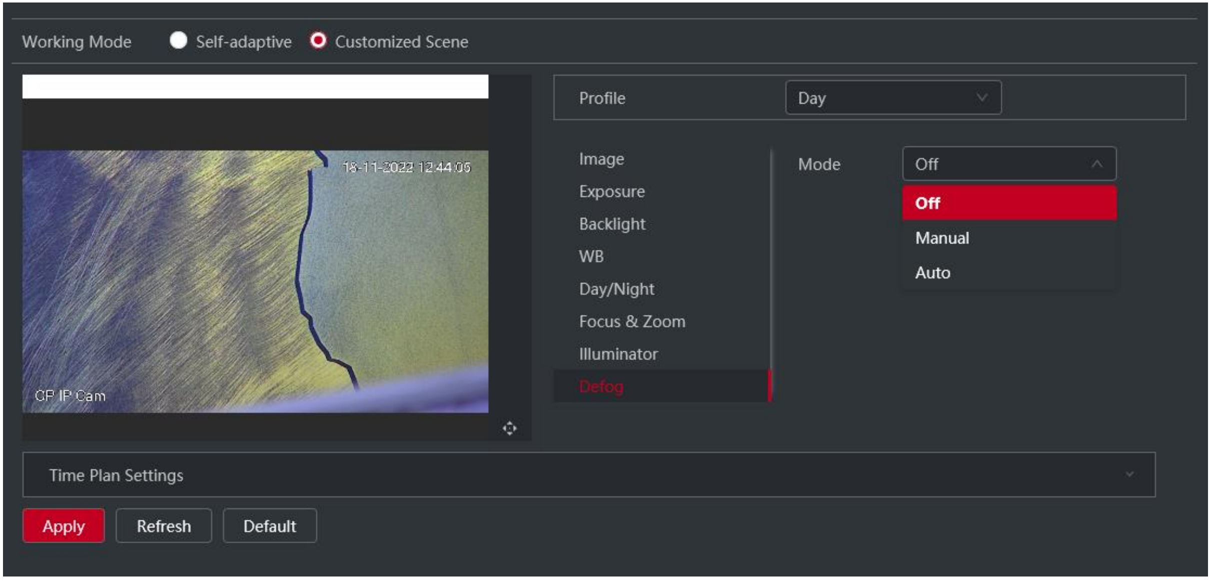
Step 3 Click **Apply**

4.3.1.10. Defog

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

Step 1 Select ⚙ → **Camera** → **Image** → **Defog**

Figure 4-12



Working Mode ○ Self-adaptive ● Customized Scene

Profile: Day

Mode: Off

Step 2 Configure defog parameters.

Table 11

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

Step 3 Click **Apply**.

4.3.2. Encode Parameters

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

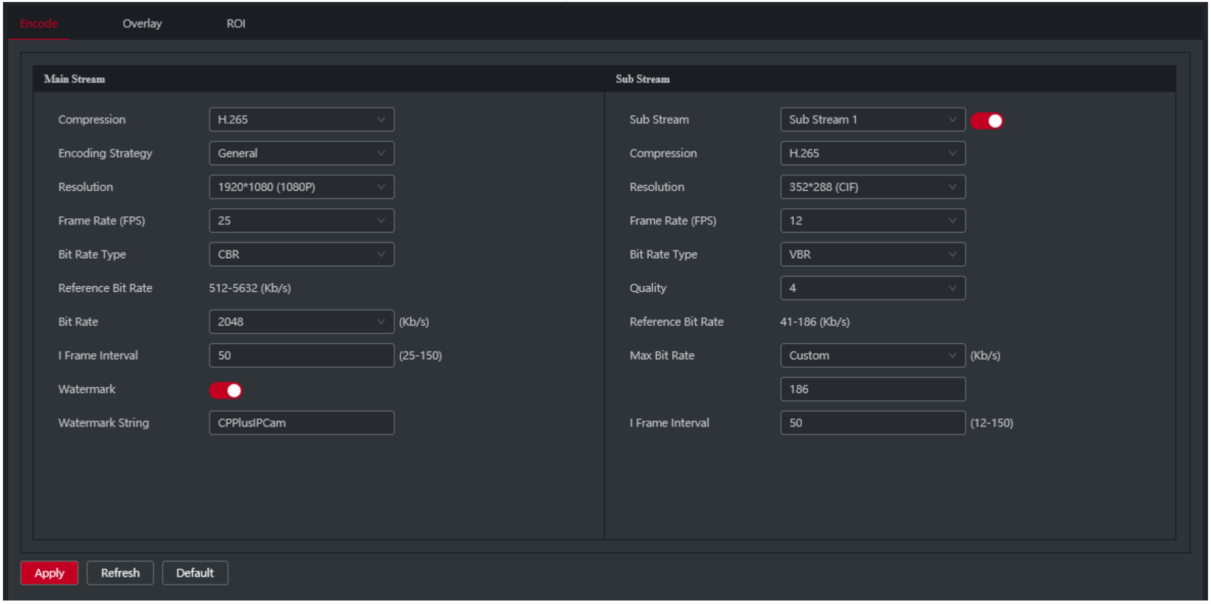
Click **Default**, and the device is restored to default configuration. Click **Refresh** to view the latest configuration.

4.3.2.1. Encode

Configure video stream parameters, such as compression, resolution, frame rate, bit rate type, bitrate, I frame interval, SVC (Scalable Video Coding) and watermark.

Step 1 Select ⚙ → Camera → Encode → Encode

Figure 4-13



Main Stream

Compression	H.265
Encoding Strategy	General
Resolution	1920*1080 (1080P)
Frame Rate (FPS)	25
Bit Rate Type	CBR
Reference Bit Rate	512-5632 (Kb/s)
Bit Rate	2048 (Kb/s)
I Frame Interval	50 (25-150)
Watermark	●
Watermark String	CPPlusIPCam

Sub Stream

Sub Stream	Sub Stream 1 ●
Compression	H.265
Resolution	352*288 (CIF)
Frame Rate (FPS)	12
Bit Rate Type	VBR
Quality	4
Reference Bit Rate	41-186 (Kb/s)
Max Bit Rate	Custom (Kb/s) 186
I Frame Interval	50 (12-150)

Step 2 Configure encode parameters.

Table 12

Parameter	Description
Sub Stream	Click ● to enable sub stream, it is enabled by default. 📖 You can enable multiple sub streams simultaneously.
Compression	Select encode mode. • **H.264**: It includes **H.264B** (baseline profile encode mode), **H.264** (main profile encode mode) and **H.264H** (high profileencode mode). Under the same image quality, the bandwidth of the threedecreases in turn. • **H.265**: Main profile encode mode. Compared with H.264, itrequires smaller bandwidth. • **MJPEG**: Under this mode, the image requires high bit rate to ensure clarity, you are recommended to set the **Bit Rate** to thebiggest value in the **Reference Bit Rate**.
Smart Codec	Click to enable smart codec to improve video compressibility and save storage space. 📖 After smart codec is enabled, the device would stop supporting thethird bit stream, ROI, and smart event detection.
Resolution	The resolution of the video. The higher the value is, the clearer theimage will be, but the bigger the required bandwidth will be.
Frame Rate (FPS)	The number of frames in one second of video. The higher the value is,the clearer and smoother the video will be.
Bit Rate Type	The bit rate control type during video data transmission. You canselect bit rate type from: • **CBR** (Constant Bit Rate): The bit rate changes a little and keepsclose to the defined bit rate value. • **VBR** (Variable Bit Rate): The bit rate changes as monitoring scene changes. 📖 The **Bit Rate Type** can only be set as **CBR** when **Encode Mode** is setas **MJPEG**.
Quality	This parameter can be configured only when the **Bit Rate Type** is setas **VBR**. The better the quality is, but the bigger the required bandwidth will be.
Reference Bit Rate	The most suitable bit rate value range recommended to useraccording to the defined resolution and frame rate.
Max Bit Rate	This parameter can be configured only when the **Bit Rate Type** is setas **VBR**. You can select the value of the **Max Bit Rate** according to the **Reference Bit Rate** value. The bit rate then changes as monitoring scene changes, but the max bit rate keeps close to the defined value.
Bit Rate	This parameter can be configured only when the **Bit Rate Type** is setas **CBR**. Select bit rate value in the list according to actual condition.
I Frame Interval	The number of P frames between two I frames, and the **I Frame Interval** range changes as **FPS** changes. It is recommended to set **IFrame Interval** twice as big

Parameter	Description
	as **FPS**.
SVC	Scaled video coding, is able to encode a high-quality video bit stream that contains one or more subset bit streams. When sending stream, to improve fluency, the system will quit some data of relatedlays according to the network status. ● 1: The default value, which means that there is no layeredcoding. ● 2, 3 and 4: The lay number that the video stream is packed.
Watermark	You can verify the watermark to check if the video has beentampered. ● Click ● to enable watermark function. ● Enter watermark string. The string is Digital CCTV by default.
Watermark String	

Step 3 Click **Apply.**

4.3.2.2. Overlay

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

4.3.2.2.1. Privacy Masking

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

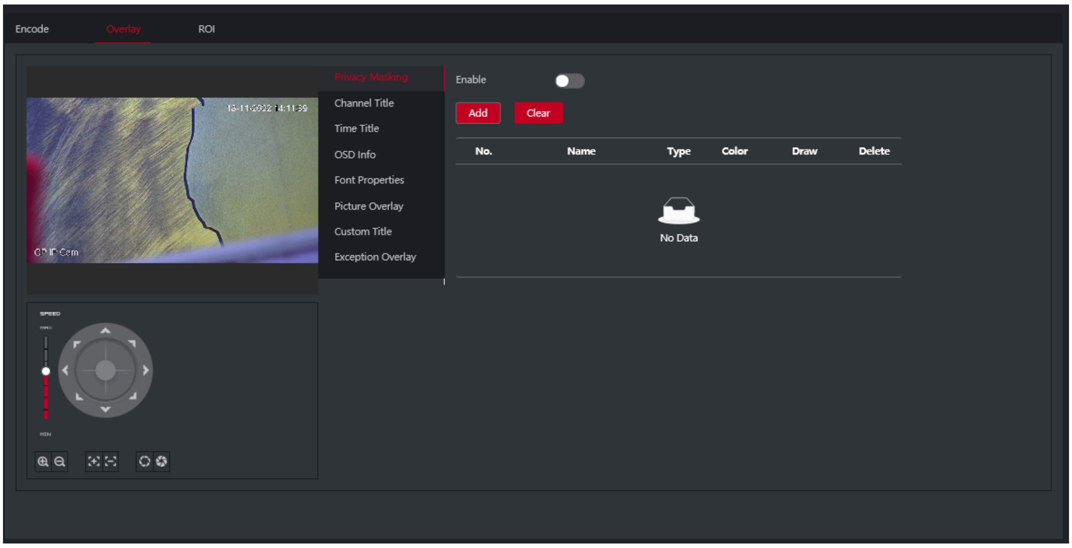
Step 1 Select ⚙ →**Camera** →**Encode** →**Privacy Masking**.

Step 2 Select **Enable**.

Step 3 Click **Add**, select **Color Block** or **Mosaic**, and then draw the blocks on the screen.

- You can draw 8 blocks at most. The same screen can add up to 4 mosaic blocks.
- Click **Clear** to delete all blocks; select the block you want to delete, click Clear to deletethe corresponding block.

Figure 4-14



Step 4 Adjust block size to protect the privacy.

Step 5 Click **Apply**.

4.3.2.2.2. Channel Title

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

Step 1 Select ⚙ → **Camera** → **Encode** → **Overlay** → **Channel Title**.

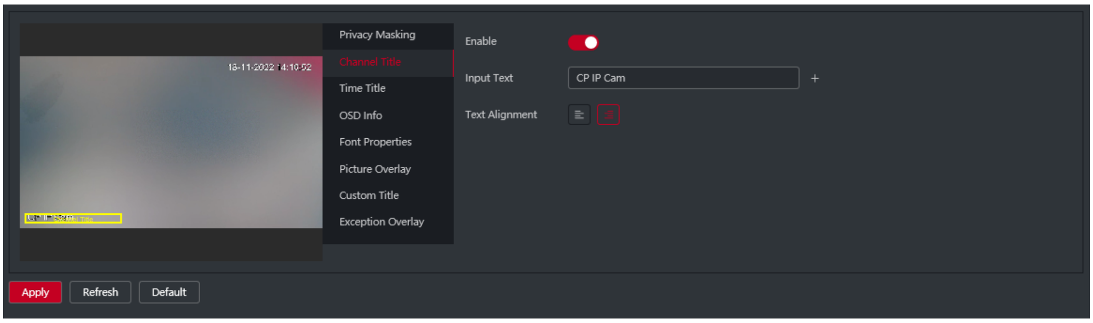
Step 2 Select **Enable**.

Step 3 Configure channel title, and then select the text alignment.

📖

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

Figure 4-15



Enable ●

Input Text CP IP Cam +

Text Alignment

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

Step 5 Click **Apply**.

4.3.2.2.3. Time Title

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

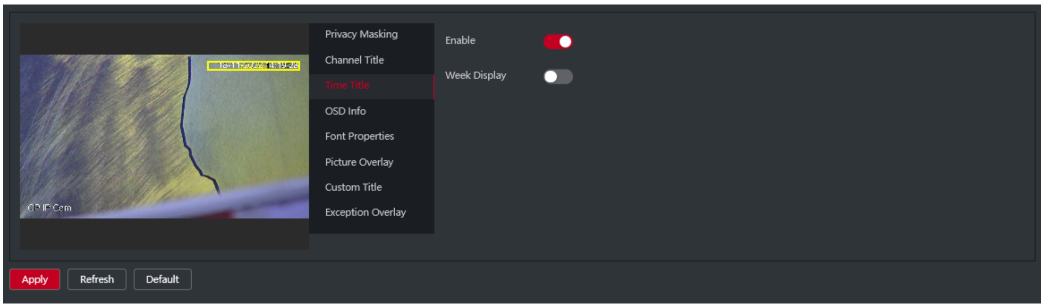
Step 1 Select ⚙ → **Camera** → **Encode** → **Overlay** → **Time Title**.

Step 2 Select **Enable**.

Step 3 (Optional) Select **Week Display** to display the day of week on the video image.

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

Figure 4-16



Enable ●

Week Display ○

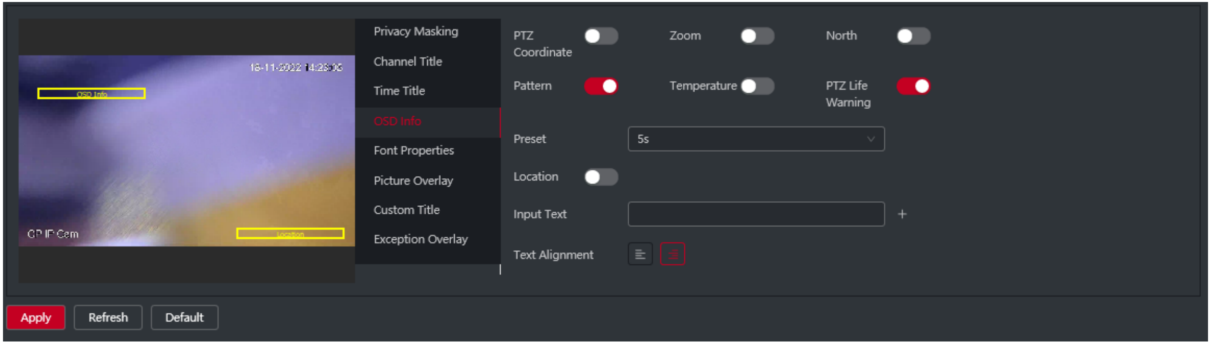
Step 5 Click **Apply**.

4.3.2.2.4. OSD Info

If you want to represent such information in video images as preset dots, PTZ/geography location, zoom and touring pattern, you can enable this function.

Step 1 Select ⚙ → **Camera** → **Encode** → **Overlay** → **OSD Info**

Figure 4-17



PTZ Coordinate ○ Zoom ○ North ○
Pattern ● Temperature ○ PTZ Life Warning ●
Preset 5s
Location ○
Input Text +
Text Alignment

Step 2 Configure OSD information.

Table 13

Parameter	Description
Presets	Select **Enable**, and the preset name is displayed on the imagewhen the camera turns to the preset, and it will disappear 3 s later.
PTZ Coordinates	Select **Enable**, and the PTZ coordinates information is displayedon the image.
Zoom	Select **Enable** and the zoom information is displayed on theimage.
North	Select **Enable**, and the north direction is displayed on the image.When you enable the due north orientation function, the systemwill prompt you to restart the PTZ.
Pattern	Select **Enable**, and the pattern information is displayed on theimage.
RS485	Select **Enable**, and the RS485 information is displayed on theimage.
Location	Select **Enable**, and the geographical location is displayed in thetext.
Text Alignment	Set the alignment mode of the displayed information on theimage.

Step 3 Move the OSD box to the position that you want on the image.

Step 4 Click **Apply**.

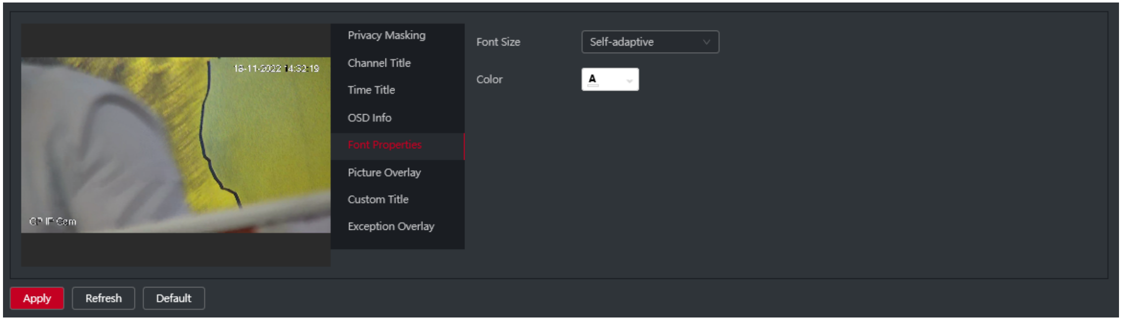
4.3.2.2.5. Font Properties

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

Step 1 Select ⚙ → **Camera** → **Encode** → **Overlay** → **Font Properties**.

Step 2 Select the font color and size. You can set the RGB value to customize the font color.

Figure 4-18



Font Size: Self-adaptive

Color: A

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

After saving the settings, the color and size of the font in the video image changeaccordingly.

4.3.2.2.6. Picture Overlay

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

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

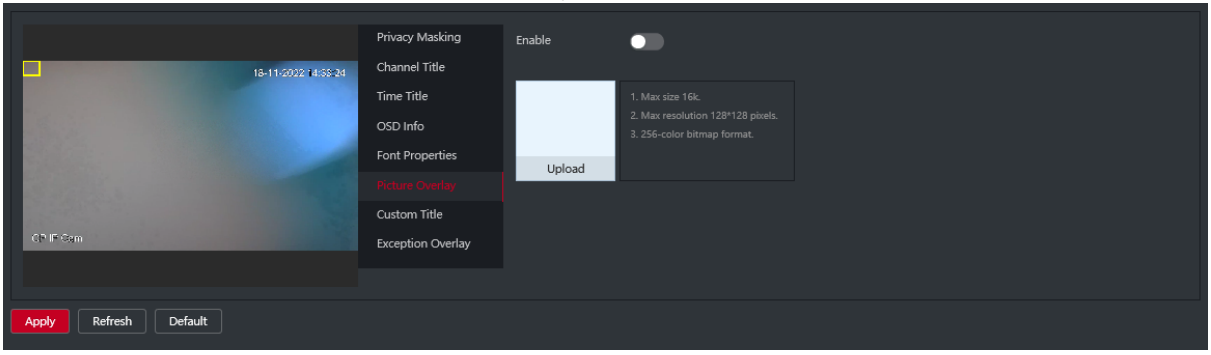
Step 1 Select ⚙ → **Camera** → **Encode** → **Overlay** → **Picture Overlay**.

Step 2 Select channel and then select **Enable**.

Step 3 Click **Upload**, and then select the overlaid image.

The image shows in the **Picture Preview**.

Figure 4-19



1. Max size 16k.
2. Max resolution 128*128 pixels.
3. 256-color bitmap format.

Step 4 You can move the overlaid image to the position you want in the image.

Step 5 Click **Apply**.

4.3.2.2.7. Custom Title

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

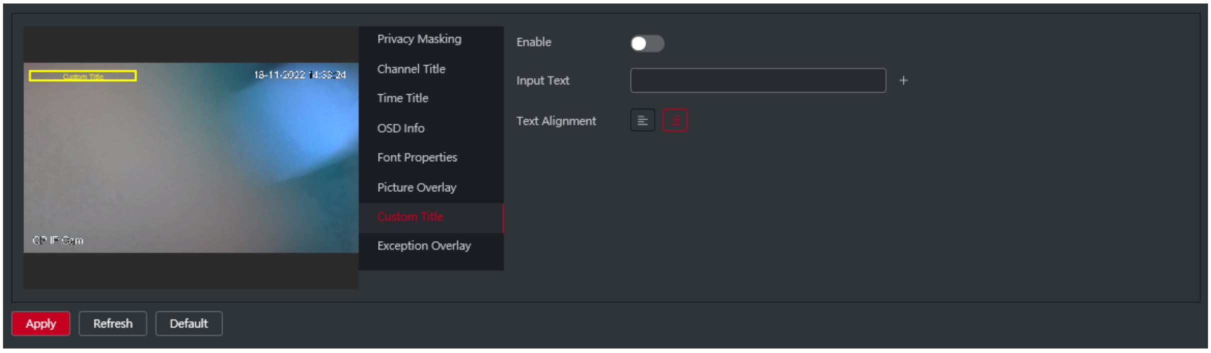
Step 1 Select ⚙ →**Camera**→**Encode**→**Overlay**→**Custom Title**.

Step 2 Select **Enable**.

Step 3 Configure custom overlay, and then select the text alignment.

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

Figure 4-20



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

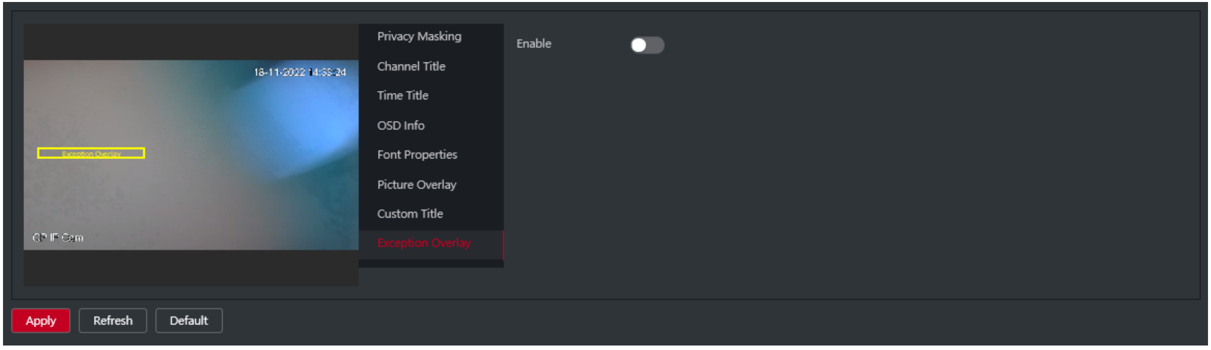
Step 5 Click **Apply**.

4.3.2.2.8. Exception Overlay

You can enable this function to display the overlaid abnormal information of the cameras on thescreen.

Step 1 Select → **Camera** → **Encode** → **Overlay** → **Exception Overlay**.

Figure 4-21



Step 2 Select **Enable**, and then click **Apply**.

4.3.2.3. ROI

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

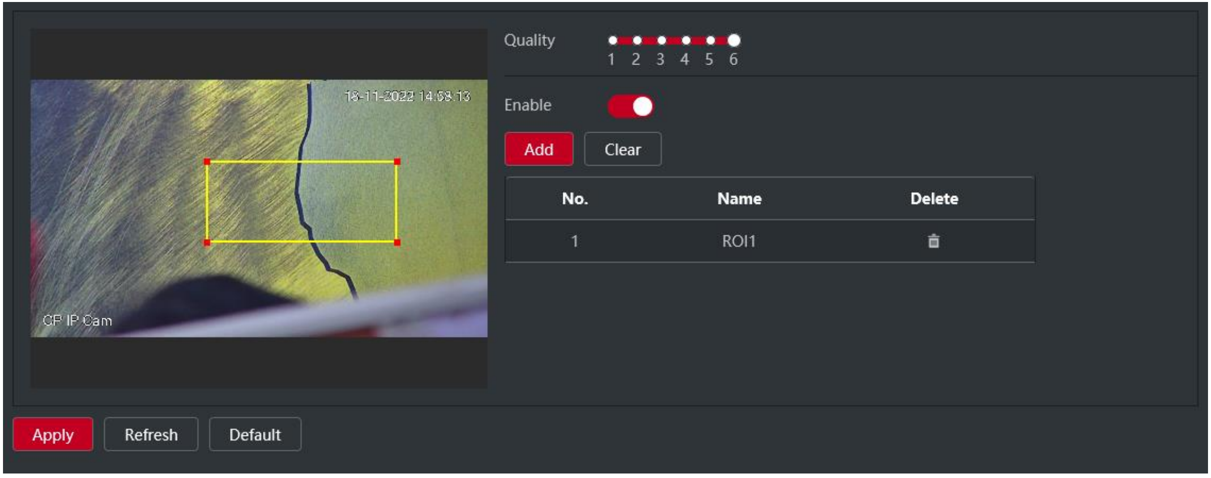
Step 1 Select → **Camera** → **Encode** → **ROI**.

Step 2 Select channel, and then select **Enable**.

Step 3 Click **Add**, draw an area on the image, and then configure the image quality of ROI.

- You can draw 4 area boxes at most.
- The higher the image quality value is, the better the quality will be.
- Click **Clear** to delete all the area boxes; select one box, and then click 🗑 to delete it

Figure 4-22



Quality 1 2 3 4 5 6

Enable

No.	Name	Delete
1	ROI1	🗑

Step 4 Click **Apply**.

4.3.3. Audio

Configure the noise filter and sampling frequency of the Camera. When enabling audio encoding,the network stream contains both audio and video, otherwise, it is only video stream.

You need to click ⚙ on the upper-right corner of the page, and then select **Camera → Encode → Encode** to enable the video stream of Sub Stream before enabling the audio.

Step 1 Click ⚙ on the upper-right corner of the page, and then select **Camera → Audio**.

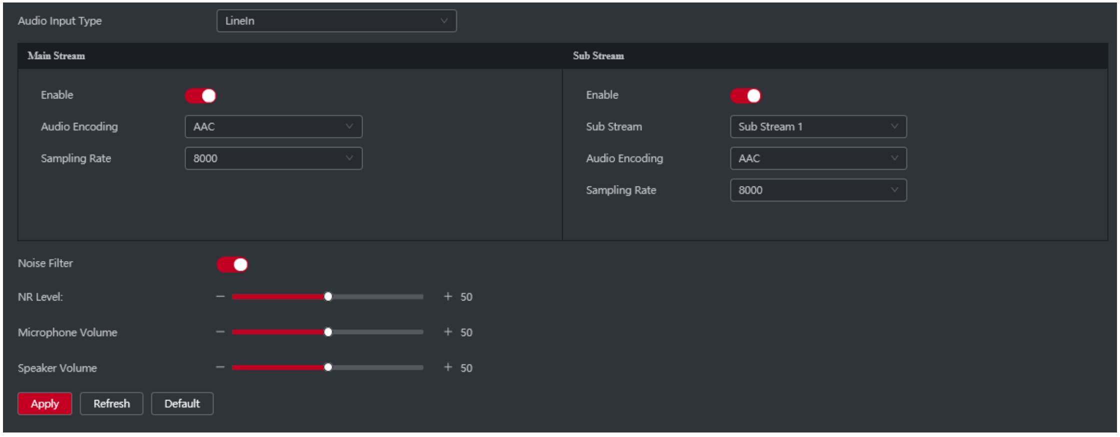
Step 2 Select **Mainstream** or **Sub Stream** to enable audio encoding.

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

⚠

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

Figure 4-23



Audio Input Type: LineIn

Main Stream

Enable: ●

Audio Encoding: AAC

Sampling Rate: 8000

Sub Stream

Enable: ●

Sub Stream: Sub Stream 1

Audio Encoding: AAC

Sampling Rate: 8000

Noise Filter: ●

NR Level: 50

Microphone Volume: 50

Speaker Volume: 50

Step 3 Configure audio parameters.

Table 14

Parameter	Description
Compression	Configure audio compression. The configured audio encode mode appliesto both audio and intercom. The default value is recommended.
Sampling Frequency	Sampling number per second. The higher the sampling frequency is, themore the sample in a second will be, and the more accuracy the restored signal will be.
Noise Filter	Enable this function, and the system automatically filters ambient noise.
Microphone Volume	Adjusts microphone volume.
Speaker Volume	Adjusts speaker volume.

Step 4 Click **Apply**.

4.4. Network

This section introduces network configuration.

4.4.1. TCP/IP

4.4.1.1. TCP/IP

You can configure IP address and DNS (Domain Name System) server and other information according to network planning to ensure the device is properly connected to other devices in thenetwork.

Prerequisites

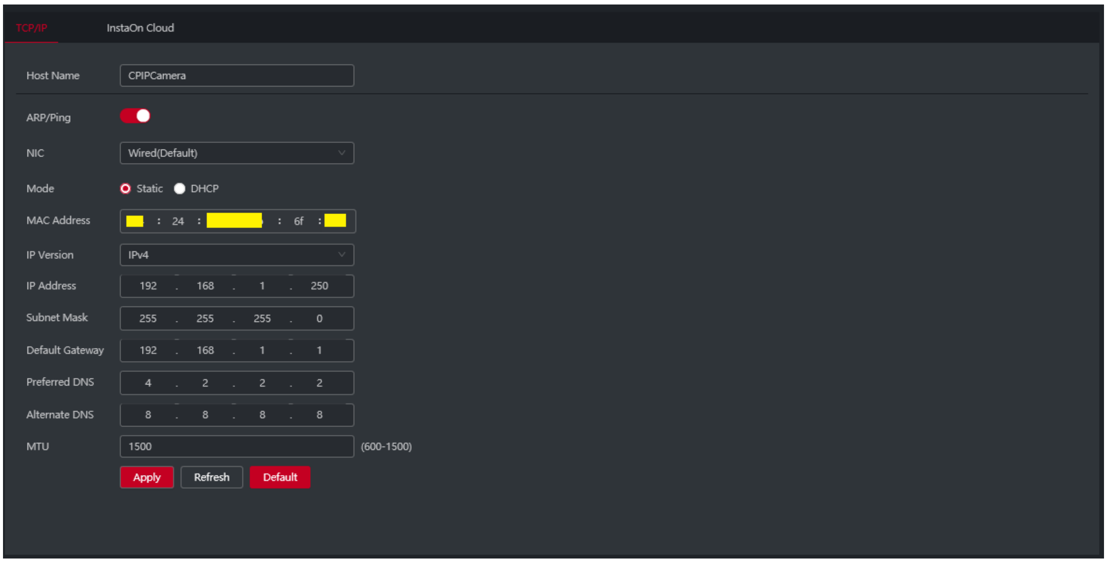
The camera has connected to the network.

Procedure

Step 1 Select ⚙ → **Network** → **TCP/IP**.

Step 2 Configure TCP/IP parameters.

Figure 4-24



Host Name: CPIPCamera

ARP/Ping: on

NIC: Wired(Default)

Mode: ● Static ○ DHCP

MAC Address: [redacted] : 24 : [redacted] : 6f : [redacted]

IP Version: IPv4

IP Address: 192 . 168 . 1 . 250

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 1 . 1

Preferred DNS: 4 . 2 . 2 . 2

Alternate DNS: 8 . 8 . 8 . 8

MTU: 1500 (600-1500)

Table 15

Parameter	Description
Host Name	Enter the host name. The maximum length is 32 characters.
ARP/Ping	Click to enable ARP/Ping to set IP address service. Get the camera MAC address, and then you can change and configure the device IP address with ARP (Address Resolution Protocol) /ping command. This is enabled by default. During restart, you will have no more than 2 minutes to configure the device IP address by a ping packet with certain length, the server will be turned off in 2 minutes, or it will be turned off immediately after the IP address is successfully configured. If this is not enabled, the IP address cannot be configuredwith ping packet.

Parameter	Description
NIC	Select the Ethernet card that need to be configured, and the defaultone is **Wire**.
Mode	The mode that the camera gets IP: ● **Static** Configure **IP Address**, **Subnet Mask**, and **Default Gateway** manually, and then click **Save**, the login page with the configuredIP address is displayed. ● **DHCP** (Dynamic Host Configuration Protocol) When there is DHCP server in the network, select **DHCP**, and thecamera acquires IP address automatically.
MAC Address	Displays host MAC (Media Access Control) address.
IP Version	Select **IPv4** or **IPv6**.
IP Address	When you select **Static** as **Mode**, enter the IP address and subnetmask according to the network plan. 📖 ● IPv6 does not have a subnet mask. ● The default gateway must be on the same network segment with the IP address.
Subnet Mask	
Default Gateway	
Preferred DNS	IP address of the preferred DNS.
Alternate DNS	IP address of the alternate DNS.

Step 3 Click **Apply**.

Related Operations

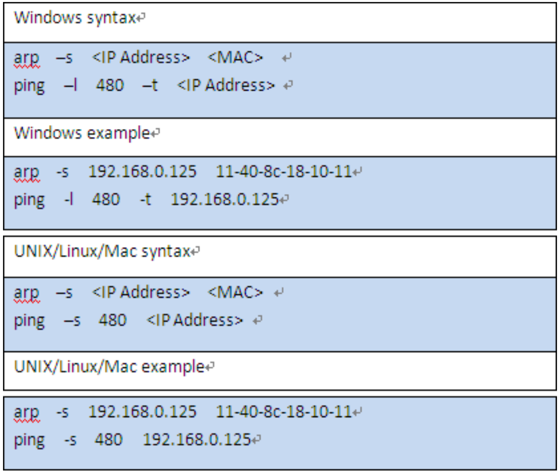
Configuring IP address with ARP/Ping.

a. Keep the camera that needs to be configured and the PC within the same local network, andthen get a usable IP address.

b. Get the MAC address of the camera from device label.

c. Open command editor on the PC and enters the following command.

Figure 4-25



Windows syntax

```
arp  –s  <IP Address>  <MAC>
ping  –l  480  –t  <IP Address>
```

Windows example

```
arp  -s  192.168.0.125  11-40-8c-18-10-11
ping  -l  480  -t  192.168.0.125
```

UNIX/Linux/Mac syntax

```
arp  –s  <IP Address>  <MAC>
ping  –s  480  <IP Address>
```

UNIX/Linux/Mac example

```
arp  -s  192.168.0.125  11-40-8c-18-10-11
ping  -s  480  192.168.0.125
```

d. Restart the Camera.

e. Check the PC command line, if information such as **Reply from 192.168.0.125…**is displayed, theconfiguration succeeds.

f. Enter *http://(IP address)* in the browser address bar to log in.

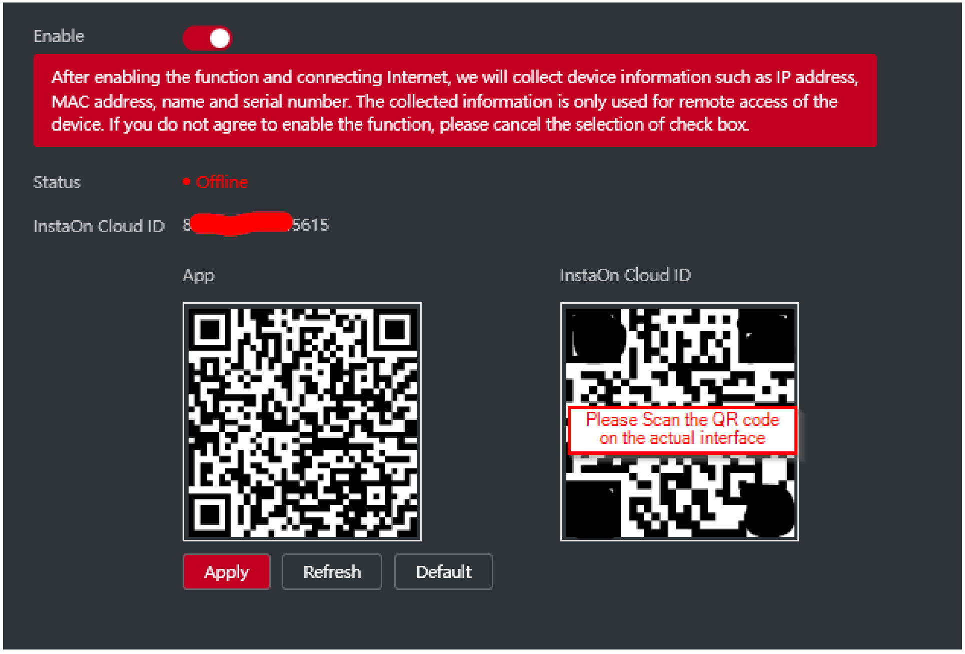
4.4.1.2. InstaOn Cloud

InstaOn Cloud technology enables users to manage devices easily without requiring DDNS, portmapping or transit server.

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

Step 1 Select ⚙ → Network → TCP/IP → InstaOn Cloud.

Figure 4-26



Enable

After enabling the function and connecting Internet, we will collect device information such as IP address, MAC address, name and serial number. The collected information is only used for remote access of the device. If you do not agree to enable the function, please cancel the selection of check box.

Status ● Offline

InstaOn Cloud ID 8[redacted]5615

App

InstaOn Cloud ID

Please Scan the QR code on the actual interface

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

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

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

Step 4 Scan the QR code on the **InstaOn Cloud** page.

Step 5 Follow the instructions to finish the settings.

4.4.2. Port

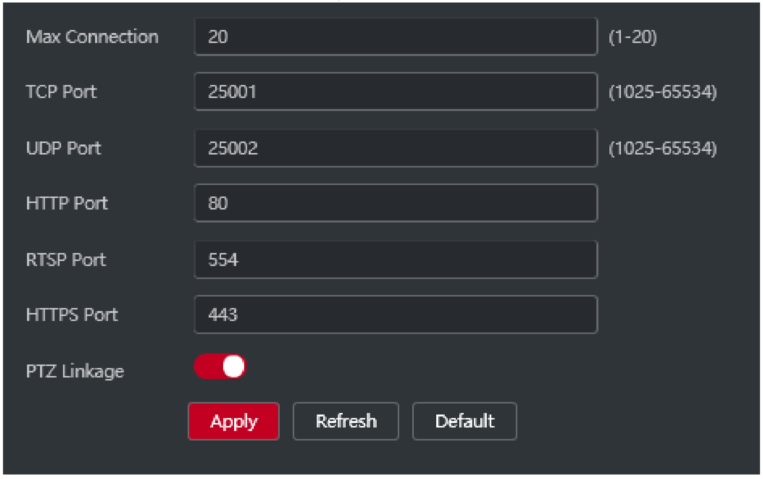
Configure the port numbers and the maximum number of users (includes web, platform client andmobile phone client) that can connect to the device simultaneously.

Step 1 Select ⚙ →**Network**→**Port**.

Step 2 Configure port parameters.

- The configuration of **Max Connection**, **RTSP Port**, **RTMP Port**, **HTTPS Port** take effect immediately, and others will take effect after reboot.
- 0—1024, 1900, 3800, 5000, 5050, 9999, 25001, 37780—37880, 39999, 42323 are occupied for specific uses, do not use them.
- Do not use the same value of any other port during port configuration.

Figure 4-27



Max Connection: 20 (1-20)

TCP Port: 25001 (1025-65534)

UDP Port: 25002 (1025-65534)

HTTP Port: 80

RTSP Port: 554

HTTPS Port: 443

PTZ Linkage: ●

Table 16

Parameter	Description
Max Connection	The max number of users (web client, platform client or mobile phone client) that can connect to the device simultaneously. Thevalue is 10 by default.
TCP Port	Transmission Control Protocol port. The value is 25001 by default.
UDP Port	User Datagram Protocol Port. The value is 25002 by default.
HTTP Port	Hyper Text Transfer Protocol Port. The value is 80 by default. If it is configured to another value, you need to add the new port numberto the IP address when logging in to the system using a browser.
RTSP Port	• Real Time Streaming Protocol Port, and the value is 554 by default. If you play live view with QuickTime, VLC (Video LAN Client) or Blackberry smart phone, the following URL (Uniform Resource Locator) format is available. • When the URL format requires RTSP, you need to specify channel number and bit stream type in the URL, and also username and password if needed. • When playing live view with Blackberry smart phone, you need to turn off the audio, and then set the codec mode to H.264B and resolution to CIF.

Parameter	Description
	URL format example: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0 **Among that:** • Username: The username, such as admin. • Password: The password, such as admin. • IP: The device IP, such as 192.168.1.112. • Port: Leave it as default (554). • Channel: The channel number, which starts from 1. For example, if you are using channel 2, then the channel=2. • Subtype: The bit stream type; 0 means mainstream (Subtype=0) and 1 means sub stream (Subtype=1). **Example:** If you require the sub stream of channel 2 from a certain device, then the URL should be: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&= 1 If username and password are not needed, then the URL can be: rtsp://ip:port/cam/realmonitor?channel=11&=0
RTMP Port	Real Time Messaging Protocol Port. This is the port that RTMP provides service. It is 1935 by default.
HTTPS Port	Hyper Text Transfer Protocol over Secure Socket Layer Port. It is 443 by default.

Step 3 Click **Apply**.

4.4.3. PPPoE

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

Prerequisites

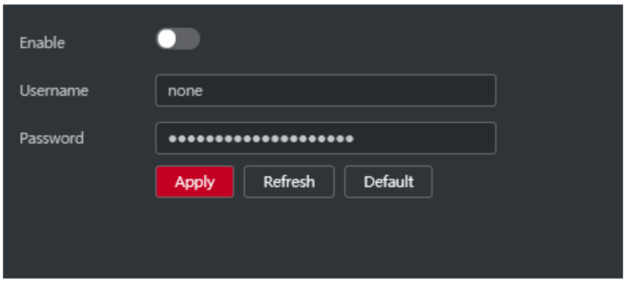
- The camera has connected to the network.
- You have gotten the account and password from ISP (Internet Service Provider).

Procedure

Step 1 Select ⚙ → **Network** → **PPPoE**.

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

Figure 4-28



Enable ○

Username: none

Password: ••••••••••••••••••••

🕮

- Disable UPnP while using PPPoE.
- After making PPPoE connection, the device IP address cannot be modified throughweb page.

Step 3 Click **Apply**.

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

4.4.4. DDNS

Properly configure DDNS (Dynamic Domain Name System), and then the domain name on the DNSserver matches your IP address and the matching relation refreshes in real time. You can always access the camera with the same domain name no matter how the IP address changes.

Prerequisites

Check the type of DNS server supported by the camera.

Procedure

Step 1 Select ⚙ → **Network** → **DDNS**.

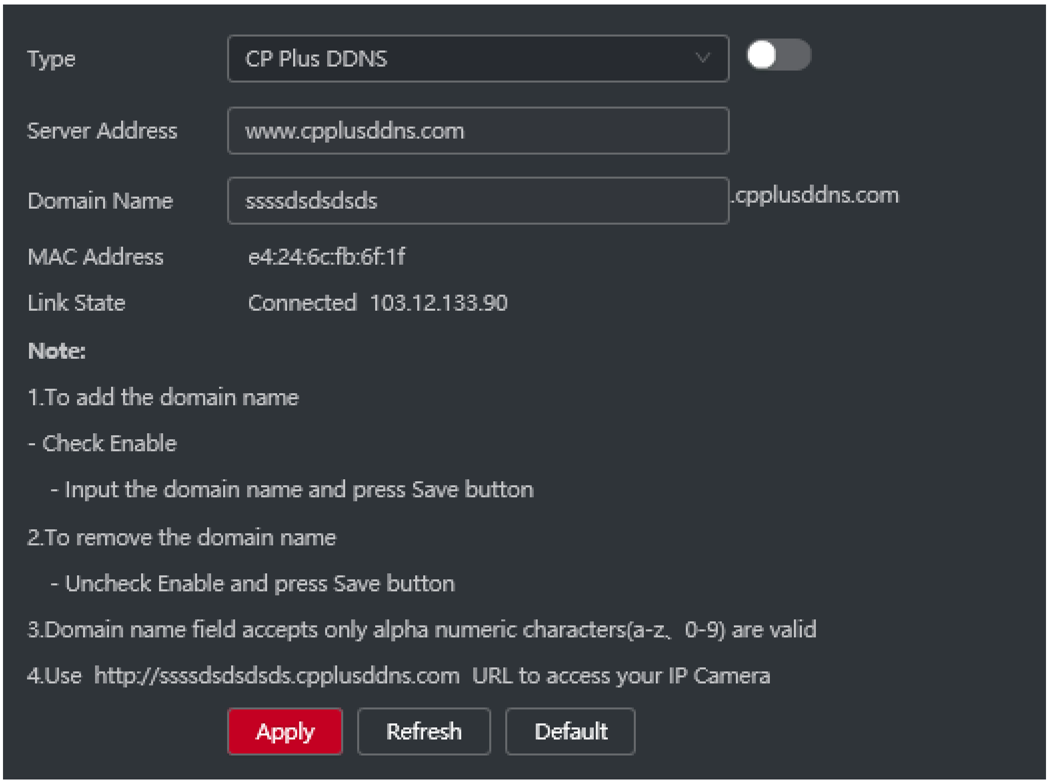
🕮

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

Step 2 Click ⚪ to enable the function.

Step 3 Configure DDNS parameters.

Figure 4-29



Type: CP Plus DDNS

Server Address: www.cpplusddns.com

Domain Name: sssdsdsdsds .cpplusddns.com

MAC Address: e4:24:6c:fb:6f:1f

Link State: Connected 103.12.133.90

Note:

1.To add the domain name

- Check Enable

  - Input the domain name and press Save button

2.To remove the domain name

  - Uncheck Enable and press Save button

3.Domain name field accepts only alpha numeric characters(a-z、 0-9) are valid

4.Use http://sssdsdsdsds.cpplusddns.com URL to access your IP Camera

Table 17

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

Step 4 Click **Apply**.

Result

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

4.4.5. Email

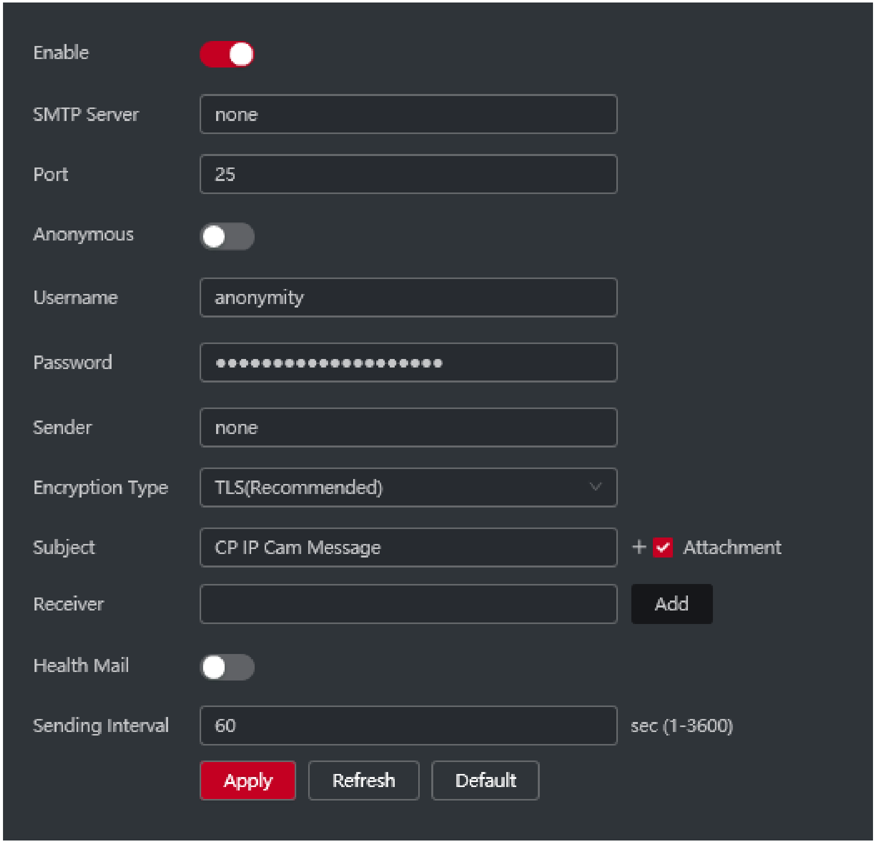
Configure email parameter and enable email linkage. The system sends email to the defined address when the corresponding alarm is triggered.

Step 1 Select ⚙ → **Network** → **Email**.

Step 2 Click ○ to enable the function.

Step 3 Configure email parameters.

Figure 4-30



Enable: ●
SMTP Server: none
Port: 25
Anonymous: ○
Username: anonymity
Password: ••••••••••••••••••••
Sender: none
Encryption Type: TLS(Recommended)
Subject: CP IP Cam Message + ☑ Attachment
Receiver:
Health Mail: ○
Sending Interval: 60 sec (1-3600)

Table 18

Parameter	Description
SMTP Server	SMTP (Simple Mail TransferProtocol) server address.
Port	The port number of the SMTPserver.
Username	The account of SMTP server.
Password	The password of SMTP server.
Anonymous	Click ○ , and the sender's information is not displayed in the email.
Sender	Sender’s email address.
Encryption Type	Select from **None**, **SSL (Secure Sockets Layer)** and **TLS (TransportLayer Security)**.

Parameter	Description
Subject	Enter maximum 63 characters in Chinese, English, and Arabic numbers.Click to select title type, including **Device Name**, **Device ID**, and **Event Type**, and you can set maximum 2 titles.
Attachment	Select the checkbox to support attachment in the email.
Receiver	• Receiver’s email address. Supports 3 addresses at most. • After entering the receiver's email address, click **Test** to testwhether the emails can be sent and received successfully.
Health Mail	The system sends test mail to check if the connection is successfully configured. Click ○ and configure the Sending Interval, and then the system sends test mail as the set interval. 🕮 Sending interval of health mail ranges from 1 second to 3,600 seconds.
Sending Interval	

Step 4 Click **Apply**.

4.4.6. UPnP

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

Prerequisites

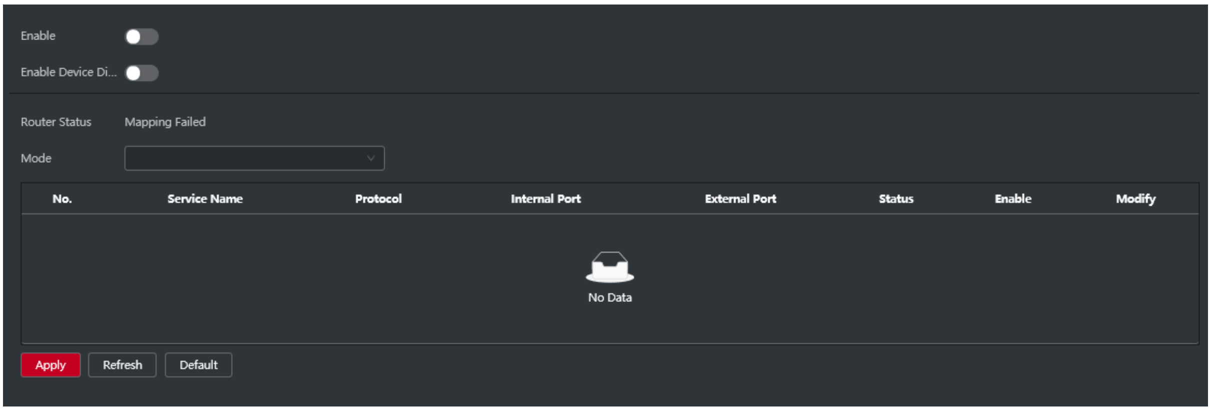
- Make sure the UPnP service is installed in the system.
- Log in to the router, and then configure WAN IP address to set up internet connection.
- Enable UPnP in the router.
- Connect your device to the LAN port of the router.
- Select ⚙ →**Network** →**TCP/IP**, in **IP Address**, enter the local area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

Procedure

Step 1 Select ⚙ → **Network** → **UPnP**.

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

Figure 4-31



Enable ○

Enable Device Di... ○

Router Status Mapping Failed

Mode

No.	Service Name	Protocol	Internal Port	External Port	Status	Enable	Modify

No Data

- Select **Custom**, click ✎ and then you can change external port.
- Select **Default**, and then the system finishes mapping with unoccupied portautomatically, and you cannot edit mapping relation.
- Select **Enable Device Discovery** to search for the device through the PC's onlineneighbors. The device name is the serial number.

Step 3 Click **Apply**.

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

4.4.7. SNMP

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

Prerequisites

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

Procedure

Step 1 Select ⚙ → **Network** → **SNMP**.

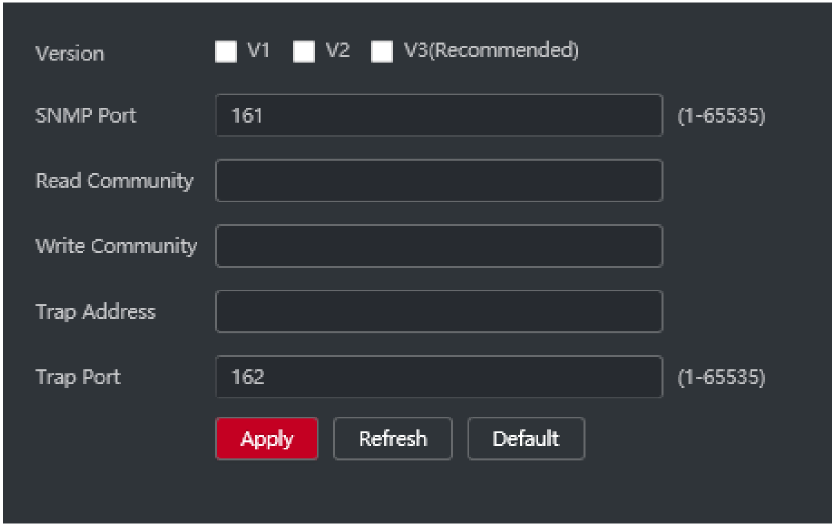
Step 2 Select SNMP version to enable SNMP.

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

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

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

Figure 4-32



Version □ V1 □ V2 □ V3(Recommended)

SNMP Port: 161 (1-65535)

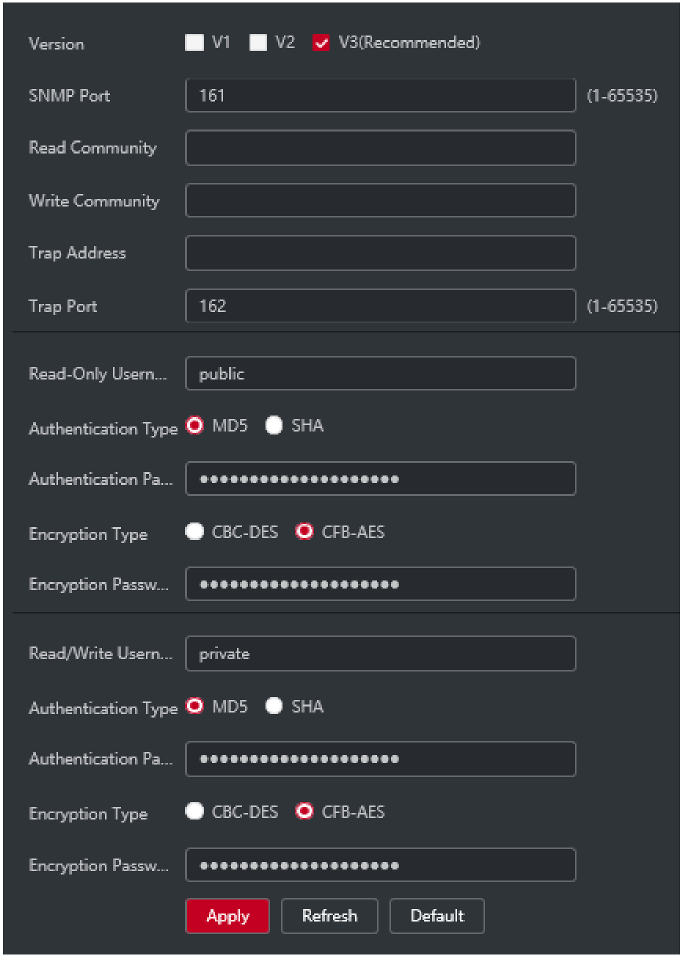
Read Community:

Write Community:

Trap Address:

Trap Port: 162 (1-65535)

Figure 4-33



Version □ V1 □ V2 ☑ V3(Recommended)

SNMP Port: 161 (1-65535)

Read Community:

Write Community:

Trap Address:

Trap Port: 162 (1-65535)

Read-Only Usern...: public

Authentication Type ● MD5 ○ SHA

Authentication Pa...: ••••••••••••••••••••

Encryption Type ○ CBC-DES ● CFB-AES

Encryption Passw...: ••••••••••••••••••••

Read/Write Usern...: private

Authentication Type ● MD5 ○ SHA

Authentication Pa...: ••••••••••••••••••••

Encryption Type ○ CBC-DES ● CFB-AES

Encryption Passw...: ••••••••••••••••••••

Table 19

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

Step 4 Click **Apply**.

Result

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

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

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

4.4.8. Bonjour

Enable this function, and the OS and clients that support Bonjour would find the camera automatically. You can have quick visit to the camera with Safari browser. When the device is automatically detected by Bonjour, the name is displayed as the defined server name.

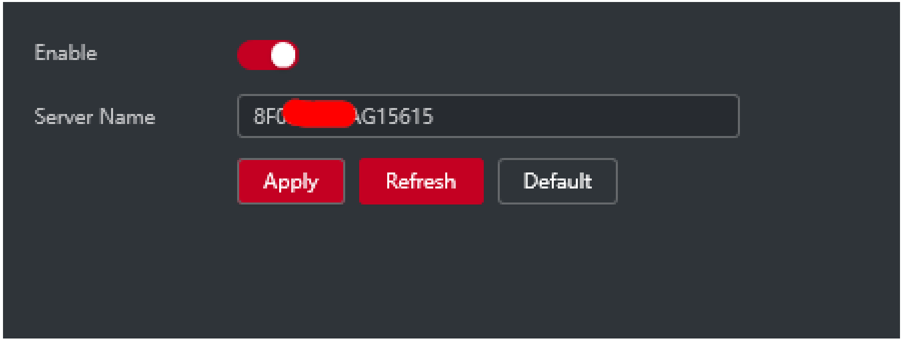
Bonjour is enabled by default.

Procedure

Step 1 Select ⚙ → **Network** → **Bonjour**.

Step 2 Click ◯, and then configure server name.

Figure 4-34



Enable ●

Server Name 8F0[redacted]G15615

Step 3 Click **Apply**.

Result

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

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

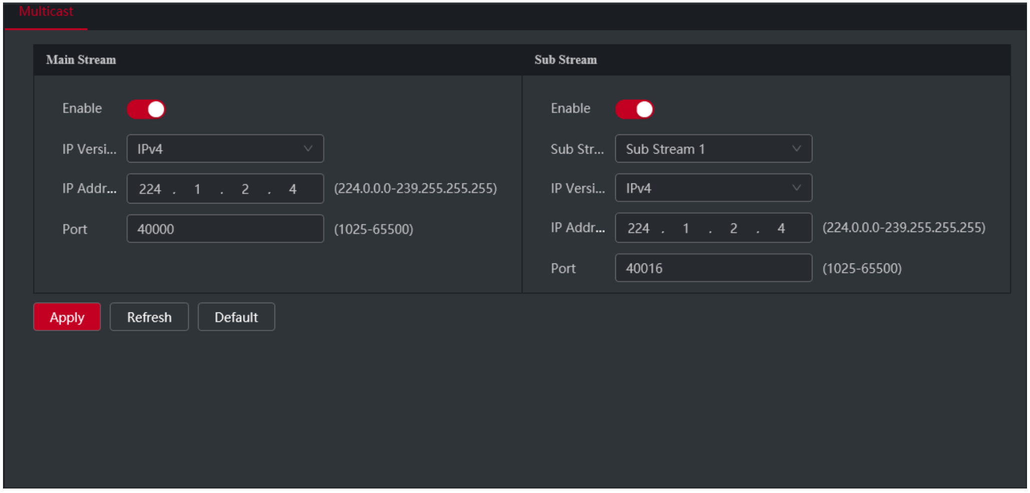
4.4.9. Multicast

When multiple users are viewing the device video image simultaneously through network, it might fail due to the limited bandwidth. You can solve this problem by setting up a multicast IP (224.0.0.0– 239.255.255.255) for the camera and adopt the multicast protocol.

Step 1 Select ⚙ → **Network** → **Multicast**.

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

Figure 4-35



Multicast

Main Stream

Enable: on

IP Versi...: IPv4

IP Addr...: 224 . 1 . 2 . 4 (224.0.0.0-239.255.255.255)

Port: 40000 (1025-65500)

Sub Stream

Enable: on

Sub Str...: Sub Stream 1

IP Versi...: IPv4

IP Addr...: 224 . 1 . 2 . 4 (224.0.0.0-239.255.255.255)

Port: 40016 (1025-65500)

Table 20

Parameter	Description
Multicast Address	The multicast IP address of **Mainstream/Sub Stream** is 224.1.2.4by default, and the range is 224.0.0.0–239.255.255.255.
Port	The range of multicast port is 1025–65500. ● Single-channel device: The multicast port of correspondingstream: **Mainstream**: 40000; **Sub Stream1**: 40016; **Sub Stream2**: 40032. ● Multi-channel device: a. Channel 1: The multicast port of corresponding stream: **Mainstream**: 40000; **Sub Stream1**: 40016; **Sub Stream2**:40032. b. Channel 2: The multicast port of corresponding stream: **Mainstream**: 40048; **Sub Stream1**: 40064; **Sub Stream2**:40080. c. Channel 3: The multicast port of corresponding stream: **Mainstream**: 40096; **Sub Stream1**: 40112; **Sub Stream2**:40128. d. Channel 4: The multicast port of corresponding stream: **Mainstream**: 40144; **Sub Stream1**: 40160; **Sub Stream2**:40176.

Step 3 Click **Apply**.

Result

- In the web page, click ⚙ and then select **local**. In the **Play Parameter** area, select **Protocol** as **Multicast.**
- Click Live on the main page of the web page, and then monitor the video image of corresponding stream in a multicast form on the **Live** page.

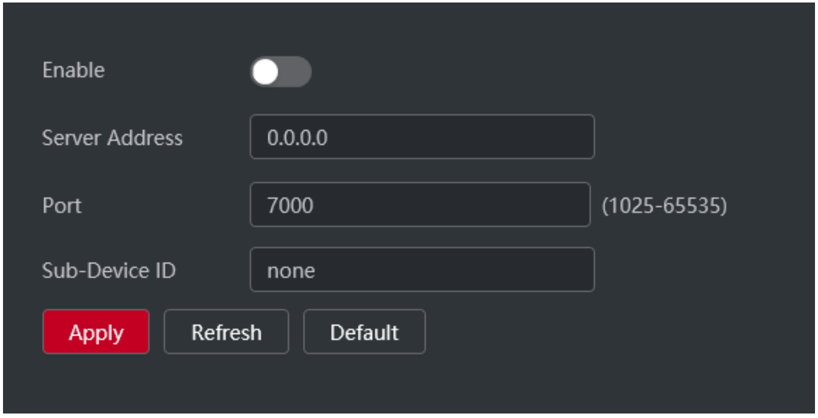
4.4.10. Register

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

Step 1 Select ⚙ → **Network** → **Register**.

Step 2 Click ○, and then configure **Server Address**, **Port** and **Sub-Device ID**.

Figure 4-36



Enable ○

Server Address: 0.0.0.0

Port: 7000 (1025-65535)

Sub-Device ID: none

Table 21

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

Step 3 Click **Apply.**

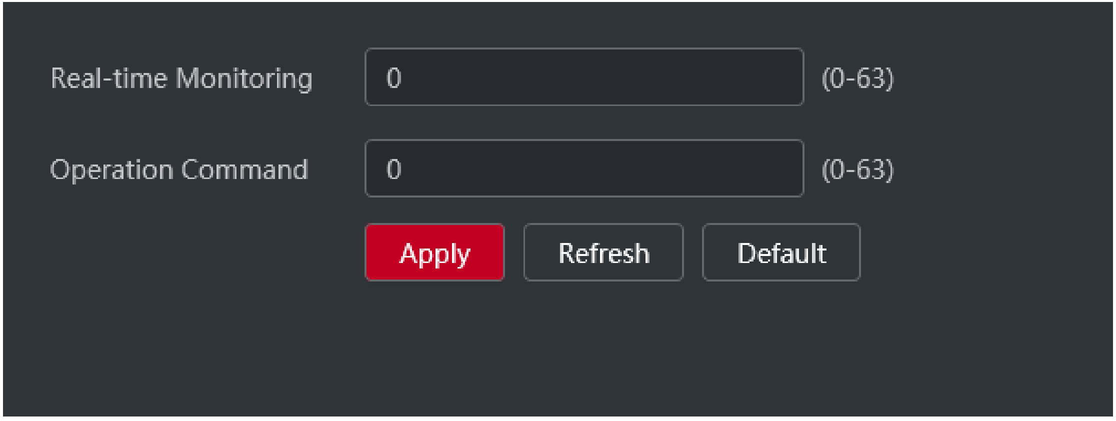
4.4.11. QoS

You can solve problems such as network delay and congestion with QoS (Quality of Service) function.It helps to assure bandwidth, reduce transmission delay, packet loss rate, and delay jitter to improve experience.

Step 1 Select ⚙ → **Network** → **QoS**.

Step 2 Configure QoS parameters

Figure 4-37



Real-time Monitoring: 0 (0-63)

Operation Command: 0 (0-63)

Table 22

Parameter	Description
Real-time Monitoring	Configure the priority of the data packets that used for networksurveillance. 0 for the lowest and 63 the highest.
Operation Command	Configure the priority of the data packets that are used for Configure or checking. 0 for the lowest and 63 the highest.

Step 3 Click **Apply**.

4.4.12. Platform Access

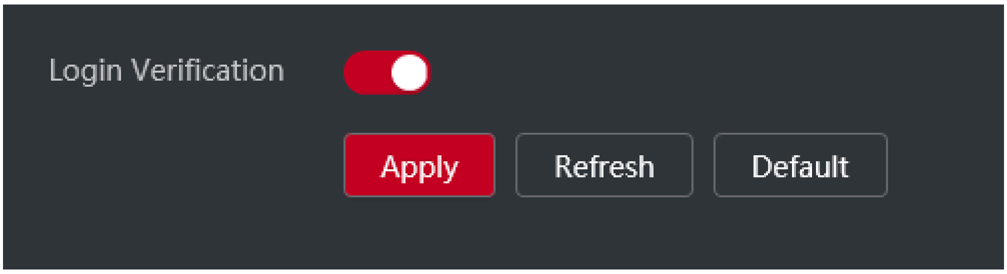
4.4.12.1. ONVIF

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

ONVIF is enabled by default.

Step 1 Select ⚙ → **Network** → **Platform Access** → **ONVIF**.

Step 2 Click ○ next to **Login Verification**.



Step 3 Click **Apply**.

4.4.12.2. RTMP

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

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

Step 1 Select ⚙ → **Network** → **Platform Access** → **RTMP**.

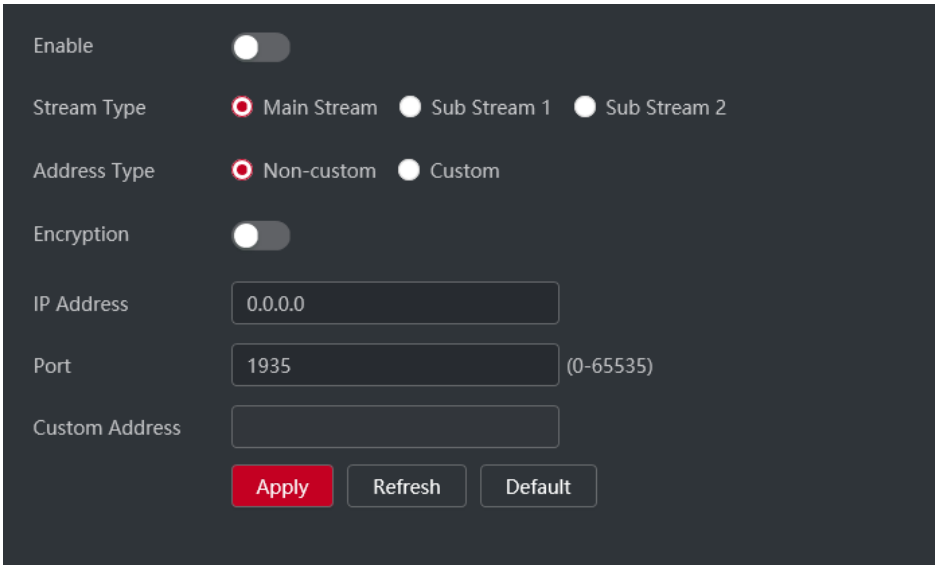
Step 2 Click ○.

⚠

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

Step 3 Configure RTMP parameters.

Figure 4-38



Enable

Stream Type: ● Main Stream ○ Sub Stream 1 ○ Sub Stream 2

Address Type: ● Non-custom ○ Custom

Encryption

IP Address: 0.0.0.0

Port: 1935 (0-65535)

Custom Address

Table 23

Parameter	Description
Stream Type	The stream for live view. Make sure that the video format is H.264, H.264 B or H.264H, and the audio format is AAC.
Address Type	• **Non-custom**: Enter the server IP and domain name. • **Custom**: Enter the path allocated by the server.
Encryption	Click ○ to enable encryption function.
IP Address	When selecting **non-custom**, you need to enter server IP addressand port. • **IP address**: Support IPv4 or domain name. • **Port**: Keep the default value.
Port	
Custom Address	When selecting **Custom**, you need to enter the path allocated bythe server.

Step 4 Click **Apply**.

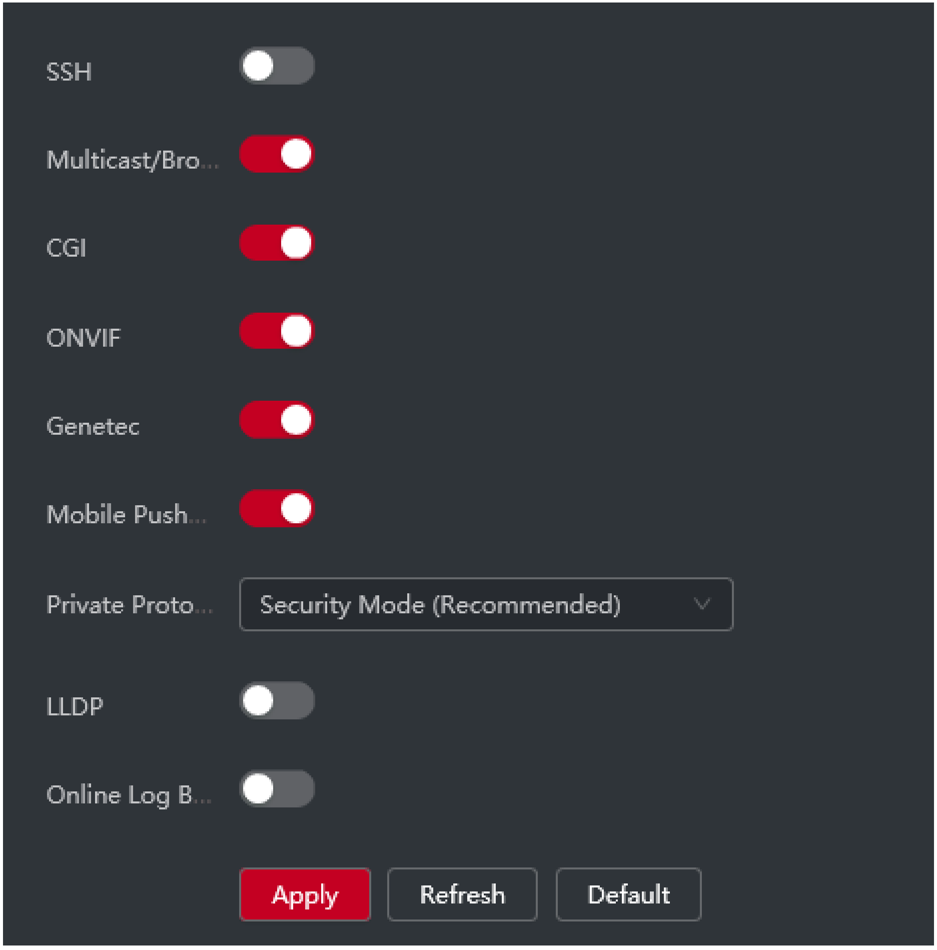
4.4.13. Basic Service

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

Step 1 Select ⚙ → Network → Basic Service.

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

Figure 4-39



SSH

Multicast/Bro...

CGI

ONVIF

Genetec

Mobile Push...

Private Proto... Security Mode (Recommended)

LLDP

Online Log B...

Table 24

Parameter	Description
SSH	You can enable SSH (Secure Shell) authentication to perform safety management. This function is disabled by default.
Multicast/Broadcast Search	Enable this function, and then when multiple users are viewingthe device video image simultaneously through network, they can find your device with multicast/broadcast protocol.
CGI	Enable this function, and then other devices can access through this service. The function is enabled by default. CGI: Common Gateway Interface.
ONVIF	
Genetec	
Mobile Push Notification	Enable this function, and then alarm capture picture triggered bythe Camera is sent to your mobile phone. This is enabled by default.
Private Protocol Authentication Mode	Select the authentication mode from **Security Mode** and **Compatible Mode**. Security mode is recommended.
RTSP Login Mode	Compatible with the old platform login mode. The default isdigest mode.

Step 3 Click **Apply**.

4.5. PTZ

This section introduces the configuration of PTZ parameters, such as preset, tour, and PTZ speed.

- The panorama camera channel and the detail camera channel support different functions and might differ from the actual page.
- Some models of panorama camera channels do not support focus, zoom and iris adjustmentfunctions, and might differ from the actual page.

You can enter the page of **PTZ** through two methods. The following content of the chapter uses thebutton entry from the upper right corner of the page as an example.

- Click **PTZ** on the main web page.
- Click ⚙ on the upper right corner of the page, and then click **PTZ**.

4.5.1. Configuring Presets

The camera saves parameters (such as current status of PTZ pan/tilt, focus) to the memory, so thatyou can quickly call these parameters and adjust the PTZ to the correct position.

Procedure

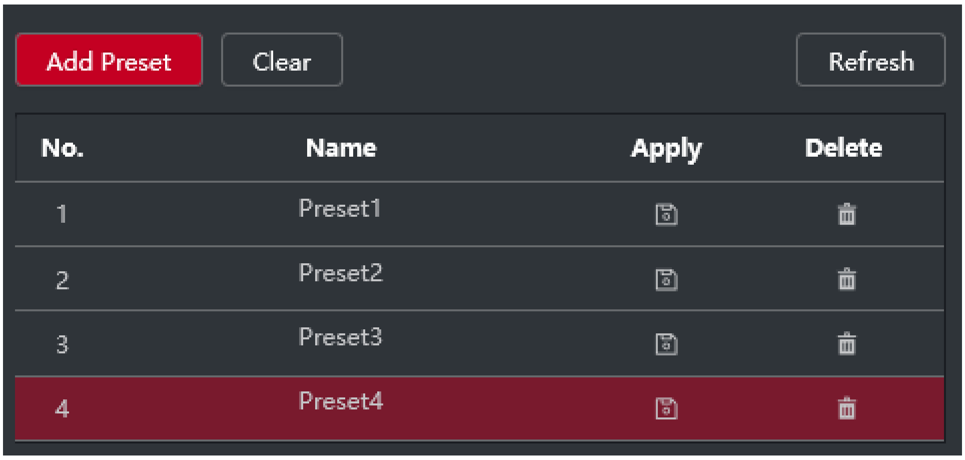
Step 1 Click ⚙ and then select **PTZ → Preset**.

Step 2 Set step length and click the direction buttons to adjust PTZ Direction. Click ⊕ ⊖ ⊞ ⊟ ○ ● to adjust zoom, focus and iris to adjust the camera to the proper position.

Step 3 Click **Add Preset**.

Add the current position to be a preset, and the preset is displayed in preset list.

Figure 4-40



No.	Name	Apply	Delete
1	Preset1	💾	🗑
2	Preset2	💾	🗑
3	Preset3	💾	🗑
4	Preset4	💾	🗑

Step 4 Double-click **Preset Title** to change the name of the corresponding preset in the screen.

Step 5 Click 💾 to save the preset.

Related Operations

- Delete preset: Click 🗑 to delete corresponding preset.
- Clear all presets: Click **Clear** to delete all added presets.

4.5.2. Configuring Tour

Configure Tour and the PTZ camera repeats performing tours among the configured presets afterconfiguration.

Prerequisites

You need to setup several preset points in advance.

Procedure

Step 1 Click ⚙ and then select **PTZ → Tour**.

Step 2 Click **Add Tour Group**, and then double click **Name** to change the name of tour.

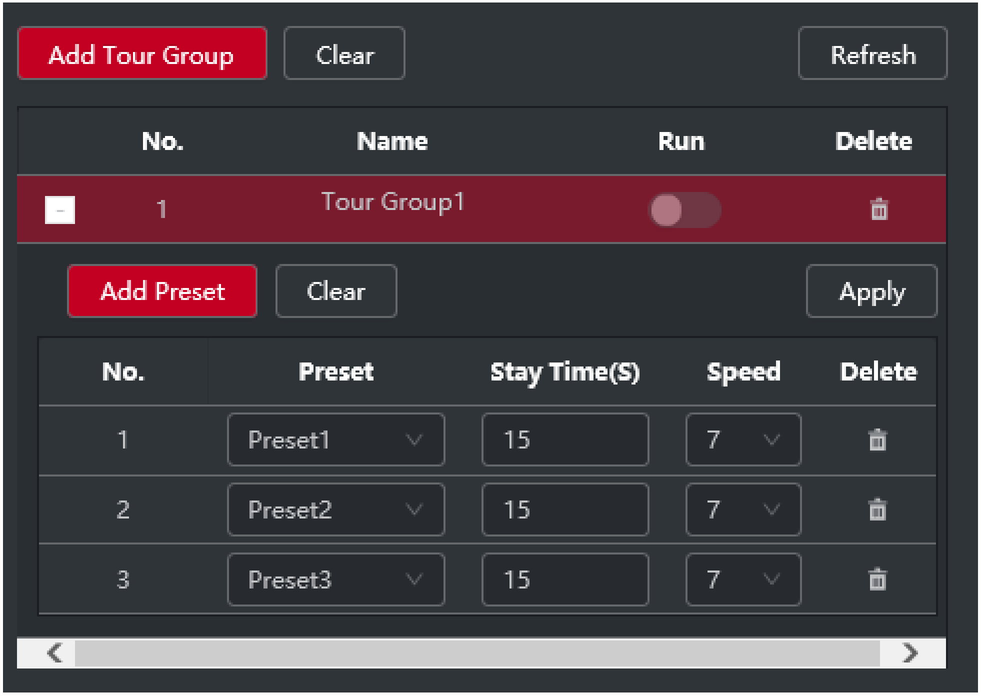
Step 3 Select tour group and then select the presets from the **Preset Point** drop-down list on the left.

Repeat this step to add several presets for the tour group.

Step 4 Configure **Stay Time(S)** and **Speed** to set the stay time of the Camera at the preset pointand its rotating speed.

Stay time is measured in seconds. The value ranges from 15 seconds to 3600 seconds.

Figure 4-41



	No.	Name	Run	Delete
□	1	Tour Group1	○	🗑

No.	Preset	Stay Time(S)	Speed	Delete
1	Preset1	15	7	🗑
2	Preset2	15	7	🗑
3	Preset3	15	7	🗑

Step 5 Select Tour mode.

- Original Path: The camera rotates in the order of selected preset points.

- Shortest path: The camera rearranges the preset points according to distance, and then rotates them according to the shortest path.

This function is available on select models.

Step 6 Click **Apply** to complete settings.

Step 7 Click ● to start tour.

- The ongoing tour stops if any operation is made to the PTZ.
- Click ○ to stop tour.

Related Operations

- Delete tour group: Click 🗑 to delete corresponding tour group.
- Clear all tour groups: Click **Clear** to delete all added tour groups.

4.5.3. Configuring Scan

Scan means the Camera moves horizontally at a certain speed between the defined left and right boundaries.

Procedure

Step 1 Click ⚙ and then select **PTZ → Scan**.

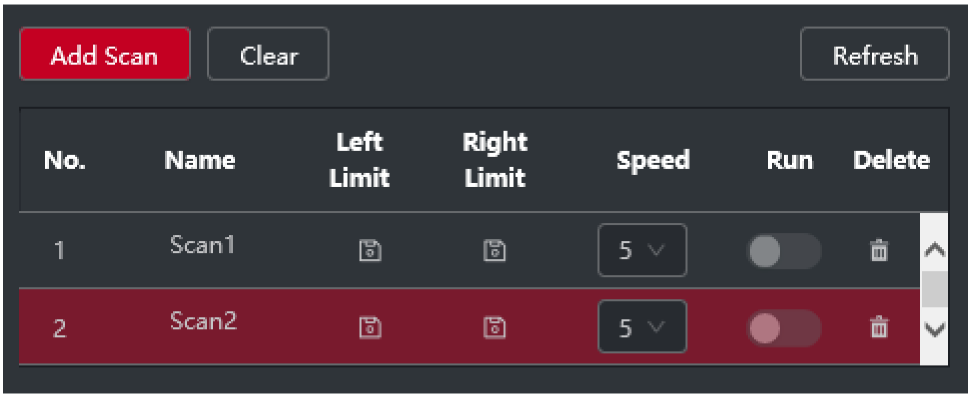
Step 2 Click **Add Scan**, and then double click **Name** to change the name of scan.

Step 3 Configure the left and right boundaries of the scan.

a. Adjust the direction of the camera to the left edge of the scan and click on the **Left Limit** to set the current position to the **Left Limit** of the camera.

b. Adjust the direction of the camera to the right edge of the scan and click on the **Right Limit** to set the current position to the **Right Limit** of the camera.

Figure 4-42



No.	Name	Left Limit	Right Limit	Speed	Run	Delete
1	Scan1	🖫	🖫	5	○	🗑
2	Scan2	🖫	🖫	5	○	🗑

Step 4 Click ● to start scanning.

Click ○ to stop scanning.

Related Operations

- Delete scan: Click 🗑 to delete corresponding scan.
- Clear all scans: Click **Clear** to delete all added scans.

4.5.4. Configuring Pattern

Pattern records a series of operations that makes to the Camera. The operations include horizontal and vertical movements, zoom and preset calling. After recording and saving the operations, you can call the pattern path directly.

Procedure

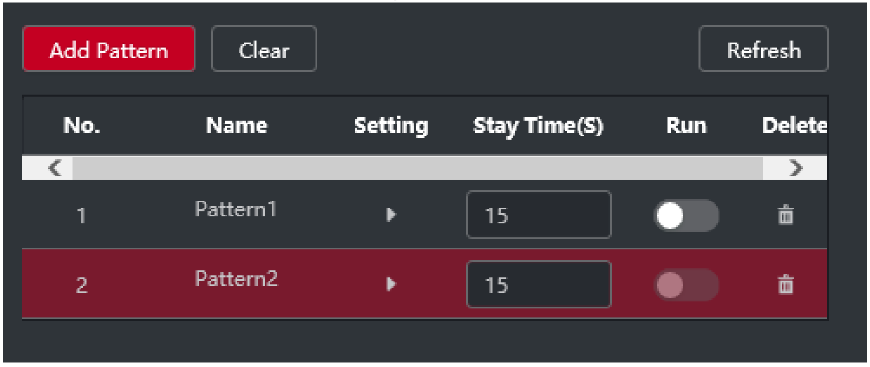
Step 1 Click ⚙ and then select **PTZ → Pattern**.

Step 2 Click **Add Pattern**, and then double click **Name** to change the name of pattern.

Step 3 Click ▶ to adjust the direction, focus, zoom and other parameters according to actualneeds.

Step 4 Click ❚❚ to complete records.

Figure 4-43



No.	Name	Setting	Stay Time(S)	Run	Delete
1	Pattern1	▶	15	○	🗑
2	Pattern2	▶	15	○	🗑

Step 5 Click ● to start scanning.

Click ○ to stop scanning.

Related operations

- Delete pattern: Click 🗑 to delete the corresponding pattern.
- Clear all patterns: Click **Clear** to delete all added patterns.

4.5.5. Configuring Pan

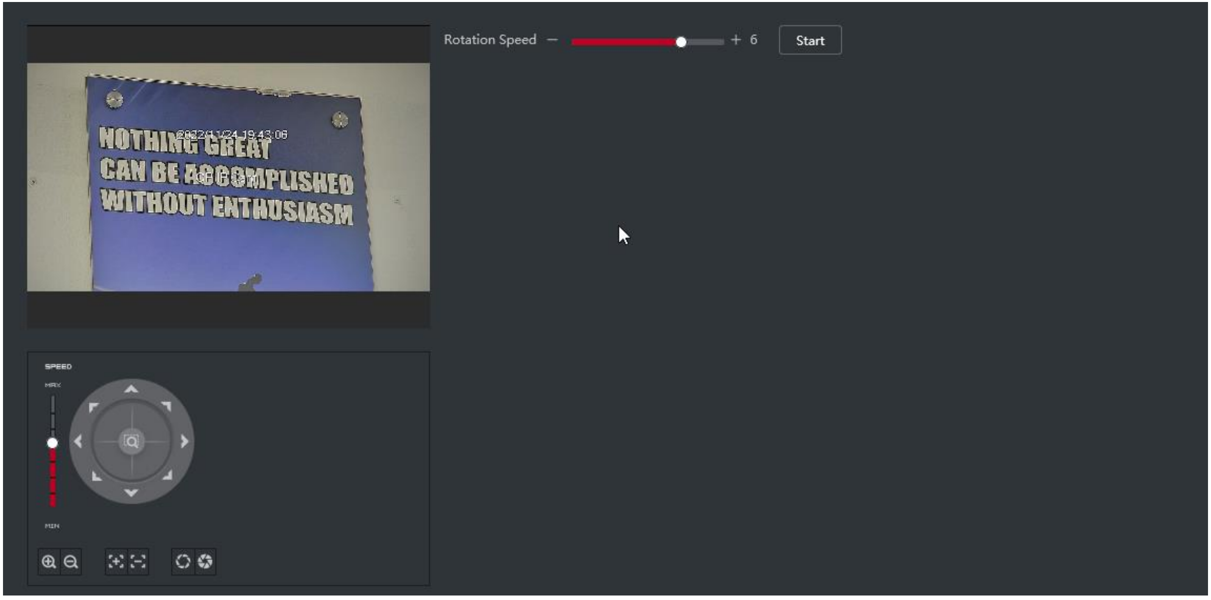
Pan refers to the continuous 360° rotation of the Camera in a horizontal way at a certain speed.

Step 1 Click ⚙, and then select **PTZ→Pan**.

Step 2 Configure the rotation speed.

- Click **Start** and PTZ starts horizontal rotation.
- Click **Stop** to stop the pan.

Figure 4-44

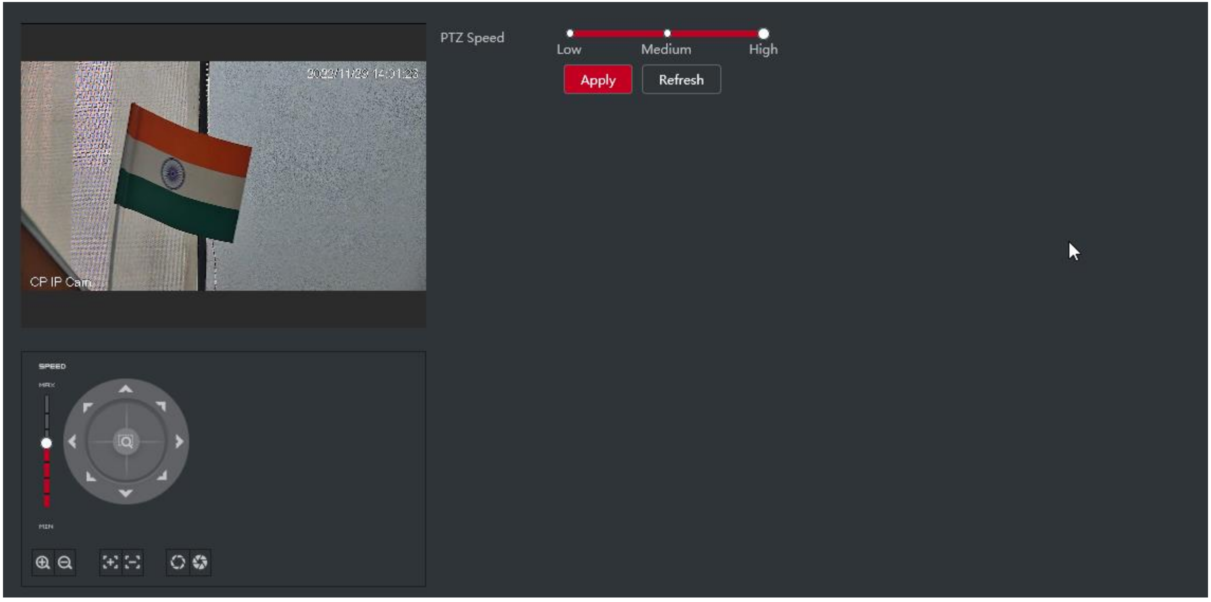


4.5.6. Configuring PTZ Speed

Configure the rotation speed when manually controlling the PTZ.

Step 1 Click ⚙ and then select **PTZ → PTZ Speed**.

Figure 4-45



Step 2 Select PTZ speed, and then click **Apply**.

4.5.7. Configuring Idle Motion

Idle motion refers to a preset motion when the PTZ does not receive any valid command within acertain period.

Prerequisites

You have set PTZ motions such as preset, tour, scan, and pattern in advance.

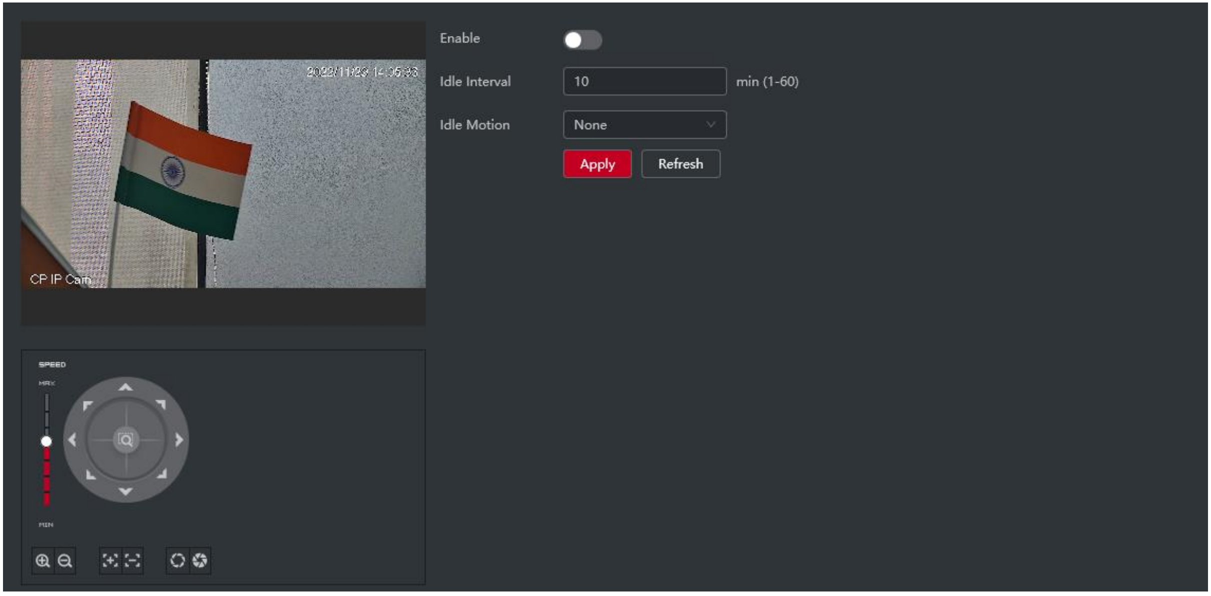
Procedure

Step 1 Click ⚙ and then select **PTZ → PTZ Speed**.

Step 2 Click to enable idle motion.

Step 3 Configure idle interval time, and then select idle motion type.

Figure 4-46



Enable

Idle Interval: 10 min (1-60)

Idle Motion: None

Step 4 Click **Apply**.

4.5.8. Configuring Power Up

After configuring Power Up, the camera will automatically perform the set motion after being powered up.

Prerequisites

You have set PTZ motions such as preset, tour, scan, and pattern in advance.

Procedure

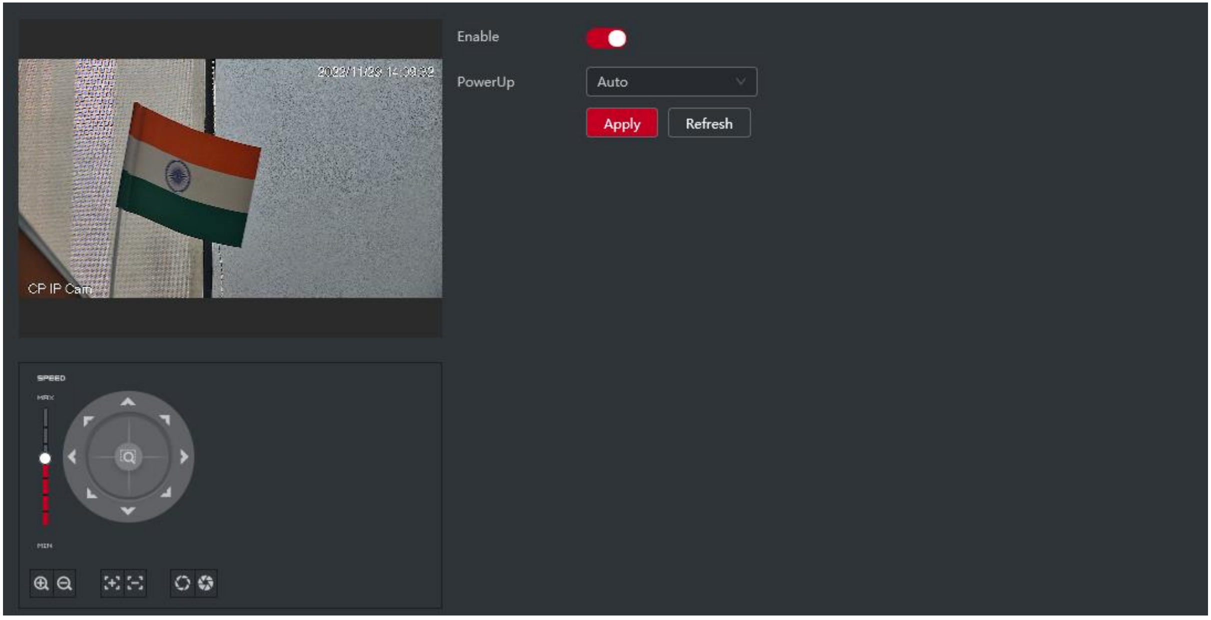
Step 1 Click ⚙ and then select **PTZ → Power Up**.

Step 2 Click to enable power up function.

Step 3 Select power up type.

Select **Auto** and the system will implement the last action performed for more than 20 seconds before the Camera is shut down.

Figure 4-47



Enable

PowerUp Auto

Step 4 Click **Apply**.

4.5.9. Configuring PTZ Rotation Limit

Configure PTZ rotation limit to enable the Camera to move only within the defined PTZ area, and to rotate only within the limit range when calling functions such as tour and pan.

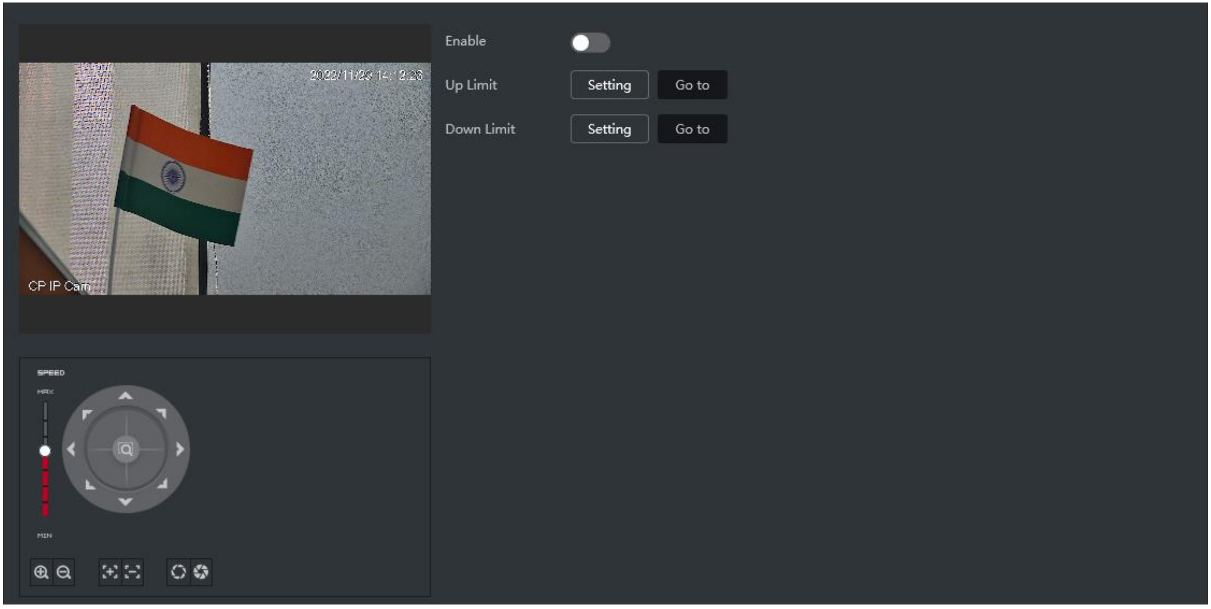
Step 1 Click ⚙ and then select **PTZ → PTZ Rotation Limit**.

Step 2 Adjust the device direction to the **Up Limit**, and then click up limit **Setting** to set thecurrent position to the up limit.

Step 3 Adjust the device direction to the **Down Limit**, and then click down limit **Setting** to set thecurrent position to the down limit.

Step 4 Click **Go to** to preview the defined up/down limit.

Figure 4-48



Step 5 Select the elevation value from the drop-down list of **Max Elevation Angle**.

This function is available on select models.

Step 6 Click **Enable** to enable **PTZ Rotation Limit**.

4.5.10. Configuring Scheduled Task

After setting scheduled task, the Camera performs the relevant motions during the set period.

Prerequisites

You have set PTZ motions such as preset, tour, scan and pattern in advance.

Procedure

Step 1 Click ⚙ and then select **PTZ → Scheduled Task**.

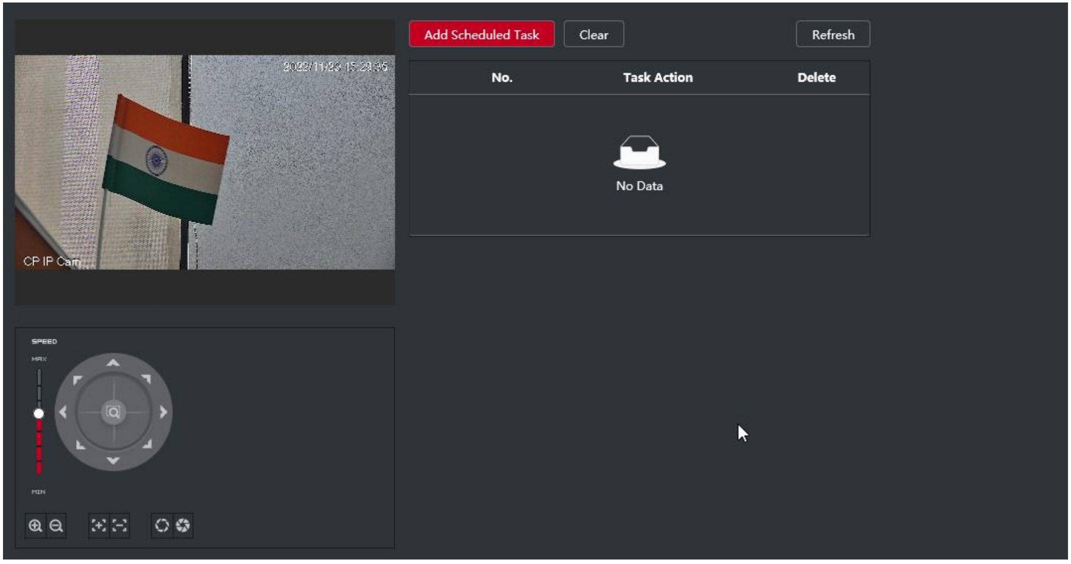
Step 2 Click **Add Scheduled Task**.

Step 3 Select **Task Action**.

Some task actions need to select corresponding action number.

Step 4 Select **Time Plan** or click **Add Schedule**. Configure the name and time of the scheduledtask in the pop-up page, and then click **Apply**.

Figure 4-49



Step 5 Set the time for **Auto Home**.

Auto Home: When the scheduled task is interrupted by an artificial call to the PTZ, thedevice will automatically resume the scheduled task after the auto home time.

Step 6 Click **Apply**.

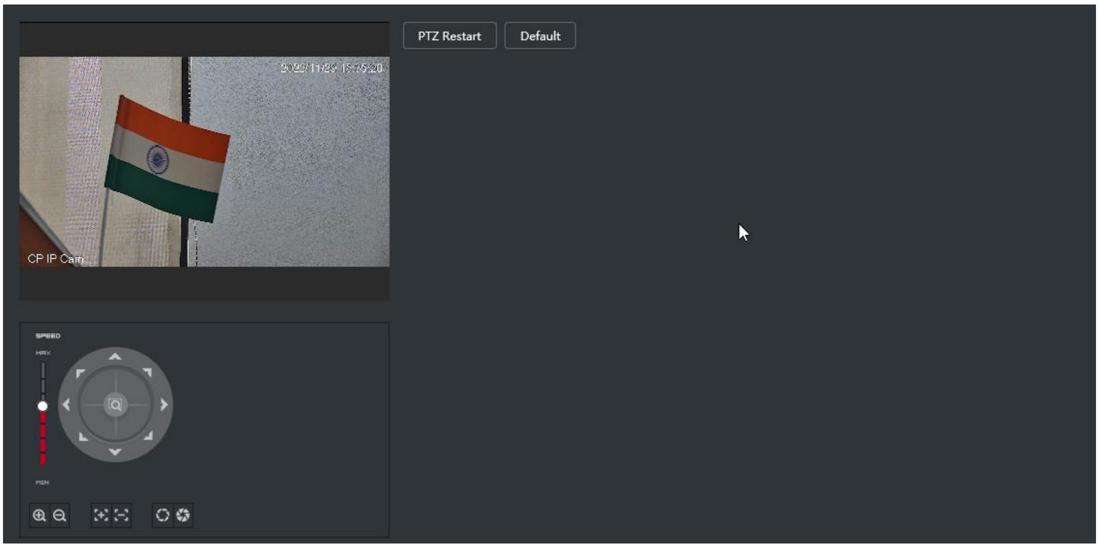
4.5.11. Configuring PTZ Maintenance

PTZ Maintenance includes **PTZ Restart** and **Default**.

Step 1 Click ⚙ and then select **PTZ → PTZ Maintenance**.

Step 2 Click **PTZ Restart** to restart PTZ or click **Default** to restore PTZ to defaults.

Figure 4-50



⚠

Default PTZ will restore the Camera to defaults. Think twice before clicking **Default**.

4.6. Event

Click **Event** to configure general events, including alarm linkage, exception, video detection, and audio detection. You can go to the **Event** page through two methods. This following section uses method 1 as anexample.

- Method 1: Click ⚙ on the right-upper corner of the main page, and then click **Event**.
- Method 2: Click **Event** on the page.

4.6.1. Alarm

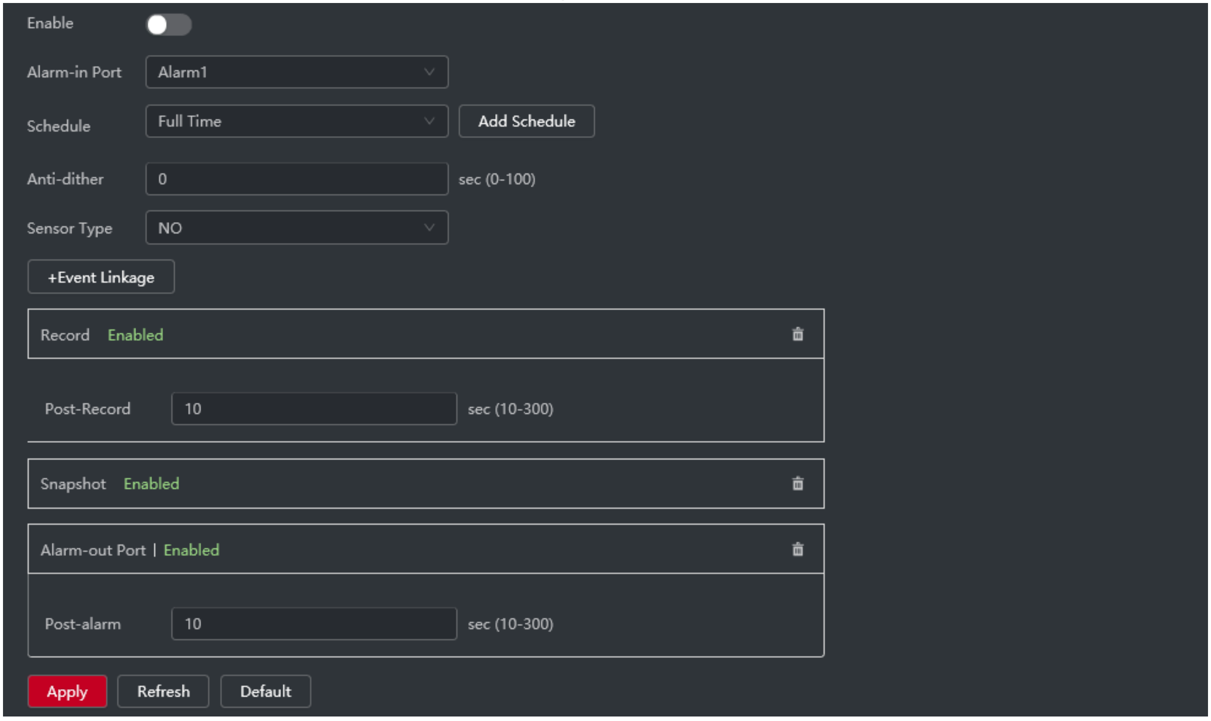
4.6.1.1. Alarm-in

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

Step 1 Select ⚙ → **Event** → **Alarm**.

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

Figure 4-51



Enable ○

Alarm-in Port: Alarm1

Schedule: Full Time

Anti-dither: 0 sec (0-100)

Sensor Type: NO

Record Enabled

Post-Record: 10 sec (10-300)

Snapshot Enabled

Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

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

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

- Sensor Type: **NO** or **NC**.

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

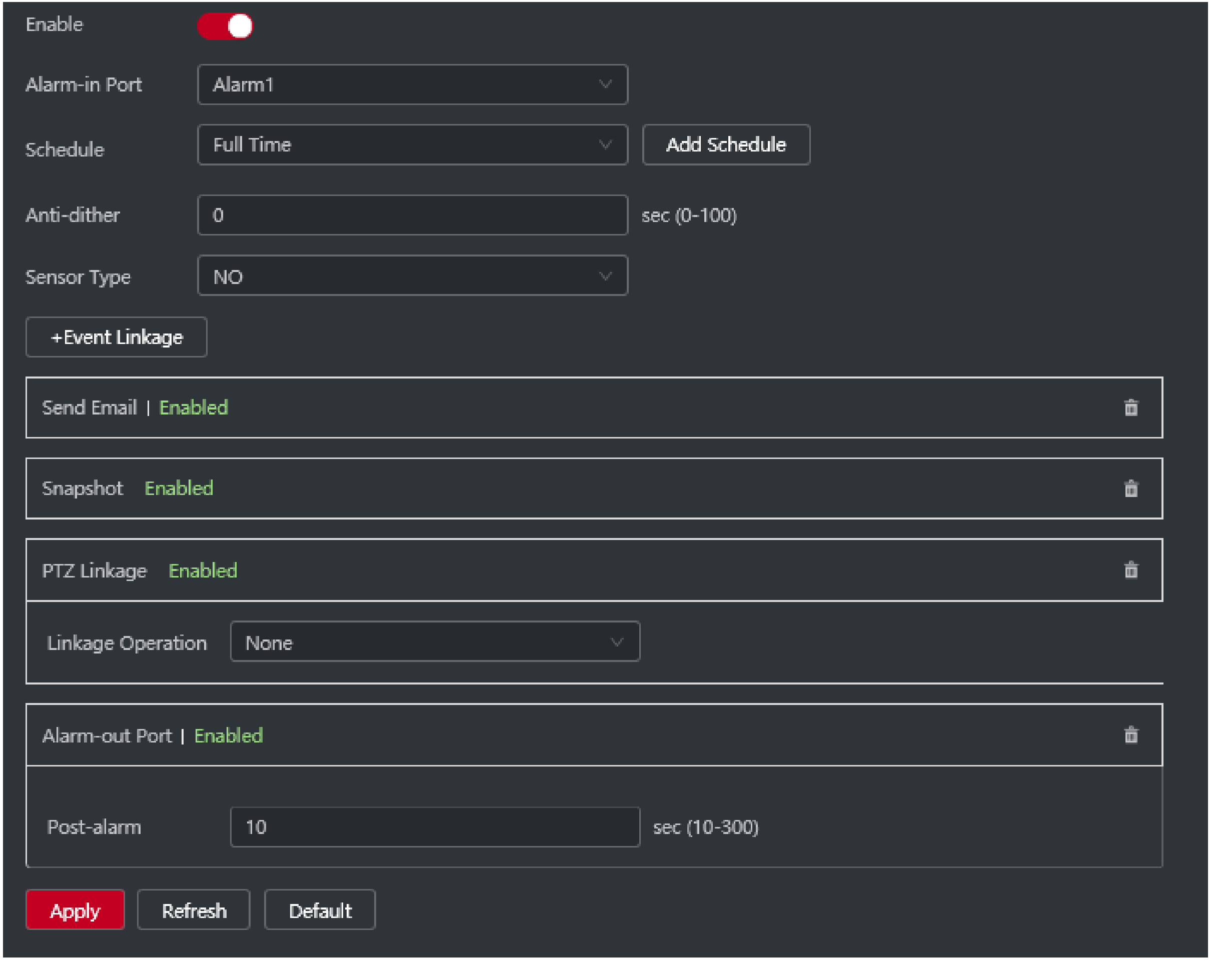
If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add new schedule.

Step 5 Click **Apply**.

4.6.1.2. Event Linkage

When configuring alarm events, select Event linkages (such as record, snapshot). When the corresponding alarm is triggered in the defined arming period, the system will trigger alarm linkage. Select ⚙ → **Event** → **Alarm**, and then click ○ next to **Enable** to enable alarm linkage.

Figure 4-52



Enable ●

Alarm-in Port: Alarm1

Schedule: Full Time

Anti-dither: 0 sec (0-100)

Sensor Type: NO

Send Email | Enabled

Snapshot Enabled

PTZ Linkage Enabled

Linkage Operation: None

Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

4.6.1.2.1. Adding Schedule

Configure arming schedule. The system only performs corresponding linkage action in the definedperiod.

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

Step 2 Click **Time Plan Table**.

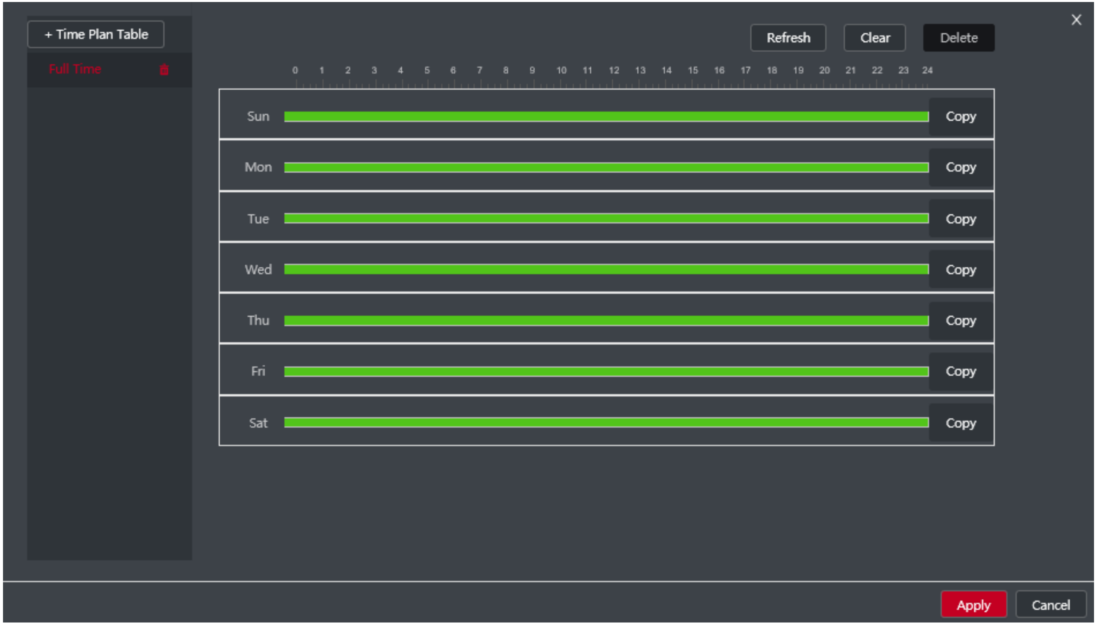
You can set up multiple time plan tables for selection.

Step 3 Configure the name of the **Time Plan Table**.

Step 4 Configure arming periods.

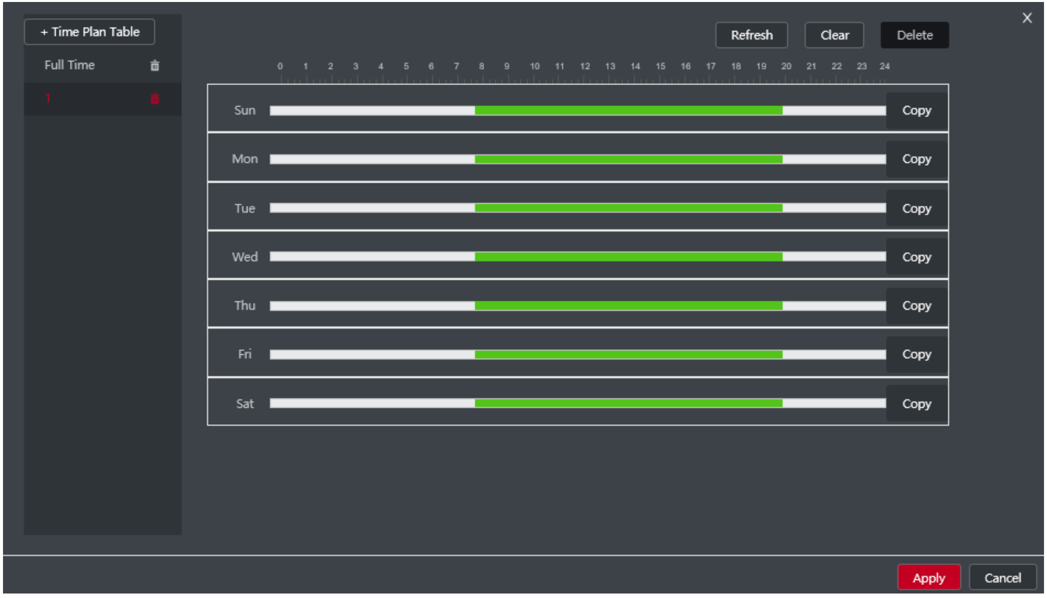
a. Press and drag the left mouse button on the timeline to set arming periods. The greenarea on the timeline means that this time period has been armed.

Figure 4-53



b. Click the selected time period, and then enter the specific time in the text box toconfigure exact arming period.

Figure 4-54



Step 5 (Optional) Click **Copy**, select weeks, and then click **Apply**.

Time plans for the current week can be quickly copied to other weeks.

Step 6 Click **Apply**.

4.6.1.2.2. Record Linkage

After enabling **Record Linkage**, the system can link record channel when an alarm event occurs. After the alarm, the system stops recording after an extended time period according to the **post-Record** setting.

Prerequisites

- Enable the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) before the record channel links recording.
- Enable auto record mode before the record linkage takes effect.

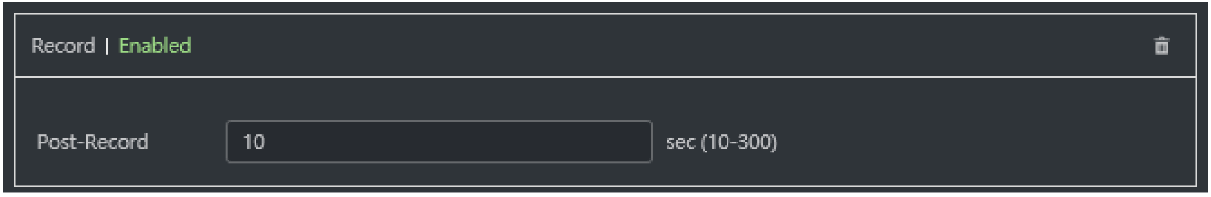
Setting Record Linkage

On the **Alarm** page, click

to select record, select the channel, and then set **post-Record** to set alarm linkage and record delay.

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

Figure 4-55



Record | Enabled

Post-Record 10 sec (10-300)

4.6.1.2.3. Snapshot Linkage

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

Prerequisites

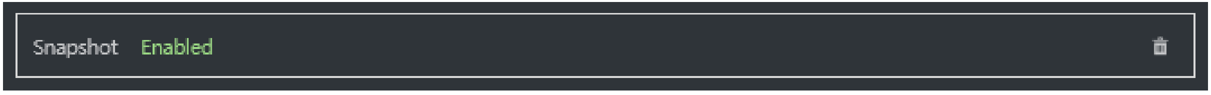
Enable the corresponding alarm type (**Normal**, **Motion**, or **Alarm**) before the snapshot channel links capturing.

Setting record linkage

On the **Alarm** page, click

to select snapshot linkage, and select the channel.

Figure 4-56



Snapshot Enabled

4.6.1.2.4. Alarm-out Linkage

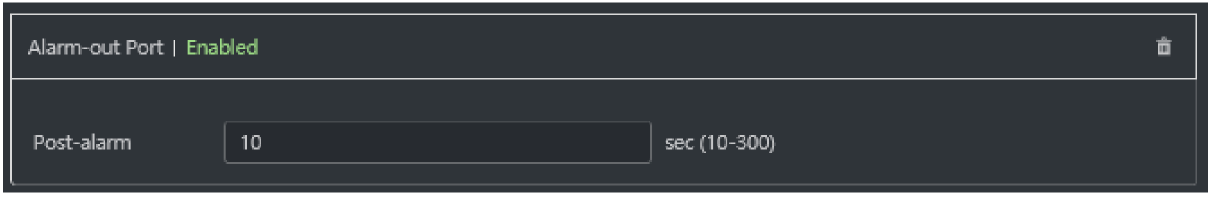
When an alarm is triggered, the system can automatically link with alarm-out device.

On the **Alarm** page, click +Event Linkage to select alarm-out linkage, select the channel and then configure **Post alarm.**

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

If the Camera has multiple alarm-out channels, you need to select the linkage alarm-out channel.

Figure 4-57



Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

4.6.1.2.5. Email Linkage

When an alarm is triggered, the system will automatically send an email to defined users.

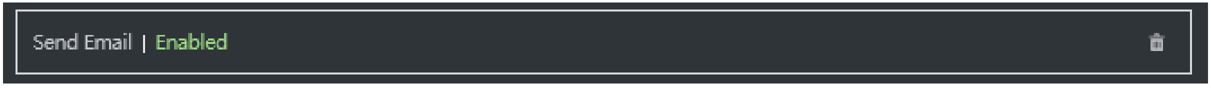
Prerequisites

Email linkage takes effect only when SMTP is configured.

Setting Email Linkage

On the **Alarm** page, click +Event Linkage to Select email linkage.

Figure 4-58



Send Email | Enabled

4.6.1.3. Subscribing to Alarm

4.6.1.3.1. Alarm Types

Following are the alarm types and preparations of alarm events.

Table 25

Alarm Type	Description
Motion Detection	The alarm is triggered when amoving object is detected.
Disk Full	The alarm is triggered when thefree space of SD card is less thanthe configured value.
Disk Error	The alarm is triggered when there is a failure or malfunctionin the SD card.
Video Tampering	The alarm is triggered when thecamera lens is covered or there isa defocus in video images.
External Alarm	The alarm is triggered when there is an external alarm input.

Alarm Type	Description
Security Warning	The alarm is triggered whenthere is a security warning.
Audio Detection	The alarm is triggered whenthere is an audio connectionproblem.
IVS	The alarm is triggered when anintelligent rule is triggered.
Scene Changing	The alarm is triggered when thedevice monitoring scene changes.
Voltage Detection	The alarm is triggered when thedevice detects abnormal voltageinput.
Security Exception	The alarm is triggered when thedevice detects malicious attack.

4.6.1.3.2. Subscribing to Alarm Information

You can subscribe alarm event. When a subscribed alarm event is triggered, the system records detailed alarm information on the bottom of the page.

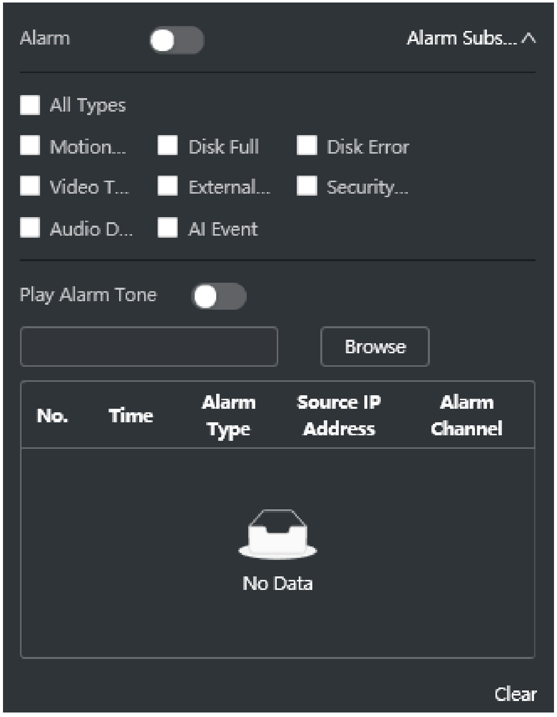
Functions of different devices might vary.

Step 1 Click 🔔 on the right-upper corner of the main page.

Step 2 Click ○ next to **Alarm** to enable alarm subscription, and then the system prompts andrecords alarm information according to actual conditions.

- When the subscribed alarm event is triggered and the alarm subscription page is notdisplayed, a number is displayed on 🔔, and the alarm information is recorded automatically. Click 🔔 to view the details in the alarm list. You can click **Clear** to clearthe record.
- When the subscribed alarm event is triggered and the system is in the alarm page, thecorresponding alarm information will be displayed in the alarm list below.

Figure 4-59



Step 3 Click next to **Play Alarm Tone**, and then select the tone path.

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

4.6.2. Exception

Abnormality includes SD card exception, network exception and tampering detection.

Only the device with SD card function has exception setting functions, including **No SD Card**, **SD Card Error**, and **Low SD card space**.

4.6.2.1. SD Card Exception

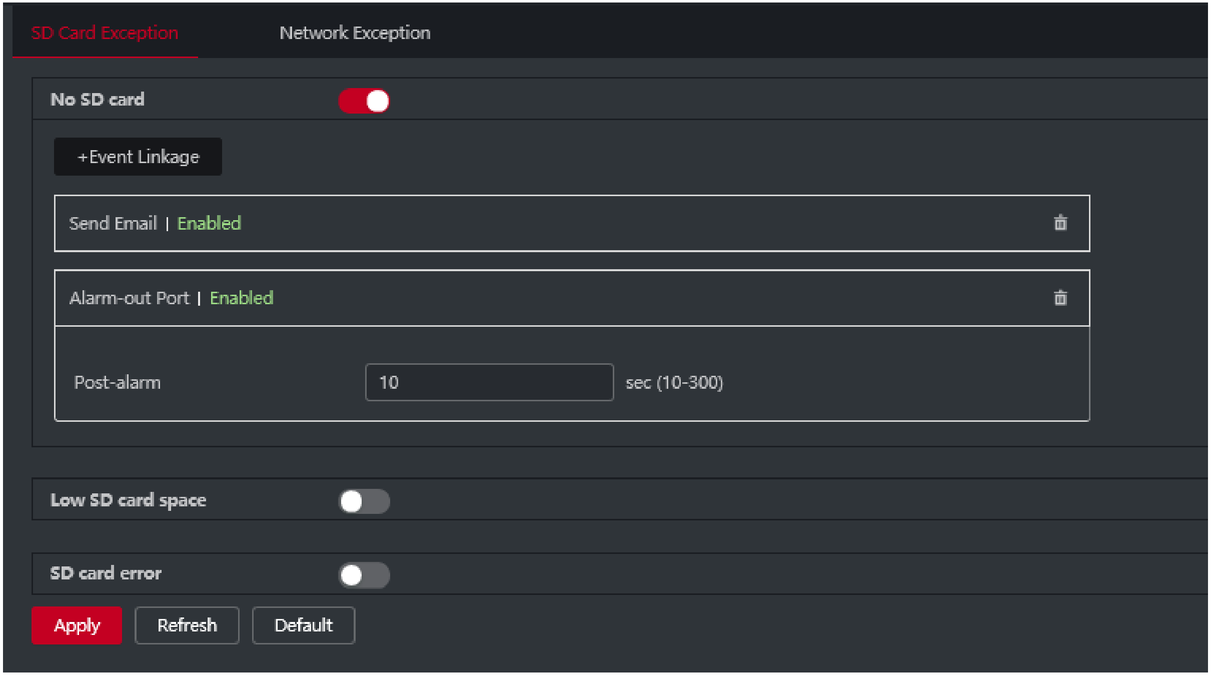
In case of SD card exception, the system performs alarm linkage. The event types include **No SD Card**, **Low SD Card Space**, and **SD Card Error**. Functions might vary with different models.

Step 1 Select ⚙ → **Event** → **Exception** → **SD Card Exception**.

Step 2 Select event type, and then enable SD card exception detection.

When the event type is **Low SD card space**, you can configure **Free Space**. When theremaining free space is less than this value, an alarm is triggered.

Figure 4-60



No SD card ●

+Event Linkage

Send Email | Enabled

Alarm-out Port | Enabled

Post-alarm 10 sec (10-300)

Low SD card space ○

SD card error ○

Step 3 Click ○ to enable the SD card detection functions.

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

Step 4 Set alarm linkage actions.

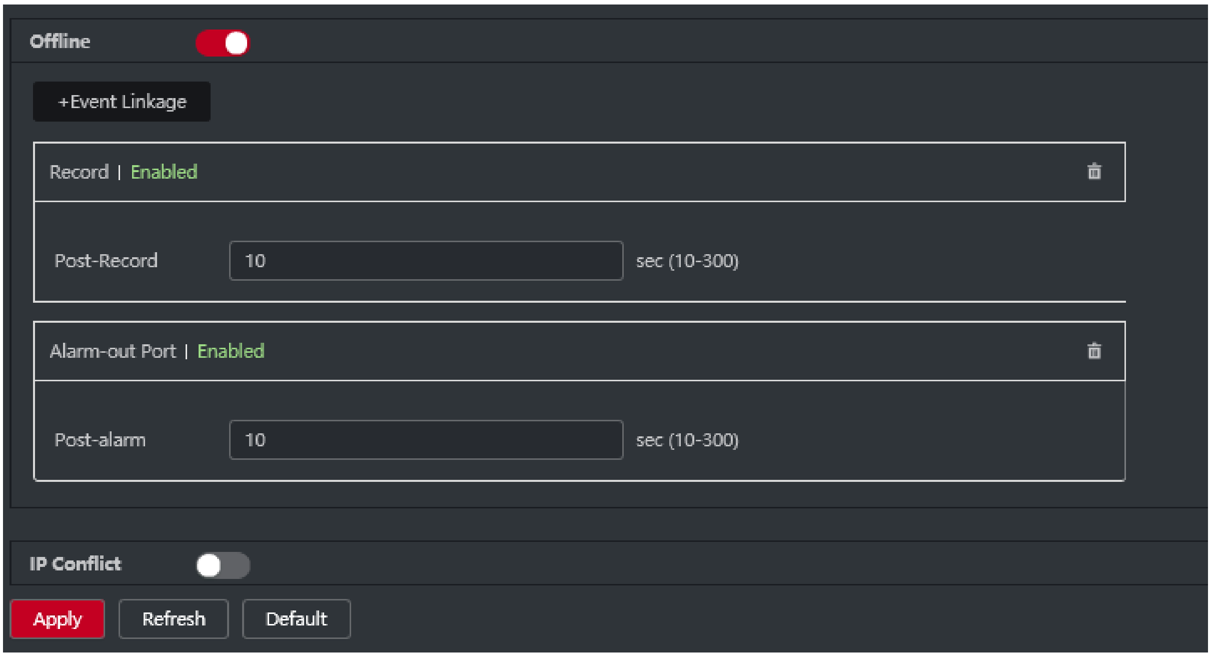
Step 5 Click **Apply**.

4.6.2.2. Network Exception

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

Step 1 Select ⚙ → **Event** → **Exception** → **Network Exception**.

Figure 4-61



Offline ●

+Event Linkage

Record | Enabled

Post-Record 10 sec (10-300)

Alarm-out Port | Enabled

Post-alarm 10 sec (10-300)

IP Conflict ○

Apply Refresh Default

Step 2 Click ○ to enable the network exception detection.

Step 3 Set alarm linkage actions.

Step 4 Click **Apply**

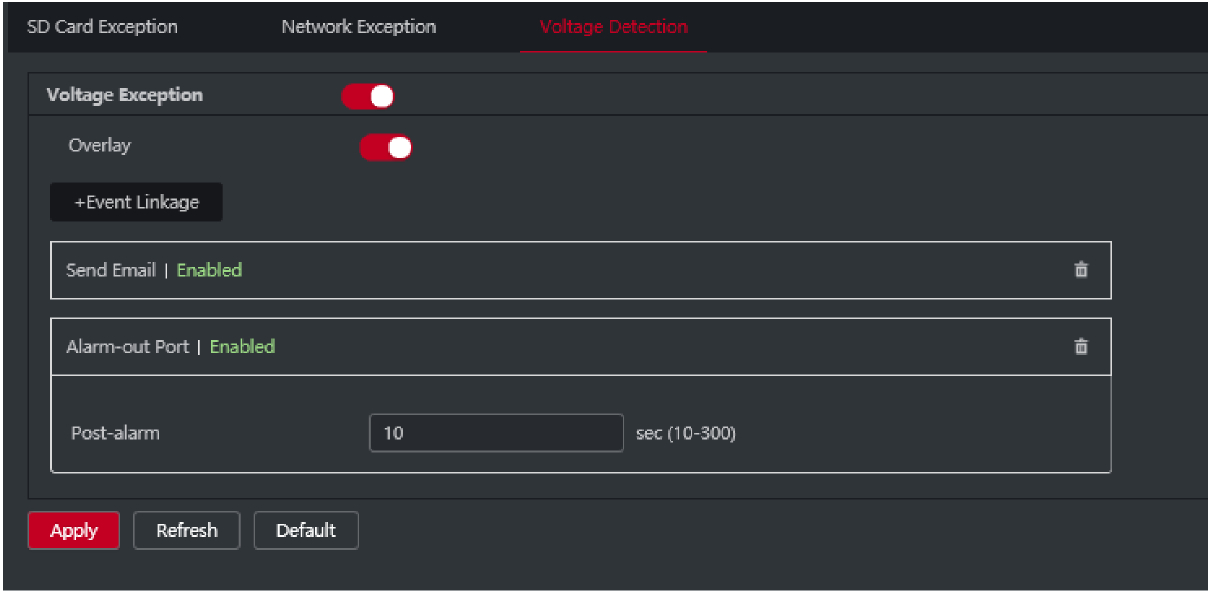
4.6.2.3. Voltage Detection

Step 1 Select ⚙ → **Event** → **Exception** → **Voltage Detection**.

Step 2 Click ○ to enable the voltage detection function.

Step 3 Configure alarm parameters.

Figure 4-62



SD Card Exception Network Exception Voltage Detection

Voltage Exception ●

Overlay ●

+Event Linkage

Send Email | Enabled

Alarm-out Port | Enabled

Post-alarm 10 sec (10-300)

Apply Refresh Default

Step 4 Click **Apply**.

4.6.3. Video Detection

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

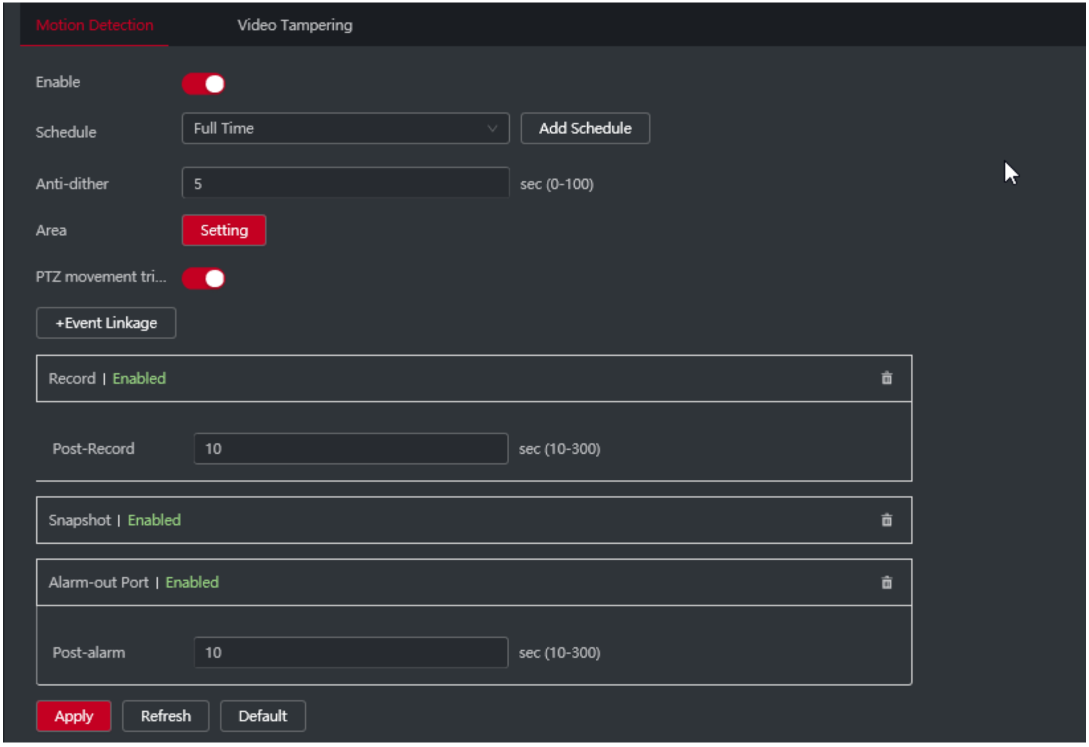
4.6.3.1. Motion Detection

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

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

Step 1 Select ⚙ → Event → Video Detection → Motion Detection.

Figure 4-63



Enable: ●

Schedule: Full Time

Anti-dither: 5 sec (0-100)

Area: Setting

PTZ movement tri...: ●

Record | Enabled

Post-Record: 10 sec (10-300)

Snapshot | Enabled

Alarm-out Port | Enabled

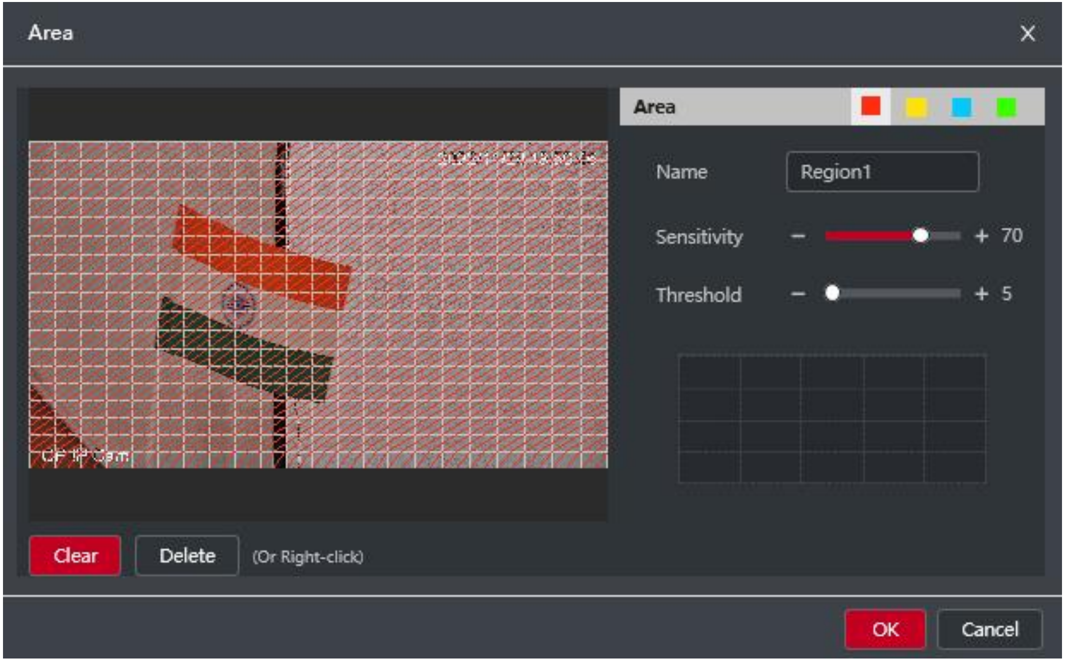
Post-alarm: 10 sec (10-300)

Step 2 Click ○ to enable the motion detection function.

Step 3 Set the area for motion detection.

a. Click **Setting** next to **Area**.

Figure 4-64



Area

Area 🟥 🟨 🟦 🟩

Name: Region1

Sensitivity: 70

Threshold: 5

b. Select a color and set the region name. Select an effective area for motion detection inthe image and set **Sensitivity** and **Threshold**.

- Select a color on 🟥 🟨 🟦 🟩 to set different detection parameters for each region.
- Sensitivity: Sensitive degree of outside changes. The higher sensitivity is, the easier to trigger the alarm.
- Threshold: Effective area threshold for Motion Detection. The smaller the thresholdis, the easier the alarm is triggered.
- The whole video image is the effective area for Motion Detection by default. Select color blocks to configure different detection parameters for different regions.
- The red line in the waveform indicates that the Motion Detection is triggered, and the green line indicates that there is no motion is detected. Adjust sensitivity and threshold according to the waveform.

c. Click **OK**.

Step 4 Set arming periods and alarm linkage action.

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

Anti-dither: After the **Anti-dither** time is set, the system only records one motion detectionevent in the period.

Step 5 Click **Apply**.

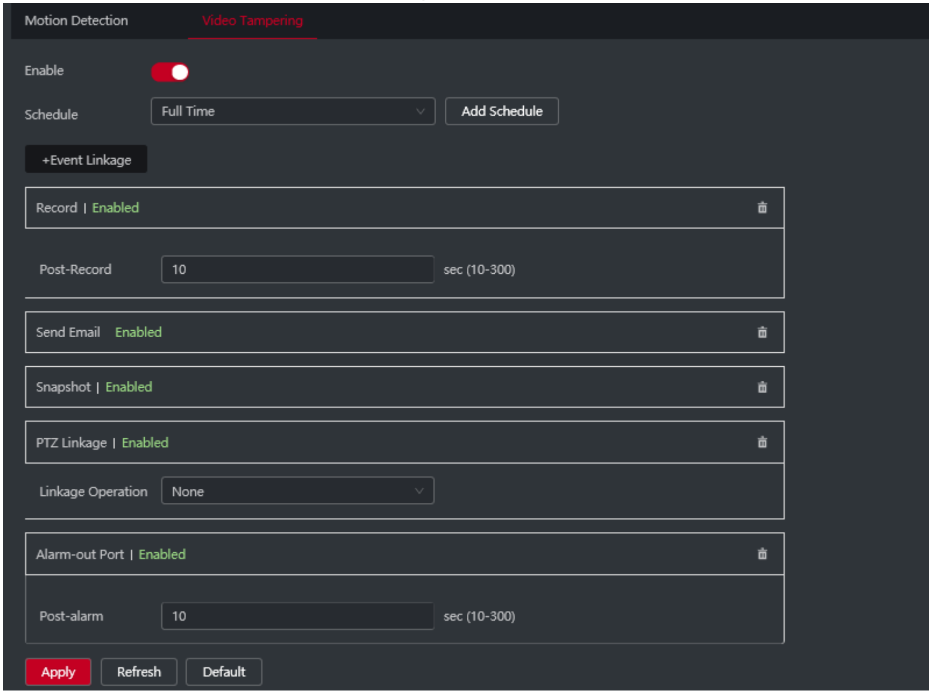
4.6.3.2. Video Tampering

The system performs alarm linkage when the lens is covered, or video output is mono color causedby light and other reasons.

Step 1 Select ⚙ → Event → Video Detection → Video Tampering.

Step 2 Select **Channel** and then click to enable the video tampering detection.

Figure 4-65



Enable

Schedule: Full Time

Record | Enabled

Post-Record: 10 sec (10-300)

Send Email Enabled

Snapshot | Enabled

PTZ Linkage | Enabled

Linkage Operation: None

Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

Step 3 Set arming periods and alarm linkage action.

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. Anti-dither: After the **Anti-dither** time is set, the system only records one motion detectionevent in the period.

Step 4 Click **Apply**.

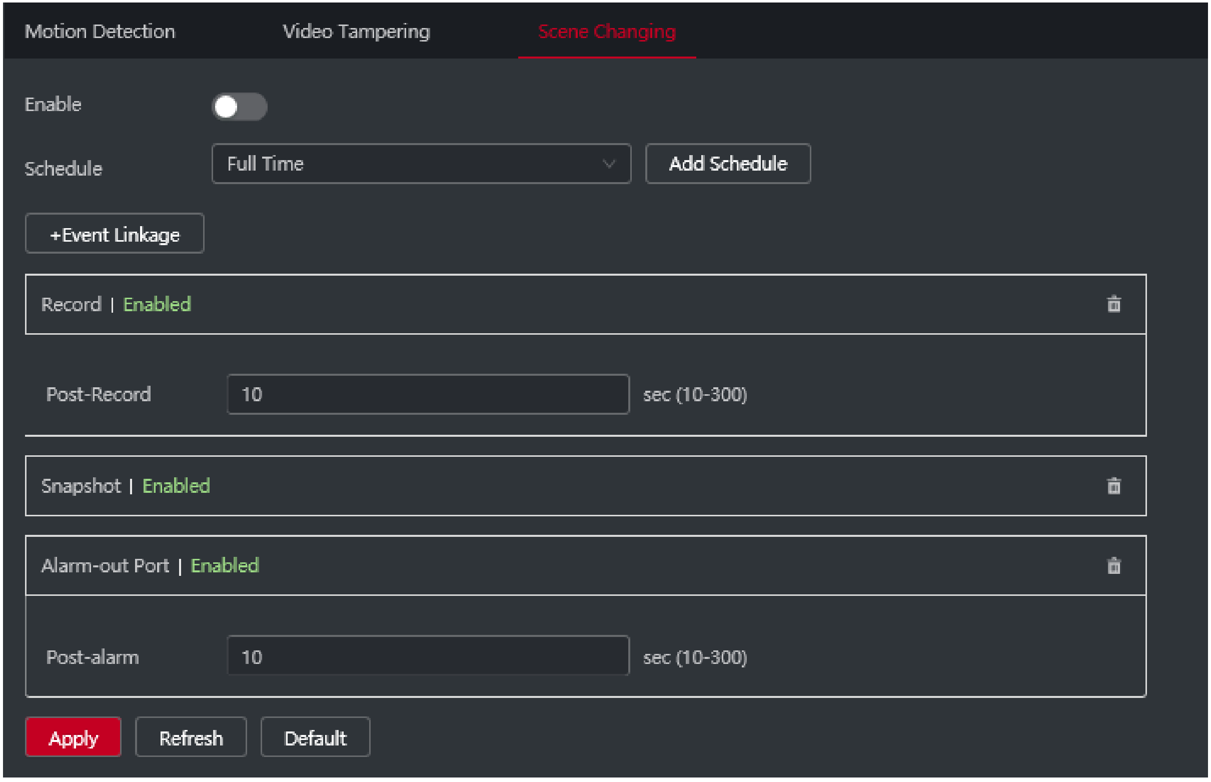
4.6.3.3. Scene Changing

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

Step 1 Select ⚙ → **Event** → **Video Detection** → **Scene Changing**.

Step 2 Select **Channel** and then click to enable the scene changing detection.

Figure 4-66



Enable

Schedule: Full Time

Record | Enabled

Post-Record: 10 sec (10-300)

Snapshot | Enabled

Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

Step 3 Set arming periods and alarm linkage action.

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

Anti-dither: After the **Anti-dither** time is set, the system only records one motion detectionevent in the period.

Step 4 Click **Apply**.

4.6.4. Audio Detection

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

Step 1 Select ⚙ → **Event → Audio Detection**.

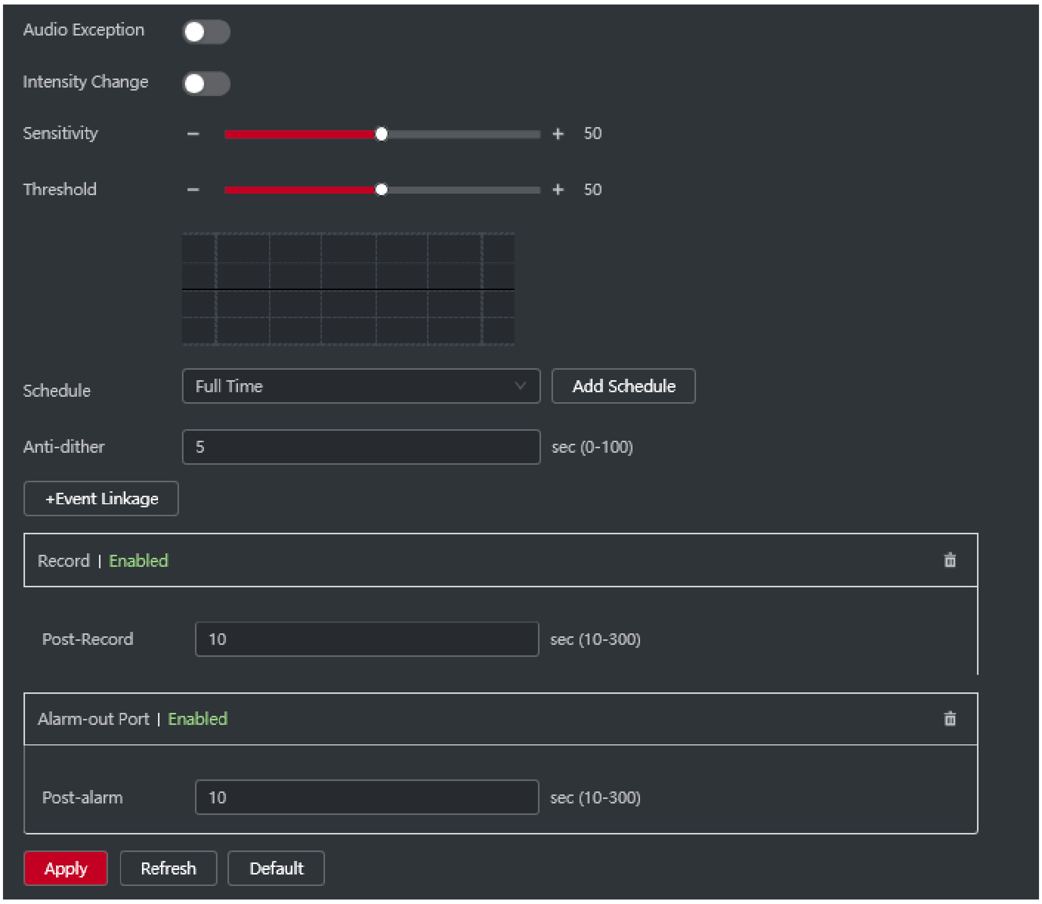
Step 2 (Optional) Select audio channels.

When the camera supports multiple audio channels, you can select different audio channels.

Step 3 Configure parameters of audio detection.

- Input abnormal: Click ○ to enable **Audio Exception**, and the alarm is triggered when the system detects abnormal sound input.
- Intensity change: Click ○ to enable **Intensity Change** and then configure **Sensitivity** and **Threshold**. The alarm is triggered when the system detects that thesound intensity exceeds the configured threshold.
    - The alarm is easier to be triggered with higher sensitivity or smaller threshold. Set ahigh threshold for noisy environment.
    - The red line in the waveform indicates audio detection is triggered, and the green one indicates no audio is detected. Adjust sensitivity and threshold according to thewaveform.

Figure 4-67



Audio Exception

Intensity Change

Sensitivity − + 50

Threshold − + 50

Schedule: Full Time

Add Schedule

Anti-dither: 5 sec (0-100)

+Event Linkage

Record | Enabled

Post-Record: 10 sec (10-300)

Alarm-out Port | Enabled

Post-alarm: 10 sec (10-300)

Apply

Refresh

Default

Step 4 Set arming periods and alarm linkage action

If the exiting schedules cannot meet the scene requirement, you can click **Add Schedule** to add a new schedule. Anti-dither: After the **Anti-dither** time is set, the system only records one motion detectionevent in the period.

Step 5 Click **Apply**.

4.7. Storage

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

Background Information

- If you enter an incorrect password for five consecutive times during authentication, password change or password clearing, the account will be locked for five minutes.
- Before using the recording and playback function, ensure that the SD card has been authenticated.
- The health status of the SD card is classified as follows.
  - Green: The SD card status is optimal.
  - Blue: The SD card status is good.
  - Orange: The SD card status is moderate.

    - Red: The SD card status is bad. Change the SD card in time.
- Functions might vary with different models.

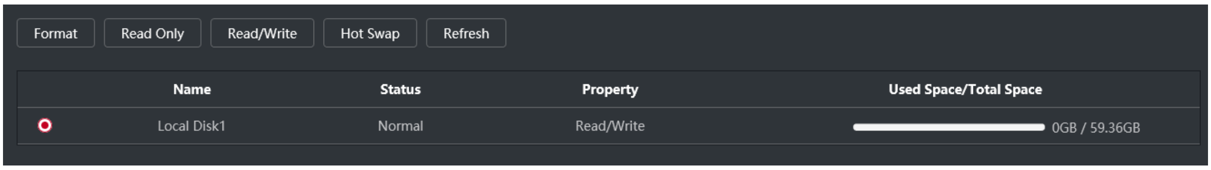
Procedure

Step 1 Select ⚙ → **Storage**.

Step 2 Select the SD card to be configured, and then perform the following operations as needed.

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

Figure 4-68



	Name	Status	Property	Used Space/Total Space
●	Local Disk1	Normal	Read/Write	0GB / 59.36GB

4.8. System

This section introduces system configurations, including general, date & time, account, peripheral management, manager and upgrade.

You can go to the **System** page through two methods. This following section uses method 1 as anexample.

- Method 1: Click ⚙ on the right-upper corner of the main page, and then click **System**.
- Method 2: Click **System** on the main page.

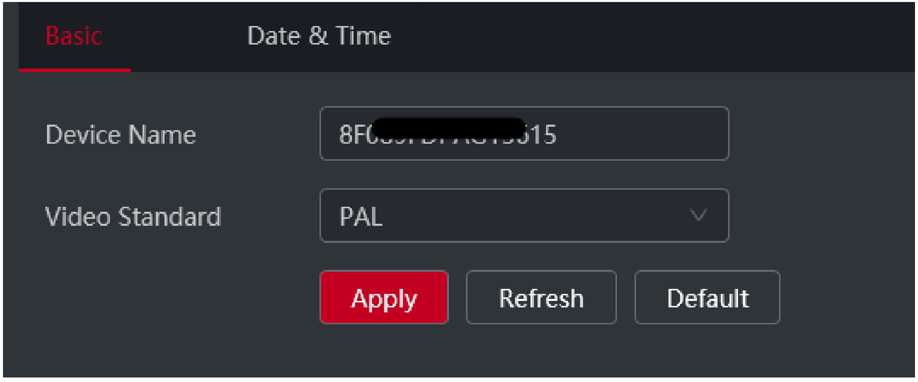
4.8.1. General

4.8.1.1. Basic

You can configure device name and video standard.

Step 1 Select ⚙ → **System** → **General** → **Basic**.

Figure 4-69



Device Name: 8F[redacted]15

Video Standard: PAL

Step 2 Configure general parameters.

Table 26

Parameter	Description
Name	Enter the device name. When a device is added by another device, the device name is displayed as the defined device name. 📖 Different devices have different names.
Video Standard	Select video standard from **PAL** and **NTSC**.
Analog Output	This function is available only for devices that support analogoutput. 📖 • Some devices automatically turn off AI function when enabling analog output, and automatically turn off analog output when enabling AI function. • Some devices support SDI (Serial Digital Interface) and HDCVI (High-Definition Composite Video Interface) function.

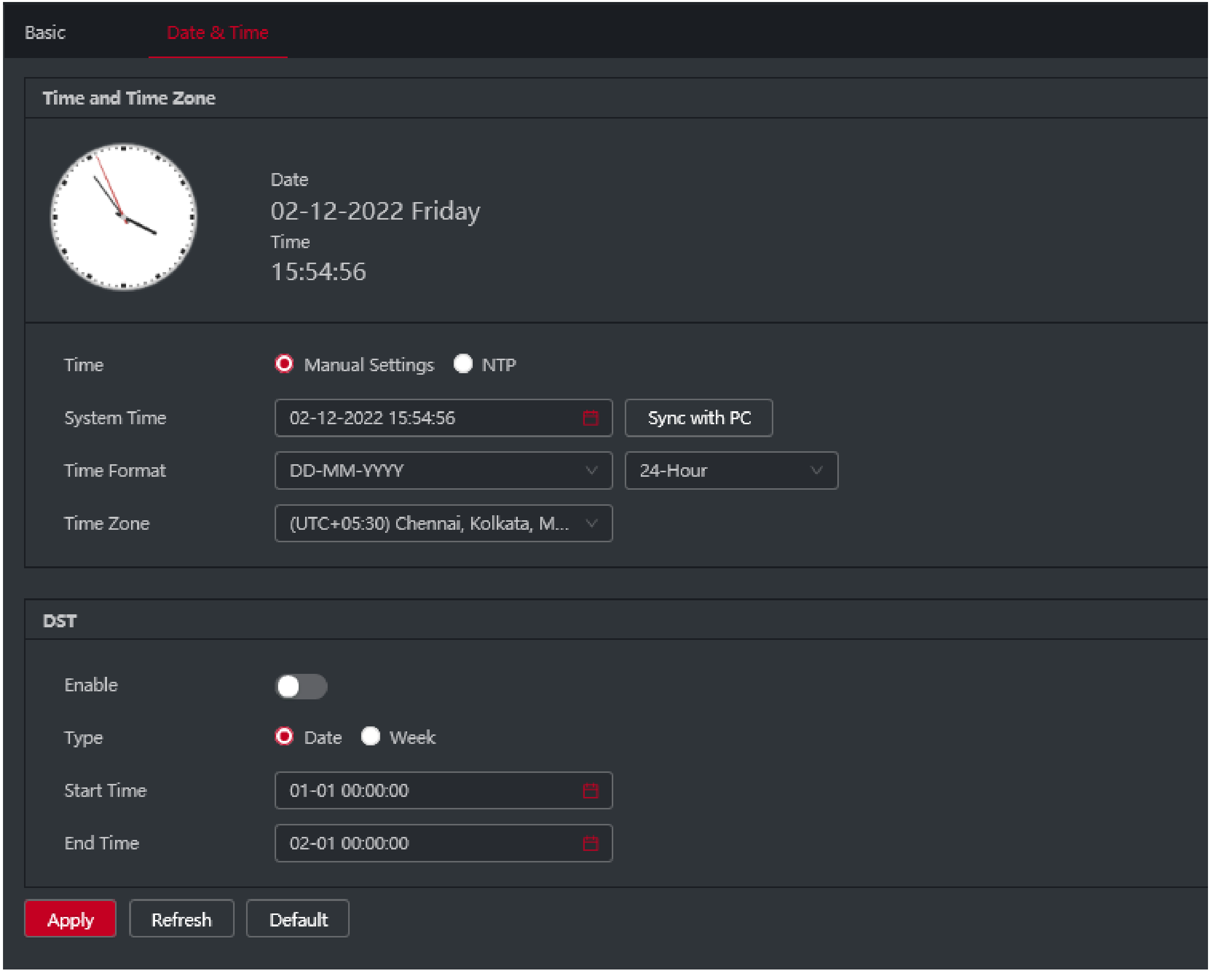
Step 3 Click **Apply**.

4.8.1.2. Date & Time

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

Step 1 Select ⚙ → **System** → **General** → **Date & Time**.

Figure 4-70



Time and Time Zone

Date
02-12-2022 Friday
Time
15:54:56

Time: ● Manual Settings ○ NTP

System Time: 02-12-2022 15:54:56 | Sync with PC

Time Format: DD-MM-YYYY | 24-Hour

Time Zone: (UTC+05:30) Chennai, Kolkata, M...

DST

Enable: off

Type: ● Date ○ Week

Start Time: 01-01 00:00:00

End Time: 02-01 00:00:00

Step 2 Configure date and time parameters.

Table 27

Parameter	Description
Time	• **Manually Setting**: Configure the parameters manually. • **NTP**: When selecting NTP, the system then syncs time with theinternet server in real time. You can also enter the IP address, time zone, port, and interval of a PC running NTP server to use NTP.
System Time	Configure system time. Click **Sync with PC**, and the system time changes to the PC time.

Parameter	Description
Time Format	Configure the time format.
Time Zone	Configure the time zone that the camera is at.
DST	Enable DST as needed. Click , and then configure start time and end time of DST with **Date** or **Week**.

Step 3 Click **Apply**.

4.8.2. Account

You can manage users, such as add, delete, or edit them. Users include admin, added users and ONVIF users. Only administrator users can manage users and groups. The operations include adding or deletingusers and user groups, modifying user information.

- The max. length of the user or group name is 31 characters which consist of number, letter, underline, dash, dot and @.
- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- You can have up to 18 users (excluding the admin user) and 1 anonymous user, and you can havesix user groups (excluding the admin and user groups).
- You can manage users through a single user or group, and duplicate usernames or group namesare not allowed. A user can only be in one group at a time, and the group users can only ownauthorities within the group authority range.
- Online users cannot edit their own authority.
- The default username of the system is admin, which has the highest authority.
- Select **Anonymous Login**, and then log in with only IP address instead of username and password. Anonymous users only have preview authorities. During anonymous login, click **Logout** to log in with another username.

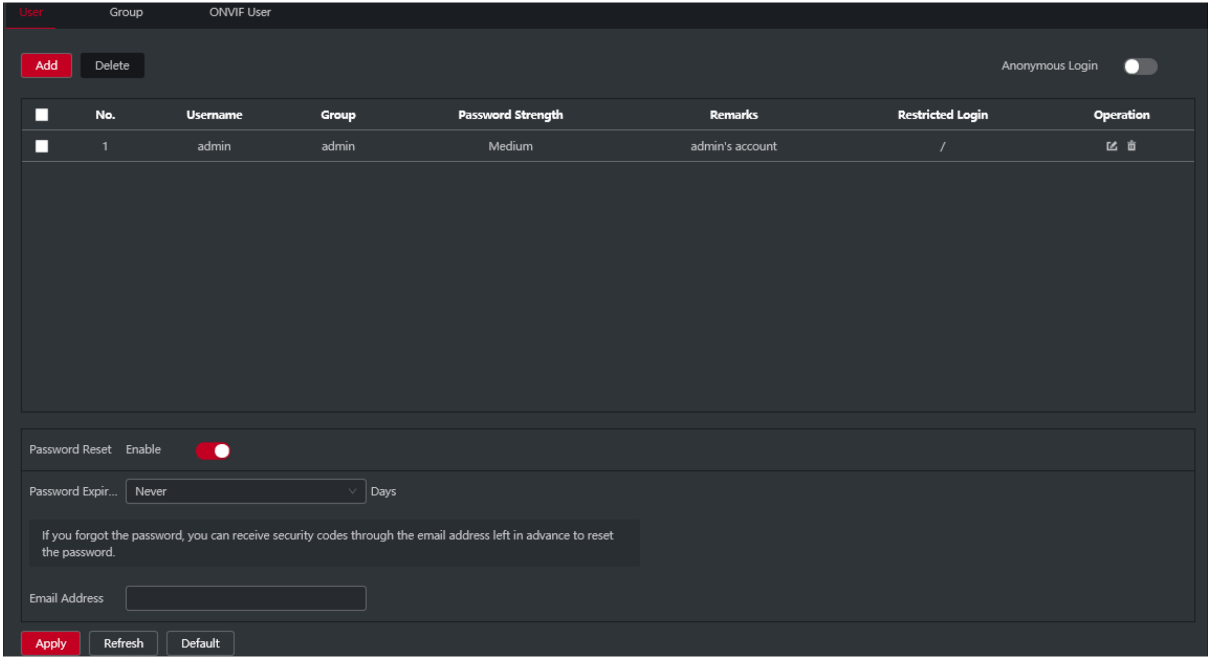
4.8.2.1. Adding User

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

Procedure

Step 1 Select ⚙ → **System** → **Account** → **User**.

Figure 4-71



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

Password Reset Enable

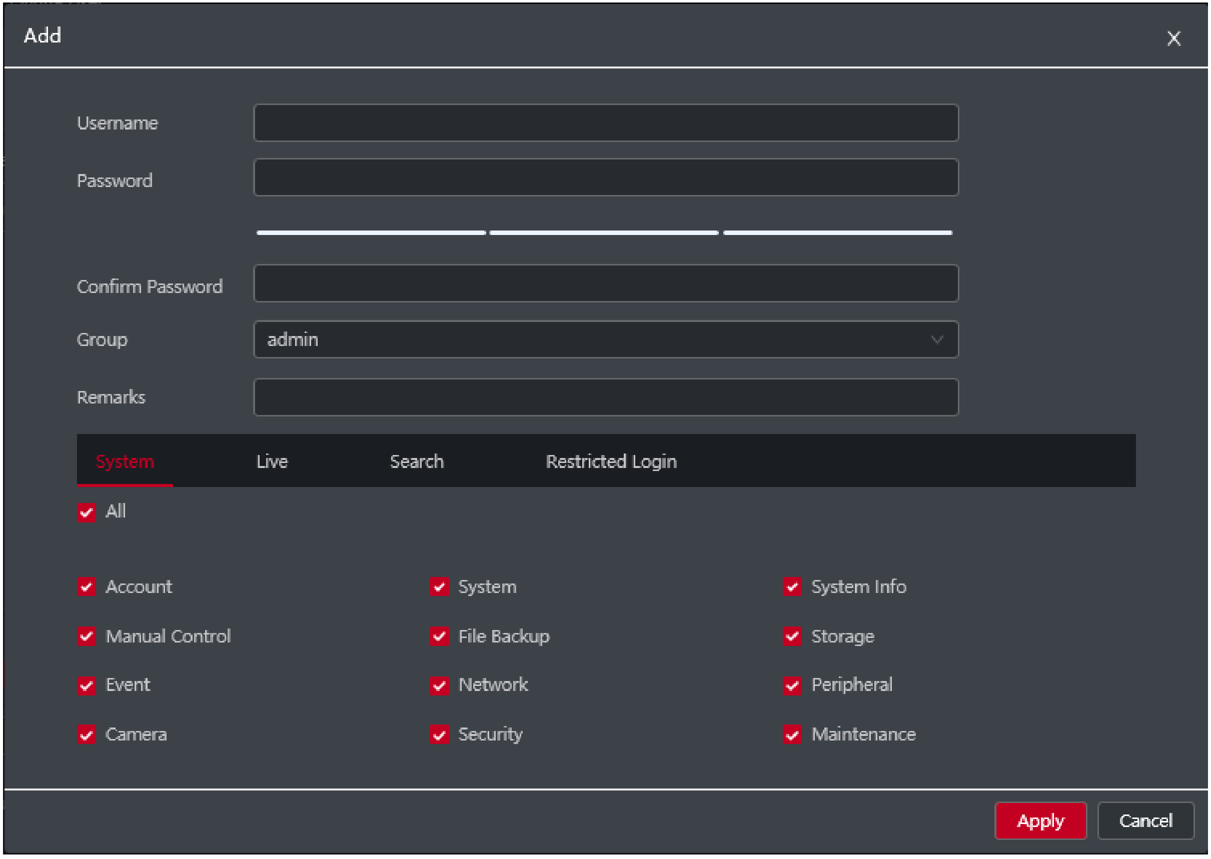
Password Expir... Never Days

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

Step 2 Click **Add**

Figure 4-72



Username

Password

Confirm Password

Group admin

Remarks

☑ All

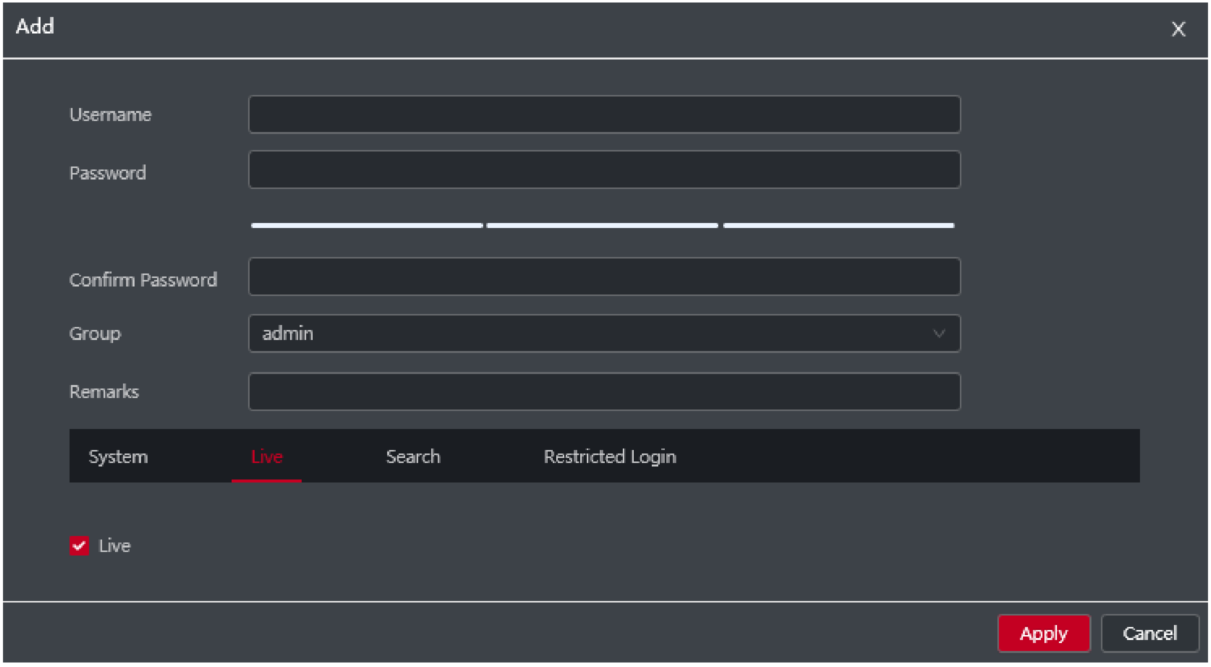
☑ Account ☑ System ☑ System Info

☑ Manual Control ☑ File Backup ☑ Storage

☑ Event ☑ Network ☑ Peripheral

☑ Camera ☑ Security ☑ Maintenance

Figure 4-73



Username

Password

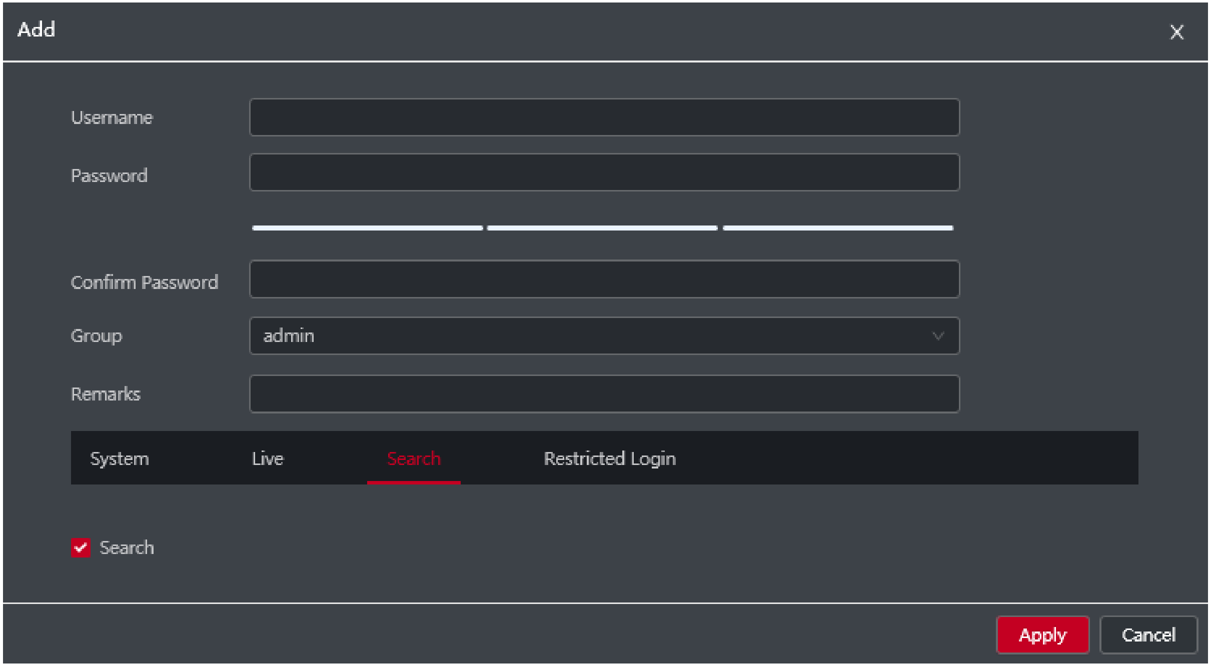
Confirm Password

Group: admin

Remarks

☑ Live

Figure 4-74



Username

Password

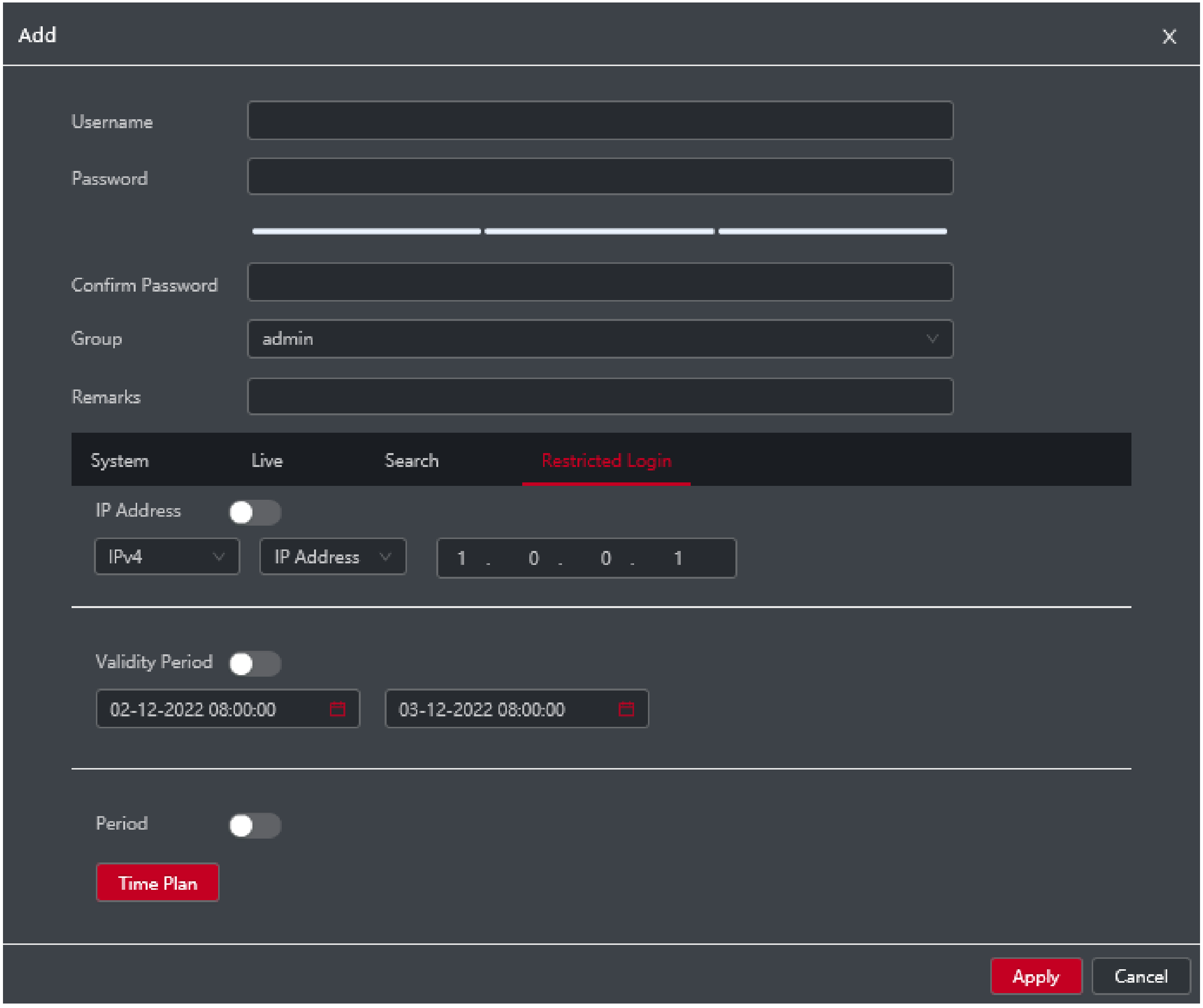
Confirm Password

Group: admin

Remarks

☑ Search

Figure 4-75



Group: admin

IP Address: IPv4, IP Address, 1 . 0 . 0 . 1

Validity Period: 02-12-2022 08:00:00 – 03-12-2022 08:00:00

Period

Step 3 Configure user parameters.

Figure 4-76

Parameter	Description
Username	User's unique identification. You cannot use existing username. The max. length of the user or group name is 31 characters which consist of number, letter, underline, dash, dot and @.
Password	Enter password and confirm it again.
Confirm Password	The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ' " ; : &). Seta high-security password based on the password strength prompt.
Group	The group that users belong to. Each group has differentauthorities.
Remarks	Describe the user.
System	Select system authorities as needed. 📖 We recommend giving fewer authorities to normal users than premium

Parameter	Description
	users.
Live	Select the live view authority for the user to be added.
Search	Select the search authority for the user to be added.
Restricted Login	Set the PC address that allows the defined user to log in to thecamera and the validity period and time range. You can log in tothe web page with the defined IP in the defined time range ofvalidity period. Set as follows: ○ Enable **IP address**, select IP type and then configure IPaddress. ○ IP address: Enter the IP address of the host to be added. ○ IP segment: Enter the start address and end address of thehost to be added. ○ Enable **Validity Period**, and then configure start and endtime. ○ Enable **Period**, and then click **Time Plan** to set the login period.

Step 4 Click **Apply**.

The newly added user is displayed in the user list.

Related Operations

- Modify user group information.

Click ✎ to edit password, group, remarks or authorities.

📖

For admin account, you can only edit the password.

- Delete user group.

Click 🗑 to delete the added user group.

📖

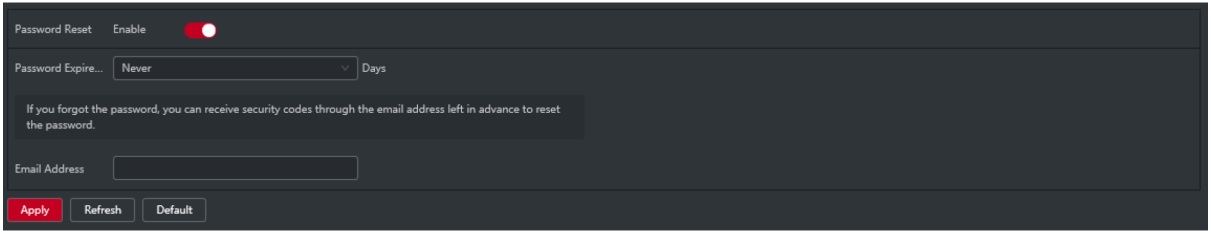
The admin account and user group cannot be deleted.

4.8.2.2. Resetting Password

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

Step 1 Select ⚙ → **System** → **Account** → **User**.

Figure 4-77



Password Reset Enable

Password Expire... Never Days

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Email Address

Step 2 Click to enable **Password Reset**.

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

Step 3 Enter the reserved email address.

After configuring the reserved email address, you can set a new password by clicking **Forgot password?** on the login page.

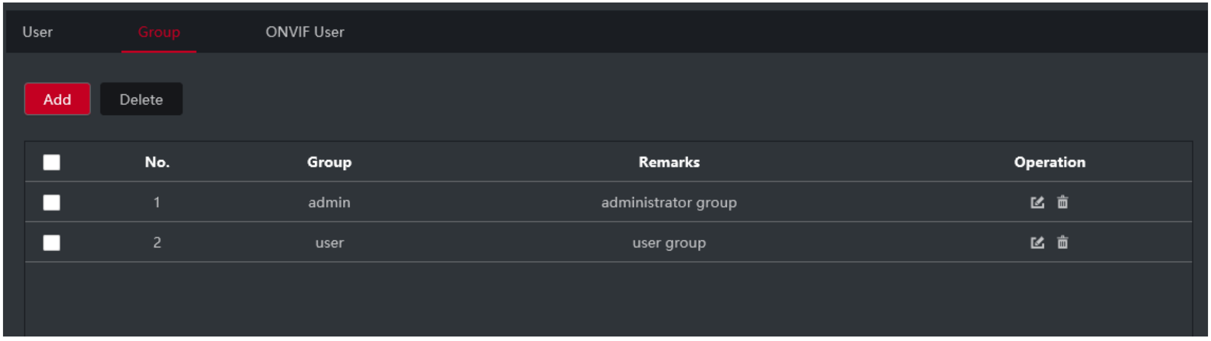
Step 4 Click **Apply**

4.8.2.3. Adding User Group

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

Step 1 Select ⚙ → **System** → **Account** → **Group**.

Figure 4-78

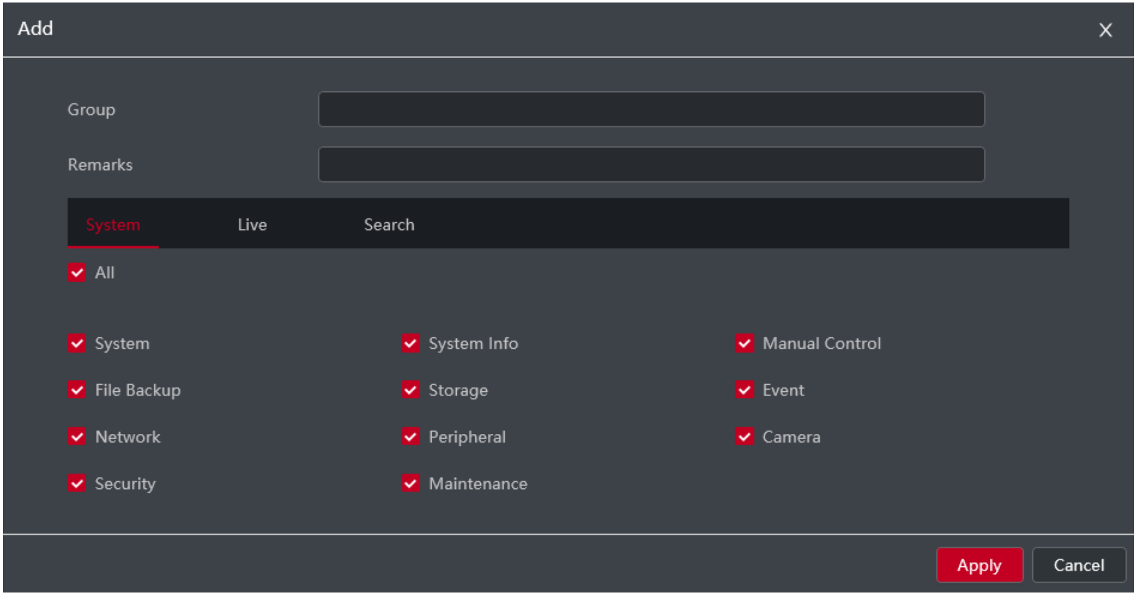


□	No.	Group	Remarks	Operation
□	1	admin	administrator group	
□	2	user	user group	

Step 2 Click **Add**.

Step 3 Enter the user group name and remarks, and then select the system, preview and playbackauthorities for the user group. The max length of the user or group name is 31 characters which consist of number, letter, underline, dash, dot and @.

Figure 4-79



☑ All

☑ System ☑ System Info ☑ Manual Control
☑ File Backup ☑ Storage ☑ Event
☑ Network ☑ Peripheral ☑ Camera
☑ Security ☑ Maintenance

Table 28

Group Authority	Admin	User	Functions
System	YES	NA	System time settingand more.
System Info	YES	NA	Version information,system logs and more.
Manual Control	YES	NA	PTZ settings.
File Backup	YES	NA	File backup.
Storage	YES	NA	Storage point configuration, snapshot recording time configuration, SFTP configurationand more.
Event	YES	NA	Video detection settings, audio detection settings, alarm settings andmore.
Network	YES	NA	IP settings, SMTP settings, SNMP settings, AP Hotspotsettings and more.
Peripheral	YES	NA	External light, wiperand serial port settings.
Camera	YES	NA	Camera property settings, audio andvideo settings andmore.
PTZ	YES	NA	Preset settings, toursettings and more.
Security	YES	NA	HTTPS settings, RTSP over TLS settings andmore.
Maintenance	YES	NA	Automatic maintenance settingsand more.

- Any user in the **Admin** group has **User** authorities to modify group authorities. The **User** group does not have this authority.
- The functions of the device correspond to the authority control respectively. Only user with specified authority can use corresponding function; the **Admin** group has all the authorities.

Step 4 Enter the group name and remarks, and then select group authorities.

Step 5 Click **OK** to finish configuration.

The newly added group displays in the group name list.

Related Operations

- Modify user group information.

Click ✎ to edit password, group, remarks or authorities.

For admin account, you can only edit the password.

- Delete user group.

Click 🗑 to delete the added users.

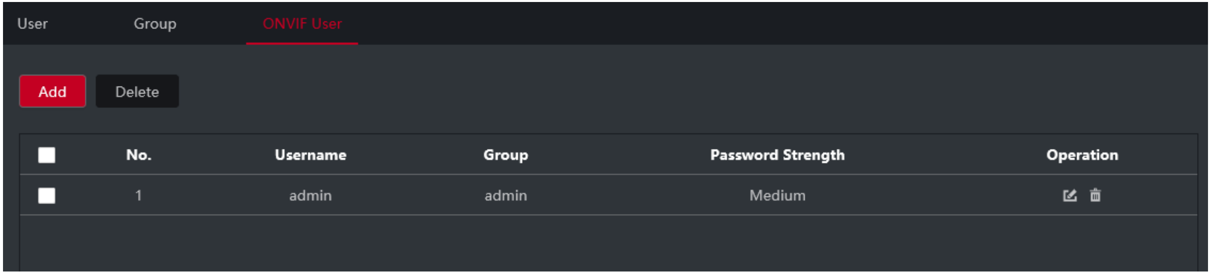
The admin account and user group cannot be deleted.

4.8.2.4. ONVIF User

You can add, delete ONVIF user, and change their passwords. The default ONVIF user is admin.

Step 1 Select ⚙ → **System** → **Account** → **ONVIF User**.

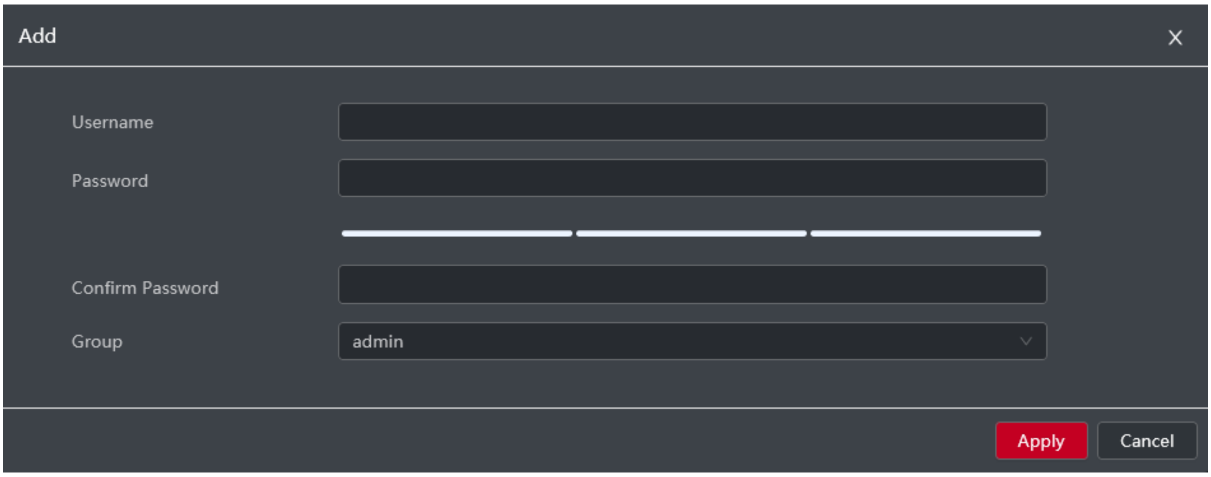
Figure 4-80



□	No.	Username	Group	Password Strength	Operation
□	1	admin	admin	Medium	✎ 🗑

Step 2 Click **Add**.

Figure 4-81



Username	
Password	
Confirm Password	
Group	admin

Step 3 Configure user parameters.

Table 29

Parameter	Description
Username	User's unique identification. You cannot use existed username. The max length of the user or group name is 31 characters whichconsist of number, letter, underline, dash, dot and @.
Password	Enter password and confirm it again. The password must consist of 8 to 32 non-blank characters andcontain at least two types of characters among upper case, lowercase, number, and special character (excluding ' " ; : &).
Confirm Password	
Group Name	The group that users belong to. Each group has differentauthorities.

Step 4 Click **OK**.

The newly added user displays in the username list.

Related Operations

- Modify user group information.

Click ✎ to edit password, group, remarks or authorities.

📖

For admin account, you can only edit the password.

- Delete user group.

Click 🗑 to delete the added users.

📖

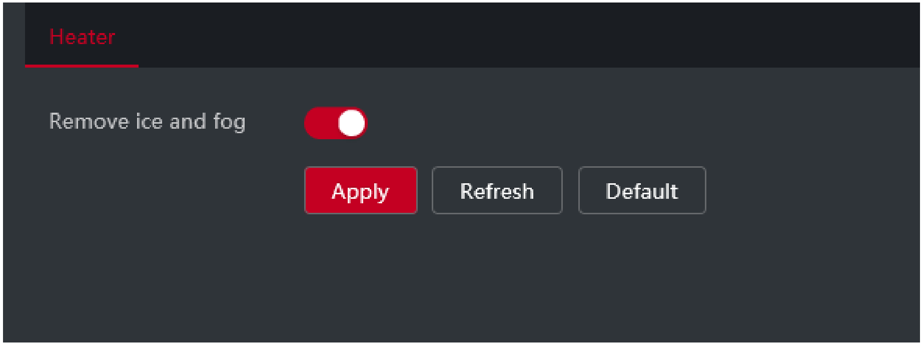
The admin account cannot be deleted.

4.8.3. Peripheral Management

Step 1 Select ⚙ → **System** → **Peripheral** → **Heater**.

Step 2 Click ○ to enable the Heater for removing Ice and fog from Camera lens.

Figure 4-82



4.8.4. Manager

4.8.4.1. Requirements

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

- Check surveillance images regularly.
- Clear regularly user and user group information that is not frequently used.
- Change the password every three months.
- View system logs and analyze them and process the abnormity in time.
- Back up the system configuration regularly.
- Restart the device and delete the old files regularly.
- Update firmware in time.

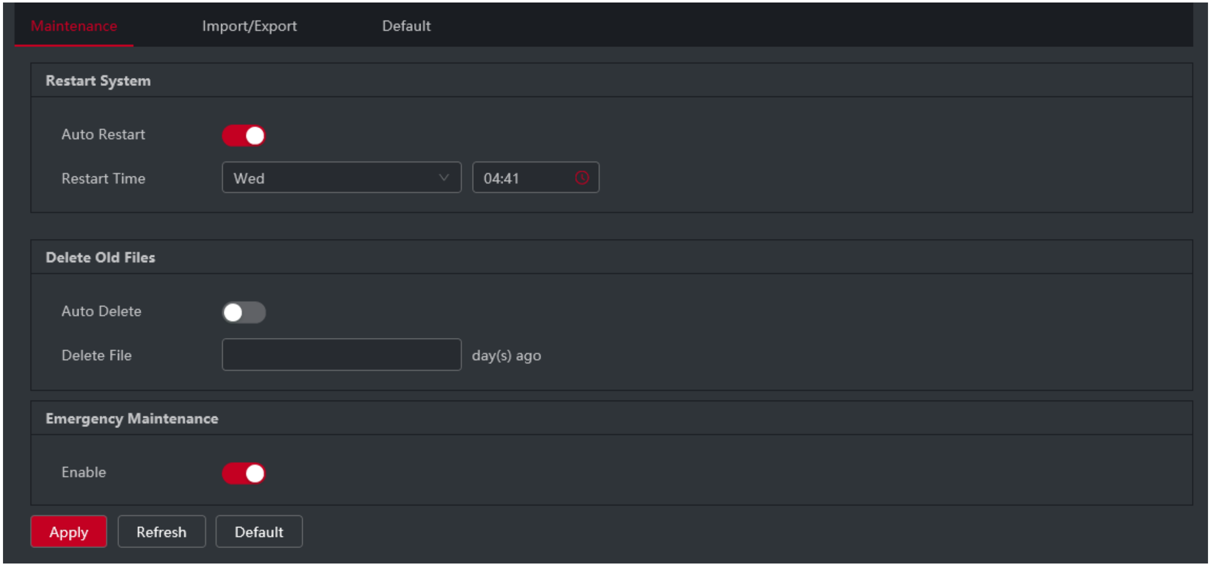
4.8.4.2. Maintenance

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

This function is disabled by default.

Step 1 Select ⚙ → **System** → **Manager** → **Maintenance**.

Figure 4-83



Restart System

Auto Restart ●

Restart Time: Wed 04:41

Delete Old Files

Auto Delete ○

Delete File: day(s) ago

Emergency Maintenance

Enable ●

Step 2 Configure auto maintain parameters.

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

📖

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

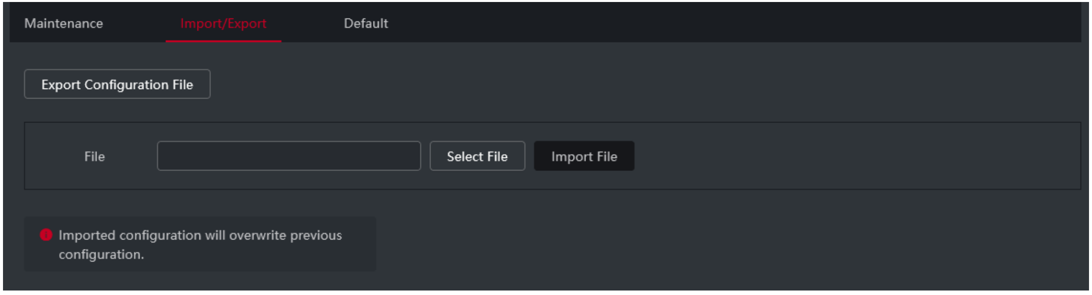
Step 3 Click **Apply**.

4.8.4.3. Import/Export

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

Step 1 Select ⚙ → **System** → **Manager** → **Import/Export**.

Figure 4-84



Imported configuration will overwrite previous configuration.

Step 2 Import and export.

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

4.8.4.4. Default

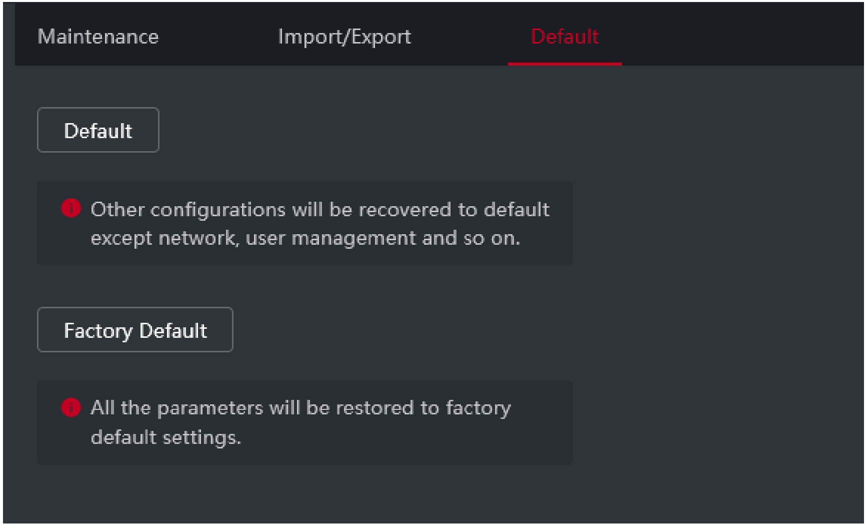
Restore the device to default configuration or factory settings.

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

Select ⚙ → **System** → **Manager** → **Default.**

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

Figure 4-85



Other configurations will be recovered to default except network, user management and so on.

All the parameters will be restored to factory default settings.

4.8.5. Upgrade

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

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

a. Online Upgrade

Step 1 Select ⚙ → **System** → **Upgrade**.

Step 2 Click on Manual check button to check new firmware release on server, System detects the new version on the cloud.

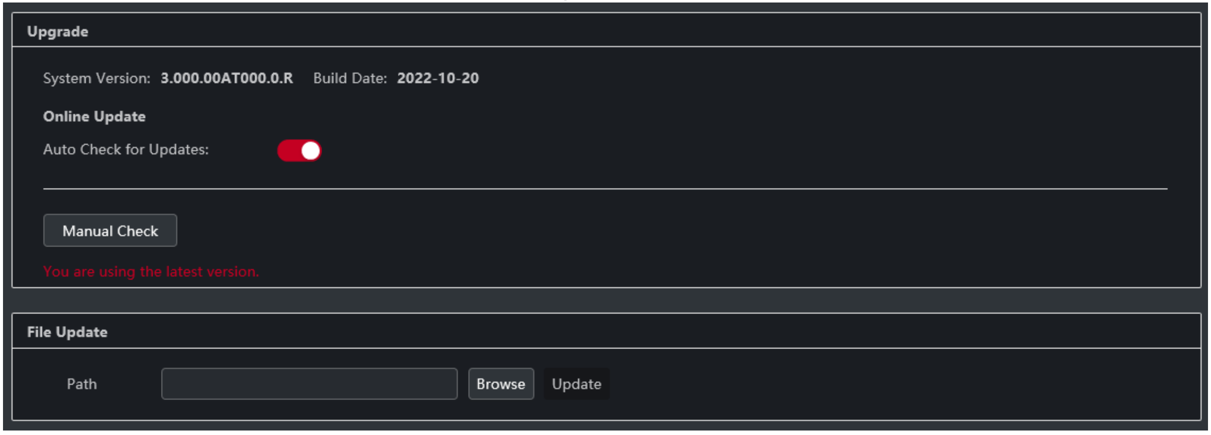
Step 3 Click on online upgrade.

Step 4 After successful operation, system pops up upgrade successful dialogue box.

b. Manual Upgrade

Step 1 Select ⚙ → **System** → **Upgrade**.

Figure 4-86



Upgrade

System Version: **3.000.00AT000.0.R** Build Date: **2022-10-20**

Online Update

Auto Check for Updates: ●

You are using the latest version.

File Update

Path

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

The upgrade file should be a .bin file.

Step 3 Click **Upgrade**.

The upgrade starts.

4.9. System Information

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

4.9.1. Version

View the **ONVIF Version**, **System Version**, **Web Version,** and other information of the Camera.

Select ⚙ →**System Info** → **Version** to view the version information of the Camera.

4.9.2. Online User

View all the current users logging into the web.

Select ⚙ → **System Info** → **Online User** to view all the current users logging into the Camera.

4.9.3. Legal Info

View the **Software License Agreement**, **Privacy Policy**, **Open-Source Software Notice** of theCamera.

Select ⚙ → **System Info** → **Legal Info** to view the legal information of the Camera.

4.10. Log

4.10.1. Log

You can view and back up logs.

Step 1 Select ⚙ → **Log** → **Log**.

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

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

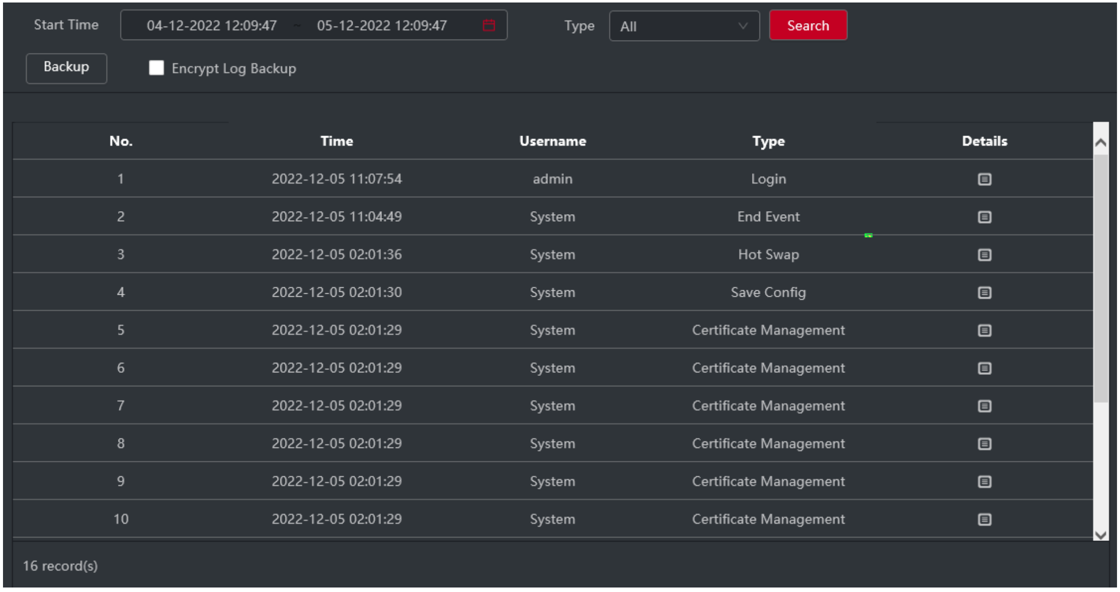
The log type includes **All**, **System**, **Setting**, **Data**, **Event**, **Record**, **Account**, and **Security.**

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

Step 3 Click **Search**.

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

Figure 4-87



Start Time 04-12-2022 12:09:47 ~ 05-12-2022 12:09:47 Type All Search

Backup □ Encrypt Log Backup

No.	Time	Username	Type	Details
1	2022-12-05 11:07:54	admin	Login	▤
2	2022-12-05 11:04:49	System	End Event	▤
3	2022-12-05 02:01:36	System	Hot Swap	▤
4	2022-12-05 02:01:30	System	Save Config	▤
5	2022-12-05 02:01:29	System	Certificate Management	▤
6	2022-12-05 02:01:29	System	Certificate Management	▤
7	2022-12-05 02:01:29	System	Certificate Management	▤
8	2022-12-05 02:01:29	System	Certificate Management	▤
9	2022-12-05 02:01:29	System	Certificate Management	▤
10	2022-12-05 02:01:29	System	Certificate Management	▤

16 record(s)

4.10.2. Remote Log

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

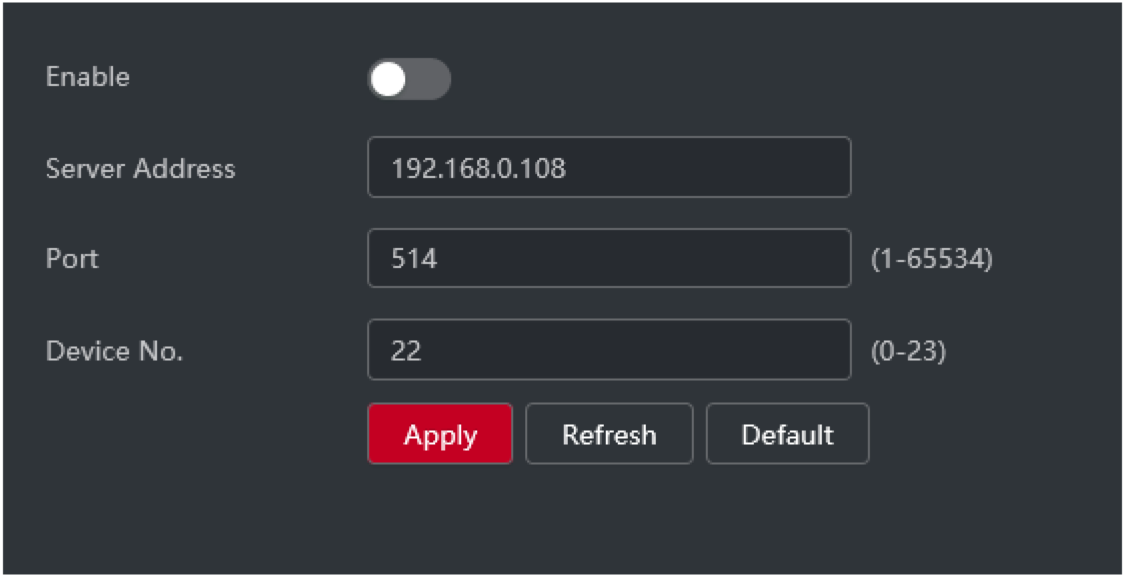
Step 1 Select →**Log**→**Remote Log**.

Step 2 Click to enable remote log function.

Step 3 Configure address, port and device number.

Step 4 Click **Apply**

Figure 4-88



Enable

Server Address 192.168.0.108

Port 514 (1-65534)

Device No. 22 (0-23)

5. Live

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

5.1. Live Page

This section respectively describes the **Live** page for single-channel and multi-channel devices. Click **Live** on the main web page to enter **Live** page.

Pages might vary with different models.

Figure 5-1

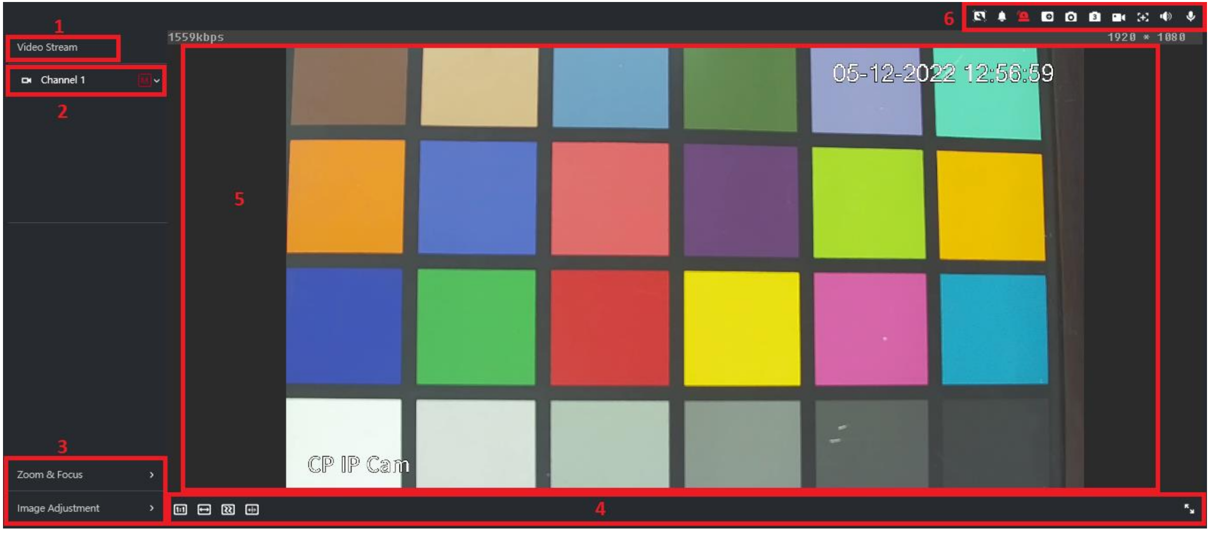


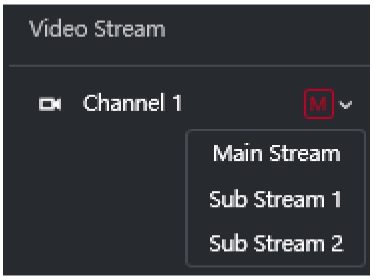
Table 30

Number	Function	Description
1	Display mode	Switches the video display mode. It includes general mode, face mode and metadata mode
3	Image adjustment	Adjusts the images in the live viewing.
4		
5	Live view	Displays the real-time monitoring image.
6	Live view function bar	Displays the shortcut for available functions. Among them, some shortcut buttons of multi-channel devices are in the upper-right corner of the channel screen.

5.2. Configuring Encoding

On the left side of the **Live** page, click ⌄ on the right side of the video channel to select the videostream.

Figure 5-2



- **Mainstream**: It has large bit stream value and image with high resolution, but also requires large bandwidth. This option can be used for storage and monitoring.
- **Sub Stream**: It has small bit stream value and smooth image and requires less bandwidth. This option is normally used to replace mainstream when bandwidth is not enough.
- means the current stream is mainstream; S1 means the current stream is sub stream 1; S2 means the current stream is sub stream 2.

Click this icon to choose whether to display the video image.

5.3. Live View Function Bar

This section introduces the shortcuts supported when viewing live video.

- Whether it is single-channel or multi-channel, the icons of "Force Alarm", "Aux Focus" and "Talk" are the same, all above **Live** page.
- Icons for other functions are on the top of the **Live** page for single-channel devices and on thetop right corner of the **Live** page for multi-channel devices.

Table 31

Icon	Function	Description
🚨	ForceAlarm	Displays alarm output state of the corresponding channel. Whenthe alarm output page is connected to the alarm output device, click the icon to force to enable or disable alarm output. ● Red: Alarm output enabled. ● Black: Alarm output disabled.
⊕	Digital Zoom	Zoom in the selected area, drag the screen in the zoomed-instatus to view other areas. You can zoom video image through two operations. ● Click the icon, and then select an area in the live image to zoom in; right-click on the image to resume the original size. ● Click the icon, and then scroll the mouse wheel in the videoimage to zoom in or out.

📷	Snapshot	Capture one image of the current screen, and it will be saved tothe configured storage path.
3	Triple Snapshot	Capture three images of the current screen, and they will besaved to the configured storage path.
📹	Record	Record video, and it will be saved to the configured storage path.
✛	Manual Position	Select the area in the panorama camera screen, and the detail camera screen will be automatically positioned to the selected area.
🔊	Sound	Enable or disable audio output of corresponding channel.
🎤	Talk	Enable or disable the audio talk.

5.4. Window Adjustment Bar

5.4.1. Adjustment

This section introduces the adjustment of image.

Table 32

Icon	Function	Description
1:1	Original Size	Only single-channel devices display this icon. Click thisicon and when the icon changes to 1:1, the actual sizeof the screen is displayed. Click the icon again to restore the screen to the appropriate size
↔	W:H	Click the icon to resume original ratio or change ratio.It supports **Original** and **Adaptive**.
≪	Fluency Adjustment	Click the icon to adjust the fluency of the image. Itsupports **Realtime**, **Fluent** and **General**. ● **Realtime**: Guarantees the real time of the image.When the bandwidth is not enough, the image might not be smooth. ● **Fluent**: Guarantees the fluency of the image. There might be delay between live view imageand real-time image. ● **General**: It is between Realtime and Fluent.
⇹	AI Rule	Click the icon, and then select **Enable** to display AIrules and detection box; select **Disable** to stop thedisplay. It is enabled by default.

5.4.2. PTZ Control

You can rotate device, zoom image, and adjust iris through PTZ control. On the **Live** page, click the **PTZ control** on the lower left corner to adjust the current video screen.

Figure 5-3

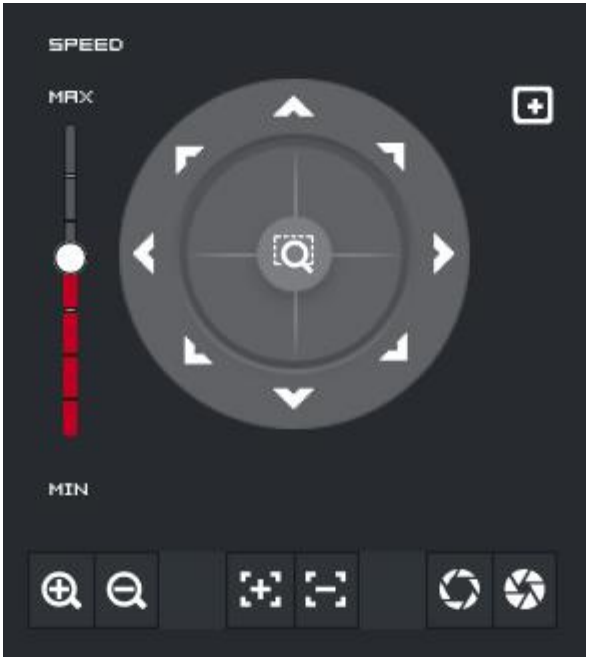
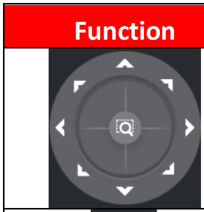
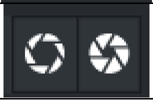


Table 33

Function	Description
	Control device toward eight directions, including up, down, left, right, left up, right up, left down and right down. Click , and then select an area in the monitor frame, the PTZ will rotate and zoom quickly to the specified area.
	Speed: The speed value changes device rotate speed. The bigger the value is, the faster the device rotates. For example, the rotation with a speed of 8 is much faster than that of 1.
	Zoom: Adjust the zooming of images.
	Focus: Adjust the focal length of the Camera.
	Iris: Adjust the brightness of images.
	Area Focus: Focus on the selected area. Select the Live page, click the icon, and select the area on the Live page. Then the device will automatically focus on this area.

5.4.3. PTZ Function

On the **Live** page, click the **PTZ Function** on the lower left corner of the page.

📖

The value range of the PTZ function (such as preset and tour) depends on the specific PTZ protocol.

Figure 5-4

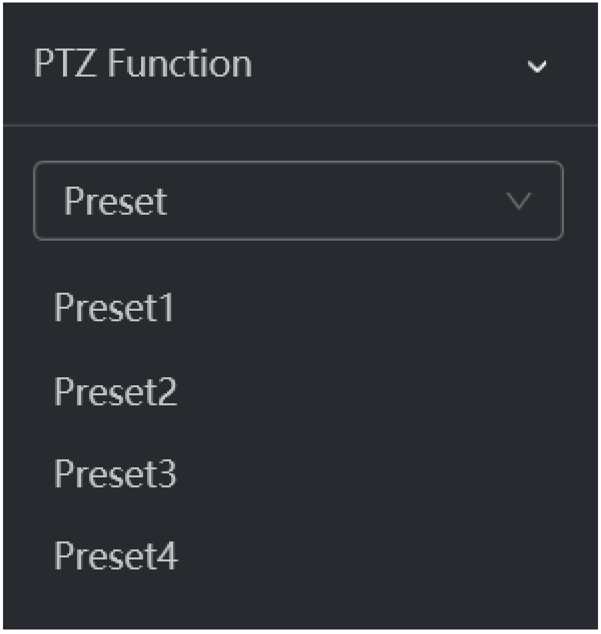


Table 34

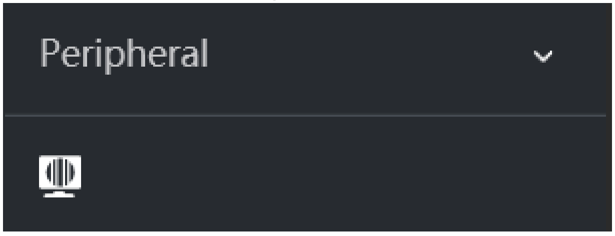
Parameter	Description
Scan	Configure the scan number. Click **Start**, and the device will scan back and forth at a certain speed according to the set boundary.Click **Stop** to finish scan.
Preset	Configure preset number, and then click **View** to position the deviceto the corresponding point. The preset contains PTZ's horizontal angle, tilt angle, lens focal length and other parameters.
Tour	Configure tour number. Click Start and the device automatically rotates back and forth in the order of the set preset points. Click Stop to finish tour.
Pattern	Configure pattern number. Click Start and the device automatically rotates back and forth according to the set operating record. Click Stop to finish pattern. The operation record includes the manual operations that the performed to the PTZ, and the changes in focus and zoom.
Pan	Click Start, and then the Camera starts continuous 360° rotation in a horizontal way at a certain speed.
Go to	Configure horizontal angle, vertical angel and zoom. Click Go to pinpoint to a point.

5.4.4. Peripheral Management

Manage peripherals of PTZ Camera.

Step 1 On the **Live** page, click the **Peripheral Management** on the lower left corner of the page.

Figure 5-5



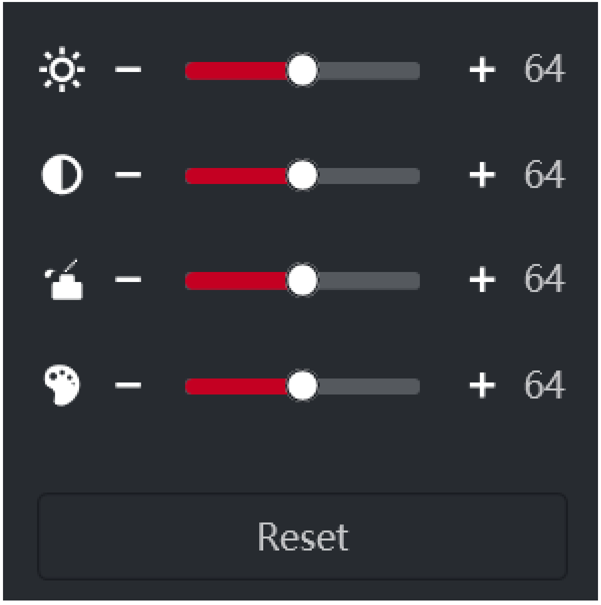
Step 2 Click to enable or disable water removal function.

5.4.5. Image Adjustment

Click **Image Adjustment** on the lower-left corner of **Live** page, and click **+** or**–** icon, or drag theslider to adjust image parameters, including brightness, contrast, hue and saturation.

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

Figure 5-6



- ☼ (Brightness adjustment): Adjusts the overall image brightness and changes the value when the image is too bright or too dark. The bright and dark areas will have equal changes.
- ◐ (Contrast adjustment): Changes the value when the image brightness is proper, but contrast isnot

enough.

- (Saturation adjustment): Adjusts the image saturation, this value does not change imagebrightness.
- (Hue adjustment): Makes the color deeper or lighter. The default value is made by the lightsensor, and it is recommended.

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

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

6. Record

This chapter introduces the functions of video playback and operations of record control, record plan and record storage.

6.1. Playback

This section describes the operations of video playback and management. It supports editing and downloading videos.

6.1.1. Playing Back Video

Query and playback video files stored in the SD card.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back video, configure record time range, record storage method, record schedule and record control.

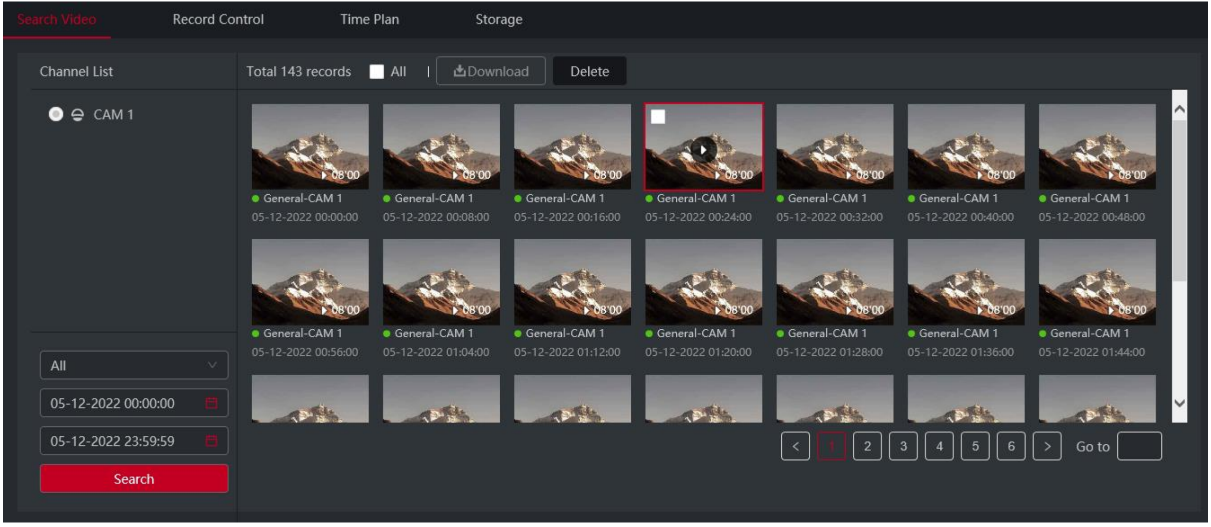
Procedure

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

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

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

Figure 6-1



All

05-12-2022 00:00:00

05-12-2022 23:59:59

Step 3 Point to the searched video, and then click ▶ to play back the selected video.

Figure 6-2

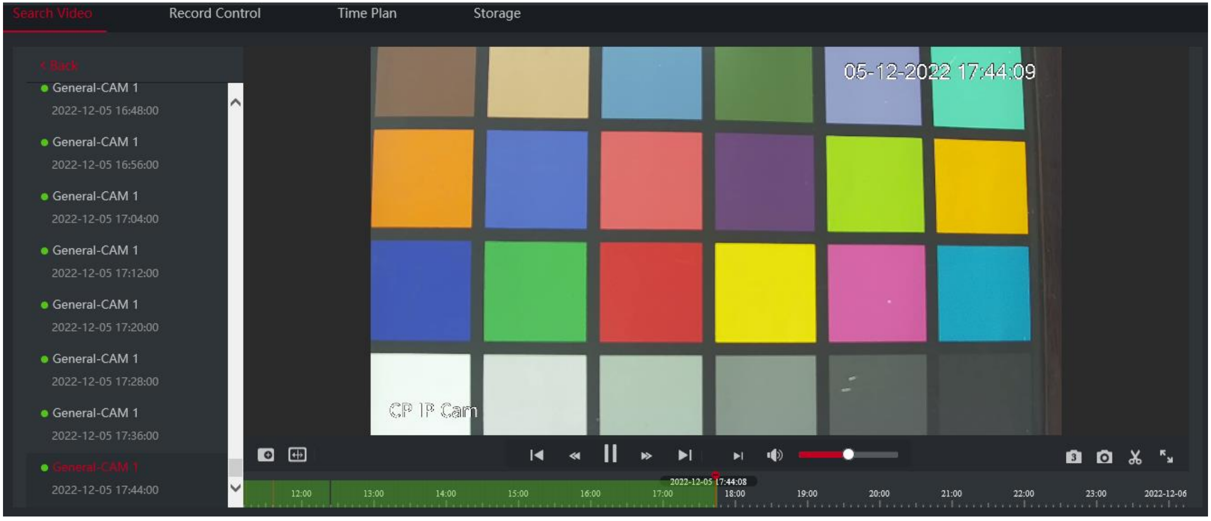


Table 35

No	Icon	Function	Description
1	Recorded video list		Displays all searched recorded video files. Click any files to view the recording. Click **Back** at the upper-left corner to go tothe **Search Video** page.
2	⊕	Digital Zoom	You can zoom in or out video image of theselected area through two operations. ● Click the icon, and then select an area in the video image to zoom in; right-click on the image to resume the original size. In zoom in state, drag the image to check other area. ● Click the icon, and then scroll the mouse wheel in the video image to zoom in orout.
	⊞	AI Rule	Click the icon, and then select **Enable** todisplay AI rules and detection box; select **Disable** to stop displaying AI rules. It is disabled by default. 📖 AI rules are valid only when you enabled therule during recording.
	Play control bar		Controls playback. ● ⏮: Click the icon to play the previous recorded video in the recorded video list. ● ⏪: Click the icon to slow down theplayback. ● ⏸: Click the icon to stop playing recorded videos. The icon changes to ▶, click the icon toplay recorded

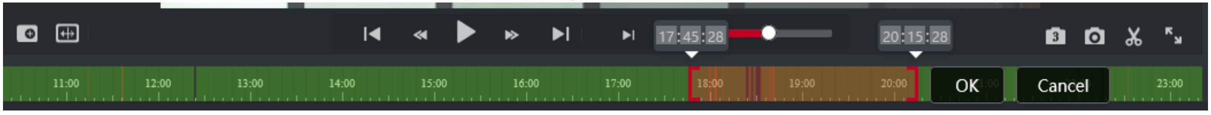
No	Icon	Function	Description
			videos. ● ⏩: Click the icon to speed up theplayback. ● ⏭: Click the icon to play the next recorded video in the recorded video list. ● ⏯: Click the icon to play the next frame.
	🔊	Sound	Controls the sound during playback. ● 🔇: Mute mode. ● 🔊: Vocal state. You can adjust the sound.
	📷	Snapshot	Click 📷 to capture one image of the currentscreen, and it will be saved to the configured storage path.
	✂	Video clip	Click ✂, and clip a certain recorded video and save it.
	⤢	Full screen	Click ⤢ , and the image is displayed in **full screen:** double-click the image or press Esc key to exit.
3	Progress bar	—	Displays the record type and the corresponding period. ● Click any point in the colored area, and the system will play back the recorded video from the selected moment. ● Each record type has its own color, and you can see their relations in Record Type bar.

6.1.2. Clipping Video

Step 1 Click ⌗ below the video during playback.

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

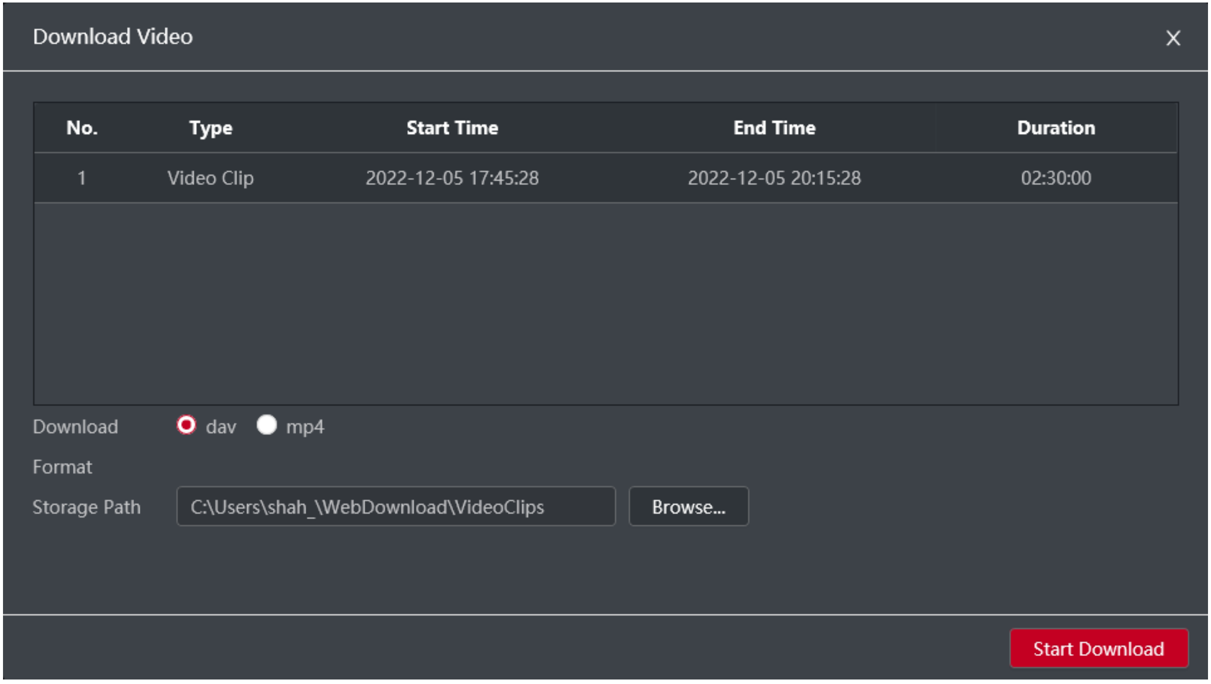
Figure 6-3



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

Step 4 Select the download format and storage path.

Figure 6-4



Download Video

No.	Type	Start Time	End Time	Duration
1	Video Clip	2022-12-05 17:45:28	2022-12-05 20:15:28	02:30:00

Download Format ● dav ○ mp4

Storage Path C:\Users\shah_\WebDownload\VideoClips

Step 5 Click **Start Download**.

The playback stops and the clipped file is saved in the configured storage path.

6.1.3. Downloading Video

Download videos to a defined path. You can download a single video or download videos inbatches.

- Playback and download at the same time is not supported.
- Operations might vary with different browsers.

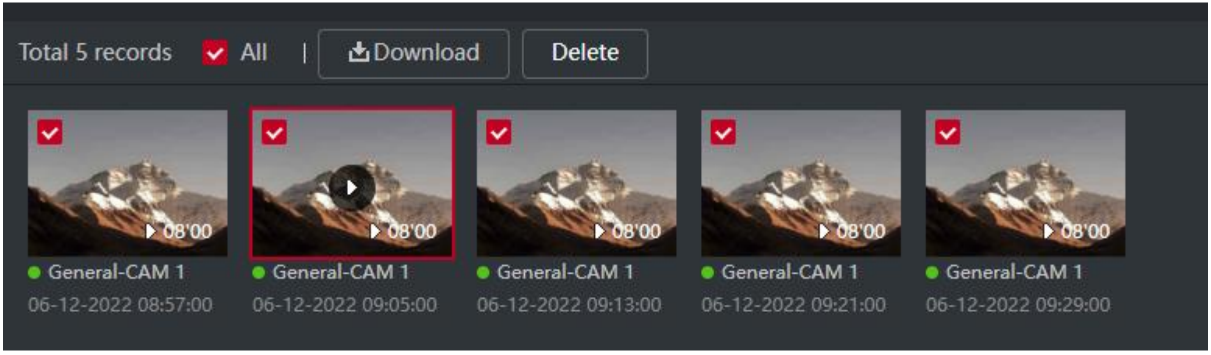
Step 1 Select **Record → Search Video**.

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

Step 3 Select videos to be downloaded.

- Select □ at the upper-right corner of each video file to select one or more videos. Theicon at the upper left corner of the selected file changes to ☑.
- Select □ next to **Select All** to select all searched videos.

Figure 6-5



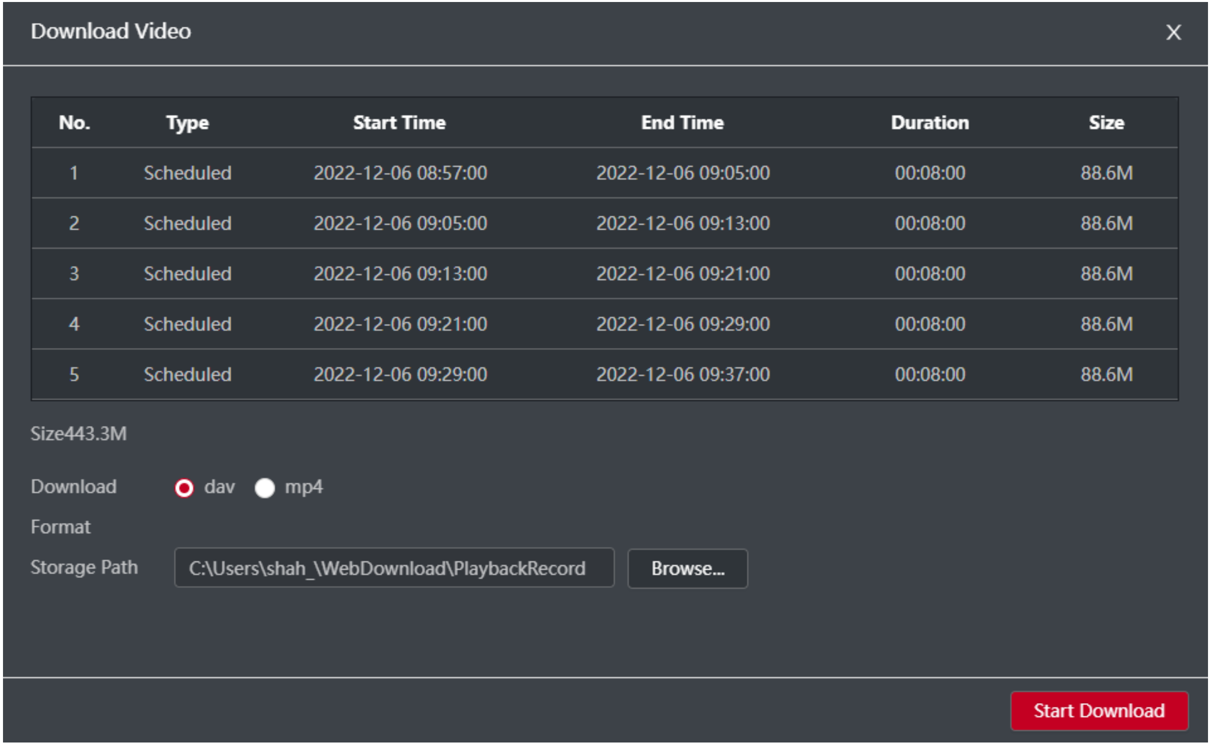
Total 5 records ☑ All | Download Delete

☑ 08'00	☑ 08'00	☑ 08'00	☑ 08'00	☑ 08'00
● General-CAM 1	● General-CAM 1	● General-CAM 1	● General-CAM 1	● General-CAM 1
06-12-2022 08:57:00	06-12-2022 09:05:00	06-12-2022 09:13:00	06-12-2022 09:21:00	06-12-2022 09:29:00

Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 6-6



Download Video ×

No.	Type	Start Time	End Time	Duration	Size
1	Scheduled	2022-12-06 08:57:00	2022-12-06 09:05:00	00:08:00	88.6M
2	Scheduled	2022-12-06 09:05:00	2022-12-06 09:13:00	00:08:00	88.6M
3	Scheduled	2022-12-06 09:13:00	2022-12-06 09:21:00	00:08:00	88.6M
4	Scheduled	2022-12-06 09:21:00	2022-12-06 09:29:00	00:08:00	88.6M
5	Scheduled	2022-12-06 09:29:00	2022-12-06 09:37:00	00:08:00	88.6M

Size443.3M

Download Format ● dav ○ mp4

Storage Path C:\Users\shah_\WebDownload\PlaybackRecord Browse...

Start Download

Step 6 Click **Start Download**.

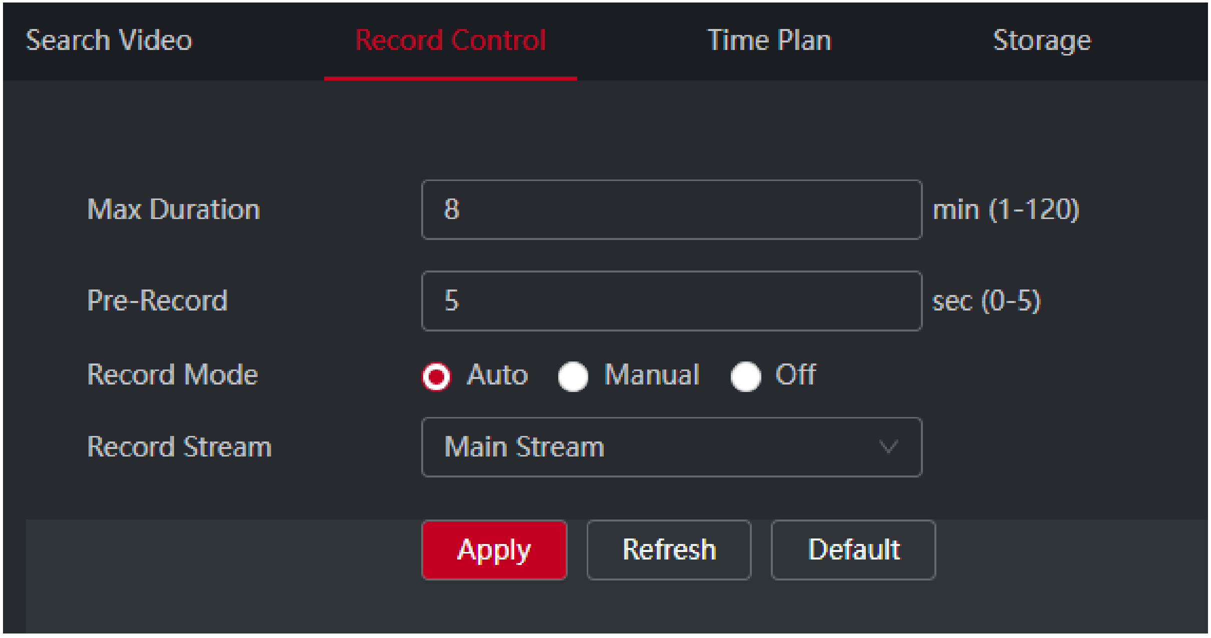
The system starts to download the video and displays the download progress. After the video is downloaded successfully, the video file is saved in the configured storage path.

6.2. Record Control

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

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

Figure 6-7



Max Duration 8 min (1-120)

Pre-Record 5 sec (0-5)

Record Mode ● Auto ○ Manual ○ Off

Record Stream Main Stream

Step 2 Set parameters.

Table 36

Parameter	Description
Max Duration	The time for packing each video file.
Pre-Record	The time to record the video in advance of a triggered alarm. Forexample, if the pre-event record is set to be 5 s, the system savesthe recorded video 5 s before the alarm. 🕮 When an alarm or motion detection links recording, and the recording is not enabled, the system saves the recording within thepre-event record time to the video file.
Record Mode	• **Manual**: the system starts recording. • **Auto**: the system starts recording in the configured time periodof record plan. • **Off**: the system does not record.
Record Stream	Select record stream, including **Mainstream** and **Sub Stream**.

Step 3 Click **Apply**.

6.3. Time Plan

Configure daily and holiday record plan, After the corresponding alarm type (**General**, **Event**, and **Alarm**) is enabled, the record channel links recording.

Background Information

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

Procedure

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

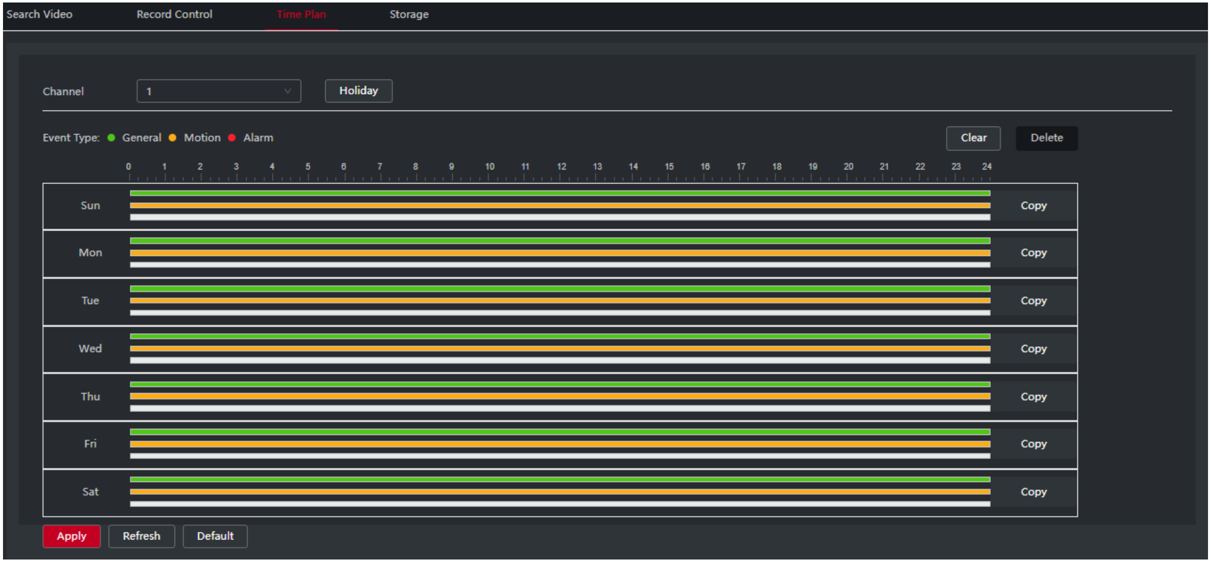
Step 2 Select record channel and then set record plan.

- Green represents normal record plan (such as timing recording).
- Yellow represents motion record plan (such as recording triggered by intelligentevents).
- Red represents alarm record plan (such as recording triggered by alarm-in).

a. Select a record type and left click and drag on the timeline to set the recording periodof each event.

Record plan from top to bottom are respectively normal record plan, motion recordplan and alarm record plan.

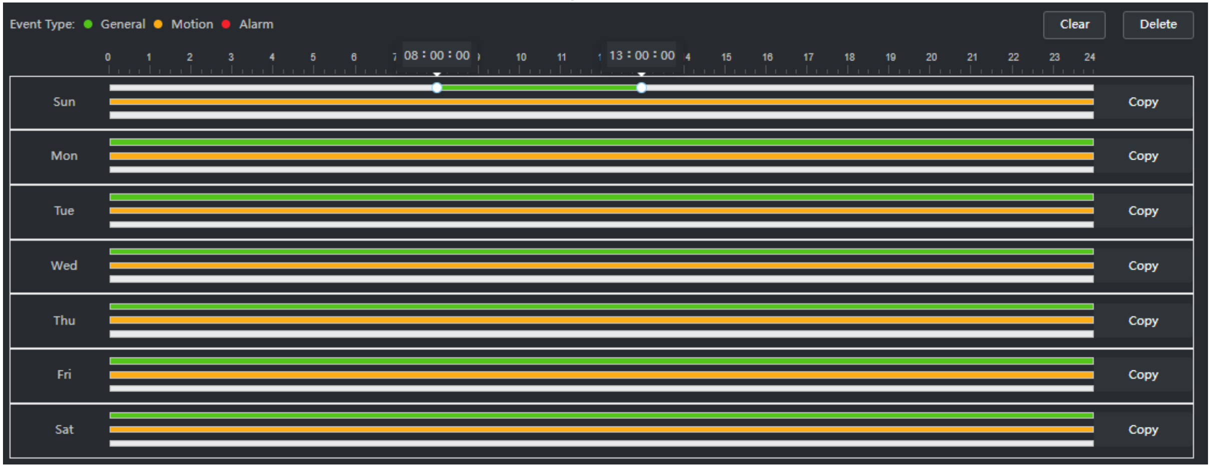
Figure 6-8



Channel 1

b. Click the selected time range and then set an accurate start and end time.

Figure 6-9



08 : 00 : 00

13 : 00 : 00

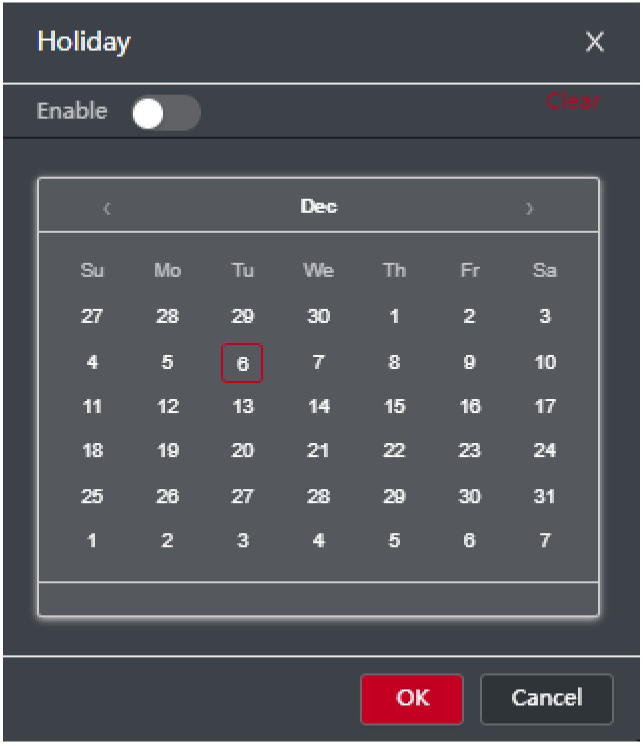
- Click **Copy** and select the days that you want to copy to in the prompt page.
- Select the **Select All** checkbox to select all day to copy the configuration.

- You can set 6 time periods per day.

Step 3 Click **Apply**.

Step 4 Click **Holiday** to set holiday record plan.

Figure 6-10



Holiday

Enable

Clear

Dec

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

OK

Cancel

- Click to enable the holiday plan and select the days that you need to set asholiday.

The selected dates are shown in blue.

- Click **Clear** to cancel the selection.

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

Step 5 Click **OK**.

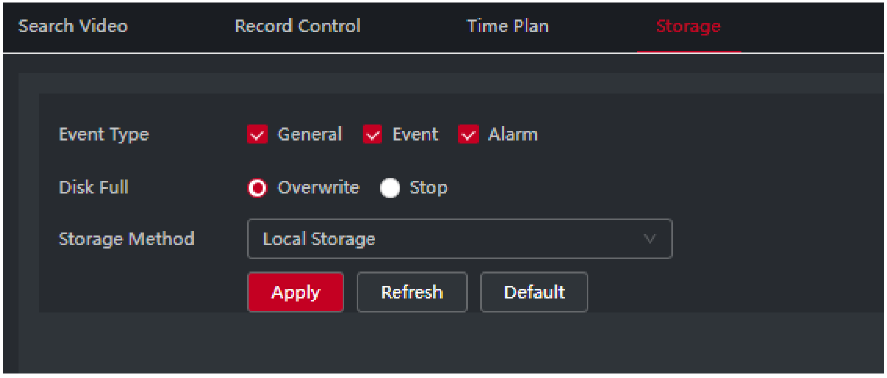
6.4. Storage

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

Step 1 Select **Record →Storage**.

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

Figure 6-11



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method Local Storage

Table 37

Parameter	Description
Event Type	Select from **General**, **Event** and **Alarm**.
Disk Full	Recording strategy when the disk is full. - **Overwrite**: Overwrite the earliest video when the disk is full. - **Stop**: Stop recording when the disk is full.
Storage Method	Select from **Local storage** and **Network storage** - **Local storage**: Save the recorded videos in the internal SD card. **Local storage** is displayed only on models that support SD card. - **Network storage**: Save the recorded videos on the FTP (File Transfer Protocol) server or NAS (Network Attached Storage).

Step 3 Click **Apply**.

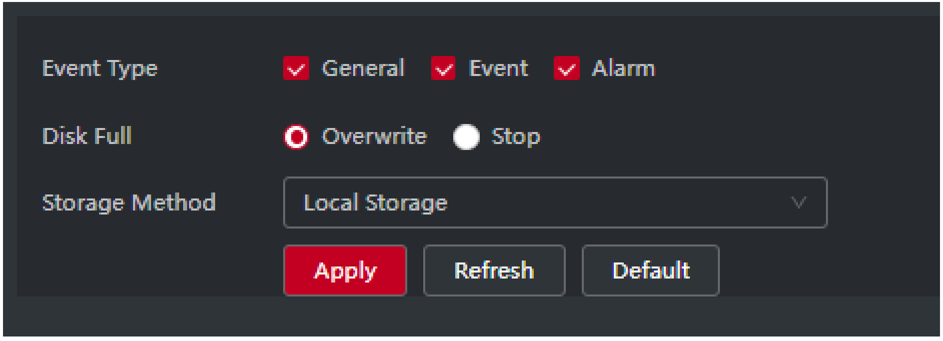
6.4.1. Local Storage

Step 1 Select **Record → Storage**.

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

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

Figure 6-12



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method Local Storage

Step 4 Click **Apply**.

6.4.2. Network Storage

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

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

6.4.2.1. FTP

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

Step 1 Select **Record → Storage**.

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

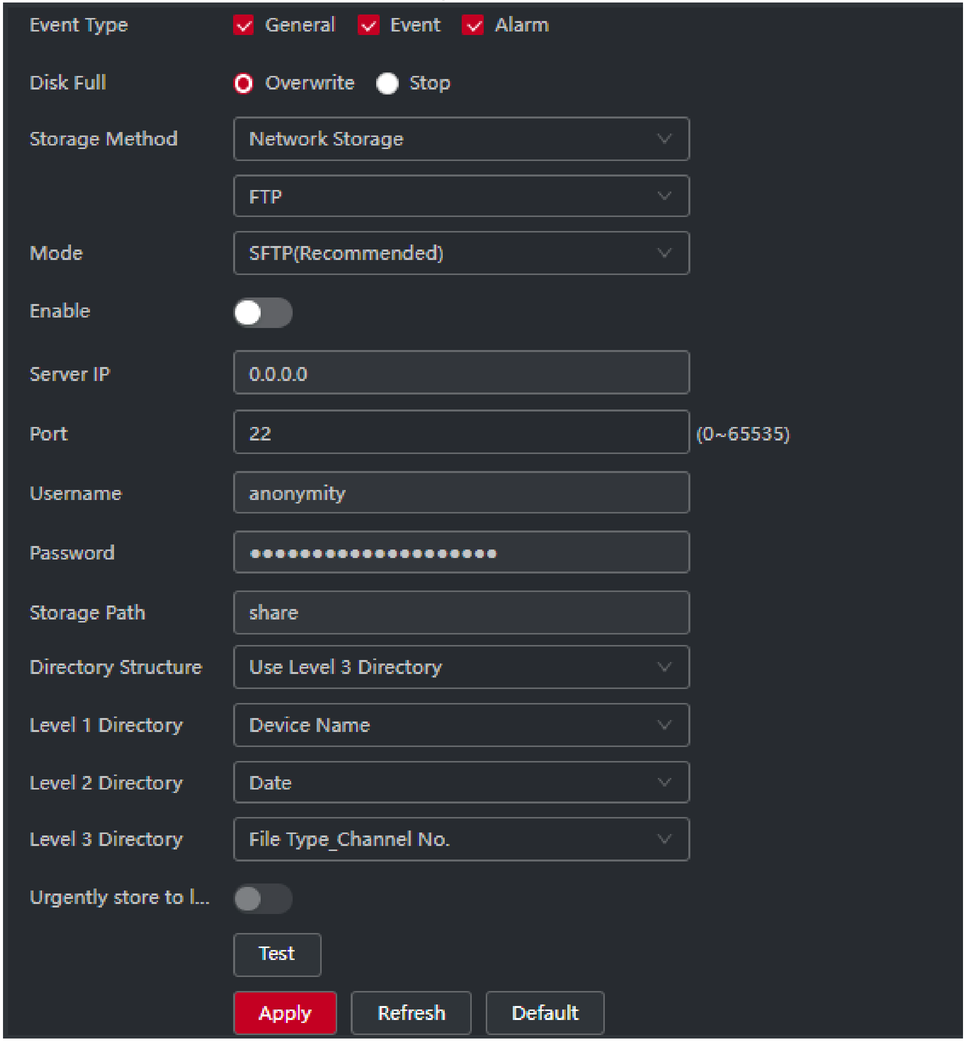
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

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

Step 4 Select **FTP** or **SFPT** from the drop-down list. **SFPT** is recommended to enhance networksecurity.

Step 5 Click ○ next to **Enable** to enable the FTP function.

Figure 6-13



Event Type	☑ General ☑ Event ☑ Alarm
Disk Full	● Overwrite ○ Stop
Storage Method	Network Storage
	FTP
Mode	SFTP(Recommended)
Enable	○
Server IP	0.0.0.0
Port	22 (0~65535)
Username	anonymity
Password	••••••••••••••••••••
Storage Path	share
Directory Structure	Use Level 3 Directory
Level 1 Directory	Device Name
Level 2 Directory	Date
Level 3 Directory	File Type_Channel No.
Urgently store to l...	○

Step 6 Configure FTP parameters.

Table 38

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The storage path in the FTP server.
Directory Structure	Select a directory level for the storage path and then set the directory name for the level.
Urgently store to local	Click , and when the FTP server does not work, all the files are saved to the internal SD card.

Step 7 Click **Apply**.

Step 8 Click **Test** to test whether FTP function works normally.

6.4.2.2. NAS

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

Step 1 Select **Record → Storage**.

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

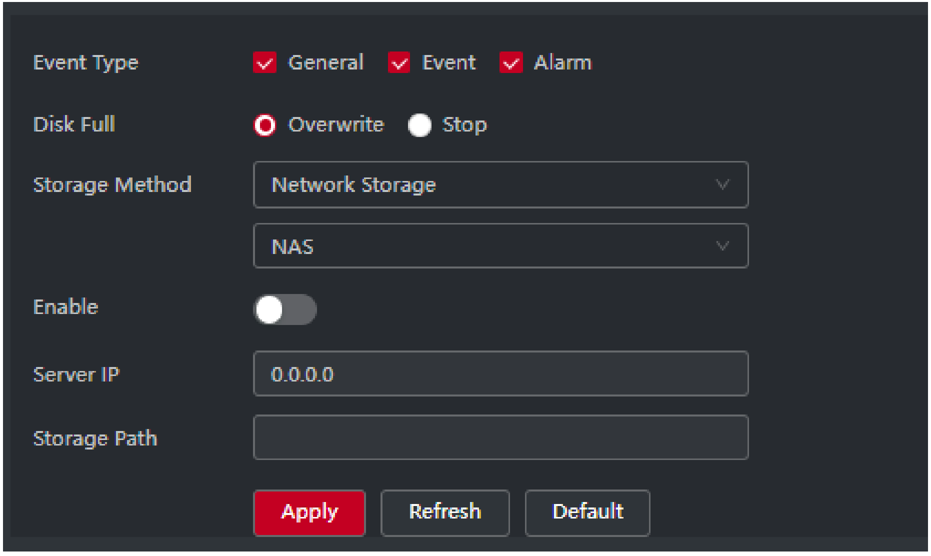
- **Overwrite**: Cyclically overwrite the earliest video when the disk is full.
- **Stop**: Stop recording when the disk is full.

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

Step 4 Select NAS protocol type.

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

Figure 6-14



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method: Network Storage

NAS

Enable

Server IP: 0.0.0.0

Storage Path:

Step 5 Select to enable NAS function, and then configure NAS parameters.

Table 39

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
Password	Password for logging in to the NAS server. 📖 This is required when the protocol type is SMB.
Username	Username for logging in to the NAS server. 📖 This is required when the protocol type is SMB.

Step 6 Click **Apply**.

7. Picture

This chapter introduces the related functions and operations of image playback, including configuring snapshot parameters, configuring snapshot plan and snapshot storage.

7.1. Playback

This section describes playing back and downloading images.

7.1.1. Playing Back Image

This section introduces the operation of image playback.

Prerequisites

- This function is available on the camera with SD card.
- Before playing back image, configure snapshot time range, snapshot storage method, snapshotplan.

Procedure

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

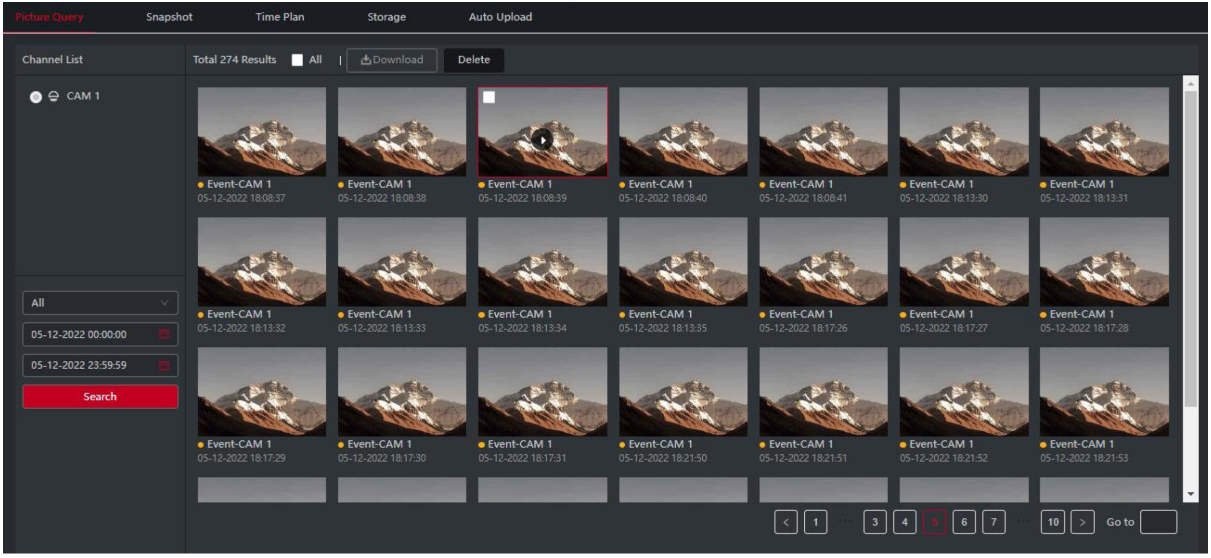
Step 2 Select the channel, the snapshot type and snapshot time, and then click **Query**.

- Click **All**, and select the snapshot type from the drop-down list, you can select from **All**,**General**, **Event**, and **Alarm**.

When selecting **Event** as the snapshot type, you can select the specific event types, such as **Motion Detection**, **Video Tamper** and **Scene Changing**.

- The dates with blue dots indicate there are snapshots on those days.

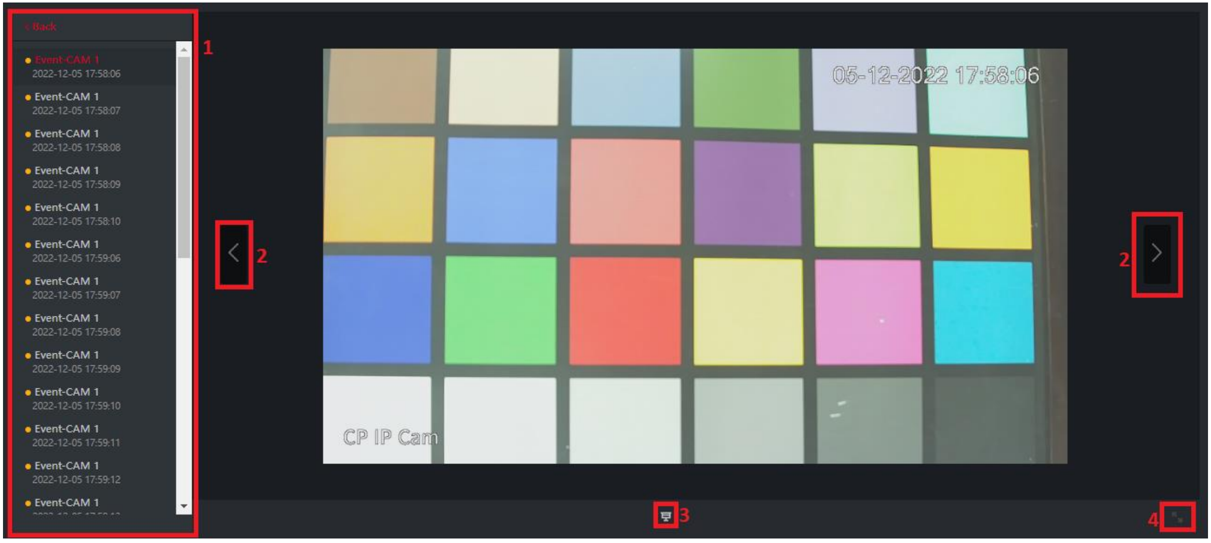
Figure 7-1



All
05-12-2022 00:00:00
05-12-2022 23:59:59

Step 3 Point to the searched image, and then click ▶ to play back the selected image.

Figure 7-2



< Back

- Event-CAM 1
  2022-12-05 17:58:06
- Event-CAM 1
  2022-12-05 17:58:07
- Event-CAM 1
  2022-12-05 17:58:08
- Event-CAM 1
  2022-12-05 17:58:09
- Event-CAM 1
  2022-12-05 17:58:10
- Event-CAM 1
  2022-12-05 17:59:06
- Event-CAM 1
  2022-12-05 17:59:07
- Event-CAM 1
  2022-12-05 17:59:08
- Event-CAM 1
  2022-12-05 17:59:09
- Event-CAM 1
  2022-12-05 17:59:10
- Event-CAM 1
  2022-12-05 17:59:11
- Event-CAM 1
  2022-12-05 17:59:12
- Event-CAM 1

Table 40

No	Function	Description
1	Snapshot list	Displays all searched snapshots. Click any files to play backit. Click **Back** at the upper-left corner to go to the **PictureQuery** page.
2	Manual display	- Click › to display the previous snapshot in thesnapshot list. - Click ‹ to display the next snapshot in the snapshotlist.
3	Slide show	Click to display the snapshots list one by one inslide show mode.
4	Full screen	Click , and the snapshot is displayed in full-screen mode; double-click the image or press Esc to exit full-screen mode.

7.1.2. Downloading Image

Download images to a defined path. You can download a single image or download images inbatches.

- Operations might vary with different browsers.

Step 1 Select **Picture → Picture Query**.

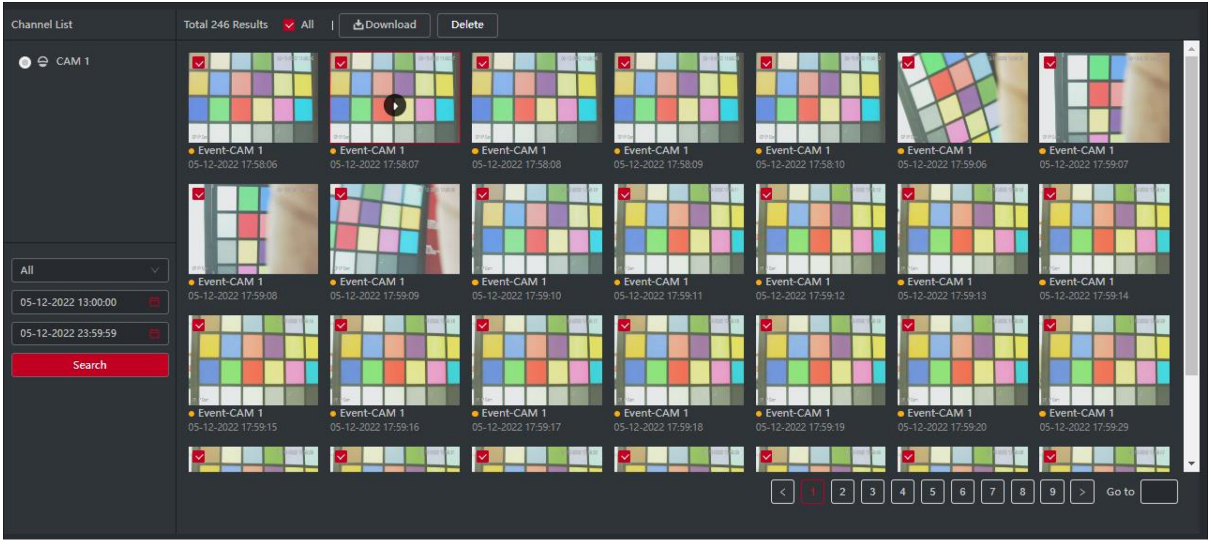
Step 2 Select the channel, the snapshot type, and snapshot time, and then click **Query**.

Step 3 Select the images to be downloaded.

- Select □ at the upper-right corner of each image file to select one or multiple images.The icon in the upper left corner of the selected file changes to ☑.

- Select □ next to **All** to select all searched images.

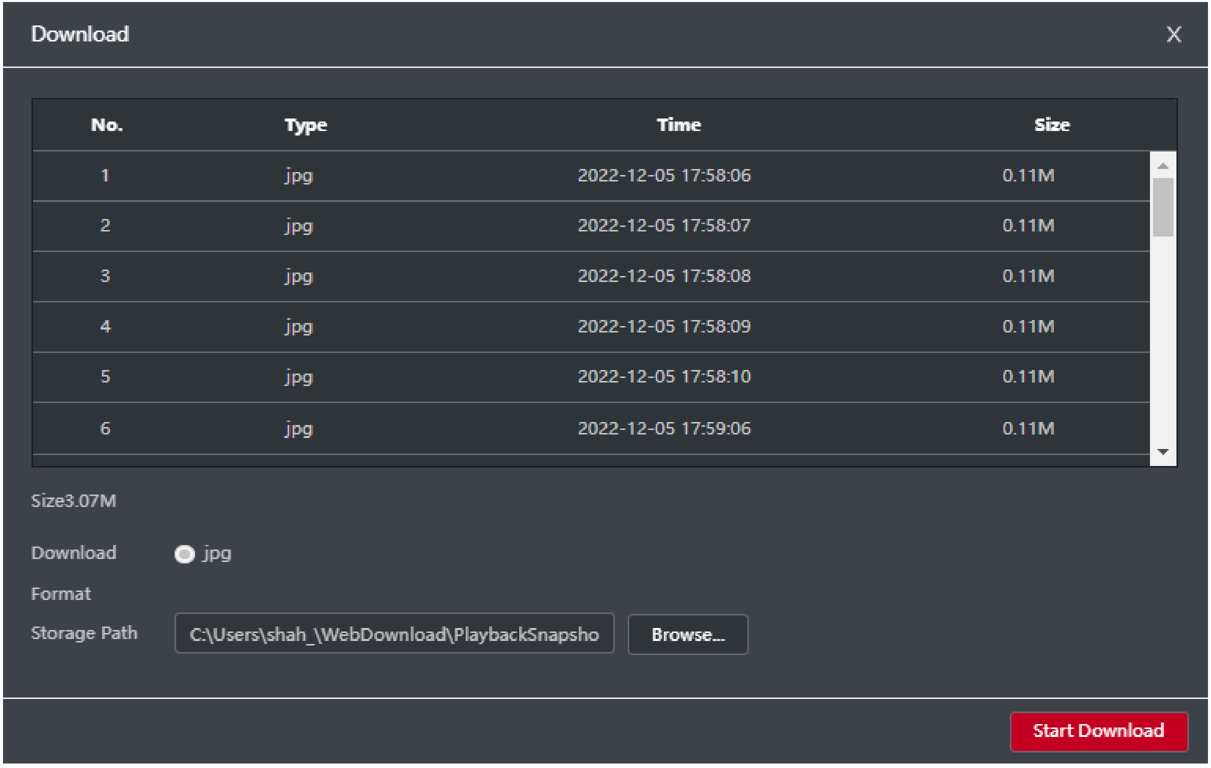
Figure 7-3


Channel List
CAM 1
All
05-12-2022 13:00:00
05-12-2022 23:59:59
Search
Total 246 Results
All
Download
Delete
Event-CAM 1 05-12-2022 17:58:06
Event-CAM 1 05-12-2022 17:58:07
Event-CAM 1 05-12-2022 17:58:08
Event-CAM 1 05-12-2022 17:58:09
Event-CAM 1 05-12-2022 17:58:10
Event-CAM 1 05-12-2022 17:59:06
Event-CAM 1 05-12-2022 17:59:07
Event-CAM 1 05-12-2022 17:59:08
Event-CAM 1 05-12-2022 17:59:09
Event-CAM 1 05-12-2022 17:59:10
Event-CAM 1 05-12-2022 17:59:11
Event-CAM 1 05-12-2022 17:59:12
Event-CAM 1 05-12-2022 17:59:13
Event-CAM 1 05-12-2022 17:59:14
Event-CAM 1 05-12-2022 17:59:15
Event-CAM 1 05-12-2022 17:59:16
Event-CAM 1 05-12-2022 17:59:17
Event-CAM 1 05-12-2022 17:59:18
Event-CAM 1 05-12-2022 17:59:19
Event-CAM 1 05-12-2022 17:59:20
Event-CAM 1 05-12-2022 17:59:29
1 2 3 4 5 6 7 8 9
Go to

Step 4 Click **Download**.

Step 5 Select the download format and storage path.

Figure 7-4



Download

No.	Type	Time	Size
1	jpg	2022-12-05 17:58:06	0.11M
2	jpg	2022-12-05 17:58:07	0.11M
3	jpg	2022-12-05 17:58:08	0.11M
4	jpg	2022-12-05 17:58:09	0.11M
5	jpg	2022-12-05 17:58:10	0.11M
6	jpg	2022-12-05 17:59:06	0.11M

Size3.07M

Download Format ● jpg

Storage Path C:\Users\shah_\WebDownload\PlaybackSnapsho

Step 6 Click **Start Download**.

The downloaded images are saved in the configured storage path

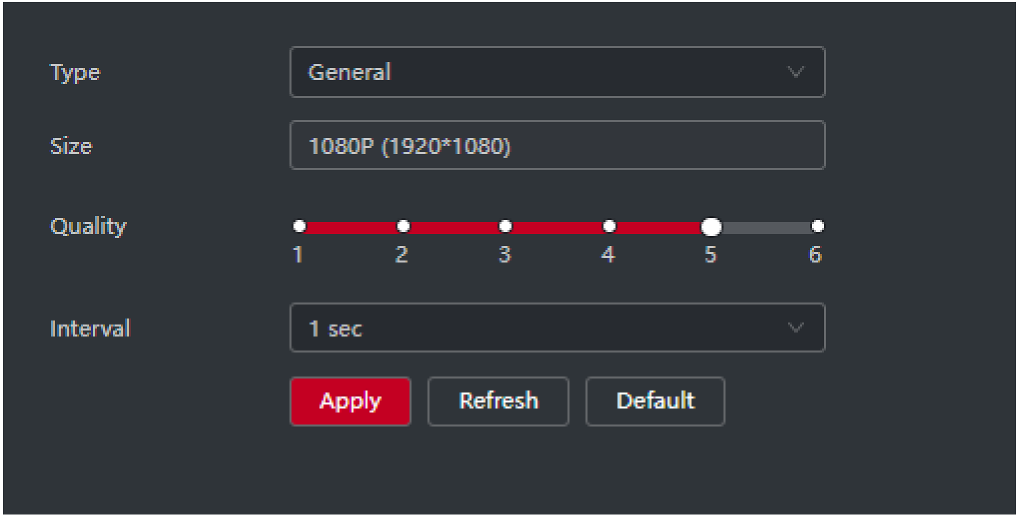
7.2. Snapshot Parameters

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

Step 1 Select **Picture** → **Snapshot**.

Step 2 Select the channel, and then set the parameters.

Figure 7-5



Type: General

Size: 1080P (1920*1080)

Quality: 5

Interval: 1 sec

Table 41

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

Step 3 Click **Apply**.

7.3. Setting Snapshot Plan

Configure daily and holiday snapshot plan. After the corresponding alarm type (**General**, **Event**, and **Alarm**) is enabled, the snapshot channel links snapshot.

Background Information

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

Procedure

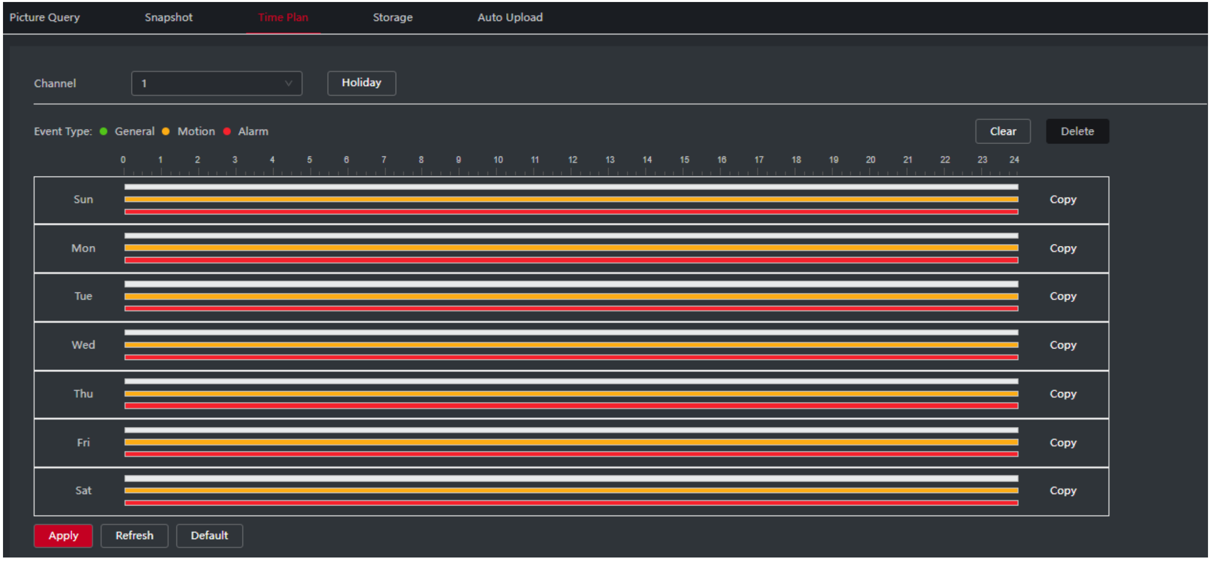
Step 1 Click **Picture** on the main page, and then click the **Time Plan** tab.

Step 2 Select snapshot channel and then set snapshot plan.

- Green represents normal snapshot plan (such as timing snapshot).
- Yellow represents motion snapshot plan (such as snapshot triggered by intelligentevents).
- Red represents alarm snapshot plan (such as snapshot triggered by alarm-in).

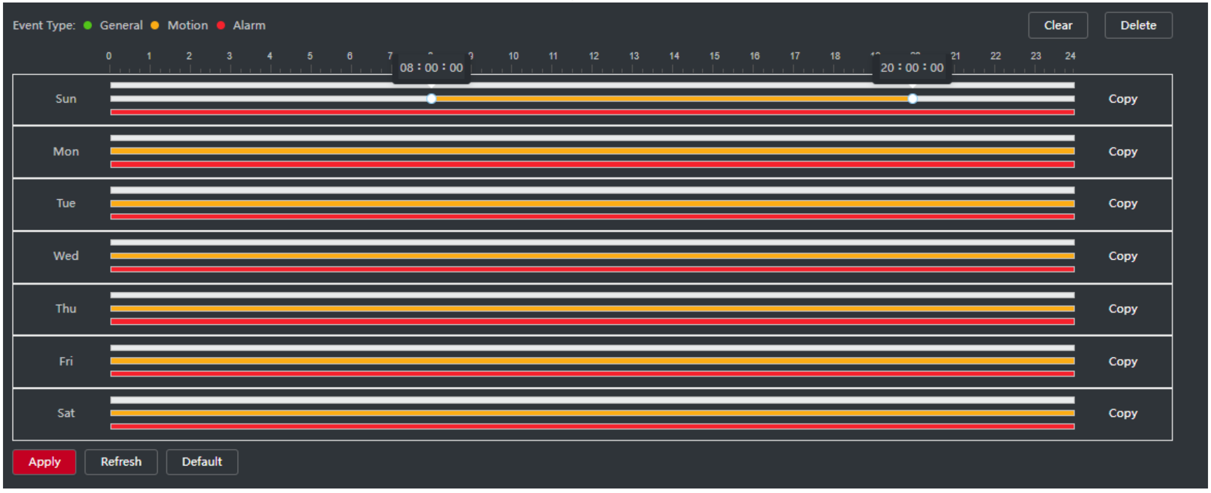
a. Select a snapshot type and left click and drag on the timeline to set the snapshot period of each event. Snapshot plan from top to bottom are respectively normal snapshot plan, motionsnapshot plan and alarm snapshot plan.

Figure 7-6



b. Click the selected time range and then set an accurate start and end time.

Figure 7-7

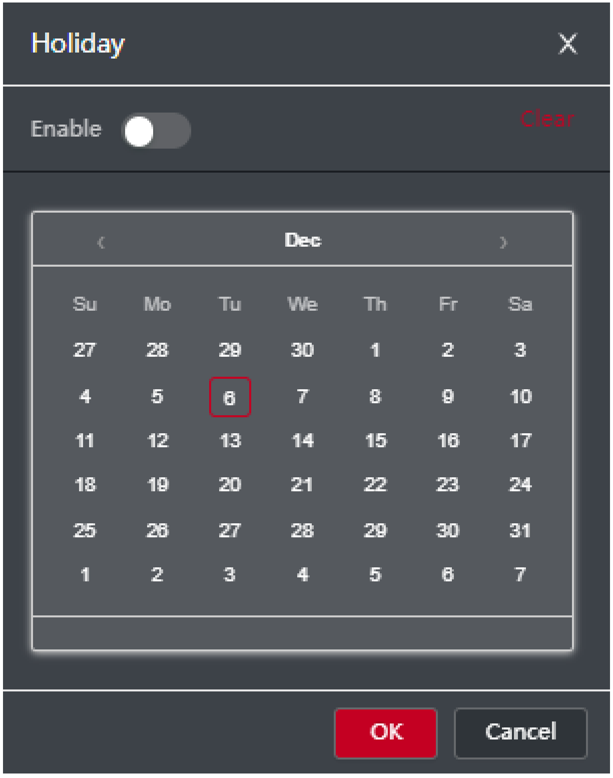


- Click **Copy** and select the days that you want to copy to in the prompt page.
- Select the **Select All** checkbox to select all day to copy the configuration.
- You can set 6 time periods per day.

Step 3 Click **Apply**.

Step 4 Click **Holiday** to set holiday snapshot plan.

Figure 7-8



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

- Click ○ to enable the holiday plan and select the days that you need to set asholiday.

The selected dates are shown in blue.

- Click **Clear** to cancel the selection.

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

Step 5 Click **OK**.

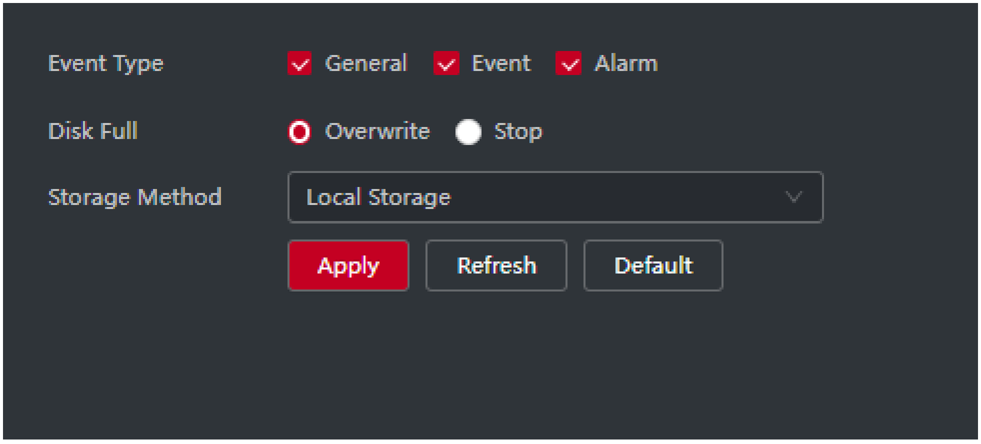
7.4. Storage

This section introduces the configuration of the storage method for the snapshot.

Step 1 Select **Picture → Storage**.

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

Figure 7-9



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method Local Storage

Table 42

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

Step 3 Click **Apply**.

7.4.1. Local Storage

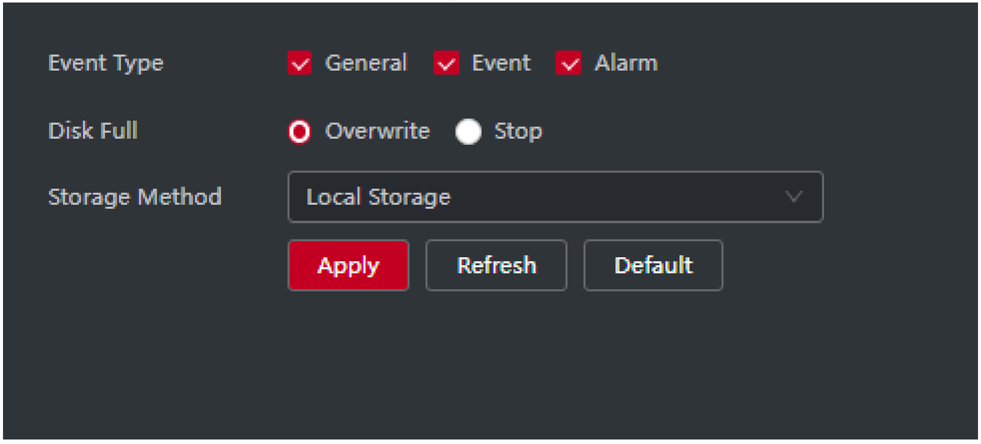
Step 1 Select **Picture → Storage**.

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

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

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

Figure 7-10



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method Local Storage

Step 4 Click **Apply**.

7.4.2. Network Storage

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

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

7.4.2.1. FTP

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

Step 1 Select **Picture → Storage**.

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

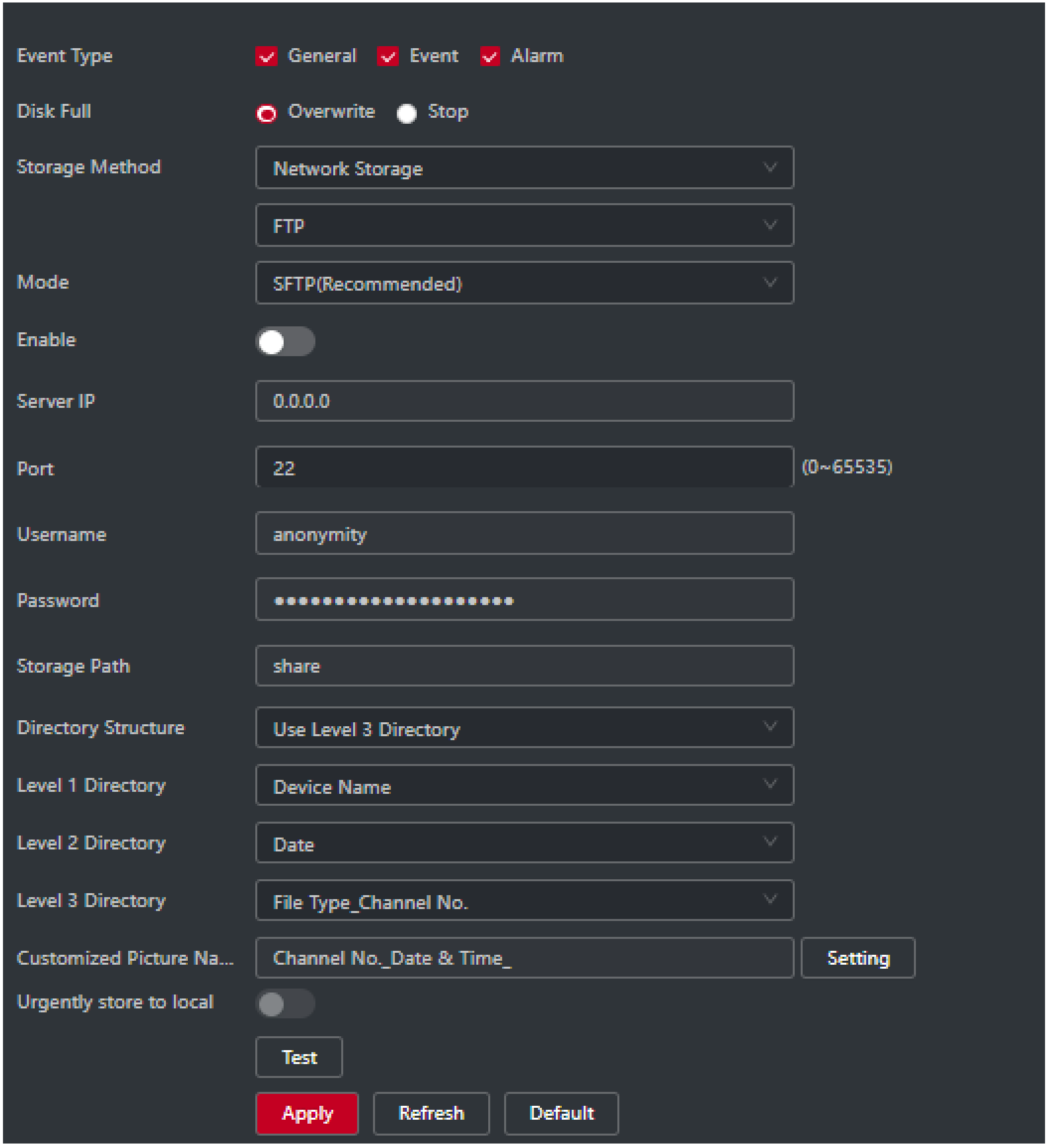
- **Overwrite**: Cyclically overwrite the earliest snapshot when the disk is full.
- **Stop**: Stop snapshot when the disk is full.

Step 3 Select **Network storage** in **Storage Method** and select **FTP** to save the snapshots in FTPserver.

You select **FTP** or **SFPT** from the drop-down list. **SFPT** is recommended.

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

Figure 7-11



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method: Network Storage

FTP

Mode: SFTP(Recommended)

Enable: ○

Server IP: 0.0.0.0

Port: 22 (0~65535)

Username: anonymity

Password: ••••••••••••••••••••

Storage Path: share

Directory Structure: Use Level 3 Directory

Level 1 Directory: Device Name

Level 2 Directory: Date

Level 3 Directory: File Type_Channel No.

Customized Picture Na...: Channel No._Date & Time_ Setting

Urgently store to local: ○

Step 5 Configure FTP parameters.

Parameter	Description
Server IP	The IP address of the FTP server.
Port	The port number of the FTP server.
Username	The username to log in to the FTP server.
Password	The password to log in to the FTP server.
Storage Path	The storage path in the FTP server.
Directory Structure	Select a directory level for the storage path and then set thedirectory name for the level.
Urgently store to local	Click ○, and when the FTP server does not work, all the files aresaved to the internal SD card.

Step 6 Click **Apply**.

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

7.4.2.2. NAS

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

Step 1 Select **Picture** → **Storage**.

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

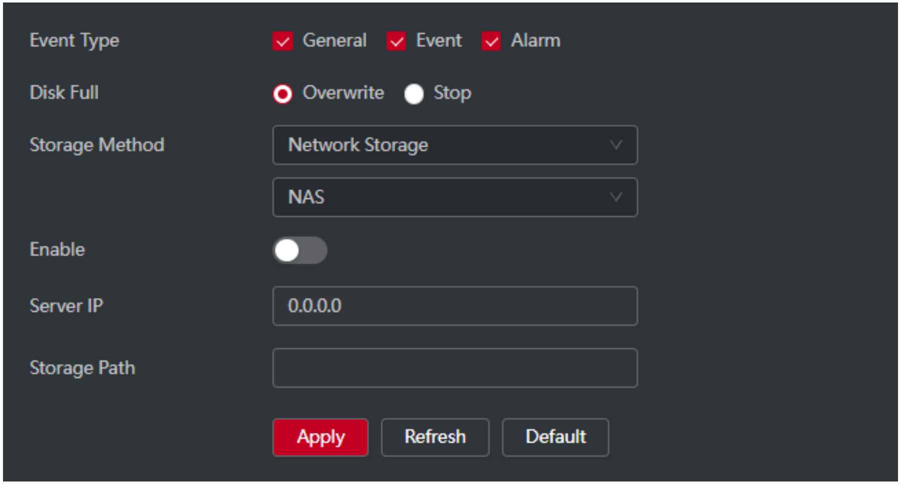
- **Overwrite**: Cyclically overwrite the earliest snapshot when the disk is full.
- **Stop**: Stop snapshot when the disk is full.

Step 3 Select **Network storage** in **Storage Method** and select **NAS** to save the snapshots in NASserver.

Step 4 Select NAS protocol type.

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

Figure 7-12



Event Type ☑ General ☑ Event ☑ Alarm

Disk Full ● Overwrite ○ Stop

Storage Method Network Storage

NAS

Enable

Server IP 0.0.0.0

Storage Path

Step 5 Select ○ to enable NAS function, and then configure NAS parameters.

Table 7-5 Description of NAS parameters

Parameter	Description
Server IP	The IP address of the NAS server.
Storage Path	The destination path in the NAS server.
Username	Username for logging in to the NAS server. This is required when the protocol type is SMB.
Password	Password for logging in to the NAS server. This is required when the protocol type is SMB.

Step 6 Click **Apply**.

8. AI

This chapter describes how to configure device AI events, including face recognition, IVS and videometadata.

8.1. Configuring Smart Plan

Smart plans include face recognition, intelligence behavior analysis, video metadata and so on. The smart functions of the camera cannot take effect until the smart plan has been enabled.

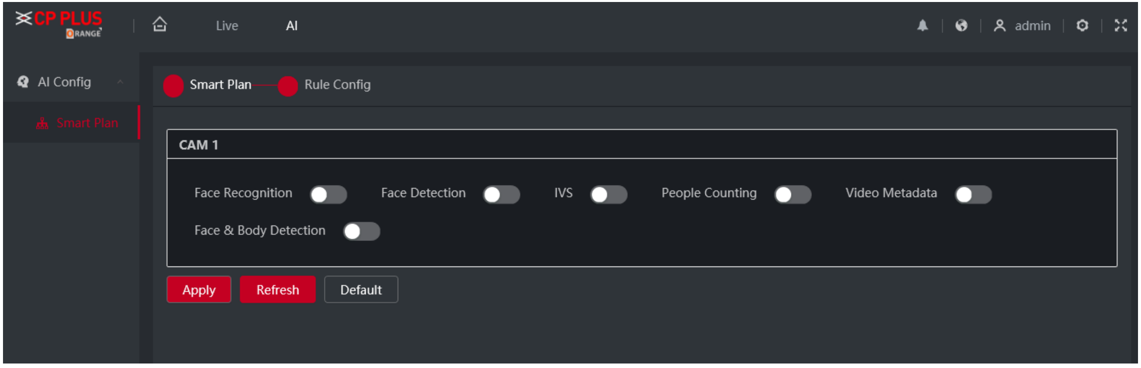
Step 1 Click **AI** → **AI Config** → **Smart Plan**.

Step 2 Enable the smart functions of the global and preset plan based on actual needs and thenclick **Next**.

Before configuring the preset plan, please add the appropriate presets in advance.

Step 3 Enable the intelligent functions of the **Global** and **Preset** as required, and then click **Next**.

Figure 8-1



Step 4 Configure smart function rule as required.

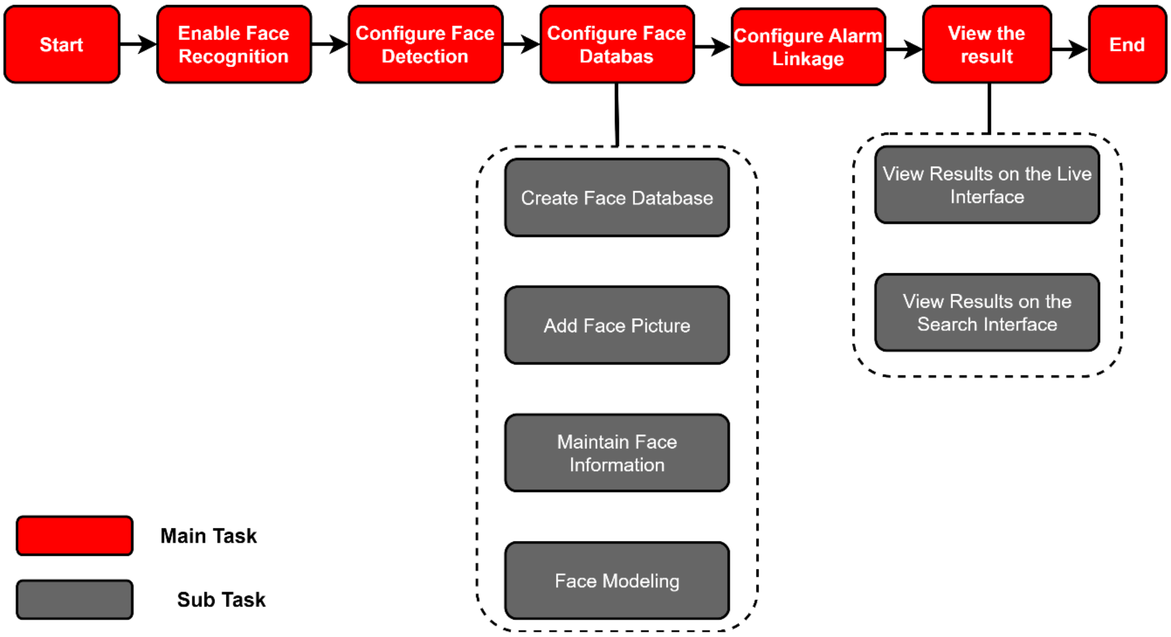
8.2. Smart Function Rule

8.2.1. Configuring Face Recognition

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

- Face detection: When a face is detected in the area, the system performs alarm linkage, such asrecording and sending emails.
- Face recognition: When a face is detected in the area, the system compares the captured face image with the information in the face database, and links alarm according to the comparisonresult.

Figure 8-2



8.2.1.1. Configuring Face Recognition Rule

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

Step 1 Click **AI →AI Config→Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**.

Step 3 (Optional) Click the icon on the right of the screen to draw detection area, exclusion areaand filtering target model on the monitoring screen.

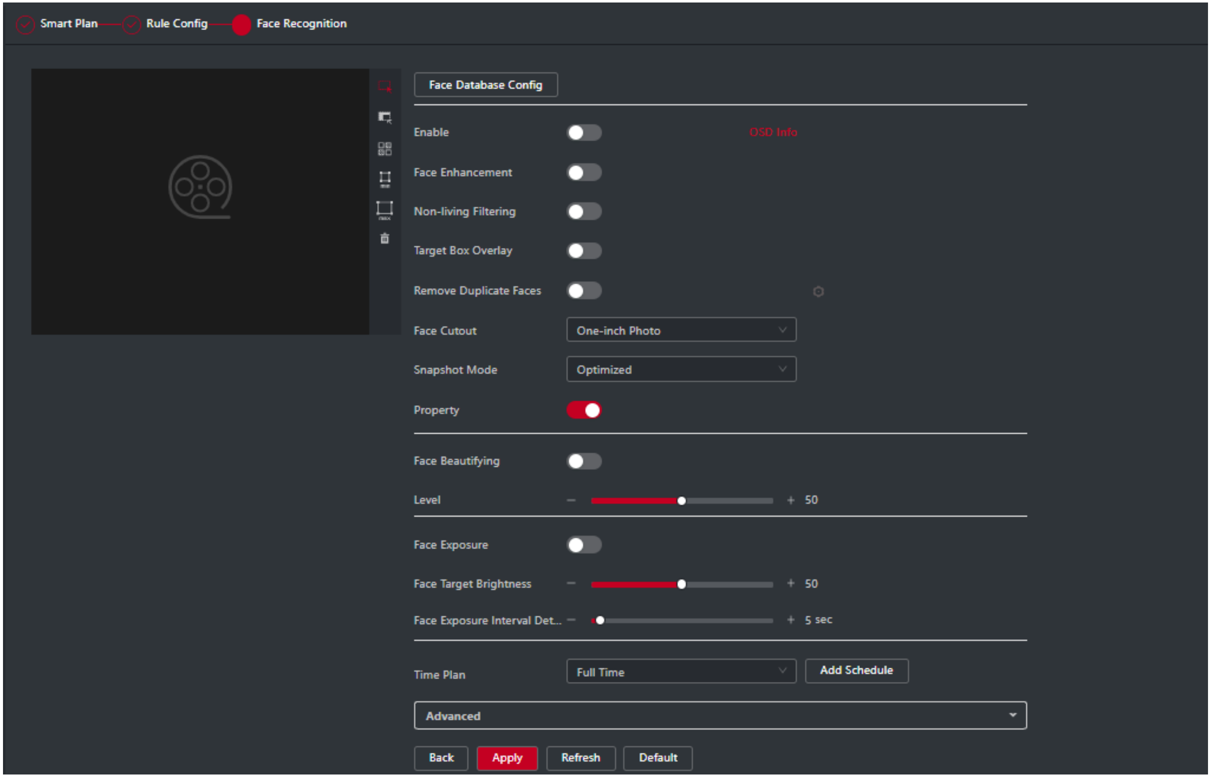
- Click to draw a face detection area in the image, and right-click to finish thedrawing.

The default detection area is the whole screen.

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

Step 4 Configure relevant parameter of face detection.

Figure 8-3



Smart Plan — Rule Config — Face Recognition

Face Database Config

Enable ○ OSD Info

Face Enhancement ○

Non-living Filtering ○

Target Box Overlay ○

Remove Duplicate Faces ○

Face Cutout: One-inch Photo

Snapshot Mode: Optimized

Property ●

Face Beautifying ○

Level: 50

Face Exposure ○

Face Target Brightness: 50

Face Exposure Interval Det...: 5 sec

Time Plan: Full Time | Add Schedule

Advanced

Back | Apply | Refresh | Default

Table 43

Parameter	Description
Face Enhancement	Select **Face Enhancement** to preferably guarantee clear faces with low stream.
Target Box Overlay	You can add a bounding box to the face in the captured image tohighlight the face. The captured face image is saved in SD card or the **Snapshot Path**.
Face Cutout	Set a range for the captured face image, including face and one-inch image. It supports custom setting. When selecting **Custom**, click ⚙ on the right side, configure the parameters on the prompt page, and then click **Apply**. ● Customized width: Set snapshot width; enter the times of the original face width. The value ranges from 1 to 5. ● Customized face height: Set face height in snapshot; enter the times of the original face height. The value ranges from 1 to 2. ● Customized body height: Set body height in snapshot; enterthe times of the original body height. The value ranges from 0to 4. When the value is 0, it cuts out the face image only.
Snap Mode	● **Recognition Priority:** The device takes snapshot immediatelywhen it detects faces. ● **Optimized Snapshot:** The device captures the clearest imageswithin the optimized duration after it detects faces.

Parameter	Description
	📖 Optimized duration is configured in the **Advanced** below.
Property	Click **Property** to enable the properties display during facerecognition.
Advanced	Optimized Duration: Set a time period to capture the clearest imageafter the camera detects face.

Step 5 Set arming periods and alarm linkage action.

- Click **Add Schedule** to add time plan.
- Click **+ Event Linkage** to set the linkage action and configure linkage parameters.

Step 6 Click **Apply**.

8.2.1.2. Configuring Face Database

By configuring face database, the face database information can be used to compare with the face captured. The configuration process includes creating face database, adding face image, and face modeling. The operations for configuring face databases are all performed on **Face Database Config**.

8.2.1.2.1. Creating Face Database

Face database is the management center of face data information, including face image and face data. It also provides comparison data for the captured face images.

Procedure

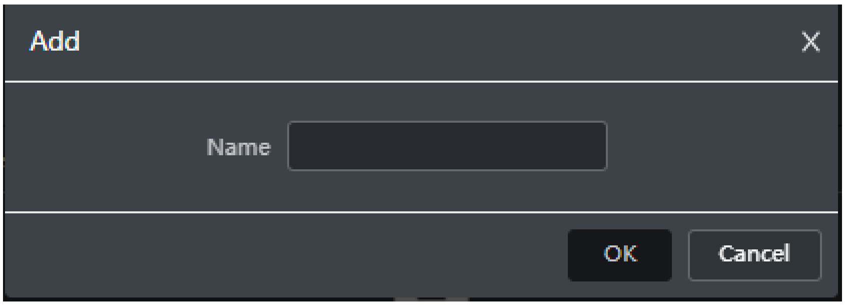
Step 1 Click **AI → AI Config → Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**, and then

Step 3 Click **Face Database Config** to enter the face database configuration page.

Step 4 Click **Add** to configure the name of face database.

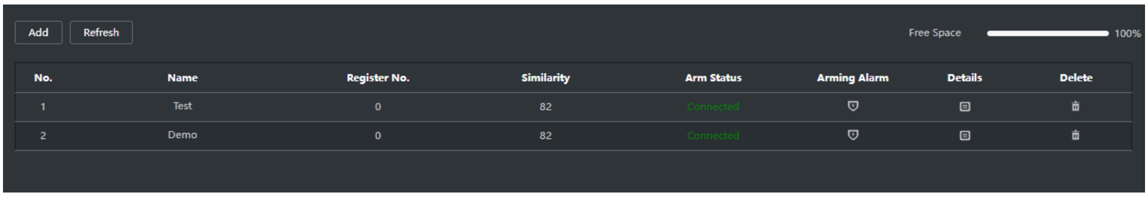
Figure 8-4



Step 5 Click **OK**.

The added face database information is displayed on the page.

Figure 8-5



No.	Name	Register No.	Similarity	Arm Status	Arming Alarm	Details	Delete
1	Test	0	82	Connected	🛡	⊟	🗑
2	Demo	0	82	Connected	🛡	⊟	🗑

Related Operations

- Change the name of face database.

Click the text box under the name to change the name of face database.

- Arm alarm.

Click 🛡 to configure relevant parameters of face database control and alarm.

- Managing face database.

Click ⊟ to manage face database. You can set search conditions, register people, modifypeople information and face modeling.

- Deleting face database.

Click 🗑 to delete face database.

8.2.1.2.2. Adding Face Images

Add face images to the created face database. You can add them one by one or in batches.Requirements on face images:

- A single image size is 50 KB–150 KB in JPEG format. The resolution is less than 1920 × 1080.
- Face size is 30%–60% of the whole image. There must be at least 100 pixels between the ears.
- Taken in full-face view directly facing the camera without makeup, filters, glasses, and fringe. Eyebrow, mouth and other face features must be visible.

Single Adding

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

Step 1 Click **AI** → **AI Config** → **Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**.

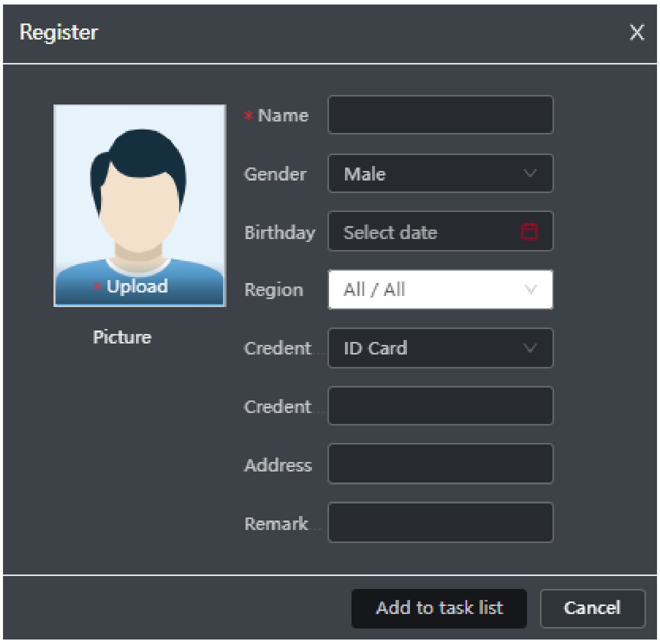
Step 3 Click **Face Database Config** to enter the face database configuration page, and then click ⊟ next to the face database to be configured.

Step 4 Click **Register**.

Step 5 Click **Upload** to select the face image you want to upload, and then click **Open**.

After uploading the image, select a face area and click **OK** to save the face image. If thereare multiple faces in a image, select the target face and click **OK** to save the face image.

Figure 8-6



* Name:
Gender: Male
Birthday: Select date
Region: All / All
Credent: ID Card
Credent:
Address:
Remark:

Step 6 Enter the information about face image according to the actual situation, and then click Add to task list.

Step 7 Click Task List 1 at the upper-right corner, and then click **Operation**.

- If image adds successfully, it shows **Stored successfully. Modeling successful**.
- If adding user fails, the error code is displayed on the page. View the fail reason according to error code table.
- If image modeling fails, the error code is displayed on the page. Please modify theimage and remodel the image.

Table 44

Parameter	Error	Description
0x1134000C	Image importing error	The image is too large, and the upper limit is 150 KB.
0x1134000E		The number of the added images is to the upper limit.
0x11340019		The space of the face database exceeds the upperlimit.
1	Image modeling error	The image format is not correct. Import the image inJPG format.
2		No face in the image or the face is not clear. Changethe image.
3		Multiple faces in the image. Change the image.
4		Failed to decode the image. Change the image.
5		The image is not suitable to be imported to the face database. Change the image.
6		Database operation error. Restart the camera andmodel faces again.
7		Fails to get the image. Import the image again.
8		System error. Restart the camera and model facesagain.

Batch Adding

Import face images in batches when you need to add a large number of face images.

Prerequisites

Before importing images in batches, name face image in a format of "Name#SGender#BDate of Birth#NRegion#PProvince#CCity#TCredentials Type#MID No.jpg" (for example, "John#S1#B1990-01-01#NIN#PNewDelhi#CNewDelhi#T1#M000000199001010000).

- The max. size of a single face image is 150 KB, and the resolution is less than 1920p× 1080p.
- When naming images, **Name** is required, and others are optional.

Table 45

Parameters	Description
Name	Enter the corresponding name.
Gender	"1" is male and "2" female.
Date of Birth	Format: yyyy-mm-dd, such as 2020-10-23.
Region	Enter the abbreviation name of the country or region, such as IN (for India), BR (for Brazil).
Province	Enter the corresponding name of the province. Supports letters (capitalize the initial letter)
City	Enter the corresponding name of the city.
Credential Type	"1" is ID card, "2" is passport, "3" is Officer Card and "4" is others.
ID number	Enter ID number.

Procedure

Step 1 Click **AI** → **AI Config** → **Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**.

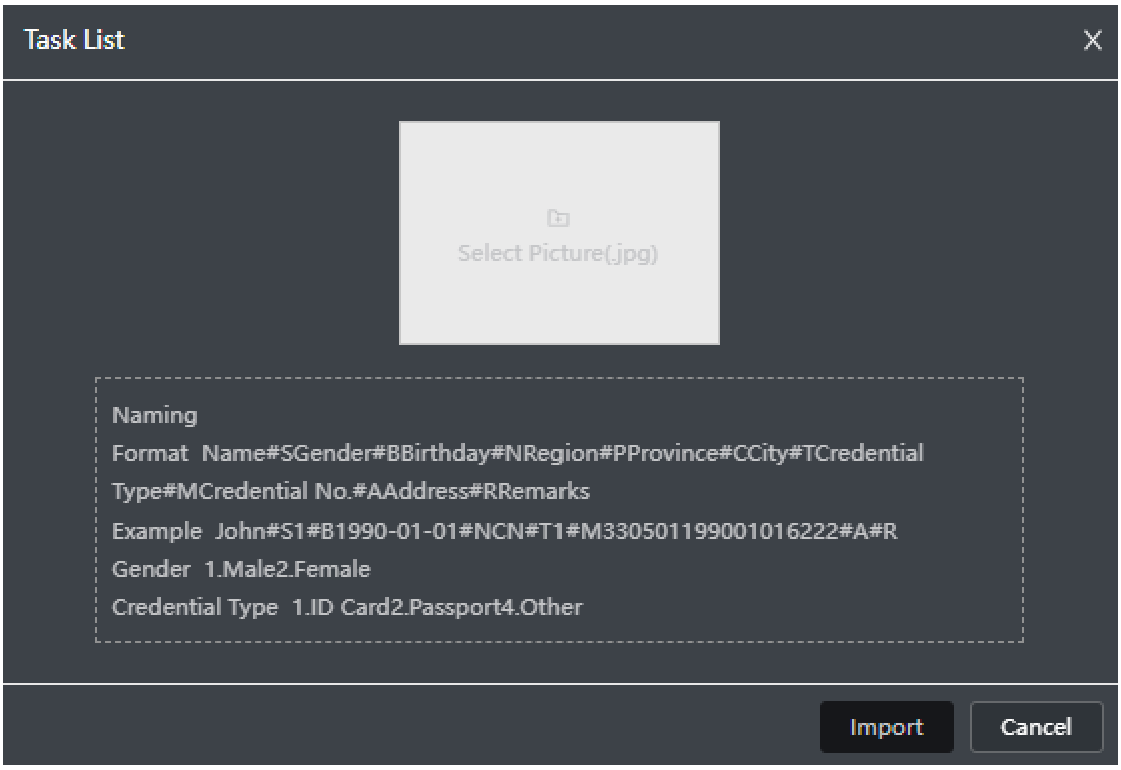
Step 3 Click **Face Database Config** to enter the face database configuration page.

Step 4 Click ▤ next to the face database to be configured.

Step 5 Click **Batch Register**.

Step 6 Click **Select Picture** and select storage path of the file.

Figure 8-7



Naming
Format Name#SGender#BBirthday#NRegion#PProvince#CCity#TCredential Type#MCredential No.#AAddress#RRemarks
Example John#S1#B1990-01-01#NCN#T1#M330501199001016222#A#R
Gender 1.Male2.Female
Credential Type 1.ID Card2.Passport4.Other

<u>Step 7</u> Click **Import** to import the face images.

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

- If the image is imported successfully, click **Next** to do modeling operation.
- If the image importing failed, click **Query** to view the details of the images and errorcode. Click **Export** to export the error details. Modify and reimport the face image accordingto the error prompt.

<u>Step 8</u> Click **Next** to do modeling operation.

The modeling result is displayed. If modeling failed, click **Query** and the failure details willbe displayed in the list. Point to the modeling status to view the details. Then you can change image according to the failure reason.

8.2.1.2.3. Managing Face Images

Add face images to face database, and then manage and maintain face images to ensure theinformation is correct.

Modifying Face Information

<u>Step 1</u> Click **AI → AI Config → Smart Plan**.

<u>Step 2</u> Click **Rule Config** and then select **Face Recognition**.

<u>Step 3</u> Click **Face Database Config** to enter the face database configuration page.

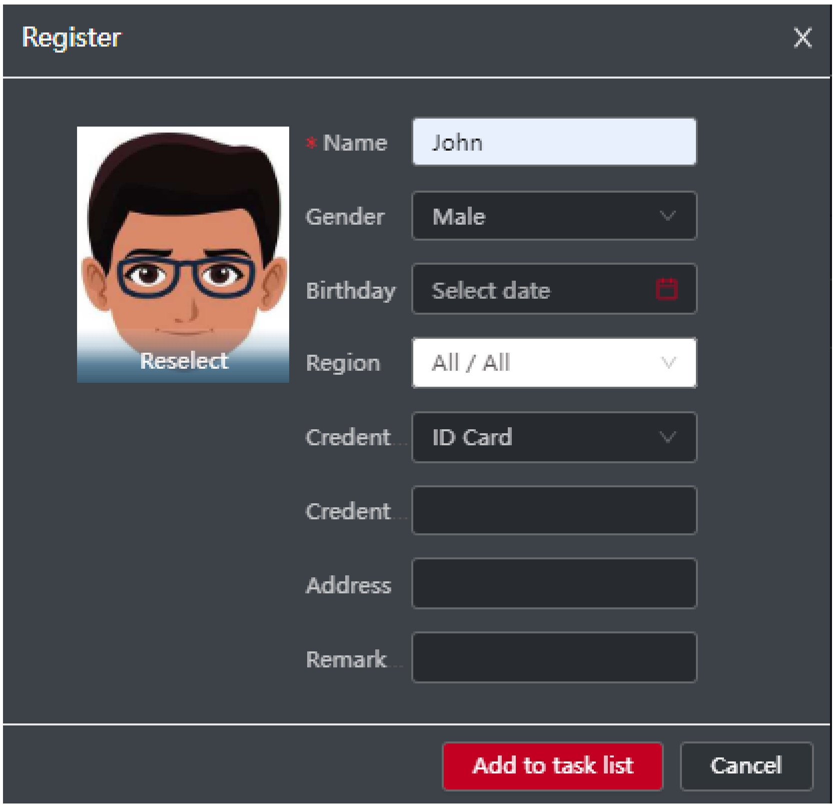
<u>Step 4</u> Click ▤ next to the face database to be configured.

<u>Step 5</u> Click **Query**, set the criteria as needed, and then click **Search**.

Step 6 Select the row where the image or the personnel information is located, and then click ✎.

Step 7 Edit face information according to the actual need. Click **Add to task list**.

Figure 8-8



Register

* Name: John

Gender: Male

Birthday: Select date

Region: All / All

Credent...: ID Card

Credent...:

Address:

Remark...:

Step 8 Click Task List 1, and then click **Operation.**

Deleting Face Data

Step 1 Click **AI → AI Config → Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**.

Step 3 Click **Face Database Config** to enter the face database configuration page.

Step 4 Click ☰ next to the face database to be configured.

Step 5 Click **Query**, and then set the search criteria. Click **Search**, and then select the faceinformation that needs to be deleted and delete it.

- Single delete: Select the row where the face image or the personnel information is located and click 🗑 to delete the face image.
- Delete in batches: Select □ at the upper-right corner of the face image or □ of the row where the personnel information is located. Select the information, click **Delete**, then click Task List 1 .Click **Operation** to delete the selected face images.

- Delete all: When viewing face images in a list, click □ of the row where the serial number is located; when viewing by thumbnail, select **All** to select all face images. Click**Delete**, then click Task List 1, and then click **Operation** to delete all face images.

8.2.1.2.4. Face Modeling

Extract and import the relevant information of face images through face modeling and create a face feature model for smart detection such as face recognition.

- The more face images you select, the longer the face modeling process will take.
- During the modeling process, some smart detection functions (such as face comparison) aretemporarily unavailable and can be resumed after the modeling is completed.

Step 1 Click **AI → AI Config → Smart Plan**.
Step 2 Click **Rule Config** and then select **Face Recognition**.
Step 3 Click **Face Database Config** to enter the face database configuration page.
Step 4 Click ▤ next to the face database to be configured.
Step 5 Start modeling.

- Modeling some images: Select the face images to be modeled, and then click **Modeling**.

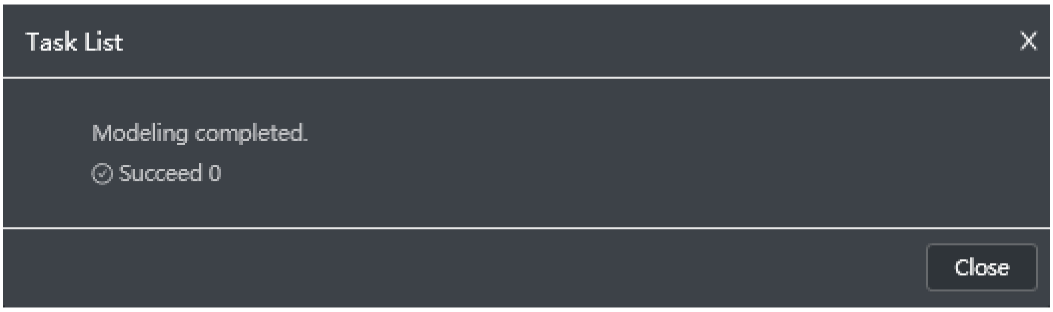
If there are many face images in the face database, you can set search criteria to selectthe images that need to be modeled.

- Modeling all images: Click **Modeling All**, and the face images in invalid state in the facedatabase are modeled

Step 6 View the modeling result.

When the modeling failed, click **Query** to view the details.

Figure 8-9


Task List

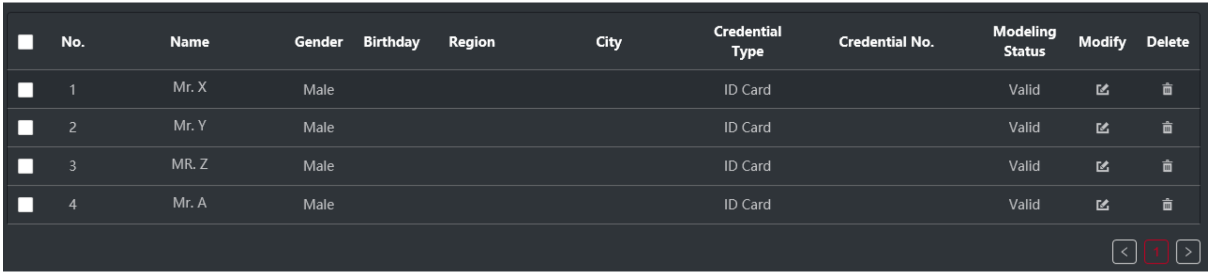
Modeling completed.
Succeed 0

Close

Click ☰ to view the face image in list format; click ▦ to view the face image inthumbnail format.

- When the modeling status is **Valid** in the list or is displayed at the lower-left corner ofthe thumbnail, it means the modeling is successful.
- When the modeling status is **Invalid** in the list or is displayed at the lower-left corner of the thumbnail, it means the modeling failed. Point to the modeling status in the list toview the details of the failure. Change the images according to the reasons.

Figure 8-10



□	No.	Name	Gender	Birthday	Region	City	Credential Type	Credential No.	Modeling Status	Modify	Delete
□	1	Mr. X	Male				ID Card		Valid	✎	🗑
□	2	Mr. Y	Male				ID Card		Valid	✎	🗑
□	3	MR. Z	Male				ID Card		Valid	✎	🗑
□	4	Mr. A	Male				ID Card		Valid	✎	🗑

8.2.1.3. Configuring Arming Alarm

When face recognition succeeded or failed, the device outputs alarms.

Step 1 Click **AI → AI Config → Smart Plan**.

Step 2 Click **Rule Config** and then select **Face Recognition**.

Step 3 Click **Face Database Config** to enter the face database configuration page.

Step 4 Click 🛡 next to the face database to be configured.

Step 5 Arm face database.

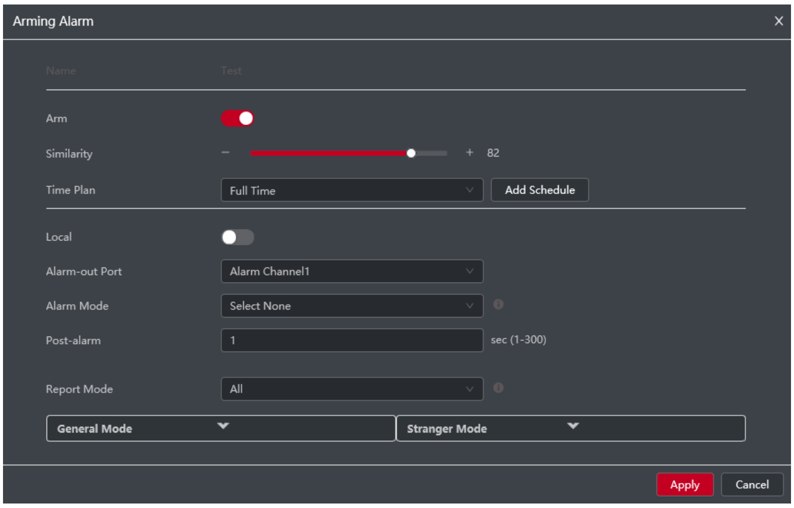
a. Click ○ to enable arm function.

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

b. Set similarity.

The detected face will only match the face features in the face database when the defined similarity is reached. After successful match, the comparison result is displayed on the **Live** page.

Figure 8-11



Arming Alarm

Name Test

Arm ●

Similarity − + 82

Time Plan Full Time

Local ○

Alarm-out Port Alarm Channel1

Alarm Mode Select None

Post-alarm 1 sec (1-300)

Report Mode All

Step 6 Select **Alarm Mode**.

- **All**: The camera outputs alarms whether the detected face matches the face picture inthe database or not.
- **General:** The camera outputs alarms when the detected face matches that in the facedatabase.
- **Stranger**: The camera outputs alarms when the detected face fails to match that in the face database.
- **Select none**: The camera does not output alarms whether the detected face matchesthe face picture in the database or not.

Step 7 Set arming periods and alarm linkage action.

- Click **Add Schedule** to add time plan.
- Set the linkage action and configure linkage parameters.

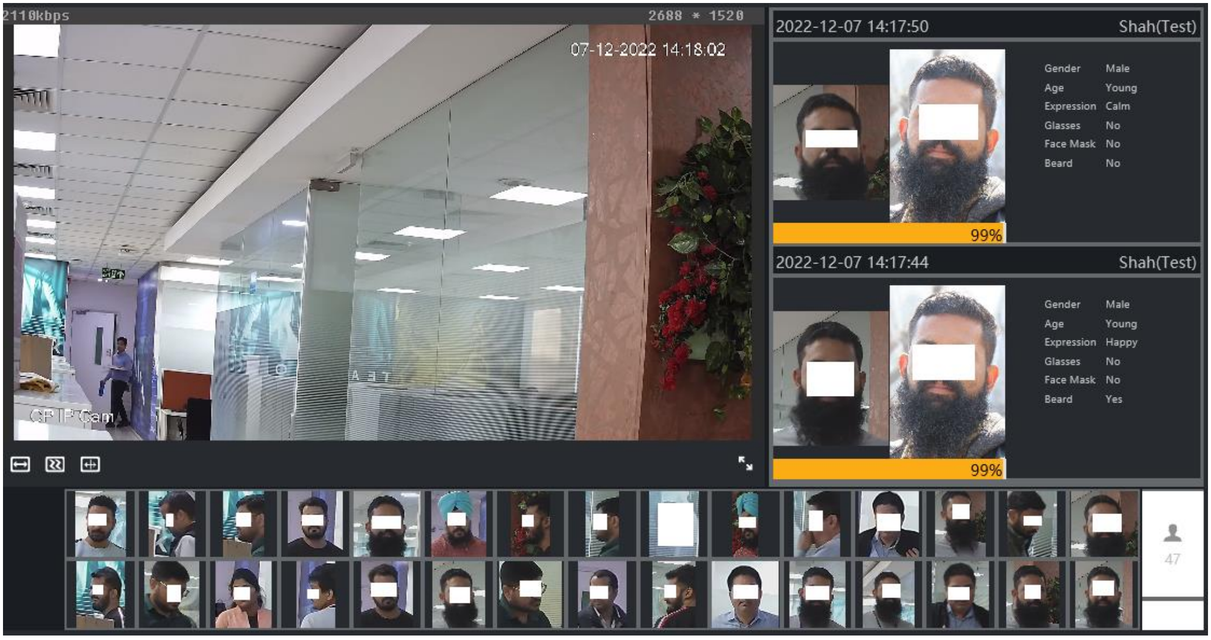
Step 8 Click **Apply**.

8.2.1.4. Viewing Face Recognition Result

On the **Live** page, select **Face Mode** from the display mode drop-down list on the upper-rightcorner to view the **Live** page of face recognition.

- The live image is displayed at the left side, and the captured face images and attribute information are displayed at the right side. When the recognition is successful, the captured face images, images in the database and the similarity of the face images and images in the database are displayed at the right side; the snapshot count and thumbnails are displayed at the bottom ofthe live image.
- Click ⚙ to set the attributes.

Figure 8-12



2022-12-07 14:17:50 Shah(Test)

Gender Male
Age Young
Expression Calm
Glasses No
Face Mask No
Beard No

99%

2022-12-07 14:17:44 Shah(Test)

Gender Male
Age Young
Expression Happy
Glasses No
Face Mask No
Beard Yes

99%

8.2.2. Configuring IVS

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

Here are the basic requirements on the scene.

- The target should occupy no more than 10% of the whole image.
- The target size in the image should be no more than 10 × 10 pixels. The size of abandoned objectin the image should be no less than 15 × 15 pixels (CIF image). The target height and width should no more than a third of the image height and width. The recommended target height is 10% of the image height.
- The brightness difference of the target and the background should be no less than 10 gray levels.
- The target should be continuously present in the image for no less than 2 seconds, and the moving distance should be larger its width and no less than 15 pixels (CIF image) at the sametime.
- Reduce the complexity of surveillance scene as much as you can. Intelligent analysis functions are not recommended to be used in scene with dense targets and frequent illumination change.
- Avoid areas such as glass, reflective ground, water surface, and areas interfered by branch, shadow and mosquito. Avoid backlight scene and direct light.

8.2.2.1. Global Configuration

Set global rules for IVS, including calibration drawing, calibration verification and sensitivity.

Background Information

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

Here is the applicable scene.

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

Pay attention to the following points.

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

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

Procedure

Step 1 Click **AI** → **AI Config** →> **Smart Plan**.

Step 2 Click **Rule Config**, and then select **IVS**.

Step 3 Click **Global Config**.

Step 4 Configure calibration area and rulers on the left screen.

a. Click □ and draw a calibration area in the image, and right-click to finish the drawing.

b. Click the ruler icon to draw one horizontal ruler and three vertical rulers in thecalibration area.

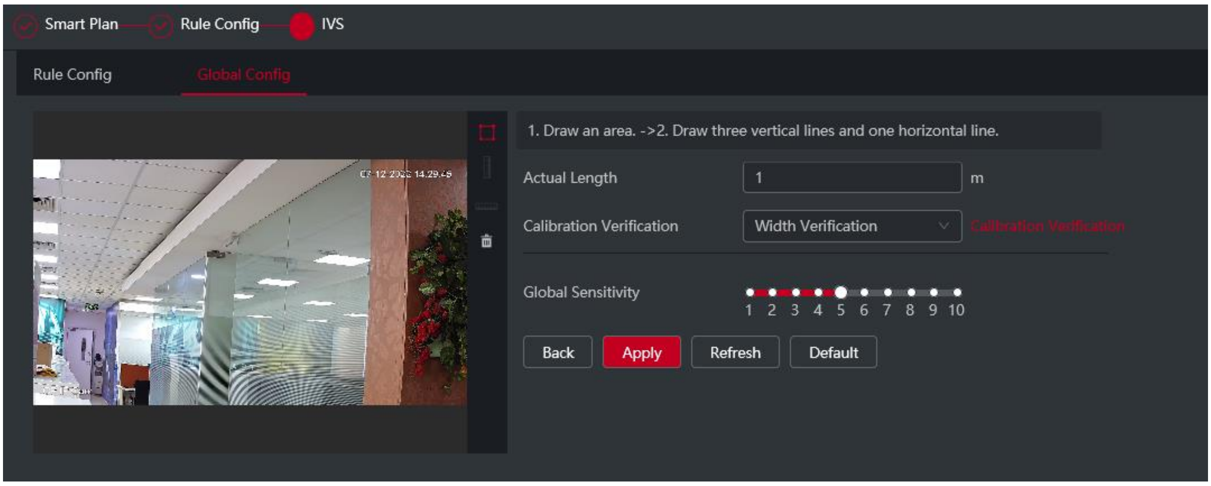
- ▯ indicates vertical ruler, and ▭ indicates horizontal ruler.
- Select an added ruler and click 🗑 to delete the ruler.

c. Configure the actual length.

Step 5 Configure parameters for the IVS of global configuration.

Sensitivity: Adjust the filter sensitivity. With higher value, it is easier to trigger an alarm when low-contrast object and small object are captured, and the false detection rate ishigher.

Figure 8-13



1. Draw an area. ->2. Draw three vertical lines and one horizontal line.

Actual Length	1 m
Calibration Verification	Width Verification
Global Sensitivity	5 (1 2 3 4 5 6 7 8 9 10)

Step 6 Click **Apply**.

Related Operations

a. Select the verification type, and then click **Calibration Verification**.

To verify vertical ruler and horizontal ruler, respectively select **Height Verification** and **Width Verification**.

b. Draw a straight line in the image to verify whether the rulers are correctly set.

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

8.2.2.2. Rule Configuration

This section introduces the rules used on IVS, including tripwire, intrusion, abandoned object, missing object, fast moving, parking detection, crowd gathering, crossing virtual fence and loitering detection.

Prerequisites

The global configuration for IVS has been completed.

Background Information

The roles and applicable scenes of various rules are as follows. The following section uses tripwire as an example to introduce the rule configuration of IVS.

Table 46

Rule	Functions	Applicable Scene
Crossing Virtual Fence	When a target crosses the fence toward the defined direction, the alarm is triggered, and the linkage isexecuted.	Scenes such as roads, airports, andother isolation zones.
Tripwire	When a target crosses the line toward the defined direction, the alarm is triggered, and the linkage is executed.	Scenes with sparse targets and no occlusion among targets, such as the perimeter protection of unattended area.
Intrusion	When the target enters, leaves, or appears in the detection area, an alarmis triggered, and the system performs defined alarm linkages.	
Abandoned Object	When an object is abandoned in thedetection area over the defined time, an alarm is triggered, and then the system performs defined alarm linkages.	Scenes with sparse targets and without obvious and frequent light change. Simple scene in the detection area is recommended. Missed alarm might increase inthe scenes with dense targets, frequent occlusion, and peoplestaying. In scenes with complex foreground and background, false alarm might be triggered for abandoned or missing object.
Missing Object	When an object is taken out of the detection area over the defined time, an alarm is triggered, and then the system performs defined alarm linkages.	
Fast Moving	When the motion speed is higher than the defined speed, an alarm is triggered, and then the system performs defined alarm linkages.	Scenes with sparse targets and less occlusion. The camera should be installed right above the monitoringarea. The light direction should be vertical to the motion direction.
Parking Detection	When the target stays over the definedtime, an alarm is triggered, and then the system performs defined alarm linkages.	Road monitoring and traffic management.
Crowd Gathering	When the crowd gathers or the crowddensity is large, an alarm is triggered, and then the system performs definedalarm linkages.	Scenes with medium or long distance, such as outdoor plaza, government entrance, station entrance and exit. Itis not suitable for short-distance view analysis.
Loitering detection	When the target loiters over the shortest alarm time, an alarm is triggered, and then the system performs defined alarm linkages. After alarm is triggered, if the target stays inthe area within the time interval of alarm, then alarm will be triggered again.	Scenes such as park and hall.

Procedure

Step 1 Click **AI** → **AI Config** → **Smart Plan**.

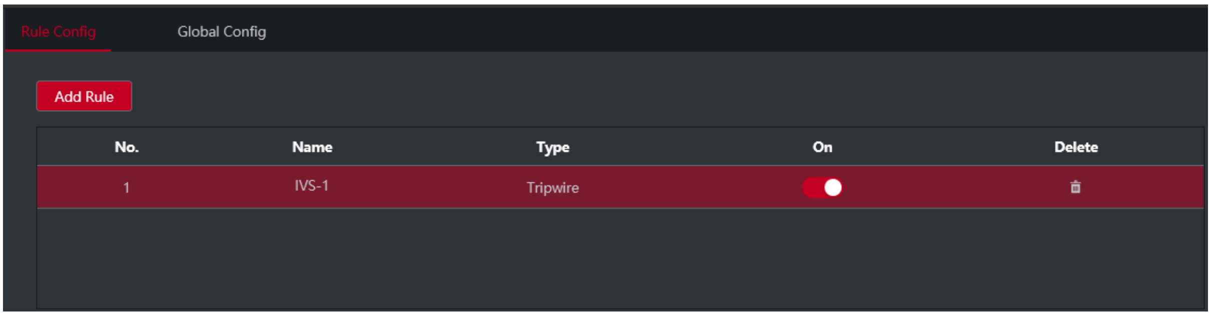
Step 2 Click **Rule Config** and then select **IVS**.

Step 3 Click **Rule Config**.

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

The added rules are displayed in the drop-down list. Click the name, and you can edit the rule name; the rule is enabled by default.

Figure 8-14



No.	Name	Type	On	Delete
1	IVS-1	Tripwire	●	🗑

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

Different rules have slightly different drawing requirements. After drawing rules, drag corners of the detection area to adjust the area range.

Table 47

Rule	Description
Crossing Virtual Fence	Draw a detection line.
Tripwire	
Intrusion	**Draw a detection area**. • During the detection of abandoned objects, the alarm is also triggered if pedestrian or vehicle stays for a long time. If the abandoned object is smaller than pedestrian and vehicle, set the target size to filter pedestrian and vehicle or properly extend duration to avoid false alarmtriggered by transient staying of pedestrian. • During the detection of crowd gathering, false alarm might be triggered by low installation height, large percentage of single person in an image or obvious target occlusion, continuous shaking of the camera, shaking of leaves and tree shade, frequent opening or closing of retractable door, or dense traffic or people flow.
Abandoned Object	
Missing Object	
Fast Moving	
Parking Detection	
Crowd Gathering	
Loitering Detection	

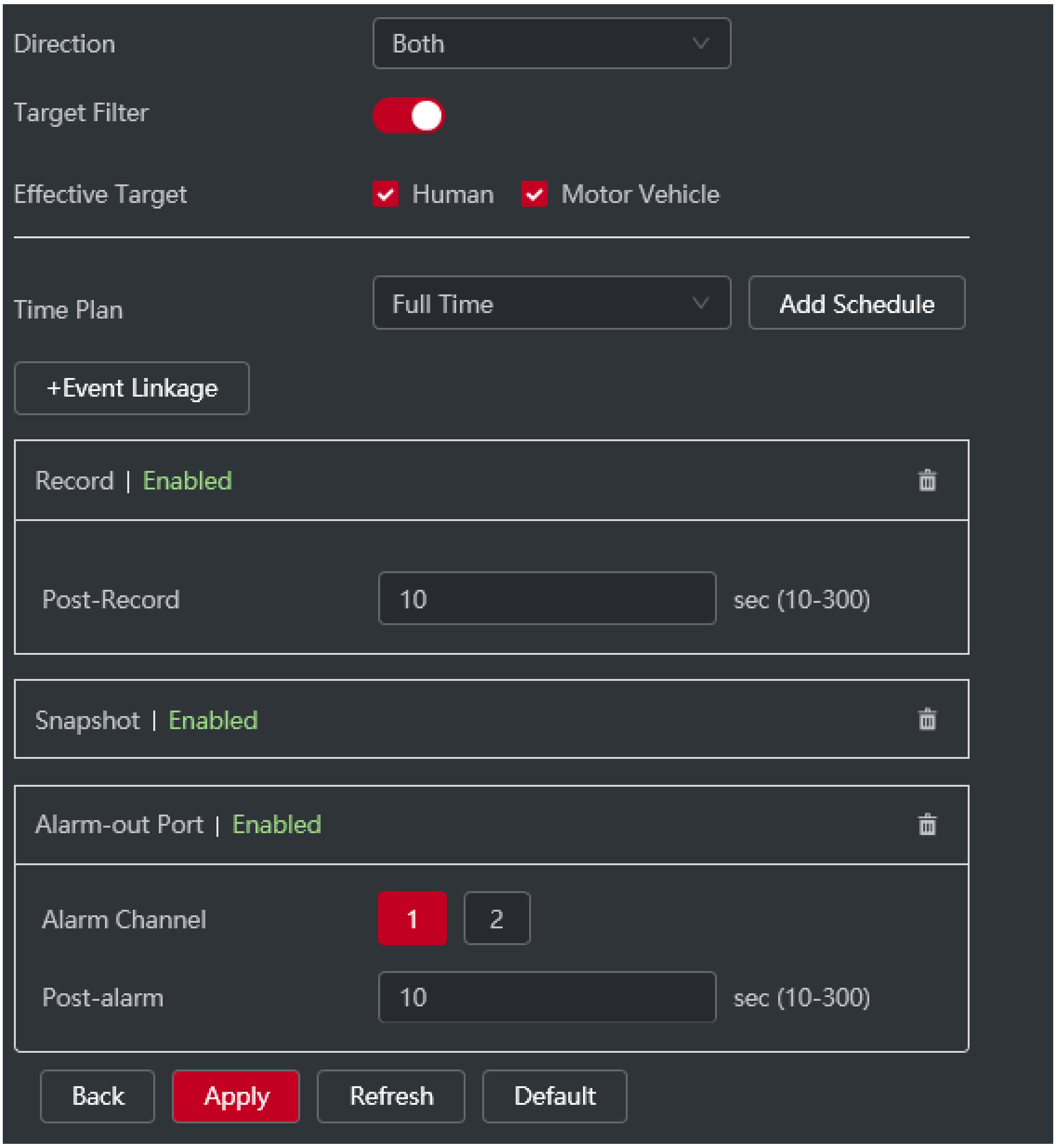
Step 6 (Optional) Click other icons at the right side of the image to filter targets in the image.

- Click min to draw the minimum size of the detection target and click max to draw themaximum size of the detection target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.

- When the rule of crowd gathering is configured, you need to draw the minimum gathering area. Click ▣ to draw the minimum gathering area in the scene. The alarmis triggered when the number of people in the detection area exceeds the minimum and the time exceeds the duration.
- Click ▦, and then press and hold the left mouse button to draw a rectangle, the pixelsize is displayed.
- Click 🗑 to delete the detection line.

Step 7 Set rule parameters for IVS.

Figure 8-15



Direction: Both

Target Filter: ●

Effective Target: ☑ Human ☑ Motor Vehicle

Time Plan: Full Time

Record | Enabled

Post-Record: 10 sec (10-300)

Snapshot | Enabled

Alarm-out Port | Enabled

Alarm Channel: 1 2

Post-alarm: 10 sec (10-300)

Table 48

Parameter	Description
Direction	Set the direction of rule detection. • When setting tripwire, select **A → B**, **B → A**, or **A ←→ B**. • When setting intrusion, select **Ente**r, **Exit,** or **Both**.
Target Filter / Effective Target	After enabling **Target filter**, effective targets are not detected, and alarms will not be triggered. This function is currently supported by tripwire, intrusion, and fast moving. 📖 Effective targets include Human and Motor Vehicle. Among them, non-motor vehicle belongs to the category of People.
Action	When setting intrusion action, select Appear or Cross.
Duration	• For abandoned object, the duration is the shortest time for triggering an alarm after an object is abandoned. • For missing object, the duration is the shortest time for triggering an alarm after an object is missing. • For parking detection, crowd gathering, or loitering detection, the duration is the shortest time for triggering an alarm after an object appears in the area.
Sensitivity	• For fast moving, sensitivity is related to the triggering speed. Lower sensitivity requires faster moving speed to trigger the alarm. • For crowd gathering, sensitivity is related to the alarm triggering time. It is easier to trigger the alarm with higher sensitivity.

Step 8 Set arming periods and alarm linkage action.

- Click **Add Schedule** to add time plan.
- Click **+ Event Linkage** to set the linkage action and configure linkage parameters.

Step 9 Click **Apply**.

If you need to click 🔔 on the upper-right corner of the page to view alarm information,you need to subscribe relevant alarm event.

8.2.3. Configuring Video Metadata

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

8.2.3.1. Global Configuration

Configure global rules for video metadata, including global parameters for faces and scenes.

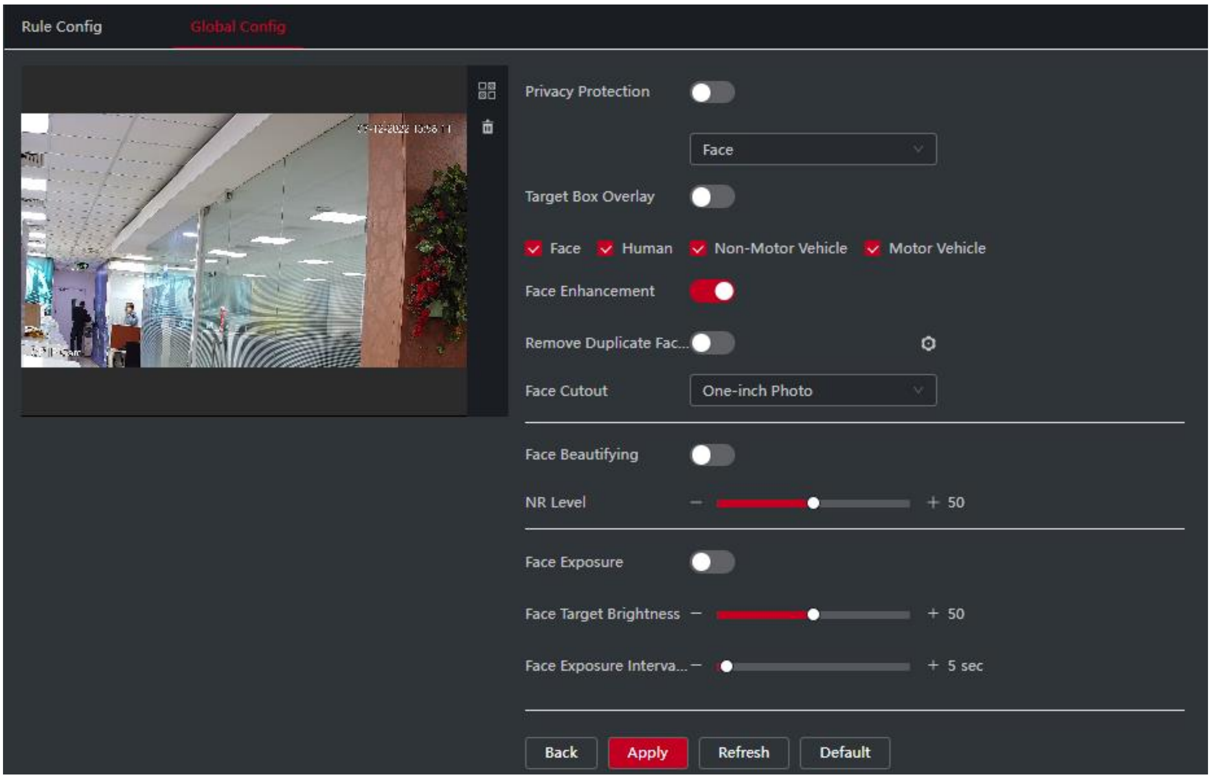
Step 1 Select **AI → AI Config → Smart Plan**.

Step 2 Click **Rule Config**, and then select **Video Metadata**.

Step 3 Click **Global Config**.

Step 4 Configure global configuration parameters.

Figure 8-16



Privacy Protection: off

Face

Target Box Overlay: off

☑ Face ☑ Human ☑ Non-Motor Vehicle ☑ Motor Vehicle

Face Enhancement: on

Remove Duplicate Fac...: off

Face Cutout: One-inch Photo

Face Beautifying: off

NR Level: 50

Face Exposure: off

Face Target Brightness: 50

Face Exposure Interva...: 5 sec

Table 49

Parameter	Description
Target Box Overlay	Overlay target box on the captured images to mark the targetposition. Four types of target boxes are supported. Select the target box asneeded. The captured images are stored in SD card or the configuredstorage path.
Face Enhancement	Enable **Face Enhancement** to preferably guarantee clear face with low stream.
Face Cutout	Set a range for matting face image, including face image andone-inch image.
Picture mode	• Default: Apply default image parameters to capture images. • Number Plate Priority: Apply the image parameters corresponding to the number plate to capture the image. • Face Priority: Apply the image parameters corresponding to theface to capture the image.

Step 5 Click **Apply**.

8.2.3.2. Rule Configuration

Configure detection scenes and rules, including the rule configuration of people, non-motor vehiclesand motor vehicle.

Prerequisites

Global configuration for video metadata has been completed.

Procedure

Step 1 Select **AI** → **AI Config** → **Smart Plan**.

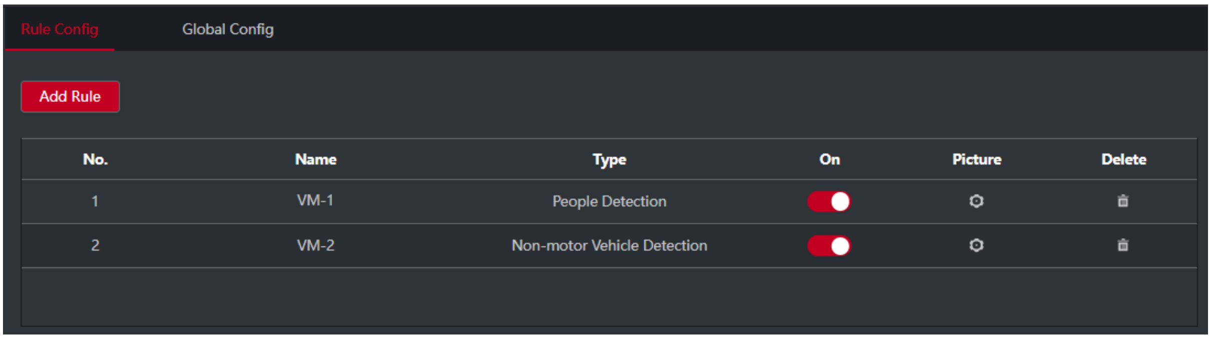
Step 2 Click **Rule Config**, and then select **Video Metadata**.

Step 3 Click **Rule Config**.

Step 4 Click **Add Rule** and then select rule type from the drop-down list.

The added rules are displayed in the drop-down list. Click the text box under **Name** to edit the rule name. The rule is enabled by default.

Figure 8-17



Rule Config | Global Config

Add Rule

No.	Name	Type	On	Picture	Delete
1	VM-1	People Detection	●	⚙	🗑
2	VM-2	Non-motor Vehicle Detection	●	⚙	🗑

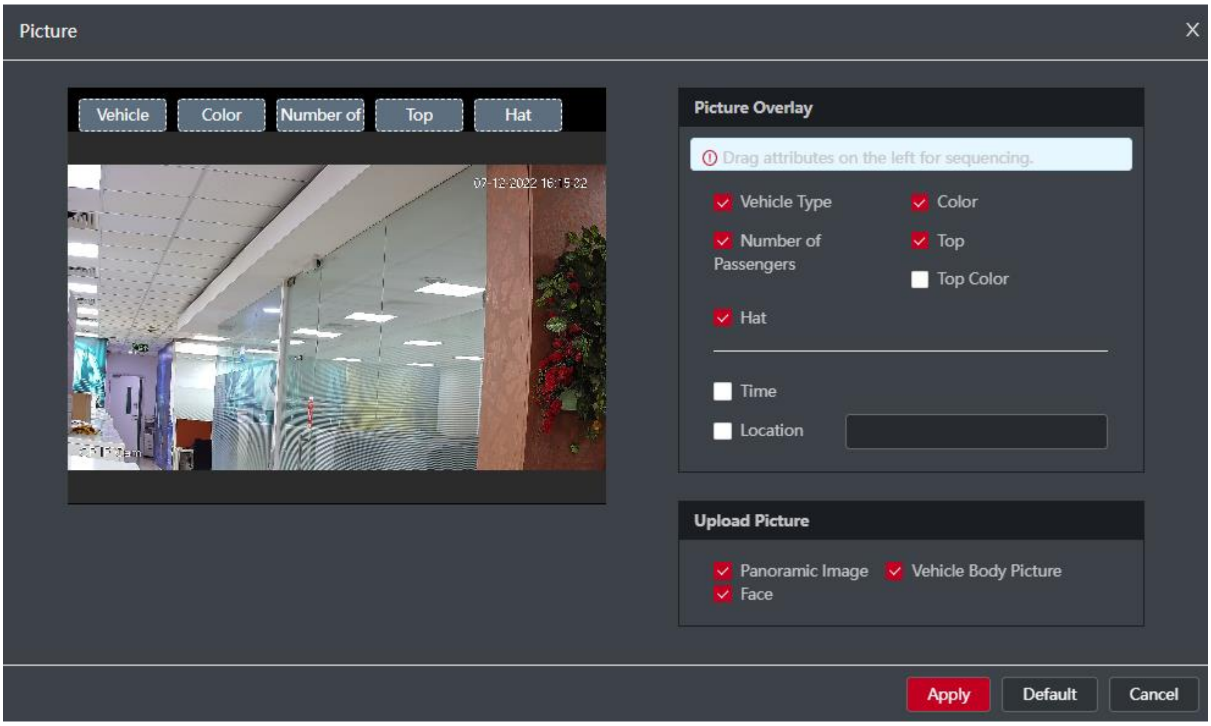
Step 5 Configure image information.

a. Click the ⚙ after the corresponding rule.

b. Configure overlay information and adjust its position.

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

Figure 8-18



Picture

Picture Overlay

Drag attributes on the left for sequencing.

☑ Vehicle Type ☑ Color
☑ Number of Passengers ☑ Top
□ Top Color
☑ Hat

□ Time
□ Location

Upload Picture

☑ Panoramic Image ☑ Vehicle Body Picture
☑ Face

Apply | Default | Cancel

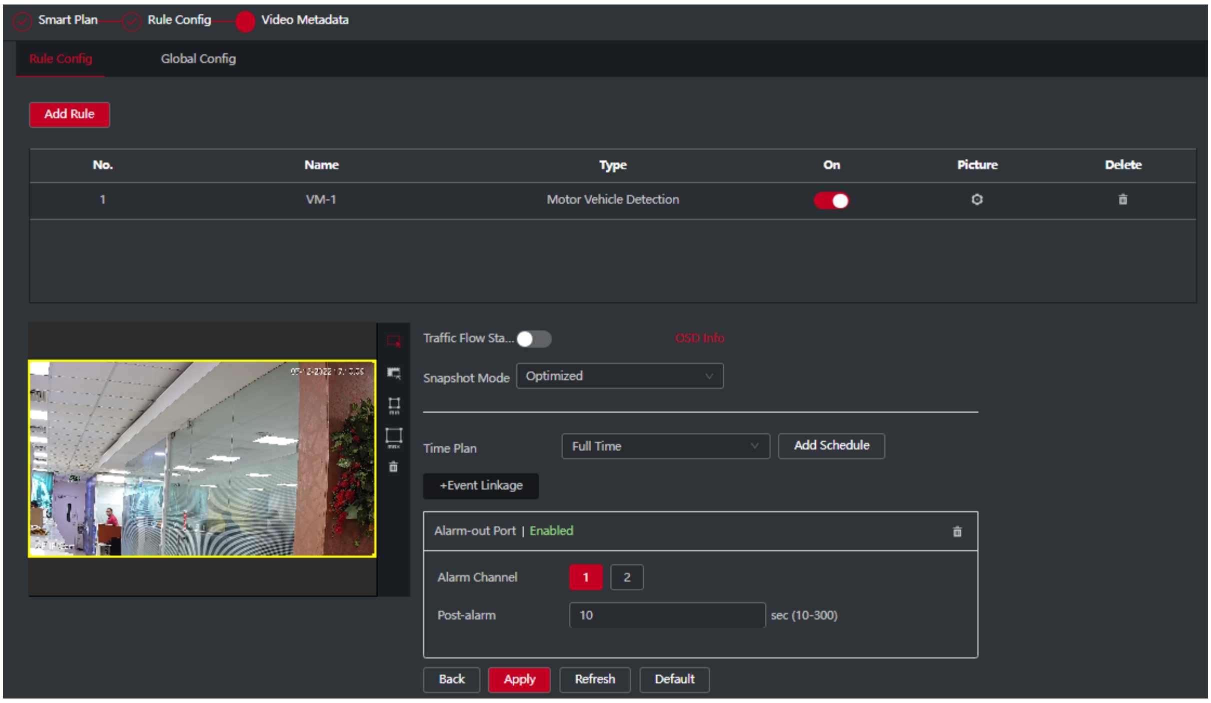
c. Click **Apply**.

Step 6 (Optional) Click the icon on the right of the screen to draw detection area, exclusion area and filtering target model on the monitoring screen.

- After enabling the rule, the detection area is displayed in the monitoring screen. Click ⬚, and then drag any corner of the box to adjust the size of the area
- Click ⬚ to draw an area exclusion area for face detection in the image, and right-click to finish the drawing.
- Click □ to draw the minimum size of the detection target and click □ to draw the maximum size of the detection target. Only when the target size is between the maximum size and the minimum size, can the alarm be triggered.
- Click 🗑 to delete the drawn filtering rule detection line or area.

Step 7 Configure the rule parameters of video metadata.

Figure 8-19



Smart Plan — Rule Config — Video Metadata

Rule Config | Global Config

Add Rule

No.	Name	Type	On	Picture	Delete
1	VM-1	Motor Vehicle Detection	●	⚙	🗑

Traffic Flow Sta... ○ OSD Info

Snapshot Mode: Optimized

Time Plan: Full Time | Add Schedule

+Event Linkage

Alarm-out Port | Enabled

Alarm Channel: 1 2

Post-alarm: 10 sec (10-300)

Back | Apply | Refresh | Default

Table 50

Parameter	Description
People Flow Statistics	Click ○ next to **People Flow Statistics** to count the number of people inthe detection area.
Traffic Flow Statistics (Non-Motor Vehicles	Click ○ next to **Traffic Flow Statistics (Non-motor Vehicles)** to countthe number of non-motor vehicles in the detection area.
Traffic Flow Statistics	Click ○ next to **Traffic Flow Statistics** to count the number of motorvehicles in the detection area.

Parameter	Description
Snapshot Mode	- Optimized: Capture the images until the vehicle disappears from the Images and upload the clearest image. - Tripwire: Capture the images when the vehicle triggers tripwire as the configured direction. The steps are as follows: a. Select **Tripwire**. b. Select the direction from **A to B**, **B to A** and **Both.** c. Adjust the position of rule line as needed.

Step 8 Set arming periods and alarm linkage action.

- Click **Add Schedule** to add time plan.
- Click **+ Event Linkage** to set the linkage action and configure linkage parameters.

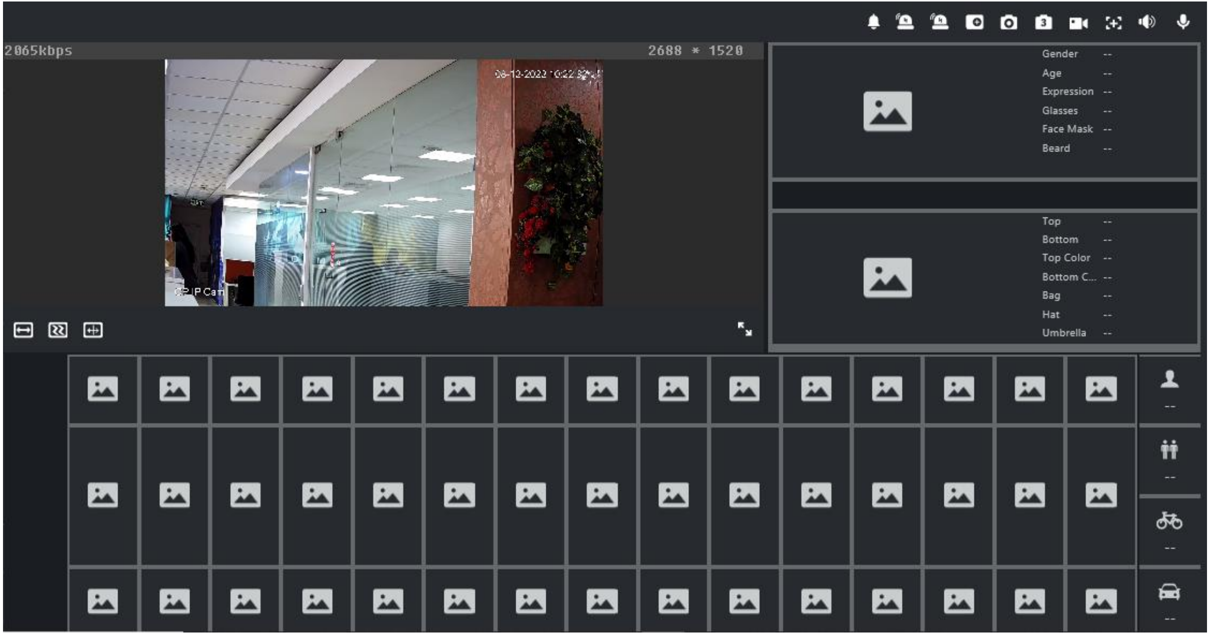
Step 9 Click **Apply**

8.2.3.3. Viewing Video Metadata Report

Select **Metadata Mode** on the upper-left corner of the **Live** page to view the live video image of video metadata.

- The left side displays real-time live screen; the right side displays large view of the snapshot and detailed attribute information; the bottom displays the face, human body, non-motor vehicle and motor vehicle snapshot statistics and snapshot thumbnails.
- Click ⚙ to change the attributes shown in the image.

Figure 8-20



8.3. Configuring Tour Plan

You can configure the tour mode and time plan for different periods.

Step 1 Select **AI** → **Tour Plan**.

Step 2 Select **Enable** to enable tour plan function.

Step 3 Select tour mode and idle interval.

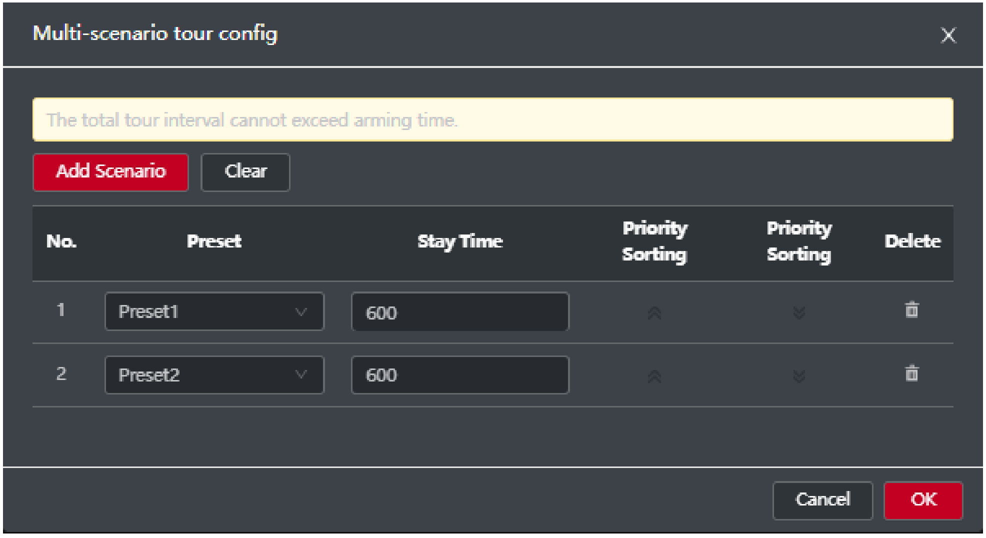
- **Tour mode Select**: It only supports **Scene Priority** at present. The Camera toursaccording to the set duration of the scene.
- **Idle Interval**: The time between the user manually operates the Camera and theCamera automatically rotates to the smart plan scene.

Step 4 Configure tour plan.

a. Set the start time and end time of the tour.

b. Select period, and then click **Setting** to configure multi-scenario tour.

Figure 8-21



Multi-scenario tour config ×

The total tour interval cannot exceed arming time.

Add Scenario | Clear

No.	Preset	Stay Time	Priority Sorting	Priority Sorting	Delete
1	Preset1	600	︽	︾	🗑
2	Preset2	600	︽	︾	🗑

Cancel | OK

Table 51

Parameter	Description
Stay Time	Set the time that the Camera stays in the scene. Double-click the staytime to modify the time.
Priority Sorting	Set the priority of multiple scenes. Click ︽ or ︾ to adjust the order.
Delete	Click 🗑 to delete the scene.
Add Scenario	Click **Add Scenario** to add a new tour scene.

c. Click **OK** to complete the configuration of multi-scenario tour.

Step 5 (Optional) Click **Copy** to copy the configuration to the selected date.

Step 6 Click **OK**

9. Security

9.1. Security Status

Background Information

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

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

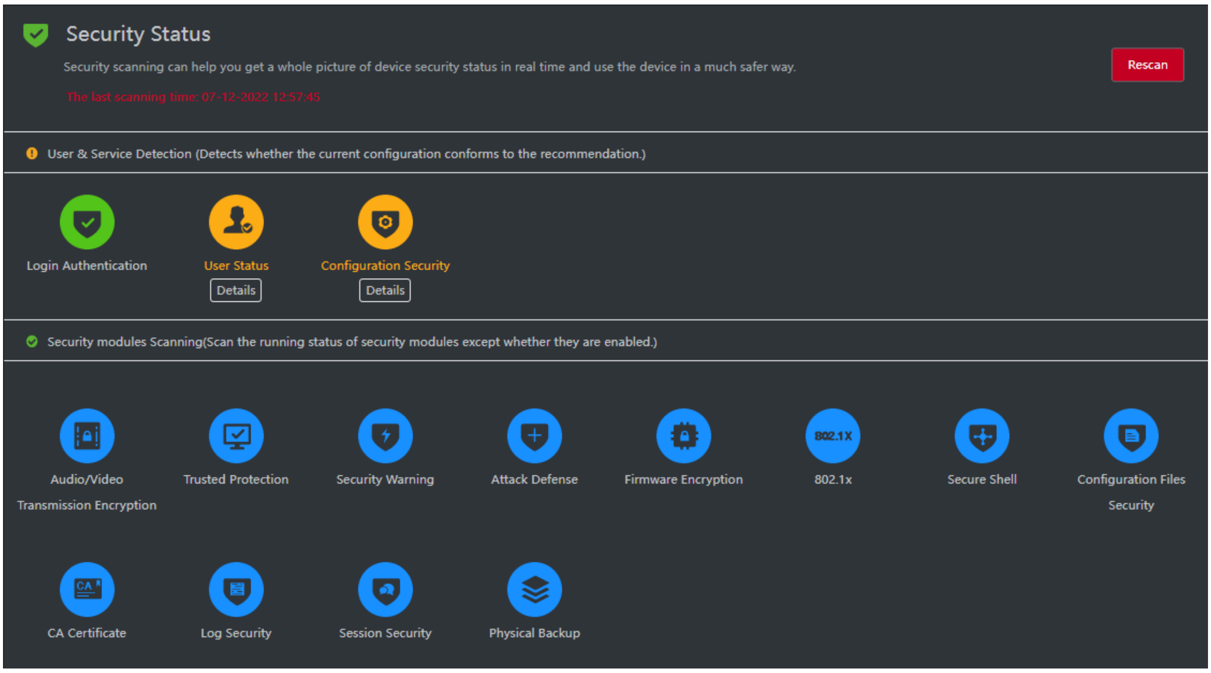
Procedure

Step 1 Select **Security** → **Security Status**.

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

During the scanning, the icon is grey. When the icon turns blue, the scanning is complete.

Figure 9-1



Security Status

Security scanning can help you get a whole picture of device security status in real time and use the device in a much safer way.

The last scanning time: 07-12-2022 12:57:45

User & Service Detection (Detects whether the current configuration conforms to the recommendation.)

Security modules Scanning(Scan the running status of security modules except whether they are enabled.)

Related Operations

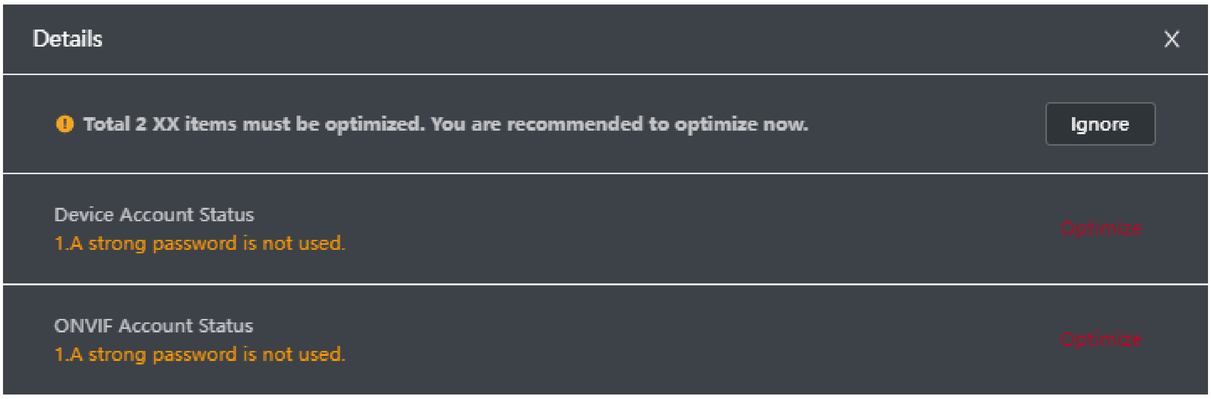
After scanning, different results will be displayed in different color. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

a. Click **Details** to view the details of the scanning result.

b. Click **Ignore** to ignore the exception, and it will not be scanned in next scanning.

c. Click **Optimize**, and the corresponding page is displayed. You can edit the configuration to clear the exception.

Figure 9-2



Details

Total 2 XX items must be optimized. You are recommended to optimize now.

Device Account Status
1.A strong password is not used.

ONVIF Account Status
1.A strong password is not used.

9.2. System Service

Service functions can be used only after system services are enabled.

9.2.1. 802.1x

Cameras can connect to LAN after passing 802.1x authentication.

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

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

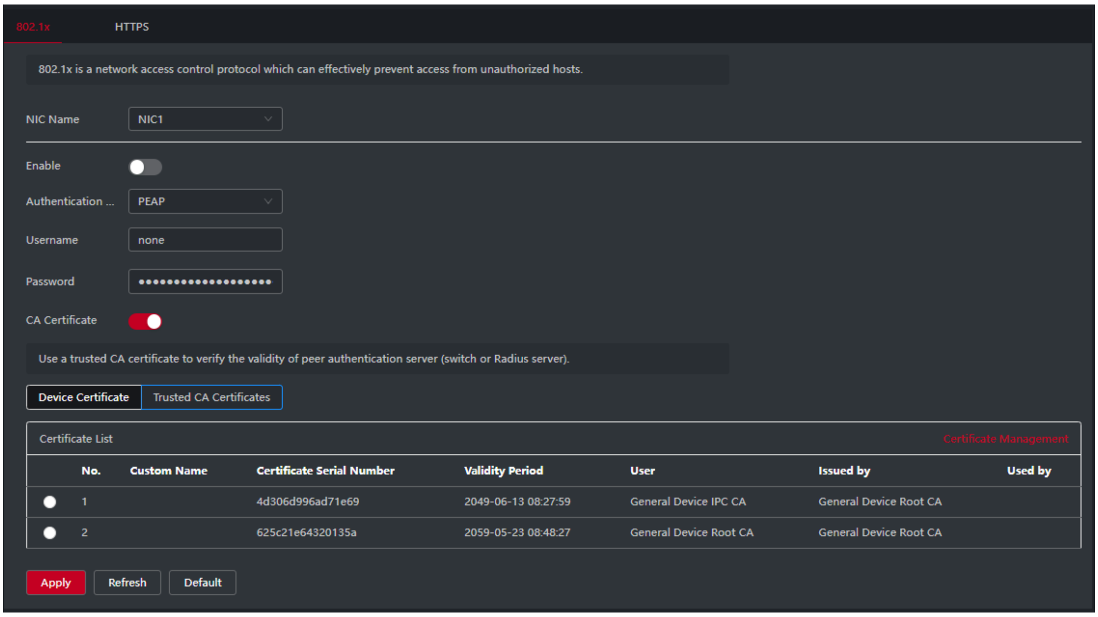
Step 3 Select the authentication mode, and then configure parameters.

- PEAP (Protected EAP protocol).

a. Select PEAP as the authentication mode.
b. Enter the username and password that has been authenticated on the server.
c. (Optional) Click ○ next to CA certificate and select the trusted CA certificate inlist.

If there is no certificate in the list, click **Certificate Management** at the leftnavigation bar.

Figure 9-3



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

NIC Name: NIC1

Enable: ○

Authentication ...: PEAP

Username: none

Password: ••••••••••••••••••

CA Certificate: ●

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

Certificate List

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
○	1		4d306d996ad71e69	2049-06-13 08:27:59	General Device IPC CA	General Device Root CA	
○	2		625c21e64320135a	2059-05-23 08:48:27	General Device Root CA	General Device Root CA	

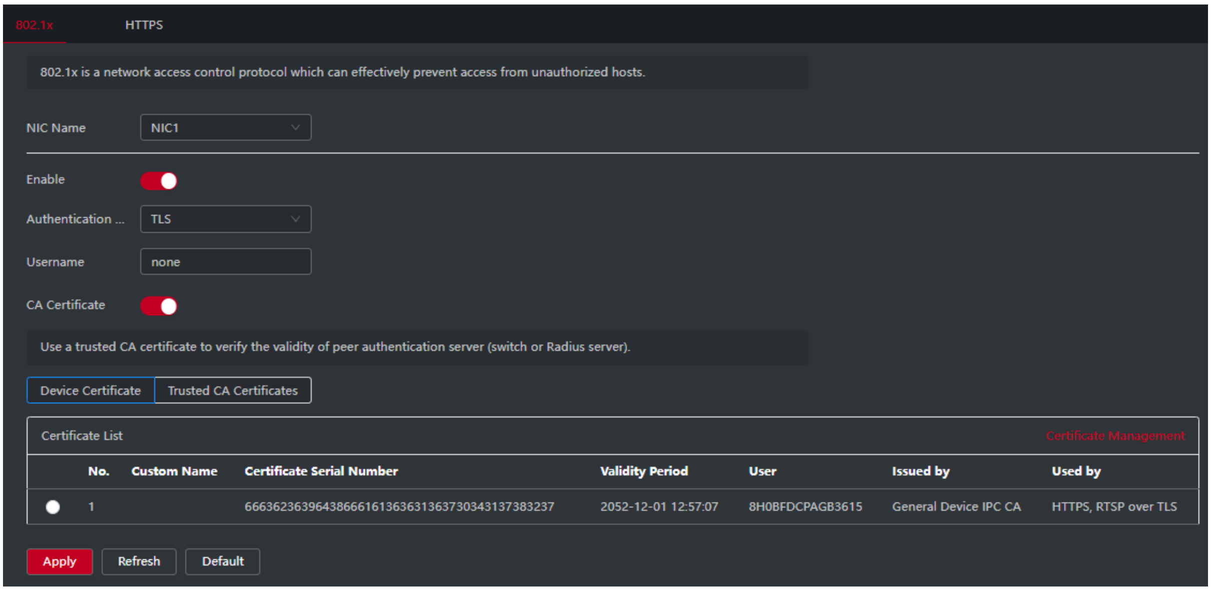
- TLS (Transport Layer Security). It is applied in two communication application programs to guarantee the security and integrity of the data.
  a. Select TLS as the authentication mode.
  b. Enter the username.
  c. Select the certificate from the certificate list on the **Device Certificate** page.

If there is no certificate in the list, click **Certificate Management** at the leftnavigation bar.

  d. (Optional) Click ○ next to CA certificate and select the trusted CA certificate inlist.

If there is no certificate in the list, click **Certificate Management** at the leftnavigation bar.

Figure 9-4



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

NIC Name: NIC1

Enable: on

Authentication ...: TLS

Username: none

CA Certificate: on

Use a trusted CA certificate to verify the validity of peer authentication server (switch or Radius server).

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
○	1		66636236396438666161363631363730343137383237	2052-12-01 12:57:07	8H0BFDCPAGB3615	General Device IPC CA	HTTPS, RTSP over TLS

Step 4 Click **Apply**.

9.2.2. HTTPS

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

- We recommend enabling the HTTPS. Otherwise, the device data may be leaked.
- After HTTPS is enabled, TLSv1.1 and earlier versions are supported by default. However, earlier version of TLS might have security risks. Please select carefully.

Procedure

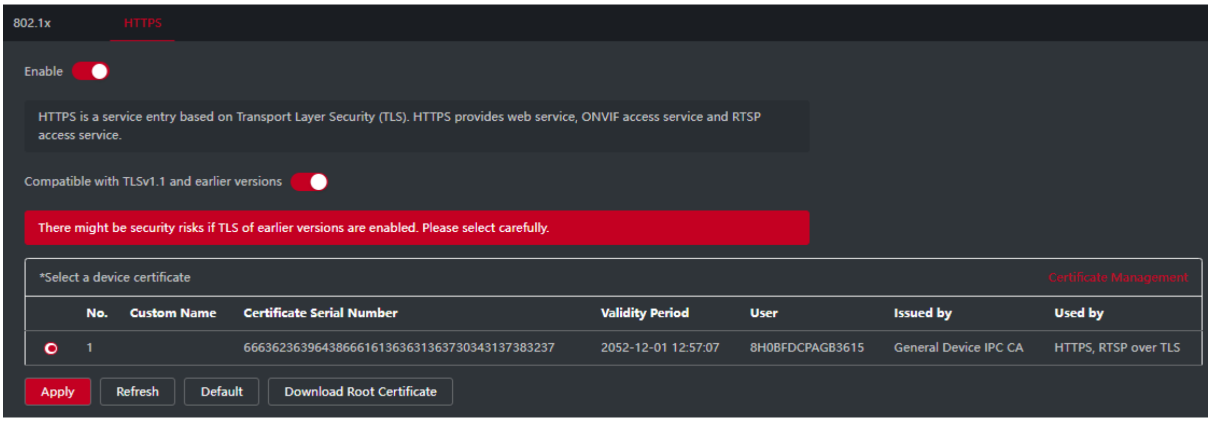
Step 1 Select **Security** → **System Service** → **HTTPS**.

Step 2 Click ○ to enable HTTPS.

Step 3 Select the certificate.

If there is no certificate in the list, click **Certificate Management** at the left navigation bar.

Figure 9-5



Enable ●

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service, ONVIF access service and RTSP access service.

Compatible with TLSv1.1 and earlier versions ●

There might be security risks if TLS of earlier versions are enabled. Please select carefully.

*Select a device certificate

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
●	1		66636236396438666161363631363730343137383237	2052-12-01 12:57:07	8H0BFDCPAGB3615	General Device IPC CA	HTTPS, RTSP over TLS

Step 4 Click **Apply**.

Related Operations

Enter https://IPaddress in the browser.

- If you have already installed the certificate, the normal login page will be displayed.
- If you have not installed the certificate, the browser displays a certificate error message.

9.3. Attack Defense

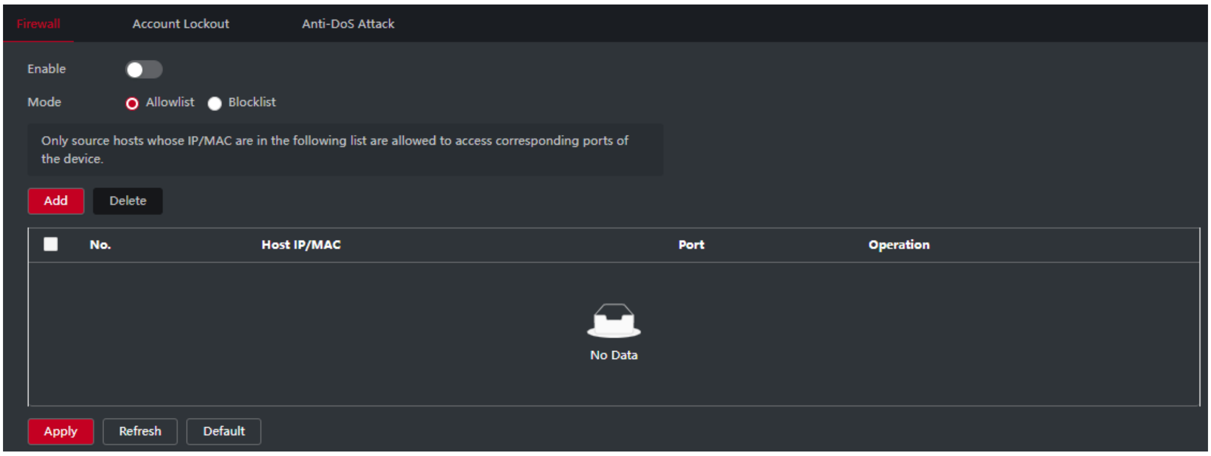
9.3.1. Firewall

Configure firewall to limit access to the camera.

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

Step 2 Click ◯ to enable the firewall function.

Figure 9-6



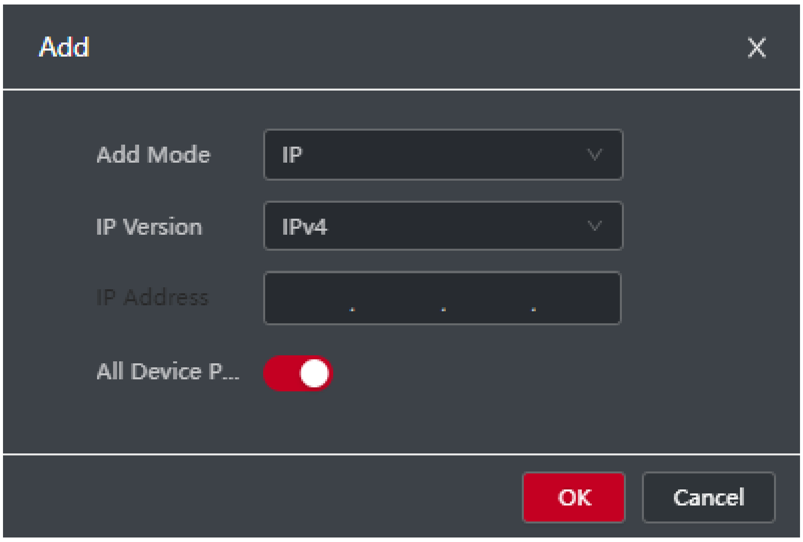
Only source hosts whose IP/MAC are in the following list are allowed to access corresponding ports of the device.

Step 3 Select **Allowlist** or **Blocklist** as the mode.

- **Allowlist**: Only when the IP/MAC address of your PC is in the allowlist, can you accessthe camera. Ports are the same.
- **Blocklist**: When the IP/MAC address of your PC is in the blocklist, you cannot access the camera. Ports are the same.

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

Figure 9-7



Add Mode: IP

IP Version: IPv4

Step 5 Click **Apply**.

Related Operations

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

9.3.2. Account Lockout

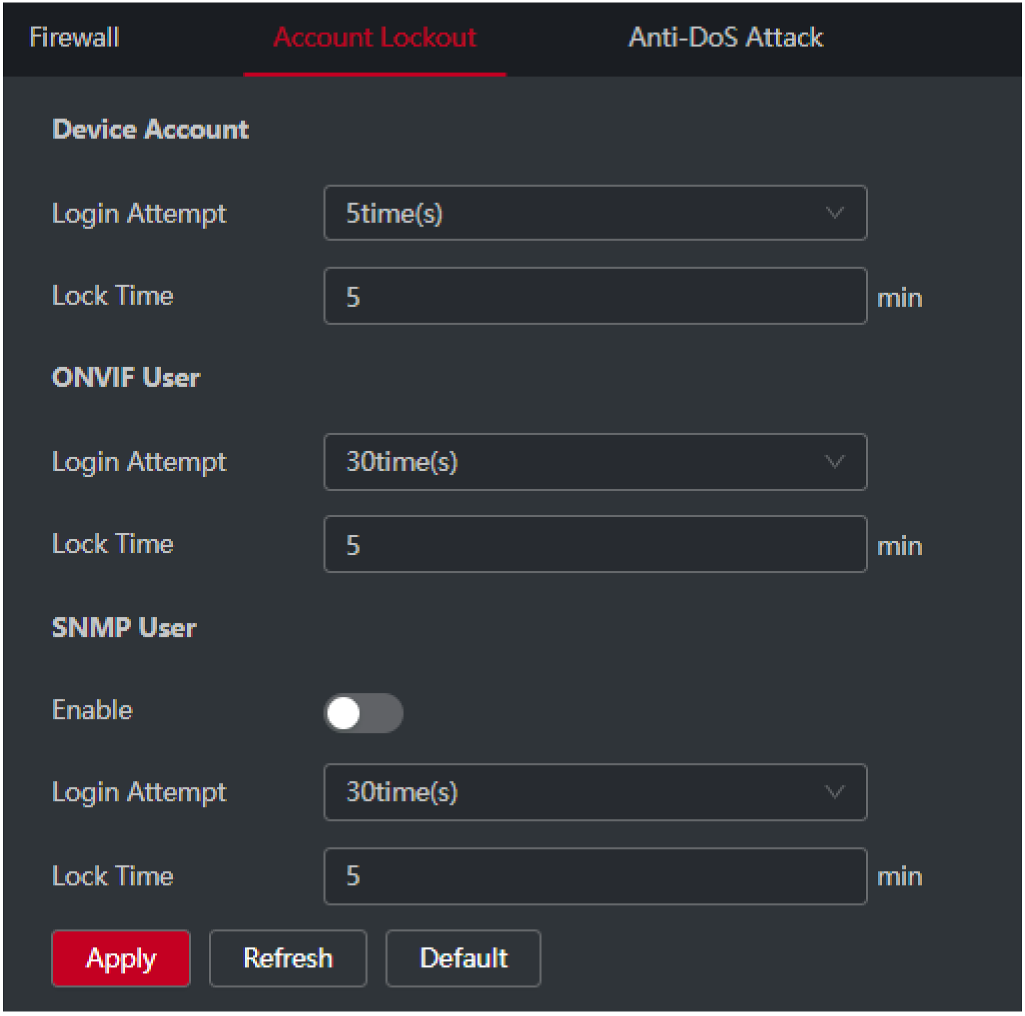
If you consecutively enter a wrong password more than the configured value, the account will belocked.

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

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

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

Figure 9-8



Device Account

Login Attempt: 5time(s)

Lock Time: 5 min

ONVIF User

Login Attempt: 30time(s)

Lock Time: 5 min

SNMP User

Enable

Login Attempt: 30time(s)

Lock Time: 5 min

Step 3 Click **Apply**.

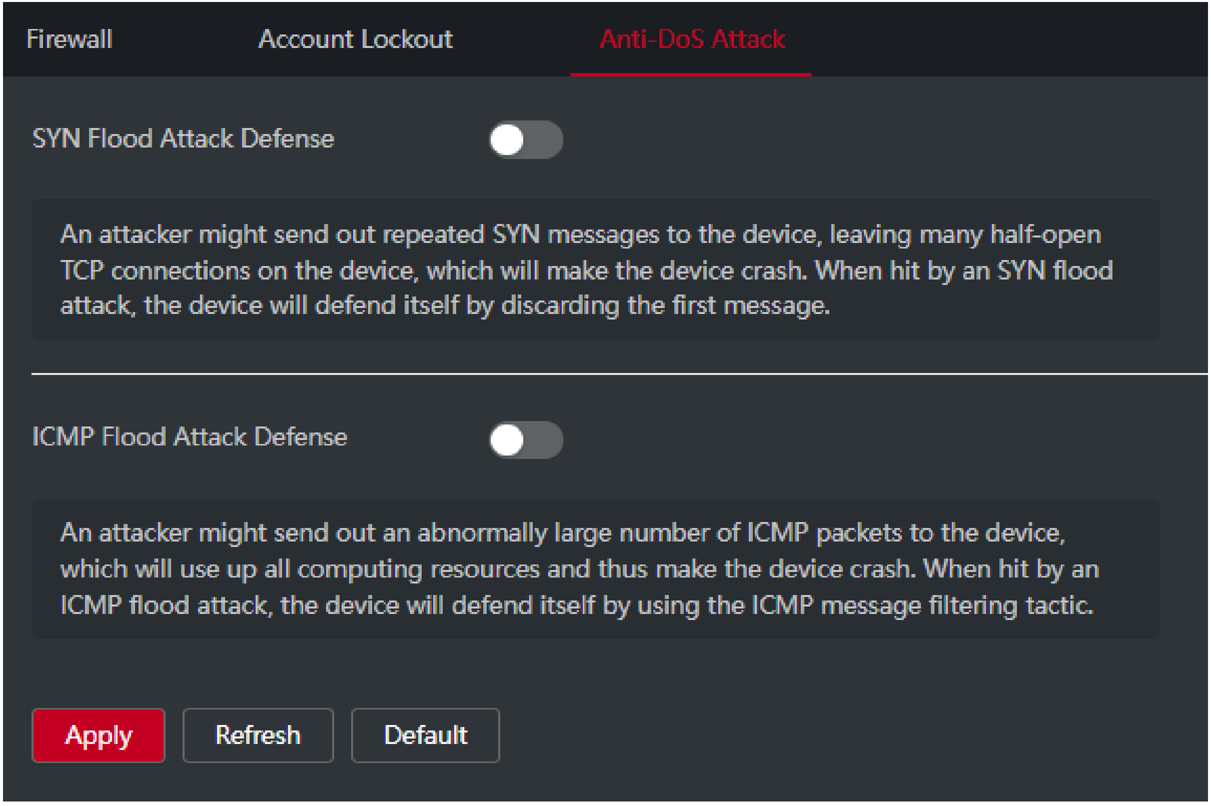
9.3.3. Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the deviceagainst DoS (Denialof Service) attack.

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

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

Figure 9-9



An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

9.4. CA Certificate

9.4.1. Installing Device Certificate

Create a certificate or upload an authenticated certificate, for example when you log in through HTTPS with your PC, you need to verify device certificate.

9.4.1.1. Creating Certificate

Creating certificate in the device.

9.4.1.1.1. Procedure

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

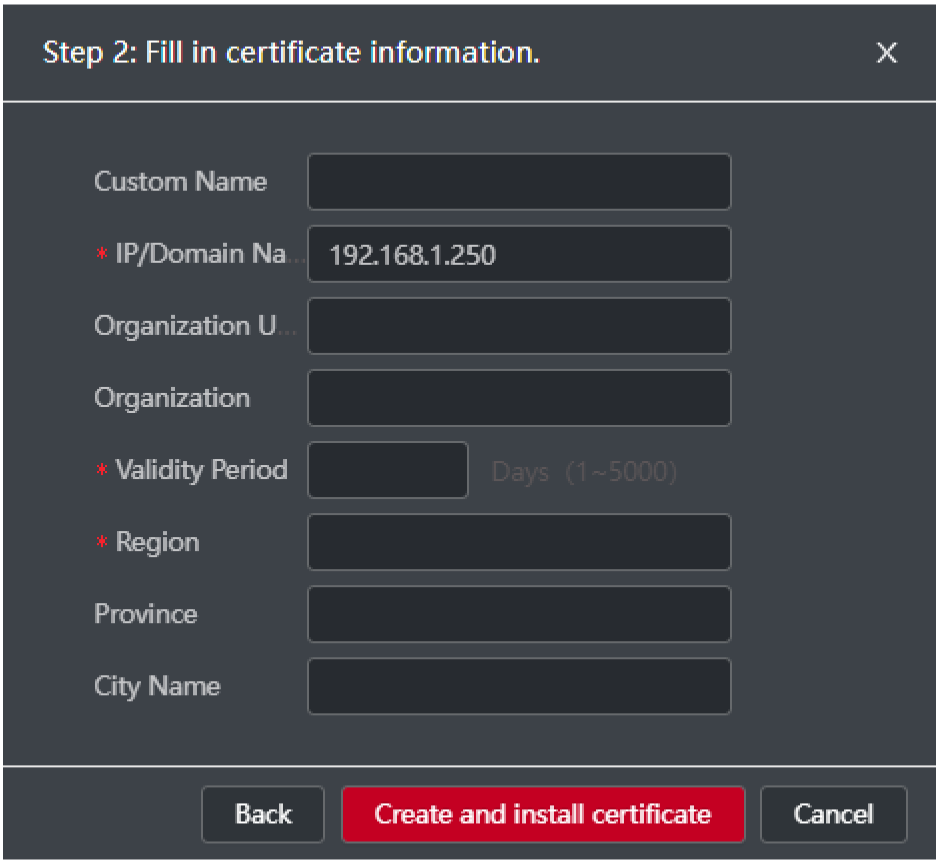
Step 2 Select **Install Device Certificate**.

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

Step 4 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 9-10



Step 2: Fill in certificate information.

Custom Name

* IP/Domain Na... 192.168.1.250

Organization U...

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

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

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

Related Operations

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

9.4.1.2. Applying for and Importing CA Certificate

Import the third-party CA certificate to the camera.

Procedure

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

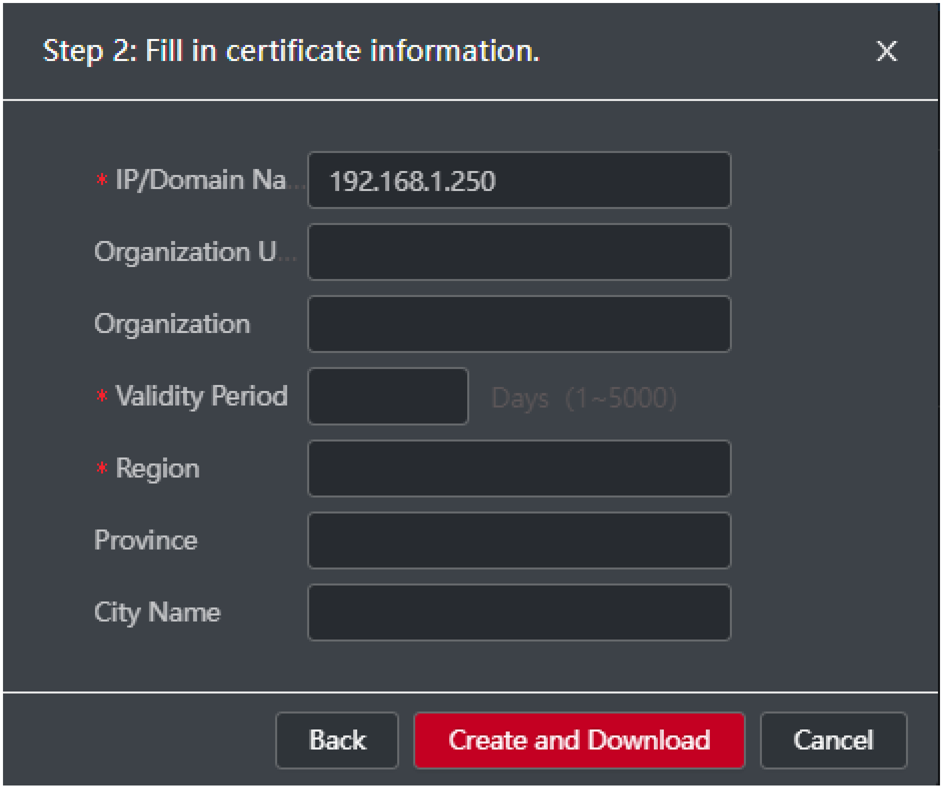
Step 2 Select **Installing Device Certificate**.

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

Step 4 Enter the certificate information.

IP or domain name of the device is automatically entered in **IP/Domain Name**.

Figure 9-11



Step 2: Fill in certificate information.

* IP/Domain Na... 192.168.1.250

Organization U...

Organization

* Validity Period Days (1~5000)

* Region

Province

City Name

<u>Step 5</u> Click **Create and Download**. Save the request file to your PC.

<u>Step 6</u> Apply for the CA certificate from the third-party certificate authority.

<u>Step 7</u> Import the signed CA certificate.

a. Save the CA certificate to the PC.
b. Select **Install Device Certificate**, click **Apply for CA Certificate and Import (Recommended)**, and then click **Next**.
c. Click **Browse** to select the signed CA certificate.
d. Click **Install and**

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

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

Related Operations

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

9.4.1.3. Installing Existing Certificate

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

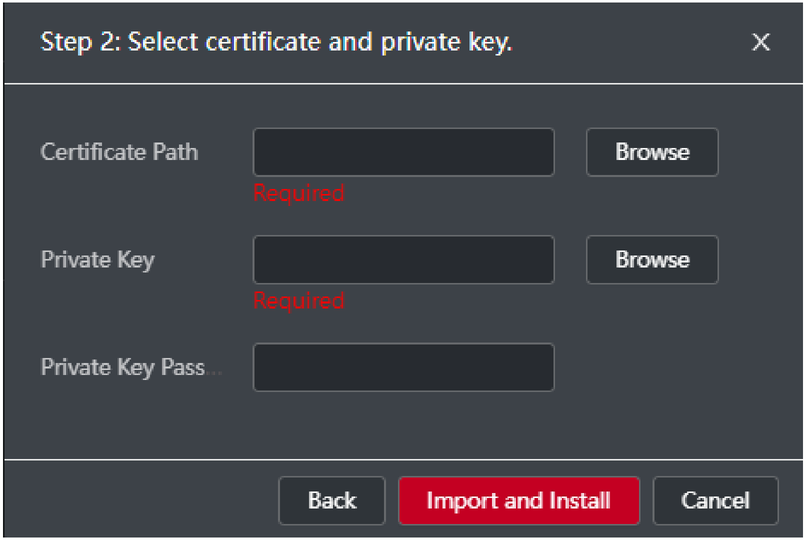
<u>Step 1</u> Select **Security → CA Certificate → Device Certificate**.

<u>Step 2</u> Select **Install Device Certificate**.

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

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

Figure 9-12



Step 2: Select certificate and private key.

Certificate Path [ ] Browse
Required

Private Key [ ] Browse
Required

Private Key Pass... [ ]

Step 5 Click **Import and Install**.

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

Related Operations

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

9.4.2. Installing Trusted CA Certificate

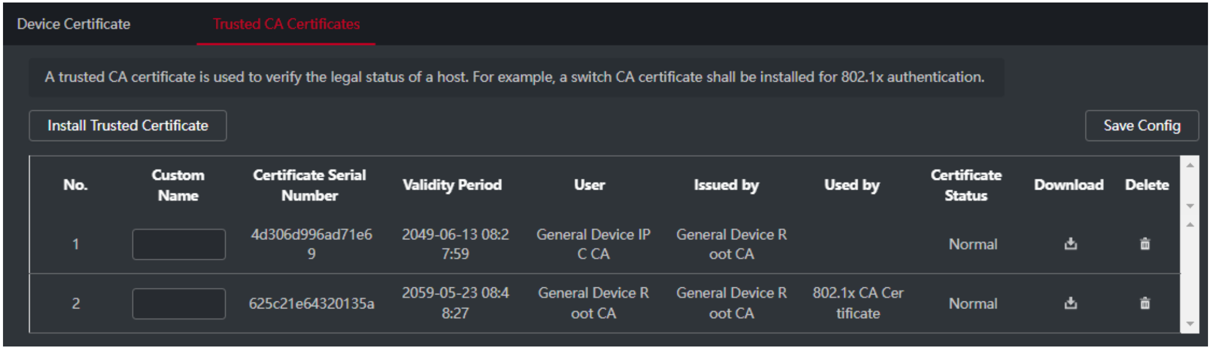
CA certificate is a digital certificate for the legal identity of the camera. For example, when thecamera accesses the LAN through 802.1x, the CA certificate is required.

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

Step 2 Select **Install Trusted Certificate**.

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

Figure 9-13



A trusted CA certificate is used to verify the legal status of a host. For example, a switch CA certificate shall be installed for 802.1x authentication.

No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by	Certificate Status	Download	Delete
1		4d306d996ad71e69	2049-06-13 08:27:59	General Device IPC CA	General Device Root CA		Normal	⬇	🗑
2		625c21e64320135a	2059-05-23 08:48:27	General Device Root CA	General Device Root CA	802.1x CA Certificate	Normal	⬇	🗑

Step 4 Click **OK**.

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

Related Operations

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

9.5. Encryption

The device supports audio and video encryption during data transmission.

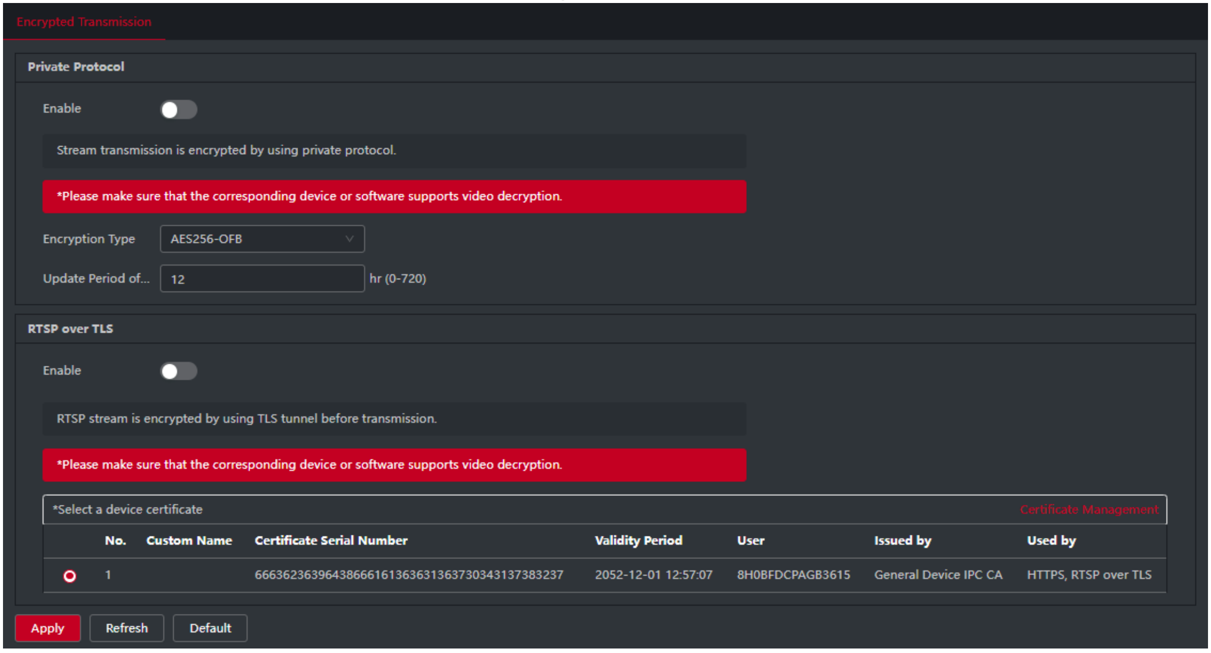
⚠

We recommend you enable A/V Encryption function. There might be safety risk if this function is disabled.

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

Step 2 Configure the parameters.

Figure 9-14



Encrypted Transmission

Private Protocol

Enable

Stream transmission is encrypted by using private protocol.

*Please make sure that the corresponding device or software supports video decryption.

Encryption Type: AES256-OFB

Update Period of...: 12 hr (0-720)

RTSP over TLS

Enable

RTSP stream is encrypted by using TLS tunnel before transmission.

*Please make sure that the corresponding device or software supports video decryption.

*Select a device certificate Certificate Management

	No.	Custom Name	Certificate Serial Number	Validity Period	User	Issued by	Used by
○	1		66636236396438666161363631363730343137383237	2052-12-01 12:57:07	8H0BFDCPAGB3615	General Device IPC CA	HTTPS, RTSP over TLS

Table 52

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption byusing private protocol. 📖 There might be safety risk if thisservice is disabled.
	Encryption Type	Use the default setting.

Area	Parameter	Description
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption byusing TLS. 📖 There might be safety risk if thisservice is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	

Step 3 Click **Apply**.

9.6. Security Warning

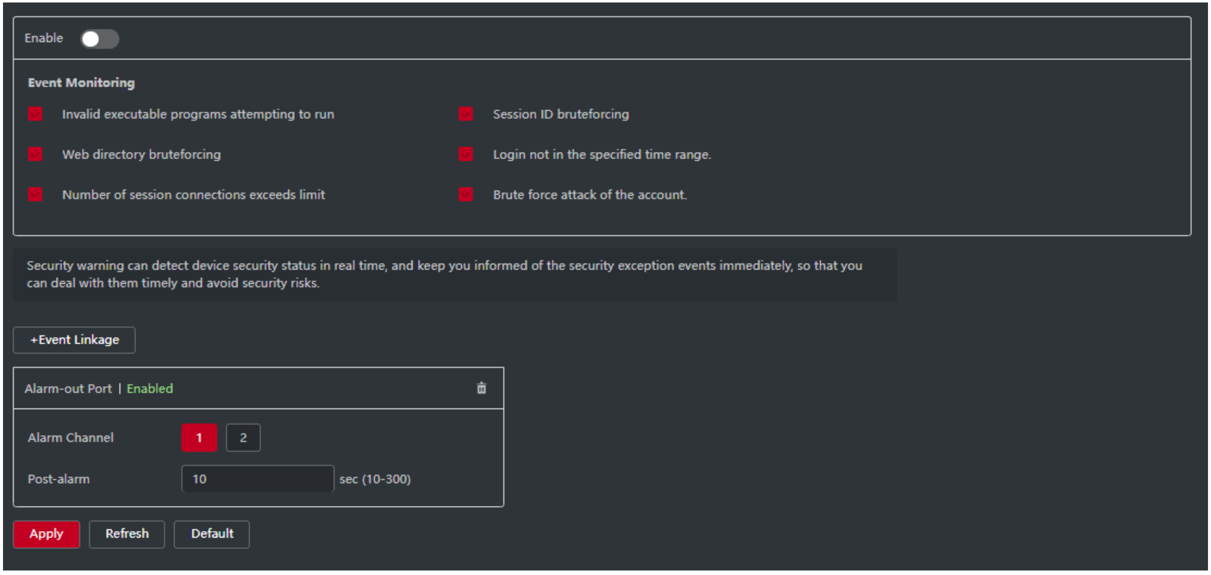
When security exception event is detected, the camera sends a warning to remind you to process ittimely, to avoid security risk.

Step 1 Select **Security → Security Warning**.

Step 2 Click ○ to enable security warning.

Step 3 Configure the parameters.

Figure 9-15



Enable ○

Event Monitoring

- ☑ Invalid executable programs attempting to run
- ☑ Web directory bruteforcing
- ☑ Number of session connections exceeds limit
- ☑ Session ID bruteforcing
- ☑ Login not in the specified time range.
- ☑ Brute force attack of the account.

Security warning can detect device security status in real time, and keep you informed of the security exception events immediately, so that you can deal with them timely and avoid security risks.

+Event Linkage

Alarm-out Port | Enabled

Alarm Channel: 1 2

Post-alarm: 10 sec (10-300)

Step 4 Set arming periods and alarm linkage action. Click **+ Event Linkage** to set the linkage action.

Step 5 Click **Apply**.

10. Report

View the statistics result of video metadata in report form.

Procedure

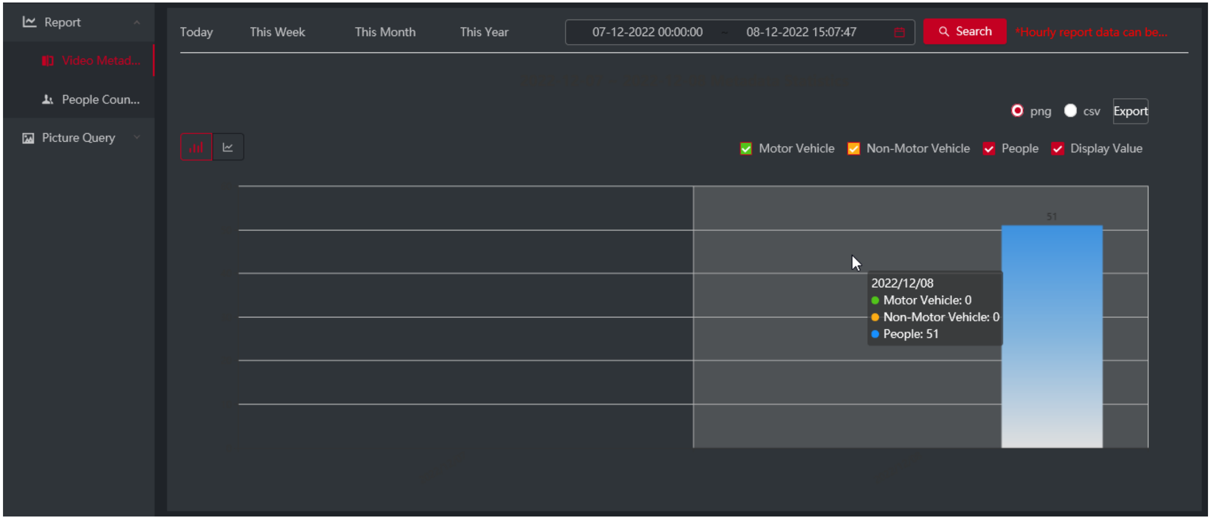
Step 1 Click **Report → Report → Video Metadata**.

Step 2 Set the period for the report.

For multi-channel camera, select the channel first.

Step 3 Click **Search**.

Figure 10-1



07-12-2022 00:00:00 – 08-12-2022 15:07:47

☑ Motor Vehicle ☑ Non-Motor Vehicle ☑ People ☑ Display Value

● png ○ csv

2022/12/08
Motor Vehicle: 0
Non-Motor Vehicle: 0
People: 51

Related Operations

- Select the report form.
  - Click to display the report in line chart.
  - Click to display the report in bar chart.
- Select the statistics type on the upper-right corner.

The statistics result of unselected types will not be displayed.

- Export reports.

Select the file format, and then click **Export**.

  - Select **png**: Displays the report in image format.
  - Select **csv**: Displays the report in list format.

11. Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more securedsecurity system.

Mandatory actions to be taken for basic equipment network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper- and lower-case letters,numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend keeping your equipment (such as NVR, DVR, IP camera, etc.) firmware up to date to ensure the system is equipped with the latest security patches and fixes. When the equipment is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

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

a. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. Forexample, place the equipment in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnelfrom carrying out physical contacts such as damaging hardware, unauthorized connection ofremovable equipment (such as USB flash disk, serial port), etc.

b. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

c. Set and Update Passwords Reset Information Timely

The equipment supports password reset function. Please set up related information for passwordreset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

d. Enable Account Lock

The account lock feature is enabled by default, and we recommend you keep it on to guarantee the account security.

If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

e. Change Default HTTP and Other Service Ports

We suggest you change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

f. Enable HTTPS

We suggest you enable HTTPS, so that you visit Web service through a secure communicationchannel.

g. MAC Address Binding

We recommend you bind the IP and MAC address of the gateway to the equipment, thusreducing the risk of ARP spoofing.

h. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

i. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
If necessary, it is highly recommended that you use safe modes, including but not limited to thefollowing services:

- SNMP: Choose SNMP v3 and set up strong encryption passwords and authenticationpasswords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode and set up strong passwords.

j. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
Reminder: encrypted transmission will cause some loss in transmission efficiency.

k. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used tolog in to your devices and their key operations.

l. Network Log

Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

m. Construct a Safe Network Environment

In order to better ensure the safety of equipment and reduce potential cyber risks, werecommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devicesfrom external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to useVLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

Thanks for Choosing CP Plus!

CP PLUS

Website: - www.cpplusworld.com

Email id: - sales@cpplusworld.com; support@cpplusworld.com